Riverstone Configuration Database Support Page

The configuration database is a collection of short documents that quickly explain how to configure a specific feature by providing a diagram, the complete configurations, and commentary.

It is intended to be a repository of common knowledge and should be used as a supplement to the product manuals.

- **BGP**
  - Basic BGP With Route Maps
  - Basic Route Reflection
  - Bogon Filtering With BGP
  - Peering with Multiple BGP Peers Using Zebra
  - Secure BGP Configuration
  - Cisco to Riverstone BGP Translation Example
  - Providing Transit With EBGP Without IBGP in the ISPs Core

- **Interface Configurations**

  ATM
  - ATM Based Metro TLS
  - ATM Cross-connects
  - ATM Interoperability with Alcatel Routers
  - ATM Interoperability with Cisco Routers
  - ATM Interoperability with Zeitnet ATM Switches
  - ATM Point-Multipoint over Multiple PVCs
  - L4 Quality of Service Mappings to VC's in ATM
  - Interoperability with Cisco DS3 ATM
  - L2 Bridging over ATM

  CWDM
  - CWDM Interoperability with Extreme

  Ethernet
  - Link Aggregation 802.3ad
  - 802.3ad Interoperability with Juniper

  POS
  - POS Interoperability with Cisco
  - POS Bridged Configuration
  - OSPF over POS Interoperability with Juniper
  - OC12 Interoperability With Extreme
  - POS APS

  Serial
  - Interoperability with Cisco HDLC
  - CT3 Interoperability with Cisco T1
  - Multirate WAN: T1/MLP and T3 to Juniper
  - IP Unnumbered between Cisco and RS
  - Spanning Tree Over Frame Relay
  - Basic PPP Configuration on Channelized T1
  - Riverstone CT3 to Cisco CT3

- **IS-IS**
  - IS-IS Interoperability with Cisco

- **Layer 2**
  - Extending an L2 Domain with Ring STP and GVRP
  - Using L2 Filters To Enable Private VLANs Within A Single RS
  - Using L2 Filters To Enable Private VLANs Discrete Layer 2 Aggregation
  - Point-to-Point VLANs over Ethernet, ATM and T1
  - Stackable VLANs - Tunneling Across the Metro
  - Smarttrunks with L4 Bridging and 802.1Q
  - VLAN Translation
  - Stackable VLANs Example
  - Native VLAN Configurations

- **MPLS**
  - MPLS LSPs with Cisco LER using RSVP
  - MPLS LSPs with Cisco LSR using RSVP
  - LDP over LDP Martini Interoperability with Juniper
  - LDP tunneling over RSVP with Riverstone LERs and Juniper LSRs
  - Using LDP Labels For Non-/32 Networks
  - MPLS & IBGP Full Mesh
  - MPLS Martini Tunnels with Avici
  - MPLS Service Levels
  - Martini port/vlan l2-fec Configurations
  - LDP over LDP Martini Interoperability with Juniper - Using Port FEC
  - LDP over LDP Martini Interoperability with Juniper - Using VLAN FEC
  - Multi-VRF Support With BGP/VPNs
  - BGP/VPNs With Different CE-PE Protocols at Different Sites
  - L2 VPNs Over a L3 VPN Core

  - **VPLS Configuration Series**
    - Extending "Virtual Switch" Domains
    - Port Based "Virtual Switch" Configuration
    - VLAN Based "Virtual Switch" Configuration
    - L2 Extranet Configuration

- **Multicast**
  - PIM-SM configuration with RP & BSR
  - PIM-SM interoperability with a Cisco RP & BSR

- **Network Management**
  - Basic Remote Syslog Configuration
  - Cistron RADIUS Configuration
  - Configuring User Authentication and Accounting with Livingston RADIUS
  - LFAP Configuration
  - "MICA" Accounting Server Setup
  - Quick Tricks with RMON2
  - Remote TFTP Config Backup
  - Remote RS Management Through a Modem Connected to the RS Console Port
  - Basic TACACS+ Configuration
  - Basic SNMP and Trap Configuration

- **NAT/LSNAT**
  - NAT Dynamic Port Overload
  - NAT Dynamic Port Overload using the Loopback Address
  - TFTP Server Load-Balancing

- **OSPF**
  - OSPF for VoIP Media Gateway & Signaling Gateway Redundancy

- **Policy Based Routing**
  - Policy Based Routing, Traffic Engineering & Recursive Lookup
  - IP-Routing Policy to Work as Cisco IP Default-Network Command

- **QoS**

- L2 QOS Weighted Fair Queuing

- **Rate Limiting/Rate Shaping**
  - Aggregate Rate Limit on L2 Architecture with ML-PPP and .1Q over WAN Links
  - Poking Holes Through Rate-limiting
  - WAN Rate Shaping with NATing Loopback Interfaces

- **Security**
  - Secure ROS Configuration
  - Building the ARP Table from DHCP

- **VRRP**
  - VRRP, Load Distribution & IP Backup

Basic BGP With Route Maps

Richard Foote
Corporate Systems Engineering
July 24, 2001

Route-maps provide a very power tool for manipulating the characteristics of an imported route. It is a very elegant way to influence how the selection of prefixes occurs in the BGP. This is a simple configuration that demonstrates how one autonomous system, AS20, can apply local policy to the learned routes from an external autonomous system, AS10.

AS10 has many secondary interfaces added to the 'AS-10Nets' interface to simulate the existence of many prefixes in the internet. The AS10-2 switch is configured with a ".254" IP Address on each of the subnets AS10 is announcing to AS20. These ".254" addresses are meant to simulate hosts. Closer examination of these prefixes reveal the ability to summarize them into three /22 aggregates.

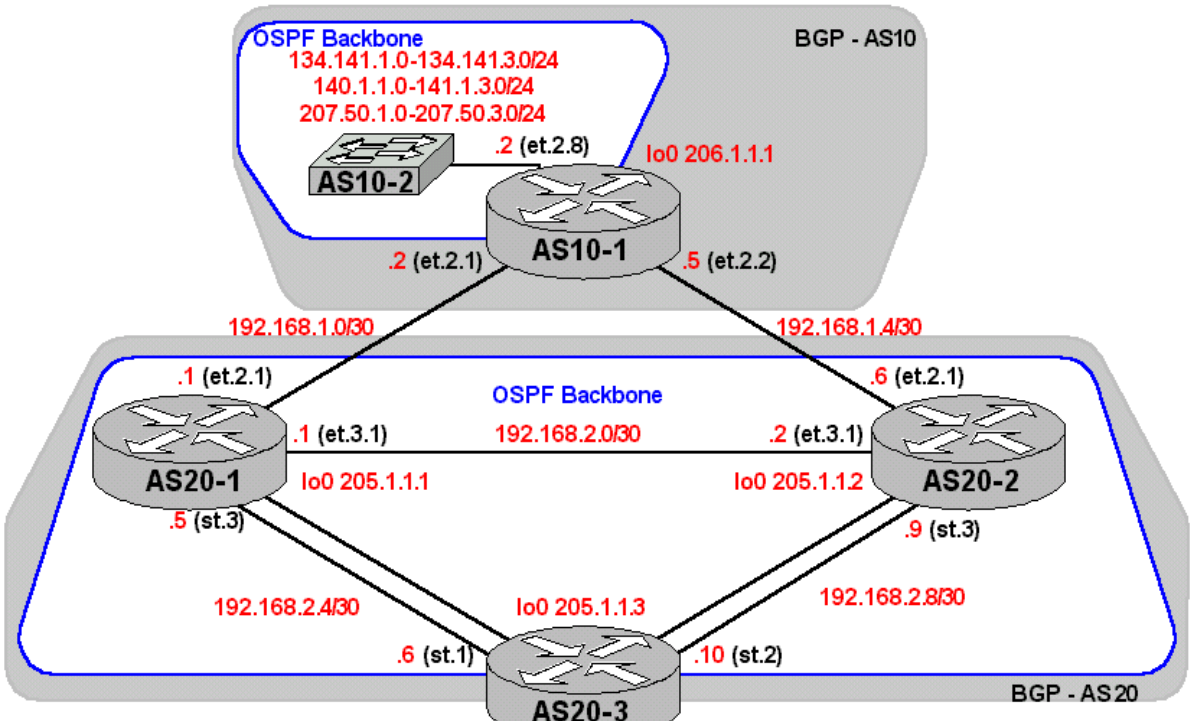
AS20 is comprise of a two EBGP peering relationship with AS10, and for perspective some PCs have been included where customer routers typically would have been found. This allows AS20 to treat these customers as subscribers and inject those routes into AS10. The configuration required to connect actual customer routers is not shown. However, it is assumed that some customers would like a complete Internet routing table (hence the requirement to run IBGP throughout the entire AS) and other customer needs would be simply a default static route.

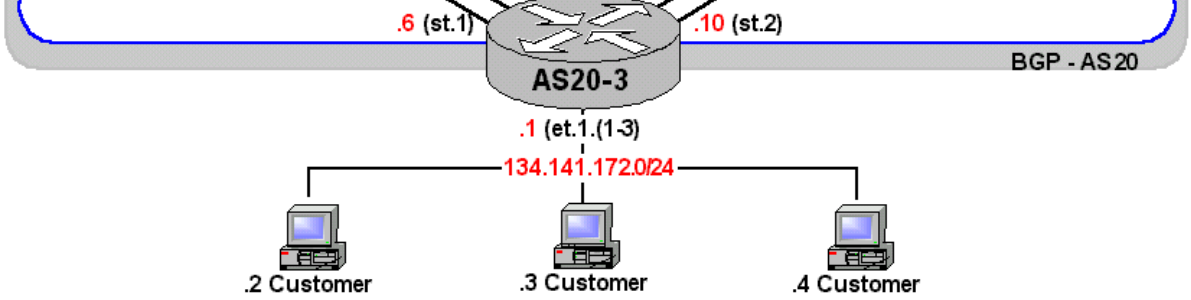
Other interesting aspects of the configuration will cover "next-hop-self", summarization, redistribution and as a point of interest, although not discussed here, 802.3ad Link Aggregation has been configured between the AS20-1 <=> AS20-3 and AS20-2 <=> AS20-3 routers. Seemed like a good thing to do :-).

Things that are not discussed here include, but are not limited to, Bogons/Martians, Service ACLs, flow-mode modifications from default, ingress filtering and all those other things done when you don't trust your Internet peers.

RapidOS Version Tested	7.0.0.3
RapidOS Versions Working with this Configuration	5.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 5.1.0.0
Hardware Specifics	N/A

Diagram





Configurations

AS10-1

```
version 7.0
interface create ip BGP-To20 address-netmask 192.168.1.2/30 port et.2.1
interface create ip AS-10Nets address-netmask 207.50.1.2/24 port et.2.8
interface create ip BGP-To20B address-netmask 192.168.1.5/30 port et.2.2
interface add ip en0 address-netmask 24.112.73.4/21
interface add ip AS-10Nets address-netmask 207.50.2.2/24
interface add ip AS-10Nets address-netmask 207.50.3.2/24
interface add ip AS-10Nets address-netmask 134.141.1.2/24
interface add ip AS-10Nets address-netmask 134.141.2.2/24
interface add ip AS-10Nets address-netmask 134.141.3.2/24
interface add ip AS-10Nets address-netmask 140.1.1.2/24
interface add ip AS-10Nets address-netmask 140.1.2.2/24
interface add ip AS-10Nets address-netmask 140.1.3.2/24
interface add ip lo0 address-netmask 10.1.1.1
interface add ip lo0 address-netmask 206.1.1.1
ip-router global set autonomous-system 10
ip-router global set router-id 206.1.1.1
ip-router policy redistribute from-proto aggregate to-proto bgp target-as 20
ospf create area backbone
ospf add interface AS-10Nets to-area backbone
ospf add stub-host 10.1.1.1 to-area backbone cost 10
ospf start
bgp create peer-group South type external autonomous-system 20
bgp add peer-host 192.168.1.1 group South
bgp add peer-host 192.168.1.6 group South
bgp start
system set name AS10-1
ip-router policy summarize route 207.50.0.0/22
ip-router policy summarize route 134.141.0.0/22
ip-router policy summarize route 140.1.0.0/22
```

AS10-2

```
version 3.1
vlan create Hosts ip id 100
interface create ip AS-10Hosts address-netmask 207.50.1.254/24 vlan Hosts
interface add ip AS-10Hosts address-netmask 207.50.2.254/24
interface add ip AS-10Hosts address-netmask 207.50.3.254/24
interface add ip AS-10Hosts address-netmask 134.141.1.254/24
interface add ip AS-10Hosts address-netmask 134.141.2.254/24
interface add ip AS-10Hosts address-netmask 134.141.3.254/24
interface add ip AS-10Hosts address-netmask 140.1.1.254/24
interface add ip AS-10Hosts address-netmask 140.1.2.254/24
interface add ip AS-10Hosts address-netmask 140.1.3.254/24
ip add route default gateway 207.50.1.2
system set name AS10-2
```

AS20-1

```
version 7.0
smarttrunk create st.3 protocol lacp
lacp set aggregator st.3 actor-key 13 partner-key 31 port-type 10-100-ethernet
lacp set port et.2.(7-8) port-key 13 enable
interface create ip BGP-To10 address-netmask 192.168.1.1/30 port et.2.1
interface create ip To20112 address-netmask 192.168.2.1/30 port et.3.1
interface create ip To205113 port st.3 address-netmask 192.168.2.5/30
interface add ip en0 address-netmask 24.112.73.3/21
interface add ip lo0 address-netmask 205.1.1.1
ip-router global set autonomous-system 20
ip-router global set router-id 205.1.1.1
ip-router policy redistribute from-proto bgp to-proto bgp target-as 20 source-as 10
ip-router policy redistribute from-proto ospf-ase to-proto bgp network
134.141.172.0/24
exact target-as 10
ospf create area backbone
```

```
ospf add stub-host 205.1.1.1 to-area backbone cost 10
ospf add interface To205113 to-area backbone
ospf add interface To20112 to-area backbone
ospf add stub-host 192.168.1.1 to-area backbone cost 10
ospf set interface To20112 priority 200
ospf start
bgp create peer-group North type external autonomous-system 10
bgp create peer-group Internal autonomous-system 20 proto ospf type routing
bgp add peer-host 192.168.1.2 group North
bgp add peer-host 205.1.1.2 group Internal
bgp add peer-host 205.1.1.3 group Internal
bgp set peer-group North route-map-in Backup in-sequence 10
bgp set peer-group Internal local-address 205.1.1.1
bgp set peer-group Internal next-hop-self
bgp start
system set name AS20-1
route-map Backup permit 10 match-prefix network 207.50.0.0/22 set-local-preference
100
route-map Backup permit 20 match-prefix network 134.141.0.0/22 set-local-preference
100
route-map Backup permit 30 match-prefix network 0.0.0.0/0.0.0.0 set-local-preference
150
```

AS20-2

```
version 7.0
smarttrunk create st.3 protocol lacp
lacp set aggregator st.3 actor-key 23 partner-key 32 port-type 10-100-ethernet
lacp set port et.2.(7-8) port-key 23 enable
interface create ip To20111 address-netmask 192.168.2.2/30 port et.3.1
interface create ip BGP-To10 address-netmask 192.168.1.6/30 port et.2.1
interface create ip To205113 address-netmask 192.168.2.9/30 port st.3
interface add ip en0 address-netmask 24.112.73.5/21
interface add ip lo0 address-netmask 205.1.1.2
ip-router global set autonomous-system 20
ip-router global set router-id 205.1.1.2
ip-router policy redistribute from-proto bgp to-proto bgp source-as 10 target-as 20
ip-router policy redistribute from-proto ospf-ase to-proto bgp network
134.141.172.0/24
exact target-as 10
ospf create area backbone
ospf add interface To20111 to-area backbone
ospf add stub-host 205.1.1.2 to-area backbone cost 10
ospf add interface To205113 to-area backbone
ospf add stub-host 192.168.1.6 to-area backbone cost 1
ospf set interface To20111 priority 100
ospf start
bgp create peer-group North type external autonomous-system 10
bgp create peer-group Internal type routing autonomous-system 20 proto ospf
bgp add peer-host 192.168.1.5 group North
bgp add peer-host 205.1.1.1 group Internal
bgp add peer-host 205.1.1.3 group Internal
bgp set peer-group North route-map-in Backup in-sequence 10
bgp set peer-group Internal local-address 205.1.1.2
bgp set peer-group Internal next-hop-self
bgp start
system set name AS20-2
route-map Backup permit 10 match-prefix network 207.50.0.0/22 set-local-preference
150
route-map Backup permit 20 match-prefix network 134.141.0.0/22 set-local-preference
150
route-map Backup permit 30 match-prefix network 0.0.0.0/0.0.0.0 set-local-preference
100
```

AS20-3

```
version 7.0
smarttrunk create st.1 protocol lacp
smarttrunk create st.2 protocol lacp
lacp set aggregator st.1 actor-key 31 partner-key 13 port-type 10-100-ethernet
lacp set aggregator st.2 actor-key 32 partner-key 23 port-type 10-100-ethernet
lacp set port et.1.(7-8) port-key 31 enable
lacp set port et.2.(7-8) port-key 32 enable
vlan create Customer ip id 2000
vlan add ports et.1.(1-3) to Customer
interface create ip To205111 address-netmask 192.168.2.6/30 port st.1
interface create ip To205112 address-netmask 192.168.2.10/30 port st.2
interface create ip Customer address-netmask 134.141.172.1/24 vlan Customer
interface add ip lo0 address-netmask 205.1.1.3
interface add ip en0 address-netmask 24.112.73.2/21
ip-router global set router-id 205.1.1.3
ip-router global set autonomous-system 20
ip-router policy redistribute from-proto direct to-proto ospf network
```

```
134.141.172.0/24 exact
ospf create area backbone
ospf add stub-host 205.1.1.3 to-area backbone cost 10
ospf add interface To205111 to-area backbone
ospf add interface To205112 to-area backbone
ospf start
bgp create peer-group Internal type routing proto ospf autonomous-system 20
bgp add peer-host 205.1.1.1 group Internal
bgp add peer-host 205.1.1.2 group Internal
bgp set peer-group Internal local-address 205.1.1.3
bgp start
system set name AS20-3
```

Comments

Using the "`ip show route`" command from each of the routers shows the preferred routes and how they were derived. The forwarding table on router AS20-3 looks like this.

```
AS20-3# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
24.112.72.0/21       directly connected   -         en0
127.0.0.1            127.0.0.1            -         lo0
134.141.0.0/22       192.168.2.9          BGP       To205112
134.141.172.0/24     directly connected   -         Customer
140.1.0.0/22         192.168.2.5          BGP       To205111
192.168.1.1          192.168.2.5          OSPF      To205111
192.168.1.6          192.168.2.9          OSPF      To205112
192.168.2.0/30       192.168.2.5          OSPF      To205111
                     192.168.2.9          OSPF      To205112
192.168.2.4/30       directly connected   -         To205111
192.168.2.8/30       directly connected   -         To205112
205.1.1.1            192.168.2.5          OSPF      To205111
205.1.1.2            192.168.2.9          OSPF      To205112
205.1.1.3            205.1.1.3            -         lo0
207.50.0.0/22        192.168.2.9          BGP       To205112
```

The interfaces that have been added to the OSPF backbone using the "`ospf add interface <name> to-area backbone`" command have a stated "`Owner`" of "`OSPF`". Routes that have been learned from the BGP process have an "`Owner`" of "`BGP`". Since the view of the routing table is from an IBGP peer, the BGP route injection would have been accomplished with the "`ip-router policy redistribute from-proto bgp to-proto bgp source-as 10 target-as 20`" on routers AS20-1 and AS20-2.

Being a good Internet citizen, the EBGP peer in AS10, router AS10-1, advertises summary routes for all the networks it exports to AS20. Being a great Internet citizen would have meant not advertising any prefixes longer than a /19 or /20 but a /22 is good enough for our example here. The summary commands are ...

```
ip-router policy redistribute from-proto aggregate to-proto bgp target-as 20
ip-router policy summarize route 207.50.0.0/22
ip-router policy summarize route 134.141.0.0/22
ip-router policy summarize route 140.1.0.0/22
```

Also since the EBGP peer in AS10 will treat both peers in AS20 the same a "`peer-group`" is created with both the AS20 routers in it, to establish the EBGP communication. The "`type external`" means that the peers are directly connected through a local interface and is the typical setting for establishing an EBGP peering session.

```
bgp create peer-group South type external autonomous-system 20
bgp add peer-host 192.168.1.1 group South
bgp add peer-host 192.168.1.6 group South
bgp start
```

In order to verify the state of each neighbor various show commands are useful. When using the "`bgp show neighbor all`" command pay particular attention to the "State" of the peer. This indicates which phase of the BGP State machine the peers have reached.

```
AS10-1# bgp show neighbor all
        Peer: 192.168.1.1+179   Local: 192.168.1.2+1028 Type: External   remoteAS
        State: Established      Flags: <GenDefault>
        Last State: OpenConfirm Last Event: RecvKeepAlive       Last Error: None
        Options: <>
        Configured parame :
        Used parameters :
        Peer Version: 4 Peer ID: 205.1.1.1      Local ID: 206.1.1.1     Active
Holdtime: 180
        Uptime 0d0h34m11s
        Last traffic (seconds): Received 37     Sent 11 Checked 11
        Input messages: Total 35        Updates 1       Octets 691
        Output messages:        Total 38        Updates 1       Octets 766
          count of sent routes 3

        Peer: 192.168.1.6+179   Local: 192.168.1.5+1027 Type: External   remoteAS
        State: Established      Flags: <GenDefault>
        Last State: OpenConfirm Last Event: RecvKeepAlive       Last Error: None
        Options: <>
        Configured parame :
        Used parameters :
        Peer Version: 4 Peer ID: 205.1.1.2      Local ID: 206.1.1.1     Active
Holdtime: 180
```

```
        Uptime 0d0h34m15s
        Last traffic (seconds): Received 58     Sent 15 Checked 15
        Input messages: Total 36        Updates 3       Octets 744
        Output messages:        Total 38        Updates 1       Octets 766
          count of sent routes 3
```

If we were to stop the BGP process on router AS20-1 by commenting out the "`bgp start`" line in the configuration the pervious display would indicate a different "`State`" for this peer.

```
AS10-1# bgp show neighbor 192.168.1.1
        Peer: 192.168.1.1+179   Local: 192.168.1.2      Type: External   remoteAS
        State: Active   Flags: <>
        Last State: Idle        Last Event: Start       Last Error: None
        Options: <>
        Configured parame :
        Used parameters :
          count of sent routes 0
```

AS20-1 and AS20-2 routers should obviously be filtering what they receive from the EBGP peers. However, in our example there is an incredible amount of trust between these two autonomous systems. Trust that exists nowhere else in the Internet. Trust me :-).

The AS20 routers establish an EBGP peering session with the AS10-1 router, in the same fashion as the AS10 router did for AS20. However, the interface that directly links the AS20 routers with the AS10 router are not included in the OSPF backbone. It is very important not to run an IGP routing protocol between EBGP peers. It is imperative though, that all nodes needing to reach routes advertised by the AS10 router understand how to reach them in an optimal fashion. There are many ways to do this, including static routes or default routes, or as was done here, IBGP. Remember, when using the command "`ip-router policy redistribute from-proto bgp to-proto bgp source-as 10 target-as 20`" on the AS20 routers to inject the imported routes from AS10 into the IBGP nodes in AS20 the next hop is that of the remote EBGP peer. To resolve the reachability issue the AS20 routers that redistribute imported BGP routes into the IBGP modify the next hop using ...

```
bgp set peer-group Internal next-hop-self
```

Checking the BGP routes on the AS20 routers we will be able to spot some interesting differences. On the EBGP peers in AS20 peering with AS10,the BGP routes have two distinct differences. The BGP routes that were learned across the direct local connection between the EBGP peers shows the "`Next-Hop`" to be that of the remote peer interface. Take for example AS20-1, it knows it can reach the 134.141/22, the 140.1/22 and the 207.50/22 networks directly, using the 192.168.1.2 interface, the AS10-1 router. Similarly, AS20-2 knows it has direct reachability to those same networks using its direct local connection to 192.168.1.5, the AS10-1 router. Ignore for a moment that multiple routes exist for some of the networks with different local preferences.

```
AS20-1# bgp show routes all
BGP table : Local router ID is 205.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network      Next Hop     Metric LocPrf Path
  -------      --------     ------ ------ ----
*>134.141/22   205.1.1.2            150 10 i
* 134.141/22   192.168.1.2          100 10 i
*>140.1/22     192.168.1.2          150 10 i
*>207.50/22    205.1.1.2            150 10 i
* 207.50/22    192.168.1.2          100 10 i
```

```
AS20-2# bgp show routes all
BGP table : Local router ID is 205.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network    Next Hop   Metric LocPrf Path
  -------    --------   ------ ------ ----
*>134.141/22 192.168.1.5          150 10 i
*>140.1/22   205.1.1.1            150 10 i
* 140.1/22   192.168.1.5          100 10 i
*>207.50/22  192.168.1.5          150 10 i
```

Before we look at the same command executed on AS20-3, an IBGP full mesh was created by configuring a common peer-group "Internal" on all the routers that required the BGP information. The "`type routing`" allows an IGP to resolve the forwarding addresses. The "`local-address`" coded as part of the peer-group set options indicates what IP address to use on the router for TCP establishment.

AS20-1

```
bgp create peer-group Internal autonomous-system 20 proto ospf type routing
bgp add peer-host 205.1.1.2 group Internal
bgp add peer-host 205.1.1.3 group Internal
bgp set peer-group Internal local-address 205.1.1.1
```

AS20-2

```
bgp create peer-group Internal type routing autonomous-system 20 proto ospf
bgp add peer-host 205.1.1.1 group Internal
bgp add peer-host 205.1.1.3 group Internal
bgp set peer-group Internal local-address 205.1.1.2
```

AS20-2

```
bgp create peer-group Internal type routing proto ospf autonomous-system 20
bgp add peer-host 205.1.1.1 group Internal
bgp add peer-host 205.1.1.2 group Internal
bgp set peer-group Internal local-address 205.1.1.3
```

Now, if we look at the same display out put on AS20-3 we see a different yet expected result. The first thing to notice is the "`Next Hop`" indicator points to the router-id of the router that injected the route into the IBGP mesh. This is the result of using the "`bgp set peer-group Internal next-hop-self`" command.

```
AS20-3# bgp show routes all
BGP table : Local router ID is 205.1.1.3
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network           Next Hop        Metric LocPrf Path
  -------           --------        ------ ------ ----
*>134.141/22        205.1.1.2              150 10 i
```

```
*>140.1/22           205.1.1.1                150 10 i
*>207.50/22          205.1.1.2                150 10 i
```

The routing table has installed the BGP routes according to the BGP table.

```
AS20-3# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
24.112.72.0/21       directly connected   -         en0
127.0.0.1            127.0.0.1            -         lo0
134.141.0.0/22       192.168.2.9          BGP       To205112
134.141.172.0/24     directly connected   -         Customer
140.1.0.0/22         192.168.2.5          BGP       To205111
192.168.1.1          192.168.2.5          OSPF      To205111
192.168.1.6          192.168.2.9          OSPF      To205112
192.168.2.0/30       192.168.2.5          OSPF      To205111
                     192.168.2.9          OSPF      To205112
192.168.2.4/30       directly connected   -         To205111
192.168.2.8/30       directly connected   -         To205112
205.1.1.1            192.168.2.5          OSPF      To205111
205.1.1.2            192.168.2.9          OSPF      To205112
205.1.1.3            205.1.1.3            -         lo0
207.50.0.0/22        192.168.2.9          BGP       To205112
```

The next noticeable difference is the fact there is only one BGP entry for each of the BGP injected networks. Not to mention the fact that these networks have the highest local preference. To understand this a quick review of IBGP is require. The BGP protocol only allows BGP peers to announce the route that has installed in the forwarding information base, or FIB. IBGP rules also state that a router may not re-announce a route learned form an IBGP peer. This explains why, we have this type of difference between the three routers in AS20.

AS20-1 & AS20-2 learn the BGP routes directly from the EBGP peer in AS10. These routes are all entered into the BGP Import database. Also, notice that these routers have more than one route to the same BGP destination network. You know, the thing I told you to ignore earlier. These additional routes have been injected into the IBGP as preferred routes.

Take the example on AS20-1, BGP route 134.141/22. It was learned via EBGP and installed with the default "`LocPrf`" or local preference of 100 and a "`Next Hop`" of 192.168.1.2, the remote EBGP interface in AS10. The route was also learned via IBGP from the router 205.1.1.2 with a preferred local preference of 150. The route with the higher local preference is select for inclusion in the FIB.

The BGP route of 140.1/22 only has a single entry on AS20-1. This is because the route it learned from the EBGP neighbor had the best local preference and it advertised its route for 140.1/22 to AS20-2. AS20-2 has two routes to 140.1/22 for the same reason explained earlier.

```
AS20-1# bgp show routes all
BGP table : Local router ID is 205.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network      Next Hop     Metric LocPrf Path
  -------      --------     ------ ------ ----
*>134.141/22   205.1.1.2            150 10 i
* 134.141/22   192.168.1.2          100 10 i
*>140.1/22     192.168.1.2          150 10 i
*>207.50/22    205.1.1.2            150 10 i
* 207.50/22    192.168.1.2          100 10 i
```

```
AS20-2# bgp show routes all
BGP table : Local router ID is 205.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network    Next Hop   Metric LocPrf Path
  -------    --------   ------ ------ ----
*>134.141/22 192.168.1.5          150 10 i
*>140.1/22   205.1.1.1            150 10 i
* 140.1/22   192.168.1.5          100 10 i
*>207.50/22  192.168.1.5          150 10 i
```

```
AS20-1# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
24.112.72.0/21       directly connected   -         en0
127.0.0.1            127.0.0.1            -         lo0
134.141.0.0/22       192.168.2.2          BGP       To20112  Route to 205.1.1.2 -
best LocPrf
134.141.172.0/24     192.168.2.6          OSPF_ASE  To205113
140.1.0.0/22         192.168.1.2          BGP       BGP-To10 Route to EBGP directly
192.168.1.0/30       directly connected   -         BGP-To10
192.168.1.6          192.168.2.2          OSPF      To20112
192.168.2.0/30       directly connected   -         To20112
192.168.2.4/30       directly connected   -         To205113
192.168.2.8/30       192.168.2.2          OSPF      To20112
                     192.168.2.6          OSPF      To205113
205.1.1.1            205.1.1.1            -         lo0
205.1.1.2            192.168.2.2          OSPF      To20112
205.1.1.3            192.168.2.6          OSPF      To205113
207.50.0.0/22        192.168.2.2          BGP       To20112  Route to 205.1.1.2 -
best LocPrf
```

How did these local reference values get set? Using route-maps on AS20-1 & AS20-2. The route maps of AS20-1 explicitly set the 207.50.0.0/22 and 134.141.0.0/22 to the default 100, with all other routes received from the EBGP peer-group "North" set to 150.

AS20-1

```
bgp set peer-group North route-map-in Backup in-sequence 10
route-map Backup permit 10 match-prefix network 207.50.0.0/22 set-local-preference
100
route-map Backup permit 20 match-prefix network 134.141.0.0/22 set-local-preference
100
```

```
route-map Backup permit 30 match-prefix network 0.0.0.0/0.0.0.0 set-local-preference
150
```

Similarly, AS20-2 applies a local preference of 150 explicitly to 207.50.0.0/22 and 134.141.0.0/22, with all other router received from the EBGP peer-group "North" set to 100.

AS20-2

```
bgp set peer-group North route-map-in Backup in-sequence 10
route-map Backup permit 10 match-prefix network 207.50.0.0/22 set-local-preference
150
route-map Backup permit 20 match-prefix network 134.141.0.0/22 set-local-preference
150
route-map Backup permit 30 match-prefix network 0.0.0.0/0.0.0.0 set-local-preference
100
```

Remembering the IBGP rule, never advertise a route learned through IBGP to other IBGP neighbors. This allows us to understand the bgp route on AS20-3.

```
AS20-3# bgp show routes all
BGP table : Local router ID is 205.1.1.3
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop        Metric LocPrf Path
  -------            --------        ------ ------ ----
*>134.141/22         205.1.1.2                150 10 i
*>140.1/22           205.1.1.1                150 10 i
*>207.50/22          205.1.1.2                150 10 i
```

What if the IBGP full mesh were not complete. For example, consider for a moment AS20-2 did not have an IBGP peering relationship with AS20-3 yet had a successfully established an IBGP peering relationship with AS20-1. This can simply be accomplished by commenting out the "`bgp add peer-host 205.1.1.3 group Internal`" command on AS20-2. Once this is done check the BGP routes on AS20-3.

```
AS20-3# bgp show routes all
BGP table : Local router ID is 205.1.1.3
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop        Metric LocPrf Path
  -------            --------        ------ ------ ----
*>140.1/22           205.1.1.1                150 10 i
```

The only route redistributed to AS20-3 would be the only route that AS20-1 has determined it has the best route for. Since AS20-1 maintains a peering relationship with AS20-2 it receives better route information, higher local preference, from another router for the other two aggregates. Therefore, AS20-1 is not allowed to forward this routing information to AS20-3. It is the responsibility of AS20-2 to inform everyone in the IBGP mesh of its best routes. Since there is no IBGP peering relationship between AS20-2 and AS20-3, well, the router can't redistribute the routes to AS20-3 and no one else can either. Route Reflectors and Confederation eliminate the need for and IBGP full mesh but are outside the scope of this document (or it will never end).

Re-establishing the IBGP full mesh, the network is in a steady state of operation. All the routes have been imported, manipulated and redistributed from AS10 to AS20. The advertisement of the AS20 networks must now be forwarded to AS10.

Consider that AS20 has a single subnet to advertise to the world, 134.141.172.0. By simply redistributing the directly connected routes on AS20-3 and the further redistributing the ospf-ase routes on AS20-1 & AS20-2 into AS10 the advertisement is complete.

AS20-3

```
ip-router policy redistribute from-proto direct to-proto ospf network
134.141.172.0/24 exact
```

AS20-2

```
ip-router policy redistribute from-proto ospf-ase to-proto bgp network
134.141.172.0/24 exact target-as 10
```

AS20-1

```
ip-router policy redistribute from-proto ospf-ase to-proto bgp network
134.141.172.0/24 exact target-as 10
```

Looking at the BGP routing table and the IP forwarding tables for AS10-1 we notice the route has been installed with two possible paths to the destination.

```
AS10-1# bgp show routes all
BGP table : Local router ID is 206.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop        Metric LocPrf Path
  -------            --------        ------ ------ ----
*>134.141.172/24     192.168.1.1                20 i
* 134.141.172/24     192.168.1.6                20 I
```

Looking at the BGP routing table, the bgp summary information and the IP forwarding tables for AS10-1 we notice the route has been installed with two possible paths to the destination.

```
AS10-1# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
```

```
10.1.1.1            10.1.1.1            -         lo0
24.112.72.0/21      directly connected  -         en0
127.0.0.1           127.0.0.1           -         lo0
134.141.0.0/22      127.0.0.1           Aggregate lo0
134.141.1.0/24      directly connected  -         AS-10Nets
134.141.2.0/24      directly connected  -         AS-10Nets
134.141.3.0/24      directly connected  -         AS-10Nets
134.141.172.0/24    192.168.1.1         BGP       BGP-To20
                    192.168.1.6         BGP       BGP-To20B
140.1.0.0/22        127.0.0.1           Aggregate lo0
140.1.1.0/24        directly connected  -         AS-10Nets
140.1.2.0/24        directly connected  -         AS-10Nets
140.1.3.0/24        directly connected  -         AS-10Nets
192.168.1.0/30      directly connected  -         BGP-To20
192.168.1.4/30      directly connected  -         BGP-To20B
206.1.1.1           206.1.1.1           -         lo0
207.50.0.0/22       127.0.0.1           Aggregate lo0
207.50.1.0/24       directly connected  -         AS-10Nets
207.50.2.0/24       directly connected  -         AS-10Nets
207.50.3.0/24       directly connected  -         AS-10Nets
```

The "`bgp show summary`" commands provides a clear indication of what is happening within each peering group, from the local routers perspective. Including the number of prefixes sent/received per peer in the specific group. The results of the command have been documented for each router running BGP. The interesting note is for the 205.1.1.3 peer in AS20, group Internal. The route 134.141.172.0/24 is not a BGP route, rather it is an OSPF route. So internally the received count on 205.1.1.1 and 205.1.1.2 for 205.1.1.3 is 0. However, as expected the router in AS10, AS10-1, receives this route as a BGP route from both of its EBGP peers, due to the export of the network from OSPF-ASE to BGP target AS 10.

```
AS10-1# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: South]
192.168.1.1     4    20      26      28   0d0h24m27s         1/3
192.168.1.6     4    20      26      28   0d0h24m16s         1/3
BGP summary, 1 groups, 2 peers

AS20-1# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: North]
192.168.1.2     4    10      30      30    0d0h27m2s         3/1
[Group Id: Internal]
205.1.1.2       4    20      30      31   0d0h25m38s         2/1
205.1.1.3       4    20      13      16   0d0h12m47s         0/1
BGP summary, 2 groups, 3 peers

AS20-2# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: North]
192.168.1.5     4    10      30      31   0d0h27m23s         3/1
[Group Id: Internal]
205.1.1.1       4    20      30      32    0d0h26m9s         1/2
205.1.1.3       4    20      15      17   0d0h13m15s         0/2
BGP summary, 2 groups, 3 peers

AS20-3# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: Internal]
205.1.1.1       4    20      16      16   0d0h13m43s         1/0
205.1.1.2       4    20      15      16   0d0h13m38s         2/0
BGP summary, 1 groups, 2 peers
```

This brings up an interesting point. If the configuration were simply left as such on all the routers, we have successfully influenced the route through the AS20 IGP network. However, the return path from AS10 is free to choose which of the equal paths to return on.

Using "traceroute" on any of the customer routers you will notice that the correct first hop is taken but all bets are off on the return path.

```
C:\>tracert 134.141.1.254 -d

Tracing route to 134.141.1.254 over a maximum of 30 hops
1       <10ms           <10ms           <10ms           134.141.172.1
2       <10ms           <10ms           <10ms           192.168.2.9
3       <10ms           <10ms           <10ms           192.168.1.2
4       <10ms           <10ms           <10ms           134.141.1.254

C:\>tracert 207.50.2.254 -d

Tracing route to 207.50.2.254 over a maximum of 30 hops
1       <10ms           <10ms           <10ms           134.141.172.1
2       <10ms           <10ms           <10ms           192.168.2.9
3       <10ms           <10ms           <10ms           192.168.1.5
4       <10ms           <10ms           <10ms           207.50.2.254

C:\>tracert 140.1.1.254 -d
```

```
Tracing route to 207.50.2.254 over a maximum of 30 hops
1       <10ms           <10ms           <10ms           134.141.172.1
2       <10ms           <10ms           <10ms           192.168.2.5
3       <10ms           <10ms           <10ms           192.168.1.2
4       <10ms           <10ms           <10ms           140.1.1.254
```

To influence the return path, the two providers would have to agree on either using Multi-Exit Discriminators (MEDs), Communities or some type of AS path pre-pending on the advertising network could also be considered.

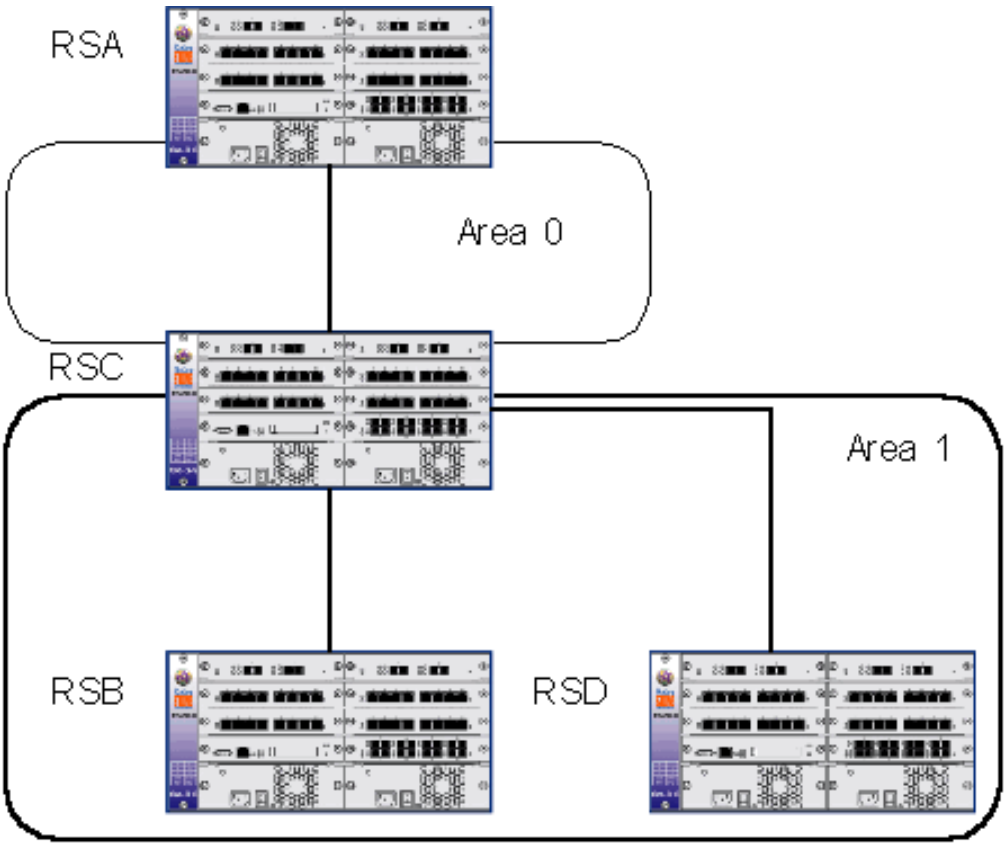
Basic Route Reflection

Jeff McLaird
Corporate Systems Engineering
April 15, 2001

One of the shortcomings of a simple IBGP design is lack of scalability. In general it is good practice to limit the number of fully meshed IBGP peers to a number less than 50. In the configuration illustrated below all routers are BGP speakers. Without a route reflector, the network shown in the diagram below will need to form a full IBGP mesh. Once RSB is configured as a route reflector a full IBGP mesh is not required. This is because RSB will reflect routes learned via RSA to RSC and RSD. In turn routes learned from RSC and RSD will be reflected back to RSA via RSB. Normally a BGP speaker will not advertise a route learned via another IBGP speaker to a third IBGP speaker. However Route Reflectors are the exception to this rule. The example shown illustrates two OSPF areas (backbone and area 1). OSPF area 1 is configured with a single route reflector (RSB) that, along with the Upstream Peering router (RSA) connected to Area 0, form a full IBGP mesh. Thus the Upstream peering router, is a non-client peer.

RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	The configuration examples should work with all revisions of hardware however please refer to the release notes for the specific firmware version you are interested.

Diagram



Configurations

RSA – Upstream Peering Router

```
vlan create core id 1000 ip
vlan add ports gi.6.1 to core
interface create ip core address-netmask 10.10.10.1/24 vlan core
interface create ip upstream address-netmask 172.16.167.6/30 port so.7.1
interface add ip lo0 address-netmask 10.10.1.1/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.1.1
ip-router policy redistribute from-proto bgp source-as 65000 to-proto bgp target-as
65412
ip-router policy redistribute from-proto bgp source-as 65412 to-proto bgp target-as
65000
ip-router policy redistribute from-proto direct to-proto bgp target-as 65412 network
172.16.167.4/30
ospf create area backbone
ospf add interface core to-area backbone
ospf add stub-host 10.10.1.1 to-area backbone cost 1
ospf start
bgp create peer-group ibgp type routing autonomous-system 65412 proto any interface
all
bgp create peer-group upstream autonomous-system 65000 type external
bgp add peer-host 172.16.167.5 group upstream
```

```
bgp add peer-host 10.10.2.1 group ibgp
bgp set peer-group ibgp local-address 10.10.1.1 log-up-down
bgp set peer-group upstream out-delay 60 log-up-down
bgp start
system set name RSA
```

RSB – Route Reflector

```
vlan create area1 id 1001 ip
vlan add ports et.(1-5).(1-8) to area1
interface create ip area1 address-netmask 10.10.11.2/24 vlan area1
interface add ip lo0 address-netmask 10.10.2.1/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.2.1
ip-router policy redistribute from-proto bgp source-as 65412 to-proto bgp target-as
65412
ospf create area 0.0.0.1
ospf add interface area1 to-area 0.0.0.1
ospf add stub-host 10.10.2.1 to-area 0.0.0.1 cost 1
ospf start
bgp create peer-group reflection type routing autonomous-system 65412 proto any
interface all
bgp create peer-group ibgp type routing proto any autonomous-system 65412 interface
all
bgp add peer-host 10.10.1.1 group ibgp
bgp add peer-host 10.10.1.2 group reflection
bgp add peer-host 10.10.2.2 group reflection
bgp set peer-group reflection reflector-client local-address 10.10.2.1
bgp set peer-group ibgp1 local-address 10.10.2.1
bgp start
system set name RSB
```

RSC – Area Border Router

```
vlan create core id 1000 ip
vlan create area1 id 1001 ip
vlan add ports gi.6.1 to core
vlan add ports et.(1-5).(1-8) to area1
interface create ip area1 address-netmask 10.10.11.1/24 vlan area1
interface create ip core address-netmask 10.10.10.2/24 vlan core
interface add ip lo0 address-netmask 10.10.1.2/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.1.2
ip-router policy redistribute from-proto direct to-proto bgp target-as 65412
ip-router policy redistribute from-proto static to-proto bgp target-as 65412
ospf create area backbone
ospf create area 0.0.0.1
```

```
ospf add interface area1 to-area 0.0.0.1
ospf add stub-host 10.10.1.2 to-area backbone cost 1
ospf add interface area1 to-area 0.0.0.1
ospf start
bgp create peer-group reflection type routing proto any interface all autonomous-system 65412
bgp add peer-host 10.10.2.1 group reflection
bgp set peer-group reflection local-address 10.10.1.2 out-delay 60 log-up-down
bgp start
system set name RSC
```

RSD – Area Router

```
vlan create area1 id 1001 ip
vlan add ports et.(1-5).(1-8) to area1
interface create ip area1 address-netmask 10.10.11.3/24 vlan area1
interface add ip lo0 address-netmask 10.10.2.2/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.2.2
ip-router policy redistribute from-proto direct to-proto bgp target-as 65412
ip-router policy redistribute from-proto static to-proto bgp target-as 65412
ospf create area 0.0.0.1
ospf add interface area1 to-area 0.0.0.1
ospf add stub-host 10.10.2.2 to-area 0.0.0.1 cost 1
ospf start
bgp create peer-group reflection type routing autonomous-system 65412 proto any interface all
bgp add peer-host 10.10.2.1 group reflection
bgp set peer-group reflection local-address 10.10.2.2
bgp start
system set name RSD
```

Comments

The configuration lines shown in red in the above example are specific to the BGP route reflection example. The configuration for RSA is a very straightforward IBGP/EBGP setup. We define both an upstream peer and an IBGP peering relationship (in this case RSB).

The configuration for the route reflector itself is again straightforward. The command syntax that defines the router as a route reflector is contained in the line "**`bgp set peer-group reflection reflector-client local-address 10.10.2.1`**". This defines the specific peer group reflection as a group of reflector clients and hence RSB as the reflector. The "**`local-address`**" definition simply means that this is the address the router should use for peering and as a source of updates. RSB also has two peer groups defined one for peering to RSA and one for peering to reflector clients.

Although not shown in this configuration example it is also possible to run with redundant route reflectors by including a cluster-id in the reflector configuration e.g. "**`bgp set cluster-id 0.0.0.1`**". In this instance the reflector clients will peer with both routers via the router-id's with the cluster id being used to define the redundant group between the two reflectors. The decision to use redundant route reflectors should not be taken lightly since this does increase the CPU and memory burdens on both the reflectors themselves and the reflector clients. Care should be taken to ensure that both entities have sufficient memory and CPU resources to provide for this type of configuration.

It is necessary to carry out a mutual redistribution on the route reflector in order to advertise the full table information to both client and non-client peers. This is illustrated with the command syntax in RSB "**`ip-router policy redistribute from-proto bgp source-as 65412 to-proto bgp target-as 65412`**".

There are no special configuration parameters for route reflector clients. From the example shown both RSC and RSD are configured exactly as they would be for peering via a straightforward IBGP session. Thus from a client perspective a route reflector is simply a normal IBGP peer. From this standpoint any router supporting BGP version 4 can act as a route reflector client with due concern of course shown to the amount of memory and CPU power the device possesses.

Bogon Filtering With BGP

Andrew Walden
Corporate Systems Engineering
February 13, 2003

This config demonstrates basic BGP prefix filtering. The prefixes listed in the config are bogus routes, or bogons. These are detailed in the Manning draft http://search.ietf.org/internet-drafts/draft-manning-dsua-08.txt The IP block are reserved by the Internet Assigned Numbers Authority at this time so any traffic concerned with these routes is bogus. This list is up to date as of 02/13/03 but does change. When the IANA allocates new address space to one of the regional registries, ARIN, RIPE or APNIC an operation message is sent out to various operational mailing lists operated by each of the registries as well as lists such as NANOG, APRICOT, JANOG and others. When new space is announced the below filters should be adjusted accordingly. Attempts will be made to ensure this document is updated also. These prefixes can be double checked at the IANA's web site at: http://www.iana.org/assignments/ipv4-address-space. This config is best installed via tftp due to its size.

RapidOS Version Tested	9.1.2.2
RapidOS Versions Working with this Configuration	5.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 5.0.0.0 and 6.x
Hardware Specifics	None

Configurations

```
interface create ip et.1.1 address-netmask 192.168.1.3/24 port et.1.1
ip-router global set autonomous-system 65002
ip-router global set router-id 192.168.1.3
bgp create peer-group test autonomous-system 65001 type external
```

```
bgp add peer-host 192.168.1.2 group test
bgp set peer-group test route-map-in nobogons in-sequence 1
bgp set peer-group test route-map-in noreserved in-sequence 2
bgp start

ip-router policy create filter bogons network 0.0.0.0/8
ip-router policy add filter bogons network 1.0.0.0/8
ip-router policy add filter bogons network 2.0.0.0/8
ip-router policy add filter bogons network 5.0.0.0/8
ip-router policy add filter bogons network 7.0.0.0/8
ip-router policy add filter bogons network 23.0.0.0/8
ip-router policy add filter bogons network 27.0.0.0/8
ip-router policy add filter bogons network 31.0.0.0/8
ip-router policy add filter bogons network 36.0.0.0/8
ip-router policy add filter bogons network 37.0.0.0/8
ip-router policy add filter bogons network 39.0.0.0/8
ip-router policy add filter bogons network 41.0.0.0/8
ip-router policy add filter bogons network 42.0.0.0/8
ip-router policy add filter bogons network 49.0.0.0/8
ip-router policy add filter bogons network 50.0.0.0/8
ip-router policy add filter bogons network 58.0.0.0/8
ip-router policy add filter bogons network 59.0.0.0/8
ip-router policy add filter bogons network 60.0.0.0/8
ip-router policy add filter bogons network 70.0.0.0/8
ip-router policy add filter bogons network 71.0.0.0/8
ip-router policy add filter bogons network 72.0.0.0/8
ip-router policy add filter bogons network 73.0.0.0/8
ip-router policy add filter bogons network 74.0.0.0/8
ip-router policy add filter bogons network 75.0.0.0/8
ip-router policy add filter bogons network 76.0.0.0/8
ip-router policy add filter bogons network 77.0.0.0/8
ip-router policy add filter bogons network 78.0.0.0/8
ip-router policy add filter bogons network 79.0.0.0/8
ip-router policy add filter bogons network 83.0.0.0/8
ip-router policy add filter bogons network 84.0.0.0/8
ip-router policy add filter bogons network 85.0.0.0/8
ip-router policy add filter bogons network 86.0.0.0/8
ip-router policy add filter bogons network 87.0.0.0/8
ip-router policy add filter bogons network 88.0.0.0/8
ip-router policy add filter bogons network 89.0.0.0/8
ip-router policy add filter bogons network 90.0.0.0/8
ip-router policy add filter bogons network 91.0.0.0/8
ip-router policy add filter bogons network 92.0.0.0/8
ip-router policy add filter bogons network 93.0.0.0/8
ip-router policy add filter bogons network 94.0.0.0/8
ip-router policy add filter bogons network 95.0.0.0/8
ip-router policy add filter bogons network 96.0.0.0/8
```

```
ip-router policy add filter bogons network 97.0.0.0/8
ip-router policy add filter bogons network 98.0.0.0/8
ip-router policy add filter bogons network 99.0.0.0/8
ip-router policy add filter bogons network 100.0.0.0/8
ip-router policy add filter bogons network 101.0.0.0/8
ip-router policy add filter bogons network 102.0.0.0/8
ip-router policy add filter bogons network 103.0.0.0/8
ip-router policy add filter bogons network 104.0.0.0/8
ip-router policy add filter bogons network 105.0.0.0/8
ip-router policy add filter bogons network 106.0.0.0/8
ip-router policy add filter bogons network 107.0.0.0/8
ip-router policy add filter bogons network 108.0.0.0/8
ip-router policy add filter bogons network 109.0.0.0/8
ip-router policy add filter bogons network 110.0.0.0/8
ip-router policy add filter bogons network 111.0.0.0/8
ip-router policy add filter bogons network 112.0.0.0/8
ip-router policy add filter bogons network 113.0.0.0/8
ip-router policy add filter bogons network 114.0.0.0/8
ip-router policy add filter bogons network 115.0.0.0/8
ip-router policy add filter bogons network 116.0.0.0/8
ip-router policy add filter bogons network 117.0.0.0/8
ip-router policy add filter bogons network 118.0.0.0/8
ip-router policy add filter bogons network 119.0.0.0/8
ip-router policy add filter bogons network 120.0.0.0/8
ip-router policy add filter bogons network 121.0.0.0/8
ip-router policy add filter bogons network 122.0.0.0/8
ip-router policy add filter bogons network 123.0.0.0/8
ip-router policy add filter bogons network 124.0.0.0/8
ip-router policy add filter bogons network 125.0.0.0/8
ip-router policy add filter bogons network 126.0.0.0/8
ip-router policy add filter bogons network 127.0.0.0/8
ip-router policy add filter bogons network 197.0.0.0/8
ip-router policy add filter bogons network 201.0.0.0/8
route-map nobogons deny 10 match-prefix filter bogons
route-map nobogons permit 20
ip-router policy create filter reserved network 10.0.0.0/8
ip-router policy add filter reserved network 192.168.0.0/16
ip-router policy add filter reserved network 172.16.0.0/12
ip-router policy add filter reserved network 127.0.0.0/8
ip-router policy add filter reserved network 169.254.0.0/16
ip-router policy add filter reserved network 192.0.2.0/24
ip-router policy add filter reserved network 192.88.99.0/24
ip-router policy add filter reserved network 198.18.0.0/15
ip-router policy add filter reserved network 224.0.0.0/3
route-map noreserved deny 10 match-prefix filter reserved
route-map noreserved permit 20
```

Comments

Since this filter is rather large, performance tests were completed to show the effects on a router. Loading 85,000 routes without the filter installed took an average of 22.5 seconds. The same routes took an average of 23.5 seconds with a difference of about 1 second for loading the routes. This shows that this filter is good security that doesn't affect the performance of the box adversely.

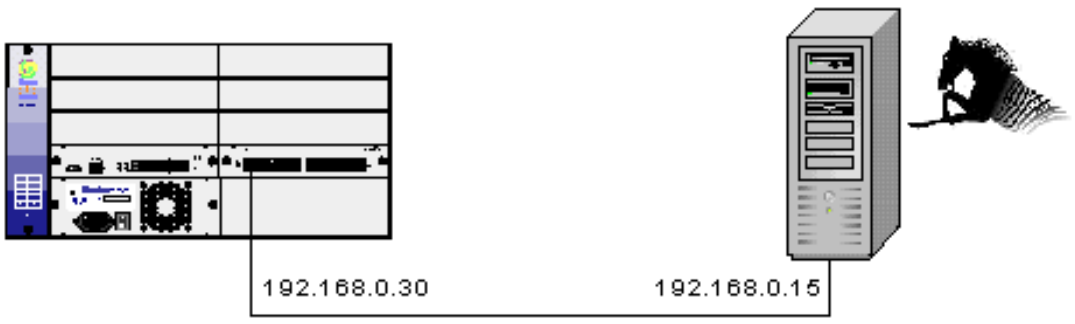
Peering with Multiple BGP Peers Using Zebra

Greg Hankins
Corporate Systems Engineering
July 18, 2001

Here is a quick configuration example on how to use Zebra to simulate multiple BGP peers between the same router. Zebra supports multiple instances of BGP, which will appear as completely different peers using different routing tables. Using the load/save patch for Zebra, you can load multiple full sets of routes from a file to send to the RS router.

RapidOS Version Tested	8.0.0.0 / Zebra 0.91a
RapidOS Versions Working with this Configuration	All
RapidOS Versions NOT Working with this Configuration	None
Hardware Specifics	N/A

Diagram



Configurations

RS8000

```
interface create ip peering address-netmask 192.168.0.30 port et.1.1
ip-router global set autonomous-system 65030
ip-router global set router-id 192.168.0.30
ip-router policy redistribute from-proto bgp to-proto bgp target-as all source-as
65015 restrict
bgp create peer-group AS65015 autonomous-system 65015 type external
bgp create peer-group AS65016 autonomous-system 65016 type external
bgp create peer-group AS65017 autonomous-system 65017 type external
bgp add peer-host 192.168.0.15 group AS65015
bgp add peer-host 192.168.0.15 group AS65016
bgp add peer-host 192.168.0.15 group AS65017
bgp set peer-group AS65015 hold-time 1200
bgp set peer-group AS65016 hold-time 1200
bgp set peer-group AS65017 hold-time 1200
bgp set multipath off
bgp start
system set name RS8000
system set idle-timeout serial 0
```

Zebra

```
hostname zebra
password zebra
log stdout
!
bgp multiple-instance
!
router bgp 65015
 bgp router-id 192.168.0.15
 neighbor 192.168.0.30 remote-as 65030
 neighbor 192.168.0.30 timers 400 1200
 neighbor 192.168.0.254 remote-as 65030
 neighbor 192.168.0.254 shutdown
!
router bgp 65016 view AS65016
 bgp router-id 192.168.0.16
 neighbor 192.168.0.30 remote-as 65030
 neighbor 192.168.0.30 timers 400 1200
 neighbor 192.168.0.253 remote-as 65030
 neighbor 192.168.0.253 shutdown
!
router bgp 65017 view AS65017
 bgp router-id 192.168.0.17
 neighbor 192.168.0.30 remote-as 65030
 neighbor 192.168.0.30 timers 400 1200
 neighbor 192.168.0.252 remote-as 65030
 neighbor 192.168.0.252 shutdown
```

```
!
line vty
 exec-timeout 0 0
```

Comments

In this example, we have three peers configured on the Riverstone and Zebra. Each peer on the RS receives a separate full routing table from Zebra, which were loaded into each dummy peer.

```
RS8000# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- -----------------
[Group Id: AS65015]
192.168.0.15    4 65015  100378      26   0d2h33m38s    100353/0
[Group Id: AS65016]
192.168.0.15    4 65016  100377      25   0d2h28m34s    100353/0
[Group Id: AS65017]
192.168.0.15    4 65017  100365      13   0d2h23m54s    100353/0
```

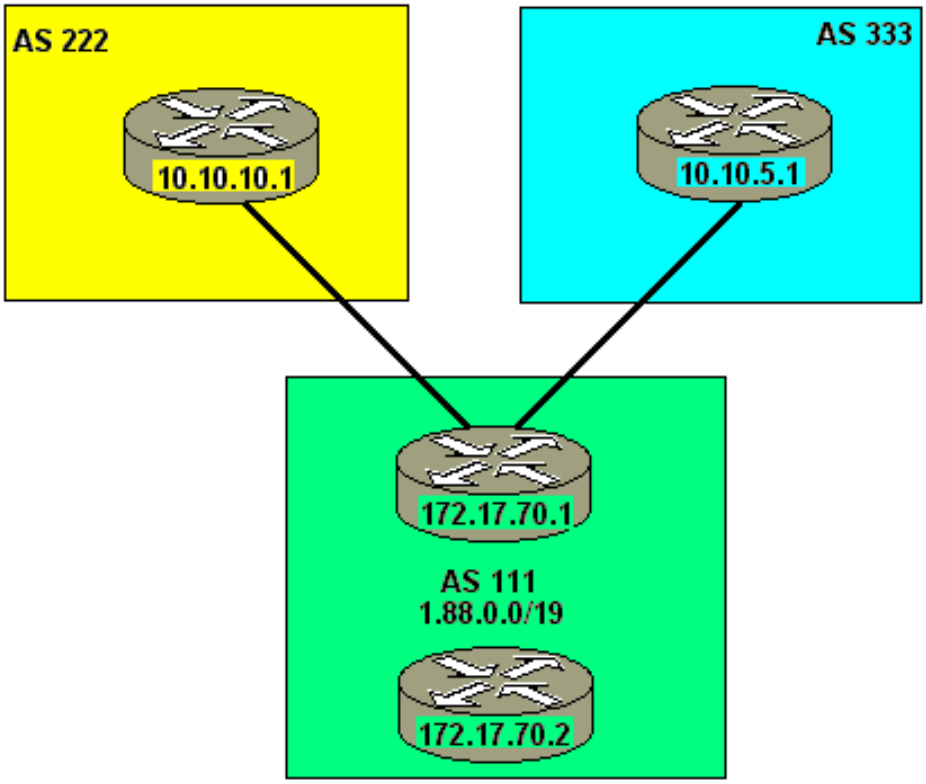
Note: each full routing table takes between 50MB - 60MB of RAM when you load them into Zebra. You need to make sure that you have enough RAM in your Zebra box to support the number of peers you have configured. The Hold Time needs to be set to a large value to prevent Zebra from missing KEEPALIVEs when loading the prefixes from disk.

Secure BGP Configuration

Andrew Walden
Corporate Systems Engineering
February 13, 2003

This is the ROS Secure BGP configuration based on the IOS secure BGP configuration http://www.cymru.com/~robt/Docs/Articles/secure-bgp-template.html by Rob Thomas. There is a single command listed that is only available in 9.0, but the rest is compatible with 8.x and higher ROS versions. As usual with BGP, 256Mb of RAM, if not 512MB, is recommended for today's growing routing table.	
RapidOS Version Tested	9.1.2.1
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	None.

Diagram



Configurations

```
! Required for BGP
ip-router global set autonomous-system 111
ip-router global set router-id 10.10.10.10

! This option is available in ROS 9.0 ONLY. This injects the advertisement
! into BGP so long as the route exists in the IGP.
bgp advertise network 1.88.0.0/19

! Create our first external peer-group
bgp create peer-group as333 autonomous-system 333 type external
bgp add peer-host 10.10.5.1 group as333

! Enable an MD5 password
bgp set peer-group as333 password bgpwith333

! Produce Syslog messages with the session changes state
bgp set peer-group as333 log-up-down

! This ensures that rejected routes don't take up memory
bgp set peer-group as333 delete-policy-rejects

! This option causes warning messages when receiving questionable BGP
! updates such as duplicate routes and/or deletions of non-existing
! routes. bgp set peer-group as333 show-warnings.
bgp set peer-group as333 show-warnings

! Hard-set for version 4. Disabled BGP version negotiation, thus
```

```
! bringing the peering session on-line more quickly.
bgp set peer-group as333 version 4

! Install our BOGON filters (See filters below)
bgp set peer-group as333 route-map-in nobogons in-sequence 5
bgp set peer-group as333 route-map-in noreserved in-sequence 10

! Install our dampening rules (See rules below)
bgp set peer-group as333 route-map-in no-dampen in-sequence 15
bgp set peer-group as333 route-map-in dampen-short in-sequence 20
bgp set peer-group as333 route-map-in dampen-med in-sequence 25
bgp set peer-group as333 route-map-in dampen-long in-sequence 30

! Install our announcement filters (See below)
bgp set peer-group as333 route-map-out announce out-sequence 1

! Prevent a mistake or mishap by our peer (or someone with whom our peer
! has a peering agreement) from causing router meltdown by filling the
! routing and BGP tables. This is a hard limit.
bgp set peer-host 10.10.5.1 max-prefixes 125000

! Configure our other external peer
bgp create peer-group as222 autonomous-system 222 type external
bgp add peer-host 10.10.10.1 group as222
bgp set peer-group as222 password bgpwith222
bgp set peer-group as222 log-up-down
bgp set peer-group as222 delete-policy-rejects
bgp set peer-group as222 show-warnings
bgp set peer-group as222 version 4
bgp set peer-group as222 route-map-in nobogons in-sequence 5
bgp set peer-group as222 route-map-in noreserved in-sequence 10
bgp set peer-group as222 route-map-in no-dampen in-sequence 15
bgp set peer-group as222 route-map-in dampen-short in-sequence 20
bgp set peer-group as222 route-map-in dampen-med in-sequence 25
bgp set peer-group as222 route-map-in dampen-long in-sequence 30
bgp set peer-group as222 route-map-out announce out-sequence 5
bgp set peer-host 10.10.10.1 group as222 max-prefixes 125000

! Configure our internal BGP peer
bgp create peer-group ibgp-111 autonomous-system 111 type routing
bgp add peer-host 172.17.70.2 group ibgp-111
bgp set peer-group ibgp-111 password bgpwith111
bgp set peer-group ibgp-111 log-up-down
bgp set peer-group ibgp-111 delete-policy-rejects
bgp set peer-group ibgp-111 show-warnings
bgp set peer-group ibgp-111 version 4

! Use the loopback IP as our source address for connectivity
bgp set peer-group ibgp-111 local-address 10.10.10.10

! Ensure that the traffic that I advertise for comes to me
bgp set peer-group ibgp-111 next-hop-self
bgp set peer-host 172.17.70.2 max-prefixes 125000
```

```
! Static routes so I can get around my own network and nail up my prefix
! announcement so that it doesn't flap
ip add route 1.88.0.0/19 blackhole
ip add route 1.88.50.0/24 gateway 192.168.50.5
ip add route 1.88.55.0/24 gateway 192.168.50.8
ip add route 1.88.75.128/25 gateway 192.168.50.10
ip add route 172.17.70.2/32 gateway 192.168.50.2

! We protect TCP port 179 (BGP port) from miscreants by limiting
! access. Allow our peers to connect and log all other attempts.
! Remember to apply this ACL to the interfaces of the router or
! add it to existing ACLs.
acl 185 permit tcp 10.10.5.1/32 172.17.70.1/32 any 179
acl 185 permit tcp 10.10.5.1/32 172.17.70.1/32 179 any
acl 185 permit tcp 10.10.10.1/32 172.17.70.1/32 any 179
acl 185 permit tcp 10.10.10.1/32 172.17.70.1/32 179 any
acl 185 permit tcp 172.17.70.2/32 172.17.70.1/32 any 179
acl 185 permit tcp  172.17.70.2/32 172.17.70.1/32 179 any
acl 185 deny tcp any any 179 179 log

! Announce only those networks we specifically list. This also prevents
! the network from becoming a transit provider. An added bit of protection
! and good netizenship.
route-map announce permit 5 match-prefix network 1.88.0.0/19
route-map announce deny 10 match-prefix network all

! The bogons prefix list prevents the acceptance of obviously bogus
! routing updates. This can be modified to fit local requirements.
! While aggregation is possible - certainly desirable - IANA tends
! to allocate netblocks on a /8 boundary. For this reason, I have
! listed the bogons largely as /8 netblocks. This will make changes
! to the bogons prefix-list easier to accomplish and less intrusive.
! I have listed more specific netblocks when documentation, such as
! RFC1918, is more granular.
! Please see the IANA IPv4 netblock assignment document at the
! following URL:
! http://www.isi.edu/in-notes/iana/assignments/ipv4-address-space
ip-router policy create filter bogons network 0.0.0.0/8
ip-router policy add filter bogons network 1.0.0.0/8
ip-router policy add filter bogons network 2.0.0.0/8
ip-router policy add filter bogons network 5.0.0.0/8
ip-router policy add filter bogons network 7.0.0.0/8
ip-router policy add filter bogons network 23.0.0.0/8
ip-router policy add filter bogons network 27.0.0.0/8
ip-router policy add filter bogons network 31.0.0.0/8
ip-router policy add filter bogons network 36.0.0.0/8
ip-router policy add filter bogons network 37.0.0.0/8
ip-router policy add filter bogons network 39.0.0.0/8
ip-router policy add filter bogons network 41.0.0.0/8
ip-router policy add filter bogons network 42.0.0.0/8
ip-router policy add filter bogons network 49.0.0.0/8
ip-router policy add filter bogons network 50.0.0.0/8
```

```
ip-router policy add filter bogons network 58.0.0.0/8
ip-router policy add filter bogons network 59.0.0.0/8
ip-router policy add filter bogons network 60.0.0.0/8
ip-router policy add filter bogons network 70.0.0.0/8
ip-router policy add filter bogons network 71.0.0.0/8
ip-router policy add filter bogons network 72.0.0.0/8
ip-router policy add filter bogons network 73.0.0.0/8
ip-router policy add filter bogons network 74.0.0.0/8
ip-router policy add filter bogons network 75.0.0.0/8
ip-router policy add filter bogons network 76.0.0.0/8
ip-router policy add filter bogons network 77.0.0.0/8
ip-router policy add filter bogons network 78.0.0.0/8
ip-router policy add filter bogons network 79.0.0.0/8
ip-router policy add filter bogons network 83.0.0.0/8
ip-router policy add filter bogons network 84.0.0.0/8
ip-router policy add filter bogons network 85.0.0.0/8
ip-router policy add filter bogons network 86.0.0.0/8
ip-router policy add filter bogons network 87.0.0.0/8
ip-router policy add filter bogons network 88.0.0.0/8
ip-router policy add filter bogons network 89.0.0.0/8
ip-router policy add filter bogons network 90.0.0.0/8
ip-router policy add filter bogons network 91.0.0.0/8
ip-router policy add filter bogons network 92.0.0.0/8
ip-router policy add filter bogons network 93.0.0.0/8
ip-router policy add filter bogons network 94.0.0.0/8
ip-router policy add filter bogons network 95.0.0.0/8
ip-router policy add filter bogons network 96.0.0.0/8
ip-router policy add filter bogons network 97.0.0.0/8
ip-router policy add filter bogons network 98.0.0.0/8
ip-router policy add filter bogons network 99.0.0.0/8
ip-router policy add filter bogons network 100.0.0.0/8
ip-router policy add filter bogons network 101.0.0.0/8
ip-router policy add filter bogons network 102.0.0.0/8
ip-router policy add filter bogons network 103.0.0.0/8
ip-router policy add filter bogons network 104.0.0.0/8
ip-router policy add filter bogons network 105.0.0.0/8
ip-router policy add filter bogons network 106.0.0.0/8
ip-router policy add filter bogons network 107.0.0.0/8
ip-router policy add filter bogons network 108.0.0.0/8
ip-router policy add filter bogons network 109.0.0.0/8
ip-router policy add filter bogons network 110.0.0.0/8
ip-router policy add filter bogons network 111.0.0.0/8
ip-router policy add filter bogons network 112.0.0.0/8
ip-router policy add filter bogons network 113.0.0.0/8
ip-router policy add filter bogons network 114.0.0.0/8
ip-router policy add filter bogons network 115.0.0.0/8
ip-router policy add filter bogons network 116.0.0.0/8
ip-router policy add filter bogons network 117.0.0.0/8
ip-router policy add filter bogons network 118.0.0.0/8
ip-router policy add filter bogons network 119.0.0.0/8
ip-router policy add filter bogons network 120.0.0.0/8
ip-router policy add filter bogons network 121.0.0.0/8
```

```
ip-router policy add filter bogons network 122.0.0.0/8
ip-router policy add filter bogons network 123.0.0.0/8
ip-router policy add filter bogons network 124.0.0.0/8
ip-router policy add filter bogons network 125.0.0.0/8
ip-router policy add filter bogons network 126.0.0.0/8
ip-router policy add filter bogons network 127.0.0.0/8
ip-router policy add filter bogons network 197.0.0.0/8
ip-router policy add filter bogons network 201.0.0.0/8
route-map nobogons deny 10 match-prefix filter bogons
route-map nobogons permit 20

! These are also BOGONS, but reserved in different ways
! then simple unallocation. Some are specified in rfc1918
! as private address space, others have purposes such as
! loopback and multicast.
ip-router policy create filter reserved network 10.0.0.0/8
ip-router policy add filter reserved network 192.168.0.0/16
ip-router policy add filter reserved network 172.16.0.0/12
ip-router policy add filter reserved network 127.0.0.0/8
ip-router policy add filter reserved network 169.254.0.0/16
ip-router policy add filter reserved network 192.0.2.0/24
ip-router policy add filter reserved network 192.88.99.0/24
ip-router policy add filter reserved network 198.18.0.0/15
ip-router policy add filter reserved network 224.0.0.0/3
route-map noreserved deny 10 match-prefix filter reserved
route-map noreserved permit 20

! Now we configure our prefix lists for our dampening requirements.
! These are configured along the lines of the recommendations made
! by RIPE. The goal is to minimalize the effect of dampening on
! the shorter and historically more stable prefixes as well as the
! netblocks that contain DNS root servers. The longer prefixes
! are dampened for longer periods of time, as these have been the
! the source of a greater percentage of the instability in the
! global routing table.
! Note that a longer prefix equates to a less-aggregated and smaller
! netblock.
ip-router policy create filter prefix-length network all between 0-24
route-map set-prefix-length permit 10 match-prefix filter prefix-length
route-map set-prefix-length deny 20

! The damplongprefixes list is for prefixes of /24 and longer.
ip-router policy create filter dampenlongprefixes network all between 24-32

! The dampmediumprefixes list is for prefixes of /22 and /23.
ip-router policy create filter dampenmediumprefixes network all between 22-23

! The dampshortprefixes list is for prefixes of /21 and shorter.
ip-router policy create filter dampenshortprefixes network all between 21-0

! The rootservers prefix list is to prevent dampening of
! the root DNS server netblocks.
ip-router policy create filter rootservers network  198.41.0.0/24 exact
```

```
ip-router policy add filter rootservers network 128.9.0.0/16 exact
ip-router policy add filter rootservers network 192.33.4.0/24 exact
ip-router policy add filter rootservers network 128.8.0.0/16 exact
ip-router policy add filter rootservers network 192.203.230.0/24 exact
ip-router policy add filter rootservers network 192.5.4.0/23 exact
ip-router policy add filter rootservers network 192.112.36.0/24 exact
ip-router policy add filter rootservers network 128.63.0.0/16 exact
ip-router policy add filter rootservers network 192.36.148.0/24 exact
ip-router policy add filter rootservers network 193.0.14.0/24 exact
ip-router policy add filter rootservers network 198.32.64.0/24 exact
ip-router policy add filter rootservers network 202.12.27.0/24 exact

route-map no-dampen permit 5 match-prefix filter rootservers
route-map no-dampen set dampenflap state disable
route-map dampen-long permit 5 match-prefix filter dampenlongprefixes
route-map dampen-long set dampenflap reach-decay 1800 unreach-decay 1800 suppress-
above 3 reuse-below 2 max-flap 4 keep-history 7200 state enable
route-map dampen-med permit 5 match-prefix filter dampenmediumprefixes
route-map dampen-med set dampenflap reach-decay 900 unreach-decay 900 suppress-above
3 reuse-below 2 max-flap 4 keep-history 7200 state enable
route-map dampen-short permit 5 match-prefix filter dampenshortprefixes
route-map dampen-short set dampenflap reach-decay 600 unreach-decay 600 suppress-
above 3 reuse-below 2 max-flap 4 keep-history 3600 state enable
```

Cisco to Riverstone BGP Translation Example

Greg Hankins
Corporate Systems Engineering
May 10, 2002

This configuration gives an example of a Cisco IOS to Riverstone ROS translation of BGP commands for a typical EBGP and IBGP scenario. Cisco commands are indented, followed by the equivalent Riverstone syntax.	
RapidOS Version Tested	9.0.0.1
RapidOS Versions Working with this Configuration	9.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.0.0.0
Hardware Specifics	N/A

Configurations

```
     router bgp 65001
      no synchronization
      bgp router-id 192.168.0.1

ip-router global set autonomous-system 65001
ip-router global set router-id 192.168.0.1
! "no synchronization" is enabled by default

      bgp log-neighbor-changes
! must be set on each peer-group or peer-host

     network 10.0.0.0 mask 255.255.240.0
     network 172.16.0.0 mask 255.255.248.0

bgp advertise network 10.0.0.0/20
```

```
bgp advertise network 172.16.0.0/21

      neighbor ibgp peer-group
      neighbor ibgp update-source Loopback0
      neighbor ibgp next-hop-self
      neighbor ibgp soft-reconfiguration inbound
      neighbor 192.168.0.2 remote-as 65001
      neighbor 192.168.0.2 peer-group ibgp
      neighbor 192.168.0.2 description core-ibgp-peer

bgp create peer-group ibgp autonomous-system 65001
bgp set peer-group ibgp local-address 192.168.0.1
bgp set peer-group ibgp next-hop-self
bgp set peer-group ibgp log-up-down
! "soft-reconfiguration inbound" is enabled by default
bgp add peer-host 192.168.0.2 group ibgp
bgp set peer-host description core-ibgp-peer

      neighbor 192.2.0.2 remote-as 65500
      neighbor 192.2.0.2 send-community
      neighbor 192.2.0.2 soft-reconfiguration inbound
      neighbor 192.2.0.2 prefix-list bogons in
      neighbor 192.2.0.2 route-map TRANSIT_OUT out
      neighbor 192.2.0.2 filter-list 1 out

bgp create peer-group transit-isp autonomous-system 65500
bgp set peer-group transit-isp log-up-down
! "send-community" is enabled by default and can be disabled with a route-map
! "soft-reconfiguration inbound" is enabled by default
bgp set peer-group transit-isp route-map-in TRANSIT_IN in-sequence 10
bgp set peer-group transit-isp route-map-out TRANSIT_OUT out-sequence 10
bgp add peer-host 192.2.0.2 group transit-isp

      no auto-summary
! "no auto-summary" is enabled by default

     ip route 10.0.0.0 255.255.240.0 Null0
     ip route 172.16.0.0 255.255.248.0 Null0

ip add route 10.0.0.0/20 gateway 127.0.0.1 blackhole preference 255
ip add route 172.16.0.0/21 gateway 127.0.0.1 blackhole preference 255

     ip bgp-community new-format
! "ip bgp-community new-format" is enabled by default

     ip as-path access-list 1 permit .*
     ip as-path access-list 2 deny .*
     ip as-path access-list 3 permit ^$
     ip as-path access-list 3 permit ^65001
     ip as-path access-list 3 deny .*

aspath-list PERMIT_ANY permit 10 ".*"
```

```
aspath-list DENY_ANY deny 10 ".*"
aspath-list PERMIT_LOCAL permit 10 ""
aspath-list PERMIT_LOCAL permit 20 "65001"
! implicit deny at end of aspath-list

     ip prefix-list bogons description BOGON_FILTER
     ip prefix-list bogons seq 5 deny 0.0.0.0/0
     ip prefix-list bogons seq 10 deny 1.0.0.0/8 le 32
     ip prefix-list bogons seq 15 deny 10.0.0.0/8 le 32
     ip prefix-list bogons seq 30 deny 127.0.0.0/8 le 32
     ip prefix-list bogons seq 35 deny 128.0.0.0/16 le 32
     ip prefix-list bogons seq 40 deny 129.156.0.0/16 le 32
     ip prefix-list bogons seq 45 deny 169.254.0.0/16 le 32
     ip prefix-list bogons seq 50 deny 172.16.0.0/12 le 32
     ip prefix-list bogons seq 60 deny 192.168.0.0/16 le 32
     ip prefix-list bogons seq 65 deny 224.0.0.0/3 le 32
     ip prefix-list bogons seq 70 permit 0.0.0.0/0 ge 8 le 24
     ip prefix-list bogons seq 75 deny 0.0.0.0/0 le 32

prefix-list BOGON_FILTER deny 5 0.0.0.0/0
prefix-list BOGON_FILTER deny 10 1.0.0.0/8 le 32
prefix-list BOGON_FILTER deny 15 10.0.0.0/8 le 32
prefix-list BOGON_FILTER deny 30 127.0.0.0/8 le 32
prefix-list BOGON_FILTER deny 35 128.0.0.0/16 le 32
prefix-list BOGON_FILTER deny 40 129.156.0.0/16 le 32
prefix-list BOGON_FILTER deny 45 169.254.0.0/16 le 32
prefix-list BOGON_FILTER deny 50 172.16.0.0/12 le 32
prefix-list BOGON_FILTER deny 55 172.16.60.0/22 le 32
prefix-list BOGON_FILTER deny 60 192.168.0.0/16 le 32
prefix-list BOGON_FILTER deny 65 224.0.0.0/3 le 32
prefix-list BOGON_FILTER permit 70 0.0.0.0/0 ge 8 le 24
! implicit deny at end of prefix-list

     access-list 1 permit 10.0.0.0 0.0.15.255
     access-list 1 permit 172.16.0.0 0.0.7.255

ip-router policy add filter MY_NETWORKS network 10.0.0.0/20 exact
ip-router policy add filter MY_NETWORKS network 172.16.0.0/21 exact

route-map TRANSIT_IN permit 10 match-prefix-list BOGON_FILTER

     route-map TRANSIT_OUT permit 10
      match ip address 1
      set community 65500:500

route-map TRANSIT_OUT permit 10 match-prefix filter MY_NETWORKS set-community-list
"65500:500"
```

Comments

Be sure to always check your advertised and received prefixes before leaving the router after making changes to BGP. The following commands are helpful in ensuring that your policies are working as you intend.

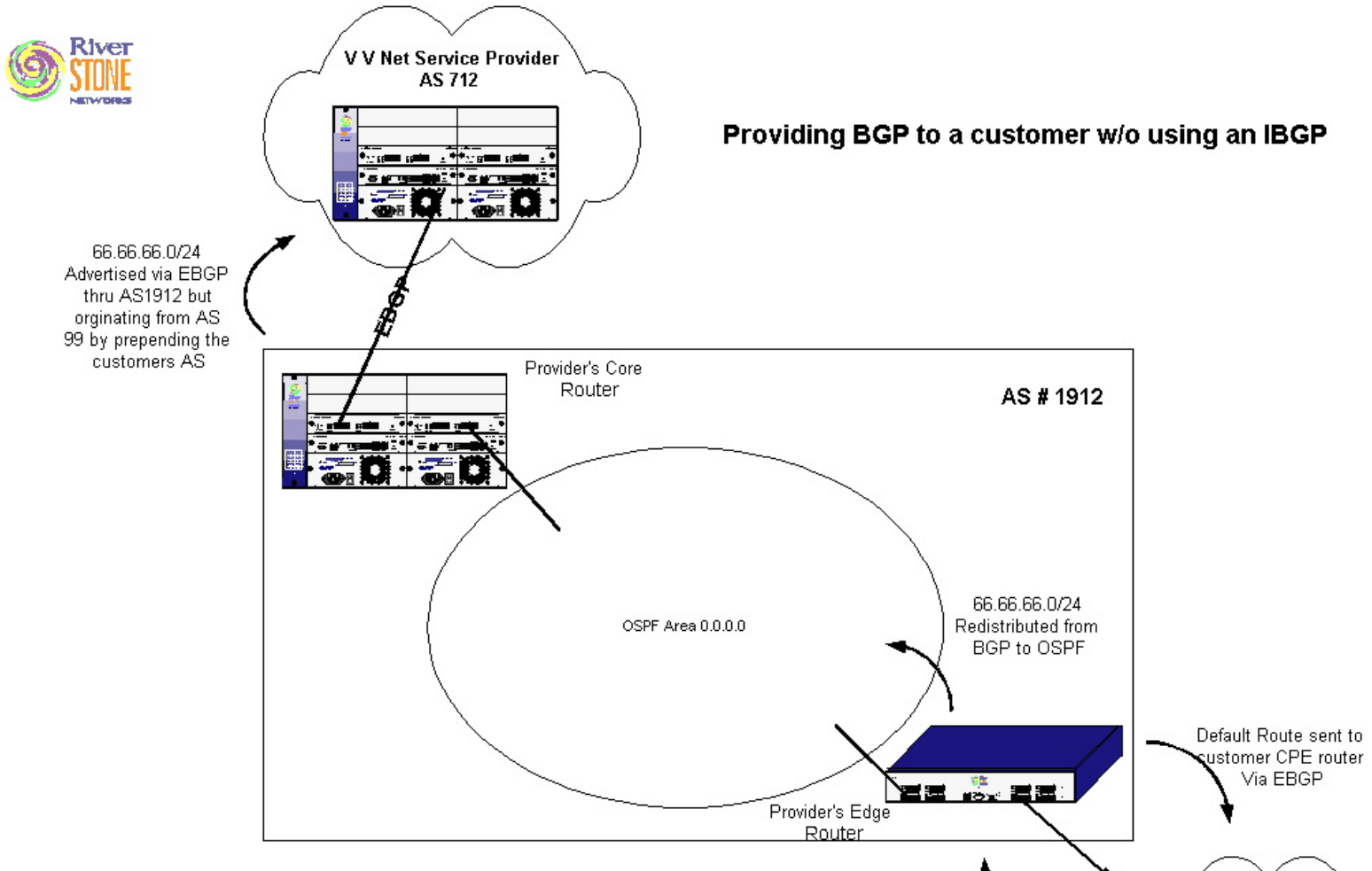
```
route-map show
bgp show summary
bgp show peer-host x.x.x.x advertised-routes
bgp show peer-host x.x.x.x received-routes
bgp show routes all
```

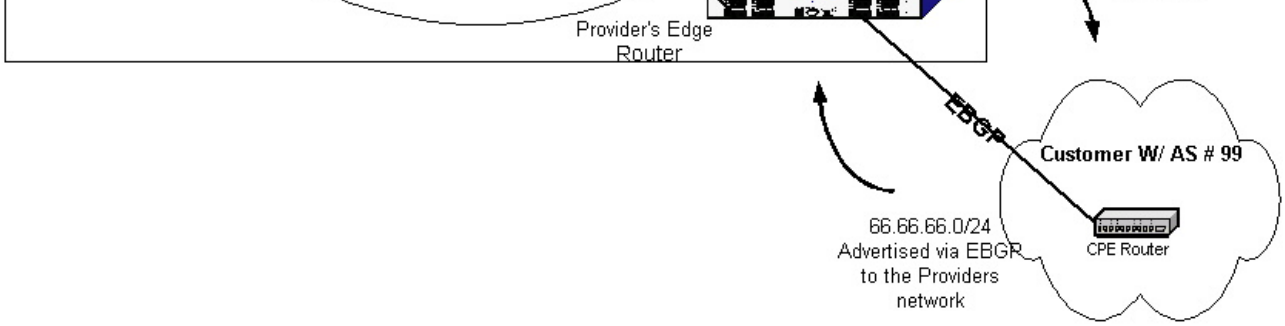
Providing Transit With EBGP Without IBGP in the ISPs Core

Scott Martin
Systems Engineering
May 16, 2002

In this situation the customer is a small ISP, (ISPX), which wants to provide one of their customer's with BGP connectivity w/o building out an IBGP within their network. ISPX will send their customer a default route via EBGP from the provider's edge router and will accept an aggregate route of 66.66.66.0/24 from the customer's BGP speaking router. The aggregate will then get redistributed into ISPX's OSPF network, their IGP. ISPX's core router will then use a route map to match the 66.66.66.0/24 to an outbound policy and prepend the AS number of the customer to the route so that the route appears to have been originated from the customers AS.	
RapidOS Version Tested	8.0.3.5, 9.0.0.2
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
NOTES	The command "bgp advertise network X.X.X.X" is only available in releases 9.0 and above.

Diagram





Configurations

Provider's Core Router

```
interface create ip 2-middlerouter address-netmask 134.141.25.2/30 port et.1.1
interface create ip VVnet address-netmask 192.168.1.1/24 port et.1.16
interface add ip lo0 address-netmask 1.1.1.1/32

ip-router global set router-id 1.1.1.1
ip-router global set autonomous-system 1912

ip add route 99.99.99.0/24 gateway 1.1.1.1 no-install blackhole

! This command will match the network and prefix as learned from OSPF and Prepend the
customers AS #99 to the BGP advertisement
route-map isp-customer permit 10 match-prefix network 66.66.66.0/24 exact set-as-path-
prepend "99"

ip-router policy redistribute from-proto bgp source-as 1912 to-proto bgp target-as
712

ospf create area backbone
ospf add interface 2-middlerouter to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 5
ospf start

bgp create peer-group EBGP autonomous-system 712 type external
bgp add peer-host 192.168.1.2 group EBGP
bgp set peer-group EBGP local-address 192.168.1.1
bgp set peer-host 192.168.1.2 group EBGP route-map-out isp-customer out-sequence 10
bgp start

system set name provider-core

bgp advertise network 99.99.99.0/24
```

Provider's Edge Router

```
interface create ip 2-middlerouter address-netmask 134.141.25.6/30 port et.1.1
interface create ip 2-toprouter address-netmask 134.141.25.9/30 port et.1.2
interface add ip lo0 address-netmask 3.3.3.3/32

ip-router global set router-id 3.3.3.3
ip-router global set trace-state on
ip-router global set autonomous-system 1912

ip add route default gateway 3.3.3.3 no-install blackhole

ip-router policy redistribute from-proto bgp source-as 99 to-proto ospf network
66.66.66.0/24 exact
ip-router policy redistribute from-proto static to-proto bgp target-as 99 network
default

ospf create area backbone
ospf add interface 2-middlerouter to-area backbone
ospf add stub-host 3.3.3.3 to-area backbone cost 5
ospf start

bgp create peer-group EBGP autonomous-system 99 type external
bgp add peer-host 134.141.25.10 group EBGP
bgp start

system set name providers-edge-router
```

Customer's Router

```
interface create ip 2-provider address-netmask 134.141.25.10/30 port et.2.1
interface add ip lo0 address-netmask 168.192.1.1/32
ip-router global set autonomous-system 99
ip-router global set router-id 134.141.25.10

ip add route 66.66.66.0/24 gateway 168.192.1.1 no-install blackhole

ip-router policy redistribute from-proto static to-proto bgp target-as 1912 network
66.66.66.0/24 exact

bgp create peer-group EBGP autonomous-system 1912 type external
bgp add peer-host 134.141.25.9 group EBGP
bgp start

system set name customer-router
```

Comments

Looking at the provider core router, the 66.66.66.0/24 route is learned via OSPF as an ASE external route.

```
provider-core# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              1.1.1.1              -         lo0
2.2.2.2              134.141.25.1         OSPF      2-middlerouter
3.3.3.3              134.141.25.1         OSPF      2-middlerouter
10.1.1.0/24          directly connected   -         en0
66.66.66.0/24        134.141.25.1         OSPF_ASE  2-middlerouter
127.0.0.1            127.0.0.1            -         lo0
134.141.25.0/30      directly connected   -         2-middlerouter
134.141.25.4/30      134.141.25.1         OSPF      2-middlerouter
192.168.1.0/24       directly connected   -         VVnet
```

Looking at the route map, the 66.66.66.0/24 network will be prepended with AS99.

```
provider-core# route-map show all

route-map isp-customer, permit, sequence 10
  Match clauses
    prefix
        Prefix             Range        Flags
        66.66.66.0/24                   Exact

  Set clauses
    aspath prepend 99
```

Looking at the Provider's-core router, the router advertises the following via BGP:

```
provider-core# bgp show peer-host 192.168.1.2 advertised-routes
BGP table : Local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop        Metric LocPrf Path
   -------            --------        ------ ------ ----
*> 99.99.99/24        192.168.1.1                   1912 ?
(Note this is the Providers own network)
*> 66.66.66/24        192.168.1.1                   1912 99 i
(Note AS(99) is in the path attrib)
```

As you can see the 66.66.66.0/24 route is advertised as if it was originated by AS99.

Looking at the VVNET router (Providers Carrier) the routes for both networks are learned as follows:

```
VVNET# bgp show routes all
BGP table : Local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop        Metric LocPrf Path
   -------            --------        ------ ------ ----
*> 66.66.66/24        192.168.1.1                100 (712) 1912 99 i
*> 99.99.99/24        192.168.1.1                100 (712) 1912 ?
```

After an network link failure on the Provider's network to the customer router, the VVNET router shows the following routes:

```
VVNET# bgp show routes all
BGP table : Local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop        Metric LocPrf Path
   -------            --------        ------ ------ ----
*> 99.99.99/24        192.168.1.1              100 (712) 1912 ?
```

The 66.66.66.0/24 route is removed as there is no longer OSPF connectivity to the customer router, so it is no longer advertised.

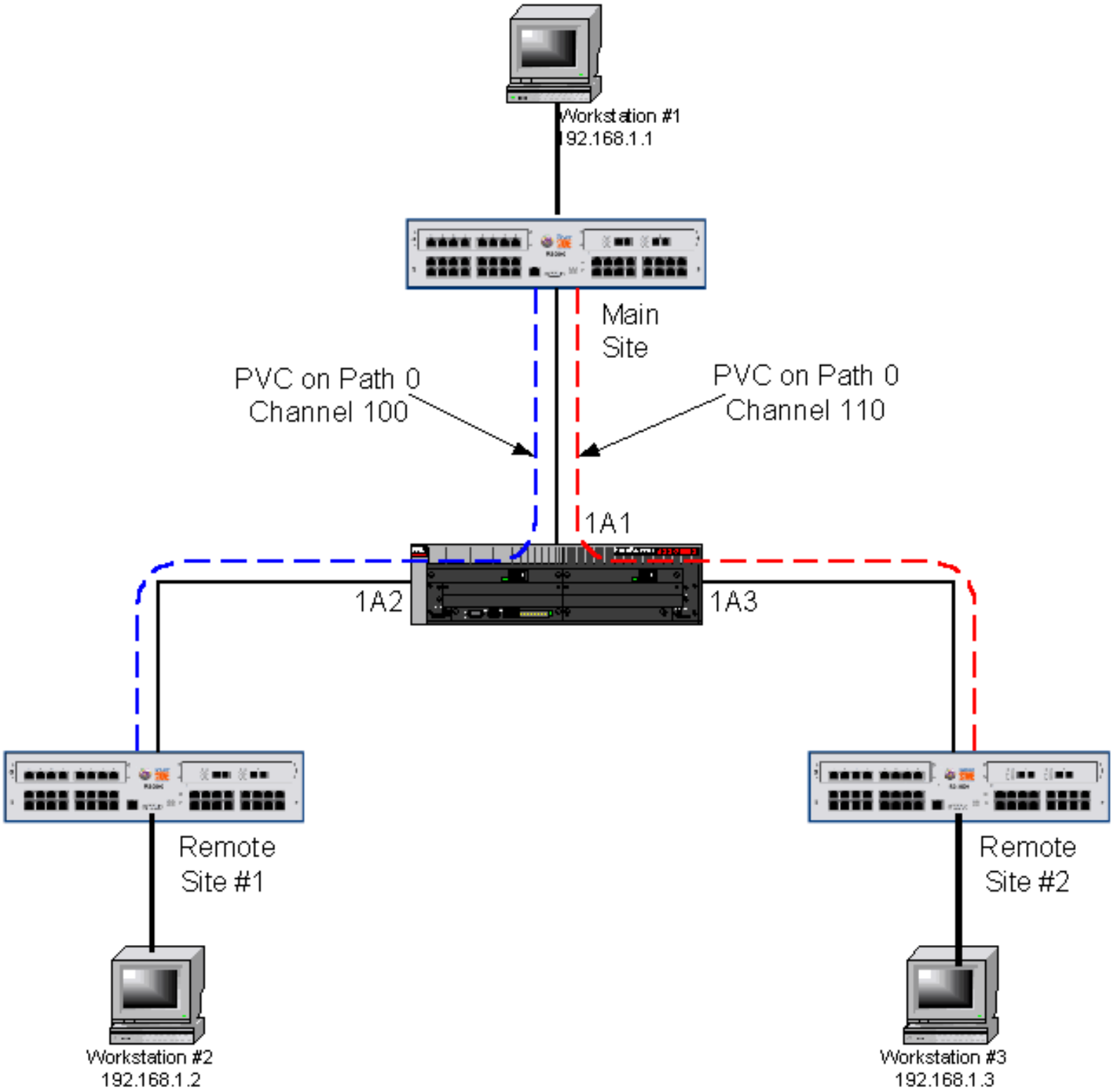
ATM Based Metro TLS

Michael Shrake
Systems Engineering
June 19, 2001

Today many metro service providers are still using ATM as a backbone technology. The need to service both data customers and voice customers has in the past mandated the use of ATM. To offer transparent LAN services across an ATM network, the customer is looking for a vendor that has support for Ethernet and ATM. To truly offer a transparent LAN to the customer, the vendor must be protocol independent. There are many people out there still using IPX and AppleTalk, and the TLS offering must allow these protocols to pass through the network.

RapidOS Version Tested	7.0.0.2
RapidOS Versions Working with this Configuration	7.0.0.2 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.2
Hardware Specifics	N/A

Diagram



Configurations

Main Site

```
atm create vcl port 3.1.0.100
atm create vcl port 3.1.0.110
vlan create atmtest port-based
```

```
vlan add ports at.3.1.0.100 to atmtest
vlan add ports at.3.1.0.110 to atmtest
vlan add ports et.1.1 to atmtest
```

Remote site #1

```
atm create vcl port 3.1.0.100
vlan create atmtest port-based
vlan add ports at.3.1.0.100 to atmtest
vlan add ports et.1.1 to atmtest
```

Remote site #2

```
atm create vcl port 3.1.0.110
vlan create atmtest port-based
vlan add ports at.3.1.0.110 to atmtest
vlan add ports et.1.1 to atmtest
```

Comments

With this configuration, all remote locations have layer-2 connectivity to the main site.

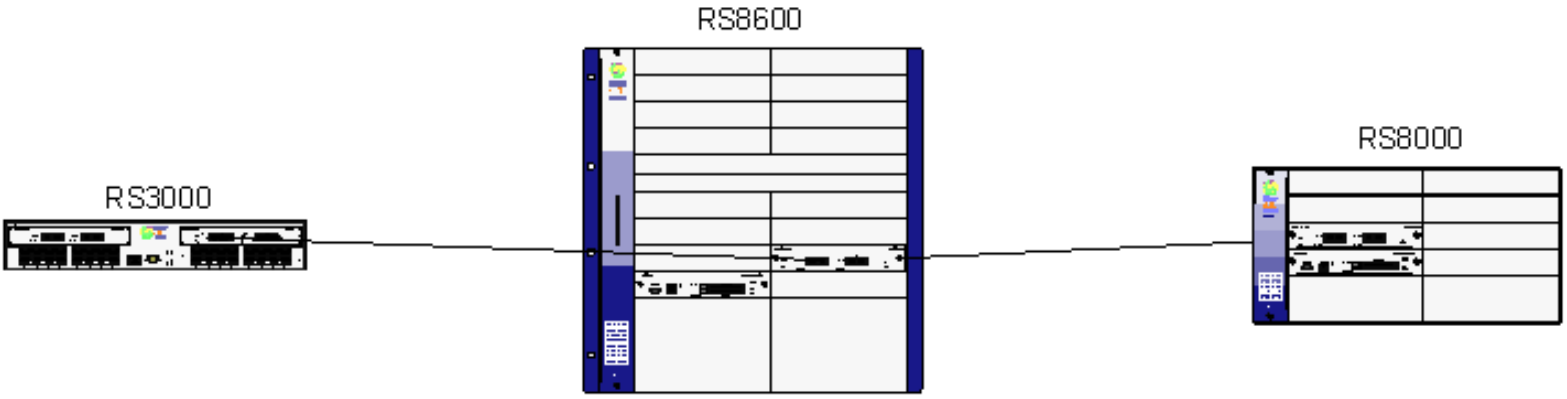
In a production environment there would be additional configuration items not shown here such as SNMP, a management IP address, etc.

ATM Cross-connects

Payam Kahen
Systems Engineering
November 30, 2001

This article demonstrates the use of the ATM Cross-connects to transparently patch together PVCs from two different ATM ports on the RS platform across the chassis. This function simulates the task of an ATM switch, while also allowing other PVCs to be switched or routed.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	ATM DS-3 and OC-3 Ports

Diagram



Configurations

RS8600

```
atm create vcl port at.3.1.0.40 aal1
atm create vcl port at.3.2.0.30 aal1
atm set cross-connect at.3.2.0.30 to at.3.1.0.40
!
system set name ATM-SWITCH
```

RS3000

```
atm create vcl port at.4.1.0.40
interface create ip ATM-LINK address-netmask 192.168.1.1/30 port at.4.1.0.40
!
system set name RS3000
```

RS8000

```
atm create vcl port at.2.1.0.30
interface create ip ATM-LINK address-netmask 192.168.1.2/30 port at.2.1.0.30
!
system set name RS8000
```

Comments

It is important to create VCs with the "aal1" option on the switch performing the cross-connect. This is to ensure that ATM traffic is processed as cells rather than the default "aal5" packets.

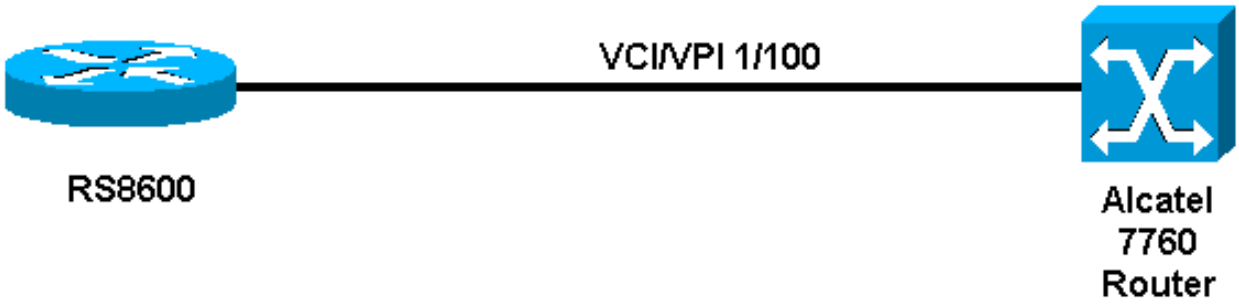
```
RS8000# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 36 data bytes
44 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.480 ms

--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.480/0.480/0.480 ms
```

ATM Interoperability with Alcatel Routers

Jeff McLaird
Corporate Systems Engineering
February 1, 2002

Sample Configuration for RS to Alcatel ATM interoperability.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	6.1.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.1.1.0
Hardware Specifics	ATM OC-12/ OC-3 line cards

Diagram



Configurations

RS8600

```
port set at.10.1 mtu 1532
!
atm create vcl port at.10.1.1.100
!
```

```
sonet set at.10.1 payload-scramble on
!
interface create ip test address-netmask 172.16.13.2/30 port at.10.1.1.100 type point-
to-point peer-address 172.16.13.1 output-mac-encapsulation ethernet_snap
!
ospf create area backbone
ospf add interface test to-area backbone
ospf start
```

Alcatel 7760

```
interface loopback 0
ip address 192.168.11.11
!
interface   1-10-2-4;1/100
encapsulation aal5snap
ip address 172.16.13.1/30
!
ip system router-id 192.168.11.11
router ospf
  redistribute connected
!
area 0.0.0.0 interface 1-10-2-4;1/100
```

Comments

The configuration example will work with all Alcatel routers that support ATM interfaces and most Newbridge/Alcatel switches. It is important to ensure that each end is set to AAL snap encapsulation since this is the only common encapsulation method supported by the Alcatel and Riverstone devices.

```
8600# atm show port-settings at.10.1
Port information for at.10.1:
    Port Type:            SONET OC-12c MMF
    Xmt Clock Source:     Local
    Reservable Bandwidth: 1236225 CPS, 524159400 bits/sec

8600# atm show vcl summary port at.10.1
VCL Table Contents for at.10.1:
              Admin     Oper      Service  PCR          SCR       MBS
  VPI/VCI    Status    Status    Category  Kbits/sec    Kbits/sec CPS
 ---------  --------  --------  ---------  ---------    --------- ---
    1/100         Up        Up   UBR       497600       NA        NA


8600# atm show vcl port at.10.1
VCL Table Contents for at.10.1:
    Virtual Path Identifier:    1
    Virtual Channel Identifier: 100
    MAC Address Limit:          No Limit
    QOS Settings:               Disabled
    Priority Settings:          Default values
    Cross Connect:              None
```

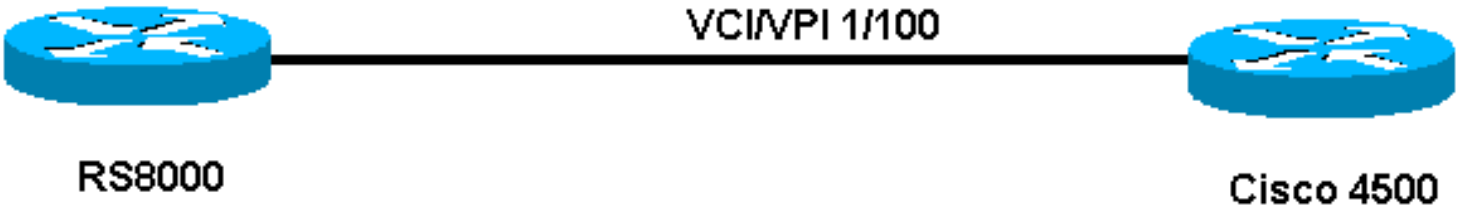
```
Force Bridge Format:        Disabled
AAL:                        AAL 5
Adminstrative Status:       Up
Operational Status:         Up
Last State Change:          14753
Service Definition:         user-default-OC12
    Service Class:      UBR
    Peak Bit Rate:      497600 Kbits/sec (1173584 CPS)
    Encapsulation Type: LLC Multiplexing
    Traffic Type:       RFC-1483, multi-protocol
    F5-OAM:             Responses Only
```

ATM Interoperability with Cisco Routers

Jeff McLaird
Corporate Systems Engineering
February 6, 2002

Sample Configuration for RS to Cisco 4500 router ATM interoperability.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	6.1.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.1.1.0
Hardware Specifics	ATM OC-12/ OC-3 line cards

Diagram



Configurations

RS8000

```
atm create vcl port at.3.1.0.100
!
interface create ip test address-netmask 10.10.1.1/30 port at.3.1.0.100
interface add ip lo0 address-netmask 10.1.1.1/32
!
ip-router global set router-id 10.1.1.1
ip-router global set autonomous-system 100
!
bgp create peer-group ebgp type external autonomous-system 200
bgp add peer-host 10.10.1.2 group ebgp
bgp start
```

Cisco 4500

```
cisco#sh conf
Using 686 out of 129016 bytes
!
version 11.1
service udp-small-servers
service tcp-small-servers
!
hostname cisco
!
enable secret 5 $1$6UuO$hr4yJHXVAhGwcrTbEaMB01
enable password yago1
!
!
!
interface Loopback0
 ip address 1.1.1.2 255.255.255.255
!
interface Fddi0
 ip address 204.132.11.1 255.255.255.0
 no keepalive
!
interface ATM0
 ip address 192.11.1.1 255.255.0.0
!
interface ATM0.100 multipoint
 ip address 10.10.1.2 255.255.255.252
 ip ospf network broadcast
 atm pvc 1 0 100 aal5snap inarp

!
autonomous-system 200
```

```
!
router bgp 200
 redistribute connected
 neighbor 10.10.1.1 remote-as 100
!
no ip classless
!
!
line con 0
line aux 0
 transport input all
line vty 0 4
 password yago1jrm
 login
!
end
```

Comments

The configuration example will work with all Cisco routers that support ATM interfaces. The configuration was testing with IOS version 11.1(3) but should work with all versions of IOS that offer ATM support.

```
rs# atm show port-settings at.3.1
Port information for at.3.1:
    Port Type:            SONET STS-3c MMF
    Media Type:           SONET
    Xmt Clock Source:     Local
    VC Mode:              1 bit of VPI, 11 bits of VCI
    Reservable Bandwidth: 309057 CPS, 131040168 bits/sec
    OAM Timers:           Detect Up: 15, Down: 15
    Service Definition:   default-OC3
        Service Class:      UBR
        Peak Bit Rate:      Best Effort
        Encapsulation Type: LLC Multiplexing
        Traffic Type:       RFC-1483, multi-protocol
        F5-OAM:             Responses Only

rs# atm show vcl port at.3.1
VCL Table Contents for at.3.1:
    Virtual Path Identifier:    0
    Virtual Channel Identifier: 100
    MAC Address Limit:          No Limit
    QOS Settings:               Disabled
    Priority Settings:          Default values
    Cross Connect:              None
```

```
    Force Bridge Format:        Disabled
    AAL:                        AAL 5
    Adminstrative Status:       Up
    Operational Status:         Up
    Last State Change:          209
    Service Definition:         default-OC3
        Service Class:      UBR
        Peak Bit Rate:      Best Effort
        Encapsulation Type: LLC Multiplexing
        Traffic Type:       RFC-1483, multi-protocol
        F5-OAM:             Responses Only

cisco#sh int atm0.100
ATM0.100 is up, line protocol is up
  Hardware is ATMizer BX-50
  Internet address is 10.10.1.2/30
  MTU 4470 bytes, BW 156250 Kbit, DLY 100 usec, rely 255/255, load 1/255
  Encapsulation ATM
```

ATM Interoperability with Zeitnet ATM Switches

Jeff McLaird
Corporate Systems Engineering
November 13, 2001

Sample Configuration for RS to Zeitnet ATM interoperability.	
RapidOS Version Tested	ROS 8.0.0.0
RapidOS Versions Working with this Configuration	ROS 6.1.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than ROS 6.1.0.0
Hardware Specifics	ATM OC-12/ OC-3 line cards

Diagram

Configurations

Zeitnet - ZX-250

```
#show pvc
PortNumber (all)

=================================================================
Conn  Conn    |       Low     VCI          |                |  Admin
Id    SubId   | Port  VPCI          Type   |  Port    Type  |  Status
=================================================================
5       1        B2     0      16   PTP        CPU     PTP        UP
6       1        B3     0      16   PTP        CPU     PTP        UP
8       1        B2     0     120   PTP         B3     PTP        UP
```

RS8000 - RSA

```
atm create vcl port at.5.1.0.120
interface create ip to-RSA address-netmask 207.141.77.1/30 port at.5.1.0.120
!
ospf create area backbone
ospf add interface to-RSA to-area backbone
ospf start
```

RS8000 - RSB

```
atm create vcl port at.4.2.0.130
interface create ip to-RSA address-netmask 207.141.77.2/30 port at.4.2.0.130
!
ospf create area backbone
ospf add interface to-RSA to-area backbone
ospf start
```

Comments

The configuration example will also work with Cabletron SmartSwitch 6500/2500 ATM switches which share the same architecture as the Zeitnet ATM switches. The configurations are very straightforward and no pay load scrambling is required.

The VCs on both RSA and RSB are configured with default settings.

```
RS-B# atm show vcl port at.4.2

VCL Table Contents for at.4.2:
```

```
Virtual Path Identifier:    0
Virtual Channel Identifier: 130
MAC Address Limit:          No Limit
QOS Settings:               Disabled
Priority Settings:          Default values
Cross Connect:              None
Force Bridge Format:        Disabled
AAL:                        AAL 5
Adminstrative Status:       Up
Operational Status:         Up
Last State Change:          362
Service Definition:         default-OC3
    Service Class:      UBR
    Peak Bit Rate:      Best Effort
    Encapsulation Type: LLC Multiplexing
    Traffic Type:       RFC-1483, multi-protocol
    F5-OAM:             Responses Only
```

ATM Point-Multipoint over Multiple PVCs

Scott Martin
Systems Engineering
August 16, 2001

This scenario depicts a CLEC which has an existing ATM infrastructure used for DSL aggregation. The use of the point to multipoint configuration allows for IP address conservation in lieu of using /30 point-to-point addresses. This is accomplished by adding multiple VPI/VCI's into a single VLAN, and then assigning an IP interface to the VLAN.

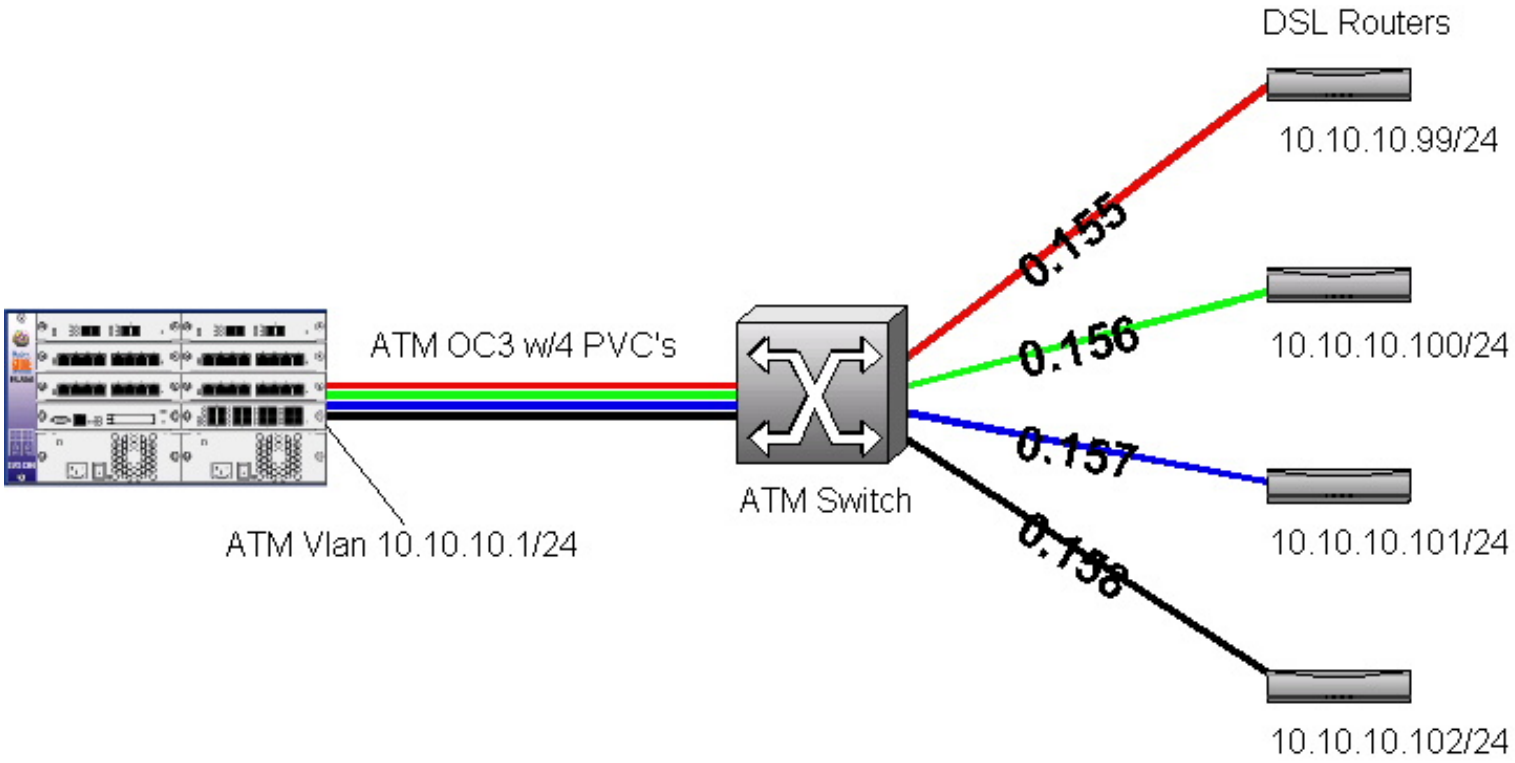
The Cisco equivalent:

```
interface ATM2/0 <-------------------------------------main atm interface
 description Connection to DSLAM's for DSL Service
 no ip address
 no ip mroute-cache
 atm framing cbitplcp
 no atm auto-configuration
 no atm ilmi-keepalive
 !
interface ATM2/0.155212176 multipoint <---------ATM subinterface
 description 155.212.176.X Multipoint DSL
 ip address 10.10.10.1 255.255.255.0 <-------gw for DSL router

pvc 0/155
  protocol ip 10.10.10.99 broadcast <-------ip DSL Router on pvc 1/2124
  encapsulation aal5snap
 !
 pvc 0/156
  protocol ip 10.10.10.100 broadcast
  encapsulation aal5snap
 !
 pvc 0/157
  protocol ip 10.10.10.101 broadcast
  encapsulation aal5snap
```

RapidOS Version Tested	7.0.0.3, 8.0.0.0
RapidOS Versions Working with this Configuration	7.0.0.3, 8.0.0.0
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0

Hardware Specifics	None

Diagram



Configurations

RS8000 ATM configuration

```
atm create vcl port at.1.1.0.155
atm create vcl port at.1.1.0.156
atm create vcl port at.1.1.0.157
atm create vcl port at.1.1.0.158

! Note Peer Addresses are needed only when the Peer does not accept inverse ARP
atm set peer-addr ip-address 10.10.10.99/24 port at.1.1.0.155
atm set peer-addr ip-address 10.10.10.100/24 port at.1.1.0.156
atm set peer-addr ip-address 10.10.10.101/24 port at.1.1.0.157
atm set peer-addr ip-address 10.10.10.102/24 port at.1.1.0.158

vlan create atm-dsl ip id 200

vlan add ports at.1.1.0.155 to atm-dsl
vlan add ports at.1.1.0.156 to atm-dsl
vlan add ports at.1.1.0.157 to atm-dsl
vlan add ports at.1.1.0.158 to atm-dsl

interface create ip atm-24 address-netmask 10.10.10.1/24 type broadcast vlan atm-dsl
```

L4 Quality of Service Mappings to VC's in ATM

Jeff McLaird
Corporate Systems Engineering
February 6, 2002

The following configuration example illustrates the use of policy based routing and ingress rate limiting to provide a mapping of L3/4 information to ATM VC's. Each VC has a specific traffic characteristic to match the traffic that will be traversing the link.

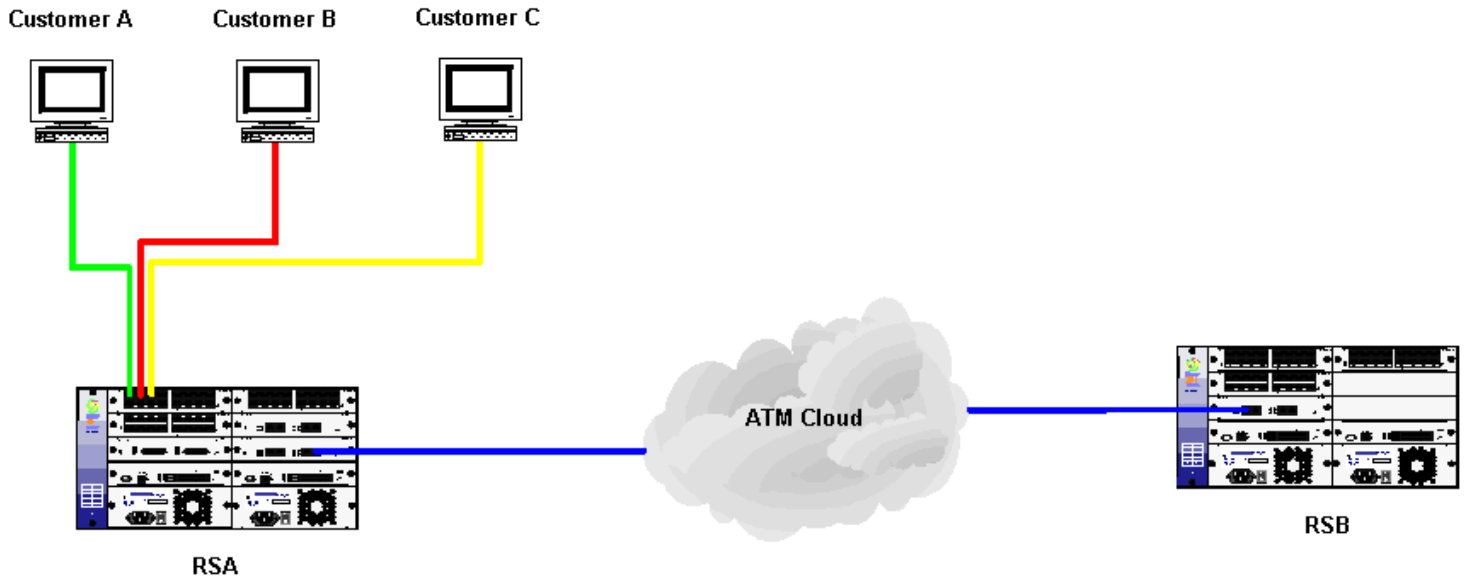
One of the challenges network administrators face when mapping customer traffic to PVC's is the lack of application sensitivity inherent in PVC configuration. In the classically quoted SVC client provisioning model the application itself requests a specific level of QoS via an API such as WinSock 2.0.

Since this is not possible in a purely static PVC environment one option available is for the ingress router or switch to classify incoming traffic based on transport layer information and map this traffic to a statically defined VC. The statically defined VC should then be configured with the service characteristics appropriate to the application that will be mapped to it.

For example a customer may be interested in providing a VoIP or video on demand service. Each of these traffic types have specific requirements in terms of relative latency and jitter. Toll quality voice will require constant cell rate guarantees. Thus a VCL for this type of traffic will be configured with a CBR service category with the appropriate Peak Cell Rate (PCR). Remember that in the case of CBR this is guaranteed bandwidth and no burst or sustainable cell rate is required.

RapidOS Version Tested	8.0.1.1
RapidOS Versions Working with this Configuration	6.1.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.1.1.0
Hardware Specifics	T-Series line cards or above. ATM OC-3

Diagram



Configurations

RS A

```
atm create vcl port at.4.1.0.100
atm create vcl port at.4.1.0.200
atm create vcl port at.4.1.0.300
atm define service HTTP srv-cat cbr pcr-kbits 5000
atm define service FTP srv-cat cbr pcr-kbits 1000
atm define service ANY srv-cat nrt-vbr pcr-kbits 5000 mbs 100 scr 4000
atm apply service HTTP port at.4.1.0.100
atm apply service FTP port at.4.1.0.200
atm apply service ANY port at.4.1.0.300
atm set vcl port at.4.1.0.(100,200,300) forced-bridged
interface create ip custA address-netmask 10.1.1.1/24 port et.1.1
interface create ip custB address-netmask 10.1.2.1/24 port et.1.2
interface create ip custC address-netmask 10.1.3.1/24 port et.1.3
interface create ip HTTP address-netmask 10.10.1.2/30 port at.4.1.0.100
interface create ip FTP address-netmask 10.10.1.6/30 port at.4.1.0.200
interface create ip ANY address-netmask 10.10.1.10/30 port at.4.1.0.300
interface add ip lo0 address-netmask 9.1.1.2/32
interface add ip en0 address-netmask 26.147.10.1/24
acl custA-HTTP permit ip 10.1.1.0/24 any any http
acl custB-HTTP permit ip 10.1.2.0/24 any any http
acl custB-FTP permit ip 10.1.2.0/24 any any ftp-cmd
acl custB-FTP permit ip 10.1.2.0/24 any any ftp-data
acl custA-FTP permit ip 10.1.1.0/24 any any ftp-cmd
acl custA-FTP permit ip 10.1.1.0/24 any any ftp-data
acl cust-A permit ip 10.1.1.0/24 any
acl cust-B permit ip 10.1.2.0/24 any
acl cust-C permit ip 10.1.3.0/24 any
acl custC-HTTP permit ip 10.1.3.0/24 any any http
acl custC-FTP permit ip 10.1.3.0/24 any any ftp-cmd
acl custC-FTP permit ip 10.1.3.0/24 any any ftp-data
ip-router global set router-id 9.1.1.2
ospf create area backbone
ospf add interface all to-area backbone
ospf add stub-host 9.1.1.2 to-area backbone cost 5
ospf add interface 10.10.1.2 to-area backbone
ospf add interface 10.10.1.6 to-area backbone
ospf add interface 10.10.1.10 to-area backbone
ospf start
ip-policy custB-HTTP permit acl custB-HTTP next-hop-list 10.10.1.1 action policy-only
sequence 20
ip-policy custB-FTP permit acl custB-FTP next-hop-list 10.10.1.5 action policy-only
sequence 20
```

```
ip-policy custA-HTTP permit acl custA-HTTP next-hop-list 10.10.1.1 action policy-only
sequence 20
ip-policy custA-FTP permit acl custA-FTP next-hop-list 10.10.1.5 action policy-only
sequence 20
ip-policy custB-any permit acl everything-else next-hop-list 10.10.1.9 action policy-
only sequence 25
ip-policy custC-HTTP permit acl custC-HTTP next-hop-list 10.10.1.1 action policy-only
ip-policy custC-FTP permit acl custC-FTP next-hop-list 10.10.1.5 action policy-only
ip-policy custC-ANY permit acl custC-ANY next-hop-list 10.10.1.9 action policy-only
ip-policy custC-any permit acl everything-else next-hop-list 10.10.1.9 action policy-
only sequence 25
ip-policy custA-ANY permit acl everything-else next-hop-list 10.10.1.9 action policy-
only sequence 25
ip-policy custB-HTTP apply interface custB
ip-policy custB-FTP apply interface custB
ip-policy custA-HTTP apply interface custA
ip-policy custA-FTP apply interface custA
ip-policy custB-any apply interface custB
system enable aggregate-rate-limiting slot 1
service gold create rate-limit burst-safe car-rate 5000000 burst-rate 7000000 car-
lower-priority burst-drop-packets
service silver create rate-limit burst-safe car-rate 3000000 burst-rate 5000000 car-
lower-priority burst-drop-packets
service bronze create rate-limit burst-safe car-rate 1000000 burst-rate 1100000 car-
drop-packets burst-drop-packets
service gold apply rate-limit acl cust-A interface custA
service silver apply rate-limit acl cust-B interface custB
service bronze apply rate-limit acl cust-C interface custC
qos create priority-map gold 0 high 1 high 2 high 3 high 4 high 5 high 6 high 7 high
qos create priority-map silver 0 medium 1 medium 2 medium 3 medium 4 medium 5 medium
6 medium 7 medium
qos create priority-map bronze 0 low 1 low 2 low 3 low 4 low 5 low 6 low 7 low
qos apply priority-map gold ports et.1.1
qos apply priority-map silver ports et.1.2
qos apply priority-map bronze ports et.1.3
```

RS B

```
atm create vcl port at.2.1.0.100
atm create vcl port at.2.1.0.200
atm create vcl port at.2.1.0.300
atm set vcl port at.4.1.0.(100,200,300) forced-bridged
interface create ip HTTP address-netmask 10.10.1.1/30 port at.2.1.0.125
interface create ip FTP address-netmask 10.10.1.5/30 port at.2.1.0.150
interface create ip ANY address-netmask 10.10.1.9/30 port at.2.1.0.175
interface add ip lo0 address-netmask 9.1.1.1/32
ip-router global set router-id 9.1.1.1
ospf create area backbone
ospf add interface all to-area backbone
ospf add stub-host 9.1.1.1 to-area backbone cost 5
ospf add interface 10.10.1.1 to-area backbone
ospf add interface 10.10.1.5 to-area backbone
ospf add interface 10.10.1.9 to-area backbone
ospf start
```

Comments

The configuration illustrated provides a QoS mapping mechanism to provide for in this instance 3 SLA's, which are provided via multiple mechanisms. The configuration provides for the commonly referenced gold, silver and bronze service levels. Additional granularity is included with the ability to map specific Layer 4 information using PBR to define separate next hop gateways. Each next hop gateway corresponds with a different VC that also has separate service characteristics.

Ingress Rate Limit Policy

In this example we start out by providing a rate limited ingress policy. This is used to define a rate limited service level based on a defined committed access rate with burst characteristics. The limits are defined as:

SLA	CAR Rate (Megs)	Burst Rate (Megs)	CAR Violation	Burst Violation

Gold	5	7	Lower Priority	Lower Priority
Silver	3	5	Lower Priority	Drop Packets
Bronze	1	1.2	Drop Packets	Drop Packets

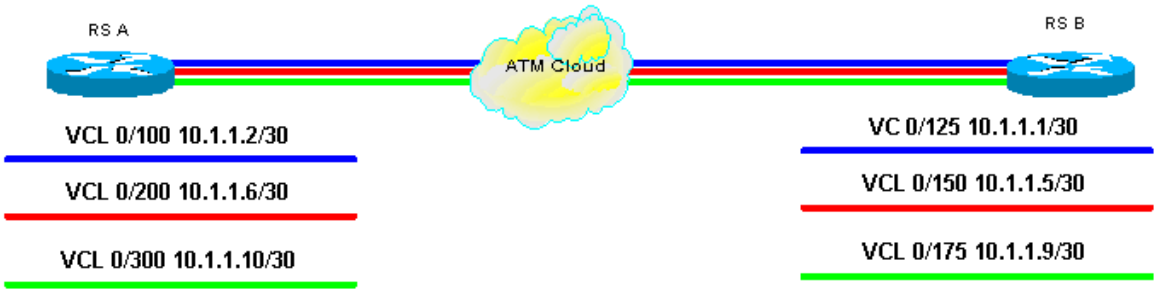
QoS Queue Mapping

In order to include a policy where the queue definition is lowered on violation of a specific rate limit it is also necessary to ensure that traffic is arriving with the correct queue mapping that will allow the traffic to be lowered in the first place. If all traffic is placed in the low priority queue it is obviously impossible to place traffic in violation of the SLA in a lower queue. This action is defined within the RS using QoS priority queuing maps. The following traffic queues are used for all traffic on ingress to RSA:

SLA	Map Traffic to Queue
Gold	High
Silver	Medium
Bronze	Low

Mapping the Next Hop

Using Policy Based Routing provides the mechanism to map specific traffic types based on the Layer 4 information to specific VC's egressing RSA. It should be noted that we are using PBR to map the traffic to a specific next hop in lieu of a mechanism to map ingress traffic directly to a specific VC. The logical for this configuration is illustrated below.



Defining the VC Service Characteristics

This configuration example contains three VC service characteristic profiles, one per VC. This is a very simple implementation containing only three Virtual Circuits and hence three profiles. The profiles are defined as:

Service	Service Class	Peak Cell Rate	Maximum Burst	Sustained Cell Rate
HTTP	CBR	5000	N/A	N/A
FTP	CBR	1000	N/A	N/A
Any	Nrt-VBR	5000	100	4000

Since it is only possible at the current time to map a single service characteristic to a VC when creating complex SLA mappings to VCL's a separate VCL must be created for each Service. The values given for the configuration are strictly for example only. An appropriate data rate should be chosen based on the application bandwidth requirements.

Interoperability with Cisco DS3 ATM

Jeff McLaird
Corporate Escalations Engineering
July 9, 2002

The following configuration example illustrates interoperability between the RS platform and Cisco's 7206 VXR. The configuration should essentially be the same for all IOS based platforms using the Enhanced ATM PA hardware.	
RapidOS Version Tested	8.0.3.5
RapidOS Versions Working with this Configuration	6.1.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.1.1.0
Hardware Specifics	T-Series line cards or newer, ATM OC-3

Diagram

Configurations

RS

```
port set et.2.1 duplex full speed 100mbps
atm set port at.7.2 cell-mapping plcp
atm set port at.7.2 pdh-cell-scramble on
atm create vcl port at.7.2.0.100
interface create ip test address-netmask 15.1.1.1/24 port et.1.1
interface create ip 2cisco address-netmask 10.10.30.2/24 port at.7.2.0.100
interface create ip serve address-netmask 172.21.4.249/16 port et.1.8
interface add ip lo0 address-netmask 143.90.200.1/32
interface add ip en0 address-netmask 172.21.4.249/16
ip-router global set autonomous-system 65200
ip-router global set router-id 143.90.200.1
ip-router policy redistribute from-proto direct to-proto ospf
ospf create area backbone
ospf add stub-host 143.90.200.1 to-area backbone cost 5
ospf add interface 10.10.30.2 to-area backbone type broadcast
ospf set interface 10.10.30.2 priority 0
ospf start
bgp create peer-group ebgp type external autonomous-system 65000
bgp create peer-group ibgp type routing autonomous-system 65200 proto ospf
bgp add peer-host 15.1.1.2 group ebgp
bgp add peer-host 10.10.2.1 group ibgp
bgp set multipath off
bgp set peer-group ibgp local-address 143.90.200.1
bgp set peer-group ibgp next-hop-self
bgp start
system set name client1
```

Cisco 7200VXR

```
!
version 12.2
no service pad
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname CiscoVXR
!
boot system disk1:c72001223.bin
logging buffered 32000 debugging
enable secret 5 $1$YG3U$Y8ROOcyEY1NN73euOmZWI1
enable password riverstone
!
clock timezone cst -6
clock summer-time edt recurring 1 Sun Apr 2:00 last Sun Oct 3:00
```

```
ip subnet-zero
!
!
no ip domain-lookup
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 10.10.2.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.0.0.60 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex full
!
interface ATM2/0
 ip address 10.10.30.1 255.255.255.0
 ip ospf network broadcast
 ip ospf mtu-ignore
 atm scrambling cell-payload
 atm framing cbitplcp
 atm pvc 1 0 100 aal5snap inarp
 no atm ilmi-keepalive
!
interface FastEthernet3/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 duplex full
!
interface FastEthernet4/0
 no ip address
 no ip route-cache
 no ip mroute-cache
 no keepalive
 shutdown
 duplex full
 hold-queue 4096 in
 hold-queue 4096 out
!
interface FastEthernet4/0.1
```

```
 no ip route-cache
 no ip mroute-cache
!
autonomous-system 65200
!
router ospf 100
 log-adjacency-changes
 network 10.10.2.1 0.0.0.0 area 0
 network 10.10.30.1 0.0.0.0 area 0
 default-information originate always
!
router bgp 65200
 no synchronization
 bgp log-neighbor-changes
 network 143.90.0.0
 network 192.168.0.0 mask 255.255.0.0
 neighbor ibgp peer-group
 neighbor ibgp remote-as 65200
 neighbor ibgp route-reflector-client
 neighbor 143.90.200.1 peer-group ibgp
 neighbor 143.90.200.1 soft-reconfiguration inbound
 neighbor 143.90.200.2 peer-group ibgp
 neighbor 143.90.200.2 soft-reconfiguration inbound
 no auto-summary
!
ip classless
ip route 143.90.0.0 255.255.0.0 Null0
ip route 172.21.1.76 255.255.255.255 172.21.4.249
ip route 172.23.4.0 255.255.255.0 10.0.0.1
ip route 192.168.0.0 255.255.0.0 Null0 250
no ip http server
!
!
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
bridge 4 protocol ieee
bridge 5 protocol ieee
!
!
gatekeeper
 shutdown
!
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 60 0
 password riverstone
```

```
 no login
line vty 5 15
 login
!
end
```

Comments

It is important to ensure that scrambling and the framing bit is set correctly to bring the link up. Other things you should consider is that in the event of configuring OSPF to run over the DS3 link it is important to set the OSPF ignore MTU line.

```
CiscoVXR#show contr atm 2/0
Interface ATM2/0 is up
Hardware is ENHANCED ATM PA - DS3 (45000Kbps)
Framer is PMC PM7345 S/UNI-PDH, SAR is LSI ATMIZER II
Firmware rev: G129, Framer rev: 1, ATMIZER II rev: 3
  idb=0x628FA7C0, ds=0x629020E0, vc=0x62932420
  slot 2, unit 1, subunit 0, fci_type 0x005B, ticks 4538
  1200 rx buffers: size=512, encap=64, trailer=28, magic=4
Curr Stats:
  VCC count: current=1, peak=1
  SAR crashes: Rx SAR=0, Tx SAR=0
  rx_cell_lost=0, rx_no_buffer=0, rx_crc_10=0
  rx_cell_len=0, rx_no_vcd=6, rx_cell_throttle=0, tx_aci_err=0
Rx Free Ring status:
  base=0x3D26E040, size=2048, write=880
Rx Compl Ring status:
  base=0x77255C20, size=2048, read=572
Tx Ring status:
  base=0x3D7135C0, size=8192, write=708
Tx Compl Ring status:
  base=0x07259C60, size=4096, read=354
BFD Cache status:
  base=0x6292C3A0, size=6144, read=6143
Rx Cache status:
base=0x629238A0, size=16, write=12
Tx Shadow status:
  base=0x62924320, size=8192, read=703, write=708
Control data:
  rx_max_spins=2, max_tx_count=17, tx_count=5
  rx_threshold=800, rx_count=12, tx_threshold=4608
  tx bfd write indx=0x10DF, rx_pool_info=0x62923940
Control data base address:
       rx_buf_base = 0x071A3780        rx_p_base = 0x6290DD00
            rx_pak = 0x62923584              cmd = 0x6290D720
            framer = 0x603D1264        framer_cb = 0x6290DB20
       framer_base = 0x3D100000     pci_pa_stats = 0x7725DCA0
```

```
    device_base[0] = 0x3D000000   device_base[1] = 0x3D400000
     ssram_base[0] = 0x3D200000    ssram_base[1] = 0x3D600000
     sdram_base[0] = 0x3D300000    sdram_base[1] = 0x3D700000
     pa_cmd_buf[0] = 0x3D27FC00    pa_cmd_buf[1] = 0x3D67FC00
       vcd_base[0] = 0x3D200000      vcd_base[1] = 0x3D618000
      chip_dump[0] = 0x0725DCC4     chip_dump[1] = 0x0725DDB4
   sar_buf_base[0] = 0x3D31C000  sar_buf_base[1] = 0x3D71C000
       bfd_base[0] = 0x3D256000      bfd_base[1] = 0x3D600000
       acd_base[0] = 0x3D220080      acd_base[1] = 0x3D638240
Framer Information:
 Framing mode: DS3 C-bit PLCP
 No alarm detected
Facility statistics: current interval elapsed 38 seconds
          lcv       fbe       ezd        pe       ppe      febe      hcse
   ---------------------------------------------------------------------

         bipe       fbe      febe
    ----------------------------

   lcv:  Line Code Violation
   be:   Framing Bit Error
   ezd:  Summed Excessive Zeros
   pe:   Parity Error
   ppe:  Path Parity Error
   febe: Far-end Block Error
   hcse: Rx Cell HCS Error
   bipe: Bit Interleave Parity (B1) Error

CiscoVXR# sh int atm 2/0
ATM2/0 is up, line protocol is up
  Hardware is ENHANCED ATM PA
  Internet address is 10.10.30.1/24
  MTU 4470 bytes, sub MTU 4470, BW 40704 Kbit, DLY 190 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Encapsulation(s): AAL5
  4095 maximum active VCs, 1 current VCCs
  VC idle disconnect time: 300 seconds
  7 carrier transitions
  Last input 00:00:09, output 00:00:02, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: Per VC Queueing
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     746 packets input, 57350 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     42 input errors, 42 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     846 packets output, 59945 bytes, 0 underruns
```

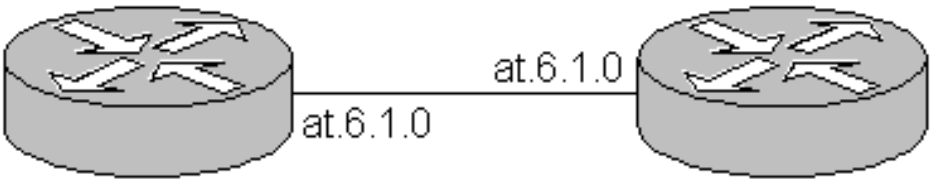
```
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

L2 Bridging over ATM

Victor A. Quiros
RTAC
July 11, 2002

The following configuration is used to demonstrate how to configure bridging over ATM interface line cards using two Riverstone routers back to back. The configuration also demonstrates rate-limiting on an ATM OC-3 interface.	
RapidOS Version Tested	8.0.3.5
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	ATM line card

Diagram



Configurations

atmbridge1

```
atm create vcl port at.6.1.0.91
atm create vcl port at.6.1.0.92
atm create vcl port at.6.1.0.93
atm create vcl port at.6.1.0.94
atm create vcl port at.6.1.0.95
atm define service 500k srv-cat cbr pcr 1179
vlan create v91 port-based id 91
vlan create v92 port-based id 92
vlan create v93 port-based id 93
vlan create v94 port-based id 94
vlan create v95 port-based id 95
vlan add ports at.6.1.0.91 to v91
vlan add ports at.6.1.0.92 to v92
vlan add ports at.6.1.0.93 to v93
vlan add ports at.6.1.0.94 to v94
vlan add ports at.6.1.0.95 to v95
atm apply service 500k port at.6.1.0
system set name atmbridge1
system set idle-timeout serial 0 telnet 0
```

atmbridge2

```
atm create vcl port at.6.1.0.1
atm create vcl port at.6.1.0.2
atm create vcl port at.6.1.0.3
atm create vcl port at.6.1.0.4
atm create vcl port at.6.1.0.5
atm define service 500k srv-cat cbr pcr 1179
vlan create v1 port-based id 1
vlan create v2 port-based id 2
vlan create v3 port-based id 3
vlan create v4 port-based id 4
vlan create v5 port-based id 5
vlan add ports at.6.1.0.1 to v1
vlan add ports at.6.1.0.2 to v2
vlan add ports at.6.1.0.3 to v3
vlan add ports at.6.1.0.4 to v4
vlan add ports at.6.1.0.5 to v5
atm apply service 500k port at.6.1.0
system set name atmbridge2
```

```
system set idle-timeout serial 0 telnet 0
```

Comments

```
atmbridge1# atm show port-stats at.6.1
Framework Counters:
  Receive VC Closed:  14
  Receive Queue Full: 0

Utopia Counters:
  Receive VC Closed: 14
  Transmit Cells:    72
  Receive Cells:     82
  Cells w/Bad HEC:   0

AAL5 Counters:
  Transmit Packets:       34
  Transmit Abort Packets: 0
  Transmit Cells:         72
  Receive Packets:        38
  Receive Abort Packets:  0
  Receive Cells:          82

FPGA statistics:
   Transmit packets dropped due to error:   0
   Transmit queue full:                     0
   Receive packets with CRC error:          0
   Receive packets with format error:       0

atmbridge1# atm show service all
default-OC3
    Service Class:       UBR
    Peak Bit Rate:       Best Effort
    Encapsulation Type:  LLC Multiplexing
    Traffic Type:        RFC-1483, multi-protocol
    OAM:                 Responses Only
    MAC Address Limit:   Disabled
    QOS Settings:        Disabled
    Priority Settings:   Default values
    AIS/RDI Support:     Disabled

default-OC3
    Service Class:       UBR
    Peak Bit Rate:       497600 Kbits/sec (1173584 CPS)
    Encapsulation Type:  LLC Multiplexing
```

```
    Traffic Type:        RFC-1483, multi-protocol
    OAM:                 Responses Only
    MAC Address Limit:   Disabled
    QOS Settings:        Disabled
    Priority Settings:   Default values
    AIS/RDI Support:     Disabled

atmbridge1# show vc-stats oam port at.6.1
at.6.1.0.90 Transmitted OAM Cells

      End Loop   Segment Loop      AIS           RDI
   +------------+-------------+------------+------------+
F5 |          0 |          0  |          0 |          0 |
   +------------+-------------+------------+------------+
F4 |          0 |          0  |          0 |          0 |
   +------------+-------------+------------+------------+

at.6.1.1.90 Received OAM Cells

      End Loop   Segment Loop      AIS           RDI
   +------------+-------------+------------+------------+
F5 |          0 |          0  |          0 |          0 |
   +------------+-------------+------------+------------+
F4 |          0 |          0  |          0 |          0 |
   +------------+-------------+------------+------------+

Cells Dropped: 0
```

Pebbles of Knowledge

When you set up a configuration of this nature and wish to rate limit the port to a certain rate you must use this command listed below. By applying this command the port traffic rate limit will be set to 500K. Note that slot number, port number and VP identifier are needed, but it cannot be per-VC.

```
atm apply service 500k port at.x.y.z
```

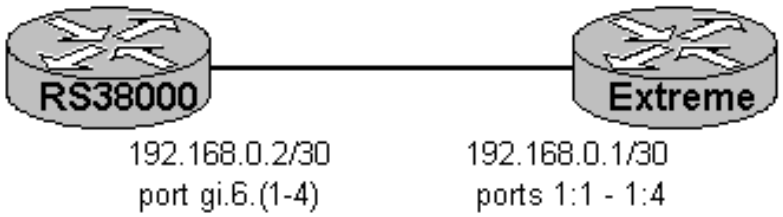
[Home][Documentation][Index]

CWDM Interoperability with Extreme

Frank Koniszewski
Systems Engineering
May 7, 2001

Demonstrate interoperability between Riverstone CWDM and Extreme CWDM. The goal was to create a 4Gb smarttrunk load sharing group with 4 lambdas in each group. The configuration consisted of a smarttrunk with 4 Gb ports on the RS38000 and an Extreme BlackDiamond.	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	CWDM

Diagram



Configurations

RS38000

```
smarttrunk create st.6 protocol no-protocol
smarttrunk add ports gi.6.(1-4) to st.6
interface create ip WDM-6 port st.6 address-netmask 192.168.0.2/30
```

Extreme BlackDiamond

```
configure slot 1 module wdm
create vlan WDM
config default delete port 1:1 - 1:4
config WDM add port 1:1 - 1:4
config WDM ipaddress 192.168.0.1/30
enable sharing 1:1 grouping 1:1,1:2,1:3,1:4 algorithm <round-robin, port-based,
address-based>
disable edp port 1:1
configure s0 add vlan WDM
disable stpd s0 port 1:1
```

Comments

Here are the results of a series of ping tests from the RS38000 smarttrunk group to the Extreme BD load-sharing group with a destination IP of 192.168.0.1.

All tests are run with the "ping 192.168.0.1 flood packets 1000 size 1500" command.

There are three sets of statistics from the RS38000, depending on the algorithm set on the Extreme for load-sharing.

In blue are the statistics from the RS38000 with the algorithm on the Extreme set to port-based- (Uses the ingress port as criteria for egress port selection),

The statistics in red are with the algorithm on the Extreme set to address-based - (Uses addressing information as criteria for egress port selection),

And the statistics in green the algorithm on the Extreme is set to round-robin - (Forwards packets to all egress ports in a round-robin fashion).

Notice in all cases we send the same number of packets out each port, but the Extreme only responds on port/lambda 1 with all responses irregardless of the algorithm set. This is also shown from the last set of statistics in black, which are from the Extreme. It is clear that the Extreme is receiving on all four lambdas, but is only replying on the first.

The only conclusion I can come to is that we will not be able to create a 4 Gb trunk between RSTN CWDM and Extreme CWDM until Extreme supports 802.3ad, which they presently do not.

```
Extreme Algorithm Port-Based
rs# statistics show port-packets gi.6.(1-4)

Port: gi.6.1
----
RMON Stats                  Received              Transmitted
----------                  --------              -----------
Unicast frames              2000                  500
```

```
Multicast frames              1                       0
Broadcast frames              0                       0
64 byte frames                1                       0
65-127 byte frames            1000                    0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         1000                    500
RMON stats cleared   2001-04-26 11:42:31

Port: gi.6.2
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       500
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 11:42:31

Port: gi.6.3
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       500
RMON stats cleared   2001-04-26 11:42:31

Port: gi.6.4
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       500
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 11:42:31

rs# statistics show port-packets gi.6.(1-4)

Port: gi.6.1
```

```
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                2001                    500
Multicast frames              0                       0
Broadcast frames              0                       1
64 byte frames                1                       1
65-127 byte frames            1000                    0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         1000                    500
RMON stats cleared   2001-04-26 12:20:45

Port: gi.6.2
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       500
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 12:20:45

Port: gi.6.3
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       500
RMON stats cleared   2001-04-26 12:20:45

Port: gi.6.4
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       501
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       501
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 12:20:45
```

```
rs# statistics show port-packets gi.6.(1-4)

Port: gi.6.1
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                2001                    500
Multicast frames              0                       0
Broadcast frames              0                       1
64 byte frames                1                       1
65-127 byte frames            1000                    0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         1000                    500
RMON stats cleared   2001-04-26 12:27:54

Port: gi.6.2
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       500
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 12:27:54

Port: gi.6.3
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       500
Multicast frames              0                       0
Broadcast frames              0                       0
Broadcast frames              0                       0
65-127 byte frames            0                       0
128-255 byte frames           0                       0
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       500
RMON stats cleared   2001-04-26 12:27:54

Port: gi.6.4
----
RMON Stats                    Received                Transmitted
----------                    --------                -----------
Unicast frames                0                       501
Multicast frames              0                       0
Broadcast frames              0                       0
64 byte frames                0                       0
65-127 byte frames            0                       501
128-255 byte frames           0                       0
```

```
256-511 byte frames           0                       0
512-1023 byte frames          0                       0
1024-1518 byte frames         0                       0
RMON stats cleared   2001-04-26 12:27:54
```

Extreme

```
Port Statistics                                          Thu Apr 26 18:00:41 2001
Port        Link      Tx Pkt     Tx Byte       Rx Pkt     Rx Byte   Rx     Rx
            Status    Count      Count         Count      Count     Bcast  Mcast
=============================================================================
 1:1          A       6008     4752512         1501     2277064       1       0
 1:2          A          0           0         1500       99000       0       0
 1:3          A          0           0         1500     2277000       0       0
 1:4          A          0           0         1501       99066       0       0
```

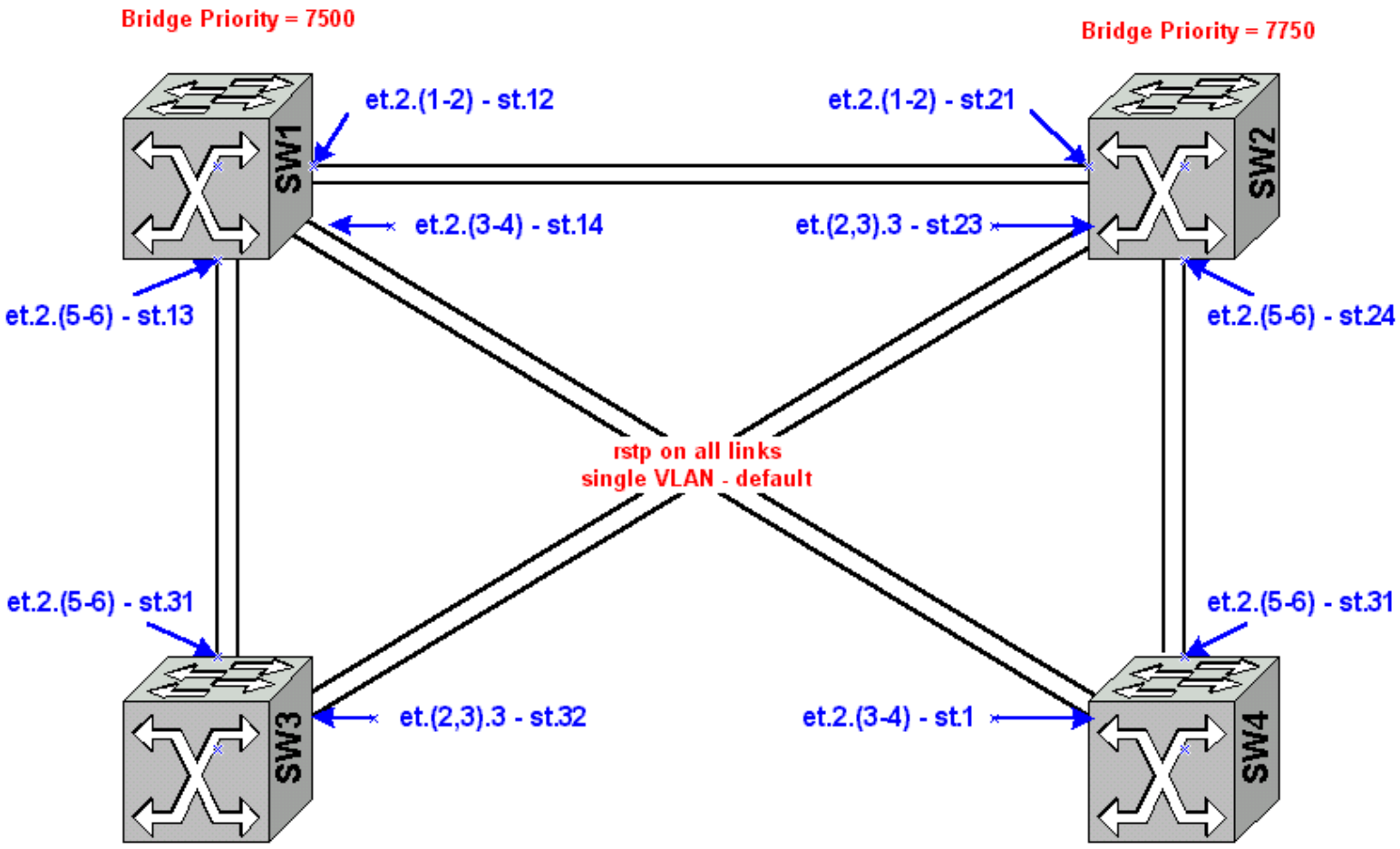
Link Aggregation 802.3ad

Richard Foote
Corporate Systems Engineering
June 22, 2001

The configuration is meant to demonstrate the basic 802.3ad configuration deployed with spanning tree to provide a highly scaleable and reliable layer two switched infrastructure. The standard 802.3ad Link Aggregation has been used instead of Riverstone's SmartTrunk technology because of the standards based nature of 802.3ad. Riverstone is not restricted on the number of Aggregations that can be deployed at a box level. The 802.3ad configuration differs from the Riverstone SmartTrunk configuration in numerous ways. All links in an aggregate must be the same link technology and specified as part of the command. As well it is important to note, the way ports are assigned to each aggregation is by the "`port-key`" command on a per port basis. This command links the port to the proper aggregation. Rapid spanning tree has been used to ensure fast convergence in the even of a spanning tree topology change. The root bridge has been designated by setting the "Bridge Priority" to be the lowest of all the switches in the infrastructure. The root bridge of choice is SW1, configured with a priority of 7500. To ensure a predictive fail over, the backup root bridge has been assigned a priority of 7750. All other switches in the infrastructure use the default priority of 8000. This configuration and commentary focus on link aggregation, 802.3ad, and not the difference between spanning tree and rapid spanning tree.

RapidOS Version Tested	7.0.0.3
RapidOS Versions Working with this Configuration	7.0.0.0 and above
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

SW1

```
smarttrunk create st.12 protocol lacp
smarttrunk create st.13 protocol lacp
smarttrunk create st.14 protocol lacp
lacp set aggregator st.12 actor-key 12 partner-key 21 port-type 10-100-ethernet
lacp set aggregator st.13 actor-key 13 partner-key 31 port-type 10-100-ethernet
lacp set aggregator st.14 actor-key 14 partner-key 41 port-type 10-100-ethernet
lacp set port et.2.(1-2) enable port-key 12
lacp set port et.2.(3-4) port-key 14 enable
lacp set port et.2.(5-6) port-key 13 enable
stp set protocol-version rstp
stp set bridging priority 7500
stp enable port st.12
stp enable port st.13
stp enable port st.14
interface add ip en0 address-netmask 24.112.73.4/21
system set name SW1
```

SW2

```
smarttrunk create st.21 protocol lacp
smarttrunk create st.23 protocol lacp
smarttrunk create st.24 protocol lacp
lacp set aggregator st.21 actor-key 21 partner-key 12 port-type 10-100-ethernet
lacp set aggregator st.24 actor-key 24 partner-key 42 port-type 10-100-ethernet
lacp set aggregator st.23 actor-key 23 partner-key 32 port-type 10-100-ethernet
```

```
lacp set port et.2.(1-2) port-key 21 enable
lacp set port et.2.(5-6) port-key 24 enable
lacp set port et.(2,3).3 port-key 23 enable
stp set protocol-version rstp
stp set bridging priority 7750
stp enable port st.21
stp enable port st.23
stp enable port st.24
interface add ip en0 address-netmask 24.112.73.3/21
system set name SW2
```

SW3

```
smarttrunk create st.31 protocol lacp
smarttrunk create st.32 protocol lacp
lacp set aggregator st.31 actor-key 31 partner-key 13 port-type 10-100-ethernet
lacp set aggregator st.32 actor-key 32 partner-key 23 port-type 10-100-ethernet
lacp set port et.2.(5-6) port-key 31 enable
lacp set port et.(2,3).3 port-key 32 enable
stp set protocol-version rstp
stp enable port st.31
stp enable port st.32
interface add ip en0 address-netmask 24.112.73.5/21
system set name SW3
```

SW4

```
smarttrunk create st.1 protocol lacp
smarttrunk create st.2 protocol lacp
lacp set aggregator st.1 actor-key 41 partner-key 14 port-type 10-100-ethernet
lacp set aggregator st.2 actor-key 42 partner-key 24 port-type 10-100-ethernet
lacp set port et.2.(3-4) port-key 41 enable
lacp set port et.2.(5-6) port-key 42 enable
stp set protocol-version rstp
stp enable port st.1
stp enable port st.2
interface add ip en0 address-netmask 24.112.73.2/21
system set name SW4
```

Comments

Verifying the actual aggregation is done by using the "**`smartrunk show connections all-smartrunks`**" command. A sample of the output is displayed from the perspective of SW1 below. The key information relates back to the "**`lacp set aggregator`**" command, where the router assigns its reference tag to allow ports to be assigned to a specific aggregation and what the partner or remote peers information is expected to be.

```
SW1# smarttrunk show connections all-smarttrunks
                                                                        Actor
Partner
SmartTRUNK Local Port  Remote Switch        Remote Module   Remote Port  State  Key
Key
---------- ----------  -------------        -------------   -----------  ------ ---- -
----
st.12      et.2.1      Riverstone CD:22:3D  --              33           Up     12
21
st.12      et.2.2      Riverstone CD:22:3D  --              34           Up     12
21
st.13      et.2.5      00:02:85:05:B2:C0    --              37           Up     13
31
st.13      et.2.6      00:02:85:05:B2:C0    --              38           Up     13
31
st.14      et.2.3      Riverstone 66:EE:71  --              35           Up     14
```

```
41
st.14      et.2.4      Riverstone 66:EE:71  --              36           Up     14
41
```

The "key" information plays a major role in troubleshooting SmartTrunk problems. You will notice that the index has some excellent information in it. Each index has the local **MAC** address used and the locally configured "**actor-key**" as well as the remote **MAC** and "**partner-key**". An example of a properly connected network will look something like this, again using SW1.

```
SW1# lacp show lag all-unique
LAG index 33
        Id: [(1, 00001D:A34E97, 12, 0, 0), (1, 00001D:CD223D, 21, 0, 0)]
        Ports in the LAG:
                et.2.1
                et.2.2
LAG index 35
        Id: [(1, 00001D:A34E97, 14, 0, 0), (1, 00E063:66EE71, 41, 0, 0)]
        Ports in the LAG:
                et.2.3
                et.2.4
LAG index 37
        Id: [(1, 00001D:A34E97, 13, 0, 0), (1, 000285:05B2C0, 31, 0, 0)]
        Ports in the LAG:
                et.2.5
                et.2.6
```

However, consider a error when configuring or cabling. The following changes to the configuration of SW1, without changing the cable plant means SmartTrunks will not connect. The original and correct "**lacp set port**" commands with the proper "**port-key**" bindings have been commented out. New "**lacp set port**" commands with the incorrect "**port-key**" bindings have been installed. There is no error indication in the configuration. There is no syntactical problem with this configuration.

```
smarttrunk create st.12 protocol lacp
smarttrunk create st.13 protocol lacp
smarttrunk create st.14 protocol lacp
lacp set aggregator st.12 actor-key 12 partner-key 21 port-type 10-100-ethernet
lacp set aggregator st.13 actor-key 13 partner-key 31 port-type 10-100-ethernet
lacp set aggregator st.14 actor-key 14 partner-key 41 port-type 10-100-ethernet
lacp set port et.2.(1-2) enable port-key 12
comment line 8 "lacp set port et.2.(3-4) port-key 14 enable"
comment line 9 "lacp set port et.2.(5-6) port-key 13 enable"
lacp set port et.2.(3-4) port-key 13 enable
lacp set port et.2.(5-6) port-key 14 enable
stp set protocol-version rstp
stp set bridging priority 7500
stp enable port st.12
stp enable port st.13
stp enable port st.14
interface add ip en0 address-netmask 24.112.73.4/21
system set name SW1
```

However, when you look at the SmartTrunk display only **st.12** is displayed, st.13 and st.14 are not shown as connected, or in the display at all for that matter.

```
SW1# smarttrunk show connections all-smarttrunks

                                                                        Actor
Partner
SmartTRUNK Local Port  Remote Switch        Remote Module   Remote Port  State  Key
Key
---------- ----------  -------------        -------------   -----------  -----  ----- -
----
st.12      et.2.1      Riverstone CD:22:3D  --              33           Up     12
21
st.12      et.2.2      Riverstone CD:22:3D  --              34           Up     12
21
```

Displaying the link aggregation control protocol information will show you that something is not quite right. Knowing when we set this up, the pairing of keys should look like this `12<->21; 13<->31; 14<->41` you notice that Index 35 & 37 show a mapping of **`13<->41`**; **`14<->31`**. This is a pretty clear indication that the configuration does not match the cable plant.

```
SW1# lacp show lag all-unique
LAG index 33
        Id: [(1, 00001D:A34E97, 12, 0, 0), (1, 00001D:CD223D, 21, 0, 0)]
        Ports in the LAG:
                et.2.1
                et.2.2
LAG index 35
        Id: [(1, 00001D:A34E97, 13, 0, 0), (1, 00E063:66EE71, 41, 0, 0)]
        Ports in the LAG:
                et.2.3
                et.2.4
LAG index 37
        Id: [(1, 00001D:A34E97, 14, 0, 0), (1, 000285:05B2C0, 31, 0, 0)]
        Ports in the LAG:
                et.2.5
                et.2.6
```

If the link aggregation control protocol has yet to discover a peer for an aggregation you will not see any peer information when using the "**`lacp shaw lag all-unique`**" command. After powering down SW1 a snapshot of the lacp information was taken from SW4.

```
SW4# lacp show lag all-unique
LAG index 35
        Id: [(1, 00E063:66EE71, 41, 0, 0), (0, 000000:000000, 0, 0, 0)]
        Ports in the LAG:
                et.2.3
                et.2.4
LAG index 37
        Id: [(1, 00E063:66EE71, 42, 0, 0), (1, 00001D:CD223D, 24, 0, 0)]
        Ports in the LAG:
                et.2.5
                et.2.6
```

802.3ad Interoperability with Juniper

Steve Cotter
Systems Engineering
July 26, 2001

Juniper only supports the actual aggregation scheme they DO NOT support the LACP protocol.

There are a few requirements to interoperability between Riverstone and Juniper:

1. Riverstone must configure Smarttrunks with the NO-PROTOCOL option, LACP or HUNTGROUP cannot be used as Juniper does not support ANY aggregation protocol.

2. BOTH ends of the link must be configured as a 802.1Q trunk, even if there is only one interface across the trunk the frames MUST be TAGGED for Juniper to function properly.

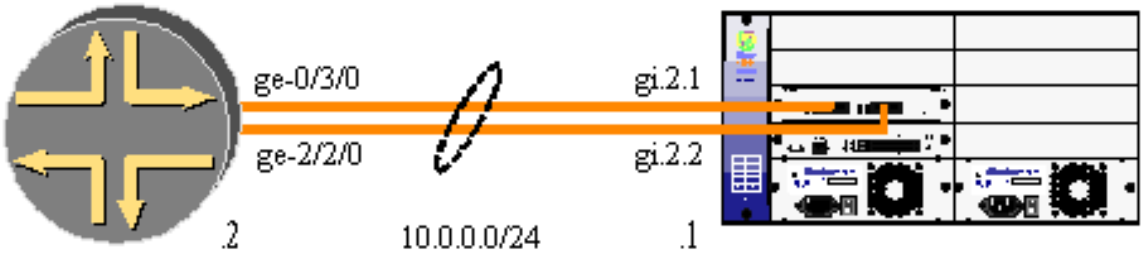
3. All links within a trunk must be IDENTICAL in bandwidth and even duplex settings.

4. Link Aggregation cannot be done on their new 48 port 10/100 PIC module.

5. Juniper does link balancing on L4 flows the same as we do, but they do not support the ping test functionality that we do (when you ping from an RS accross a Smarttrunk the RS will round robin all links within the trunk.)

RapidOS Version Tested	ROS 7.0.0.3 / JUNOS 4.4
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

Riverstone

```
smarttrunk create st.1 protocol no-protocol
smarttrunk add ports gi.2.1 to st.1
smarttrunk add ports gi.2.2 to st.1
vlan make trunk-port st.1
vlan create mg ip id 100
vlan add ports et.4.9-16 to mg
vlan add ports st.1 to mg
interface create ip MG address-netmask 10.0.0.1/24 vlan mg
```

Juniper

```
chassis {
        aggregated-devices {
                ethernet {
                        device-count 16;
                }
        }
}

interfaces {
        ge-0/3/0 {
                gigether-options {
                        802.3ad ae0;
        }
}
        ge-2/2/0 {
                gigether-options {
                        802.3ad ae0;
```

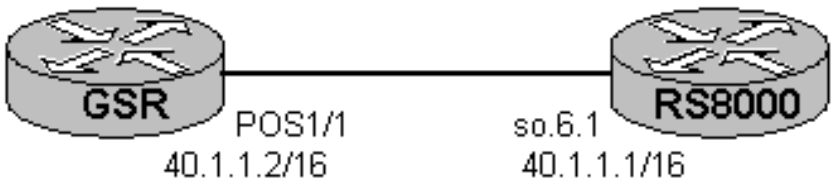
```
        }
}
ae0 {
        vlan-tagging;
        aggregated-ether-options{
                minimum-links 1;
        }
unit 0 {
        vlan-id 100;
        family inet {
                address 10.0.0.2/24;
                }
        }
}
```

POS Interoperability with Cisco

Greg Hankins
Corporate Systems Engineering
April 10, 2001

Sample configurations for RS and Cisco POS interoperability.	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	Packet over SONET interface

Diagram



Configurations

Cisco GSR

```
interface POS1/1
 mtu 9216
 ip address 40.2.1.2 255.255.0.0
 no ip directed-broadcast
 encapsulation ppp
 no keepalive
 crc 32
 pos scramble-atm
 pos flag c2 22
 no cdp enable
!
router ospf 1
 network 40.2.0.0 0.0.255.255 area 0
```

RS8000

```
port set so.6.1 mtu 9216
interface create ip to-gsr address-netmask 40.1.1.1/16 port so.6.1
!
ospf create area backbone
ospf add interface to-gsr to-area backbone
ospf start
```

Comments

- Specify MTU size of 9216 on the GSR.
- Use PPP encapsulation.
- Set CRC to 32-bit (CRC-32). The RS defaults to CRC-32.
- Turn on scrambling (RFC 2615).
- Set the C2 byte to 22 (0x16) to indicate PPP payload with scrambling.

POS Bridged Configuration

Jeff McLaird
Corporate Systems Engineering
April 15, 2001

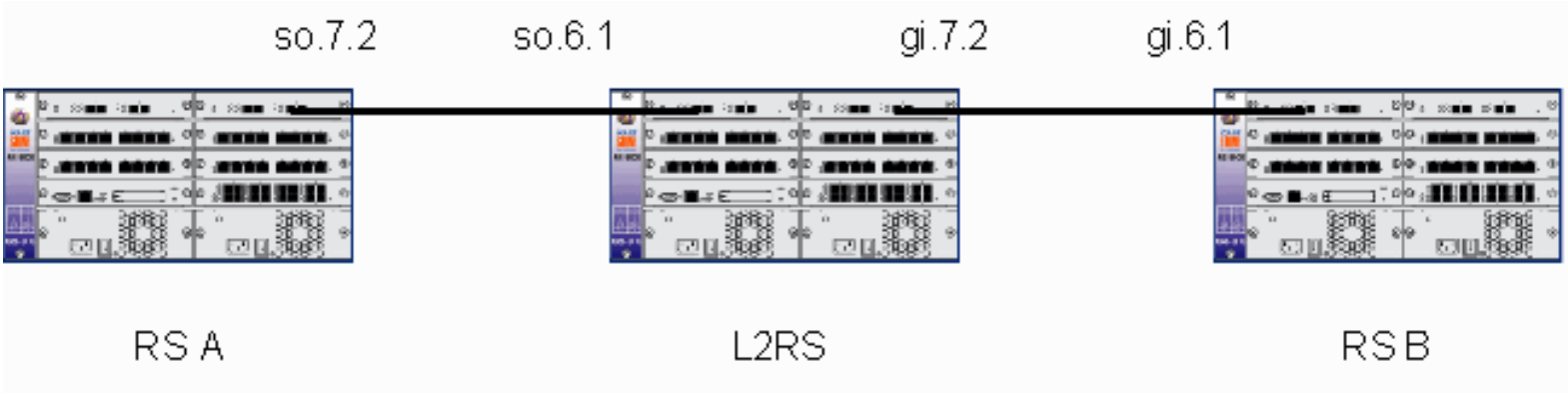
In some circumstances it is desirable to maintain a layer 2 core in order to provide for infrastructure connectivity. This example illustrates a layer two core provisioned with both PoS and Gigabit Ethernet ports bridging between disparate technologies in a port-based VLAN scenario.

By default, PoS ports are set for point-to-point protocol (PPP) encapsulation on the RS platform. In the instance that connectivity is required via an L2 fabric this causes a problem. The packets forwarded across the L2 Ethernet fabric must contain specific Ethernet MAC headers. Otherwise, the packets will be dropped at the L2 switch.

To provide for connectivity via a L2 core the RS platform also supports bridged Ethernet over PPP encapsulation. By default the switch will configure its PoS interface for PPP with bridged encapsulation. Thus bridged encapsulation must also be configured on the router's PoS/PPP interface connecting to the switch. It is important to note that the switch can only be configured for bridged encapsulation since there is no routing functionality supported in its configuration file.

RapidOS Version Tested	5.0.0.3
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	Require PoS line cards and CM2

Diagram



Configurations

RS A

```
ppp set ppp-encaps-bgd ports so.7.2
vlan create area1 id 1001 ip
vlan create core id 1000 ip
vlan add ports so.7.(1-2) to core
vlan add ports gi.6.(1-2) to area1
vlan add ports et.(1-5).(1-8) to area1
interface create ip core address-netmask 10.10.10.1/24 vlan core
interface create ip area1 address-netmask 10.10.11.1/24 vlan area1
interface add ip lo0 address-netmask 10.10.15.1/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.15.1
ip-router policy redistribute from-proto direct to-proto bgp target-as 65412
ip-router policy redistribute from-proto static to-proto bgp target-as 65412
ospf create area backbone
ospf create area 0.0.0.1
ospf add interface core to-area backbone
ospf add interface area1 to-area 0.0.0.1
ospf add stub-host 10.10.15.1 to-area backbone cost 1
ospf start
bgp create peer-group reflector type routing autonomous-system 65412 proto any
interface all
bgp add peer-host 10.10.11.254 group reflector
bgp set peer-group reflector local-address 10.10.15.1
bgp start
system set name RSA
```

L2RS

```
vlan create core id 1000 ip
vlan add ports et.(1-5).(1-8) to core
```

```
vlan add ports so.7.(1-2) to core
vlan add ports gi.6.(1-2) to core
interface create ip mgt address-netmask 10.10.10.254/24 vlan core
ip disable forwarding
ip disable proxy-arp interface all
ip add route default gateway 10.10.10.1
system set name L2RS
```

RS B

```
vlan create area2 id 1002 ip
vlan create core id 1000 ip
vlan add ports gi.6.(1-2) to core
vlan add ports gi.7.(1-2) to area2
vlan add ports et.(1-5).(1-8) to area2
interface create ip core address-netmask 10.10.10.2/24 vlan core
interface create ip area2 address-netmask 10.10.12.1/24 vlan area2
interface add ip lo0 address-netmask 10.10.15.2/32
ip disable proxy-arp interface all
ip disable icmp-redirect interface all
ip-router global set autonomous-system 65412
ip-router global set router-id 10.10.15.2
ip-router policy redistribute from-proto direct to-proto bgp target-as 65412
ip-router policy redistribute from-proto static to-proto bgp target-as 65412
ospf create area backbone
ospf create area 0.0.0.2
ospf add interface core to-area backbone
ospf add interface area2 to-area 0.0.0.2
ospf add stub-host 10.10.15.2 to-area backbone cost 1
ospf start
bgp create peer-group reflector type routing autonomous-system 65412 proto any
interface all
bgp add peer-host 10.10.12.254 group reflector
bgp set peer-group reflector local-address 10.10.15.2
bgp start
system set name RSB
```

Comments

Once the links are configured correctly the PPP negotiation process will enable and the OSPF adjacencies will be made. Troubleshooting at this point will be the same as with any other PPP connection.

It should be noted that this configuration is strictly for bridged encapsulation. In firmware versions after and including version 3.1 bridged encapsulation of PoS links were enabled once a strictly L2 configuration was enabled.

$Id: 0008.html,v 1.6 2002/05/10 18:15:48 webmaster Exp $

OSPF over POS Interoperability with Juniper

Joseph A. Duarte
Corporate Systems Engineering
April 16, 2001

By default, POS ports are set for point-to-point protocol (PPP) encapsulation on the RS platform. During PPP negotiations, several parameters are negotiated via Control Protocols. Not all parameters are mandatory, and vendor implementations can vary.

Unlike our PPP implementation, Juniper *does not* send any optional parameters, most notably the MRU in the Link Control Protocol (LCP), and the IP Address in the Internet Protocol Control Protocol (IPCP).

In ROS versions 6.3.0.3, 7.0.0.0, and higher when a device does not accept or send MRU information, we will defer to the configured port MTU. In order to ensure interoperability with Juniper you need to manually specify the port MTU to ensure that the MTU values for OSPF are the same between the RS and the Juniper.

Juniper uses 4470 as its default MTU for POS interfaces. They add another 4 bytes for the PPP L2 header giving them a max packet of 4474. OSPF will use the MTU size 4470. In order to ensure interoperability, we need to set our MTU to be 4478. The reason for that is because we use 8 bytes as our max ppp L2 header OSPF will use the MTU 0f 4470 (4478 port MTU minus the PPP header).

The keys to ensuring interoperability between the RS and the Juniper are:

1.) Ensure that the IP peer address is specified when creating the interface.

2.) Ensure that our MTU is set to 4478, 8 bytes above Junipers default MTU of 4470

Note: Both Cisco and Juniper default to 4K on their POS interfaces, we default to 9K. The reason that we do not have this problem with Cisco is they support the optional negotiation parameters listed above.

RapidOS Version Tested	6.3.0.3 and 7.0.0.0
RapidOS Versions Working with this Configuration	6.3.0.3 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.3.0.3

Hardware Specifics	POS interface

Diagram

Configurations

Riverstone

```
port set so.5.3 mtu 4478
!
sonet set so.5.3 framing sdh
sonet set so.5.3 payload-scramble on
sonet set so.5.3 protection 1+1 protected-by so.5.4
sonet set so.5.3 loopback none
!
interface create ip sonet1 address-netmask 10.16.1.1/30 port so.5.3 peer-address
10.16.1.2
interface add ip lo0 address-netmask 10.16.1.254/32
!
ip-router global set router-id 10.16.1.254
!
ospf create area backbone
ospf add stub-host 10.16.1.254 to-area backbone cost 1
ospf add interface 10.16.1.1 to-area backbone
ospf start
```

Juniper M40

```
juniper@> show configuration
version 4.2R2.4;

    so-0/2/0 {
        traceoptions {
            flag all;
        }
        keepalives;
        traps;
        clocking external;
```

```
        encapsulation ppp;
        sonet-options {
            payload-scrambler;
            rfc-2615;
        }
        unit 0 {
            description "Sonet STM-1 Circuit to Riverstone";
            family inet {
                address 10.16.1.2/30 {
                    destination 10.16.1.1;
                }
            }
        }
    }
protocols {
        ospf {

        area 0.0.0.0 {
            interface so-0/2/0.0;
        }
    }
}
```

Comments

You can use the following show commands to verify connectivity and OSPF adjacency:

```
riverstone# ppp show stats ports so.5.3
so.5.3:
    Port:                       Enabled/Up
    IP:                         Enabled/Up
    IPX:                        Disabled/Down
    Bridging:                   Enabled/Down
    LCP/NCP Max Failure:        10
    LCP/NCP Max Configure:      10
    LCP/NCP Max Terminate:      2
    LCP/NCP Retry Interval:     30
    LCP Use Magic Numbers:      Off
    LCP Send Echo Requests:     Off
    Effective  PPP MTU:         4470
    Negotiated PPP MRU:         4478

Riverstone# ospf monitor neighbors
Codes: E  - Interface to neighbor does not belong to stub/NSSA area
       NP - Interface to Neighbor belongs to NSSA area
       MS - Neighbor is the Master during Database exchange
       I  - Initial packet being exchanged during DB exchange
       M  - More packets to be exchanged during DB exchange
```

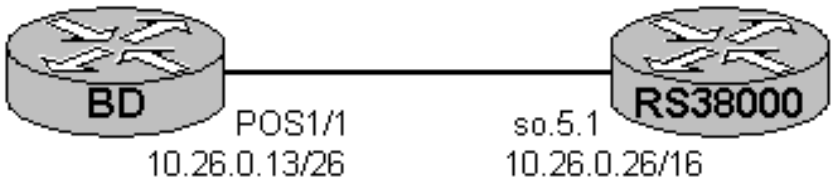
```
Interface: 10.16.1.1    Area: 0.0.0.0
Neighbor ID     Nbr IP Addr     State      Mode   Options    Pri
-------------------------------------------------------------
10.16.0.2    10.16.1.2    Full       MS     E O        1
```

OC12 Interoperability With Extreme

Greg Hankins
Corporate Systems Engineering
May 10, 2002

This example documents a working configuration for OC12 MPLS interoperability with Extreme Networks' OC12 interface.	
RapidOS Version Tested	9.1.0.0
RapidOS Versions Working with this Configuration	9.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.1.0.0
Hardware Specifics	MPLS OC12

Diagram



Configurations

RS1

```
sonet set so.5.1 payload-scramble off
interface create ip to-extreme address-netmask 10.26.0.26/16 port so.5.1
interface add ip en0 address-netmask 10.0.26.26/16
interface add ip lo0 address-netmask 10.255.26.26/32
ip-router global set router-id 10.255.26.26
ospf create area backbone
ospf add interface to-extreme to-area backbone
ospf add stub-host 10.255.26.26 to-area backbone cost 5
ospf start
mpls add interface to-extreme
mpls create label-switched-path lsp-to-extreme to 10.26.0.13 no-cspf
mpls start
rsvp add interface to-extreme
rsvp start
```

Comments

The only non-standard setting needed was to turn of SONET payload scrambling on each router, and to set the Extreme's interface to line clocking.

[Home][Documentation][Index]

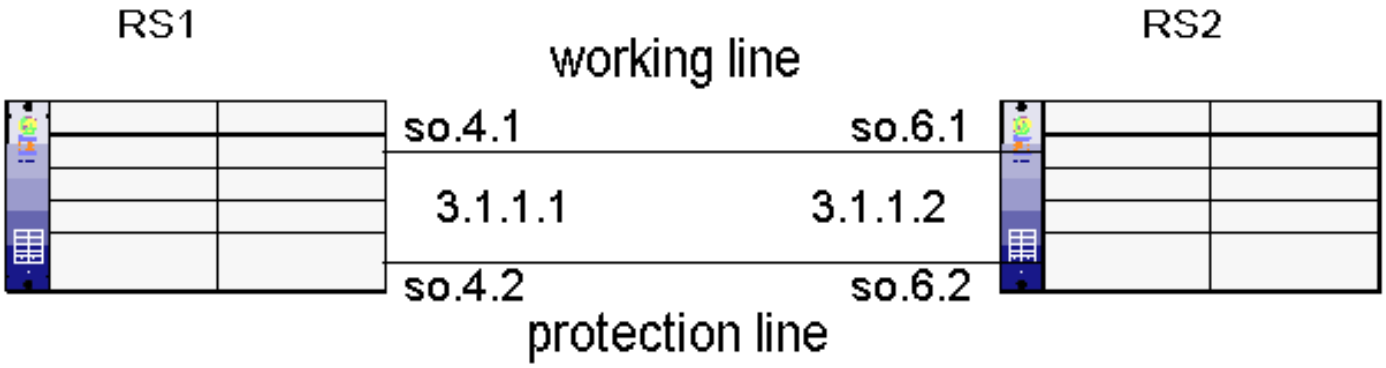
POS APS

Fang Fang
RTAC
May 10, 2002

The APS (automatic protection switch) provides link redundancy for POS. It refers to the protection mechanism of using a "protect" POS interface in the SONET network as the backup for "working" POS interface. When there's a fiber cut, a signal fail, e.g, Loss of Frame (LOF), Loss of Signal (LOS), Alarm Indication Signal (AIS), or a signal degradation, or bit error exceeds the threshold, the traffic will automatically switch over from working line to protection line. APS is very fast because it performs switchovers at Layer 1. The following configuration shows how to configure POS APS on Riverstone Routers.

RapidOS Version Tested	9.0.0.0
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	POS OC-3/OC-12 card

Diagram



Configurations

RS1

```
port set so.4.1 mtu 4478
sonet set so.4.1 loopback none
sonet set so.4.1 payload-scramble on
sonet set so.4.1 c2 22
sonet set so.4.1 framing sonet
sonet set so.4.1 protection 1+1 protected-by so.4.2
interface create ip TW2OC12 address-netmask 3.1.1.1/24 peer-address 3.1.1.2 port
so.4.1
system set name RS1
```

RS2

```
port set so.6.1 mtu 4478
sonet set so.6.1 loopback none
sonet set so.6.1 payload-scramble on
sonet set so.6.1 c2 22
sonet set so.6.1 framing sonet
sonet set so.6.1 protection 1+1 protected-by so.6.2
interface create ip TW1OC12 address-netmask 3.1.1.2/24 peer-address 3.1.1.1 port
so.6.1
system set name RS2
```

Comments

By doing "sonet show aps" you can show the SONET APS status.

```
RS1# sonet show aps so.4.1
                                                                    Switch
Port    Protection         Configured As       Status               Status
----    ----------         -------------       ------               ------
so.4.1  1+1,unidirectional working             working            Do Not Revert
```

```
Far End 1+1,unidirectional                                          Do Not Revert

RS1# sonet show aps so.4.2
                                                                     Switch
Port    Protection         Configured As       Status               Status
----    ----------         -------------       ------               ------
so.4.2  1+1,unidirectional protecting so.4.1   protecting so.4.1    Do Not Revert
Far End 1+1,unidirectional                                          Do Not Revert

RS1# sonet show alarms so.4.1
Section
  Alarms:
  BIP = 240                                                        -----> B1 error
Line
  Alarms:
  BIP = 5  FEBE = 4                                                -----> B2 error
Path
  Alarms:
  BIP = 240  FEBE = 4                                              -----> B3 error
  Corrected HCS errors = 0  Uncorrected HCS errors = 0
```

The traffic switches over from working line to protection line then.

```
RS1# sonet show aps so.4.1
                                                                     Switch
Port    Protection         Configured As       Status               Status
----    ----------         -------------       ------               ------
so.4.1  1+1,unidirectional working             protecting so.4.2 Signal fail
Far End     Signal Failure

RS1# sonet show aps so.4.2
                                                                     Switch
Port    Protection         Configured As       Status               Status
----    ----------         -------------       ------               ------
so.4.2  1+1,unidirectional protecting so.4.1   working              Do Not Revert
Far End 1+1,unidirectional                                          Do Not Revert
```

By default, RS will NOT switchover from the protecting line to the working line after the working line restores. If you want automatic switchover from the protecting line to the working line after the working line becomes available, you need issue the following command to the protecting interface under config mode.

```
sonet set so.4.2 revertive on
```

There are 5 minutes wait-to-restore time by default after the working line becomes available that automatic switchover from the protecting line to the working line takes place.

```
RS1# sonet show aps so.4.1
                                                                     Switch
Port    Protection         Configured As       Status               Status
----    ----------         -------------       ------               ------
so.4.1  1+1,unidirectional working             protecting so.4.2  Wait-to-restore
```

```
Far End 1+1,unidirectional                                    Wait-to-restore

RS1# 2002-04-12 13:31:16 %SONET-I-SONETAPS_SWITCH, Wait-to-restore event caused an
APS switch from so.4.2 to so.4.1

RS1# sonet show aps so.4.1
                                                               Switch
Port    Protection         Configured As       Status          Status
----    ----------         -------------       ------          ------
so.4.1  1+1,unidirectional working             working         Do Not Revert
Far End 1+1,unidirectional

RS1# sonet show aps so.4.2
                                                               Switch
Port    Protection         Configured As       Status          Status
----    ----------         -------------       ------          ------
so.4.2  1+1,unidirectional protecting so.4.1   protecting so.4.1  Do Not Revert
Far End 1+1,unidirectional                                    Do Not Revert
```

Pebbles of Knowledge

It is important to know the following points when configure APS on POS interfaces.

First, any pairs of POS interface on the same RS router (can be located in the same POS line module, or located in different POS line module) can be configured for APS. The protection interface Can NOT be on different Riverstone routers.

Second, the protection interface automatically has the same configuration of the working interface, and it can't be configured for other properties.

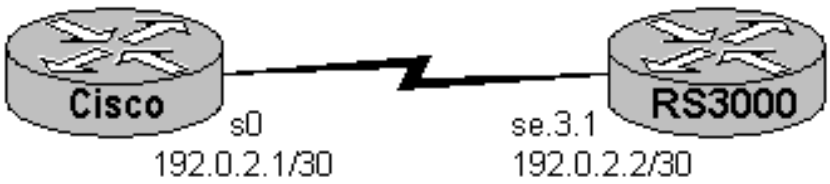
Third, the working and protecting interface must support identical optical carrier rates.

Interoperability with Cisco HDLC

Greg Hankins
Corporate Systems Engineering
April 12, 2001

Sample configurations for RS and Cisco HDLC interoperability on a serial interface.	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	6.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.0.0.0
Hardware Specifics	WAN interfaces

Diagram



Configurations

Cisco Router

```
interface Serial0
```

```
 ip address 192.0.2.1 255.255.255.252
 no ip directed-broadcast
 no cdp enable
!
router ospf 1
 log-adjacency-changes
 network 192.0.2.0 0.0.0.3 area 0
```

RS3000

```
port set se.3.1 wan-encapsulation cisco-hdlc speed 1544000
interface create ip s0 address-netmask 192.0.2.2/30 port se.3.1
!
ospf create area backbone
ospf add interface s0 to-area backbone
ospf start
```

Comments

The following commands can be used to show the status and statistics of each interface.

Cisco Router

```
cisco#show interfaces s0
Serial0 is up, line protocol is up
  Hardware is HD64570
  Internet address is 192.0.2.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:06, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     276 packets input, 13540 bytes, 0 no buffer
     Received 130 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     301 packets output, 13874 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
```

```
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

RS3000

```
RS3000# cisco-hdlc show stats summary ports all-ports
                Link    Keepalive
               Adm/Opr   sec
Port           States
----           --/--    -----
se.3.1         Up/Up     10

RS3000# cisco-hdlc show stats ports se.3.1
    SLARP Keepalive       10
    SLARP Local Seq       120
    SLARP Remote Seq      136
    SLARP Seq Retries     1
    Local Ip address 192.0.2.2, Peer Ip address 192.0.2.1, netmask fffffffc

    Service Features Status
    -----------------------
    RMON:                       Disabled
    RED:                        Disabled

    Current Output Queue States
    ---------------------------
        High priority queue depth                          20
        Med  priority queue depth                          20
        Low  priority queue depth                          20
        Ctrl priority queue depth                          20
        Max number frames enqued in high priority queue    0
        Max number frames enqued in med priority queue     0
        Max number frames enqued in low priority queue     1
        Max number frames enqued in ctrl priority queue    1
        Current number of frames in high priority queue    0
        Current number of frames in med  priority queue    0
        Current number of frames in low  priority queue    0
        Current number of frames in ctrl priority queue    0
        Frames dropped due to ctl queue depth exceeded     0
        Frames dropped due to high queue depth exceeded    0
        Frames dropped due to med queue depth exceeded     0
        Frames dropped due to low queue depth exceeded     0

    MIB II Stats
    ------------
```

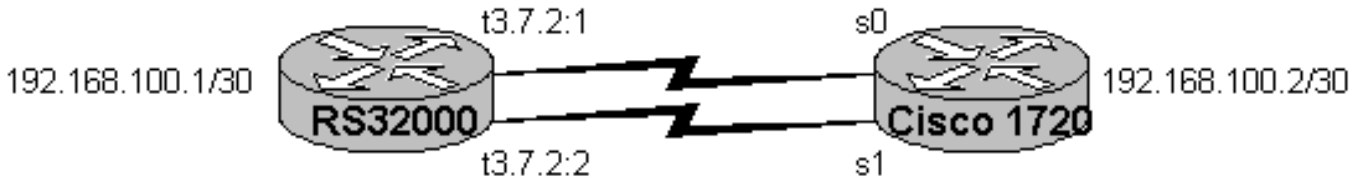
```
        Transmitted octets            10380
        Transmitted unicast frames    137
        Transmitted broadcast frames  1
        Transmitted multicast frames  0
        Discarded transmit frames     3
        Error transmit frames         0
        Received octets               10336
        Received unicast frames       134
        Received broadcast frames     0
        Received multicast frames     0
        Discarded receive frames      0
        Error receive frames          0

RS3000# port show serial-link-info se.3.1
Port    Port Type              CD   CTS  RTS/DTR  DSR  LL     LINK
----    ---------              ---  ---  -------  ---  ---    ----
se.3.1  V.35                   on   on   on       on   off    on

RS3000# statistics show port-stats se.3.1

Port: se.3.1
-------------
Port Stats                    Received                Transmitted
----------                    --------                -----------
Frames/Packets                156                     160
Bytes                         12008                   12008
1 minute traffic rates
. Average bits/sec            60                      59
. Packet discards             0                       0
. Packet errors               0                       0
. Unicast packets             6                       6
. Multicast packets           0                       0
. Broadcast packets           0                       0
Port stats cleared  * Never Cleared *
```

CT3 Interoperability with Cisco T1

Payam Kahen
Systems Engineering
May 8, 2001

This configuration will show a multilink PPP setup between an RS32000, and a Cisco device over two T1 links.	
RapidOS Version Tested	6.3.0.1
RapidOS Versions Working with this Configuration	6.3.0.2-5 and any other code version that supports CT3 blade.
RapidOS Versions NOT Working with this Configuration	6.3.0.0 and below, 7.0.0.0, and any other version of code which does not support the CT3 blade.
Hardware Specifics	CT3 blade.

Diagram



Configurations

RS32000

```
port set t3.7.2:1-2 wan-encapsulation ppp timeslots 1-24
port set t3.7.2 framing m23
!
ppp create-mlp mp.1 slot 7
ppp add-to-mlp mp.1 port t3.7.2:1-2
!
interface create ip MP.1 address-netmask 192.168.100.1/30 port mp.1
!
system set name RS32000-CT3
```

Cisco

```
Current configuration:
!
version 12.0
!
hostname Cisco-1720
!
ip subnet-zero
!
multilink virtual-template 1
!
interface Virtual-Template1
 ip address 192.168.100.2 255.255.255.252
 no ip directed-broadcast
 load-interval 30
 ppp multilink
!
interface Serial0
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
!
interface Serial1
 no ip address
 encapsulation ppp
 no fair-queue
 ppp multilink
!
interface FastEthernet0
 no ip address
 shutdown
!
```

```
ip classless
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
```

Comments

The framing used on the T3 interface is 'm23' which is the most popular, however, check with local loop provider on actual framing used. Framing on T1 links on both ends is 'esf'.

As can be seen in the following output, the RS32000 has placed 2 T1 ports in multilink-ppp logical port 'mp.1':

```
RS32000-CT3# ppp show mlp all-ports
mp.1:
            Slot          7
            PPP ports     t3.7.2:(1-2)
```

The output for port status shows the two T1 links as part of a bundle as denoted by 'B' in far right column:

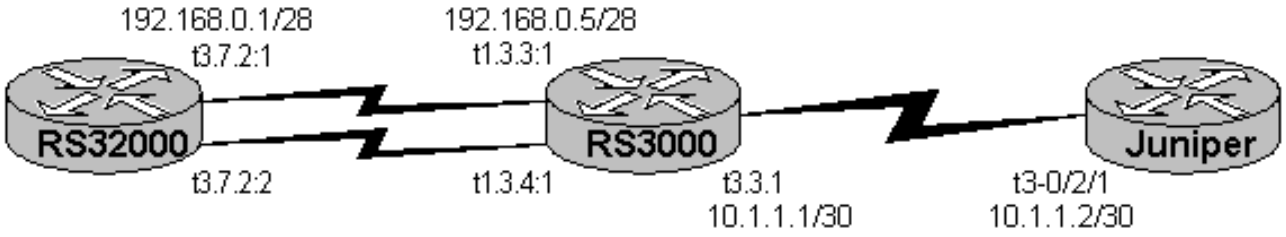
```
RS32000-CT3# port show port-status all-ports
t3.7.2   T3                    Full  44736000   n/a          Up    Up
t3.7.2:1 T3                    Full  1536000    n/a          Up    Up     B
t3.7.2:2 T3                    Full  1536000    n/a          Up    Up     B
```

Multirate WAN: T1/MLP and T3 to Juniper

Payam Kahen
Systems Engineering
May 9, 2001

This configuration shows an interconnection between Riverstone and Juniper routers across a T3 Link, as well as a Multilink-PPP link across multiple T1's between Riverstone gear. Also included is a simple EBGP configuration between Juniper and Riverstone.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	Any version that supports Clear Channel T3 WIC for the Multirate WAN Card
RapidOS Versions NOT Working with this Configuration	6.3.1 and earlier code versions, 7.0.0.x.
Hardware Specifics	Clear Channel T3 WIC only, connection to Juniper will not work on Channelized T3 ports.

Diagram



Configurations

RS3000

```
port set t1.3.3-4:1 wan-encapsulation ppp timeslots 1-24
port set t3.3.1 wan-encapsulation ppp framing cbit-parity clock-source loop
!
ppp create-mlp mp.1 slot 3
ppp add-to-mlp mp.1 port t1.3.3:1
ppp add-to-mlp mp.1 port t1.3.4:1
!
interface create ip T3-to-M20 address-netmask 10.1.1.1/30 peer-address 10.1.1.2 port
t3.3.1
interface create ip T1-to-RS32k address-netmask 192.168.0.5/28 port mp.1
!
ip-router global set router-id 10.1.1.1
ip-router global set autonomous-system 40000
!
bgp create peer-group AS26443 autonomous-system 26443 type external
bgp add peer-host 10.1.1.2 group AS26443
bgp start
!
system set name RS3000
```

RS32000

```
port set t3.7.2 framing m23
port set t3.7.2:1-2 wan-encapsulation ppp timeslots 1-24
!
ppp create-mlp mp.1 slot 7
ppp add-to-mlp mp.1 port t3.7.2:1-2
!
interface create ip PUBLIC address-netmask 10.79.1.236/24 port et.2.1
interface create ip MLP-to-RS3k address-netmask 192.168.0.1/28 port mp.1
!
ip add route default gateway 192.168.0.5
```

Juniper

```
version 4.2R2.4;
system {
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
    }
}
t3-0/2/1 {
        unit 0 {
```

```
            family inet {
                address 10.1.1.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 127.0.0.1/32;
        }
    }
}
protocols {
    bgp {
        local-as 26443;
        group AS40000 {
        peer-as 40000;
            neighbor 10.1.1.1;
        }
    }
}
```

Comments

The framing used on the T3 link between RS3000 and Juniper M20 is 'cbit-parity'. This must match on the other side, whether cbit, or other framing type.

The framing used on the CT3 interface on the RS32000 is 'm23' which is the most common, however, check with local loop provider on actual framing used. Framing on T1 links on both ends is 'esf'.

As can be seen in the following output, each Riverstone switch has placed 2 T1 ports in multilink-ppp logical port ‘mp.1’:

```
RS32000# ppp show mlp all-ports
mp.1:
            Slot          7
            PPP ports     t3.7.2:(1-2)

RS3000# ppp show mlp all-ports
mp.1:
            Slot          3
            PPP ports     t1.3.3:1,t1.3.4:1
```

The output for port status shows the two T1 links as part of a bundle as denoted by 'B' in far right column:

```
RS32000# port show port-status all-ports
...
t3.7.2   T3                    Full  44736000   n/a          Up    Up
t3.7.2:1 T3                    Full  1536000    n/a          Up    Up     B
t3.7.2:2 T3                    Full  1536000    n/a          Up    Up     B
...
```

```
RS3000# port show port-status all-ports
...
t3.3.1   T3                    Full  44736000   n/a          Up    Up
t1.3.3   T1                    Full  1544000    n/a          Up    Up
t1.3.3:1 T1                    Full  1536000    n/a          Up    Up     B
t1.3.4   T1                    Full  1544000    n/a          Up    Up
t1.3.4:1 T1                    Full  1536000    n/a          Up    Up     B
```

The following output from RS3000 shows that the BGP session is up to the Juniper:

```
RS3000# bgp show summary
Neighbor         V    AS MsgRcvd MsgSent      Up/Down State
--------         -    -- ------- -------      ------- -----
10.1.1.2   4 26443       4       5    0d0h1m24s Established
BGP summary, 1 groups, 1 peers
```

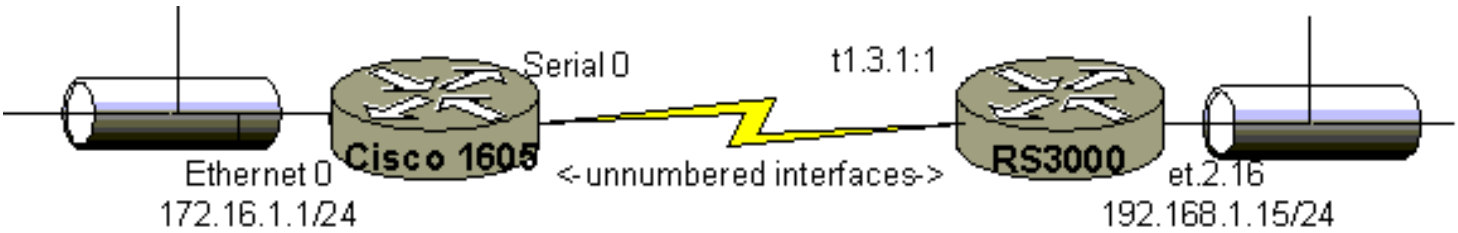
$Id: 0022.html,v 1.6 2002/05/10 18:15:48 webmaster Exp $

IP Unnumbered between Cisco and RS

Payam Kahen
Systems Engineering
July 19, 2001

This configuration will show a WAN link configured with IP Unnumbered on a Cisco and an RS device.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	This configuration applies only to WAN Interfaces

Diagram



Configurations

RS3000

```
port set t1.3.1:1 wan-encapsulation ppp timeslots 1-24
interface create ip PUBLIC address-netmask 192.168.1.15/24 port et.2.16
interface create ip T1 unnumbered PUBLIC port t1.3.1:1
ip add route 172.16.1.1 host interface T1
system set name RS3000
```

Cisco 1605

```
version 11.2
!
hostname Cisco-1605
!
interface Ethernet0
 ip address 172.16.1.1 255.255.255.0
!
interface Serial0
 ip unnumbered Ethernet 0
 encapsulation ppp
!
no ip classless
!
line con 0
line vty 0 4
 login
!
end
```

Comments

An Interface configured as "unnumbered" essentially borrows its IP address from another Interface. Note that it is necessary to statically add a host route for the peer-address in the RS config. As shown in the following output, while PPP negotiates the peer address upon initiation, that address is not input into the routing table. The route to the IP Unnumbered peer address is statically specified. This is not necessary on the Cisco, because IOS automatically inputs the peer router's IP address into its routing table.

```
RS3000# ip show interfaces T1

Interface T1:
    Admin State:          up
    Operational State:    up
    Capabilities:         <POINTTOPOINT,SIMPLEX,MULTICAST,WAN,UNNUMBERED>
    Configuration:
       VLAN:              SYS_L3_T1
```

```
       Ports:             t1.3.1:1
       MTU:               1500
       MAC Encapsulation: ETHERNET_II
       MAC Address:       00:02:85:05:92:00
       IP Address:        192.168.1.15/24 --> 172.16.1.1

RS3000# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
127.0.0.1            127.0.0.1            -         lo0
172.16.1.1           Unnumbered           Static    T1
192.168.1.0/24       directly connected   -         ET.2.16

Router#sh ip route
...
     192.168.1.0/32 is subnetted, 1 subnets
C       192.168.1.15 is directly connected, Serial0
     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Ethernet0
```

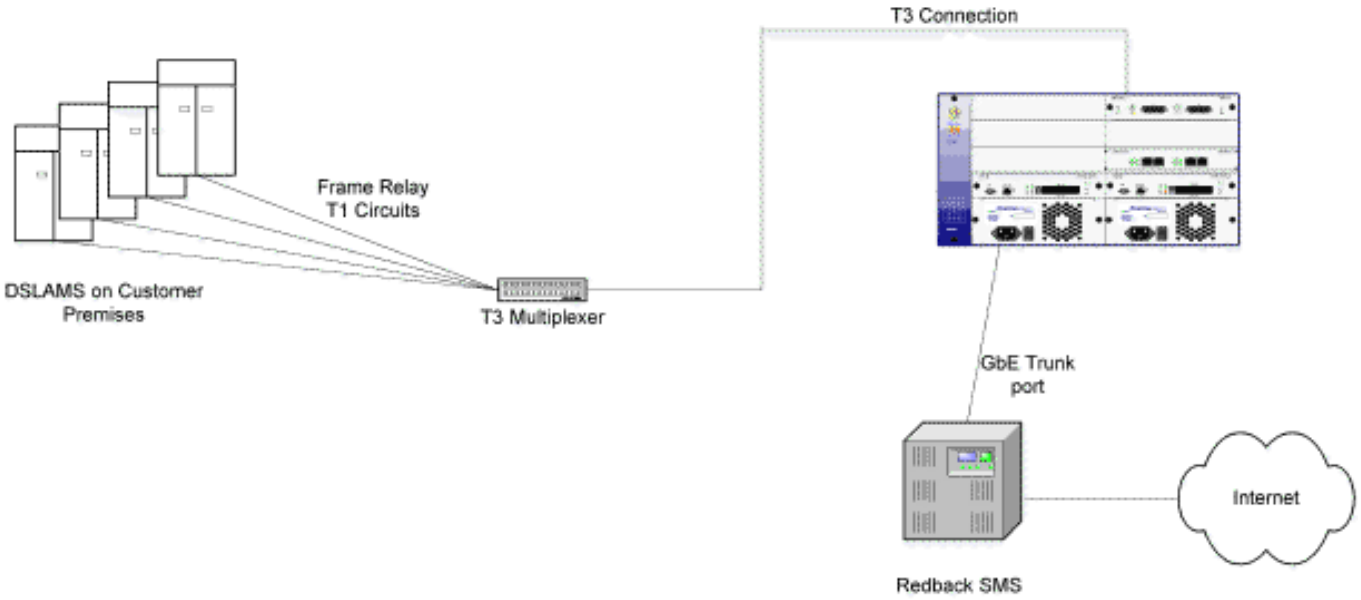
However, a routing protocol such as OSPF may also be used in place of the static route, which will also input the correct route into the route table.

Spanning Tree Over Frame Relay

Dennis L. Faust
Systems Engineering
December 4, 2001

This is an example of how to setup Spanning Tree on Channelized T3 card. This is useful if the T3 channels are on a private network with no other lower level protocols running to detect loops. A T3 multiplexer will typically put any unused ports into loopback, which could be catastrophic. The L2 filter ensure that any broadcast traffic from one T3 channel will not go to another T3 channel.	
RapidOS Version Tested	8.0.0.1
RapidOS Versions Working with this Configuration	8.0.0.1 and newer
RapidOS Versions NOT Working with this Configuration	Older thank 8.0.0.1
Hardware Specifics	CT3 card

Diagram



Configurations

```
!
! Last modified from Console on 2001-08-29 14:02:39
!
version 8.0
port set t3.10.1:1 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:2 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:3 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:4 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:5 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:6 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:7 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:8 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:9 timeslots 1-24 wan-encapsulation frame-relay clock-source internal
port set t3.10.1:10 timeslots 1-24 wan-encapsulation frame-relay clock-source
internal
port set t3.10.1:11 timeslots 1-24 wan-encapsulation frame-relay clock-source
internal
port set t3.10.1:12 timeslots 1-24 wan-encapsulation frame-relay clock-source
internal
port set t3.10.1:13 timeslots 1-24 wan-encapsulation frame-relay clock-source
internal
port set t3.10.1:14 timeslots 1-24 wan-encapsulation frame-relay clock-source
internal
port set t3.10.1:15 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:16 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:17 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:18 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:19 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:20 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:21 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:22 timeslots 1-24 wan-encapsulation ppp clock-source internal
```

```
port set t3.10.1:23 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:24 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:25 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:26 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:27 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1:28 timeslots 1-24 wan-encapsulation ppp clock-source internal
port set t3.10.1 framing m23 clock-source internal
frame-relay create vc port t3.10.1:1.35
frame-relay create vc port t3.10.1:2.35
frame-relay create vc port t3.10.1:3.35
frame-relay create vc port t3.10.1:4.35
frame-relay create vc port t3.10.1:5.35
frame-relay create vc port t3.10.1:6.35
frame-relay create vc port t3.10.1:7.35
frame-relay create vc port t3.10.1:8.35
frame-relay create vc port t3.10.1:9.35
frame-relay create vc port t3.10.1:10.35
frame-relay create vc port t3.10.1:11.35
frame-relay create vc port t3.10.1:12.35
frame-relay create vc port t3.10.1:13.35
frame-relay create vc port t3.10.1:14.35
frame-relay create vc port t3.10.1:1.100
frame-relay create vc port t3.10.1:2.100
frame-relay create vc port t3.10.1:3.100
frame-relay create vc port t3.10.1:4.100
frame-relay create vc port t3.10.1:5.100
frame-relay create vc port t3.10.1:6.100
frame-relay create vc port t3.10.1:7.100
frame-relay create vc port t3.10.1:8.100
frame-relay create vc port t3.10.1:9.100
frame-relay create vc port t3.10.1:10.100
frame-relay create vc port t3.10.1:11.100
frame-relay create vc port t3.10.1:12.100
frame-relay create vc port t3.10.1:13.100
frame-relay create vc port t3.10.1:14.100
vlan make trunk-port gi.12.2
vlan create VLAN1 id 10 port-based
vlan create VLAN2 id 20 port-based
vlan create VLAN3 id 30 port-based
vlan create VLAN4 port-based id 40
vlan add ports t3.10.1:1.35 to vlan2
vlan add ports t3.10.1:2.35 to vlan2
vlan add ports t3.10.1:3.35 to vlan2
vlan add ports t3.10.1:4.35 to vlan2
vlan add ports t3.10.1:5.35 to vlan2
vlan add ports t3.10.1:6.35 to vlan2
vlan add ports t3.10.1:7.35 to vlan2
vlan add ports t3.10.1:8.35 to vlan2
vlan add ports t3.10.1:9.35 to vlan2
vlan add ports t3.10.1:10.35 to vlan2
vlan add ports t3.10.1:11.35 to vlan2
vlan add ports t3.10.1:12.35 to vlan2
vlan add ports t3.10.1:13.35 to vlan2
```

```
vlan add ports t3.10.1:14.35 to vlan2
vlan add ports t3.10.1:15 to vlan2
vlan add ports t3.10.1:16 to vlan2
vlan add ports t3.10.1:17 to vlan2
vlan add ports t3.10.1:18 to vlan2
vlan add ports t3.10.1:19 to vlan2
vlan add ports t3.10.1:20 to vlan2
vlan add ports t3.10.1:21 to vlan2
vlan add ports t3.10.1:22 to vlan2
vlan add ports t3.10.1:23 to vlan2
vlan add ports t3.10.1:24 to vlan2
vlan add ports t3.10.1:25 to vlan2
vlan add ports t3.10.1:26 to vlan2
vlan add ports t3.10.1:27 to vlan2
vlan add ports t3.10.1:28 to vlan2
vlan add ports t3.10.1:1.100 to vlan3
vlan add ports t3.10.1:2.100 to vlan3
vlan add ports t3.10.1:3.100 to vlan3
vlan add ports t3.10.1:4.100 to vlan3
vlan add ports t3.10.1:5.100 to vlan3
vlan add ports t3.10.1:6.100 to vlan3
vlan add ports t3.10.1:7.100 to vlan3
vlan add ports t3.10.1:8.100 to vlan3
vlan add ports t3.10.1:9.100 to vlan3
vlan add ports t3.10.1:10.100 to vlan3
vlan add ports t3.10.1:11.100 to vlan3
vlan add ports t3.10.1:12.100 to vlan3
vlan add ports t3.10.1:13.100 to vlan3
vlan add ports t3.10.1:14.100 to vlan3
vlan add ports et.4.16 to vlan2
vlan add ports gi.12.2 to vlan2
vlan add ports gi.12.2 to vlan4
vlan add ports et.4.1 to vlan4
interface create ip VLAN1 address-netmask 192.168.202.2/24 vlan vlan1
interface create ip VLAN3 address-netmask 192.168.230.1/24 vlan vlan3
interface add ip en0 address-netmask 192.168.3.31/24
frame-relay set peer-addr ip-address 192.168.230.5/24 ports t3.10.1:19.100
pvst create spanningtree vlan_name vlan2
pvst create spanningtree vlan_name vlan4
pvst set bridging priority 0 spanning-tree vlan2
pvst enable port t3.10.1:3.35 spanning-tree vlan2
pvst enable port t3.10.1:4.35 spanning-tree vlan2
pvst enable port t3.10.1:5.35 spanning-tree vlan2
pvst enable port t3.10.1:6.35 spanning-tree vlan2
pvst enable port t3.10.1:7.35 spanning-tree vlan2
pvst enable port t3.10.1:8.35 spanning-tree vlan2
pvst enable port t3.10.1:9.35 spanning-tree vlan2
pvst enable port t3.10.1:10.35 spanning-tree vlan2
pvst enable port t3.10.1:11.35 spanning-tree vlan2
pvst enable port t3.10.1:12.35 spanning-tree vlan2
pvst enable port t3.10.1:13.35 spanning-tree vlan2
pvst enable port t3.10.1:14.35 spanning-tree vlan2
```

```
pvst enable port t3.10.1:15 spanning-tree vlan2
pvst enable port t3.10.1:16 spanning-tree vlan2
pvst enable port t3.10.1:17 spanning-tree vlan2
pvst enable port t3.10.1:18 spanning-tree vlan2
pvst enable port t3.10.1:19 spanning-tree vlan2
pvst enable port t3.10.1:20 spanning-tree vlan2
pvst enable port t3.10.1:21 spanning-tree vlan2
pvst enable port t3.10.1:22 spanning-tree vlan2
pvst enable port t3.10.1:23 spanning-tree vlan2
pvst enable port t3.10.1:24 spanning-tree vlan2
pvst enable port t3.10.1:25 spanning-tree vlan2
pvst enable port t3.10.1:26 spanning-tree vlan2
pvst enable port t3.10.1:27 spanning-tree vlan2
pvst enable port t3.10.1:28 spanning-tree vlan2
pvst enable port t3.10.1:2.35 spanning-tree vlan2
pvst enable port t3.10.1:1.35 spanning-tree vlan2
system set idle-timeout serial 0
system set idle-timeout telnet 0
filters add static-entry name FIXBC restriction force source-mac any dest-mac
FF:FF:FF:FF:FF:FF vlan 20 in-port-list t3.10.1 out-port-list gi.12.2
```

Comments

This feature was added to the CT3 card to allow for a private Frame Relay network. The Frame Relay network normally will detect when a channel is in a loop condition and take that individual T1 circuit down, based on the LMI. However, when there is no Frame Relay switch, these looped T1s will cause havoc on the layer 2 network. A single broadcast will flood all of the T1s, since they will be continuously sent by the looped circuits. The example shown is using Frame Relay. Since these are private connections, there is no LMI running to detect loops. When a port is looped back for testing (or is unused), it would create a loop in the Ethernet topology (collapsing into a flat LAN in the RS platform) and cause the entire network to become non-functional.

Basic PPP Configuration on Channelized T1

A. V. Rajesh
RTAC
May 11, 2002

The purpose of this document is to explain setting up PPP configuration between two RS connected over channelized T1. All of the T1 timeslots (1-24) is used as a single instance. Besides that, it also contains useful tips to verify the operation of PPP in a step-by-step manner. We also support Cisco's HDLC encapsulation for WAN interface.	
RapidOS Version Tested	8.0.3.4
RapidOS Versions Working with this Configuration	6.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.3.0.0
Hardware Specifics	WIC module

Diagram

Configurations

RS1

```
port set t1.4.3:1 wan-encapsulation ppp timeslots 1-24
```

```
port set t1.4.3 framing esf line-coding b8zs
interface create ip WAN1 address-netmask 10.1.1.1/30 port t1.4.3:1
system set name RS1
system set idle-timeout serial 0 telnet 0
```

RS2

```
port set t1.4.1:1 wan-encapsulation ppp timeslots 1-24
port set t1.4.1 framing esf line-coding b8zs
interface create ip WAN2 address-netmask 10.1.1.2/30 port t1.4.1:1
system set name RS2
system set idle-timeout serial 0 telnet 0
```

Comments

Check the end-to-end connectivity between RS1 and RS2

```
RS1# ping 10.1.1.2
PING 10.1.1.2 (10.1.1.2): 36 data bytes
44 bytes from 10.1.1.2: icmp_seq =0 ttl=255 time=2.038 ms

--- 10.1.1.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.038/2.038/2.038 ms
```

In case you have issues with end-to-end connectivity, please follow the steps given below to troubleshoot the T1.

Use the following command to check if the T1 controller and the link status are up. If the link is down, check with your local Telco.

```
RS1# port show port-status t1.4.3

Flags: M - Mirroring enabled  B - MLP Bundle  S - SmartTRUNK port P - Configured as
802.1p

                                        Negot-  IFG    Link  Admin
Port     Port Type       Duplex Speed   iation Value  State  State Flags
----     ---------       ------  -----  ------ -----  -----  ----- -----
t1.4.3    T1              Full  1544000  n/a            Up     Up
```

Ensure that the link is receiving and transmitting data.

```
RS1# statistics show port-stats t1.4.3

Port: t1.4.3:1
-------------
Port Stats                  Received               Transmitted
----------                  --------               -----------
Frames/Packets              63805                  2515
Bytes                       32006                  39184
1 minute traffic rates
```

```
. Average bits/sec            51                        44
. Packet discards             0                         0
. Packet errors               0                         0
. Unicast packets             24                        24
. Multicast packets           0                         0
. Broadcast packets           0                         0
Port stats cleared  * Never Cleared *
```

Check to see if there are any port errors.

```
RS1# statistics clear port-errors t1.4.3:1
RS1# statistics show port-errors t1.4.3:1

Port: t1.4.3:1
----
Error Stats                   Received                  Transmitted
----------                    --------                  -----------
Discarded Frames              0                         0
Errored Frames                0                         0
Error stats cleared   2002-04-22 16:52:20
```

Check for incrementing code violations and other errors.

```
RS1# port show serial-link-info t1.4.3 all
T1 Slot 4 Port 3:        Channelized
  Module Revision:         1.0
  T1 WIC Version:          0.0
  Cablelength:             133 feet
  Clock source:            Loop
  Framing:                 ESF
  Line coding:             B8ZS
  Loopback:                None
  Remote loopback receive: Enabled
  FDL enable:              ANSI
  Idle code:               0xff (255)
  BERT state:              Stopped
  BERT status:             not available
  BERT start time:         No BERT since powerup
  BERT end time:           No BERT since powerup
  BERT time remaining:     00H 00M 00S
  BERT pattern:            2^11
  BERT interval (minutes): 1
  BERT sync count:         0
  BERT total errors:       0
  BERT total mb:           0
  BERT errors since sync:  0
  BERT kb since sync:      0
  Total Data (Last 24 hour interval):
    0 Line Code Violations,   0 Path Code Violations
    0 Slip Secs,   0 Fr Loss Secs,   0 Line Err Secs,   0 Degraded Mins
    0 Errored Secs,   0 Bursty Err Secs,   0 Severely Err Secs, 0 Unavail Secs
```

```
  Total Data (Last 15 minute interval):
    0 Line Code Violations,   0 Path Code Violations
    0 Slip Secs,   0 Fr Loss Secs,   0 Line Err Secs,   0 Degraded Mins
    0 Errored Secs,   0 Bursty Err Secs,   0 Severely Err Secs, 0 Unavail Secs
```

Note: If the errors increment in the above output, contact your local Telco and RTAC immediately.

Verify the status of PPP using the following commands,

```
RS1# ppp show stats summary ports t1.4.3
          Link      IP       IPX    Bridge    Encr     Comp     Imux
        Adm/Opr  Adm/Opr  Adm/Opr  Adm/Opr  Adm/Opr  Adm/Opr  Adm/Opr
Port     States   States   States   States   States   States   States
----     --/--    --/--    --/--    --/--    --/--    --/--    --/--
t1.4.3:1  Up/Up    Up/Up    Up/Up    Up/Up    Dn/Dn    Dn/Dn    Dn/Dn

(L) denotes compression/encryption on an individual link
(M) denotes compression/encryption on the MLP bundle
```

NOTE: For more details on the status of your PPP connection you can use this command.

```
ppp show stats ports <port>
```

NOTE: We don’t support encryption or compression on T1. Moreover Imux is not enabled by default. That explains the "down" status on the above fields. Make sure the Link status is up for all the protocols.

```
RS1# ppp show stats link-status ports t1.4.3
t1.4.3:1:
    Bad Addresses        0
    Bad Controls         0
    Packet Too Longs     0
    Bad FCS's            0
    Local MRU            1524
    Remote MRU           1524
    Send ACC Map:        0xFF, 0xFF, 0xFF, 0xFF
    Receive ACC Map:     0xFF, 0xFF, 0xFF, 0xFF
    Send Protocol Compression:    Disabled
    Receive Protocol Compression: Disabled
    Send AC Compression:            Disabled
    Receive AC Compression:         Disabled
    Send FCS size: 16
    Receive FCS Size: 16
```

NOTE: Ensure the FCS and MRU are the same on both ends.

NOTE: Sometimes if the PPP connection is down or does not seem to be functioning properly you might need to restart the PPP process on your routers. To restart the PPP process at both the end routers use the following command.

```
ppp restart lcp-ncp ports <port>
```

Pebbles of Knowledge

The source of several T1 issues start with a mismatch in framing and line code specification. Always ensure that they comply with the local Telco. Make sure that the line is tested by the local Telco for loops, loss of frame and loss of carrier.

NOTE: You can verify the settings using the following command.

```
port show serial-link-info <port> all
```

Typical T1 Framing and Line coding schemes

Interface	Framing	Line coding
T1	Extended Super Frame format (ESF)*	Bipolar 8 Zero Substitution (B8ZS)*
T1	Super frame – D4 framing (SF)	Alternate Mark Inversion (AMI)

* Denotes Default settings

If you have problems keep these things in mind.

- Ensure that the T1 WIC module is properly seated in the line card and screwed in.
- **WARNING:** You cannot hot swap the T1 WIC module. Doing so may result in severe damage to equipment.

RS also supports HDLC encapsulation for interoperability with CISCO. To configure HDLC encapsulation instead of PPP, use the following command to set the wan encapsulation to HDLC. Substitute this line for the wan-encapsulation PPP line shown in the example.

```
port set t1.4.3:1 wan-encapsulation cisco-hdlc timeslots 1-24
```

Riverstone CT3 to Cisco CT3

Rico E. Vitale
Systems Engineering
July 11, 2002

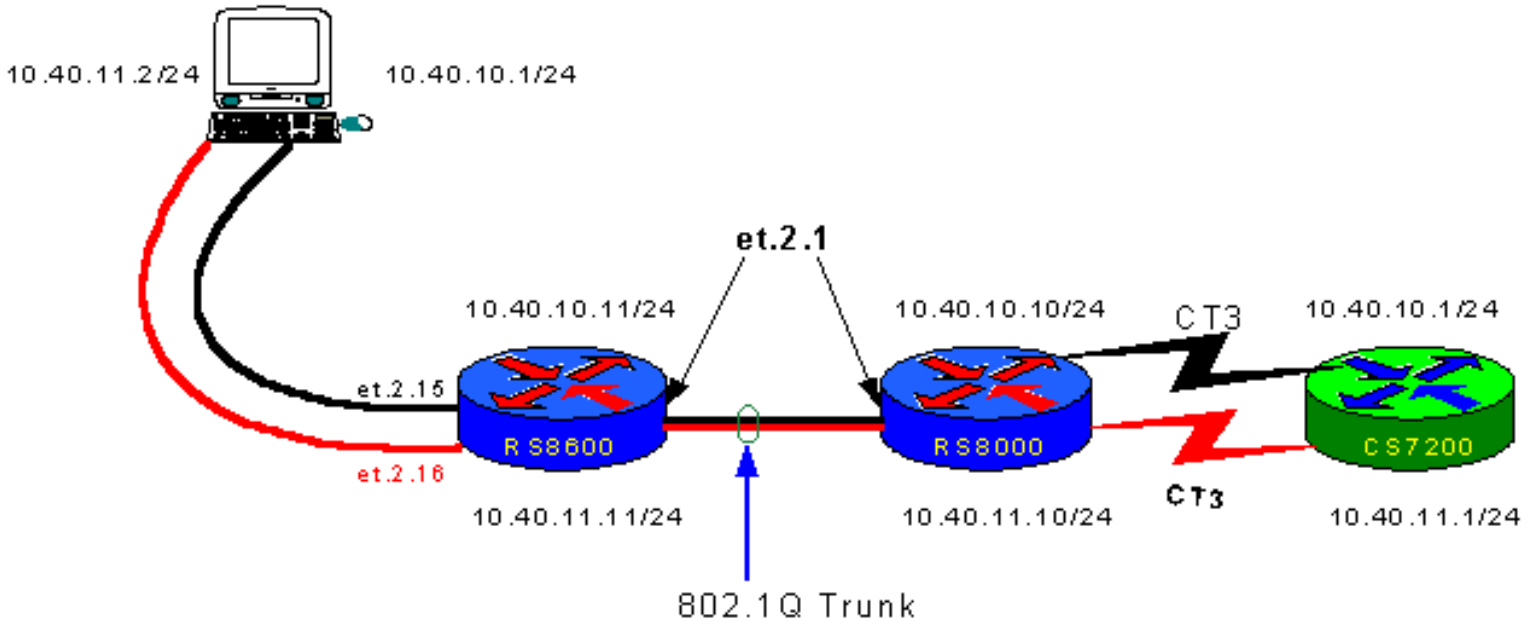
This configuration describes a simple point-to-point connection from a Riverstone channelized T3 (CT3) to another CT3 port and to to a Cisco channelized CT3 port in a 7200 router. The purpose of this test was:

- show the WAN ports could switch and route simultaneously
- act as a 802.1Q trunk port
- co-exist with LAN ports in a VLAN

The PC was equipped with two NICs. Each was configured on a separate subnet and internal IP forwarding was disabled. A 10/100 port was configured between the two Riverstones.

RapidOS Version Tested	8.0.2.1
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	CT3 line card

Diagram



Configurations

RS8600

```
vlan make trunk-port et.2.1
vlan create 10-Net port-based id 2
vlan create 11-Net port-based id 3
vlan add ports et.2.1 to 10-Net
vlan add ports et.2.1 to 11-Net
vlan add ports et.2.15 to 10-Net
vlan add ports et.2.16 to 11-Net
interface create ip 10-Net address-netmask 10.40.10.11/24 vlan 10-Net
interface create ip 11-Net address-netmask 10.40.11.11/24 vlan 11-Net
system set name RS-8600
```

RS8000

```
port set t3.4.1:1 wan-encapsulation ppp timeslots 1-24
port set t3.4.2:2 wan-encapsulation ppp timeslots 1-24
vlan make trunk-port t3.4.2:1
vlan make trunk-port t3.4.2:2
vlan make trunk-port et.2.1
vlan create 10-Net ip id 2
vlan create 11-Net ip id 3
vlan add ports t3.4.1:1 to 10-Net
vlan add ports t3.4.2:2 to 11-Net
vlan add ports et.2.1 to 10-Net
vlan add ports et.2.1 to 11-Net
interface create ip 10-Net address-netmask 10.40.10.10/24 vlan 10-Net
```

```
interface create ip 11-Net address-netmask 10.40.11.10/24 vlan 11-Net
system set name RS-8000
```

Cisco

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
ip subnet-zero
!
controller T3 2/0
 cablelength 10
 t1 1 channel-group 1 timeslots 1-24
!
controller T3 2/1
 cablelength 10
 t1 2 channel-group 2 timeslots 1-24
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial2/0/1:1
 ip address 10.40.10.1 255.255.255.0
 encapsulation ppp
!
interface Serial2/1/2:2
 ip address 10.40.11.2 255.255.255.0
 encapsulation ppp
!
ip classless
no ip http server
!
line con 0
line aux 0
line vty 5 15
!
end
```

Comments

The framing used on the T3 interface is 'm23' which is the most popular, however, check with local loop provider on actual framing used.

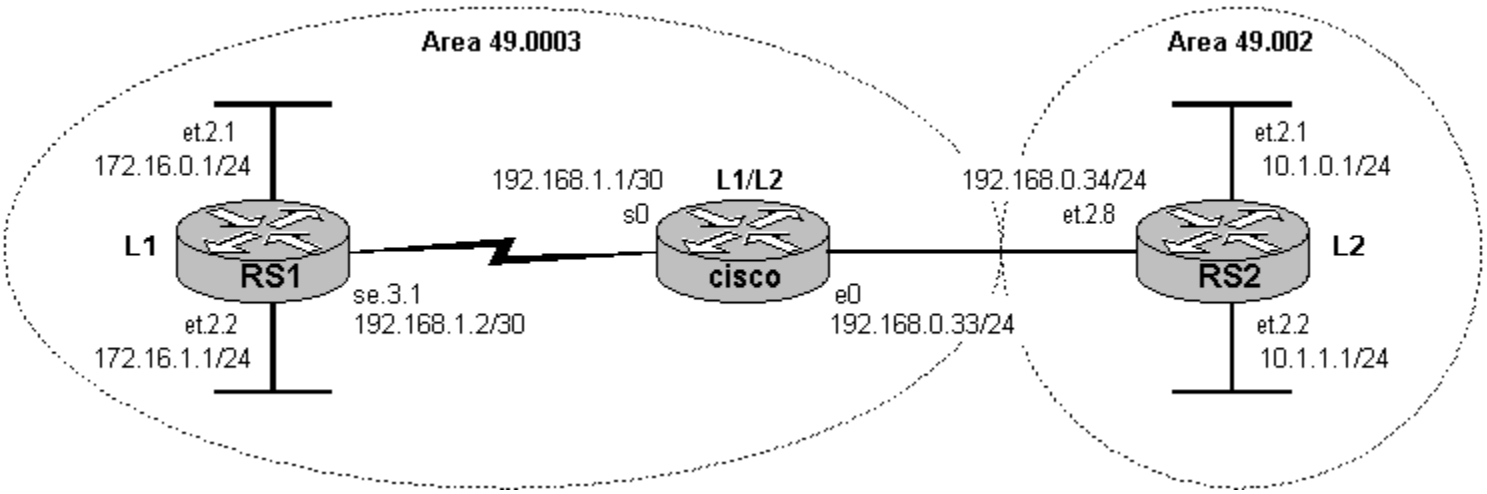
There were no additional configuration needed for this scenario.

IS-IS Interoperability with Cisco

Greg Hankins
Corporate Systems Engineering
April 17, 2001

These configurations show how to configure IS-IS between Riverstone and Cisco routers over ethernet and serial interfaces. Riverstone routers are L1 and L2 routers, and the Cisco is an L1/L2 router.	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	5.x.0.0, 7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	3.1.0.0 and 6.x.0.0
Hardware Specifics	N/A

Diagram



Configurations

RS1

```
version 7.0
port set se.3.1 wan-encapsulation ppp speed 1544000
```

```
interface create ip core address-netmask 192.168.1.2/30 port se.3.1
interface create ip edge1 address-netmask 172.16.0.1/24 port et.2.1
interface create ip edge2 address-netmask 172.16.1.1/24 port et.2.2
interface add ip lo0 address-netmask 192.168.3.1/32
ip-router policy redistribute from-proto direct to-proto isis-level-1
isis add area 49.0003
isis add interface core
isis set level 1
isis start
system set name RS1
```

Cisco

```
version 12.1
!
hostname cisco
!
clns routing
!
interface Loopback0
ip address 192.168.3.2 255.255.255.255
!
interface Ethernet0
 ip address 192.168.0.33 255.255.255.0
 ip router isis
!
interface Serial0
 ip address 192.168.1.1 255.255.255.252
 ip router isis
 encapsulation ppp
!
router isis
 redistribute connected
 net 49.0003.0000.0c35.0e1c.00
```

RS2

```
version 7.0
interface create ip core address-netmask 192.168.0.34/24 port et.2.8
interface create ip edge1 address-netmask 10.1.0.1/24 port et.2.1
interface create ip edge2 address-netmask 10.1.1.1/24 port et.2.2
interface add ip lo0 address-netmask 192.168.3.3/32
ip-router policy redistribute from-proto direct to-proto isis-level-2
isis add area 49.0002
isis add interface edge1
isis add interface edge2
isis add interface core
isis set level 2
isis start
system set name RS2
```

Comments

For each router, the IS-IS adjacencies and IP routing table is shown. Remember that L2 routers never inject routes into L1 areas under normal circumstances, and L1 routers always inject routes into L2 areas. L1 routers install a default route to the nearest L1/L2 router.

RS1

```
RS1# isis show adjacencies

Adjacencies

Interface   SystemID       State  Level Hold(s) SNPA                  Priority
core        0000.0c35.0e1c  up    L1     26

RS1# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
default              192.168.1.1          ISIS_L1   core
127.0.0.1            127.0.0.1            -         lo0
172.16.0.0/24        directly connected   -         edge1
172.16.1.0/24        directly connected   -         edge2
192.168.0.0/24       192.168.1.1          ISIS_L1   core
192.168.1.0/30       192.168.1.1          -         core
192.168.1.1          192.168.1.2          -         core
192.168.1.2          127.0.0.1            -         lo0
192.168.3.1          192.168.3.1          -         lo0
```

Cisco

On a Cisco, you must configure the NET to be the Area ID and System ID. You can just use the MAC address of an interface as the System ID. The NET then becomes "**49.0003.0000.0c35.0e1c.00**". Riverstone routers choose their System ID automagically, but one can be configured if you want.

```
cisco#show interfaces e0 | include addr
  Hardware is Lance, address is 0000.0c35.0e1c (bia 0000.0c35.0e1c)
  Internet address is 192.168.0.33/24

cisco#show clns neighbors

System Id      Interface   SNPA            State  Holdtime  Type Protocol
0000.0202.0202 Et0         00e0.6366.47f1  Up     7         L2   IS-IS
0000.C0A8.0301 Se0         *PPP*           Up     22        L1   IS-IS

cisco#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 2 subnets
i L1    172.16.0.0 [115/10] via 192.168.1.2, Serial0
i L1    172.16.1.0 [115/10] via 192.168.1.2, Serial0
     10.0.0.0/24 is subnetted, 2 subnets
i L2    10.1.1.0 [115/20] via 192.168.0.34, Ethernet0
i L2    10.1.0.0 [115/20] via 192.168.0.34, Ethernet0
C    192.168.0.0/24 is directly connected, Ethernet0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/30 is directly connected, Serial0
C       192.168.1.2/32 is directly connected, Serial0
     192.168.3.0/32 is subnetted, 3 subnets
i L2    192.168.3.3 [115/10] via 192.168.0.34, Ethernet0
```

```
C       192.168.3.2 is directly connected, Loopback0
i L1    192.168.3.1 [115/10] via 192.168.1.2, Serial0
```

RS2

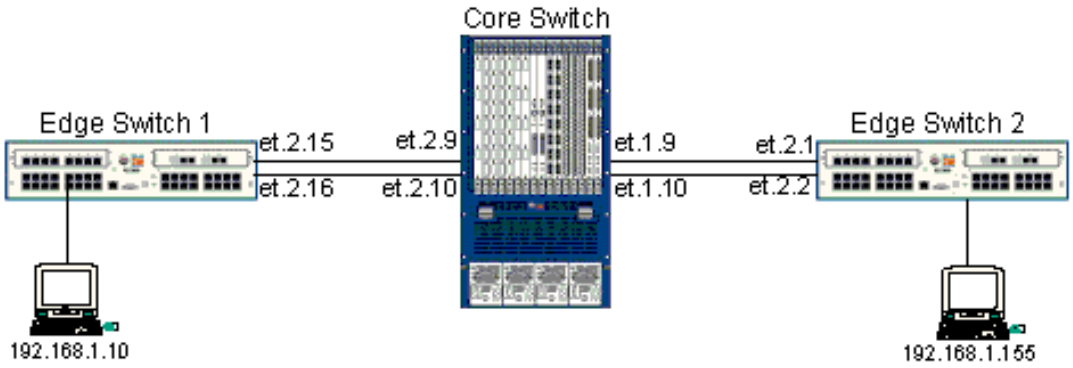
```
RS2# isis show adjacencies

Adjacencies

Interface   SystemID       State  Level Hold(s) SNPA                  Priority
core        0000.0c35.0e1c  up     L2     24     802.2 0:0:c:35:e:1c     64

RS2# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.1.0.0/24          directly connected   -         edge1
10.1.1.0/24          directly connected   -         edge2
127.0.0.1            127.0.0.1            -         lo0
172.16.0.0/24        192.168.0.33         ISIS_L2   core
172.16.1.0/24        192.168.0.33         ISIS_L2   core
192.168.0.0/24       directly connected   -         core
192.168.1.0/30       192.168.0.33         ISIS_L2   core
192.168.1.2          192.168.0.33         ISIS_L2   core
192.168.3.1          192.168.0.33         ISIS_L2   core
192.168.3.2          192.168.0.33         ISIS_L2   core
192.168.3.3          192.168.3.3          -         lo0
```

Extending an L2 Domain with Ring STP and GVRP

Payam Kahen
Systems Engineering
September 5, 2001

This article demonstrates the use of Ring STP to extend the traditional limitation of 6-7 switches in a Spanning Tree. GVRP is used for dynamic VLAN creation through a Layer-2 broadcast domain, across multiple Spanning Tree rings.	
RapidOS Version Tested	7.0.2.0
RapidOS Versions Working with this Configuration	7.0.2.0, 9.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	6.x, 7.0.0.x, 7.0.1.x, 8.x
Hardware Specifics	N/A

Diagram



Configurations

Edge Switch #1

```
stp set protocol-version rstp
stp enable port et.2.15-16
vlan make trunk-port et.2.15-16
vlan create cust0 ip id 10
vlan add ports et.1.5 to cust0
vlan add ports et.2.15-16 to cust0
system set name Edge-1
gvrp enable ports et.2.15-16
gvrp enable ports et.1.5
gvrp start
```

Core Switch

```
stp set protocol-version rstp
stp rer-create ring ring_id 2000
stp rer-create ring ring_id 1000
stp rer-add ports et.1.9-10 to 2000
stp rer-add ports et.2.9-10 to 1000
stp rer-enable
vlan make trunk-port et.1.9-10
vlan make trunk-port et.2.9-10
system set name CORE-Switch
gvrp enable ports et.1.9-10
gvrp enable ports et.2.9-10
gvrp enable dynamic-vlan-creation
gvrp start
```

Edge Switch #2

```
stp set protocol-version rstp
stp enable port et.2.1-2
vlan make trunk-port et.2.1-2
vlan create cust0 port-based id 10
vlan add ports et.1.1 to cust0
vlan add ports et.2.1-2 to cust0
system set name Edge-2
gvrp enable ports et.2.1-2
gvrp enable ports et.1.1
gvrp start
```

Comments

The Core switches with Ring STP will contain Spanning Tree BPDU traffic among each configured ring, yet transmit Ethernet frames beyond the ring, based on the regular l2-table entries.

```
[payamk@lab-ws log]# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) from 192.168.1.155 : 56(84) bytes of data.
64 bytes from 192.168.1.10: icmp_seq=0 ttl=128 time=344 usec
64 bytes from 192.168.1.10: icmp_seq=1 ttl=128 time=1.400 msec
--- 192.168.1.10 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.344/0.872/1.400/0.528 ms
```

Ring STP only needs to be configured on the Core switches that are connecting to more than one ring. Switches connecting to only a single Ethernet Ring are not required to run Ring STP. GVRP needs to be enabled on all switches, but "dynamic-vlan-creation" only on Core switches.

STP status on ports with Ring STP enabled can be viewed with the following:

```
CORE-Switch# stp show ring-port-info ring_id 1000
Status for Spanning Tree Instance 1000
   Bridge ID        : 8000:000285054cc0
   Root bridge      : 8000:00028502dd80
   To Root via port : et.2.9  (Bridge Port Number: 41)
   Root port cost   : 10
   Ports in bridge  : 2
   Max age          : 20 secs
   Hello time       : 2 secs
   Forward delay    : 15 secs
   Topology changes : 2
   Last Topology Chg: 0 days 1 hours 8 min 57 secs ago
                                                                    Designated
Port          Priority  Cost   STP       State      Designated-Bridge  Port
----          --------  ----   ---       -----      -----------------  ----------
et.2.9           000    00010  Enabled   Forwarding 8000:00028502dd80     0 02f
et.2.10          000    00010  Enabled   Blocking   8000:00028502dd80     0 030

CORE-Switch# stp show ring-port-info ring_id 2000
Status for Spanning Tree Instance 2000
   Bridge ID        : 8000:000285054cc0
   Root bridge      : 8000:000285054cc0
   To Root via port : n/a
   Ports in bridge  : 2
   Max age          : 20 secs
   Hello time       : 2 secs
   Forward delay    : 15 secs
   Topology changes : 0
   Last Topology Chg: 0 days 4 hours 13 min 29 secs ago
                                                                    Designated
Port          Priority  Cost   STP       State      Designated-Bridge  Port
----          --------  ----   ---       -----      -----------------  ----------
et.1.9           000    00010  Enabled   Forwarding 8000:000285054cc0     0 019
et.1.10          000    00010  Enabled   Forwarding 8000:000285054cc0     0 01a
```

Because Ring STP has not been enabled on the Edge switches, Spanning Tree status on ports can be viewed through the ordinary command "port show stp-info <port-list>":

```
Edge-2# port show stp-info et.2.1-2
                                                                    Designated
Port          Priority  Cost   STP       State      Designated-Bridge  Port
----          --------  ----   ---       -----      -----------------  ----------
et.2.1           000    00010  Enabled   Forwarding 8000:000285054cc0     0 019
et.2.2           000    00010  Enabled   Blocking   8000:000285054cc0     0 01a
```

The output of "vlan show" demonstrates that vlan id 10 has been created on a Core switch:

```
CORE-Switch# vlan show
VID      VLAN Name        Used for                          Ports
---      ---------        --------                          -----
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-8,10-16), et.2.(1-
8,11-16)
10   SYS_GVRP_10    IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.9, et.2.(9-10)
```

Using L2 Filters To Enable Private VLANs Within A Single RS

Richard Foote
Corporate Systems Engineering
May 25, 2001

Layer two filters are a powerful and flexible tool to provide customer isolation within the same IP and VLAN space. If you are familiar with the Cisco Systems *"Private VLAN"* concept then you should be comfortable with the concepts delivered here. To reduce the learning curve the Cisco terms and definitions are presented in this document. For further information on the Cisco approach to *Private VLANs* refer to http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm.

Here it will be shown how layer two filters can provide the security necessary to allow the provider to share a common VLAN and IP Address space across many different customers who share the same aggregation node. This approach saves the provider IP addresses and VLAN identifiers.

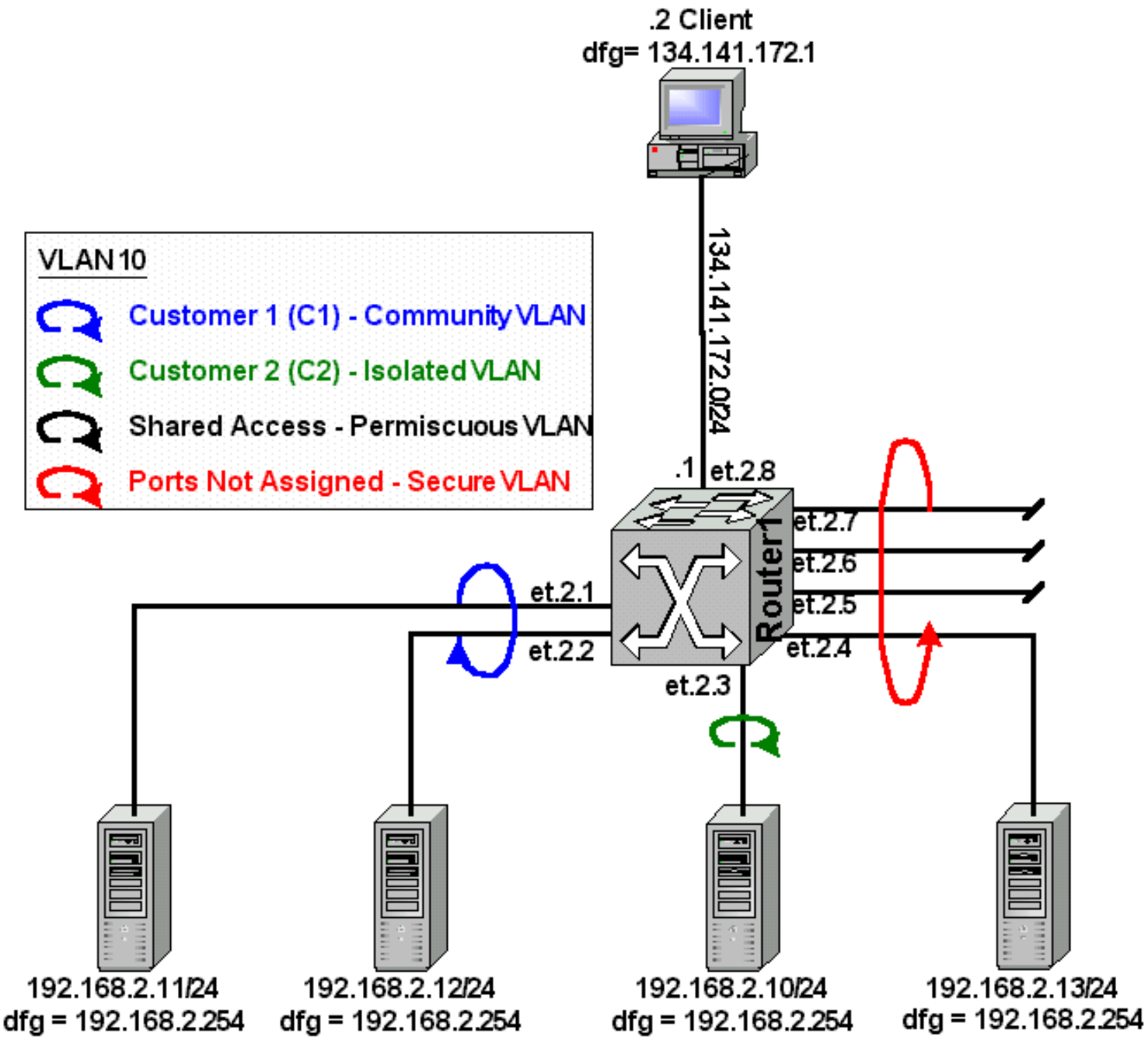
Four different VLAN personalities sharing the space need to be defined. The shared port(s) that all nodes in the VLAN need access to is referred to as *Promiscuous VLAN*. Any single port customer that requires access only to the promiscuous port is an *Isolated VLAN.* Thirdly, and multi-port customer that requires their ports to directly communicate at layer two and also access the promiscuous port is viewed as a *Community VLAN.* Finally, a concept not explicitly defined by Cisco, is the lockdown of unused customer facing ports. These unallocated customer facing ports are the *Secure VLAN.*

This paper provides a slightly different configuration than represented by the configuration document "Using L2 Filters To Enable Private VLANs Discrete Layer 2 Aggregation". This document consolidates everything into a single RS.

RapidOS Version Tested	7.0.0.0 & 7.0.0.1
RapidOS Versions Working with this Configuration	6.2.x.x & 6.3.x.x
RapidOS Versions NOT Working with this Configuration	5.1.x.x & 6.0.x.x [1]
Hardware Specifics	None

[1] Missing the ability to set "**`dest-mac any`**" as part of the "**`filters add static-entry`**" command.

Diagram



Configurations

Router1

```
vlan create Servers ip id 10
vlan add ports et.2.(1-7) to Servers
interface create ip Shared address-netmask 192.168.2.254/24 vlan Servers
interface create ip Interent address-netmask 134.141.172.1/24 port et.2.8
```

```
system set name Router1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2)
out-port-list et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3
out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
```

Comments

All four VLAN personalities are represented in this document. For the configuration above let's assume the only ports available for customer consumption sharing the same VLAN and IP address space are et.2.(1-7). Any other ports on the RS would be configured outside this *"Private VLAN"* (ie. On a separate VLAN and IP Address space). In this case, et.2.8 is actually a separate VLAN and IP address space leading to our test client. In the real world port et.2.8 could be a link to another router, not just some test client.

There is no physical port defined as the *promiscuous* VLAN. In this case the IP address 192.168.2.254 is assigned to the group of ports in VLAN 10, et.2.(1-7). All of these ports have access to this interface. Therefore, it is providing promiscuous service to all sub-VLANs within this *Private VLAN.*

The command "**`filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2)out-port-list et.2.(3-7) vlan 10 restriction disallow`**" creates a *Community VLAN*, C1, consisting of et.2.1 & et.2.2. The devices connected to these ports, server 192.168.2.11 & server 192.168.2.12 can communicate directly with each other as well as communicating with the default gateway 192.1682.254. There is no communication capable between the C1 community ports et.2.(3-7).

The command "**`filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow`**" creates an

Isolated VLAN, C2, consisting of a single physical port, et.2.3. This port only has access to the default gateway 192.168.2.254. There is no communication capable between the C2 isolated port et.2.1 and the ports et.2.(1-2,4-7).

The command "**`filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction source`**" locks down any ports that are available for customers but have not been populated, creating the *Secure VLAN*. This is a security measure to prevent someone from plugging in to one of the unassigned ports and being able to generate traffic into the other sub-VLANs in the *Private VLAN*. Thus, preventing a possible DoS type attack by dropping all packets that are generated by devices on these ports.

Client 134.141.172.2/24 has complete and full access to all devices in the *Private VLAN*.

Simple testing demonstrate how these features work. Consider using either Web based http, TCP port 80, traffic or simple ping. Ping shows better because of the real-time nature of the interruption, when the security filters are applied. The table below shows which devices can communicate. Note: All devices can communicate to their respective default gateways except for nodes in the *Secure VLAN.*

	192.168.2.10	192.168.2.11	192.168.2.12	192.168.2.13	134.141.172.2
192.168.2.10		No	No	No	Yes
192.168.2.11	No		Yes	No	Yes
192.168.2.12	No	Yes		No	Yes

192.168.2.13	**No**	**No**	**No**		**No**
134.141.172.2	**Yes**	**Yes**	**Yes**	**Yes**	

Start the ping communication between all devices, as shown in the table above, without any security filters. Now add the security features and watch the clients after each filter is added. The ping streams between the devices will now adhere to the applied security rules. Once all the rules have been applied, communication between the devices should resemble the above.

Note: You may notice that changing these filters as new customers are added may become a bit administrative. Consider this implementation and design detail. When a new customer is added ensure the "**`out-port-list`**" used in each customer filter covers all possible customer facing ports. This way, as new customers are added and ports are removed from the *Secure VLAN* and assigned to customer sub-VLAN, be they isolated or community, no changes will be required to the existing customer filters. They have already been instructed not to use any of those ports.

Note: If new blades are added, then all existing customer filters will need to be changed to ensure those new ports are excluded from the customers that should not communicate to the new ports.

Multiple rules of the same name - If a current filter exists covering a port or set of ports and a new rule is added with the same name, expanding the "**`out-port-list`**", the command is accepted and used, instead of the old rule. Here is a description of what actually occurs.

Starting Router Config.

```
vlan create Servers ip id 10
vlan add ports et.2.(1-7) to Servers
interface create ip Shared address-netmask 192.168.2.254/24 vlan Servers
interface create ip Interent address-netmask 134.141.172.1/24 port et.2.8
system set name Router1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2)
out-port-list et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3
out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
```

Router1# filters show static-entry - Everything is right with the world.

```
Name:            C1
----
Direction:       destination
Restriction:     disallow-to-go
VLAN:            10
Source MAC:      000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:        any
Dest MAC Mask:   FFFFFF:FFFFFF
In-List ports:   et.2.(1-2)
Out-List ports: et.2.(3-7)
```

```
Name:            C2
----
Direction:       destination
Restriction:     disallow-to-go
VLAN:            10
Source MAC:      000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:        any
Dest MAC Mask:   FFFFFF:FFFFFF
In-List ports:   et.2.3

Out-List ports: et.2.(1-2,4-7)
```

New Router Config - Added new ports to VLAN 10 and expanded C1 rule to exclude gi.3.1 & gi.3.2.

```
version 7.0
vlan create Servers ip id 10
vlan add ports et.2.(1-7) to Servers
vlan add ports gi.3.(1-2) to Servers
interface create ip Shared address-netmask 192.168.2.254/24 vlan Servers
interface create ip Interent address-netmask 134.141.172.1/24 port et.2.8
interface add ip en0 address-netmask 24.112.72.1/21
system set name Router1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list
et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7),gi.3(1-2) vlan 10 restriction disallow
```

Console message - `%L2TM-I-CLI_ACK, Successful static entry registration (C1)`

Router1# filters show static-entry - Everything is right with the world.

```
Name:           C1
----
Direction:      destination
Restriction:    disallow-to-go
VLAN:           10
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.2.(1-2)
Out-List ports: et.2.(3-7),gi.3.(1-2)
```

```
Name:           C2
----
Direction:      destination
Restriction:    disallow-to-go
VLAN:           10
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.2.3
Out-List ports: et.2.(1-2,4-7)
```

Removing either C1 static entry rule - (1st in config or 2nd in config) causes the entire rule set for C1 to be removed! No more static filters apply to C1.

```
Router1(config)# negate 8
Router1(config)# save active
%L2TM-I-CLI_ACK, Successful static entry unregistration (C1)
```

Router Config

```
version 7.0
vlan create Servers ip id 10
vlan add ports et.2.(1-7) to Servers
vlan add ports gi.3.(1-2) to Servers
interface create ip Shared address-netmask 192.168.2.254/24 vlan Servers
interface create ip Interent address-netmask 134.141.172.1/24 port et.2.8
```

```
interface add ip en0 address-netmask 24.112.72.1/21
system set name Router1
filters add static-entry name C2 dest-mac any in-port-list et.2.3
out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7)
vlan 10 direction source
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2)
out-port-list et.2.(3-7),gi.3.(1-2) vlan 10 restriction disallow
```

Router1# filters show static-entry - Everything is not okay with the world.

(No C1 rules exist)	Name: C2 ---- Direction: destination Restriction: disallow-to-go VLAN: 10 Source MAC: 000000:000000 Source MAC Mask:FFFFFF:FFFFFF Dest MAC: any Dest MAC Mask: FFFFFF:FFFFFF In-List ports: et.2.3 Out-List ports: et.2.(1-2,4-7)

Ghost commands in configuration remain and can be cleaned out.

```
Router1(config)# negate 10
Router1(config)# save active
%CLI-E-FAILED, Execution failed for "no filters add static-entry name C1 dest-mac any
in-port-list et.2.(1-2) out-port-list et.2.(3-7),gi.3.(1-2) vlan 10 restriction
disallow"
```

Using L2 Filters To Enable Private VLANs Discrete Layer 2 Aggregation

Richard Foote
Corporate Systems Engineering
May 25, 2001

Layer two filters are a powerful and flexible tool to provide customer isolation within the same IP and VLAN space. If you are familiar with the Cisco Systems *"Private VLAN"* concept then you should be comfortable with the concepts delivered here. To reduce the learning curve the Cisco terms and definitions are presented in this document. For further information on the Cisco approach to *Private VLANs* refer to http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/c65sp_wp.htm.

Here it will be shown how layer two filters can provide the security necessary to allow the provider to share a common VLAN and IP Address space across many different customers who share the same aggregation node. This approach saves the provider IP addresses and VLAN identifiers.

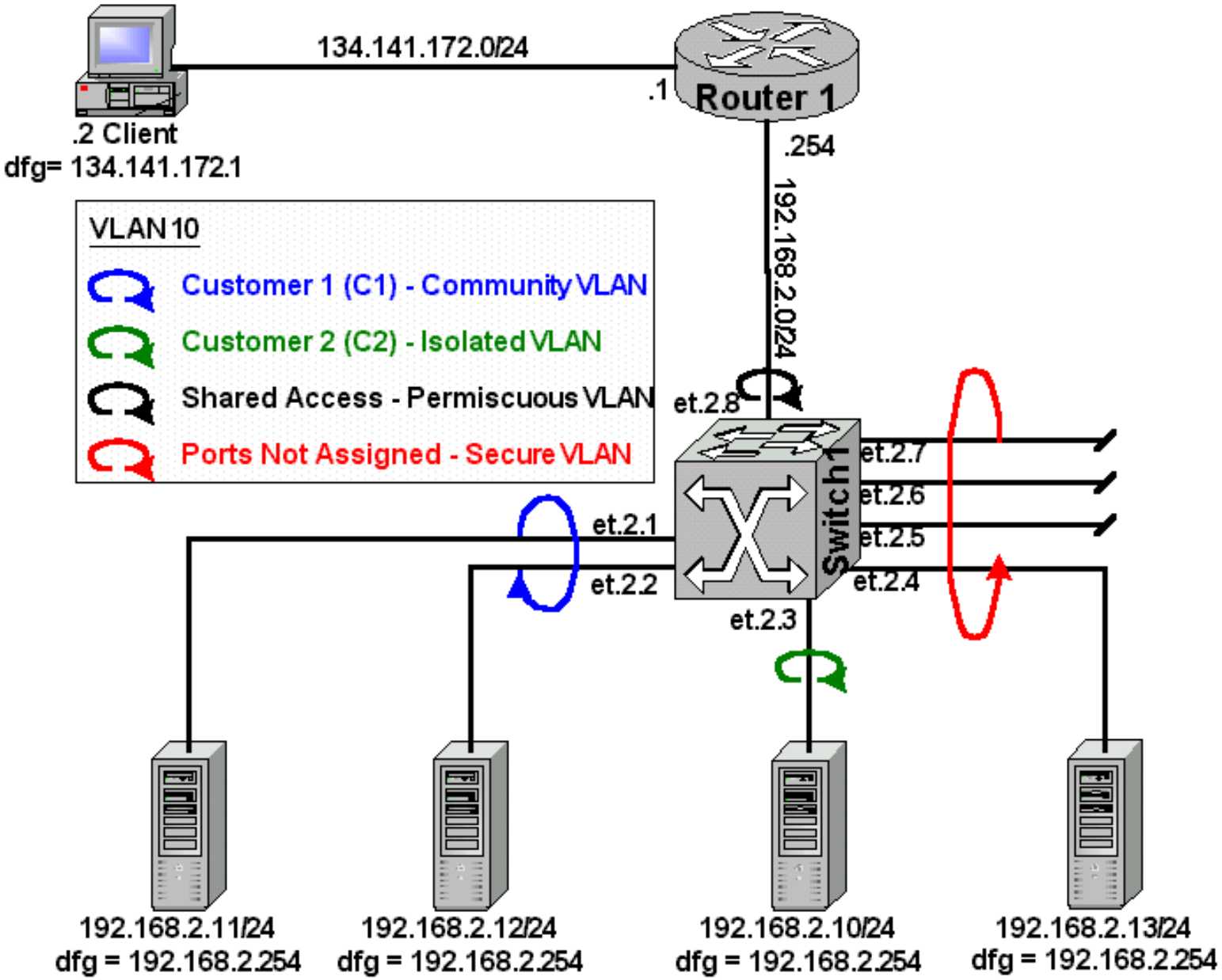
Four different VLAN personalities sharing the space need to be defined. The shared port(s) that all nodes in the VLAN need access to is referred to as *Promiscuous VLAN*. Any single port customer that requires access only to the promiscuous port is an *Isolated VLAN.* Thirdly, and multi-port customer that requires their ports to directly communicate at layer two and also access the promiscuous port is viewed as a *Community VLAN.* Finally, a concept not explicitly defined by Cisco, is the lockdown of unused customer facing ports. These unallocated customer facing ports are the *Secure VLAN.*

This paper provides a slightly different configuration than represented by the configuration document "Using L2 Filters To Enable Private VLANs Within A Single RS". This document separates the layer two and layer three functions across different RS.

RapidOS Version Tested	7.0.0.0 & 7.0.0.1
RapidOS Versions Working with this Configuration	6.2.x.x & 6.3.x.x
RapidOS Versions NOT Working with this Configuration	5.1.x.x & 6.0.x.x [1]
Hardware Specifics	None

[1] Missing the ability to set "**`dest-mac any`**" as part of the "**`filters add static-entry`**" command.

Diagram



Configurations

Switch1

```
vlan create Servers ip id 10
vlan add ports et.2.8 to Servers
interface create ip Servers address-netmask 192.168.2.254/24 vlan Servers
interface create ip Net address-netmask 134.141.172.1/24 port et.2.1
system set name Router1
```

Router1

```
vlan create Servers ip id 10
vlan add ports et.2.(1-8) to Servers
system set name Switch1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list
et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
```

Comments

All four VLAN personalities are represented in this document. For the configuration above let's assume the only ports available for customer consumption sharing the same VLAN and IP address space are et.2.(1-8). Any other ports on the RS would be configured outside this *"Private VLAN"* (ie. On a separate VLAN and IP Address space).

Port et.2.8 is acting as a normal port in VLAN 10. Since there are no rules preventing it from talking to anybody else and no rules preventing anyone else communicating with it, it is accessible to all ports in VLAN 10. This essentially places port et.2.8 in the *promiscuous VLAN*.

The command "**`filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2)out-port-list et.2.(3-7) vlan 10 restriction disallow`**" creates a *Community VLAN*, C1, consisting of et.2.1 & et.2.2. The devices connected to these ports, server 192.168.2.11 & server 192.168.2.12 can communicate directly with each other as well as communicating with the default gateway 192.1682.254. There is no communication capable between the C1 community ports et.2.(3-7).

The command "**`filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow`**" creates an

Isolated VLAN, C2, consisting of a single physical port, et.2.3. This port only has access to the default gateway 192.168.2.254. There is no communication capable between the C2 isolated port et.2.1 and the ports et.2.(1-2,4-7).

The command "**`filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction source`**" locks down any ports that are available for customers but have not been populated, creating the *Secure VLAN*. This is a security measure to prevent someone from plugging in to one of the unassigned ports and being able to generate traffic into the other sub-VLANs in the *Private VLAN*. Thus, preventing a possible DoS type attack by dropping all packets that are generated by devices on these ports.

Client 134.141.172.2/24 has complete and full access to all devices in the *Private VLAN*.

Simple testing demonstrate how these features work. Consider using either Web based http, TCP port 80, traffic or simple ping. Ping shows better because of the real-time nature of the interruption, when the security filters are applied. The table below shows which devices can communicate. Note: All devices can communicate to their respective default gateways except for nodes in the *Secure VLAN.*

	192.168.2.10	192.168.2.11	192.168.2.12	192.168.2.13	134.141.172.2
192.168.2.10		No	No	No	Yes
192.168.2.11	No		Yes	No	Yes

192.168.2.12	**No**	**Yes**		**No**	**Yes**
192.168.2.13	**No**	**No**	**No**		**No**
134.141.172.2	**Yes**	**Yes**	**Yes**	**Yes**	

Start the ping communication between all devices, as shown in the table above, without any security filters. Now add the security features and watch the clients after each filter is added. The ping streams between the devices will now adhere to the applied security rules. Once all the rules have been applied, communication between the devices should resemble the above.

Note: You may notice that changing these filters as new customers are added may become a bit administrative. Consider this implementation and design detail. When a new customer is added ensure the "**`out-port-list`**" used in each customer filter covers all possible customer facing ports. This way, as new customers are added and ports are removed from the *Secure VLAN* and assigned to customer sub-VLAN, be they isolated or community, no changes will be required to the existing customer filters. They have already been instructed not to use any of those ports.

Note: If new blades are added, then all existing customer filters will need to be changed to ensure those new ports are excluded from the customers that should not communicate to the new ports.

Multiple rules of the same name – If a current filter exists covering a port or set of ports and a new rule is added with the same name, expanding the "**`out-port-list`**", the command is accepted and used, instead of the old rule. Here is a description of what actually occurs.

Starting Router Config.

```
vlan create Servers ip id 10
vlan add ports et.2.(1-8) to Servers
system set name Switch1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list
et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
```

Router1# Filters show static-entry - Everything is right with the world.

```
Name:             C1
----
Direction:        destination
Restriction:      disallow-to-go
VLAN:             10
Source MAC:       000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:         any
Dest MAC Mask:    FFFFFF:FFFFFF
In-List ports:    et.2.(1-2)
Out-List ports:   et.2.(3-7)
```

```
Name:             C2
----
Direction:        destination
Restriction:      disallow-to-go
VLAN:             10
Source MAC:       000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:         any
Dest MAC Mask:    FFFFFF:FFFFFF
In-List ports:    et.2.3
Out-List ports:   et.2.(1-2,4-7)
```

New Switch1 Configuration - Added new ports to **VLAN 10** and expanded **C1 rule to exclude gi.3.1 & gi.3.2**.

```
version 7.0
vlan create Servers ip id 10
vlan add ports et.2.(1-8) to Servers
vlan add ports gi.3.(1-2) to Servers
system set name Switch1
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7) vlan 10 restriction disallow
filters add static-entry name C2 dest-mac any in-port-list et.2.3 out-port-list
et.2.(1-2,4-7) vlan 10 restriction disallow
filters add secure-port name LockDown in-port-list et.2.(4-7) vlan 10 direction
source
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7),gi.3.(1-2) vlan 10 restriction disallow
```

Console message - `%L2TM-I-CLI_ACK, Successful static entry registration (C1)`

Router1# Filters show static-entry - Everything is right with the world.

```
Name:           C1
----
Direction:      destination
Restriction:    disallow-to-go
VLAN:           10
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.2.(1-2)
Out-List ports: et.2.(3-7),gi.3.(1-2)
```

```
Name:           C2
----
Direction:      destination
Restriction:    disallow-to-go
VLAN:           10
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.2.3
Out-List ports: et.2.(1-2,4-7)
```

Removing either C1 static entry rule - (1st in config or 2nd in config) causes the entire rule set for C1 to be removed! No more static filters apply to C1.

```
Router1(config)# negate 8
Router1(config)# save active
%L2TM-I-CLI_ACK, Successful static entry unregistration (C1)
```

Router Config

```
vlan create Servers ip id 10
vlan add ports et.2.(1-8) to Servers
vlan add ports gi.3.(1-2) to Servers
system set name Switch1
filters add static-entry name C2 dest-mac any in-port-list et.2.3
out-port-list et.2.(1-2,4-7) vlan 10 restriction disallow filters add secure-port
name LockDown in-port-list et.2.(4-7) vlan 10 direction source
filters add static-entry name C1 dest-mac any in-port-list et.2.(1-2) out-port-list
et.2.(3-7),gi.3.(1-2) vlan 10 restriction disallow
```

Router1# Filters show static-entry – Everything is not okay with the world.

(No C1 rules exist)	Name: C2 ---- Direction: destination Restriction: disallow-to-go VLAN: 10 Source MAC: 000000:000000 Source MAC Mask:FFFFFF:FFFFFF Dest MAC: any Dest MAC Mask: FFFFFF:FFFFFF In-List ports: et.2.3 Out-List ports: et.2.(1-2,4-7)

Ghost commands in configuration remain and can be cleaned out.

```
Router1(config)# negate 10
Router1(config)# save active
%CLI-E-FAILED, Execution failed for "no filters add static-entry name C1 dest-mac any
in-port-list et.2.(1-2) out-port-list et.2.(3-7),gi.3.(1-2) vlan 10 restriction
disallow"
```

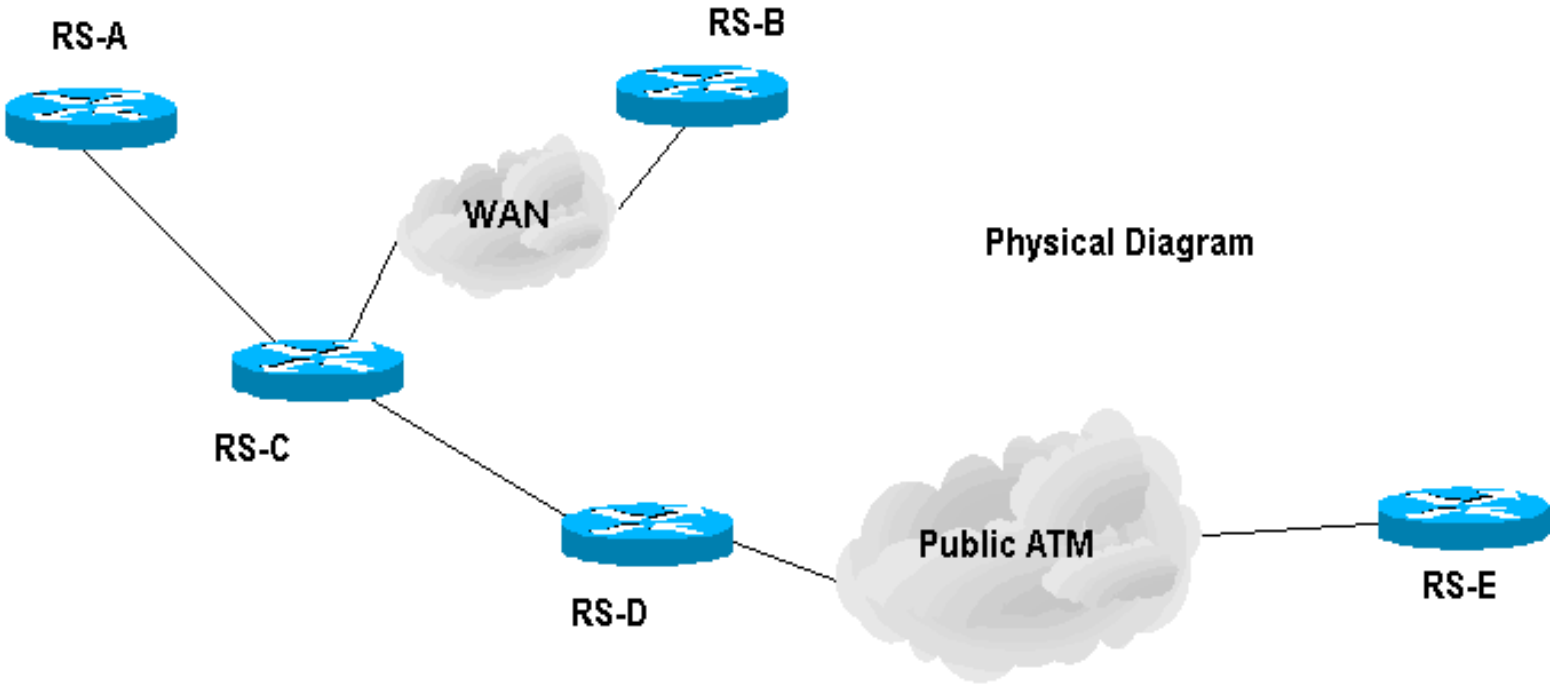
Point-to-Point VLANs over Ethernet, ATM and T1

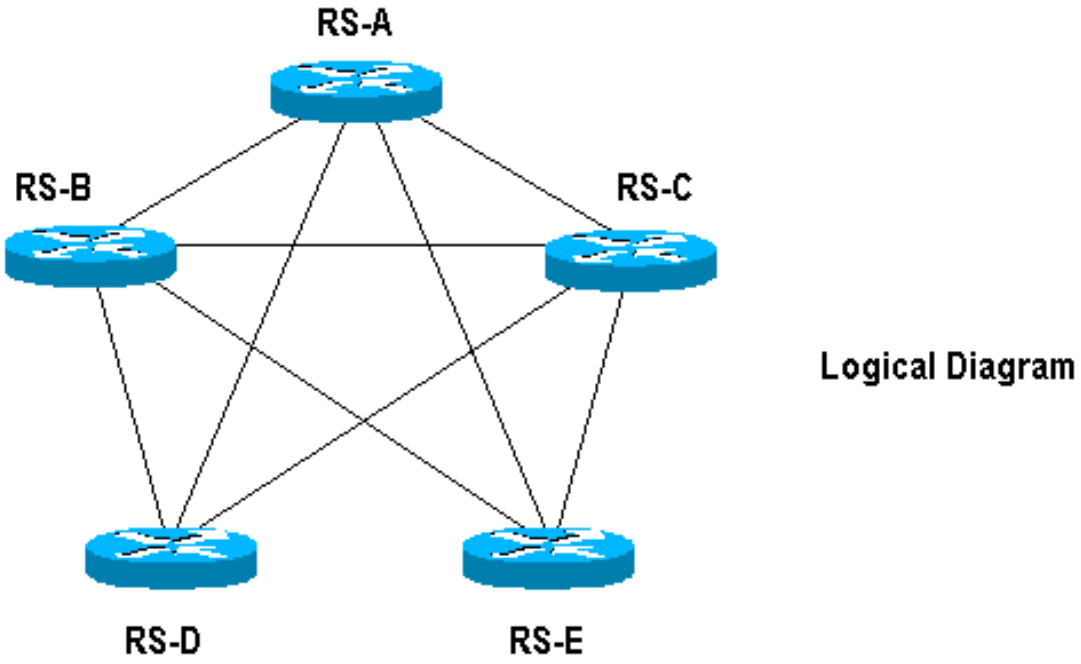
Jeff McLaird
Corporate Systems Engineering
November 13, 2001

One problem facing many providers is maintaining a contiguous backbone whilst still allowing for expansion. A possible solution to this can be realized by using WDM technology or MPLS. However each require a further investment in both training and equipment. By using a point-to-point VLAN configuration the network administrator is able to maximize the existing infrastructure equipment while maintaining full mesh connectivity and providing a methodology for growth.

RapidOS Version Tested	ROS 8.0.1.1
RapidOS Versions Working with this Configuration	All versions of ROS should work, but there are some technology related firmware dependencies. Please refer to release notes for more information.
RapidOS Versions NOT Working with this Configuration	As above
Hardware Specifics	N/A

Diagram





Configurations

RS8000 - RS-A

```
vlan make trunk-port et.1.1
vlan create a2b ip id 10
vlan create a2c ip id 20
vlan create a2d ip id 30
vlan create a2e ip id 40
vlan add ports et.1.1 to a2b
vlan add ports et.1.1 to a2c
vlan add ports et.1.1 to a2d
```

```
vlan add ports et.1.1 to a2e
!
interface create ip a2b address-netmask 10.10.10.1/30 vlan a2b
interface create ip a2c address-netmask 10.10.10.5/30 vlan a2c
interface create ip a2d address-netmask 10.10.10.9/30 vlan a2d
interface create ip a2e address-netmask 10.10.10.13/30 vlan a2e
```

RS8000 - RS-B

```
port set se.4.1 wan-encapsulation ppp speed 1536000
!
vlan make trunk-port se.4.1
vlan create a2b ip id 10
vlan create b2c ip id 50
vlan create b2d ip id 60
vlan create b2e ip id 70
vlan add ports se.4.1 to a2b
vlan add ports se.4.1 to b2c
vlan add ports se.4.1 to b2d
vlan add ports se.4.1 to b2e
!
interface create ip b2c address-netmask 10.10.10.17/30 vlan b2c
interface create ip b2d address-netmask 10.10.10.21/30 vlan b2d
interface create ip b2e address-netmask 10.10.10.25/30 vlan b2e
interface create ip a2b address-netmask 10.10.10.2/30 vlan a2b
```

RS8000 - RS-C

```
vlan make trunk-port et.1.1
vlan make trunk-port et.1.2
vlan create a2b ip id 10
vlan create a2c ip id 20
vlan create a2d ip id 30
vlan create a2e ip id 40
vlan create c2d ip id 80
vlan create c2e ip id 90
vlan create b2c ip id 50
vlan add ports et.1.1 to a2c
vlan add ports et.1.1 to a2d
vlan add ports et.1.2 to a2d
vlan add ports et.1.1 to a2e
vlan add ports et.1.2 to a2e
vlan add ports et.1.2 to c2d
vlan add ports et.1.2 to c2e
vlan add ports et.1.2 to b2c
vlan add ports et.1.1 to a2b
vlan add ports et.1.2 to a2b
!
interface create ip a2c address-netmask 10.10.10.6/30 vlan a2c
interface create ip c2d address-netmask 10.10.10.29/30 vlan c2d
interface create ip c2e address-netmask 10.10.10.33/30 vlan c2e
```

```
interface create ip b2c address-netmask 10.10.10.18/30 vlan b2c
```

RS8000 - RS-D

```
port set se.4.3 wan-encapsulation ppp speed 1536000
!
atm create vcl port at.6.1.0.120
!
vlan make trunk-port at.6.1.0.120
vlan make trunk-port et.2.1
vlan make trunk-port se.4.3
vlan create a2d ip id 30
vlan create b2d ip id 60
vlan create c2d ip id 80
vlan create c2e ip id 90
vlan create d2e ip id 100
vlan create a2e ip id 40
vlan create b2c ip id 50
vlan create b2e ip id 70
vlan create a2b ip id 10
vlan add ports se.4.3 to b2d
vlan add ports et.2.1 to a2d
vlan add ports at.6.1.0.120 to d2e
vlan add ports at.6.1.0.120 to a2e
vlan add ports et.2.1 to a2e
vlan add ports se.4.3 to b2c
vlan add ports et.2.1 to b2c
vlan add ports se.4.3 to b2e
vlan add ports at.6.1.0.120 to b2e
vlan add ports se.4.3 to a2b
vlan add ports et.2.1 to a2b
vlan add ports et.2.1 to c2d
vlan add ports et.2.1 to c2e
vlan add ports at.6.1.0.120 to c2e
!
interface create ip d2e address-netmask 10.10.10.37/30 vlan d2e
interface create ip c2d address-netmask 10.10.10.30/30 vlan c2d
interface create ip b2d address-netmask 10.10.10.22/30 vlan b2d
interface create ip a2d address-netmask 10.10.10.10/30 vlan a2d
```

RS8000 - RS-E

```
atm create vcl port at.4.2.0.130
atm set vcl port at.4.2.0.130 forced-bridged
!
vlan make trunk-port at.4.2.0.130
vlan create a2e ip id 40
vlan create b2e ip id 70
vlan create c2e ip id 90
vlan create d2e ip id 100
vlan add ports at.4.2.0.130 to d2e
```

```
vlan add ports at.4.2.0.130 to c2e
vlan add ports at.4.2.0.130 to b2e
vlan add ports at.4.2.0.130 to a2e
!
interface create ip d2e address-netmask 10.10.10.38/30 vlan d2e
interface create ip c2e address-netmask 10.10.10.34/30 vlan c2e
interface create ip b2e address-netmask 10.10.10.26/30 vlan b2e
interface create ip a2e address-netmask 10.10.10.14/30 vlan a2e
```

Comments

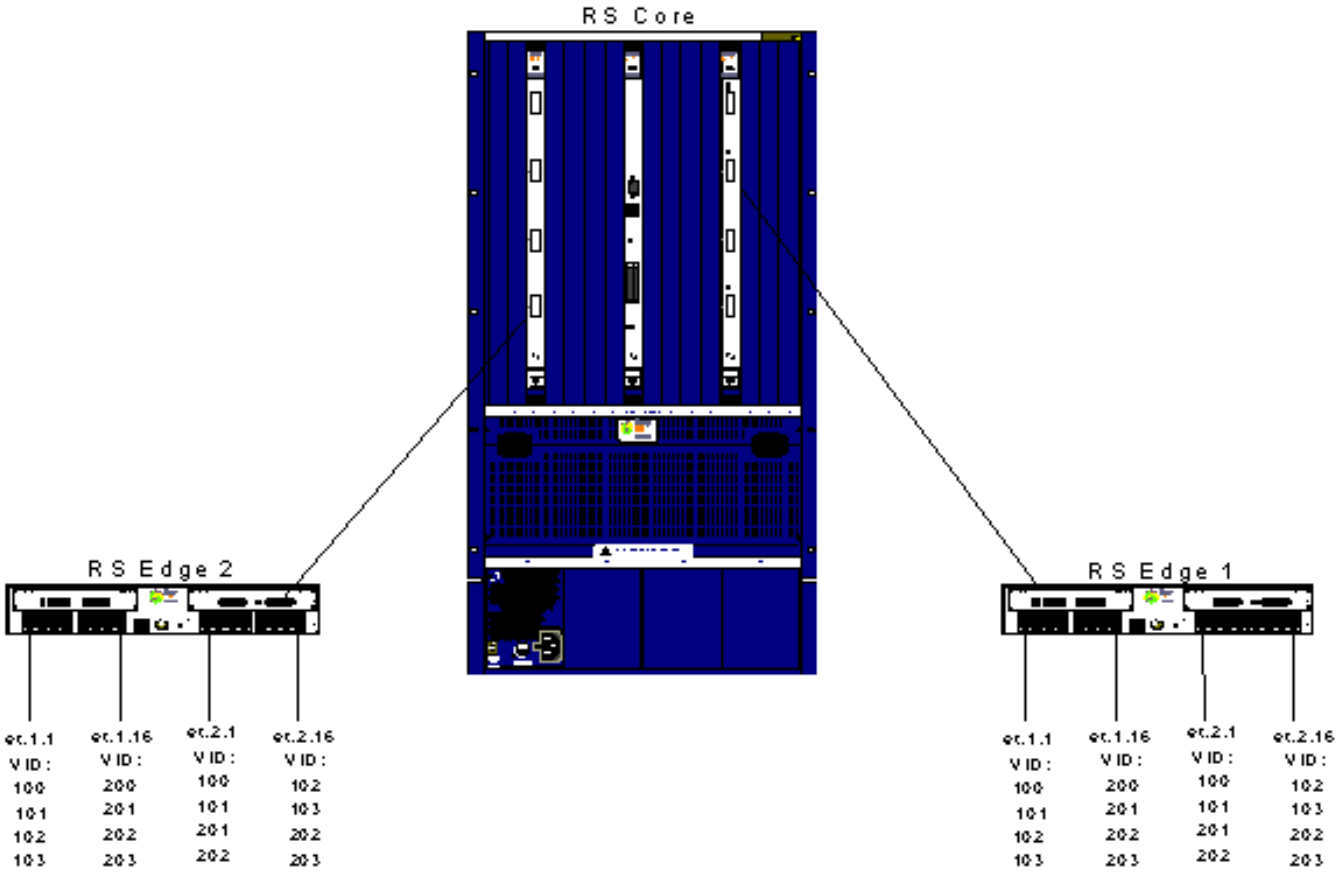
The above configuration is a good example of the versatility of the Riverstone platform in terms of connectivity options and VLAN implementation. Each VLAN contains a point-to-point IP connection between adjacent routers. This allows the network administrator to create a logical full mesh even though the physical connectivity will not allow this. Additional physical connections will allow for a greater level of redundancy.

Stackable VLANs - Tunneling Across the Metro

Payam Kahen
Systems Engineering
March 27, 2002

Stackable VLANs in a scenario where Edge switches are receiving Ethernet frames tagged with an 802.1Q header. The same VLAN ID is received on multiple ports, however. Stackable VLANs will apply a second 802.1Q tag in addition to the existing tag information to distinguish between traffic received on different ports, but with the same VLAN tag. This is effectively a mechanism to tunnel traffic across a MAN regardless of the tags being received.	
RapidOS Version Tested	9.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	Stackable VLANs supported on Ethernet Interfaces only.

Diagram



Configurations

Core Switch

```
vlan make trunk-port gi.3.4,gi.13.2
vlan create BBONE1 port-based id 2001
vlan create BBONE2 port-based id 2002
vlan create BBONE3 port-based id 2003
vlan create BBONE4 port-based id 2004
vlan add ports gi.3.4,gi.13.2 to BBONE1
vlan add ports gi.3.4,gi.13.2 to BBONE2
vlan add ports gi.3.4,gi.13.2 to BBONE3
vlan add ports gi.3.4,gi.13.2 to BBONE4
```

Two Edge Switches

```
! Make port connecting to Core a trunk-port with sVLAN enabled
vlan make trunk-port gi.4.1 stackable-vlan

! Make ports connecting to customers access-ports capable of receiving .1q frames
vlan make access-port et.(1-2).1 stackable-vlan
```

```
vlan make access-port et.(1-2).16 stackable-vlan

! Create Backbone VLANs, and ports to it
vlan create BBONE1 port-based id 2001
vlan create BBONE2 port-based id 2002
vlan create BBONE3 port-based id 2003
vlan create BBONE4 port-based id 2004
vlan add ports gi.4.1 to BBONE1
vlan add ports gi.4.1 to BBONE2
vlan add ports gi.4.1 to BBONE3
vlan add ports gi.4.1 to BBONE4

! Create the customer VLANs
vlan create-range 100-103 port-based
vlan create-range 200-203 port-based

! Add ports to VLANs
vlan add-to-vlan-range ports et.1.1 to 100-103
vlan add-to-vlan-range ports et.1.16 to 200-203
vlan add-to-vlan-range ports et.2.1 to 100-101,201,202
vlan add-to-vlan-range ports et.2.16 to 102-103,202-203

! Configure Stackable VLAN
vlan enable stackable-vlan on et.1.1 backbone-vlan BBONE1
vlan enable stackable-vlan on et.1.16 backbone-vlan BBONE2
vlan enable stackable-vlan on et.2.1 backbone-vlan BBONE3
vlan enable stackable-vlan on et.2.16 backbone-vlan BBONE4
```

Comments

This setup is ideal for test cases checking against "leaks" from one Stackable VLAN to another, as well general usability of the feature.

Traffic received on the access-ports on the edge switches is tagged with 802.1Q information. The edge switch merely adds a second 802.1Q header to the frame based on the backbone-vlan selected for the port before forwarding onto the Core switch(es). The Core switches do not have any knowledge of Stackable VLANs. They apply normal switch forwarding rules based on destination MAC address and VLAN ID in the outer (second) 802.1Q tag.

To view information regarding Stackable VLANs:

```
RS3000# vlan show stackable-vlan
Stackable VLAN Information
==========================

(1, 2001):4289
   Applied On: et.1.1
   Flooded On: et.1.2,gi.4.(1-2)

(1, 2002):4294
   Applied On: et.1.16
```

```
   Flooded On: et.1.2,gi.4.(1-2)

(1, 2003):4299
   Applied On: et.2.1
   Flooded On: et.1.2,gi.4.(1-2)

(1, 2004):4304
   Applied On: et.2.16
   Flooded On: et.1.2,gi.4.(1-2)

(100, 2001):4290
   Applied On: et.1.1
   Flooded On: gi.4.1

(100, 2003):4300
   Applied On: et.2.1
   Flooded On: gi.4.1

(101, 2001):4291
   Applied On: et.1.1
   Flooded On: gi.4.1

(101, 2003):4301
   Applied On: et.2.1
   Flooded On: gi.4.1

(102, 2001):4292
   Applied On: et.1.1
   Flooded On: gi.4.1

(102, 2004):4305
   Applied On: et.2.16
   Flooded On: gi.4.1

(103, 2001):4293
   Applied On: et.1.1
   Flooded On: gi.4.1

(103, 2004):4306
   Applied On: et.2.16
   Flooded On: gi.4.1

(200, 2002):4295
   Applied On: et.1.16
   Flooded On: gi.4.1

(201, 2002):4296
   Applied On: et.1.16
   Flooded On: gi.4.1

(201, 2003):4302
   Applied On: et.2.1
```

```
   Flooded On: gi.4.1

(202, 2002):4297
   Applied On: et.1.16
   Flooded On: gi.4.1

(202, 2003):4303
   Applied On: et.2.1
   Flooded On: gi.4.1

(202, 2004):4307
   Applied On: et.2.16
   Flooded On: gi.4.1

(203, 2002):4298
   Applied On: et.1.16
   Flooded On: gi.4.1

(203, 2004):4308
   Applied On: et.2.16
   Flooded On: gi.4.1

Stackable VLAN Trunk Ports:   gi.4.1
Stackable VLAN Access Ports:  et.1.(1,16),et.2.(1,16)
Stackable VLAN Transit Ports:
```

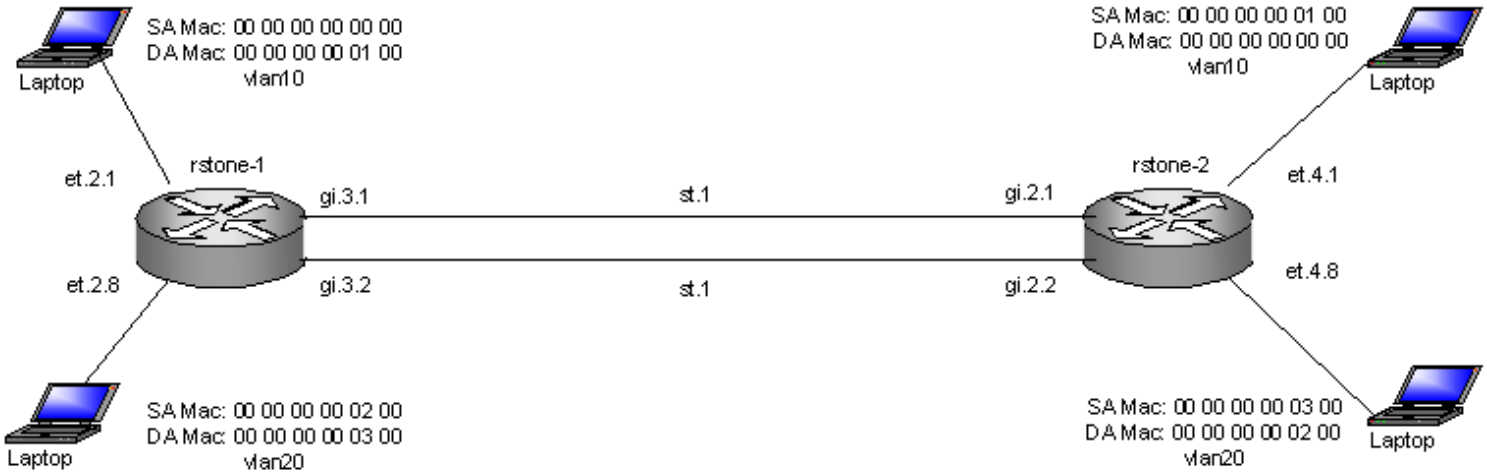
Note the mappings between the original VLAN ID tag, and the new tag the Edge switch is applying.

Smarttrunks with L4 Bridging and 802.1Q

Arshad Syed
RTAC Carrier Accounts Team
May 10, 2002

The example shown demonstrates how to configure load-balancing using Smarttrunks with L4-Bridging enabled across multiple vlans using a 802.1q trunk. A SmartTRUNK is Riverstone's technology for load balancing and load sharing across a number of ports. A SmartTRUNK is a group of two or more physical ports that have been combined into a single logical port. As flows are set up on the SmartTRUNK, traffic is balanced across all ports in the combined link, balancing overall available bandwidth. This examples uses the Round-Robin Load balancing policy. Layer-4 bridging is the RS's ability to use layer-3/4 information to perform filtering or QoS during bridging.	
RapidOS Version Tested	8.0.3.4
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

rstone-1

```
smarttrunk create st.1 protocol no-protocol
smarttrunk add ports gi.3.1 to st.1
smarttrunk add ports gi.3.2 to st.1
smarttrunk set load-policy round-robin on st.1
vlan make trunk-port st.1
vlan create vlan10 ip id 10
vlan create vlan20 ip id 20
vlan enable l4-bridging on vlan10
vlan enable l4-bridging on vlan20
vlan add ports st.1 to vlan10
vlan add ports st.1 to vlan20
vlan add ports et.2.1 to vlan10
vlan add ports et.2.8 to vlan20
system set name rstone-1
system set idle-timeout serial 0
```

rstone-2

```
smarttrunk create st.1 protocol no-protocol
smarttrunk add ports gi.2.1 to st.1
smarttrunk add ports gi.2.2 to st.1
smarttrunk set load-policy round-robin on st.1
vlan make trunk-port st.1
vlan create vlan10 ip id 10
vlan create vlan20 ip id 20
vlan enable l4-bridging on vlan10
vlan enable l4-bridging on vlan20
vlan add ports et.4.1 to vlan10
vlan add ports st.1 to vlan10
vlan add ports st.1 to vlan20
vlan add ports et.4.8 to vlan20
system set name rstone-2
system set idle-timeout serial 0
```

Comments

Some useful show commands to verify proper operation.

- The **smarttrunk show trunks** command shows information about all SmartTRUNKs, including active and inactive ports, and the control protocol used. The Primary port is the port on the SmartTRUNK that has be elected for sending broadcast and multicast packets. The command also shows the load policy being used by the SmartTRUNK, in this case Round-Robin (RR).

- The **smarttrunk show distribution** command provides statistics on how traffic is distributed across the ports in a SmartTRUNK. Link Status shows the current status of the link. Possible values are **forwarding** and **inactive**. The **inactive** state occurs if a link is either manually or operationally disabled. Verify that the link state is **Forwarding**

- The **smarttrunk show protocol-state** command shows information about the control protocol on a SmartTRUNK and the state of its ports. Verify that the protocol state is **Up** and port state is **Forwarding**

- The **vlan show** command lists all the VLANs that have been configured on the RS. It provides the type of traffic being forwarded across those vlans.

```
rstone-1# smarttrunk show trunks
Flags:  D - Disabled    I - Inactive
```

```
Policy: LU - Link Utilization   RR - Round Robin

SmartTRUNK Active Ports         Inactive Ports       Primary Port   Protocol Policy
Flags
---------- -----------          -------------       -----------    -------- ------ --
---
st.1       gi.3.(1-2)                               gi.3.1         None     RR

rstone-1# smarttrunk show distribution st.1
SmartTRUNK  Member       % Link Utilization Link Status Grp Status
----------  -----------  -----------------  ----------- ----------
st.1        gi.3.1                    0.66 Forwarding  Up
st.1        gi.3.2                    0.66 Forwarding  Up

rstone-1# smarttrunk show protocol-state st.1
SmartTRUNK  Protocol        State     Port    Port State
----------  --------        -----     ----    ----------
st.1        None            Up        gi.3.1  Forwarding
                                      gi.3.2  Forwarding

rstone-1# vlan show
VID  VLAN Name      Used for                              Ports
---  -------------  ------------------------------------ ----------------------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.2.(2-7), gi.6.(1-2), st.1
10   vlan10         IP,L4BDG                           et.2.1,st.1
20   vlan20         IP,L4BDG                             et.2.8,st.1

rstone-2# smarttrunk show trunks
Flags:  D - Disabled    I - Inactive
Policy: LU - Link Utilization   RR - Round Robin

SmartTRUNK Active Ports         Inactive Ports       Primary Port    Protocol Policy
Flags
---------- -----------          -------------       -----------     -------- ------ -
----
st.1       gi.2.(1-2)                               gi.2.1          None     RR

rstone-2# smarttrunk show distribution st.1
SmartTRUNK  Member       % Link Utilization Link Status Grp Status
----------  -----------  -----------------  ----------- ----------
st.1        gi.2.1                    0.66 Forwarding  Up
st.1        gi.2.2                    0.66 Forwarding  Up


rstone-2# smarttrunk show protocol-state st.1
SmartTRUNK  Protocol        State     Port    Port State
----------  --------        -----     ----    ----------
st.1        None             Up       gi.2.1  Forwarding
                                      gi.2.2  Forwarding

rstone-2# vlan show
VID  VLAN Name      Used for                              Ports
---  -------------  ------------------------------------ ----------------------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         se.3.(1-4), et.4.(2-
7),gi.6.(1-),st.1
10   vlan10         IP,L4BDG                             et.4.1,st.1
20   vlan20         IP,L4BDG                             et.4.8,st.1
```

Pebbles of Knowledge

- Layer-4 Bridging works for IP and IPX traffic only. The RS will drop non-IP/IPX traffic on a Layer-4 Bridging VLAN. Hence vlans need to be configured as ip-based and cannot be configured as port-based.

- If you use a SmartTRUNK with Layer-4 Bridging VLAN, the RS maintains the packet order on a per-flow basis, rather than per-MAC pair. This means that for traffic between a MAC pair consisting of more than one flow, the packets may be disordered if they go through a SmartTRUNK. For traffic that doesn.t go through a SmartTRUNK, the per-MAC pair packet order is kept.

- With ROS 7.x, the default smarttrunk load-policy is Round Robin (RR). Starting 8.x.x.x and above the default is Link Utilization. Hence with ROS 7.x code , the command ‘smarttrunk set load-policy round-robin on st.1’ in the config is not required.

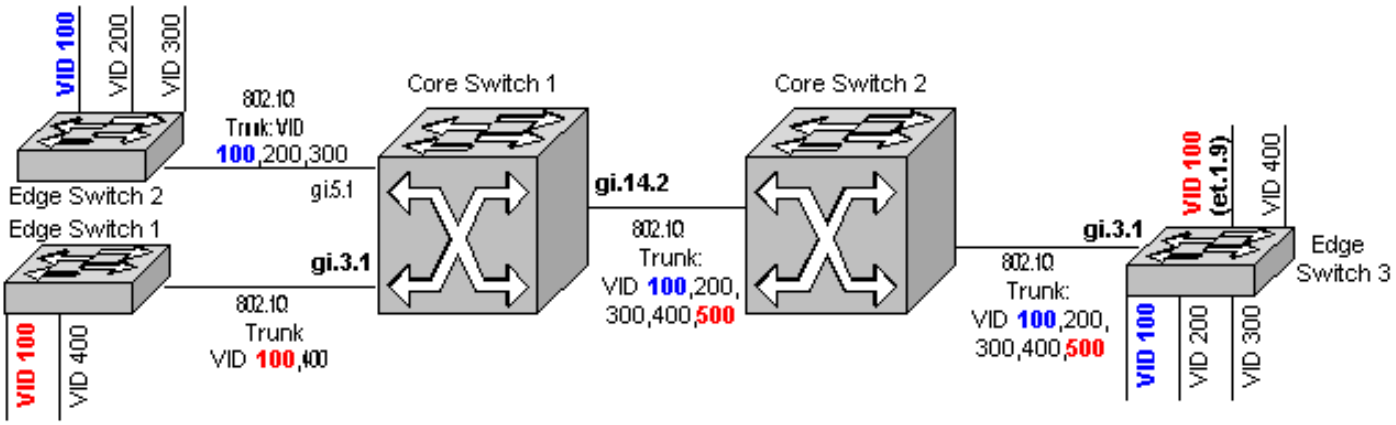
- An important tip on how to setup flows if using IXIA with L4-Bridging in such a scenario for proper operation is to configure the ixia with protocol field of something different than 255. If the protocol field is set to 255 (reserved) in L4 bridging mode, all packets will be sent to the cpu as well as flooded out all ports in the vlan. What will be observed is an uneven distribution of flows.

VLAN Translation

Payam Kahen, Doug Turner
Systems Engineering
May 15, 2002

This article demonstrates an application of VLAN translation whereby a VLAN ID is changed based on the network administrator's requirements.	
RapidOS Version Tested	8.0.3.4
RapidOS Versions Working with this Configuration	8.0.3.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.3.0
Hardware Specifics	

Diagram



Configurations

Edge Switch 1

```
vlan make trunk-port gi.3.1
vlan make trunk-port et.1-3
vlan create vlan100 port-based id 100
vlan create vlan200 port-based id 200
vlan create vlan300 port-based id 300
vlan add ports et.1.1,gi.3.1 to vlan100
vlan add ports et.1.2,gi.3.1 to vlan200
vlan add ports et.1.3,gi.3.1 to vlan300
```

Edge Switch 2

```
vlan make trunk-port gi.4.1
vlan make trunk-port et.2.(8-9)
vlan create vlan100 port-based id 100
vlan create vlan400 port-based id 400
vlan add ports et.2.8,gi.4.1 to vlan100
vlan add ports et.2.9,gi.4.1 to vlan400
```

Core Switch 1

```
! Make ports to each provider, as well as link to other Core Switch 802.1Q trunk
ports
vlan make trunk-port gi.3.1-2
vlan make trunk-port gi.14.2

! Create each VLAN, including the desired translated VID
vlan create vid100 port-based id 100
vlan create vid200 port-based id 200
vlan create vid300 port-based id 300
vlan create vid400 port-based id 400
vlan create vid500 port-based id 500

! Add ports to each appropriate VLAN. Add VID 100 everywhere it will be received, and
VID 500 only to where it will be transmitted
vlan add ports gi.(3,5).1,gi.14.2 to vid100
vlan add ports gi.5.1,gi.14.2 to vid200
vlan add ports gi.5.1,gi.14.2 to vid300
vlan add ports gi.3.1,gi.14.2 to vid400
vlan add ports gi.14.2 to vid500

! Create Layer-2 filter to perform VLAN Translation: Each instance of VID 100
incoming on port "gi.3.1" is translated to VID 500 outgoing on port "gi.14.2" and
vice-versa.
filters add vlan-switching in-port-list gi.3.1 in-vlan 100 out-port-list gi.14.2 out-
vlan 500 reverse-mapping dest-mac any name VLAN100-500 policy-id 1
```

Core Switch 2

```
vlan make trunk-port gi.(3,10).1
vlan create vid100 port-based id 100
```

```
vlan create vid200 port-based id 200
vlan create vid300 port-based id 300
vlan create vid400 port-based id 400
vlan create vid500 port-based id 500
vlan add ports gi.(3,10).1 to vid100
vlan add ports gi.(3,10).1 to vid200
vlan add ports gi.(3,10).1 to vid300
vlan add ports gi.(3,10).1 to vid400
vlan add ports gi.(3,10).1 to vid500
```

Edge Switch 3

```
! Make all links 802.1Q trunk ports
vlan make trunk-port gi.3.1
vlan make trunk-port et.1.(5-9)

! Create each VLAN, including the desired translated VID
vlan create vlan100 port-based id 100
vlan create vlan200 port-based id 200
vlan create vlan300 port-based id 300
vlan create vlan400 port-based id 400
vlan create vlan500 port-based id 500

! Add ports to each appropriate VLAN. Add VID 100 everywhere it will be received, and
VID 500 only to where it will be transmitted
vlan add ports et.1.(5,9),gi.3.1 to vlan100
vlan add ports et.1.6,gi.3.1 to vlan200
vlan add ports et.1.7,gi.3.1 to vlan300
vlan add ports et.1.8,gi.3.1 to vlan400
vlan add ports gi.3.1 to vlan500

! Create Layer-2 filter to perform VLAN Translation: Each instance of VID 100
incoming on port "et.1.9" is translated to VID 500 outgoing on port "gi.3.1" and vice-
versa.
filters add vlan-switching in-port-list et.1.9 in-vlan 100 out-port-list gi.3.1 out-
vlan 500 reverse-mapping dest-mac any name VLAN100-500 policy-id 1
```

Comments

Our challenge here is that two customers are using the same VLAN ID (VID) of 100. Thus, it becomes necessary for the provider to distinguish between VID 100 between each customer. This is achieved by applying filters that translates VID 100 to VID 500 for one of the customers (highlighted throughout with red), while leaving intact VID 100 from the other customer (highlighted with blue).

Further, these filters need to applied to one of two places: either the edge of the core, or the edge of the network where it can still be distinguished between each customer. In this document we've applied a filter at a core switch (Core Switch 1) and an edge switch (Edge Switch 3). Each switch is the last place where it is still possible to distinguish between the different customers using VID 100.

With this configuration we alleviate the problem of having two customers using the same VID, by transparently to the customers switching from one VID to another while transporting across our network.

To ensure that the right parameters have been set in the configurations, issue the following enable mode command:

```
Core-switch-1# filters show vlan-switch
```

```
Name:           VLAN100-500
----
Direction:      destination
Restriction:    allow-to-go
In VLAN:        100
Out VLAN:       500
Mac VLAN:       4096
Dest MAC:       any
In-List ports:  gi.3.1
Out-List ports: gi.14.2


Name:           VLAN100-500 - Reverse
----
Direction:      destination
Restriction:    allow-to-go
In VLAN:        500
Out VLAN:       100
Mac VLAN:       4096
Dest MAC:       any
In-List ports:  gi.14.2
Out-List ports: gi.3.1
```

As you can see, two filters have been added. The first specifies the initial translation from VID 100 to 500. The second, however, applies the first filter in reverse by translating VID 500 back to 100. This is a critical step to guarantee end-to-end communication, and is accomplished with the keyword "reverse-mapping" in the filter creation process.

Stackable VLANs Example

Rajesh Saranathan
RTAC
May 16, 2002

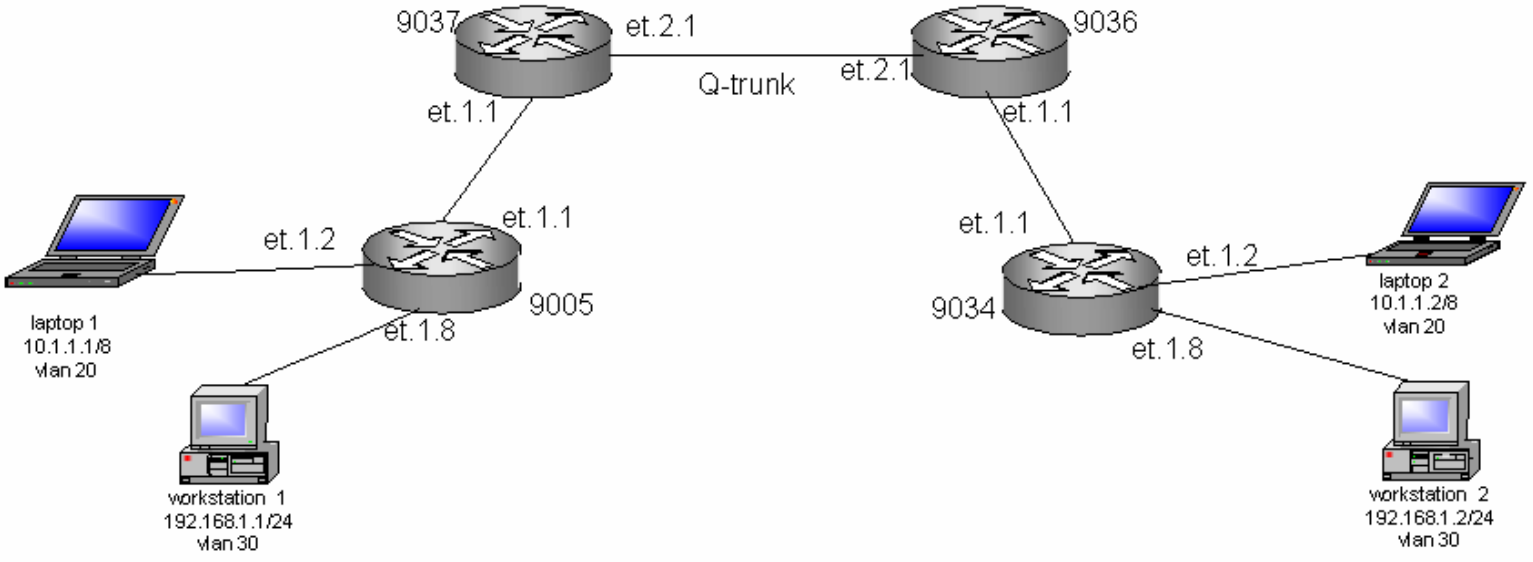
The stackable VLAN feature on the Riverstone platform allows you to tunnel multiple VLANs through a metropolitan area network (MAN) over a backbone VLAN.

This feature enables the transport of traffic for multiple VLANs, or traffic for multiple customers, can be aggregated to run through a MAN over a single backbone VLAN. This is achieved by adding a second 802.1Q tag to the Ethernet frames at the tunnel entry port. The RS supports a maximum of 4094 customers or VLANs and up to 4094 backbone VLANs.

This document shows a very basic configuration which employs two routers 9037 and 9036 in the backbone. The routers 9005 and 9034 are customer router at two different sites. The customer have two vlans 20 and 30 that are being tunneled through the backbone vlan 100.

RapidOS Version Tested	9.0.0.0
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

RS9005

```
vlan make trunk-port et.1.1
vlan create mktg port-based id 20
vlan create eng port-based id 30
vlan add ports et.1.(1-5) to mktg
vlan add ports et.1.(1,8) to eng
system set name 9005
system set idle-timeout serial 0
```

RS9034

```
vlan make trunk-port et.1.1
vlan create mktg port-based id 20
vlan create eng port-based id 30
vlan add ports et.1.(1-5) to mktg
vlan add ports et.1.(1,8) to eng
system set name 9034
system set idle-timeout serial 0
```

RS9037

```
vlan make trunk-port et.2.1 stackable-vlan
vlan make access-port et.1.1 stackable-vlan
vlan create core port-based id 100
vlan create mktg port-based id 20
vlan create eng port-based id 30
vlan add ports et.1.1 to mktg
vlan add ports et.2.1 to core
vlan add ports et.1.1 to eng
system set name 9037
system set idle-timeout serial 0
vlan enable stackable-vlan on et.1.1 backbone-vlan core
```

RS9036

```
vlan make trunk-port et.2.1 stackable-vlan
vlan make access-port et.1.1 stackable-vlan
vlan create core port-based id 100
vlan create mktg port-based id 20
vlan create eng port-based id 30
vlan add ports et.2.1 to core
vlan add ports et.1.1 to mktg
vlan add ports et.1.1 to eng
system set name 9036
system set idle-timeout serial 0 telnet 0
vlan enable stackable-vlan on et.1.1 backbone-vlan core
```

Comments

The **vlan show** command lists all the VLANs that have been configured on the RS. The **vlan show id** and the **vlan show name** commands lists information about specific VLANs configured on the RS. You can specify the VLAN by either ID number or name. The following VLAN information is shown:

- the VLAN ID
- the name of the VLAN
- the type of VLAN (determines the types of traffic the RS forwards on the VLAN)
- the ports included in the VLAN

```
9005# vlan show
```

```
VID  VLAN Name      Used for                                        Ports
---  -------------  ------------------------------------ ----------------------------
-------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,6-7), et.2.(1-8)
20   mktg           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-5)
30   eng            IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,8)

9037# vlan show

VID  VLAN Name      Used for                                         Ports
---  -------------  ------------------------------------ ----------------------------
-------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-8), et.2.(1-8)
20   mktg           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.1
30   eng            IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.1
100  core           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.2.1

9036# vlan show

VID  VLAN Name      Used for                                         Ports
---  -------------  ------------------------------------ ----------------------------
-------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-8), et.2.(1-8)
20   mktg           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.1
100  core           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.2.1

9034# vlan show

VID  VLAN Name      Used for                                         Ports
---  -------------  ------------------------------------ ----------------------------
-------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,6-7), et.2.(1-8)
20   mktg           IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-5)
30   eng            IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,8)
```

The **vlan show stackable-vlan** command lists all the stackable VLANs that have been configured on the RS. It provides the following information:

- the ID of the VLAN to be tunneled and the ID of the backbone VLAN
- tunnel entry/exit ports
- ports on which multicast, broadcast, or unknown unicast packets are flooded
- tunnel backbone ports
- stackable VLAN access ports

Looking at output of this command you can see the mappings indicating that customer vlans 20, 30,default vlan (vlan id =1) will be tunneled through the backbone vlan 100.

```
9037# vlan show stackable-vlan

Stackable VLAN Information
==========================
(1, 100):4289
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

(20, 100):4290
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

(30, 100):4291
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

Stackable VLAN Trunk Ports:   et.2.1
Stackable VLAN Access Ports:  et.1.1
Stackable VLAN Transit Ports:

9036# vlan show stackable-vlan
```

```
Stackable VLAN Information
==========================
(1, 100):4289
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

(20, 100):4290
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

(30, 100):4291
   Applied On: et.1.1
   Flooded On: et.1.1,et.2.1

Stackable VLAN Trunk Ports:   et.2.1
Stackable VLAN Access Ports:  et.1.1
Stackable VLAN Transit Ports:
```

To verify the setup you can ping from laptop 2 in vlan 20 connected to port et.1.2 on customer router 9034 to laptop 1 in vlan 20 connected to port et.1.2 to customer router 9005 in a different site. Looking at the arp table on laptop 2 , you see an entry for 10.1.1.1 which is the IP address of laptop 1 and the corresponding mac address.

```
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time<10ms TTL=128
Reply from 10.1.1.1: bytes=32 time<10ms TTL=128
Reply from 10.1.1.1: bytes=32 time<10ms TTL=128
Reply from 10.1.1.1: bytes=32 time<10ms TTL=128

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>arp -a

Interface: 10.1.1.2 on Interface 0x2
  Internet Address      Physical Address      Type
  10.1.1.1              00-b0-d0-27-d7-54     dynamic
```

Pebbles of Knowledge

If you are having connectivity issues between the hosts within the same vlan then one of reasons could be related to Layer 2. You may want to verify that the arp requests are being processed by 9005 and 9034. The l2-tables command output shown below has an entry for the mac address of `both the laptops in vlan 20.`

```
9005# l2-tables show all-macs verbose
  Id            MAC         VLAN     Source Port        Ports that have MAC as a
dest.
------  -----------------  ----  -----------------  --------------------------------
-------
000001  FF:FF:FF:FF:FF:FF   0020     mcast*              et.1.1
000002  01:80:C2:00:00:00   4095     mcast               et.1.1
000003  01:80:C2:00:00:00   0030     mcast               et.1.(1,8)
000004  01:80:C2:00:00:00   0020     mcast               et.1.(1-5)
000005  01:80:C2:00:00:00   0001     mcast               et.1.(1,6-7),et.2.(1-8)
000006  00:10:A4:8A:01:06   0020     et.1.1              et.1.2
000007  00:B0:D0:27:D7:54   0020     et.1.2              et.1.1

Statistics Summary
------------------
Total number of unique MACs found      7
MACs that reside on a port as a source 2
MACs that reside on port(s) as a dest  7
```

```
Multicasts (subset of dest MACs)       5
9034# Abort
9034#

9034# l2-tables show all-macs verbose
  Id            MAC         VLAN     Source Port       Ports that have MAC as a dest.
------  -----------------  ----  -----------------  --------------------------------
-------
000001  FF:FF:FF:FF:FF:FF   0020     mcast*             et.1.2
000002  01:80:C2:00:00:00   4095     mcast              et.1.1
000003  01:80:C2:00:00:00   0030     mcast              et.1.(1,8)
000004  01:80:C2:00:00:00   0020     mcast              et.1.(1-5)
000005  01:80:C2:00:00:00   0001     mcast              et.1.(1,6-7),et.2.(1-8)
000006  00:10:A4:8A:01:06   0020     et.1.2             et.1.1
000007  00:B0:D0:27:D7:54   0020     et.1.1             et.1.2

Statistics Summary
------------------
Total number of unique MACs found      7
MACs that reside on a port as a source 2
MACs that reside on port(s) as a dest  7
Multicasts (subset of dest MACs)       5
```

Building on this configuration, you can also create IP interfaces for the customer vlans on routers 9005 and 9034 to manage these vlans or enable forwarding between vlans.

The command below creates an IP interface for vlan mktg

```
9005(config)# interface create ip mktgip address-netmask 10.1.1.254/8 vlan mktg

9034(config)# interface create ip mktgip2 address-netmask 10.1.1.253/8 vlan mktg
```

Once you assign an IP address for the vlan mktg you can reach the hosts in vlan mktg from the routers 9005 and 9034.

```
RS9005# ip show routes

Destination        Gateway                 Owner      Netif
-----------        -------                 -----      -----
10.0.0.0/8         directly connected      -          mktgip
127.0.0.1          127.0.0.1               -          lo0
```

The arp table on 9005 shows entries for laptop 1, laptop 2, the IP interface created for vlan mktg on 9005 and 9034.

```
9005# show arp
Total ARP entries: 4
--------------------|------------------------------|--------------------------|------
-----
IP Address          |     MAC Address              |     Interface[~Port]     |
Flags
--------------------|------------------------------|--------------------------|------
-----
10.1.1.1            | 00:B0:D0:27:D7:54            | mktgip~et.1.2            |
10.1.1.2            | 00:10:A4:8A:01:06            | mktgip~et.1.1            |
10.1.1.253          | 00:02:85:04:20:00            | mktgip~et.1.1            |
10.1.1.254          | 00:02:85:06:E5:80            | lo0                      |
Static
```

Interesting point to note:

When the command ***vlan make access-port et.1.1 stackable-vlan*** is executed you will see the CLI message which indicates that the port et.1.1 changes from the normal access port to trunk.

```
%VLAN-I-ACCESSCHNG, Port et.1.1 successfully changed to 'trunk'.
```

Negating this statement will change the port back to access.

$Id: 0078.html,v 1.2 2002/05/17 17:06:46 webmaster Exp $

Native VLAN Configurations

Rico E. Vitale
Systems Engineering
July 11, 2002

Riverstone's RapidOS routes IP and IPX and allows IPX and legacy protocols to be switched within VLANs. As campus-style service providers add Metro-like infrastructures, they may be faced with problems unknown in the pure-IP Metro world. IPX, AppleTalk and other protocols still exist and cannot be removed from these networks. Additionally, these protocols may need to traverse uplinks created to be 802.1Q trunks

These protocols do not support the tagging structure of Ethernet IP, yet must share the physical port. To accomplish this, Riverstone has introduced *Native VLANs*. Native VLANs allow untagged packets from non-IPv4 traffic to be attached to one specific VLAN on the router. All traffic from that protocol arriving on the 802.1Q trunk port will be switched to that VLAN.

To accomplish this the user creates all the necessary VLANs on the router, creates an 802.1Q trunk port, then sets a specific VLAN on each router as the Native VLAN for that protocol type. When packets arrive they will be evaluated and forwarded out only those ports associated with the specific Native VLAN.

This configuration contains four zones, each represented by a single Riverstone router.

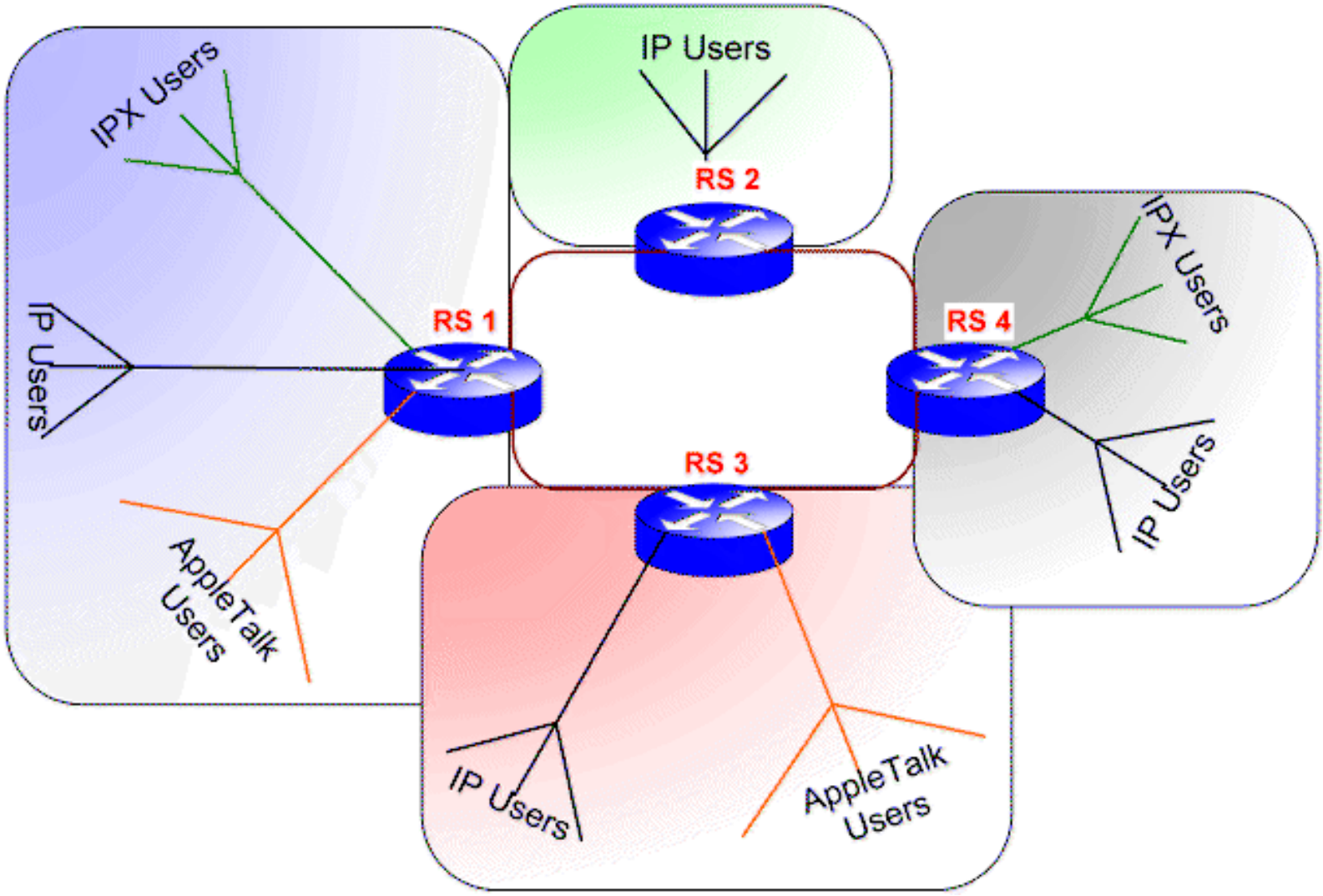
1. Router 1 – Contains IP, IPX and AppleTalk users
2. Router 2 – Contains only IP users
3. Router 3 – Contains IP and AppleTalk users
4. Router 4 – Contains IP and IPX users

- When users are connected to the router the associated VLAN is named *Native_<type>*.
- When no users are connected to the router the associated VLAN is named *Pass_thru_<type>*.

RapidOS Version Tested	9.0.0.2
RapidOS Versions Working with this Configuration	9.0.0.0 and newer

RapidOS Versions NOT Working with this Configuration	Older than 9.0.0.0
Hardware Specifics	The uplink port must be set to a 802.1Q trunk port. This feature will not be available on any hardware not supporting this functionality (e.g., RPR OC-48)

Diagram



Configurations

Router 1

```
vlan make trunk-port et.1.1 exclude-default-vlan
```

```
vlan make trunk-port et.2.1 exclude-default-vlan
vlan create Native_AppleTalk appletalk id 100
vlan create Native_IPX ipx id 200
vlan create Other_IP ip id 1000
vlan set native-vlan et.1.1 appletalk Native_AppleTalk
vlan set native-vlan et.1.1 ipx Native_IPX
vlan set native-vlan et.2.1 appletalk Native_AppleTalk
vlan set native-vlan et.2.1 ipx Native_IPX
vlan add ports et.1.1 to Native_AppleTalk
vlan add ports et.1.1 to Native_IPX
vlan add ports et.1.1 to Other_IP
vlan add ports et.2.1 to Native_AppleTalk
vlan add ports et.2.1 to Native_IPX
vlan add ports et.2.1 to Other_IP
vlan add ports et.1.2-5 to Native_AppleTalk
vlan add ports et.1.6-9 to Native_IPX
vlan add ports et.1.10-16 to Other_IP
interface create ip Other_IP address-netmask 10.1.1.1/24 vlan Other_IP
system set name Router_1
```

Router 2

```
vlan make trunk-port et.1.1 exclude-default-vlan
vlan make trunk-port et.2.1 exclude-default-vlan
vlan create Pass_thru_AppleTalk appletalk id 100
vlan create Pass_thru_IPX ipx id 200
vlan create Other_IP ip id 1000
vlan set native-vlan et.1-2.1 appletalk Pass_thru_AppleTalk
vlan set native-vlan et.1-2.1 ipx Pass_thru_IPX
vlan set native-vlan et.2.1 appletalk Pass_thru_AppleTalk
vlan set native-vlan et.2.1 ipx Pass_thru_IPX
vlan add ports et.1.1 to Pass_thru_AppleTalk
vlan add ports et.1.1 to Pass_thru_IPX
vlan add ports et.1.1 to Other_IP
vlan add ports et.2.1 to Pass_thru_AppleTalk
vlan add ports et.2.1 to Pass_thru_IPX
vlan add ports et.2.1 to Other_IP
vlan add ports et.1.10-16 to Other_IP
interface create ip Other_IP address-netmask 10.1.1.2/24 vlan Other_IP
system set name Router_2
```

Router 3

```
vlan make trunk-port et.1.1 exclude-default-vlan
vlan make trunk-port et.2.1 exclude-default-vlan
vlan create Native_AppleTalk appletalk id 100
```

```
vlan create Pass_thru_IPX ipx id 200
vlan create Other_IP ip id 1000
vlan set native-vlan et.1.1 appletalk Native_AppleTalk
vlan set native-vlan et.1.1 ipx Pass_thru_IPX
vlan set native-vlan et.2.1 appletalk Native_AppleTalk
vlan set native-vlan et.2.1 ipx Pass_thru_IPX
vlan add ports et.1.1 to Native_AppleTalk
vlan add ports et.1.1 to Pass_thru_IPX
vlan add ports et.1.1 to Other_IP
vlan add ports et.2.1 to Native_AppleTalk
vlan add ports et.2.1 to Pass_thru_IPX
vlan add ports et.2.1 to Other_IP
vlan add ports et.1.2-5 to Native_AppleTalk
vlan add ports et.1.10-16 to Other_IP
interface create ip Other_IP address-netmask 10.1.1.3/24 vlan Other_IP
system set name Router_3
```

Router 4

```
vlan make trunk-port et.1.1 exclude-default-vlan
vlan make trunk-port et.2.1 exclude-default-vlan
vlan create Pass_thru_AppleTalk appletalk id 100
vlan create Native_IPX ipx id 200
vlan create Other_IP ip id 1000
vlan set native-vlan et.1.1 appletalk Pass_thru_AppleTalk
vlan set native-vlan et.1.1 ipx Native_IPX
vlan set native-vlan et.2.1 appletalk Pass_thru_AppleTalk
vlan set native-vlan et.2.1 ipx Native_IPX
vlan add ports et.1.1 to Pass_thru_AppleTalk
vlan add ports et.1.1 to Native_IPX
vlan add ports et.1.1 to Other_IP
vlan add ports et.2.1 to Pass_thru_AppleTalk
vlan add ports et.2.1 to Native_IPX
vlan add ports et.2.1 to Other_IP
vlan add ports et.1.6-9 to Native_IPX
vlan add ports et.1.10-16 to Other_IP
interface create ip Other_IP address-netmask 10.1.1.4/24 vlan Other_IP
system set name Router_4
```

Comments

The command "port show vlan-info et.1.1" shows the VLAN status on one of the 802.1Q trunk ports.

```
Router_1# port show vlan-info et.1.1
```

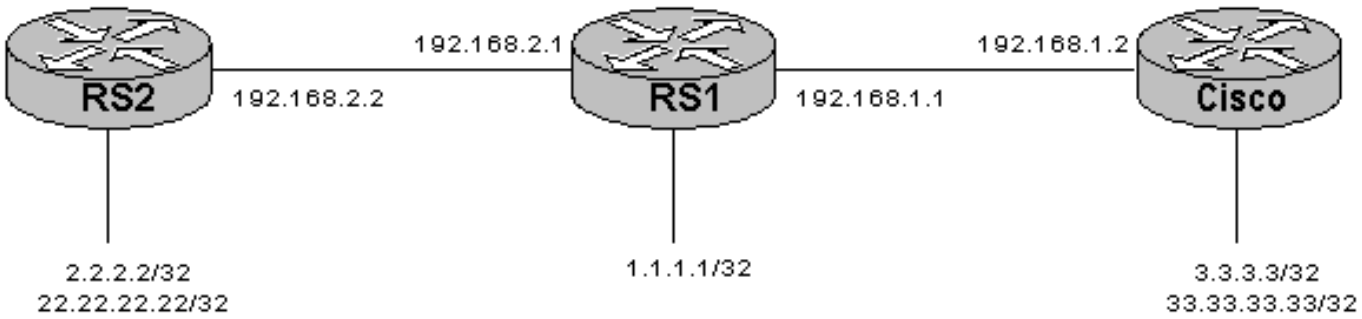
```
[Native vlans are printed in boldface] Port Type IP IPX Bridging ATALK DEC SNA IPv6 ------- ------- -------
--------- --------- --------- --------- --------- --------- et.1.1 trunk Other_IP Native_I Native_A
```

MPLS LSPs with Cisco LER using RSVP

Ray Qiu
Corporate Systems Engineering
April 20, 2001

This configuration demonstrates how to setup MPLS LSPs using **RSVP strict explicit path** with Cisco. Cisco is the LER here. It is running Cisco IOS version 12.1(5)T5. OSPF is used as the IGP protocol. Also it shows how to define and attach policies for LSPs.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS-enabled hardware

Diagram



Configurations

RS1

```
interface create ip to_cisco address-netmask 192.168.1.1/24 port gi.1.1
interface create ip to_RS2 address-netmask 192.168.2.1/24 port gi.1.2
interface add ip lo0 address-netmask 1.1.1.1/32
!
ip-router global set router-id 1.1.1.1
!
ospf create area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf add interface to_cisco to-area backbone
ospf add interface to_RS2 to-area backbone
ospf start
!
mpls add interface to_cisco
mpls add interface to_RS2
mpls start
!
rsvp add interface to_cisco
rsvp add interface to_RS2
rsvp start
!
system set name RS1
system set idle-timeout serial 0
!
ospf set traffic-engineering on
ospf set opaque-capability on
```

RS2

```
interface create ip to_RS1 address-netmask 192.168.2.2/24 port gi.1.1
interface add ip lo0 address-netmask 2.2.2.2/32
interface add ip lo0 address-netmask 22.22.22.22
!
ip-router global set router-id 2.2.2.2
!
ospf create area backbone
ospf add interface to_RS1 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
!
mpls add interface to_RS1
mpls create path to_cisco num-hops 3
mpls set path to_cisco hop 1 ip-addr 192.168.2.2
mpls set path to_cisco hop 2 ip-addr 192.168.2.1
mpls set path to_cisco hop 3 ip-addr 192.168.1.2
mpls create label-switched-path L1 to 3.3.3.3
mpls create policy p1 dst-ipaddr-mask 33.33.33.33/32
mpls set label-switched-path L1 primary to_cisco no-cspf
```

```
mpls set label-switched-path L1 policy p1
mpls start
!
rsvp add interface to_RS1
rsvp start
!
system set name RS2
system set idle-timeout serial 0
!
ospf set traffic-engineering on
ospf set opaque-capability on
```

Cisco

```
mpls traffic-eng tunnels
mpls traffic-eng link-management timers bandwidth-hold 300
mpls traffic-eng signalling advertise implicit-null
mpls traffic-eng reoptimize timers frequency 0
no tag-switching advertise-tags
no tag-switching ip
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface Loopback1
 ip address 33.33.33.33 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback0
 tunnel destination 2.2.2.2
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 1 explicit identifier 1
 tunnel mpls traffic-eng record-route
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 75000 75000
!
router ospf 1
 network 3.3.3.3 0.0.0.0 area 0
 network 192.168.1.0 0.0.0.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip classless
ip route 22.22.22.22 255.255.255.255 Tunnel0
!
ip explicit-path identifier 1 enable
```

```
 next-address 192.168.1.1
 next-address 192.168.2.2
 next-address 2.2.2.2
```

Comments

The second loopback addresses are not advertised by OSPF but are specified by the MPLS LSP policies, so we should be able to ping from one end to the other. We should see all the LSPs are up in RS2 and Cisco.

RS2

```
RS2# mpls show label-switched-paths L1

Label-Switched-Path: L1

state: Up               lsp-id: 0x4
proto: <rsvp>           protection: primary
attributes: <POLICY PRI>

to: 3.3.3.3             from: 2.2.2.2
setup-pri: 7            hold-pri: 0
retry-limit: 1000       retry-int: 30
retry-count: 1000       next_retry_int: 30

===>Protection-Path "to_cisco": Active, Primary
    State: Up   lsp-id: 0x4001      attributes: <>

--->Path-Signalling-Parameters:
    attributes: <STANDBY NO-CSPF>
    preference: 7       hop-limit: 255  opt-int: 0
    bps: 0
    lsp-handle: 0x81f4ae50
    user-path: to_cisco
               num-hops: 3     used-count: 1
               hop: 192.168.2.2 - strict
               hop: 192.168.2.1 - strict
               hop: 192.168.1.2 - strict

RS2# mpls show policy p1
Name : p1
Type                : L3
Source address       : anywhere
Source Port         : any
Destination address : 33.33.33.33/32
Destination Port    : any
TOS                 : any
TOS Mask            :
Protocol            : IP
```

```
RS2# ping 33.33.33.33
PING 33.33.33.33 (33.33.33.33): 36 data bytes
44 bytes from 33.33.33.33: icmp_seq=0 ttl=254 time=2.190 ms

--- 33.33.33.33 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.190/2.190/2.190 ms
```

Cisco

```
cisco#show mpls traffic-eng tunnels

Name: cisco_t0                            (Tunnel0) Destination: 2.2.2.2
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected

    path option 1, type explicit 1 (Basis for Setup, path weight 21)

  Config Parameters:
    Bandwidth:  0        kbps  Priority: 7  7   Affinity: 0x0/0x0
    AutoRoute:  disabled  LockDown: disabled  Loadshare: 0        bw-based

  InLabel  :  -
  OutLabel : GigabitEthernet0/0, 18
  RSVP Signalling Info:
       Src 3.3.3.3, Dst 2.2.2.2, Tun_Id 0, Tun_Instance 1
    RSVP Path Info:
      My Address: 192.168.1.2
      Explicit Route: 192.168.1.1 192.168.2.1 192.168.2.2 2.2.2.2
      Record   Route:
      Tspec: ave rate=0 kbits, burst=8000 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route: 192.168.2.2 192.168.1.1
      Fspec: ave rate=0 kbits, burst=0 bytes, peak rate=0 kbits
  History:
    Current LSP:
      Uptime: 3 minutes, 53 seconds

LSP Tunnel L1_to_cisco is signalled, connection is up
  InLabel  : GigabitEthernet0/0, implicit-null
  OutLabel :  -
  RSVP Signalling Info:
       Src 2.2.2.2, Dst 3.3.3.3, Tun_Id 16385, Tun_Instance 1
    RSVP Path Info:
      My Address: 192.168.1.2
      Explicit Route:  NONE
      Record   Route: 192.168.2.2 192.168.1.1
      Tspec: ave rate=0 kbits, burst=0 bytes, peak rate=0 kbits
    RSVP Resv Info:
      Record   Route:  NONE
```

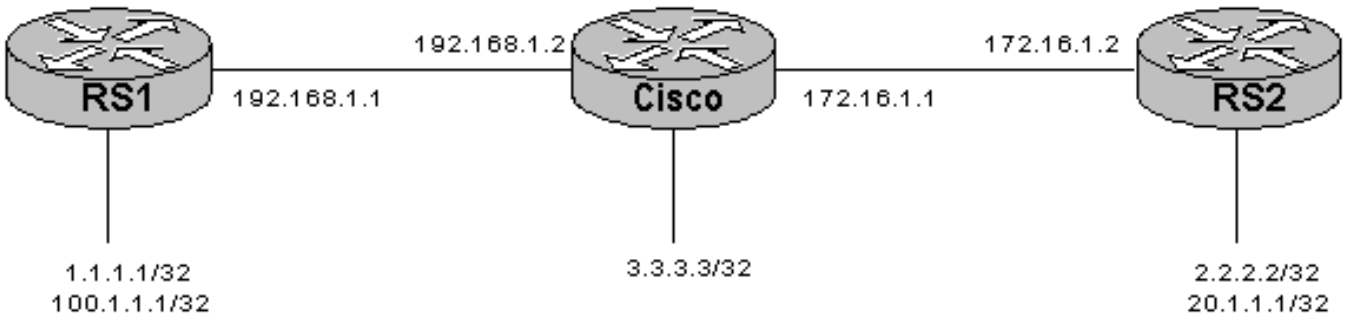
```
      Fspec: ave rate=0 kbits, burst=0 bytes, peak rate=0 kbits

cisco#ping
Protocol [ip]:
Target IP address: 22.22.22.22
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 33.33.33.33
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

MPLS LSPs with Cisco LSR using RSVP

Ray Qiu
Corporate Systems Engineering
April 12, 2001

This configuration demonstrates how to setup MPLS LSPs using **RSVP strict explicit path** with Cisco. Cisco is the LSR here. It is running Cisco IOS version 12.1(5)T5. OSPF is used as the IGP protocol. Also it shows how to define and attach policies for LSPs.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS-enabled hardware

Diagram



Configurations

RS1

```
interface create ip 192net address-netmask 192.168.1.1/24 port gi.1.1
interface add ip lo0 address-netmask 1.1.1.1/32
interface add ip lo0 address-netmask 100.1.1.1/32
ip-router global set router-id 1.1.1.1
ospf create area backbone
ospf add stub-host 1.1.1.1 cost 10 to-area backbone
ospf add interface 192net to-area backbone
ospf start
mpls add interface 192net
mpls create path to_RS2 num-hops 3
mpls set path to_RS2 hop 1 ip-addr 192.168.1.1
mpls set path to_RS2 hop 2 ip-addr 192.168.1.2
mpls set path to_RS2 hop 3 ip-addr 172.16.1.2
mpls create policy p1 dst-ipaddr-mask 20.1.1.1/32
mpls create label-switched-path L1 to 2.2.2.2
mpls set label-switched-path L1 primary to_RS2 no-cspf
mpls set label-switched-path L1 policy p1
mpls start
rsvp add interface 192net
rsvp start
system set name RS1
```

RS2

```
interface create ip 172net address-netmask 172.16.1.2/24 port gi.1.1
interface add ip lo0 address-netmask 2.2.2.2/32
interface add ip lo0 address-netmask 20.1.1.1/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add stub-host 2.2.2.2 cost 10 to-area backbone
ospf add interface 172net to-area backbone
ospf start
mpls add interface 172net
mpls create path to_RS1 num-hops 3
mpls set path to_RS1 hop 1 ip-addr 172.16.1.2
mpls set path to_RS1 hop 2 ip-addr 172.16.1.1
mpls set path to_RS1 hop 3 ip-addr 192.168.1.1
mpls create label-switched-path L1 to 1.1.1.1
mpls create policy p1 dst-ipaddr-mask 100.1.1.1/32
mpls set label-switched-path L1 primary to_RS1 no-cspf
mpls set label-switched-path L1 policy p1
mpls start
rsvp add interface 172net
rsvp start
system set name RS2
```

Cisco

```
mpls traffic-eng tunnels
mpls traffic-eng link-management timers bandwidth-hold 300
mpls traffic-eng signalling advertise implicit-null
mpls traffic-eng reoptimize timers frequency 0
no tag-switching advertise-tags
no tag-switching ip
call rsvp-sync
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.255
!
interface GigabitEthernet0/0
 ip address 172.16.1.1 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 75000 75000
!
interface GigabitEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 mpls traffic-eng tunnels
 ip rsvp bandwidth 75000 75000
!
router ospf 1
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0.0.0.0
 network 172.16.1.0 0.0.0.255 area 0.0.0.0
 network 192.168.1.0 0.0.0.255 area 0.0.0.0
```

Comments

The second loopback addresses are not advertised by OSPF, but are specified by the MPLS LSP policies. So we should be able to ping from one end to the other. And in the Cisco LSR, we should be able to see the MPLS forwarding table.

RS1

```
RS1# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              1.1.1.1              -         lo0
2.2.2.2              192.168.1.2          OSPF      192net
3.3.3.3              192.168.1.2          OSPF      192net
100.1.1.1            100.1.1.1            -         lo0
127.0.0.1            127.0.0.1            -         lo0
172.16.1.0/24        192.168.1.2          OSPF      192net
192.168.1.0/24       directly connected   -         192net

RS1# mpls show label-switched-paths L1
```

```
        Label-Switched-Path: L1

        state: Up               lsp-id: 0x4
        proto: <rsvp>           protection: primary
        attributes: <POLICY PRI>

        to: 2.2.2.2             from: 1.1.1.1
        setup-pri: 7            hold-pri: 0
        retry-limit: 1000       retry-int: 30
        retry-count: 1000       next_retry_int: 210

        ===>Protection-Path "to_RS2": Active, Primary
            State: Up   lsp-id: 0x1000001          attributes: <>

        --->Path-Signalling-Parameters:
            attributes: <STANDBY NO-CSPF>
            preference: 7       hop-limit: 255  opt-int: 0
            lsp-handle: 0x826b2bc0
            user path: to_RS2
                num-hops: 3     used-count: 1
                hop: 192.168.1.1 - strict
                hop: 192.168.1.2 - strict
                hop: 172.16.1.2 - strict

RS1# mpls show policy all verbose
p1
L3 policy
Source address         : anywhere
Source Port            : any
Destination address : 20.1.1.1/32
Destination Port : any
Protocol         : IP

RS1# ping 20.1.1.1
PING 20.1.1.1 (20.1.1.1): 36 data bytes
44 bytes from 20.1.1.1: icmp_seq=0 ttl=254 time=2.608 ms

--- 20.1.1.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.608/2.608/2.608 ms
```

Cisco

```
cisco#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     16          2.2.2.2 1 [5]    656        Gi0/0      192.168.1.1
17     16          1.1.1.1 1 [4]    902        Gi0/1      172.16.1.2
```

RS2

```
RS2# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              172.16.1.1           OSPF      172net
2.2.2.2              2.2.2.2              -         lo0
3.3.3.3              172.16.1.1           OSPF      172net
20.1.1.1             20.1.1.1             -         lo0
127.0.0.1            127.0.0.1            -         lo0
172.16.1.0/24        directly connected   -         172net
192.168.1.0/24       172.16.1.1           OSPF      172net

RS2# mpls show label-switched-paths L1

        Label-Switched-Path: L1

        state: Up               lsp-id: 0x4
        proto: <rsvp>           protection: primary
        attributes: <POLICY PRI>

        to: 1.1.1.1             from: 2.2.2.2
        setup-pri: 7            hold-pri: 0
        retry-limit: 1000       retry-int: 30
        retry-count: 1000       next_retry_int: 210

        ===>Protection-Path "to_RS1": Active, Primary
            State: Up   lsp-id: 0x1000001           attributes: <>

        --->Path-Signalling-Parameters:
            attributes: <STANDBY NO-CSPF>
            preference: 7       hop-limit: 255  opt-int: 0
            lsp-handle: 0x81f0f288
            user path: to_RS1
                num-hops: 3     used-count: 1
                hop: 172.16.1.2 - strict
                hop: 172.16.1.1 - strict
                hop: 192.168.1.1 - strict

RS2# mpls show policy p1
p1
L3 policy
Source address         : anywhere
Source Port            : any
Destination address : 100.1.1.1/32
Destination Port : any
Protocol         : IP

RS2# ping 100.1.1.1
PING 100.1.1.1 (100.1.1.1): 36 data bytes
44 bytes from 100.1.1.1: icmp_seq=0 ttl=254 time=11.588 ms
```

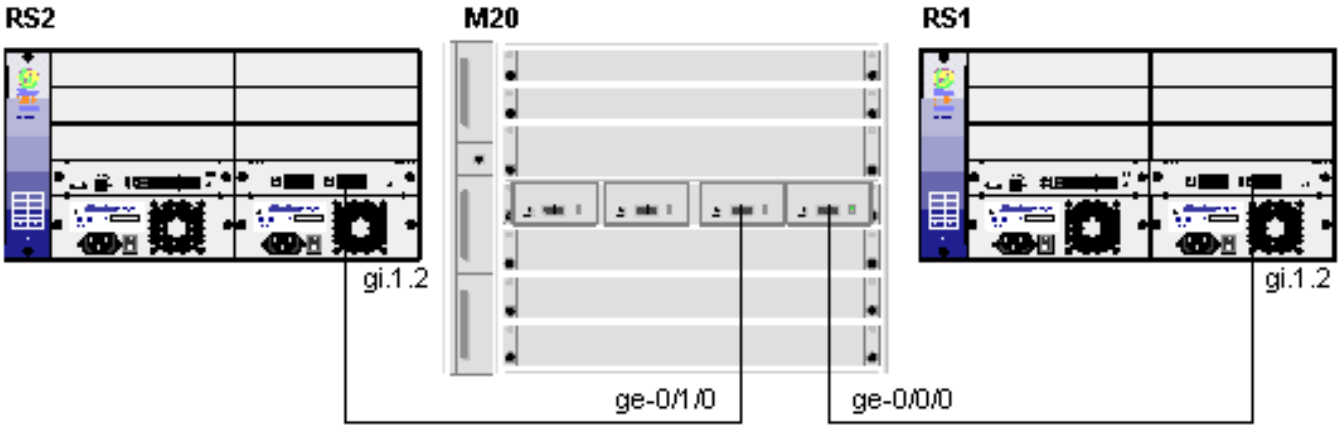
```
--- 100.1.1.1 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 11.588/11.588/11.588 ms
```

LDP over LDP Martini Interoperability with Juniper

Rich Martin
Systems Engineering
September 17, 2001

This configuration example is from a successful test of Martini tunnels using LDP over LDP through a Juniper M20. This example maps a physical port to a Martini tunnel. Configurations will be different if you intend to map a VLAN to a Martini tunnel.	
RapidOS Version Tested	8.0.0.0 / JUNOS 4.4R2.3
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS

Diagram



Configurations

RS1

```
port set gi.1.2 auto-negotiation off mtu 2000
vlan make trunk-port gi.1.2 untagged
vlan create to-juniper port-based id 110
vlan add ports gi.1.2 to to-juniper
interface create ip to-juniper address-netmask 10.1.3.1/24 vlan to-juniper
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ip-router global set trace-state on
ospf create area backbone
ospf add interface to-juniper to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
mpls add interface to-juniper
mpls start
ldp add interface to-juniper
ldp add interface lo0
ldp map ports gi.1.1 customer-id 1
ldp add remote-peer 2.2.2.2
ldp add l2-fec customer-id 1 to-peer 2.2.2.2
ldp start
system set name RS1
ospf set traffic-engineering on
```

Juniper M20

```
version 4.4R2.3;
system {
    host-name M20;
    login {
```

```
        user lab {
            uid 2000;
            class super-user;
        }
    }
    services {
        telnet;
    }
}
interfaces {
    ge-0/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.1.3.2/24;
            }
            family mpls {
                mtu 1800;
            }
        }
    }
    ge-0/1/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.2.3.2/24;
            }
            family mpls {
                mtu 1800;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.3/32;
            }
        }
    }
}
routing-options {
    router-id 3.3.3.3;
}
protocols {
    mpls {
        traceoptions {
```

```
            file cwp-mpls.log;
            flag all;
        }
        interface all;
    }
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface ge-0/0/0.0;
            interface ge-0/1/0.0;
        }
    }
    ldp {
        traceoptions {
            file ldp-log1 size 1m files 10;
            flag label detail;
            flag packets;
        }
        interface all;
    }
}
```

RS2

```
port set gi.1.2 auto-negotiation off mtu 2000
vlan make trunk-port gi.1.2 untagged
vlan create to-juniper port-based id 120
vlan add ports gi.1.2 to to-juniper
interface create ip to-juniper address-netmask 10.2.3.1/24 vlan to-juniper
interface add ip en0 address-netmask 169.254.208.1/16
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ip-router global set trace-state on
ospf create area backbone
ospf add interface to-juniper to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
mpls add interface to-juniper
mpls start
ldp add interface to-juniper
ldp add interface lo0
ldp map ports gi.1.1 customer-id 1
ldp add remote-peer 1.1.1.1
ldp add l2-fec customer-id 1 to-peer 1.1.1.1
```

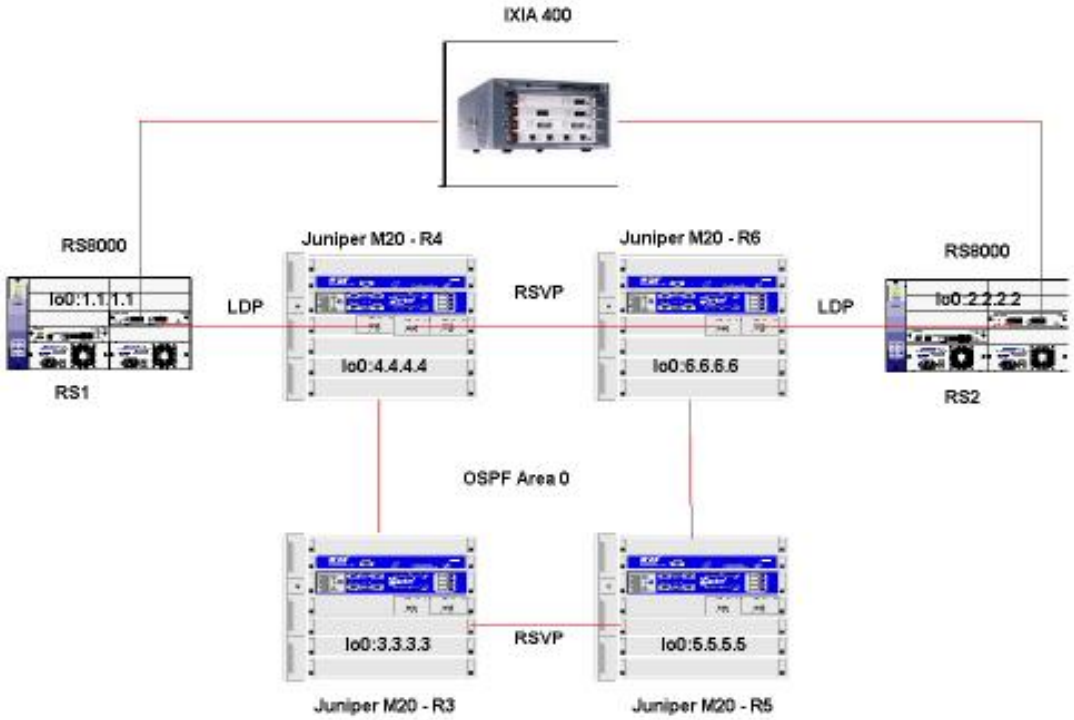
```
ldp start
system set name RS2
ospf set traffic-engineering on
```

LDP tunneling over RSVP with Riverstone LERs and Juniper LSRs

Harold Rojas
Systems Engineering
September 21, 2001

This configuration describes the MPLS inter-operability with Juniper Networks M20. LDP was used to establish the MPLS tunnel information and a customer profile was created for customer-1. This profile was mapped to a physical port. The profile allowed any kind of traffic arriving on gig.1.1 of RS1 to be sent across the LDP tunnel to the port gig.1.1 of RS2 and vice-versa. Rsvp was used in the Juniper M20 with fail-over.	
RapidOS Version Tested	8.0.0.0 / JUNOS 4.4R2.3
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS

Diagram



Configurations

RS1

```
port set gi.1.2 auto-negotiation off mtu 2000
!
vlan make trunk-port gi.1.2 untagged
vlan create to-juniper port-based id 110
vlan add ports gi.1.2 to to-juniper
!
interface create ip to-juniper address-netmask 10.1.3.1/24 vlan to-juniper
interface add ip lo0 address-netmask 1.1.1.1/32
!
ip-router global set router-id 1.1.1.1
ip-router global set trace-state on
!
ospf create area backbone
ospf add interface to-juniper to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
!
mpls add interface to-juniper
mpls start
!
ldp add interface to-juniper
ldp add interface lo0
ldp map ports gi.1.1 customer-id 1
ldp add remote-peer 2.2.2.2
ldp add l2-fec customer-id 1 to-peer 2.2.2.2
ldp start
!
```

```
system set name RS1
!
ospf set traffic-engineering on
```

RS2

```
port set gi.1.2 auto-negotiation off mtu 2000
!
vlan make trunk-port gi.1.2 untagged
vlan create to-juniper port-based id 120
vlan add ports gi.1.2 to to-juniper
!
interface create ip to-juniper address-netmask 10.2.3.1/24 vlan to-juniper
interface add ip en0 address-netmask 169.254.208.1/16
interface add ip lo0 address-netmask 2.2.2.2/32
!
ip-router global set router-id 2.2.2.2
ip-router global set trace-state on
!
ospf create area backbone
ospf add interface to-juniper to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
!
mpls add interface to-juniper
mpls start
!
ldp add interface to-juniper
ldp add interface lo0
ldp map ports gi.1.1 customer-id 1
ldp add remote-peer 1.1.1.1
ldp add l2-fec customer-id 1 to-peer 1.1.1.1
ldp start
!
ospf set traffic-engineering on
```

Juniper M20 - R3.3.3.3

```
version 4.4R2.3;
interfaces {
    ge-0/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.3.4.1/24;
            }
            family mpls {
                mtu 1800;
    ge-1/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
```

```
                address 10.3.5.1/24;
            }
            family mpls {
                mtu 1800;
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.255.15/24;
    lo0 {
        unit 0 {
            family inet {
                address 3.3.3.3/32;
routing-options {
    router-id 3.3.3.3;
}
protocols {
    rsvp {
        interface all;
    }
    mpls {
        interface all;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface all;
}
```

Juniper M20 - R4.4.4.4

```
version 4.4R2.3;
interfaces {
    ge-0/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.1.4.2/24;
            }
            family mpls {
                mtu 1800;
    ge-0/1/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.4.6.1/24;
            }
            family mpls {
                mtu 1800;
    ge-0/2/0 {
        mtu 2000;
        unit 0 {
            family inet {
```

```
            address 10.3.4.2/24;
        }
        family mpls {
            mtu 1800;
    ge-0/3/0 {
        vlan-tagging;
        unit 1500 {
            vlan-id 1500;
            family inet {
                address 100.100.100.1/24;
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.255.16/24;
    lo0 {
        unit 0 {
            family inet {
                address 4.4.4.4/32;
routing-options {
    router-id 4.4.4.4;
}
protocols {
    rsvp {
        interface ge-0/1/0.0;
        interface ge-0/2/0.0;
        interface lo0.0;
    }
    mpls {
        label-switched-path 4-to-6 {
            from 4.4.4.4;
            to 6.6.6.6;
            ldp-tunneling;
            primary strict-6;
            secondary strict-5 {
                standby;
            }
        }
        path strict-5 {
            3.3.3.3 strict;
        }
        path strict-6 {
            6.6.6.6 strict;
        }
        interface all;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0;
            interface ge-0/0/0.0;
            interface ge-0/1/0.0;
            interface ge-0/2/0.0;
        }
```

```
    }
    ldp {
        interface ge-0/0/0.0;
        interface lo0.0;
}
```

Juniper M20 - R5.5.5.5

```
version 4.4R2.3;
interfaces {
    ge-0/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.3.5.2/24;
            }
            family mpls {
                mtu 1800;
    ge-1/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.5.6.1/24;
            }
            family mpls {
                mtu 1800;
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.255.17/24;
    lo0 {
        unit 0 {
            family inet {
                address 5.5.5.5/32;

routing-options {
    router-id 5.5.5.5;
}
protocols {
    rsvp {
        interface all;
    }
    mpls {
        interface all;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface all;
}
```

Juniper M20 - R6.6.6.6

```
version 4.4R2.3;
interfaces {
    ge-0/0/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.2.6.2/24;
            }
            family mpls {
                mtu 1800;
    ge-0/1/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.4.6.2/24;
            }
            family mpls {
                mtu 1800;
    ge-0/2/0 {
        mtu 2000;
        unit 0 {
            family inet {
                address 10.5.6.2/24;
            }
            family mpls {
                mtu 1800;
    ge-0/3/0 {
        vlan-tagging;
        unit 1500 {
            vlan-id 1500;
            family inet {
                address 100.100.100.2/24;
    fxp0 {
        unit 0 {
            family inet {
                address 192.168.255.18/24;
    lo0 {
        unit 0 {
            family inet {
                address 6.6.6.6/32;
routing-options {
    router-id 6.6.6.6;
protocols {
    rsvp {
        interface lo0.0;
        interface ge-0/1/0.0;
        interface ge-0/2/0.0;
    }
    mpls {
        label-switched-path 6-to-4 {
            from 6.6.6.6;
            to 4.4.4.4;
```

```
            ldp-tunneling;
            primary strict-4;
            secondary strict-3 {
                standby;
            }
        }
        path strict-4 {
            4.4.4.4 strict;
        }
        path strict-3 {
            5.5.5.5 loose;
        }
        interface all;
    }
    ospf {
        traffic-engineering;
        area 0.0.0.0 {
            interface lo0.0;
            interface ge-0/0/0.0;
            interface ge-0/1/0.0;
            interface ge-0/2/0.0;
        }
    }
    ldp {
        interface ge-0/0/0.0;
        interface lo0.0;
}
```

Comments

The main purpose of this lab was to test the interoperability of Riverstone's LDP into Juniper's RSVP tunneling.

```
RS1.1.1.1# ldp show all
Global parameters
------ ----------
Ordered control mode
Path vector loop detection disabled
Hop count loop detection disabled

Interface parameters
--------- ----------
Interface            Label space              Nbr count  Next hello(seconds)
lo                   1.1.1.1:0                    1          0
to-juniper           10.1.4.1:0                   1          0
Neighbor parameters
-------- ----------
Address             Interface           Label space ID      Hold Time(seconds)
2.2.2.2             lo                  2.2.2.2:0             8
10.1.4.2            to-juniper          4.4.4.4:0             12
Session parameters
------- ----------
```

```
Codes: Tx - Sent, Rx tot - Received Total, Rx fltd - Received Filtered
Address          State         Connection       Hold Time(sec) Tx/Rx tot/Rx fltd
2.2.2.2          Operational   Open             8              5/5/0
4.4.4.4          Operational   Open             12             4/4/0
Label Database
----- --------
Input label database, 1.1.1.1:0-2.2.2.2:0
  Label     Prefix
   2048     6.6.6.6/32
   2049     4.4.4.4/32
   2050     1.1.1.1/32
      3     2.2.2.2/32
   2051     Customer ID 1
Output label database, 1.1.1.1:0-2.2.2.2:0
  Label     Prefix
   2049     4.4.4.4/32
   2050     6.6.6.6/32
      3     1.1.1.1/32
   2052     2.2.2.2/32
   2053     Customer ID 1
Input label database, 1.1.1.1:0-4.4.4.4:0
  Label     Prefix
      3     4.4.4.4/32
 100012     6.6.6.6/32
 100017     1.1.1.1/32
 100018     2.2.2.2/32
Output label database, 1.1.1.1:0-4.4.4.4:0
  Label     Prefix
   2049     4.4.4.4/32
   2050     6.6.6.6/32
      3     1.1.1.1/32
   2052     2.2.2.2/32
LDP Statistics
--- ----------
Message type                Total                      Last 5 seconds
============                =====                      ==============
                       Sent    Received                Sent    Received
                       ----    --------                ----    --------
Hello                  847     1712                    2       3
Initialization         3       3                       0       0
Keepalive              303     301                     2       2
Notifcation            2       0                       0       0
Address                3       3                       0       0
Address withdraw       0       0                       0       0
Label mapping          15      30                      0       0
Label request          0       0                       0       0
Label withdraw         2       2                       0       0
Label release          1       2                       0       0
Label abort            0       0                       0       0
All UDP                847     748                     2       1
All TCP                329     316                     2       2
```

```
Event type                    Total                 Last 5 seconds
==========                    =====                 ==============
Sessions opened               21                    0
Sessions closed               19                    0
Shutdown received             0                     0
Shutdown sent                 1                     0

Keep alive expired            0                     0
Malformed TLV                 0                     0
Bad TLV length                0                     0
Bad message length            0                     0
Bad PDU length                0                     0
Bad LDP identifiers           0                     0
Hello errors                  0                     0
Advertisement errors          0                     0
Max PDU errors                0                     0
Label range errors            0                     0

RS1.1.1.1# mpls show all
MPLS Controller : <mpls_1>
--------------------------
lsr-id      : 1.1.1.1
trace level : 1
flags       : <merge auto-lsp>
protocols   : <MPLS LDP>
Label Switched Paths:
--------------------------
Explicit Paths:
--------------------------
MPLS Interfaces:
--------------------------
Interface        State       Administrative groups
lo               Up          <none>
to-juniper       Up          <none>
Admin Groups:
--------------------------
        Group                Bit index
        -----                ---------
MPLS L3 Policies:
--------------------------
Name        Type Destination     Port   Source          Port   TOS Prot  Use
----------- ---- --------------- ------ --------------- ------ --- ----- -----
MPLS L2 Policies:
--------------------------
Name         Type  Source MAC       Dest MAC            Vlan     Use
-------------------------------------------------------------------------

RS2.2.2.2# ldp show all
Global parameters
------ ----------
Ordered control mode
Path vector loop detection disabled
Hop count loop detection disabled
```

```
Interface parameters
--------- ----------
Interface            Label space              Nbr count  Next hello(seconds)
lo                   2.2.2.2:0                    1          0
to-juniper           10.2.6.1:0                   1          0
Neighbor parameters
-------- ----------
Address             Interface           Label space ID      Hold Time(seconds)
10.2.6.2            to-juniper          6.6.6.6:0             12
1.1.1.1             lo                  1.1.1.1:0             9
Session parameters
------- ----------
Codes: Tx - Sent, Rx tot - Received Total, Rx fltd - Received Filtered
Address          State         Connection       Hold Time(sec) Tx/Rx tot/Rx fltd
6.6.6.6          Operational   Open             12             4/4/0
1.1.1.1          Operational   Open             9              5/5/0
Label Database
----- --------
Input label database, 2.2.2.2:0-6.6.6.6:0
  Label     Prefix
      3     6.6.6.6/32
 100013     4.4.4.4/32
 100020     1.1.1.1/32
 100021     2.2.2.2/32
Output label database, 2.2.2.2:0-6.6.6.6:0
  Label     Prefix
   2049     6.6.6.6/32
   2050     4.4.4.4/32
      3     2.2.2.2/32
   2051     1.1.1.1/32

Input label database, 2.2.2.2:0-1.1.1.1:0
  Label     Prefix
   2048     4.4.4.4/32
   2049     6.6.6.6/32
   2050     Customer ID 1
   2051     2.2.2.2/32
      3     1.1.1.1/32

Output label database, 2.2.2.2:0-1.1.1.1:0
  Label     Prefix
   2048     Customer ID 1
   2049     6.6.6.6/32
   2050     4.4.4.4/32
   2051     1.1.1.1/32
      3     2.2.2.2/32


LDP Statistics
--- ----------
Message type               Total                        Last 5 seconds
============               =====                        ==============
                       Sent    Received                Sent    Received
```

```
                        ----    --------                ----    --------
Hello                   222     421                     2       7
Initialization          2       2                       0       0
Keepalive               43      43                      1       1
Notifcation             0       0                       0       0
Address                 2       2                       0       0
Address withdraw        0       0                       0       0
Label mapping           9       18                      0       0
Label request           0       0                       0       0
Label withdraw          0       0                       0       0
Label release           0       0                       0       0
Label abort             0       0                       0       0
All UDP                 222     169                     2       3
All TCP                 56      51                      1       1


Event type                      Total                   Last 5 seconds
==========                      =====                   ==============
Sessions opened                 28                      0
Sessions closed                 26                      0
Shutdown received               0                       0
Shutdown sent                   0                       0

Keep alive expired              0                       0
Malformed TLV                   0                       0
Bad TLV length                  0                       0
Bad message length              0                       0
Bad PDU length                  0                       0
Bad LDP identifiers             0                       0
Hello errors                    0                       0
Advertisement errors            0                       0
Max PDU errors                  0                       0
Label range errors              0                       0

RS2.2.2.2# mpls show all


MPLS Controller : <mpls_1>
-------------------------
lsr-id      : 2.2.2.2
trace level : 1
flags       : <merge auto-lsp>
protocols   : <MPLS LDP>
Label Switched Paths:
-------------------------
Explicit Paths:
-------------------------
MPLS Interfaces:
-------------------------
Interface        State       Administrative groups
lo               Up          <none>
to-juniper       Up          <none>
Admin Groups:
```

```
-------------------------
        Group                Bit index
        -----                ---------

MPLS L3 Policies:
-------------------------
Name         Type Destination     Port   Source          Port   TOS Prot  Use
----------- ---- --------------- ------ --------------- ------ --- ----- -----
MPLS L2 Policies:
-------------------------
Name          Type  Source MAC       Dest MAC            Vlan     Use
-----------------------------------------------------------------------
```

The second part of the test was to focus on the RSVP fail-over. R4 and R6 have both a primary and secondary path configured for MPLS. The following is the MPLS show command in R6:

```
admin@R6.6.6.6# run show mpls lsp detail
Ingress LSP: 1 sessions

4.4.4.4
  From: 6.6.6.6, State: Up, ActiveRoute: 0, LSPname: 6-to-4
  ActivePath: strict-4 (primary)
  LoadBalance: Random
 *Primary   strict-4         State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 1)
              10.4.6.1 S
  Standby   strict-3         State: Up
    Computed ERO (S [L] denotes strict [loose] hops): (CSPF metric: 3)
              10.5.6.1 S         10.3.5.1 S         10.3.4.2 S
Total 1 displayed, Up 1, Down 0

Egress LSP: 2 sessions

6.6.6.6
  From: 4.4.4.4, LSPstate: Up, ActiveRoute: 0, LSPname: 4-to-6
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  129,  Since: Mon Aug 20 23:03:08 2001
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 7 receiver 17 protocol 0
  PATH rcvfrom: 10.4.6.1  (ge-0/1/0.0) 995 pkts
  PATH sentto: localclient
  RESV rcvfrom: localclient
  Record route: 10.4.6.1  <self>

6.6.6.6
  From: 4.4.4.4, LSPstate: Up, ActiveRoute: 0, LSPname: 4-to-6
  Resv style: 1 FF, Label in: 3, Label out: -
  Time left:  129,  Since: Mon Aug 20 22:56:48 2001
  Tspec: rate 0bps size 0bps peak Infbps m 20 M 1500
  Port number: sender 5 receiver 18 protocol 0
  PATH rcvfrom: 10.5.6.1  (ge-0/2/0.0) 984 pkts
  PATH sentto: localclient
  RESV rcvfrom: localclient
```

```
  Record route: 10.3.4.2  10.3.5.1  10.5.6.1  <self>
Total 2 displayed, Up 2, Down 0

Transit LSP: 0 sessions
Total 0 displayed, Up 0, Down 0
```

Using LDP Labels For Non-/32 Networks

Ian Cowburn
Corporate Systems Engineering
October 16, 2001

LDP can be used as a label distribution protocol with MPLS. By default, LDP will only distribute labels for /32 networks - these usually being assigned to lo0 and are used for BGP next-hops.

In order to use LDP distributed labels for non-/32 networks, the following is required:

- a label needs to be distributed for the chosen network

- in order to use the distributed label, these conditions must be satisfied on an LSR

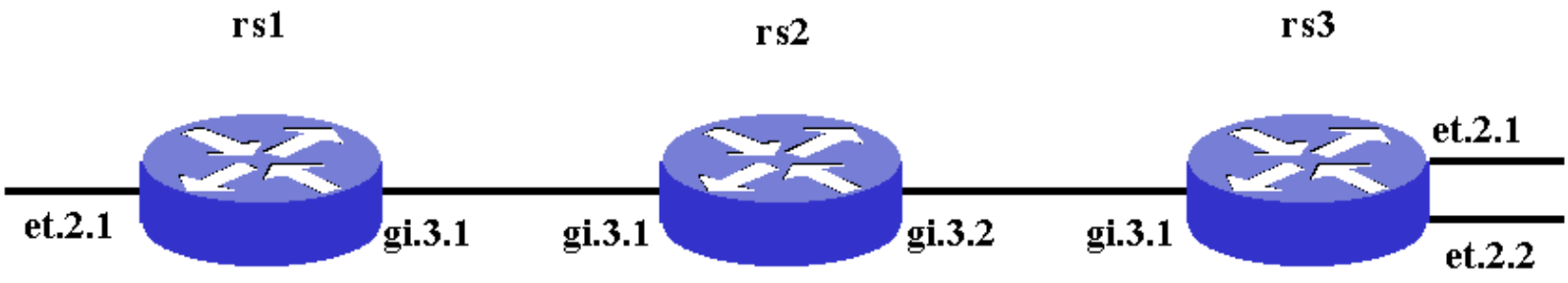
  - a route needs to exist in the routing table for the chosen network
  - this route must be an exact match of the chosen route, i.e. same address and netmask
  - the next hop of the route in the routing table must be the same LSR from which the label was received

The use of the LDP label can be verified with the diag mode command

ip show routes show-route-handles

RapidOS Version Tested	8.0.0.3
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS

Diagram



Configurations

rs1

```
vlan create lan1 ip
vlan create link1 ip
vlan add ports et.2.1 to lan1
vlan add ports gi.3.1 to link1
interface create ip lan1 address-netmask 192.168.254.254/24 vlan lan1
interface create ip link1 address-netmask 11.1.0.1/30 vlan link1
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ospf create area backbone
ospf add interface lan1 to-area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
mpls add interface link1
mpls start
ldp add interface link1
ldp start
system set name rs1
system set idle-timeout serial 0
system set idle-timeout telnet 0
```

rs2

```
vlan create link1 ip
vlan create link2 ip
vlan add ports gi.3.1 to link1
vlan add ports gi.3.2 to link2
interface create ip link1 address-netmask 11.1.0.2/30 vlan link1
interface create ip link2 address-netmask 11.2.0.1/30 vlan link2
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add interface link2 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
mpls add interface link1
mpls add interface link2
mpls start
ldp add interface link1
ldp add interface link2
ldp start
system set name rs2
system set idle-timeout serial 0
system set idle-timeout telnet 0
```

rs3

```
vlan create lan2 ip
vlan create lan3 ip
vlan create link2 ip
vlan add ports et.2.1 to lan2
vlan add ports et.2.2 to lan3
vlan add ports gi.3.1 to link2
interface create ip link2 address-netmask 11.2.0.2/30 vlan link2
interface create ip lan2-ldp address-netmask 10.1.1.1/24 vlan lan2
```

```
interface create ip lan3-not-ldp address-netmask 10.2.2.1/24 vlan lan3
interface add ip lo0 address-netmask 3.3.3.3/32
ip-router global set router-id 3.3.3.3
ospf create area backbone
ospf add interface link2 to-area backbone
ospf add stub-host 3.3.3.3 to-area backbone cost 10
ospf add interface lan2-ldp to-area backbone
ospf add interface lan3-not-ldp to-area backbone
ospf start
mpls add interface link2
mpls start
ldp add interface link2
ldp set egress-policy peer-address 2.2.2.2 route-map test sequence 1
ldp start
system set name rs3
system set idle-timeout serial 0
system set idle-timeout telnet 0
route-map test permit 5 match-prefix network 3.3.3.3/32
route-map test permit 10 match-prefix network 10.1.1.0/24
```

Comments

In this example we want rs1 to use an LDP distributed label in order to send traffic to network 10.1.1.0/24 on rs3. To start with, we need to get rs3 to distribute the required label to rs2. This is achieved by

```
ldp set egress-policy peer-address 2.2.2.2 route-map test sequence 1
route-map test permit 5 match-prefix network 3.3.3.3/32
route-map test permit 10 match-prefix network 10.1.1.0/24
```

Note that the route-map must specify 3.3.3.3/32 if a label for this network is still to be distributed.

On rs2 we then see:

```
rs2# ldp show database

Input label database, 2.2.2.2:0-3.3.3.3:0
  Label     Prefix
   2048     2.2.2.2/32
   2049     1.1.1.1/32
      3     10.1.1.0/24
      3     3.3.3.3/32

Output label database, 2.2.2.2:0-3.3.3.3:0
  Label     Prefix
   2048     1.1.1.1/32
   2049     3.3.3.3/32
   2050     10.1.1.0/24
      3     2.2.2.2/32

Input label database, 2.2.2.2:0-1.1.1.1:0
  Label     Prefix
   2048     2.2.2.2/32
   2049     3.3.3.3/32
   2050     10.1.1.0/24
      3     1.1.1.1/32

Output label database, 2.2.2.2:0-1.1.1.1:0
  Label     Prefix
   2048     1.1.1.1/32
   2049     3.3.3.3/32
   2050     10.1.1.0/24
```

```
      3     2.2.2.2/32
```

rs2 will then re-distribute a label for 10.1.1.0/24 to rs1, so on rs1 we then see:

```
rs1# ldp show database

Input label database, 1.1.1.1:0-2.2.2.2:0
  Label     Prefix
   2048     1.1.1.1/32
   2049     3.3.3.3/32
   2050     10.1.1.0/24
      3     2.2.2.2/32

Output label database, 1.1.1.1:0-2.2.2.2:0
  Label     Prefix
   2048     2.2.2.2/32
   2049     3.3.3.3/32
   2050     10.1.1.0/24
      3     1.1.1.1/32
```

To satisfy the conditions for this label to be used, we need the exact route in the routing table with rs2 being the next hop:

```
rs1# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              1.1.1.1              -         lo0
2.2.2.2              11.1.0.2             OSPF      link1
3.3.3.3              11.1.0.2             OSPF      link1
10.1.1.0/24          11.1.0.2             OSPF      link1
10.2.2.0/24          11.1.0.2             OSPF      link1
11.1.0.0/30          directly connected   -         link1
11.2.0.0/30          11.1.0.2             OSPF      link1
127.0.0.1            127.0.0.1            -         lo0
192.168.254.0/24     directly connected   -         lan1
```

We can then check the route-handles to verify that this route is using the LDP label (note: this is a diag command):

```
rs1? ip show routes show-route-handles

Destination          Gateway              Owner     Handle Netif
-----------          -------              -----     ------ -----
1.1.1.1              1.1.1.1              -         -      lo0
2.2.2.2              11.1.0.2             OSPF      1      link1
3.3.3.3              11.1.0.2             OSPF      2      link1
10.1.1.0/24          11.1.0.2             OSPF      3      link1
10.2.2.0/24          11.1.0.2             OSPF      -      link1
11.1.0.0/30          directly connected   -         -      link1
11.2.0.0/30          11.1.0.2             OSPF      -      link1
127.0.0.1            127.0.0.1            -         -      lo0
192.168.254.0/24     directly connected   -         -      lan1
```

Notice that 10.2.2.0/24 does not have a handle and therefore is not using LDP labels. You can see the labels associated with this route-handle via this command:

```
rs1? mpls show ott-flow-mgr

Handle Index Ref Count    DP Nexthop    POTT   ROTT  Label Depth    Label
------ ----- --------- --------------- ------ ------ ----------- ----------
1      0     1         11.1.0.2        1      0      1           3
2      0     1         11.1.0.2        2      3      1           2049
3      0     1         11.1.0.2        3      5      1           2050
```

MPLS & IBGP Full Mesh

Richard Foote
Corporate Systems Engineering
March 22, 2002

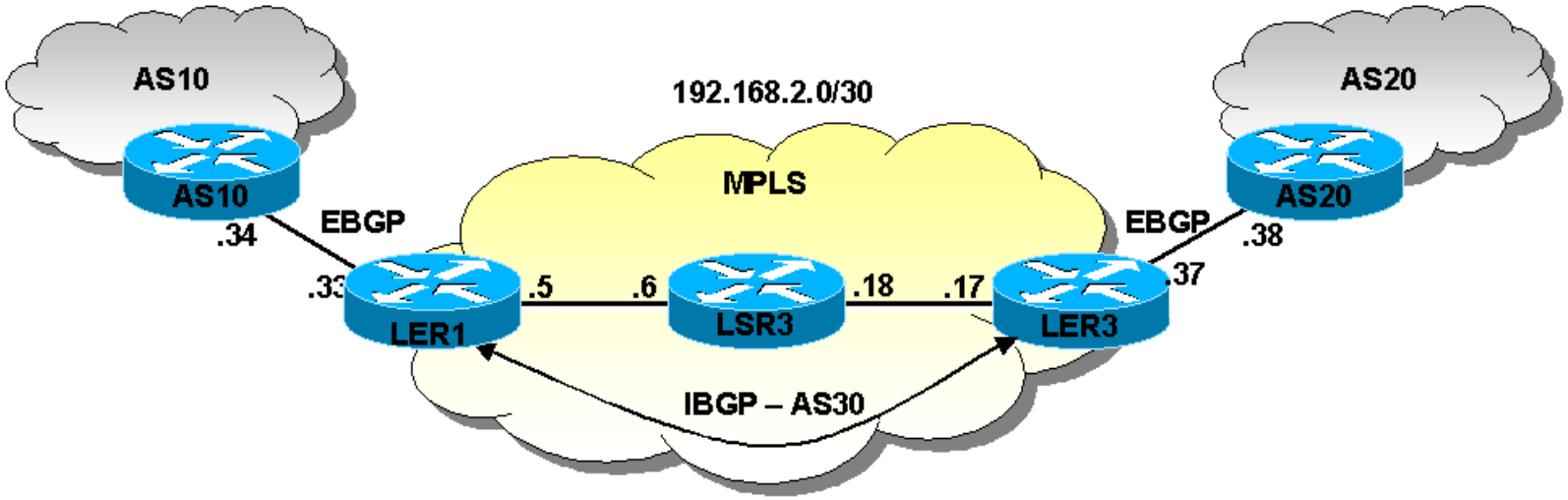
When BGP is deployed in a network, it is a requirement to create an IBPG full mesh to ensure all the necessary routes are distributed to all the internal routers that require a full routing table to transport IP requests to the destination network. The inception of route reflectors and confederations went a long way to providing better scalability than could be achieved without such approaches. However, the routers inside the providers AS were all still required to hold all the routes necessary to move packets toward their destination.

Enter the wonder of MPLS. Combining the use of BGP features like next-hop-self and MPLS' classification to Forward Equivalence Class (FEC) and data forwarding using labels, the requirement to run BGP in the core of a providers internal network is removed. The IBGP mesh is only required between the providers routers that act as EBGP peers to other autonomous systems. This greatly reduces the capacity/resource requirements of the internal routers and simplifies network deployments.

When prefixes are distributed to an EBGP peer, they are processed normally. However, before the prefix is distributed into the internal AS the EBGP router sets the next hop for that prefix to its loopback interface, using next hop self. The route is sent to the IBGP peers, using loopback addresses, allowing any packets destined for that prefix to be label switched rather than IP routed.

RapidOS Version Tested	9.0.0.0
RapidOS Version Working with this Configuration	9.0.0.0 and newer
RapidOS Version NOT Working with this Configuration	Older than 9.0.0.0
Hardware Specifics	MPLS enabled hardware facing and contained within the MPLS network

Diagram



Configurations

AS10

```
interface create ip AS10 port et.1.1 address-netmask 192.168.2.34/30
interface create ip adnet address-netmask 50.50.50.1/24 port et.2.1
interface add ip lo0 address-netmask 4.4.4.4/32
ip-router global set router-id 3.3.3.3
ip-router global set autonomous-system 10
ip-router policy redistribute from-proto direct to-proto bgp network 50.50.50.0/24
 source-as 10 target-as 30
ip-router policy redistribute from-proto bgp to-proto ospf network 100.100.100.0/24
source-as 30
bgp create peer-group as30-outside autonomous-system 30 type external
bgp add peer-host 192.168.2.33 group as30-outside
bgp set peer-group as10-outside local-address 192.168.2.34
bgp start
system set name AS10
```

LER1

```
interface create ip Edge13 port gi.7.2 address-netmask 192.168.2.5/30
interface create ip AS10 port et.2.1 address-netmask 192.168.2.33/30
interface add ip en0 address-netmask 192.168.3.1/24
interface add ip lo0 address-netmask 2.2.2.1/32
ip-router global set router-id 2.2.2.1
ip-router global set autonomous-system 30
ip-router policy redistribute from-proto bgp source-as 10 network 50.50.50.0/24
target-as 30 to-proto bgp
ip-router policy redistribute from-proto bgp to-proto bgp source-as 30 target-as 10
ospf create area backbone
ospf add interface Edge11 to-area backbone
ospf add interface Edge13 to-area backbone
ospf add stub-host 2.2.2.1 to-area backbone cost 10
ospf start
bgp create peer-group as30-inside type routing proto ospf autonomous-system 30
bgp create peer-group as10-outside autonomous-system 10 type external
bgp add peer-host 2.2.2.3 group as30-inside
bgp add peer-host 192.168.2.34 group as10-outside
bgp set peer-group as30-inside local-address 2.2.2.1
bgp set peer-group as10-outside local-address 192.168.2.33
bgp set peer-group as30-inside next-hop-self
bgp start
mpls add interface Edge11
mpls add interface Edge13
mpls start
ldp add interface Edge11
ldp add interface Edge13
ldp add interface lo0
ldp start
system set name ler1
```

LSR3

```
interface create ip edge33 address-netmask 192.168.2.18/30 port gi.7.1
interface create ip edge13 address-netmask 192.168.2.6/30 port gi.7.2
interface add ip en0 address-netmask 192.168.3.7/24
interface add ip lo0 address-netmask 1.1.1.3/32
ip-router global set router-id 1.1.1.3
ospf create area backbone
ospf add stub-host 1.1.1.3 to-area backbone cost 10
ospf add interface all to-area backbone
ospf start
mpls add interface all
mpls start
ldp add interface all
ldp start
system set name lsr3
```

LER3

```
interface create ip Edge33 address-netmask 192.168.2.17/30 port gi.7.1
interface create ip Edge215 address-netmask 192.168.2.37/30 port et.2.15
interface add ip en0 address-netmask 192.168.3.3/24
interface add ip lo0 address-netmask 2.2.2.3/32
ip-router global set router-id 2.2.2.3
```

```
ip-router global set autonomous-system 30
ip-router policy redistribute from-proto bgp to-proto bgp source-as 20
target-as 30 network 100.100.100.0/24
ospf create area backbone
ospf add stub-host 2.2.2.3 to-area backbone cost 10
ospf add interface Edge33 to-area backbone
ospf add interface Edge34 to-area backbone
ospf start
bgp create peer-group as30-inside type routing proto ospf autonomous-system 30
bgp create peer-group as20-outside autonomous-system 20 type external
bgp add peer-host 2.2.2.1 group as30-inside
bgp add peer-host 192.168.2.38 group as20-outside
bgp set peer-group as30-inside local-address 2.2.2.3
bgp set peer-group as30-inside next-hop-self
bgp set peer-group as20-outside local-address 192.168.2.37
bgp start
mpls add interface Edge33
mpls add interface Edge34
mpls start
ldp add interface Edge33
ldp add interface Edge34
ldp add interface lo0
ldp start
system set name ler3
```

AS20

```
interface create ip AS30 address-netmask 192.168.2.38/30 port et.1.1
interface create ip adnet address-netmask 100.100.100.1/24 port et.2.1
interface add ip lo0 address-netmask 3.3.3.3/32
ip-router global set autonomous-system 20
ip-router global set router-id 3.3.3.3
ip-router policy redistribute from-proto direct to-proto bgp network 100.100.100.0/24
source-as 20 target-as 30
ip-router policy redistribute from-proto bgp to-proto ospf source-as 30 network
50.50.50.0/24
bgp create peer-group AS30 autonomous-system 30 type external
bgp add peer-host 192.168.2.37 group AS30
bgp set peer-group AS30 local-address 192.168.2.38
bgp start
system set name as20
```

Comments

The above example is a simple one, meant to demonstrate the feature in an easily representable manner. In a more complex network, the core router configurations would remain very simple and follow the exact same concepts to that of the existing one, LSR3. Similarly, new edge router, or EBGP peer routers, would follow the same configuration techniques to that of the existing EBGP routers.

Checking the MPLS network information reveals that any packets that use a LSR ID, loopback address designated as the Router-ID, as the next hop will have an MPLS label applied to it and packets will be processed by MPLS, not the underlying IGP.

Displaying the LDP database reveals the label to prefix (FEC) binding. Since LDP uses the IGP for an initial decision, to determine which label to push based on the active next hop, it is important to be able to view that information easily. The label to prefix binding information is stored as "ip-binding" information.

All routers have their LDP database and active binding tables represented below.

```
ler1# ldp show database
Input label database, 2.2.2.1:0-1.1.1.3:0
  Label     Prefix
      3     1.1.1.3/32
     17     2.2.2.3/32
     18     2.2.2.1/32

Output label database, 2.2.2.1:0-1.1.1.3:0
  Label     Prefix
      3     2.2.2.1/32
     17     2.2.2.3/32
     18     1.1.1.3/32

ler1# mpls show ip-binding
  1.1.1.3/32
```

```
       output label:   18            Active
       input label:    imp-null      lsr: 1.1.1.3:0   inuse
  2.2.2.1/32
       output label:   imp-null      Active, Egress
       input label:    18            lsr: 1.1.1.3:0
  2.2.2.3/32
       output label:   17            Active
       input label:    17            lsr: 1.1.1.3:0   inuse

lsr3# ldp show database
Input label database, 1.1.1.3:0-2.2.2.1:0
  Label     Prefix
      3     2.2.2.1/32
     17     2.2.2.3/32
     18     1.1.1.3/32

Output label database, 1.1.1.3:0-2.2.2.1:0
  Label     Prefix
      3     1.1.1.3/32
     17     2.2.2.3/32
     18     2.2.2.1/32

Input label database, 1.1.1.3:0-2.2.2.3:0
  Label     Prefix
      3     2.2.2.3/32
     17     1.1.1.3/32
     18     2.2.2.1/32

Output label database, 1.1.1.3:0-2.2.2.3:0
  Label     Prefix
      3     1.1.1.3/32
     17     2.2.2.3/32
     18     2.2.2.1/32

lsr3# mpls show ip-binding
  1.1.1.3/32
       output label:   imp-null      Active, Egress
       input label:    18            lsr: 2.2.2.1:0
       input label:    17            lsr: 2.2.2.3:0
  2.2.2.1/32
       output label:   18            Active
       input label:    18            lsr: 2.2.2.3:0
       input label:    imp-null      lsr: 2.2.2.1:0   inuse
  2.2.2.3/32
       output label:   17            Active
       input label:    17            lsr: 2.2.2.1:0
       input label:    imp-null      lsr: 2.2.2.3:0   inuse

ler3# ldp show database
Input label database, 2.2.2.3:0-1.1.1.3:0
  Label     Prefix
      3     1.1.1.3/32
     17     2.2.2.3/32
     18     2.2.2.1/32

Output label database, 2.2.2.3:0-1.1.1.3:0
  Label     Prefix
      3     2.2.2.3/32
     17     1.1.1.3/32
     18     2.2.2.1/32

ler3# mpls show ip-binding
  1.1.1.3/32
       output label:   17            Active
       input label:    imp-null      lsr: 1.1.1.3:0   inuse
  2.2.2.1/32
       output label:   18            Active
       input label:    18            lsr: 1.1.1.3:0   inuse
  2.2.2.3/32
       output label:   imp-null      Active, Egress
       input label:    17            lsr: 1.1.1.3:0
```

Checking the BGP summary information shows that only the routers that are EBGP have BGP peering sessions, IBGP for internal peers and EBGP for peers outside of the local AS. The LSR does not have the BGP process enabled thus cannot, and need not, participate in any BGP sessions.

```
AS10# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: as30-outside]
192.168.2.33    4    30      71      69    0d1h4m35s         1/1

ler1# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: as30-inside]
2.2.2.3         4    30      85      83   0d1h17m10s         1/1
[Group Id: as10-outside]
192.168.2.34    4    10      64      68   0d0h59m59s         1/1
BGP summary, 2 groups, 2 peers

ler3# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: as30-inside]
2.2.2.1         4    30      93      96   0d1h28m15s         1/1
[Group Id: as20-outside]
192.168.2.38    4    20      56      56    0d0h51m3s         1/1
BGP summary, 2 groups, 2 peers

as20# bgp show summary
Neighbor        V    AS MsgRcvd MsgSent      Up/Down Prefixes Rcvd/Sent
--------        -    -- ------- -------      ------- ------------------
[Group Id: AS30]
192.168.2.37    4    30      57      59    0d0h53m9s         1/1
BGP summary, 1 groups, 1 peers
```

The BGP route information at each BGP node shows what routes have been learned and who is the active next hop. For the EBGP session, external routes have their peers physical interface. However, the IBGP sessions have the external routes learned with a next hop of the peer IBGP loopback address. This is accomplished by coding the "next-hop-self" option for the internal peer-group.

```
AS10# bgp show routes all
BGP table : Local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop        Metric LocPrf Path
  -------            --------        ------ ------ ----
*>100.100.100/24     192.168.2.33                  30 20 i

ler1# bgp show routes all
BGP table : Local router ID is 2.2.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop        Metric LocPrf Path
   -------            --------        ------ ------ ----
*> 50.50.50/24        192.168.2.34             100 (30) 10 i
*>i100.100.100/24     2.2.2.3                  100 (30) 20 i

ler3# bgp show routes all
BGP table : Local router ID is 2.2.2.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            Next Hop        Metric LocPrf Path
   -------            --------        ------ ------ ----
*>i50.50.50/24        2.2.2.1                  100 (30) 10 i
*> 100.100.100/24     192.168.2.38             100 (30) 20 i

as20# bgp show routes all
BGP table : Local router ID is 3.3.3.3
Status codes: s suppressed, d damped, h history, * valid, > best
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network            Next Hop        Metric LocPrf Path
  -------            --------        ------ ------ ----
*>50.50.50/24        192.168.2.37                  30 10 i
```

Of course, good form may suggest using a route-map command to set the origin of the route.

Finally, a look at the forwarding information base, or FIB, for all the routers completes the example. Notice that LSR3 knows nothing about the external routes. However, since all packets destined to external networks arrives with an MPLS label, simple label switching allows the LSR to forward the packet to the next hop.

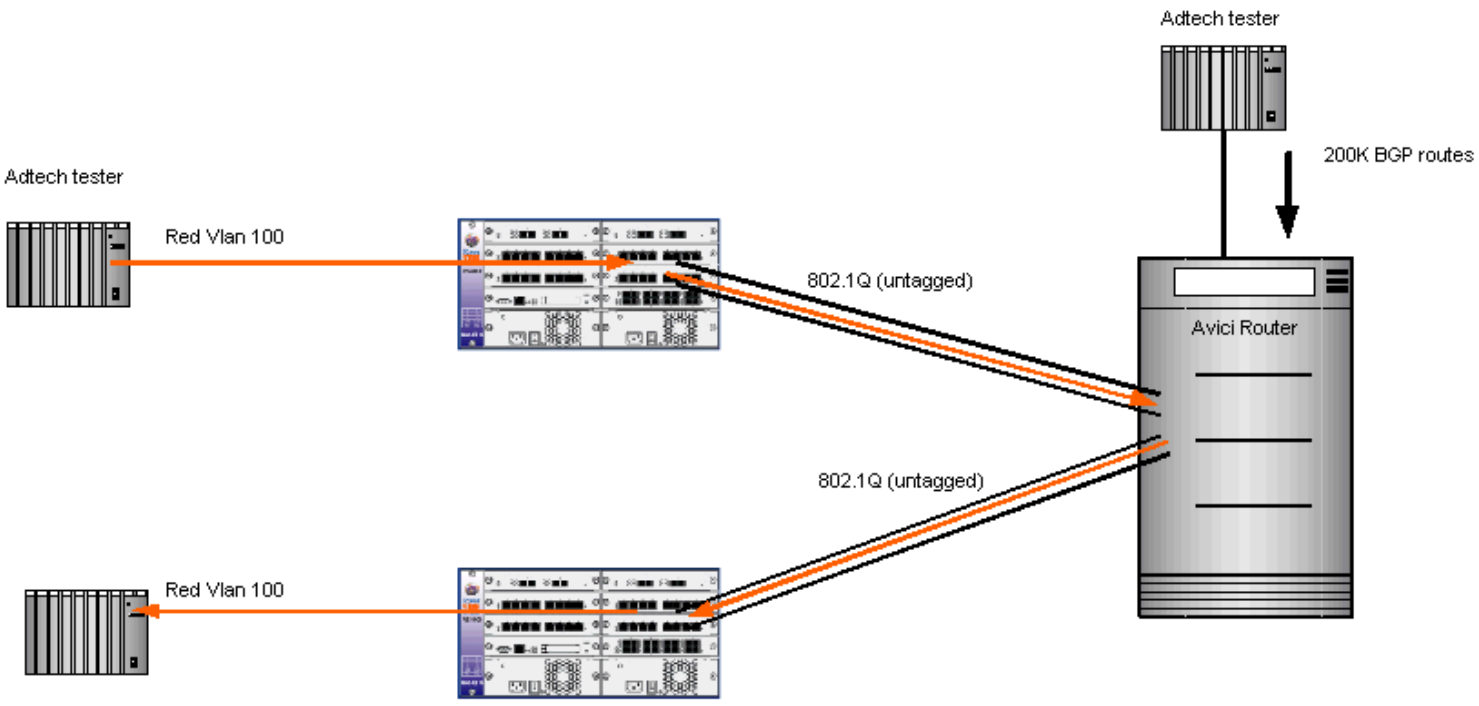
```
AS10# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
4.4.4.4              4.4.4.4              -         lo0
50.50.50.0/24        directly connected   -         adnet
100.100.100.0/24     192.168.2.33         BGP       AS10
127.0.0.1            127.0.0.1            -         lo0
192.168.2.32/30      directly connected   -         AS10

ler1# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.3              192.168.2.6          OSPF      Edge13
2.2.2.1              2.2.2.1              -         lo0
2.2.2.3              192.168.2.6          OSPF      Edge13
50.50.50.0/24        192.168.2.34         BGP       AS10
100.100.100.0/24     192.168.2.6          BGP       Edge13
127.0.0.1            127.0.0.1            -         lo0
192.168.2.4/30       directly connected   -         Edge13
192.168.2.16/30      192.168.2.6          OSPF      Edge13
192.168.2.32/30      directly connected   -         AS10
192.168.3.0/24       directly connected   -         en0

lsr3# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.3              1.1.1.3              -         lo0
2.2.2.1              192.168.2.5          OSPF      edge13
2.2.2.3              192.168.2.17         OSPF      edge33
127.0.0.1            127.0.0.1            -         lo0
192.168.2.4/30       directly connected   -         edge13
192.168.2.16/30      directly connected   -         edge33
192.168.3.0/24       directly connected   -         en0

ler3# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.3              192.168.2.18         OSPF      Edge33
2.2.2.1              192.168.2.18         OSPF      Edge33
2.2.2.3              2.2.2.3              -         lo0
50.50.50.0/24        192.168.2.18         BGP       Edge33
100.100.100.0/24     192.168.2.38         BGP       Edge215
127.0.0.1            127.0.0.1            -         lo0
192.168.2.4/30       192.168.2.18         OSPF      Edge33
192.168.2.16/30      directly connected   -         Edge33
192.168.2.36/30      directly connected   -         Edge215
192.168.3.0/24       directly connected   -         en0

as20# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
3.3.3.3              3.3.3.3              -         lo0
50.50.50.0/24        192.168.2.37         BGP       AS30
100.100.100.0/24     directly connected   -         adnet
127.0.0.1            127.0.0.1            -         lo0
192.168.2.36/30      directly connected   -         AS30
```

MPLS Martini Tunnels with Avici

Scott Martin
Systems Engineering
March 27, 2002

This configuration demonstrates MPLS Martini interoperability between Riverstone and Avici.	
RapidOS Version Tested	8.0.0.5, 8.0.0.5L
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.x
Hardware Specifics	MPLS enabled GIG modules

Diagram



Configurations

Riverstone Top Router

```
port description gi.3.1 to-adtech
port description gi.3.2 to-avici
vlan make trunk-port gi.3.2 untagged
vlan create test ip id 100
vlan add ports gi.3.1 to test

interface create ip to-Avici address-netmask 10.4.0.2/24 port gi.3.2
interface add ip lo0 address-netmask 10.10.10.2/32
interface add ip en0 address-netmask 10.0.0.100/24

ip-router global set router-id 10.10.10.2
ip-router global set autonomous-system 65060
ip-router global set trace-state on

ospf create area backbone
ospf add interface to-Avici to-area backbone
ospf add stub-host 10.10.10.2 to-area backbone cost 2
ospf add interface to-adtech to-area backbone
ospf set interface to-adtech passive
ospf start

bgp create peer-group IBGP type routing autonomous-system 65060
bgp add peer-host 10.10.10.1 group IBGP
bgp set peer-group IBGP local-address 10.10.10.2
bgp start

mpls add interface all
mpls start

ldp add interface lo0
ldp add interface to-Avici
ldp add remote-peer 10.10.10.3
ldp add l2-fec vlan 100 to-peer 10.10.10.3
ldp start

system set name RS-top
```

Riverstone Bottom Router

```
port description gi.3.1 to-adtech
port description gi.3.2 to-avici
vlan make trunk-port gi.3.2 untagged
vlan create test ip id 100
vlan add ports gi.3.1 to test
vlan add ports gi.3.2 to test

interface create ip to-Avici address-netmask 10.5.0.2/24 port gi.3.2
interface add ip lo0 address-netmask 10.10.10.3/32
interface add ip en0 address-netmask 10.0.0.99/24

ip-router global set router-id 10.10.10.3
ip-router global set autonomous-system 65060
ip-router policy redistribute from-proto direct to-proto ospf

ospf create area backbone
ospf add interface to-Avici to-area backbone
ospf add stub-host 10.10.10.3 to-area backbone cost 2
ospf add interface to-adtech to-area backbone
ospf set interface to-adtech passive
ospf start

bgp create peer-group IBGP type routing autonomous-system 65060
bgp add peer-host 10.10.10.1 group IBGP
bgp set peer-group IBGP local-address 10.10.10.3
bgp start

mpls add interface all
```

```
mpls start

ldp add interface lo0
ldp add interface to-Avici
ldp add remote-peer 10.10.10.2
ldp add l2-fec vlan 100 to-peer 10.10.10.2
ldp start

system set name rs-bottom
```

Avici

```
server-id 1 upper

server-location 1/11

warm-standby

hostname mini-me

system-password 7 S9bQQdb9Sd
enable password 7 S9bQQdb9Sd

user admin password 7 S9bQQdb9Sd
watchdog soft

no fabric link heuristic shutdown

mpls ldp
 no auto-upgrade
random-detect parameter-set high min-th 1544.00kb max-th 1544.00kb max-mark-spacing 8
 packet-treatment parameter-set high bandwidth t1 queue-depth 10.00ms random-det
ect-parameters high
 mpls classifier high exp 7

interface Loopback 0
 ip address 10.10.10.1 255.255.255.0
 no shutdown

interface Ethernet 0
 ip address 10.0.0.1 255.255.255.0
 no shutdown

module 1/4 1xoc48c
 no shutdown

interface pos 1/4/1
 clock source internal
ip address 10.1.0.1 255.255.255.0
 peer default ip address 10.1.0.2
 no keepalive
 no shutdown

module 1/5 2x1gbe
 no shutdown

interface gbe 1/5/1
 no negotiation auto
 no shutdown
 ip address 10.3.0.1 255.255.255.0

interface gbe 1/5/2
 mtu 1582
 no shutdown
 ip address 10.4.0.1 255.255.255.0
 mpls ldp

module 1/6 1xoc48c
```

```
 no shutdown

interface pos 1/6/1
no ip address
 no keepalive
 no shutdown

module 1/7 2x1gbe
 no shutdown
interface gbe 1/7/1
 no ip address

interface gbe 1/7/2
 no ip address
module 1/14 1xoc48c
 no shutdown

interface pos 1/14/1
 clock source internal
 no ip address

module 1/15 2x1gbe
 no shutdown
interface gbe 1/15/1
 mtu 1582
 no shutdown
 ip address 10.5.0.1 255.255.255.0
 mpls ldp

interface gbe 1/15/2
 no ip address

module 1/16 1xoc48c
 no shutdown

interface pos 1/16/1
 clock source internal
 ip address 10.2.0.1 255.255.255.0
 peer default ip address 10.2.0.2
 no shutdown

module 1/17 2x1gbe
 no shutdown

interface gbe 1/17/1
 no ip address
interface gbe 1/17/2
 no ip address

router ospf 1
 passive-interface Loopback 0
 network 10.1.0.0 0.0.0.255 area 0.0.0.0
 network 10.3.0.0 0.0.0.255 area 0.0.0.0
 network 10.4.0.0 0.0.0.255 area 0.0.0.0
 network 10.5.0.0 0.0.0.255 area 0.0.0.0
 network 10.10.10.1 0.0.0.0 area 0.0.0.0

router bgp 65060
 neighbor test peer-group
 neighbor test remote-as 65060
 neighbor 10.1.0.4 peer-group test
 neighbor 10.1.0.6 peer-group test
 neighbor 10.1.0.7 peer-group test
 neighbor 10.1.0.8 peer-group test
 neighbor 10.1.0.9 peer-group test
 neighbor 10.1.0.10 peer-group test
 neighbor 10.1.0.11 peer-group test
```

```
 neighbor 10.1.0.12 peer-group test
 neighbor 10.1.0.13 peer-group test
 neighbor 10.1.0.14 peer-group test
 neighbor 10.1.0.15 peer-group test
 neighbor 10.1.0.16 peer-group test
 neighbor rr-client peer-group
 neighbor rr-client remote-as 65060
 neighbor rr-client route-reflector-client
 neighbor rr-client next-hop-self
 neighbor rr-client update-source loopback 0
 neighbor 10.1.0.5 peer-group rr-client
 neighbor 10.10.10.2 peer-group rr-client
 neighbor 10.10.10.3 peer-group rr-client
 neighbor 10.2.0.4 remote-as 65060

mpls traffic-engineering ospf
ip route 10.10.11.0 255.255.255.0 10.1.0.2

bay 1/1
end
```

Comments

```
rs-bottom# ldp show all

Global parameters
------ ----------

Ordered control mode
Path vector loop detection disabled
Hop count loop detection disabled

Interface parameters
--------- ----------

Interface            Label space              Nbr count  Next hello(seconds)
lo                   10.10.10.3:0                 1          0
to-Avici             10.5.0.2:0                   1          0

Neighbor parameters
-------- ----------

Address             Interface           Label space ID      Hold Time(seconds)
10.5.0.1            to-Avici            10.10.10.1:0          7
10.10.10.2          lo                  10.10.10.2:0          12

Session parameters
------- ----------

Codes: Tx - Sent, Rx tot - Received Total, Rx fltd - Received Filtered

Address          State         Connection       Hold Time(sec) Tx/Rx tot/Rx fltd
10.5.0.1         Operational   Open             7              2/1/0
10.10.10.2       Operational   Open             12             3/3/0

Label Database
----- --------

Input label database, 10.10.10.3:0-10.10.10.1:0
  Label     Prefix
  32767     10.10.10.2/32

Output label database, 10.10.10.3:0-10.10.10.1:0
  Label     Prefix
      3     10.10.10.3/32
   2108     10.10.10.2/32
```

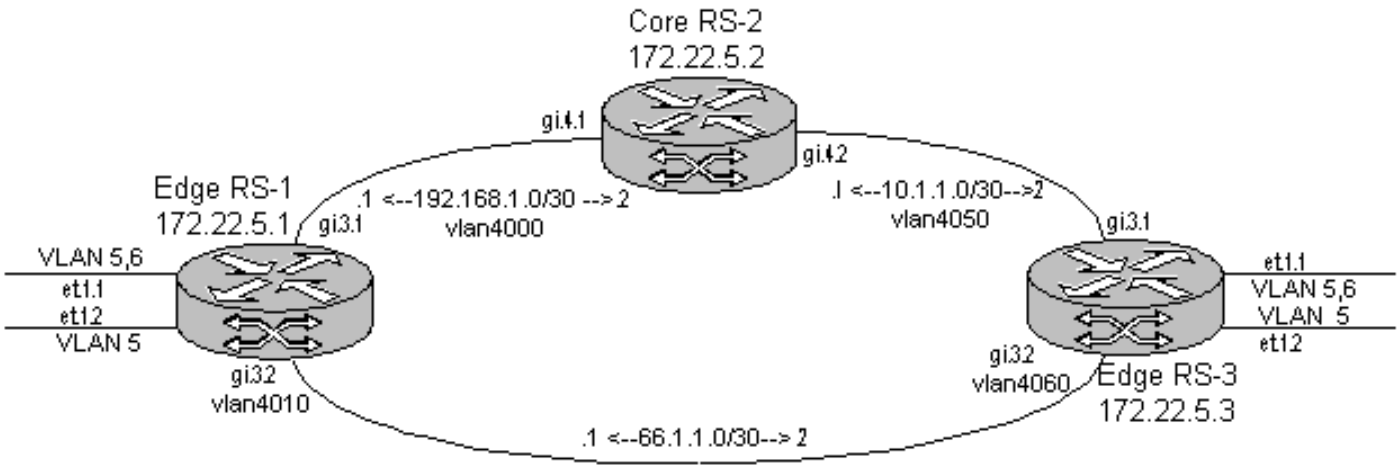
```
Input label database, 10.10.10.3:0-10.10.10.2:0
  Label     Prefix
      3     10.10.10.2/32
   2095     VLAN ID 100
   2107     10.10.10.3/32

Output label database, 10.10.10.3:0-10.10.10.2:0
  Label     Prefix
      3     10.10.10.3/32
   2096     VLAN ID 100
   2108     10.10.10.2/32

LDP Statistics
--- ----------
Message type                Total                     Last 5 seconds
============                =====                     ==============
                       Sent    Received               Sent    Received
                       ----    --------               ----    --------
Hello                  1280    2317                   2       4
Initialization         39      39                     0       0
Keepalive              611     523                    1       0
Notifcation            41      29                     0       0
Address                39      40                     0       0
Address withdraw       0       1                      0       0
Label mapping          157     356                    0       0
Label request          0       0                      0       0
Label withdraw         74      146                    0       0
Label release          73      134                    0       0
Label abort            0       0                      0       0
All UDP                1280    1161                   2       2
All TCP                1034    867                    1       0


Event type                  Total                     Last 5 seconds
==========                  =====                     ==============
Sessions opened             40                        0
Sessions closed             38                        0
Shutdown received           0                         0
Shutdown sent               35                        0

Keep alive expired          0                         0
Malformed TLV               0                         0
Bad TLV length              0                         0
Bad message length          0                         0
Bad PDU length              0                         0
Bad LDP identifiers         0                         0
Hello errors                0                         0
Advertisement errors        0                         0
Max PDU errors              0                         0
Label range errors          0                         0
```

MPLS Service Levels

Payam Kahen, Doug Turner
Systems Engineering
May 15, 2002

This article shows an example of how to use an MPLS network incorporating Martini Tunnels while differentiating customer traffic into various service levels based on VLAN ID. We will offer two Service Levels: Gold and Bronze to transport traffic from two customers, one of each is preferred over the other.	
RapidOS Version Tested	8.0.3.4
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0
Hardware Specifics	MPLS

Diagram



Configurations

Edge RS-1

```
! The ports connecting to the customers are trunk ports
vlan make trunk-port et.1.1-2

! The ports connecting router to the MPLS network must be specified as trunk ports,
however, they must NOT send out 802.1Q tagged packets
vlan make trunk-port gi.3.1-2 untagged

! Create Customer VLANs
vlan create vlan5 port-based id 5
vlan create vlan6 port-based id 6

! Create Backbone (MPLS) VLANs
vlan create vlan4000 port-based id 4000
vlan create vlan4010 port-based id 4010

! Add Customer ports to appropriate VLANs
vlan add ports et.1.1-2 to vlan5
vlan add ports et.1.(1-2) to vlan6

! Add Backbone ports to Customer VLANs and both Backbone VLANs
vlan add ports gi.3.1-2 to vlan5
vlan add ports gi.3.1-2 to vlan6
! Add each Backbone port only to its INDIVIDUAL Backbone VLAN
vlan add ports gi.3.2 to vlan4010
vlan add ports gi.3.1 to vlan4000

! Create IP Interfaces over each Backbone VLAN
interface create ip RS-CORE-2 address-netmask 192.168.1.1/30 vlan vlan4000
interface create ip RS-EDGE-3 address-netmask 66.1.1.1/30 vlan vlan4010

! Add a Loopback IP address to be used for OSPF and LDP, and set it as the Router’s
ID
interface add ip lo0 address-netmask 172.22.5.1/32
ip-router global set router-id 172.22.5.1

! Create and start the OSPF process on all IP Interfaces
ospf create area backbone
ospf add stub-host 172.22.5.1 to-area backbone cost 5
ospf add interface RS-CORE-2 to-area backbone
ospf add interface RS-EDGE-3 to-area backbone
ospf start

! Add the Backbone Interfaces and lo0 to the MPLS process
mpls add interface RS-EDGE-3
mpls add interface RS-CORE-2
mpls add interface lo0

! Create two disparate paths for the Gold and Silver paths
```

```
mpls create path GOLD-PATH num-hops 1
mpls create path SILVER-PATH num-hops 2

! The IP address used for the hops is that either of the locally assigned IP (first
hop), or IP address corresponding to the other side of the link (second and
subsequent hops)
mpls set path GOLD-PATH ip-addr 66.1.1.1 type strict hop 1
mpls set path SILVER-PATH ip-addr 192.168.1.1 type strict hop 1
mpls set path SILVER-PATH ip-addr 192.168.1.2 type strict hop 2

! Create two LSPs to the Loopback IP of Edge RS-3 named GOLD and SILVER, and specify
the appropriate ‘path’ (as formed above)
mpls create label-switched-path GOLD to 172.22.5.3 no-cspf preference 10
mpls set label-switched-path GOLD primary GOLD-PATH no-cspf retry-interval 5
mpls create label-switched-path SILVER to 172.22.5.3 no-cspf preference 10
mpls set label-switched-path SILVER primary SILVER-PATH no-cspf retry-interval 10

! Start the MPLS processs
mpls start

! Add the Backbone Interfaces (not Loopback, though!) to RSVP and start
rsvp add interface RS-EDGE-3
rsvp add interface RS-CORE-2
rsvp start

! Add ONLY the Loopback interface to LDP
ldp add interface lo0

! Add Edge RS-3 as a remote Martini peer
ldp add remote-peer 172.22.5.3

! Create the Martini tunnels based on VLAN ID to the Loopback IP of RS Edge-3;
specify that an alternate LSP maybe used for transport
ldp add l2-fec vlan 5 to-peer 172.22.5.3
ldp set l2-fec vlan 5 transport-lsp GOLD to-peer 172.22.5.3 alternate-acceptable
ldp add l2-fec vlan 6 to-peer 172.22.5.3
ldp set l2-fec vlan 6 transport-lsp SILVER to-peer 172.22.5.3 alternate-acceptable

! Start the LDP process
ldp start

system set name "Edge RS-1"
```

Core RS-2

```
! Create the Backbone VLANs corresponding to attached Routers, but there is NO NEED
to make ports 802.1Q enabled on core routers
vlan create vlan4000 port-based id 4000
vlan create vlan4050 port-based id 4050
vlan add ports gi.4.1 to vlan4000
vlan add ports gi.4.2 to vlan4050

! Create IP Interfaces over the VLANs and add the Loopback ID; set that IP as the
```

```
Router ID
interface create ip RS-EDGE-1 address-netmask 192.168.1.2/30 vlan vlan4000
interface create ip RS-EDGE-2 address-netmask 10.1.1.2/30 vlan vlan4050
interface add ip lo0 address-netmask 172.22.5.2/32
ip-router global set router-id 172.22.5.2

! Start the OSPF process on all Interfaces
ospf create area backbone
ospf add interface all to-area backbone
ospf add stub-host 172.22.5.2 to-area backbone cost 5
ospf start

! Start the MPLS process on all Interfaces
mpls add interface all
mpls start

! Start the RSVP processs on all Interfaces
rsvp add interface all
rsvp start

system set name "Core RS-2"
```

Edge RS-3

```
vlan make trunk-port et.1.(1-2)
vlan make trunk-port gi.3.1-2 untagged
vlan create vlan5 port-based id 5
vlan create vlan6 port-based id 6
vlan create vlan4050 port-based id 4050
vlan create vlan4060 port-based id 4060
vlan add ports et.1.(1-2) to vlan5
vlan add ports et.1.(1-2) to vlan6
vlan add ports gi.3.1-2 to vlan5
vlan add ports gi.3.1-2 to vlan6
vlan add ports gi.3.1 to vlan4050
vlan add ports gi.3.2 to vlan4060
interface create ip RS-CORE-2 address-netmask 10.1.1.1/30 vlan vlan4050
interface create ip RS-EDGE-1 address-netmask 66.1.1.2/30 vlan vlan4060
interface add ip lo0 address-netmask 172.22.5.3/32
ip-router global set router-id 172.22.5.3
ospf create area 0.0.0.0
ospf add stub-host 172.22.5.3 to-area 0.0.0.0 cost 5
ospf add interface UPLINK to-area 0.0.0.0
ospf add interface RS-EDGE-1 to-area 0.0.0.0
ospf start
mpls add interface RS-EDGE-1
mpls add interface RS-CORE-2
mpls add interface lo0
mpls create path GOLD-PATH num-hops 1
mpls create path SILVER-PATH num-hops 2
mpls set path GOLD-PATH ip-addr 66.1.1.2 type strict hop 1
mpls set path SILVER-PATH ip-addr 10.1.1.1 type strict hop 1
```

```
mpls set path SILVER-PATH ip-addr 10.1.1.2 type strict hop 2
mpls create label-switched-path GOLD to 172.22.5.1 no-cspf preference 10
mpls create label-switched-path SILVER to 172.22.5.1 no-cspf preference 20
mpls set label-switched-path GOLD primary GOLD-PATH no-cspf retry-interval 5
mpls set label-switched-path SILVER primary SILVER-PATH no-cspf retry-interval 10
mpls start
rsvp add interface RS-CORE-2
rsvp add interface RS-EDGE-1
rsvp start
ldp add interface lo0
ldp add remote-peer 172.22.5.1
ldp add l2-fec vlan 5 to-peer 172.22.5.1
ldp add l2-fec vlan 6 to-peer 172.22.5.1
ldp set l2-fec vlan 5 transport-lsp GOLD to-peer 172.22.5.1 alternate-acceptable
ldp set l2-fec vlan 6 transport-lsp SILVER to-peer 172.22.5.1 alternate-acceptable
ldp start
system set name "Edge RS-3"
```

Comments

The configuration for RS Edge-3 is similar to that of RS Edge-1. RS Core-2 is not involved in the LDP process because there are no tunnels originating or terminating at this router. Furthermore, there is no need for 802.1Q enabled links as all traffic arriving at the router and leaving the router will be MPLS encapsulated, not .1Q. Thus, across all routers, the VID used for the MPLS backbone links is only locally siginificant and do not need to match across routers.

With this configuration we are able to show a very significant use of MPLS with the RS platform. We are able to classify customer traffic into multiple Service Levels each utilizing a different path. In our example we see that the LSP named "Gold" has only one hop to traverse, while the "Bronze" path takes two hops to get to the same end-point. Of course, it’s easy to imagine a diameter much larger than one or two with this application.

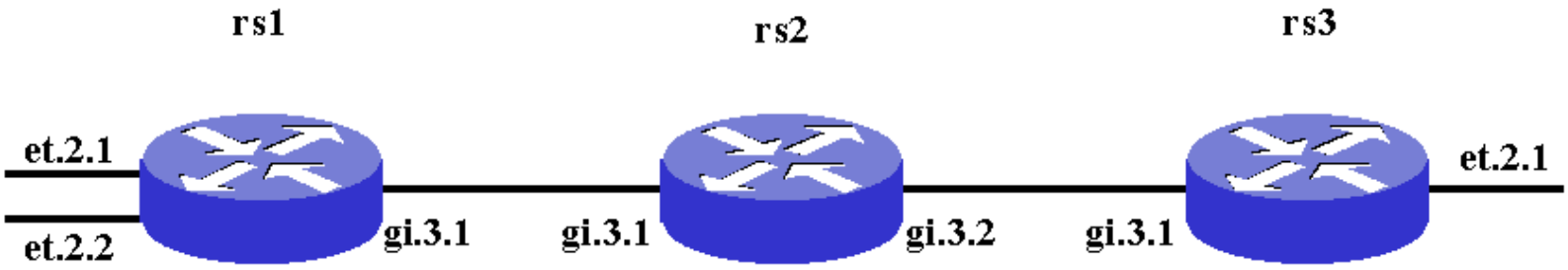
All traffic from VLAN 5 uses the Gold service level path, while traffic from VLAN 6 uses the Bronze path. However, if one of the paths becomes unavailable, the other path is used to get traffic to its destination. Upon restoral, traffic will revert to its original path.

Martini port/vlan l2-fec Configurations

Ian Cowburn
Corporate Systems Engineering
July 9, 2002

This document shows two configuration possibilities when using martini port/vlan l2-fecs, namely • It is possible to have the port on one end of the martini tunnel as an access port and the other as a trunk port • It is possible to configure multiple customer-id's on a port, each corresponding to a specific (non-overlapping) set of vlans	
RapidOS Version Tested	9.1.0.0
RapidOS Versions Working with this Configuration	9.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.1.0.0
Hardware Specifics	MPLS line cards

Diagram



Configurations

rs1

```
vlan make trunk-port et.2.2
vlan create link1 ip
vlan create 100 id 100
vlan create 200 id 200
vlan add ports gi.3.1 to link1
vlan add ports et.2.1 to 100
vlan add ports et.2.2 to 200
interface create ip link1 address-netmask 11.1.0.1/30 vlan link1
interface add ip lo0 address-netmask 1.1.1.1/32
```

```
ip-router global set router-id 1.1.1.1
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
mpls add interface link1
mpls create label-switched-path tunnel-lsp to 3.3.3.3 no-cspf
mpls start
rsvp add interface link1
rsvp start
ldp add interface lo0
ldp map ports et.2.1 customer-id 1000
ldp map ports et.2.2 customer-id 2000
ldp add l2-fec customer-id 1000 vlan 100 to-peer 3.3.3.3
ldp add l2-fec customer-id 2000 vlan 200 to-peer 3.3.3.3
ldp add remote-peer 3.3.3.3
ldp start
system set name rs1
system set idle-timeout serial 0 telnet 0
```

rs2

```
vlan create link1 ip
vlan create link2 ip
vlan add ports gi.3.1 to link1
vlan add ports gi.3.2 to link2
interface create ip link1 address-netmask 11.1.0.2/30 vlan link1
interface create ip link2 address-netmask 11.2.0.1/30 vlan link2
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add interface link2 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
mpls add interface link1
mpls add interface link2
mpls start
rsvp add interface link1
rsvp add interface link2
rsvp start
system set name rs2
system set idle-timeout serial 0 telnet 0
```

rs3

```
vlan make trunk-port et.2.1
vlan create link2 ip
vlan create 100 id 100
vlan create 200 id 200
vlan add ports gi.3.1 to link2
vlan add ports et.2.1 to 100
vlan add ports et.2.1 to 200
interface create ip link2 address-netmask 11.2.0.2/30 vlan link2
interface add ip lo0 address-netmask 3.3.3.3/32
ip-router global set router-id 3.3.3.3
ospf create area backbone
ospf add interface link2 to-area backbone
ospf add stub-host 3.3.3.3 to-area backbone cost 10
ospf start
mpls add interface link2
mpls create label-switched-path tunnel-lsp to 1.1.1.1 no-cspf
```

```
mpls start
rsvp add interface link2
rsvp start
ldp add interface lo0
ldp map ports et.2.1 customer-id 1000
ldp map ports et.2.1 customer-id 2000
ldp add l2-fec customer-id 1000 vlan 100 to-peer 1.1.1.1
ldp add l2-fec customer-id 2000 vlan 200 to-peer 1.1.1.1

ldp add remote-peer 1.1.1.1
ldp start
system set name rs3
system set idle-timeout serial 0 telnet 0
```

Comments

In the configurations you can see that two port/vlan l2-fecs have been created between rs1 and rs3, as follows:

Customer-id	vlan	rs1 port	port type	rs3 port	port type
1000	100	et.2.1	access	et.2.1	trunk
2000	200	et.2.2	trunk	et.2.1	trunk

L2-fec output:

```
rs1# ldp show l2-fec

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 3.3.3.3:0

FEC                                 in-lbl  out-lbl Transport LSP name/label

Customer ID 2000, VLAN ID 200       17      18      tunnel-lsp/4097
Customer ID 1000, VLAN ID 100       18      17      tunnel-lsp/4097


rs3# ldp show l2-fec

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 1.1.1.1:0

FEC                                 in-lbl  out-lbl Transport LSP name/label

Customer ID 1000, VLAN ID 100       17      18      tunnel-lsp/4097
Customer ID 2000, VLAN ID 200       18      17      tunnel-lsp/4097
```

Communication between devices connected to both l2-fecs was verified using both ixia generated traffic and pc pings.

These configuration are additional options which increase the flexibility of using martini port/vlan l2-fecs.

LDP over LDP Martini Interoperability with Juniper - Using Port FEC

Xu Yang
Systems Engineering, China
July 27, 2002

This configuration example is from a successful test of Martini tunnels using LDP over LDP with a Juniper M5 & a RS8000 as the LERs, and Cisco 7206VXR as the LSR. This example is based on port FEC. For configuration example based on VLAN FEC, please refer to the paper titled 'LDP over LDP Martini Interoperability with Juniper – Using VLAN FEC'.

The RS supports the following types of layer 2 FECs.

RS L2-FEC	Description	Group ID	VC ID
VLAN	802.1Q VLAN		Value of VLAN ID
Customer-Id	Physical Port		Value of Customer-id configured
Customer-Id, VLAN	Physical Port, 802.1Q VLAN	Value of Customer-id configured	Value of VLAN ID

Juniper's port FEC works in a similar fashion as RS. It maps a physical port to virtual-circuit-id, which is equivalent to RS's customer-id, and Ethernet-ccc encapsulation needs to be configured. For VLAN FEC, it maps a VLAN to virtual-circuit-id, which is equivalent to RS's VLAN ID, and VLAN-ccc encapsulation needs to be configured. Juniper does not support port+VLAN FEC. However, they do support same VLAN ID on different physical port. It maps the same VLAN on different physical port to different virtual-circuit-id. It does not use Group ID.

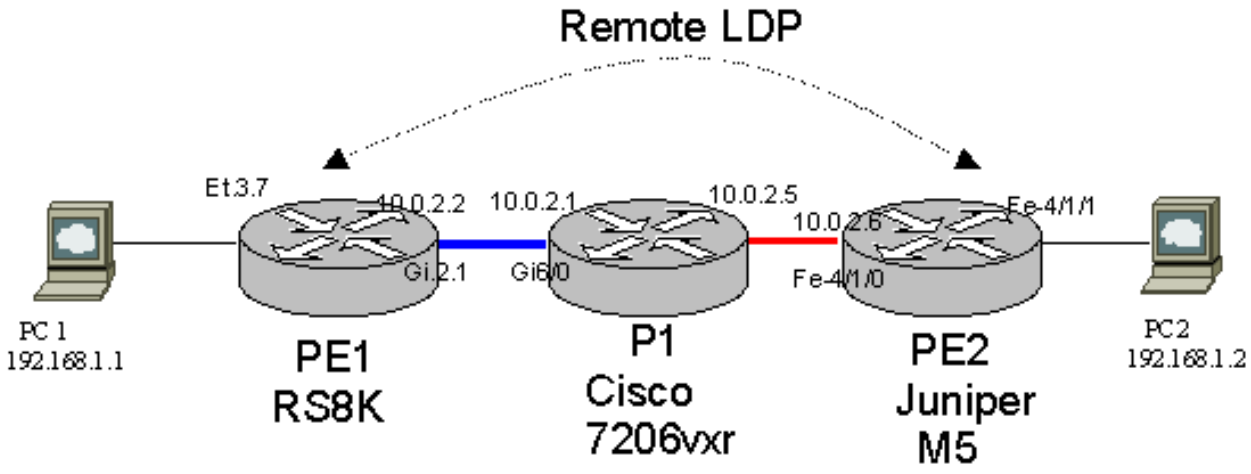
Juniper M5 was running Junos 5.3 R2.4, and Cisco 7206VXR was running 12.0.21 ST.

Due to time constrain, LDP over RSVP was not tested.

RapidOS Version Tested	9.0.0.3 / JUNOS 5.3R2.4 / IOS10.0.21ST
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0

Hardware Specifics	MPLS

Diagram



Configurations

PE1 - RS8K

```
port set et.3.7 auto-negotiation off duplex full speed 100mbps
interface create ip toP1 address-netmask 10.0.2.2/30 port gi.2.1
interface add ip lo0 address-netmask 10.0.1.11/32
ip-router global set router-id 10.0.1.11
isis add area 49.0001
isis add interface toP1
isis add interface lo0
isis set system-id 0000.0000.0011
isis set wide-metrics-only
isis set level 2
isis set traffic-engineering on
isis start
mpls add interface toP1
mpls start
ldp add interface lo0
ldp add interface toP1
ldp map ports et.3.7 customer-id 100
ldp add remote-peer 10.0.1.12
ldp add l2-fec customer-id 100 to-peer 10.0.1.12
ldp start
system set name PE1
```

Note: Both Cisco and Juniper use IS-IS wide metrics. On RS, IS-IS traffic-engineering needs to be enabled to use IS-IS wide-metrics.

PE2 - Juniper M5

```
version 5.3R2.4;
system {
    host-name M5-2;
    root-authentication {
        encrypted-password "$1$0fVsZ$4N6tjjYiKvlYSTg.DFrAS1"; # SECRET-DATA
    }
    login {
        message Welcome;
        class lab {
            permissions all;
        }
        class test {
            permissions [ clear configure edit interface-control network routing
routing-control trace trace-control view ];
        }
        user lab {
            uid 2003;
            class lab;
            authentication {
                encrypted-password "$1$XXQ.5$twVip2HBLp/JkyVmRrVCX."; # SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
    syslog {
        file messages {
            any info;
        }
    }
}
interfaces {
    fe-0/0/0 {
        unit 0 {
            family inet {
                address 10.0.2.6/30;
            }
            family iso;
            family mpls;
        }
    }
    fe-0/0/1 {
        mtu 1500;
        encapsulation ethernet-ccc;
        unit 0;
    }
    lo0 {
```

```
        unit 0 {
            family inet {
                address 10.0.1.12/32;
            }
            family iso {
                address 49.0001.0000.0000.0012.00;
            }
        }
    }
}
protocols {
    mpls {
        interface fe-0/0/0.0;
    }
    isis {
        interface fe-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface fe-0/0/0.0;
        interface lo0.0;
    }
    l2circuit {
        neighbor 10.0.1.11 {
            interface fe-0/0/1.0 {
                virtual-circuit-id 100;
            }
        }
    }
}
```

P1 - Cisco7206vxr

```
version 12.0
hostname P1
!
boot system flash disk0:c7200-p-mz.120-21.ST1.bin
enable password cisco
!
ip subnet-zero
ip cef
!
mpls label protocol ldp
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
 no ip directed-broadcast
 ip router isis test
!
interface FastEthernet0/0
```

```
 ip address 10.0.2.5 255.255.255.252
 no ip directed-broadcast
 ip router isis test
 speed auto
 half-duplex
 tag-switching ip
!
interface GigabitEthernet6/0
 ip address 10.0.2.1 255.255.255.252
 no ip directed-broadcast
 ip router isis test
 negotiation auto
 tag-switching ip
!
router isis test
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
 metric-style wide
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Comments

PC1 and PC2 are on the same ip subnet, PC1 should ping PC2 successfully.

PE1 - RS8K

```
PE1# ldp show l2-fec

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 10.0.1.12:0

FEC                                 in-lbl  out-lbl Transport LSP name/label

Customer ID 100                     100009  20      LDP 10.0.1.12/17
Customer ID 100                     100009  20      LDP 10.0.1.12/17

PE1# ldp show database

Input label database, 10.0.1.11:0-10.0.1.12:0
  Label     Prefix
      3     10.0.1.12/32
```

```
 100005     10.0.2.0/30
 100005     10.0.1.1/32
 100006     10.0.1.11/32
 100009     Customer ID 100

Output label database, 10.0.1.11:0-10.0.1.12:0
  Label     Prefix
      3     10.0.1.11/32
     17     10.0.1.1/32
     18     10.0.2.4/30
     19     10.0.1.12/32
     20     Customer ID 100

Input label database, 10.0.1.11:0-10.0.1.1:0
  Label     Prefix
      3     10.0.2.0/30
      3     10.0.2.4/30
      3     10.0.1.1/32
     16     10.0.1.11/32
     17     10.0.1.12/32

Output label database, 10.0.1.11:0-10.0.1.1:0
  Label     Prefix
      3     10.0.1.11/32
     17     10.0.1.1/32
     18     10.0.2.4/30
     19     10.0.1.12/32
```

PE2 - Juniper M5

```
PE2-M5# run show ldp database extensive
Input label database, 10.0.1.12:0--10.0.1.1:0
  Label     Prefix
     17     10.0.1.12/32
            State: Active
      3     10.0.1.1/32
            State: Active
      3     10.0.2.4/30
            State: Active
      3     10.0.2.0/30
            State: Active
     16     10.0.1.11/32
            State: Active

Output label database, 10.0.1.12:0--10.0.1.1:0
  Label     Prefix
 100011     10.0.1.11/32
            State: Active
      3     10.0.1.12/32
            State: Active
 100010     10.0.1.1/32
            State: Active
```

```
 100010     10.0.2.0/30
            State: Active

Input label database, 10.0.1.12:0--10.0.1.11:0
  Label     Prefix
     17     10.0.1.1/32
            State: Active
     19     10.0.2.4/30
            State: Active
      3     10.0.1.11/32
            State: Active
     18     10.0.1.12/32
            State: Active
     20     L2CKT ETHERNET VC 100
            State: Active

Output label database, 10.0.1.12:0--10.0.1.11:0
  Label     Prefix
 100011     10.0.1.11/32
            State: Active
      3     10.0.1.12/32
            State: Active
 100010     10.0.1.1/32
            State: Active
 100010     10.0.2.0/30
            State: Active
 100009     L2CKT ETHERNET VC 100
            State: Active

PE2-M5# run show l2circuit connections up-down
Layer-2 Circuit Connections:

Legend for connection status (St)   Legend for interface status
EI -- encapsulation invalid         UP -- operational
MM -- mtu mismatch                  Dn -- down
EM -- encapsulation mismatch        NP -- no present
OL -- no outgoing label             DS -- disabled
Dn -- down                          WE -- wrong encapsulation
VC-Dn -- Virtual circuit Down       UN -- uninitialized
UP -- operational
XX -- unknown

Neighbor: 10.0.1.11
    Interface                 Type  St     Time last up          # Up trans
    fe-0/0/1.0 (vc 100)       rmt   Up     Jul 25 14:19:06 2002           5
      Local interface: fe-0/0/1.0, Status: Up, Encapsulation: ETHERNET
      Remote PE: 10.0.1.11
      Incoming label: 100009, Outgoing label: 20
```

P1 - Cisco7206vxr

```
P1#show mpls ldp bindings
```

```
tib entry: 10.0.1.1/32, rev 18
      local binding:  tag: imp-null
      remote binding: tsr: 10.0.1.11:0, tag: 17
      remote binding: tsr: 10.0.1.12:0, tag: 100005
tib entry: 10.0.1.11/32, rev 218
      local binding:  tag: 16
      remote binding: tsr: 10.0.1.11:0, tag: imp-null
      remote binding: tsr: 10.0.1.12:0, tag: 100006
tib entry: 10.0.1.12/32, rev 220
      local binding:  tag: 17
      remote binding: tsr: 10.0.1.11:0, tag: 19
      remote binding: tsr: 10.0.1.12:0, tag: imp-null
tib entry: 10.0.2.0/30, rev 216
      local binding:  tag: imp-null
      remote binding: tsr: 10.0.1.12:0, tag: 100005
tib entry: 10.0.2.4/30, rev 214
      local binding:  tag: imp-null
      remote binding: tsr: 10.0.1.11:0, tag: 18
```

LDP over LDP Martini Interoperability with Juniper - Using VLAN FEC

Xu Yang
Systems Engineering, China
July 27, 2002

This configuration example is from a successful test of Martini tunnels using LDP over LDP with a Juniper M5 & RS8000 as the LERs, and Cisco 7206VXR as the LSR. This example is based on VLAN FEC. For configurations based on port FEC, please refer to the paper titled 'LDP over LDP Martini Interoperability with Juniper – Using Port FEC'.

The RS supports the following types of layer two FECs.

RS L2-FEC	Description	Group ID	VC ID
VLAN	802.1Q VLAN		Value of VLAN ID
Customer-Id	Physical Port		Value of Customer-id configured
Customer-Id, VLAN	Physical Port, 802.1Q VLAN	Value of Customer-id configured	Value of VLAN ID

Juniper's port FEC works in a similar fashion as RS. It maps a physical port to virtual-circuit-id, which is equivalent to RS's customer-id, and Ethernet-ccc encapsulation needs to be configured. For VLAN FEC, it maps a VLAN to virtual-circuit-id, which is equivalent to RS's VLAN ID, and VLAN-ccc encapsulation needs to be configured. Juniper does not support port+VLAN FEC. However, they do support same VLAN ID on different physical port. It maps the same VLAN on different physical port to different virtual-circuit-id. It does not use Group ID.

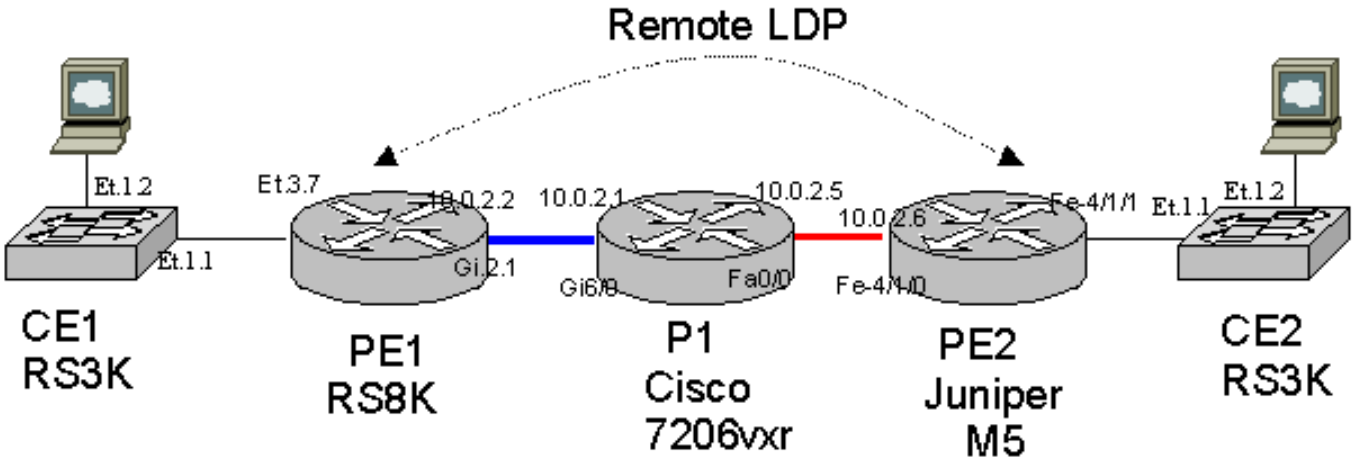
Juniper M5 was running Junos 5.3 R2.4, and Cisco 7206VXR was running 12.0.21 ST.

Due to time constrain, LDP over RSVP was not tested.

RapidOS Version Tested	9.0.0.3 / JUNOS 5.3R2.4 / IOS10.0.21ST
RapidOS Versions Working with this Configuration	8.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.0.0

Hardware Specifics	MPLS

Diagram



Configurations

PE1 - RS8K

```
vlan make trunk-port et.3.7
vlan make trunk-port gi.2.1
vlan create 600 port-based id 600
vlan create toP1 port-based id 10
vlan add ports et.3.7 to 600
vlan add ports gi.2.1 to toP1
vlan add ports gi.2.1 to 600
interface create ip toP1 address-netmask 10.0.2.2/30 vlan toP1
interface add ip lo0 address-netmask 10.0.1.11/32
ip-router global set router-id 10.0.1.11
isis add area 49.0001
isis add interface toP1
isis add interface lo0
isis set system-id 0000.0000.0011
isis set wide-metrics-only
isis set level 2
isis set traffic-engineering enable
isis start
mpls add interface toP1
mpls start
ldp add interface lo0
ldp add interface toP1
ldp add remote-peer 10.0.1.12
ldp add l2-fec vlan 600 to-peer 10.0.1.12
ldp start
```

```
system set name PE1
```

Note: Both Cisco and Juniper use IS-IS wide metrics. On RS, IS-IS traffic-engineering needs to be enabled to use IS-IS wide-metrics.

PE2 - Juniper M5

```
version 5.3R2.4;
system {
    host-name M5-2;
    root-authentication {
        encrypted-password "$1$0fVsZ$4N6tjjYiKvlYSTg.DFrAS1"; # SECRET-DATA
    }
    login {
        message Welcome;
        class lab {
            permissions all;
        }
        class test {
            permissions [ clear configure edit interface-control network routing
routing-control trace trace-control view ];
        }
        user lab {
            uid 2003;
            class lab;
            authentication {
                encrypted-password "$1$XXQ.5$twVip2HBLp/JkyVmRrVCX."; # SECRET-DATA
            }
        }
    }
    services {
        ftp;
        telnet;
    }
    syslog {
        file messages {
            any info;
        }
    }
}
interfaces {
    fe-0/0/0 {
        unit 0 {
            family inet {
                address 10.0.2.6/30;
            }
            family iso;
            family mpls;
        }
    }
    fe-0/0/1 {
        vlan-tagging;
```

```
        mtu 1500;
        encapsulation vlan-ccc;
        unit 600 {
            encapsulation vlan-ccc;
            vlan-id 600;
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.1.12/32;
            }
            family iso {
                address 49.0001.0000.0000.0012.00;
            }
        }
    }
}
protocols {
    mpls {
        interface fe-0/0/0.0;
    }
    isis {
        interface fe-0/0/0.0;
        interface lo0.0;
    }
    ldp {
        interface fe-0/0/0.0;
        interface lo0.0;
    }
    l2circuit {
        traceoptions {
            file l2cir;
            flag all detail;
        }
        neighbor 10.0.1.11 {
            interface fe-0/0/1.600 {
                virtual-circuit-id 600;
            }
        }
    }
}
```

P1 - Cisco7206vxr

```
version 12.0
hostname P1
!
boot system flash disk0:c7200-p-mz.120-21.ST1.bin
enable password cisco
!
ip subnet-zero
```

```
ip cef
!
mpls label protocol ldp
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
 no ip directed-broadcast
 ip router isis test
!
interface FastEthernet0/0
 ip address 10.0.2.5 255.255.255.252
 no ip directed-broadcast
 ip router isis test
 speed auto
 half-duplex
 tag-switching ip
!
interface GigabitEthernet6/0
 no ip address
 no ip directed-broadcast
 negotiation auto
 tag-switching ip
!
interface GigabitEthernet6/0.10
 encapsulation dot1Q 10
 ip address 10.0.2.1 255.255.255.252
 no ip directed-broadcast
 ip router isis test
 tag-switching ip
!
router isis test
 net 49.0001.0000.0000.0001.00
 is-type level-2-only
 metric-style wide
!
ip classless
!
line con 0
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

CE1 - RS3K

```
vlan make trunk-port et.1.1
vlan create 600 port-based id 600
vlan add ports et.1.1 to 600
vlan add ports et.1.2 to 600
```

```
system set name CE1
```

CE2 - RS3K

```
vlan make trunk-port et.1.1
vlan create 600 port-based id 600
vlan add ports et.1.1 to 600
vlan add ports et.1.2 to 600
system set name CE2
```

Comments

2 PCs connect to the CE should ping each other successfully.

PE1 - RS8K

```
PE1# ldp show database

Input label database, 10.0.1.11:0-10.0.1.1:0
  Label     Prefix
      3     10.0.2.0/30
      3     10.0.2.4/30
      3     10.0.1.1/32
     16     10.0.1.11/32
     17     10.0.1.12/32

Output label database, 10.0.1.11:0-10.0.1.1:0
  Label     Prefix
      3     10.0.1.11/32
     18     10.0.1.1/32
     19     10.0.2.4/30
     20     10.0.1.12/32

Input label database, 10.0.1.11:0-10.0.1.12:0
  Label     Prefix
      3     10.0.1.12/32
 100000     VLAN ID 600
 100000     VLAN ID 600
 100012     10.0.2.0/30
 100012     10.0.1.1/32
 100015     10.0.1.11/32

Output label database, 10.0.1.11:0-10.0.1.12:0
  Label     Prefix
      3     10.0.1.11/32
     17     VLAN ID 600
     18     10.0.1.1/32
     19     10.0.2.4/30
     20     10.0.1.12/32

PE1# ldp show l2-fec
```

```
FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 10.0.1.12:0

FEC                                 in-lbl  out-lbl Transport LSP name/label

VLAN ID 600                         100000  17      LDP 10.0.1.12/17
VLAN ID 600                         100000  17      LDP 0.0.0.0/17

PE1# vlan show
VID  VLAN Name      Used for                              Ports
---  -------------  ------------------------------------ ----------------------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         gi.2.(1-2), et.3.(1-16)
10   toP1           IP,IPX,ATALK,DEC,SNA,IPv6,L2         gi.2.1
600  600            IP,IPX,ATALK,DEC,SNA,IPv6,L2         gi.2.1, et.3.7
```

PE2 - Juniper M5

```
PE2-M5# run show ldp database
Input label database, 10.0.1.12:0--10.0.1.1:0
  Label     Prefix
     17     10.0.1.12/32
      3     10.0.1.1/32
      3     10.0.2.4/30
      3     10.0.2.0/30
     16     10.0.1.11/32

Output label database, 10.0.1.12:0--10.0.1.1:0
  Label     Prefix
 100015     10.0.1.11/32
 100012     10.0.1.1/32
 100012     10.0.2.0/30
      3     10.0.1.12/32

Input label database, 10.0.1.12:0--10.0.1.11:0
  Label     Prefix
     18     10.0.1.1/32
      3     10.0.1.11/32
     20     10.0.1.12/32
     19     10.0.2.4/30
     17     L2CKT VLAN VC 600

Output label database, 10.0.1.12:0--10.0.1.11:0
  Label     Prefix
 100015     10.0.1.11/32
 100012     10.0.1.1/32
 100012     10.0.2.0/30
      3     10.0.1.12/32
 100000     L2CKT VLAN VC 600
```

P1 - Cisco7206vxr

```
P1#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     10.0.1.11/32     276051     Gi6/0.10   10.0.2.2
17     Pop tag     10.0.1.12/32     337463     Fa0/0      10.0.2.6
```

CE1 - RS3K

```
CE1# vlan show
VID  VLAN Name      Used for                              Ports
---  -------------  ------------------------------------ ----------------------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,3-16), et.2.(1-16),
NP.4.(1-2)
600  600            IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-2)
```

CE2 - RS3K

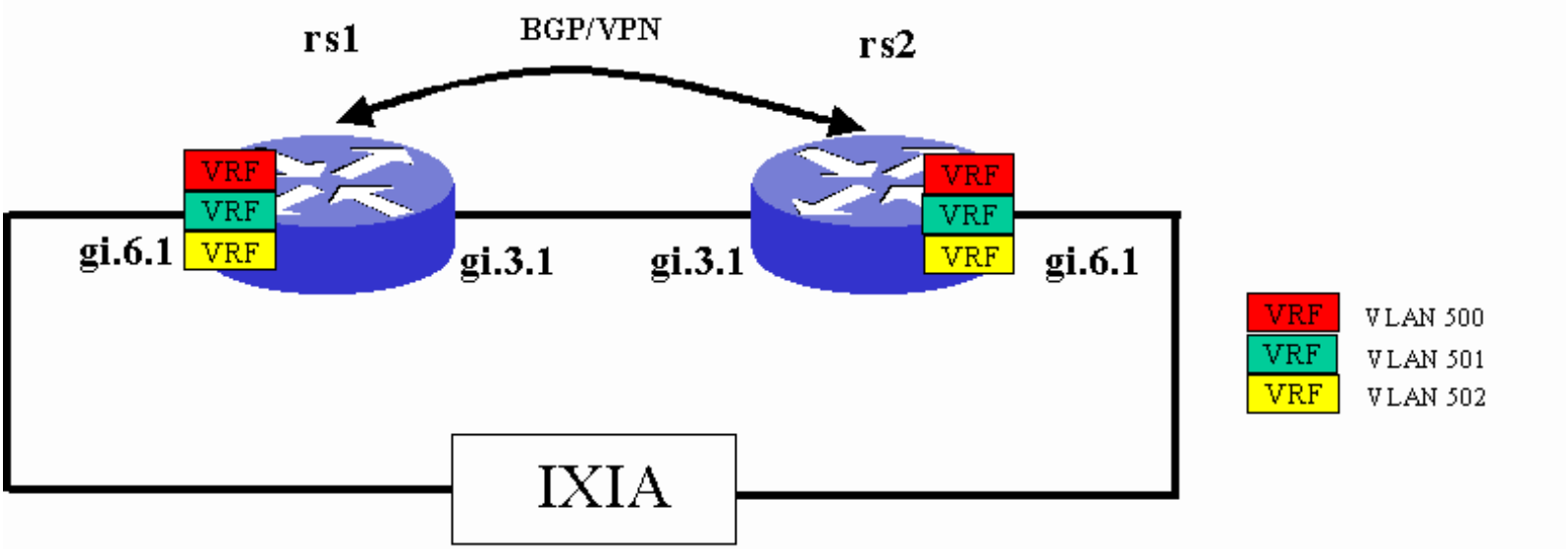
```
CE2# vlan show
VID  VLAN Name      Used for                              Ports
---  -------------  ------------------------------------ ----------------------
1    DEFAULT        IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1,3,5-16), et.2.(1-
16), NP.4.(1-2)
600  600            IP,IPX,ATALK,DEC,SNA,IPv6,L2         et.1.(1-2)
```

Multi-VRF Support With BGP/VPNs

Ian Cowburn
PSE, EMEA
January 7, 2003

This example shows the configuration required to support multiple customer vrfs on the same physical port when using BGP/VPNs (rfc2547bis).	
RapidOS Version Tested	9.3.0.0
RapidOS Versions Working with this Configuration	9.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.3.0.0
Hardware Specifics	This required the use of "v5" asics.

Diagram



Configurations

rs1

```
vlan make trunk-port gi.6.1 exclude-default-vlan
vlan create link1 ip id 10
vlan create-range 500-502 port-based
vlan add ports gi.3.1 to link1
port enable multi-vrf-support port gi.6.1 overwrite destination-socket
vlan add-to-vlan-range ports gi.6.1 to 500-502
interface create ip link1 address-netmask 11.1.0.1/30 vlan link1
interface create ip int500 address-netmask 10.0.1.1/30 vlan 500
interface create ip int501 address-netmask 10.0.2.1/30 vlan 501
interface create ip int502 address-netmask 10.0.3.1/30 vlan 502
interface add ip en0 address-netmask 192.168.254.40/24
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes bgp
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 2.2.2.2 group provider
bgp set peer-group provider local-address 1.1.1.1
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface link1
mpls start
ldp add interface link1
ldp start
system set name PE1
system set location home
system set idle-timeout serial 0 telnet 0
routing-instance vrf1 vrf set route-distinguisher "100:500"
routing-instance vrf1 vrf set community "100:500"
routing-instance vrf1 vrf add interface int500
routing-instance vrf1 ip add route 101.0.1.0/24 gateway 10.0.1.2
routing-instance vrf1 ip add route 101.0.2.0/24 gateway 10.0.1.2
routing-instance vrf2 vrf set route-distinguisher "100:501"
routing-instance vrf2 vrf set community "100:501"
routing-instance vrf2 vrf add interface int501
routing-instance vrf2 ip add route 101.0.1.0/24 gateway 10.0.2.2
routing-instance vrf2 ip add route 101.0.2.0/24 gateway 10.0.2.2
routing-instance vrf3 vrf set route-distinguisher "100:502"
routing-instance vrf3 vrf set community "100:502"
routing-instance vrf3 vrf add interface int502
routing-instance vrf3 ip add route 101.0.1.0/24 gateway 10.0.3.2
routing-instance vrf3 ip add route 101.0.2.0/24 gateway 10.0.3.2
```

rs2

```
vlan make trunk-port gi.6.1 exclude-default-vlan
vlan create link1 ip id 10
vlan create-range 500-502 port-based
vlan add ports gi.3.1 to link1
port enable multi-vrf-support port gi.6.1 overwrite destination-socket
vlan add-to-vlan-range ports gi.6.1 to 500-502
interface create ip link1 address-netmask 11.1.0.2/30 vlan link1
interface create ip int500 address-netmask 10.1.1.1/30 vlan 500
```

```
interface create ip int501 address-netmask 10.1.2.1/30 vlan 501
interface create ip int502 address-netmask 10.1.3.1/30 vlan 502
interface add ip lo0 address-netmask 2.2.2.2/32
interface add ip en0 address-netmask 192.168.254.50/24
ip-router global set router-id 2.2.2.2
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes bgp
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 1.1.1.1 group provider
bgp set peer-group provider local-address 2.2.2.2
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface link1
mpls start
rsvp start
ldp add interface link1
ldp start
system set name PE2
system set idle-timeout serial 0 telnet 0
routing-instance vrf1 vrf set route-distinguisher "100:500"
routing-instance vrf1 vrf set community "100:500"
routing-instance vrf1 vrf add interface int500
routing-instance vrf1 ip add route 101.1.1.0/24 gateway 10.1.1.2
routing-instance vrf1 ip add route 101.1.2.0/24 gateway 10.1.1.2
routing-instance vrf2 vrf set route-distinguisher "100:501"
routing-instance vrf2 vrf set community "100:501"
routing-instance vrf2 vrf add interface int501
routing-instance vrf2 ip add route 101.1.1.0/24 gateway 10.1.2.2
routing-instance vrf2 ip add route 101.1.2.0/24 gateway 10.1.2.2
routing-instance vrf3 vrf set route-distinguisher "100:502"
routing-instance vrf3 vrf set community "100:502"
routing-instance vrf3 vrf add interface int502
routing-instance vrf3 ip add route 101.1.1.0/24 gateway 10.1.3.2
routing-instance vrf3 ip add route 101.1.2.0/24 gateway 10.1.3.2
```

Comments

When using line cards with pre-v5 asics, the IP flow information used to switch traffic does not contain vlan information for the incoming traffic. Consequently, if three IP flows enter the same port, but on different vlans, they will be treated as the same flow. This is not an issue where the IP addressing information is unique, or when NAT is used.

BGP/VPNs support multiple VPN Routing and Forwarding tables (VRFs) with over-lapping address spaces, i.e. multiple customers can have the same IP address space. If multiple VRFs are configured with IP interfaces on different VLANs on the same physical port, we have the possibility of having different customer IP flows which are only distinguishable by the vlan id on which they are received. This brings us the constraint mentioned above for the pre-v5 asics.

A new command has been added in ros9300 to enable the use of multiple vrfs on a single port, using over-lapping address spaces. This is configured with line cards using v5 asics (and later), and allows the vlan information to be included in the IP flow information.

```
port enable multi-vrf-support port gi.6.1 overwrite destination-socket
```

The command uses new functionality in the v5+ asics to overwrite either the source or destination socket information in the IP flows with the vlan information. This keeps the IP flows unique with respect to the incoming vlans. Note that the information that is overwritten is still usable for controlling traffic, e.g. if you overwrite the destination socket then, for example, it is still possible have an acl deny access based on the destination

socket. However, if you are using dynamic NAT for the traffic from a vrf to, say, the Internet, you should overwrite the destination socket and as NAT uses the source socket to identify the incoming connection.

The diagram and configuration show two rs's acting as BGP/VPN PE's. On port gi.6.1 of each PE there are 3 vrfs defined, on vlans 500 through 502. The example is using static routes within the vrfs, but the logic is applicable when using any CE-PE protocol.

The IXIA sends bi-direction traffic between 101.0.1.2 and 101.1.1.2 in each of the vrfs, i.e. in vlans 500, 501 and 502.

When you enable the multi-vrf-support, the following message is printed

```
%SYS-I-ENABLEMULTIVRF, Multi VRF support overwriting destination socket is enabled on
port gi.6.1.
```

If the line card is pre-v5, then the command will error and this message is printed

```
%CLI-E-FAILED, Execution failed for "port enable multi-vrf-support port gi.4.1
overwrite d>estination-socket"
%SYS-E-ENABLEMULTIVRF, Cannot enable multi VRF support overwriting destination socket
on port gi.4.1.
```

If we look at the IP flow information *without* the multi-vrf-support command

```
PE1? debug l3 l3t-decode channel 6
Hash  PEnty Src Addr        Dst Addr        SSock DSock Pr TOS NextHopMAC
ExitPorts Pkts
----- ----- --------        --------        ----- ----- -- --- ----------    ---------
----
32    97    101.0.1.2       101.1.1.2       63    63    17 0   00001d:cc75bd gi.3.1
9467
```

Although there are three IP streams, only one IP flows is seen. At the egress, all of the traffic is sent out to the same vrf.

If we configure the *multi-vrf-support*, then we can see each IP flow

```
PE1? debug l3 l3t-decode channel 6
Hash  PEnty Src Addr        Dst Addr        SSock DSock Pr TOS NextHopMAC
ExitPorts Pkts
----- ----- --------        --------        ----- ----- -- --- ----------    ---------
----
489   97    101.0.1.2       101.1.1.2       63    502   17 0   00001d:cc75bd gi.3.1
59181
490   97    101.0.1.2       101.1.1.2       63    501   17 0   00001d:cc75bd gi.3.1
59197
491   97    101.0.1.2       101.1.1.2       63    500   17 0   00001d:cc75bd gi.3.1
59279
```

Note that the destination socket information has been overwritten with the vlan ids, keeping the flows unique. The three IP flows are then sent out of the correct vrfs.

In order to determine whether a line card has v5+ asics, enter the following command

```
PE1# system show hardware slot 6

Slot Information
  Slot     6,  Module: 2-Gigabit "T" (GBIC)  Rev. 5.1
    Port:   gi.6.1,  Media Type: GBIC-Gigabit-SX,  Physical Port: 97
    Port:   gi.6.2,  Media Type: GBIC-Gigabit-SX,  Physical Port: 101
PE1# system show hardware slot 6 verbose
```

```
Slot Information
  Slot     6,  Module: 2-Gigabit "T" (GBIC)  Rev. 5.1
     Service String: 93_H2.0_16_SI4.0_16_SO2.2_16_32
     SIPP Information:
          Memory : 2 Banks @ 8388608 bytes each (Total 16777216)
          PIT Memory: 16777216
     SOPP Information:
          Memory : 33554432 bytes
    Port:   gi.6.1,  Media Type: GBIC-Gigabit-SX,  Physical Port: 97
     Hydra MAC Information:
          Table Memory:  16777216 bytes
          Packet Memory: 16777216 bytes
    Port:   gi.6.2,  Media Type: GBIC-Gigabit-SX,  Physical Port: 101
     Hydra MAC Information:
          Table Memory:  16777216 bytes
          Packet Memory: 16777216 bytes
```

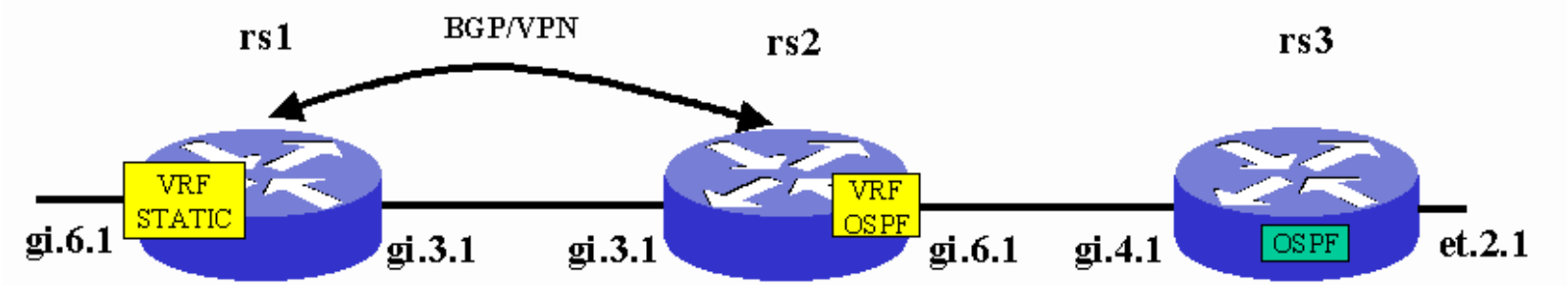
For v5 asic line cars, the "SI" field in the *ServiceString* must be at least 4.0.

BGP/VPNs With Different CE-PE Protocols at Different Sites

Ian Cowburn
PSE, EMEA
January 7, 2003

Using BGP/VPNs it is possible to configure the network using different CE-PE protocols at each customer site and have all of the routing information be propagated via BGP to each site. This example shows two sites of the same customer. One site is using static routes and the other is using OSPF as the CE-PE protocol. The routes for the two sites are propagated via BGP to the remote vrf and sites (in the case where OSPF connects rs3).	
RapidOS Version Tested	9.3.0.0
RapidOS Versions Working with this Configuration	9.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.3.0.0
Hardware Specifics	MPLS

Diagram



Configurations

PE1

```
vlan make trunk-port gi.6.1 exclude-default-vlan
vlan create link1 ip id 10
vlan create-range 500-502 port-based
vlan add ports gi.3.1 to link1
vlan add-to-vlan-range ports gi.6.1 to 500-502
interface create ip link1 address-netmask 11.1.0.1/30 vlan link1
```

```
interface create ip int500 address-netmask 10.0.1.1/30 vlan 500
interface add ip en0 address-netmask 192.168.254.40/24
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes bgp
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 2.2.2.2 group provider
bgp set peer-group provider local-address 1.1.1.1
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface link1
mpls start
ldp add interface link1
ldp start
system set name PE1
system set location home
system set idle-timeout serial 0 telnet 0
routing-instance vrf1 vrf set route-distinguisher "100:500"
routing-instance vrf1 vrf set community "100:500"
routing-instance vrf1 vrf add interface int500
routing-instance vrf1 ip add route 101.0.1.0/24 gateway 10.0.1.2
routing-instance vrf1 ip add route 101.0.2.0/24 gateway 10.0.1.2
```

PE2

```
vlan make trunk-port gi.6.1 exclude-default-vlan
vlan create link1 ip id 10
vlan create 501 port-based
vlan add ports gi.3.1 to link1
vlan add ports gi.6.1 to 501
interface create ip link1 address-netmask 11.1.0.2/30 vlan link1
interface create ip int501 address-netmask 10.1.2.1/30 vlan 501
interface add ip lo0 address-netmask 2.2.2.2/32
interface add ip en0 address-netmask 192.168.254.50/24
ip-router global set router-id 2.2.2.2
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes bgp
route-map ospf-routes-out permit 10 match-route-type bgp
ospf create area backbone
ospf add interface link1 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 1.1.1.1 group provider
bgp set peer-group provider local-address 2.2.2.2
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface link1
mpls start
ldp add interface link1
ldp start
system set name PE2
system set idle-timeout serial 0 telnet 0
routing-instance vrf1 vrf set route-distinguisher "100:500"
routing-instance vrf1 vrf set community "100:500"
routing-instance vrf1 vrf add interface int501
```

```
routing-instance vrf1 ospf create area backbone
routing-instance vrf1 ospf add interface int501 to-area backbone
routing-instance vrf1 ospf start
routing-instance vrf1 ospf set route-map-vpn ospf-routes-out
```

rs3

```
vlan make trunk-port gi.4.1 exclude-default-vlan
vlan create 501 port-based
vlan add ports gi.4.1 to 501
interface create ip int501 address-netmask 10.1.2.2/30 vlan 501
interface create ip lan address-netmask 201.1.1.1/24 port et.2.1
ip-router global set router-id 3.3.3.3
ospf create area backbone
ospf add interface int501 to-area backbone
ospf add interface lan to-area backbone
ospf start
system set name rs3
system set idle-timeout serial 0 telnet 0
```

Comments

vrf1 is configured on rs1 and rs2 for a particular customer. The VRF on rs1 uses static routes while the VRF on rs2 uses OSPF. A third rs, rs3, is connected to rs2 and injects a route into vrf1 on rs2 using OSPF.

The routing information in vrf1 is propagated between rs1 and rs2 via BGP.

If we look at the routing information of each rs we see:

```
PE1# ip show routes show-vrf vrf1

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.0.1.0/30          directly connected   -         int500
10.1.2.0/30          11.1.0.2             BGP       link1
101.0.1.0/24         10.0.1.2             Static    int500
101.0.2.0/24         10.0.1.2             Static    int500
127.0.0.1            127.0.0.1            -         lo0
201.1.1.0/24         11.1.0.2             BGP       link1
```

Here we see the locally connected networks and the two locally defined static routes, plus 10.1.2.0/30 from the remote vrf1 (on rs2) together with the route 201.1.1/24 that rs2 has learnt from rs3 via OSPF.

On rs2 we see

```
PE2# ip show routes show-vrf vrf1

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.0.1.0/30          11.1.0.1             BGP       link1
10.1.2.0/30          directly connected   -         int501
101.0.1.0/24         11.1.0.1             BGP       link1
101.0.2.0/24         11.1.0.1             BGP       link1
127.0.0.1            127.0.0.1            -         lo0
201.1.1.0/24         10.1.2.2             OSPF      int501
```

Again we see the locally directly connected networks. We see 10.0.1.0/30 from the vrf1 on rs1, and the two static routes defined in vrf1 on rs1, 101.0.1.0/24 and 101.0.2.0/24. Finally, we see the OSPF route learnt by OSPF from rs3, 201.1.1.0/24.

On rs3 we see

```
rs3# ip show routes

Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.0.1.0/30          10.1.2.1             OSPF_ASE  int501
10.1.2.0/30          directly connected   -         int501
101.0.1.0/24         10.1.2.1             OSPF_ASE  int501
101.0.2.0/24         10.1.2.1             OSPF_ASE  int501
127.0.0.1            127.0.0.1            -         lo0
201.1.1.0/24         directly connected   -         lan
```

As above, there are the directly connected networks, plus the networks learnt via rs2 from rs1, these being the directly connected interface on rs1 and the two static routes. Note that these routes are seen as OSPF_ASE, as defined by draft-rosen-vpns-ospf-bgp-mpls-04.txt.

L2 VPNs Over a L3 VPN Core

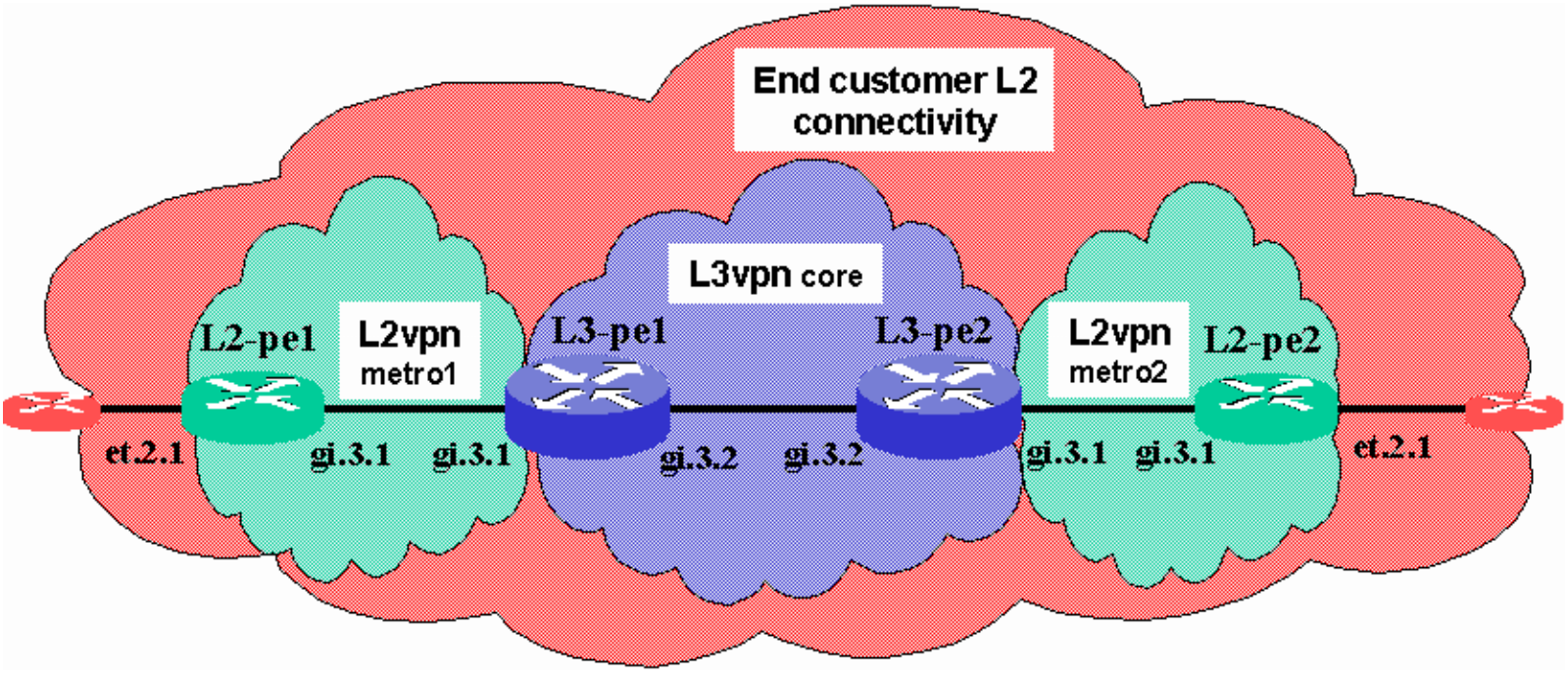
Ian Cowburn
European Product Engineer
April 19, 2003

This document describes a mechanism for tunneling L2 vpns over a L3 vpn core.

L2 vpns, using martini/TLS implemented in a metro, can be tunneled over a L3 vpn core based on rfc2547bis. The L2 vpn must be configured with LDP-over-LDP, i.e. the tunnel LSP is based on LDP. This allows the tunnel LSP to be extended across the core by using the Carrier's Carrier feature within 2547.

RapidOS Version Tested	9.3.0.1
RapidOS Versions Working with this Configuration	9.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.3.0.0
Hardware Specifics	Requires MPLS line cards.

Diagram



Configurations

L2-pe1

```
vlan make trunk-port gi.3.1 exclude-default-vlan
vlan make trunk-port et.2.1
vlan create 10 port-based id 10
vlan create to-provider id 4001
vlan add ports et.2.1 to 10
vlan add ports gi.3.1 to to-provider
interface create ip to-provider address-netmask 11.1.0.2/30 vlan to-provider
interface add ip lo0 address-netmask 1.1.1.1/32
interface add ip en0 address-netmask 192.168.254.40/24
ip-router global set router-id 1.1.1.1
ospf create area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf add interface to-provider to-area backbone
ospf start
mpls add interface to-provider
mpls set customer-profile cust1 customer_id 10 in-port-list et.2.1 vlans 10 type port-vlan
mpls start
ldp add interface lo0
ldp add interface to-provider
ldp add remote-peer 2.2.2.2
ldp connect customer-profile cust1 remote-peer 2.2.2.2
ldp start
system set name L2-pe1
system set idle-timeout serial 0 telnet 0
```

L3-pe1

```
vlan make trunk-port gi.3.2 exclude-default-vlan
vlan create 4001 port-based id 4001
vlan create link ip id 20
vlan add ports gi.3.1 to 4001
vlan add ports gi.3.2 to link
interface create ip to-metro1 address-netmask 11.1.0.1/30 vlan 4001
interface create ip link address-netmask 11.11.0.1/30 vlan link
interface add ip lo0 address-netmask 3.3.3.3/32
interface add ip en0 address-netmask 192.168.254.70/24
ip-router global set router-id 3.3.3.3
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes on
route-map ospf-out permit 10 match-route-type bgp
ospf create area backbone
ospf add stub-host 3.3.3.3 to-area backbone cost 10
ospf add interface link to-area backbone
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 4.4.4.4 group provider
bgp set peer-group provider local-address 3.3.3.3
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface to-metro1
mpls add interface link
mpls set interface to-metro1 no-php
mpls set interface link no-php
mpls set interface lo0 no-php
mpls start
ldp add interface to-metro1
ldp add interface link
ldp start
system set name L3-pe1
```

```
system set idle-timeout serial 0 telnet 0
routing-instance vrf3 vrf set route-distinguisher "2002:103"
routing-instance vrf3 ospf create area backbone
routing-instance vrf3 ospf start
routing-instance vrf3 vrf add interface to-metro1
routing-instance vrf3 ospf add interface to-metro1 to-area backbone
routing-instance vrf3 ospf set route-map-vpn ospf-out
routing-instance vrf3 vrf set community "target:2002:103"
```

L3-pe2

```
vlan make trunk-port gi.3.2 exclude-default-vlan
vlan create 4002 port-based id 4002
vlan create link ip id 20
vlan add ports gi.3.1 to 4002
vlan add ports gi.3.2 to link
interface create ip to-metro2 address-netmask 11.2.0.1/30 vlan 4002
interface create ip link address-netmask 11.11.0.2/30 vlan link
interface add ip en0 address-netmask 192.168.254.80/24
interface add ip lo0 address-netmask 4.4.4.4/32
ip-router global set router-id 4.4.4.4
ip-router global set autonomous-system 2002
ip-router global set install-lsp-routes on
route-map ospf-out permit 10 match-route-type bgp
ospf create area backbone
ospf add stub-host 4.4.4.4 to-area backbone cost 10
ospf add interface link to-area backbone
ospf start
bgp create peer-group provider autonomous-system 2002
bgp add peer-host 3.3.3.3 group provider
bgp set peer-group provider local-address 4.4.4.4
bgp set peer-group provider vpnv4-unicast ipv4-unicast
bgp start
mpls add interface to-metro2
mpls add interface link
mpls set interface to-metro2 no-php
mpls set interface link no-php
mpls set interface lo0 no-php
mpls start
ldp add interface to-metro2
ldp add interface link
ldp start
system set name L3-pe2
system set idle-timeout serial 0 telnet 0
routing-instance vrf3 vrf set route-distinguisher "2002:103"
routing-instance vrf3 ospf create area backbone
routing-instance vrf3 ospf start
routing-instance vrf3 vrf add interface to-metro2
routing-instance vrf3 ospf add interface to-metro2 to-area backbone
routing-instance vrf3 ospf set route-map-vpn ospf-out
routing-instance vrf3 vrf set community "target:2002:103"
```

L2-pe2

```
vlan make trunk-port gi.3.1 exclude-default-vlan
vlan make trunk-port et.2.1
vlan create 10 port-based id 10
vlan create to-provider ip id 4002
vlan add ports et.2.1 to 10
vlan add ports gi.3.1 to to-provider
interface create ip to-provider address-netmask 11.2.0.2/30 vlan to-provider
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf add interface to-provider to-area backbone
ospf start
```

```
mpls add interface to-provider
mpls set customer-profile cust1 customer_id 10 in-port-list et.2.1 vlans 10 type port-vlan
mpls start
ldp add interface lo0
ldp add interface to-provider
ldp add remote-peer 1.1.1.1
ldp connect customer-profile cust1 remote-peer 1.1.1.1
ldp start
system set name L2-pe2
system set idle-timeout serial 0 telnet 0
```

Comments

The two PE devices on the customer edge of the L2 metros are configured to provide an L2 vpn to a customer attached to port et.2.1 via a port-vlan TLS L2-fec.

```
mpls set customer-profile cust1 customer_id 10 in-port-list et.2.1 vlans 10 type port-vlan
ldp connect customer-profile cust1 remote-peer 1.1.1.1
```

The next hop ip interface from each L2 PE is to the adjacent L3 PE device. LDP is enabled on this interface to provide the tunnel LSP to the remote L2 PE.

NOTE: The Carrier's Carrier part of rfc2547bis does not support RSVP as the mechanism to send/receive MPLS labels to/from the L3 vpn customer, consequently LDP *must* be used as the TLS (in this example) tunnel LSP signaling mechanism.

```
interface create ip to-provider address-netmask 11.2.0.2/30 vlan to-provider
ldp add interface to-provider
```

The L3 VPN is transparent to the L2 PEs.

The L3 VPN core is configured to support rfc2547bis,

```
bgp set peer-group provider vpnv4-unicast ipv4-unicast
```

and a VRF is created on the L3 PEs which provides both routing (in this example via OSPF) and label switching between the two metros.

```
route-map ospf-out permit 10 match-route-type bgp
routing-instance vrf3 vrf set route-distinguisher "2002:103"
routing-instance vrf3 ospf create area backbone
routing-instance vrf3 ospf start
routing-instance vrf3 vrf add interface to-metro1
routing-instance vrf3 ospf add interface to-metro1 to-area backbone
routing-instance vrf3 ospf set route-map-vpn ospf-out
routing-instance vrf3 vrf set community "target:2002:103"
```

Note that LDP is enabled both on the link from each L3 PE to their adjacent L2 PE and between the two L3 PEs.

```
ldp add interface to-metro1
ldp add interface link
```

This allows the tunnel LSP from the L2 VPN to be extended across the L3 VPN.

NOTE: Penultimate-hop-popping has been disabled (via no-php) on the MPLS interfaces on the L3 VPN PEs, this was only done to show (below) that the MPLS frame switched between L3-pe1 and L3-pe2 has the correct three MPLS labels.

The final point to note about the L3 PE configuration is the setting of the following

```
ip-router global set install-lsp-routes on
```

This is required to enable BGP to resolve the next hop address in the "Internet Unicast" RIB, with its associated label (NOTE: the parameter here is "on", not "bgp").

We can now look at each device to see the status.

On the L2 PEs, we see the routing shows OSPF routes to the remote L2 PE lo0 address

```
L2-pe1# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              1.1.1.1              -         lo0
2.2.2.2              11.1.0.1             OSPF_IA   to-provider
11.1.0.0/30          directly connected   -         to-provider
11.2.0.0/30          11.1.0.1             OSPF_ASE  to-provider
127.0.0.1            127.0.0.1            -         lo0
192.168.254.0/24     directly connected   -         en0
```

The address to 2.2.2.2 in the above is an OSPF_IA route as it was received via the VRF on L3-pe1.

The L2-fec is signaled using LDP-over-LDP:

```
L2-pe1# ldp show l2-fec
FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent
Remote neighbor 2.2.2.2:0
FEC                                  in-lbl  out-lbl Transport LSP name/label
Customer ID 10, VLAN ID 10           19      19      LDP 2.2.2.2/22
```

Note that the tunnel is using LDP.

On the L3 PEs we have routes between the two PE devices and to the adjacent L2-pe in the Internet Unicast RIB

```
L3-pe1# ip show routes
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
3.3.3.3              3.3.3.3              -         lo0
4.4.4.4              11.11.0.2            OSPF      link
11.1.0.0/30          directly connected   -         to-metro1
11.11.0.0/30         directly connected   -         link
127.0.0.1            127.0.0.1            -         lo0
192.168.254.0/24     directly connected   -         en0
```

And we have routes to both L2 PE devices' lo0 in the RIB for vrf3:

```
L3-pe1# ip show routes show-vrf vrf3
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
1.1.1.1              11.1.0.2             OSPF      to-metro1
2.2.2.2              11.11.0.2            BGP       link
11.1.0.0/30          directly connected   -         to-metro1
11.2.0.0/30          11.11.0.2            BGP       link
127.0.0.1            127.0.0.1            -         lo0
```

We can see the LDP labels in use to get to the adjacent L2 PE lo0 and the adjacent L3 PE lo0:

```
L3-pe1# mpls show ip-binding
  11.2.0.0/30
        output label:   23            Active
        input label:    18            lsr: 1.1.1.1:0
 1.1.1.1/32
      input label:    imp-null      lsr: 1.1.1.1:0   inuse
 2.2.2.2/32
        output label:   22            Active
        input label:    17            lsr: 1.1.1.1:0
  3.3.3.3/32
```

```
        output label:   16            Active, Egress
        input label:    21            lsr: 4.4.4.4:0
  4.4.4.4/32
       output label:   21          Active
       input label:    16          lsr: 4.4.4.4:0   inuse
```

To complete the picture, on the L3 PEs we see the label received from its BGP peer (the other L3 PE) for the address to the lo0 on the remote L2 PE:

```
L3-pe1# bgp show routes all
Local router ID is 3.3.3.3
Status codes: > - best, * - valid, i - internal, t - stale
              s - suppressed, d - damped
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop        Metric LocPrf Label       Path
    -------             --------        ------ ------ ----------- ----
*> i2.2.2.2/32        4.4.4.4           13    100        20 i
*> i11.2.0.0/30       4.4.4.4                  100          17 i
```

Finally, this is an MPLS frame sent by L3-pe1 to L3-pe2 for traffic through the L2 vpn:

```
DLC:  ----- DLC Header -----
      DLC:
      DLC:  Frame 15191 arrived at  17:32:52.5736; frame size is 90 (005A hex) bytes.
      DLC:  Destination = Station 000285011FC0
      DLC:  Source      = Station 0002850116C0
      DLC:  Ethertype   = 8847 (MPLS)
      DLC:
MPLS: ----- MPLS Label Stack  -----
      MPLS:
     MPLS: Label Value               = 00010
      MPLS: Reserved For Experimental Use = 0
      MPLS: Stack Value                   = 0 (Label Stack Entry)
      MPLS: Time to Live                  = 254 (hops)
      MPLS:
     MPLS: Label Value               = 00014
      MPLS: Reserved For Experimental Use = 0
      MPLS: Stack Value                   = 0 (Label Stack Entry)
      MPLS: Time to Live                  = 254 (hops)
      MPLS:
     MPLS: Label Value               = 00013
      MPLS: Reserved For Experimental Use = 0
      MPLS: Stack Value                   = 1 (Bottom of Stack)
      MPLS: Time to Live                  = 255 (hops)
      MPLS:
```

Taking the labels in turn from the top of the stack:

Label 1 = 10(hex) = 16 = LDP label for L3-pe1 to get to the lo0 on L3-pe2 (with no-php in place)

Label 2 = 14(hex) = 20 = BGP label for L3-pe1 to get to 2.2.2.2 in vrf3 on L3-pe2

Label 3 = 13(hex) = 19 = LDP label for the vc-lsp on L2-pe1 to the corresponding L2-fec on L2-pe2

Extending "Virtual Switch" Domains
VPLS Configuration Series

Austin Hawthorne
Principal Systems Engineer
May 16, 2003

In the ‘Port Based "Virtual Switch" Configuration’ and ‘VLAN Based "Virtual Switch" Configuration’ documents the aspects of using the VPLS feature set to gain the capability of having multiple overlapping VLAN domains per switch were covered. Please review these documents for details of the service characteristics.

The capabilities exist within the VPLS feature set to extend these domains beyond a single switch. This will be accomplished by bridging the traffic onto MPLS LSPs and setting up the LSPs to signal each switch with the awareness necessary to differentiate traffic between virtual domains. This is covered in depth in the following IETF draft: *http://www.ietf.org/internet-drafts/draft-lasserre-vkompella-ppvpn-vpls-04.txt*.

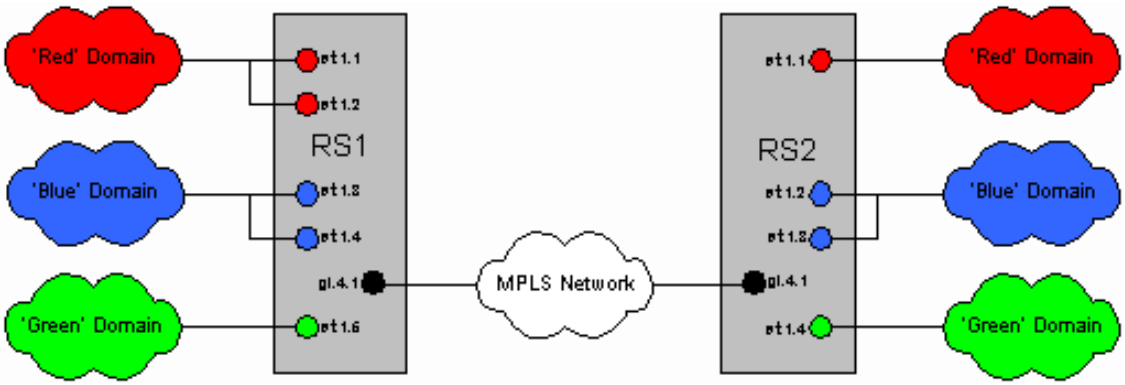
Comparisons can be made to 802.1Q. IEEE 802.1Q defined a set of standards that allowed a single LAN to be segmented into multiple Virtual LANs. These Virtual LANs (VLANs) could traverse multiple switches by being tagged with an added header signaling the VLAN membership of each frame. The same is true for VPLS. VPLS (Virtual Private LAN Services) allows for an added level of hierarchy to 802.1Q VLANs. Whereas the 4095 possible VLANs were of global significance, VPLS allows multiple VLAN domains, each consisting of up to 4095 VLANs each, to exist on the same network. VPLS adds an MPLS header to each frame, with the Label ID providing segmentation between the different VLAN domains. Also, LDP (Label Distribution Protocol) is used to signal a vc-id and group-id between VPLS peers to identify the label ID mapping to virtual domains.

VPLS will provide for a full-mesh loop-free topology between two or more switches, thereby extending multiple broadcast domains that are geographically dispersed. The culmination of all the edge switches and the MPLS core network appear to be as a single Ethernet switch to the end-users. The edge switches acting as the access ports and the MPLS network being the full-mesh fabric between ports. VPLS also allows a L2 Ethernet switched service to be created on top of a resilient and reliable IP/MPLS network core infrastructure. Spanning-Tree and GVRP are no longer necessary in the core and can be run transparently within each domain (To provide for backdoor links around the VPLS domain). IP routing protocols such as OSPF now can be used instead of STP to create a environment that is more resilient and reliable than those provided by spanning-tree, and without the problems of blocked links. Traffic Engineering extensions can be employed to provide a constraint-based method of controlling which paths traffic is allowed to traverse. RSVP can be used to signal not only primary Traffic-Engineered paths through the MPLS core, but also backup paths around failed nodes and failed paths with Sonet-like failover speed.

In this configuration example, the local switch examples in the documents stated above will be extended between two switches separated by an MPLS network. The specifics on the service activation configuration will not be discussed as they are detailed in the Port Based and VLAN Based Virtual Switch documents. Only the MPLS portions of the configuration will be detailed.

RapidOS Version Tested	9.3.0.1
RapidOS Versions Working with this Configuration	9.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.3.0.0
Hardware Specifics	Any PPP, Frame-Relay, Ethernet, Link Aggregation, ATM interface. MPLS line cards needed for network-facing interfaces.

Diagram



The above diagram depicts a common scenario where multiple virtual LAN domains have been configured on each switch. In the Blue and Green domain examples common domains exist on each switch (blue is a VLAN-based example, and Green is a Port-based example) and connectivity must be made between the switches to complete the broadcast domain connectivity. With the Red domain, some flexibility in VPLS is shown by having the Red domain on the right act as a satellite location with only 1 VLAN (100) coming in on an access port (untagged). This must be transported to the corporate HQ on the left, but must be sent to the HQ switches with am 802.1Q tag of 100. No other traffic must be sent to the satellite location.

NOTE: In VPLS there are usually two labels that are added to the Ethernet frames at the PE, one that signals the Tunnel LSP, and one for the VC LSP. Usually RSVP is used to signal a traffic engineered tunnel LSP hop by hop and LDP is used to signal a single VC LSP per customer-profile between the two or more PE's. In this example, only LDP will be covered because only two PEs will be used and no P routers exist. With PHP, the tunnel labels in this example would not be used. The use of RSVP will be covered in another document entitled 'RSVP with VPLS Configuration'. This will cover traffic-engineering, failover, redundancy, and path setup and teardown capabilities within RSVP.

Below is how we will configure the systems:

System	Name	Local/Remote/Both	VLANs	Peer
RS1	red-remote	both	100	RS2
RS1	red-default-local	local	1	

RS1	red-local	local	2-99,101-4000	
RS1	blue-default	both	1	RS2
RS1	blue-remote	both	2-4000	RS2
RS1	green-default	remote	all	RS2

Configurations

RS1

```
port disable et.1.(6-16) force-link-down
port disable et.2.(1-16) force-link-down
vlan make trunk-port et.1.(1-5)
vlan create-range 2-4000 port-based
!
!  Create an explicit VLAN for the IP interface to be used for MPLS signaling.  It is
!  required to set aside a group of VLANs for the IP interfaces used in VPLS.
!
vlan create ip4001 ip id 4001
vlan set native-vlan et.1.(1-2) all default
vlan set native-vlan et.1.(3-4) all default
vlan set native-vlan et.1.5 all default
!
!  Add the network facing port to the IP interface VLAN
!
vlan add ports gi.4.1 to ip4001
vlan add-to-vlan-range ports et.1.(1-2) to 2-4000
vlan add-to-vlan-range ports et.1.(3-4) to 2-4000
!
!  Create the IP interface between the two switches.  These switches are classified
as PE-rs
!  (provider-edge switch routers) or LER (Label Edge Routers) because they act as the
entry
!  point into the VPLS network.  As such they require an IP interface to signal the
MPLS
!  label information between each PE and any P (provider) or LSR (Label Switch
Routers)
!  that may exist in the network.  LDP and RSVP will use this interface for it's
transport.
!
interface create ip gi.4.1-to-rs2 address-netmask 172.16.1.1/30 vlan ip4001
interface add ip en0 address-netmask 192.168.0.12/24
!
!  For OSPF and LDP setup a global router-id and bind it to the loopback interface
```

```
!
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
!
!  Configure OSPF to provide IP level connectivity between nodes to be used for MPLS
!  signaling of label information
!
ospf create area backbone
ospf add interface gi.4.1-to-rs2 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
!
!  Add the network facing interfaces to the MPLS process.
!
mpls add interface gi.4.1-to-rs2
!
!  Create your customer-profiles.  Note that we have configured some locally switched
only
!  domains as well as some that require connectivity to the remote PE.  For example,
!  customer 'RED' requires that VLANs 2-4000 be switched locally between their two
member
!  ports, but that VLAN 100 be switched locally plus to the remote location.
!
!  It is important to note that each customer-id must be unique per VPLS and in most
cases
!  match the customer-id on the remote PEs.  See the 'Comments' section below for
more
!  details.
!
mpls set customer-profile red-remote customer_id 1 type port-vlan vlans 100 in-port-
list et.1.(1-2)
mpls set customer-profile red-default-local customer_id 2 type port-vlan vlans 1 in-
port-list et.1.(1-2)
mpls set customer-profile red-local customer_id 3 type port-vlan-range vlans
everything-else in-port-list et.1.(1-2)
mpls set customer-profile blue-default customer_id 4 type port-vlan vlans 1 in-port-
list et.1.(3-4)
mpls set customer-profile green-remote customer_id 6 type port in-port-list et.1.5
mpls set customer-profile blue-remote customer_id 5 type port-vlan-range vlans 2-4000
in-port-list et.1.(3-4)
!
!  Start the MPLS process.
!
mpls start
!
!  Add the interfaces that will be required to signal label information via LDP.  You
must
!  always include the loopback.
!
ldp add interface gi.4.1-to-rs2
ldp add interface lo0
!
!  Add the remote-peer(s) to the ldp process.
```

```
!
ldp add remote-peer 2.2.2.2
!
!  Instruct LDP to ‘connect’ the specified ‘customer-profile’ to the specified
‘remote-peer’
!  This will negotiate a label between peers that correlate label information to VPLS
!  forwarding instances.  For VLAN-Range type profiles the ‘vc-id’, which is the VPLS
!  identifier, must be specified.  See the ‘Comments’ section below for specifics.
!
!  The locally switches only profiles can be set for a remote-peer of 127.0.0.1.
!
ldp connect customer-profile red-remote remote-peer 2.2.2.2 vc-id 1 vc-type ethernet-
vlan
ldp connect customer-profile blue-default remote-peer 2.2.2.2 vc-id 4 vc-type
ethernet-vlan
ldp connect customer-profile green-remote remote-peer 2.2.2.2 vc-id 6 vc-type
ethernet
ldp connect customer-profile blue-remote remote-peer 2.2.2.2 vc-id 5 vc-type ethernet-
vlan
ldp connect customer-profile red-default-local remote-peer 127.0.0.1
ldp connect customer-profile red-local remote-peer 127.0.0.1 vc-id 3 vc-type ethernet-
vlan
ldp start
system set name rs1
system set idle-timeout telnet 0
stp tunnel mpls ports et.1.(1-5)
stp set vlan-disable port-list et.1.(1-4)
```

RS2

```
vlan make trunk-port et.1.(2-4)
vlan create-range 2-4000 port-based
vlan create ip4001 ip id 4001
vlan set native-vlan et.1.(2-3) all default
vlan set native-vlan et.1.4 all default
!
!  Note here that we have not configured the et.1.1 port as a trunk port (so it is
natively
!  untagged), yet on RS1 it is tagged.  With VPLS, local decisions on whether frames
will
!  be transmitted tagged or untagged are made locally through the VLAN statements.
Frames
!  are transmitted along the MPLS LSP as untagged for port-vlan type profiles.
!
vlan add ports et.1.1 to 100
vlan add ports gi.4.1 to ip4001
vlan add-to-vlan-range ports et.1.(2-3) to 2-4000
interface create ip gi.4.1-to-rs1 address-netmask 172.16.1.2/30 vlan ip4001
interface add ip en0 address-netmask 192.168.0.11/24
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add interface gi.4.1-to-rs1 to-area backbone
```

```
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
mpls add interface gi.4.1-to-rs1
mpls set customer-profile red-remote customer_id 1 type port-vlan vlans 100 in-port-
list et1.1
mpls set customer-profile blue-default customer_id 4 type port-vlan vlans 1 in-port-
list et1.(2-3)
mpls set customer-profile blue-remote customer_id 5 type port-vlan-range vlans 2-4000
in-port-list et.1.(2-3)
mpls set customer-profile green-remote customer_id 6 type port in-port-list et.1.4
mpls start
ldp add interface lo0
ldp add interface gi.4.1-to-rs1
ldp add remote-peer 1.1.1.1
ldp connect customer-profile red-remote remote-peer 1.1.1.1 vc-id 1 vc-type ethernet-
vlan
ldp connect customer-profile blue-default remote-peer 1.1.1.1 vc-id 4 vc-type
ethernet-vlan
ldp connect customer-profile blue-remote remote-peer 1.1.1.1 vc-id 5 vc-type ethernet-
vlan
ldp connect customer-profile green-remote remote-peer 1.1.1.1 vc-id 6 vc-type
ethernet
ldp start
system set name rs2
system set idle-timeout telnet 0
stp tunnel mpls ports et.1.(1-4)
stp set vlan-disable port-list et.1.(1-3)
```

Comments

The most important step in configuring VPLS is the assignment of the vc-id and group-id. This value must be global and must be configured to be the same among all PE's per VPLS profile. The RS a default behavior for assigning these values, but in many instances these values must be assigned statically. Below is a chart that details the default behavior for assigning these values.

VPLS Type	**VC-Type**	**VC-ID**	**Group-ID**
Port	Ethernet	Customer-id	0
VLAN	Ethernet-VLAN	VLAN	0
VLAN-Range	Ethernet-VLAN	N/A	0
Port-VLAN-Range	Ethernet-VLAN	N/A	0

Port-VLAN	Ethernet-VLAN	VLAN	Customer-id

Notes:

1. The 'VC-Type', 'VC-ID', and 'Group-ID' can be optionally configured as part of the 'ldp connect' command.
2. The 'VLAN' used for the 'VC-ID' is taken from the vlan list in the 'mpls set customer-profile' command.

3. Where the chart denotes ‘N/A’, these values MUST be manually configured with the ‘ldp connect’ command.

The default behavior should work in all any situation (with exception of L2 extranet configuration). The group-id makes the vc-id unique. The following is an example:

```
mpls set customer-profile test1 customer-id 2 type port in-port-list et.1.1
mpls set customer-profile test2 customer-id 3 type port-vlan vlan 2 in-port-list
et.1.2
```

In this example, both vc-id’s would be equal to ‘2’, but with the profile ‘test2’ the group-id is ‘3’ as opposed to ‘0’ for ‘test1’.

Once configured, the local-filters can be checked with the following command (note MPLS specific filters will be in place as well to direct traffic from the LSPs to the appropriate port/vlan combinations. This is one location to locate the MPLS label to VPLS mappings):

```
rs1# filters show static-entry

Name:           Port-Vlan  MPLS: 2
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           1
Customer:       2
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 6
----
Direction:      destination
Restriction:    allow-to-go
Vlan-range:     0 2-99
Customer:       3
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 8
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           100
Label:          19
Customer:       1
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
```

```
Dest MAC Mask:  000000:000000
In-List ports:  gi.4.1
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 7
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           1
Label:          18
Customer:       4
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  gi.4.1
Out-List ports: et.1.(3-4)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 9
----
Direction:      destination
Restriction:    allow-to-go
Vlan-range:     2-4000
Label:          20
Customer:       5
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  gi.4.1
Out-List ports: et.1.(3-4)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 1
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           100
Customer:       1
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2),gi.4.1
802.1Q:         honor incoming 802.1Q value

Name:           Port-To-Port  MPLS: 10
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           any VLAN
```

```
Label:          21
Customer:       6
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  gi.4.1
Out-List ports: et.1.5
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 3
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           1
Customer:       4
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(3-4)
Out-List ports: et.1.(3-4),gi.4.1
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 5
----
Direction:      destination
Restriction:    allow-to-go
Vlan-range:     2-4000
Customer:       5
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(3-4)
Out-List ports: et.1.(3-4),gi.4.1
802.1Q:         honor incoming 802.1Q value

Name:           Port-To-Port  MPLS: 4
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           any VLAN
Customer:       6
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.5
Out-List ports: et.1.5,gi.4.1
802.1Q:         honor incoming 802.1Q value
```

To check the LDP status and label mappings use the ‘ldp show command:

```
rs1# ldp show neighbor
Address          Interface           Label space ID      Hold Time(secs) FT Capable
2.2.2.2          lo                  2.2.2.2:0           11              No
172.16.1.2       gi.4.1-to-rs2       2.2.2.2:0           10              No

rs1# ldp show l2-fec

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 2.2.2.2:0

FEC                                 in-lbl  out-lbl Transport LSP name/label

Customer ID 1, VLAN ID 100          18      19      LDP 2.2.2.2/3
Customer ID 4, VLAN ID 1            19      18      LDP 2.2.2.2/3
Customer ID 5, VLAN Range ...       20      20      LDP 2.2.2.2/3
Signalled FEC: vc-type: Ethernet VLAN, vc-id: 5, group-id: 0
Customer ID 6                       21      21      LDP 2.2.2.2/3
```

It is important to note that LDP will withdraw the label mappings (or will not establish the label mappings) if none of the ports in the profile are in an ‘up’ status. As long as one port in the profile is up, the label mapping will be established.

Port Based "Virtual Switch" Configuration
VPLS Configuration Series

Austin Hawthorne
Principal Systems Engineer
May 16, 2003

In some switched environments it might be necessary to support multiple overlapping 802.1Q (VLAN) domains within a single switch. These environments would include Ethernet Service Providers providing 802.1Q service to customers as well as campus/enterprise environments where separately administered 802.1Q domains must be bridged onto a common infrastructure. Both of these examples might require that a single platform be able to support the logical separation of duplicate VLAN domains between different administrative domains.

By default an L2 Ethernet switch has one global VLAN policy. If a port belongs to a specific VLAN, then traffic coming in on that port is allowed to flood to other VLAN member ports thereby creating a broadcast domain (a.k.a. a VLAN). In the above scenarios, two or more user groups may be using the same VLAN ID, but for security and administrative reasons the VLAN must be broken up to support a segmented broadcast domain per user group. This is not native to a generic 802.1Q aware switch and special configuration must be used to break up the VLAN forwarding domain on a per-user/per-vlan basis.

This configuration template will detail how the Riverstone RS series of products can accomplish this by 'virtualizing' the forwarding plane between these separate administrative domains. There are a number of ways that this can be accomplished dependant on the goal of the network administrator. Some possibilities exist below:

Port Based: This configuration will allow a group of ports to be part of a separate forwarding domain from the rest of the switch. The criteria that determines what is 'allowed' in this separate forwarding instance is based solely on the port designation. Anything coming in the port is allowed to be forwarded to any other port that is part of the same forwarding instance, 802.1Q tagged with any value and untagged.

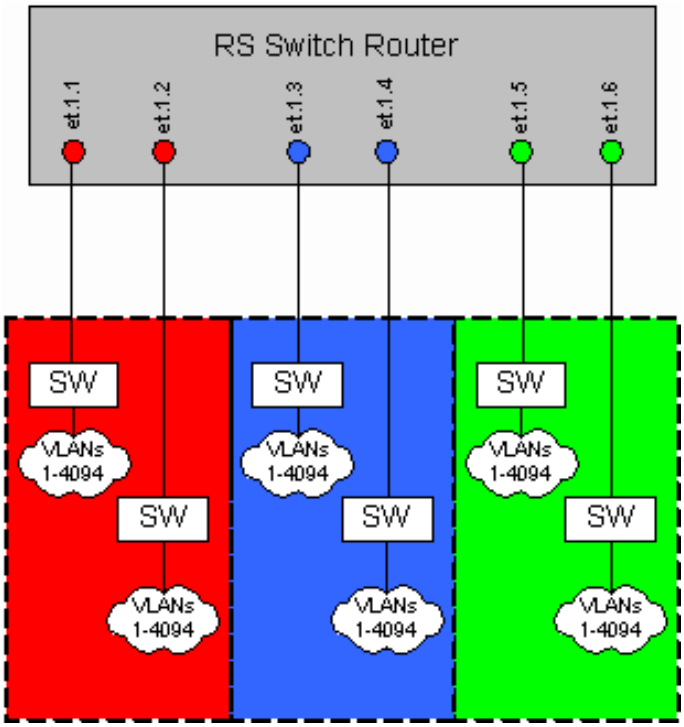
Port-VLAN or Port-VLAN-Range Based: This configuration will take into consideration not only the port designations, but also what 802.1Q VLAN ID's are being assigned to a specific forwarding instance to determine to which administrative domain the frame belongs. This configuration is discussed in the following document: 'VLAN Based 'Virtual Switch' Configuration"

This configuration template will cover the Port Based configuration. Dependant on the code version deployed there are a few ways to configure this service, and some special handling mechanisms that need to be put in place for each, these will all be addressed within this document. This feature is technically only supported in 9.3.0.0 and above as part of the VPLS (Virtual Private LAN Services, see http://www.ietf.org/internet-drafts/draft-lasserre-vkompella-ppvpn-vpls-04.txt) feature set, but an additional configuration has been added for the benefit of users of pre-9.3.0.0 code. This additional configuration does not have all of the advancements of the post-9.3 code, but will accomplish the same objective as long as guidelines are followed.

Regardless of the code deployed, the feature works in much the same way across all branches of RS firmware. A

L2 learning and forwarding filter is applied to the ports designated as a single administrative domain. L2 learning and forwarding from these ports are restricted to the policy applied. So, for example, if port et.1.1 and et.1.2 were set aside as instance 1, and et.1.3 and et.1.4 were set aside as instance 2, forwarding of unknown unicast, broadcast, multicast and of course known unicast arriving on et.1.1 would only be allowed to traverse et.1.2. In pre-9.3, the use of filters will be explicitly configured, while in post-9.3.0.0, the VPLS command set will be used. Added benefits have been placed in the 9.3 and above VPLS feature set to protect against unwanted leakage of frames while filters are changed as well as to reduce VLAN configuration on port-based services.	
RapidOS Version Tested	8.0.3.11, 9.3.0.2
RapidOS Versions Working with this Configuration	Any ROS firmware with the exceptions listed in the above notes.
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	Any PPP, Frame-Relay, Ethernet, Link Aggregation, ATM interface. (No MPLS cards required unless bridging onto MPLS LSPs are required)

Diagram



The above diagram depicts a simple scenario where there are 3 different administrative VLAN domains. We can assume that all 3 need to use VLANs 1~4094 and that VLAN 1 is the untagged (native) vlan for ‘Red’ and ‘Green’ and VLAN 1000 is the untagged (native) vlan for ‘Blue’.

Configurations (9.3.0.0 and newer)

```
!
!  Make all ports trunk ports so ports can send/receive 802.1Q tagged frames
!
vlan make trunk-port et.1.(1-6)
!
!  Create the native-vlan for untagged traffic (VID 1 is already created by default)
!
vlan create 1000 port-based id 1000
!
!  Add ports to their respective native-vlans
!
vlan set native-vlan et.1.(1-2,5-6) all default
vlan set native-vlan et.1.(3-4) all 1000
!
!  Create the VPLS profiles
!
mpls set customer-profile red customer_id 1 type port in-port-list et.1.(1-2)
mpls set customer-profile blue customer_id 2 type port in-port-list et.1.(3-4)
mpls set customer-profile green customer_id 3 type port in-port-list et.1.(5-6)
!
!  Use the 'ldp connect' command to establish the profile.  This is part of the
!  VPLS command set and must be used even if no MPLS uplinks are needed.  This
!  step guarantees that migration to a full VPLS implementation with MPLS is
!  seamless.  All that is required is some additional ldp statements and new ldp
!  connect commands.  This is covered in: "Extending 'Virtual Switch' Domains".
!
ldp connect customer-profile red remote-peer 127.0.0.1
ldp connect customer-profile blue remote-peer 127.0.0.1
ldp connect customer-profile green remote-peer 127.0.0.1
!
!  As part of the transparent service objective, the standard STP BPDU
!  forwarding entry must be removed to allow the STP BPDUs to be bridged
!  transparently within the separate domains.  This will allow the RS switch
!  to be transparent to STP.
!
stp tunnel mpls ports et.1.(1-6)
!
!  Disable all ports that are not in use.  This will prevent leakage from these
unused
!  ports into the configured domains.  It is important to note that once a switch is
!  configured for VPLS, all ports must be configured for VPLS to be used for VLAN
!  switching.  A filter is applied to the configured ports, but not to the
unconfigured
!  ports, so the possibility exists that traffic on these unconfigured ports could
penetrate
!  the configured ports causing security issues.
!
port disable et.1.(7-16) force-link-down
```

Comments (9.3.0.0 and newer)

In the above configuration 3 separate administrative VLAN domains have been created, red, blue, and green. Another way to look at this is that there are now logically 3 separate 802.1Q switches. Once the 'ldp connect' command is issued, the filters are applied. Notice that VLANs, other than the native VLAN, do not have to be configured for Port based services. The 'type port' in the profile command allows for 'any vlan' to be passed. The filter can be viewed with the following example command for the 'red' domain:

```
rs# filters show static-entry customer-id 1

Name:           Port-To-Port  MPLS: 1
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           any VLAN
Customer:       1
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value
```

A simple test can confirm that the VPLS profile is in place and working. In the following output a broadcast frame is sent in on VLAN 2 on port et.1.1. Normally this packet would be flooded to all ports belonging to VLAN 2. In this configuration it is only flooded to all ports belonging to the 'RED' profile. Take special note of the exits ports below.

```
rs# l2-tables show port-macs verbose port et.1.1

L2 table information for port et.1.1
----------------------------------------
Number of source MAC addresses: 0
Number of destination MAC addresses: 0
Number of management-configured MAC addresses: 2
Port table capacity: 5888
Port table demand deletion upper & lower thresholds: 95% - 85%
Number of times table usage has reached upper threshold: 0
Number of times buckets have become full: 0
Number of duplicate learning frames: 0
Number of times LG port got out-of-sync: 0
Number of times L4 Bridging Received non-IP/IPX Packets: 0
Number of times L4 Bridging Received bad IP/IPX Packets: 0
Number of requests to learn a frame on an invalid VLAN: 0
Number of frames discarded due to port not authorized: 0
Number of frames received from this switch (possible loop): 0
Number of flows going out of this SmartTRUNK port: 0
Aging is enabled
Addresses will be aged-out after 300 seconds

 Id            MAC         VLAN    Type      Frames     Age         Exit Ports
-----  ------------------  ----  --------  ----------  -----  ------------------------
----
00001  00:00:00:00:00:01   0002  Src       661         0
00002  FF:FF:FF:FF:FF:FF   0002  Dst       671         0      et.1.2
```

Configurations (older than 9.3.0.0)

```
!
!  Allow all ports to receive and send multiple 802.1Q tagged frames
!
vlan make trunk-port et.1.(1-6)
!
!  Create the entire range of VLANs (NOTE:  The VLAN CREATE-RANGE command was added
!  in version 7.0.2.0 and merged into the 9.x.x.x code.  Code versions prior to
7.0.2.x
!  and between 7.0.2.x and 9.x.x.x will need to explicitly create each vlan with the
VLAN
!  CREATE command.
!
vlan create-range 2-4094 port-based
!
!  Set the untagged VLAN on the ports
!
vlan set native-vlan et.1.(1-2,5-6) all default
vlan set native-vlan et.1.(3-4) all 1000
!
!  Add all ports to all VLANs
!
vlan add-to-vlan-range ports et.1.(1-6) to 2-4094
!
!  Create a static-entry filter that restricts traffic on the ‘in’ ports to only
!  egress the ‘out’ ports.
!
filters add static-entry name red restriction allow in-port-list et.1.(1-2) out-port-
list et.1.(1-2) vlan any dest-mac any
filters add static-entry name blue restriction allow in-port-list et.1.(3-4) out-port-
list et.1.(3-4) vlan any dest-mac any
filters add static-entry name green restriction allow in-port-list et.1.(5-6) out-
port-list et.1.(5-6) vlan any dest-mac any
!
!  Disable all ports that are not in use.  This will prevent leakage from these
unused
!  ports into the configured domains.  It is important to note that once a switch is
!  configured for VPLS, all ports must be configured for VPLS to be used for VLAN
!  switching.  A filter is applied to the configured ports, but not to the
unconfigured
!  ports, so the possibility exists that traffic on these unconfigured ports could
penetrate
!  the configured ports causing security issues.
!
port disable et.1.(7-16) force-link-down
```

Comments (older than 9.3.0.0)

It is important to note that this configuration does not provide the advantages of the VPLS profile, such as protection against unwanted traffic leakage during changes to the profile. Whenever possible, an upgrade should be made to the latest RS firmware to support the

VPLS feature set. Below is the output of the filters command and the l2-tables command to show the similarities to the VPLS config.

```
rs# filters show static-entry

Name:           Dynamic Dest Filter - 6
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           2
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value

Name:           red
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           any VLAN
Source MAC:     000000:000000
Source MAC Mask:FFFFFF:FFFFFF
Dest MAC:       any
Dest MAC Mask:  FFFFFF:FFFFFF
In-List ports:  et.1.(1-2)
Out-List ports: et.1.(1-2)
802.1Q:         honor incoming 802.1Q value
```

In the above output, the ‘RED’ profile is created and a ‘dynamic’ entry has been added for the broadcast flow. In the below output we see the l2-table entry.

```
rs# l2-tables show port-macs verbose port et.1.1

L2 table information for port et.1.1
----------------------------------------
Number of source MAC addresses: 1
Number of destination MAC addresses: 0
Number of management-configured MAC addresses: 1
Port table capacity: 5888
Port table demand deletion upper & lower thresholds: 95% - 85%
Number of times table usage has reached upper threshold: 0
Number of times buckets have become full: 0
Number of duplicate learning frames: 0
Number of times LG port got out-of-sync: 0
Number of times L4 Bridging Received non-IP/IPX Packets: 0
Number of times L4 Bridging Received bad IP/IPX Packets: 0
Number of requests to learn a frame on an invalid VLAN: 0
Number of frames discarded due to port not authorized: 0
Number of frames received from this switch (possible loop): 0
Number of flows going out of this SmartTRUNK port: 0
Aging is enabled
Addresses will be aged-out after 300 seconds
```

```
 Id            MAC          VLAN    Type      Frames     Age         Exit Ports
-----  ------------------  ----  --------  ----------  -----  -------------------------
----
00001  00:00:00:00:00:01   0002  Src       341         0
00002  FF:FF:FF:FF:FF:FF   0002  Dst       341         0      et.1.2
```

VLAN Based "Virtual Switch" Configuration
VPLS Configuration Series

Austin Hawthorne
Principal Systems Engineer
May 16, 200

In the ‘Port Based "Virtual Switch" Configuration’ document the basics of why a ‘Virtual Switch’ feature was needed and how to configure a simple port-based service were covered. Please refer to that document for a brief overview of the common topics discussed within. This document will expand the ‘Virtual Switch’ concept by including flexibility to provide designated forwarding domains based on the port and VLAN combination. In this instance, the configuration will address how to provision an RS series switch to provide separate broadcast domains to overlapping VLANs belonging to two or more distinct administrative domains.

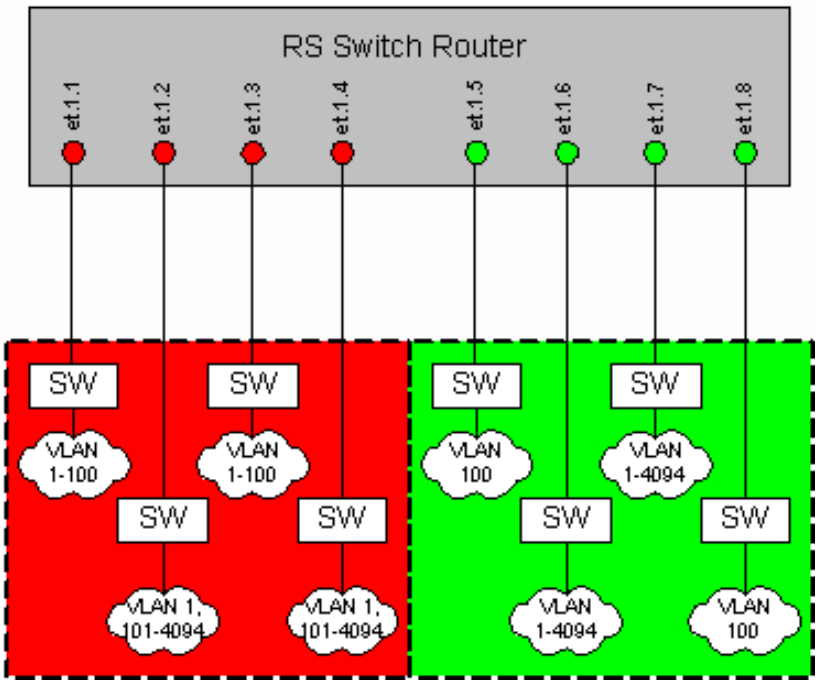
In the Port Based scenario the configuration segmented a single 802.1Q switch into multiple logical 802.1Q switches with the criteria being only as granular as the port assignment. This allows for a level of transparency to whatever might be downstream from the logical switch. Essentially the owner of the administrative domain has complete control over the VLAN assignments in their domain. The unwanted side effect is that this level of transparency does not allow the Virtual Switch to maintain broadcast domain boundaries between VLANs within the logical domain, in other words, a broadcast coming in on one port of a logical domain belonging to VLAN 2 will be sent out all other ports belonging to that same logical domain whether or not a downstream switch or router is bound to VLAN 2.

To relieve this, a more intrusive configuration is necessary that will require a level of coordination between the Virtual Switch administrator and the administrator of the domain to be served. In this scenario, the admin of the domain will need to let the Virtual Switch admin know which ports belong to which VLANs within their domain. This will allow for proper broadcast, multicast, and unknown unicast forwarding within the logical domain. A complex example of this is detailed below for both the VPLS feature set in Riverstone firmware 9.3.0.0 and above, and also a suitable configuration for users of pre-9.3.0.0 firmware.

RapidOS Version Tested	8.0.3.11, 9.3.0.2
RapidOS Versions Working with this Configuration	Any ROS firmware with the exceptions listed in the above notes.
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0

Hardware Specifics	Any PPP, Frame-Relay, Ethernet, Link Aggregation, ATM interface. (No MPLS cards required unless bridging onto MPLS LSPs are required)

Diagram



The above diagram depicts a complex scenario where a higher touch service is required to ensure broadcast domains within the logical administrative domains are maintained. In the 'Red' domain all user switches need to receive the default VLAN (1) untagged, but only two switches need VLANs 2-100, and the other two require only 101-4094. In the 'Green' domain all switches need the VLAN 100 untagged, but only two switches within the domain require the rest of the VLANs.

Configurations (9.3.0.0 and newer)

```
!
!  Disable all ports that are not in use.  This will prevent leakage from these
unused
!  ports into the configured domains.  It is important to note that once a switch is
!  configured for VPLS, all ports must be configured for VPLS to be used for VLAN
!  switching.  A filter is applied to the configured ports, but not to the
unconfigured
!  ports, so the possibility exists that traffic on these unconfigured ports could
penetrate
!  the configured ports causing security issues.
!
port disable et.1.(9-16) force-link-down
!
!  Make all ports trunk ports so ports can send/receive 802.1Q tagged frames
!
vlan make trunk-port et.1.(1-8)
```

```
!
!  Create the range of VLANs needed, in this case it is all of them.
!
vlan create-range 2-4094 port-based
!
!  Set the untagged VLANs
!
vlan set native-vlan et.1.(1-4) all default
vlan set native-vlan et.1.(5-8) all 100
!
!  Add the ports to the appropriate VLANs per user requirements
!
vlan add ports et.1.(5,8) to 100
vlan add-to-vlan-range ports et.1.(1,3) to 2-100
vlan add-to-vlan-range ports et.1.(2,4) to 101-4094
vlan add-to-vlan-range ports et.1.(6-7) to 2-4094
!
!  Create the VPLS customer profiles with the VLAN and port assignments
!
mpls set customer-profile red_vlan-1 customer_id 1 type port-vlan vlans 1 in-port-
list et.1.(1-4)
mpls set customer-profile red_vlan-2-100 customer_id 2 type port-vlan-range vlans 2-
100 in-port-list et.1.(1,3)
!
!  The ‘everything-else’ keyword can be used if all other VLANs except for those
configured
!  in a separate policy on the ports defined in the ‘in-port-list’, need to be used.
This
!  is automatically updated if a new policy need to be configured for a VLAN that
falls
!  within the current ‘everything-else’ envelope.  VLAN 1 (Default) is not included.
!
mpls set customer-profile red_vlan-101-4094 customer_id 3 type port-vlan-range vlans
everything-else in-port-list et.1.(2,4)
mpls set customer-profile green_vlan-100 customer_id 4 type port-vlan vlans 100 in-
port-list et.1.(5-8)
mpls set customer-profile green_vlan-1 customer_id 5 type port-vlan vlans 1 in-port-
list et.1.(6-7)
!
!  Note, this is an example of what is required if ‘everything-else’ was not
supported.
!
mpls set customer-profile green_vlan-2-4094 customer_id 6 type port-vlan-range vlans
2-99,101-4094 in-port-list et.1.(6-7)
!
!  Use the ‘ldp connect’ command to establish the profile.  This is part of the
!  VPLS command set and must be used even if no MPLS uplinks are needed.  This
!  step guarantees that migration to a full VPLS implementation with MPLS is
!  seamless.  All that is required is some additional ldp statements and new ldp
!  connect commands.  This is covered in: "Extending ‘Virtual Switch’ Domains".
!
ldp connect customer-profile red_vlan-1 remote-peer 127.0.0.1
ldp connect customer-profile green_vlan-100 remote-peer 127.0.0.1
```

```
ldp connect customer-profile green_vlan-1 remote-peer 127.0.0.1
!
!  As stated previously we are using a subset of the VPLS feature set to make a
virtual
!  switch.  As such we are bound to some additional VPLS restrictions even though
they
!  are not currently utilized, like the remote-peer.  Also, for type 'port-vlan-
range'
!  profiles the vc-id and vc-type must be specified (see the following for more
detail:
!  http://www.ietf.org/internet-drafts/draft-lasserre-vkompella-ppvpn-vpls-04.txt).
!  For simplicity just place the customer-id value in this field and type will be
!  'ethernet-vlan'.  The vc-id values will become significant in the 'Extending
"Virtual
!  Switch" Configuration' scenario.
!
ldp connect customer-profile red_vlan-2-100 remote-peer 127.0.0.1 vc-id 2 vc-type
ethernet-vlan
ldp connect customer-profile red_vlan-101-4094 remote-peer 127.0.0.1 vc-id 3 vc-type
ethernet-vlan
ldp connect customer-profile green_vlan-2-4094 remote-peer 127.0.0.1 vc-id 6 vc-type
ethernet-vlan
!
!  To ensure that VLANs not configured or needed on a certain port are dropped in
hardware
!  configure the following command on all VLAN based services ports (DO NOT configure
this
!  on port based services ports).
!
stp set vlan-disable port-list et.1.(1-8)
!
!  As part of the transparent service objective, the standard STP BPDU
!  forwarding entry must be removed to allow the STP BPDUs to be bridged
!  transparently within the separate domains.  This will allow the RS switch
!  to be transparent to STP.
!
stp tunnel mpls ports et.1.(1-8)
```

Comments (9.3.0.0 and newer)

In the above configuration 2 separate administrative VLAN domains have been created, red and green. Another way to look at this is that there are now logically 2 separate 802.1Q switches. Once the 'ldp connect' command is issued, the filters are applied. All VLANs must now be configured and applied to the appropriate ports. The same applies for the customer profiles. Any unconfigured VLANs will be dropped per port. The filters can be viewed with the following example command for the 'red' domain:

```
rs# filters show static-entry

Name:           Port-Vlan  MPLS: 1
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           1
```

```
Customer:       1
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1-4)
Out-List ports: et.1.(1-4)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 2
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           100
Customer:       4
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(5-8)
Out-List ports: et.1.(5-8)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 3
----
Direction:      destination
Restriction:    allow-to-go
VLAN:           1
Customer:       5
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(6-7)
Out-List ports: et.1.(6-7)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 4
----
Direction:      destination
Restriction:    allow-to-go
Vlan-range:     2-100
Customer:       2
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(1,3)
Out-List ports: et.1.(1,3)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 5
----
Direction:      destination
```

```
Restriction:    allow-to-go
Vlan-range:     0
Customer:       3
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(2,4)
Out-List ports: et.1.(2,4)
802.1Q:         honor incoming 802.1Q value

Name:           Port-Vlan  MPLS: 6
----
Direction:      destination
Restriction:    allow-to-go
Vlan-range:     2-99 101-4094
Customer:       6
Source MAC:     any
Source MAC Mask:000000:000000
Dest MAC:       any
Dest MAC Mask:  000000:000000
In-List ports:  et.1.(6-7)
Out-List ports: et.1.(6-7)
802.1Q:         honor incoming 802.1Q value
```

A simple test can confirm that the VPLS profile is in place and working. In the following output a broadcast frame is sent in on VLAN 4000 on port et.1.6. Normally this packet would be flooded to all ports belonging to VLAN 4000. In this configuration it is only flooded to all ports belonging to the ‘GREEN’ profile ports that belong to VLAN 4000. Take special note of the exits ports below.

```
rs# l2-tables show port-macs verbose port et.1.6

L2 table information for port et.1.6
----------------------------------------
Number of source MAC addresses: 0
Number of destination MAC addresses: 0
Number of management-configured MAC addresses: 2
Port table capacity: 5888
Port table demand deletion upper & lower thresholds: 95% - 85%
Number of times table usage has reached upper threshold: 0
Number of times buckets have become full: 0
Number of duplicate learning frames: 3
Number of times LG port got out-of-sync: 0
Number of times L4 Bridging Received non-IP/IPX Packets: 0
Number of times L4 Bridging Received bad IP/IPX Packets: 0
Number of requests to learn a frame on an invalid VLAN: 0
Number of frames discarded due to port not authorized: 0
Number of frames received from this switch (possible loop): 0
Number of flows going out of this SmartTRUNK port: 0
Aging is enabled
Addresses will be aged-out after 300 seconds

 Id            MAC         VLAN    Type      Frames     Age         Exit Ports
-----  ------------------  ----  --------  ----------  -----  ------------------------
----
```

```
00001  FF:FF:FF:FF:FF:FF   4000  Dst       241         0      et.1.7
00002  00:00:00:00:00:01   4000  Src       251         0
```

Configurations (older than 9.3.0.0)

```
port disable et.1.(9-16) force-link-down
vlan make trunk-port et.1.(1-8)
!
!  Create the entire range of VLANs (NOTE:  The VLAN CREATE-RANGE command was added
!  in version 7.0.2.0 and merged into the 9.x.x.x code.  Code versions prior to
7.0.2.x
!  and between 7.0.2.x and 9.x.x.x will need to explicitly create each vlan with the
VLAN
!  CREATE command.
!
vlan create-range 2-4094 port-based
vlan set native-vlan et.1.(1-4) all default
vlan set native-vlan et.1.(5-8) all 100
vlan add ports et.1.(5,8) to 100
vlan add-to-vlan-range ports et.1.(1,3) to 2-100
vlan add-to-vlan-range ports et.1.(2,4) to 101-4094
vlan add-to-vlan-range ports et.1.(6-7) to 2-4094
stp set vlan-disable port-list et.1.(1-8)
stp tunnel mpls ports et.1.(1-8)
!
!  Create a static-entry filter that restricts traffic on the ‘in’ ports to only
!  egress the ‘out’ ports with only the VLANs allowed.
!
filters add static-entry name red_vlan-1 restriction allow vlan 1 in-port-list
et.1.(1-4) out-port-list et.1.(1-4) dest-mac any
filters add static-entry name red_vlan-2 restriction allow vlan 2 in-port-list
et.1.(1,3) out-port-list et.1.(1,3) dest-mac any
!
!  Continue this for all VLANs required.
!
```

Comments (older than 9.3.0.0)

This type of configuration is very possible with the ‘filters add static-entry’ command but is very intensive cli work. Each VLAN needs a separate command or ‘any’ can be applied. So for some of the VLAN ranges above, up to 4000 line of configuration will be necessary. Please see the following document for a port-based example ‘Port Based "Virtual Switch" Configuration’ more an alternative to this configuration and for more details on how to configure these services with Riverstone firmware prior to 9.3.0.0.

L2 Extranet Configuration
VPLS Configuration Series

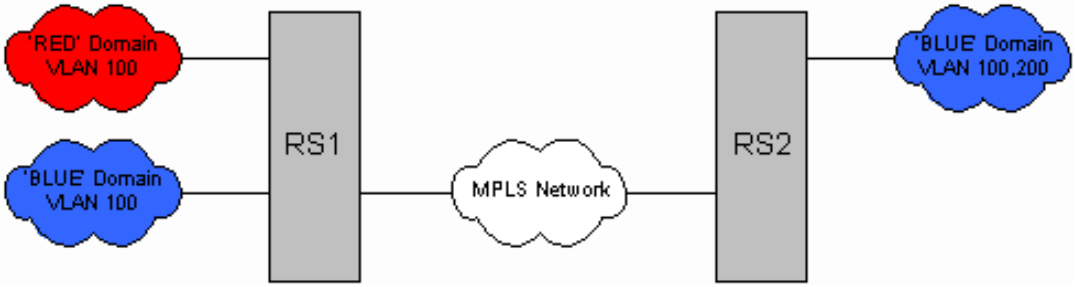
Austin Hawthorne
Principal Systems Engineer
May 16, 2003

This configuration template will detail the use of VLAN translation between virtual switched domains across a VPLS network (For details on VPLS network configuration please review the document entitled 'Extending Virtual Switch Domains'). Applications of this feature are useful in Extranet environments. To be more specific, if two or more 802.1Q VLAN domains require connectivity between them, different administrative policies on VLAN assignment within the domains could become a roadblock. For instance if domain 'A' needed access to a service or network within domain 'B' at layer 2, a common 802.1Q VLAN would need to be provisioned between the domains. This is sometimes unrealistic because these two domains might have established 802.1Q VLAN policies that prohibit the provisioning of a common VLAN ID between both. In these instances, VLAN translation can be employed to translate an 802.1Q VLAN assigned by one provider to another assigned by the second provider. From this point forward this will be considered a L2 or VPLS Extranet.

This can be accomplished by signaling a common vc-id between the two domains that identify this connectivity. This vc-id equates to a VPLS. The type will be 'port-vlan'. This means that the VLAN header is a service delimiter and will be removed before transmitting onto the LSP. The local site will remove the VLAN header and place it onto the appropriate LSP. The remote site will receive a MPLS frame and perform a lookup of the label ID to the mapped VC-ID. This VC-ID will produce a list of exit ports. The local configuration of the exit port and profile will determine the encapsulation locally regardless of the remote configuration. As long as both systems agree on a VC-ID, locally VLANs can be configured differently.

RapidOS Version Tested	9.3.0.1
RapidOS Versions Working with this Configuration	9.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.3.0.0
Hardware Specifics	Any PPP, Frame-Relay, Ethernet, Link Aggregation, ATM interface. MPLS line cards needed for network-facing interfaces.

Diagram



The above diagram depicts a simple scenario where users in the ‘RED’ domain requires access to services in the ‘BLUE’ domain. Users in the ‘RED’ domain would like to use VLAN 100 for this connectivity, but pre-existing connectivity exists within the ‘BLUE’ domains for VLAN 100 to another location. In the following configuration, the ‘RED’ domain will use VLAN 100 locally, but the VPLS network will ‘translate’ this to VLAN 200 within the ‘BLUE’ domain and vice-versa.

Configurations

RS1

```
port disable et.1.(6-16) force-link-down
port disable et.2.(1-16) force-link-down
vlan make trunk-port et.1.1
vlan make trunk-port et.1.2
vlan create ip4001 ip id 4001
vlan create 100 port-based id 100
vlan add ports gi.4.1 to ip4001
vlan add ports et.1.1 to 100
vlan add ports et.1.2 to 100
interface create ip gi.4.1-to-rs2 address-netmask 172.16.1.1/30 vlan ip4001
interface add ip en0 address-netmask 192.168.0.12/24
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ospf create area backbone
ospf add interface gi.4.1-to-rs2 to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf start
mpls add interface gi.4.1-to-rs2
!
!  Create the customer-profile to be type = ethernet-vlan and identify the ‘local’
vlan.
!
mpls set customer-profile red-blue-extranet customer_id 1 type port-vlan vlans 100 in-
port-list et.1.1
mpls set customer-profile blue-intranet customer_id 2 type port-vlan vlans 100 in-
port-list et.1.2
mpls start
ldp add interface gi.4.1-to-rs2
ldp add interface lo0
ldp add remote-peer 2.2.2.2
!
!  Assign a ‘global’ vc-id for this service and signal that via LDP.
!
```

```
ldp connect customer-profile red-blue-extranet remote-peer 2.2.2.2 vc-id 12345 vc-
type ethernet-vlan
ldp connect customer-profile blue-intranet remote-peer 2.2.2.2
ldp start
system set name rs1
system set idle-timeout telnet 0
stp tunnel mpls ports et.1.(1-5)
stp set vlan-disable port-list et.1.(1-4)
```

RS2

```
vlan make trunk-port et.1.1
vlan create ip4001 ip id 4001
vlan create 100 port-based id 100
vlan create 200 port-based id 200
vlan add ports gi.4.1 to ip4001
vlan add ports et.1.1 to 100
vlan add ports et.1.1 to 200
interface create ip gi.4.1-to-rs1 address-netmask 172.16.1.2/30 vlan ip4001
interface add ip en0 address-netmask 192.168.0.11/24
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ospf create area backbone
ospf add interface gi.4.1-to-rs1 to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf start
mpls add interface gi.4.1-to-rs1
!
!  Create the customer-profile to be type = ethernet-vlan and identify the ‘local’
vlan.
!
mpls set customer-profile blue-red-extranet customer_id 1 type port-vlan vlans 200 in-
port-list et.1.1
mpls set customer-profile blue-intranet customer_id 2 type port-vlan vlans 100 in-
port-list et.1.1
mpls start
ldp add interface lo0
ldp add interface gi.4.1-to-rs1
ldp add remote-peer 1.1.1.1
!
!  Assign a ‘global’ vc-id for this service and signal that via LDP.
!
ldp connect customer-profile blue-red-extranet remote-peer 1.1.1.1 vc-id 12345 vc-
type ethernet-vlan
ldp connect customer-profile blue-intranet remote-peer 1.1.1.1
ldp start
system set name rs2
system set idle-timeout telnet 0
stp tunnel mpls ports et.1.(1-5)
stp set vlan-disable port-list et.1.(1-4)
```

Comments

The label mappings to vc-id and VLAN can be gleaned from the following commands:

```
rs1# ldp show l2-fec verbose

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 2.2.2.2:0

FEC: Customer ID 1, VLAN ID 100
Signalled FEC: vc-type: Ethernet VLAN, vc-id: 12345, group-id: 0
in-lbl: 18, out-lbl: 18
Ports: et.1.1
Transport LSP name/label: LDP 2.2.2.2/3
Bytes In: 0, Pkts In: 0, In Pkts Drop: 0
Bytes Out: 0, Pkts Out: 0, Out Pkts Drop: 0

FEC: Customer ID 2, VLAN ID 100
in-lbl: 19, out-lbl: 17
Ports: et.1.2
Transport LSP name/label: LDP 2.2.2.2/3
Bytes In: 0, Pkts In: 0, In Pkts Drop: 0
Bytes Out: 0, Pkts Out: 0, Out Pkts Drop: 0
```

And on RS2:

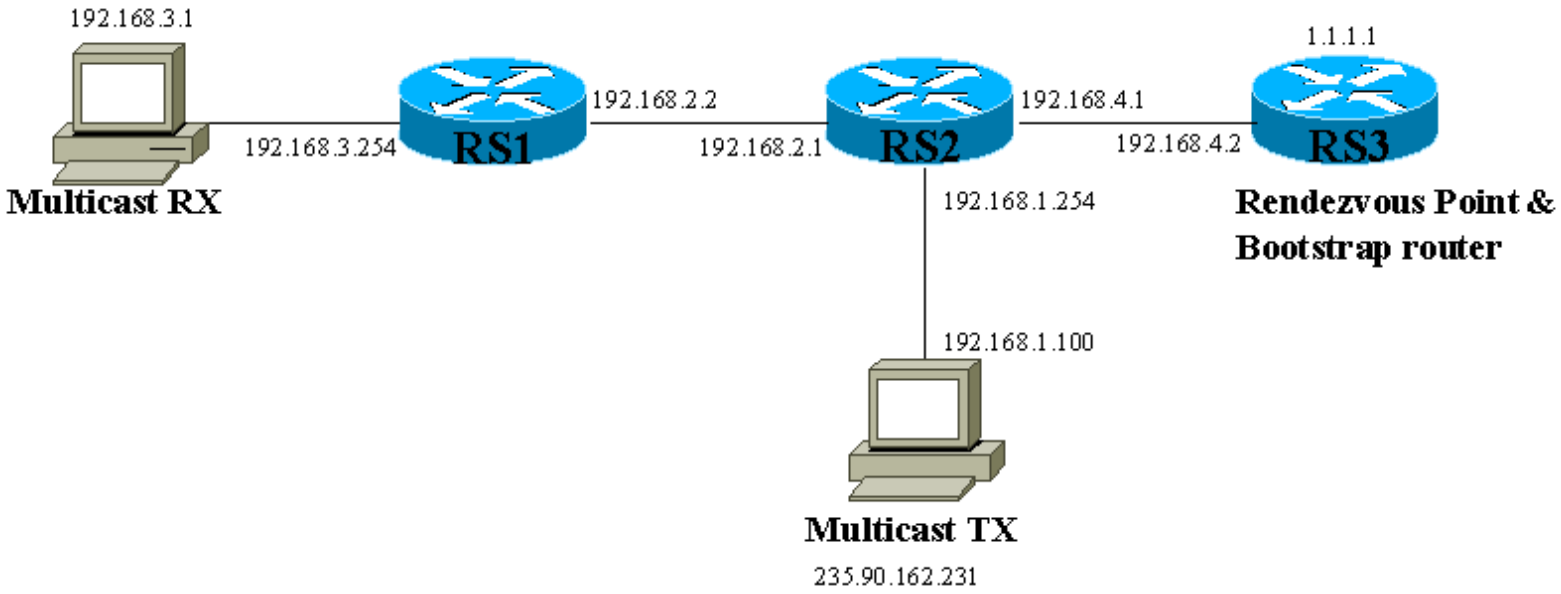
```
rs2# ldp show l2-fec verbose

FEC: Forward Equivalence class, in-lbl: Label received, out-lbl: Label sent

Remote neighbor 1.1.1.1:0

FEC: Customer ID 2, VLAN ID 100
in-lbl: 17, out-lbl: 19
Ports: et.1.1
Transport LSP name/label: LDP 1.1.1.1/3
Bytes In: 0, Pkts In: 0, In Pkts Drop: 0
Bytes Out: 0, Pkts Out: 0, Out Pkts Drop: 0

FEC: Customer ID 1, VLAN ID 200
Signalled FEC: vc-type: Ethernet VLAN, vc-id: 12345, group-id: 0
in-lbl: 18, out-lbl: 18
Ports: et.1.1
Transport LSP name/label: LDP 1.1.1.1/3
Bytes In: 0, Pkts In: 0, In Pkts Drop: 0
Bytes Out: 0, Pkts Out: 0, Out Pkts Drop: 0
```

PIM-SM configuration with RP & BSR

John Schaap
Systems Engineering, EMEA
February 20, 2002

This configuration shows how to configure PIM-SM in an all Riverstone network. RS3 is configured as the rendezvous point (RP) and bootstrap router (BSR). Multicast TX used - LiveCaster - http://www.live.com/liveCaster/ Multicast RX used - FreeAmp - http://www.freeamp.org/	
RapidOS Version Tested	9.0.0.0
RapidOS Versions Working with this Configuration	9.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.0.0.0
Hardware Specifics	None

Diagram



Configurations

RS1

```
interface create ip to_multicast_rx address-netmask 192.168.3.254/24 port et.2.1
interface create ip to_rs2 address-netmask 192.168.2.2/24 port et.1.1
isis add area 49.0001
isis add interface to_rs2
isis add interface to_multicast_rx
isis set level 2
isis set rib multicast
isis start
igmp add interface to_multicast_rx
igmp start
pim sparse add interface to_rs2
pim sparse start
system set name RS1
system set timezone uct+1
system set idle-timeout serial 0 telnet 0
system set terminal baud 38400
```

RS2

```
interface create ip to_rs1 address-netmask 192.168.2.1/24 port et.1.1
interface create ip to_multicast_tx address-netmask 192.168.1.254/24 port et.2.16
interface create ip to_rs3 address-netmask 192.168.4.1/24 port et.2.1
isis add area 49.0001
isis add interface to_rs1
isis add interface to_rs3
isis add interface to_multicast_tx
isis set rib multicast
isis set level 2
isis start
pim sparse add interface to_rs1
pim sparse add interface to_rs3
pim sparse add interface to_multicast_tx
pim sparse start
system set timezone uct+1
system set name RS2
system set terminal baud 38400
system set idle-timeout serial 0 telnet 0
```

RS3

```
interface create ip to_rs2 address-netmask 192.168.4.2 port et.7.1
interface add ip lo0 address-netmask 1.1.1.1/32
isis add area 49.0001
isis add interface to_rs2
isis add interface lo0
isis set level 2
isis set spf-interval 1
isis set rib multicast
isis start
pim sparse add interface to_rs2
pim sparse add interface 1.1.1.1
pim sparse crp address 1.1.1.1
pim sparse cbsr address 1.1.1.1
pim sparse start
system set name RS3
system set timezone uct+1
```

```
system set idle-timeout serial 0 telnet 0
system set terminal baud 38400
```

Comments

```
RS1# pim show interface
Interface Address: 192.168.2.2, Interface name: to_rs2
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.2.2
Interface Address: 127.0.0.2, Interface name: register
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 0 seconds, Current DR: (null)

RS1# pim show neighbor
Neighbor information for interface to_rs2
        Neighbor information for 192.168.2.1
                Creation Time: 2002-02-15 17:57:27
                Refresh Time: 2002-02-15 18:01:42
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:15    , Flags:  USE_PRIORITY,

RS1# pim show bsr-info
Comp Status     CBSR-Pri CBSR-Addr       CBSR-mask
---- ------     -------- ---------       ---------
sm0  Ineligible N/A      N/A             N/A

Comp Elec-Pri Elec-Addr       Elec-mask Interval
---- -------- ---------       --------- --------
sm0  0        1.1.1.1         30        00:01:26

RS1# pim show rpset

BSR (dynamic RP) mechanism used to derieve RPset.

Comp Group/Mask           Src/RP          Pri  Uptime   Expires
---- ----------           ------          ---  ------   -------
sm0  224/4                1.1.1.1         0    4:55     never

RS1# pim show routes

PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
       R - RP-bit set, T - SPT-bit set
       J - Join SPT, F - Directly connected source, E - External join
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports

 (0.0.0.0/0, 235.90.162.231/32), 00:03:26/never, RP 1.1.1.1, flags: SPE
  Incoming interface: to_rs2, RPF nbr 192.168.2.1,
  Outgoing interface list: n/a

 (192.168.1.100/32, 235.90.162.231/32), 00:03:26/00:03:42, flags: SPT
  Total packet/byte count: 2627/3451163, Rate: n/a
  Incoming interface: to_rs2, RPF nbr 192.168.2.1,
  Outgoing interface list: n/a

RS1# igmp show memberships
Group Address   Interface       Uptime   Expires  Last Reporter   Ports
--------------- --------------- -------- -------- --------------- --------
235.90.162.231  to_multicast_rx 3:35     2:59     192.168.3.1     et.2.1
```

```
RS2# pim show interface
Interface Address: 192.168.2.1, Interface name: to_rs1
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.2.2
Interface Address: 192.168.1.254, Interface name: to_multicast_tx
        Status: Up, Mode: Sparse
        Neighbor count: 1, Query Interval: 30 seconds, Current DR: 192.168.1.254
Interface Address: 192.168.4.1, Interface name: to_rs3
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.4.2
Interface Address: 127.0.0.2, Interface name: register
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 0 seconds, Current DR: (null)

RS2# pim show neighbor
Neighbor information for interface to_rs1
        Neighbor information for 192.168.2.2
                Creation Time: 2002-02-15 07:57:41
                Refresh Time: 2002-02-15 08:05:41
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:24    , Flags:  USE_PRIORITY,
Neighbor information for interface to_multicast_tx
Neighbor information for interface to_rs3
        Neighbor information for 192.168.4.2
                Creation Time: 2002-02-15 07:44:31
                Refresh Time: 2002-02-15 08:05:32
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:15    , Flags:  USE_PRIORITY,

RS2# pim show bsr-info
Comp Status     CBSR-Pri CBSR-Addr       CBSR-mask
---- ------     -------- ---------       ---------
sm0  Ineligible N/A      N/A             N/A

Comp Elec-Pri Elec-Addr       Elec-mask Interval
---- -------- ---------       --------- --------
sm0  0        1.1.1.1         30        00:01:51

RS2# pim show rpset

BSR (dynamic RP) mechanism used to derieve RPset.

Comp Group/Mask           Src/RP          Pri  Uptime   Expires
---- ----------           ------          ---  ------   -------
sm0  224/4                1.1.1.1         0    10:25    never

RS2# pim show routes

PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
       R - RP-bit set, T - SPT-bit set
       J - Join SPT, F - Directly connected source, E - External join
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports

 (0.0.0.0/0, 235.90.162.231/32), 00:07:02/never, RP 1.1.1.1, flags: S
  Incoming interface: to_rs3, RPF nbr 192.168.4.2,
  Outgoing interface list:
     to_rs1 (192.168.2.1), 00:07:02/00:03:28, et.1.1,
```

```
 (192.168.1.100/32, 235.90.162.231/32), 02:38:57/00:00:35, flags: STRF
  Total packet/byte count: 120685/153255484, Rate: 16968 bytes/sec
  Incoming interface: to_multicast_tx, RPF nbr 192.168.1.100,
  Outgoing interface list:
     to_rs1 (192.168.2.1), 00:07:02/00:03:28, et.1.1,

RS3# pim show interface
Interface Address: 1.1.1.1, Interface name: lo
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 30 seconds, Current DR: (null)
Interface Address: 192.168.4.2, Interface name: to_rs2
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.4.2
Interface Address: 127.0.0.2, Interface name: register
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 0 seconds, Current DR: (null)

RS3# pim show neighbor
Neighbor information for interface lo
Neighbor information for interface to_rs2
        Neighbor information for 192.168.4.1
                Creation Time: 2002-02-15 07:40:04
                Refresh Time: 2002-02-15 07:57:04
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:30    , Flags:  USE_PRIORITY,

RS3# pim show bsr-info
Comp Status     CBSR-Pri CBSR-Addr       CBSR-mask
---- ------     -------- ---------       ---------
sm0  Elected    0        1.1.1.1         30

Comp Elec-Pri Elec-Addr       Elec-mask Interval
---- -------- ---------       --------- --------
sm0  0        1.1.1.1         30        00:00:23

RS3# pim show rpset

BSR (dynamic RP) mechanism used to derieve RPset.

Comp Group/Mask           Src/RP          Pri  Uptime   Expires
---- ----------           ------          ---  ------   -------
sm0  224/4                1.1.1.1         0    13:50    1:40

RS3# pim show routes

PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
       R - RP-bit set, T - SPT-bit set
       J - Join SPT, F - Directly connected source, E - External join
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports

 (0.0.0.0/0, 235.90.162.231/32), 00:10:17/never, RP 1.1.1.1, flags: S
  Incoming interface: register, RPF nbr (null),
  Outgoing interface list:
     to_rs2 (192.168.4.2), 00:10:17/00:03:13, et.7.1,

 (192.168.1.100/32, 235.90.162.231/32), 00:10:17/00:01:49, flags: SPR
  Total packet/byte count: NA/NA, Rate: NA
  Incoming interface: register, RPF nbr (null),
```

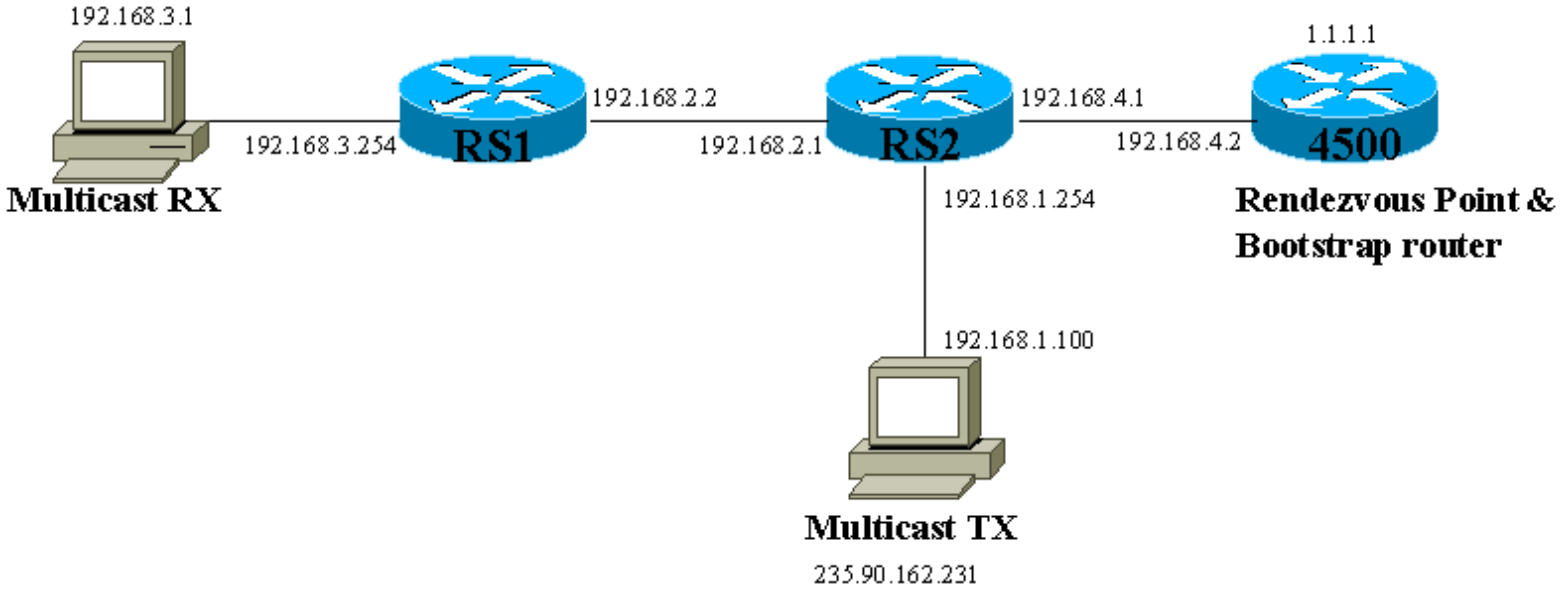
$Id: 0060.html,v 1.3 2002/08/27 02:32:23 webmaster Exp $

PIM-SM interoperability with a Cisco RP & BSR

John Schaap
Systems Engineering, EMEA
February 20, 2002

This configuration shows how to configure PIM-SM between Riverstone and Cisco routers. The Cisco is configured as the rendezvous point (RP) and bootstrap router (BSR). Multicast TX used - LiveCaster - http://www.live.com/liveCaster/ Multicast RX used - FreeAmp - http://www.freeamp.org/	
RapidOS Version Tested	9.0.0.0
RapidOS Versions Working with this Configuration	9.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 9.0.0.0
Hardware Specifics	None

Diagram



Configurations

RS1

```
interface create ip to_multicast_rx address-netmask 192.168.3.254/24 port et.2.1
interface create ip to_rs2 address-netmask 192.168.2.2/24 port et.1.1
isis add area 49.0001
isis add interface to_rs2
isis add interface to_multicast_rx
isis set level 2
isis set rib multicast
isis start
igmp add interface to_multicast_rx
igmp start
pim sparse global cisco-hash
pim sparse add interface to_rs2
pim sparse start
system set name RS1
system set timezone uct+1
system set idle-timeout serial 0 telnet 0
system set terminal baud 38400
```

RS2

```
interface create ip to_rs1 address-netmask 192.168.2.1/24 port et.1.1
interface create ip to_multicast_tx address-netmask 192.168.1.254/24 port et.2.16
interface create ip to_cisco address-netmask 192.168.4.1/24 port et.2.1
isis add area 49.0001
isis add interface to_cisco
isis add interface to_rs1
isis add interface to_multicast_tx
isis set rib multicast
isis set level 2
isis start
pim sparse global cisco-hash
pim sparse add interface to_cisco
pim sparse add interface to_rs1
pim sparse add interface to_multicast_tx
pim sparse start
system set timezone uct+1
system set name RS2
system set terminal baud 38400
system set idle-timeout serial 0 telnet 0
```

Cisco

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco
!
enable password c
!
ip subnet-zero
!
ip multicast-routing
!
interface Loopback0
```

```
 ip address 1.1.1.1 255.255.255.255
 ip router isis
!
interface FastEthernet0
 ip address 192.168.4.2 255.255.255.0
 ip router isis
 ip pim sparse-dense-mode
 full-duplex
!
router isis
 net 49.0001.0010.7b2c.7c61.00
 is-type level-2-only
!
ip classless
no ip http server
no ip pim bidir-enable
ip pim bsr-candidate Loopback0 4 255
ip pim rp-candidate Loopback0
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password c
 login
!
end
```

Comments

```
cisco#sh ip pim neighbor
PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.4.1       FastEthernet0            03:10:16/00:01:29 v2    1 /

cisco#sh ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 1.1.1.1 (?)
  Uptime:      04:01:47, BSR Priority: 255, Hash mask length: 4
  Next bootstrap message in 00:00:14
  Candidate RP: 1.1.1.1(Loopback0)
    Advertisement interval 60 seconds
    Next advertisement in 00:00:54

cisco#sh ip pim rp
Group: 235.90.162.231, RP: 1.1.1.1, v2, next RP-reachable in 00:00:48

cisco#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
```

```
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.0.1.40), 04:00:51/00:00:00, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0, Forward/Sparse-Dense, 03:08:10/00:00:00

(*, 235.90.162.231), 03:59:23/00:03:12, RP 1.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0, Forward/Sparse-Dense, 02:11:16/00:03:12

(192.168.1.100, 235.90.162.231), 03:59:23/00:02:46, flags: PT
  Incoming interface: FastEthernet0, RPF nbr 192.168.4.1
  Outgoing interface list: Null

RS1# pim show interface
Interface Address: 192.168.2.2, Interface name: to_rs2
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.2.2
Interface Address: 127.0.0.2, Interface name: register
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 0 seconds, Current DR: (null)

RS1# pim show neighbor
Neighbor information for interface to_rs2
        Neighbor information for 192.168.2.1
                Creation Time: 2002-02-15 11:46:49
                Refresh Time: 2002-02-15 14:12:34
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:21    , Flags:  USE_PRIORITY,

RS1# pim show bsr-info
Comp Status     CBSR-Pri CBSR-Addr       CBSR-mask
---- ------     -------- ---------       ---------
sm0  Ineligible N/A      N/A             N/A

Comp Elec-Pri Elec-Addr       Elec-mask Interval
---- -------- ---------       --------- --------
sm0  255      1.1.1.1         4         00:01:51

RS1# pim show rpset
BSR (dynamic RP) mechanism used to derieve RPset.

Comp Group/Mask           Src/RP          Pri  Uptime   Expires
---- ----------           ------          ---  ------   -------
sm0  224/4                1.1.1.1         0    2:26:15  never

RS1# pim show routes

PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
       R - RP-bit set, T - SPT-bit set
       J - Join SPT, F - Directly connected source, E - External join
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports

 (0.0.0.0/0, 235.90.162.231/32), 00:01:05/never, RP 1.1.1.1, flags: SPE
  Incoming interface: to_rs2, RPF nbr 192.168.2.1,
  Outgoing interface list: n/a

 (192.168.1.100/32, 235.90.162.231/32), 00:01:05/00:02:32, flags: SPT
```

```
  Total packet/byte count: NA/NA, Rate: NA
  Incoming interface: to_rs2, RPF nbr 192.168.2.1,
  Outgoing interface list: n/a

RS1# igmp show memberships
Group Address   Interface       Uptime   Expires  Last Reporter   Ports
--------------- --------------- -------- -------- --------------- --------
235.90.162.231  to_multicast_rx 1:33     3:14     192.168.3.1     et.2.1

RS2# pim show interface
Interface Address: 192.168.2.1, Interface name: to_rs1
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.2.2
Interface Address: 192.168.1.254, Interface name: to_multicast_tx
        Status: Up, Mode: Sparse
        Neighbor count: 1, Query Interval: 30 seconds, Current DR: 192.168.1.254
Interface Address: 192.168.4.1, Interface name: to_cisco
        Status: Up, Mode: Sparse
        Neighbor count: 2, Query Interval: 30 seconds, Current DR: 192.168.4.2
Interface Address: 127.0.0.2, Interface name: register
        Status: Up, Mode: Sparse
        Neighbor count: 0, Query Interval: 0 seconds, Current DR: (null)

RS2# pim show neighbor
Neighbor information for interface to_rs1
        Neighbor information for 192.168.2.2
                Creation Time: 2002-02-15 05:24:47
                Refresh Time: 2002-02-15 05:30:17
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:43    , Flags:  USE_PRIORITY,
Neighbor information for interface to_multicast_tx
Neighbor information for interface to_cisco
        Neighbor information for 192.168.4.2
                Creation Time: 2002-02-15 04:28:18
                Refresh Time: 2002-02-15 05:30:18
                Holdtime: 1:45 seconds, Priority: 1, genid: 1
                Time to expire: 1:44    , Flags:  USE_PRIORITY,

RS2# pim show bsr-info
Comp Status     CBSR-Pri CBSR-Addr       CBSR-mask
---- ------     -------- ---------       ---------
sm0  Ineligible N/A      N/A             N/A

Comp Elec-Pri Elec-Addr       Elec-mask Interval
---- -------- ---------       --------- --------
sm0  255      1.1.1.1         4         00:01:57

RS2# pim show rpset
BSR (dynamic RP) mechanism used to derieve RPset.

Comp Group/Mask           Src/RP          Pri  Uptime   Expires
---- ----------           ------          ---  ------   -------
sm0  224/4                1.1.1.1         0    1:05:52  never

RS2# pim show routes
PIM Multicast Routing Table
Flags: S - Sparse, C - Directly connected host, L - Local, P - Pruned
       R - RP-bit set, T - SPT-bit set
       J - Join SPT, F - Directly connected source, E - External join
Timers: Uptime/Expires
Interface state: Interface, Timers, Output Ports
```

```
(0.0.0.0/0, 235.90.162.231/32), 00:05:39/never, RP 1.1.1.1, flags: S
 Incoming interface: to_cisco, RPF nbr 192.168.4.2,
 Outgoing interface list:
    to_rs1 (192.168.2.1), 00:05:39/00:02:51, et.1.1,

(192.168.1.100/32, 235.90.162.231/32), 00:04:22/00:01:10, flags: STRF
 Total packet/byte count: NA/NA, Rate: NA
 Incoming interface: to_multicast_tx, RPF nbr 192.168.1.100,
 Outgoing interface list:
    to_rs1 (192.168.2.1), 00:05:39/00:03:08, et.1.1,
    to_cisco (192.168.4.1), 00:01:18/00:02:12, et.2.1,
```

Basic Remote Syslog Configuration

Andrew Walden
Corporate Systems Engineering
May 25, 2001

This configuration is how to setup a basic remote syslog server for an RS router.	
RapidOS Version Tested	7.0.0.1
RapidOS Versions Working with this Configuration	All
RapidOS Versions NOT Working with this Configuration	None
Hardware Specifics	None

Configurations

```
interface create ip et.2.16 address-netmask 192.168.1.3/24 port et.2.16
interface add ip lo0 address-netmask 1.1.1.1/32
system set syslog level info facility local7 source 1.1.1.1 server 192.168.1.2
```

Comments

The above config creates an interface for basic connectivity, adds an IP to lo0 for easy identification and sets up remote syslog to the server 192.168.1.2. The possible levels are:

Error - Display Fatal and Error messages only

Fatal - Display Fatal messages only

Info - Display ALL messages

Warning - Display Fatal, Error and Warning messages only

The level is choosen depending upon the situation, how detailed the logging needs to be and the amount of log file that is generated. I

The router portion of the configuration is only half of setting up remote syslog. The other half is configuring the *nix server. Though it is not RS's job to help customers admin their *nix servers, the more information we can offer, the better.

I tested this with a Linux server (Slackware). This should be applicable to most every *nix server though.

Edit the /etc/syslog.conf to tell it what to do with the router log data. Syslog allows for 8 custom local facilities (local0-local7). I used local7 in my example syslog.conf line below.

```
local7.* /var/log/riverstone
```

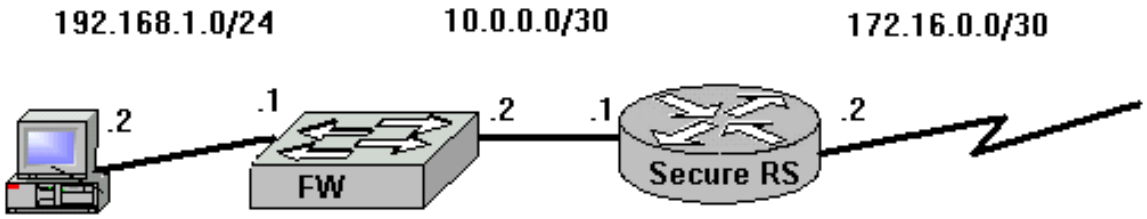
This will put all log messages set for local7 into the file /var/log/riverstone as was designated in the router config above. You will want to "touch" the log file before you restart the syslogd daemon so it has somewhere to write the file. You will want to kill -1 or -HUP your syslogd daemon after making the change to the syslog.conf. You may need to add a command line switch when you start syslogd to tell it to listen on port 514 for remote syslog messages. On the Linux box I used the switch was: `syslogd -r` to get syslog to listen on port 514.

Cistron RADIUS Configuration

Andrew Walden
Corporate System Engineering
August 16, 2001

This document shows how to setup a RADIUS server on a Linux box and configure a router for authentication against the server.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	None

Diagram



Configurations

```
interface create ip et.1.1 address-netmask 192.168.1.3/24 port et.1.1
interface add ip lo0 address-netmask 10.0.0.1
system set password login secret
system set password enable verysecret
! This uses radius for logging into the router via telnet/ssh/console
radius authentication login
! This uses radius for enable after logging in
```

```
radius authentication enable
! This indicates the radius server and how we want to identify this router to the
server
radius set server 192.168.1.2 key secretkey source 10.0.0.1
! This sends every command to the radius server, every command registers 9 lines of
text in
! the detail file.
radius accounting command level 15
! This sends every system message to the radius server, every message registers 9
lines of
! text in the detail file, syslog is probably a better option instead
radius accounting system info
! This is very import so you can get into your router when the radius server is
inavailable
radius set last-resort password
! Startup radius
radius enable
```

Comments

This config details the installation and setup of Cistron RADIUS, which is freely available at http://www.radius.cistron.nl/ This is the most accessible RADIUS server available today. The original Livingston server is now only available to Lucent customers, a newer version of Cistron called FreeRADIUS is still in beta, and other servers such as Steel-belted RADIUS are commercial products. There are also alternatives such as the Cistron derivative ICRadius which uses MYSQL as a back-end, but is out of the scope of this document. This installation and setup is performed on a linux box (Slackware/2.4.4), so some of the commands may use linux specific flags, but the radius daemon should be platform independent.

Installation

After downloading Cistron RADIUS you would use the following steps to install it:

```
! Untar the file
# tar zxvf radiusd-cistron-1.6-stable.tar.gz
! cd into the directory
# cd radiusd-cistron-1.6.4
! check out the simple install instructions
# more INSTALL
! Follow the simple install instructions
# cd src
# ls
# cp Makefile.lnx Makefile
! This version of RADIUS is still using the old port numbers, so lets update it
! Edit the file radius.h and change:
#define PW_AUTH_UDP_PORT                1645
#define PW_ACCT_UDP_PORT                1646
! to:
#define PW_AUTH_UDP_PORT                1812
#define PW_ACCT_UDP_PORT                1813
! then
# make
# make install
```

Configuration

When you run "make install", the binaries are placed into /usr/local/bin and /etc/raddb is created for the configuration files. The noteworthy configuration files consist of:

Users: This file contains the security and authentication information for each user.
Naslist: This file contains a list of routers, associates them to a nickname and defines the type of device they are.
Clients: This file lists all of the routers and associates them to their respective encryption key.

First lets setup our clients file. For our setup above we will place the following into the clients file:

```
# Client Name           Key
#----------------       ----------
10.0.0.1                secretkey
```

To setup the naslist file for the above setup we will place the following entry:

```
# NAS Name            Short Name            Type
#---------------     ----------------      --------
10.0.0.1              secure-rs1            other
```

The user file is the most complex file of them all. There are numerous options available for authenticating users, with most of the options only being relevant to dial-up access. We will demonstrate three of the available options relevant to our setup, local passwords, local encrypted passwords and using the /etc/passwd. Unless using the users file for authentication elsewhere, you should ensure the existing configuration in the users file is commented out or deleted.

Local Password entries for users noc and admin, which uses clear-text passwords, an insecure option, this file should keep very restrictive permissions:

```
 noc    Auth-Type = Local, Password = "secret1"
 admin  Auth-Type = Local, Password = "secret2"
```

Authenticate off the /etc/passwd file where users are already stored, which doesn't leave anyway to control what users can and cannot log into the routers:

```
noc     Auth-Type = System
admin   Auth-Type = System
```

Local Encrypted Password entries for users noc and admin, which use encrypted passwords, which is the most secure option with the best control. Even though the passwds are encrypted, the can be cracked, so restrictive permissions are recommended:

```
noc     Auth-Type = Crypt-Local, Password = " $1$/qzjvMw5$6kt7pYWtx3s/4yw0.T6yG1"
admin   Auth-Type = Crypt-Local, Password = " $1$/35KvMtf$zbZpsriVnd5dKBNBAnd1U/"
```

After you make any change to the users file you must HUP radiusd to reread the file:

kill -1 `cat /var/run/radiusd.pid`

Running RADIUS

To start RADIUS just type /usr/local/bin/radiusd. Some of the available handy switches for RADIUS are:

-a - Accounting directory: Within the accounting directory, radiusd will create a directory for each one of the routers and store its detail file for that router in that directory. Default is /var/log/radacct

-l - Log directory: This is where the radius.log file is stored. Default is /var/log

-C - Checks the syntax of the config files

-y - Details each user's incorrect password attempt. Can be handy for troubleshooting fat fingers.

-z - Details each user's password, correct and incorrect. This is obviously a very insecure option.

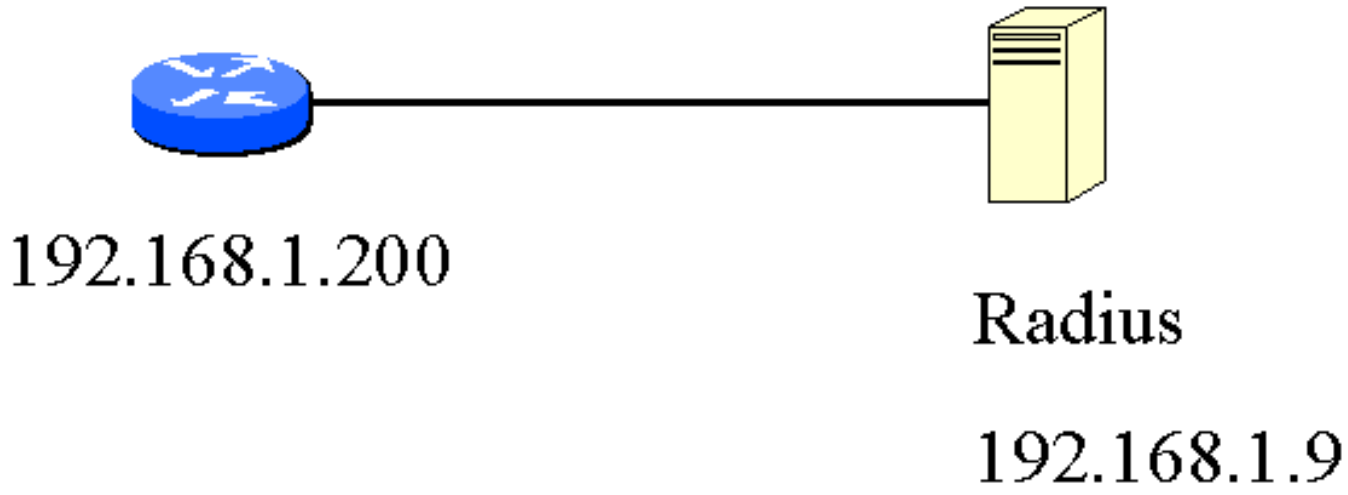
Configuring User Authentication and Accounting with Livingston RADIUS

Nick Slabakov
Corporate Systems Engineering
April 15, 2001

The purpose of this note is to assist with quickly bringing up Authentication and Accounting of the RS using Livingston RADIUS server. Configurations for the RS as well as the RADIUS server are included. When configured with RADIUS authentication, the RS prompt for Username/Password upon login, and every individual user could be configured with unique combination of those.

RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	5.1.0.0, 6.x.x.x
RapidOS Versions NOT Working with this Configuration	3.1.0.0 and below although working with this configuration, have known RADIUS problems, please check release notes
Hardware Specifics	none

Diagram



Configurations

Router

```
version 7.0
interface create ip RMON address-netmask 192.168.1.200/24 port et.2.1
system set hashed-password enable zJzuqz abc1ff9c061beceb0cce8806521f959f
radius set server 192.168.1.9
comment line 4 "Authenticate via RADIUS when entering Enable mode "
radius authentication enable
comment line 6 "This key must be matched at the RADIUS server "
radius set key key1
radius enable
comment line 9 "If the RADIUS server does not respond, authenticate with local
password "
radius set last-resort password
comment line 11 "Account allactivities and log-in/log-out events "
radius accounting command level 15
radius accounting shell all
```

Livingston RADIUS running on FreeBSD

Livingston RADIUS is free software that can be obtained at http://www.livingston.com/marketing/products/radius.html. After a default installation, the executable will be in /etc/radiusd, and the configuration files will be in /etc/raddb. Two configuration files are most important, the "clients" file, describing all routers that are allowed to request authentication, and the "users" file, containing username/password pairs. Simplified examples of those files are included below:

```
RADIUS# more clients
#-----------------------------------------------------------------------
#
# @(#)clients   1.1 2/21/96  Copyright 1991 Livingston Enterprises Inc
#
#-----------------------------------------------------------------------
```

```
#
#       This file contains a list of clients which are allowed to
#       make authentication requests and their encryption key.
#       The first field is a valid hostname.
#       The second field (seperated by blanks or tabs) is the
#       encryption key.
#
#Client Name            Key
#----------------       ------------------

router1                 key1
RADIUS#
```

The name "router1" must be DNS-resolvable.

```
RADIUS# more users
#-----------------------------------------------------------------------------
#
# @(#)users     1.2 5/20/97  Copyright 1991, 1997 Livingston Enterprises Inc
#
#-----------------------------------------------------------------------------
#
#       This file contains security and configuration information for
#       each user.  The first field is the user's name and can be up to
#       8 characters in length.  This is followed (on the same line)
#       with the list of authentication requirements for that user.
#       This can include password, comm server name, comm server port
#       number, and an expiration date of the user's password.  When an
#       authentication request is received from the comm server, these
#       values are tested.  Special users named "DEFAULT", "DEFAULT2",
#       "DEFAULT3" can be created (and should be placed at the end of
#       the user file) to specify what to do with users not contained
#       in the user file.
#
#       Indented (with the tab character) lines following the first
#       line indicate the configuration values to be passed back to
#       the comm server to allow the initiation of a user session.
#       This can include things like the PPP configuration values
#       or the host to log the user onto.
#
#       Delete or comment out these examples before using this file!

joe     Password = "whatever1"
jill    Password = "whatever2"
yoda    Password = "whatever3"

RADIUS#
```

Also note that Livingston RADIUS defaults to UDP port numbers 1812 and 1813 for authentication and accounting respectively, as suggested by RFC 2138, while the RS defaults to the "original" port numbers 1644 and 1645. To ensure interoperability, the RADIUS must be started with the following line:

/etc/radiusd –o &

The "-o" option causes the RADIUS to listen to the original port numbers.

Comments

In this example configuration, the RS is set up to only use RADIUS when the user attempts to enter "Enable" mode. For "User" mode, the system password is used.

```
------------------------------------------------------------------------
RS 2000 System Software, Version 7.0.0.0
Copyright (c) 2000-2001 Riverstone Networks
System started on 2001-04-14 23:14:59
------------------------------------------------------------------------

Press RETURN to activate console . . .

Password:
rs> en
Username: yoda
Password:
rs#
```

In addition, the RS is also configured for accounting using RADIUS. The RADIUS maintains the accounting files (when using default installation) in:

```
/usr/adm/radacct/<client name>/detail
```

where <client name> is replaced with the name of the router, as configured in the /etc/raddb/clients. The records in this file look like this:

```
Sat Apr 14 21:54:44 2001
        Acct-Status-Type = Start
        Acct-Session-Id = "60"
        Acct-Authentic = RADIUS
        User-Name = "yoda"
        Service-Type = Administrative-User
        NAS-IP-Address = 192.168.1.200
        Timestamp = 987306884

Sat Apr 14 21:54:50 2001
        Acct-Status-Type = Accounting-On
        Acct-Session-Id = "0"
        Acct-Authentic = RADIUS
        User-Name = "yoda"
        Vendor-Specific-5567-1 = "Command-Code (level: 10): arp show all"
        NAS-IP-Address = 192.168.1.200
        Timestamp = 987306890
```

```
Sat Apr 14 21:54:55 2001
        Acct-Status-Type = Accounting-On
        Acct-Session-Id = "0"
        Acct-Authentic = RADIUS
        User-Name = "yoda"
        Vendor-Specific-5567-1 = "Command-Code (level: 10): arp clear all"
        NAS-IP-Address = 192.168.1.200
        Timestamp = 987306895

Sat Apr 14 21:54:58 2001
        Acct-Status-Type = Accounting-On
        Acct-Session-Id = "0"
        Acct-Authentic = RADIUS
        User-Name = "yoda"
        Vendor-Specific-5567-1 = "Command-Code (level: 15): en"
        NAS-IP-Address = 192.168.1.200
        Timestamp = 987306898

Sat Apr 14 21:55:04 2001
        Acct-Status-Type = Start
        Acct-Session-Id = "0"
        Acct-Authentic = RADIUS
        User-Name = "joe"
        Service-Type = Administrative-User
        NAS-IP-Address = 192.168.1.200
        Timestamp = 987306904
```

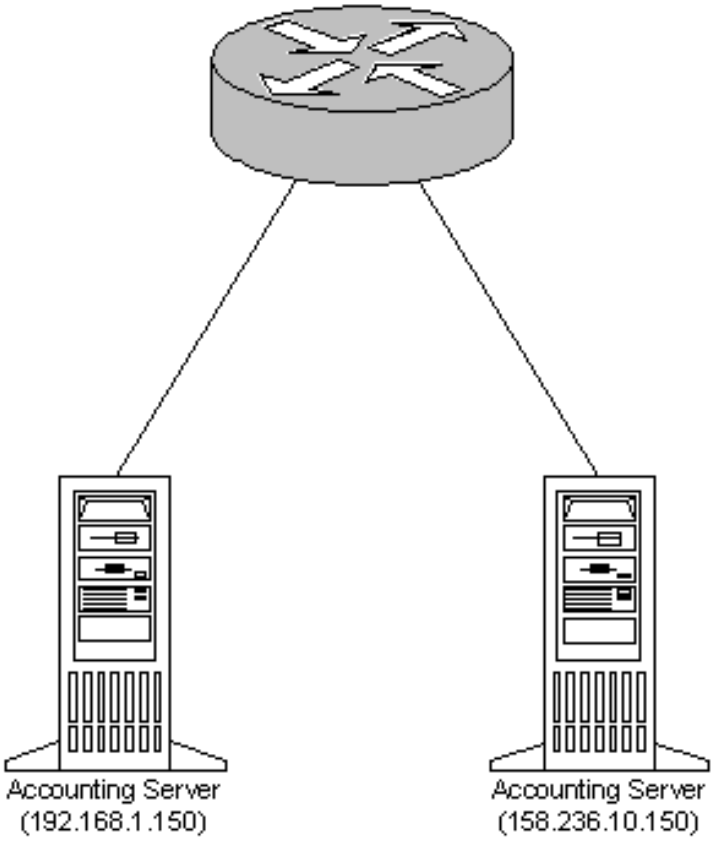
In the next version of this document a simple PERL script will be included to illustrate how this raw accounting file can be parsed and a useful WEB page can be produced for auditing all activities on the router.

LFAP Configuration

Ron Patin
Corporate Systems Engineering
April 17, 2001

The following will show how to configure a simple LFAP Process on Riverstone Products using redundant account servers	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	N/A

Diagram



Configurations

```
port description et.1.8 "To Lab"
port description et.2.8 "To Customer 1"
!
interface create ip LAB address-netmask 192.168.1.120/24 port et.1.8
interface create ip TO-CUSTOMER-1 address-netmask 158.236.10.1/24 port et.2.8
!
acl lfap permit ip any any any any accounting hourly
acl lfap apply interface TO-CUSTOMER-1 input output
!
lfap set server "192.168.1.150 158.236.10.150"
lfap start
```

Comments

Please note in the above configuration that when specifying multiple accounting servers, you must use quotation marks

around the server IP addresses. Also, please note that up to 3 accounting servers can be specified.

The following show command will give you a very detailed view of the LFAP process.

```
rs# lfap show all

LFAP Agent Status:  started
      LFAP version:  4
       conn status:  connection established to server 192.168.1.150

 LFAP Agent Flow Accounting Servers (FASs):
    1) 192.168.1.150
    2) 158.236.10.150

 LFAP Agent Configuration:
    Poll Interval:              15 minutes
    Batch Size:                 32
    Batch Interval:             1 second
    Lost Contact Interval:      30 seconds
    Server Retry Interval:      60 seconds
    Maximum Send Queue Size:    50000 messages
    Task Priority:              default

 LFAP Information Elements:
    Source Port:                enabled
    Protocol Id:                enabled
    Type of Service:            enabled
    Priority Queue:             enabled
    Source CCE Address:         enabled
    Ingress Port:               enabled
    Egress Port:                enabled
    Source AS Number:           disabled
    Destination AS Number:      disabled

LFAP Agent Statistics:
    2 servers total
    FAS: 192.168.1.150
        server is in the current FAS list
        up time: 0 00:00:14
        connecting: 1 success, 1 failure
            Messages sent:                  Messages received:
                84 bytes                        68 bytes
                4 successful                    5 successful
                0 in queue                      0 in queue
                2 AR msgs                       2 AR msgs
                1 VR msgs                       0 VR msgs
                1 ARA msgs                      2 ARA msgs
                0 VRA msgs                      1 VRA msgs
```

```
            0 FAR msgs                          0 FAR msgs
            0 FUN msgs                          0 FUN msgs
                                                0 unknown msgs
            0 dropped total                     0 dropped total
            0 dropped while conn
            0 dropped AR
            0 dropped VR
            0 dropped ARA
            0 dropped FAR
            0 dropped FUN-I
            0 dropped FUN
        Lost information:
            0 0 bytes sent                      0 0 bytes rcvd
            0 0 packets sent                    0 0 packets rcvd
        Flows:
            0 setups
            0 teardowns
          134 currently active
        Peak:
            2 msgs in send queue
            0 active flows

FAS: 158.236.10.150
        server is in the current FAS list
        up time: 0 00:00:00
        connecting: 0 successes, 0 failures
            Messages sent:                  Messages received:
            0 bytes                             0 bytes
            0 successful                        0 successful
            0 in queue                          0 in queue
            0 AR msgs                           0 AR msgs
            0 VR msgs                           0 VR msgs
            0 ARA msgs                          0 ARA msgs
            0 VRA msgs                          0 VRA msgs
            0 FAR msgs                          0 FAR msgs
            0 FUN msgs                          0 FUN msgs
                                                0 unknown msgs
            0 dropped total                     0 dropped total
            0 dropped while conn
            0 dropped AR
            0 dropped VR
            0 dropped ARA
            0 dropped FAR
            0 dropped FUN-I
            0 dropped FUN
        Lost information:
            0 0 bytes sent                      0 0 bytes rcvd
            0 0 packets sent                    0 0 packets rcvd
```

```
Flows:
    0 setups
    0 teardowns
    0 currently active
Peak:
    0 msgs in send queue
    0 active flows
```

The "dropped while conn" count should be zero. A nonzero count means the RS is having difficulty getting messages to the FAS quickly enough. This problem must be investigated if it occurs.

"MICA" Accounting Server Setup

Ron Patin
Corporate Systems Engineering
April 16, 2001

This document will describe the install process for the newly re- branded Accounting Server (MICA).	
RapidOS Version Tested	N/A
RapidOS Versions Working with this Configuration	N/A
RapidOS Versions NOT Working with this Configuration	N/A
Hardware Specifics	N/A

Configurations

```
#gzip -d Mica_V3.0_solaris.tar.gz
#untar xvf Mica_V3.0_solaris.tar.gz
#cd fas_vcd*
```

To start the installation, execute the install.cd script

```
#./install.cd
```

When the installation is completed, the system displays the following message:

```
LFAP Installation was successful.
```

Once installation is complete the FAS process will be running. No further configuration is necessary. To start/stop the MICA process, ensure you are logged in as root and issue the following command:

```
#/usr/csi/bin/start_fas
#/usr/csi/bin/stop_fas
```

To check the status of the MICA process, issue the following command:

```
#/usr/csi/bin/status_fas
```

One of two messages will appear:

```
#FAS is running
```

or

```
#FAS is stopped
```

In order to have the FAS process automatically restarted if the process crashes follow these steps as root:

```
1. cp /usr/csi/docs/watcher_fas /usr/csi/bin
2. crontab -e
3. enter this line
        0-59 * * * * /usr/csi/bin/watcher_fas
```

Comments

Once the MICA server has been setup, the Lightweight Flow Accounting Protocol (LFAP) should be configured on all Riverstone Networks devices. Please see the LFAP configuration document for guidelines on configuring LFAP.

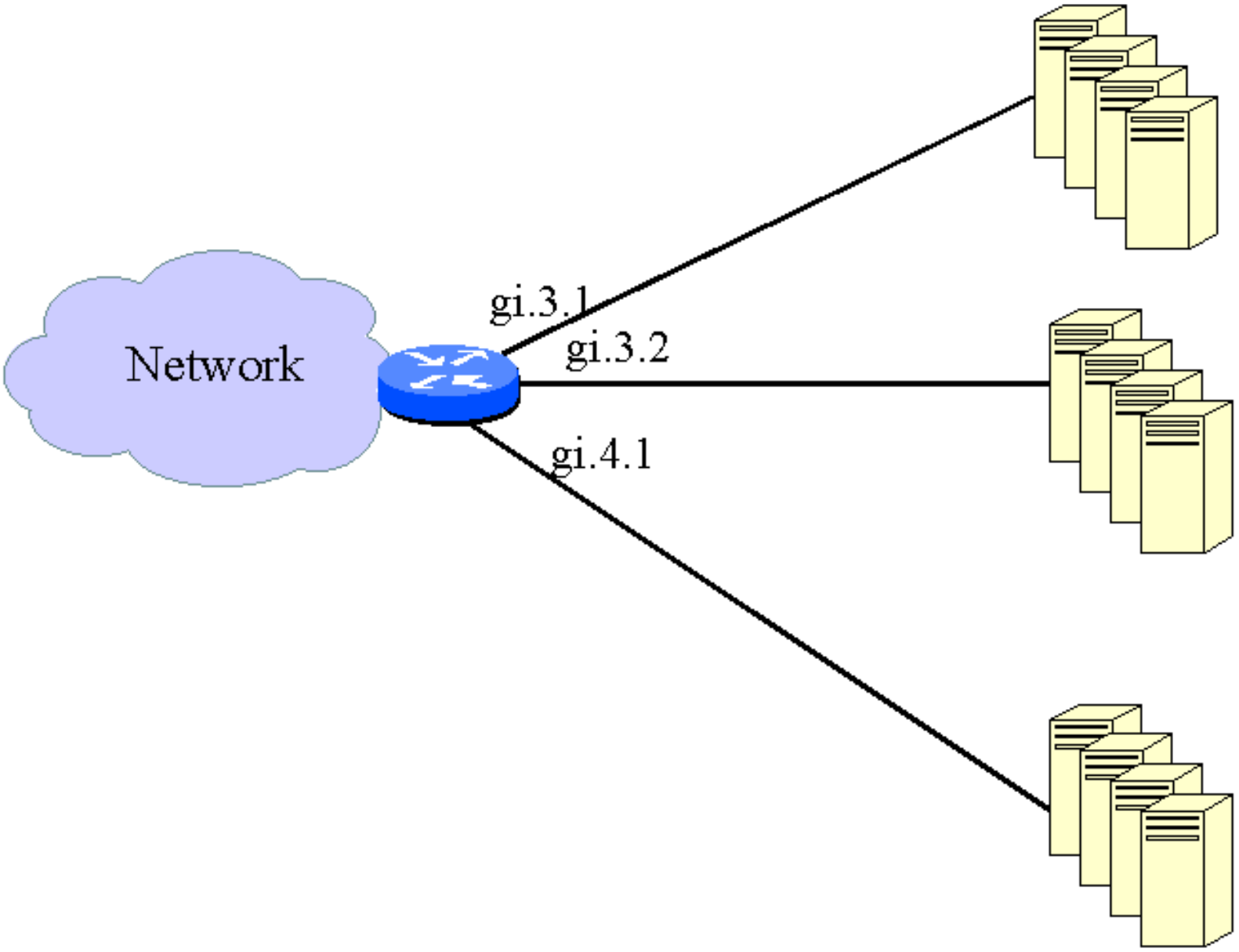
Quick Tricks with RMON2

Nick Slabakov
Corporate Systems Engineering
April 15, 2001

The RS router is a fully functional RMON1/2 probe on every port. While complex configurations of RMON can be done using an external RMON Manager application (such as Concord, Netscout, etc.), this note documents quick useful features of RMON that can be done through CLI only. This type of configuration can be useful for both troubleshooting and trending.	
RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	N/A

Diagram

A collocation environment with three customers. We want to investigate problems with the traffic of Customer 1, connected to gi.3.1.



Configurations

```
version 7.0
interface create ip RMON address-netmask 198.144.10.1/30 port gi.3.1
rmon set ports gi.3.1
rmon set lite default-tables yes
rmon set standard default-tables yes
rmon set professional default-tables yes
rmon set memory 24
rmon enable
```

In the above configuration RMON is only enabled on the uplink port (to minimize memory consumption), and RMON memory usage is capped at 24 MB.

Comments

This is a "bare-bone" RMON configuration, allowing for quick observation and statistic collection on port gi.3.1. Many statistics are available via the "port show …" or "statistics show …" commands, however when we need protocol-specific information, RMON2 is a better tool (RMON2 was enabled with the "rmon set professional default-tables yes" command.

The following questions can be easily answered with the respective "rmon show …" commands, once the above configuration is installed.

1. What MAC/IP address bindings has this customer used?

```
rs# rmon show address-map-logs all-ports
RMON II Address Map Control Table
Port       macAdd        nlAdd           Protocol
----       ------        -----           --------
gi.3.1     0010A4:E62886 10.10.254.254   ip-v4
gi.3.1     005056:95FEFE 10.10.1.2       ip-v4
gi.3.1     0010A4:E628A4 10.10.254.2     ip-v4
gi.3.1     005056:953344 10.10.1.3       ip-v4
```

Checking the ARP cache of the router produces similar output, however the above information obtained with RMON never ages, so it provides a more complete history of IP/MAC address usage.

2. If the customer is routinely exceeding their rate limit (and experiences reduced performance because of that), which application contributes to that the most?

```
rs# rmon show protocol-distribution all-ports
RMON II Protocol Distribution Table

Index: 500, Port: gi.3.1, Owner: monitor
      Pkts     Octets   Protocol
      ----     ------   --------
   6869843 3374119013   ether2
   6869843 3374119013   ip-v4
        67       5358   icmp
     20112    1719561   igmp
   3430497 1796272662   tcp
         6       1028   echo
         7       2206   ftp-data
     56939   71733973   ftp
       138      17166   ssh
      4988     472516   telnet
       123      13566   smtp
     10947     971398   domain
   3433419 1296142652   doom
    498712   47773592   pop3
```

It is evident that the DOOM traffic dominates this link and bears further investigation.

3. Which pair of hosts contributes most to the traffic and for which application?

```
rs# rmon show al-matrix all-ports
RMON II Application Layer Host Table

Index: 500, Port: gi.3.1, Inserts: 2555, Deletes: 0, Owner: monitor
SrcAddr         DstAddr            Packets     Octets  Protocol
-------         -------            -------     ------  --------

< … output truncated …>
134.141.172.7   10.10.254.254      7252235  323345681  ip-v4
134.141.172.7   10.10.254.254      7252235  323345681  tcp
134.141.172.7   10.10.254.254           14        896  domain
134.141.172.7   134.141.178.24     3335673  974638992  doom
134.141.171.129 224.0.0.4            20112    1720159  ip-v4
134.141.171.129 224.0.0.4            20112    1720159  igmp
< … output truncated …>
```

It appears that 134.141.172.7 is the main DOOM user.

Remote TFTP Config Backup

Andrew Walden
Corporate Systems Engineering
June 20, 2001

This document demonstrates a process backing up a router configuration file remotely using SNMP and TFTP to a *nix platform via a shell script.	
RapidOS Version Tested	7.0.0.1
RapidOS Versions Working with this Configuration	3.0.0.0 and newer
Other requirements	SNMP toolkit, TFTP server

Configurations

```
interface create ip et.1.1 address-netmask 192.168.1.3/24 port et.1.1
snmp set mib name ctron-ssr-config-mib status enable
snmp set community secret privilege read-write
```

Comments

This configuration requires a TFTP server and some additional tools to be able to set the SNMP OIDS remotely. Net-SNMP is used for this example. It can be found at http://sourceforge.net/projects/net-snmp After installing this package you will have access to snmpset. This installs to /usr/local/bin by default. If the default is changed, SNMPPATH will need to be updated in the script. There are a number of variables that need to be entered on the command line for this script to work. There are as follows:

TFTPSERVER- This is the hostname or IP address of the TFTP server.

HOST - This is the hostname or IP address of the router that is being backed up.

COMMUNITY - This is the SNMP community string used to access the router.

CFGNAME - This is the full filename of the config

The script is listed below. If you use this exact script, you will want to fix the word wrap. The script is a very simple proof of concept so

that it can be easily understood and incorporated into other larger automation systems.

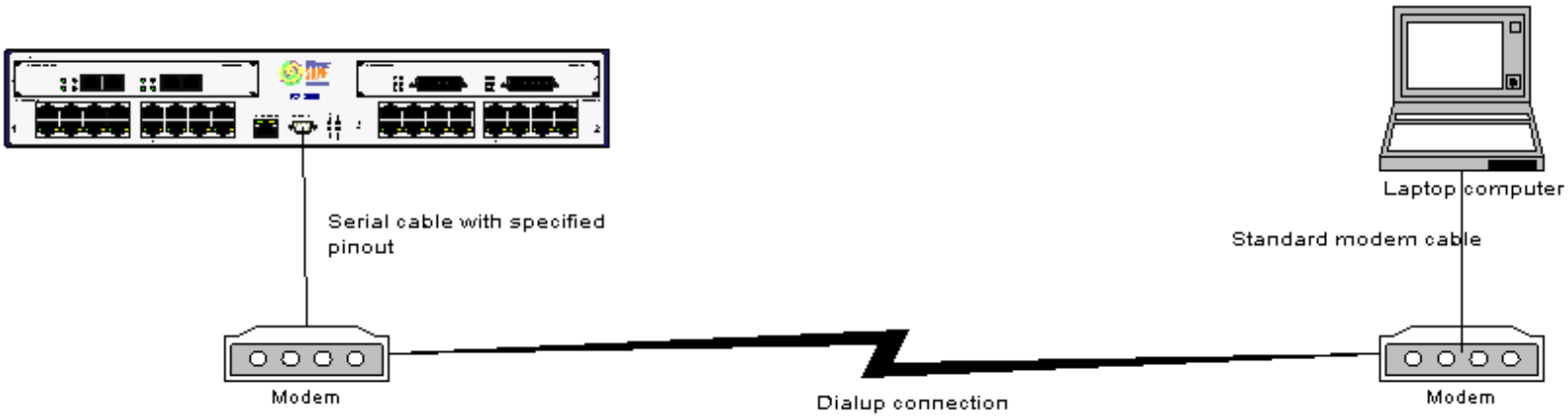
```
#!/bin/sh

SNMPPATH=/usr/local/bin

if [ -n $1 ]; then


 if [ $# != 4 ]; then
  echo "Usage: tftpback router_ip community config_name tftp_server"
  exit
 fi

HOST=$1
COMMUNITY=$2
CFGNAME=$3
TFTPSERVER=$4

fi

/bin/touch $CFGNAME

$SNMPPATH/snmpset  $HOST $COMMUNITY enterprises.52.2501.1.231.1.0 i 3 > /dev/null
$SNMPPATH/snmpset  $HOST $COMMUNITY enterprises.52.2501.1.231.2.0 a $TFTPSERVER >
/dev/null
$SNMPPATH/snmpset  $HOST $COMMUNITY enterprises.52.2501.1.231.3.0 s $CFGNAME >
/dev/null
$SNMPPATH/snmpset  $HOST $COMMUNITY enterprises.52.2501.1.231.4.0 i 1 >/dev/null

STATUS=`$SNMPPATH/snmpget  $HOST $COMMUNITY enterprises.52.2501.1.231.7.0 2>&1| awk -
F= '{print $2}'`

 if [ $STATUS = "6" ]; then
  echo "The configuration was successfully backed up"
  exit
 else
  echo "Something seems to have gone wrong"
 fi
```

Remote RS Management Through a Modem Connected to the RS Console Port

Louis Dehner
Systems Engineering
August 29, 2001

Configuring a modem to communicate with the Console Port on an RS switch router.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	All supported versions
RapidOS Versions NOT Working with this Configuration	N/A
Hardware Specifics	Serial cable with specified pinout

Diagram



Configurations

Modem AT command configuration (USRobotics)

```
ati4
USRobotics Sportster 14400 Fax Settings...
```

```
B0  E1  F1  M1  Q1  V1  X1  Y0
BAUD=9600    PARITY=N  WORDLEN=8
DIAL=PULSE  ON HOOK

&A1  &B1  &C1  &D0  &G0  &H1  &I0  &K0
&M4  &N6  &P0  &R2  &S0  &T5  &Y1

S00=001  S01=000  S02=043  S03=013  S04=010  S05=008  S06=002
S07=060  S08=002  S09=006  S10=007  S11=070  S12=050  S13=000
S14=000  S15=000  S16=000  S17=000  S18=000  S19=000  S20=000
S21=010  S22=017  S23=019  S24=000  S25=005  S26=000  S27=000
S28=008  S29=020  S30=000  S31=000  S32=000  S33=000  S34=006
S35=000  S36=014  S37=000  S38=000  S39=000  S40=000  S41=000
S42=000  S43=000  S44=015  S45=000  S46=000  S47=000  S48=000
S49=000  S50=000  S51=000
```

DIP switch settings must be as follows:
1 Down (DTR Override)
2 UP
3 UP (Suppress result codes)
4 UP
5 UP
6 UP
7 UP (Load NVRAM defaults. Make sure you've saved the AT commands to both NVRAM templates with AT&W0 and AT&W1)
8 UP (Puts the modem in Dumb mode)

Cable Pinout
DB9 DB25
2--------->2
3--------->3
5--------->7
7--------->5
8--------->4

Riverstone

```
rs-boot> set flow_control on
```

Comments

The Console port on the RS switch router must have Flow Control set to On. The modem must be set for hardware flow control (AT&H1); furthermore, request to send (RTS) must be set so that received data is sent to the computer only on RTS (AT&R2).

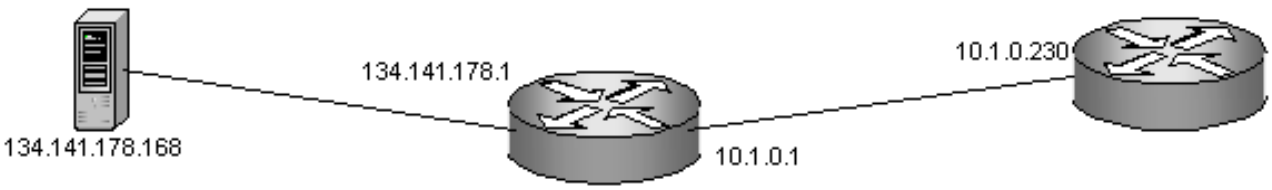
Modem DIP switch settings vary depending on make and model. For example, on a USR 56Kbps Faxmodem Product #USR5686D the proper dip switch settings should be 1, 3 & 8 DOWN and the rest UP.

Basic TACACS+ Configuration

Eric Hoberman
RTAC
April 20, 2003

TACACS+ is an industry standard protocol that provides access control for network devices. This protocol supports the security features of authentication, authorization, and accounting. This document shows a basic TACACS+ configuration between a router and one server. It also discusses the commands you can use to monitor the operation of TACACS+ on the router.	
RapidOS Version Tested	9.0.0.1
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

```
!
! Startup configuration for the next system reboot
!
! Last modified from Console on 2002-04-11 09:20:29
```

```
!
version 9.0
interface create ip tacacs address-netmask 10.1.0.230/16 port et.3.1
ip add route 134.141.178.0/24 gateway 10.1.0.1
system set hashed-password login czPLmafd13ffbb3be2b3baabf56113c2218c97
system set idle-timeout serial 0
tacacs-plus set server 134.141.178.168
tacacs-plus set key yago
tacacs-plus set last-resort password
tacacs-plus authentication login
tacacs-plus enable
tacacs-plus accounting shell all
tacacs-plus accounting command level 15
```

Comments

The following command sets the authentication key to be shared with the configured TACACS+ server:

```
tacacs-plus set key
```

The following command allows you to specify when TACACS+ authentication is performed, such as at the RS login or when users attempt to access enable mode:

```
tacacs-plus authentication login|enable
```

The following command allows you to track shell usage on the RS. It causes an entry to be logged on the TACACS+ server when a shell is either started or stopped, or both:

```
tacacs-plus accounting shell start|stop|all
```

The following shows the process for logging into this router:

```
Press RETURN to activate console . . .




User Access Verification

Username: labuser
Password:
rs> en
%SYS-W-NOPASSWD, no password for enable, use 'system set password' in Config mode
rs#


On the TACACS+ server, there should be a corresponding log entry:

Fri Apr 12 10:29:33 2002        10.1.0.230  labuser tty0    unknown start   task_id=5
     service=shell   priv-lvl=15     cmd=login
Fri Apr 12 10:29:39 2002        10.1.0.230  labuser tty0    unknown unknown task_id=5
     service=shell   priv-lvl=15     cmd=en
```

Note: If the TACACS+ server is down, users will be prompted for the last-resort password, as specified in the configuration. Be sure to have a local password configured for this situation:

```
Press RETURN to activate console . . .



%CONS-W-AUTH_PASSWD, contact TACACS+ server failed: last-resort password
Password:
rs> en
%SYS-W-NOPASSWD, no password for enable, use 'system set password' in Config mode
rs#
```

Warning: If the last-resort password option is not configured, you will be locked out of the router if the TACACS+ server is down:

```
Press RETURN to activate console . . .



%CONS-W-AUTH_NONE, contact TACACS+ server failed: login denied
%CONS-E-LOGINFAIL, console login failed
```

The following command displays the accepts, rejects, and timeouts for each TACACS+ server:

```
rs# tacacs-plus show stats

TACACS+ servers listed in order of priority:

Server:              134.141.178.168
Port:                49
Timeout (seconds):   <Default>
Retries:             <Default>
Deadtime (minutes):  <Default>
Source IP:           <Default>

TACACS+ server statistics:

Host               Accepts   Rejects   Timeouts
134.141.178.168    0         0         0
```

The following command displays the above info, as well as the TACACS+ configuration parameters:

```
rs# tacacs-plus show all
TACACS+ status:                        ACTIVE
TACACS+ last resort:                   System Password
Default TACACS+ timeout (seconds):     3
Default TACACS+ retries:               3
Default TACACS+ deadtime (minutes):    0
Default TACACS+ source IP address:     10.1.0.230

TACACS+ servers listed in order of priority:

Server:              134.141.178.168
Port:                49
Timeout (seconds):   <Default>
Retries:             <Default>
Deadtime (minutes):  <Default>
Source IP:           <Default>

TACACS+ server statistics:

Host               Accepts   Rejects   Timeouts
134.141.178.168    0         0         0
```

Pebbles of Knowledge

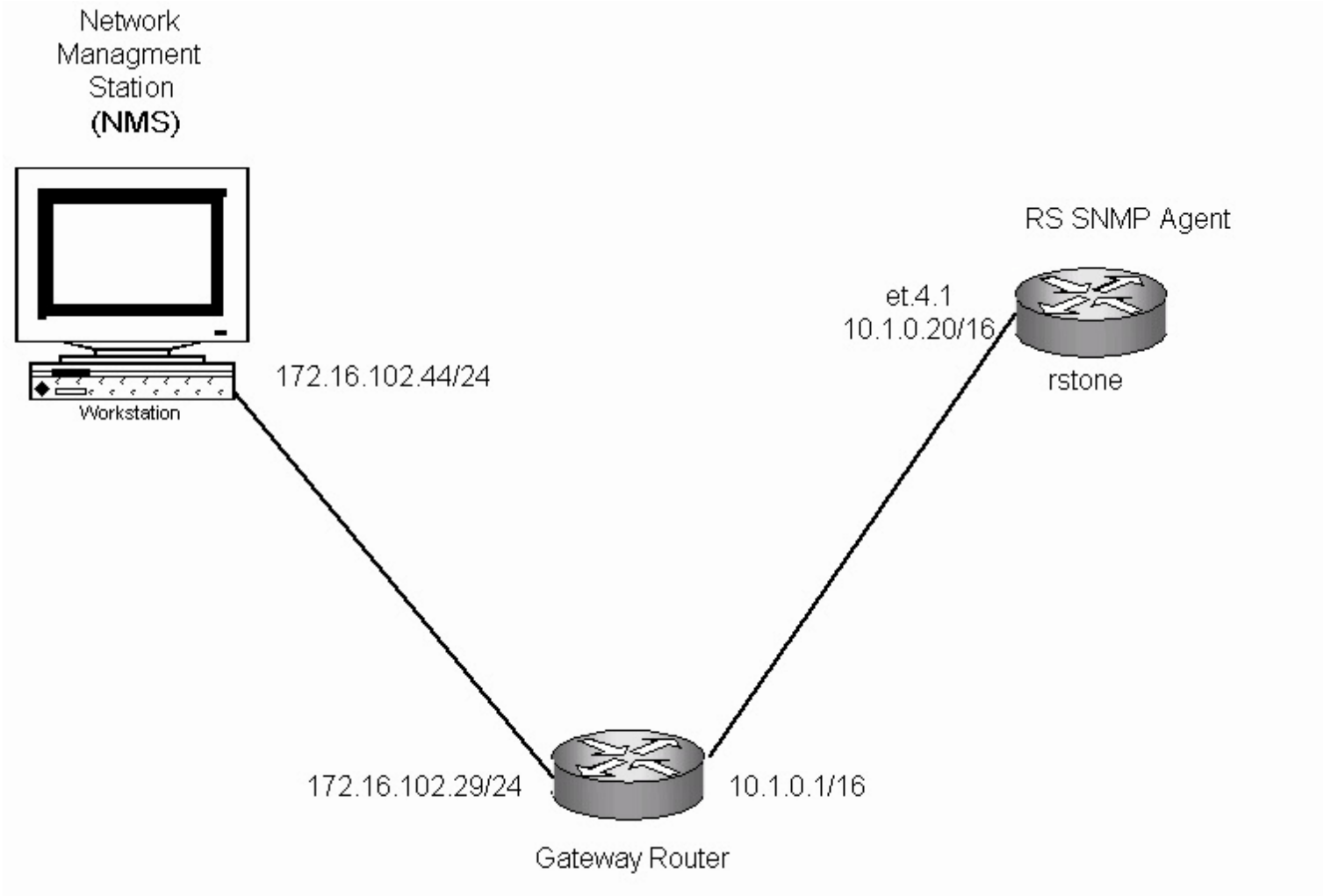
The **tacacs-plus accounting command level** command allows you to specify the types of commands logged to the TACACS+ server. Level 15 logs all configure, enable, and user commands. Level 10 logs all configure and enable commands. Level 5 logs only configure commands. Recall that each log entry has a user ID and timestamp, so the level setting is an important consideration for controlling the size and granularity of the server's log.

Basic SNMP and Trap Configuration

Arshad Syed
RTAC Carrier Account Team
May 15, 2002

The Simple Network Management Protocol (SNMP) is an application layer protocol used to monitor and manage TCP/IP-based networks. SNMP defines a client/server relationship. The client program (called the network manager) makes virtual connections to a server program (called the SNMP agent) which executes on a remote network device, and serves information to the manager regarding the device's status. The example below demonstrates how to configure the SNMPv1 agent on the RS router. The basic configuration shows how to restrict which Network Management Station (NMS) or network manager is allowed access to the RS agent. It also shows how to configure the agent to send traps to the network manager and also how to source the traps from a specific interface.	
RapidOS Version Tested	8.0.3.5
RapidOS Versions Working with this Configuration	7.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 7.0.0.0
Hardware Specifics	N/A

Diagram



Configurations

```
interface create ip to_rs_manager address-netmask 10.1.0.20/16 port et.4.1
acl rs_manager permit udp 172.16.102.44 any any any
acl rs_manager apply service snmp
ip add route 172.16.102.0/24 gateway 10.1.0.1
system set name rstone
system set idle-timeout serial 0
snmp set trap-source to_rs_manager
snmp set community readonly privilege read
snmp set community readwrite privilege read-write
snmp set target 172.16.102.44 community traponly status enable
```

Comments

Verify ip connectivity between the Network Management Station (NMS) and the RS snmp agent.

```
rstone# ping 172.16.102.44
PING 172.16.102.44 (172.16.102.44): 36 data bytes
44 bytes from 172.16.102.44: icmp_seq=0 ttl=127 time=1.476 ms

--- 172.16.102.44 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.476/1.476/1.476 ms
```

The following SNMP show commands provide information on the community strings configured, the snmp trap target address and snmp statistics.

- **snmp show community** displays all the community strings configured on RS snmp agent and the privileges associated with each community.

```
rstone# snmp show community

Community Table:
Index Community String         Privilege
1.    readonly                 READ-ONLY
2.    readwrite                READ-WRITE
```

- **snmp show trap** displays the ip address of the trap target server. By default, the RS sends traps to UDP port 162. By default, all traps are enabled once a trap target is enabled except for SNMPv1 authentication traps.

```
rstone# snmp show trap

Trap Target Table:
Index Trap Target Addr    Community String    Status    Port  Owner

1.    172.16.102.44       traponly            enabled   162   monitor

Traps by Type:
Authentication trap: disabled
Frame Relay  : enabled
OSPF         : enabled
Spanning Tree: enabled
BGP          : enabled
VRRP         : enabled
Environmental: enabled
Link Up/Down : enabled
Link Up/Down Traps disabled by physical port:
No traps per port are disabled.

Trap source address: 10.1.0.20
Trap transmit rate: 1 per 2 seconds
```

- **snmp show statistics** displays snmp stats such as number of bad community names received or the number of ‘get’ or ‘set’ requests processed by the agent.

```
rstone# snmp show statistics
SNMP statistics:
        332 packets received
                332 get requests
                0 get-next requests
                0 get-bulk requests
                0 set requests
                0 bad SNMP versions
                0 bad community names
                0 ASN.1 parse errors
                0 PDUs too big
        333 packets sent
                332 get responses
                0 get-next responses
                0 get-bulk responses
                0 set responses
                0 response PDUs too big
                0 no such name errors
                0 bad values
                0 general errors
        1 traps sent
```

```
                0 traps in queue
                0 traps dropped due to queue overflow
                0 traps dropped due to send failures
```

- **snmp show all** displays all the above information.

```
rstone# snmp show all
SNMP Agent status:
        enabled mode
SNMP Last 5 Clients:
        172.16.102.44   2002-04-22 19:18:42
        172.16.102.44   2002-04-22 19:19:12
        172.16.102.44   2002-04-22 19:17:12
        172.16.102.44   2002-04-22 19:17:42
        172.16.102.44   2002-04-22 19:18:12

SNMP tftp status:

Agent address: 0.0.0.0
Config filename: None configured
Transfer active: false
Transfer status: idle (1)
Transfer operation: No Operation (1)
Current Errors: No error status to report

SNMP Chassis Identity:
not configured.

Trap Target Table:
Index Trap Target Addr    Community String    Status    Port  Owner

1.    172.16.102.44       traponly            enabled   162   monitor

Traps by Type:
Authentication trap: disabled
Frame Relay  : enabled
OSPF         : enabled
Spanning Tree: enabled
BGP          : enabled
VRRP         : enabled
Environmental: enabled
Link Up/Down : enabled
Link Up/Down Traps disabled by physical port:
No traps per port are disabled.

Trap source address: 10.1.0.20
Trap transmit rate: 1 per 2 seconds

Community Table:
Index Community String         Privilege
1.    readonly                 READ-ONLY
2.    readwrite                READ-WRITE

SNMP statistics:
        337 packets received
                337 get requests
                0 get-next requests
                0 get-bulk requests
                0 set requests
                0 bad SNMP versions
```

```
        0 bad community names
        0 ASN.1 parse errors
        0 PDUs too big
338 packets sent
        337 get responses
        0 get-next responses
        0 get-bulk responses
        0 set responses
        0 response PDUs too big
        0 no such name errors
        0 bad values
        0 general errors
1 traps sent
        0 traps in queue
        0 traps dropped due to queue overflow
        0 traps dropped due to send failures
```

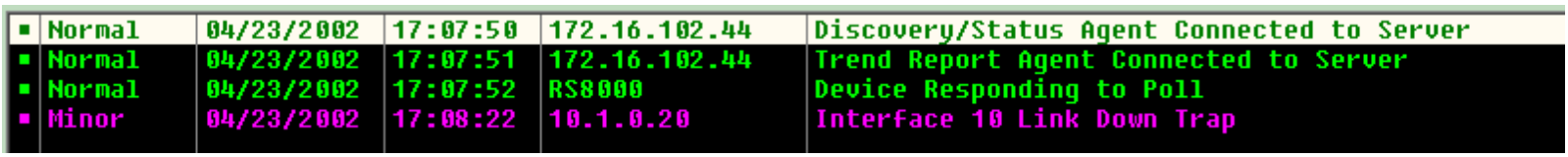
Trap Example

The following example shows a trap being sent from the RS router, in the event a link on the RS router goes down, in this example port et.4.8. The subsequent capture on the NMS shows the source address from where the trap was sent i.e 10.1.0.20

RS SNMP Agent Sending Link Down Trap

```
2002-04-23 17:08:17 %STP-I-PORT_STATUS, Port status change detected: et.4.8 - Port
Down
```

Network Manager Receiving Link Down Trap



■	Normal	04/23/2002	17:07:50	172.16.102.44	Discovery/Status Agent Connected to Server
■	Normal	04/23/2002	17:07:51	172.16.102.44	Trend Report Agent Connected to Server
■	Normal	04/23/2002	17:07:52	RS8000	Device Responding to Poll
■	Minor	04/23/2002	17:08:22	10.1.0.20	Interface 10 Link Down Trap

Pebbles of Knowledge

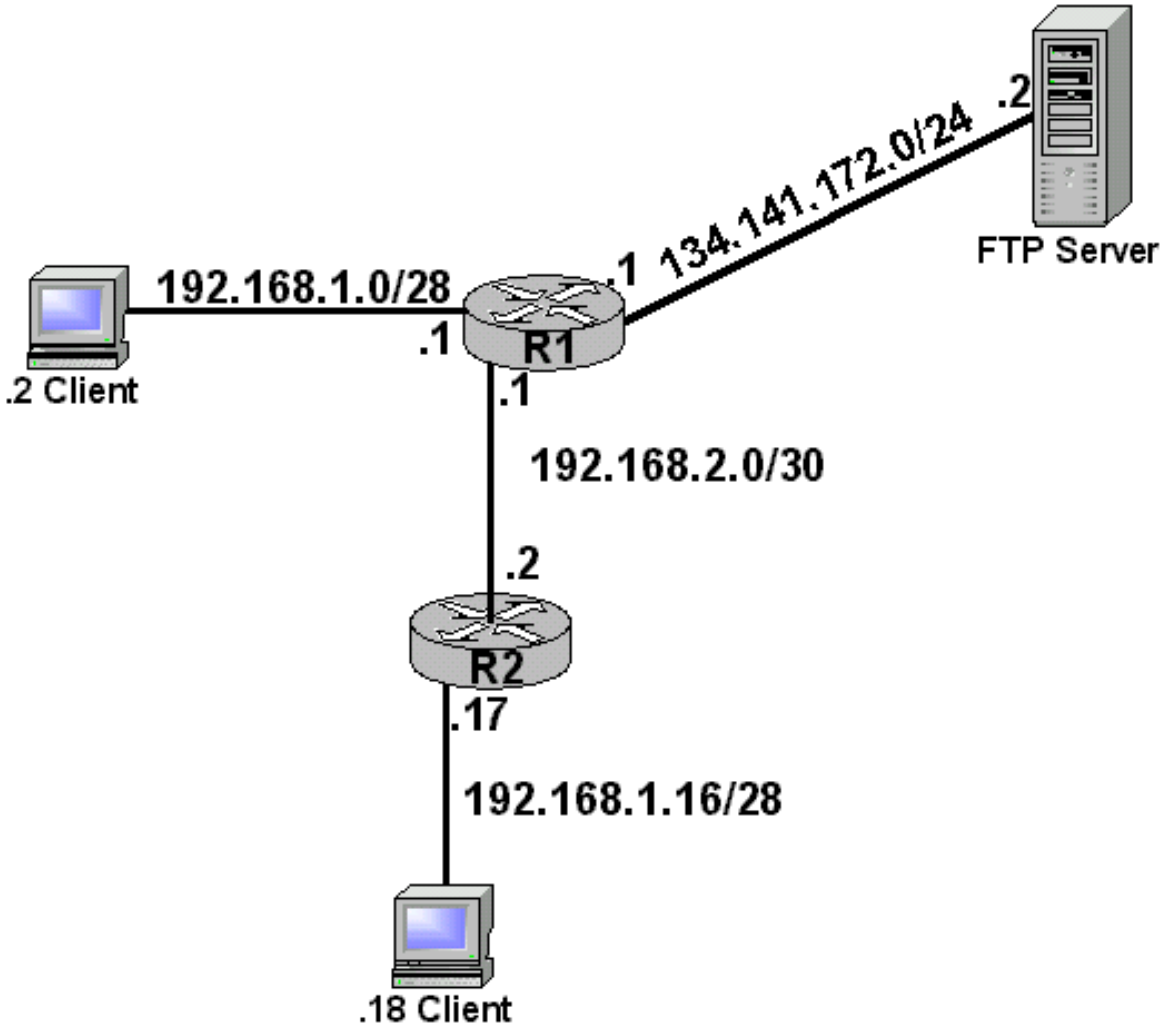
- By default, the SNMP agent is not enabled until an SNMP community string is set via the CLI. This step is mandatory.
- In the example above, only SNMP messages from source IP address 172.16.102.44 will be processed by the SNMP agent, any other source IP address will be dropped. This is done by configuring access control lists (ACLs) as shown, to prevent unauthorized access and serves as an additional level of security. However, this step is optional.
- Configuration of SNMPv1 traps in the RS is a two step process. First, its necessary to specify one or more management stations address. These addresses are referred to as "targets." The RS agent supports up to 32 targets. For each trap generated in the agent, each target will receive a copy of each trap sent. The second step is to define which traps the target should receive. Except for authentication , the rest of the traps are enabled by default.
- Two community strings have been configured with separate levels of privileges. The READ-ONLY privilege allows the administrator to restrict less authorized users the ability to only monitor the network via snmp ‘get’ messages. The READ-WRITE privilege gives full access to monitor and control the network via both ‘get’ and ‘set’ messages.

Network Address Translation Dynamic Port Overload

Richard Foote
Corporate Systems Engineering
April 10, 2001

This configuration will demonstrate the basic NAT function with port overload. It will demonstrate how NAT translations can be performed for both local and non-local clients using port address translation. The internal clients requiring translations need not be directly connected to the RS performing the translations. If a profile, or ACL, matches a packet that enters on an interface marked as "inside" and that packet is destined beyond the interface marked as "outside" the NAT process will occur.	
RapidOS Version Tested	ROS 7.0.0.0 & IA 7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	-AA and above line cards are required to support. *Special Note* - SIPPv3 "T-Series" line cards do not support Port Address Translation. See technical bulletin TB0017-1

Diagram



Configurations

Router R1

```
interface create ip Internet address-netmask 134.141.172.1/24 port et.2.5
interface create ip 1-16Net address-netmask 192.168.1.17/28 port et.2.1
interface create ip Peer address-netmask 192.168.2.1/30 port et.2.8
acl NatACL permit ip 192.168.1.0/24 any any any
ospf create area backbone
ospf add interface all to-area backbone
ospf start
system set name R1
dhcp Server define parameters address-netmask 134.141.172.0/24 gateway 134.141.172.1
dhcp 1-16Net define parameters address-netmask 192.168.1.16/28 gateway 192.168.1.17
dhcp Server define pool 134.141.172.2-134.141.172.2
dhcp 1-16Net define pool 192.168.1.18-192.168.1.30
nat set interface Internet outside
nat set interface Peer inside
nat set interface 1-16Net inside
nat create dynamic local-acl-pool NatACL global-pool 134.141.172.1 enable-ip-overload
```

Router R2

```
interface create ip Peer address-netmask 192.168.2.2/30 port et.2.8
interface create ip 1-0Net address-netmask 192.168.1.1/28 port et.2.1
ospf create area backbone
ospf add interface all to-area backbone
ospf start
system set name R2
dhcp 1-0Net define parameters address-netmask 192.168.1.0/28 gateway 192.168.1.1
dhcp 1-0Net define pool 192.168.1.2-192.168.1.14
```

Comments

The "**`nat show translations all`**" command will provide a view of the binding table. R1's binding table will look very similar to this:

```
Proto  Local/Inside IP        Global/Outside IP      Type       No. of flows
-----  ---------------------  ---------------------  ---------  ------------
TCP    192.168.1.2:1027       134.141.172.1:1025     Dyn. ovr.  0
TCP    192.168.1.2:1026       134.141.172.1:1024     Dyn. ovr.  0
TCP    192.168.1.18:1031      134.141.172.1:1028     Dyn. ovr.  0
TCP    192.168.1.18:1029      134.141.172.1:1027     Dyn. ovr.  0
TCP    192.168.1.18:1028      134.141.172.1:1026     Dyn. ovr.  0
TCP    192.168.1.18:1032      134.141.172.1:1029     Dyn. ovr.  2
```

Using the "**`l3 l3t channel x`**" command in debug mode, where 2 is the channel relating to the hardware flow, you will see these types of entries. These entries relate back to the Network Address Binding table above. The "**`hash: 1024`**" index is the response to the initial request, or ftp server to client. The "**`hash: 61247`**" index is the initial client to server request.

```
Channel: 2, Hash: 1024, Link-location: 3, Address: 0x098dfec0
 Next-index: 0             Flags    : 0x8 ( Ip )
 Security  : ON            Drop opts: OFF
 PortEntry : 37            Tos      : 0              Prot: 6 (TCP)
 SrcSock   : 20            SrcIp    : 134.141.172.2
 DstSock   : 1029          DstIp    : 134.141.172.1
 FwdPtr    : 0x00000000    BkdPtr   : 0x817d06c0
 CEP       : 0x00000004    HH       : 0x00000000 0x000c0028
 NATDestIp : 192.168.1.18  NATDestSock: 1032
 PktCnt    : 6             ByteCnt  : 552
 TtlCnt    : 0             NxtHopMac: 0000c0:04bd9b   AgeCnt: 1

Channel: 2, Hash: 61247, Link-location: 3, Address: 0x090dff00
 Next-index: 0             Flags    : 0x8 ( Ip )
 Security  : ON            Drop opts: OFF
 PortEntry : 33            Tos      : 0              Prot: 6 (TCP)
 SrcSock   : 1032          SrcIp    : 192.168.1.18
 DstSock   : 20            DstIp    : 134.141.172.2
 FwdPtr    : 0x00000000    BkdPtr   : 0x81755cf0
 CEP       : 0x00000004    HH       : 0x00080000 0x00080018
 NATSrcIp  : 134.141.172.1 NATSrcSock: 1029
 PktCnt    : 4             ByteCnt  : 324
 TtlCnt    : 0             NxtHopMac: 000086:43edff   AgeCnt: 1.
```

The diagnostics mode provides the ability to watch the translations as they are being performed. Use the trace commands in diag mode to watch the process. There are three different trace functions that can be enabled. INSIDE, OUTSIDE and APPLICATION translations can be monitored. The "**`nat trace out-in-translations on`**" and the "**`nat trace in-out-translations on`**" commands were enabled and presented to the following output to the console.

```
NAT_OUTSIDE: translated TCP packet Src-ip 134.141.172.2 Src-port 21 Dst-ip
192.168.1.18 Dst-port 1044 is translated to trans_ip 134.141.172.1 trans_port 1028
NAT_INSIDE: received TCP packet Src-ip 192.168.1.18 Src-port 1044 Dst-ip
134.141.172.2 Dst-port 21
NAT_INSIDE: translated TCP packet Src-ip 192.168.1.18 Src-port 1044 is translated to
trans_ip 192.168.1.18 trans_port 1044, Dst-ip 134.141.172.2 Dst-port 21
NAT_OUTSIDE: received TCP packet Src-ip 134.141.172.2 Src-port 21 Dst-ip
134.141.172.1 Dst- port 1028
NAT_OUTSIDE: translated TCP packet Src-ip 134.141.172.2 Src-port 21 Dst-ip
192.168.1.18 Dst-port 1044 is translated to trans_ip 134.141.172.1 trans_port 1028
NAT_INSIDE: MAX. trace count has reached
NAT_INSIDE: received TCP packet Src-ip 192.168.1.18 Src-port 1044 Dst-ip
134.141.172.2 Dst-port 21
```

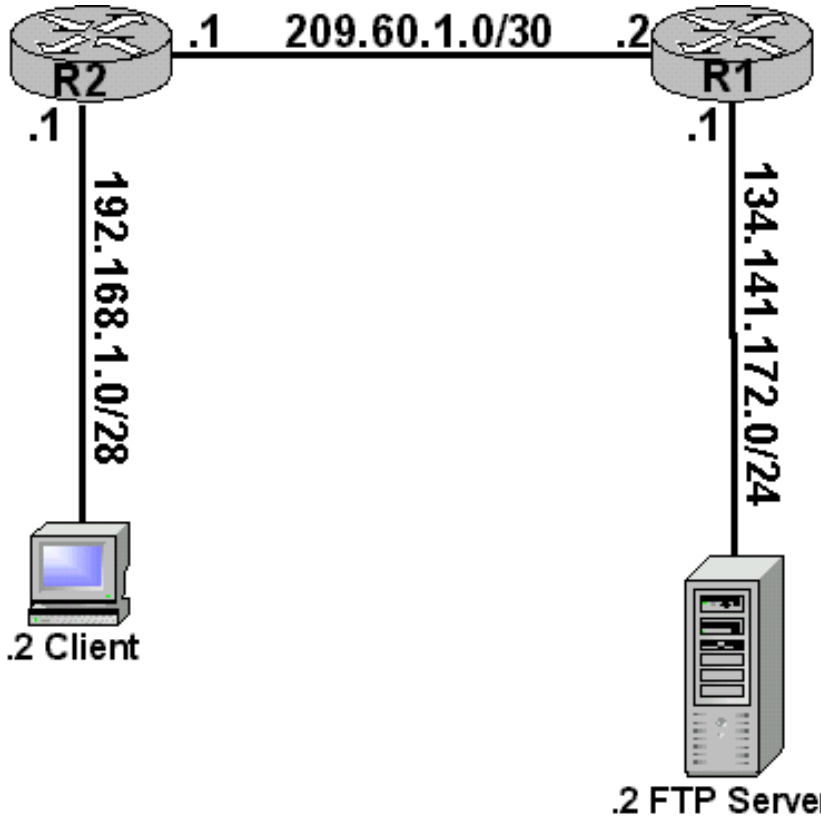
Network Address Translation Dynamic Port Overload Using the Loopback

Richard Foote
Corporate Systems Engineering
April 10, 2001

This configuration will demonstrate the basic dynamic NAT function with port overload. It will demonstrate how the interface deemed as "outside" does not have to be used as the global IP address. When the outside interface is used as the global IP address that interface is no longer available for direct communication, like ping or management queries. This configuration will show how an additional interface applied to the loopback can be used as the global IP address. This may play an important role for BLECs, who needs to manage the in building gear as well as provide address translation services.

RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	-AA and above line cards are required to support. *Special Note* - SIPPv3 "T-Series" line cards do not support Port Address Translation. See technical bulletin TB0017-1

Diagram



Configurations

Router R1

```
interface create ip ServerOfOrigin address-netmask 134.141.172.1/24 port et.2.5
interface create ip Internet address-netmask 209.60.1.2/30 port et.2.8
ospf create area backbone
ospf add interface all to-area backbone
ospf start
dhcp ServerOfOrigin define parameters address-netmask 134.141.172.0/24 gateway
134.141.172.1
dhcp ServerOfOrigin define pool 134.141.172.2-134.141.172.2
```

Router R2

```
interface create ip Client1 address-netmask 192.168.1.1/28 port et.2.1
interface create ip Internet address-netmask 209.60.1.1/30 port et.2.8
interface add ip lo0 address-netmask 207.50.20.1
acl NatACL permit ip 192.168.1.0/28 any any any
ospf create area backbone
ospf add stub-host 207.50.20.1 to-area backbone cost 1
ospf add interface all to-area backbone
ospf start
system set name R2
dhcp client define parameters address-netmask 192.168.1.0/28 gateway 192.168.1.1
dhcp client define pool 192.168.1.2-192.168.1.14
nat set interface Internet outside
nat set interface Client1 inside
```

```
nat create dynamic local-acl-pool NatACL global-pool 207.50.20.1 enable-ip-overload
```

Comments

The "**`nat show translations all`**" command will provide a view of the binding table. Notice the binding table uses the loopback address 207.50.20.1 for a translations and not the actual outside interface 209.60.1.1. This can bee seen in the binding table under "Global/Outside IP".

```
Proto  Local/Inside IP        Global/Outside IP      Type       No. of flows
-----  ---------------------  ---------------------  ---------  ------------
TCP    192.168.1.2:1055       207.50.20.1:1024       Dyn. ovr.  0
TCP    192.168.1.2:1056       207.50.20.1:1025       Dyn. ovr.  2
```

Using the "**`l3 l3t channel x`**" command in debug mode, where 2 is the channel relating to the hardware flow, you will see these types of entries. These entries relate back to the Network Address Binding table above. The "**`hash: 61191`**" index is the initial client to serve request. The "**hash: 62904**" is the response to the initial request, or ftp server to client.

```
Channel: 2, Hash: 61191, Link-location: 3, Address: 0x098dfec0
 Next-index: 0             Flags    : 0x8 ( Ip )
 Security  : ON            Drop opts: OFF
 PortEntry : 33            Tos      : 0              Prot: 6 (TCP)
 SrcSock   : 1056          SrcIp    : 192.168.1.2
 DstSock   : 20            DstIp    : 134.141.172.2
 FwdPtr    : 0x00000000    BkdPtr   : 0x816c11d0
 CEP       : 0x00000004    HH       : 0x000e0000 0x000c0018
 NATSrcIp  : 207.50.20.1   NATSrcSock: 1025
 PktCnt    : 4             ByteCnt  : 324
 TtlCnt    : 0             NxtHopMac: 00e063:66ee71   AgeCnt: 0

Channel: 2, Hash: 62904, Link-location: 3, Address: 0x090dff00
 Next-index: 0             Flags    : 0x8 ( Ip )
 Security  : ON            Drop opts: OFF
 PortEntry : 40            Tos      : 0              Prot: 6 (TCP)
 SrcSock   : 20            SrcIp    : 134.141.172.2
 DstSock   : 1025          DstIp    : 207.50.20.1
 FwdPtr    : 0x00000000    BkdPtr   : 0x819b12b8
 CEP       : 0x00000004    HH       : 0x00000000 0x00080028
 NATDestIp : 192.168.1.2   NATDestSock: 1056
 PktCnt    : 6             ByteCnt  : 552
 TtlCnt    : 0               NxtHopMac: 0000c0:04bd9b   AgeCnt: 0
```

The diagnostics mode provides the ability to watch the translations as they are being performed. Use the trace commands in diag mode to watch the process. There are three different trace functions that can be enabled. INSIDE, OUTSIDE and APPLICATION translations can be monitored. The "**`nat trace out-in-translations on`**" and the "**`nat trace in-out-translations on`**" commands were enabled and presented to the following output to the console.

```
NAT_INSIDE: received TCP packet Src-ip 192.168.1.2 Src-port 1055 Dst-ip 134.141.172.2
Dst-port 21
NAT_INSIDE: translated TCP packet Src-ip 192.168.1.2 Src-port 1055 is translated to
trans_ip 192.168.1.2 trans_port 1055, Dst-ip 134.141.172.2 Dst-port 21
NAT_INSIDE: destination port is ftp control port hence not installing the flow.
NAT_OUTSIDE: received TCP packet Src-ip 134.141.172.2 Src-port 21 Dst-ip 207.50.20.1
```

```
Dst-port 1024
NAT_OUTSIDE: translated TCP packet Src-ip 134.141.172.2 Src-port 21 Dst-ip
192.168.1.2 Dst-port 1055 is translated to trans_ip 207.50.20.1 trans_port 1024
NAT_OUTSIDE: destination port is ftp control port hence not installing the flow
```

TFTP Server Load-Balancing

Austin Hawthorne
Systems Engineering
June 26, 2002

TFTP Load-balancing is a useful feature for architectures that require TFTP servers to reside on the network for mission critical applications such as CMTS configurations, Router/Switch firmware boot systems, etc. The TFTP application acts in such a way that causes it to break many load-balancing (LSNAT) applications. This configuration document will spell out the challenges with the TFTP application and will detail how the RS platform can be used to overcome them to provide a robust and scalable TFTP load-balancing architecture.

The TFTP application uses the concept of Session Identifiers (SID). The SID's are essentially the L4 port numbers used in the UDP header of the transaction. Initially the client sends a Read Request (RRQ) or a Write Request (WRQ) to the server using the well known TFTP port number of 69 as the destination port (dst_port). The client chooses a SID to place in the source port (src_port), let's choose 1025 for this example. When the server sees this request he responds with either data, in case of a RRQ, or an acknowledgment, in case of a WRQ. The server responds to the client using the client's SID as the dst_port (1025), and chooses a SID for itself to use as the src_port, let's choose 2000 for this example. The rest of the transaction takes place between the two SID's chosen by the server and the client. The well known port is not used after the initial packet.

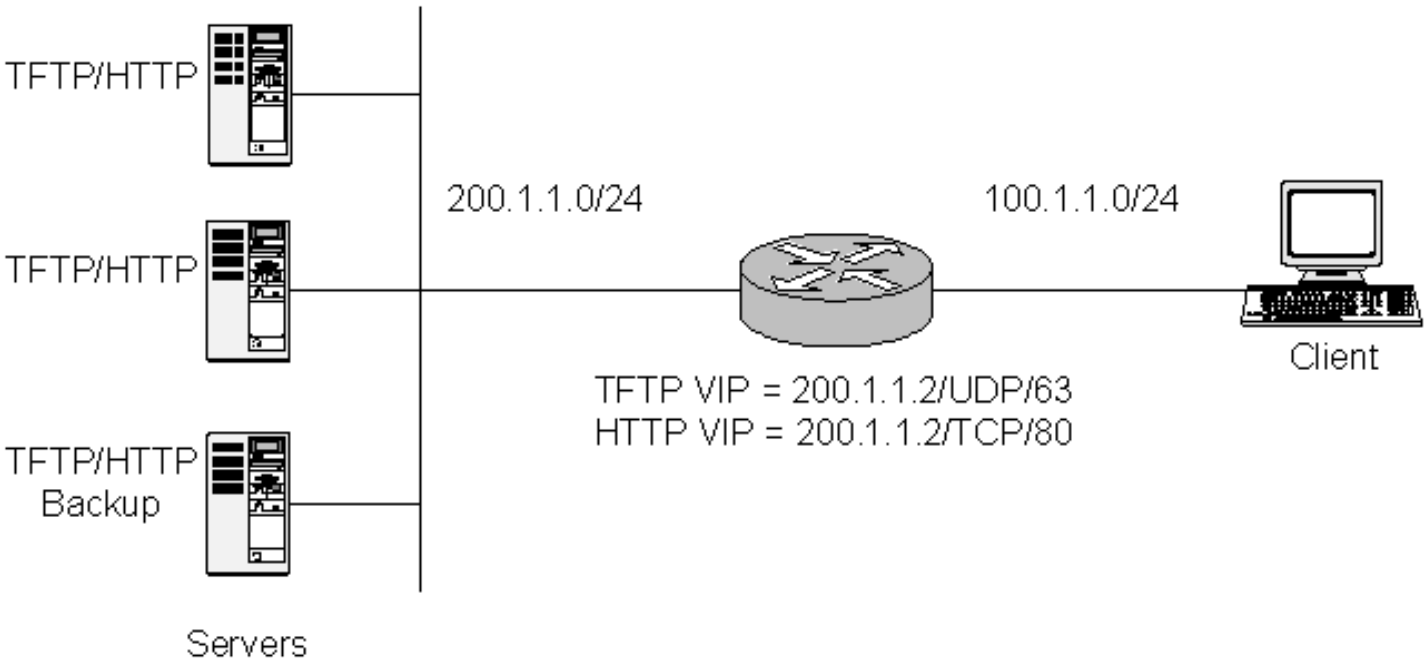
The above behavior breaks traditional load-balancing (LSNAT) because the communication after the initial packet does not take place on the TFTP well-known port number, of which the Virtual IP (VIP) is based (The VIP normally consists of an IP address, protocol, and a port number). We can see this if we walk the packet through. When client sends a RRQ to the server, it sends a packet to the VIP which is based on UDP port number 69. The load-balancer chooses a real-server to send the packet to and then translates the destination IP address of the frame to equal that of the real-server. It then forwards the packet to the real-server. The server processes the packet and replies to the client. It is here that we encounter some issues. Remember that the server arbitrarily chooses a SID and replaces the well-known TFTP port number with the SID. When this packet is seen by the load-balancer, it does not match the original flow installed (source port is different and it does not match the VIP's TFTP port number) when the first packet arrived and the translation was applied, so it bypasses the load-balancing policy without being translated. The packet arrives at the client with the real-server IP address, not the VIP. This will break some TFTP client applications because the process does not recognize that this packet is a reply to the same request it sent to a different IP. Also, if the real-server IP is not routable (for example, RFC 1918 address space), the client will not be able to reach the server again to complete the transaction.

The RS load-balancing feature set can be used to overcome this behavior by providing a change in the flow persistence level. By default the RS classifies a flow with the L4 port information as well as the L3 IP information. You can change this behavior to provide persistence based solely on the IP source and destination addresses. This is called sticky persistence. This allows the application to change the port numbers during the transaction without losing the functionality of the load-balancing feature. The configuration is detailed below.

With this functionality we loss none of the enhanced load-balancing functionality available within the RS firmware, such as Application Check Verifications (ACV), load-distribution algorithms based on least-loaded and

fastest response, and health-check clusters. The configuration below will detail a TFTP load-balancing setup along with a typical setup for HTTP load-balancing (for comparison purposes). Added are configurations for ACV on both, health-check clusters, and the least-loaded load distribution algorithm. The health-check-clusters are needed for the TFTP group. Typically an ACV can run on a generic group of servers, but because a port number was not defined in the VIP for TFTP, the ACV option is not valid, so the health-check-cluster is used to work around this. This is also need to run an ACV with the UDP protocol. Two IP addresses are needed per TFTP server to accomplish this. The configurations reflect load-balancing between two servers with an additional server acting as backup.	
RapidOS Version Tested	8.0.0.10
RapidOS Versions Working with this Configuration	6.1.0.0 and newer for relevant functionality 8.0.0.0 and newer for advanced functions
RapidOS Versions NOT Working with this Configuration	Older than 6.1.0.0
Hardware Specifics	"T" Series

Diagram



Configurations

```
! Create the interfaces for the router
!
interface create ip to_clients address-netmask 100.1.1.1/24 port et.5.9
interface create ip to_servers address-netmask 200.1.1.1/24 port et.5.10
!
! Create a load-balance group for TFTP.  No port will be identified and persistence
is based on source and destination IP address.
```

```
!
load-balance create group-name TFTP virtual-ip 200.1.1.2 protocol udp persistence-
level sticky
!
! Create a Health Check Cluster for the primary servers to check application port 69.
This will contain the first IP on the Server's interface or loopback.
!
load-balance create health-check-cluster TFTP_1 ip-to-check 200.1.1.10 port-to-check
69
load-balance create health-check-cluster TFTP_2 ip-to-check 200.1.1.12 port-to-check
69
load-balance create health-check-cluster TFTP_Backup ip-to-check 200.1.1.14 port-to-
check 69
!
! Configure the Health Check Clusters to use UDP for the ACV
!
load-balance set health-check-cluster-options TFTP_1 check-udp
load-balance set health-check-cluster-options TFTP_2 check-udp
load-balance set health-check-cluster-options TFTP_Backup check-udp
!
! Add the servers IP to the Health Check Cluster.  This will contain the second IP
configured on the server’s interface or loopback.
!
load-balance add host-to-group 200.1.1.11 group-name TFTP health-check-cluster TFTP_1
load-balance add host-to-group 200.1.1.13 group-name TFTP health-check-cluster TFTP_2
load-balance add host-to-group 200.1.1.15 group-name TFTP health-check-cluster
TFTP_Backup status backup
!
! Configure the load policy to be based on least-loaded server.
!
load-balance set group-options TFTP policy least-loaded
!
! Configure HTTP load-balancing on the same real-servers with the same IP address but
! different port.
!
load-balance create group-name HTTP virtual-ip 200.1.1.2 protocol tcp virtual-port 80
persistence-level tcp
!
load-balance add host-to-group 200.1.1.11 group-name HTTP port 80
load-balance add host-to-group 200.1.1.13 group-name HTTP port 80
load-balance add host-to-group 100.1.1.15 group-name HTTP port 80 status backup
load-balance set group-options HTTP policy least-loaded
```

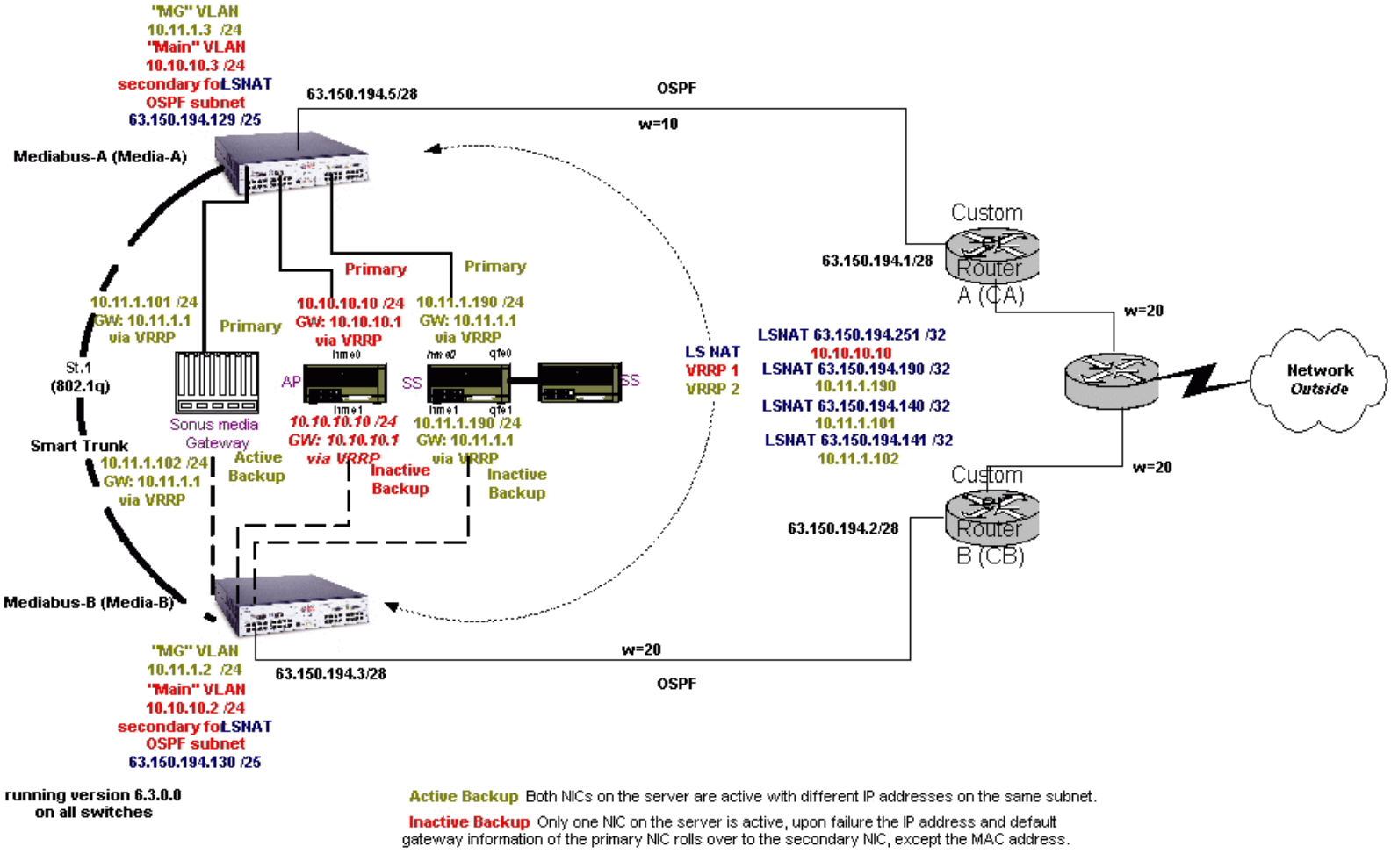
OSPF for VoIP Media Gateway & Signaling Gateway Redundancy

Navid Feizy
Systems Engineering
May 25, 2001

We provide 100% redundancy and resiliency for Sonus VoIP media and signaling gateways to the IP and the PSTN world using OSPF as the routing protocol. We used VRRP and LSNAT for resiliency and redundancy as well. With this design we allowed for a 1second down time upon any link failures due to OSPF re-convergence. 1 Second is acceptable downtime for a carrier to offer toll quality VoIP solution to their customers. Also this design allowed for all TCP sessions "active calls" to remain intact and no calls were lost during a 1 second link failure. This design provides the 99.999% uptime for any telecommunication carrier.

RapidOS Version Tested	6.3.0.0
RapidOS Versions Working with this Configuration	6.3.0.0 and newer
RapidOS Versions NOT Working with this Configuration	5.x.x.x
Hardware Specifics	N/A

Diagram



running version 6.3.0.0
on all switches

Active Backup Both NICs on the server are active with different IP addresses on the same subnet.

Inactive Backup Only one NIC on the server is active, upon failure the IP address and default gateway information of the primary NIC rolls over to the secondary NIC, except the MAC address.

Configurations

Media_Bus_A

```
smarttrunk create st.1 protocol no-protocol
smarttrunk add ports gi.4.2 to st.1
vlan make trunk-port st.1
vlan create main ip id 10
vlan create mg ip id 11
vlan create public ip id 101
vlan add ports et.1.(1-16) to public
vlan add ports et.2.(1-4) to mg
vlan add ports et.2.(7-10) to main
vlan add ports et.2.5 to public
vlan add ports et.2.6 to mg
vlan add ports et.2.16 to public
interface create ip to_CA address-netmask 63.150.194.5/28 port gi.4.1
interface create ip main address-netmask 10.10.10.3/24 vlan main
interface create ip mg address-netmask 10.11.1.3/24 vlan mg
interface create ip public address-netmask 63.150.194.129/25 vlan public
interface add ip lo0 address-netmask 1.1.1.1/32
ip-router global set router-id 1.1.1.1
ip add route default gateway 63.150.194.1
system set name mediabus-A
system set password login !1mediabus
system set password enable !1password
ntp set server 10.10.10.10 interval 60
ospf create area backbone
ospf add interface to_CA to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 10
ospf add interface 63.150.194.129 to-area backbone
ospf start
ip-redundancy create vrrp 1 interface main
ip-redundancy create vrrp 2 interface mg
ip-redundancy associate vrrp 1 interface main address 10.10.10.1/24
ip-redundancy associate vrrp 2 interface mg address 10.11.1.1/24
ip-redundancy set vrrp 1 interface main preempt-mode disabled
ip-redundancy set vrrp 2 interface mg preempt-mode disabled
ip-redundancy set vrrp 1 interface main priority 200
ip-redundancy set vrrp 2 interface mg priority 200
ip-redundancy start vrrp 1 interface main
ip-redundancy start vrrp 2 interface mg
arp set interface all keep-time 1
smarttrunk set load-policy link-utilization on st.1
load-balance create group-name AP1 virtual-ip 63.150.194.251 protocol ip persistence-
level ip
load-balance add host-to-group 10.10.10.10 group-name AP1 port ip
load-balance create group-name MG1c11 virtual-ip 63.150.194.140 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.101 group-name MG1c11 port ip
load-balance create group-name MG1c21 virtual-ip 63.150.194.142 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.103 group-name MG1c21 port ip
load-balance create group-name MG2c11 virtual-ip 63.150.194.145 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.105 group-name MG2c11 port ip
load-balance create group-name MG2c21 virtual-ip 63.150.194.147 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.107 group-name MG2c21 port ip
load-balance set group-options AP1 ping-int 1 ping-tries 1
load-balance set group-options MG1c11 ping-int 1 ping-tries 1
load-balance set group-options MG1c21 ping-int 1 ping-tries 1
load-balance set group-options MG2c11 ping-int 1 ping-tries 1
load-balance set group-options MG2c21 ping-int 1 ping-tries 1
```

Media_Bus_B

```
smarttrunk create st.1 protocol no-protocol
smarttrunk add ports gi.4.2 to st.1
vlan make trunk-port st.1
```

```
vlan create main ip id 10
vlan create mg ip id 11
vlan create public ip id 101
vlan add ports et.1.(1-16) to public
vlan add ports et.2.(1-4) to mg
vlan add ports et.2.(7-10) to main
vlan add ports et.2.5 to public
vlan add ports et.2.6 to mg
vlan add ports et.2.16 to public
interface create ip to_CA address-netmask 63.150.194.3/28 port gi.4.1
interface create ip main address-netmask 10.10.10.2/24 vlan main
interface create ip mg address-netmask 10.11.1.2/24 vlan mg
interface create ip public address-netmask 63.150.194.130/25 vlan public
interface add ip lo0 address-netmask 2.2.2.2/32
ip-router global set router-id 2.2.2.2
ip add route default gateway 63.150.194.2
system set name mediabus-B
system set password login !1mediabus
system set password enable !1password
ntp set server 10.10.10.10 interval 60
ospf create area backbone
ospf add interface to_CA to-area backbone
ospf add stub-host 2.2.2.2 to-area backbone cost 10
ospf add interface 63.150.194.130 to-area backbone
ospf start
ip-redundancy create vrrp 1 interface main
ip-redundancy create vrrp 2 interface mg
ip-redundancy associate vrrp 1 interface main address 10.10.10.1/24
ip-redundancy associate vrrp 2 interface mg address 10.11.1.1/24
ip-redundancy set vrrp 1 interface main preempt-mode disabled
ip-redundancy set vrrp 2 interface mg preempt-mode disabled
ip-redundancy set vrrp 1 interface main priority 200
ip-redundancy set vrrp 2 interface mg priority 200
ip-redundancy start vrrp 1 interface main
ip-redundancy start vrrp 2 interface mg
arp set interface all keep-time 1
smarttrunk set load-policy link-utilization on st.1
load-balance create group-name AP1 virtual-ip 63.150.194.251 protocol ip persistence-
level ip
load-balance add host-to-group 10.10.10.10 group-name AP1 port ip
load-balance create group-name MG1c11 virtual-ip 63.150.194.140 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.101 group-name MG1c11 port ip
load-balance create group-name MG1c21 virtual-ip 63.150.194.142 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.103 group-name MG1c21 port ip
load-balance create group-name MG2c11 virtual-ip 63.150.194.145 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.105 group-name MG2c11 port ip
load-balance create group-name MG2c21 virtual-ip 63.150.194.147 protocol ip
persistence-level ip
load-balance add host-to-group 10.11.1.107 group-name MG2c21 port ip
load-balance set group-options AP1 ping-int 1 ping-tries 1
load-balance set group-options MG1c11 ping-int 1 ping-tries 1
load-balance set group-options MG1c21 ping-int 1 ping-tries 1
load-balance set group-options MG2c11 ping-int 1 ping-tries 1
load-balance set group-options MG2c21 ping-int 1 ping-tries 1
```

Comments

Users need to have the ability to access the following servers from the Internet via the public IP address that is associated to each server. These servers in reality have a private IP address. Riverstone takes on the intelligence of translating a single public IP address to a single or multiple private IP addresses of the customer's AP "adjunct processor", Media Gateway, and SS "Soft switch controllers" via LSNAT. LSNAT is used for three purposes, one is for security, the other is for ease of customer configuration and finally a customer can use any private IP address they wish for their suite of VoIP gateways and servers, while they can save on using scarce public IP addresses for these devices.

The AP is the brains of the operation. In order to configure any of the servers you will need to log into the AP, the AP also gathers SNMP type information from all the other servers and reports results to a management station(s). Also the AP provides the boot up operating system as NFS for all the servers. Among other things access to the AP and the Media Gateway at all times is the most crucial part of the customer's solution. The Media Gateway handles calls being processed and calls already in process and is the SIP "session initiation protocol" signaling brains of the VoIP solution to the data "IP" world and the voice "PSTN" world. Riverstone has to provide access to the AP and the Media Gateway by all means. In case of a link, router, and server failure, or all at the same time, the down time before redundancy kicks in and makes full restoration must be **1 second**. If this time is any more than 1 second the VoIP solution is not considered viable and carriers cannot guarantee 99.999% uptime. Riverstone makes this a reality!

Call center personnel doing provisioning and all other things a call center personnel does is accomplished by accessing the LSNAT IP addresses such as 63.150.194.xxx from the Network "outside ".

Note the public IP addresses used for Media_Bus_A's and Media_Bus_B's **Public VLAN**, they are **63.150.194.129/25** and **63.150.194.130/25**. We chose the subnet mask of /25 to make sure all the /32 public IP addresses that are being used for LSNAT and both /28 public IP addresses for the uplinks to CA and CB by both Riverstone routers are included within this range. This way OSPF will hide the stub host addresses inside this range by always keeping the full range "/25" in the FIB of all routers participating in OSPF and OSPF re-convergence during a router failure allows us to have an instant route change thus maintaining 1 second fail-over time. We could have used stub hosts instead, but using stub hosts causes OSPF to make an SPF recalculation and it will take up to 40 seconds before a new route is discovered. Especially since the stub hosts are the OSPF router ids. With doing this we essentially fooled OSPF by keeping the whole subnet in the fib at all times. Also, what makes this design possible is our capability to pass 802.1Q tags over a smart trunk, this gives us the ability to have the same identical LSNAT configuration on both routers! The customer wanted one link to always be the primary link and if it failed the secondary link needs to pick up in 1 second, that's why we gave the link to CA a cost of 10.

Upon a server NIC failure, the IP address and all related information on that NIC will roll over to the secondary NIC on the same server, that's why in essence we need the same identical information available in the L2/L3 tables of both Riverstone routers and 802.1Q tagging along with routing, LSNAT, and being able to assign IP addresses to VLANs makes all this a reality!!! The Riverstone "Media_Bus_A" serving the active side should automatically know, that it is the active side, and populate its L2/L3 tables accordingly and as servers roll over to the other side the other Riverstone "Media_Bus_B" automatically becomes active and assumes responsibility until things change again!!

Policy Based Routing, Traffic Engineering & Recursive Lookup

Richard Foote
Corporate Systems Engineering
April 16, 2001

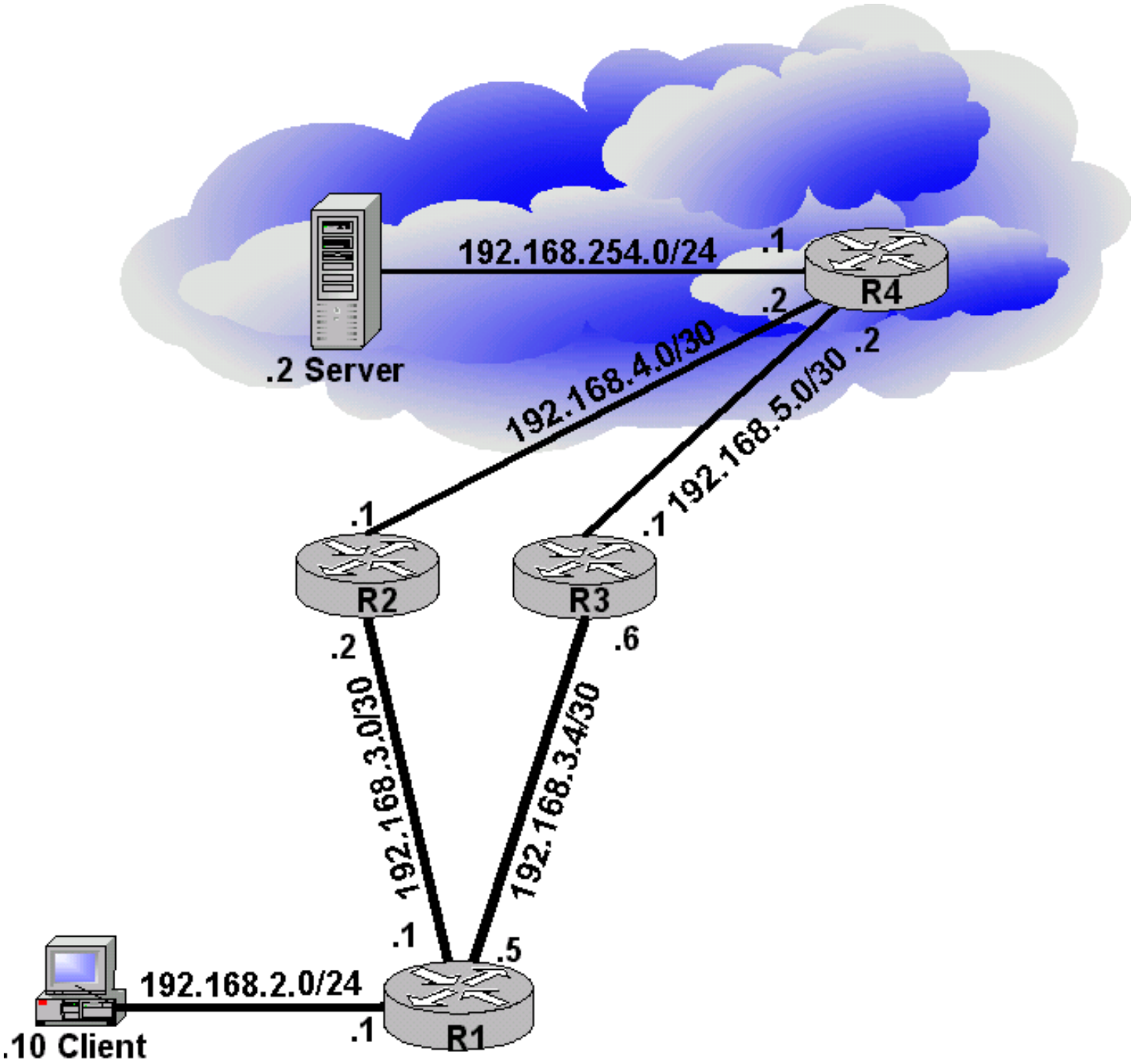
The configuration will demonstrate how policy based routing can be used to provide a level of traffic engineering. In this example, two possible next hops are available. However, one of the next hops is preferred and for whatever reason it would be advantageous to use it over the other. This could be because of reliability, dollar cost or some other reason. This configuration also demonstrates how to ensure that the entire path is valid before forwarding the request into a potential black hole. By pointing the next hop to "wan egress" the pinger task will ensure that the "wan egress" port is responding to pings before forwarding traffic in that direction. Using a next hop that is not local to the router defining the policy is know as recursive lookup. Simply put, the router with the defined policy uses its routing table to find out how to resolve the next-hop-gateway to the next hop router.

RapidOS Version Tested	6.3.0.5
RapidOS Versions Working with this Configuration	6.2.0.3
RapidOS Versions NOT Working with this Configuration	3.1.0.0, 6.0.0.0, 5.1.x.x [1] & 7.0.0.0 [2]
Hardware Specifics	N/A

[1] Unable to set "**`pinger-options`**". All other functionality is available.

[2] Unable to set "**`pinger-options`**" less than default. This will be resolved in a 7.0 patch release. This appears to have been an issue with the merge code. All other functionality is available.

Diagram



Configurations

Router R1

```
vlan create Client ip
vlan add ports et.2.(1-2) to Client
interface create ip ToNet address-netmask 192.168.3.1/30 port et.2.8
interface create ip ToNetAlt address-netmask 192.168.3.5/30 port et.2.7
interface create ip Client address-netmask 192.168.2.1/24 vlan Client
interface add ip en0 address-netmask 24.112.72.1/21
interface add ip lo0 address-netmask 10.1.1.1
acl PolACL permit ip any any any any
```

```
ip-router global set router-id 10.1.1.1
ospf create area backbone
ospf add interface all to-area backbone
ospf start
aging l3 set timeout 5
system set name R1
ip-policy PreferredRoutePol permit acl PolACL next-hop-list 192.168.4.1 action policy-
first
ip-policy PreferredRoutePol apply interface Client
ip-policy PreferredRoutePol set pinger on
ip-policy PreferredRoutePol set pinger-options ping-int 2 ping-tries 2
dhcp Client define parameters address-netmask 192.168.2.0/24 gateway 192.168.2.1
dhcp Client define pool 192.168.2.10-192.168.2.15
```

Router R2

```
interface create ip ToClientRouter address-netmask 192.168.3.2/30 port et.2.8
interface create ip PrimeRoute address-netmask 192.168.4.1/30 port et.2.1
interface add ip lo0 address-netmask 10.2.2.2
ip-router global set router-id 10.2.2.2
ospf create area backbone
ospf add interface all to-area backbone
ospf start
system set name R2
```

Router R3

```
interface create ip ToCLientRouter address-netmask 192.168.3.6/30 port et.2.7
interface create ip AltRoute address-netmask 192.168.5.1/30 port et.2.2
interface add ip lo0 address-netmask 10.3.3.3
ip-router global set router-id 10.3.3.3
ospf create area backbone
ospf add interface all to-area backbone
ospf start
system set name R3
```

Router R4

```
interface create ip Service address-netmask 192.168.254.1/24 port et.2.8
interface create ip InternetPrime address-netmask 192.168.4.2/30 port et.2.1
interface create ip InternetAlt address-netmask 192.168.5.2/30 port et.2.2
interface add ip lo0 address-netmask 10.4.4.4
ip-router global set router-id 10.4.4.4
ospf create area backbone
ospf add interface all to-area backbone
ospf start
system set name R4
dhcp Service define parameters address-netmask 192.168.254.0/24 gateway 192.168.254.1
dhcp Service define pool 192.168.254.2-192.168.254.2
```

Comments

The configuration statement on Router R1, **"aging l3 set timeout 5"** is used to age out the l3 flows quickly in order to show how normal packet distribution would occur without the policy statement. Normal L3 aging is 30 seconds.

In order to properly demonstrate the affect of policy based routing it is suggested you use the following methodology when performing validation of the above.

Remove the **"ip-policy PreferredRoutePol apply interface Client"** from the router R1 configuration. Use the client workstation to trace the route from client to 192.168.254.2. Perform this tracing numerous times, waiting a minimum of five seconds between traces. You will notice each path is being used to distribute the load across requests.

```
Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.2
   1    1 ms     1ms    1ms     192.168.4.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.

Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.6
   1    1 ms     1ms    1ms     192.168.5.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.
```

Add the **"ip-policy PreferredRoutePol apply interface Client"** to router R1 configuration. Perform the same tracing tests that were performed without the command from the previous step. You will notice all client to 192.168.254.2 requests take the same path every time, following the policy.

```
Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.2
   1    1 ms     1ms    1ms     192.168.4.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.

Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.2
   1    1 ms     1ms    1ms     192.168.4.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.
```

Take a look at the active policy for status information. Use the **"ip-policy show all"** form enable mode. You will notice that you may also perform application level checks, TCP port open/close and content verification, for the configured policy. The pinger task is not the only validation process.

```
R1# ip-policy show all
-------------------------------------------------------------------------------
IP Policy name     : PreferredRoutePol
Applied Interfaces : Client
Load Policy        : first available
Health Check       : enabled

Pinger Options:
```

```
-------------
Destination Port                  : 0
Ping Interval (in secs.)          : 2
Ping Tries                        : 2
Application Interval (in secs.)   : 15
Application Tries                 : 15
Application Checking              : Disabled

ACL          Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort   TOS TOS-MASK
Prot
---          --------------     -------------      -------   -------   --- -------- --
--
PolACL       anywhere           anywhere           any       any       any  None
IP

                                                      Next Hop Information
                                                      --------------------
 Seq   Rule   ACL          Cnt      Action       Next Hop        Cnt      Last
 ---   ----   --------     ---      -----------  --------        ---      ----
 10    permit PolACL       65       Policy First 192.168.4.1     32       Up
 65536 deny   deny         0        N/A          normal fwd      N/A      N/A
```

If the pinger task fails to validate the next-hop, in this case 192.168.4.1, then the **"policy first"** action will allow the policy to be bypassed. The routing table will be consulted for alternate routes.

You can simulate this by simply pulling the interconnection between router R2 and router R4. The results of your trace route will show all packets traversing the alternate path. Before pulling the link connecting router R2 and router R4 start a continuous ping from the client station to 192.168.254.2 using "`ping 192.168.2.254 –t`" dos command or platform equivalent. You will notice the following results.

```
Pinging 192.168.254.2 with 32 bytes of data:
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=1ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Request timed out.
Request timed out.
Reply from 192.168.254.2: bytes=32 time=3ms TTL=125
Reply from 192.168.254.2: bytes=32 time=1ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=1ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.2.1: Destination host unreachable
Reply from 192.168.254.2: bytes=32 time=1ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
Reply from 192.168.254.2: bytes=32 time=2ms TTL=125
```

The "`Request timed out`" message was a result of the cable being disconnected which connected R2 to R4. The ping automatically found another path through the network and continued. The "`Destination host unreachable`" was a result of the slight interruption which occurred when the link between router R2 and R4 was recovered. Once again traffic used the policy to select the preferred path as indicated in the policy.

When the link between router R2 and R4 failed the status for the policy changed. Using the **"ip-policy show all"** you notice the state has changed to down. This is the indication the pinger task can not validate the next hop in the policy statement.

```
R1# ip-policy show all
-------------------------------------------------------------------------------

IP Policy name     : PreferredRoutePol
Applied Interfaces : Client
Load Policy        : first available
Health Check       : enabled

Pinger Options:
-------------
Destination Port                  : 0
Ping Interval (in secs.)          : 2
Ping Tries                        : 2
Application Interval (in secs.)   : 15
Application Tries                 : 15
Application Checking              : Disabled

ACL          Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort   TOS TOS-MASK
Prot
---          --------------     -------------      -------   -------   --- -------- --
--
PolACL       anywhere           anywhere           any       any       any  None
IP

                                                      Next Hop Information
                                                      --------------------
 Seq   Rule   ACL          Cnt      Action       Next Hop        Cnt      Last
 ---   ----   --------     ---      -----------  --------        ---      ----
 10    permit PolACL       92       Policy First 192.168.4.1     55       Dwn
 65536 deny   deny         0        N/A          normal fwd      N/A      N/A
```

During this failure you can check the traffic flow by tracing the route from the client to 192.168.254.2. The results will look like this.

```
Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.6
   1    1 ms     1ms    1ms     192.168.5.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.

Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.6
   1    1 ms     1ms    1ms     192.168.5.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.
```

Once the link is recovered tracing reveals the preferred path, as stated by the policy, is once again being used.

```
Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
```

```
   1    1 ms     1ms    1ms     192.168.3.2
   1    1 ms     1ms    1ms     192.168.4.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.

Tracing route to 192.168.254.2 over a maximum of 30 hops
   1    1 ms     1ms    1ms     192.168.2.1
   1    1 ms     1ms    1ms     192.168.3.2
   1    1 ms     1ms    1ms     192.168.4.2
   1    1 ms     1ms    1ms     192.168.254.2
Trace complete.
```

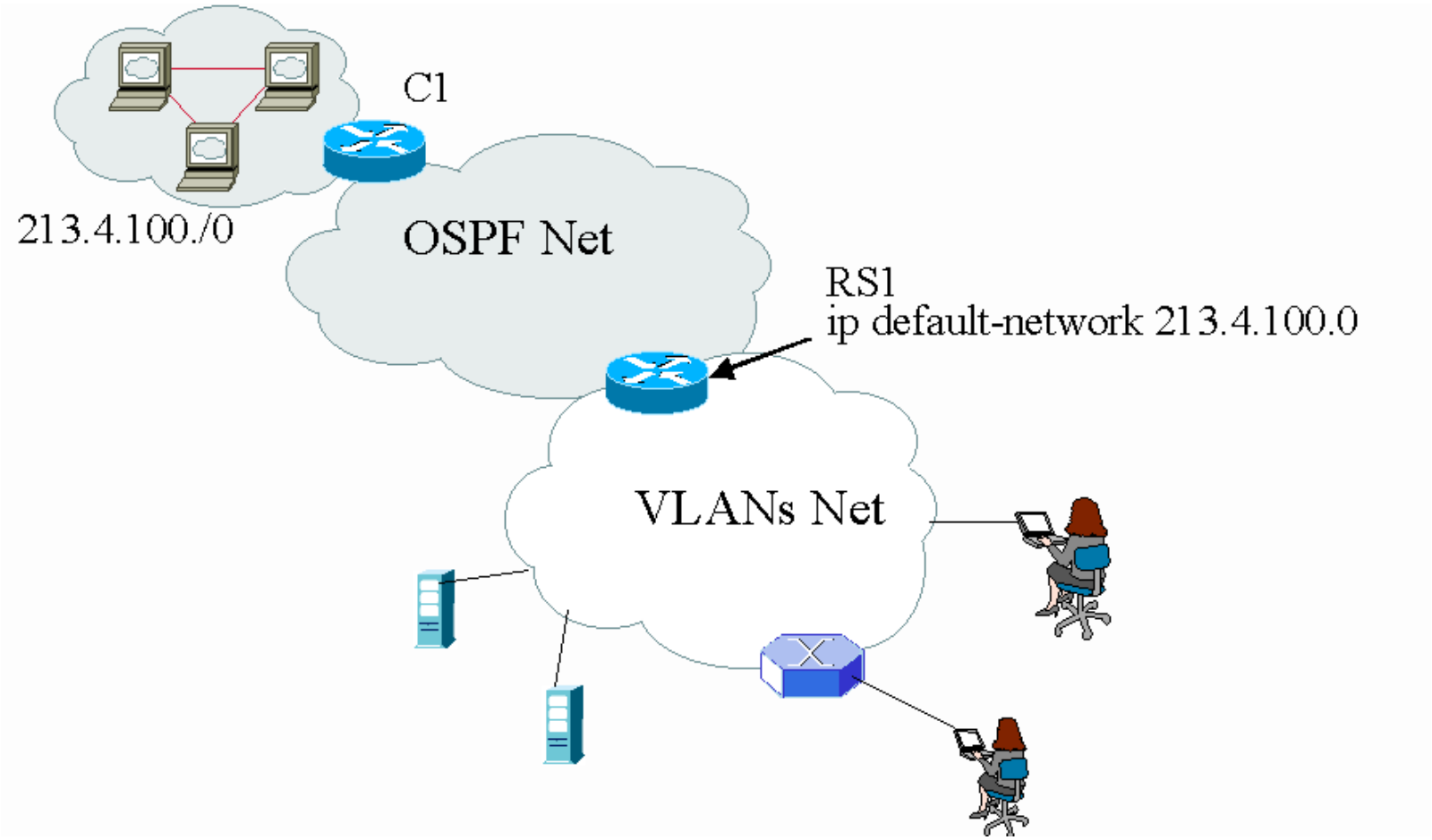
The **"action policy-first"** used when defining the next-hop for the policy on router R1 is one of three available action settings. We have seen how the Policy-first will use the policy configured and only consult the routing table when the policy can not service the need. Policy-only ensures that every matching packet will only use the policy configuration and never consult the routing table even in the event of failure. With Policy-only, should the next hop enter a down status any policy matching packets will be dropped. Policy-last means the policy will only be consulted in the event the routing table cannot resolved the next hop for a request.

IP-Routing Policy to Work as Cisco IP Default-Network Command

Roberto Garcia
Systems Engineering
April 19, 2003

Cisco uses the IP Default Network command as a way to configure a Network Last Resort. When a router is configured with "ip default-network", if the router has a route to this network this router is considered as a default gateway. In this way you can reach networks that are not directly reachable by a next-hop.	
RapidOS Version Tested	9.3.0.0
RapidOS Versions Working with this Configuration	Older than 9.3.0.0
RapidOS Versions NOT Working with this Configuration	9.3.0.0 and newer
Hardware Specifics	N/A

Diagram



Configurations

```
vlan make trunk-port gi.3.1 exclude-default-vlan
vlan make trunk-port gi.3.2 exclude-default-vlan
vlan create 10 port-based id 10
vlan create 20 port-based id 20
vlan add ports gi.3.1 to 10
vlan add ports gi.3.2 to 20
!
interface create ip TO_OSPF1 address-netmask 192.168.0.2/24 vlan 10
interface create ip TO_VLANs address-netmask 192.168.5.2/24 vlan 20
interface add ip lo0 address-netmask 1.1.1.1/32
!
acl all_traffic permit ip any any any any
!
ip-router global set router-id 1.1.1.1
!
ospf create area backbone
ospf add interface TO_OSPF to-area backbone
ospf add stub-host 1.1.1.1 to-area backbone cost 1
ospf start
!
ip-policy Internet permit acl all_traffic action policy-last next-hop-list 213.4.100.1
ip-policy Internet apply interface all
system set name RS1
```

Comments

In this example the network 213.4.100.0/24 is known by the router C1 but is not advertise to the OSPF net. In the router RS1 we would like to introduce the configuration with the same behavior that the Cisco "ip default-network" command. So we use "ip-policy" in the RS1 to reach the not directly attached next-hop.

This is a very simple configuration but useful when you are compared with Cisco. This is very interesting in Internet datacenter environments where you do not have very complex routing policies in the low level routers and also if the routing policies change in the core it is very simple to make a change in the low level routers

---

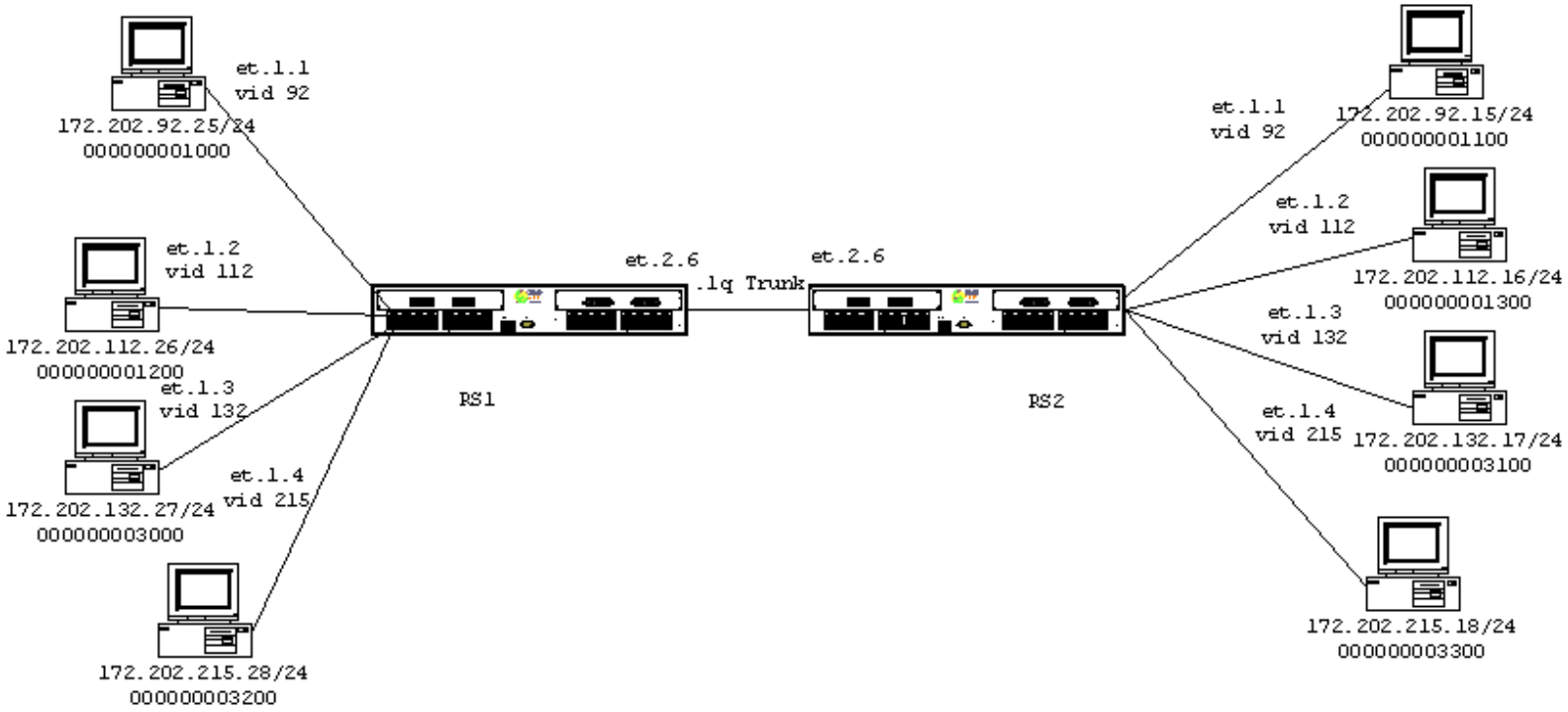
L2 QOS Weighted Fair Queuing

Wade M. Price
RTAC Carrier Accounts Team
March 22, 2002

This scenario depicts a BLEC provider implementing weighted fair queue policy across two RS3000 routers. Each customer has chosen different types of service from the BLEC and will be prioritized based on guarantee commitments. Subnet-based VLANs are configured for each customer and is transmitted across an 802.1Q Trunk to other BLEC customers within the MAN. The BLEC provider is marketing four different types of service from platinum (control), gold (high), silver (medium) and bronze (low) or best effort. Weighted-fair queuing distributes priority throughput among the four priorities based on the percentages. QoS policies applied at L2 allows you to assign priorities based on SA MAC, DA MAC, port-list, and vlan id fields. In this example, weighted fair queuing is configured among the four customers using the port-list and VID number.

RapidOS Version Tested	8.0.3.2
RapidOS Versions Working with this Configuration	6.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.1.0.0
Hardware Specifics	N/A

Diagram



Configurations

RS1

```
port flow-bridging all-ports
vlan make trunk-port et.2.6
vlan create test-v92 id 92 port-based
vlan create test-v112 id 112 port-based
vlan create test-v132 id 132 port-based
vlan create test-v215 id 215 port-based
vlan add ports et.1.1 to test-v92
vlan add ports et.1.2 to test-v112
vlan add ports et.1.3 to test-v132
vlan add ports et.1.4 to test-v215
vlan add ports et.2.6 to test-v92
vlan add ports et.2.6 to test-v112
vlan add ports et.2.6 to test-v132
vlan add ports et.2.6 to test-v215
qos set l2 name test-v92 vlan 92 priority control in-port-list et.1.1 source-mac any
dest-mac any
qos set l2 name test-v112 vlan 112 priority high in-port-list et.1.2 source-mac any
dest-mac any
qos set l2 name test-v132 vlan 132 priority medium in-port-list et.1.3 source-mac any
dest-mac any
qos set l2 name test-v215 vlan 215 priority low in-port-list et.1.4 source-mac any
dest-mac any
qos set queueing-policy weighted-fair port all-ports
qos set weighted-fair control 30 high 40 medium 25 low 5
system set name RS1
```

RS2

```
port flow-bridging all-ports
vlan make trunk-port et.2.6
vlan create test-v92 id 92 port-based
```

```
vlan create test-v112 id 112 port-based
vlan create test-v132 id 132 port-based
vlan create test-v215 id 215 port-based
vlan add ports et.1.1 to test-v92
vlan add ports et.1.2 to test-v112
vlan add ports et.1.3 to test-v132
vlan add ports et.1.4 to test-v215
vlan add ports et.2.6 to test-v92
vlan add ports et.2.6 to test-v112
vlan add ports et.2.6 to test-v132
vlan add ports et.2.6 to test-v215
qos set l2 name test-control vlan 92 in-port-list et.1.1 priority control source-mac
any dest-mac any
qos set l2 name test-v112 vlan 112 priority high in-port-list et.1.2 source-mac any
dest-mac any
qos set l2 name test-v132 vlan 132 priority medium in-port-list et.1.3 source-mac any
dest-mac any
qos set l2 name test-v215 vlan 215 priority low in-port-list et.1.4 source-mac any
dest-mac any
qos set queueing-policy weighted-fair port all-ports
qos set weighted-fair control 30 high 40 medium 25 low 5
system set name RS2
```

Comments

To verify that the L2 flow is being prioritized correctly internally to the RS, we can debug the L2 flow and by decoding the hardware header of the flow. To do this we need to give the internal port number, which can be seen with the "system show hardware verbose" command.

```
Port:   et.1.1,  Media Type: 10/100-Mbit Ethernet,  Physical Port: 17
     QMAC Information:
          Table Memory:  524288 bytes
          Packet Memory: 524288 bytes

RS1? debug l2 l2t port 17
Port: 17 (et.1.1), Hash: 65187, Link-location: 0, Address: 0x06024100
 Next-index    : 2304             Flags         : 0x182 ( Dst-addr Fltrd )
 Dst/Src-mac   : 000000:001100    Src-mac       : 000000:001000
 CEP           : 0x00000004       HH            : 0x000a011c 0x01700004
 L3-ptr        : 0x00000000
 Fwd-ptr       : 0x00000000       Bkwd-ptr      : 0x00000000
 Dst Frames    : 138723137        Dst Bytes     : 318571520
 Src Frames    : 0                Src Bytes     : 0
 To-bcast Frms: 0                 To-mcast Frms: 0
 Age Cnt       : 0



RS1? debug decode hardware-header "0x000a011c 0x01700004"


hh[0] = 0x000A011C
hh[1] = 0x01700004

Decoded:
-------
epti               = 5
sfti               = 17
int-prio           = control
VLAN Id            = 92
802.1Q flag        = 0
```

```
802.1Q prio        = 0

Flags:
   Force tx        = 0
   Switching type  = L2 (bridging)
   L3 protocol     = ipx
   Tag type        = untagged
   Encap type      = ethII
   802.1Q field    = VLAN info
   CPU req type    = no request
   Pkt replication = 0
   Multicast       = 0
```

Also if you are oversubscribing a link and you want to see what traffic is being dropped check out the following command on the output port. In this case it would be the port on the 802.1Q trunk port et.2.6.

```
RS1# statistics show port-errors et.2.6

Port: et.2.6
----
Error Stats                          Error Stats
-----------                          -----------
CRC errors                 0         Carrier sense errors       0
Single collision (tx OK)   0         Many collisions (tx OK)    0
Many collisions (drop)     0         Late collisions            0
Long frames  >1518 bytes   0         Invalid long frames        0
Short frames <64 bytes     0         Alignment errors           0
Deferred transmissions     0         Transmit underruns         0
IP - bad version           0         IP - bad checksum          0
IP - bad header            0         IP - small datagram        0
IP - expand TTL ring       0         IPX - bad header           0
Non-IP/IPX protocol        0         Invalid MAC encap.         0
Internal frame tx error    0         Internal frame rx error    0
Input buffer overflow      0         Packet request overflow    0
Out buffer (low) ovflow    216398078 Out buffer (med) ovflow    0
Out buffer (high) ovflow   0         Out buffer (ctrl) ovflow   0
Input VLAN dropped frames  N/A       Output VLAN dropped frames 0
Error stats cleared   2002-03-05 15:25:22
```

You should not rely on the above command alone to determine if the QOS is setup correctly, because by default all L2 traffic is assigned to the Low queue. First check the L2 flow. Then decode the Hardware Header to see the priority of the flow. In this example I was oversubscribing the output port by 20%, which was dropping the Low priority traffic only.

Pebbles of Knowledge

It is very important to know your traffic when implementing QOS policies. The reason for this is if you are applying an IP/IPX QOS policy and the traffic is being bridged (not destined to the RS MAC) then the QOS policy will not work (unless you are using L4 bridging). The default behavior of L2 QOS is sending everything to the Low queue.

The RS default L2 forwarding mode is Address based forwarding. To get this configuration to work you need to make sure you change the ports to "flow bridging mode". This is because the QOS L2 policy is not just looking for a L2 address, but a L2 flow, which includes in-port-list, VID number, Source Address, and Destination Address.

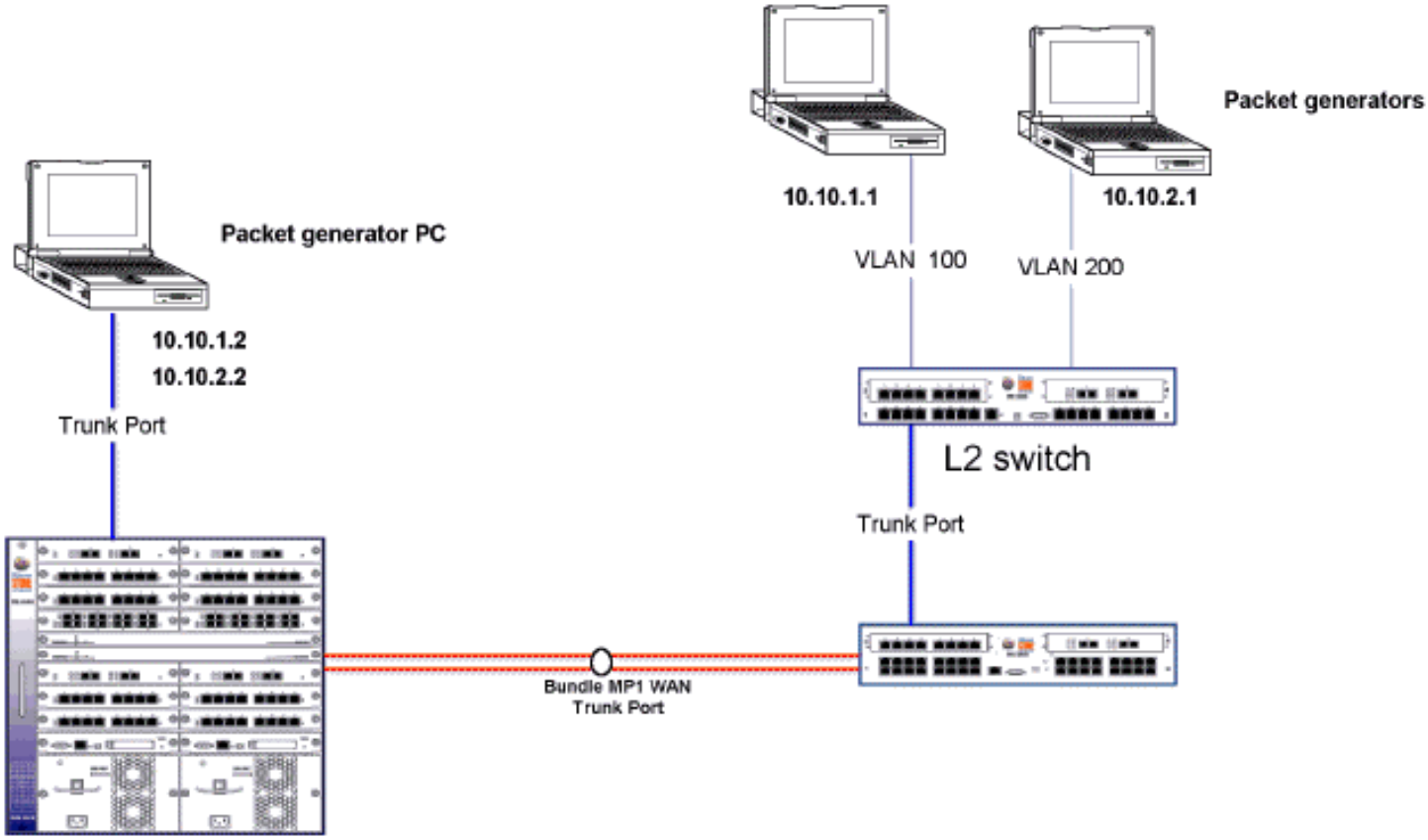
Aggregate Rate Limit on L2 Architecture with ML-PPP and .1Q over WAN Links

Doug Turner
Systems Engineering
May 25, 2001

This depicts a Metro provider using L2 services to interconnect his buildings. This architecture is limited scale, but does allow TLS services to be placed end to end through the path. Using .1Q over WAN links, each VLAN can be trunked across the path to the aggregation switch where the traffic is then routed. ML-PPP is being used to bundle T1s for additional bandwidth needs from the building to aggregation point. Aggregate Rate limiting is being applied at the ingress data port, (assuming that each customer is attaching to a separate switch at different riser points and the RS router is in the basement).The rate and VLAN information is identical on both routers to provide a symmetrical rate. Using L4 bridging allows an ACL match on the IP subnet achieving a rate based on the VLANs IP traffic.

RapidOS Version Tested	6.1.1.0, 6.2.0.0
RapidOS Versions Working with this Configuration	6.0.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.0.0.0
Hardware Specifics	None

Diagram



Configurations

Router 1

```
port set t1.3.1:1 timeslots 1-24 wan-encapsulation ppp
port set t1.3.2:1 timeslots 1-24 wan-encapsulation ppp
port set et.1.1 speed 100Mbps duplex full auto-negotiation off
!
ppp create-mlp mp.1 slot 3
ppp add-to-mlp mp.1 port t1.3.1
ppp add-to-mlp mp.1 port t1.3.2
vlan make trunk-port mp.1
vlan make trunk-port et.1.1
vlan create Cust-1 ip id 100
vlan create Cust-2 ip id 200
vlan add ports mp.1 to cust-1
vlan add ports mp.1 to cust-2
vlan add ports et.1.1 to cust-1
vlan add ports et.1.1 to cust-2
vlan enable l4-bridging on cust-1
vlan enable l4-bridging on cust-2
!
acl cust1 permit ip 10.10.1.0/24 any any any
acl cust2 permit ip 10.10.2.0/24 any any any
ip l3-hash module 3 variant 4
!
```

```
system set name Building 1
!
system enable aggregate-rate-limiting slot 1
system disable input port level-rate-limiting slot 1
rate-limit cust-ag1 aggregate acl cust1 rate 384000 drop-packets
rate-limit cust-ag2 aggregate acl cust2 rate 768000 drop-packets
rate-limit cust-ag1 apply port et.1.1
rate-limit cust-ag2 apply port et.1.1
```

Router 2

```
port set t1.3.1:1 timeslots 1-24 wan-encapsulation ppp
port set t1.3.2:1 timeslots 1-24 wan-encapsulation ppp
port set et.1.1 speed 100Mbps duplex full auto-negotiation off
!
ppp create-mlp mp.1 slot 3
ppp add-to-mlp mp.1 port t1.3.1
ppp add-to-mlp mp.1 port t1.3.2
vlan make trunk-port mp.1
vlan make trunk-port et.1.1
vlan create Cust-1 ip id 100
vlan create Cust-2 ip id 200
vlan add ports mp.1 to cust-1
vlan add ports mp.1 to cust-2
vlan add ports et.1.1 to cust-1
vlan add ports et.1.1 to cust-2
vlan enable l4-bridging on cust-1
vlan enable l4-bridging on cust-2
!
acl cust1 permit ip 10.10.1.0/24 any any any
acl cust2 permit ip 10.10.2.0/24 any any any
ip l3-hash module 3 variant 4
!
system set name Building 1
!
system enable aggregate-rate-limiting slot 1
system disable input port level-rate-limiting slot 1
rate-limit cust-ag1 aggregate acl cust1 rate 384000 drop-packets
rate-limit cust-ag2 aggregate acl cust2 rate 768000 drop-packets
rate-limit cust-ag1 apply port et.1.1
rate-limit cust-ag2 apply port et.1.1
```

Poking Holes Through Rate-limiting

Ian Cowburn
Corporate Systems Engineering
August 28, 2001

There are times when you want to rate limiting all traffic apart from some specific traffic. Two examples might be:

a. you want to constrain a customer's traffic but do not want to effect their voice-over-ip.
   In this case you may rate limit the total traffic from the customer but configure the rs so that the voice-over-ip is not rate-limited.
b. you want to rate limit icmp to avoid dos attacks but allow trusted networks to send icmp without being rate limited.

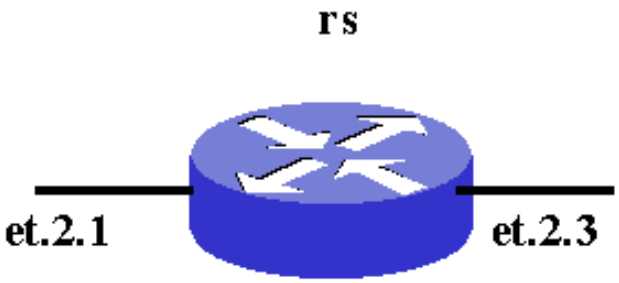
In each case, you configure a rate limiting statement for the traffic that you DO NOT want to rate limit, giving this an action of "no-action" and then another statement for the traffic that you DO want to rate limit, with the required action (drop, lower priority etc…). Here it is assumed that the first traffic profile (do not rate limit) is more specific than the second (do rate limit).

These rate limiting statements are then applied to the relevant interface, with the "do not rate limit" statement applied last. This will cause the "do not rate limit" statement to be processed first by the hardware.

The significant algorithm is that the rate-limiting statements are processed by the hardware in the reverse order in which they are applied, i.e. the last to be applied gets processed first.

RapidOS Version Tested	7.0.0.2
RapidOS Versions Working with this Configuration	3.1.0.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 3.1.0.0
Hardware Specifics	

Diagram



Configurations

```
interface create ip lan address-netmask 192.168.254.254/24 port et.2.1
interface create ip lan1 address-netmask 10.1.1.1/24 port et.2.3
interface add ip lan1 address-netmask 10.2.2.1/24
acl rlicmp permit icmp
acl no-rlicmp permit icmp 10.2.2.0/24 any
system set name rs2
system enable aggregate-rate-limiting slot 2
rate-limit rlicmp aggregate acl rlicmp drop-packets rate 5000
rate-limit no-rlicmp aggregate acl no-rlicmp no-action rate 5000
rate-limit rlicmp apply interface lan1
rate-limit no-rlicmp apply interface lan1
system set idle-timeout serial 0
system set idle-timeout telnet 0
```

Comments

This example shows icmp rate limiting using two aggregate rate limit statements.

The "rlicmp" acl/rate-limit statement will rate limit icmp traffic received on interface lan1 to 5000 bps. The "no-rlicmp" acl/rate-limit statement will cause icmp traffic, sourced from network 10.2.2.0/24 and received on interface lan1, to NOT be rate limited (due to the "no-action" parameter).

This functions as intended because the "no-rlicmp" rate-limit statement is applied to interface lan1 after the "rlicmp" statement has been applied.

Unfortunately, we cannot see the order in which the rate limiting is processed from the show output:

```
rs2# rate-limit show all

--------------------------------------------------------------------------------
Rate Limit Policy name     : rlicmp     Type: Aggregate
Parent Policy       : None
Applied Interfaces : lan1
ACL          Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort   TOS TOS-MASK
Prot
---          --------------     -------------      --------- --------- --- -----------
-- ----
rlicmp       anywhere           anywhere           any       any       any None
ICMP
```

```
   Seq   ACL        Rate Limit  Exceed Action Credits Time Interval
   ---   ----       --------    ------------- ------- -------------
   10    rlicmp     5000        Drop Packets  83      34.36 sec

-------------------------------------------------------------------------------
Rate Limit Policy name     : no-rlicmp     Type: Aggregate
Parent Policy       : None
Applied Interfaces : lan1
ACL          Source IP/Mask     Dest. IP/Mask      SrcPort   DstPort   TOS TOS-MASK
Prot
---          --------------     -------------      --------- --------- --- -----------
-- ----
no-rlicmp    10.2.2.0/24        anywhere           any       any       any None
ICMP

   Seq   ACL        Rate Limit  Exceed Action Credits Time Interval
   ---   ----       --------    ------------- ------- -------------
   10    no-rlicmp  5000        Pass Packets  83      34.36 sec
rs2#
```

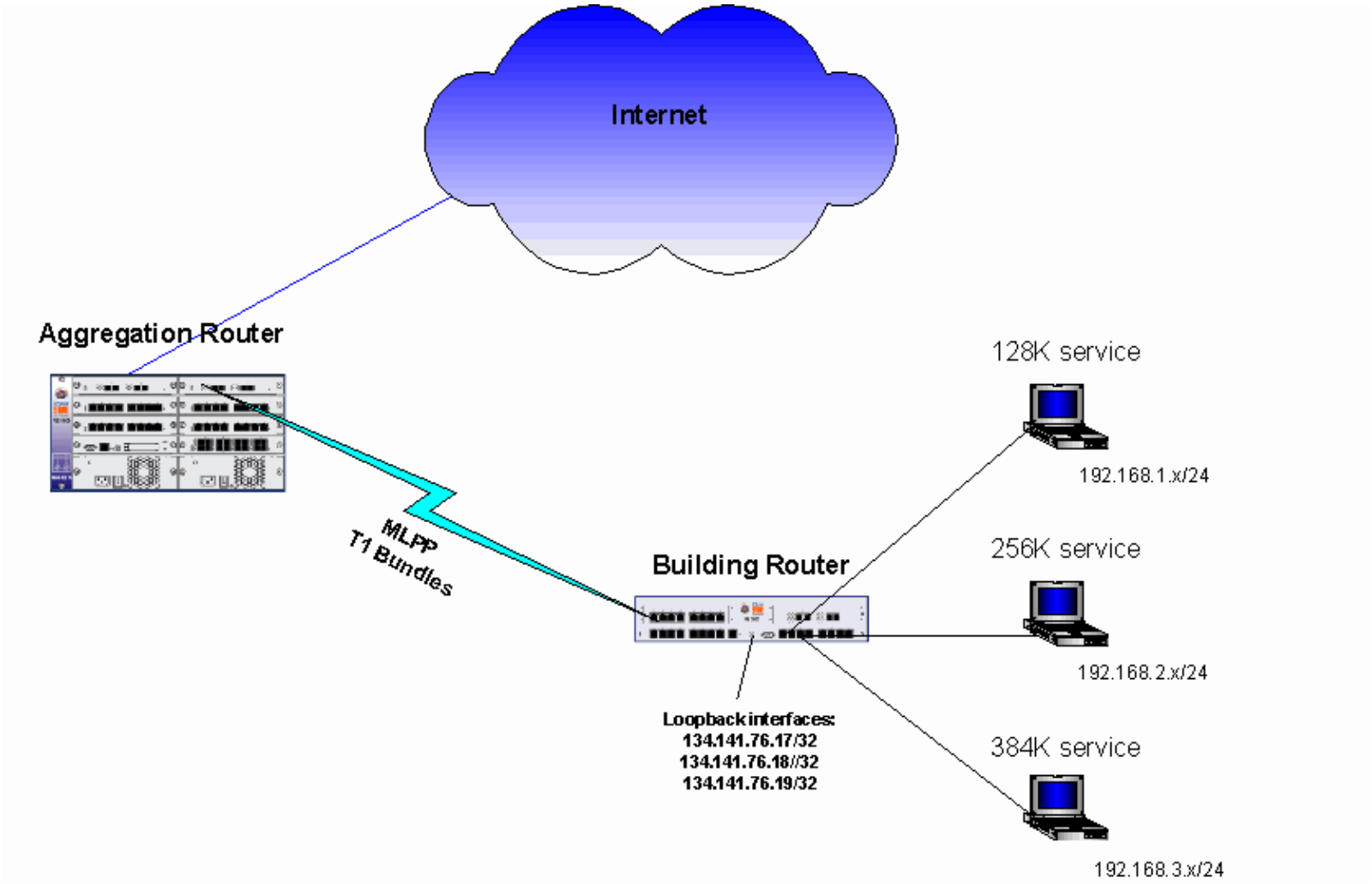
WAN Rate Shaping with NATing Loopback Interfaces

Scott Martin
Systems Engineering
May 12, 2001

This scenario depicts a BLEC utilizing the Lo0 interface for NAT assignment as well as applying WAN Rate Shaping parameters for different class of services for their customers. WAN Rate Shaping allows you to define CIR (Committed Information Rate), BE (Burst Exceed), and BC (Burst Commit) and apply those parameters on source IP, destination IP, L4 source port, port name, or VLAN ID. The following example applies the Wan Rate Shaping parameters based upon source IP for upstream traffic on the RS2000, and is also applied on RS8000 based upon destination IP for downstream traffic. This ensures that the customer cannot exceed the CIR for traffic in either direction. The Lo0 addresses are valid ARIN assigned address space, which allows the BLEC to preserve precious IP addresses, as NAT with IP overload is utilized.

RapidOS Version Tested	6.3.1.0, 6.3.2.0, 7.0.0.0
RapidOS Versions Working with this Configuration	6.3.1.0 and newer
RapidOS Versions NOT Working with this Configuration	Older than 6.3.0.0
Hardware Specifics	-AA and newer

Diagram



Configurations

RS2000 Building Router

```
port set t1.3.1:1 timeslots 1-24 wan-encapsulation ppp
port set t1.3.2:1 timeslots 1-24 wan-encapsulation ppp
port flow-bridging all-ports

ppp create-mlp mp.1 slot 3
ppp add-to-mlp mp.1 port t1.3.1:1
ppp add-to-mlp mp.1 port t1.3.2:1

interface create ip et-1.3 address-netmask 192.168.3.1/24 port et.1.3
interface create ip et-1.4 address-netmask 192.168.4.1/24 port et.1.4
interface create ip et-1.5 address-netmask 192.168.5.1/24 port et.1.5
interface create ip mp.1 address-netmask 10.0.18.6/30 port mp.1

interface add ip lo0 address-netmask 134.141.76.17/32
interface add ip lo0 address-netmask 134.141.76.18/32
interface add ip lo0 address-netmask 134.141.76.19/32

acl lcl1 permit ip 192.168.1.0/24
acl lcl2 permit ip 192.168.2.0/24
acl lcl3 permit ip 192.168.3.0/24

ip-router global set router-id 19.19.19.19

ospf create area backbone
```

```
ospf add interface mp.1 to-area backbone
ospf add stub-host 134.141.76.17 to-area backbone cost 1
ospf add stub-host 134.141.76.18 to-area backbone cost 1
ospf add stub-host 134.141.76.19 to-area backbone cost 1
ospf start

nat set interface mp.1 outside
nat set interface et-1.3 inside
nat set interface et-1.4 inside
nat set interface et-1.5 inside

nat create dynamic local-acl-pool lcl1 global-pool 134.141.76.17 enable-ip-overload
nat create dynamic local-acl-pool lcl2 global-pool 134.141.76.18 enable-ip-overload
nat create dynamic local-acl-pool lcl3 global-pool 134.141.76.19 enable-ip-overload

wan define rate-shape-parameters 128 cir 128000
wan define rate-shape-parameters 256 cir 256000
wan define rate-shape-parameters 384 cir 384000
wan define rate-shape-parameters 512 cir 512000
wan define rate-shape-parameters 768 cir 768000
wan define rate-shape-parameters 1-5 cir 1536000

wan apply rate-shape-parameters 128 source-ip-address 134.141.76.17 port mp.1
wan apply rate-shape-parameters 256 source-ip-address 134.141.76.18 port mp.1
wan apply rate-shape-parameters 384 source-ip-address 134.141.76.19 port mp.1
```

RS8000 Aggregation Router

```
port set t3.3.(1-2):(1-28) timeslots 1-24 wan-encapsulation ppp
port set t3.6.(1-2):(1-28) timeslots 1-24 wan-encapsulation ppp
port set t3.3.(1-2) framing m23
port set t3.6.(1-2) framing m23

! following lines are used only if the Carrier is NOT providing clock on individual
T1 circuits !

port set t3.3.1:(1-28) clock-source internal
port set t3.3.2:(1-28) clock-source internal

ppp create-mlp mp.20 slot 3
ppp add-to-mlp mp.20 port t3.3.1:20
ppp add-to-mlp mp.20 port t3.3.2:18

interface create ip mp20 address-netmask 10.0.18.5/30 port mp.20
interface add ip lo0 address-netmask 134.141.64.2/32
ip-router global set autonomous-system 193
ip-router global set router-id 134.141.64.2

! following line is used to inject a default gateway within OSPF w/o installing the
route on this router !
ip add route default no-install gateway 134.141.64.2 reject

ospf create area backbone
ospf add interface mp20 to-area backbone
ospf start

wan define rate-shape-parameters 128k cir 128000
wan define rate-shape-parameters 256k cir 256000
wan define rate-shape-parameters 384k cir 384000
wan define rate-shape-parameters 512k cir 512000
wan define rate-shape-parameters 768k cir 768000
wan define rate-shape-parameters T1 cir 1536000
```

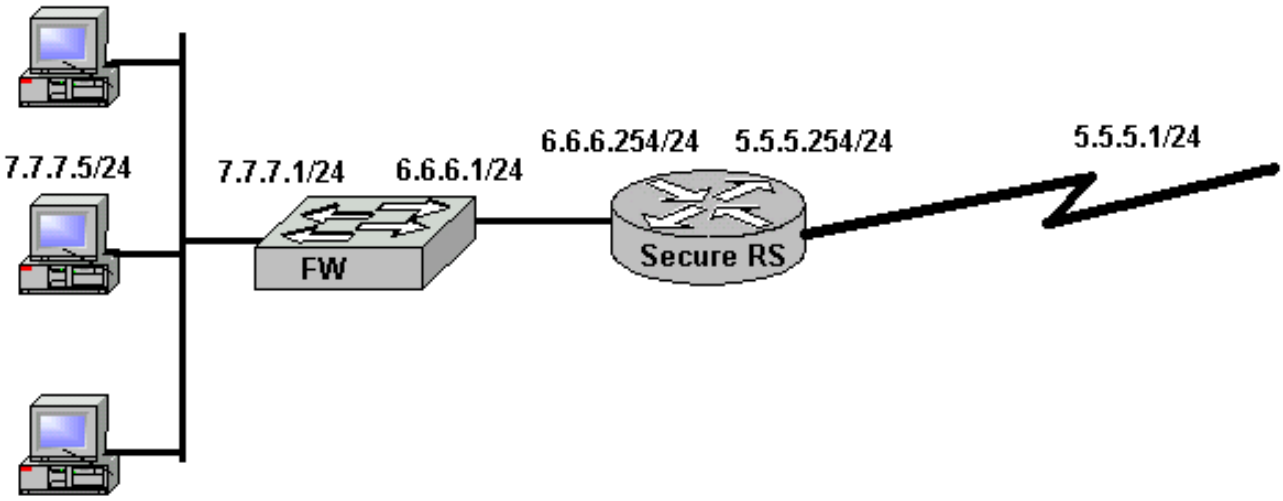
```
wan apply rate-shape-parameters 128k destination-ip-address 134.141.76.17 port mp.20
wan apply rate-shape-parameters 256k destination-ip-address 134.141.76.18 port mp.20
wan apply rate-shape-parameters 384k destination-ip-address 134.141.76.19 port mp.20
```

Secure ROS Configuration

Andrew Walden
Corporate System Engineering
February 13, 2003

This config is intended to be used as a template and reference to an existing security policy. There are many different aspects of security listed below, and not all will be applicable to every situation. This is based on the Secure IOS Template http://www.cymru.com/~robt/Docs/Articles/secure-ios-template.html by Rob Thomas.	
RapidOS Version Tested	8.0.0.0
RapidOS Versions Working with this Configuration	8.0.0.0
RapidOS Versions NOT Working with this Configuration	Older then 8.0.0.0
Hardware Specifics	None

Diagram



Configurations

```
system set name secure-rs01
!
!
! Use RADIUS for AAA.
radius enable
radius authentication login
radius authentication enable
radius accounting command level 15
radius set last-resort password
radius accounting shell all
radius accounting snmp startup
radius set key cheezit
radius set source 10.10.10.10
radius set server 7.7.7.5
! This may be redundant if your also using syslog
radius accounting system info

! Lock it down with hard to guess passwords
system set password login
system set password enable
system set password diag

! Set the timezone properly. It is best to standardize on one
! timezone for all routers, thus making problem tracking easier.
system set timezone utc

! Synchronize our clocks with a local NTP server.
ntp set server 7.7.7.5 source 10.10.10.10

! Configure the loopback0 interface as the source of our log
! messages. This is often used for routing protocols as well.
! Select an IP address that uniquely identifies this router.
! One trick is to allocate a netblock for use as the router
! loopback netblock.
interface add ip lo0 address-netmask 10.10.10.10/32

! Create Internet facing interface
interface create unprotected ip address-netmask 5.5.5.254/24 port et.1.1
port description et.1.1 "Unprotected interface, facing towards Internet"

! Enable acl rate-limiting for line card
system enable aggregate-rate-limiting slot 1

 ! Allow UDP to occupy no more than 2 Mb/s of the pipe.
rate-limit udplimit aggregate acl 150 rate 2010000 drop-packets
rate-limit udplimit appy interface unprotected

! Allow ICMP to occupy no more than 500 Kb/s of the pipe.
rate-limit icmplimit aggregate acl 160 rate 500000 drop-packets
rate-limit udplimit appy interface unprotected

! Allow multicast to occupy no more than 5 Mb/s of the pipe.
rate-limit mcastlimit aggregate acl 170 rate 5000000 drop-packets
rate-limit mcastlimit appy interface unprotected
```

```
! IP Options (IP directed broadcast is turned off by default)
ip disable source-routing
ip disable icmp-redirect interface all
ip disable proxy-arp interface all

! Drop all ICMP fragments
ip dos enable fragments-attack-protection

! Create protect interface connecting local network
interface create protected-dmz ip address-netmask 6.6.6.254/24 port et.1.2
port description et.1.1 "Protected interface, facing towards DMZ"

! Default route to the Internet (could be a routing
! protocol instead)
ip add route 0.0.0.0 0.0.0.0 5.5.5.1

! Route to network on the other side of the firewall
ip add route 7.7.7.0 255.255.255.0 6.6.6.1

! Black hole routes.
ip add route 1.0.0.0/8 blackhole
ip add route 2.0.0.0/8 blackhole
ip add route 5.0.0.0/8 blackhole
ip add route 7.0.0.0/8 blackhole
ip add route 10.0.0.0/8 blackhole
ip add route 23.0.0.0/8 blackhole
ip add route 27.0.0.0/8 blackhole
ip add route 31.0.0.0/8 blackhole
ip add route 36.0.0.0/8 blackhole
ip add route 37.0.0.0/8 blackhole
ip add route 39.0.0.0/8 blackhole
ip add route 41.0.0.0/8 blackhole
ip add route 42.0.0.0/8 blackhole
ip add route 49.0.0.0/8 blackhole
ip add route 50.0.0.0/8 blackhole
ip add route 58.0.0.0/8 blackhole
ip add route 59.0.0.0/8 blackhole
ip add route 60.0.0.0/8 blackhole
ip add route 69.0.0.0/8 blackhole
ip add route 70.0.0.0/8 blackhole
ip add route 71.0.0.0/8 blackhole
ip add route 72.0.0.0/8 blackhole
ip add route 73.0.0.0/8 blackhole
ip add route 74.0.0.0/8 blackhole
ip add route 75.0.0.0/8 blackhole
ip add route 76.0.0.0/8 blackhole
ip add route 77.0.0.0/8 blackhole
ip add route 78.0.0.0/8 blackhole
ip add route 79.0.0.0/8 blackhole
ip add route 82.0.0.0/8 blackhole
ip add route 83.0.0.0/8 blackhole
ip add route 84.0.0.0/8 blackhole
```

```
ip add route 85.0.0.0/8 blackhole
ip add route 86.0.0.0/8 blackhole
ip add route 87.0.0.0/8 blackhole
ip add route 88.0.0.0/8 blackhole
ip add route 89.0.0.0/8 blackhole
ip add route 90.0.0.0/8 blackhole
ip add route 91.0.0.0/8 blackhole
ip add route 92.0.0.0/8 blackhole
ip add route 93.0.0.0/8 blackhole
ip add route 94.0.0.0/8 blackhole
ip add route 95.0.0.0/8 blackhole
ip add route 96.0.0.0/8 blackhole
ip add route 97.0.0.0/8 blackhole
ip add route 98.0.0.0/8 blackhole
ip add route 99.0.0.0/8 blackhole
ip add route 100.0.0.0/8 blackhole
ip add route 101.0.0.0/8 blackhole
ip add route 102.0.0.0/8 blackhole
ip add route 103.0.0.0/8 blackhole
ip add route 104.0.0.0/8 blackhole
ip add route 105.0.0.0/8 blackhole
ip add route 106.0.0.0/8 blackhole
ip add route 107.0.0.0/8 blackhole
ip add route 108.0.0.0/8 blackhole
ip add route 109.0.0.0/8 blackhole
ip add route 110.0.0.0/8 blackhole
ip add route 111.0.0.0/8 blackhole
ip add route 112.0.0.0/8 blackhole
ip add route 113.0.0.0/8 blackhole
ip add route 114.0.0.0/8 blackhole
ip add route 115.0.0.0/8 blackhole
ip add route 116.0.0.0/8 blackhole
ip add route 117.0.0.0/8 blackhole
ip add route 118.0.0.0/8 blackhole
ip add route 119.0.0.0/8 blackhole
ip add route 120.0.0.0/8 blackhole
ip add route 121.0.0.0/8 blackhole
ip add route 122.0.0.0/8 blackhole
ip add route 123.0.0.0/8 blackhole
ip add route 124.0.0.0/8 blackhole
ip add route 125.0.0.0/8 blackhole
ip add route 126.0.0.0/8 blackhole
ip add route 127.0.0.0/8 blackhole
ip add route 169.254.0.0/16 blackhole
ip add route 172.16.0.0/12 blackhole
ip add route 192.0.2.0/24 blackhole
ip add route 192.168.0.0/16 blackhole
ip add route 197.0.0.0/8 blackhole
ip add route 201.0.0.0/8 blackhole
ip add route 219.0.0.0/8 blackhole
ip add route 221.0.0.0/8 blackhole

! Export our LFAP data to our LFAP server, 7.7.7.5. LFAP
```

```
! provides some statistics that can be of use when tracing the true
! source of a spoofed attack and its data can be converted to Netflow.
acl lfap permit ip any any any any accounting hourly
acl lfap apply interface unprotected input output
lfap set server 7.7.7.5
lfap start

! Log anything interesting to the loghost. Capture all of
! the logging output with FACILITY LOCAL5.
system set syslog level info facility local5 source 10.10.10.10 server 7.7.7.5 buffer-
size 50

! With the ACLs, it is important to log the naughty folks.
! Thus, the implicit drop all ACL is replaced (augmented,
! actually) with an explicit drop all that logs the attempt.
! You may wish to keep a second list (e.g. 2011) that does not
! log. During an attack, the additional logging can impact the
! performance of the router. Simply copy and paste acl 2010,
! remove the log keyword, and name it acl 2011. Then
! when an attack rages, you can replace acl 2010 on the
! Internet-facing interface with acl 2011.
!
! Block SNMP access to all but the loghost
acl 20 permit ip 7.7.7.5
acl 20 deny any log
acl 20 apply service snmp logging deny-only

! Block local multicast
acl 30 deny ip 224.0.0.0/8
! Locally scoped
acl 30 deny 239.0.0.0/24
! sgi-dogfight
acl 30 deny 224.0.1.2/32
! rwhod
acl 30 deny 224.0.1.3/32
! ms-srvloc
acl 30 deny 224.0.1.22/32
! ms-ds
acl 30 deny 224.0.1.24/32
! ms-servloc-da
acl 30 deny 224.0.1.34/32
! hp-device-disc
acl 30 deny 224.0.1.60/32
! Permit all other multicast traffic
acl 30 permit 224.0.0.0/28
acl 30 apply interface unprotected
acl 30 apply interface protected-dmz

! Block access to all but the loghost and the firewall, and log any
! denied access attempts. This also serves to create an audit trail
! of all access to the router.
acl 100 permit tcp 7.7.7.5 5.5.5.254 log
acl 100 deny ip any any log
acl 100 apply service ssh logging on
```

```
! Configure an ACL that prevents spoofing from within our network.
! This ACL assumes that we need to access the Internet only from the
! 7.7.7.0/24 network. If you have additional networks behind
! 7.7.7.0/24, then add them into this ACL.
! First, allow our intranet to access the Internet.
acl 115 permit ip 7.7.7.0/24 any

! Second, allow our firewall to access the Internet. This is useful
! for testing.
acl 115 permit ip host 6.6.6.1 any

! Now log all other such attempts.
acl 115 deny ip any any log

! Apply the filter
acl 115 apply interface et.1.2
!
! Rate limit (CAR) ACLs for UDP, ICMP, and multicast.
acl 150 permit udp any any
acl 160 permit icmp any any
acl 170 permit ip any 224.0.0.0/5

! Deny any packets from the RFC 1918, IANA reserved, test,
! multicast as a source, and loopback netblocks to block
! attacks from commonly spoofed IP addresses.
!
! Claims it came from the inside network, yet arrives on the
! outside (read: Internet) interface..
acl 2010 deny ip 6.6.6.0/24 any log
acl 2010 deny ip 7.7.7.0/24 any log
! Bogons
acl 2010 deny ip 1.0.0.0/8 any log
acl 2010 deny ip 2.0.0.0/8 any log
acl 2010 deny ip 5.0.0.0/8 any log
acl 2010 deny ip 7.0.0.0/8 any log
acl 2010 deny ip 10.0.0.0/8 any log
acl 2010 deny ip 23.0.0.0/8 any log
acl 2010 deny ip 27.0.0.0/8 any log
acl 2010 deny ip 31.0.0.0/8 any log
acl 2010 deny ip 36.0.0.0/8 any log
acl 2010 deny ip 37.0.0.0/8 any log
acl 2010 deny ip 39.0.0.0/8 any log
acl 2010 deny ip 41.0.0.0/8 any log
acl 2010 deny ip 42.0.0.0/8 any log
acl 2010 deny ip 49.0.0.0/8 any log
acl 2010 deny ip 50.0.0.0/8 any log
acl 2010 deny ip 58.0.0.0/8 any log
acl 2010 deny ip 59.0.0.0/8 any log
acl 2010 deny ip 60.0.0.0/8 any log
acl 2010 deny ip 69.0.0.0/8 any log
acl 2010 deny ip 70.0.0.0/8 any log
acl 2010 deny ip 71.0.0.0/8 any log
acl 2010 deny ip 72.0.0.0/8 any log
```

```
acl 2010 deny ip 73.0.0.0/8 any log
acl 2010 deny ip 74.0.0.0/8 any log
acl 2010 deny ip 75.0.0.0/8 any log
acl 2010 deny ip 76.0.0.0/8 any log
acl 2010 deny ip 77.0.0.0/8 any log
acl 2010 deny ip 78.0.0.0/8 any log
acl 2010 deny ip 79.0.0.0/8 any log
acl 2010 deny ip 82.0.0.0/8 any log
acl 2010 deny ip 83.0.0.0/8 any log
acl 2010 deny ip 84.0.0.0/8 any log
acl 2010 deny ip 85.0.0.0/8 any log
acl 2010 deny ip 86.0.0.0/8 any log
acl 2010 deny ip 87.0.0.0/8 any log
acl 2010 deny ip 88.0.0.0/8 any log
acl 2010 deny ip 89.0.0.0/8 any log
acl 2010 deny ip 90.0.0.0/8 any log
acl 2010 deny ip 91.0.0.0/8 any log
acl 2010 deny ip 92.0.0.0/8 any log
acl 2010 deny ip 93.0.0.0/8 any log
acl 2010 deny ip 94.0.0.0/8 any log
acl 2010 deny ip 95.0.0.0/8 any log
acl 2010 deny ip 96.0.0.0/8 any log
acl 2010 deny ip 97.0.0.0/8 any log
acl 2010 deny ip 98.0.0.0/8 any log
acl 2010 deny ip 99.0.0.0/8 any log
acl 2010 deny ip 100.0.0.0/8 any log
acl 2010 deny ip 101.0.0.0/8 any log
acl 2010 deny ip 102.0.0.0/8 any log
acl 2010 deny ip 103.0.0.0/8 any log
acl 2010 deny ip 104.0.0.0/8 any log
acl 2010 deny ip 105.0.0.0/8 any log
acl 2010 deny ip 106.0.0.0/8 any log
acl 2010 deny ip 107.0.0.0/8 any log
acl 2010 deny ip 108.0.0.0/8 any log
acl 2010 deny ip 109.0.0.0/8 any log
acl 2010 deny ip 110.0.0.0/8 any log
acl 2010 deny ip 111.0.0.0/8 any log
acl 2010 deny ip 112.0.0.0/8 any log
acl 2010 deny ip 113.0.0.0/8 any log
acl 2010 deny ip 114.0.0.0/8 any log
acl 2010 deny ip 115.0.0.0/8 any log
acl 2010 deny ip 116.0.0.0/8 any log
acl 2010 deny ip 117.0.0.0/8 any log
acl 2010 deny ip 118.0.0.0/8 any log
acl 2010 deny ip 119.0.0.0/8 any log
acl 2010 deny ip 120.0.0.0/8 any log
acl 2010 deny ip 121.0.0.0/8 any log
acl 2010 deny ip 122.0.0.0/8 any log
acl 2010 deny ip 123.0.0.0/8 any log
acl 2010 deny ip 124.0.0.0/8 any log
acl 2010 deny ip 125.0.0.0/8 any log
acl 2010 deny ip 126.0.0.0/8 any log
acl 2010 deny ip 127.0.0.0/8 any log
```

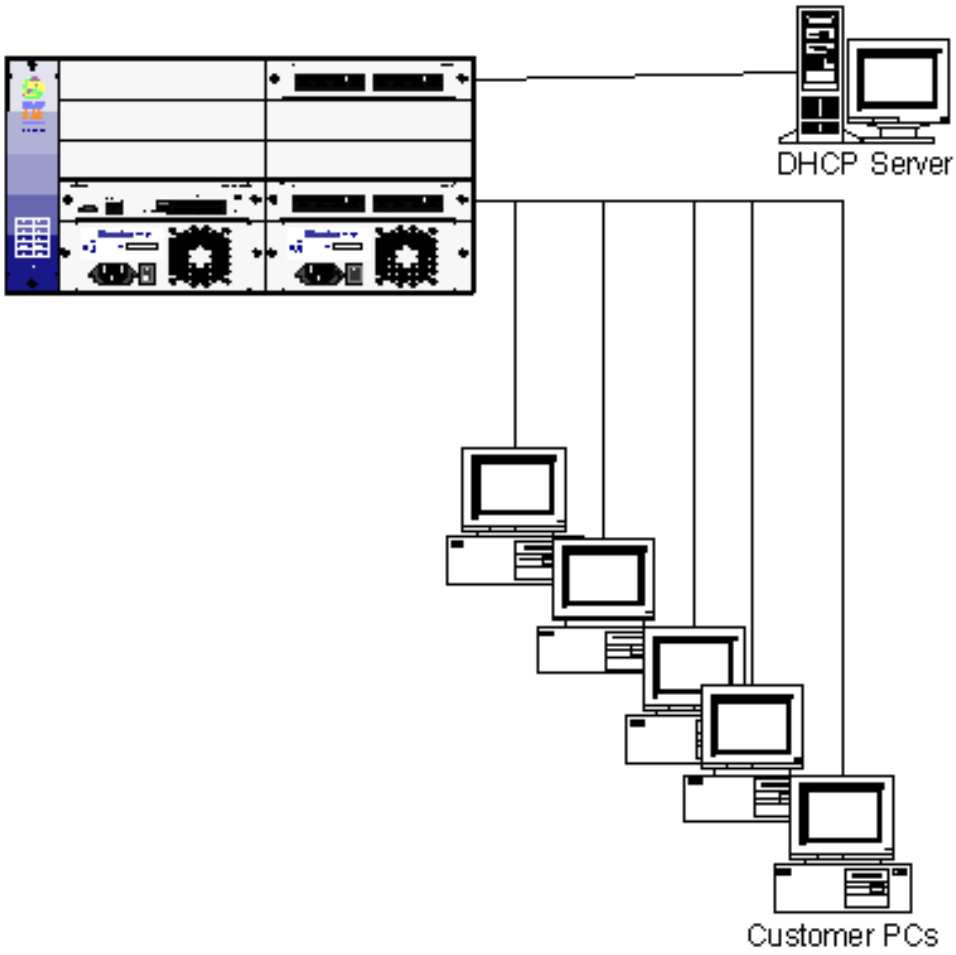
```
acl 2010 deny ip 169.254.0.0/16 any log
acl 2010 deny ip 172.16.0.0/12 any log
acl 2010 deny ip 192.0.2.0/24 any log
acl 2010 deny ip 192.168.0.0/16 any log
acl 2010 deny ip 197.0.0.0/8 any log
acl 2010 deny ip 201.0.0.0/8 any log
acl 2010 deny ip 219.0.0.0/8 any log
acl 2010 deny ip 220.0.0.0/8 any log
acl 2010 deny ip 221.0.0.0/8 any log
acl 2010 deny ip 224.0.0.0/5 any log

! Allow IP access to the intranet (firewall filters specific ports)
acl 2010 permit ip any 7.7.7.0/24

! Allow multicast to enter. See also acl 30 for more
! specific multicast rules.
acl 2010 permit ip any 224.0.0.0/5

! Our explicit (read: logged) drop all rule
acl 2010 deny ip any any log

! Apply the filter
acl 2010 apply interface unprotected

! SNMP is VERY important, particularly with MRTG.
! Treat the COMMUNITY string as a password - keep it difficult to guess.
snmp set community  privilege read

! Introduce ourselves with an appropriately stern banner.
system set login-banner "Router foo.\n Unauthorized access to this device or the
attached networks is\n prohibited without express written permission.  Violators will
be\n prosecuted to the fullest extent of both civil and criminal law.\n\n  We don't
like you. Go Away."

! Turn off telnet in favor of SSH, Don't forget to enter the command:
! 'ssh server generate_key rsa' at the command prompt to enable ssh
system disable telnet-server

! Set idle timeouts to 15 minutes.
system set idle-timeout serial 15 ssh 15 telnet 15
```

Building the ARP Table from DHCP

Dennis L. Faust
Systems Engineering
August 26, 2002

This configuration is an example of how to utilize the feature that allows for the building of the ARP table by snooping on DHCP ACKs.	
RapidOS Version Tested	8.0.2.2
RapidOS Versions Working with this Configuration	8.0.2.2 and newer
RapidOS Versions NOT Working with this Configuration	Older than 8.0.2.2
Hardware Specifics	None.

Diagram



Configurations

```
atm set port at.1.1 vpi-bits 4
atm set port at.1.1 mac-addr-hop-prevention
atm create vcl port at.1.1.1-10.32-176
vlan create vlan11 port-based id 11
vlan create dhcp port-based id 300
vlan add ports at.1.1.1-10.32-176 to vlan11
vlan add ports et.16.24 to dhcp
interface create ip VLAN11 address-netmask 10.11.0.1/16 vlan vlan11
interface create ip DHCP address-netmask 10.2.0.1/16 vlan dhcp
ip helper-address interface VLAN11 10.2.0.50 snoop-l2-l3-info
```

Comments

This function is very useful for service providers that are trying to create a more secure environment for their customers. By enabling this feature, the end user cannot spoof an IP address. The only way the ARP table for the VLAN will be built is from the DNCP ACKs from the DHCP server. A user cannot manually install an IP address on their computer and have the Riverstone chassis learn it through ARP, as would normally happen. If a customer were to manually populate his IP address (either by accident or to try to "spoof" another user), the Riverstone will never

learn that IP address, since it will not be learned as part of the DHCP process. If some systems on the VLAN are not supported by DHCP, the ARP table may also be manually populated with static entries.

The use of the "mac-addr-hop-prevention" command on the ATM port also improves the security of the network, because that command prevents a user from "stealing" another users MAC address.

VRRP, Load Distribution & IP Backup

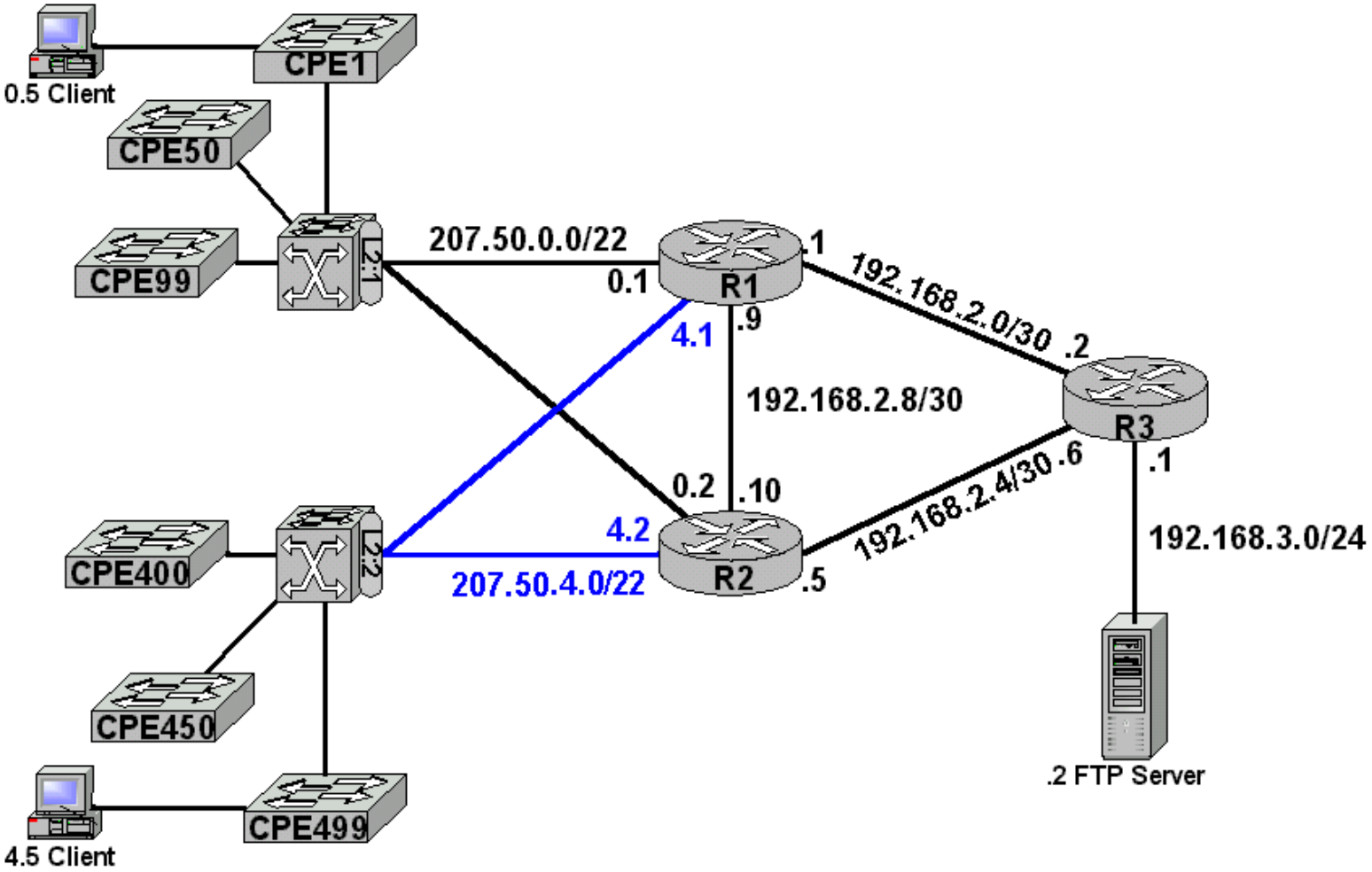
Richard Foote
Corporate Systems Engineering
April 17, 2001

This configuration will demonstrate how VRRP can play a significant role in ensuring service reliability for the access provider and provide load distribution across VRRP routers. When access providers deliver default gateways addresses to their subscribers it is important to ensure the clients default gateway is not a single point of failure. It is also important to ensure that all the network elements handle part of the load. Here we can see the access customers have a dedicated CPE device, acting in transparent mode, connecting to a larger layer two aggregation. The larger layer two aggregation node has two connections to the routed environment. The CPE gear has been shown in the diagram as a point of reference. Since the CPE gear is transparent to the network, for our purposes, the client can actually be directly connected to the layer two aggregation node for demonstration purposes. No configuration for the CPE equipment is presented because of the assumption it is a layer two device without redundant connections. Notice also, there are multiple larger L2 aggregation switches which are used to split the traffic load, provide redundancy and scalability. Using well defined IP addressing schemes, the provider can distribute groupings of DHCP addresses and different default gateways based on which layer two aggregation node the subscriber is connected to. For example, all subscribers connected to the L2:1 aggregation switch would receive addressing in the range of 207.50.0.5-207.50.3.254, a mask of /22 and a default gateway of 207.50.0.1. The subscribers connected to the L2:2 aggregation switch would receive addressing in the range of 207.50.4.5-207.50.7.254, a mask of /22 and a default gateway of 207.50.4.2. This could be a simple all Ethernet view of what cable providers like @home© maybe be deploying using cable modems/CMTS head-ends or DSL/DSLAM deployments.

RapidOS Version Tested	7.0.0.0
RapidOS Versions Working with this Configuration	2.2.0.0 [1]
RapidOS Versions NOT Working with this Configuration	Older than 2.2.0.0
Hardware Specifics	N/A

[1] This refers to the VRRP configuration. Certain OSPF features require 5.1.x.x or 7.0.0.0 (like "**`ospf set interface Client1 passive`**").

Diagram



Configurations

Router R1

```
vlan create Client1 ip id 101
vlan create Client2 ip id 102
vlan add ports et.2.1 to Client1
vlan add ports et.2.2 to Client2
interface create ip Client1 address-netmask 207.50.0.1/22 vlan Client1
interface create ip Client2 address-netmask 207.50.4.1/22 vlan Client2
interface create ip ToNet address-netmask 192.168.2.1/30 port et.2.3
interface create ip Peer address-netmask 192.168.2.9/30 port et.2.5
interface add ip lo0 address-netmask 10.1.1.1
ip-router global set router-id 10.1.1.1
ospf create area backbone
ospf add stub-host 10.1.1.1 to-area backbone cost 1
ospf add interface Client1 to-area backbone
ospf add interface Client2 to-area backbone
ospf add interface Peer to-area backbone
ospf add interface ToNet to-area backbone
ospf set interface Client1 passive
ospf set interface Client2 passive
ospf set interface Client2 cost 100
ospf start
system set name R1
ip-redundancy create vrrp 1 interface Client1
ip-redundancy create vrrp 1 interface Client2
ip-redundancy associate vrrp 1 address 207.50.0.1/22 interface Client1
ip-redundancy associate vrrp 1 address 207.50.4.2/22 interface Client2
```

```
ip-redundancy start vrrp 1 interface Client1
ip-redundancy start vrrp 1 interface Client2
```

Router R2

```
vlan create Client1 ip id 101
vlan create Client2 ip id 102
vlan add ports et.2.2 to Client1
vlan add ports et.2.1 to Client2
interface create ip Client1 address-netmask 207.50.0.2/22 vlan Client1
interface create ip Client2 address-netmask 207.50.4.2/22 vlan Client2
interface create ip ToNet address-netmask 192.168.2.5/30 port et.2.7
interface create ip Peer address-netmask 192.168.2.10/30 port et.2.5
interface add ip lo0 address-netmask 10.2.2.2
ip-router global set router-id 10.2.2.2
ospf create area backbone
ospf add stub-host 10.2.2.2 to-area backbone cost 1
ospf add interface Client1 to-area backbone
ospf add interface Client2 to-area backbone
ospf add interface ToNet to-area backbone
ospf add interface Peer to-area backbone
ospf set interface Client2 passive
ospf set interface Client1 passive
ospf set interface Client1 cost 100
ospf start
system set name R2
ip-redundancy create vrrp 1 interface Client1
ip-redundancy create vrrp 1 interface Client2
ip-redundancy associate vrrp 1 address 207.50.0.1/22 interface Client1
ip-redundancy associate vrrp 1 address 207.50.4.2/22 interface Client2
ip-redundancy start vrrp 1 interface CLient1
ip-redundancy start vrrp 1 interface CLient2
```

Router R3

```
interface create ip ToR1 address-netmask 192.168.2.2/30 port et.2.3
interface create ip ToR2 address-netmask 192.168.2.6/30 port et.2.7
interface create ip Service address-netmask 192.168.3.1/24 port et.2.1
interface add ip lo0 address-netmask 10.3.3.3
ip-router global set router-id 10.3.3.3
ospf create area backbone
ospf add stub-host 10.3.3.3 to-area backbone cost 1
ospf add interface ToR1 to-area backbone
ospf add interface ToR2 to-area backbone
ospf add interface Service to-area backbone
ospf start
system set name R3
dhcp Service define parameters address-netmask 192.168.3.0/24 gateway 192.168.3.1
dhcp Service define pool 192.168.3.2-192.168.3.254
```

Switch L2:1

```
vlan create Client1 ip id 101
vlan add ports et.2.(1-8) to Client1
system set name L2-1
```

Switch L2:2

```
vlan create Client2 ip id 102
vlan add ports et.2.(1-8) to Client2
system set name L2-2
```

Comments

It is important to note, as stated in RFC2338, when acting as a VRRP Master, the Master MUST not respond to direct request of the VRRP IP address unless it owns that IP address as a real physical interface.

Riverstone Networks supports a maximum of six VRRP Virtual Router ID's per interface, five if IPX is configured.

There are many tuning capabilities for VRRP. These include the ability to allow for a warm-up period, provide preempt services, adjust timers and the like. Consult the user guide for tunable parameters.

This configuration provides clients connected to the L2:1 aggregation switch to have IP addressing that ranges form 207.50.0.5-207.50.3.254, a mask of /22 and a default gateway of 207.50.0.1. The Layer two aggregation switch is a single VLAN and provides the means for the VRRP Routers to communicate using the VRRP protocol. Router R1provides the active "MASTER" interface for clients connected to the L2:1 aggregation switch. Router R2 provides the backup IP interface for these clients. Similarly, clients connected to the L2:2 aggregation switch to have IP addressing that ranges form 207.50.4.5-207.50.7.254, a mask of /22 and a default gateway of 207.50.4.2. The Layer two aggregation switch is again a single VLAN and provides the means for the VRRP Routers to communicate using the VRRP protocol. Router R2 provides the active "MASTER" interface for clients connected to the L2:2 aggregation switch. Router R1 provides the backup IP interface for these clients

During normal operations the **"ip-redundancy show vrrp"** command issued on router R1 will show it to have the following VRRP interface dispositions.

```
R1# ip-redundancy show vrrp

VRRP Virtual Router 1 - Interface Client1
-----------------------------------------
Uptime                  0 days, 0 hours, 41 minutes, 1 second.
State                   Master
Priority                255 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.0.1
Associated Addresses    207.50.0.1

VRRP Virtual Router 1 - Interface Client2
-----------------------------------------
Uptime                  0 days, 1 hour, 31 minutes, 47 seconds.
State                   Backup
Priority                100 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.4.1
Associated Addresses    207.50.4.2
```

During normal operations the **"ip-redundancy show vrrp"** command issued on router R2 will show it to have the following VRRP interface dispositions.

```
R2# ip-redundancy show vrrp

VRRP Virtual Router 1 - Interface Client1
-----------------------------------------
Uptime                  0 days, 1 hour, 28 minutes, 37 seconds.
State                   Backup
Priority                100 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.0.2
Associated Addresses    207.50.0.1

VRRP Virtual Router 1 - Interface Client2
-----------------------------------------
Uptime                  0 days, 1 hour, 26 minutes, 37 seconds.
State                   Master
Priority                255 (default value)
```

```
Virtual MAC address    00005E:000101
Advertise Interval     1 sec(s) (default value)
Preempt Mode           enabled (default value)
Authentication         None (default value)
Primary Address        207.50.4.2
Associated Addresses   207.50.4.2
```

The routing tables also provide some good reference information. Providing symmetrical traffic may make the best use of element resources. One could consider enabling ip-enable **"ip enable reverse-flow"** in these types of environments to optimize hardware flow setup rates on the platform. One may also consider the use of different flow modes available to further optimize the flow setup rate, **"ip set port <port> forwarding-mode".**

Using the **"ip show route"** command on the three routers shows the following tables

Router R1

```
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.1.1.1             10.1.1.1             -         lo0
10.2.2.2             192.168.2.10         OSPF      Peer
10.3.3.3             192.168.2.2          OSPF      ToNet
127.0.0.1            127.0.0.1            -         lo0
192.168.2.0/30       directly connected   -         ToNet
192.168.2.4/30       192.168.2.2          OSPF      ToNet
                     192.168.2.10         OSPF      Peer
192.168.2.8/30       directly connected   -         Peer
207.50.0.0/22        directly connected   -         Client1
207.50.4.0/22        directly connected   -         Client2
```

Router R2

```
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.1.1.1             192.168.2.9          OSPF      Peer
10.2.2.2             10.2.2.2             -         lo0
10.3.3.3             192.168.2.6          OSPF      ToNet
127.0.0.1            127.0.0.1            -         lo0
192.168.2.0/30       192.168.2.6          OSPF      ToNet
                     192.168.2.9          OSPF      Peer
192.168.2.4/30       directly connected   -         ToNet
192.168.2.8/30       directly connected   -         Peer
207.50.0.0/22        directly connected   -         Client1
207.50.4.0/22        directly connected   -         Client2
```

Router R3

```
Destination          Gateway              Owner     Netif
-----------          -------              -----     -----
10.1.1.1             192.168.2.1          OSPF      ToR1
10.2.2.2             192.168.2.5          OSPF      ToR2
10.3.3.3             10.3.3.3             -         lo0
127.0.0.1            127.0.0.1            -         lo0
192.168.2.0/30       directly connected   -         ToR1
192.168.2.4/30       directly connected   -         ToR2
192.168.2.8/30       192.168.2.1          OSPF      ToR1
                     192.168.2.5          OSPF      ToR2
207.50.0.0/22        192.168.2.1          OSPF      ToR1
207.50.4.0/22        192.168.2.5          OSPF      ToR2
```

From the client stations trace the packet flow from a client on each of the 207.50.0.0/22 & 207.50.4.1/22 networks to the server n the 192.168.3.0/24 network. You will notice the following.

Clients on the 207.50.0.0/22 network will use this path:

```
Tracing route to 192.168.3.2 over a maximum of 30 hops
```

```
        1       2 ms    1 ms     1 ms   207.50.0.1
        2       2 ms    2 ms     2 ms   192.168.2.2
        3       3 ms    1 ms     1 ms   192.168.3.2
```

Clients on the 207.50.4.1/22 network will use this path:

```
Tracing route to 192.168.3.2 over a maximum of 30 hops
        1       2 ms    1 ms     1 ms   207.50.4.2
        2       2 ms    2 ms     2 ms   192.168.2.6
        3       3 ms    1 ms     1 ms   192.168.3.2
```

Now should a link failure between the acting master and the aggregation switch fail, clients will not notice any session disruption. From one of the clients initiate an ftp transfer with the sever 192.168.3.2. All will proceed normally, with only a slight pause but this pause does not result in a dropped session. After the link is failed perform the trace from client to 192.168.3.2. You will notice something interesting. The path is now using the VRRP backup interface. You can tell simply by looking at the results of the trace. The VRRP backup responds with the real interface IP address.

```
Tracing route to 192.168.3.2 over a maximum of 30 hops
        1       2 ms    1 ms     1 ms   207.50.0.2
        2       2 ms    2 ms     2 ms   192.168.2.6
        3       3 ms    1 ms     1 ms   192.168.3.2
```

Also the VRRP states have adjusted given the new condition. Using the **"ip-redundancy show vrrp"** command on router R1 and router R2 you will notice the adjusted states.

```
R1# ip-redundancy show vrrp

VRRP Virtual Router 1 - Interface Client1
-----------------------------------------
Uptime                  Interface is currently down
State                   Initialize
Priority                255 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.0.1
Associated Addresses    207.50.0.1

VRRP Virtual Router 1 - Interface Client2
-----------------------------------------
Uptime                  0 days, 2 hours, 10 minutes, 47 seconds.
State                   Backup
Priority                100 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.4.1
Associated Addresses    207.50.4.2

R2# ip-redundancy show vrrp

VRRP Virtual Router 1 - Interface Client1
-----------------------------------------
Uptime                  0 days, 2 hours, 11 minutes, 26 seconds.
State                   Master
Priority                100 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.0.2
Associated Addresses    207.50.0.1

VRRP Virtual Router 1 - Interface Client2
```

```
----------------------------------------
Uptime                  0 days, 2 hours, 9 minutes, 27 seconds.
State                   Master
Priority                255 (default value)
Virtual MAC address     00005E:000101
Advertise Interval      1 sec(s) (default value)
Preempt Mode            enabled (default value)
Authentication          None (default value)
Primary Address         207.50.4.2
Associated Addresses    207.50.4.2
```

The routing has also converged around the failure. The three routers now present the following routing tables. Now all requests for 207.50.0.0/22 point to the R2 router. This is different from the routing table that was presented under normal operating conditions.

Router R1

Destination	Gateway	Owner	Netif
10.1.1.1	10.1.1.1	-	lo0
10.2.2.2	192.168.2.10	OSPF	Peer
10.3.3.3	192.168.2.2	OSPF	ToNet
127.0.0.1	127.0.0.1	-	lo0
192.168.2.0/30	directly connected	-	ToNet
192.168.2.4/30	192.168.2.2	OSPF	ToNet
	192.168.2.10	OSPF	Peer
192.168.2.8/30	directly connected	-	Peer
192.168.3.0/24	192.168.2.2	OSPF	ToNet
207.50.0.0/22	192.168.2.10	OSPF	Peer
207.50.4.0/22	directly connected	-	Client2

Router R2

Destination	Gateway	Owner	Netif
10.1.1.1	192.168.2.9	OSPF	Peer
10.2.2.2	10.2.2.2	-	lo0
10.3.3.3	192.168.2.6	OSPF	ToNet
127.0.0.1	127.0.0.1	-	lo0
192.168.2.0/30	192.168.2.6	OSPF	ToNet
	192.168.2.9	OSPF	Peer
192.168.2.4/30	directly connected	-	ToNet
192.168.2.8/30	directly connected	-	Peer
192.168.3.0/24	192.168.2.6	OSPF	ToNet
207.50.0.0/22	directly connected	-	Client1
207.50.4.0/22	directly connected	-	Client2

Router R3

Destination	Gateway	Owner	Netif
10.1.1.1	192.168.2.1	OSPF	ToR1
10.2.2.2	192.168.2.5	OSPF	ToR2
10.3.3.3	10.3.3.3	-	lo0
127.0.0.1	127.0.0.1	-	lo0
192.168.2.0/30	directly connected	-	ToR1
192.168.2.4/30	directly connected	-	ToR2
192.168.2.8/30	192.168.2.1	OSPF	ToR1
	192.168.2.5	OSPF	ToR2
192.168.3.0/24	directly connected	-	Service
207.50.0.0/22	192.168.2.5	OSPF	ToR2
207.50.4.0/22	192.168.2.5	OSPF	ToR2

Reinstating the primary connection from router R1 to router the layer two aggregation switch L2:1 causes all ip-redundancy tables and routing tables to return to the normal operating conditioning state. Again no session loss is encountered when the link is restored. Also, try evoking other types of failures and watching the different recoveries that occur.