Secure Router 4134

Engineering

> Avaya Secure Router 4134 with Silver Peak VX-Series WAN Optimization Appliances Technical Configuration Guide

Avaya Networking

Document Date: January 2012

Document Number: NN48500-635

Document Version: 1.0

Notices
While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer
Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty
Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses
THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright
Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks
The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http:// www.avaya.com/support.

Abstract

This Technical Configuration Guide describes a solution comprised of the Avaya Secure Router 4134 and Silver Peak VX-Series Virtual WAN optimization appliance. The test scenario simulates a typical branch deployment of Enterprise WAN routers. For interoperability testing, the Avaya Secure Router 4134 serves as the WAN router and a Silver Peak VX-Series appliance accelerates LAN traffic. This solution provides an effective strategy for cost reduction towards the use of WAN technologies.

Testing was conducted at the Silver Peak Interoperability Test Lab.

Acronym Key

Throughout this guide the following acronyms will be used:

ACL	Access control list
AES	Advanced encryption standard
AS	Autonomous system
BGP	Border Gateway Protocol
FEC	Forward error correction
GRE	Generic Routing Encapsulation
IPsec	Internet Protocol Security
LAG	Link aggregation group
NX	Silver Peak WAN acceleration hardware
OSPF	Open Shortest Path First
PBR	Policy-based routing
SLA	Service level agreement
VPN	Virtual private network
WoC	WAN optimization controller

Revision Control

No	Date	Version	Revised By	Remarks
1	July 2011	x.y	Team	Initial Draft
2	Dec 2011	0	T. Tedijanto	Updated performance data, added configuration information, other edits
3	Jan 2012	0.1	M. Fitzgerald	Minor edits pages 1, 3, 4, 15, 19, 25
4	Jan 2012	1.0	M. Fitzgerald	Release

Table of Contents

Figures

No table of figures entries found.

Tables

No table of figures entries found.

Conventions

This section describes the text, image, and command conventions used in this document.

Symbols

👍 Tip – Highlights a configuration or technical tip.

ⓘ Note – Highlights important information to the reader.

△ Warning – Highlights important information about an action that may result in equipment damage, configuration or data loss.

Text

Bold text indicates emphasis.

Italic text in a Courier New font indicates text the user must enter or select in a menu item, button or command:

```
ERS5520-48T# show running-config
```

Output examples from Avaya devices are displayed in a Lucida Console font:

```
ERS5520-48T# show sys-info


Operation Mode:         Switch
MAC Address:            00-12-83-93-B0-00
PoE Module FW:          6370.4
Reset Count:            83
Last Reset Type:        Management Factory Reset
Power Status:           Primary Power
Autotopology:           Enabled
Pluggable Port 45:      None
Pluggable Port 46:      None
Pluggable Port 47:      None
Pluggable Port 48:      None
Base Unit Selection:    Non-base unit using rear-panel switch
sysDescr:               Ethernet Routing Switch 5520-48T-PWR
                        HW:02      FW:6.0.0.10  SW:v6.2.0.009
                        Mfg Date:12042004    HW Dev:H/W rev.02
```

Introduction

This Technical Configuration Guide describes a solution comprised of the Avaya Secure Router 4134 and the Silver Peak VX-Series Virtual WAN Optimization Appliance. This solution provides a feature-rich WAN router solution with the added value of WAN data traffic optimization of normal data rate. This document uses Sliver Peak VX 3000 as the reference. It is hosted on the Service Module of SR4134. SR4134 has been validated to support Silver Peak VX-1000, VX-2000, and VX-3000 virtual appliances.

The following figure shows a front view of the Avaya Secure Router 4134:

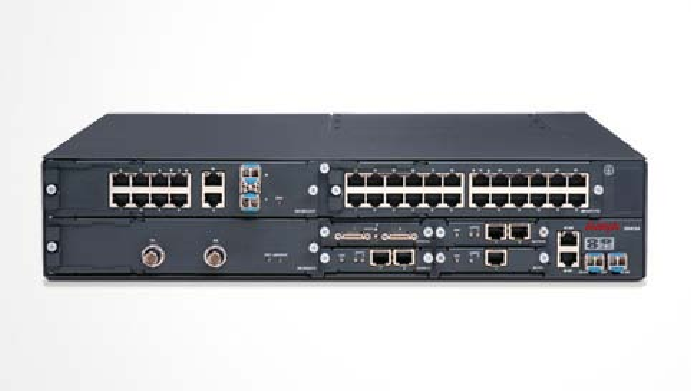

Figure 1 Avaya Secure Router 4134

Avaya Secure Router 4134 Features

The Secure Router 4134 (SR 4134) provides high-end performance and capacity, and integrates multiple networking functions into a single device.

These functions include:

- IPv4 and IPv6 routing
- Wide Area Networking
- High-density Ethernet switching
- Power over Ethernet
- Voice media gateway
- Application hosting
- Security

The above functions enable businesses to realize the promise of the unified branch. The Secure Router 4134 addresses the routing and connectivity needs of large enterprise branches as well as regional or headquarter sites.

Connectivity

For connectivity, the Secure Router 4134 supports a wide range of LAN, WAN, voice gateway, and application options for converged branch and remote sites. WAN connectivity options include T1/E1, serial, ISDN, ADSL2+, channelized DS3/T3 and HSSI, as well as 1000BT and GigE SFP Ethernet.

With full IPv4, IPv6, BGP-4, and multicast routing, the Secure Router 4134 supports sophisticated enterprise deployments. It offers integrated Ethernet switching, with support for up to 58 Gigabit Ethernet and 72 Fast Ethernet ports.

Security

To protect your network, the Secure Router 4134 integrates security that includes a stateful packet inspection firewall and high-speed IPsec VPN encryption. This ensures secure connections to the Internet or public IP networks.

Resiliency

To maximize uptime, the Secure Router 4134 includes the following features that deliver maximum reliability and resiliency:

- Hot-swappable modules
- Redundant power
- Port and platform resiliency
- Voice services that continue voice calling when the primary IP connection is lost

Silver Peak VX Virtual Appliance Features

The Silver Peak VX virtual appliances provide a robust WAN acceleration solution that addresses the bandwidth, latency, and packet loss issues that are common to most enterprise environments.

Silver Peak's optimization techniques are all performed in real-time and primarily at the network (IP) layer to ensure maximum performance across the widest range of applications and WAN environments.

By using the various WAN acceleration techniques, the VX virtual appliances provide the following tangible business benefits:

- ***Improve application performance:*** Applications are no longer subject to the bandwidth and latency issues inherent to WANs.
- ***Increase employee productivity:*** Better application response time makes end users more productive.
- ***Reduce server hardware costs:*** Branch office servers and storage can be eliminated as infrastructure is centralized within a data center. In addition, enterprises do not have to pay additional facility and environmental costs to house servers at remote facilities.
- ***Minimize software licensing costs:*** Reducing the amount of application servers can minimize licensing costs in some application pricing models.
- ***Decrease WAN expenditures:*** When information is localized, less traffic traverses the WAN. This maximizes bandwidth utilization, which minimizes WAN costs.

- ***Lower IT support costs:*** Server centralization minimizes the need for onsite technical support staff in remote offices and reduces travel costs to these facilities.
- ***Maximize security and data protection:*** Enterprise data is best protected when servers are placed in a data center with proper security precautions and environmental protections.
- ***Facilitate compliance:*** IT staff can better audit servers to ensure that they are properly configured in a centralized environment.
- ***Improve disaster recovery:*** It is easier to enforce server backups and ensure proper data storage and retrieval when branch office infrastructure is centrally controlled and managed.

Benefits	**Technology Features**
Enterprise Scalability (from remote offices to large data centers)	▪ Not limited by TCP flows ▪ Support 2 Mbps to 1 Gbps of WAN bandwidth capacity
LAN-like Performance (for optimal application delivery across a distributed enterprise)	▪ Information delivered locally when possible - Only deltas traverse the WAN when delivering “similar” data. ▪ Advanced payload and header compression ▪ Latency/loss mitigation, including TCP acceleration, and adaptive FEC ▪ Quality of Service
Complete Application Transparency	▪ No modification required to clients, servers, or network infrastructure ▪ Byte-level visibility works across all applications
Secure Data Protection (within the NX appliance and across the WAN)	▪ Real-time encryption of disk drives using 128-bit AES ▪ IPsec tunneling between Silver Peak appliances
Network Resiliency (maximum application performance with maximum up-time)	▪ NX appliances feature redundant power supplies ▪ Fail-to-wire (in most models) ▪ Redundant deployment options
Manageability (rapid deployment and cost effective operations)	▪ Easy-to-use setup wizard ▪ Intuitive UI for configuration, monitoring, management, and reporting

SR 4134 with Integrated WAN Optimization

The SR 4134 delivers Silver Peak WAN optimization features by integrating a VX virtual appliance on its server module. The VX virtual appliance runs on various widely used hypervisors. On the SR 4134, the VX virtual appliance runs on VMWare vSphere hypervisor.

Figure 2.0 shows a reference deployment configuration of SR 4134 with WAN optimization. (Note: IP addresses are provided as examples; they match those in the sample router configuration in later sections). The VX appliance is deployed in the router (or out-of-path) mode. SR 4134 router is configured to redirect traffic coming from the LAN interface (or interfaces) to the VX appliance through the backplane interface using the PBR (Policy Based Routing) feature. The VX appliance sends optimized traffic back to the router that in turn routes it to the wide area network.

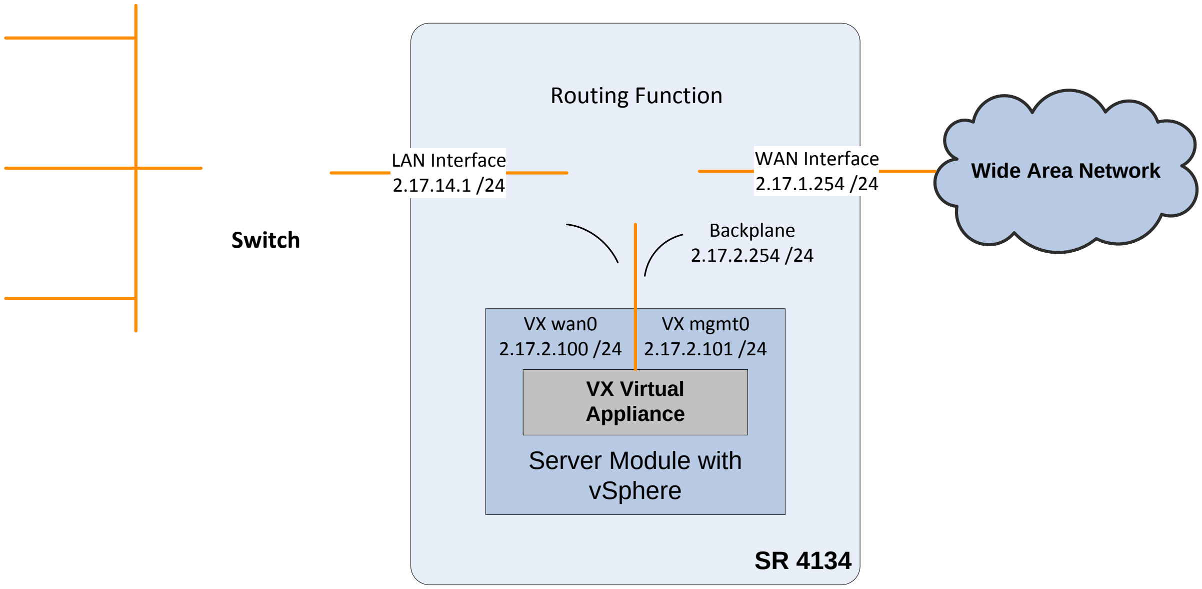

Figure 2 SR 4134 with WAN Optimization

Installing VMWare vSphere on SR4134 Server Module

VMWare vSphere Version 5.0.0 Build 469512 was tested on the SR4134 Server Module for the purposes of this TCG. Silver Peak VX appliances are supported on the latest release of vSphere 5. To install vSphere 5 on the server module, follow these steps:

1. Download the ISO image of vSphere 5.0.0 Build 469512 (or other vSphere 5 version) from the VMWare site http://www.vmware.com/download/.
2. Create a bootable CD/DVD from the ISO image.
3. Connect a video monitor, a keyboard and a mouse to the server module.
4. Enable Intel Virtualization Technology on the SR4134 server module.
    a. Reboot the server module. Press F2 as the server module comes up to enter the BIOS
    b. Click on the “Advanced” tab

   c. Select “> Processor Configuration”

   d. Change Intel® Virtualization Technology setting to “Enabled”

   e. Press Esc to go to the Exit menu

   f. Select “Exit Saving Changes”

5. Boot the ESX installer from the CD/DVD.

   a. Connect the CD/DVD ROM drive containing the bootable disc to one of the server module USB ports

   b. Press F2 as the server module comes up to enter the BIOS

   c. Click on the “Boot” tab

   d. Select “> Boot Device Priority”

   e. Use the arrow key to move “USB CDROM” to the top of the list

   f. Press Esc to go to the Exit menu

   g. Select “Exit Saving Changes”

6. When the vSphere installer comes up, select “Install vSphere Using the Graphical Mode”

   A series of installation messages scroll past until the Welcome page appears.

7. On the Welcome page, click “Next” to continue.

8. Accept the terms of the license agreement and click “Next”.

9. Select keyboard type and click “Next”.

10. Select “No” to install custom drivers with the vSphere installation.

11. Select “Enter a license key later” and click Next. (Note: You can enter a license key later using the VSphere client.)

12. Select the network adapter for the vSphere service console. (Note: There is only one interface on the server module.)

13. Network configuration:

    a. You can configure a static IP address or use DHCP.

    b. If a static IP address was chose, type the complete host name including the domain.

Deploying VX Virtual Appliance

The customer is expected to purchase the VX virtual appliance directly from Silver Peak. The virtual appliance is packaged in an industry-standard format call OVF (Open Virtualization Format) and is delivered as a single file call the OVA (OVF Archive) file. An activation license key is provided with the virtual appliance.

To install a VX OVA on the SR 4134 Server Module, follow these steps:

1. Configure the server module backplane interface

```
interface servmod 5/1
ip address 2.17.2.254 255.255.255.0
exit servmod
```

2. Configure the vSphere host with an IP address in the same subnet as servmod (see step 13 of "Installing VMWare ESX on SR4134 Server Module").
3. Use a browser to connect to the vSphere host IP address. Click on "Download VSphere Client" on the Welcome page. Run the downloaded executable file and follow the direction to install VSphere Client on your workstation.
4. Connect VSphere Client to the vSphere host.
5. Configure wan0 and mgmt0 interfaces on virtual switch vSwitch0. This virtual switch is automatically created by vSphere to connect to the vSphere service console to vmnic0 – the only physical interface on the server module. Virtual interfaces wan0 and mgmt0 will be mapped to interfaces on the VX with the same name.
    a. On the VSphere Client's home page, click on the "Inventory" button. Click on the IP address of the vSphere host to highlight it and click on the "Configuration" tab.
    b. Select "Networking" on the "Hardware" panel and click "Add Networking…" near the upper right corner of the page.
    c. Tthe "Connection Type" screen appears. Select the "Virtual Machine" radio button and click "Next".
    d. Select the "Use vSwitch0" radio button on the "Virtual Machine – Network Access" screen.
    e. Enter wan0 in the "Network Label" field on the "Virtual Machine – Connection Settings" screen and click "Next".
    f. Repeat steps b to e for mgmt0.
6. Configure lan0 and mgmt1 interfaces on vSwitch1. This virtual switch needs to be created and its only purpose is as a place holder for lan0 and mgmt1. No physical network adapter is attached to vSwitch1.
    a. For lan0, follow the same steps as in creating wan0. The only difference is on the "Virtual Machine – Network Access" screen, select the "Create a Virtual Switch" radio button.
    b. For mgmt1, follow the same steps as in creating wan0. The only difference is on the "Virtual Machine – Network Access" screen, select "Use vSwitch1" radio button.
7. At this point, it is assumed that you have the VX OVA file on your workstation (or on a remote server mapped to a local drive). You will be downloading and deploying the OVA file from your workstation onto the vSphere host.
    a. From the "File" menu, select "Deploy OVF Template…"
    b. On the "Deploy OVF Template" screen, use the "Browse" button to point vSphere Client to the location of the VX OVA file.
    c. The "OVF Template Details" screen appears. Click "Next".
    d. The "Name and Location" screen appears. Click "Next".
    e. The "Datastore" screen appears. Click "Next".
    f. The "Network Mapping" screen appears. Click "Next".
    g. The "Ready to Complete" screen appears. Click "Finish".
    h. VSphere Client shows a progress bar while the OVA file is being installed.
8. When the VX OVA file installation is done, set the memory setting of the virtual machine to 3 GB.

   a. Left click on the virtual machine in the navigation panel.
   b. Pick “Edit Settings” in the drop-down menu.
   c. Click “Memory” in the “Virtual Machine Properties” pop-up window and enter 3 GB in the “Memory Size” field.
   d. Click “OK” to finish.

9. Start the VX by clicking on the “Virtual Machines” tab, highlighting the VX, and clicking on the “Play” (green triangle) button.

VX Virtual Appliance Configuration

Configure the VX appliance in the router for “out-of-path” mode. In this deployment mode, the VX appliance is not in the direct path of the network traffic. This ensures that, when the VX is not available to perform WAN optimization, e.g. during a software upgrade, traffic still gets forwarded to the destination across the wide area network, albeit un-optimized.

Silver Peak appliances (VX virtual appliances as well as NX physical appliances) between multiple sites create tunnel mesh among themselves. Administrators can either create a UDP, GRE, or IPsec tunnel. All the traffic processed for optimization is forwarded using this tunnel. Optimized traffic from one site to another site is carried over this tunnel and received at the other end of the tunnel. IPSec tunnels, as do VPN services provided by the ISP, ensure security of the traffic.

Notes:

1. Use VXOA Version 4.4.0.0 or newer.
2. Configure mgmt0 with a static IP address. The use of DHCP is not recommended in the deployment configuration described in this TCG.

Configuring SR 4134 for WAN Optimization

Note- PBR and IP SLA (described below) are currently available in the Secure Router 10.2.1.2 software release. Future date for release in the 10.3.x or later software streams has not been published. PBR is used to redirect traffic that is destined for the WAN to the Silver Peak VX appliance. Redirection policy needs to be applied to all interfaces that may carry this traffic. PBR is a common technique that redirects flows of traffic using an Access Control List (ACL) and a policy instead of normal routing table lookups. Once PBR is enabled on the intended interfaces, all the traffic which matches the rule will be forwarded to Silver Peak VX appliance. The VX appliance receives only those packets that have been redirected to it and applies the WAN optimization techniques. The VX appliance has the option of selectively optimizing the traffic sent to it, based on rules defined in its configuration; all other traffic passes through the appliance unmodified.

To avoid prolonged traffic disruption during times when the VX appliance is not capable of processing traffic, use the IP-SLA feature to track the VX. The PBR-Tracker module monitors the VX appliance. If the VX appliance fails to respond, the tracker module overrides the PBR rules and falls back to the routing table.

The following is a sample policy-map on the SR 4134 for ingress LAN traffic on interface ethernet 0/2. Interface 0/1 is the WAN facing interface and interface servmod 5/1 is the backplane interface facing the server module. The VX IP address is 2.17.2.100.

```
sla profile 2
  icmp-echo 2.17.2.100
  action packet-loss
  threshold-type xofy
  threshold-value 2 5
  exit profile
sla schedule 2
track 20
  service-sla-profile 2
  exit track
qos
  module
    exit module
  chassis
    policy-map map1
      class-map class1 root
        match dest-ip 2.17.5.0/24
        pbr-redirect nexthop  2.17.2.100
        pbr-tracker 20
        exit class-map
      exit policy-map
    exit chassis
  exit qos
interface ethernet 0/1
  ip address 2.17.1.254 255.255.255.0
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 2.17.14.1 255.255.255.0
  aaa
    exit aaa
  qos
    chassis
      service-policy input map1
      exit chassis
    exit qos
  exit ethernet
interface servmod 5/1
  ip address 2.17.2.254 255.255.255.0
  exit servmod
interface console
  aaa
    exit aaa
  exit console
```

Test Methodology and Results

To validate the performance of the reference deployment configuration shown in Figure 2, another Silver Peak appliance is connected across the WAN. Test traffic is then run between two traffic generators, one connected to the LAN interface of the SR 4134 router and the other behind the far-end Silver Peak appliance.

Test Cases

Reducible Dataset Tests

In these tests, we use datasets with known reducibility. These are generated by injecting certain amount of data from a relatively shorter stream of bytes to a longer random stream of bytes. After a while, chunks of data from the shorter stream tend to repeat and thus are deduplicable. By varying the amount of data from the shorter stream relative to that from the longer stream, we can control the reducibility of the dataset. The sizes of the chunks from the shorter stream are also varied. The fine dataset uses smaller chunk and the coarse dataset bigger.

Repeated Transfer Tests

In these tests, we do multiple transfers of the same dataset. The dataset itself does not contain byte patterns that are repeated, and it's only slightly reducible. The dataset used in the tests is sufficiently large that it does not fit in the appliances' RAM. So, for the second and subsequent passes, the appliances need to fetch data from their respective disk.

Test Results

Reducible Dataset Tests

In these tests, test traffic is sent from the traffic generator connected to the LAN interface of the SR 4134 router to the far-end traffic generator. The WAN latency is 100ms, and packet loss is 1%. The WAN link bandwidth is 20 Mbps.

The following are the throughput and reduction ratio charts.

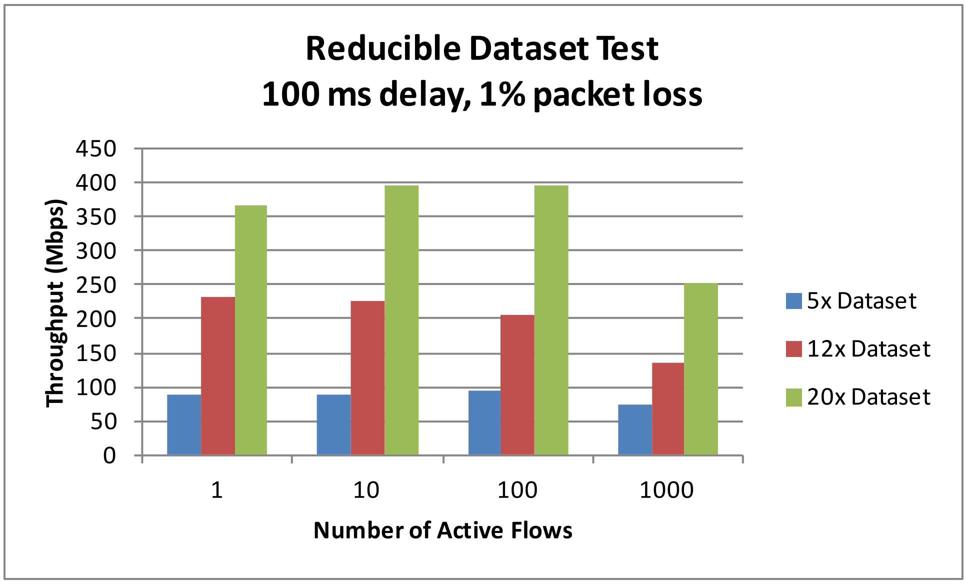

Figure 3 Reducible Dataset Throughput

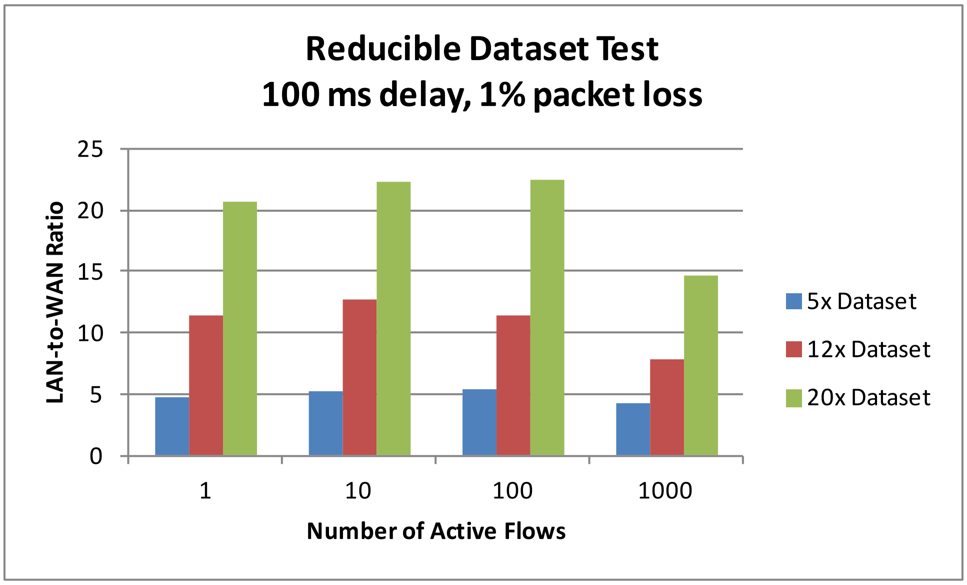

Figure 4 Reducible Dataset Reduction

Repeated Transfer Test

In these tests, test traffic is sent from the traffic generator connected to the LAN interface of the SR 4134 router to the far-end traffic generator. The WAN latency is 100ms, and packet loss is 1%. The WAN link bandwidth is 20 Mbps. The dataset used is slightly compressible as you can see in the first pass throughput and reduction numbers.

The following are the throughput and reduction ratio charts.

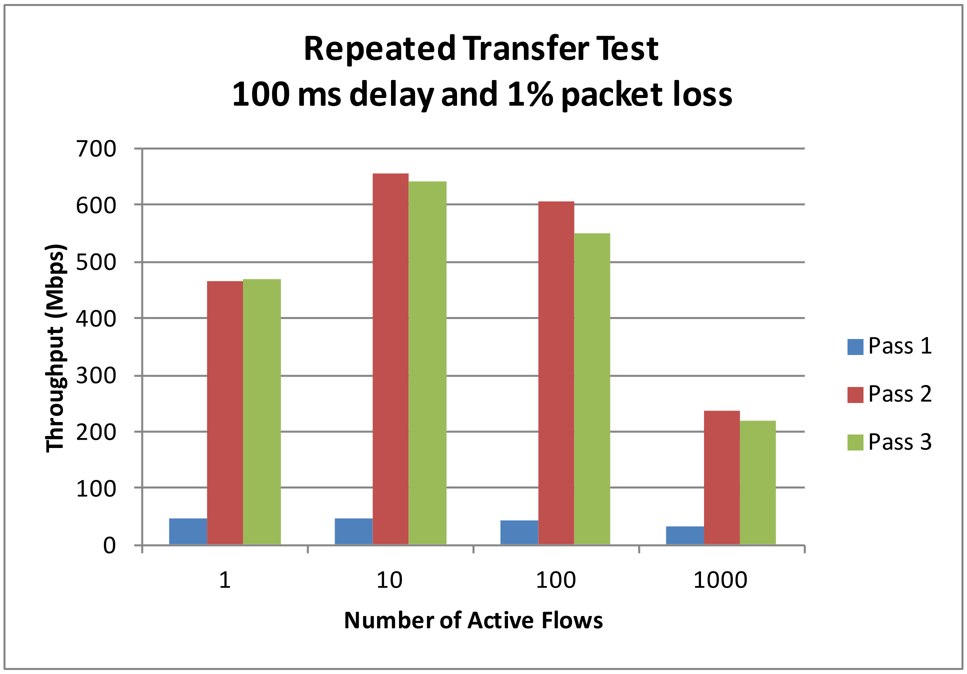

Figure 5 Repeated Transfer Throughput

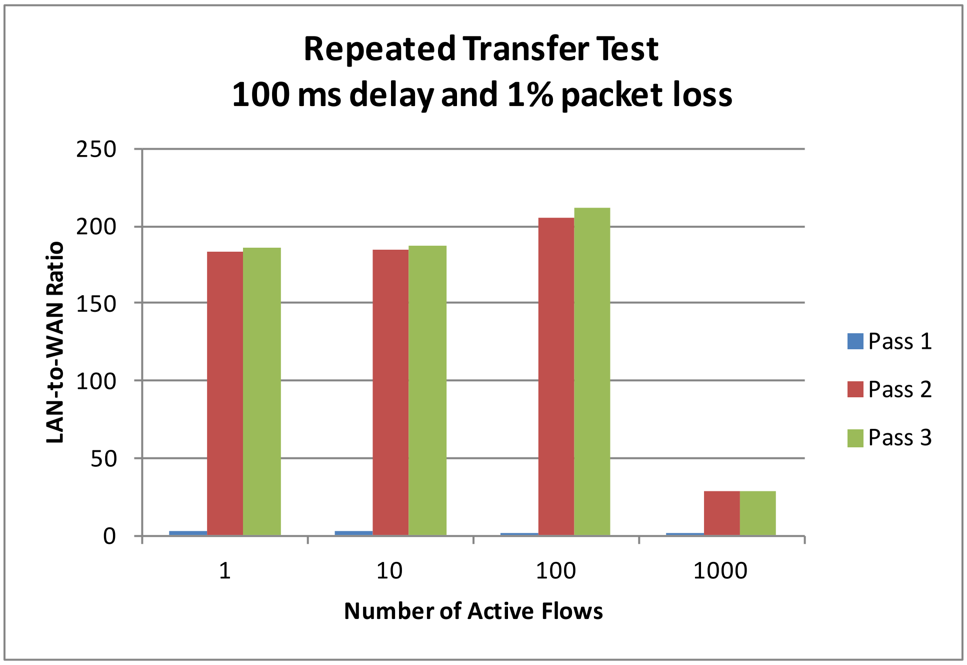

Figure 6 Repeated Transfer Reduction

Conclusion

The Avaya Data Solutions Test Lab’s interoperability testing demonstrated that the Avaya Secure Router 4134 with integrated Silver Peak VX appliance is an effective solution for optimizing the WAN in enterprise networks. The tests highlight the significant traffic reduction and bandwidth optimization with this solution.

After thorough interoperability testing, all test cases were successfully completed and confirm that this solution meets Avaya’s quality and interoperability standards.

Appendix

Secure Router 4134 Sample Configuration

The following code sample shows how to configure the SR 4K edge router.

```
system logging
  console
    priority crit
    exit console
  syslog
    module alarms local0 none
    module dos local0 none
    module forwarding local0 none
    module voip-ssm-cdr local0 none
    module voip-cdr local0 none
    exit syslog
  exit logging
hostname SR
log utc
event
  exit event
usb
  exit usb
terminal
  exit terminal
sla profile 2
  icmp-echo 2.17.2.100
  action packet-loss
  threshold-type xofy
  threshold-value 2 5
  exit profile
sla schedule 2
track 20
  service-sla-profile 2
  exit track
qos
  module
    exit module
  chassis
    policy-map map1
      class-map class1 root
        match dest-ip 2.17.5.0/24
        pbr-redirect nexthop  2.17.2.100
        pbr-tracker 20
        exit class-map
      exit policy-map
    exit chassis
  exit qos
aaa
  tacacs
    exit tacacs
  radius
    primary_server
      exit primary_server
    secondary_server
      exit secondary_server
    exit radius
  exit aaa
vlan database
  exit database
vlan classification
  exit classification
bridge
 mstp
   exit mstp
  exit bridge
lacp
  exit lacp
interface ethernet 0/1
  ip address 2.17.1.254 255.255.255.0
  aaa
    exit aaa
  qos
    chassis
      exit chassis
    exit qos
  exit ethernet
interface ethernet 0/2
  ip address 2.17.14.1 255.255.255.0
  aaa
    exit aaa
  qos
    chassis
      service-policy input map1
      exit chassis
    exit qos
  exit ethernet
interface servmod 5/1
  ip address 2.17.2.254 255.255.255.0
  exit servmod
interface console
  aaa
    exit aaa
  exit console
gvrp
  exit gvrp
snmp-server
  chassis-id SR
  enable traps
    exit traps
  exit snmp-server
rmon
```

```
  exit rmon
oam
  cfm
    enable
    ethtype 88e6
    exit cfm
  exit oam
icmp_timestamp
telnet_banner
  exit telnet_banner
sntp
  exit sntp
reverse_telnet
  set_baud_rate 56000
  exit reverse_telnet
access-list temp permit any
route-map corp permit 100
 match ip address temp
 match interface ethernet
 match source-protocol static
  exit route-map
ip proxy-dns
  exit proxy-dns
ip load-balancing per-flow
ip icmp rate-limit 500
ip dhcps
  exit dhcps
ip route 0.0.0.0/0 2.17.14.5
ip route 2.17.4.0/24 2.17.1.5
ip route 2.17.5.0/24 2.17.1.5
ipv6 icmp rate-limit 500
ipv6 unicast-routing
ipv6 load-balancing per-flow
mpls tunnel-mode uniform
firewall global
  algs
    dns
      exit dns
    exit algs
  max-connection-limit self 2048
  exit firewall
firewall internet
  exit firewall
firewall corp
  policy 1024 out permit
    exit policy
  exit firewall
dst
  no enable
  exit dst


terminal
```

VX Appliance Sample Configuration

The following code sample shows how to configure the Silver Peak NX appliance:

```
##
## Network interface configuration
##
   interface lan0 create
no interface lan0 dhcp
   interface lan0 display
   interface lan0 mtu 1500
   interface lan0 shutdown
   interface lan0 speed-duplex auto/auto
no interface mgmt0 dhcp
   interface mgmt0 ip address 2.17.2.101 /24
   interface wan0 create
no interface wan0 dhcp
   interface wan0 display
   interface wan0 ip address 2.17.2.100 /24
   interface wan0 mtu 1500
no interface wan0 shutdown
   interface wan0 speed-duplex auto/auto

##
## Routing configuration
##
   ip default-gateway 2.17.2.254 mgmt0

##
## Other IP configuration
##
   hostname BRAvaya
   ip name-server 2.17.14.10

##
## Logging configuration
##
   logging local info

##
## System Network Config
##
   system mode router ip 2.17.2.100 /24 nexthop 2.17.2.254

##
## Tunnel Creation
##
   interface tunnel t0 create 2.17.2.100 2.17.4.100 32 auto gre

##
## Tunnel Config
##
   interface tunnel t0 acceleration cifs interactive enable
   interface tunnel t0 acceleration cifs sign-override enable
   interface tunnel t0 acceleration cifs smb2 enable
   interface tunnel t0 acceleration cifs write enable
   interface tunnel t0 acceleration tcp congest-control auto
   interface tunnel t0 acceleration tcp window-scale 6
   interface tunnel t0 admin up
   interface tunnel t0 compression ipheader enable
   interface tunnel t0 compression rtpheader disable
   interface tunnel t0 control-packet dscp be
   interface tunnel t0 gre-protocol 2048
   interface tunnel t0 ipsec disable
   interface tunnel t0 ipsec replay-check-window 1024
   interface tunnel t0 mtu 1500
   interface tunnel t0 packet coalesce enable
   interface tunnel t0 packet coalesce wait 0
   interface tunnel t0 packet fec enable
   interface tunnel t0 packet fec ratio 1:10
   interface tunnel t0 packet reorder wait 100
   interface tunnel t0 threshold dyn-bw-aimd disable
   interface tunnel t0 threshold retry-count 30
   interface tunnel t0 traffic-class 1 min-bandwidth 500000
   interface tunnel t0 traffic-class 1 priority 5
   interface tunnel t0 udp-flow 256
   interface tunnel t0 udp-port 4163

##
## Pass-Through Config
##
   interface pass-through max-bandwidth 10000

##
## Policy Config
##
   route-map map1 1000 match protocol icmp any any dscp any
   route-map map1 1000 set tunnel t0 if-down pass-through

##
## Network management configuration
##
   clock timezone America North United_States Pacific
no ntp disable
no ntp server 2.17.4.6 disable
   ntp server 2.17.4.6 version 4

##
```

Converting SR0004062E6 “Unified Communications Mediation Services Module for MSFT OCS-R2” for use by VMWare and Silver Peak VX

The following process can be used to enable VMWare and Silver Peak VX virtual appliances to run on existing SR0004062E6 modules.:

1. Increase memory from 2Gb to 4Gb: Replace (qty 2) memory modules with (qty 2) Micron MT18HVF25672PZ-667H1
2. Upgrade BIOS to support virtualization. Contact Product Management (Mike Fitzgerald at mifitzge@avaya.com, or Dave Norton at nortond@avaya.com) to obtain new BIOS and field upgrade instructions.

3. De-install Windows 2008 (or format drive).
4. Follow instructions above to load VMWare VSphere and Silver Peak VX virtual appliance.

Additional Resources

- For Avaya Secure Router 4134 product documentation, go to http://support.avaya.com/.
- For Silver Peak products, go to http://www.silver-peak.com/
- For Silver Peak product documentation, go to http://www.silver-peak.com/Technology/.