NetQoS SuperAgent
Spanning Best Practices

INTRODUCTION

The NetQoS SuperAgent Spanning Best Practices document is designed to illustrate the best strategies for mirroring traffic to a SuperAgent collector for monitoring in an enterprise environment. While many methods exist for mirroring TCP traffic to SuperAgent, this document highlights the most common SPAN configurations for Cisco switches. The concepts illustrated in this document apply to all switches that support port mirroring capabilities but Cisco configuration commands are used as an example.

SuperAgent passively monitors traffic on its collectors through a Monitor Network Interface Card (NIC). This document is designed to leverage the capabilities of SuperAgent collectors to monitor the most traffic possible by understanding application data flow and monitoring traffic efficiently. By strategically implementing spanning scenarios, SuperAgent can monitor more traffic accurately.

Oftentimes the temptation in SuperAgent spanning is to SPAN all traffic over to the monitor NIC. This scenario can yield adverse results in both the data reporting and the collector's capacity. An overloaded SuperAgent collector will experience high CPU utilization and/or discard useful traffic, yielding incomplete data. In the examples provided below, common data flow scenarios are used to guide users in the correct ways to monitor SuperAgent data through spanning.

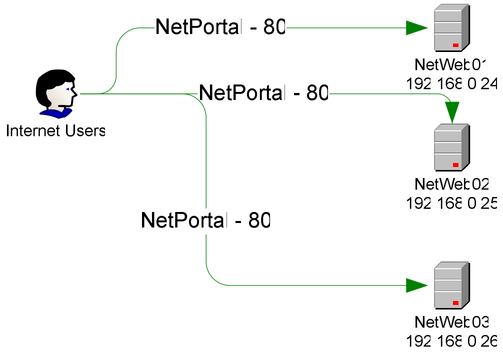
This document provides the best methodologies for using SPAN sessions to mirror traffic to SuperAgent. Port mirroring is a safe, effective way to mirror the traffic to SuperAgent collectors. Some switches do not provide the diverse range of SPAN capabilities required for these scenarios. For instances where traffic can not be mirrored optimally, alternatives are available like fiber taps.

Single-Tier Application

For this scenario, a single tier of an application is monitored. This scenario is effective for the first-tier into the application architecture. With the current client-server model, front-end portal applications are either web-based or Citrix-based applications which serve up application data to the end-user.

The NetPortal application is a web-based application used by Internet users to purchase products and services from the XYZ Company. It is accessed from the Internet by users connecting to one of three web servers.

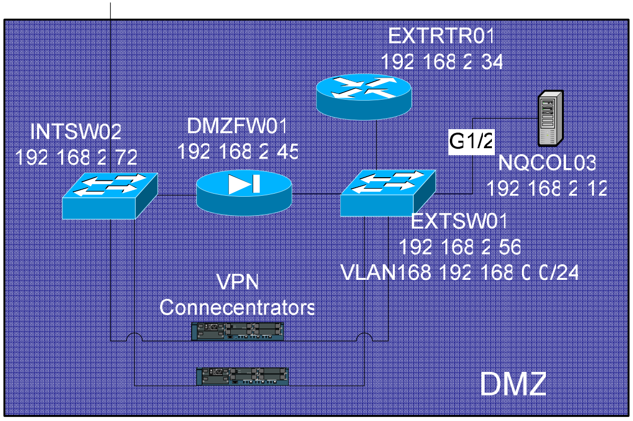
Figure 1: Company XYZ Single-Tier Application Architecture



With this environment, the web servers and a SuperAgent collector have been placed in the XYZ enterprise DMZ. All three web servers are members of VLAN168. Figure 2 illustrates the network diagram of the DMZ. The monitor NIC's switch port is labeled in the white text box. The bulleted list below indicates the switch port connections for the three web servers:

- NetWeb01 – 192.168.0.24 – FastEthernet0/2
- NetWeb02 – 192.168.0.25 – FastEthernet0/5
- NetWeb03 – 192.168.0.26 – FastEthernet0/9
- NQCOL03MON – GigabitEthernet1/2
- NQCOL03 – 192.168.2.12 – FastEthernet0/3

Figure 2: Company XYZ DMZ Network Diagram



For this scenario, spanning the individual server ports for the three web servers is the optimal way to obtain SuperAgent collection. To SPAN this traffic, specify the three server ports as the source interfaces and the destination interface of the SuperAgent Collector. Below are the SPAN configuration commands to implement the required port mirroring for Cisco Catalyst switches.

SPAN Configuration Example for IOS Software

```
EXTSW01 (config)# monitor session 1 source interface fa0/2
EXTSW01(config)# monitor session 1 source interface fa0/5
EXTSW01(config)# monitor session 1 source interface fa0/9
EXTSW01(config)# monitor session 1 destination interface gi1/2
```

SPAN Configuration Example for Catalyst OS Software

```
Console> (enable) set span 0/2,0/5,0/9 1/2 create
```

SPAN on Catalyst 6500 Series

Due to limitations in spanning individual ports, span the VLAN 168 and enable duplicate packet checking on the collector (see Duplicate Packets section for more details).

```
Console> (enable) set span 168 1/2 create
```

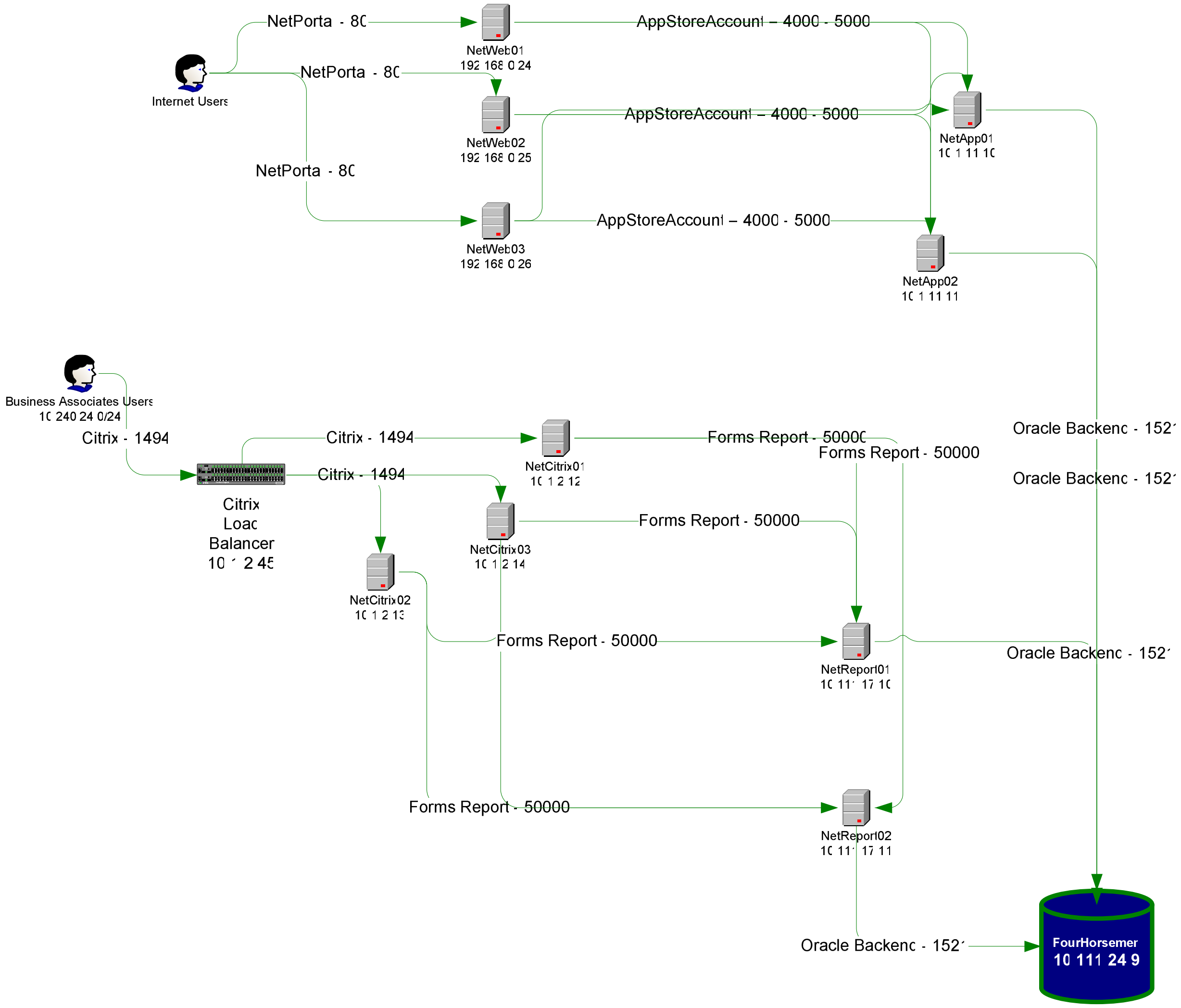
Spanning VLANs

While many devices support spanning VLANs to support this configuration, it is not the optimal utilization of SuperAgent's collection abilities. In this scenario, VLAN 168 has the capacity of handling 253 hosts. At peak hours of operation, 253 possible circuits transmitting data at full-duplex 100Mbps can easily overload a single 1000Mbps circuit (the monitor port). If many of the servers not monitored by SuperAgent overload the monitor NIC, causing it to discard packets, SuperAgent won't see all of the traffic necessary to make accurate metrics. This could result in incomplete data due to discarded packets. Also, spanning VLANs duplicates the traffic (adding even more load to the monitor port) and requires the Duplicate Packet reduction.

MULTI-TIER APPLICATION

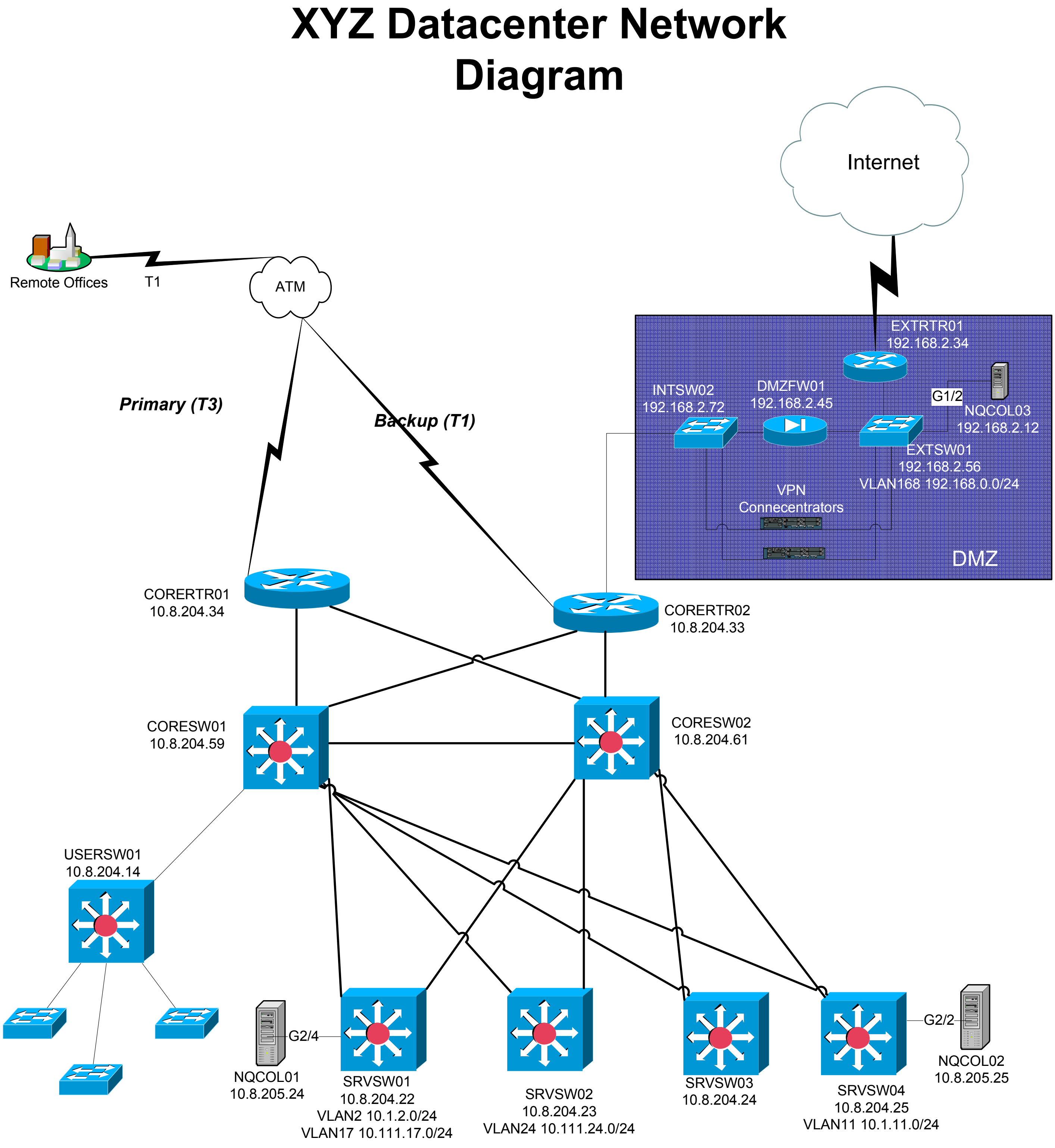
For the multi-tiered application a distributed SuperAgent solution is required to provide the visibility for each application tier. Understanding the application architecture is essential when designing the SuperAgent collection solution. As indicated by the network diagram, SuperAgent collectors are placed on individual switches to monitor server communications. In this scenario, not all of the servers need to be spanned to obtain the right metrics for SuperAgent. In fact, spanning all of the servers in this scenario will yield more duplicate packets and reduce the capacity of the collectors.

Figure 3: XYZ Company Application Architecture



Since the SPAN configuration includes all transmit and receive packets, the ports that are required to be spanned are reduced. This is caused by the fact that the collector will see front-end and back-end traffic to the servers from spanning the middle tier of the architectures. For this scenario, the ports that should be spanned are the Citrix Load Balancer, the NetReport, NetWeb, and NetApp servers. The data for the Oracle backend server will be obtained from the NetReport and NetApp server spans. Traffic from the Citrix Load balancer SPAN and NetReport SPAN will provide visibility into the NetCitrix tier.

Figure 4: XYZ Company Network Diagram



The bulleted list below outlines the ports and switches where the servers are connected:
EXTSW01:

- NetWeb01 – 192.168.0.24 – FastEthernet0/2
- NetWeb02 – 192.168.0.25 – FastEthernet0/5
- NetWeb03 – 192.168.0.26 – FastEthernet0/9
- NQCOL03MON – GigabitEthernet1/2
- NQCOL03 – 192.168.2.12 – FastEthernet0/3

SRVSW01:

- Citrix Load Balancer – 10.1.2.45 – FastEthernet1/4
- NetCitrix01 – 10.1.2.12 – FastEthernet4/2
- NetCitrix02 – 10.1.2.13 – FastEthernet4/6
- NetCitrix03 – 10.1.2.14 – FastEthernet6/2
- NetReport01 – 10.111.17.10 – FastEthernet2/1
- NetReport02 – 10.111.17.11 – FastEthernet2/7
- NQCOL01MON – GigabitEthernet2/4
- NQCOL01 – 10.8.205.24 – FastEthernet4/4

SRVSW02:

- FourHorsemen – 10.111.24.9 – FastEthernet2/2

SRVSW04:

- NetApp01 – 10.1.11.10 – FastEthernet1/2
- NetApp02 – 10.1.11.11 – FastEthernet3/4
- NQCOL02MON – GigabitEthernet2/2
- NQCOL02 – 10.8.205.25 – FastEthernet3/8

To monitor this multi-tiered application, multiple SPAN sessions should be configured on EXTSW01, SRVSW01, and SRVSW04. The configuration commands for the switches are given below.

Configuration Example for IOS Software

EXTSW01

```
EXTSW01(config)# monitor session 1 source interface fa0/2
EXTSW01(config)# monitor session 1 source interface fa0/5
EXTSW01(config)# monitor session 1 source interface fa0/9
EXTSW01(config)# monitor session 1 destination interface gi1/2
```

SRVSW01

```
EXTSW01(config)# monitor session 1 source interface fa1/4
EXTSW01(config)# monitor session 1 source interface fa2/1
EXTSW01(config)# monitor session 1 source interface fa2/7
EXTSW01(config)# monitor session 1 destination interface gi2/4
```

SRVSW04

```
EXTSW01(config)# monitor session 1 source interface fa1/2
EXTSW01(config)# monitor session 1 source interface fa3/4
EXTSW01(config)# monitor session 1 destination interface gi2/2
```

Configuration Example for Catalyst OS Software

EXTSW01

```
Console> (enable) set span 0/2,0/5,0/9 1/2 create
```

SRVSW01

```
Console> (enable) set span  1/4,2/1,2/7 2/4 create
      SRVSW04
Console> (enable) set span 1/2,3/4 2/2 create
```

MULTI-TIER APPLICATION – VACL WITH RSPAN

For this same multi-tiered scenario, the limitations on Catalyst 6500 series switches do not allow for the proper SPAN configuration. An alternative method, VACL with RSPAN, creates the flexibility required to properly monitor traffic for the multi-tiered application.

RSPAN, remote spanning, captures the traffic on one switch, mirrors it to a designated VLAN, and forwards this traffic to one or more destination ports for analysis. Coupling this technology with the ability to have Layer 2, Layer 3, and Layer 4 security afforded by VLAN access lists (VACLs) gives the SuperAgent collector visibility into a wide variety of the applications without overloading the switch port. The RSPAN scenario spans the proper VLANs over to the capture port while the VACL limits the captured traffic to ensure the switch port is not overloaded. In this scenario, enable duplicate packet discarding to ensure accurate results in SuperAgent.

This example scenario illustrates the configuration parameters for SRVSW01 using VACLs with RSPAN technology on the Cisco Catalyst 6500.

Catalyst 6500 using Cisco IOS Software

The following configuration example was used to achieve the results described in this example on a Supervisor Engine 2 with MSFC2 using Cisco IOS Software Release 12.1(13)E4 on the supervisor engine.

```
!
Hostname SRVSW01

! Defines L2 VLANS 2 and 17
vlan 2, 17

! Defines VLAN 100 as the RSPAN VLAN
vlan 100
 remote-span

!
! The monitor port requires no special configuration
interface GigabitEthernet2/4
 description NQCOL01MON
 no ip address

!
! Defines L3 VLANS 2 and 17
interface VLAN2
 ip address 10.1.2.0 255.255.255.0
!
interface VLAN17
 ip address 10.111.17.0 255.255.255.0

! VACLs require that a corresponding SVI (L3 Interface) exists
! It can remain unconfigured and administratively shutdown
interface VLAN100
 description RSPAN VLAN - Must exist for VACL on RSPAN VLAN
 no ip address
 shutdown
```

```
! The IP extended ACL that matches TCP traffic for the servers to be spanned
ip access-list extended TCP-TRAFFIC
 permit tcp ip any host 10.1.2.45
 permit tcp ip host 10.1.2.45 any
 permit tcp ip any host 10.111.17.10
 permit tcp ip host 10.111.17.10 any
 permit tcp ip any host 10.111.17.11
 permit tcp ip host 10.111.17.11 any

! Defines the VLAN access-map (VACL)
Vlan access-map RSPAN-VACL 10
 match ip address TCP-TRAFFIC
 action forward

! Maps the VACL to the RSPAN VLAN
 vlan filter RSPAN-VACL vlan-list 100

! Monitor Session 1 captures bidirectional traffic from
! VLANs 2 and 17 to RSPAN VLAN 100
monitor session 1 source vlan 2, 17
monitor session 1 destination remote vlan 100

! Monitor session 2 captures bidirectional traffic from
! RSPAN VLAN 100 to interface gig2/4
monitor session 2 source remote vlan 100
monitor session 2 destination interface Gi2/4
```

Catalyst 6500 using Cisco Catalyst OS Software

The following configuration was used on Supervisor Engine 2 with MSFC2 to achieve the results described in this example using Cisco Catalyst OS Software Release 7.5(1) on the supervisor engine and Cisco IOS Software Release 12.1(13)E4 on the MSFC2.

```
#CatOS Configuration on Supervisor Engine:
set system name SRVSW01
!
# Defines L2 VLANs 2 and 17
set vlan 2, 17

# Defines RSPAN VLAN 100
set vlan 100 rspan name VLAN100 state active

#Defines VACL TCP-TRAFFIC that matches TCP Traffic
# For Citrix Load Balancer and Report Servers
set security acl ip TCP-TRAFFIC permit tcp ip any host 10.1.2.45
set security acl ip TCP-TRAFFIC permit tcp ip host 10.1.2.45 any
set security acl ip TCP-TRAFFIC permit tcp ip any host 10.111.17.10
set security acl ip TCP-TRAFFIC permit tcp ip host 10.111.17.10 any
set security acl ip TCP-TRAFFIC permit tcp ip any host 10.111.17.11
set security acl ip TCP-TRAFFIC permit tcp ip host 10.111.17.11 any

# Commits the VACL to the hardware
commit security acl TCP-TRAFFIC
```

```
#Maps the VACL to the RSPAN VLAN
set security acl map TCP-TRAFFIC 100

#Defines the RSPAN source as bidirectional traffic on VLANs 2 and 17
set rspan source 2, 17 100 both multicast enable create

#Defines the RSPAN destination as port 2/4
set rspan destination 2/4 100 inpkts disable learning enable create
```

```
! Cisco IOS configuration on MSFC2:
!
hostname SRVSW01

!Defines L3 VLANs (SVIs) 2 and 17
interface VLAN2
 ip address 10.1.2.0 255.255.255.0

!
interface VLAN17
 ip address 10.111.17.0 255.255.255.0
```

Duplicate Packets

When spanning VLANs, the SuperAgent collector will receive two copies of each packet. In this situation, the SuperAgent collector requires additional configuration parameters. On the collector, there is a file named RetransPacketDefs.ini.sav located in the D:\NetQoS\bin directory. Remove the .sav from the file name on all collectors and restart the SuperAgent service.

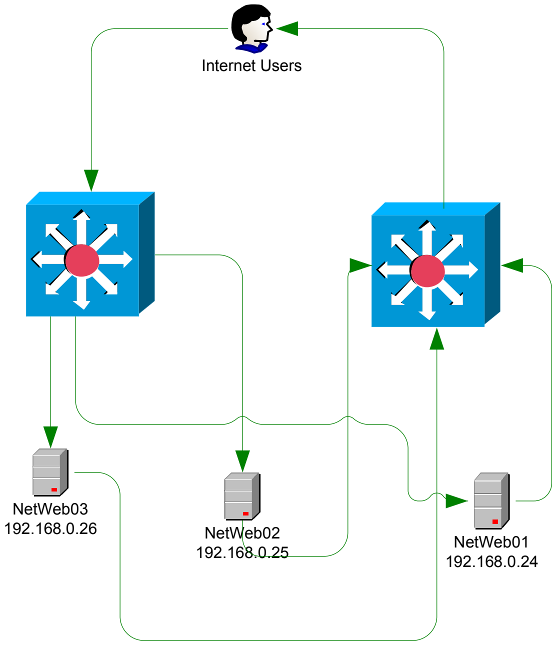
Multi-NIC collectors

SuperAgent is currently designed to have a single monitor port. However all collectors are capable of being ordered with two copper or two fiber network interface cards (NIC). There is one case in which a multi-nic collector is required. When the transmit traffic and receive traffic are flowing through two channels, SuperAgent may be licensed for a multi-nic environment. This requires a special licensing capability.

There are two primary ways in which the unidirectional streams may be seen. The first is with an inline fiber tap. Some fiber taps are designed to go inline with two network cards coming out, one for transmit traffic and one for receive. In this case, a multi-nic collector would be required so that SuperAgent may accurate account for its metrics.

The second case for a multi-nic collector is in an asymmetric routing environment, as pictured below. In this scenario, two core switches route traffic differently. Data going into the data center is switched by the first core switch while data going out of the data center is switched by the second core switch. In this case, two port mirrors to the same collector must be used to capture the transmit and receive traffic for the server farm.

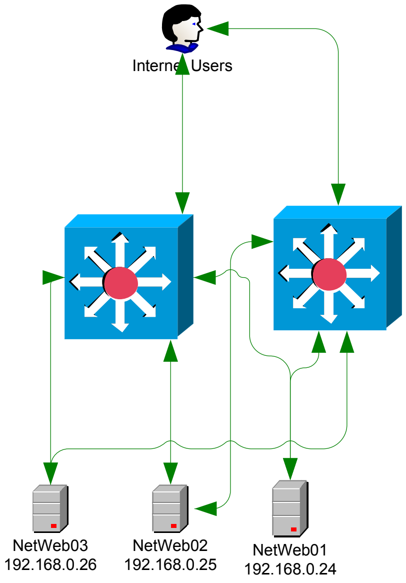
Figure 5: Asymmetric Routing environment Diagram



Load Balanced Core Switch Monitoring

In the case where two core switches are being used to monitor traffic and the switches are load balanced (i.e. connections from the client to the same server could be accomplished through either switch), SuperAgent allows every server to be monitored by two switches. As pictured, the clients may establish a session through core switch 1 or core switch 2. The traffic and sessions would continue to use that route throughout the transaction but may be initialized by either switch. In this case, when assigning a server to a collector, select two collectors. The first collector would be monitoring traffic off switch 1 and the second would be monitoring the sessions off of switch 2. When SuperAgent reports these metrics up to the environment for that server, the metrics and server health are combined from the two collectors' collected data.

Figure 6: Load Balanced Core switches



PRODUCT SUPPORT MATRIX

The configuration examples illustrated in this document are produced from Cisco Catalyst Switch documentation. While multiple vendors support port mirroring capabilities, the limitations and abilities of port mirroring differ for each company and product platform. The below product support matrix illustrates the array of switching devices on the market with the ability to mirror port(s).

Many nuances with port mirroring capabitilities for these switches exist that may inhibit the ability of SuperAgent to monitor traffic correctly. Consult the Administration and User guides for each of these switching architectures to understand the performance implications for the devices where SuperAgent Collection will be configured.

For many products on the market, only a single port may be mirrored to the collection device. In this scenario, mirroring the uplink port is the most effective way to get a portion of the traffic. Any inter-switch traffic would not however be captured.

3Com switches support Roving Port Analysis, a single port solution for the majority of their switches. The configuration guide for the information may be located at 3Com Roving Port Analysis Configuration.

Company	*Product Name/Model*	*Port mirroring supported*
3Com Corp.	Super Stack II Switch 3300	Yes
Addtron Technology	ADS-824M	Yes
Addtron Technology	ADS-816M	Yes
Allied Telesyn International	AT-8224XL	Yes
Asante Technologies	IntraStack 6014DSB	Yes
KTI Networks	KS2316 10/100 Fact Ethernet Switch	Yes
Matrox Electronic Systems	Matrox Switchbox 12	Yes
Bay Networks, a Nortel Networks Line of Business	Bay Stack 350T-HD 10/100 Autosense Switch	Yes
Bay Networks, a Nortel Networks Line of Business	Bay Stack 350T 10/100 Autosense Switch	Yes
Bay Networks, a Nortel Networks Line of Business	Bay Stack 350 F - HD 10/100 Autosense Switch	Yes
Bay Networks, a Nortel Networks Line of Business	Bay Stack 350F 10/100 Autosense Switch	Yes
Cisco Systems	Cisco Catalyst 2924C XL	Yes
Cisco Systems	Cisco Catalyst 2924 XL	Yes
Matrox Electronic Systems	Matrox Switchbox 12 (FX)	Yes
NBase-Xyplex	MegaSwitch II SX-2024	Yes
Teleware Corp.	Teleway 1080EX	Yes
Enterasys Networks	Vertical Horizon VH-4802	Yes
Foundry Networks	FastIron Workgroup Switch 16 port	Yes
Foundry Networks	FastIron Workgroup Switch 24 port	Yes
IBM Corp.	IBM 8271-712 NWAYS Ethernet LAN Switch	Yes
Intel Corp.	Express 550T Routing Switch (ES550T)	Yes
NBase-Xyplex	MegaSwitch SX-2016	Yes
LANart Corp.	ETS 1210 Fast Ethernet Switch	Yes
Lucent Technologies (formerly Prominet)	Lucent P550 Cajun Switch	Yes
Network Peripherals	FE-D512	Yes
Olicom	CrossFire 8420 Fast Ethernet Switch	Yes
NBase-Xyplex	Mega Switch II SX-2012	Yes
Proteon LAN Products by Microvitec	ProNet/E Series 84 Fast Ethernet Switch	Yes
Network Peripherals	FE-DS-24	Yes
Performance Technologies	Nebula 6000 Departmental Switch	Yes
Performance Technologies	Nebula 4000 Workgroup Switch	Yes
Performance Technologies	Nebula 8000 Fault Tolerant Backbone Switch	Yes
Point Com	CEM56-100	Yes
Asante Technologies	Friendly Net FS4004DS Switch	No
NDC Communications	Plug-n-Switch	No
Asante Technologies	Friendly Net FS4008DS Switch	No
Compaq Computer Corp.	Compaq NETELLIGENT 5708 TX	No
Omnitron Systems Technology	FlexSwitch 600X 10/100 Switch with Opitonal Fiber/UTP Plug-Ins	No
Omnitron Systems Technology	FlexSwitch 600X3 10/100 Ethernet Modular Switch (Model # 6200)	No
Compex	Compex Ready Switch SNW 1213	No
TRENDware International	TE100-S1212	No
D-Link Systems	5016	No

Related Articles and Documentation

Span feature documentation for Cisco switches: http://www.cisco.com/warp/public/473/41.html
Port Monitoring Configuration Guides (Cisco):
http://www.cisco.com/en/US/tech/tk389/tk816/tech_configuration_guides_list.html
Interface Mirroring (Juniper): http://www.juniper.net/techpubs/software/erx/junose52/swconfig-system-basics/download/interface-mirroring-config.pdf
General Commands Reference for various vendors: http://www.networkintrusion.co.uk/switch.htm

NetQoS Contact information

Technical Support

The Technical Support center at NetQoS is responsible for handling technical inquiries into product installation, configuration, and operations.

- Phone: 877-835-9575 ext 612
- email: support@netqos.com
- Hours of Operation: 7 AM - 7 PM CST

Account Management

Account Management department is responsible for handling any inquiries into customer satisfaction. Additionally the account manager is responsible for assisting with sales contacts and procurement of equipment.

- Phone: 877-835-9575
- website: http://www.netqos.com