DESIGN/PLANNING/ IMPLEMENTATION GUIDE

CISCO MDS 9000 FAMILY SANTAP DESIGN GUIDE

AUDIENCE

This guide is for network designers, planners, and administrators who are responsible for configuring and maintaining the Cisco MDS 9000 Family of multilayer director and fabric switches.

TECHNICAL OVERVIEW

The Cisco MDS 9000 SANTap service enables customers to deploy third-party appliance-based storage applications without compromising the integrity, availability, or performance of a data path between the server and disk. The Cisco SANTap service provides a reliable copy of storage write operations to a third-party appliance, thereby enabling applications to provide data protection, data migration, remote replication, and SLA monitoring, without the traditional drawbacks of deploying devices in-band within the data path or out-of-band in conjunction with host-based software agents.

The Cisco SANTap service runs on the Cisco Storage Services Module (SSM), which can be inserted into any Cisco MDS 9500 Series or Cisco MDS 9200 Series multilayer intelligent storage switch. The architecture of the SSM enables SANTap to service devices connected directly to the ports on the module, or to devices connected anywhere in the fabric, including devices attached to legacy switches.

The SANTap service can be configured to run in two different operating modes: proxy mode and transparent mode. Both modes offer unique design advantages which permit SANTap to fit customer requirements with minimal changes to current configurations.

SANTap Proxy Mode

SANTap proxy mode is designed to provide SANTap functionality to devices connected anywhere in the fabric, whether using modern SANTap capable switches or legacy switches. Proxy mode allows SANTap to be enabled in a fabric with minimal downtime and minimal reconfiguration and recabling. The keys to SANTap functioning in this mode are the ability to segment fabrics using VSANs and the virtual interfaces that the SSM presents to the fabric. These virtual interfaces can be instantiated into any VSAN and present a virtual initiator to the target in one VSAN and present a virtual target to a host in another VSAN.

SANTap proxy mode offers the following advantages:

- The ports to which the storage devices and hosts are attached are not moved.
- Devices can remain attached to a legacy switch rather than be migrated to a modern SANTap capable switch.
- More than four hosts can use the same data path processor (DPP).
- The SANTap service is not coupled to a physical port.

Figure 1 shows SANTap proxy mode.

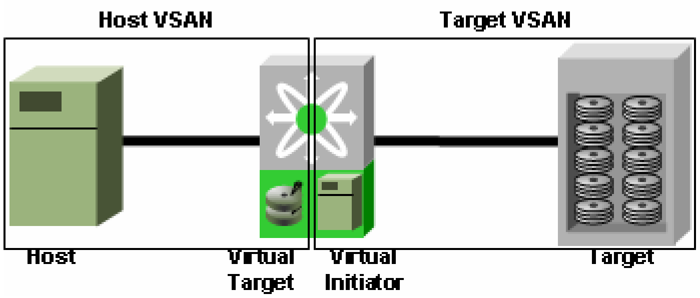

Figure 1. SANTap Proxy Mode

SANTap Transparent Mode

SANTap transparent mode captures traffic between a host attached directly to an SSM port and a target attached to a port anywhere in the fabric. This configuration appears like a traditional setup in which both the host and target reside in the same VSAN, but can also be used with more complex configurations using inter-VSAN routing (IVR).

SANTap transparent mode offers the following advantages:

- There is a logical simplicity of the host interface being physically attached to the SSM.
- Up to four hosts can share the same DPP.
- The FCID of the hosts and storage does not change.
- Hosts running UNIX operating systems, such as HP-UX and AIX, do not require reconfiguration.

Figure 2 shows SANTap transparent mode.

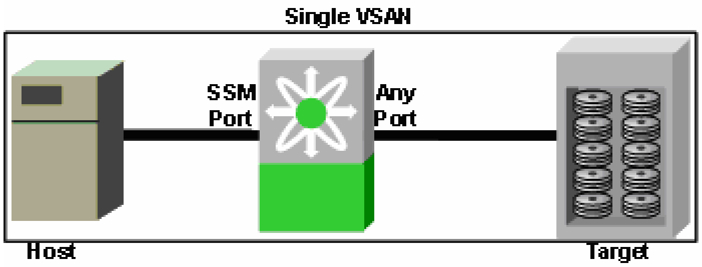

Figure 2. SANTap Transparent Mode

ARCHITECTURE AND DESIGN

The Cisco SANTap service provides a level of availability that cannot be achieved with an appliance in the data path between a host and storage. By removing that appliance from the data path, the SANTap service enables a significantly more reliable solution than an appliance could offer because the primary data path between host and storage is independent of the appliance.

Enhanced Availability

If a SANTap enabled appliance fails, data continues to flow between host and storage. This level of availability may be suitable for data migration, which is generally not mission critical, but not for continuous data protection. Redundant components can be used when deploying the SANTap service in the same way they are used with building fabrics.

Best Practices

The following hardware may be added to enhance the availability of SANTap-enabled applications:

- Redundant SANTap-connected partner appliances to the same fabric. The SANTap service can provide functionality to redundant SANTap connected appliances.
- Redundant SSMs within the same director.

- Redundant switches or directors which have multi-homed SANTap appliances.
- Multiple links between hosts and storage devices.

Multipathing Drivers and Software

The SANTap service enables hosts to see storage through the service as if the service were transparent. For instance, if a particular storage subsystem is attached and being serviced by SANTap, the same communication between host and storage device is uninhibited by the SANTap service. This transparency allows multipathing software to use multiple paths through separate fabrics, even when the SANTap service is enabled on that storage path. A configuration with multipathing software can even be nondisrputively migrated to use the SANTap service by failing over to a single fabric, adding the service to the fabric, failing back to the SANTap enabled fabric, and upgrading the other fabric.

Using SANTap and Other Intelligent Applications on an SSM Simultaneously

The SANTap service must be provisioned on all ports or in groups of four ports on an SSM. If SANTap is provisioned on only part of the module, additional intelligent features can be provisioned on other groups of ports on the same SSM. The SSM operates as a standard 32-port switching module until intelligent applications are provisioned. See the "Deployment Examples" section for specific instructions on how to provision data path processors on the SSM for the SANTap service.

Scaling SANTap

The SANTap service scales linearly by using additional data path processors (DPP) on a SSM or by adding additional SSMs to the fabric. There is no limit to the number of SSMs that can be added to a fabric. Additional SANTap appliances may need to be added. Check with the SANTap partner for specifications on how many devices their appliances can support.

LUN Mapping and LUN Masking Considerations

LUN masking is an access control method that a storage device uses to restrict or permit access to volumes of data, or LUNs (logical unit numbers). The device has a list of hosts, typically identified by worldwide names (WWN), which are allowed to access particular LUNs on the storage device. LUN mapping generally incorporates the LUN masking function, but also adds a reference to a volume that is specific to the host accessing the data. For instance, host A and host B connect to the same port on a storage device. If both of these hosts want to access a volume identified as LUN 0 on the storage device, LUN masking either permits or denies the hosts access to this same volume. LUN mapping provides an additional layer to actually associate a request from host A for LUN 0 to a different internal volume than a request from host B for LUN 0. Some vendors may have brand names for LUN mapping such as LUN Security or AccessLogix.

The SANTap service was designed in such a way that LUN masking and LUN mapping on a storage device never needs to be changed when SANTap is introduced into the fabric. The SANTap-enabled appliance can send and receive traffic through the virtual initiator, using the virtual initiator's WWN, which eliminates changes required on the storage device. Some SANTap vendors have not implemented this feature and may require changes to LUN masking and LUN mapping to overcome these limitations. Consult the SANTap vendor's documentation regarding any configuration changes that may be required on the storage device.

Best Practices

A common problem when configuring the SANTap service is that a host may be unable to see a LUN that is being serviced by SANTap. This problem is most likely caused by zoning issues. The best way to configure SANTap is using an incremental process, whereby zoning is checked after the completion of each configuration step. In some instances, it may be practical to enable the default zone set policy in a VSAN to be set to permit to see if the problem is related to zoning. However, never use this method to troubleshoot zoning problems if any critical data resides on storage that is attached to that fabric. Doing so could cause data corruption.

Securing SANTap Using VSANs and Zoning

SANTap entities are presented as virtual devices into the SAN. They are placed into VSANs and send and receive SCSI commands over Fibre Channel, just as any other target or host. Because of these common characteristics that virtual devices share with real devices, they are managed in the same way as real devices. Namely, they are placed into VSANs, which provides fabric isolation, and placed into zones, which isolates communication between the devices.

Best Practices

The most effective way to ensure the security of the fabric is to follow the general best practices of security for both the fabric and management interfaces. Treat SANTap virtual devices as any other devices and incrementally zone the devices as they are added to the fabric. An incremental zoning approach aids in determining which devices are actually the virtual devices that were just added to the fabric. Never rely on a default zone permit communication between devices because this provides no access control when additional devices are added to the fabric.

Treat appliances and virtual devices just as any other device and zone these devices as they are added. Although some SANTap vendors may encourage short-cutting these processes, the additional care ensures the integrity of the fabric in case of error or misconfiguration.

Design Considerations

Devices connected to legacy switches leverage intelligent applications on the Cisco MDS 9000 Family without requiring the storage and hosts to be directly connected to the Cisco MDS 9000 Director. Some limitations of legacy switches must be considered when adding them to a SANTap design.

Transparent mode is the simpler of the two modes to use for connecting legacy fabrics. The same design considerations apply when using modern directors and switches as well as using legacy switches, namely that either the hosts or disks must be connected directly to the SSM running the SANTap service.

Figure 3 shows a transparent mode configuration with a legacy director.

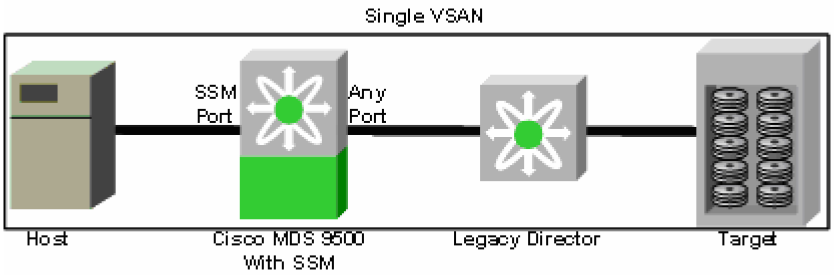

Figure 3. SANTap Transparent Mode with Legacy Director

Proxy mode requires hosts and disks to be connected to separate VSANs. Because legacy switches are incapable of supporting multiple fabrics, virtual or otherwise, the Cisco MDS 9000 Director or fabric switch must be connected between two legacy fabrics and those two fabrics must be in separate VSANs. Inter-VSAN routing (IVR) can be used to allow devices on the legacy switches other than devices serviced by the SANTap service to communicate with each other.

Figure 4 shows a proxy mode configuration with a legacy director.

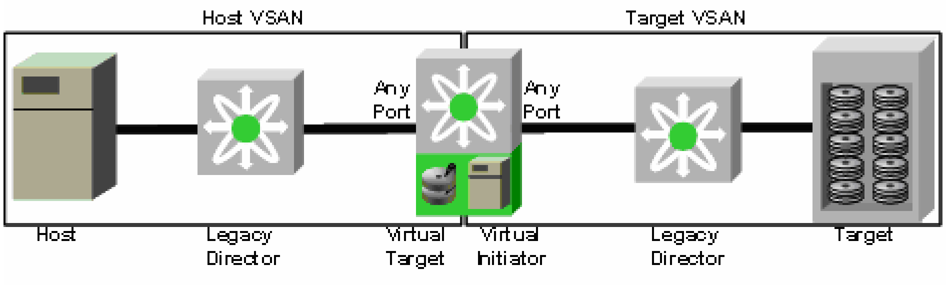

Figure 4. SANTap Proxy Mode Configuration with a Legacy Director

Potential Impacts

Local Only Configuration

Traditionally, with legacy switches, deploying separate, redundant fabrics was mandatory. However, the fabric isolation provided by VSANs and the reliability of the Cisco MDS 9500 Director has eliminated the need to deploy redundant fabrics. Even so, some customers want the additional protection of having physically separate SANs.

The following hardware is required for a local-only configuration with redundant SSMs:

- Two SSMs.
- An MDS 9500 Director or two MDS 9216 fabric switches, with two open slots for the SSM.
- Two SSE licenses, one for each SSM.
- Two partner appliances or partner software loaded on two partner appliances per the vendor's specifications.

Additionally, if the customer wants director level redundancy, the SSMs must not reside in the same MDS 9500 Director.

Figure 5 shows a local only configuration.

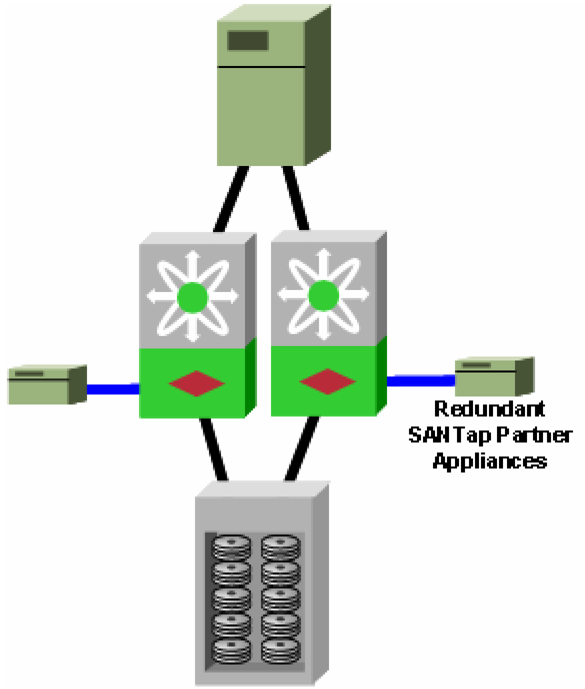

Figure 5. Local Only Configuration

Local and Remote Configuration

The majority of SANTap enabled partner applications are targeted for remote replication and remote continuous data protection (CDP). Most applications fall into this category and require the following hardware:

- Two SSMs.
- An MDS 9500 Director or two MDS 9216 fabric switches, with two open slots for the SSM.
- Two SSE licenses, one for each SSM.
- Two partner appliances or partner software loaded on two partner appliances per the vendor’s specifications.

The following hardware is required on the remote site:

- Two SSMs.
- An MDS 9500 Director or two MDS 9216 fabric switches, with two open slots for the SSM.
- Two SSE licenses, one for each SSM.
- Two partner appliances or partner software loaded on two partner appliances per the vendor’s specifications.

The following element is required between the primary and the remote site:

- WAN connectivity to interconnect the partner appliances.

Partner appliances require WAN connectivity for remote replication environments. Check with the vendor of the SANTap enabled appliance for specific configuration information on redundancy and WAN requirements

Figure 6 shows a local and remote configuration.

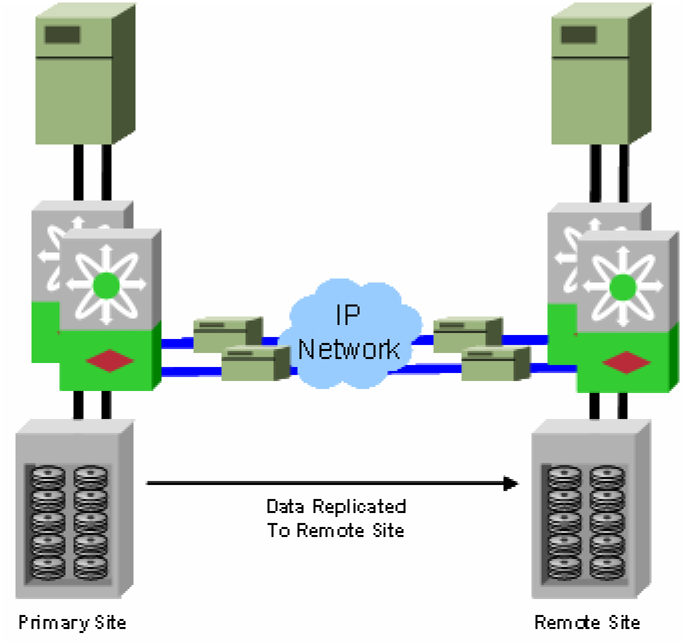

Figure 6. Local and Remote Configuration

OPERATION AND MANAGEMENT

The following steps are common to configuring both proxy mode and transparent mode. They are the recommended process to ensure the highest integrity of data in the SAN. SANTap vendors may recommend additional settings to protect their unique architectures.

1. Create a unique VSAN just for SANTap enabled appliances and the SANTap virtual interfaces that communicate with the appliance.

2. Provision the SANTap service on the SSM if it has not already been provisioned.

3. Enable the SANTap service in the appliance VSAN using the instructions in the “Deployment Examples” section.

Best Practices

The SANTap service allows appliances to communicate indirectly to storage targets through the virtual SANTap initiator, thereby eliminating the need to change LUN masking and LUN mapping on the storage device. Some SANTap vendors may require that the appliance communicate directly with the storage devices, which either requires overlapping an appliance VSAN with a target VSAN in proxy mode, or using inter-VSAN routing to route traffic from the appliance device to the storage devices.

Configuring SANTap Transparent Mode

To configure SANTap transparent mode, follow these steps:

1. Follow the common steps for both proxy mode and transparent mode.

2. Create a VSAN for the storage and host.

3. Zone the host to the storage device.

4. Enable the SANTap service using the partner appliance.

Figure 7 shows a SANTap transparent mode configuration.

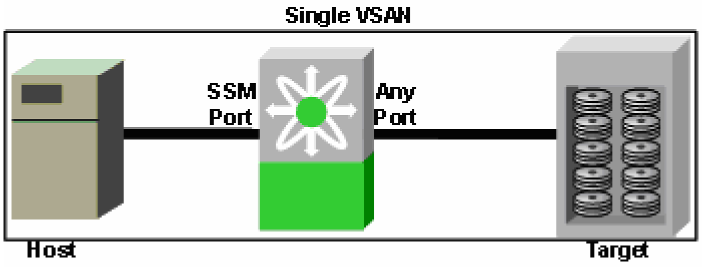

Figure 7. SANTap Transparent Mode Configuration

Configuring SANTap Proxy Mode

To configure SANTap proxy mode, follow these steps:

1. Follow the common steps for both proxy mode and transparent mode.
2. Create a VSAN for the host.
3. Create a VSAN for the storage device.
4. Zone the host to the virtual target in the host VSAN.
5. Zone the virtual initiator to the target in the target VSAN.
6. Enable the SANTap service using the partner appliance.

Figure 8 shows a SANTap proxy mode configuration.

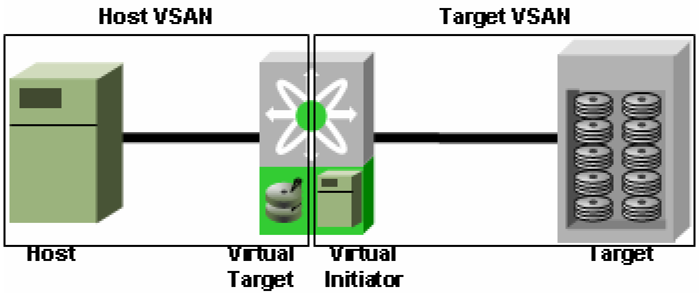

Figure 8. SANTap Proxy Mode Configuration

DEPLOYMENT EXAMPLES

This section provides procedures that can be used when configuring SANTap.

Booting a Storage Services Interface (SSI) Code Image on an SSM

Intelligent features are included in a software image that is separate from the main switch system and kickstart images. This image must be downloaded from Cisco Connection Online and set to run on the module before proceeding with any SANTap configuration.

To boot the SSI image, enter the following commands:

```
switch# config terminal

switch(config)# no boot ssi

switch(config)# boot ssi bootflash: m9000-ek9-ssi-mz.2.1.1a.bin module slot-number
```

Provisioning the SANTap Service on the SSM

The SSM has eight data path processors (DPP) integrated into the module. These DPPs logically sit behind groups of four ports on the SSM. Each DPP can be provisioned for separate intelligent storage applications using the command-line interface (CLI).

To enable all DPPs on an SSM for SANTap, use the following commands:

```
switch# config terminal

switch(config)# ssm enable feature santap module slot-number
```

To enable SANTap only on specific DPPs on an SSM module, use the following commands:

```
switch# config terminal

switch(config)# ssm enable feature santap interface fc slot-number starting-interface –
ending-interface
```

For example, the following command will provision the two DPPs behind ports 1 through 8 on an SSM inserted in slot 2:

```
switch(config)# ssm enable feature santap interface fc 2/1 – 8
```

Creating the SANTap Interface to the Replication Appliance (Control Virtual Target)

The control virtual target (CVT) is the SANTap interface on the SSM that is presented to the SANTap appliance. This interface appears as a virtual device in the VSAN that the partner appliance is connected to, once the following command is issued. Only create the CVT after the appliance VSAN has been created on the switch.

```
switch# config terminal

switch(config)# santap module slot-number appl-vsan VSAN-id
```

Checking SANTap Virtual Devices and Sessions

The following commands show information about the SANTap configuration.

To show information about the device virtual target, enter the following command:

```
switch# show santap module slot-number dvt
```

To show information about the device virtual target LUNs, enter the following command:

```
switch# show santap module slot-number dvtlun
```

To show information about the sessions that the SANTap appliance has created, enter the following command:

```
switch# show santap module slot-number session
```

If the output of this command shows no information, the SANTap appliance either has not created or cannot create any sessions. This command shows information only after the host has successfully communicated with the actual target through the SANTap virtual target and the appliance has created a session.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International
BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA