C H A P T E R **3**

Deployment Considerations

This chapter describes the requirements and guidelines that are necessary to successfully deploy your Cisco I/O Accelerator SAN. Read this chapter before installing or configuring Cisco I/O Accelerator (IOA).

This chapter includes the following sections:

Supported Topologies

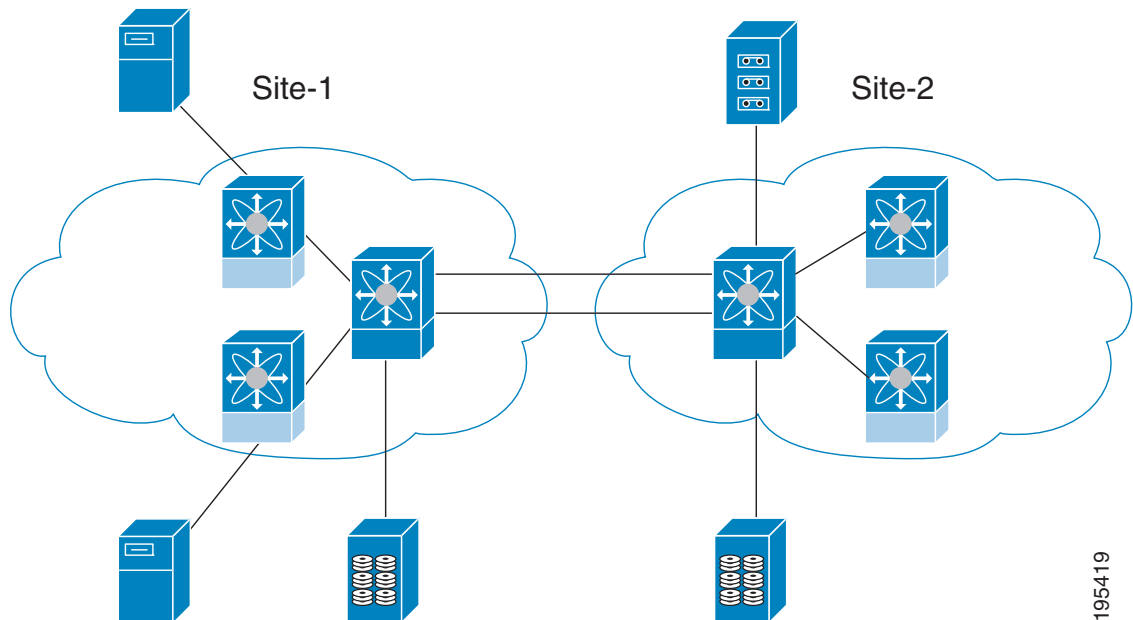This section includes the following topics:

Core-Edge Topology

Figure 3-1 illustrates the core-edge topology where you are recommended to place the IOA interfaces (MSM-18/4 or SSN-16) in the core switches that interconnect the two sites. The ISLs interconnecting the two sites over a MAN or WAN are typically on the core switches as well, so this becomes a natural place to deploy the IOA service. This deployment provides the following benefits:

- Provides consolidation of IOA service at the core.
- Allows easy scalability of the IOA service engines based on the desired throughput.

- Allows you to plan and transition from FC or FCIP acceleration solutions to IOA. This is because these acceleration solutions will likely be deployed at the core switches already and will allow for a smooth transition to IOA.

- Facilitates planning the capacity based on WAN ISL throughput on the core switches themselves.

- Provides optimal routing as the flows have to traverse these core switches to reach the remote sites.
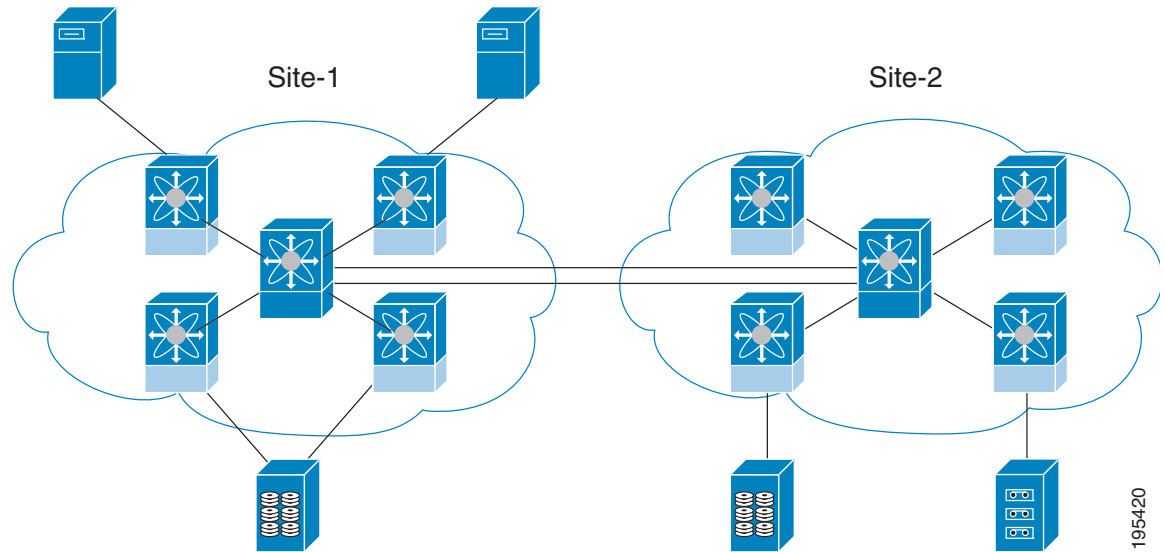
Figure 3-1   Core-Edge Topology

Edge-Core-Edge Topology

Figure 3-2 illustrates the edge-core-edge topology where you are recommended to place the MSM-18/4 Module or SSN-16 Module at the core switches that interconnect the two sites.
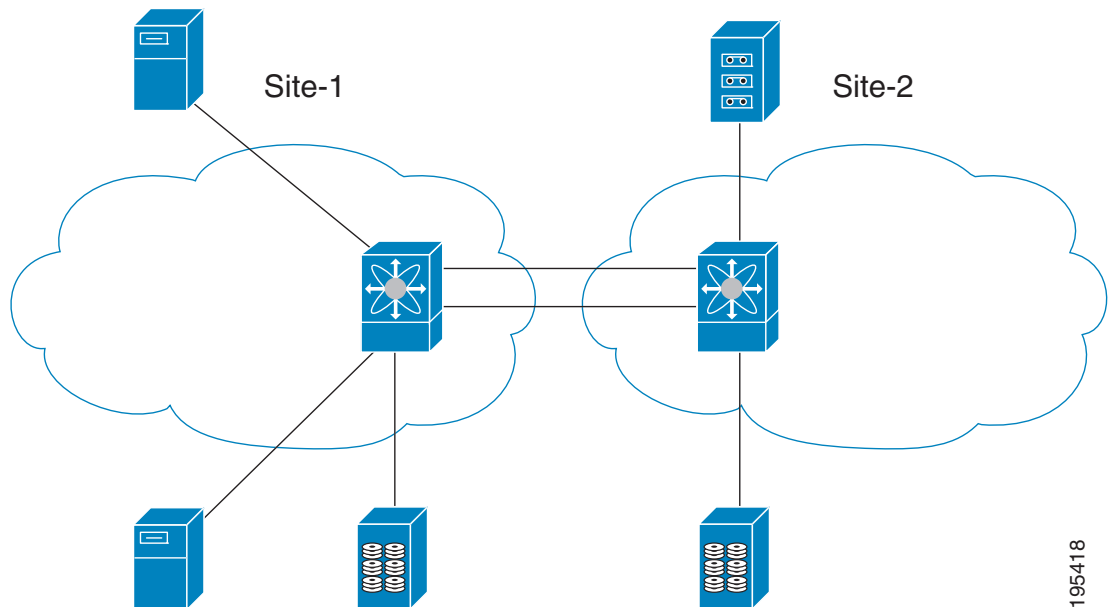
Figure 3-2   Edge-Core-Edge Topology

Collapsed Core Topology

Figure 3-3 illustrates the collapsed core toplogy where you are recommended to place the MSM-18/4 Module or SSN-16 Module (IOA interfaces) in the core switches that interconnect the two sites.

Figure 3-3   *Collapsed Core Topology*

Extended Core-Edge Topology

Figure 3-4 illustrates the extended core-edge topology where you are recommended to place the IOA interfaces (MSM-18/4 Module or SSN-16 Module) in all the core switches. As the IOA service load balances the traffic by selecting any IOA interface from each site and forms the IOA interface pair for a given flow, certain failures may result in sub-optimal routing. The recommendation is to interconnect the core switches within each site for maximum availability of IOA service. The ISLs between the core switches in the specific site has as much throughput as the WAN ISLs between the sites.

Figure 3-4   Extended Core-Edge Topology
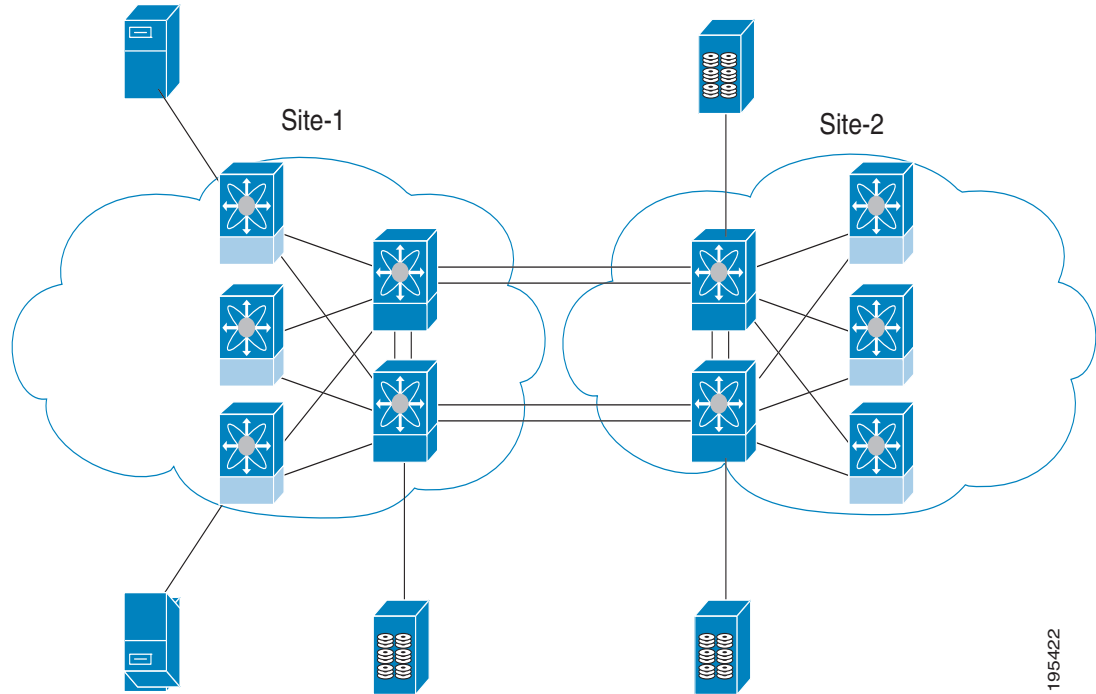
Extending Across Multiple Sites

Figure 3-5 illustrates the IOA implementation where the IOA service is extended across multiple sites. In this example, Site-4 consolidates the tape backup from Site-1, Site-2, and Site-3. Each IOA cluster represents a site pair, which means that there are three unique clusters. This topology provides segregation and scalability of the IOA service across multiple sites. In Site-4, a single switch participates in multiple IOA clusters.

Figure 3-5   *Extended Across Multiple Sites*
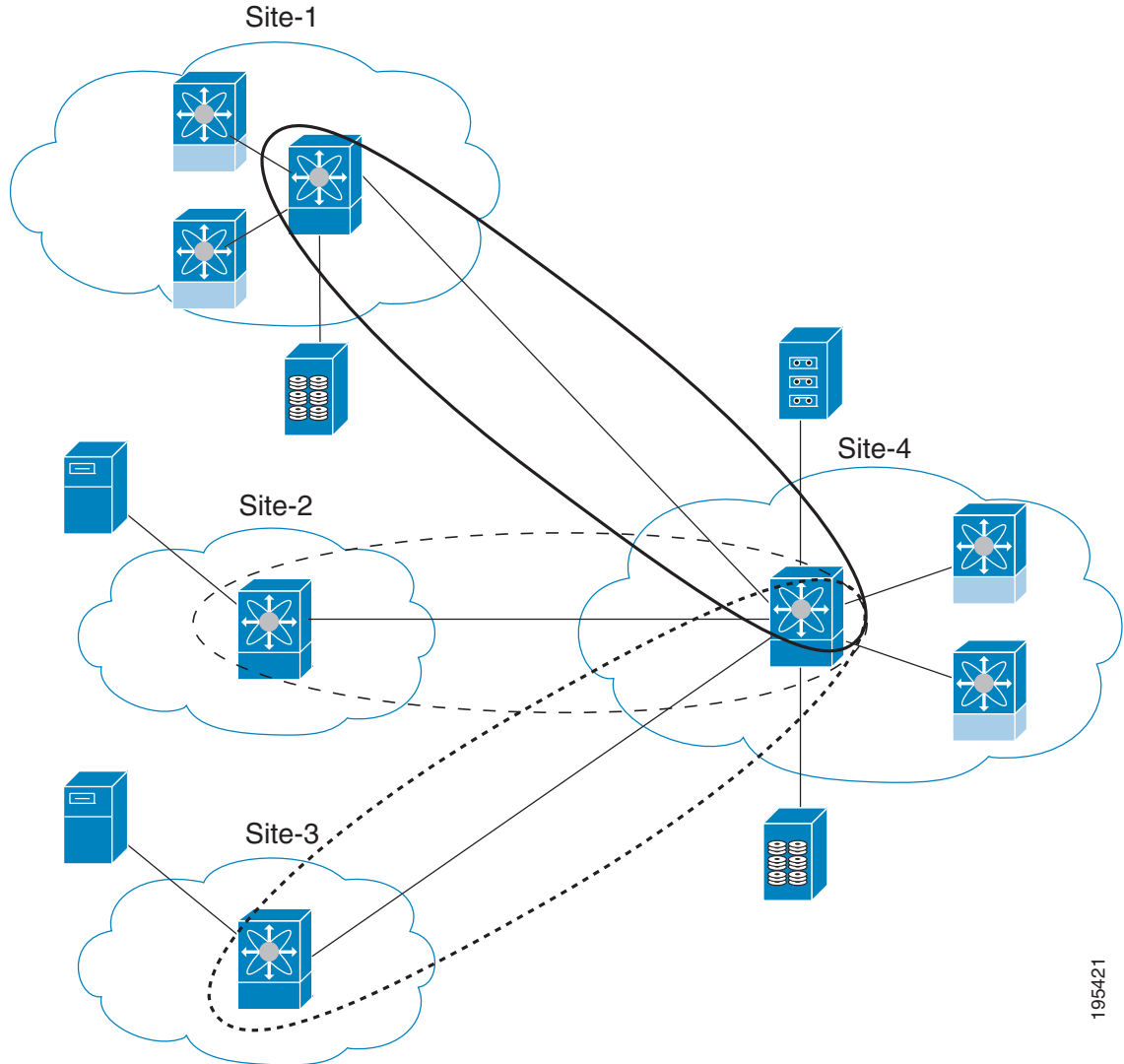
IVR Topologies

For IOA to support IVR flows, we recommend that you place the IOA interfaces on the MSM-18/4 or SSN-16 module in the IVR border switches for optimum routing. IOA must always be deployed on the host and target VSANs. Packets from the host get redirected to the IOA interface in the host VSAN, traverses the IVR transit VSANs for routing, and again gets redirected to the IOA interface in the Target VSAN before it reaches the target and vice-versa. IVR transit VSANs are used only for FC routing. IOA is not supported or deployed on transit VSANs.

For more information, refer to the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*.

Other Topologies

In certain other topologies, the edge switches are connected across the WAN. In such cases, we recommend that you do the following:

- Transition the WAN links from the edge to core switches to provide consolidation and optimal routing services.

- Deploy the IOA service in the core switches.

> **Note**   IOA is supported for IVR flows starting from the Cisco MDS NX-OS Release 5.0(1a).

Deployment Guidelines

This section includes the following topics:

General Guidelines

When you deploy IOA, consider these general configuration guidelines:

- The IOA flows bound to the IOA interfaces on the module undergoing an upgrade will be affected.

- Clustering infrastructure uses the management IP network connectivity to communicate with the other switches. In the case of a switchover, the management IP network connectivity should be restored quickly to preserve the cluster communication. If the management port is connected to a Layer 2 switch, spanning-tree must be disabled on these ports. In a Cisco Catalyst 6000 Series switch, you can implement this by configuring the **spanning-tree portfast** command on these ports which will treat these ports as access or host ports.

Scalability and Optimal Performance Considerations

For maximum scalability and optimal performance, follow these IOA configuration guidelines:

- Zoning considerations: In certain tape backup environments, a common practice is to zone every backup server with every tape drive available to allow sharing of tape drives across all the backup servers. For small and medium tape backup environments, this may be retained when deploying IOA. For large backup environments, the scalability limit of number of flows in IOA must be considered to check if the zoning configuration can be retained. Best practice for such an environment is to create multiple tape drive pools, each with a set of tape drives and zones of only a set of backup servers to a particular tape drive pool. This allows sharing of tape drives and drastically reduces the scalability requirements on IOA.

- Deploy IOA interfaces (MSM-18/4 or SSN-16) in the core switches in both core-edge and edge-core-edge topologies. When multiple core switches are interconnected across the MAN or WAN, do the following:

  - Deploy the IOA interfaces equally among the core switches for high availability.

- – Interconnect core switches in each site for optimal routing.
- • Plan for Geneneration 2 and above line cards to avoid any FC-Redirect limitations. There is a limit of only 32 targets per switch if Generation 1 modules are used to link the ISLs connecting the IOA switch and target switches or if the host is directly connected to a Generation 1 module.
- • Depending on the WAN transport used, you may have to tune the Fibre Channel extended B2B credits for the round-trip delay between the sites.

Resiliency Considerations

When you configure IOA, consider the following resiliency guidelines:

- • Plan to have a minimum of one additional IOA service engine for each site for handling IOA service engine failures.
- • Tuning for E_D_TOV: Fibre Channel Error Detect Timeout Value (E_D_TOV) is used by Fibre Channel drives to detect errors if any data packet in a sequence takes longer than the specified timeout value. The default timeout value for E_D_TOV is 2 seconds. IOA has an built-in reliability protocol (LRTP) to detect and recover from ISL failures by doing the necessary retransmissions. However, you need to ensure that it recovers before the expiry of E_D_TOV. LRTP is not required if the FCP-2 sequence level error-recovery procedures are enabled end-to-end (primarily in the tape drivers) because this helps to recover from timeout issues.When the FCP-2 sequence level error-recovery procedure is not enabled, you must tune certain timers in order to protect the site from ISL failures.
  - – Reduce the LRTP retransmit value from the default value of 2.5 seconds to 1.5 seconds. For more information, see the .
  - – If the ISLs are FCIP links, the FCIP links must be tuned in order to detect link flaps quickly. By default, FCIP links detect a link failure in 6 seconds based on TCP maximum retransmissions. To reduce the time taken to detect failures, you need to set the maximum retransmission attempts in the FCIP profile from the default value of 4 to 1.

⚠️

Caution   Modifying the default setting to a lower value results in quick link failure detections. You must make sure that this is appropriate for your deployment. We recommend that you modify the default setting only for those applications which are sensitive to E_D_TOV values. For other applications, the default configuration is sufficient.

Limitations and Restrictions

When you configure IOA, consider the following limitations:

- • Only 512 flows are supported when IOA and IVR co-exists.
- • You can provision only one intelligent application on a single service engine. In SSN-16 there are 4 service engines and each service engine can host a single intelligent application.
- • In Cisco NX-OS Release 4.2(1), only IOA and FCIP can run on the same SSN-16 as in the following example:
  - – If one of the service engines runs SME on an SSN-16, you cannot configure another application to run the remaining service engines on this SSN-16.

- – If one of the service engines runs IOA or FCIP, you can configure other service engines to run either FCIP or IOA.

- IOA uses the image that is bundled as a part of the Cisco MDS NX-OS Release. In Cisco MDS NX-OS Release 4.2(1), SSI images are not supported for IOA.

- IOA decides the master based on a master election algorithm. If you have multiple switches in the IOA cluster, you must add all the switches in the site that you manage from into the cluster before adding switches from the remote site. For more information see Appendix B, "Cluster Management and Recovery Scenarios."

- IOA clustering framework uses IP connectivity for its internal operation. In Cisco NX-OS Release 4.2(1) and later releases, if an IOA cluster becomes nonoperational due to IP connectivity, IOA flows are brought down to offline state. In this state, the hosts may not be able to see the targets. To accelerate the IOA flows, the IOA cluster must be operational and there must be at least one IOA switch in each site that is online within this IOA cluster.

- The targets must be connected to a FC-Redirect-capable switch running Cisco MDS NX-OS Release 4.2(1) or later. The hosts must be connected to a FC-Redirect-capable switch running Cisco MDS SAN-OS Release 3.3(1c) or later.

- In Cisco MDS NX-OS Release 4.2(1), the following features cannot coexist with IOA for a specific flow: SME, DMM, IVR, NPV and NPIV, F PortChannel or Trunk. In Cisco NX-OS Release 5.0(1), IVR is supported with IOA.

- To implement IOA on IVR flows, the host switches, target switches, border switches, and the IOA switches must all be running AAM-supported Cisco MDS NX-OS Release 5.0(1) or later. For more information, refer to the *Cisco MDS 9000 Family NX-OS Inter-VSAN Routing Configuration Guide*.

- If there are multiple Cisco IOA clusters in a region, a target can be part of the IOA configuration in only one cluster. To change the target to a different cluster, the configuration in the first cluster must be deleted before creating the configuration in the second cluster.

- IOA licenses are not tied to a specific IOA service engine. IOA licenses are checked out when any of the following event occurs:

  - – An IOA interface is configured.

  - – A line card that contains the IOA interface comes online. There are no links between an IOA license and a IOA service engine. If a line card goes offline, another IOA interface can be brought up using the same IOA license. In such cases, when the line card comes back online, the IOA interface is automatically brought down with status displaying No License. You need to install licenses corresponding to the number of IOA interfaces configured regardless of the status of the line card.

- If IOA flows are configured and a copy running to startup is not performed, FCR rules are removed automatically for these flows in all VSANs except VSAN 1. VSAN 1 is a default VSAN that is always persistent even without a copy running to startup and so, FCR rules are preserved for this VSAN. To recover from this, you can execute "clear fc-redirect decommision-switch" prior to the reboot of the switch to purge the FCR configs in VSAN 1. Alternately, you can cleanup the entire IOA flow configuration prior to the reboot of the switch.

- If an MDS switch is connected through an ISL using a twinpeak line card and the targets are connected to the MDS switch, then this MDS switch can connect to a maximum of 160 targets. This because the maximum number of ELS entries on the twinpeak line card is 320 entries. For example, in an IOA configuration that has 5 flows (1 host : 1 target) you can have 10 ELS entries on a module with ISL and in a IOA configuration that has 10 flows (2 hosts : 1 target), you can have only 10 ELS entries. This because ELS entries depends on the number of targets.

  The workaround for such a case would be to implement allowed VSAN on ISL. For example, if

ISL-1 is connected to module 9 and is limited to VSAN 2000, then all the ELS entries specific to VSAN 2000 will be on module 9. If ISL-2 is connected to module 2 and is limited to VSAN-3000, then all the ELS entries specific to targets of VSAN-3000 will be on module 2.

- IOA flow takes a few seconds to become active upon certain triggers such as host or target port flaps. PLOGI from the hosts are buffered until the IOA flow becomes active. Once the IOA flow becomes active, it sends a RSCN to request the host to PLOGI again. Certain target arrays perform a few back-to-back PLOGIs prior to the flow becoming active and upon seeing a failure requires a manual corrective action. To prevent this, IOA flows that have been configured for Write-Acceleration are set up with a default timeout of 10 seconds after which the flow becomes unaccelerated. This is useful specifically in cases where IOA is unable to take over the flow prior to the timeout. For example, linecard reloads where no other IOA interface is available to handle the flow. In certain target arrays, the 10 second timeout is not sufficient and these arrays may require manual recovery using the storage management interfaces. One example of such a target array is HDS AMS.

  The workaround for such a case would be to set the timeout to 5 seconds using the CLI command "tune wa-fcr-rule-timeout 5" under the ioa cluster configuration sub-mode. This configuration is cluster-wide persistent across reboots.

- When IOA is used to accelerate EMC SRDF family of products, switching between SRDF adaptive Copy and SRDF/A can cause your RDF pairs to go into TransIdle state. If your SRDF deployment requires switching between these 2 modes, we recommend using FCIP Write Acceleration instead of IOA"

Configuration Limits

Table 3-1 lists the IOA configurations and the corresponding limits.

Table 3-1   Cisco I/O Accelerator Configuration Limits

Configuration	Limit
Number of switches in a cluster	4
Number of Switches in the SAN for FC-Redirect	34
Number of IOA interfaces in a switch	44
Number of IOA interfaces in a cluster	44
Number of hosts per target	128
Number of flows in a cluster	1024
Number of flows across all clusters	1024
Number of flows per IOA service engine (hard limit)	128
Number of flows per IOA service engine (soft limit)	64

Note   When the new flows are load balanced again to the functional IOA interface, the soft limit is enforced to account for IOA interface failures. If the number of switches in the SAN exceeds the scalability limit, consider using CFS regions as described in "Using FC-Redirect with CFS Regions" section on page 2-4.