Fabric Best Practices

This IBM® Redpaper™ publication describes preferred practices for deploying and using advanced Brocade Fabric Operating System (FOS) features to identify, monitor, and protect Fibre Channel (FC) SANs from problematic devices and media behavior.

**FOS:** This paper focuses on the FOS command options and features that are available in versions 7.4.2 and 8.1.
Introduction

Faulty or improperly configured devices, misbehaving hosts, and faulty or substandard FC media can significantly impact the performance of FC fabrics and the applications that they support. In most real-world scenarios, these issues cannot be corrected or completely mitigated within the fabric itself. Rather, the behavior must be addressed directly.

However, with the proper knowledge and capabilities, the fabric can often identify and, in some cases, mitigate or protect against the effects of these misbehaving components to provide better fabric resiliency. This document concentrates specifically on Brocade Fabric Vision features (and related capabilities) that help provide optimum fabric resiliency.

For more information about the features that are described in this publication, see the product documents that are appropriate for your FOS release. They are available to registered users at: http://my.brocade.com. Brocade documentation can also be found by searching the Brocade web site:

- SAN Design and Best Practices
- Fabric OS Administrator's Guide
- Fabric OS Monitoring and Alerting Policy Suites Configuration Guide
- Fabric OS Flow Vision Configuration Guide
- Brocade Network Advisor Administrator's Guide

Factors affecting fabric resiliency

There are several common types of abnormal behavior originating from fabric components or attached devices:

- Faulty media (fiber-optic cables and Small Form-factor Pluggables (SFPs)/optics): Faulty media can cause frame loss due to excessive cyclic redundancy check (CRC) errors, Forward Error Correction (FEC) errors, invalid transmission words, and other conditions, which can result in I/O failure and application performance degradation.

- Misbehaving devices, links, or switches: Occasionally, a condition arises where a device (server or storage array) or link (inter-switch link (ISL)) behaves erratically and causes disruptions in the fabric. If not immediately addressed, this situation might result in severe stress on the fabric.

- Congestion: Congestion is caused by latencies or insufficient link bandwidth. End devices that do not respond as quickly as expected can cause the fabric to hold frames for excessive periods, which can result in application performance degradation or, in extreme cases, I/O failure.

- Credit loss: Credit loss happens when the receiving end of a link fails to acknowledge a request to transmit a frame because no buffers are available to receive the frame.

Faulty media

In addition to high-latency devices causing disruptions to data centers, fabric problems are often the result of faulty media. Faulty media can include bad cables, SFPs, extension equipment, receptacles, patch panels, improper connections, and so on. Media can fault on any SAN port type and fail, often unpredictably and intermittently, making it even harder to diagnose. Faulty media involving server/host and storage device ports (F_Ports) results in an impact to the end device attached to the F_Port, and to devices communicating with this device.
Failures on ISLs or E_Ports can have an even greater impact. Many flows (host and target pairs) can simultaneously traverse a single E_Port. In large fabrics, this can be hundreds or thousands of flows. If there is a media failure involving one of these links, it is possible to disrupt some or all of the flows that use the path. Severe cases of faulty media, such as a disconnected cable, can result in a complete failure of the media, which effectively brings a port offline.

This situation is typically easy to detect and identify. When it occurs on an F_Port, the impact is specific to flows involving the F_Port. E_Ports are typically redundant, so severe failures on E_Ports typically only result in a minor drop in bandwidth because the fabric automatically uses redundant paths. Also, error reporting that is built into FOS readily identifies the failed link and port, allowing for simple corrective action and repair. With moderate cases of faulty media, failures occur, but the port can remain online or transition between online and offline. This situation can cause repeated errors, which can occur indefinitely or until the media fails. When these types of failures occur on E_Ports, the result can be devastating because there can be repeated errors that impact many flows, which can result in significant impacts to applications that last for prolonged durations.

Signatures of these types of failures include:

- CRC errors on frames
- Invalid Transmission Words (includes encoder out errors)
- State Changes (ports going offline or online repeatedly)
- Credit loss (complete loss of credit on a virtual channel (VC) on an E_Port prevents traffic from flowing on that VC, resulting in frame loss and I/O failures for devices that use the VC)

**Misbehaving devices**

Another common class of abnormal behavior originates from high-latency end devices (host or storage). A high-latency end device is one that does not respond as quickly as expected, and therefore causes the fabric to hold frames for excessive periods. This situation can result in application performance degradation or, in extreme cases, I/O failure. Common examples of moderate device latency include disk arrays that are overloaded and hosts that cannot process data as fast as requested.

Misbehaving hosts, for example, become more common as hardware ages. Bad host behavior is usually caused by defective host bus adapter (HBA) hardware, bugs in the HBA firmware, and problems with HBA drivers. Storage ports can produce the same symptoms due to defective interface hardware or firmware issues. Some arrays deliberately reset their fabric ports if they are not receiving host responses within their specified timeout periods.

Severe latencies are caused by badly misbehaving devices that stop receiving, accepting, or acknowledging frames for excessive periods. However, with the proper knowledge and capabilities, the fabric can often identify and, in some cases, mitigate or protect against the effects of these misbehaving components to provide better fabric resiliency.

**Congestion**

Congestion occurs when the traffic being carried on a link exceeds its capacity. Sources of congestion can be links, hosts, or storage responding more slowly than expected. Congestion is typically due to either fabric latencies or insufficient link bandwidth capacity.
As FC link bandwidth has increased from 1 to 16 Gbps, instances of insufficient link bandwidth capacities have radically decreased. Latencies, particularly device latencies, are the major source of congestion in today’s fabrics due to their inability to promptly return buffer credits to the switch.

**Device-based latencies**

A device experiencing latency responds more slowly than expected. The device does not return buffer credits (through `R_RDY` primitives) to the transmitting switch fast enough to support the offered load, even though the offered load is less than the maximum physical capacity of the link that is connected to the device.

Figure 1 illustrates the condition where a buffer backup on ingress port 6 on B1 causes congestion upstream on S1, port 3. When all available credits are exhausted, the switch port that is connected to the device must hold additional outbound frames until a buffer credit is returned by the device.

![Figure 1  Device latency example](image)

When a device does not respond in a timely fashion, the transmitting switch is forced to hold frames for longer periods, resulting in high buffer occupancy, which results in the switch lowering the rate at which it returns buffer credits to other transmitting switches. This effect propagates through switches (and potentially multiple switches, when devices attempt to send frames to devices that are attached to the switch with the high-latency device), and ultimately affects the fabric.

Figure 2 shows how latency on a switch can propagate through the fabric.

![Figure 2  Latency on a switch can propagate through the fabric](image)
**Note:** The impact to the fabric (and other traffic flows) varies based on the severity of the latency that is exhibited by the device. The longer the delay that is caused by the device in returning credits to the switch, the more severe the problem.

**Moderate device latencies**

Moderate device latencies from the fabric perspective are defined as those not severe enough to cause frame loss. If the time between successive credit returns by the device is between a few hundred microseconds to tens of milliseconds, the device exhibits mild to moderate latencies because this delay is typically not enough to cause frame loss. This situation does cause a drop in application performance but typically does not cause frame drops or I/O failures.

The effect of moderate device latencies on host applications might still be profound, based on the average disk service times that are expected by the application. Mission-critical applications that expect average disk service times of, for example, 10 ms, are severely affected by storage latencies in excess of the expected service times. Moderate device latencies have traditionally been difficult to detect in the fabric.

Advanced monitoring capabilities that are implemented in Brocade ASICs and FOS have made these moderate device latencies much easier to detect by providing the following information and alerts:

- Switches in the fabric generate Fabric Performance Impact (FPI) alerts if FPI is enabled on the affected ports
- Elevated `tim_txcrd_z` counts on the affected F_Port, so the F_Port where the affected device is connected
- Potentially elevated `tim_txcrd_z` counts on all E_Ports carrying the flows to and from the affected F_Port/device

**Note:** `tim_txcrd_z` is defined as the number of times that the port was polled and that the port was unable to transmit frames because the transmit buffer-to-buffer credit (BBC) was zero (0). The purpose of this statistic is to detect congestion or a device that is affected by latency. This parameter is sampled at intervals of 2.5 microseconds, and the counter is incremented if the condition is true.

Each sample represents 2.5 microseconds of time with zero Tx BBC. `tim_txcrd_z` counts are not an absolute indication of significant congestion or latencies and are just one of the factors in determining whether real latencies or fabric congestion are present. Some level of congestion is to be expected in a large production fabric, and is reflected in `tx_crd_z` counts. The Brocade FPI feature was introduced to remove uncertainty around identifying congestion in a fabric.

**Note:** `tim_latency_vc` is a Brocade Gen5 Condor3 ASIC counter that measures the latency time that a frame incurs in the transmit queue of its corresponding VC. The purpose of this statistic is to directly measure the frame transmit latency of a switch port. Each unit of the counter value represents 250 nanoseconds of latency. The Brocade FPI feature uses this counter to enhance the detection of devices introducing latency into the fabric.
Severe device latencies
Severe device latencies result in frame loss, which triggers the host Small Computer System Interface (SCSI) stack to detect failures and to retry I/Os. This process can take tens of seconds (possibly as long as 30 - 60 seconds), which can cause a noticeable application delay and potentially results in application errors. If the time between successive credit returns by the device is in excess of 100 ms, the device is exhibiting severe latency.

When a device exhibits severe latency, the switch is forced to hold frames for excessively long periods (on the order of hundreds of milliseconds). When this time becomes greater than the established timeout threshold, the switch drops the frame (per FC standards). Frame loss in switches is also known as Fibre Channel Class 3 (C3®) discards or timeouts.

Because the effect of device latencies often spreads through the fabric, frames can be dropped due to timeouts, not just on the F_Port to which the misbehaving device is connected, but also on E_Ports carrying traffic to the F_Port. Dropped frames typically cause I/O errors that result in a host retry, which can result in significant decreases in application performance.

The implications of this behavior are compounded and exacerbated by the fact that frame drops on the affected F_Port (device) result not only in I/O failures to the misbehaving device (which are expected), but also on E_Ports, which might cause I/O failures for unrelated traffic flows involving other hosts (and typically are not expected).

Latencies on ISLs
Latencies on ISLs are usually the result of back pressure from latencies elsewhere in the fabric. The cumulative effect of many individual device latencies can result in slowing the link. The link itself might be producing latencies, if it is a long-distance link with distance delays or there are too many flows that use the same ISL.

Although each device might not appear to be a problem, the presence of too many flows with some level of latency across a single ISL or trunked ISL can become a problem. Latency on an ISL can ripple through other switches in the fabric and affect unrelated flows.

FOS can provide alerts and information indicating possible ISL latencies in the fabric, through one or more of the following items:
- Switches in the fabric generate FPI Alerts if FPI is enabled on the affected ports
- C3 transmit discards (er_tx_c3_timeout) on the device E_Port or EX_Port carrying the flows to and from the affected F_Port or device
- Brocade MAPS alerts, if they are configured for C3 timeouts
- Elevated tim_txcrd_z counts on the affected E_Port, which also might indicate congestion
- C3 receives discards (er_rx_c3_timeout) on E_Ports in the fabric containing flows of a high-latency F_Port

Credit loss
Buffer credits are a part of the FC flow control and the mechanism that Fibre Channel connections use to track the number of frames that are sent to the receiving port. Every time a frame is sent, the credit count is reduced by one. When the sending port runs out of credits, it is not allowed to send any more frames to the receiving port. When the receiving port successfully receives a frame, it tells the sending port that it has the frame by returning an r_rdy primitive.

When the sending port receives an r_rdy, it increments the credit count. Credit loss occurs when either the receiving port does not recognize a frame (usually due to bit errors), so it
does not return an r_rdy, or the sending port does not recognize the r_rdy (usually due to link synchronization issues).

FC links are never perfect, so the occasional credit loss can occur, but it becomes an issue only when all available credits are lost. Credit loss can occur on both external and internal FC links. When credit loss occurs on external links, it is usually caused by faulty media, and credit lost on internal ports is usually associated with jitter, which in most cases is adjusted for by the internal adapter firmware.

The switch automatically tries to recover from a complete loss of credit on external links after 2 seconds by issuing a link reset. For the switch to perform automatic recovery from internal link credit loss, the Credit Loss Detection and Recovery feature must be enabled.

**High-performance networks**

With the use of low-latency SDD and Flash controllers the performance of the SAN becomes critical to achieving the full performance potential from those technologies. Eliminating latency from the SAN requires a level of planning and consideration that’s often above what’s necessary for traditional enterprise class storage, given the nominal operating ranges of those devices.

Poorly constructed and maintained SANs can add latency to the SCSI exchange completion times to varying degrees. This additional latency can often go undetected, or be considered insignificant for “spinning disk” subsystems, because it is often a small percentage of the response time those devices are capable of achieving. This response time can be in the 10’s to 100’s of milliseconds. This is not true of SDD/Flash storage, where the latency contribution from sub-optimal SAN conditions can easily equal or exceed the capable response time for those technologies.

The Fabric Resiliency Best Practices described in this paper are especially critical because they pertain to maintaining a high-performance SAN. However, in addition to those practices, there are SAN design considerations that also need to be made about the use of mixed-speed devices and ISLs.

**Mixed-speed SANs**

It is generally required for multiple device speeds to exist in the SAN in order to enable the technology to be refreshed from one generation to the next. For that reason, the existence of mixed-speed devices cannot be avoided. However, mixed-speed devices spanning more than one generation of technology should be avoided.

For example, mixing 4-Gb and 8-Gb devices is generally acceptable; however, mixing 4-Gb and 16-Gb is not. The speed matching required to accommodate these large speed differentials introduces latency and potential congestion points that can significantly degrade the performance and stability of SAN.

**ISLs and multi-hop ISLs**

Many flows between servers and storage, or storage-to-storage devices, need to flow across the ISLs and, because of this, ISLs are notorious for introducing latency into the transmission flows. The size and, more importantly, the number of ISLs required between switches now needs to consider response time requirements and bandwidth requirements.

With storage devices getting into the sub-millisecond response times, ISLs need to ensure that credits are available all the time so that frames do not get delayed. This may require multiple ISL trunks instead of fewer larger bandwidth trunks.
If frames need to traverse multiple switches to reach their destination, delays can be introduced with each hop required between the source and destination switches. Multi-hop ISLs should never be used, with the exception of being used for migration purposes on a temporary basis.

Where strict performance requirements exist, the use of ISLs for access to SDD/Flash should be avoided altogether.

**Note:** Avoid introducing devices to the SAN that span more than one generation of technology.

**Note:** Avoid traversing ISLs when accessing SDD/Flash for high performance use cases.

---

**Designing resiliency into the fabric**

This document is not intended to cover the general set of design considerations that are required for designing a Storage Area Network (SAN), but there are a set of technologies that should be considered to ensure that the fabric is resilient by design. This section includes preferred practices for each of the following areas:

- Inter-switch link trunking
- Routing policies
- Credit recovery tools
- Meaningful naming convention
- Dynamic port naming
- Fabric Performance Impact

For more information, see “Preferred implementation open systems” on page 37.

General topics that are related to the architecture, topology, and capacity planning for a SAN are described in *SAN Design and Best Practices*:

http://my.brocade.com

**Inter-switch link trunking**

Trunking optimizes the use of bandwidth by allowing a group of ISLs to merge into a single logical link, which is called a *trunk group*. Traffic is distributed evenly and in order over this trunk group, achieving greater performance with fewer links. Within the trunk group, multiple physical ports appear as a single port, thus simplifying management.

Trunking improves system reliability by maintaining in-order delivery of data and avoiding I/O retries if one link within the trunk group fails.

Trunking provides excellent protection from credit lost on ISLs. If credit loss occurs on an ISL, frames continue to flow by using the other link until the switch can detect the credit loss (typically 2 seconds) and perform a link reset to recover the credits.

More IT environments are relying on server virtualization technologies that can share host adapter connections. Specifically, N_Port ID Virtualization (NPIV) allows many clients (servers, guest, or hosts) to use a single physical port on the SAN.

Each of these communications paths from server, virtual or otherwise, is a data flow that must be considered when planning for how many interswitch links are needed. These virtualized environments often lead to a situation where there are many data flows from the
edge switches potentially leading to frame-based congestion if there are not enough ISL or trunk resources.

To avoid frame-based congestion in environments where there are many data flows between switches, it is better to create several two-link trunks than one large trunk with multiple links. For example, it is better to have two 2-link trunk groups than one 4-link trunk group.

Routing policies

The routing policy determines the route or path frames take when traversing the fabric. There are three routing policies available:

- The default exchange-based routing (EBR)
- Port-based routing (PBR)
- Device-based routing (DBR)

Open systems FCP fabrics

EBR is always the preferred routing policy for FCP fabrics.

FICON fabrics

Before 2013, cascaded IBM FICON® configurations supported only static PBR across ISLs. In this case, the ISL (route) for a given port was assigned statically based on a round-robin algorithm at fabric login (FLOGI) time. PBR can result in some ISLs being overloaded.

In mid-2013, IBM z® Systems® added support for DBR, which spread the routes across ISLs based on a device ID hash value. With the IBM z13® release in mid-2015, IBM added FICON Dynamic Routing (FIDR), which supports Brocade EBR to improve load balancing for cascaded FICON across ISLs.

The prerequisite z13 driver levels, adapter features, storage, and FOS levels to support FIDR are included in the following white paper:


FICON cascaded configurations with z13 and all other appropriate prerequisites should use EBR. All other FICON cascaded configurations should use DBR.

For more information about the FICON Dynamic Routing feature, see Get More Out of Your IT Infrastructure with IBM z13 I/O Enhancements, REDP-5134:


Note: For FICON it should be EBR (if IBM z/OS® and z System supports FIDR) regardless if it is a FICON/FCP intermix or not. If z System does not support FIDR then it must be DBR.

Credit recovery tools

FC traffic uses credit-based flow control where each side of a given connection provides a number of buffers. These buffers are advertised to the partner side of a connection as credits, indicating how many frames can be outstanding.
Credits are replenished when transmissions are successful and acknowledged. In rare error scenario situations, credit-based flow control acknowledgements are either not sent or not received, leading to a credit loss condition. If the problem causing this failure is persistent, credit loss can result in a stall of traffic.

FC credit-based recovery applies to external switch ports and back-end ports (ports that are connected to the core blade or core blade back-end ports) that are used for traffic within a switch. Traffic stalls on these internal back-end ports can have a wide impact, particularly when they impact virtual circuits of an ISL. Brocade introduced enhanced credit recovery tools to mitigate this type of problem. These tools can be enabled to automatically reset back-end ports when a loss of credits is detected on internal ports.

As a preferred practice, enable the credit recovery tools.

There are two main choices for how the recovery can proceed when enabled:

- An escalating recovery based on the results of a single link reset only (onLrOnly)
- A threshold-based approach that uses multiple link resets (onLrThresh).

When used with the onLrOnly option, the recovery mechanism takes the following escalating actions:

- When it detects credit loss, it performs a link reset and logs a RASlog message (RAS Cx-1014).
- If the link reset fails to recover the port, the port reinitializes. A RASlog message is generated (RAS Cx-1015). The port reinitialization does not fault the blade.
- If the port fails to reinitialize, the port is faulted. A RASlog message (RAS Cx-1016) is generated.
- If a port is faulted and there are no more online back-end ports in the trunk, the core blade is faulted. (The port blade is always faulted.) A RASlog message is generated (RAS Cx-1017).

When used with the onLrThresh option, recovery is attempted through repeated link resets and a count of the link resets is kept. If the threshold of more than the configured threshold value (by using the -lrthreshold option) per hour is reached, the blade is faulted (RAS Cx-1018). Regardless of whether the link reset occurs on the port blade or on the core blade, the port blade is always faulted.

As a preferred practice, enable the credit tools with the onLrOnly recovery option.

**Meaningful naming convention**

The use of a strict and well-thought-out naming convention is critical to the reliable operation and serviceability of the environment.

*Note:* Implementing and maintaining a meaningful naming convention is an important disaster prevention option available that requires no software to control. It provides administrators the ability to visually determine the site and detail of the device.

The naming convention can vary depending on the needs and architecture. The naming convention should be designed in a user-friendly fashion, consistent and documented.

User-friendly alias names ensure that zone members can be understood at a glance, and configuration errors can be minimized.
User-friendly Switch names ensure that there is no possible confusion when connecting and configuring the switch.

The naming convention can contain the following information:
Location_FabricName_DeviceGroup_DeviceName_Port/Domain

- Location can contain DR to qualify a Disaster Recovery site, the room name and the rack name.
- Fabric name should contain the name of that fabric.
- Device Group can mention the type of application or service, and identify the device as test or production.
- Device name is the name of the device.
- Port/Doman is the description of the port or the Domain ID of the switch.

Example 1 shows an example alias for different devices.

**Example 1  Alias for a storage device**

**Alias Example for SVC device:**
NY_Green_SAPProd_DS5020-1_C1P2

- NY: New York
- Green: the name of the fabric
- SAPProd: This is an SAP production instance
- DS5020-1: This is a DS5020 number 1
- C1P2: The card and the port

**Alias Example for SVC device:**
NY_Green_SAPProd_SVC1_I0GRO_01
DR_Blue_SAP2_SVC_NIS3_2

**Alias for a server:**
NY_Green_backup_TSM02_fc3
NY_Blue_SAPProd_ESX11_hba1

**Naming convention for a Switch:**
NY_Green_Prod_DCX11_030
NY_Green_Test_DCX12_031

**Alias for a zone (differs a bit from the other scheme because this can contain the name of multiple devices, or groups of devices, that are included in the same zone):**
NY_Green_SAPProd_ESX11_FC1-TAPE33_Zone

**Alias for a config:**
A good practice is to name the config with the name of the fabric, and the version and date it was activated:
NY_Green_v3.7_20180801_config

Zone config versioning can help for fallback scenario and troubleshooting purposes.

Adding the word zone or alias is also useful to avoid confusion, especially when configuring zones using the CLI.

As a preferred practice, use aliases and make all of the names meaningful.
Dynamic port naming

Every port on a Brocade FC switch has a port name that by default is slot number port number. The port name is displayed in many of the switch event messages, MAPS alert, and Network Advisor dashboards.

Using a more meaningful port name makes these messages and dashboards more meaningful, and makes identifying external devices that are causing fabric problems easier and quicker to identify.

The problem is that manually setting port names to more meaningful names is labor-intensive, and typically done only with scripts to set the port name to the alias name of the attached device.

With FOS V7.4, Brocade introduced dynamic port names that dynamically set the port name to `<switch name>.<port type>.<port index>.<alias name>`. Dynamic port name is enabled by using the `configure` command and setting the dynamic port name to `on`.

In FOS V8 and higher, enhancements were made to allow configuring the dynamic port name by using any of the following fields:

- Switch Name
- Port Type
- Port Index
- F_Port Alias
- FDMI Host name
- Remote Switch Name
- Slot/Port Number

Example 2 shows examples of both dynamically and manually set port names.

**Example 2  Examples of dynamically and manually set port names**

<table>
<thead>
<tr>
<th>Index</th>
<th>Port</th>
<th>PortWWN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>103</td>
<td>2</td>
<td>20:67:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.E_PORT.103</td>
</tr>
<tr>
<td>133</td>
<td>7</td>
<td>20:85:00:05:1e:d0:b5:05</td>
<td>CLSS14_HBA3</td>
</tr>
<tr>
<td>134</td>
<td>7</td>
<td>20:86:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.F_PORT.134.(null)</td>
</tr>
<tr>
<td>135</td>
<td>7</td>
<td>20:87:00:05:1e:d0:b5:05</td>
<td>DS5300_B2</td>
</tr>
<tr>
<td>134</td>
<td>7</td>
<td>20:86:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.F_PORT.134.(null)</td>
</tr>
<tr>
<td>145</td>
<td>7</td>
<td>20:91:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.F_PORT.145.XIV3_M5P</td>
</tr>
<tr>
<td>147</td>
<td>7</td>
<td>20:93:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.F_PORT.147.DS4800_B2</td>
</tr>
<tr>
<td>192</td>
<td>8</td>
<td>20:c0:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.(none).192</td>
</tr>
<tr>
<td>208</td>
<td>8</td>
<td>20:d0:00:05:1e:d0:b5:05</td>
<td>SANC_DCX1.F_PORT.208.(null)</td>
</tr>
</tbody>
</table>

Example 3 shows an example to set and display the dynamic port name.

**Example 3  Setting and displaying the dynamic port name**

```
Brocade_def:FID128:admin > portname -d "S.T.I.F.A.R"
Brocade_def:FID128:admin > switchshow -portname
```

<table>
<thead>
<tr>
<th>Index</th>
<th>Port</th>
<th>PortWWN</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>8</td>
<td>20:08:00:05:33:a5:cf:20</td>
<td>ISL_F48_01_20_F48_02_20_16G</td>
</tr>
<tr>
<td>9</td>
<td>9</td>
<td>20:09:00:05:33:a5:cf:20</td>
<td>ISL_F48_01_20_F48_02_20_8G</td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>20:a8:00:05:33:a5:cf:20</td>
<td>MarleneHBA2p0_F</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>20:0b:00:05:33:a5:cf:20</td>
<td>MariaF_default</td>
</tr>
<tr>
<td>12</td>
<td>12</td>
<td>20:0c:00:05:33:a5:cf:20</td>
<td>-</td>
</tr>
</tbody>
</table>
Another advantage of using consistent manual or automatic port naming is to be able to create MAPS Port group based on port name.

The following command is an example:

```
logicalgroup --create group_name -type type -feature feature_type -pattern pattern
```

For `feature_type`, either port names or WWNs can be used, not both. Quotation marks around the pattern value are required. If “!” is specified in the pattern it must be within single quotation marks (‘!’). You can only specify one feature as part of a group definition.

Example 4 creates a group named `GroupWith_ISL_F48` that has a membership defined as ports connected to a device with a node WWN that starts with `30:08:00:05`.

Example 4 - Creating the group

```
switch:admin> logicalgroup --create GroupWith_ISL_F48 -type port -feature portname -pattern "ISL_F48*"
```

```
PFE_F48_01def:FID128:admin> logicalgroup --show
```

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Predefined</th>
<th>Type</th>
<th>Member Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupWith_ISL_F48</td>
<td>No</td>
<td>Port</td>
<td>0</td>
</tr>
</tbody>
</table>

Note that the following operators are available:

* Match any set of characters in the position indicated by the asterisk.

? Match any single character in the position indicated by the question mark.

[expression] Match any character defined by the expression inside the square brackets.

! Match the string following and exclude any ports that match.
Fabric Performance Impact

Fabric Performance Impact (FPI) monitors congestion related issues on all physical E_Ports and F_Ports at all times. FPI added automatic mitigation capabilities through Slow Drain Device Quarantine (SDDQ) and Port Toggle actions.

FPI detects different severity levels of latency and reports three latency states:

- The IO_FRAME_LOSS state is a severe level of latency. In this state, frame timeouts either have occurred or are likely to occur. Administrators should take immediate action to prevent application interruption.
- The IO_PERF_IMPACT state is a moderate level of latency. In this state, device-based latencies can negatively impact the overall network performance.
- The IO_LATENCY_CLEAR alert occurs when the latency conditions clear.

Administrators should act to mitigate the effect of latency devices. The separate states enable administrators to apply different MAPS actions for different severity levels.

FOS V8.0.1 enhances FPI monitoring to include the FPI monitoring rules and thresholds in the MAPS default base policy. Switches running FOS V8.0.1 without a Fabric Vision license are monitored by MAPS for congestion and slow drain device conditions.

Preferred settings

The following settings are preferred:

- Enable FPI and setup MAPS actions.
- On switches with FOS V7.4, enable FPI.
- On switches with FOS V8.1 and higher, set up MAPS to quarantine the port for IO_FRAME_LOSS events by using the SDDQ option (see SDDQ here and in “Enabling Monitoring Alerting Policy Suite” on page 50).

Note: To use SDDQ, quality of service (QoS) must be enabled on all switches, which is the factory default.

Maintaining an optimal FC SAN environment

In each subsequent release of FOS, Brocade has added and enhanced features to assist with monitoring, protecting, and troubleshooting fabrics. The majority of the features has been available since FOS V7.2. Starting in FOS V7.2, this set of features is referred to as Fabric Vision. When implemented and administered properly, these features can dramatically improve the reliability and resiliency of the fabric.

This section focuses on the Fabric Vision features that are available in FOS versions 7.2 to 7.4, and specifically on the following subset of features that apply to monitoring and alerting:

- Bottleneck Detection
- Fabric Performance Impact (FPI)
Slow-Drain Device Quarantine and Port Toggling

In a fabric, many flows share the same link or virtual channel (VC). However, the credits used to send traffic or packets across the link are common to all of the flows using the same link. Therefore, a slow-draining device can slow down the return of credits and have a negative effect on the healthy flows through the link.

To remedy this, two actions were introduced:

- **Port Toggling**, which takes a port offline for a specified period of time and then brings it back online. The intent is that cycling the port resets the attached device and enables the switch and device to start from a clean initialization point.

- **Slow-Drain Device Quarantine (SDDQ)**, which uses the Quality of Service (QoS) facility. SDDQ enables MAPS to identify a slow-draining device with FPI events and quarantine it by automatically moving all traffic destined to the F_Port that is connected to the slow-draining device to a low-priority VC so that the traffic in the original VC does not experience back-pressure.

When a device is marked as being slow-draining, only the flows destined to it are shifted to the low-priority Virtual Circuit (VC). Flows in the reverse direction are not affected.

SDDQ action is blocked when at least one of the following reasons apply:

- The total number of ports in a zone is >32.
- Defzone is labeled as *all access*, and there is no user-defined zoning configuration.

FOS V8.1.0 introduces an un-quarantine action (UNQUAR) for Gen6 switches. The un-quarantine action moves a previously quarantined slow drain device out of the quarantine automatically, if the slow drain behavior has cleared for a defined timeout period. An un-quarantine action can be applied with the IO_LATENCY_CLEAR state monitoring. Users can configure an un-quarantine timeout value along with the un-quarantine action.

FOS V8.1.0 includes the UNQUAR action of the default FPI rules in the predefined conservative policy and moderate policy. A use case for the usage of the un-quarantine action is when a path is needed for different traffic during the day and night, where night traffic needs to be quarantined and day traffic needs to use the high priority virtual channel.

The maximum number of devices that can be isolated per unit (chassis or fixed-port switch) is 32. The default value is 10.

**SDDQ and FICON**

In most cases, you should not enable the Slow-Drain Device Quarantining (SDDQ) feature in a FICON environment. The way FICON operates does not benefit from the usage of SDDQ.

When SDDQ is enabled, all traffic to a slow-draining device is moved to the lowest-priority virtual circuit. In a single-zone environment, this impacts all traffic in the zone.

**Slow-Drain Device Quarantining on long-distance links**

SDDQ is supported on long-distance links. In long-distance mode, the QoS virtual-channel (VC) priority is still maintained. However, you need to explicitly enable QoS again, because enabling a long-distance mode, by default, disables QoS mode.
After you explicitly enable QoS mode again, you must disable and enable the port to bring up the link in the long-distance and QoS modes. The usage of MAPS rule enables delaying the quarantining of the port until after a specified number of rule violations, and is automatically unquarantined one hour after device latency clear.

The port toggling (PT) action and the SDDQ action are mutually exclusive. When using the mapsconfig command, you cannot enable the SDDQ and PT actions at the same time.

**Preferred Settings**

Enable SDDQ for IO_FRAME_LOSS events on FOS V8.1 and later with the un-quarantine option.

**Port Fencing**

The Brocade MAPS Port Fencing action provides the ability to protect against faulty components and conditions that impact links by automatically blocking ports when predefined thresholds are reached.

Enabling MAPS rules with the Port Fencing option should be used with care so that fencing ports happens only on ports that have severe issues. As a preferred practice, only MAPS rules for host ports for the CRC and Link Reset thresholds should be enabled for port fencing.

Before enabling MAPS policy, it is advised to disable fencing for the MAPS policy action. This will globally disable fencing even if a specific rule of a policy is configured with a fencing action. Disabling fencing allows you to monitor the behavior of the policy without any risk to unnecessarily fence a port and create an unexpected impact during normal operations.

When the behavior of the MAPS policy is considered good, the fence MAPS policy action can be enabled.

**Configuring Port Fencing**

Complete the following steps:

1. From the MAPS configuration, click Monitor → Fabric Vision → MAPS → Configure, select the MAPS policy to modify, and click Edit.
2. Select the rule to modify and click the left arrow, or create a rule and select the Fence check box to enable the port fencing action.
3. Click the right arrow to transfer the rule to the selected policy.
Figure 3 shows the editing of a MAPS rule.

<table>
<thead>
<tr>
<th>Port</th>
<th>Switch Status</th>
<th>Fabric</th>
<th>FRU</th>
<th>Security</th>
<th>Resource</th>
<th>FCP</th>
<th>Traffic Flows</th>
<th>FPI</th>
</tr>
</thead>
</table>

Rules defined are thresholds measured on ports or SFPs and determine if an out of range violation is sent for the following rule.

Add/Edit Rule

- **Rule Name**: ○ Auto  ○ Custom

- **Measure**: CRC Errors (CRC)

- **Threshold Value**: >= 120 Count

- **Time Base**: Hour

- **Actions**: ✓ FAS Log Event
  - Port Decommission
  - Fence
  - SNMP Trap
  - Email

4. After the rules are modified or created, activate the MAPS policy and monitor to ensure that the rules are operating properly, then enable the port fencing facility. From the MAPS configuration, click **Actions** and select the **Fence** check box.
Figure 4 shows the activate MAPS policy actions.

**Preferred settings**
Enable port fencing on well-managed fabrics with high availability requirements, and then only on host ports for the link reset and CRC metrics.

**Monitoring Alerting Policy Suite**

MAPS provides an easy-to-use solution for policy-based threshold monitoring and alerting. When configured properly, MAPS provides real-time monitoring and logging of many switch metrics, eliminating the need to clear stats and monitor the stats over time. With MAPS, events are logged that enable you to see exactly when these threshold events occurred. This information then enables you to correlate events that happen during a performance or host impacting event.

MAPS alerting through email or SNMP notifies you of conditions that require attention, enabling marginal links or components to be resolved before they impact operations.

MAPS can also be used to automatically fence, toggle, or quarantine ports, providing levels of protection for the fabric without operations intervention.

MAPS was introduced in FOS V7.2 and replaces Fabric Watch as the preferred monitoring tool. With FOS V7.4, Fabric Watch is no longer available and MAPS is enabled by default.
FOS V7.4 introduced a basic set of monitoring rules to monitor overall switch status, FRU health, and base Fabric Performance Impact, and to monitor events without the need for a Fabric Vision or Fabric Watch License. To use the full suite of MAPS monitoring, reporting, and actions capabilities, a Fabric Vision (or Fabric Watch and Advanced Performance Monitoring) license is required.

FOS V7.4 also added several new monitoring metrics, including several metrics for FCIP circuits and tunnels. Two new actions for FPI events were also added where MAPS can be set up to behave in the following ways:

- Toggle (bounce the port offline then back online) when FPI detects congestion on the port
- Quarantine the flow (place the flow into a lower quality of service) to minimize the impact the congested flow has on the rest of the fabric

FOS V8.0 added additional FCIP monitors to add monitoring of the ethernet ports, and tunnel metrics.

FOS V8.1 added Rule On Rule, which allows a rule to monitor how many times another rule was triggered, enabling a threshold to be exceeded a number of times and not generate alerts or actions. However, if the threshold is exceeded several times, it can be alerted or actioned.

FOS V8.1 added the FPI SDDQ unquarantine action which allows quarantined ports to be automatically unquarantined based on a time value or the IO_Latency_Clear event.

**Configure MAPS**

Enable a default MAPS policy (typically the dlft_conservative policy) unless you have a high availability or high performance fabric. If so, see the advice for a custom policy. To enable a MAPS policy with Network Advisor, complete the following steps:

1. Select **Monitor → Fabric Vision → MAPS → Configure**.

   Figure 5 shows the Network Advisor Fabric Vision MAPS Configure menu.

   ![Network Advisor Fabric Vision MAPS Configure menu](image)

2. Set up the appropriate MAPS actions and, at a minimum, the RAS Log Event should be selected. Do not select the Fencing action unless a custom policy is being used with appropriate port fencing metrics and thresholds.
Figure 6 shows the Network Advisor MAPS Policy Actions dialog.

![MAPS Policy Actions Dialog](image)

**Note:** IBM suggests enabling MAPS with the `dflt_conservative` policy, with the RAS Log, SNMP, and E-mail actions selected. IBM does not recommend selecting the Fencing action.

Smaller installations that do not have Network Advisor running FOS V7.2 or V7.3 can enable MAPS by running `mapsconfig --enablemaps`. In FOS V7.4 and later, MAPS is enabled by default, but unless you have a license, you can use only the limited base monitoring policy.

The `dflt_conservative` policy can be enabled using the `mapspolicy --enable` command, and the MAPS actions can be set up using the `mapconfig --actions` command (see Example 5 on page 21).

**Note:** For switches with Virtual Fabrics enabled, all logical switches need to have MAPS enabled and configured. Using the `FOSEXEC --fid all` command issues the commands to all logical switches.
Example 5   CLI commands enabling MAPS and MAPS actions

SANA_DCX2:FID16:dlutz> fosexec --fid all -cmd "mapspolicy --enable
dflt_conservative_policy"
---------------------------------------------------
"mapspolicy" on FID 128:
---------------------------------------------------
"mapspolicy" on FID 4:

SANA_DCX2:FID16:dlutz> fosexec --fid all -cmd "mapsconfig --actions
RASLOG,SNMP,EMAIL,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL"
---------------------------------------------------
"mapsconfig" on FID 128:
---------------------------------------------------
"mapsconfig" on FID 4:

Custom policy for high availability fabrics
Fabrics that have high availability and performance requirements require a more stringent
approach to monitoring and altering attributes than the default policies provide.

As a preferred practice, we suggest using a custom set of MAPS rules that combine the
thresholds from the moderate policy and aggressive policy into a single custom policy. The
custom policy has aggressive rules that log minor threshold violations so that you can detect
marginal conditions and act on them in a proactive way.

The custom policy uses moderate rules to alert you through SNMP or email for conditions that
need more immediate attention, and a set of safety net rules to use automatic actions, such
as for port fencing, or port quarantine for severe issues. The overall strategy is to copy (clone)
the moderate default policy, because there are many default rules (such as power supply or
SFP thresholds) that we want to use without the need to define every rule.

Port metrics
For the port metrics that you want to customize, delete the default policy equivalent rules and
replace them with your thresholds, as shown in Table 1. Port thresholds should be customized
for the Non_E_F_PORTS, ALL_E_PORTS, ALL_OTHER_F_PORTS, ALL_HOSTS_PORTS, and
ALL_TARGET_PORTS groups.

Table 1   Custom MAPS port metrics threshold

<table>
<thead>
<tr>
<th>Type</th>
<th>Time</th>
<th>OP</th>
<th>RASLOG</th>
<th>Alert</th>
<th>Fence (host only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3TXTO</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>CRC</td>
<td>min</td>
<td>ge</td>
<td>10</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>CRC</td>
<td>hour</td>
<td>ge</td>
<td></td>
<td></td>
<td>240</td>
</tr>
<tr>
<td>ITW</td>
<td>min</td>
<td>ge</td>
<td>20</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>LF</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>LOSS_SIGNAL</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LOSS_SYNC</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LR</td>
<td>min</td>
<td>ge</td>
<td>5</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>LR</td>
<td>hour</td>
<td>ge</td>
<td></td>
<td></td>
<td>60</td>
</tr>
</tbody>
</table>
Switch fabric metrics

For switch metrics, set the EPORT_DOWN and FAB_SEG thresholds to greater than or equal to 1, to create alerts for every E_Port link that is down, or switch segmentation, by using the thresholds that are shown in Table 2.

Table 2  Custom MAPS switch metrics thresholds

<table>
<thead>
<tr>
<th>Type</th>
<th>Timebase</th>
<th>OP</th>
<th>RASLOG</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPORT_DOWN</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>FAB_SEG</td>
<td>min</td>
<td>ge</td>
<td>75</td>
<td>90</td>
</tr>
<tr>
<td>STATE_CHG</td>
<td>min</td>
<td>ge</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>

Note: Thresholds in the Fence column should be created only in the ALL_HOST_PORTS group.

Fabric Performance Impact metrics

For FPI metrics at FOS V7.x and FOS V8.0, MAPS should be set up to log FPI events to the RASLOG. Most fabrics experience congestion due to the shared workloads in the fabric, and the number of FPI events can be large, so alerting on FPI events is not recommended, as shown in Example 6.

Example 6  The mapsrule CLI command to enable logging for FPI events

mapsRule --create FPI_IO_PERF_IMPACT_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_PERF_IMPACT -action RASLOG -policy <policy_name>
mapsRule --create FPI_IO_FRAME_LOSS_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_FRAME_LOSS -action RASLOG -policy <policy_name>
mapsRule --create FPI_IO_LATENCY_CLEAR_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_LATENCY_CLEAR -action RASLOG -policy <policy_name>

Although SDDQ was introduced in FOS V7.4, MAPS can only be configured to quarantine a port. To remove the port from quarantine requires manual operator intervention, which can easily be missed. With FOS V8.1 and the unquarantine action, you can update the IO_FRAME_LOSS event to automatically quarantine a port for a given time interval, at which time it will be unquarantined, as shown in Example 7.

Example 7  The mapsrule CLI command to enable sddq

mapsRule --create FPI_IO_FRAME_LOSS_sddq -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_FRAME_LOSS -action RASLOG,SDDQ,UNQUAR -uqrt=30 -uqrt_unit min -policy <policy_name>
With FOS V8.2.1 a rule can be set up for FPI IO FRAME LOSS with an action of alerting so that you can be alerted if ports are being repeatedly put in and out of quarantine state, as shown in Example 8.

Example 8  The mapsRule CLI command to enable altering for repeat sddq events

```
mapsRule --createRoR FPI_IO_FRAME_LOSS_ror -group ALL_PORTS -monitor FPI_IO_FRAME_LOSS_sddq -op ge -timebase DAY -value 5 -action RASLOG,EMAIL,SNMP -policy <policy_name>
```

FCIP metrics

Typical IP traffic can tolerate higher rates of packet loss (driving retransmits) than Fibre Channel over IP (FCIP) can tolerate. There have been many cases were storage devices experience replication failures due to packet loss on the FCIP tunnel where the IP infrastructure does not record or report any issues. For FCIP metrics, we suggest that you log any packet loss over 5%, and alert and take action for packet loss over 10%, as shown in Table 3.

Table 3  Custom MAPS FCIP metrics thresholds

<table>
<thead>
<tr>
<th>Type</th>
<th>Time</th>
<th>Op</th>
<th>RASLOG</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKTLOSS</td>
<td>min</td>
<td>ge</td>
<td>0.05</td>
<td>0.1</td>
</tr>
<tr>
<td>JITTER</td>
<td>min</td>
<td>ge</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>RTT</td>
<td>none</td>
<td>ge</td>
<td>see note</td>
<td>see note</td>
</tr>
</tbody>
</table>

**Note:** Round Trip Time will vary greatly with every installation. Therefore, after you establish what the normal RTT value is, establish a logging threshold when RTT exceeds 10%, and an alerting threshold when it exceeds 25%.

Preferred settings

Enable MAPS with the default conservative policy on all switches running FOS V7.2 or higher. For fabrics that have high availability requirements, create a custom policy to provide additional monitoring and alerting for marginal issues.

Network Advisor dashboards

Network Advisor 12 introduced dashboards and was further enhanced in subsequent releases. Dashboards are a visual way to view key fabric metrics to help quickly identify issues.

The dashboard displays different widgets that contain switch and port status, port thresholds, performance monitors, and other items. Network Advisor comes with some standard dashboards, such as Product Status and Traffic and SAN Port Health, and you can create additional custom dashboards.

A dashboard provides a high-level overview of the network and the current states of managed devices. You can easily check the status of the devices in the network. The dashboard also provides several features to help you quickly access reports, device configurations, and system event logs.
The custom Fabric Health dashboard that is shown in Figure 7 has several widgets defined that can quickly show the current state and health of the fabric. At the top, the Scope field defines which switches and what time frame is used to populate the widgets.

Widgets, such as the Out of Range widget that shows the number of ports that had violations for each category for the selected time range, enable double-clicking the category. Dialog boxes open where you can drill down to the specific details for the violations. Similarly, you can use the Events widgets to click the event severity to display the individual event messages.

Figure 7   Network Advisor Fabric Health dashboard

One of the more powerful features of the dashboards is the ability to select the time frame or which fabric is used to populate the widgets. You can set the time frame for the last 24 hours to see what issues occurred in the past day to monitor for marginal issues that might be occurring, or dial down the scope to 30 minutes to focus on the current metrics for real time problem investigation.

Figure 8 on page 25 shows the dashboard time and fabric scope selection window.

Note: For more information about setting up dashboards and configuring the dashboard widgets, see the Brocade Network Advisor SAN User Manual for your release by searching in the Brocade Document Library: http://www.brocade.com/en/support/document-library.html
Another useful feature of the dashboard widgets is the ability to double-click most of the widget metrics to see additional details or a graph of the metric. Figure 9 shows the ITW port widget. By double-clicking the port name, a chart showing the ITW occurrences opens. Figure 9 shows the Host port ITW widget showing 427 ITWs.

Figure 8  Network Advisor dashboard scope selection

Figure 9  Network Advisor dashboard ITW widget
Figure 10 shows the ITW graph after double-clicking the port on the ITW widget.

As a preferred practice, create a customized dashboard to monitor the overall fabric health, and a dashboard to monitor port metrics. Optionally, create specialized custom dashboards to show port metrics for storage devices, server ports, and ISLs. These dashboards are used during major incidents, and can help identify whether there is a storage port, server port, or ISL that is causing a problem.

Preferred settings
Create Fabric Health and Ports dashboards with the widgets that are shown in Table 4.

Table 4  Suggested Product Status and Ports dashboards widgets

<table>
<thead>
<tr>
<th>Dashboard name</th>
<th>Status widget</th>
<th>Performance widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Health</td>
<td>SAN Inventory</td>
<td>Top Product CPU</td>
</tr>
<tr>
<td></td>
<td>Events</td>
<td>Top Product Memory</td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Out of Range Violations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Health Violations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom Events</td>
<td></td>
</tr>
<tr>
<td>Bottlenecked Ports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Ports</td>
<td>Port Health Violations</td>
<td>Top Port C3 Discards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port C3 Discards TX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port CRC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port ITW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port PCS Block Errors</td>
</tr>
</tbody>
</table>
Optionally, create Host, Storage, and ISL port dashboards, as shown in Table 5, which can be useful when performing problem determination.

**Table 5  Optional Host, Storage, and ISL dashboard widgets**

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Status widget</th>
<th>Performance widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Ports (continued)</td>
<td>Port Health Violations</td>
<td>Top Port Sync Losses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Utilization Percent</td>
</tr>
<tr>
<td>Host Ports</td>
<td>Initiator Port Health Violations</td>
<td>Top Initiator Ports ITWs</td>
</tr>
<tr>
<td></td>
<td>Initiator Bottleneck Ports</td>
<td>Top Initiator Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Ports C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Ports C3 Discards TX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator PCS Block Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port Sync Losses</td>
</tr>
<tr>
<td>Storage Ports</td>
<td>Target Port Health Violations</td>
<td>Top Target Ports C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td>Target Bottleneck Ports</td>
<td>Top Target Ports C3 Discards TX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Ports CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Ports Encode Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port Sync Loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port ITWs</td>
</tr>
<tr>
<td>ISL Ports</td>
<td>ISL Port Health Violations</td>
<td>Top ISL Port Utilization</td>
</tr>
<tr>
<td></td>
<td>ISL Bottleneck Ports</td>
<td>Top ISL Ports CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports Encode Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Sync Loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports C3 Discards TX TO</td>
</tr>
</tbody>
</table>
Create FCIP Dashboard
You can use the built-in WAN Vision dashboard or create a custom FCIP Dashboard using the widgets shown in Table 6 to monitor fabric FCIP metrics.

Table 6  Optional FCIP dashboard widgets

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Status Widgets</th>
<th>Performance Widgets</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCIP</td>
<td>Top Circuit FC Extension Utilization</td>
<td>Top Circuit IP Extension Utilization</td>
</tr>
<tr>
<td></td>
<td>Top Circuit Jitter</td>
<td>Top Circuit Jitter</td>
</tr>
<tr>
<td></td>
<td>Top Circuit Utilization</td>
<td>Top Duplicate Ack</td>
</tr>
<tr>
<td></td>
<td>Top Slow Start</td>
<td>Top Slow Start</td>
</tr>
<tr>
<td></td>
<td>Top Tunnel Dropped Packets</td>
<td>Top Tunnel Dropped Packets</td>
</tr>
<tr>
<td></td>
<td>Top Tunnel Utilization</td>
<td>Top Tunnel Utilization</td>
</tr>
</tbody>
</table>

Maintaining an optimal FCIP SAN environment

Starting with FOS V7.2, Brocade has added features to assist with monitoring, protecting, and troubleshooting FCIP connectivity. These features are part of Fabric Vision Monitoring Alerting Policy Suite (MAPS). When implemented and administered with care, these features can have a positive impact with regards to the reliability and resiliency of FCIP solutions and overall SAN fabric operations.

This section focuses on methods, tools, and features available in FOS 7.4 - 8.1 and especially as they apply to the following topics.:
- Bandwidth Validation
- Using Multiple Circuits
- Monitoring Alerting Policy Suite (MAPS)
- Troubleshooting

Ensure proper FCIP bandwidth

The task of determining the necessary FCIP bandwidth can be broken down into two general objectives. The first involves defining the bandwidth that will be required to meet the needs of the business, and the second involves validating that the actual bandwidth being delivered matches the projected and expected bandwidth of the solution as implemented.

This document is not intended to be a broad architectural review, but rather more specific to the type of questions that should be considered, in addition to tests and methodologies that can be performed to arrive with the answers to the objectives stated above. There are many implementation and design considerations for a Fibre Channel storage area network, and more information is available in the Brocade white paper: SAN Design and Best Practices.

The tools discussion in this section focuses on what is available on Brocade extension switches and director blades.
How much bandwidth

There are a number of basic questions to be answered when determining how much bandwidth is necessary to the needs of a business. First, the amount of data that will be transferred or replicated needs to be calculated. Next, the amount of time for how quickly this data must be transferred from the local to remote site needs to be determined. When these values are known, the simple math of dividing the total data amount by the time determines a starting point for the minimum amount of bandwidth necessary.

To determine the current amount of data to be transferred or replicated, the following questions need to be considered:

- How much data will need to be initially transferred for synchronized copies at both the local and remote data sites?
- How frequently is the initial data being changed?
- What is the profile of the change rate over a period of time?
- What is the maximum amount of the data change rate?

The starting point for data sizing is the first question. Using a data replication solution as an example, the initial amount of data to be synchronized to a remote data site needs to be determined. This answer requires determining which local data sets, volumes, and consistency groups need to be replicated to the remote data site, and then simply calculating the total size of all of the data to be transferred.

If there are multiple storage systems replicating data between the local and remote data sites, then all of the individual replication streams must be known to have a reliable answer for the amount of data to be initially transferred. Therefore, the characteristics of data transfer and replication applications sharing a given FCIP tunnel must be understood.

Because data sets, volumes, and consistency groups are rarely consistent in size, most storage systems apply a fairness algorithm so that each item to be transferred has equal portions of the bandwidth. With a mixture of large and small volumes and consistency groups, the balanced transfer rates result in smaller volumes or consistency groups being synchronized before the larger ones.

After a smaller volume or consistency group is synchronized, most systems begin to transfer data that was changed in the source volume or consistency group while the larger volumes and consistency groups are still being synchronized. This sizing scope is determined with questions about change frequency, workload profile, maximum change, and change rate over a period of time.

When the amount of initial data to be transferred or replicated is understood, the next step involves determining the rate of change of the data to be mirrored. This value is not a percentage of how much of each volume or consistency group is changing, but the amount of data that changes in terms of size, such as bytes. Depending on the type of data and applications using the data, the change rate may be consistent over time, or it may vary greatly over a given time period.

The best answer for the change rate of each data set, volume, or consistency group is the maximum change rate for a set time period, such as 24 hours. The change rates for the various data units to be transferred or replicated should be determined based on a common time period.

The combination of the initial amount of data to be synchronized with the amount of change data is the total scope of the data to be transferred or replicated. The next step is to determine what the business needs, or requirements in terms of how quickly the data can be initially transferred and then what the recovery point objective (RPO) needs to be.
When the time factor is known, the bandwidth needed for the FCIP tunnel is just a math exercise to determine the bandwidth value in bits per second. This bandwidth setting is what will be needed for the current amount of data to be replicated.

At this point, one additional factor needs to be considered, and that factor is growth over time. Most businesses experience growth of their replication needs over time. As previously stated, the exercises and calculations have been for the current needs, and no consideration has been given for data growth.

As a business grows and expands, the amount of data to be synchronized and the change rate will likely increase over time. Therefore, meeting the bandwidth needs for the moment is likely to be insufficient for the future operations of the replication solution.

The current bandwidth requirement needs to be adjusted accordingly for future needs based on trend metrics. If a business has been experiencing data growth of approximately 25% per year, then the replication needs in a year will likely see similar growth. There are no rigid rules for “future proofing” bandwidth needs, but this point does need to be considered, evaluated, and result in an adjustment to the current bandwidth needs to account for future data growth.

Brocade extension switches and blades have one optional feature that might have some consideration when determining the bandwidth needs for mirror and replication solutions, which is compression. Brocade hardware and the Fabric Operating System (FOS) provide a number of compression modes. However, the compression modes depend on a number of factors, such as the hardware platform, the protocol (FCIP or IP extension) and the available tunnel bandwidth.

See the Brocade Fabric OS Extension Configuration Guide for additional information. Throughput for any compression mode is very dependent on the compressibility of the data to be replicated. Do not expect compression to provide any reduction factor of bandwidth needs.

**Actual versus allocated bandwidth**

Continuing with the replication solution scenario, the following simple example for bandwidth needs is provided. A company has 17 TB of data that needs to be replicated, and the maximum change rate is 3 TB per day for a total of 20 TB. The business needs of the company states that initial synchronization and starting with the change data during the synchronization period is to be completed within 24 hours.

Trending data shows growth rate of the data is just under 10% per year. Therefore, the calculations described previously works out as follows:

\[
\frac{(17 \text{ TB} + 3 \text{ TB}) \times 8 \text{ bits/B}}{(24 \text{ hours} \times 3600 \text{ second/hour})} = 1.852 \text{ Gbps}
\]

To account for the growth over one year, the bandwidth needed should be adjusted:

\[
1.852 \text{ Gbps} \times 1.10 = 2.037 \text{ Gbps}
\]

By rounding down, the company should plan on approximately 2 Gbps total bandwidth between the local and remote data sites to meet the current replication requirements and remain viable for almost a year into the future. With redundant fabrics, one implementation design for this replication solution example could be comprised on single 1 Gbps links per fabric across their two redundant fabrics.
Therefore, the bandwidth needs for replication have been determined and implemented as 1 Gbps FCIP tunnel per fabric between the local and remote data sites. The next suggested step is to verify that the actual bandwidth meets the design target before the FCIP tunnels are put into production.

There are a number of WAN analysis tools designed for testing connections, tracing routes, and estimating the end-to-end IP path performance characteristics between the local and remote data sites. These tools are available using the `portCmd` command with options. The following options are available:

- `portCmd --wtool` This generates traffic over a circuit to test the network link for issues, such as maximum throughput, congestion, loss percentage, out of order delivery, and other network metrics.
- `portCmd --ping` This tests the connection between a local Ethernet port and a destination IP address. If testing a VLAN connection, then a VLAN tag table entry must be manually added on both the local and remote sides of the route.
- `portCmd --traceroute` This traces routes from the local Ethernet port to a destination IP address. When tracing a route across a VLAN, a VLAN tag table entry must be manually added on both the local and remote sides of the route.
- `portShow fcipTunnel --perf` This displays the performance statistics generated from the WAN analysis (wtool) testing.

The reason for using these tools prior to the FCIP tunnel going into production is that the tunnel cannot be passing any other traffic while the WAN Tool option is running. The WAN tool can be run on multiple circuits consecutively, but only one wtool session per circuit is allowed at a time. One notable feature of the WAN tool is the ability to test the end-to-end connectivity with jumbo frames to verify that the end-to-end pathway fully supports jumbo frames.

After an FCIP tunnel and its associated circuits are in production mode, the ability to use the WAN analysis tools will be disruptive and therefore not likely to be utilized. There is a method to check the throughput by using TCP/IP metrics displayed from the extension switch data. TCP/IP data can be used to determine what a circuit is capable of delivering. A good validation is if the TCP/IP viewpoint shows the potential for throughput is equal to or greater than the configured bandwidth.

For example, consider an FCIP tunnel that has two circuits on two different GE ports, and each circuit is configured for a maximum bandwidth of 100 Mbps. By using the TCP/IP metric data from the TCP session data of the extension switch, the TCP/IP point shows a potential bandwidth of more than 400 Mbps for each circuit.

In this example, the potential is greater than the configured solution, which is a good check. Although TCP/IP shows that the circuit is capable of much greater throughput, the 100 Mbps threshold limits the traffic level that the extension switch allows.

**Note:** For more information about setting up dashboards and configuring the dashboard widgets, see the Brocade Fabric OS Extension Configuration Guide for your release by searching in the Brocade Document Library:

Example 9 shows two methods to check how much bandwidth has been configured for circuits using the `portshow fciptunnel` command. The first version using the command shows the basic configuration of the FCIP tunnel and its associated circuits, while the second version of the command shows the breakout bandwidth allocations based on priority.

**Example 9  The portshow fciptunnel command options**

<table>
<thead>
<tr>
<th>Tunnel Circuit</th>
<th>OpStatus</th>
<th>Flags</th>
<th>Uptime</th>
<th>TxMBps</th>
<th>RxMBps</th>
<th>ConnCnt</th>
<th>CommRt</th>
<th>Met/G</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>-</td>
<td>Up</td>
<td>------d-</td>
<td>24d5h</td>
<td>23.21</td>
<td>0.11</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>24</td>
<td>ge1</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>11.54</td>
<td>0.05</td>
<td>6</td>
<td>20/100</td>
</tr>
<tr>
<td>24</td>
<td>ge3</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>11.67</td>
<td>0.05</td>
<td>6</td>
<td>20/100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tunnel Circuit</th>
<th>OpStatus</th>
<th>Flags</th>
<th>Uptime</th>
<th>TxMBps</th>
<th>RxMBps</th>
<th>ConnCnt</th>
<th>CommRt</th>
<th>Met/G</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>-</td>
<td>Up</td>
<td>cM------d-</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>24</td>
<td>ge1</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>0/100</td>
</tr>
<tr>
<td>24</td>
<td>ge3</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>0/100</td>
</tr>
<tr>
<td>24</td>
<td>-</td>
<td>Up</td>
<td>hM------d-</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>24</td>
<td>ge1</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>0/100</td>
</tr>
<tr>
<td>24</td>
<td>ge3</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>0.00</td>
<td>0.00</td>
<td>6</td>
<td>0/100</td>
</tr>
<tr>
<td>24</td>
<td>-</td>
<td>Up</td>
<td>mM------d-</td>
<td>24d5h</td>
<td>23.21</td>
<td>0.11</td>
<td>6</td>
<td>-</td>
</tr>
<tr>
<td>24</td>
<td>ge1</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>11.54</td>
<td>0.05</td>
<td>6</td>
<td>20/100</td>
</tr>
<tr>
<td>24</td>
<td>ge3</td>
<td>Up</td>
<td>----a---4</td>
<td>24d5h</td>
<td>11.67</td>
<td>0.05</td>
<td>5</td>
<td>0/100</td>
</tr>
</tbody>
</table>

Each circuit has been configured for a maximum bandwidth of 100 Mbps. Although each circuit is connected to a GE Ethernet port with a capacity of 1000 Mbps, the extension switch limits the maximum throughput to only 100 Mbps. The method for manually checking the throughput is a similar type of situation. As long as the TCP/IP driver shows more bandwidth than configured, the circuit is in a good condition.

Manually checking what the TCP/IP driver considers the available bandwidth to be requires doing some calculations using the size of the receive window divided by the Round-Trip Time (RTT). The simple version of the equation is:

\[ \frac{\text{size of receive window in bits}}{\text{RTT in seconds}} = \text{detected bandwidth in Mbps} \]

Using the `portshow fciptunnel` command and specific options displays the necessary information to perform the calculation. Most FCIP tunnel implementations do not use quality of service (QoS) zoning, which results in the replication traffic being passed with medium QoS.
Therefore, only the medium TCP flows need to be measured, as shown in Example 10.

**Example 10  The portshow fc iptunnel command**

```
portshow fc iptunnel -cd --ha --qos --tcp
```

TCP Connection 24.0 HA-Type:Main Pri:Medium Conn:0x02f77549

Local / Remote Port : 3226 / 49671
Duration : 24d5h
MSS : 1460 bytes
ARL Min / Cur / Max : 3000 / 33032 / 50000
ARL Reset Algo® : StepDown
Send Window
Size / Scale : 1240064 / 9
Slow Start Threshold : 16777216
Congestion Window : 16854320
Pkts InFlight : 0
Recv Window
Size / Scale : 1249792 (Max:1249792) / 9
SendQ Nxt / Min / Max : 0xe12631b8 / 0xe122e5a8 / 0xe12631b8
RecvQ Nxt / Min / Max : 0x8e4328c7 / 0x8e4328c7 / 0x8e563ac7
RecvQ Pkts : 745107039
Sender Stats
Sent Bytes / Pkts : 137233698073 / 1126716089
Unacked Data : 216080
Retransmits Slow / Fast : 342 / 96497 (High:0)
SlowStart : 0
Receiver Stats
Recv Bytes / Pkts : 28859842579 / 578869489
Out-of-Order : 0 (High:45)
Duplicate Acks : 368298
RTT / Variance (High) : 46 ms (72 ms) / 0 ms (29 ms)

The receive window size in the example output is in bytes, not bits, so it will need to be converted by multiplying this value by 8 to get bits. The Round-trip Time value is shown in milliseconds, which needs to be converted to seconds by dividing the RTT value by 1000. In the above example, the equation becomes:

\[(1249792 \text{ bytes} \times 8 \text{ bits/byte}) / (46 \text{ ms} / 1000 \text{ msps}) = 217.355 \text{ Mbps}\]

The TCP/IP driver used in the Brocade extension switch and blade is programmed to create a sufficient number of TCP sessions to drive the circuit to its maximum with a measure of failover capability. In Example 11, there are two TCP sessions that are identified by the unique TCP connection identifier. In the example, the second TCP session has similar values for the receive window size and Round-trip Time.

**Example 11  TCP sessions**

TCP Connection 24.1 HA-Type:Main Pri:Medium Conn:0x02f7755d

Local / Remote Port : 3225 / 55818
Duration : 24d5h
MSS : 1460 bytes
ARL Min / Cur / Max : 3000 / 43000 / 50000
ARL Reset Algo : StepDown
Send Window
Size / Scale : 1240064 / 9
Slow Start Threshold : 16777216
Congestion Window : 16907848
Pkts InFlight : 0
So the two TCP sessions are capable of driving traffic at the rate of 434.71 Mbps, which is greater than the configured 100 Mbps for the circuit. Therefore, the configured and allocated bandwidth is being used, and this verification has been performed while the FCIP tunnel and its circuits were in production.

**Use multiple circuits**

FCIP is a tunneling protocol that maps FC and IP for connectivity with their inherent characteristics. However, the characteristics of the FC and IP protocols are not an easy match. Fibre Channel is based on lossless connections between device ports with a high emphasis on in-order delivery of frames, but IP is based on the assumption that some degree of packet loss will occur.

An FCIP tunnel is a single Inter-Switch Link (ISL) that contains at least one, or more, circuits. When multiple circuits are used to create the FCIP tunnel, it is also known as an *extension trunk*. A circuit is a physical connection between a pair of IP addresses that are associated with the local and remote endpoints of an FCIP tunnel. Circuits provide the pathways for traffic flows between the local and remote interfaces at each end of the tunnel.

Multiple circuits can be configured per Ethernet port by assigning them unique IP interfaces. When configuring a circuit, the IP addresses for the local and remote interfaces are provided, and each circuit must be composed of unique pairs of local and remote IP interfaces, as shown in Figure 11.
**Extension Trunking** is a method for the aggregation and management of the use of IP WAN bandwidth. Extension Trunking provides a method of using redundant paths over the WAN for lossless failover and increased resiliency due to WAN failure. Extension Trunking also improves load balancing on a weighted round-robin basis. Trunking is enabled by creating multiple circuits within a FCIP tunnel so that the tunnel can use the circuits passing traffic between multiple local and remote addresses.

Extension Trunking provides lossless link loss (LLL), which ensures that all data lost in flight is retransmitted and reassembled back in order, prior to being delivered to upper layer protocols. This is an essential feature for both FICON environments to prevent interface control checks (IFCCs), and for open systems replication environments to prevent SCSI time-outs.

While multiple FCIP tunnels can be defined between pairs of extension switches or extension blades, this design defeats the benefits of a multiple-circuit FCIP tunnel. Defining two tunnels between a pair of extension switches or blades is not as redundant or fault-tolerant as having multiple circuits in one FCIP tunnel. The advantage of multiple circuits is where some circuits within an Extension Trunk can be configured as failover circuits or as spillover circuits.

The **failover circuit** is essentially a standby circuit to be used when an active circuit fails. A **spillover circuit** is a secondary circuit that is used only during periods of high traffic usage. When configuring an FCIP tunnel with multiple circuits, failover circuits and spillover circuits cannot be used at the same time.

For solutions that have high bandwidth requirements between the local and remote data sites, multiple FCIP tunnels might be necessary. In this situation, each FCIP tunnel should be composed of multiple circuits. When multiple parallel FCIP tunnels are created between the local and remote data sites, lossless dynamic load sharing (DLS) should be enabled. This functionality is enabled to properly handle routing updates that occur when FCIP tunnels come up or go down. Each routing update can cause dropped or un-routable frames if the destination is via a peer tunnel.

Adaptive Rate Limiting (ARL) is a licensed feature and can be implemented on individual circuits. ARL enables the extension switch to change the circuit’s throughput rate by working with the IP network. ARL uses information from the TCP sessions to dynamically adjust the throughput rate for the circuit. ARL is implemented by configuring minimum and maximum bandwidth rates for a circuit. The minimum configured bandwidth is maintained, and the maximum configured rate will not be exceeded.

When replication traffic starts passing over a circuit, ARL starts at the minimum rate and attempts to increase the data throughput until it reaches the maximum configured rate (or TCP information indicates that no more bandwidth is available). If the actual throughput data rate is not at the maximum configured rate, ARL routinely checks TCP conditions for more bandwidth.

If the indicators show that more bandwidth is available, ARL continues to increase up to the maximum configured bandwidth rate. If problems are detected on the circuit, ARL reduces the rate appropriately.

If the long distance WAN path is shared with multiple types of mirror and replication traffic such that the bandwidth cannot be guaranteed, ARL is recommended. The following three common scenarios are some where ARL would be effective:

- Storage and non-storage traffic are sharing a single WAN link
- More than one extension interface is utilizing a single WAN link that has been dedicated to a given storage system
- Any combination of the above two scenarios
A key design element of a SAN solution is the use of redundant fabrics. This design element should also be applied to WAN connectivity between the local and remote site. If redundant fabrics with separate extension switches use a single WAN link between sites, any interruption of the WAN link is disruptive to the redundant fabrics. The distribution of the connections can be based at the following levels:

- Circuit, where one or more circuits per fabric use separate WAN links
- Fabric, where all circuits for a given fabric have dedicated WAN links

**Preferred settings**
Create FCIP tunnels with multiple circuits between a pair of extension switches or blades with ARL configured using multiple WAN links if possible. If using multiple FCIP tunnels with protocol optimization features, such as FICON Acceleration or Brocade Open Systems Tape Pipelining (OSTP), then Traffic Isolation (TI) zones or logical switch/logical fabric (LS/LF) configurations must be used.

**Ensure effective monitoring**
On switches running FOS V7.4 or higher, use the MAPS to monitor the FCIP tunnels and circuits. To ensure that consistent settings and policies are enabled on all switches in the fabric, use Network Advisor.

As described earlier, MAPS is a ready-made solution for policy-based threshold monitoring and alerting. By leveraging prebuilt, policy-based rules templates, MAPS simplifies threshold configuration, monitoring, and alerting. The following sections focus on the FCIP Health category for monitoring.

Fabrics with long distance connections for replication and data migration that have high availability requirements must have strict monitoring of those connections. As a preferred practice, use a custom set of MAPS rules that combines a number of thresholds from the default aggressive policy, in addition to customized rules for the solution’s round-trip time (RTT) and circuit utilization. Table 7 shows the monitoring items and the MAPS thresholds for the three default policies.

**Table 7  Default MAPS FCIP monitoring thresholds**

<table>
<thead>
<tr>
<th>Monitoring Statistic</th>
<th>Unit</th>
<th>Default FCIP monitoring threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Aggressive</td>
</tr>
<tr>
<td>Circuit packet loss percentage (CIR_PKTLOSS)</td>
<td>Percentage per minute</td>
<td>0.01</td>
</tr>
<tr>
<td>Circuit state change (CIR_STATE)</td>
<td>Changes per hour</td>
<td>0</td>
</tr>
<tr>
<td>Circuit utilization percentage (CIR_UTIL)</td>
<td>Percentage per hour</td>
<td>60</td>
</tr>
<tr>
<td>Circuit jitter (JITTER)</td>
<td>Percentage of delay change per minute</td>
<td>5</td>
</tr>
<tr>
<td>Circuit round trip time (RTT)</td>
<td>Milliseconds</td>
<td>250</td>
</tr>
<tr>
<td>Tunnel (STATE_CHG)</td>
<td>Changes per minute</td>
<td>0</td>
</tr>
</tbody>
</table>
Typical IP traffic can tolerate higher rates of packet loss and the resulting retransmission of FCIP packets than the Fibre Channel layer of FCIP can tolerate. There have been many cases where storage devices experience replication failures due to packet loss on the FCIP tunnel where the IP infrastructure did not record or report any issues. For FCIP metrics, we suggest logging any packet loss of 0.01%, and to alert and take action for packet loss of 0.05% or higher.

**Preferred FCIP MAPS settings**
Enable MAPS with a custom policy based on the default Aggressive policy on all switches running FOS V7.4 or higher. The monitoring options that should be customized are Round-trip Time and Jitter. Round-trip Time will vary greatly with every installation, so after you establish what the normal RTT value is, establish a logging threshold when RTT exceeds 10% and an alerting threshold when it exceeds 25%. For Jitter metrics, we suggest logging when Jitter reaches 10% and to alert when Jitter becomes 25% or higher.

Be aware that excessive packet loss, variable RTT times, or inconsistent Jitter are indications of issues within the LAN or WAN pathway between the local and remote sites, and not with the extension switch.

**Summary of preferred practices**
Here is a summary of the preferred features and capabilities to improve the overall resiliency of FOS-based FC fabric environments:
- Enable an appropriate routing policy.
- Configure an appropriate In Order Delivery (IOD) setting.
- Configure an appropriate Dynamic Load Sharing (DLS) setting.
- Verify Edge Hold Time.
- Enable Credit Recovery Tool.
- Enable Dynamic Port name.
- Enable Fabric Performance Impact or Bottleneck monitoring.
- Enable MAPS monitoring and alerting.
- Enable Slow Drain Device Quarantine.
- Configure and use Network Advisor Dashboards.

**Preferred implementation open systems**
This section describes the preferred sequence for implementing the fabric resiliency features that are provided by the Brocade FOS along with the preferred configuration values.

**Note:** The preferred sequence and associated thresholds that are presented are identified for most environments. It is possible that specific environments might require alternative settings to meet specific requirements.

**Enabling the routing policy**
Enable the appropriate routing policy based on the environment that the fabric supports.

Enable EBR for open systems environments by using the Advanced Performance Tuning Policy (`aptpolicy`) command.
Example 12 shows the `aptpolicy` command that is used to set the EBR policy.

**Example 12  The `aptpolicy` command for exchange-based routing**

DCX1_Default:FID128:dlutz> aptpolicy 3
Policy updated successfully.

DCX1_Default:FID128:dlutz> aptpolicy
Current Policy: 3

3 : Default Policy
1: Port Based Routing Policy
2: Device Based Routing Policy (FICON support only)
3: Exchange Based Routing Policy

Enable EBR policy for switches that support only FICON, or FICON and open systems environments.

Example 13 shows the `aptpolicy` command that is used to set the DBR policy.

**Example 13  The `aptpolicy` command for device-based routing**

DCX1_Default:FID128:dlutz> aptpolicy 2
Policy updated successfully.

DCX1_Default:FID128:dlutz> aptpolicy
Current Policy: 2

3 : Default Policy
1: Port Based Routing Policy
2: Device Based Routing Policy (FICON support only)
3: Exchange Based Routing Policy

**Enabling in-order delivery**

Disable in-order delivery (IOD) for switches unless you are using FICON.

Example 14 shows the `iodset` and `iodshow` commands to enable frame IOD.

**Example 14  The `iodset` and `iodshow` commands**

DCX1_SANA:FID16:dlutz> iodset
IOD is set

DCX1_SANA:FID16:dlutz> iodshow
IOD is set

**Note:** EBR is the default routing policy.
Example 15 shows the `iodreset` and `iodshow` commands to disable frame IOD.

**Example 15  The iodreset command**

```
DCX1_SANA:FID16:dlutz> iodreset
IOD is not set

DCX1_SANA:FID16:dlutz> iodshow
IOD is not set
```

**Enabling dynamic load sharing**

Dynamic load sharing (DLS) is enabled when the exchange-based or EBR policies are used and cannot be changed. Lossless should be enabled. Example 16 shows the `dlsset` command to enable lossless.

**Example 16  The dlsset command to enable lossless**

```
DCX1_Default:FID128:dlutz> dlsset --enable -lossless
DLS and Lossless are set

DCX1_Default:FID128:dlutz> dlsshow
DLS is set with Lossless enabled
E_Port Balance Priority is not set
```

E_Port balance priority should be enabled. Example 17 shows the `dlsset` commands to enable E_port balance priority.

**Example 17  The dlsset commands to enable E_port balance priority**

```
DCX1_SANA:FID16:dlutz> dlsset --enable -eportbal
E_Port Balance Priority is set

DCX1_SANA:FID16:dlutz> dlsshow
DLS is set with Lossless enabled
E_Port Balance Priority is set
```

**Enabling the dynamic port name**

On switches running FOS V7.4 and higher, enable the dynamic port name.

**Note:** To enable the dynamic port name on switches with virtual fabrics, run the `configure` command from all logical switches.

Example 18 shows the `configure` commands that are used to enable the dynamic port name.

**Example 18  The configure command to enable the dynamic port name**

```
F48a_Default:FID128:dlutz> configure

Not all options will be available on an enabled switch.
To disable the switch, use the "switchDisable" command.

Configure...
```
Fabric parameters (yes, y, no, n): [no] y

WWN Based persistent PID (yes, y, no, n): [no]
Allow XISL Use (yes, y, no, n): [yes]
Dynamic Portname (on, off): [on] on
Edge Hold Time (Low(80ms), Medium(220ms), High(500ms), UserDefined(80-500ms)): (80..500) [220]

Example 19 show the portname -d command to configure the parameters to be displayed, where the parameters are the following: S - Switch Name, T - Port Type, I - Port Index, A - Alias name, F - FDMI Host name, R - Remote Switch Name, C - Slot / Port Number (only for SAN Director).

Example 19 The portname -d command to set the parameters and display the setting
PFE_F48_01_20:FID20:admin> portname -d "S.T.I.F.A.R"
PFE_F48_01_20:FID20:admin> portname -d S.T.A.F.R

Enabling Slow-Drain Device Quarantine

On switches with FOS V8.1 and higher, enable SDDQ for the MAPS IO_FRAME_LOSS events with the un-quarantine option.

Note: To use the SDDQ switch, QOS must be enabled on all switches.

Complete the following steps:

1. To verify whether QOS is active on the ISL switch ports, run the islshow command on the switch and look for QOS next to each ISL link. You can view the port QOS setting by running the portcfgshow command. If QOS is not enabled, run the portcfgqos command.

Example 20 shows the islshow command on an ISL that has QOS active.

Example 20 The islshow command showing the QOS setting
SANA_DCX1:FID16:dlutz> islshow
1:199-> 28 10:00:00:05:33:99:12:02  20 SANA_DCX2 sp:  4.000G bw: 4.000G TRUNK QOS

Example 21 shows the portcfgshow command on ports with the default QOS AutoEnable setting.

Example 21 The portcfgshow command showing the QOS setting
SANA_DCX1:FID16:dlutz> portcfgshow
Ports of Slot 2  16 17 18 19  20 21 22 23 29 30 31
-----------------+---+---+---+---+-----+---+---+---+---+---+---
Speed            AN AN AN AN AN AN AN AN AN AN AN
Fill Word(On Active) 0 0 0 0 0 0 0 0 0 0 0
Fill Word(Current) 0 0 0 0 0 0 0 0 0 0 0
AL_PA Offset 13   .. .. .. .. .. .. .. .. .. .. ..
QOS Port         AE AE AE AE AE AE AE AE AE AE AE
EX Port          .. .. .. .. .. .. .. .. .. .. ..
2. To enable SDDQ, update the appropriate IO_FRAME_LOSS MAPS rules to use the SDDQ action.

3. Start the MAPS configuration dialog box by clicking Monitor → Fabric Vision → MAPS → Configure. In the MAPS Configure dialog box, select the appropriate MAPS policy and click Edit. Edit the IO_FRAME_LOSS rule on the FPI tab and select the SDDQ check box.

Figure 12 on page 42 shows the FPI rule IO_FRAME_LOSS with the SDDQ and un-quarantine action enabled.
Note: Run several weeks with this rule enabled but with the SDDQ facility disabled to ensure that the rule works as expected.
4. Enable the SDDQ facility on the MAPS configuration dialog box by selecting the fabric and clicking **Actions**.

Figure 13 shows the MAPS Policy actions dialog box with the FPI SDDQ action enabled.

![MAPS Policy Actions](image)

**Figure 13** Network Advisor MAPS Policy Actions with SDDQ enabled

### Preferred implementation for FICON

With the release of FOS V8.1.0c, Brocade and IBM qualified FICON multi-hop configurations. Initial multi-hop configurations are limited to three hops with specific configurations.

For more information, see the *FICON Multihop: Requirements and Configurations* white paper.
Access control/zoning

FICON switches can be set up in one of two ways:

- FICON switches can be set up to be like older ESCON directors, which did not use zoning, but used Allow/Prohibit matrixes that were created by the ESCON director console, or mainframe software, such as hardware configuration definition (HCD). To set up a switch in this manner, set the default access to **no access** and do not implement any zoning. You can then create Allow/Prohibit matrixes using Network Advisor or mainframe software.

- FICON switches can also be set up using zoning. Because FICON enforces host to device access through the Input Output Configuration DataSet (IOCDS) there is no need to create separate zones for each host to device connection. It is a common practice to place all FICON host and devices into a single zone.

As a preferred practice, Brocade and IBM suggest one zone for all FICON connectivity.

Although domain index zoning is supported, WWN zoning for quality of service (QoS) is advised in environments where N_Port ID Virtualization (NPIV) is deployed.

A mix of index zoning and WWN zoning is not recommended.

Disable the default zone, save it, and enable your new zoneset, as shown in Example 22.

**Example 22  Enabling the new zoneset**

```
Brocade_def:FID128:admin> defzone --no access
You are about to set the Default Zone access mode to No Access
Do you want to set the Default Zone access mode to No Access ? (yes, y, no, n): [no] y
Brocade_def:FID128:admin> cfgsave
You are about to save the Defined zoning configuration. This action will only save the changes on Defined configuration.
If the update includes changes to one or more traffic isolation zones, you must issue the 'cfgenable' command for the changes to take effect.
Do you want to save the Defined zoning configuration only? (yes, y, no, n): [no] y
Updating flash ...
Brocade_def:FID128:admin> cfgenable mynewzone
You are about to enable a new zoning configuration.
This action will replace the old zoning configuration with the current configuration selected. If the update includes changes to one or more traffic isolation zones, the update may result in localized disruption to traffic on ports associated with the traffic isolation zone changes.
Do you want to enable 'mynewzone' configuration (yes, y, no, n): [no] y
zone config "mynewzone" is in effect
Updating flash ...
Brocade_def:FID128:admin>
```
Configuring the FICON switch routing policy

Example 23 shows the suggested Device Based Routing (DBR) policy.

Example 23  Suggested DBR policy

Brocade_def:FID128:admin> aptpolicy
Current Policy: 3
  3 : Default Policy
  1: Port Based Routing Policy
  2: Device Based Routing Policy (FICON support only)
  3: Exchange Based Routing Policy
Brocade_def:FID128:admin> switchdisable
Brocade_def:FID128:admin> aptpolicy 2
Policy updated successfully.
Brocade_def:FID128:admin> aptpolicy
Current Policy: 2
  3 : Default Policy
  1: Port Based Routing Policy
  2: Device Based Routing Policy (FICON support only)
  3: Exchange Based Routing Policy
Brocade_def:FID128:admin> switchenable

Dynamic load sharing

The preferred practice is to enable dynamic load sharing (DLS); however, DLS is only supported when lossless is enabled:

Brocade_def:FID128:admin> dlsSet --enable -lossless

DLS and lossless are set.

Note: If lossless DLS is not enabled, the routing policy must be port-based routing (aptPolicy 1).

In-order delivery

Set in-order delivery using the iodset command, as shown in Example 24.

Example 24  The iodset command to enable in-order delivery

Brocade_def:FID128:admin> iodset
IOD is set
Configure the SCC policies

To configure the SCC policies, complete the following steps:

1. Use secPolicyCreate to create and activate the policy, as shown in Example 25.

   Example 25  Using secPolicy to create and activate policy

   Brocade_def:FID128:admin > secpolicyshow
   ______________________________________________________
   ACTIVE POLICY SET
   ______________________________________________________
   DEFINED POLICY SET
   Brocade_def:FID128:admin > secpolicycreate "SCC_POLICY",
   "10:00:c4:5f:7c:96:0a:c0;10:00:c4:5f:7c:95:ab:e4"
   SCC_POLICY has been created.
   Brocade_def:FID128:admin > secpolicysave
   secpolicysave command was completed successfully.
   Brocade_def:FID128:admin > secpolicyshow
   ______________________________________________________
   ACTIVE POLICY SET
   ______________________________________________________
   DEFINED POLICY SET
   SCC_POLICY
   WWN                     DId  swName
   -----------------------------------------------
   10:00:c4:5f:7c:95:ab:e4  57  PFE_up_def
   10:00:c4:5f:7c:96:0a:c0  49  PFE_lo_def

2. We activate the policy as shown in Example 26 (note that swName may show Unknown status).

   Example 26  Activate the policy

   Brocade_def:FID128:admin > secpolicyactivate
   About to overwrite the current Active Policy Set.
   ARE YOU SURE (yes, y, no, n): [no] y
   secpolicyactivate command was completed successfully.
   Brocade_def:FID128:admin > secpolicyshow
   ______________________________________________________
   ACTIVE POLICY SET
   ______________________________________________________
   DEFINED POLICY SET
   SCC_POLICY
   WWN                     DId  swName
   -----------------------------------------------
   10:00:c4:5f:7c:95:ab:e4  57  PFE_up_def
   10:00:c4:5f:7c:96:0a:c0  49  PFE_lo_def
   SCC_POLICY
   WWN                     DId  swName
   -----------------------------------------------
   10:00:c4:5f:7c:95:ab:e4  57  PFE_up_def
   10:00:c4:5f:7c:96:0a:c0  49  PFE_lo_def
3. Enter the `fddCfg` command to enable the ACL fabric-wide consistency policy and enforce a strict SCC policy, as shown in Example 27.

   **Example 27  The fddCfg command to enable ACL fabric wide consistency policy**

   Brocade_def:FID128:admin > fddcfg --fabwideset "SCC:S"
   Brocade_def:FID128:admin >

4. To create a policy that includes all the switches in the fabric, enter the command shown in Example 28.

   **Example 28   Create a policy to include all the switches in the fabric**

   Brocade_def:FID128:admin > secPolicyCreate SCC_POLICY "*
   SCC_POLICY has been created.

5. Configure the switch parameters using the `configure` command, as shown in Example 29. The configuration change will be saved only if all parameters are acknowledged (only the values to change are displayed here). Note that the switch needs to be disabled before running the `configure` command.

   **Example 29   Switch configure command to setup SCC policies for FICON**

   Brocade_def:FID128:admin > switchdisable
   Choose a unique domain ID (20 in this example):
   Brocade_def:FID128:admin> configure
   Configure...
   Fabric parameters (yes, y, no, n): [no] y
   Domain: (1..239) [4] 20
   Disable device probing:
   Disable Device Probing: (0..1) [0] 1
   Leave E_D_TOV value at 2 seconds (2000) unless connected to extension equipment. In some cases, when connecting to extension equipment, it must be set to 5 seconds (5000):
   E_D_TOV: (1000..5000) [2000]
   The preferred practice is to set the domain ID to be insistent. Setting the insistent domain ID is required for two-byte addressing.
   Insistent Domain ID Mode (yes, y, no, n): [no] y

   **Note:** Before setting HIF mode, the following attributes must be configured:
   - An insistent domain ID (IDID)
   - A fabric-wide consistency policy → SCC:S (Strict mode)
   - A valid SCC_Policy (configured and activated)

   If one of these parameters is not configured, you get the following error message before enabling HIF:

   Error: Unable to set HIF Mode. No valid SCC policy or Fabric wide(SCC:S) configuration
Example 30 shows the configuration process.

**Example 30  Setting the insistent domain ID**

```bash
configure
Fabric parameters (yes, y, no, n): [no] y
High Integrity Fabric Mode (yes, y, no, n): [no] y
```

**Enable High-Integrity Fabric mode:**
```
configure
Fabric parameters (yes, y, no, n): [no] y
High Integrity Fabric Mode (yes, y, no, n): [no] y
```

```
HIF mode is enabled on the switch
```

Preferred implementation (all systems)

This section describes the preferred sequence for implementing the fabric resiliency features that are provided by FOS, and describes the preferred configuration values.

Enabling the Credit Recovery Tool

Enable the Credit Recovery Tool with the `link reset only` (LROnly) option. Options have changed with the different FOS releases, and some options are now hard-coded into the FOS, and other options do not apply to new hardware platforms.

Example 31 shows the `creditrecoverymode` command to enable credit tools and display the credit tools settings for FOS V7.3.

**Example 31  The creditrecoverymode command for FOS V7.3**

```bash
DCX1_SANA:FID16:dlutz> creditrecoverymode --cfg on onLROnly
DCX1_SANA:FID16:dlutz> creditrecoverymode --fe_crdloss on

DCX1_SANA:FID16:dlutz> creditrecoverymode --show
Internal port credit recovery is Enabled with LrOnly
LR threshold (not currently activated): 2
Fault Option (not currently activated): EDGEBLADE
C2 FE Complete Credit Loss Detection is Enabled
```
Example 32 shows the `creditrecovmode` command to enable credit tools and display the credit tools settings for FOS V7.4 and FOS V8.0.

**Example 32  The creditrecovmode command for FOS V7.4 and V8.0**

```
DCX1_SANA:FID16:dlutz> creditrecovmode --cfg on onLrOnly
DCX1_SANA:FID16:dlutz> creditrecovmode --fe_crdloss on
DCX1_SANA:FID16:dlutz> creditrecovmode --be_crdloss on
DCX1_SANA:FID16:dlutz> creditrecovmode --be_losync on

DCX1_SANA:FID16:dlutz> creditrecovmode --show
Internal port credit recovery is Enabled with LrOnly
LR threshold (not currently activated): 2
Fault Option (not currently activated): EDGEBLADE
C2 FE Complete Credit Loss Detection is Enabled
```

Example 33 shows the `creditrecovmode` command to enable credit tools and display the credit tools for FOS V8.1.

**Example 33  The creditrecovmode command for FOS V8.1**

```
F48a_Default:FID128:dlutz> creditrecovmode --cfg on onLrOnly
F48a_Default:FID128:dlutz> creditrecovmode --be_crdloss on
F48a_Default:FID128:dlutz> creditrecovmode --be_losync on
F48a_Default:FID128:dlutz> creditrecovmode --show
Internal port credit recovery is Enabled with LrOnly
Back end port Loss of Sync's Link Reset is Enabled with LrOnly
```

### Enable Fabric Performance Impact

On switches running FOS V7.3 or V7.4, enable Fabric Performance Impact (FPI). Switches running FOS V8.0 and higher will have FPI always enabled by default. Example 34 shows how to enable FPI.

**Example 34  Enabling FPI**

```
Brocade_def:FID128:admin > mapsconfig -enableFPImon
```

Example 35 shows how to verify whether FPI Monitoring is enabled.

**Example 35  Verifying that FPI Monitoring is enabled**

```
Brocade_def:FID128:admin > mapsconfig --show
Configured Notifications: RASLOG,SNMP,EMAIL,FENCE,SW_CRITICAL,SW_MARGINAL
Mail Recipient: Not Configured
FPI Monitoring: Enabled
Paused members :
===============
PORT :
CIRCUIT :
SFP :
```
Example 36 shows that FPI enabled/disabled is no longer displayed on the `mapsconfig` command, because FPI is always enabled in FOS V8.x.

**Example 36  FPI no longer displayed in FOS 8.x**

```
F48a_Default:FID128:dlutz> mapsconfig --show
Configured Notifications:
RASLOG,SNMP,EMAIL,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL
Mail Recipient: dlutz@ca.ibm.com
Paused members :
================
PORT :
CIRCUIT :
SFP :
```

---

**Enabling Monitoring Alerting Policy Suite**

On switches running FOS V7.2 or later, use the MAPS to monitor the switches over Fabric Watch. To ensure that consistent settings and policies are enabled on all switches in the fabric, use Network Advisor.

**Enabling Monitoring Alerting Policy Suite**

To enable MAPS, complete the following steps on switches running FOS V7.x. Switches running FOS V8.x have MAPS always enabled.

1. Log in to Network Advisor and click **Monitor → Fabric Vision → MAPS → Enable**.

   Figure 14 shows the Network Advisor menu options to enable MAPS.

![Network Advisor Monitoring Alerting Policy Suite Enable menu](image)

2. Select the switches that you want to enable MAPS on by selecting them in the Available Switches pane and click the right arrow to move them to the Selected Switches pane. After all of the switches that you want to enable MAPS on are selected, click **OK** to enable MAPS on those switches.
Figure 15 shows the Network Advisor MAPS enable switch selection window.

![Network Advisor MAPS enable switch selection](image)

**Figure 15** Network Advisor MAPS enable switch selection

Configure MAPS Actions

To configure MAPS Actions, complete the following steps:

1. After MAPS is enabled, click **Monitor → Fabric Vision → MAPS → Configure**.
   
   Figure 16 shows the Network Advisor menu options to open the MAPS configuration window.

   ![Network Advisor MAPS open Configure menu](image)

   **Figure 16** Network Advisor MAPS open Configure menu

2. In the MAPS Configuration window, select the switches on which to enable policy actions. To select multiple switches, hold the Ctrl key while selecting the switches. After the switches are selected, click **Actions**.
3. In the MAPS Policy Actions dialog box, select the **RAS Log Event**, **SNMP Trap**, **E-mail**, **Switch Status Marginal**, **Switch Status Critical**, and **SFP Status Marginal** check boxes, and for switches with FOS V7.4 and later, select **FPI Actions** and **SDDQ**. Click **OK**.

**Note:** Do not enable the Fence action.
Figure 18 shows the MAPS Policy Actions dialog box.

![MAPS Policy Actions Dialog Box](image)

**Figure 18** Network Advisor MAPS Policy Actions
Enable MAPS default policy
In the MAPS Configuration dialog box, expand the list of available policies for each of the switches. Select the `dft_conservative_policy` for each switch. To select a policy for each switch, hold the Ctrl key while selecting the policies. After policies for each switch are selected, click **Activate**. Figure 19 shows the MAPS Configuration dialog box with `dft_conservative_policy` selected.

Figure 19   Network Advisor MAPS Configuration with conservative policy selected

MAPS is now enabled with the default conservative policy.

Creating a custom MAPS policy for high availability fabrics
For switches that require strict monitoring to provide highly available fabrics, implement custom MAPS rules for the port and switch thresholds that are listed in the tables in this section by completing the following steps:

1. Create a custom MAPS policy by making a copy of the default moderate policy by running the `mapspolicy --clone` command, as shown in Example 37.

   Example 37   The mapspolicy clone command
   ```
   mapspolicy --clone dflt_moderate_policy -name IBM_Custom_policy
   ```

Port metrics
2. Create custom rules for the following port metrics, as shown in Table 8.

   Table 8   Custom MAPS port metrics threshold
<table>
<thead>
<tr>
<th>Type</th>
<th>Time</th>
<th>OP</th>
<th>RASLOG</th>
<th>Alert</th>
<th>Fence (host only)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3TXTX</td>
<td>min</td>
<td>ge</td>
<td>3</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>CRC</td>
<td>min</td>
<td>ge</td>
<td>10</td>
<td>20</td>
<td>40</td>
</tr>
<tr>
<td>CRC</td>
<td>hour</td>
<td>ge</td>
<td></td>
<td></td>
<td>240</td>
</tr>
</tbody>
</table>
3. Display existing rules in the newly created customer policy by running the `mapspolicy --show <policyname>` command, as shown in Example 38.

Example 38  The mapspolicy show command for default CRC metrics

```
F48a_Default:FID128:dlutz> mapspolicy --show IBM_Custom_policy | grep -i CRC
defALL_D_PORTSCRC_2 | ALL_D_PORTS(CRC/MIN>2) | RASLOG,SNMP,EMAIL |
defALL_D_PORTSCRC_D1000 | ALL_D_PORTS(CRC/DAY>1000) | RASLOG,SNMP,EMAIL |
defALL_D_PORTSCRC_H60 | ALL_D_PORTS(CRC/HOUR>60) | RASLOG,SNMP,EMAIL |
defALL_E_PORTSCRC_10 | ALL_E_PORTS(CRC/MIN>10) | RASLOG,SNMP,EMAIL |
defALL_E_PORTSCRC_20 | ALL_E_PORTS(CRC/MIN>20) | FENCE,DECOM,SNMP,EMAIL |
defALL_HOST_PORTSCRC_10 | ALL_HOST_PORTS(CRC/MIN>10) | RASLOG,SNMP,EMAIL |
defALL_HOST_PORTSCRC_20 | ALL_HOST_PORTS(CRC/MIN>20) | FENCE,DECOM,SNMP,EMAIL |
defALL_OTHER_F_PORTSCRC_10 | ALL_OTHER_F_PORTS(CRC/MIN>10) | RASLOG,SNMP,EMAIL |
defALL_TARGET_PORTSCRC_10 | ALL_TARGET_PORTS(CRC/MIN>10) | RASLOG,SNMP,EMAIL |
defALL_TARGET_PORTSCRC_5 | ALL_TARGET_PORTS(CRC/MIN>5) | RASLOG,SNMP,EMAIL |
defNON_E_F_PORTSCRC_10 | NON_E_F_PORTS(CRC/MIN>10) | RASLOG,SNMP,EMAIL |
defNON_E_F_PORTSCRC_20 | NON_E_F_PORTS(CRC/MIN>20) | RASLOG,SNMP,EMAIL |
```

4. Remove any existing default maps rules for metrics that are shown in the tables in this section by running the `mapspolicy --delrule` commands, as shown in Example 39.

Example 39  mapspolicy delrule for default CRC metrics

```
mapspolicy --delrule IBM_Custom_policy -rulename defALL_D_PORTSCRC_2
mapspolicy --delrule IBM_Custom_policy -rulename defALL_D_PORTSCRC_D1000
mapspolicy --delrule IBM_Custom_policy -rulename defALL_D_PORTSCRC_H60
mapspolicy --delrule IBM_Custom_policy -rulename defALL_E_PORTSCRC_10
mapspolicy --delrule IBM_Custom_policy -rulename defALL_E_PORTSCRC_20
mapspolicy --delrule IBM_Custom_policy -rulename defALL_HOST_PORTSCRC_10
mapspolicy --delrule IBM_Custom_policy -rulename defALL_HOST_PORTSCRC_20
mapspolicy --delrule IBM_Custom_policy -rulename defALL_TARGET_PORTSCRC_10
mapspolicy --delrule IBM_Custom_policy -rulename defALL_TARGET_PORTSCRC_5
mapspolicy --delrule IBM_Custom_policy -rulename defNON_E_F_PORTSCRC_10
mapspolicy --delrule IBM_Custom_policy -rulename defNON_E_F_PORTSCRC_20
```
5. Create custom rules by running the `mapsrule --create` command, and add these rules to the newly created custom policy, as shown in Example 40.

```
Example 40  mapsrule create for custom CRC metrics

mapsRule --create ALL_E_CRC_log -group ALL_E_PORTS -monitor CRC -op ge
           -timebase MIN -value 10 -action RASLOG -policy IBM_Custom_policy
mapsRule --create ALL_E_CRC_alert -group ALL_E_PORTS -monitor CRC -op ge
           -timebase MIN -value 20 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy
mapsRule --create ALL_TARGET_CRC_log -group ALL_TARGET_PORTS -monitor CRC -op ge
           -timebase MIN -value 10 -action RASLOG -policy IBM_Custom_policy
mapsRule --create ALL_TARGET_CRC_alert -group ALL_TARGET_PORTS -monitor CRC -op ge
           -timebase MIN -value 20 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy
mapsRule --create ALL_TARGET_CRC_fence -group ALL_TARGET_PORTS -monitor CRC -op ge
           -timebase MIN -value 40 -action RASLOG,EMAIL,SNMP,DECOM,FENCE -policy IBM_Custom_policy
mapsRule --createRoR ALL_HOST_CRC_ror -group ALL_HOST_PORTS -monitor
           -timebase HOUR -value 10 -action RASLOG,EMAIL,SNMP,DECOM,FENCE -policy IBM_Custom_policy
mapsRule --create ALL_D_PORTSCRC_3_log -group ALL_D_PORTS -monitor CRC -op ge
           -timebase MIN -value 3 -action RASLOG -policy IBM_Custom_policy
mapsRule --create ALL_D_PORTSCRC_D1500_log -group ALL_D_PORTS -monitor CRC -op ge
           -timebase DAY -value 1500 -action RASLOG -policy IBM_Custom_policy
mapsRule --create ALL_D_PORTSCRC_H90_log -group ALL_D_PORTS -monitor CRC -op ge
           -timebase HOUR -value 90 -action RASLOG -policy IBM_Custom_policy
```
Figure 20 shows the custom port metrics in Network Advisor policy editor.

**Switch Fabric**

6. As shown in Table 9, create custom rules for the following switch fabric metrics to alert on any E_Port down or fabric segmentation event.

<table>
<thead>
<tr>
<th>Type</th>
<th>Timebase</th>
<th>OP</th>
<th>RASLOG alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>EPORT_DOWN</td>
<td>min</td>
<td>ge</td>
<td>1</td>
</tr>
<tr>
<td>FAB_SEG</td>
<td>min</td>
<td>ge</td>
<td>1</td>
</tr>
</tbody>
</table>

7. Remove any existing default maps rules for metrics by running the `mapspolicy --delrule` commands, as shown in Example 41.

*Example 41*  
The `mapspolicy delrule` command for default switch fabric metrics

```bash
mapspolicy --delrule IBM_Custom_policy -rulename defSWITCHFAB_SEG_4
mapspolicy --delrule IBM_Custom_policy -rulename defSWITCHEPORT_DOWN_4
```
8. Create custom rules by running the `mapsrule --create` command, and add these rules to the newly created custom policy, as shown in Example 42.

```
Example 42  The mapsrule create command for custom switch fabric metrics

mapsRule --create SWITCH_EPORT_DOWN_alert -group SWITCH -monitor EPORT_DOWN -op ge -timebase MIN -value 1 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy
mapsRule --create SWITCH_FAB_SEG_alert -group SWITCH -monitor FAB_SEG -op ge -timebase MIN -value 1 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy
```

Figure 21 shows the custom switch fabric metrics in Network Advisor policy editor.

```
Figure 21   Network Advisor switch fabric policy editor
```

FPI

There can be many fabric performance impact events that you want to be aware of but that do not warrant real time alerting. Set up a set of custom FPI MAPS rules to only log FPI events for periodic review to identify congesting workloads, or for analysis of a performance issue.

9. Remove any existing default maps FPI rules by running the `mapspolicy --delrule` commands, as shown in Example 43.

```
Example 43  The mapspolicy delrule command for default FPI metrics

mapspolicy --delrule IBM_Custom_policy -rulename defALL_PORTS_IO_FRAME_LOSS_UNQUAR
mapspolicy --delrule IBM_Custom_policy -rulename defALL_PORTS_IO_LATENCY_CLEAR
mapspolicy --delrule IBM_Custom_policy -rulename defALL_PORTS_IO_PERF_IMPACT_UNQUAR
```

10. Create custom rules by running the `mapsrule --create` command, and add these rules to the newly created custom policy, as shown in Example 44.

```
Example 44  The mapsrule create command for custom FPI metrics for FOS V7.x

mapsRule --create FPI_IO_PERF_IMPACT_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_PERF_IMPACT -action RASLOG -policy IBM_Custom_policy
mapsRule --create FPI_IO_FRAME_LOSS_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_FRAME_LOSS -action RASLOG -policy IBM_Custom_policy
mapsRule --create FPI_IO_LATENCY_CLEAR_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_LATENCY_CLEAR -action RASLOG -policy IBM_Custom_policy
```
Figure 22 shows the custom FPI metrics in Network Advisor policy editor.

With FOS V8.x, the SDDQ un-quarantine action was added. This allows MAPS rules to be set up to automatically quarantine a congesting workload, and then have the quarantine removed after a given period of time, as shown in Example 45.

**Example 45** The mapsrule create command for custom FPI metrics for FOS 8.x

```bash
mapsRule --create FPI_IO_PERF_IMPACT_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_PERF_IMPACT -action RASLOG -policy IBM_Custom_policy
mapsRule --create FPI_IO_FRAME_LOSS_sddq -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_FRAME_LOSS -action RASLOG,SDDQ,UNQUAR -uqrt=30 -uqrt_unit min -policy IBM_Custom_policy
mapsRule --create FPI_IO_LATENCY_CLEAR_log -group ALL_PORTS -monitor DEV_LATENCY_IMPACT -op eq -timebase NONE -value IO_LATENCY_CLEAR -action RASLOG -policy IBM_Custom_policy
```

**FCIP**

Monitoring FCIP extension metrics is critical for the proper operation of FCIP tunnels.

11. Create a set of custom rules to log marginal FCIP tunnel behavior and alert when tunnel performance approaches impactive levels based on Table 10.

**Table 10** Custom maps FCIP metrics thresholds

<table>
<thead>
<tr>
<th>Type</th>
<th>Time</th>
<th>Op</th>
<th>RASLOG</th>
<th>Alert</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKTLOSS</td>
<td>min</td>
<td>ge</td>
<td>0.05</td>
<td>0.1</td>
</tr>
<tr>
<td>JITTER</td>
<td>min</td>
<td>ge</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>RTT</td>
<td>none</td>
<td>ge</td>
<td>see note</td>
<td>see note</td>
</tr>
</tbody>
</table>

12. Create custom rules by running the `mapsrule --create` command, and add these rules to the newly created custom policy for each of the QOS Circuit and Tunnel groups, as shown in Example 46.

**Example 46** mapsrule create for custom FCIP metrics

```bash
mapsRule --create ALL_CIRCUIT_MED_QOS_PKTLOSS_log -group ALL_CIRCUIT_MED_QOS -monitor PKTLOSS -op ge -timebase MIN -value 0.05 -action RASLOG -policy IBM_Custom_policy
```
mapsRule --create ALL_CIRCUIT_MED_QOS_PKTLOSS_alert -group ALL_CIRCUIT_MED_QOS -monitor PKTLOSS -op ge -timebase MIN -value 0.1 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy

mapsRule --create ALL_TUNNEL_MED_QOS_PKTLOSS_log -group ALL_TUNNEL_MED_QOS -monitor PKTLOSS -op ge -timebase MIN -value 0.05 -action RASLOG -policy IBM_Custom_policy

mapsRule --create ALL_TUNNEL_MED_QOS_PKTLOSS_alert -group ALL_TUNNEL_MED_QOS -monitor PKTLOSS -op ge -timebase MIN -value 0.1 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy

mapsRule --create ALL_CIRCUITS_JITTER_log -group ALL_CIRCUITS -monitor JITTER -op ge -timebase NONE -value 10 -action RASLOG -policy IBM_Custom_policy

mapsRule --create ALL_CIRCUITS_JITTER_alert -group ALL_CIRCUITS -monitor JITTER -op ge -timebase NONE -value 20 -action RASLOG,EMAIL,SNMP -policy IBM_Custom_policy

Figure 23 shows the custom extensions metrics in Network Advisor policy editor.

<table>
<thead>
<tr>
<th>Groups/Rules</th>
<th>Monitor Condition</th>
<th>Time Base</th>
<th>RAS Log Event</th>
<th>SNMP Trap</th>
<th>E-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL_CIRCUITS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>defALL_CIRCUITS_IP_UTIL_P_50</td>
<td>P_UTIL &gt; 90 %</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>defALL_CIRCUITS?url_PKTLOSS_PER_5</td>
<td>PKTLOSS &gt; 0.5 %</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>defALL_CIRCUITS?url_STATE_5</td>
<td>CIR_STATE &gt; 5</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>defALL_CIRCUITS?url_PKTLOSS_P_5</td>
<td>PKTLOSS &gt; 0.5 %</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS_JITTER_alert</td>
<td>Jitter &gt; 20 mSec</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>defALL_CIRCUITS?url_PKTLOSS_P_5</td>
<td>PKTLOSS &gt; 0.5 %</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>defALL_CIRCUITS?url_PKTLOSS_PER_90</td>
<td>CIR_UTIL &gt; 90 %</td>
<td>Min</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS?url_PKTLOSS_log</td>
<td>Jitter &gt;= 10 %</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS?url_PKTLOSS_alert</td>
<td>Jitter &gt; 20 %</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS?url_RTT_250</td>
<td>RTT &gt; 250 mSec</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS?url_JITTER_log</td>
<td>Jitter &gt; 10 mSec</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ALL_CIRCUITS?url_JITTER_alert</td>
<td>Jitter &gt; 20 %</td>
<td>None</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>

Figure 23  Network Advisor extensions policy editor
Creating dashboards

Complete the following steps:

1. Create Fabric Health and Ports dashboards with the widgets that are shown in Table 11.

   \[Table 11 \ Suggested \ Product \ Status \ and \ Ports \ dashboards \ widgets\]

<table>
<thead>
<tr>
<th>Dashboard name</th>
<th>Status widget</th>
<th>Performance widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Health</td>
<td>SAN Status</td>
<td>Top Product CPU</td>
</tr>
<tr>
<td></td>
<td>SAN Inventory</td>
<td>Top Product Memory</td>
</tr>
<tr>
<td></td>
<td>Events</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Out of Range Violations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Health Violations</td>
<td></td>
</tr>
<tr>
<td>Ports</td>
<td>Port Health Violations</td>
<td>Top Port C3 Discards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port C3 Discards TX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port CRC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port ITW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Too Long Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Port Utilization Percent</td>
</tr>
</tbody>
</table>

2. Optionally, create a Host, Storage, and ISL port dashboards (which can be useful when doing problem determination), as shown in Table 12.

   \[Table 12 \ Optional \ Host, \ Storage, \ and \ ISL \ dashboard \ widgets\]

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Status widget</th>
<th>Performance widget</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Ports</td>
<td>Initiator Port Health Violations</td>
<td>Top Initiator Ports C3 Discards</td>
</tr>
<tr>
<td></td>
<td>Initiator Bottleneck Ports</td>
<td>Top Initiator Ports CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Ports Encode Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port Sync Loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Initiator Port ITWs</td>
</tr>
<tr>
<td>Storage Ports</td>
<td>Target Port Health Violations</td>
<td>Top Target Ports C3 Discards</td>
</tr>
<tr>
<td></td>
<td>Target Bottleneck Ports</td>
<td>Top Target Ports CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Ports Encode Error</td>
</tr>
</tbody>
</table>
3. Create a dashboard by selecting the **My Dashboard** group and clicking **Add**.

Figure 24 shows the Network Advisor window that is used to add a dashboard.

![Network Advisor: Add dashboard](image)

<table>
<thead>
<tr>
<th>Dashboard</th>
<th>Status widget</th>
<th>Performance widget</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Top Target Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port Sync Loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top Target Port ITWs</td>
</tr>
<tr>
<td>ISL Ports</td>
<td>ISL Port Health Violations</td>
<td>Top ISL Ports C3 Discards</td>
</tr>
<tr>
<td></td>
<td>ISL Bottleneck Ports</td>
<td>Top ISL Ports CRC Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports Encode Error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Link Failures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Sync Loss</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Port Link Resets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports C3 Discards RX TO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Top ISL Ports C3 Discards TX TO</td>
</tr>
</tbody>
</table>
4. Enter the dashboard name in the Name entry field in the Add Dashboard dialog box and click OK.

Figure 25 shows the Add Dashboard dialog box.

![Add Dashboard](image)

**Figure 25  Network Advisor Add Dashboard dialog box**

5. Use the Customize Dashboard tool to add widgets to the empty dashboard.

Figure 26 shows the icon to start the Customize Dashboard tool.

![Customize Dashboard](image)

**Figure 26  Network Advisor Customer Customize Dashboard icon**

6. To add widgets to the dashboard, choose the required widgets by selecting the check box next to the widget titles.
Figure 27 shows the Customize Dashboard Status dialog box.

Figure 27  Network Advisor Customer Dashboard Status dialog box

7. Select the **Performance** tab to add performance widgets.

Figure 28 shows the Customize Dashboard Performance dialog box.

Figure 28  Network Advisor Customize Dashboard Performance dialog box
Figure 29 shows the completed dashboard with widgets.

Figure 29  Network Advisor Fabric Health dashboard

## Access gateway

BladeCenter and chassis-style systems typically have embedded switches that are installed in them. These switches can operate in native fabric mode or access gateway (AG) mode. AG mode uses NPIV to connect the devices in the chassis to the network instead of native fabric mode, which operates as a standard switch, requires its own fabric domain, and requires a copy of the name server and configuration databases. In AG mode, the embedded switch does not use any of these items.

Embedded switches can support trunking, which usually requires an optional license. Trunking allows transparent failover and failback within the trunk group. Trunked links are more efficient and can distribute I/O more evenly across all the links in the trunk group.

Run embedded switches in AG mode. For chassis with high throughput or high availability goals, use F_port trunking.

For more information, see the Brocade Access Gateway Administrator’s Guide:
http://my.brocade.com
Frame Viewer

Frames that are discarded are sent to the CPU for processing. During subsequent CPU processing, information about the frame, such as SID, DID, and transmit port number, is retrieved and logged. This information is maintained for a certain fixed number of frames.

Frame Viewer captures FC frames that are dropped. Depending on the hardware platform and FOS version, frames captured can be for different types, such as timeouts, un-routable, or unreachable destinations that are received on an Edge ASIC (an ASIC with front-end (FE) ports). If the frame is dropped on a Core ASIC, the frame is not captured by Frame Viewer.

By default, only the timeout frame type is enabled, if you are seeing high frame discards for other reasons, you might want to enable Frame Viewer to log other discard types to capture the source and destination address to help isolate the issue.

Example 47 shows the framelog command to show the frame viewer status.

Example 47  The framelog --status command output

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
</table>
| F48a_Default:FID128:dlutz> framelog --status | Service Status: Enabled  
Enabled Disc Frame Types: timeout du type1miss unroute type2miss type6miss |

Example 48 shows the framelog command to enable logging of different frame types on a GEN 5 switch running FOS V8.1.

Example 48  The framelog --enable command on a GEN5 switch

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type timeout</td>
<td>Nothing to do: service is already enabled.</td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type du</td>
<td></td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type unroute</td>
<td></td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type type1miss</td>
<td></td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type type2miss</td>
<td></td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type type6miss</td>
<td></td>
</tr>
<tr>
<td>F48a_Default:FID128:dlutz&gt; framelog --enable -type all</td>
<td>Nothing to do: service is already enabled.</td>
</tr>
</tbody>
</table>

Example 49 shows the framelog command to enable logging of different frame types on a GEN 4 switch running FOS V7.4.

Example 49  The framelog --enable command on a GEN 4 switch

<table>
<thead>
<tr>
<th>Command</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANA_DCX2:FID16:dlutz&gt; framelog --enable -type du</td>
<td>Error: Feature requested is not supported</td>
</tr>
<tr>
<td>SANA_DCX2:FID16:dlutz&gt; framelog --enable -type unroute</td>
<td></td>
</tr>
<tr>
<td>SANA_DCX2:FID16:dlutz&gt; framelog --enable -type all</td>
<td></td>
</tr>
</tbody>
</table>

Error: Feature requested is not supported |
Figure 50 shows the `framelog` command to show C3 frame Tx timeouts.

**Example 50  The framelog command output**

```
framelog --show -n 1200
========================================================================
========================================================================

<table>
<thead>
<tr>
<th>Log</th>
<th>TX</th>
<th>RX</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>port</td>
<td>port</td>
</tr>
<tr>
<td>-----</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>Sep 18 05:56:05</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Sep 18 05:56:04</td>
<td>9/46</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Sep 18 05:39:08</td>
<td>-1/-1</td>
<td>3/16</td>
</tr>
<tr>
<td>Sep 18 05:39:08</td>
<td>9/46</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Sep 04 05:21:56</td>
<td>9/46</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Sep 04 05:21:55</td>
<td>-1/-1</td>
<td>1/1</td>
</tr>
<tr>
<td>Aug 03 12:00:44</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Aug 03 12:00:44</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Aug 02 04:47:23</td>
<td>-1/-1</td>
<td>4/2</td>
</tr>
<tr>
<td>Aug 02 04:47:23</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Aug 02 04:47:23</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
<tr>
<td>Aug 02 04:47:23</td>
<td>2/22</td>
<td>-1/-1</td>
</tr>
</tbody>
</table>
```

**Forward Error Correction**

Brocade Gen5 (16 Gbps) platforms support Forward Error Correction (FEC) that automatically corrects bit errors. This function enhances the link reliability, and improves resiliency with the presence of marginal media. FEC is preferred between all supported devices. FEC is mandatory on Gen6 link (32 Gbps) speed.

FEC on Gen5 can correct up to 11-bit errors in every 2112-bit transmission in a 10 Gbps/16 Gbps data stream in both frames and primitives. FEC is enabled by default on the back-end (BE) links of Condor 3 ASIC-based switches and blades, and minimizes the loss of credits on BE links.

FEC is also enabled by default on FE links when connected to another FEC-capable device. FEC on Gen6 uses a more robust coding algorithm that corrects up to seven 10-bit streams and detects up to fourteen 10-bit streams, without the requirement that the errors be in a burst. FEC is mandatory on Gen6 platforms for 32 Gbps speed to ensure that the bit-error rate stays within the standard requirement. Condor 4 ASIC automatically turns on FEC when a port operates at 32 Gbps speed, and cannot be disabled.

Enable FEC on 10 Gbps/16 Gbps connections when both ends of the link support it.
Authors

This paper was produced by a team of specialists from around the world, working at the IBM International Technical Support Organization. The content is based on Brocade documentation and is presented in a form that specifically identifies IBM preferred practices.

**Jim Blue**
IBM Systems

**David Lutz**
IBM Systems

**Ian MacQuarrie**
IBM Systems

**Serge Monney**
IBM GTS

This project was managed by:

**Jon Tate**
IBM ITSO

Special thanks to Brocade for their support of this paper in terms of equipment and support in many areas, and to the following people at Brocade:

Silviano Gaona, Tom Chen, Brian Steffler

Now you can become a published author, too

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time. Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)
Stay connected to IBM Redbooks

- Find us on Facebook:
  http://www.facebook.com/IBMRedbooks
- Follow us on Twitter:
  http://twitter.com/ibmredbooks
- Look for us on LinkedIn:
  http://www.linkedin.com/groups?home=&gid=2130806
- Explore new IBM Redbooks® publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM’s future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided “AS IS”, without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.
Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Algo®  Redpaper™  z/OS®
C3®      Redbooks (logo)®  z13®
IBM®     z Systems®

The following terms are trademarks of other companies:

Other company, product, or service names may be trademarks or service marks of others.