

This section describes how to use FACT.

Contents

- [1 Scanning](#)
- [2 Maintaining the Repository](#)
- [3 Showing Network Information](#)
- [4 Using Annotation](#)
- [5 Using Port Counters](#)
- [6 Installing Firmware with FACT](#)
 - ◆ [6.1 Installing Firmware in Managed Switches](#)
 - ◆ [6.2 Installing Firmware in Unmanaged Switches](#)

Scanning

Before FACT can perform other network tasks, you must first scan the network to determine which hosts and switches are in the network and to determine how they are connected. FACT scans an entire subnet at the same time, connecting to each managed Cisco switch and, optionally, to each port.

FACT has four scan types:

- **Fabric scan**--Finds the static configuration of the network. After collecting a fabric scan, FACT can display the network components and show how they are connected.
- **Tech-support scan**--Collects information that can be forwarded to a customer-support organization. A tech-support scan includes a fabric scan, which FACT can use, although FACT does not use the additional information. FACT saves that information for an expert to inspect.
- **Port-counters scan**--Collects port counters from the Performance Manager, in addition to the data collected in a fabric scan. See [Using Port Counters](#) for more information.
- **Incomplete scan**--A scan that has failed, either because of misconfiguration or because devices are not responding. The most common reason for an incomplete scan is either because the configuration does not include the device that is running the master Subnet Manager or because it includes two master Subnet Managers. In either case, change your configuration so that it includes exactly one master Subnet Manager. Alternately, you can force FACT to use the correct master Subnet Manager by setting *subnet-manager:* in the `.fact.conf` file or with the **subnet-manager hostname** command option.

Note: If you are using the High-Performance Subnet Manager, then you must allow FACT to scan the hosts running HSM.

You can use the `--trace` command option to show FACT communication with each managed node as it scans.

Use the following commands to scan with FACT:

- **scan fabric**
- **scan tech-support**

Maintaining the Repository

FACT maintains a repository that contains the results of past scans. FACT considers the last-performed scan in the repository as the current scan, which it uses for queries, annotations, port control, and firmware upgrades. Whenever you scan the network, the new scan becomes the current scan, although the repository has a history mechanism that allows the current scan to be rolled back to an earlier version.

By default, the repository is located at \$HOME/.fact.

Use the **show history** command to view all scans. Each scan has an index number that you use to select any particular scan. Use the **select** command to change the current scan.

The following example shows that the current scan is scan 6, as designated by the letter ?Y?:

```
$ fact
fact> show history
index current type          date          subnet-manager
-----
1      fabric      2007-12-27 19:37:25 PST  ibmg-r1-120-1
2      fabric      2007-12-27 19:39:28 PST  ibmg-r1-360-1
3      fabric      2008-01-03 17:09:51 PST  kbob-s1
4      fabric      2008-01-03 20:14:50 PST  209.165.200.225
5      fabric      2008-01-08 15:30:29 PST  kbob-s1
6      Y fabric      2008-01-08 15:33:52 PST  kbob-s1
fact>
```

From the current scan shown in the previous example, the following example shows selecting scan 4:

```
$ fact
fact> select 4
fact> show history
index current type          date          subnet-manager
-----
1      fabric      2007-12-27 19:37:25 PST  ibmg-r1-120-1
2      fabric      2007-12-27 19:39:28 PST  ibmg-r1-360-1
3      fabric      2008-01-03 17:09:51 PST  kbob-s1
4      Y fabric      2008-01-03 20:14:50 PST  209.165.200.225
5      fabric      2008-01-08 15:30:29 PST  kbob-s1
6      fabric      2008-01-08 15:33:52 PST  kbob-s1
fact>
```

You can delete old scans by selecting the scan number from the index and using the **delete scans** command. The following example shows deleting the first three scans from the list in the previous example:

```
$ fact
fact> delete scans 1-3
Proceed with scan delete [Y/n]? y
fact> show history
index current type          date          subnet-manager
-----
1      Y fabric      2008-01-03 20:14:50 PST  209.165.200.225
2      fabric      2008-01-08 15:30:29 PST  kbob-s1
3      fabric      2008-01-08 15:33:52 PST  kbob-s1
fact>
```

Note: After you deleted scans 1 through 3, the scans that were previously listed as scans 4, 5, and 6 have remained, but they have now moved up in the index to become scans 1, 2, and 3.

You can export the current scan to a file with the **export scan** command, or you can export the entire repository with the **export repository** command. Similarly, you can import a scan with the **import scan** command or the import the entire repository with the **import repository** command.

If you need assistance in troubleshooting your network, you can use the **export repository** command. You can export the repository, save it to your specified location, and then make a copy to send to technical support.

You can clean out your repository with the **delete scans** command.

Note: Importing a repository deletes your existing repository and replaces it with the new repository that you import.

Use the following commands to maintain and manage your repository:

- **show history**
- **select**
- **export scan**
- **export repository**
- **import repository**
- **import scan**
- **delete scans**

Showing Network Information

Use the FACT **help** command to list all commands that are available. Generally, each query has several different output formats. The common formats are summary, guides, and detail.

The notation "someswitch/M/N" is called a chassis-view port name. The notation shows port N on slot M of chassis someswitch. The notation "someswitch/L:M/N" is a chip-view port name. The notation shows port N on chip M of slot L of chassis someswitch. Some switches require a mapping between external port numbers and chip-level port numbers. The chassis view uses external port numbers, and the chip view uses internal port numbers.

Note: The colon character (":") appears only in the chip view, so its appearance in a string indicates that the string is in chip view notation.

The show ports command shows the ports and also the port neighbors of each port. If a port has no current neighbor, the last-known neighbor is shown. Last-known neighbors appear in square brackets ("[...]").

Using Annotation

When a file is annotated, FACT searches it for numeric constants and presents network components. It adds an annotation to each numeric constant, showing a human-readable name for that component.

FACT_Scanning

FACT can annotate a log file or any file. When a file is annotated, FACT appends each GUID with a short explanation of what that GUID represents, as shown in the following example of an original log:

A port GUID is changed from this

```
00:00:00:00:00:00:00:00
```

to this:

```
00:00:00:00:00:00:00:00 (switch03/4/5, switch03/4:6/7, neighbor=switch12/2/3)
```

The preceding example shows the port chassis view and chip view, followed by the neighbor chassis view and chip view.

A node GUID is changed to this:

```
00:00:00:00:00:00:00:00 (switch03/4:6)
```

A chassis GUID is changed to this:

```
00:00:00:00:00:00:00:00 (switch03)
```

A LID is changed to this:

```
23 (switch03/4/0, switch03/4:6/0, 00:00:00:00:00:00:00:00)
```

A port GUID is changed to this:

```
ff:12:60:1b:ff:ff:00:00:00:00:00:00:01:ff:33:2b:52 (switch03/4/0, switch03/4:6/0, neighbor=host14/1/1)
```

A Python source file, `/usr/local/cisco/fact/annotation.py`, contains sets of regular expression patterns for identifying interesting messages, for identifying messages containing node, chassis and port GUIDs and LIDs. Advanced users can edit that file to customize the syslog output.

[Add output here]

You can use the annotation as an element in a UNIX shell pipeline to annotate GUIDs in any command output, as shown in the following example:

```
$ ibtstat | fact annotate /dev/stdin
```

You can pass an entire syslog through FACT annotation, as shown in the following example:

```
$ fact annotate follow /var/logs/messages
```

If you do not provide a specific file with the annotate command, FACT looks for log-file parameters in the master configuration file.

Note: Annotation always uses the current scan.

Using Port Counters

InfiniBand switch chips maintain a set of counters for each port. These counters count the occurrence of various types of errors. You can use FACT to collect and display port counters.

FACT can collect three types of port counter scans:

- **Raw**?The Subnet Manager does not need to be configured to collect raw port counters. FACT tells the Subnet Manager to enter every switch chip in the subnet to collect its port counters.
- **Monitored**?The Subnet Manager must be configured to collect monitored port counters. The Subnet Manager can be configured to monitor specified counters or all counters.
- **Threshold**?The Subnet Manager must be configured to collect threshold port counters. The threshold scan collects just those monitored port counters that have exceeded their error thresholds.

For information about configuring the Subnet Manager, see the `ib pm` command in the Cisco SFS Product Family Command Reference at this URL:

http://www.cisco.com/en/US/docs/server_nw_virtual/2.10.0_release/command/reference/cli210.html

For information about configuring the High-Performance Subnet Manager, see the **config pm monitored state** command and the **config pm threshold** command in the *Cisco High-Performance Subnet Manager for InfiniBand Server Switches User Guide* at this URL:

http://www.cisco.com/en/US/products/ps6985/products_installation_and_configuration_guides_list.html

FACT can scan the port counters in a network. Viewing the port counters is a three-stage process:

1. Reset counters with the `reset port-counters` command. FACT records the reset in the scan history, which you can view later with the `show history` command.
2. Scan the counters (wait a minimum of 60 seconds or longer for errors to occur). For more information about the port-counters scan, see the `?Scanning?` section.
3. Show the port counters. To show the port counters or to restrict the output to those counters that are non-zero, use the **show counters** commands.

Consult the *Cisco High Performance Subnet Manager for InfiniBand Server Switches User Guide* or the *Cisco SFS Product Family Command Reference* for information about configuring port counter monitoring with the Cisco InfiniBand Subnet Manager.

Use the following commands to use port counters:

- **reset port-counters**
- **show counters monitored**
- **show counters raw**
- **show counters threshold**

Installing Firmware with FACT

You can use FACT to install firmware on Cisco Server Fabric Switches running SFS OS, both on managed and unmanaged switches. Likewise, you can install firmware either on a single switch or on multiple

FACT_Scanning

switches simultaneously. (This firmware upgrade feature is not available for the OEM switches: Cisco SFS 7012 or Cisco SFS 7024.)

Note: Because each firmware image is for a specific switch model, if you upgrade firmware on multiple switches simultaneously, all switches must be of the same model for which the firmware file is intended. FACT returns an error message if the firmware image does not match the switch model.

Installing Firmware in Managed Switches

To install firmware on a managed Cisco Server Fabric Switch, perform the following steps:

Step 1 Log in to the host as a superuser.

Step 2 Enter the **install** command to obtain and install the new firmware image. For an SFS OS switch, FACT instructs the switch to download the firmware from an FTP server, which you must set up in advance. The path argument must be an FTP URL with the following syntax:

```
ftp://user:password@host/path/file
```

Step 3 FACT checks the firmware on each switch that you want to upgrade and prints version numbers to the screen, grouped by version number. FACT then asks for confirmation. Confirm the version by typing **y**. FACT installs the new firmware on all specified switches.

Note: When you install firmware on an SFS OS switch that is configured to be the master Subnet Manager, wait for at least one minute after the installation for the Subnet Manager to take control of the subnet before rescanning the fabric, or the scan fails and no master Subnet Manager is found.

The following example shows an SFS OS firmware upgrade from build 137 to build 154 on switches 1 through 2. The example shows that while the user attempted to upgrade switch 3, FACT determined that switch 3 was already running the updated build, and FACT disregarded the installation:

```
$ fact
fact> install switch[1-3] from
ftp://user:passwd@host/path/Topspin90-TopspinOS-2.8.0-build154.img
Checking switch1
Checking switch2
Checking switch3
These switches are running TopspinOS 2.8.0 build 137:
    switch1
    switch2
These switches are running TopspinOS 2.8.0 build 154:
    switch3
Install [Y/n]?y
Installing switch1
Installing switch2
Skipping switch3
Waiting for switch1
Waiting for switch2
Waiting for switch3
switch1 rebooted
switch2 rebooted
```

FACT_Scanning

```
switch3 rebooted
Rescan fabric to update switch versions
```

Step 4 Enter the **scan fabric** command so that FACT can learn the current version that the switches are running.

Step 5 Enter the **show versions** command to ensure that the correct version appears in the output.

Installing Firmware in Unmanaged Switches

For unmanaged switches, FACT uses the ibspark tool to install firmware. The ibspark tool transmits the firmware through InfiniBand to the switch, so the tool must run on a host that is directly connected to the InfiniBand network. However, ibspark is not required to reside on the same host as FACT. FACT can use SSH to reach the host with ibspark. (For information about obtaining the ibspark tool, see [Obtaining and Installing Optional Software Tools](#) .) (For information about configuring FACT to use ibspark, see [About Master Configuration Files](#).)

To install firmware on an unmanaged Cisco Server Fabric Switch, perform the following steps:

Step 1 Log in to the host as a superuser.

Step 2 Enter the **install** command to obtain and install the new firmware image. For an unmanaged switch, the file parameter is a regular firmware image file. A firmware image file ends in .img.

Step 3 FACT checks the firmware version on each switch that you want to upgrade and prints the version numbers to the screen, grouped by version number. FACT then asks for confirmation.

Confirm the version by typing **Y**. FACT installs the new firmware on all specified switches.

The following example shows a firmware upgrade on unmanaged switches 4 through 6:

```
$ fact
fact> install switch[4-6] from somefile.img
Checking switch4
Checking switch5
Checking switch6
These switches are running version 1.2.3:
    switch4
    switch5
Install [Y/n]?y
Installing switch4
Installing switch5
Skipping switch6
Switches are rebooting. Rescan fabric after network stabilizes.
fact>
```

Step 4 Enter the **scan fabric command** so that FACT can learn the current version that the switches are running.

Step 5 Enter the **show versions** command to ensure that the correct version appears in the output.