Release Notes for Cisco Global Site Selector, Release 1.0

August 12th, 2002

Contents

These release notes contain information about the Cisco Global Site Selector (GSS) Software, Version 1.0. It describes the following topics:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

Cisco's Cisco Global Site Selector (GSS) is a next-generation networking product that allows customers to leverage global content deployment across multiple distributed and mirrored data locations, optimizing site selection, improving DNS responsiveness, and assuring data center availability.

Inserted into the traditional DNS routing hierarchy and closely integrated with your Cisco- or third party server load balancers (SLBs), the GSS monitors the health and load of the SLBs in each of your data centers, then uses that information along with customer-controlled routing algorithms to select the best suited and least loaded data center in real time.

The GSS is capable of detecting site outages, ensuring that Web-based applications are always online and that customer requests to data centers that go offline are quickly re-routed to available resources.

Finally, the GSS off-loads tasks from traditional DNS servers by fronting for part, or all of your domain name space. Capable of transmitting requests at a rate of thousands of requests per second, the GSS greatly improves DNS responsiveness to those sub-domains.

The Cisco Global Site Selector offers the following key capabilities:

- Disaster recover—the GSS can detect and instantaneously route requests around site outages.
- Improved site performance—in multiple datacenter deployments, the GSS speeds up the selection process through the application of state-of-the-art load balancing algorithms that take the load and health of Cisco- and third party SLBs into account when routing requests.
- Scalability—the GSS is capable of scaling to support hundreds of separate data centers and SLBs, while working seamlessly with a heterogeneous mixture of SLBs including Cisco- and third party devices.
- Improved DNS performance—inserted into the traditional DNS hierarchy, the GSS off-loads traffic from DNS servers, becoming the authoritative DNS server for some (or all) of your domain name space.
- Centralized domain management—through an easy-to-use graphical user interface, the Global Site Selector Manager, administrators can manage quickly configure their GSS network as well as monitor the health and performance of request routing across their entire GSS network.

These release notes provide the information on issues related to the release of Cisco Global Site Selector Version 1.0, as well as a list of known issues at the time of release.

System Requirements

This section describes the hardware and software components, including third-party applications, that are used by the Cisco Global Site Selector.

Cisco-Supported Hardware

Cisco Global Site Selector operates with the following Cisco hardware:

- Cisco Global Site Selector 4480
- Cisco Content Services Switch running WebNS software Version 5.0 or higher
- Cisco Catalyst 6000/6500 Content Switching Module Version 2.2(3) or higher

Refer to the Cisco documentation that came with each device for detailed, device-specific instructions on handling, installing, and configuring your Cisco hardware.

Software Compatibility

For the beta release of GSS Version 1.0, the following upgrade sequences are supported:

1.0.0.0.17 —>1.0.0.25

Upgrading to a New Software Release

The following sections explain the steps that must be taken to upgrade your GSS software, or to enable a new installation of the GSS software.

1. Configuring your GSS device network settings (new installations only)
2. Determining the current software version (existing installations only)
3. Performing a full backup of your primary GSSM (existing installations only)
4. Obtaining the software update (existing installations only)
5. Upgrading the software on your GSS devices (existing installations only)
6. Verifying your upgrade (existing installations only)
7. Starting the GSSM software and enabling the GUI

Step 1—Configure Network Settings

If you have not already done so, follow instructions for unpacking and mounting your Global Site Selector 4480 hardware. Refer to the *Cisco Global Site Selector 4480 Hardware Installation Guide* for instructions on setting up your Cisco hardware.

Once your hardware is properly installed and running, refer to the "Network Configuration" section in "Chapter 2: Getting Started" of the *Cisco Global Site Selector Configuration Guide* for detailed instructions on configuring your GSS device network settings.

If you have already configured network settings on your GSS devices, proceed to "Step 2—Determine the Current Software Version".

If this is a new GSS software installation, proceed to "Step 7—Start the GSSM Software and Enable the GUI".

Step 2—Determine the Current Software Version

Before attempting to upgrade to a new software version, first verify which version of the GSS software you are running. Confirming the current software version will help you determine:

- If an upgrade is necessary
- If there is a direct upgrade path between the software version you are running and the version to which you are upgrading

You can determine the software version running on any of your GSS devices either by logging in to those devices directly and using the CLI show version command, or by accessing the Global Site Selectors page on your GSSM GUI.

Determining the Current Software Version from the CLI

To determine the current software version using the CLI:

Step 1 Log on to the CLI of your GSSM, following the instructions in the *Cisco Global Site Selector Command Reference*. The Cisco CLI prompt will appear.

Step 2 Enable Privileged EXEC mode, for example:

```
gss1.yourdomain.com>enable
gss1.yourdomain.com#
```

Step 3 Use the show version command to display the software version, for example:

```
gss1.yourdomain.com#show version
Global Site Selector (GSS)
Copyright (c) 1999-2002 by Cisco Systems, Inc.
Version 1.0(0.22.3)
Compiled Tue Jul  9 16:56:08 2002 by atripath - changeset 25175
uptime is 5 Days 2 Hours 31 Minutes and 18 seconds
Model Number: GSS-3380-K9
```

Determining the Current Software Version from the GSSM GUI

If you have already configured your primary GSSM, you can use the GSSM GUI to verify the current software version being used on any of your configured GSS devices.

To use the GSSM GUI to verify the software version:

Step 1 From the GSSM GUI, click the **Resources** button.

Step 2 From the drop-down list, choose **Global Site Selectors**. The Global Site Selectors list page appears.

Step 3 Click the edit icon for the GSS device you will be upgrading. The details page for the GSS device appears.

Step 4 Under the heading **Node Information**, look for the **Version** field. The number in this field is the software version being used by the device.

Step 5 Click **Cancel** to return to the Global Site Selectors list page.

Step 3—Back up the GSSM

Before you attempt to upgrade your GSS software, first make sure that you have a full backup of your GSSM that is current. That way, should the upgrade fail for some reason, you will be able to quickly restore your GSS network to its current state.

You can perform a full backup at any time. Doing so will not interfere with the functioning of the GSSM or any of your other GSS devices.

Note Performing a full backup of the GSSM requires access to the CLI.

To perform a full backup of your GSSM:

Step 1 Log on to the Cisco command line interface (CLI) of your GSSM, following the instructions in the *Cisco Global Site Selector Command Reference*. The Cisco CLI prompt will appear.

Step 2 Enable Privileged EXEC mode, for example:

```
gss1.yourdomain.com>enable
gss1.yourdomain.com#
```

Step 3 Use the **gssm**- command to create a full backup of your GSSM. You will need to supply a file name for your full backup. For example:

```
gss1.yourdomain.com#gssm backup full gssfullbk
GSSM database backup succeeded [gssfullbk.full]
```

Step 4 After you have received confirmation that the GSSM has successfully created your full backup, copy or move the file off your GSSM to ensure that it is not also lost in the event of a media failure or other catastrophic loss on your GSSM.

Either the secure copy (SCP) or FTP commands can be used to move your full backup to a remote host, for example:

```
gss1.yourdomain.com#scp gssfullbk.full server.yourdomain.com:home
```

Step 4—Obtain the Software Upgrade

Before you can update your Cisco GSS Software, you must first acquire the appropriate software update file from Cisco.

In order to acquire the software update from Cisco, you must first:

- Access the Cisco.com website and locate the software update files.
- Download the software update files to a server within your own organization that is accessible via FTP or SCP from your GSSs and GSSMs.

You must have a Cisco.com username and password before attempting to download a software update from Cisco.com. In order to acquire a Cisco.com login, go to http://www.cisco.com and click the **Register** link.

Note You need a service contract number, Cisco.com registration number and verification key, Partner Initiated Customer Access (PICA) registration number and verification key, or packaged service registration number in order to obtain a Cisco.com username and password.

To add an update file for the Cisco GSS:

Step 1 Launch your preferred web browser and point it to the Cisco Global Site Selector download page.

Step 2 When prompted, log in to Cisco.com using your designated Cisco.com username and password.

The Cisco GSS Software download page appears, listing the available software updates for the Cisco GSS Software product.

Note Each software update consists of two files: a binary-format update file (*.upg) and a smaller meta file (*.meta). Only the UPG file must be downloaded in order to successfully complete a Cisco GSS Software update. The META file contains the version number and the size of the upgrade file and can be used for verification of file integrity.

Step 3 Locate the files you wish to download by referring to the Release column for the proper release version of the software.

Step 4 Click the link for the UPG file. The download page appears.

Step 5 Click the Software License Agreement link. A new browser window will open displaying the license agreement.

Step 6 After you have read the license agreement, close the browser window displaying the agreement and return to the Software Download page.

Step 7 Click the filename link labeled **Download**.

Step 8 Click **Save to file** and then choose a location on your workstation to temporarily store the UPG upgrade file.

Step 9 Post the file you downloaded UPG file to a designated area on your network that is accessible to all your GSS devices.

Step 10 Repeat Step 3 through Step 9 for the META file, if you wish.

Step 5—Upgrade your GSS Devices

When executing an upgrade, you use the CLI **install** command.

Before going forward with the installation of the software upgrade, the **install** command also validates the upgrade file, then unpacks the upgrade archive and installs the updated software. Finally, the affected GSS device is stopped and restarted.

Note Upgrading your GSS devices will cause a temporary loss of service for each affected device.

To upgrade the GSS software on a Global Site Selector:

Step 1 Log on to the Cisco command line interface (CLI) of your Global Site Selector, following the instructions in the *Cisco Global Site Selector Command Reference*. The Cisco CLI prompt will appear.

Step 2 If you have not already done so, use the FTP command to copy the GSS software upgrade file from the network location to which you downloaded it from Cisco.com to a directory on the current Global Site Selector. For example, to copy an upgrade file named *gss.upg* from a remote host, your FTP session might look like the following:

```
gss1.yourdomain.com>ftp host.yourdomain.com
Connected to host.yourdomain.com.
220 host.yourdomain.com FTP server (Version wu-2.6.1-0.6x.21) ready.
Name (host.yourdomain.com:root): admin
331 Password required for admin.
Password:
230 User admin logged in.  Access restrictions apply.
Remote system type is UNIX.
```

```
Using ascii mode to transfer files.
ftp> binary
ftp> get
(remote-file) gss.upg
(local-file) gss.upg
local: gss.upg remote: gss.upg
200 PORT command successful.
...
```

Step 3 Enable Privileged EXEC mode, for example:

```
gss1.yourdomain.com>enable
gss1.yourdomain.com#
```

Step 4 Use the install- command to install the upgrade. For example:

```
gss1.yourdomain.com#install gss.upg
Performing software install. This will take a few minutes.
Device will reboot when the install is complete.
```

The GSS device will reboot, causing you to lose any network CLI connections. Console connections will remain active.

Step 5 Once the GSS device has rebooted, see the"Step 6—Verify Your Upgrade" section to determine whether the upgrade completed successfully.

Step 6—Verify Your Upgrade

Use the following procedure to log on to your upgraded GSS device and verify that the upgrade completed successfully.

Step 1 Log on to the Cisco command line interface (CLI) of your Global Site Selector, following the instructions in the *Cisco Global Site Selector Command Reference*. The Cisco CLI prompt will appear.

Step 2 Enable Privileged EXEC mode, for example:

```
gss1.yourdomain.com>enable
gss1.yourdomain.com#
```

Step 3 Use the **show version** command to verify that the intended software version has been successfully installed, for example:

```
gss1.cisco.com#show version
Global Site Selector (GSS)
Copyright (c) 1999-2002 by Cisco Systems, Inc.

Version 1.0(0.22.3)

Compiled Tue Jul  9 16:56:08 2002 by atripath - changeset 25175
uptime is 5 Days 2 Hours 31 Minutes and 18 seconds
Model Number: GSS-3380-K9
```

Step 4 Next, use the **gss status** command to verify that the device is running and confirm that the installed software version is correct, for example:

```
gss1.yourdomain.com>gss status
Cisco GSS(1.0.0.22.3) GSSM - primary [Mon May 20 13:46:21 GMT 2002]

Normal Operation [runmode = 5]

%CPU %MEM START   PID SERVER
```

```
0.0  0.3 May17   813          system
0.0  0.4 May17  1079      postgresql
0.0  1.6 May17  1083          tomcat
0.0  0.1 May17  1353          apache
0.0  2.2 May17  1092      controller
0.0  1.7 May17  1109      CrDirector
0.0  0.1 May17  1110        selector
0.0  0.1 May17  1122            kale
0.0  0.0 May17  1140        boomserv
0.0  1.7 May17   937         nodemgr
0.0  0.0 May17   304         syslogd
---  ---   ---   ---           snmpd [DISABLED]
---  ---   ---   ---       ucd-snmpd [DISABLED]
```

Step 7—Start the GSSM Software and Enable the GUI

After you have enabled your GSS devices, you must start the GSS software before the device will begin acting as a GSSM or GSS, and before you will be able to access the GSSM GUI.

To start the GSS software on your GSS devices:

Step 1 Log on to the Cisco command line interface (CLI) of the GSSM, following the instructions in the *Cisco Global Site Selector Command Reference*. The Cisco CLI prompt will appear.

Step 2 Enable Privileged EXEC mode, then Global Configuration mode on the device, for example:

```
gss1.yourdomain.com>enable
gss1.yourdomain.com#config
gss1.yourdomain.com(config)#
```

Step 3 Use the **gss start** command to start the GSS software, for example:

```
gss1.yourdomain.com(config)#gss start
```

You can now access the GSSM GUI using your preferred Web browser by pointing that browser to the URL of the GSSM.

If you have not already done so, log on to the GSSM graphic user interface (GUI) and use the features provided to begin configuring content routing.

Refer to the “Global Server Load Balancing Configuration” section in “Chapter 2: Getting Started” of the C*isco Global Site Selector Configuration Guide* for detailed instructions on using the features of the GSSM to configure request routing and global server load balancing using the GSS.

Caveats

This section describes the caveats that are known to exist with at the time of release of the Cisco Global Site Selector Version 1.0.

Open Caveats

The following caveats are open (unresolved). Unresolved caveats are listed according to their tracking number.

- CSCdx91076

  Symptom: Keepalives are in an incorrect state (INIT, OFFLINE), or show many transitions.

  Condition: The GSSM GUI should enforce a limit of 512 unique keepalives each for the ICMP and HTTP-HEAD keepalive types. It does not currently do this. Configuring more than 512 HTTP-HEAD or more than 512 ICMP keepalives causes the keepalive subsystem to operate incorrectly, and will affect the behavior of other subsystems.

  Workaround: There is no workaround. The user must make sure that these limits are not exceeded.

- CSCdx58395

  Symptom: CAPP may not recognize dropped fragments when KAL-AP spans multiple packets

  Condition: When the KAL-AP keepalive spans multiple datagrams due to large payloads, if one of the spanned packets is dropped, the GSS does not 'retry' the request. Instead. the GSS waits until the next period and sends the packets again. This results in the dropped datagram not getting updated load values on the VIPs that expect them.

  Workaround: This behavior only occurs in situations where the GSS consumes the full datagram (roughly 1.4K) with tag names, or vips. Otherwise all data fits in one single datagram. In situations where there is the need to query hundreds of VIPs associated with a single primary and secondary keepalive, utilize the KAL-AP by VIP option. Alternatively, use the KAL-AP by Tag option, but limit the length of tag names so that the packets do not grow beyond 1.4K.

- CSCdx68188

  Symptom: Load is sometimes missing in output from **show statistics kale kalap list** CLI command

  Condition: When issuing the **show statistics keepalive kalap list** CLI command, a list of all VIPs (virtual internet protocols) will be displayed with their load values in parenthesis. However if a load value is not yet known (or has the value of zero) the load will not be displayed at all, for example:

  ```
  10.1.1.147:ONLINE(235)
  10.1.1.156:ONLINE(251)
  10.1.1.157:ONLINE(253)
  10.1.1.158:ONLINE
  10.1.1.159:ONLINE(20)
  ```

  Workaround: There is no workaround. The VIP displays 'no load' because it may not have been obtained or the remote host is not sending a value between 2 and 254.

- CSCdx54156

  Symptom: Customers viewing GSSM GUI through Netscape Navigator aren’t forced to select Answer type first when creating a new answer.

  Condition: Customers viewing the GSSM GUI using Netscape Navigator aren’t forced to select an answer type before configuring their answer. As a result, customers have to re-enter answer information to complete the operation.

  Workaround: No workaround. The GSSM GUI prompts the user to re-enter missing fields if answer type is not selected when the user clicks **Save**.

- CSCdx64544

  Symptom: Web clients issue security warning to user while logged in to active GSSM GUI session.

Condition: SSL certificates contain the hostname of the GSSM at the time the device is enabled, but are not updated if the hostname subsequently changes. As a result, Web clients to issue a warning to the GSSM user during login.

Workaround: Use the following procedure to work around this issue:

- Log on to the CLI of the primary GSSM and perform a database backup of the device, for example:

```
gss1.yourdomain.com# gssm backup database <backup_filename>
```

- Copy the backup file off the GSSM.
- Restore the GSSM to factory settings, for example:

```
gss1.yourdomain.com# restore-factory-defaults
```

- Reconfigure GSSM network connectivity using the CLI.
- Copy the backup file back to the GSSM.
- Configure the device as a GSSM, for example:

```
gss1.yourdomain.com# gssm database create
gss1.yourdomain.com# gss enable gssm-primary
```

- Restore the backup file, for example:

```
gss1.yourdomain.com# gss stop
gss1.yourdomain.com# gssm restore <backup_filename>
gss1.yourdomain.com# gss enable gssm-primary
```

- Re-enable all other GSSs and GSSMs on the network by completing the following steps for each device:
  - Delete the device from the GUI
  - Enable the device from the CLI
  - Activate the device from the GUI

- CSCdx59427

  Symptom: Screens showing CRA RTT should show one-way delay

  Condition: Round Trip Time values are displayed for the CRAs (Content Router Agents) in the **show stat kale cra list** and **show stat kale cra** *<IP_address>* commands, and on the GSSM GUI Show KeepAlive Statistics page. To be consistent with other Cisco products, such as the CR 4430, these should show the One way delay values.

  Workaround: There is no workaround. The One way delay is simply RTT/2.

- CSCdx82760

  Symptom: GSS lags when logging a large number of messages.

  Condition: When receiving a high volume of logging activity (for example from applications in debug mode), the GSS lags behind the message activity. Logging continues after messages have ceased, and the timestamp on logged messages is inaccurate.

  Workaround: There is no workaround.

- CSCdx72509

  Symptom: Outbound FTP connection hangs CLI session.

  Condition: When using FTP to connect the GSS to a site that only accepts "PASV" FTP, the GSS CLI becomes suspended. The CTRL C key combination does not break the connection.

Workaround: Do the following:

- Terminate your suspended FTP session and reconnect to the FTP site.
- When reconnected to the remote site, first enter the **passive** command to switch your FTP session to passive mode, for example:

```
ftp> passive
Passive mode on.
ftp>
```

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.