3906/3926 Service Virtualization Switch

Installation and startup for AT&T FlexWare Specialized MOP

101-2018-011 - Standard Revision B
December 2018

LEGAL NOTICES

THIS DOCUMENT CONTAINS CONFIDENTIAL AND TRADE SECRET INFORMATION OF CIENA CORPORATION AND ITS RECEIPT OR POSSESSION DOES NOT CONVEY ANY RIGHTS TO REPRODUCE OR DISCLOSE ITS CONTENTS, OR TO MANUFACTURE, USE, OR SELL ANYTHING THAT IT MAY DESCRIBE. REPRODUCTION, DISCLOSURE, OR USE IN WHOLE OR IN PART WITHOUT THE SPECIFIC WRITTEN AUTHORIZATION OF CIENA CORPORATION IS STRICTLY FORBIDDEN.

EVERY EFFORT HAS BEEN MADE TO ENSURE THAT THE INFORMATION IN THIS DOCUMENT IS COMPLETE AND ACCURATE AT THE TIME OF PUBLISHING; HOWEVER, THE INFORMATION CONTAINED IN THIS DOCUMENT IS SUBJECT TO CHANGE.

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing CIENA PROVIDES THIS DOCUMENT “AS IS” WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice. For the most up-to-date technical publications, visit www.ciena.com.

Copyright© 2018 Ciena® Corporation. All Rights Reserved

The material contained in this document is also protected by copyright laws of the United States of America and other countries. It may not be reproduced or distributed in any form by any means, altered in any fashion, or stored in a data base or retrieval system, without express written permission of the Ciena Corporation.

Security

Ciena® cannot be responsible for unauthorized use of equipment and will not make allowance or credit for unauthorized use or access.

Contacting Ciena

Corporate Headquarters	410-694-5700 or 800-921-1144	www.ciena.com
Customer Technical Support/Warranty		
In North America	1-800-CIENA-24 (243-6224) 410-865-4961	
In Europe, Middle East, and Africa	800-CIENA-24-7 (800-2436-2247) +44-207-012-5508 00 0800 77 454 (Slovenia)	
In Asia-Pacific	800-CIENA-24-7 (800-2436-2247) +81-3-6367-3989 +91-124-4340-600 120 11104 (Vietnam) 000 8004401369 (India)	
In Caribbean and Latin America	800-CIENA-24-7 (800-2436-2247) 1230-020-0845 (Chile) 009 800-2436-2247 (Colombia) 0800-77-454 (Mexico and Peru) 00 008000442510 (Panama)	
Sales and General Information	North America: 1-800-207-3714 International: +44 20 7012 5555	E-mail: sales@ciena.com
In North America	410-694-5700 or 800-207-3714	E-mail: sales@ciena.com
In Europe	+44-207-012-5500 (UK)	E-mail: sales@ciena.com
In Asia	+81-3-3248-4680 (Japan)	E-mail: sales@ciena.com
In India	+91-22-42419600	E-mail: sales@ciena.com
In Latin America	011-5255-1719-0220 (Mexico City)	E-mail: sales@ciena.com
Training		E-mail: learning@ciena.com

For additional office locations and phone numbers, please visit the Ciena web site at www.ciena.com.

READ THIS LICENSE AGREEMENT (“LICENSE”) CAREFULLY BEFORE INSTALLING OR USING CIENA SOFTWARE OR DOCUMENTATION. THIS LICENSE IS AN AGREEMENT BETWEEN YOU AND CIENA COMMUNICATIONS, INC. (OR, AS APPLICABLE, SUCH OTHER CIENA CORPORATION AFFILIATE LICENSOR) (“CIENA”) GOVERNING YOUR RIGHTS TO USE THE SOFTWARE. BY INSTALLING OR USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AND AGREE TO BE BOUND BY IT.

1. License Grant. Ciena may provide “Software” to you either (1) embedded within or running on a hardware product or (2) as a standalone application, and Software includes upgrades acquired by you from Ciena or a Ciena authorized reseller. Subject to these terms, and payment of all applicable License fees including any usage-based fees, Ciena grants you, as end user, a non-exclusive, non-transferable, personal License to use the Software only in object code form and only for its intended use as evidenced by the applicable product documentation. Unless the context does not permit, Software also includes associated documentation.

2. Open Source and Third Party Licenses. Software excludes any open source or third-party programs supplied by Ciena under a separate license, and you agree to be bound by the terms of any such license. If a separate license is not provided, any open source and third party programs are considered “Software” and their use governed by the terms of this License.

3. Title. You are granted no title or ownership rights in or to the Software. Unless specifically authorized by Ciena in writing, you are not authorized to create any derivative works based upon the Software. Title to the Software, including any copies or derivative works based thereon, and to all copyrights, patents, trade secrets and other intellectual property rights in or to the Software, are and shall remain the property of Ciena and/or its licensors. Ciena's licensors are third party beneficiaries of this License. Ciena reserves to itself and its licensors all rights in the Software not expressly granted to you.

4. Confidentiality. The Software contains trade secrets of Ciena. Such trade secrets include, without limitation, the design, structure and logic of individual Software programs, their interactions with other portions of the Software, internal and external interfaces, and the programming techniques employed. The Software and related technical and commercial information, and other information received in connection with the purchase and use of the Software that a reasonable person would recognize as being confidential, are all confidential information of Ciena (“Confidential Information”).

5. Obligations. You shall:

i) Hold the Software and Confidential Information in strict confidence for the benefit of Ciena using your best efforts to protect the Software and Confidential Information from unauthorized disclosure or use, and treat the Software and Confidential Information with the same degree of care as you do your own similar information, but no less than reasonable care;

ii) Keep a current record of the location of each copy of the Software you make;

iii) Use the Software only in accordance with the authorized usage level;

iv) Preserve intact any copyright, trademark, logo, legend or other notice of ownership on any original or copies of the Software, and affix to each copy of the Software you make, in the same form and location, a reproduction of the copyright notices, trademarks, and all other proprietary legends and/or logos appearing on the original copy of the Software delivered to you; and

v) Issue instructions to your authorized personnel to whom Software is disclosed, advising them of the confidential nature of the Software and provide them with a summary of the requirements of this License.

6. Restrictions. You shall not:

i) Use the Software or Confidential Information a) for any purpose other than your own internal business purposes; and b) other than as expressly permitted by this License;

ii) Allow anyone other than your authorized personnel who need to use the Software in connection with your rights or obligations under this License to have access to the Software;

iii) Make any copies of the Software except such limited number of copies, in machine readable form only, as may be reasonably necessary for execution in accordance with the authorized usage level or for archival purposes only;

iv) Make any modifications, enhancements, adaptations, derivative works, or translations to or of the Software;

v) Reverse engineer, disassemble, reverse translate, decompile, or in any other manner decode the Software;

vi) Make full or partial copies of the associated documentation or other printed or machine-readable matter provided with the Software unless it was supplied by Ciena in a form intended for reproduction;

vii) Export or re-export the Software from the country in which it was received from Ciena or its authorized reseller unless authorized by Ciena in writing; or

viii) Publish the results of any benchmark tests run on the Software.

7. Audit: Upon Ciena's reasonable request you shall permit Ciena to audit the use of the Software to ensure compliance with this License.

8. U.S. Government Use. The Software is provided to the Government only with restricted rights and limited rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in FAR Sections 52-227-14 and 52-227-19 or DFARS Section 52.227-7013(C)(1)(ii), as applicable. The Software and any accompanying technical data (collectively "Materials") are commercial within the meaning of applicable Federal acquisition regulations. The Materials were developed fully at private expense. U.S. Government use of the Materials is restricted by this License, and all other U.S. Government use is prohibited. In accordance with FAR 12.212 and DFAR Supplement 227.7202, the Software is commercial computer software and the use of the Software is further restricted by this License.

9. Term of License. This License is effective until the applicable subscription period expires or the License is terminated. You may terminate this License by giving written notice to Ciena. This License will terminate immediately if (i) you breach any term or condition of this License or (ii) you become insolvent, cease to carry on business in the ordinary course, have a receiver appointed, enter into liquidation or bankruptcy, or any analogous process in your home country. Termination shall be without prejudice to any other rights or remedies Ciena may have. Upon any termination of this License you shall destroy and erase all copies of the Software in your possession or control, and forward written certification to Ciena that all such copies of Software have been destroyed or erased. Your obligations to hold the Confidential Information in confidence, as provided in this License, shall survive the termination of this License.

10. Compliance with laws. You agree to comply with all laws related to your installation and use of the Software. Software is subject to U.S. export control laws, and may be subject to export or import regulations in other countries. If Ciena authorizes you to import or export the Software in writing, you shall obtain all necessary licenses or permits and comply with all applicable laws.

11. Limitation of Liability. ANY LIABILITY OF CIENA SHALL BE LIMITED IN THE AGGREGATE TO THE AMOUNTS PAID BY YOU TO CIENA OR ITS AUTHORIZED RESELLER FOR THE SOFTWARE. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, INCLUDING WITHOUT LIMITATION BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS. THE LIMITATIONS OF LIABILITY DESCRIBED IN THIS SECTION ALSO APPLY TO ANY LICENSOR OF CIENA. NEITHER CIENA NOR ANY OF ITS LICENSORS SHALL BE LIABLE FOR ANY INJURY, LOSS OR DAMAGE, WHETHER INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL INCLUDING WITHOUT LIMITATION ANY LOST PROFITS, CONTRACTS, DATA OR PROGRAMS, AND THE COST OF RECOVERING SUCH DATA OR PROGRAMS, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE.

12. General. Ciena may assign this License to an affiliate or to a purchaser of the intellectual property rights in the Software. You shall not assign or transfer this License or any rights hereunder, and any attempt to do so will be void. This License shall be governed by the laws of the State of New York without regard to conflict of laws provisions. The U.N. Convention on Contracts for the International Sale of Goods shall not apply hereto. This License constitutes the complete and exclusive agreement between the parties relating to the license for the Software and supersedes all proposals, communications, purchase orders, and prior agreements, verbal or written, between the parties. If any portion hereof is found to be void or unenforceable, the remaining provisions shall remain in full force and effect.

Contents

CHAPTER 1
Publication History

This document has the following version history.

October 2018

Standard Revision A

First Formal Release of this document.

December 2018

Standard Revision B

Second Standard Release of this document to add a check for D-NFVI license and more troubleshooting topics.

CHAPTER 2
About this document

The purpose of this Method of Procedure (MOP) document is to on-board the newly installed Ciena® 39xx Switch Platform into the AT&T network to enable the NOC to deploy the necessary virtualized services.

Trademark acknowledgements

Ciena is a trademark of Ciena Corporation.

Intended audience

This document is intended for NCR installation technicians who will on-board the newly installed Ciena 39xx Switch Platform into the AT&T network.

It assumes that the intended users possess basic knowledge of, but not limited to:

- Changing the IP address of a network interface card
- Connecting to devices using PuTTY via Ethernet port
- Connecting to a console using TerraTerm
- Sharing screens with a desktop sharing application

Glossary

The following abbreviations are used within this document.

Table 1 Glossary

FRU	Field-replaceable unit. The x86-based processor blade used for virtualization hosting.
OS	Operating system
D-NFVI	Distributed Network Function Virtualization Infrastructure
D-NFVI OS	The Linux-based OS running on the FRU

D-NFVI UI	The user interface (UI) subsystem running as a docker container within the D-NFVI OS.
SAOS	Service Aware Operating System. The OS for the Ciena Carrier Ethernet Switch (CES).
39xx	Shorthand notation for reference to the Ciena 3906 or 3926 Switch Platform
SFP	Small Form Pluggable
CuSFP	Copper SFP

CHAPTER 3
Prerequisites

Before installation, ensure the following pre-installation requirements are met.

Site readiness and physical installation

The following site readiness and physical installation requirements must be completed prior to beginning the on-site MOP workflow.

Ensure that:

- the 39xx Switch Platform is installed in the rack and powered (dual power as applicable).
- the D-NFVI FRU is installed into the right side of the 39xx Switch Platform after removing the faceplate panel. Take care to remove the plastic battery tab if present.

  Note: The D-NFVI field-replaceable unit (FRU) is shipped in a separate box.

- power has been applied for more than a minimum of eight (8) minutes to allow the software to boot and initialize.
- LAN/WAN cables are installed in the 39xx Switch Platform according to site requirements. If necessary, install pluggables (SFP or CuSFP). At a minimum, the WAN cable must be connected before proceeding to allow external connectivity of the 39xx Switch Platform.

ATTENTION

Cable management and labeling must be implemented in accordance with customer site requirements.

Technician requirements

The technician must have the following prior to installation.

Note: Ensure that, as you complete the workflow, you fill out and update the checklist at the end of this document.

Equipment:

- a straight through Ethernet cable (RJ-45 to RJ-45) for connecting to the 3906/3926 Switch Platform
- (optional) a USB to DB-9 serial console adapter and the Ciena DB-9 to RJ-45 console cable for backup connectivity to the devices
- a laptop (with software, listed below, installed)
- 4G/LTE dongle (or an equivalent such as a phone hotspot) as backup Internet connectivity to provide remote access to the laptop for troubleshooting

Software:

- PuTTY, for IP connectivity
- TerraTerm, for D-NFVI console access (if required)
- desktop sharing application installed such as TeamViewer, Webex™, or an equivalent

Files:

- **command_saos_xxxx.** SAOS (3906/3926) base configuration, where xxxx is the site name.
- **command_vrouter_xxxx**. vRouter configuration, where xxxx is the site name.
- **checkvrfloop.vcli**. Creates a script called checkvrfloop.vcli.
- **command_dnfvi_xxxx**. D-NFVI IP configuration, where xxxx is the site name.
- **vrouter_verification_xxxx**. Verification commands for vRouter, where xxxx is the site name.

  Note: These files must be provided by AT&T or NCR and installed on the laptop prior to the site visit.

CHAPTER 4
Workflow overview

The Ciena 39xx Switch platform is comprised of a Ciena Carrier Ethernet Switch and a DNFVI Virtualization Blade. The DNFVI Virtualization Blade is a Field Replaceable Unit (FRU) shipped separately that requires insertion into the right-hand side of the switch platform after the filler plate has been removed and discarded.

There are 3 major components that require configuration:

- 39xx Switch CLI.
- D-NFVI. The D-NFVI has two CLI consoles. The user interface (UI) subsystem and the D-NFVI OS CLI, which is accessed from the UI console CLI.
- Vyatta ® Virtual Router (vRouter) running as a virtual machine (VM) on the D-NFVI FRU.

The components are accessed via a CLI console, however, it is necessary to “tunnel” from one console to another.

Physical connectivity is via direct Ethernet cable from the laptop to the 39xx Switch Platform dedicated Management port.

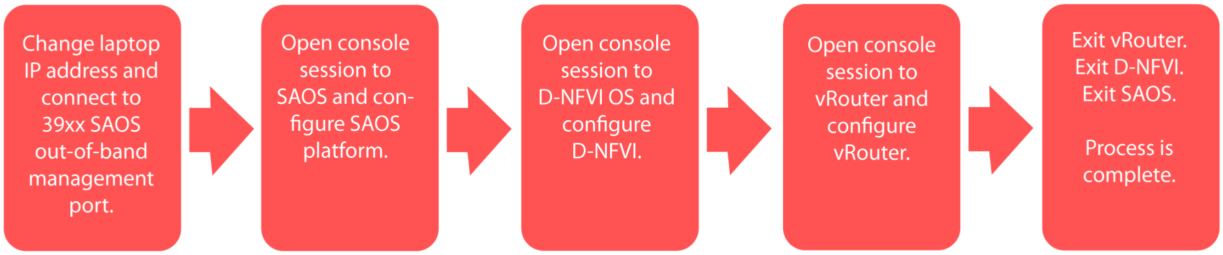
The Management port provides direct access to the 39xx Switch CLI. From the 39xx Switch CLI, the D-NFVI UI subsystem console is accessed. From the D-NFVI UI console the D-NFVI OS console is accessed. Lastly, from the D-NFVI OS console the vRouter console is accessed.

To summarize, the logical sequence of console access is:

1. 39xx Switch CLI accessed via physical Ethernet connection to the Mgmt port
2. D-NFVI UI CLI accessed from the 39xx Switch CLI
3. D-NFVI OS CLI accessed from the D-NFVI UI CLI
4. vRouter CLI accessed from the D-NFVI OS CLI

The below diagram provides the high level workflow required by the on-site technician, once the 39xx Switch Platform has been physically installed and the D-NFVI FRU has been inserted.

Figure 1 Workflow


Change laptop IP address and connect to 39xx SAOS out-of-band management port.
Open console session to SAOS and configure SAOS platform.
Open console session to D-NFVI OS and configure D-NFVI.
Open console session to vRouter and configure vRouter.
Exit vRouter. Exit D-NFVI. Exit SAOS.
Process is complete.

Usernames and passwords

Table 2 Usernames and passwords

Location	Username	Password
SAOS	su	tA0P#w3R
DNFVI	diag	FL#Xw4r#pR) (password for console)
DNFVI	diag@cn_core_host	FL#Xw4r#pR) (password for console)
DNFVI	user	Sp3(1aLi53d
Vyatta router	attuser	Th3k3yt#themA

Prompts

Each console displays a different identifying prompt.

- 3906 CLI: 3906>
- 3926 CLI: 3926>
- D-NFVI UI container: NFV-FRU.ui
- D-NFVI OS: NFV-FRU
- Vyatta router: vyatta:~$

CHAPTER 5
MOP

Follow the procedures in the MOP workflow in the order they are presented.

They are:

1 "Identify the Switch Platform" on page 9
2 "Powering up with the D-NFVI FRU installed" on page 11
3 "Changing the laptop IP address" on page 13
4 "Configure the 39xx Switch Platform" on page 14
5 "Configuring the D-NFVI FRU IP address" on page 16
6 "Connecting to the vRouter VM console" on page 19

Identify the Switch Platform

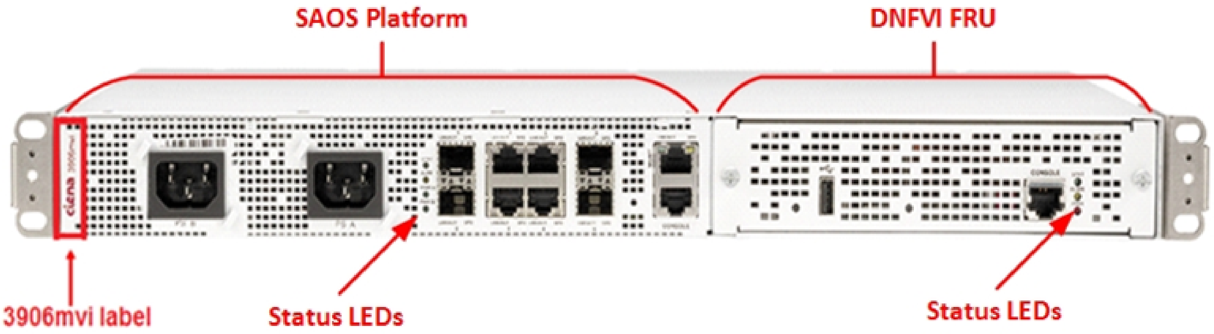
Identify the unit being installed and configured. It will either be a 3906 or a 3926 Switch Platform.

> ***Note:*** The D-NFVI FRU is shipped separately and must be installed by the tech on site.

After identification, update the "Checklist" on page 31.

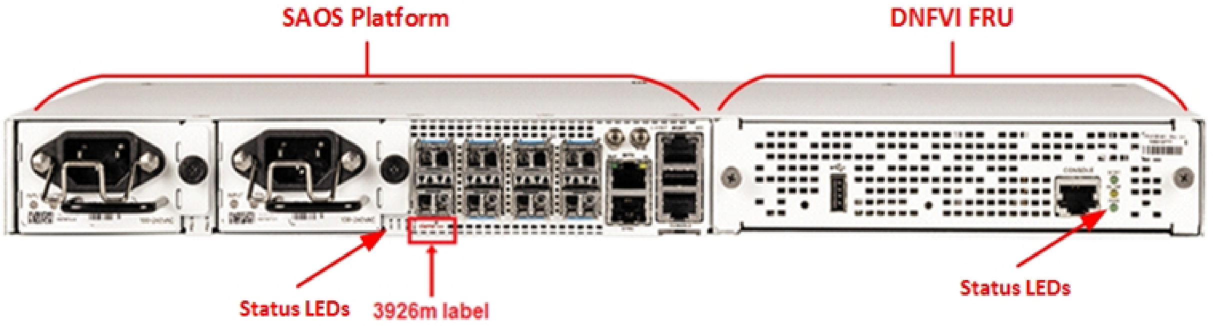
3906 Switch Platform

The 3906 Switch Platform contains a label on the left side of the chassis as shown below.



3926 Switch Platform

The 3926 Switch Platform contains a label on the bottom of the chassis as shown below.



Procedure 1 Powering up with the D-NFVI FRU installed

Overview

The following steps verify that the 39xx Switch Platform is operational. Ensure that power has been applied for eight (8) minutes before performing the following steps.

Note: Refer to the "Status LED overview" on page 27, if required.

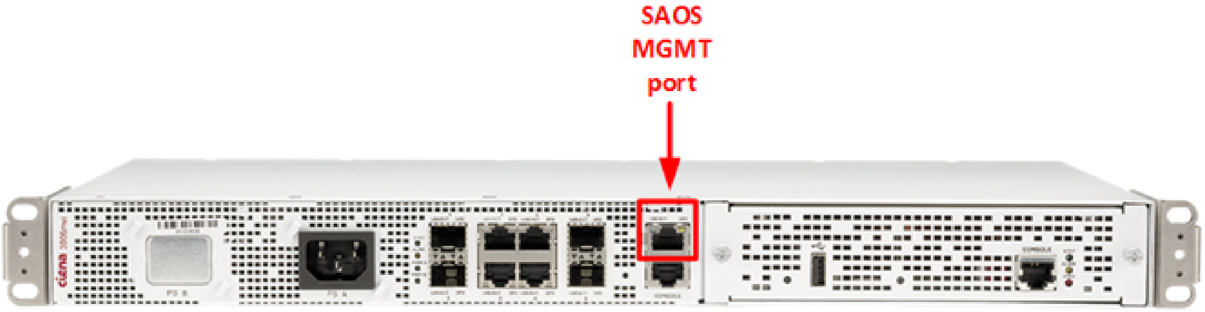
Steps

1 Verify that the LED next to STAT is solid green on the 39xx Switch Platform chassis.

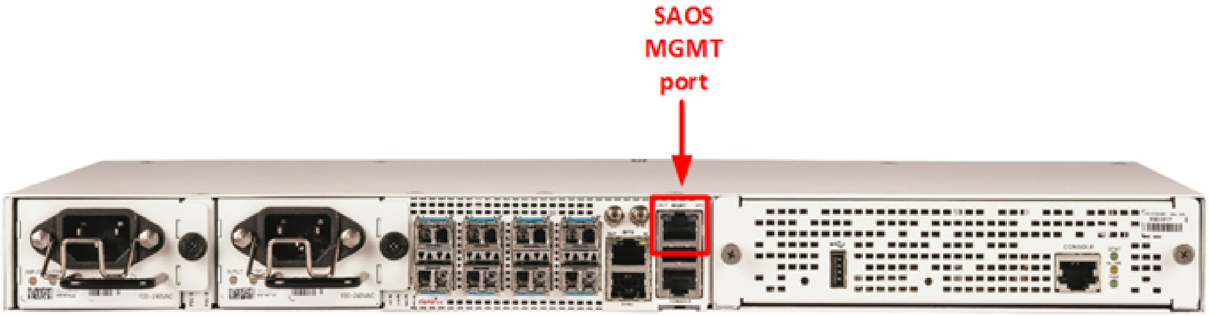
2 Verify that the LED next to STAT is solid green on the D-NFVI FRU.

3 Connect a straight-through Ethernet cable from the laptop to Ethernet port labeled MGMT, as shown below. Verify physical connectivity by checking that the LED next to **the MGMT port** is blinking green.

Note: The MGMT port is used for access to the 39xx Switch Platform console, D-NFVI FRU console and vRouter VM console.



3906



3926

> **ATTENTION**
> Observe 3926 port numbering prior to connecting cables. The 3926 port arrangement is different than the 3906.

4 Update the “Checklist” on page 31.

Procedure 2 Changing the laptop IP address

Overview

The following steps change the laptop wired interface IP address to a static IP address that is on same subnet as the default 39xx Switch CLI local IP, accessible via the dedicated Management faceplate port.

Steps

1 Change IP address of laptop with the following information. (These details are always the same.)

```
Laptop IP address: 172.16.233.210
Subnet mask: 255.255.255.0
Default gateway: should be left blank
```

2 Open the DOS command window (or equivalent) and ping the IP address **172.16.233.214** to ensure connectivity to the 39xx Switch Platform.

3 Update the “Checklist” on page 31.

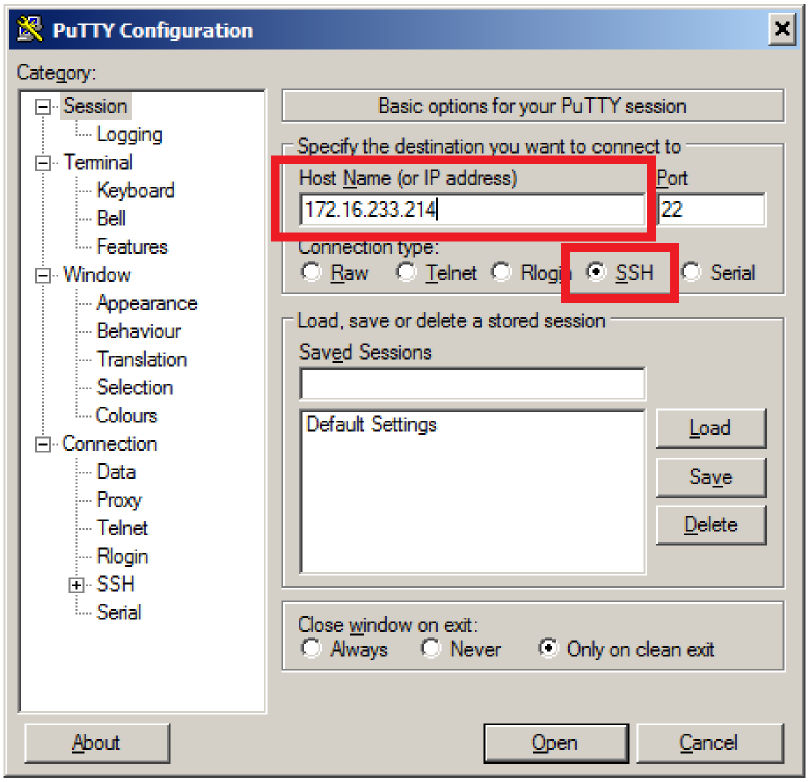
Procedure 3 Configure the 39xx Switch Platform

Overview

The following steps open a 39xx Switch Platform console session, check the **su** password, and configure the 39xx Switch Platform.

Steps

1 Open SSH/console client application (PuTTY) and connect by SSH to the 39xx Switch Platform. In the Host Name (or IP address) field, enter 172.16.233.214, and ensure the SSH radio button is selected as shown in the following screenshot.



Host Name (or IP address): 172.16.233.214

Port: 22

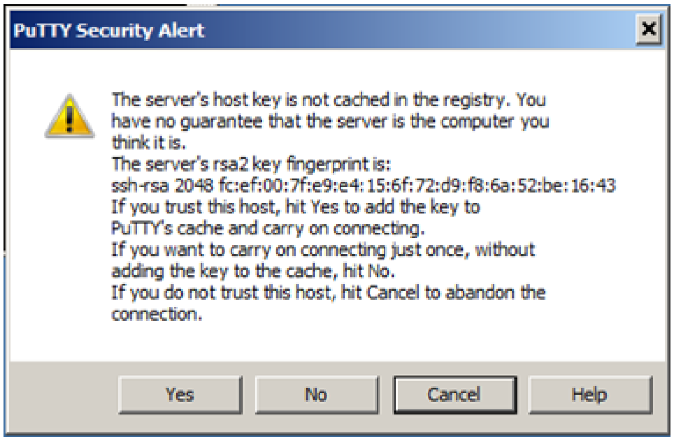
Connection type: ○ Raw ○ Telnet ○ Rlogi ● SSH ○ Serial

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

2 Click **Open** to open the SSH session. This will open the command window to the 39xx Switch CLI.

3 A prompt may appear like the below. Click **Yes** to continue.



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 2048 fc:ef:00:7f:e9:e4:15:6f:72:d9:f8:6a:52:be:16:43
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

4 Once the 39xx Switch Platform command window is open, log in with the following details:

```
Username: su
Password: tA0P#w3R (where 0 is a numerical zero)
```

Note: Some 39xx Switch Platforms may use a different password. If the above password does not work, try the following password: wwp. If the password is wwp, use the set command to change the password from wwp to tA0P#w3R.

user set user su echoless-password

```
Enter Old Password: wwp
Enter New Password: tA0P#w3R
Verify New Password: tA0P#w3R
```

5 After logging in, a prompt should appear.

```
3906> or 3926>
```

6 Open the `command_saos_xxxx` file with the base 3906/3926 Switch Platforms commands. Copy all commands, except comments, from the text file and paste into the console. Ensure all commands have been entered.

7 Update the “Checklist” on page 31.

Procedure 4 Configuring the D-NFVI FRU IP address

Overview

The DNFVI console is accessed from the 39xx Switch CLI. The D-NFVI runs separate “containers” for the various software functions, and initially the console connects to the user interface (UI) subsystem. The UI subsystem is used to run a special D-NFVI CLI shell for viewing and configuring D-NFVI settings. Some configurations, like setting the IP address of the D-NFVI OS, must be performed on the base OS. The D-NFVI OS is accessed by SSH from the UI subsystem to the base OS.

Predefined host entries are defined in the `/etc/hosts` file to assist with ssh login.

Table 3

Hostname	Value	Prompt
Base DNFVI Linux OS	cn_core_host	NFV-FRU
UI container	ui	NFV-FRU.ui

ATTENTION

The D-NFVI console session accessed via the 39xx Switch CLI “resumes” where it previously left off. Thus, in regard to navigation, if you do not “exit” a subsystem, then subsequent console sessions “reconnect” to where the previous session terminated. If in doubt about what subsystem is logged into, use “exit” repeatedly to go back to the D-NFVI login prompt.

Pay attention to the prompt as that indicates the host that is logged into.

Steps

1 At the 39xx Switch Platform CLI prompt, enter the following command.

```
module diag-shell module NFV
```

Then, press the **Tab** key to complete the command and then press **Enter**.

2 At the `Terminal ready` prompt, press **Enter**.

The console connection “resumes” from where it was previously. If this is the first time accessing the D-NFVI OS after the FRU has powered up, or previous sessions were properly logged out from, then you will be greeted with another login prompt, which is the D-NFVI UI container.

3 Enter the following login details:

```
Username: diag
Password: FL#Xw4r#pR)
```

You are now at the shell level within the UI container as the user diag as indicated by the `diag@NFV-FRU.ui` prompt.

4 Verify the license status of the D-NFVI software. To do this, use the following command to enter the “yp shell” CLI.

yp-shell

Enter the following yp shell command to get the license state.

sget /license-management-state/license-client-state/license-feature/properties/acquired-count

Note: Press the **Tab** key to complete the command after typing the first few characters.

In the lines of output, you should see three (3) separate instances of the phrase “acquired count”. For example, "acquired-count":1. The count must not be zero (0).

Exit the yp-shell CLI.

quit

Note: If all three (3) licenses are not acquired (that is, the count is 0 for any of the instances), then refer to the “Restarting the UI container” on page 25 and “Setting the D-NFVI system date and time” on page 25 troubleshooting topics.

5 From the UI container it is necessary to SSH into the base D-NFVI Linux OS. To do this, use the following command:

ssh cn_core_host

If prompted with the following text, type **yes** and press **Enter**.

```
authenticity of host 'diag (169.254.160.2)' can't be
established. ECDSA key fingerprint is
SHA256:Npk0+gK7G6L9aDKblN0cR+7iLudKmZcFQhstHf8WFCY. Are
you sure you want to continue connecting (yes/no)?
```

At the password prompt, enter the following password:

```
Password: FL#Xw4r#pR)
```

Now you are at the shell level of the D-NFVI Linux OS.

6 Switch to the root user.

sudo su

The command prompt now displays:

```
/home/diag#
```

7 Verify that the system date/time/time zone is accurate. If the date/time needs to be changed, refer to the “Setting the D-NFVI system date and time” on page 25 troubleshooting topic.

```
root@NFV-FRU:/home/diag# date
Tue Oct 16 18:11:31 UTC 2018
```

Once the date/time/time zone is correct, sync the hw clock to the system clock.

```
root@NFV-FRU:/home/diag# sudo hwclock --systohc
```

Note: If you do not enter this command, then the system date may roll back to a past date following an FRU reboot.

8 Open the `command_dnfvi_xxxx` file with the base D-NFVI OS commands. Copy all commands, except for comments, from the text file and paste into the console. Ensure all commands are entered.

9 Verify that the vrouter VM is running.

virsh list —-all

The IP address is now configured and the router VM is running. If the vrouter is not running refer to the "Starting and Stopping the vRouter VM" on page 26troubleshooting topic.

10 Update the "Checklist" on page 31.

Procedure 5 Connecting to the vRouter VM console

Overview

The following steps access the vRouter VM console and configure the vRouter.

Steps

1 While still within the D-NFVI OS console session (from previous procedure), execute the following command to access the vRouter VM console:

```
virsh console vrouter
```

2 When the text `Escape character is ^]` is displayed, press **Enter** a few times in order to access the console login prompt.

3 Enter the following login details:

```
Username: attuser
Password: Th3k3yt#themA
```

4 Open the `checkvrfloop.vcli` file and follow the instructions to create the script.

5 Open the command_vrouter_xxxx file with the base vRouter VM commands. Copy all commands, except for comments, from the text file and paste into the console. Ensure all commands are entered.

6 Run through the verification steps provided in the `vRouter_verification_xxxx` file.

7 Press and hold **Ctrl** and **]** (right square bracket) to close the console session to the vRouter VM. This returns to the D-NFVI OS console.

8 Exit the D-NFVI OS CLI and return to the D-NFVI UI CLI.

```
exit
```

9 Log out from the D-NFVI UI CLI and return to the login prompt.

```
exit
```

10 Press and hold **Ctrl** and **a** and **x** to close the console session to D-NFVI OS. This returns you to the 39xx Switch Platform console.

11 Close the 39xx Switch Platform console session using the exit command.

```
exit
```

At this stage the procedure is complete, and the device should be remotely accessible.

12 Update the “Checklist” on page 31.

CHAPTER 6
Troubleshooting

This following provides a common list of commands that can be used when troubleshooting.

Ensure that you are logged into the 3906 or a 3926 Switch Platform per the login instructions provided in “Configure the 39xx Switch Platform” on page 14.

Procedure 6 Unlocking the D-NFVI OS console

Overview

When trying to connect to the console of the x86 FRU, and the 3906/3926 Switch Platform console displays the message: “Diag shell already in use”.

Steps

1 Run the following commands on the 3906/3926 Switch Platform console to unlock the D-NFVI OS console:

cd /tmp

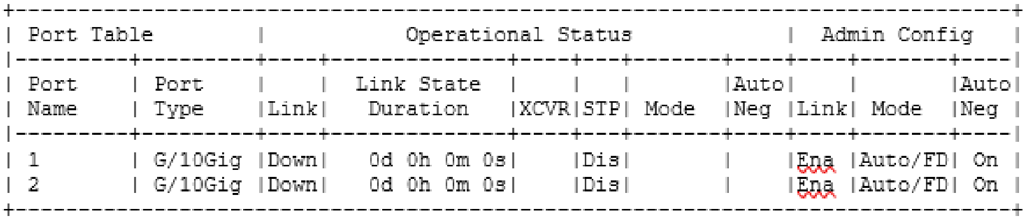
rm -f module.lock

3906/3926 switch platform commands

```
port show
```

Displays the status of all ports. Provides a snapshot of important parameters of all ports. For example, link state (up or down), Auto-negotiation configuration and state.

```
> port show
```



```
+--------------------------------------------------------------------------------+
| Port Table        |            Operational Status            |  Admin Config   |
|---------+---------+----+--------------+----+---+--------+----+----+-------+----|
| Port    | Port    |    | Link State   |    |   |        |Auto|    |       |Auto|
| Name    | Type    |Link|  Duration    |XCVR|STP| Mode   |Neg |Link| Mode  |Neg |
|---------+---------+----+--------------+----+---+--------+----+----+-------+----|
| 1       | G/10Gig |Down|   0d 0h 0m 0s|    |Dis|        |    |Ena |Auto/FD| On |
| 2       | G/10Gig |Down|   0d 0h 0m 0s|    |Dis|        |    |Ena |Auto/FD| On |
+--------------------------------------------------------------------------------+
```

```
port show port <x>
```

Replace <x> with the port number being troubleshooted. Provides detailed information on the status of a single port.

```
port show statistics
```

Displays traffic in and out (in Bytes and Packets) for all ports on the device. Can be used to verify if traffic is flowing in and out of a port.

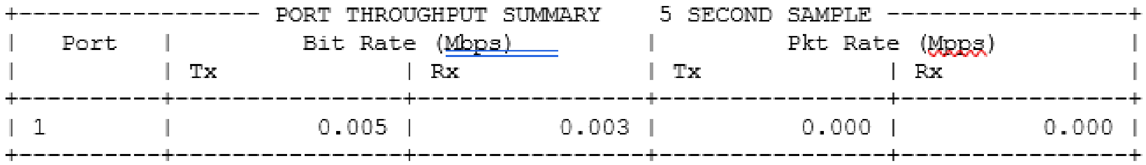
```
port show port <x> statistics
```

Replace <x> with the port number being troubleshooted. Provides detailed statistics for a single port. Can be used to verify traffic flowing in and out of a port.

```
port show throughput active
```

Provides throughput in Mbps for any ports that are transmitting and receiving traffic. Useful to verify the rate at which traffic is flowing into/out of the switch.

```
> port show throughput active
```

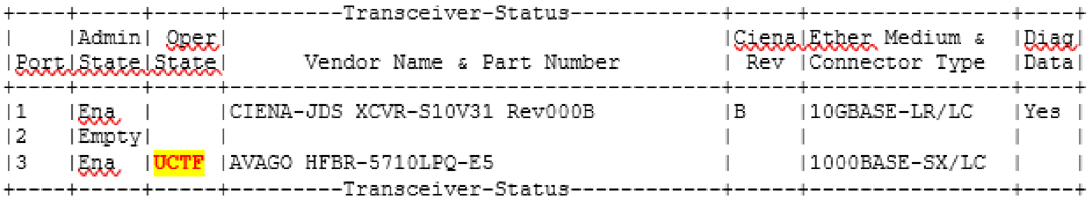


```
+----------------- PORT THROUGHPUT SUMMARY    5 SECOND SAMPLE -----------------+
|   Port    |              Bit Rate (Mbps)          |         Pkt Rate (Mpps)           |
|           | Tx                | Rx                | Tx                | Rx                |
+-----------+-----------------+-----------------+-----------------+-----------------+
| 1         |           0.005 |           0.003 |           0.000 |           0.000 |
+-----------+-----------------+-----------------+-----------------+-----------------+
```

```
port xcvr show
```

Displays the status of SFPs plugged into the device. Ciena recommends Ciena branded SFPs in the devices as these have gone through rigorous testing to ensure performance.

```
> port xcvr show
```



```
+----+-----+-----+---------Transceiver-Status------------+-----+----------------+----+
|    |Admin| Oper|                                       |Ciena|Ether Medium &  |Diag|
|Port|State|State|      Vendor Name & Part Number        | Rev |Connector Type  |Data|
+----+-----+-----+---------------------------------------+-----+----------------+----+
|1   |Ena  |     |CIENA-JDS XCVR-S10V31 Rev000B          |B    |10GBASE-LR/LC   |Yes |
|2   |Empty|     |                                       |     |                |    |
|3   |Ena  |UCTF |AVAGO HFBR-5710LPQ-E5                  |     |1000BASE-SX/LC  |    |
+----+-----+-----+---------Transceiver-Status------------+-----+----------------+----+
```

In the above example, UTCF refers to an uncertified SFP. It is recommended that this be swapped out for a Ciena branded SFP.

FRU type mismatch active alarm on a 3906

There is a known issue where a 3906 platform running SAOS 6.17.1.138 will sometimes display an FRU type mismatch alarm.

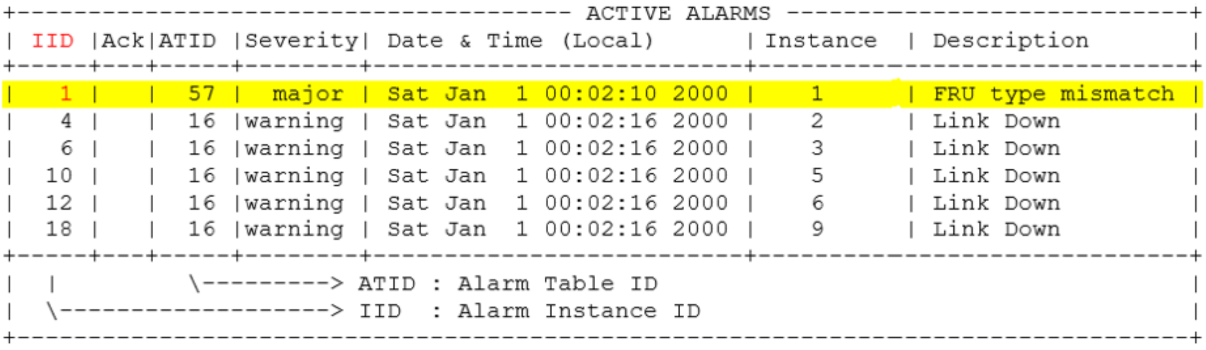
This alarm applies to TDM-FRU module types and can be ignored on the 3906 platform, which only support a NFV-FRU module type. A permanent solution will be available in the next software release. Acknowledge the alarm to clear the alarm LED on the device.

To do this:	Enter this command:
Verify if the “FRU type mismatch” alarm exists	3906> **alarm show active-alarms**
Acknowledge the alarm to clear the alarm LED on the device	3906> **alarm acknowledge alarm-instance-id <IID>**

The alarm-instance-id is the IID provided in the alarm instance table. For example, using the table below the IID is 1:

3906> alarm acknowledge alarm-instance-id 1

Figure 2



```
+--------------------------------------- ACTIVE ALARMS ----------------------------+
| IID |Ack|ATID |Severity| Date & Time (Local)        | Instance   | Description            |
+-----+---+-----+--------+----------------------------+------------------------------+
|   1 |   |  57 |  major | Sat Jan  1 00:02:10 2000 |     1      | FRU type mismatch |
|   4 |   |  16 |warning | Sat Jan  1 00:02:16 2000 |     2      | Link Down              |
|   6 |   |  16 |warning | Sat Jan  1 00:02:16 2000 |     3      | Link Down              |
|  10 |   |  16 |warning | Sat Jan  1 00:02:16 2000 |     5      | Link Down              |
|  12 |   |  16 |warning | Sat Jan  1 00:02:16 2000 |     6      | Link Down              |
|  18 |   |  16 |warning | Sat Jan  1 00:02:16 2000 |     9      | Link Down              |
+-----+---+-----+--------+----------------------------+------------------------------+
|  |         \---------> ATID : Alarm Table ID                                        |
|  \-------------------> IID  : Alarm Instance ID                                     |
+----------------------------------------------------------------------------------+
```

Note: This alarm is raised again following the 3906 reboot and must be re-acknowledged to clear the alarm LED on the device.

D-NFVI commands

Verify IP configuration

Use the following command to verify the IP configuration.

To do this:	Enter this command:
Verify the IP address of the management bridge	sudo ifconfig mgmtbr0

Accessing the D-NFVI CLI from within the D-NFVI OS CLI

Use the following commands to SSH into the D-NFVI UI subsystem from the D-NFVI OS CLI.

To do this:	Enter this command:
SSH into the UI container from the cn_core_host	ssh user@ui
Exit the SSH session	exit

Note: The user password is: **Sp3(1aLi53d**.

Restarting the UI container

If all three (3) licenses are not acquired, then it is necessary to restart the UI container to activate the license.

Use the following command to restart the UI container from within the cn_core-host.

To do this:	Enter this command:
Restart the UI container	sudo docker restart cn_ui_1

Setting the D-NFVI system date and time

The D-NFVI system date and time is set via the D-NFVI OS CLI.

To do this:	Enter this command:
Set the date and time	root@NFV-FRU:/home/diag# **date -s "<DOW> <MMM> <HH>:<MM>:<SS> UTC <YYYY>"** Substitute the proper day/month/hour/min/second/year as needed. Use the 24-hour time format for the hour. For example, date -s "Tue Oct 16 18:12:31 UTC 2018"
Verify the date and time	root@NFV-FRU:/home/diag# **date**
Sync the hardware clock to the system clock	root@NFV-FRU:/home/diag# **sudo hwclock --systohc**

ATTENTION

The time zone MUST be in UTC. Adjust the time as required by adding/subtracting offset. To determine the time zone offset, use Google.

Starting and Stopping the vRouter VM

Use the following commands to start and shut down the vRouter from the D-NFVI OS CLI (logged in with root access).

To do this:	Enter this command:
Start the vRouter VM	virsh start vrouter
Shut down the vRouter VM	virsh shutdown vrouter

YP_shell commands

The following commands are issues from within the UI container while running the DNFVI “yp shell” CLI interface.

The yp shell is entered automatically when logging into the UI container as “user”. When logging in as “diag”, use the command “yp-shell” to enter the yp shell, and “quit” to exit.

To do this:	Enter this command:
Show license state	sget license-management-state
Show VM configuration and state info	sget sfs
Show Service chain	sget sffs
Show classifiers	sget classifiers
Show running config	show running

CHAPTER 7
Status LED overview

The 39xx Switch Platforms have three system status indicators.

- On - The LED lights steadily.
- Off - The LED is off.
- Blinking - The LED cycles on and off in equal time periods.

3906 system LEDs

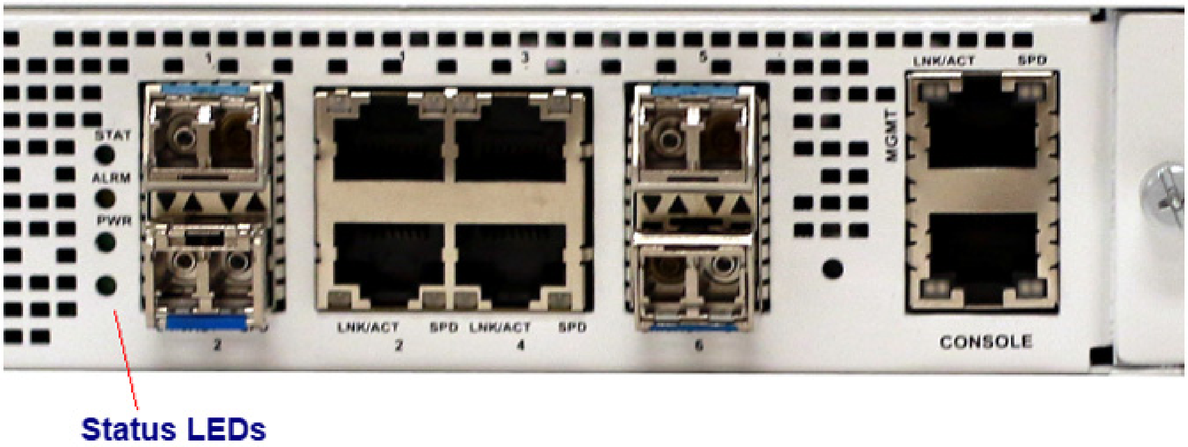


Table 4 The following table defines the 3906 LED states.

LED	Indication	Description
STAT	Off	Indicates an alarm condition.
	Green	Indicates status normal/system ready.
	Blinking Green	System is initializing and performing self tests.
ALRM	Off	Indicates normal operation condition.
	Yellow or blinking yellow	Indicates POST failure, port failure or other error condition.

LED	Indication	Description
PWR A	Off	System is not powered, or a failure has occurred on power supply A.
	Green	Indicates power is on and operating normally.
PWR B (if equipped)	Off	System is not powered, or a failure has occurred on power supply B.
	Green	Indicates power is on and operating normally.

3926 system LEDs

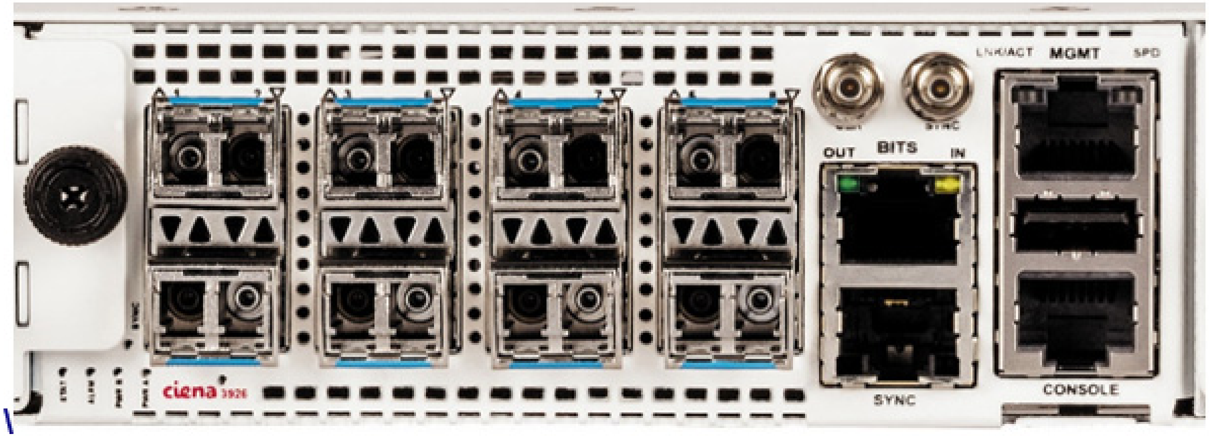


Table 5 The following table defines the 3926 LED states.

LED	Indication	Description
STAT	Off	Indicates an alarm condition.
	Green	Indicates status normal/system ready.
	Blinking Green	System is initializing and performing self tests.
ALRM	Off	Indicates normal operation condition.
	Yellow or blinking yellow	Indicates POST failure, port failure or other error condition.
PWR A	Off	System is not powered, or a failure has occurred on power supply A.
	Green	Indicates power is on and operating normally.
PWR B (if equipped)	Off	System is not powered, or a failure has occurred on power supply B.
	Green	Indicates power is on and operating normally.

LED	Indication	Description
SYNC	Off	The system is in free run timing mode.
	Green	The system is operating normally and is locked to a synchronization source such as external input, 1588, SyncE.
	Blinking green	The system is acquiring synchronization.
	Yellow	The system is in holdover timing mode. For example, phase locked loop (PLL) is holding the system within frequency drift tolerance.

x86 NFV FRU Server Module LEDs

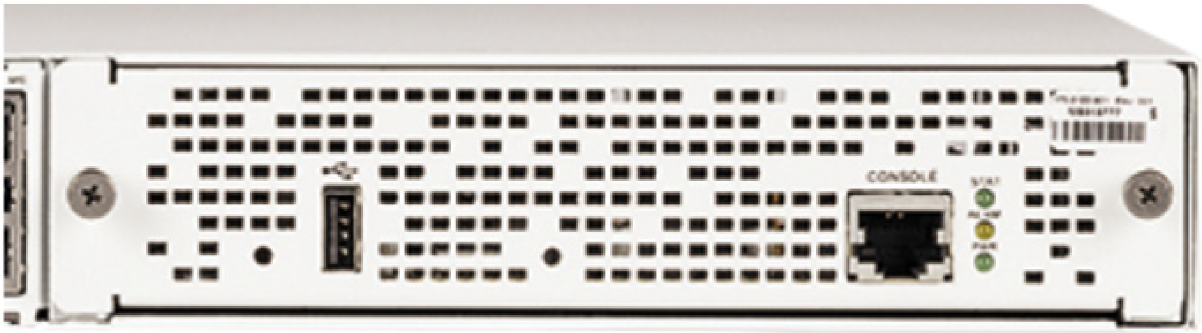


Table 6 The following table defines the x86 NFV FRU Server Module LED states.

LED	Indication	Description
STAT	Green	Normal operation.
	Blinking Green	POST (Power On Self Tests)
ALRM	Off	Normal operation.
	Blinking yellow	Error condition exists.
PWR	Off	No input or power failure.
	Green	Normal operation.

CHAPTER 8
Checklist

Initial each item completed. Start by filling in the site, date, time and verifying that the files are on-hand.

Site: ____________________

Date: ____________________

Tech: ____________________

Initials	Activity
Prerequisites: Site readiness	
	Obtained a hard copy of the most recent Low Touch Provisioning (LTP) document.
	39xx Switch Platform is installed in the rack and powered (dual power as applicable).
	FRU is installed on the right side of the 39xx Switch Platform after removing the faceplate panel. Plastic battery tab, if present, is removed.
	LAN/WAN cables connected according to MDS site information. HA cables connected according to MDS site information, if applicable.
Prerequisites: Technician requirements	
	RJ-45 Ethernet cable plugged into 39xx Switch Platform management port.
	Software is installed on the laptop.
	Obtained an LTE Dongle or hotspot.
	Obtained required configuration files and placed them on the laptop.
MOP procedures: 1. Identified platform	
	Ciena platform identified.
MOP procedures: 2. Powered up	
	Power has been applied for more a minimum of eight (8) minutes to allow the software to boot and initialize. GREEN STAT LED on the 39xx and the D-NFVI FRU.

Initials	Activity
MOP procedures: 3. Changed laptop IP	
	Changed laptop IP address and subnet. Ping test was successful.
MOP procedures: 4. Configured the 39xx Switch Platform	
	From a 39xx Switch CLI console session, verified the SAOS **su** password is correct.
	Copied all commands, except comments, to console from the **command_saos_xxxx** file.
MOP procedures: 5. Configured D-NFVI FRU	
	Verified D-NFVI license status.
	D-NFVI OS date and time are correct and the format is UTC.
	Copied all base D-NFVI OS commands, except for comments, to the console from the **command_dnfvi_xxxx** file.
MOP procedures: 6. Configured vRouter	
	Created script using the **checkvrfloop.vcli** file.
	Configured the vRouter by coying all commands, except for the comments, from the **command_vrouter_xxxx** configuration file.
	Ran through verification steps provided in the **vRouter_verification_xxxx** file.
End of Session	
	Closed the console session to the vRouter VM and returned to the D-NFVI OS CLI.
	Exited the D-NFVI OS CLI and returned to the D-NFVI UI CLI.
	Closed the console session to the D-NFVI UI CLI and returned to the 39xx Switch Platform CLI.
	Closed the console session to the 39xx Switch Platform.

3906/3926 Service Virtualization Switch

Installation and Startup for ATT FlexWare Specialized MOP

Publication: 101-2018-011
Document status: Standard
Revision B
Document release date: December 2018

CONTACT CIENA
For additional information, office locations, and phone numbers, please visit the Ciena web site at **www.ciena.com**

Tech's REFERENCE GUIDE:

BRIEF DESCRIPTION- In short:

Techs will be Removing 2 Cisco ASA Firewalls, Stacking/installing 2 Ciena 3906 devices which will be installed in the rack that will be labeled with yellow sticker labeled (Ciena) or (NCR), connecting 6 patch cords per cable matrix, (cable and matrix provided by customer), testing with remote engineer, and re-boxing old devices. And a Possible short CAT 6 DMARC extension up to 25'; anything longer will need to be confirmed by NCR. (name of approver is required).

VETTING DETAILS:

1. Check in with our OSBT Call Center.
2. Arrive onsite **ON TIME PRIOR to store Closure** and let the MOD/Guard know that you are an NCR tech and will need to be escorted to the communication/network room.
3. Locate new equipment and unpack boxes; verify inventory received;
   Two (2) Ciena 3906, minimum of (4) power cables, patch cables, CAT 6 cable for DMARC extension, SFP's and sim card.
4. Do NOT remove the ASA firewall from the rack until instructed by the bridge engineer.
5. Verify and locate circuit demark, verify circuit handoff is 1000 Base-T RJ-45.
6. Rackmount Ciena equipment, cage nuts provided may not work with the equipment, please buy some prior to dispatch.
   Please keep the receipt as it will be needed for reimbursement purposes.

** Important, please do not install new equipment into the rack if the rack is mounted high off the ground. Equipment will need to be tested before mounting them into the rack to ensure tech will not be on the ladder and consoled into the switch at the time for testing. Once all equipment is tested, then the equipment can be racked. If the rack is not mounted high off of the ground, disregard.

7. On the right side of the Ciena 3906 (by loosening the thumb screws), take off the cover to expose the FRU Module card. Capture a clear photo of the label.
8. Inspect the battery to ensure that it does not have a plastic battery tab on the connector. If there is a plastic tab, remove it and re-install the battery into the slot- (hand tighten the screws to secure the cover to prevent stripping or breakage.)
9. If there are SFP's installed in both Ciena 3906, we need to unplug the SFP's and leave it in the port NOT connected (if it is left connected it will disable ports 1 & 2.)
10. Tech to Connect to the bridge and work with remote engineer.

    a) Take a picture of the customer equipment and patch panel before removing any equipment.
    b) Technician will connect laptop to the LTE mobile hotspot

11. Engineer on the bridge will instruct when to power up the equipment. (Equipment has already been pre-configured for Zero Touch Provisioning, it should come up and properly connect to the network.)
12. Connect laptop to the hot spot and the management port of the equipment (3906) using a straight through cable (this will allow the remote engineer to perform remote control using a Webex or Teamviewer.)
13. Change the IP Address on your laptop per instructions on the work order.
14. Cable the patch ports on each 3906 as indicated by the bridge.

15. Take pictures of installed 3906 and patch cables, pictures of patch panel, and any equipment that was worked on and the work area.
16. Contact Remote engineer to verify the testing. Based upon input from the remote engineer, perform any additional requested functions.
17. Remove two Cisco ASA firewalls, and package them in the boxes in which the Ciena 3906 devices were shipped, using packing tape that you brought.
18. Attach tracking label on box. Capture photo of the tracking label. Boxes will be left near where the ASAs were de-installed, ** Inform Lowes personnel/MOD and capture the name.

** If the Bridge engineer or the Lowes IT informs the tech to leave the old equipment in the rack, please document who signed off on leaving the equipment in the rack.

19. Capture required pictures:

- Serial number for each Ciena 3906 located on the Front Left of the devices.
- FRU number for each Ciena 3906 located on the Front Right of the device.
- Picture of the Circuit connection
- Picture of where the old equipment (ASA Firewall) was left
- Picture of the tracking label on the box of the old packaged ASA Firewall
- Distance and close up photos of Before and After of the patch panel
- Distance Before and after photos of the work area
-Perspective Distance photo of the Network Rack.

Pictures must be sent to the team Distro and verified before leaving the site and checking out to ensure we have clear pictures of the serial numbers of the chassis and serial numbers for the FRU label and all necessary pictures needed for the customer. Team distro email: NCR-Lowes@osbt.com

** Technician cannot leave the site until the tech is released from site by the engineer and the site contact. Please ensure to document the remote engineers name that you worked with.

20. Once the remote engineer releases you, cleaned up the work area, gather AFTER site photos, get work order signed, and call into the OSBT Call Center to check out prior to leaving site.

Stress the importance of bringing the required materials to site!

Note to tech: if any of the following is needed onsite and not brought with them and the site fails, it can result in a customer's billing dispute later and will be unpayable.

o Standard Data Technician Tools
o LTE hotspot (either a separate device or configured on a Smart Phone connected to their laptop)
o Laptop -**MUST BE WINDOWS 10! NO EXCEPTIONS!!! Must have RJ45 Port!!!** once we console in to the Ciena device, it disables the wireless on your laptop and then you will not be able to connect to your LTE hotspot. With a windows 10 laptop it does not disable your wireless, that is why we require Windows 10.

- laptop must have PuTTY Pre-installed
- laptop must have WebEx & Team Viewer Pre-installed
- laptop must have RJ 45 ethernet port!

o RJ45 to RJ 45 Ethernet (Straight through cable)
o CAT 6 Patch Cables
o 300 FT of CAT 6 Cable
o Twelve (12) Cage nuts with screws (VERY IMPORTANT as this will be used to mount the equipment)
o Serial Console Cable (USB to DB-9)

- Console Cable (Ciena DB-9 to RJ-45)
- A cell phone with a digital camera
- Velcro and Zip ties
- Packing Tape
- Power Strip
- Standard Power Cable (2) - (NCR has specifically request that the tech carry 2 standard power cables for cases where the equipment shipped to site has the wrong power cables in the box).

MUST ACT PROFESSIONALLY AT ALL TIMES AND UNDER NO CIRCUMSTANCES -HAVE CANDID CONVERSATIONS IN THE PRESENCE OF THE CUSTOMER.

If there are any questions about the SOW, you can call into the OSBT Callcenter who can get you with a PC/PM to assist.
If during install night, there are any questions, techs can reach out to our night support, Rohan and Dorian.