SkyLIGHT™ VCX Controller User Manual

Firmware Release 1.1

Published

July 3, 2015

Document Revision: 1

Released on July 3, 2015.

Accedian Networks Inc.

Attention: Technical Publications
2351 Alfred-Nobel Boulevard, Suite N-410
Saint-Laurent, Québec
Canada H4S 2A9

Tel: 514-331-6181
Fax: 514-331-2210
Toll free: 1-866-685-8181
support@accedian.com
accedian.com

Contents

1 About This Manual

Intended for network designers and network administrators, this document will help in the design, configuration and use of Accedian's network solutions such as the SkyLIGHT VCX Controller. The term "unit" in this document refers to an instance of the VCX Controller. The term "management Web interface" refers to the Web-based interface that is used to access the VCX Controller.

A VCX Controller can be viewed as an *extended* Performance Element, since it is equipped with multiple (i.e., over 100) virtual communication ports. Accedian Performance Modules (ants, Nanos) are linked to the VCX Controller and provide the physical ports used for communication with the VCX Controller.

1.1 Organization

This document contains an introduction, as well as several chapters of detailed procedures and examples.

The **Introduction** chapter provides information about technologies and standards used in Accedian's equipment.

The various chapters containing information and procedures for configuring the equipment are as follows:

- "Managing the SkyLIGHT VCX Controller"
- "Managing Remote Devices"
- "Configuring the SkyLIGHT VCX Controller"
- "Managing Ports"
- "Managing Traffic"
- "Managing Loopbacks"
- "Monitoring Network Performance with Service OAM"
- "Testing Network Performance"
- "Managing Alarms and System Messages"

Tables of parameters are provided to help you understand the function of each parameter that is available for a particular feature. Whenever possible, parameters are listed in the order in which they appear in the interface.

Typographical standards for this document are provided in "Conventions" on page 3.

1.2 Conventions

This manual uses certain types of document conventions to help you distinguish between commands, keywords and language elements. Furthermore, special formatting elements have been added to draw your attention to certain types of information.

The conventions described below appear throughout this manual:

Commands and keywords are presented in **bold**.

Menu options when navigating in the Web interface's menu system are shown as follows: **SOAM ▸ CFM ▸ DMM ▸ Configuration**

Brackets [ ] are used when several options are available and you need to select a specific option. For example, in the following line you need to select a specific port name when you reach the PHY page: **Port ▸ PHY ▸ [Port name]**

Alarm numbers are composed of three parts: x.yyyy.zz. The first number (x) refers to a general category. The second number (yyyy) refers to the specific component. The third number (z) is the specific alarm code. For example, in 2.0001.01, the 2 refers to SFP modules, 0001 is for SFP-1 and 01 means temperature high alarm. So, 2.0001.01 means SFP-1 temperature high alarm. In the alarm descriptions, <SFP module> can refer to any SFP module, depending on the value of the component number yyyy.

Note: Information that emphasizes or supplements points within the main text. Notes often provide details that only apply in certain situations.

Tip: A suggestion or hint concerning the procedure being described. Tips may suggest an alternative method or clarify product capabilities.

***CAUTION**: Describes a situation where failure to take or avoid a specified action could result in damage to equipment.*

1.3 References

The use of solutions such as the SkyLIGHT VCX Controller involves the understanding of different networking standards, technical specifications and technologies. This document provides basic information on the standards and technologies. For more information about the standards and technical specifications, refer to the following:

- IEEE 802.1ag – Connectivity Fault Management
- RFC-2544 – Benchmarking Methodology for Network Interconnect Devices
- RFC-5357 – Two-Way Active Measurement Protocol
- Technical Specification MEF 17 – Service OAM Requirements & Framework – Phase 1
- Technical Specification MEF 6.1 – Ethernet Services Definitions – Phase 2
- Technical Specification MEF 10.2 – Ethernet Services Attributes – Phase 2

2 Managing the SkyLIGHT VCX Controller

This chapter contains the following sections:

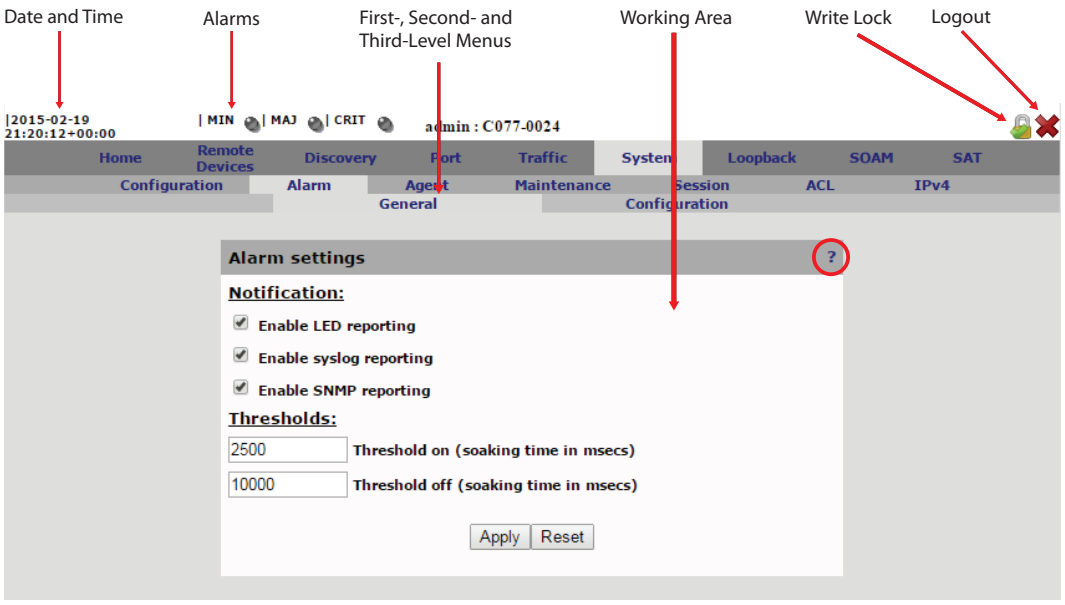
2.1 About the Management Web Interface

The Web-based management interface provides secure access, via an SSL client, to all system control, management and monitoring functions. It is running within a virtual machine.

The management station is the computer that you use to connect to the management Web interface; it must be equipped with a JavaScript-enabled Web browser (such as Mozilla Firefox, Google Chrome or Microsoft Internet Explorer v6.0 or later) installed.

The elements of a typical user interface screen are shown below. Help is available for each page of the interface by clicking the question mark icon (**?**) to the right of the section title bar.

Typical Screen



Date and time: The date and time configured on this instance of the VCX Controller. To set the date and time, access the page **System ▶ Configuration ▶ Time**.

Alarms: Indicates alarms that have been triggered. For more information on alarms, refer to the chapter "Managing Alarms and System Messages" on page 147. Beside the alarms, the username of the currently-logged in user along with the VCX Controller's serial number appears.

Working area: This is where you view information and configure system parameters.

First-, second- and third-level menus: The top row presents the first-level menu, and is always visible. The second row presents a menu of second-level options based on the item selected from the first-level menu. The third-level items are dependent on the option selected from the second-level menu.

To navigate to the various Controller functions, click an item from the first-level menu, then click a second-level menu item until you access the function you want to use. Each menu item you select will be highlighted. For example, in the figure above, the selected menu item is **System ▸ Alarm ▸ General**.

Selecting a third-level menu option often displays a summary of the information requested. If you then click one of the elements listed in the summary, you will obtain detailed information on that element. The parameters present on both the summary and detailed pages are described within one table in this manual. For example, the table for **System ▸ Session ▸ Permissions** describes all parameters present on both the summary page for all sessions and the detailed page for a specific session. The parameters are listed in the tables in the order in which they appear on the screen, wherever possible.

Writelock button: Use this button to toggle between *yes* and *no* for **Writelock**. For more information about this function, refer to the section on "Locking or Unlocking User Sessions" on page 22.

Logout button: Use this button to logout from the current session.

Reset: Use this button to reset the value of a page, before you apply the change. This is useful when you are not sure precisely which values you changed and want to start over using the previous configuration. This action has the same effect as leaving this page to view another page and then returning to this page. Available on some pages only.

Apply: Use this button to apply the changes made on the page to the equipment. This action changes the equipment configuration immediately. Available on some pages only.

Search: Use this button to filter any list shown on a page to narrow down the list to elements you have specified on the drop-down list. Once you have the desired list shown on the page, you can also click this button to refresh the status and values of each field. For example, this can be useful in a **Results** page, helping you to view the changing results while a test is performed.

> *Note: Using your browser's **Refresh** command **does not** simply refresh the values or list shown on one page; it reloads the page completely, thereby eliminating any filter that you had previously applied.*

2.2 Starting the Management Web Interface

2.2.1 Physically Connecting to the SkyLIGHT VCX Controller

Before logging in to the unit via the Management Web interface, you must first establish communication between your workstation and the VCX Controller, which is running on a virtual machine:

- Connect your workstation's *LOCAL-1* network interface to the LAN where the physical server (i.e., hypervisor or virtual machine monitor) running the VCX Controller's virtual machine is also located.
- Bridge the *LOCAL-1* network interface of the physical server running the VCX Controller's virtual machine to the corresponding interface on the virtual machine.

Once the virtual machine is powered on and actively running, you are ready to login and configure the SkyLIGHT VCX Controller for the first time.

2.2.2 Logging In

Once you have a physical connection to the equipment, you can login. Depending on the configuration of the unit, you may login in different ways. You would usually connect to the SkyLIGHT VCX Controller for the first time using the Management port. Normally you would then configure another interface, e.g. Network, for in-band management through the network.

▶ **When logging in for the first time**

1. Assign the VCX Controller a static IP address belonging to the same subnet as the equipment to which you want to log in. The address **192.168.1.254** is used in this procedure.
2. Start your Web browser and enter the following in the address bar: **https://192.168.1.254**.

   Note: This is the factory default IP address of each instance of the SkyLIGHT VCX Controller. If you are using static IP addresses, you should then modify the VCX Controller instance's IP address to be unique, thereby avoiding duplicate IP addresses with other factory default units. As an alternative, you can also configure the VCX Controller to use DHCP.

   For more information on modifying IP addresses, using DHCP and other options for logical interfaces, refer to "Configuring the Logical Interfaces" on page 15.

3. The login page for the VCX Controller opens. Login as **admin** with the password **admin**.

   Note: This is the default password for the user "admin", which is a special user account that has been granted full read/write access to all the VCX Controller's settings. It is strongly recommended to change the default admin password after your first login; doing so ensures that only the admin user can perform admin functions and control access to the VCX Controller. To change the password, refer to the section "Changing Passwords" on page 30.

▶ When logging in for the first time (if you have already configured another logical interface)

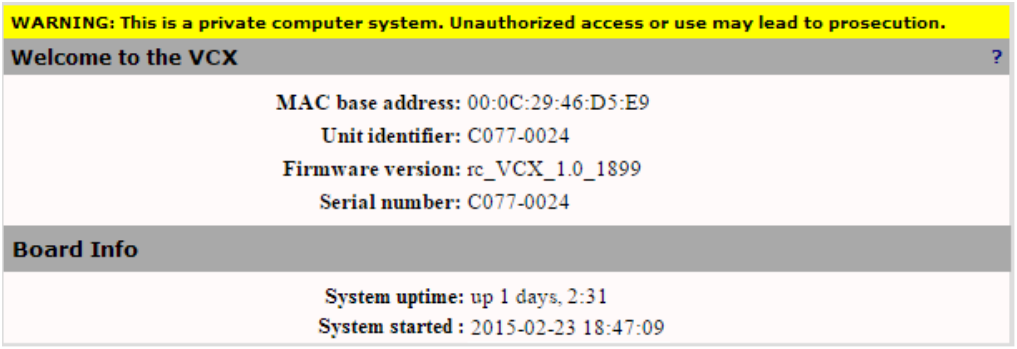
1. Ensure your management station has a route to the equipment.
2. Launch your Web browser and enter the equipment address in the address bar, e.g. **https://192.168.1.254** (or **host_name.domain_name** if you are using a DNS).
3. The login page opens. Login using the admin username and account password.

2.2.3 Working in the Home Page

The home page provides general information about the SkyLIGHT VCX Controller.

To view the home page shown in the figure below, access the page **Home**.

Home Page



For information on specific parameters displayed on the home page, refer to the following table.

Home Page Parameters (Home)

Parameter	Description
MAC Base Address	The base MAC address of the SkyLIGHT VCX Controller.
Unit Identifier	The name that identifies the SkyLIGHT VCX Controller on the network

Parameter	Description
Firmware Version	The version number of the firmware running on the SkyLIGHT VCX Controller. Access the page **System ▸ Maintenance ▸ Firmware** to upgrade the firmware.
Serial Number	The serial number assigned to the SkyLIGHT VCX Controller
Board Info	
System Uptime	The period of time that has elapsed since the SkyLIGHT VCX Controller was last restarted, whether it be following a firmware upgrade, a manual reboot or a power cycle
System Started	The time when the SkyLIGHT VCX Controllerwas last powered on, as reported by the system clock. To set the system clock, see **System ▸ Configuration ▸ Time**. *Note: This value is reset when a power cycle is performed on the SkyLIGHT VCX Controller.*

2.2.4 Modifying the SkyLIGHT VCX Controller'sUnit Identifier

The default host name (or unit identifier) is the serial number assigned to the SkyLIGHT VCX Controller; it is displayed in the banner at the top of the screen after logging in. You can change the host name to a name more meaningful to your organization or use other DHCP host name options. The **Host Name** identifies the SkyLIGHT VCX Controlleron the network and can be used when you login to it, as shown in the figure in the section "About the Management Web Interface" on page 6.

> *Note: The host name is also used in the CLI prompt and is added to system log entries to help you identify the SkyLIGHT VCX Controller more clearly.*

▸ To modify the SkyLIGHT VCX Controller's unit identifier

1. Access the page **System ▸ Configuration ▸ DNS**.
2. Enter the new unit identifier in the **Host Name** field.
3. Click **Apply** to save your changes.

For information on specific parameters, refer to the following table.

DNS Parameters (System ▸ Configuration ▸ DNS)

Parameter	Description
Use DHCP Results	Enables use of DNS settings obtained via DHCP. You can then select the interface to use for obtaining DHCP information using **From Interface**.

Parameter	Description
Host Name	The name that identifies the SkyLIGHT VCX Controller on the network. A maximum of nine alphanumeric characters is supported. This parameter is only valid when DHCP host name is set to **Current Hostname**.
DHCP Host Name	The source of the DHCP host name The available options are: • **Current Hostname**: The host name is the string entered in the **Host Name** field. • **Serial Number** (DHCP option 12): The host name is the serial number of the SkyLIGHT VCX Controller. • **Custom Hostname** (DHCP option 12): The host name is the text string you enter in the field to the right of the **DHCP Host Name**.
Field to the right of DHCP host name	This field is only used when the DHCP host name is set to **Custom Hostname**.
DHCP Client ID	This corresponds to DHCP option 61. It allows you to enter a text string for use as the SkyLIGHT VCX Controller's unique identifier when communicating with the DHCP host. When the text box is empty, the MAC address is used as the SkyLIGHT VCX Controller's client ID.
From Interface	The interface used for obtaining DHCP information *Note: This field is only available when the* **Use DHCP Results** *option is enabled.*
DNS Server 1	The address of DNS server 1 is available only when **Use DHCP Results** is not selected.
DNS Server 2	The address of DNS server 2 is available only when **Use DHCP Results** is not selected.
Domain	The local domain name associated with the DNS is available only when **Use DHCP Results** is not selected.

2.2.5 Managing SSL Certificates

The SSL protocol is used to secure the communication over the Internet between the management station and the SkyLIGHT VCX Controller. You must load a valid SSL certificate, from a certificate authority, into the VCX Controller, to provide secure

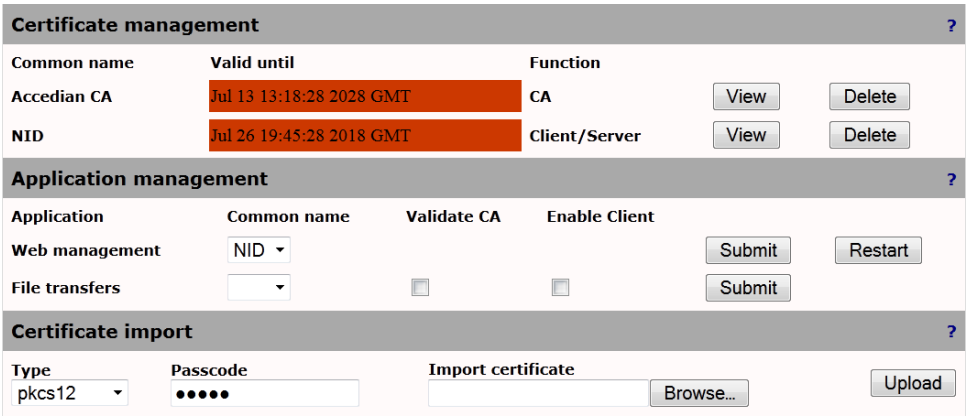
communication. To learn more about certificates, refer to the certificate authority and *ITU-T Recommendation X.509*.

> *Note: You may install the SSL certificate in each browser that you want to use when connecting to the VCX Controller.*

In other cases, you may want the VCX Controller to communicate with other applications such as an FTP server. You can configure the VCX Controllerfor secure communication with these applications by using **Application Management**, therefore managing the validation of certificate use.

Access the page **System ▸ Maintenance ▸ Certificates** to manage SSL certificates.

System ▸ Maintenance ▸ Certificates



You can view the SSL certificates installed on the VCX Controllerin the **Certificate Management** section. To view the details of the installed certificates, click the **View** button.

To delete a certificate, click the **Delete** button.

To import a new certificate, select the certificate by using **Browse** in the **Certificate Import** section, complete the other fields and click **Upload** when ready. The certificate will be loaded into the VCX Controllerand will appear in the **Certificate Management** section.

To assign a certificate to a specific application such as an FTP server, select it from the **Common Name** drop-down list in the **Application Management** section. Complete the other parameters as required, then click **Submit** to assign it to the application.

> *Note: If you submitted a certificate for **Web Management** (the one you are using right now), you must restart the Web GUI interface session by clicking **Restart**. As the interface's web server restarts, a message will be briefly displayed before the login page appears.*

For information on specific parameters, refer to the following three tables.

Certificate Parameters (System ▸ Maintenance ▸ Certificates)

Parameter	Description
Common Name	For a certificate authority (CA), this is the name of the organization that issued the certificate.

Parameter	Description
	For a server, this is the Fully Qualified Domain Name of the service using the certificate (only the Web server at this time). For a client, this may be the name of the application.
Valid Until	The date when the certificate expires. It may still be valid if the peer has disabled checking.
Function	Describes how the certificate can be used in the VCX Controller. • **CA**: Used to validate peer certificates; provided as part of the certificate chain for server applications • **Client/Server:** These certificates were imported with a private key. It is possible for a CA certificate imported with a private key to be used for this function. In this case, it does not show up as a CA.

Application Management (System ▶ Maintenance ▶ Certificates)

Parameter	Description
Application	The available options are: • **Web Management**: This is the application you are currently using. • **File Transfers**: All applications sending or receiving files through a secure channel (HTTPS or FTPS). For example firmware upgrades and configuration import/export using the CLI.
Common Name	For a certificate authority (CA), this is the name of the organization that issued the certificate. For a server, this is the Fully Qualified Domain name of the service using the certificate (only the Web server at this time). For a client, this may be the name of the application.
Validate CA	For client applications, perform peer certificate validation. This includes expiration date, hostname and CA chain.
Enable Client	For client applications, enable or disable the use of the selected client certificate.

Certificate Import (System ▶ Maintenance ▶ Certificates)

Parameter	Description
Type	The following certificate file types are supported: • **pkcs12**: For importing client certificates, including the private key and the CA chain of certificates • **pkcs7**: For importing multiple CA certificates • **x509-PEM** For importing either: – A client or server certificate and its private key – A single or multiple CA certificate • **x509-DER**: For importing single CA certificates *Note: Importing a private key separately from its certificate is not supported.*
Passcode	Applies to pkcs12 or PEM encoded private keys, which use a pass code. The pass code is only used once for importing.
Import Certificate	The name of the selected certificate appears here before you upload it.

2.3 Configuring the Logical Interfaces

You can define one or more **logical interfaces** for managing the VCX Controller instance; the types of interfaces available include standard IPv4, VLAN, or VLAN-in-VLAN interfaces. Once the interface is defined, you can also define a route to access the VCX Controller from outside its management subnet.

You can configure interfaces for dual homing by specifying a second IP address (IP address alias). When specifying an alias, only the address, network mask and gateway parameters can be defined. An alias interface is always set up as a static IP address (no DHCP).

> *Note: An interface can also be used for other purposes. For example, you can use an interface for loopback or for test set interaction.*

The following types of logical interface are available:

- **Standard**: This interface type is associated with a single port. You would use a standard interface to manage the SkyLIGHT VCX Controller from one defined port.
- **VLAN**: Like standard interfaces, this interface type is also associated with a single port. An example of when you would use a VLAN interface would be if you want to separate the management traffic from the client traffic. In this example, you would create a VLAN for the management and another VLAN for the customer traffic. Using filters and policies, you would 'drop' the management traffic and permit the customer traffic to flow through the VCX Controller. For more information on filters and policies, refer to the chapter "Managing Traffic" on page 89.

  > *Note: Setting up policies and filters in this manner does not prevent the Management VLAN traffic from communicating with the SkyLIGHT VCX Controller.*

- **VLAN-in-VLAN (.1q in .1q)**: This interface type is also associated with a single port. You can use this interface type when you want to use sub-VLAN. With a VLAN-in-VLAN interface, you can assign priority and choose the Ethertype.

By default, the following logical interfaces are defined:

- **Management**: The default interface (type **Standard**) that enables access to the management Web interface via the management port

▶ To view a logical interface

1. Access the page **System ▶ Configuration ▶ Interface**.

   A listing of all logical interfaces associated with this instance of the VCX Controller is displayed.

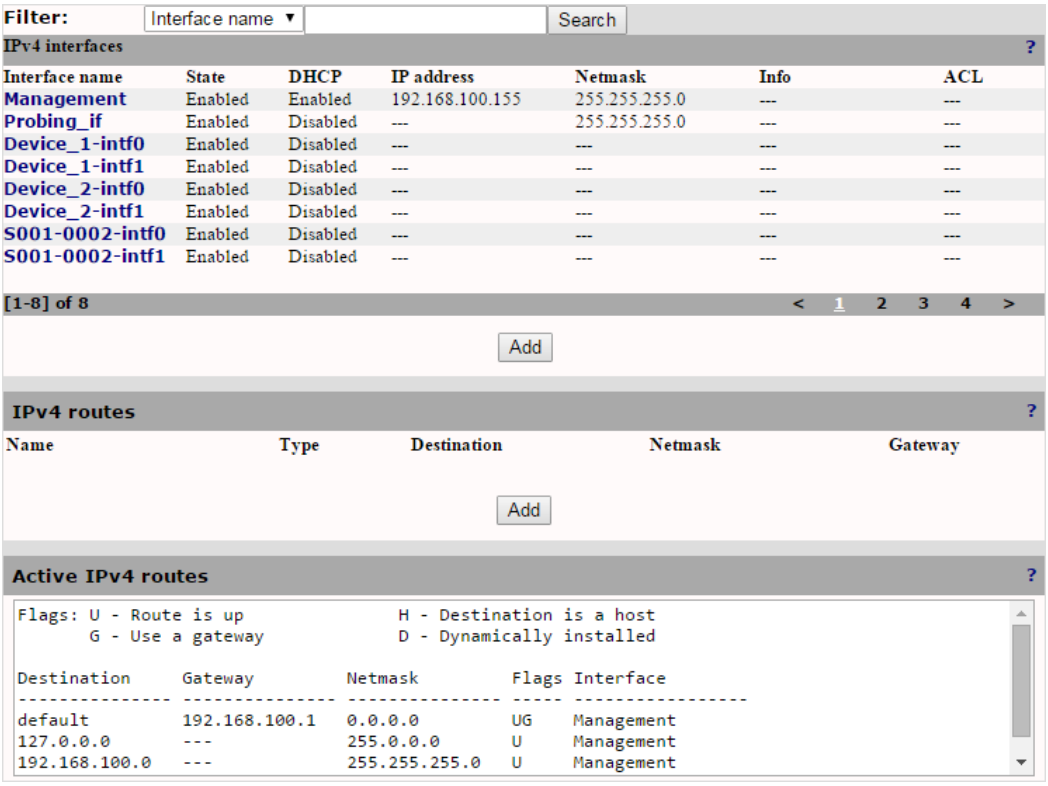
   The total number of interfaces found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for

example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain interfaces, enter a value on which to filter, then click **Search**. You can filter by the interface name, interface state, IP address, netmask, the info field value, ACL, or whether or not DHCP has been enabled.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

System ▸ Configuration ▸ Interface



For information on specific parameters, refer to the table "Interface Settings (System ▸ Configuration ▸ Interface)" on page 17.

2.3.1 Adding or Editing a Logical Interface

After a factory default reset, a logical interface named **Management** is bound to a port. For details, refer to "Physically Connecting to the SkyLIGHT VCX Controller" on page 8. You can add and edit more logical interfaces to provide the VCX Controller with multiple management options.

> ***CAUTION**: If you modify an interface, you or another user may lose access to the management Web interface.*

▶ To add or edit a logical interface

1. Access the page **System ▶ Configuration ▶ Interface**.
2. Click **Add** to create a new interface or click the **Interface Name** of an existing interface to edit its settings.

   Note: You cannot modify a remote interface's IPv4 settings when adding a new interface.
3. Complete the required fields, then click **Apply**.

   Note: The fields displayed will vary, depending on the Interface type you select.

   Note: You can set the IP address for an interface to 0.0.0.0 when the interface is not required to be an IP interface, such as when the interface is used for loopback or test set interaction.

For more information on specific parameters, refer to the following table.

Interface Settings (System ▶ Configuration ▶ Interface)

Parameter	Description
All Interface Types	
State	Enabled or disabled
Interface Name	A name to identify the interface
Interface Type	• **Standard**: Standard IP interface associated with a single port • **VLAN**: VLAN interface associated with a single port • **VLANinVLAN**: VLAN-in-VLAN (.1q in .1q) interface associated with a single port
On Port(s)	The port on which the interface is active *Note: The list provided corresponds to the local ports on the VCX Controller, as well as the remote devices' ports.*
IPv4	
Automatic IP (DHCP)	Allows the interface to act as a DHCP client and automatically obtain its IP address, DNS server and gateway settings from a DHCP server
Use DHCP Route Information	Allows the SkyLIGHT VCX Controller to obtain routing information from the DHCP server
Use Static IP Until	Uses the manually configured IP address on the interface until

Parameter	Description
DHCP Response	an address is resolved by DHCP *Note: Available only when using Automatic IP (DHCP) mode. Not available with Auto interface.*
Manual Configuration	Select this box to enable manual configuration of the IP address settings
IP Address	IP address assigned to the interface, if required
Network Mask	The network mask associated with the IP address, if required
Default Gateway	A default gateway address provides a shortcut to creating a default gateway through the route configuration. Only one default gateway can be set per unit.
IP Address Alias	A second IP address that you may assign to the interface if dual homing is required. This address must belong to a different subnet than the primary IP address.
Network Mask Alias	The network mask associated with the IP address alias, if required
Default Gateway Alias	The default gateway associated with the IP address alias, if required
VLAN Settings (**VLAN** and **VLANinVLAN** Interface Types Only)	
VLAN ID	VLAN ID (Management VLAN) assigned to the interface
VLAN Priority	VLAN priority of 0–7
Ethertype	Ethertype for the first and second VLAN IDs. The Ethertype may vary, depending on the equipment to which the VCX Controller is connected: • **C-VLAN**: 0x8100 • **S-VLAN**: 0x88A8 • **T-VLAN**: 0x9100
ACL Settings (**All** Interface Types)	
ACL State	Enable or disable the use of ACL for this interface
ACL	The ACL assigned to this interface
ACL Types	Enable or disable the use of ACL for each management type: • **CLI**: SSH and Telnet

Parameter	Description
	• WEB • SNMP

2.3.2 Adding or Editing an IPv4 Route

You can define an IPv4 route that is outside the subnet defined by each interface that is bound locally to a VCX Controller in order to access a remote device that is not in the management station's subnet.

Access the page **System ▸ Configuration ▸ Interface** to view the existing, active IPv4 routes and update their settings.

▸ To add or edit an IPv4 route

1. Access the page **System ▸ Configuration ▸ Interface**.
2. In the *IPV4 Routes* section of the screen, click the **Add** button to add a new route or click the route **Name** to edit an existing route.
3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

IPv4 Route (System ▸ Configuration ▸ Interface)

Parameter	Description
Name	The name to assign to the route. It can also be a brief description of the route, such as *Default Route*.
Type	The route type may be either *Network* (for a range of addresses) or *Host* (for a specific IP address).
Interface	The interface with which the route is associated. The list of interfaces only includes the local interfaces that have been bound to the VCX Controller itself.
Destination	The route's network or host address. The default IPv4 destination is *0.0.0.0*.
Network Mask / Netmask	The mask assigned to the route *Note: Only used for Network routes.*
Gateway	The gateway associated with this route

2.4 Finding a Host (Ping and Traceroute)

The equipment provides ping and traceroute functions to help administrators troubleshoot network problems.

- Use the **ping** function to verify whether a specific host (IP address) is reachable.

  Note: Ping can be used to reach a logical interface bound to a remote device's port.

- Use the **traceroute** function to identify the route used by an IP packet to traverse the network and reach a specific destination.

▶ To ping a remote host

1. Access the page **System ▶ Maintenance ▶ System Tools**.
2. Enter the host **IP address** and the **timeout** and click the button.

▶ To trace a route to a remote host

1. Access the page **System ▶ Maintenance ▶ System Tools**.
2. Enter the host **IP address** and the maximum number of **Hops**, then click the button.

For more information on specific parameters, refer to the following two tables.

Ping (System ▶ Maintenance ▶ System Tools)

Parameter	Description
IP Address	The IP address to which to send a ping message
Timeout	The number of ping messages to send before timing out Acceptable values range from *1* to *10*.
Ping	Executes an IPv4 ping

Traceroute (System ▶ Maintenance ▶ System Tools)

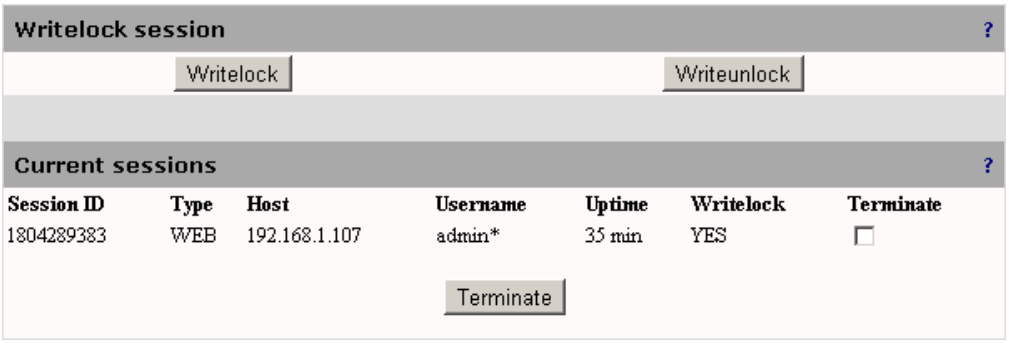
Parameter	Description
IP Address	The IP address to traceroute
Hops	The number of hops to attempt Acceptable values range from *1* to *30*.
Traceroute	Executes an IPv4 traceroute

2.5 Managing Sessions

The SkyLIGHT VCX Controller's management system provides multiple configurable management sessions to allow multiple users to control the VCX Controller. A writelock mechanism has been implemented to prevent two users from writing changes to the VCX Controller at the same time.

To view current sessions, access the page **System ▸ Session ▸ Management**.

System ▸ Session ▸ Management



For more information on specific values, refer to the following table.

Current Sessions (System ▸ Session ▸ Management)

Parameter	Description
Session ID	Session identification number
Type	Interface the session is using
Host	IP address of the management station for that session
Username	The user account that is currently logged in. An asterisk (*) appears beside your own session.
Uptime	How long the session has been active
Writelock	Indicates which session has the ability to make configuration changes
Terminate	Selecting one or more sessions then clicking **Terminate** forces a log out

2.5.1 Terminating a User Session

It may be sometimes necessary to terminate one or more sessions.

> *Note: You need the right privileges to terminate a session. Refer to "Managing Users and Privileges" on page 26.*

To terminate a session, access the page **System ▸ Session ▸ Management**, select the session you want to terminate by checking the **Terminate** check box and the **Terminate** button. The session is immediately terminated and the current user is logged out.

2.5.2 Locking or Unlocking User Sessions

Administrators can communicate with the SkyLIGHT VCX Controller within a particular session. Users open their own sessions to administer the VCX Controller. Since the Web interface supports concurrent sessions, to maintain the integrity of the configuration settings, only one user at a time has the ability to make changes.

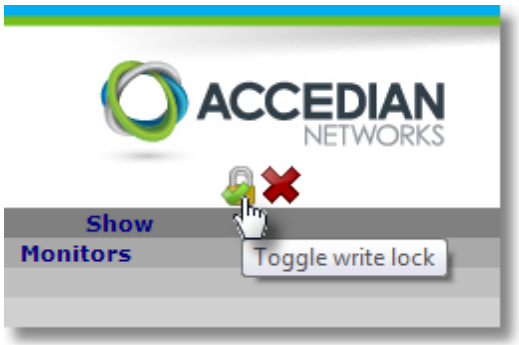
To lock a session for write access, access the page **System ▸ Session ▸ Management** and click the **Writelock** button. Only you will have access to modify parameters of the VCX Controller. The other users will only be able to view its configuration.

To unlock a session for write access so other users can lock it, access the page **System ▸ Session ▸ Management** and click the **Writeunlock** button. You will no longer be able to modify parameters on the VCX Controller.

Writelock (System ▸ Session ▸ Management)

Parameter	Description
Writelock	Locks your session so that only you have write access
Writeunlock	Unlocks write access so that is available to other users

> *Note: You can also control the locking and unlocking of your session using the **Writelock** button located at the upper-right corner of the Web interface.*



2.5.3 Configuring Session Options

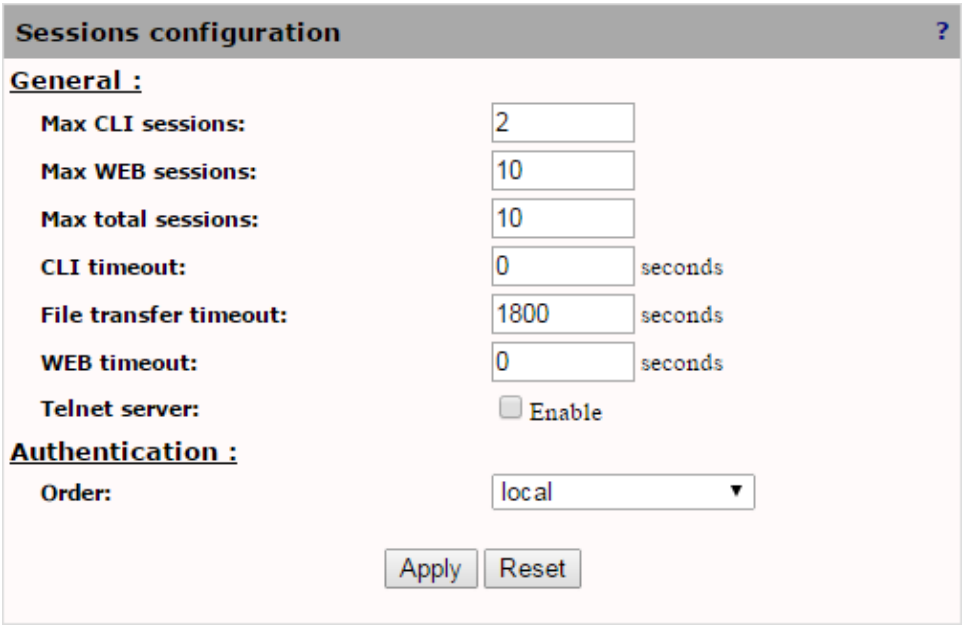
Use this page to configure the following session-related parameters:

- The maximum number of CLI sessions allowed
- The maximum number of web interface sessions allowed
- The maximum number of total sessions (CLI and web combined)
- The CLI timeout value
- The file transfer timeout value, to ensure firmware updates and configuration maintenance entities have sufficient time to load successfully
- The web interface timeout value
- Whether or not a telnet server is enabled
- The authentication order when users log in to the system

▶ To configure session parameters

1. Access the page **System ▶ Session ▶ Configuration**.
2. Update the various session configurations parameters, then click **Apply**.

System ▶ Session ▶ Configuration



For more information on specific parameters, refer to the following table.

Session Configuration (System ▶ Session ▶ Configuration)

Parameter	Description
General	
Max CLI Sessions	The maximum number of concurrent CLI sessions that can be supported
Max WEB Session	The maximum number of concurrent management tool sessions that can be supported
Max Total Sessions	The total number of CLI and WEB sessions that can be supported
CLI Timeout	The maximum number of seconds that a CLI session can remain idle before it is automatically logged out
File Transfer Timeout	The maximum number of seconds that must elapse before a file transfer (firmware upgrade, history data file transfers, configuration files, etc.) is automatically terminated Minimum value is *900* (15 minutes); maximum value is *3600* (60 minutes). Default value is *1800* (30 minutes).
WEB Timeout	The maximum number of seconds that a management tool session can remain idle before it is automatically logged out
Telnet Server	The telnet server on the VCX Controller may be enabled or disabled
Authentication	
Order	The authentication method to use, in order of availability. The available options are: • **Local**: Validate locally only. • **Radius**: Validate on the RADIUS server only. • **Local-Radius**: Validate locally first; if the validation does not succeed, then validate on the RADIUS server. • **Radius-Local**: Validate on the RADIUS server first, and if the validation does not succeed, then validate on local server. • **Strict Radius-Local**: Validate on the RADIUS server first. If the authentication fails, access is denied. The fall back to local only occurs when the RADIUS authentication times out. • **TACACS+**: Validate on the TACACS+ server only.

Parameter	Description
	• **Local-TACACS+**: Validate locally first; if the validation does not succeed, then validate on the TACACS+ server. • **TACACS+-Local**: Validate on the TACACS+ server first, and if the validation does not succeed, then validate on the local server. • **Strict TACACS+-Local**: Validate on the TACACS+ server(s) first. If the authentication fails, access is denied. The fall back to local only occurs when the TACACS+ authentication process times out.

2.6 Managing Users and Privileges

With Vision EMS, you can configure each unit to be managed by several users, each with different privileges. Privileges, also referred to as *permissions*, are used to grant precise levels of access to different user groups. You may choose to limit certain users to only specific configuration options, such as firmware updates, ports or traffic, while others have full access to all features.

Note: You must define the permissions to assign to user groups before defining the user accounts.

2.6.1 Setting Up the Administrator Account

One administrator account is created by default with username and password both set to **admin**. The username and password are case-sensitive. It is recommended that you change the default password immediately after installation to safeguard the system (refer to "Changing Passwords" on page 30). The administrator account provides access to all features.

Note: To prevent losing administrator access to the VCX Controller, you cannot modify the administrator account privileges or delete the administrator account.

***CAUTION**: If you, as the administrator, forget your username or password the only way to regain access to the management Web interface is to perform a factory reset. Refer to "Restoring Factory Default Settings" on page 70.*

2.6.2 Defining Permissions for a Group of Users

You must first define group permissions before you can assign users to groups.

▶ To define permissions for a group of users

1. Access the page **System ▶ Sessions ▶ Permissions**.
2. Click **Add** or click the **Group Name** that you want to edit.
3. Select the **Privileges** to assign to the selected user group, then click **Apply**.

   Note: You cannot change the privileges of user group Admin. This user group has full access to all functions.

For more information on specific parameters, refer to the following table.

Group Privileges (System ▶ Session ▶ Permissions)

Parameter	Description
Group Name	The name of the user permission group
Privileges	The privileges given to the user permission group allow its members to edit, add or enable within these sections. The following commands can be used by all users regardless of their privileges: • board • date • exit • help • ping • quit • sfp • syntax • tcp-connect • traceroute • version **ACL**: Edit/Enable ACL settings. **Alarms**: Edit/Add/Enable alarm reporting configurations. **CFM**: Edit/Add the SOAM CFM feature. **Config**: Import/Export configuration files through CLI. **Discovery**: Add/Edit/Delete/Show discovery instance **Feature-Suites**: Import/Delete/Show feature suites **Filters**: Edit/Add Layer-2 filters, IPv4 filters and VLAN: • filter **Firmware**: Upgrade the firmware. **FlowMETER**: Edit/Show FlowMETER information **History**: Edit the history bucket statistics. **Log**: Edit syslog configuration and view logged entries.

Parameter	Description
	Loopback: Add/Edit/Enable loopback **Management**: Edit/Add management access to the VCX Controller: • dns • interface • inventory • motd • ntp • route • sfp • snmp • snmp-trap **Policies**: Edit/Add/Enable policies for filtering traffic. **Port**: Edit/Add/Enable port configurations: • port • statistics **RFC-2544**: Add/Edit/Enable the RFC-2544 menu. **Remote-Device-Mgnt**: Add/Edit/Delete/Show remote device information **SAT-Reporting**: Edit/Enable Service Activation Testing reporting. **Security-Key**: Import/Test/Edit/Show remote device key management settings **Sessions**: Manage sessions and edit session configuration: • RADIUS • TACACS+ • reboot • session **TWAMP**: Edit/Enable TWAMP settings. **Users**: Edit/Add and manage user accounts and permissions:

Parameter	Description
	• permission-group • user **All-add**: Permission to add in all sections that are viewable **All-edit**: Permission to edit in all sections that are viewable **All-enable**: Permission to enable in all sections that are viewable

2.6.3 Adding or Editing User Accounts

▶ To add or edit a user account

1. Access the page **System ▶ Sessions ▶ Users**.

   A list of all user accounts that exist for this instance of the VCX Controlleris displayed.

2. Click **Add** or click a **User Name** if you want to edit a user account.

3. In the **[User name] user settings** page, complete the fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

User Settings (System ▶ Session ▶ Users)

Parameter	Description
User Name	The login name for the account
First Name	The account holder's first name
Last Name	The account holder's last name
Phone Number	The account holder's phone number
Email Address / Email	The account holder's email address
Password	Enter the password for this account
Confirm Password	Re-enter the password for this account

2.6.4 Administering User Account Privileges

You can grant different privileges or permissions to each user account, if you have already defined both the user account and permission groups.

▶ To give privileges to a user account

1. Access the page **System ▶ Sessions ▶ Users**.

2. Click the user name that you want to edit.

3. In the **[User Name] user settings** page, click the **Permission** button.

   The user's *User Permission* page is displayed. All available user permission groups are listed.

   Note: You can create more groups in the **Session ▸ Permissions** *page.*

4. Select the user groups that you want to assign to this user, then click **Apply**.

   ***CAUTION**: Modifying or reassigning the user groups for your account may result in you being unable to perform some tasks.*

2.6.5 Changing Passwords

▸ To change a user's password

1. Access the page **System ▸ Sessions ▸ Users**.
2. Click the user name that you want to edit.
3. Enter the user's new password in both the **Password** and **Confirm Password** fields, then click **Apply**.

   Note: If you forget your username or password, contact your Administrator for a password reset.

For more information on specific parameters, refer to the table "User Settings (System ▸ Session ▸ Users)" on page 29.

2.7 Using a RADIUS Server for Authentication

You can use a RADIUS server for authenticating users. When RADIUS authentication is enabled, the SkyLIGHT VCX Controller supports Authentication and Authorization as configured on the RADIUS server. A RADIUS server can be useful if you want to centrally manage user accounts instead of managing them on each instance of the VCX Controller individually. The VCX Controller can be connected to up to two RADIUS servers allowing for RADIUS server redundancy.

▶ To configure session parameters

1. Access the page **System ▶ Session ▶ RADIUS**.
2. Enter the various RADIUS configuration parameters, then click **Apply**.

For more information on specific parameters, refer to the following table.

RADIUS Configuration (System ▶ Session ▶ RADIUS)

Parameter	Description
General	
Authentication Method	The authentication method to use. The only option available is: **PAP**: Password Authentication Protocol
RADIUS Timeout	How long the RADIUS server will wait before retrying the connection. After the number of retries has been exhausted, a connection to the next configured server will be attempted, in which the same timeout and retry scheme apply.
RADIUS Retry	The number of times to retry the server before trying the next server configured
Realm	The string to append to the user's name using the *username@realm* method
Vendor-Specific attribute in Access-Request	Enable this box to include vendor-specific information as part of the RADIUS access request. Sending this information enables the RADIUS server to better identify the type of equipment requesting access.
Server-1 / Server-2	
Host	The RADIUS server host-name or IPv4 address
Port	The RADIUS server UDP port to which to connect
Secret	The shared secret for this RADIUS server
Source Address	The optional bind address for the RADIUS server

2.7.1 RADIUS Server Configuration Examples

The following examples are configurations for the RADIUS *server*, and not for the VCX Controller.

Two methods are supported by RADIUS servers for providing authorization using standard RADIUS attributes:

- **Callback-Id (id=20)**: Provides a fine-grained permissions mechanism. The permissions are the same as those that can be configured locally on the VCX Controller. The list of tokens is separated by commas. They can be a mix of locally-defined user permission groups and individual privileges. See also "Managing Users and Privileges" on page 26.
- **Service-Type (id=6)**: Provides for full admin privileges if attribute is set to "Administrative-User".

  Notes: You cannot view RADIUS assigned permissions with the CLI or Web-based interface. The permissions tokens are case sensitive.

The following are a few configuration examples for the RADIUS Server using these attributes:

- To assign a user to the built-in Admin group: **Callback-Id = "Admin"**
- To grant a user full administration privileges (same as first example): **Service-Type = "Administrative-User"**
- To give a user a list of individual privileges: **Callback-Id = "Config, Firmware, Log, Management, Users"**

If a user is authenticated by RADIUS but no attributes are specified in the server configuration, the permissions will be set as follows:

- Local permissions (i.e. as configured in the VCX Controller), if the username exists locally
- Viewer-only permission, if the username does not exist locally

2.8 Using a TACACS+ Server for Authentication

You can use a TACACS+ server for authenticating users. When TACACS+ authentication is enabled, the SkyLIGHT VCX Controller supports Authentication and Authorization as configured on the TACACS+ server. A TACACS+ server can be useful if you want to centrally manage user accounts instead of managing them on each instance of the VCX Controller individually. The VCX Controller can be configured to connect to a second TACACS+ server, allowing for TACACS+ server redundancy.

▶ To configure TACACS+ session parameters

1. Access the page **System ▶ Session ▶ TACACS+**.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

TACACS+ Configuration (System ▶ Session ▶ TACACS+)

Parameter	Description
General	
Authentication Method	The authentication method to be used by the TACACS+ server The only option available is: **PAP**: Password Authentication Protocol
TACACS+ Timeout	The lapse of time that the TACACS+ client will wait before retrying the connection, expressed in seconds After the specified number of retries has been exhausted, a connection to the next configured server will be attempted, for which the same timeout and retry scheme apply.
TACACS+ Retries	The number of times to retry the server before attempting to connect to the next configured TACACS+ server
TACACS+ Service Name	The name of the service to pass to TACACS+ for authorization, via the *Show Advanced Settings* box The default value is *shell*.
TACACS+ Privilege Attribute	The attribute to extract from the authorization response in order to determine the privilege level of the user requesting authentication, via the *Show Advanced Settings* box The default value is *priv-lvl*.
Server-1 / Server-2	
Host	The TACACS+ server's host-name or IPV4 address

Parameter	Description
	*Note: to disable this server, enter **0.0.0.0** or **::** as the address.*
Port	The TCP port on the TACACS+ server to which to connect
Secret	The shared secret for this TACACS+ server
Show Secret	Enable this box to display the shared secret for this TACACS+ server in plain text
Source Address	The optional bind address associated with this TACACS+ client *Note: This parameter is only used when the TACACS+ server validates the address of the VCX Controller.*

2.8.1 TACACS+ Server Configuration Examples

The following examples are configurations for the *TACACS+ server*, not for the SkyLIGHT VCX Controller. They apply to a *tac_plus* server; configuration values may differ for other servers.

Logging in is a two-part process. First, the user is authenticated. Once authenticated, the user may be authorized to gain rights on the system. The server should return AV (attribute-value) pairs for the requested service name.

The first attribute, the privilege level (usually **priv-lvl**), is evaluated first. This attribute is a numerical value that should be between *0* and *15*. On this system, an attribute value of 15 grants Admin rights (All-show, All-Add, All-edit), and all other attribute values grant Viewer rights (All-show). If the specified attribute value is not found, the login attempt is refused because the AV pair was not supplied by the server.

The second attribute, the privilege list (**accedian-priv-list**), is subsequently evaluated. This attribute is an optional attribute, and is ignored if the privilege level is already set to 15 (Admin). The purpose of this attribute is to provide a fine-grained permissions mechanism. The permissions are the same as those that can be configured locally on the VCX Controller. The list of tokens is separated by commas. The tokens you indicate can be a mix of locally-defined user permission groups and individual privileges.

> *Note: You cannot view TACACS+ assigned permissions with the CLI or Web-based interface.*
>
> *Note: Permission tokens are case-sensitive.*

Selected configuration examples for the TACACS+ Server using these attributes are given below.

▶ **To assign a user to the built-in Admin group**

```
user = tacadmin {
    login = cleartext tacadmin
    pap = cleartext tacadmin
    name = "Test Admin"
    # 'shell' service referred to as 'exec'
    # in the config
    service = exec {
        priv-lvl = 15
    }
}
```

▶ **To assign a user viewer-only privileges**

```
user = tacviewer {
    login = cleartext tacviewer
    pap = cleartext tacviewer
    name = "Test Tac Viewer"
    # 'shell' service referred to as 'exec'
    # in the config
    service = exec {
        priv-lvl = 1
    }
}
```

▶ **To assign a user a customized set of privileges**

```
user = taccfm {
    login = cleartext taccfm
    pap = cleartext taccfm
    name = "Test Tac User CFM"
    # 'shell' service referred to as 'exec'
    # in the config
    service = exec {
        priv-lvl = 1
        accedian-priv-list = CFM,PAA
    }
}
```

If a user is authenticated by TACACS+, but no attributes are specified in the server configuration, the permissions will be set as follows:

- **If the username exists locally**: Local permissions, as configured on the VCX Controller
- **If the username does not exist locally**: Viewer-only permissions

2.9 Managing Access Control Lists

You may use an Access Control List (ACL), which is a network access control mechanism, to prevent or allow specific MAC or IP addresses to access the VCX Controller for management purposes.

You can create up to 10 lists, and each list can contain up to 20 rules. Each rule allows or blocks addresses. Rules are prioritized using the **Priority** field, with the rule configured with the highest priority applied first.

It is recommended to set the priorities so the most restrictive rules are performed first. For example, a high-priority rule could grant access to a specific IP address within a subnet, and the next rule could deny access to the whole subnet, thus blocking all remaining IP addresses from that subnet. Another example would be to first deny access to subnet 10.10.10.0/26, then allow access to subnet 10.10.0.0/16.

> *Note: Once all rules have executed, all remaining frames are dropped (this is the default rule). You must therefore ensure the addresses you want to allow are accepted by at least one rule of the ACL.*

Once the ACL is created, you can then assign it to one or more interfaces. On each interface you can also select the type of protocol (CLI [SSH and Telnet], WEB, SNMP) to which the ACL applies. Refer to the section "Configuring the Logical Interfaces" on page 15.

> ***CAUTION**: If you assign a rule to an interface, you or another user may lose access to the VCX Controller.*

> *Note: ACLs apply to local interfaces only.*

2.9.1 Setting Up an ACL

▶ **To set up an ACL**

1. Access the page **System ▶ ACL**.

   A summary of all lists that have been configured is displayed. For more information on specific parameters, refer to the table at the end of this procedure.

2. Click **Add** to add a new ACL, or click the **Name** of an existing ACL to edit its settings.

3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

ACL Definition Summary (System ▶ ACL)

Parameter	Description
Name	The name of the ACL list
State	State of the list: • **Assigned**: The list is used by at least one interface. • **Unassigned**: The list is not currently used by an interface.
Interface List	Names of the interfaces using this list Clicking on an interface name will open the ACL statistics, showing the number of packets hit, on a per-rule basis, for this specific interface
ACL Definition	
Type	The type of ACL list: • **ipsrc**: IPv4 address values are filtered • **macsrc**: MAC address values are filtered
Value	The source addresses (IP or MAC) to filter. IP addresses can be entered using a subnet mask. If the **Type** is **ipsrc**: • Unique IPv4 address (ex: 192.168.0.100) • IPv4 subnet (ex: 192.168.0.0/24) If **Type** is **macsrc**: • Unique MAC address
Action	The filter action to take: • **Drop**: This rule drops CPU-destined frames/packets coming from the address specified in the field **Value**. • **Accept**: This rule accepts CPU-destined frames/packets coming from the address specified in the **Value** field. *Note: Frames/packets that are dropped from a higher-priority rule cannot be recovered with an **Accept** rule.*
Name	The name of the rule
Priority	The priority of the rule Range: 1-255, with 1 being the highest priority

Parameter	Description
State	Enable or disable the rule.
Packets	The number of packets that have been intercepted by the rule; • If the **Action** is set to **accept** for this rule, the number of packets accepted and sent to the CPU for processing. • If the **Action** is set to **drop** for this rule, the number of packets dropped.

2.9.2 Deleting an ACL

▶ To delete an ACL

1. Access the page **System ▶ ACL**.
2. Click the ACL **Name** to delete.
3. Click **Delete**.

▶ To view ACL statistics for each interface

1. Access the page **System ▶ ACL**.
2. Click the name of the interface in the **Interface List**.

   A count of **Packets** for each ACL rule defined is displayed. The **Default Dropped Packets** statistic (i.e., associated with the default rule) is displayed at the top of the page. For more information on specific parameters, refer to the table "ACL Definition Summary (System ▶ ACL)".
3. To clear the statistics, click the **Clear** button.
4. To update the statistics, click the **Refresh** button.

3 Managing Remote Devices

This chapter describes functions related to how remote devices are discovered and managed by the SkyLIGHT Controller; it contains the following sections:

3.1 About Remote Devices

One key feature of the SkyLIGHT VCX Controller is the ability to discover remote devices (i.e., Nano and antMODULE units) and maintain an inventory of them. These devices can be considered as extensions of the VCX Controller, which uses their ports to deliver system functionality remotely.

Each instance of the VCX Controller must know which remote devices are under its control, since it might discover devices that are intended for another Controller.

There are three ways in which you can associate a remote device with the appropriate instance of the VCX Controller:

- **Manual Definition**: Remote device parameters are entered in the VCX Controller one at a time.
- **Remote Device Definition List**: Parameters for multiple remote devices are imported as a batch through a CSV (Comma-Separated Value) file.
- **Via the Discovery Inventory**: Remote devices that have been discovered by the VCX Controller using the remote device discovery instances that were created in the **Discovery ▸ Configuration** page can be added here individually or in groups of up to 25 devices.

For details on both methods, see "Adding Remote Devices" on page 41.

3.2 Adding Remote Devices

The list of all remote devices that have previously been added to the SkyLIGHT VCX Controller appears here when you first open the page. The following details are provided for each device:

- **Device Name**: Displays the name provided when adding the device to the VCX Controller
- **MAC Address**: Displays the address provided when adding the device to the VCX Controller
- **Linked**: Indicates if this device has been linked to the VCX Controller. For details, see "Linking to the SkyLIGHT VCX Controller" on page 43.
- **Authorized**: Indicates if the link between this remove device and the VCX Controller has been approved. The remote device's ports are not accessible to the VCX Controller until it has been duly authorized, as described below.
- **Admin State**: Indicates whether the remote device is *In Service* or *Out of Service*.
- **Active Feature**: The current feature load used on the remote device.
- **Current Feature Suite**: The version of the current feature load used on the remote device.

You can quickly manage all the devices listed on this page by clicking the **Delete All**, **Authorize All**, and **Deny All** buttons.

> *Note: Except in the case of **Delete All**, the system will not prompt you for a confirmation when you click these buttons.*

▶ To add a remote device to the SkyLIGHT VCX Controller

> *Note: If you have multiple remote devices that have already been discovered by the VCX Controller, you can also access the **Discovery ▶ Inventory** page can to quickly add them in groups of up to 25 at a time.*

1. Access the page **Remote Devices ▶ Configuration**.

   A listing of all devices currently associated with this instance of the VCX Controller is displayed.

   The total number of remote devices found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain remote devices, enter a value on which to filter, then click **Search**. You can filter by the device name, MAC address, admin state,

active feature, current feature suite, or whether or not the device has been linked or authorized.

Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

2. Click **Add**.

   The *New Remote Device Configuration* page is displayed.

3. Do one of these actions:

   - **To add a single remote device**: Enter the device details, using the information in the following table as a guide. Click **Apply** to save your changes.
   - **To add multiple remote devices**: Click **Browse** to navigate to the CSV file containing the device details, then click **Import** to upload the file.

   The CSV file you select must contain the first three parameters listed in the following table (an example is given below).

```
Serial Number,MAC,Grain Key
S001-0000,00:15:01:00:00:00,00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f
```

For information on specific parameters, refer to the following table.

Remote Device Parameters (Remote Devices ▶ Configuration)

Parameter	Description
Remote Device Name	A name that uniquely identifies the VCX Controller across the network
MAC Address	The VCX Controller's base MAC address, for example *00:15:AD:1D:72:00*. This address value is incremented to determine the MAC address assigned to the device's second port (for example *00:15:AD:1D:72:01*).
Security Key	The device-specific Grain-128 security key that is associated with each device. The expected format is *00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF* The security key is used to establish a secured session between the VCX Controller and the remote device. These sessions are used to report the link state, as well as to ensure that the parameter and register settings on the remote device can be managed from the VCX Controller instance. To use the Accedian Management Key (AMK) as the security key, leave this field blank. The AMK ensures a universal authentication mechanism on Accedian devices; its value can be used to connect to all newly-shipped devices that have never been managed.

Parameter	Description
	Regardless of the type of security key being used to protect to remove device, the key value is periodically changed to prevent the management sessions with the VCX Controller from being spoofed.
Authorized	Select this box to allow this VCX Controller instance to gain access to the remote device's ports.
Extra Reconnection Delay	Select this box to make the VCX Controller allow extra time when reconnecting to this remote device before declaring it unreachable.

3.2.1 Linking to the SkyLIGHT VCX Controller

The **Linked** column of the summary table indicates whether or not the remote device has been linked to this instance of the VCX Controller. A remote device is considered *linked* to a VCX Controller when the following is true:

- It has been added to the VCX Controller and configured properly, including authorization
- It has been discovered by the VCX Controller and a management session has been established between them

No direct intervention on your part is required to link a device to a VCX Controller. Once linked, the remote device's physical ports are added to the list of ports available in the system.

3.2.2 Unlinking Devices From the SkyLIGHT VCX Controller

You can unlink a remote device from its Controller simply by revoking the VCX Controller's authorization over the device.

▶ To unlink a remote device from the SkyLIGHT VCX Controller

1. Access the page **Remote Devices ▶ Configuration**.

   A listing of all devices currently associated with this instance of the VCX Controller is displayed.

2. Click the name of the remote device that you want to unlink from the VCX Controller.

   The *Remote Device Configuration* page is displayed. Details related to the selected device are provided.

3. Revoke the VCX Controller's authorization over the device by clearing the **Authorized** check box.
   The selected device is automatically unlinked from the VCX Controller.

3.3 Managing Remote Device Features

Use this page to view attributes and specific information about the state and features supported by the selected remote device. You can also configurable certain parameters here.

▶ To manage remote device features

1. Access the page **Remote Devices ▶ Configuration**.

   A listing of all remote devices currently associated with this instance of the VCX Controller is displayed.

2. Click the **Active Feature** hyperlink that corresponds to the remote device whose features you want to manage.

   The *<Device Name> Feature Management* page is displayed.

3. Do one or more of these actions, as required:

   - **Update the Device's Administrative State**: Toggle the **Admin State**, then click **Apply** to save your changes.
   - **Change the In-Service Feature Load**: Choose either the **PMON** or **TGEN** feature load by making a selection in the drop-down list, then click **Apply** to save your changes.

For information on specific parameters, refer to the following table.

Remote Device Parameters (Remote Devices ▶ Configuration)

Parameter	Description
Remote Device Name	The name assigned to this remote device
Admin State	The remote device's administrative state. Available options are: • **In Service (IS)**: The remote device is active • **Out of Service (OOS)** The remote device is inactive and ready to have its feature load updated Update the Admin State if you need to change the current active feature load being used. You must set the administrative state to *Out-of-Service* before changing the feature load, then change it back to *In-Service* in order to return the device to active mode. *Note: A remote device's administrative state has an impact on the system's ports status, since changing this*

Parameter	Description
	state affects the ports that are in use.
In-Service Feature	The in-service feature associated with each device. Available options are: • **TGEN** Traffic generation (used to perform SAT tests) • **PMON**: Packet monitoring (all other features, including service OAM, traffic management and loopbacks)
Active Feature	The current feature load present on the remote device. Available options are: • **TGEN** Traffic generation (used to perform SAT tests) • **PMON**: Packet monitoring (all other features, including service OAM, traffic management and loopbacks) • **None**: No load is detected *Note: Changing the active feature load running on a remote device impacts the traffic flowing through it.*
Available Feature Suites	The current feature suite on the remote device

3.4 Configuring Security Key Management

Each remote device is associated with a unique Grain-128a authentication security key. In addition to the device-specific security key, remote devices from release 1.3 or later also support the use of the Accedian Management Key (AMK), which is a security key that is unique to Accedian Networks.

Use this page to define how the security key information associated with the most recent management session is backed up to an external server. You can also import a file containing the security key for multiple remote devices here.

▶ To back up remote device security keys

1. Access the page **Remote Devices ▶ Security Key Management**.
2. Complete the fields in the **Security Key Management Configuration** section of the page.
3. *(Optional)* Click **Test** to ensure that the parameters entered are valid.
4. Click **Apply** to save your changes.

For information on specific parameters, refer to the following table.

Security Key Management Parameters (Remote Devices ▶ Security Key Management)

Parameter	Description
Backup Period (min)	The period of time, expressed in minutes, between each backup of the remote devices' security information. The default value is *1440* minutes, i.e., once every 24 hours. Minimum value is *5* minutes. *Note: Set this value to 0 to disable backing up the security information.*
Server URL	The address of the server where the security key information file generated by the VCX Controller is saved. *Note: The SCP password parameter applies to all secure protocols, not only SCP.* Examples of the expected syntax is as follows: • ftps://username@domain.com • sftp://username@192.168.10.10 • scp://username:password@192.168.10.10:/target_directory

Parameter	Description
SCP Password	The password for the Secure Copy Protocol (SCP) used when transferring the security key information file to the remote file server.

▶ To import a list of remote device security keys

1. Access the page **Remote Devices ▶ Security Key Management**.
2. In the **Import Security Key** section of the page, click **Browse** to navigate to the CSV file containing the security key values.
3. Click **Import** to upload the file.

The CSV file you select must contain the device's details, as shown in the example below.

```
Serial Number,MAC,Grain Key
S001-0000,00:15:01:00:00:00,00:01:02:03:04:05:06:07:08:09:0a:0b:0c:0d:0e:0f
```

3.5 Managing Feature Suites

With the VCX Controller, you can manage a number of distinct feature suites to be applied as needed to the remote devices. Use this page to import and delete feature suites. You can also import new feature suites here as they become available.

▶ To view the feature suites currently in use

1. Access the page **Remote Devices ▶ Feature Suites Management**.

   The Available Suites page appears. A listing of all feature suites available to the system is displayed, along with whether or not they are in use at the current time.

▶ To delete a feature suite

Note: You cannot delete a feature suite that is currently in use.

Note: Once, deleted, a feature suite cannot be recovered and must be reimported.

1. Access the page **Remote Devices ▶ Feature Suites Management**.

   The Available Suites page appears. A listing of all feature suites available to the system is displayed, along with whether or not they are in use at the current time.

2. Enable the **Select** box beside the feature suite you want to delete.

3. Click **Delete** to permanently remove the feature suite from the VCX Controller. You are not prompted to confirm your actions.

▶ To import a feature suite

1. Access the page **Remote Devices ▶ Feature Suites Management**.

   The Available Suites page appears. A listing of all feature suites available to the system is displayed, along with whether or not they are in use at the current time.

2. In the **Import Suite** section of the page, click **Browse** to navigate to the file containing the feature suite.

3. Click **Import** to upload the file.

   The file you selected appears in the Available Suite section of the page.

4 Discovering Remote Devices

This chapter describes functions related to how remote devices are discovered by the SkyLIGHT VCX Controller; it contains the following sections:

4.1 Discovering Remote Devices

The VCX Controller is able to quickly and reliably discover the remote devices (i.e., Nano and ant modules) to be linked with an instance of the VCX Controller. These remote devices are extensions of the VCX Controller, providing it with remote ports that deliver system functionality. Use this page to specify the remote device discovery instances using the local ports on the server that were allocated to each VCX controller instance.

Even if you have created discovery instances to specify how to discover the remote devices, it can occur that more than the allocated devices are found by the VCX Controller. In order to associate and link only the appropriate devices with their intended VCX Controller instance, you must supply each VCX Controller instance with a predefined list of the remote devices to control. For details on adding a remote device or importing a list of remote devices in a CSV file, see "Adding Remote Devices".

4.1.1 Configuring the Discovery of Remove Devices

There are two different discovery methods you can use in order to configure and define remote device discovery instances in a VCX Controller:

- **IPAD**: The IP Agnostic Discovery (IPAD) protocol, between a VCX Controller and the remote devices. Supply an IP address assigned to a specific Nano/ant module or other network device, or a subnet that will be scanned to discover all reachable remote devices.
- **ACP Layer-2**: The ACP protocol can be used to discover remote devices in Layer-2 networks.

▶ To discover remote devices

1. Access the page **Discovery ▶ Configuration**.

   The *Remote Device Discovery Configuration* page appears. A listing of all remote device discovery instances is displayed.

2. Click **Add** to create a new remote device discovery instance or click the **Name** of an existing instance to edit its settings.

3. Complete the required fields in the **New Remote Device Discovery Configuration** section of the page.

4. Click **Apply** to save your changes.

For information on specific parameters, refer to the following table.

Remote Device Discovery Parameters (Discovery ▶ Configuration)

Parameter	Description
Name	A unique name assigned to the remote device discovery instance.
Enable	Select this box to enable the remote device discovery instance.
Method	The protocol to use when discovering remote devices. Available options are: • **IPAD**: Suitable for both Layer-2 and Layer-3 networks • **ACP Layer-2**: Layer-2 networks only
Rate	The frequency at which discovery messages will be sent over the network. Available options are: • **One-Shot**: A one-time, single-use discovery message • **3 Seconds**: Discovery messages are automatically sent every three seconds • **60 Seconds**: Discovery messages are automatically sent once a minute. This is the default value. • **5 Minutes**: Discovery messages are automatically sent every five minutes • **10 minutes**: Discovery messages are automatically sent every ten minutes • **60 minutes**: Discovery messages are automatically sent every hour
Hop Limit	The maximum number of hops that the discovery messages can go through in order to discover remote devices. Default value: *255* *Note: Applies to IPAD discovery instances only.*
Timeout (sec)	The period of time after which the discovery messages sent by the VCX Controller instance expire. Use this parameter to have the VCX Controller stop listening for reply messages (i.e., advertisements) from the remote devices. *Note: Applies to IPAD discovery instances only.*

Parameter	Description
Destination IP Address	An IP address assigned to a specific Nano/ant module or other network device. You can also indicate a subnet that will be scanned to discover all reachable remote devices. *Note: Applies to IPAD discovery instances only.*
Type	The type and delivery scope of the Layer-3 discovery messages. Available options are: • **UNICAST**: Unicast discovery messages expect a host destination IP address assigned to a network device other than a Nano or ant module. • **UNICAST-DIRECTED**: Unicast-directed messages expect a destination IP address assigned to a specific Nano or ant module. This type of discovery message is typically used to ensure a specific remote device is reachable. • **SUBNET**: Subnet discovery messages expect a subnet destination IP address that covers an entire subnet where remote devices are located. This discovery type has the VCX Controller send out multiple unicast discovery messages to ensure that whole subnet is covered. *Note: The SUBNET discovery type does not support Layer-3 multicast messages.* *Note: The SUBNET discovery type requires a discovery message rate of at least 60 seconds. Setting a rate of 5 minutes is recommended.* *Note: Applies to IPAD discovery instances only.*
Interface	The logical (i.e., network) interface to use when discovering remote devices, such as LOCAL-2. The logical interface is bound to the server's local ports, meaning that the logical interfaces defined in **Port ▸ Configuration** are the same ones bound to the local ports. *Note: Applies to ACP Layer-2 discovery instances only.*
Serial Number	Enter the serial number of a remote device here to create a probe limited to this specific device. *Note: Applies to IPAD discovery instances using the Unicast-Directed method only.*
Netmask Subnet	Enter a subnet to be used on the destination address. The maximum subnet size is 23 bits (255.255.254.0), providing a

Parameter	Description
	total of 512 addresses. *Note: Applies to IPAD discovery instances using the SUBNET method only.*

4.2 Remote Device Inventory

Use this page to view the full inventory of remote devices that have been discovered by the VCX Controller using the remote device discovery instances that were created in the **Discovery ▸ Configuration** page.

Note: All remote devices are listed here together, regardless of the device discovery method (i.e. IPAD or ACP Layer-2) used.

▸ To view an inventory of discovered remote devices

1. Access the page **Discovery ▸ Inventory**.

   The full inventory of remote devices that have been discovered by the VCX Controller is displayed.

   The total number of devices found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain remote devices, enter a value on which to filter, then click **Search**. You can filter by remote device IP, system description, serial number, firmware version or hostname.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. *(Optional)* In the **Serial Number** column of the table, click the serial number of the remote device for which you want to view detailed information.

For information on specific parameters, refer to the following tables.

Remote Device Inventory Parameters (Discovery ▸ Inventory)

Parameter	Description
Remote Device IP	The IP address, if any, that is assigned to the remote device acting as a logical interface
System Description	The product name of the discovered remote device. Typically, Nano devices are named *ANN-1000-CT*, whereas ant devices are named *ANT-1000-TX*.
Serial Number	The unique serial number assigned to the remote device. Click the serial number to access device details such as typical ACP (Plug & Go) inventory information, as described in the following table.
FW Version	The firmware version of the remote device
Hostname	The remote device's host name, which is also the device's serial number

Remote Device Detailed Information (Discovery ▸ Inventory)

Parameter	Description
System Name	The remote device's unique serial number, as well as its products name. Nano modules are typically named ANN-1000-CT, whereas ant modules are typically named ANT-1000-TX.
Primary IP Address	The IP address assigned to one of the remote device's interfaces
Secondary IP Address	The secondary IP address (or alias) assigned to one of the remote device's interfaces
Domain ID	The domain ID is typically used by ACP discovery instances to align the domains used over a network
Base MAC	The base MAC address assigned to the remote device
Interface MAC	The MAC address assigned to the remote device used to link the remote device to a VCX Controller instance
Remote Port	The name of the remote port sending ACP advertisement frames, if any
Firmware Version	The current firmware version being used, such as *PMON* or *TGEN*
Chassis Subtype	Set to *1* for remote devices
Chassis ID	The remote device's configured host name, which is also the device's serial number
Config Status	The type of configuration used to set the device's settings
CLEI Code	The Common Language Equipment Identifier (CLEI) code assigned to this telecommunications device by its manufacturer. You cannot change this value.
Discovery Instance	The discovery instance used to discover this remote device

▸ To add a remote device to the SkyLIGHT VCX Controller

1. Access the page **Discovery ▸ Inventory**.

   The full inventory of remote devices that have been discovered by the VCX Controller is displayed.

   The total number of remote devices found in the system is given in the lower-left corner of the page, as well as the index values of the devices currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain remote devices, enter a value on which to filter, then click **Search**. You can filter by remote device ID, system description, serial

number, firmware version or hostname.

Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. Click the box associated with the devices you want to add to the VCX Controller, then click **Add**.

   Note: Click the box in the table header to quickly select all devices displayed.

   The *Inventory Configuration* page is displayed with a confirmation message indicating how many of the selected devices were added to the VCX Controller, for example "0 of 1 remote device(s) added" or " 50 of 50 remote device(s) added".

▶ To clear the inventory of discovered remote devices

1. Access the page **Discovery ▶ Inventory**.

   The full inventory of remote devices that have been discovered by the VCX Controller is displayed.

   The total number of remote devices found in the system is given in the lower-left corner of the page, as well as the index values of the devices currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain remote devices, enter a value on which to filter, then click **Search**. You can filter by remote device ID, system description, serial number, firmware version or hostname.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. Click **Clear**.

   The page is refreshed. The selected entries have been removed from inventory of remote devices discovered by the VCX Controller.

   To discover these devices again, you must wait for the period of time specified in the **Rate** field of the appropriate discovery instance that was created in the **Discovery ▶ Configuration** page.

4.3 Configuring Remote Device Ports

After the remote devices have been configured and discovered, their ports are added to the list of ports attached to the VCX Controller instance. Once added to the list, these ports can be used by the VCX Controller instance as if they were the controller's own physical ports.

As shown in the example below, since Nano and ant modules are equipped with two available ports, two ports are added to the VCX Controller's list of supported ports for each such linked remote device.

List of Available Ports

Port configuration and status ?

Status	Connector	Port name	Port state	Speed	MAC address
	RJ45	LOCAL-1	Enabled	Auto	08:00:27:7A:2C:BD
	RJ45	LOCAL-2	Enabled	Auto	08:00:27:BC:FE:81
	RJ45-2	Ant-NNI	Enabled	Auto	00:15:AD:16:FE:E0
	RJ45-1	Ant-UNI	Enabled	Auto	00:15:AD:16:FE:E0
	RJ45-2	C100-0301-NNI	Enabled	Auto	00:15:AD:1B:57:BA
	RJ45-1	C100-0301-UNI	Enabled	Auto	00:15:AD:1B:57:BA
	RJ45-2	C100-0159-NNI	Enabled	Auto	00:15:AD:1B:56:9E
	RJ45-1	C100-0159-UNI	Enabled	Auto	00:15:AD:1B:56:9E
	FIBER	E005-0230-NNI	Enabled	Auto	00:15:AD:14:EA:22
	SFPHOST	E005-0230-UNI	Enabled	Auto	00:15:AD:14:EA:22
	SFPHOST	E005-0227-NNI	Enabled	Auto	00:15:AD:14:EA:1C
	FIBER	E005-0227-UNI	Enabled	Auto	00:15:AD:14:EA:1C

5 Configuring the SkyLIGHT VCX Controller

This chapter contains the following sections:

5.1 Setting the System Date and Time

Accurate, precise date and time value are important when managing and troubleshooting a network. They allow, among other useful functions, time-stamping of alarms.

The system date and time can be set manually, or automatically controlled via an NTP server.

Note: To avoid conflicts, only one NTP server can be used in a network.

Instructions for manually or automatically setting the date and time follow.

5.1.1 Setting Date and Time Manually

▶ **To set the date and time manually**

1. Access the page **System ▶ Configuration ▶ Time**.
2. Specify the current date and time in the provided fields.
3. Select the **Change to entered date and time if possible when applied** box to allow a single manual update to the system date and time.

   Note: When you click **Apply***, this box is reset to the unselected state.*
4. Click **Apply**.

For more information on specific parameters, refer to the table on page 61.

5.1.2 Setting Date and Time Automatically

▶ **To update the date and time automatically using Network Time Protocol**

Note: You can enable up to two NTP servers for NTP synchronization.

1. Access the page **System ▶ Configuration ▶ Time**.
2. Select the **NTP Enable** option.
3. Verify that the NTP server you want to use appears in the **NTP Service List**.

   If not, add a new server by specifying its name or IP address in the **NTP Server** box then clicking **Add**.
4. Select a time server from the list, then click **Apply**.

▶ To delete an NTP server

1. Access the page **System ▶ Configuration ▶ Time**.
2. Select the NTP server's line from the **NTP Service List** by clicking its name or IP address. Do not click the check box.
3. Click **Delete**.

Date and Time Parameters (System ▶ Configuration ▶ Time)

Parameter	Description
Set Time and NTP	
NTP Enable	Sets the system time automatically by polling an NTP server. Select a server from the list or add your own.
Date and Time	If you are not using NTP, the date and time can be set manually by entering values here. Select the **Change to entered date and time if possible when applied** box to allow a single manual update to the system date and time. When you click **Apply**, this box is reset to the unselected state.
NTP Server List	One or two NTP servers can be enabled simultaneously. The VCX Controllerwill automatically update its date and time from one of the enabled NTP servers. If the NTP server being used is unreachable, the VCX Controllerwill attempt to contact the other enabled NTP server.
NTP Server	When using an NTP client instance, the name or the IP address of the NTP server to add.
Number of Messages	When using NTP, the number of synchronization messages exchanged with the NTP server during each time interval. Acceptable values range from *5* to *60*.
DSCP	When using NTP, the priority can be set in the Differentiated Services Code Point.
VLAN Priority	When using NTP, the priority of the VLAN frames can be set in the VLAN priority bits if the link is through a VLAN.

5.2 Setting Up DNS

You can use the DHCP to automatically configure the SkyLIGHT VCX Controller's IP parameters. When the VCX Controlleruses DHCP, it can be configured to use the DNS settings from the DHCP. If the VCX Controller does not use DHCP, you can manually specify the address for each DNS server.

Note: Two DNS servers can be used for redundancy.

▶ To use DHCP to specify the address of DNS servers

1. Access the page **System ▶ Configuration ▶ DNS**.
2. Enable the **Use DHCP Results** box.
3. Use **From Interface** to select the interface from which to obtain DHCP information.

For more information on specific parameters, refer to the table "DNS Parameters (System ▶ Configuration ▶ DNS)" on page 10.

▶ To manually specify the address of DNS servers

1. Access the page **System ▶ Configuration ▶ DNS**.
2. Remove the check mark from the **Use DHCP results** box.
3. Manually specify the address of DNS server 1 and DNS server 2 (if required),
4. Specify the **Domain**, then click **Apply**.

For more information on specific parameters, refer to the table "DNS Parameters (System ▶ Configuration ▶ DNS)" on page 10.

5.3 Upgrading the Firmware

New firmware versions typically provide:

- Additional functionality
- Enhancements to the existing feature set
- Defect corrections

To verify the current software version, see the **Current version** field of the **Firmware Maintenance** section in the **System ▸ Maintenance ▸ Firmware** page.

You can upgrade the SkyLIGHT VCX Controller's firmware by downloading the firmware directly from your computer or network. If using the Command Line Interface (CLI), you can also upgrade the VCX Controller's firmware via an SFTP, HTTP, FTP or SCP server for a file transfer.

There are two ways to upgrade a unit's firmware:

- **One-step firmware upgrade**: Use this method when you want the upgrade to take effect immediately.
- **Two-step firmware upgrade**: Use this method when you to want to download the firmware file now, then activate it on the VCX Controllerat a later time (such as during an upcoming maintenance window).

  Note: If you download a firmware file as part of a two-step firmware upgrade, it will overwrite the rollback firmware file in the One-Step tab (if any) that is currently stored on the VCX Controller. You cannot concurrently store both a rollback firmware file and a pending two-step upgrade download on the VCX Controller.

▸ To perform a one-step firmware upgrade

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Click the **Browse** button next to the **New Firmware** field.
3. In the dialog box that appears, select the firmware file from your computer or network, then click **Open**.

   Note: The firmware is distributed in a binary file with the filename extension .afl.

4. Click the **Upgrade** button.

   The firmware begins loading. Once it has finished, the VCX Controller restarts to activate the new firmware.

   To verify that the upgrade was successful, access the page **Home** and examine value of the **Firmware version** field.

▸ To perform a two-step firmware upgrade

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Click the **Two-Step** tab.

   The screen refreshes to display the tab contents.

3. Click the **Browse** button next to the **New firmware** field.

4. In the dialog box that appears, select the firmware file on your computer or network, then click **Open**.

   Note: The firmware is distributed in a binary file with the filename extension .afl.

5. Click the **Download** button.

   The firmware is loaded onto the VCX Controller, pending activation as described below. The *Rollback Version* field in the One-Step tab is updated to "No rollback available".

▸ To activate the downloaded firmware file

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Click the **Two-Step** tab.

   The screen refreshes to display the tab contents.

3. Ensure that the version number displayed next to the **Downloaded version** is the correct version to activate on the VCX Controller.

4. Click the **Activate** button.

   The VCX Controllerrestarts to activate the new firmware. You are not prompted to confirm your actions.

   To verify that the upgrade was successful, access the page **Home** and examine value of the **Firmware version** field.

▸ To delete the downloaded firmware file

Note: This feature is provided for your convenience only; deleting a downloaded firmware file once it has been applied is optional. Furthermore, downloading a new firmware file will automatically overwrite the existing file (if any) on the VCX Controller.

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Click the **Two-Step** tab.

   The screen refreshes to display the tab contents.

3. Click the **Clear Download** button.

   The firmware file is permanently removed from the VCX Controller. You are not prompted to confirm your actions. The value of the **Downloaded version** is updated to *None*.

▸ To revert to the previous firmware version

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Ensure that the version number displayed next to the **Rollback version** is the correct version to which to revert.

3. Click **Rollback**.

For more information on specific parameters, refer to the following table.

Firmware Parameters (System ▸ Maintenance ▸ Firmware)

Parameter	Description
Firmware Maintenance, One-Step Tab	
Current Version	The current version of the firmware
New Firmware	The firmware version that is applied when you click *Upgrade*
Browse Button	Click to navigate to the firmware file to which you want to upgrade the VCX Controller
Rollback Version	The previous firmware version to which you can revert
Rollback Button	Click to revert the VCX Controller's firmware to the version indicated in *Rollback Version*
Reboot Button	Click to reboot the VCX Controller and activate the new

Parameter	Description
	configuration
Firmware Maintenance, Two-Step Tab	
Current Version	The current version of the firmware
New Firmware	The firmware version that is downloaded when you click *Download*
Browse Button	Click to navigate to the firmware file to which you want to upgrade the VCX Controller
Download Button	Click to begin downloading the selected firmware file
Downloaded Version	The firmware file that has been previously downloaded on this unit
Activate Button	Click to upgrade the VCX Controller's firmware to the version indicated in *Downloaded version*
Clear Download Button	Click to remove the previously-downloaded firmware file from the VCX Controller

***CAUTION**: Reverting to an older firmware version is advisable ONLY through the Rollback feature. With Rollback, compatible configuration settings are loaded with the previous firmware. A simple firmware downgrade is NOT advisable because the older firmware may not match the existing (newer) configuration. Attempting a firmware downgrade using the **Upgrade** button may corrupt the configuration.*

▸ To reset the SkyLIGHT VCX Controller to factory values while performing a firmware downgrade

1. Access the page **System ▸ Maintenance ▸ Firmware**.

   The Firmware Maintenance window is displayed; the *One-Step* tab is visible by default.

2. Click the **Factory Default** button.

3. Click the **Browse** button next to the **New firmware** field and select the new firmware file.

4. Click the **Upgrade** button.

   The VCX Controller will restart with a factory default configuration after downgrading the firmware.

5.4 Importing/Exporting the Unit's Configuration

If you need multiple units in your network to have the same configuration, you can configure your first unit and then export these configuration values to a file. You will then be able to import this configuration file into other units to configure them in the same way. You can export and import the configuration files that are stored locally on each SkyLIGHT VCX Controller.

> ***CAUTION**: Pay special attention to the DNS settings when using the import/export function. The IP connectivity to each unit might be at risk if you are using a static IP address configuration in the Management interface. The use of DHCP is therefore recommended when importing a configuration to multiple units.*

Each configuration file provides an identifier to help prevent importing an incorrect file.

> ***CAUTION**: Although you can edit a configuration file, you risk corrupting its data! The file is in a UNIX text format, and should not be opened with a Windows text editor such as Notepad.*

> ***CAUTION**: After making configuration changes, it is recommended to wait at least 30 seconds before exporting the configuration file. Doing so ensures that the latest changes have been written to the file, and that it is ready to be exported.*

▸ To export a configuration file

1. Access the page **System ▸ Maintenance ▸ Firmware**.
2. Enter a configuration filename in the **Config Export Filename** text box.
3. Click **Export**.

For more information on the other parameters, refer to the following table.

▸ To import a configuration file

1. Access the page **System ▸ Maintenance ▸ Firmware**.
2. Click the **Factory Default** button.

   Note: This step is optional if you are importing a configuration file of the same version as the currently running firmware. If you are importing a configuration from an older firmware version, you must reset the current configuration (factory default) before importing the older version.
3. Click the **Browse** button next to the **Config Import File** field.
4. Select the firmware file on the local VCX Controller, then click **OK**.

5. Click the **Import** button.
6. Once the file is uploaded, click **Reboot** to activate the new configuration.

For more information on specific parameters, refer to the following table.

Configuration Import/Export Parameters (System ▸ Maintenance ▸ Firmware)

Parameter	Description
Config Import File	After you click *Browse* and navigate to a new configuration file to import, its name appears here.
Config Export Filename	Enter a configuration file name here, then click *Export* to export the current configuration for later use.
Factory Default Button	Click to apply the factory default settings to this unit.
Cancel Changes Button	The factory default and rollback actions require a system reboot. You can cancel these actions if needed simply by clicking *Cancel Changes*.
Rollback Button	Click to revert the VCX Controller's configuration to the version from the last time it rebooted.

5.5 Rebooting the SkyLIGHT VCX Controller

Rebooting the SkyLIGHT VCX Controller is required in order to apply certain types of modifications made to its configuration. You must also reboot after importing new configuration values.

For details, refer to "Importing/Exporting the Unit's Configuration" on page 67.

> ***CAUTION**: Rebooting the VCX Controller is disruptive. It applies changes in its configuration and affects current operations.*

▶ To reboot the SkyLIGHT VCX Controller

1. Access the page **System ▶ Maintenance ▶ Firmware**.
2. Click the **Reboot** button.

5.6 Restoring Factory Default Settings

▶ To reset the SkyLIGHT VCX Controller to factory default settings via the Web interface

1. Access the page **System ▶ Maintenance ▶ Firmware**.
2. Click the **Factory default** button.
3. Click the **Reboot** button.

6 Managing Ports

This chapter describes how to manage the ports, which are physical interfaces on the SkyLIGHT VCX Controller; it contains the following sections:

6.1 Setting Up Ports

You can configure the parameters for each port on the SkyLIGHT VCX Controller to manage options, such as link speed (auto-negotiation) and flow control.

▶ To view or configure port settings

1. Access the page **Port ▶ Configuration**.

   All VCX Controller local ports and their current status are displayed, followed by a listing of all remote devices' ports. Each remote device is listed with paired ports: one UNI port (for example, *E011-0036-UNI*) and one NNI port (for example, *E011-0036-NNI*) per device.

   The total number of ports found in the system is given in the lower-left corner of the page, as well as the index values of the ports currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain ports, enter a value on which to filter, then click **Search**. You can filter by port name, connector, speed or MAC address.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. To update a port's settings, click its name under the **Port Name** heading.

   The *Port Configuration* page is displayed.

4. Enter values in the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

> ***CAUTION**: If you set the Port MTU to a value smaller than 1518 bytes on a port used for management, you or another user may lose access to the management Web interface.*

Port Configuration (Port ▶ Configuration)

Parameter	Description
Status	The following colors in the summary page indicate the port status: • **Green**: The port is up and running; in the case of a remote device, it means that the device has been linked with the VCX Controller. • **Blue**: The port is enabled and a signal is detected

Parameter	Description
	• **Red**: The port is enabled, but the physical link is down and no signal is detected • **Yellow**: The port is not totally functional; in the case of a remote device, it means that the device has been provisioned, but not linked. • **Gray**: The port is disabled
Connector	The type of physical connector associated with the port Available options are: • SFP • RJ45 • FIBER • SFPHOST • Management
Port Name Name	The name that identifies the port
Host Detection Status	The host associated with the remote device: **NanoLINK**, or **Host** *Note: A series of three dashes appears here if no NanoLINK host is detected.*
Port State	The port may be either enabled or disabled.
Speed Link Speed	Sets the port speed and duplex type **Auto-Negotiation**: The VCX Controller automatically negotiates port speed and duplex type with the device to which it is connected. For auto-negotiation to be successful, the other device must also be set up for auto-negotiation. If **Auto-Negotiation** is not in use, you can manually define port speed: • 100 Mbps • 1 Gbps If **Auto-Negotiation** is not in use, you can manually define duplex type: • **Half-Duplex**: Transmission in one direction at a time

Parameter	Description
	• **Full-Duplex**: Transmission in both directions at the same time *Note: Unsupported options, if any, are disabled.* In 1G mode, auto-negotiation may be selected (advertises 1000 Mbps, full-duplex only). *Note: Auto-negotiation is mandatory for 1000 BASE-T.*
Alias	The port's assigned alias name, as specified by a network manager
Port MTU	The maximum transmission unit that a port can receive and forward, including all headers. Expressed in bytes. Supported values: 64 to 10240 Default value: 2000 *Note: Setting the MTU to a value smaller than 1518 bytes on a port used for management may cause a loss of access to the VCX Controller.*
MAC Address	The MAC address of the port
Current Status	The current link speed and duplex type when **Auto-Negotiation Enable** is selected: • **Current Connector Configuration**: If the link partner is also using **Auto MDI**, the resulting connector configuration is correct but random. A cross-over cable present on the cabling plant results in both partners using the same connector configuration.

6.2 Network Requirements — TCP/UDP Ports

Accedian's demarcation devices, including the VCX Controller, rely on a large number of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports in order to support their various features and protocols.

The following table lists the TCP and UDP ports used by Accedian demarcation devices. This information will prove useful when configuring firewalls on a network.

TCP/UDP Port Usage by Accedian Devices

Protocol	Dest. Port	Service Name	Applications	Direction
TCP	443	HTTPS	Web Interface	User station to Device
TCP	22	SSH	Command Line Interface (CLI)	User station to Device
TCP	23	Telnet	Command Line Interface (CLI)	User station to Device
UDP	161	SNMP	SNMP Polling	Server to Device
TCP	49	TACACS+	User authentication and authorization	Device to Server
TCP	14040	Vision Collect	Performance Counters Transmission	Device to Server
UDP	162	SNMP	SNMP Trap Sending	Device to Server
UDP	1812	RADIUS	User authentication and authorization	Device to Server
UDP	514	Syslog	Remote Syslog	Device to Server
UDP	123	NTP	Network Time Protocol Synchronization	Device to Server
UDP	320	PTP	Precision Time Protocol Synchronization	Device to Server
TCP	21	FTP	File Transfers: • Configuration exports • Configuration imports • Firmware upgrades	Device to Server; Server to Device

Protocol	Dest. Port	Service Name	Applications	Direction
			• SAT reporting • RFC-2544 report uploads	
UDP	69	TFTP	File Transfers: • Configuration exports • Configuration imports • Firmware upgrades • SAT reporting • RFC-2544 report uploads	Device to Server
TCP	990	FTPS	File Transfers: • Configuration exports • Configuration imports • Firmware upgrades	Device to Server
TCP	22	SCP	File Transfers: • Configuration exports • Configuration imports • Firmware upgrades	Device to Server
TCP	22	SFTP	File Transfers: • Configuration exports • Configuration imports • Firmware upgrades • SAT reporting • RFC-2544 report uploads	Device to Server
TCP	80	HTTP	File Transfers:	Device to Server

Protocol	Dest. Port	Service Name	Applications	Direction
			• Configuration exports • Configuration imports • Firmware upgrades	
UDP	6000 (see note)	TWAMP	Two-Way Active Measurement Protocol	Device to Server
UDP	8000 (see note)	SAT	Y.1564 One-Way Test Communication	Device to Device
UDP	9000 (see note)	SAT	Y.1564 One-Way Test Traffic	Device to Device
UDP, TCP	53	DNS	Domain Name System	Device to Server
UDP	67	DHCP	Automatic IP Assignment	Device to Server
UDP	68	DHCP	Automatic IP Assignment	Device to Server
UDP	67	Plug & Go	Layer-3 Beacon	Device to Device
UDP	68	Plug & Go	Layer-3 Beacon	Device to Device
UDP	9065	Plug & Go	Layer-3 Advertisement	Device to Device

Note: The indicated destination port is the default value; you can configure this value as needed.

6.3 Viewing Port Statistics

You can view detailed port statistics for each port. The port's statistics are sampled once per second. To view a summary of statistics, access the page **Port ▸ Statistics**. For more information on specific parameters, refer to the following table.

▸ To view detailed port statistics

1. Access the page **Port ▸ Statistics**.
2. Select a port name from the list.

   The *<port name> Port Statistics* page appears. Transmit and Receive statistics for the selected port are displayed.

   The total number of ports found in the system is given in the lower-left corner of the page, as well as the index values of the ports currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.
3. *(Optional)* To limit the view to only certain ports, enter a value on which to filter, then click **Search**.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.
4. *(Optional)* Select the **Poll Every Seconds** box and enter the number of seconds between each time the data is automatically refreshed. You can also refresh the port statistics by clicking the **Refresh** button.

   Tip: To clear the statistics for all ports, click the  *icon on the right side of the table header. To clear the statistics for a specific port, click its associated icon in the table.*

For more information on specific parameters, refer to the following table.

Port Statistics (Port ▸ Statistics)

Parameter	Description
Summary Page	
Port Name	Ports for which statistics are displayed
Txm Packets	The count of the total number (i.e., both good and bad) of frames/packets transmitted by the port. Bad frames include normal collisions, late collisions and FIFO underflows.
Txm Errors	Number of transmission errors
Rcv Packets	The count of the total number (i.e., both good and bad) of frames/packets received by the port. Bad frames include short

Parameter	Description
	frames (less than 64 bytes), long frames (greater than the port's configured MTU), frames with bad CRC, frames with PHY errors and frames with receive FIFO errors.
Rcv Errors	Number of errors received

6.4 Setting Up Port PHY Parameters

You can view both SFP and copper ports and can set up PHY parameters for each copper port. The PHY parameters are used to set the abilities that are advertised to the link partner.

▶ **To view PHY parameters**

1. Access the page **Port ▶ PHY**.

   A list of PHY configuration and status for all ports is displayed.

   The total number of configurations found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain PHY configurations, enter a value on which to filter, then click **Search**. You can filter by the port name, connector type, whether or not auto-negotiation is enabled, or the port's auto-negotiation state.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

For more information on specific parameters, refer to the following table.

Port Configuration (Port ▶ PHY)

Parameter	Description
Status	Port status may be one of the following: • **Green**: The port is up and running. • **Blue**: The port is enabled and a signal is detected. • **Red**: The port is enabled but the physical link is down and no signal is detected. • **Yellow**: The port is not totally functional. • **Gray**: The port is disabled.
Connector	The physical connector the port is using
Port Name	The logical name assigned to the port
Auto-Nego	Indicates whether the auto-negotiation feature is enabled or disabled If enabled, the SkyLIGHT VCX Controller automatically negotiates port speed and duplex type with the device to which

Parameter	Description
	it is connected. For auto-negotiation to be successful, the device and its partner must both be configured to support auto-negotiation (**Port Configuration**).
State	The current auto-negotiation state of the port

▶ To set up a port's PHY parameters

1. Access the page **Port ▶ PHY**.

   A list of PHY configuration and status for all copper ports is displayed.

2. Click the **Port name** to edit its settings.

3. Define port PHY parameters as required by your setup, then click **Apply**.

For more information on specific parameters, refer to the following table.

PHY Configuration (Port ▶ PHY ▶ [Port name])

Parameter	Description
Advertisement Configuration	The abilities that are advertised to the link partner Possible options include: • 10 Mbps Half • 100 Mbps Half • 1 Gbps Half • 10 Gbps Half • 10 Mbps Full • 100 Mbps Full • 1 Gbps Full • 10 Gbps Full • Pause Symmetric (can receive and transmit pause frames) • Pause Asymmetric (can either receive or transmit pause frames) *Note: Unsupported options, if any, are disabled.*
Link Partner Ability	The abilities of the link partner Possible options include:

Parameter	Description
	• 10 Mbps Half • 100 Mbps Half • 1 Gbps Half • 10 Gbps Half • 10 Mbps Full • 100 Mbps Full • 1 Gbps Full • 10 Gbps Full • Pause Symmetric (can receive and transmit pause frames) • Pause Asymmetric (can either receive or transmit pause frames) *Note: Unsupported options, if any, are disabled.*
State	The state field corresponds to *ifMauAutoNegConfig* and *ifMauAutoNegRemoteSignaling* from RFC3636. The state **disabled** indicates that auto-negotiation is not supported by the media or is disabled by the configuration. Possible values are: • Other • Configuring • Complete • Disabled • Parallel Detect Fail Each of the above values may be configured **With Auto** or **Without Auto**.

6.5 Viewing SFP Information

Use this page to view both summary and detailed information about all currently-detected SFPs.

▶ To view a summary of all SFPs

1. Access the page **Port ▶ SFP**.

   Summary information for all SFPs currently detected by the SkyLIGHT VCX Controller is displayed.

▶ To view detailed information for all SFPs

1. Access the page **Port ▶ SFP**.

   Summary information for all SFPs currently detected by the VCX Controller is displayed.

   The total number of SFPs found in the system is given in the lower-left corner of the page, as well as the index values of the SFPs currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain SFPs, enter a value on which to filter, then click **Search**. You can filter by the port name, part number, serial number, wave length or speed.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. In the **Port Name** column of the table, click the SFP for which you want to view detailed information.

   The details pertaining to the selected SFP are displayed.

   For more information on specific parameters, refer to the following tables.

SFP Information (Port ▶ SFP)

Parameter	Description
Present	**Green**: The SFP is present. **Red**: The SFP is not present.
Port Name	The physical connector the port is using
Part Number	The manufacturer's part number or product name
Serial Number	The manufacturer's serial number for the transceiver
Wavelength	The nominal transmitter wavelength at room temperature, expressed in nanometers

Parameter	Description
Speed	The speed supported by the SFP, such as 1 Gbps or 10 Gbps
SFP Configuration	
Force Link Up	Enable this box to force SFP signals to the *Up* state.
Laser	The laser on the device's port can be set to either *ON* or *OFF*.
Fiber Information	
Connector Type	The external cable connector provided as the media interface
Vendor	The manufacturer name This is a 16-character field that contains ASCII characters padded on the right with ASCII spaces (20h).
Wave Length	Indicates the nominal transmitter wavelength at room temperature, expressed in nanometers
Part Number	The manufacturer part number or product name This is a 16-byte field that contains ASCII characters padded on the right with ASCII spaces (20h).
Serial Number	The manufacturer serial number for the transceiver This is a 16-character field that contains ASCII characters padded on the right with ASCII spaces (20h).
Revision	The manufacturer's product revision This is a 16-character field that contains ASCII characters padded on the right with ASCII spaces (20h).
SFP Present	Indicates the presence of a recognized SFP
Diagnostics	Supported or unsupported A value of *supported* indicates that diagnostic information is provided in the SFP memory section.
Calibration	**Internal**: The values are calibrated to absolute measurements, which should be interpreted according to the "Internal Calibration" convention. **External**: The values are A/D counts, which are converted into real units according to the "External Calibration" convention.
Thresholds	Indicates whether alarm and warning thresholds are supported
Speed	The speed supported by the SFP, such as 1 Gbps or 10 Gbps

Parameter	Description
Monitoring Information	
Temperature	Transceiver temperature, measured internally Temperature accuracy is manufacturer-specific, but must be better than 3 degrees Celsius for the specified operating temperature and voltage.
Supply Voltage	Transceiver supply voltage, measured internally *Note: Transmitter supply voltage and receiver supply voltage are isolated in some transceivers. In that case, only one supply is monitored. Refer to the device specifications for details.*
Receive Power	Received optical power, measured internally Accuracy depends on the exact optical wavelength. For the manufacturer's specified wavelength, accuracy should be better than 3 dB for the specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Accuracy beyond this minimum required received input optical power range is manufacturer specific.
Laser Bias Current	Coupled TX output power, measured internally Accuracy is manufacturer-specific but must be better than 3 dB for the specified operating temperature and voltage. Data is assumed to be based on measurement of a laser monitor photodiode current. Data is not valid when the transmitter is disabled.
Receive Power	Received optical power, measured internally Accuracy depends on the exact optical wavelength. For the manufacturer's specified wavelength, accuracy should be better than 3 dB for the specified temperature and voltage. This accuracy should be maintained for input power levels up to the lesser of maximum transmitted or maximum received optical power per the appropriate standard. It should be maintained down to the minimum transmitted power minus cable plant loss (insertion loss or passive loss) per the appropriate standard. Accuracy beyond this minimum required received input optical power range is manufacturer specific.

SFP Thresholds (Port ▶ SFP ▶ [connector])

Parameter	Description
SFP Thresholds	
Temperature	**High Alarm**: High-temperature alarm for the transceiver **Low Alarm**: Low-temperature alarm for the transceiver **High Warning**: High-temperature warning for the transceiver **Low Warning**: Low-temperature warning for the transceiver
Vcc	**High Alarm**: High-supply voltage alarm for the transceiver **Low Alarm**: Low-supply voltage alarm for the transceiver **High Warning**: High-supply voltage warning for the transceiver **Low Warning**: Low-supply voltage warning for the transceiver
Laser Bias Current	**High Alarm**: High-laser bias current alarm for the TX (micro-Amps) **Low Alarm**: Low-laser bias current alarm for the TX (micro-Amps) **High Warning**: High-laser bias current warning for the TX (micro-Amps) **Low Warning**: Low-laser bias current warning for the TX (micro-Amps)
Tx Power	**High Alarm**: High-output power alarm for the TX (~ -40 to +8.2 dBm) **Low Alarm**: Low-output power alarm for the TX (~ -40 to +8.2 dBm) **High Warning**: High-output power warning for the TX (~ -40 to +8.2 dBm) **Low Warning**: Low-output power warning for the TX (~ -40 to +8.2 dBm)
Rx Power	**High Alarm**: High-input power alarm for the Rx (~ -40 to +8.2 dBm) **Low Alarm**: Low-input power alarm for the Rx (~ -40 to +8.2 dBm) **High Warning**: High-input power warning for the Rx (~ -40 to +8.2 dBm) **Low Warning**: Low-input power warning for the Rx (~ -40 to +8.2 dBm)

SFP Memory (Port ▶ SFP ▶ [connector])

The SFP memory field provides access to sophisticated identification information that describes the transceivers capabilities, standard interfaces, manufacturer and other information. Refer to INF-8074 for detailed descriptions of the individual data fields.

7 Managing Traffic

This chapter describes how to create and manage Ethernet services; it contains the following sections:

7.1 Setting Up Traffic Policies

7.1.1 Viewing a Summary of the Policy Configurations

Access the page **Traffic ▸ Policies** to view a summary of the policy configurations. Click the name in the **Policy Lists** to view the summary of the policy configurations of a particular port.

Each frame's VLAN ID is analyzed and the value of the VLAN ID is used to directly access the appropriate policy to apply.

For more information on specific parameters, refer to the following table.

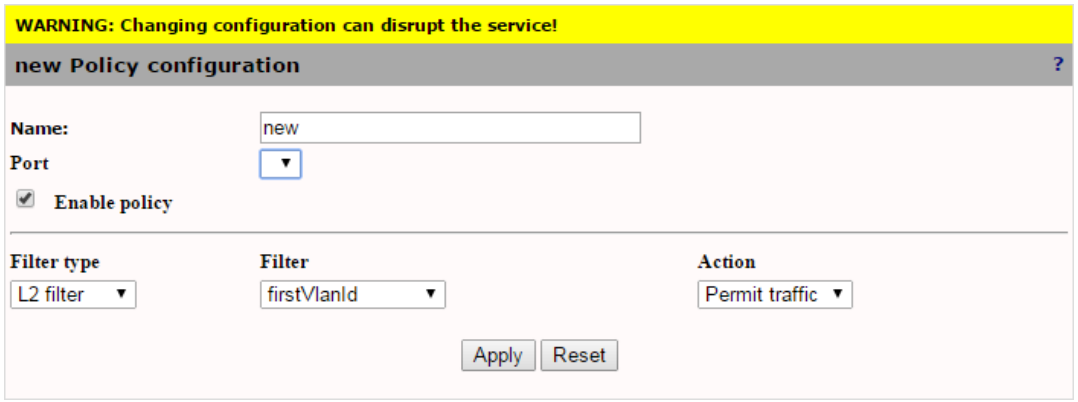
Policy (Traffic ▸ Policies)

Parameter	Description
Name	Name of the traffic policy
State	The policy may be enabled or disabled. Disabled policies are ignored when the rules are applied to incoming data.
Action	Action that the policy applies to data that it matches
Filter Name	Name of the filter assigned to the policy
Type	The filter type (L2 - IPv4 or VID set) used to classify traffic
Port	Name of the port of the traffic policies

7.1.2 Assigning Filters to a Traffic Policy

Once you have set up the filters, you are ready to assign them to a traffic policy so they can become a service.

Traffic ▸ Policies



▶ To set up a traffic policy

1. Access the page **Traffic ▶ Policies**.

   The *Traffic Policies Configuration* page opens.

2. Click a policy name.

   The *Policy 1 Configuration* page opens.

3. Select the filter to classify traffic and the required action, then click **Apply**.

   Note: Only the traffic matching the filter will have the rules applied to it. The maximum number of traffic policies using a specific filter (L2 filter or IPv4 filter) is limited by the type of unit you use. Refer to your unit's datasheet for the maximum number of specific filters possible for traffic policies.

For more information on specific parameters, refer to the following table.

Policy Configuration (Traffic ▶ Policies)

Parameter	Description
Enable Policy	Activates the policy
Filter Type	The filter type (Layer-2 filter, IPv4 filter or **VID set**) used to classify traffic
Filter	The name of the filter. By default, a *catch-all* filter is defined. This enables you to monitor all traffic on a port.
Action	The action applied to traffic that matches the filter. Make a selection from the drop-down list: • **Drop Traffic**: The traffic matching the filter is dropped. Policy statistics are collected as part of this policy. • **Permit Traffic**: The traffic matching the filter is counted in the statistics then forwarded. Policy statistics are collected as part of this policy.

7.2 Defining Filters

You can set up a specific filter (Layer-2 or IPv4) for use with loopbacks, measuring bandwidth utilization per flow or traffic policies. This way, you can loop back traffic or set up a traffic policy based on specific characteristics such as Ethernet Header settings, VLAN settings and DSCP for Layer-2 filters, or based on IPv4 Header settings, UDP/TCP settings and VLAN settings. You can also use the preconfigured Layer-2 or IPv4 filters.

*Note: The maximum number of **traffic policies** using a specific filter (L2 filter or IPv4 filter) is limited by the type of unit you use. Refer to your unit's datasheet for the maximum number of specific filters possible for traffic policies.*

7.2.1 Configuring a Layer-2 Filter

▶ To set up a Layer-2 filter

1. Access the page **Traffic ▶ Filters ▶ L2 Filters**.

   A summary of all Layer-2 filters that are currently set up is displayed. For more information on specific parameters, refer to the table at the end of this procedure.

   Note: Commonly-used filters have been predefined for your convenience.

2. Click **Add** to add a new filter or click the **Filter Name** of an existing Layer-2 filter to edit its settings.

3. Check the appropriate check box to enable this field, complete the required fields, then click **Add**.

   Note: For all fields, check the box to enable the field. If the check box is not checked, the value will be ignored.

   Note: You can specify several VLAN fields for the first VLAN (VLAN 1) as well as for the second level VLAN (VLAN 2).

For more information on specific parameters, refer to the following table.

Layer-2 Filters (Traffic ▶ Filters ▶ L2 Filters)

Parameter	Description
L2 Filter Name / Filter Name	Unique name to identify the filter
Ethernet Header Settings	
MAC Destination / Mask	The destination MAC address and mask. Only the bits specified by the mask are used. The other bits are ignored.

Parameter	Description
	Address Format: six pairs of hexadecimal digits separated by colons (xx:xx:xx:xx:xx:xx).
Remote Device MAC	Enable this box to automatically assign the remote device's own MAC address as the frames' destination address. Using the remote device's MAC address means you do not have to create a filter per device when several devices share the same loopback.
MAC Source / Mask	The source MAC address and mask. Only the bits specified by the mask are used. The other bits are ignored. **Address Format**: six pairs of hexadecimal digits separated by colons (xx:xx:xx:xx:xx:xx).
Encapsulated Ethertype	Protocol may be selected or entered manually (hexadecimal): • IPv4 (0x0800) • X.25 Layer3 (0x0805) • ARP (0x0806) • REVARP (0x8035) • IPX (0x8137) • VLAN (0x8100) • SNMP (0x814C) • WCP (0x80FF) • IPv6 (0x86DD) • MAC Control (0x8808) • MAC Protocol (0x22E2) • PPP (0x880B) • MPLS (0x8847) • MPLS Multicast (0x8848) • PPPOE Discovery (08863x) • PPPOE Session (0x8864) • S-VLAN (0x88A8)

Parameter	Description
	• T-VLAN (0x9100) • LLDP (0x88CC) • 3GPP2 (0x88d2) • LOOP
VLAN Stack Size	Enable this box, then make a selection in the drop-down list to indicate the number of VLAN tags that packets must have in order to match this filter.
VLAN and VLAN-in-VLAN Settings	
Ethertype	The VLAN Ethernet Type may be one of the following: • **C-VLAN**: Customer VLAN (typically inner tag) • **S-VLAN**: Service VLAN (typically outer tag) • **T-VLAN**: Tunnel VLAN (inner or outer tag)
CFI/DEI	The *Canonical Format Indicator* (CFI) or the *Drop Eligibility Indicator* (DEI). This value should always be set to *zero* for connections to Ethernet switches. CFI is used to ensure compatibility between Ethernet type networks and Token Ring type networks. If a frame received at an Ethernet port has a CFI set to *1*, the frame should not be forwarded "as-is" to an untagged port. In the context of bandwidth regulation, DEI can be used to carry the frame color. When set to *0*, the frame is green; when set to *1* the frame is yellow.
Priority	VLAN priority allows provisioning CoS prioritization using the standard 802.1Q priority tag. Interpreting the priorities is based on the carrier's equipment and administrative policies. The valid operator types are: • Greater than • Less than • Equal to • Range (inclusive range) The possible values for each operator are: 0 to 7. *Note: You can set only one VLAN (**VLAN** or **VLAN-in-VLAN**) to a*

Parameter	Description
	*range; the other must be set to **Equal to**. For instance, if you select a range for the second VLAN (**VLAN-in-VLAN**), you must select **Equal to** for the first VLAN (**VLAN**).*
VLAN ID	The VLAN ID used to filter traffic. The valid operator types are: • Greater than • Less than • Equal to • Range (inclusive range) *Note: You can set only one VLAN (**VLAN** or **VLAN-in-VLAN**) to a range; the other must be set to **Equal to**. For instance, if you select a range for the second VLAN (**VLAN-in-VLAN**), you must select **Equal to** for the first VLAN (**VLAN**).*
DSCP/IP Precedence	
DSCP/IP Precedence	The DSCP/IP precedence operator may be one of the following: • Greater than • Less than • Equal to • Range (inclusive range)

7.2.2 Configuring an IPv4 Filter

▶ To set up an IPv4 filter

1. Access the page **Traffic ▶ Filters ▶ IPv4 Filters**.

   A summary of all IPv4 filters that have been set up is displayed. For more information on specific parameters, refer to the table at the end of this procedure.

   Note: Commonly-used filters have been predefined for your convenience.

2. Click the **Add** button to add a new filter, or click the **Filter Name** of an existing IPv4 filter to edit its settings.

3. Check the appropriate check box to enable this field, complete the required fields, then click **Add**.

   Note: For all fields, check the box to enable the field. If the check box is not checked, the value will be ignored.

Note: You can specify several VLAN fields for the first VLAN (VLAN 1), as well as for the second-level VLAN (VLAN 2).

For more information on specific parameters, refer to the following table.

IPv4 Filters (Traffic ▶ Filters ▶ IPv4 Filters)

Parameter	Description
IPv4 Filter Name Filter Name	A unique name used to identify the filter
IPv4 Header Settings	
IPv4 Source / Mask IP Source	The source address and mask. Only the bits specified by the mask are used; the other bits are ignored. *Note: Filtering source or destination IP addresses that are assigned by Dynamic Host Control Protocol (DHCP) can be problematic. It is recommended to only specify static or reserved IP addresses in a filter, otherwise the filter must be updated manually whenever the addresses change.*
IPv4 Destination / Mask IP Destination	The destination address and mask. Only the bits specified by the mask are used; the other bits are ignored. *Note: Filtering source or destination IP addresses that are assigned by Dynamic Host Control Protocol (DHCP) can be problematic. It is recommended to only specify static or reserved IP addresses in a filter, otherwise the filter must be updated manually whenever the addresses change.*
TTL	The time-to-live value
ECN	Explicit Congestion Notification. Specify either *0* or *3*.
Header Length	The header length, expressed in 32-bit words. Specify a value in the range of 5–15.
Protocol	Either select a protocol from the list below or enter a port number (decimal) manually. Common protocols are TCP (6), UDP (17) and ICMP (1). TCP is used by HTTP, FTP, Telnet and SMTP. UDP is used by DNS, SNMP and RIP. ICMP is used by Ping. The available protocols, expressed in the format of *protocol name (port number)*, are: • ICMP (1) • ICMP (2) • IP (4)

Parameter	Description
	• TCP (6) • EGP (8) • IGP (9) • UDP (17) • IPv6 (41) • SDRP (42) • IPv6-Route (43) • IPv6-Frag (44) • IDRP (45) • RSVP (46) • GRE (47) • MHRP (48) • ESP (50) • AH (51) • MOBILE (55) • SKIP (57) • EIGRP (88) • OSPFIG (89) • IPComp (108) • VRRP (112)
UDP/TCP Port Settings	
Source Port	Specify the UDP or TCP port number used by the IPv4 source port field. This setting is valid only when the Protocol is set to *TCP (6)* or *UDP (17)*.
Destination Port	Specify the UDP or TCP port number used by the IPv4 destination port fields.

Parameter	Description
	This setting is valid only when the Protocol is set to *TCP (6)* or *UDP (17)*.
ICMP Settings	
ICMP Type	Enables the use of ICMP. You must specify the ICMP message type to be matched by this filter. *Note: These settings are only valid when the "Protocol" parameter is set to **ICMP (1)**.* Some well-known ICMP types are: • Echo Reply (0) • Destination Unreachable (3) • Redirect (5) • Echo (8) • Time Exceeded (11) Other ICMP Codes: See www.iana.org/
ICMP Code	Enables the use of ICMP code
VLAN and VLAN-in-VLAN Settings	
Ethertype	The VLAN Ethernet Type may be one of the following: • **C-VLAN**: Customer VLAN (typically inner tag) • **S-VLAN**: Service VLAN (typically outer tag) • **T-VLAN**: Tunnel VLAN (inner or outer tag)
CFI/DEI	The *Canonical Format Indicator* (CFI) or the *Drop Eligibility Indicator* (DEI). This value should always be set to *zero* for connections to Ethernet switches. CFI is used to ensure compatibility between Ethernet type networks and Token Ring type networks. If a frame received at an Ethernet port has a CFI set to *1*, the frame should not be forwarded "as-is" to an untagged port. In the context of bandwidth regulation, DEI can be used to carry the frame color. When set to *0*, the frame is green; when set to *1* the frame is yellow.
Priority	VLAN priority allows provisioning CoS prioritization using the standard 802.1Q priority tag. Interpreting the priorities is based on the carrier's equipment and administrative policies. The valid

Parameter	Description
	operator types are: • Greater than • Less than • Equal to • Range (inclusive range) The possible values for each operator are: 0 to 7. *Note: You can set only one VLAN (**VLAN** or **VLAN-in-VLAN**) to a range; the other must be set to **Equal to**. For instance, if you select a range for the second VLAN (**VLAN-in-VLAN**), you must select **Equal to** for the first VLAN (**VLAN**).*
VLAN ID	The VLAN ID used to filter traffic. The valid operator types are: • Greater than • Less than • Equal to • Range (inclusive range) *Note: You can set only one VLAN (**VLAN** or **VLAN-in-VLAN**) to a range; the other must be set to **Equal to**. For instance, if you select a range for the second VLAN (**VLAN-in-VLAN**), you must select **Equal to** for the first VLAN (**VLAN**).*
DSCP/IP Precedence	
DSCP/IP Precedence	The DSCP/IP precedence operator may be one of the following: • Greater than • Less than • Equal to • Range (inclusive range)

7.3 Working with the FlowMETER

7.3.1 Setting Up Bandwidth Utilization per Flow

Access the FlowMETER Rules page to obtain the current report from the FlowMETER, which is useful when determining bandwidth utilization on a per-flow basis. Bandwidth measurements for the various flows on configured ports are available in the Traffic page of the Management Web interface. The critical step when creating or managing bandwidth usage per flow is defining the Layer-2 filters.

The FlowMETER collects throughput samples on each supported port with counters that are continuously incremented, making it possible to determine the maximum, minimum and average throughput for each report period, expressed in bits per second.

The FlowMETER calculates throughput as the average rate of successful message delivery over a port, expressed in bits per second (bps). The statistics for each report period include the throughput, the number of bytes, and the number of packets for the configured flow. Port statistics are reported as flow statistics as soon as the FlowMETER is enabled. The port statistics cannot be disabled.

> *Note: The FlowMETER calculates throughput using the bytes received on Layer 2 only. Layer 1 overhead is not included in the throughput calculations.*

The system is designed in such a way that the traffic flow must first be defined as a set of valid received frames that match a filter. Once classified, bandwidth usage can be determined for a flow.

Collecting all statistics on ports and flows once is called a *measurement*. Each such measurement has a sampling period, which is the time that elapses between when each measurement is sampled.

7.4 Setting Up FlowMETER Flow Rules

Once you have set up filters, you are ready to assign them to a traffic flow for which the bandwidth utilization can be calculated. Use the following procedure to view or configure port settings for the various traffic flows for which bandwidth utilization is to be calculated in the system.

▸ To view or configure traffic flow port settings

1. Access the page **Traffic ▸ FlowMETER ▸ Rules**.

   A listing of all FlowMETER ports available in the system is displayed.

2. Click the **Name** of a FlowMETER port from the list to edit its settings.

   The page refreshes to reflect your selection.

3. In the **Flow Configuration** section, click one of the **Index** values to insert a flow definition at this entry in the list.

4. The following statistics are provided in the **Flow Statistics Sample** section:

   - The number of packets
   - The number of bytes
   - The delta of the packets and bytes between the last two samples
   - The throughput of the current sample.

   These statistics are shown for each flow defined, as well as for the port (which indicates the sum of all the flows' statistics).

5. The following statistics are provided in the **Flow Report** section for each report period:

   - The number of packets
   - The number of bytes
   - The average, minimum and maximum throughput calculated

   These statistics are shown for each flow defined, as well as for the port (which indicates the sum of all the flows' statistics).

7.4.1 Configuring Flow Filters per Port

You can define the flows for which statistics will be gathered for each of the VCX Controller's available ports. Follow the steps below to configure flows for which statistics will be calculated on a per port basis.

▶ To configure flows for calculating per-port statistics

1. Access the page **Traffic ▶ FlowMETER ▶ Rules**.

   A listing of all FlowMETER ports available in the system is displayed.

2. Click the **Name** of a FlowMETER port from the list to view its settings.

   The page refreshes to reflect your selection.

The parameters in the Flow Configuration section are described in the following table.

Flow Configuration Parameters (Traffic ▶ FlowMETER ▶ Rules)

Parameter	Description
Index	The filter identifier associated with the flow *Note: A port index is created by default to cover the statistics related to the port itself, and not to a specific flow.*
State	The flow may be either *Enabled* or *Disabled*. *Note: Disabled flows are ignored when the rules are applied to incoming data.*
Filter Name	The name of the L2 filter created in the **Traffic ▶ Filters ▶ L2 Filters** page in order to define the flow for which statistics will be gathered *Note: The equivalent of a catch-all L2 flow filter takes precedence over any other filters defined after this entry. As such, devices will not report any statistics for other flow filters being defined.* ***CAUTION**: Only the following L2 filter parameters are applicable when defining the flow to be measured. As such, an L2 filter that does not have these and only these parameters defined will cause an error in both the Management Web interface and the Command Line Interface (CLI).* • **Ethertype**: The underlying Ethertype must be set to *IPv4* if enabled. It will automatically be set to IPv4 if DSCP or IP precedence IP header bits are defined. • **VLAN Stack Size**: Enable this box, then make a selection in the drop-down list to indicate the number of VLAN tags that packets must have in order to match this filter. • **VLAN or VLAN-in-VLAN settings**:

Parameter	Description
	– **CFI/DEI**: Used when filtering to indicate priority – **Priority**: VLAN priority allows provisioning CoS prioritization using the standard 802.1Q priority tag. Interpreting the priorities is based on the carrier's equipment and administrative policies. The valid operator types are: – Greater than – Less than – Equal to – Range (inclusive range) – The possible values for each operator are: 0 to 7. – **VLAN ID**: The VLAN ID used to filter traffic. • **DSCP/IP Precedence**: The DSCP/IP precedence operator may be one of the following: – Greater than – Less than – Equal to – Range (inclusive range)
Type	The type of filter that defines the flow for which statistics are to be gathered

7.4.2 Viewing Flow Statistics per Port

Once flow filters have been configured, you can view the statistics for each flow, as well as for the port to which the flows are configured.

Note: Flow statistics reported per port through a VCX Controller instance are accessible only once the reporting parameters have been properly set.

▶ To view per-port flow statistics

1. Access the page **Traffic ▶ FlowMETER ▶ Rules**.

   A listing of all FlowMETER ports available in the system is displayed.

2. Click the **Name** of a FlowMETER port from the list to view its settings.

   The page refreshes to reflect your selection.

The values in the Flow Statistics section and the Flow Statistics Report section are described in the following tables.

Flow Statistics Values (Traffic ▸ FlowMETER ▸ Rules)

Value	Description
Index	The filter identifier associated with the flow *Note: A port index is created by default to cover the statistics related to the port itself, and not to a specific flow.*
State	The policy may be either *Enabled* or *Disabled*. *Note: Disabled policies are ignored when the rules are applied to incoming data.*
Filter Name	The name of the L2 filter created in the **Traffic ▸ Filters ▸ L2 Filters** page in order to define the flow for which statistics will be gathered
Packets	The number of packets received for the specific flow filter
Bytes	The number of bytes received for the specific flow filter
DeltaPackets	The delta in the number of packets received for the specific flow filter between the last two complete sample periods
DeltaBytes	The delta in the number of packets received for the specific flow filter between the last two complete sample periods
Throughput	The throughput calculated according to the number of bytes received during the sampling periods

Flow Statistics Report Values (Traffic ▸ FlowMETER ▸ Rules)

Value	Description
Index	The filter identifier associated with the flow *Note: A port index is created by default to cover the statistics related to the port itself, and not to a specific flow.*
Filter Name	The name of the L2 filter created in the **Traffic ▸ Filters ▸ L2 Filters** page in order to define the flow for which statistics will be gathered
Packets	The number of packets received for the specific flow filter
Bytes	The number of bytes received for the specific flow filter
Throughput Avg	The average throughput calculated according to the number of

Value	Description
	bytes received in the sampling periods
Throughput Min	The minimum throughput calculated according to the number of bytes received in one of the sampling periods
Throughput Max	The maximum throughput calculated according to the number of bytes received in one of the sampling periods

7.5 Configuring FlowMETER Flows

Once you have set up filters, you are ready to assign them to a traffic flow for which the bandwidth utilization can be calculated. Use the following procedure to configure the traffic flows for which bandwidth utilization is to be calculated in the system.

▶ To view or configure traffic flow port settings

1. Access the page **Traffic ▶ FlowMETER ▶ Rules**.

   A listing of all FlowMETER ports available in the system is displayed.

2. Click the **Name** of a FlowMETER port from the list.

   The page refreshes to reflect your selection.

3. In the **Flow Configuration** section, click one of the **Index** values to insert a flow definition at this entry in the list.

4. Enter values in the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Flow Configuration Parameters (Traffic ▶ FlowMETER ▶ Rules ▶ [Device])

Parameter	Description
Enable Flow	Select this box to enable the flow
Filter Type	The filter type is taken from the **Traffic ▶ Filters** pages; you cannot modify this value here.
Filter	Make a selection from the drop-down list to indicate the kind of filter to use with this flow

7.6 Setting Up Flow Reporting

Once you have set up rules per port using flow filters, you are ready to configure the reporting of the bandwidth utilization calculated by the FlowMETER. Use the **Traffic ▸ FlowMETER ▸ General** page to configure the flow reporting settings for the various traffic flows for which bandwidth utilization will be calculated.

If the remote device has not been assigned an IP address, flow reporting is still possible when in IPAD mode, since this mode does not rely on the device's IP address when sending FlowMETER-related information to the VCX.

▸ To configure reporting settings for a traffic flow

1. Access the page **Traffic ▸ FlowMETER ▸ General**.
2. Complete the required fields, then click **Apply** to save your changes.

For information on specific parameters, refer to the following table.

Traffic Flow Reporting Parameters (Traffic ▸ FlowMETER ▸ General)

Parameter	Description
Destination UDP Port	The UDP port associated with the IP address of the VCX Controller instance that will receive, process and display the flow statistics and report. *Note: For the flow reporting to work properly, you must set the port to a value other than 0.*

7.7 Configuring Traffic

7.7.1 Setting the Working Rate

You must select the layer (Layer 1 or Layer 2) used by the SkyLIGHT VCX Controller to determine the rate for the traffic generators. For example, if you set up a traffic generator flow with a bit rate of 20,000 kbps, the remote device must be informed of which bytes are being used to calculate the bit rate. The working rate options are:

- **Layer-1**: Layer-1 Ethernet frames contain all Ethernet frame fields plus the Inter-Frame Gap (IFG), Preamble and Start-Frame Delimiter (SFD).
- **Layer-2**: Layer-2 Ethernet frames contain all Ethernet frame fields. This does not include the Inter-Frame Gap (IFG), Preamble and Start-Frame Delimiter (SFD).

Note: Exercise caution when setting up the working rate. You should ensure that you set the different working rates to the same layer when they work together in a particular setup in order to generate accurate test results.

▶ To set the working rate

1. Access the page **Traffic ▶ Configuration**.
2. Select the working rate to be applied to all entities, then click **Apply**.

For more information on specific parameters, refer to the following table.

Traffic Configuration (Traffic ▶ Configuration)

Parameter	Description
Generator Working Rate	The layer used by the VCX Controller to determine the working rate: • **Layer-1**: Layer-1 Ethernet frames contain all Ethernet frame fields plus the Inter-Frame Gap (IFG), Preamble and Start-Frame Delimiter (SFD). • **Layer-2**: Layer-2 Ethernet frames contain all Ethernet frame fields. This does not include the Inter-Frame Gap (IFG), Preamble and Start-Frame Delimiter (SFD).

8 Managing Loopbacks

This chapter describes how to manage loopbacks; it contains the following sections:

8.1 Understanding Loopback Testing

Layer 1 to 4 loopbacks (MAC address, IP address and port swap frame reflection) enable remote QoS testing Ethernet, IP and triple-play services. You can establish loopbacks using any of the following combination of parameters:

- The source and/or destination MAC address
- The VLAN ID
- The source and/or destination IP address
- The source and/or destination UDP/TCP ports
- The service level

Loopbacks can be performed either in-band or out-of-band, thereby not impacting customer traffic while tests are being performed.

The VCX Controller supports the following two types of loopbacks:

- **Local (or Private) Loopback**: Loops back all traffic matching the custom loopback parameters you define
- **Remotely-Controlled Loopback**: Loops back traffic upon the reception of a predefined frame type from a JDSU/Acterna™ test set

8.2 Setting Up and Enabling Loopbacks

Follow the steps below to set up a local loopback:

- Create a filter that specifies the matching criteria for capturing traffic (applies to custom loopbacks only).
- Create the loopback, as explained in the following procedure.

▶ To set up a local loopback

1. Access the page **Loopback ▶ Configuration**.

   A summary of all OAM loopback instances that have been set up is displayed.

2. To add a new instance, click **Add**, or click an instance's **Name** to edit its settings.
3. Enter values in the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Note: Only the fields listed in the following table are required for a local loopback. Leave all other fields at their default settings.

Loopback (Loopback ▶ Configuration)

Parameter	Description
Name	The OAM Loopback instance name, as defined in the page
Device	The name of the remote device to which the loopback applies
Port	The port on the remote device to which the loopback operation applies. Both UNI and NNI ports are supported.
State	The current state of the loopback, either *Enabled* or *Disabled*. Default value: Disabled.
Loopback Enable	Select this box to activate this loopback instance, then choose the **Type** from the drop-down list.
Type	Type may be one of the following: • **Custom**: Loops back all traffic that matches the user-defined filter (**Filter Type** and related fields)
Filter Type	The type of filter to be applied to the loopback traffic: • **L2 Filter** • **IPv4 Filter**

Parameter	Description
L2 Filter	The L2 filter to be applied to loopback traffic, if the filter type is *L2 Filter* ***CAUTION**: Only the following L2 filter parameters are applicable when defining the loopback flow. As such, an L2 filter that does not have these and only these parameters defined will cause an error in both the Management Web interface and the Command Line Interface (CLI).* *No DSCP/IP precedence is filtered in loopbacks.* • **Source MAC Address/Mask**: The source MAC address of the frame with the mask must be byte-oriented, i.e., a 0-, 8-, 16-, 24-, 32-, 40- or 48-bit mask. • **Destination MAC Address/Mask**: The destination MAC address of the frame with the mask must be byte-oriented, i.e., a 0-, 8-, 16-, 24-, 32-, 40- or 48-bit mask. • **Ethertype**: The underlying Ethertype must be *IPv4* if IP precedence IP header bits are to be defined. • **VLAN Ethertype**: The first VLAN Ethertype value. • **VLAN or VLAN-in-VLAN Settings**: – VLAN ID: The VLAN ID used to filter traffic – No priority bits are filtered in loopbacks
IPv4 Filter	The IPv4 filter to be applied to loopback traffic, if the filter type is *IPv4 Filter* ***CAUTION**: Only the following IPv4 filter parameters are applicable when defining the loopback flow. As such, an IPv4 filter that does not have these and only these parameters defined will cause an error in both the Management Web interface and the Command Line Interface (CLI).* • **Source IPv4 Address/Mask**: The source IPv4 address of the packet with the mask must be byte-oriented, i.e., a 0-, 8-, 16-, 24- or 32-bit mask.

Parameter	Description
	• **Destination IPv4 Address/Mask**: The destination IPv4 address of the packet with the mask must be byte-oriented, i.e., a 0-, 8-, 16-, 24- or 32-bit mask. • **Protocol**: The *Protocol* field in the IP header to be filtered. • **TCP/UDP Port**: Both the source and destination ports are required when the *Protocol* field is set to either *6* or *17*. • **VLAN Ethertype**: The first VLAN Ethertype value. • **No DSCP/IP precedence filtered in loopbacks** • **VLAN or VLAN-in-VLAN Settings**: – VLAN ID: The VLAN ID used to filter traffic – No priority bits are filtered in loopbacks
Actions	The action may be one or more of the following: • **Swap MAC Addresses**: Swaps the source and destination MAC addresses • **Swap IP Addresses**: Swaps the source and destination IP addresses • **Swap TCP/UDP Ports**: Swaps the source and destination TCP/UDP ports
Drop Opposite Traffic	Drops the traffic entering the device on the opposite port *Note: enabling this option interrupts the Ethernet service in one direction.* *Note: The Drop Opposite Traffic option is disabled 5 seconds after the last frame to loop back has been received. The loopback itself is automatically terminated once this period elapses.*
Loopback Timeout	Number of minutes for the loopback to remain enabled. When the timeout expires, the loopback is automatically terminated.
Remote Loopback Enable	
JDSU/Acterna™	Select this box to indicate that this remote loopback will be controlled by a JDSU/Acterna™ device.
Enable Discovery Loop Commands	Select this box to indicate that this remote loopback will accept JDSU/Acterna™ discovery loopback commands.

Parameter	Description
Loop Up Timeout	The timeout period after the *Loop Up* command has been received before initiating the JDSU loopback tests.

9 Monitoring Network Performance with Service OAM

The SkyLIGHT VCX Controller allows for monitoring network performance using a proprietary Service OAM technology and a standard Service OAM protocol (IEEE 802.1ag). These monitoring techniques are presented in the following sections:

9.1 Using Service OAM

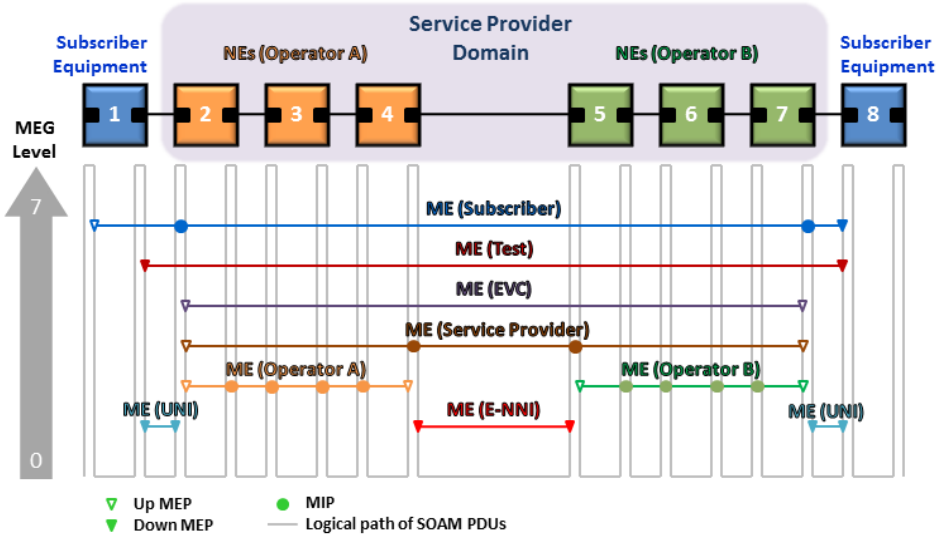
This section describes the IEEE 802.1ag "Service OAM" function and how to set it up on your Metro Ethernet Network to perform end-to-end monitoring.

Service OAM (or CFM Connectivity Fault Management) encompasses fault management and performance management capabilities of the VCX Controller.

> *Note: The VCX Controller's implementation of Service OAM is primarily focused on reflecting loopback message frames and delay measurements.*

The following figure shows an overview of Service OAM.

Overview of Service OAM



9.1.1 Setting Up CFM

The steps required to set up Connectivity Fault Management (CFM) are:

- Set up Maintenance Domains (MD).
- Set up Maintenance Associations (MA), also known as Maintenance Entity Groups (MEG).
- Set up Maintenance association End Points (MEP).

Once these are set up, you can use Service OAM for performing the following fault management functions:

- Loopback Messages. See "Setting Up and Enabling Loopbacks".

Setting Up Maintenance Domains (MD)

There are eight pseudo MDs defined by default, one for each level, named **Y.1731 level 0** to **Y.1731 level 7**. These MDs exist only to simplify the integration of MEGs for Y.1731 with the CFM MIB, which requires MDs. The Y.1731 protocol uses MEG-IDs, which are MAIDs without an MD name. User interfaces show the pseudo MD name, but this name is not included in the Y.1731 CCM's MEG-ID.

Note: Pseudo MDs cannot be deleted from the system.

▶ To set up a Maintenance Domain

1. Access the page **SOAM ▶ CFM ▶ MD**.

   A listing of all existing Maintenance Domains is displayed.

2. Click the **Add** button to create a new Maintenance Domain or click the **Name** of an existing Maintenance Domain to edit its settings.

3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Maintenance Domain (SOAM ▶ CFM ▶ MD)

Parameter	Description
Name Format	The format of the Maintenance Domain name The available options are: • **Character String**: RFC-2579 display string, except that the character codes 0–31 (decimal) are not used • **DNS-Like Name**: Domain Name-like string, a globally-unique text string derived from a DNS name

Parameter	Description
	The name format must be the same for the other endpoints.
Name MD Name	Unique name for the Maintenance Domain
Level	Maintenance Level of the Maintenance Domain Possible values: 0-7

Deleting a Maintenance Domain (MD)

▶ To delete a maintenance domain

1. Access the page **SOAM ▶ CFM ▶ MD**.

   A listing of all existing Maintenance Domains is displayed.

2. Click the name of the MD instance to be deleted.

3. Click **Delete**.

> ***CAUTION**: Deleting an MD will also delete all instances (e.g. MA/MEG) that use this MD.*

Setting Up Maintenance Associations (Maintenance Entity Groups)

Before setting up an MA (also referred to as a MEG), you must first set up the MD to which you want the MA/MEG to belong. Maintenance Associations (MA) are discussed in IEEE 802.1ag; Maintenance Entity Groups (MEG) are discussed in ITU-T Y.1731.

▶ To set up a Maintenance Association or Maintenance Entity Group

1. Access the page **SOAM ▶ CFM ▶ MA/MEG**.

   A listing of all Maintenance Associations / Maintenance Entity Groups is displayed.

2. Click the **Add** button to add a new Maintenance Association or Maintenance Entity Group or click the **Name** of an existing Maintenance Association or Maintenance Entity Group to edit its settings.

3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Maintenance Association (SOAM ▶ CFM ▶ MA/MEG)

Parameter	Description
MD	Maintenance Domain for this Maintenance Association or Maintenance Entity Group

Parameter	Description
Name Format	The format of the Maintenance Association or Maintenance Entity Group name The available options are: • **String**: RFC-2579 display string • **ICC-Based**: ITU Carrier Code format
Name MA/MEG Name	The name of this Maintenance Association or Maintenance Entity Group
CCM Interval	The required time interval between Continuity Check Messages (CCM). Expressed in milliseconds. Default: 1000 milliseconds
VLAN Type	The VLAN type associated with this Maintenance Association or Maintenance Entity Group Possible values are: • **None**: The association is not attached to a VLAN and the content of the VLAN ID list is ignored • **C-VLAN**: Customer VLAN (typically inner tag) • **S-VLAN**: Service VLAN (typically outer tag) • **T-VLAN**: Tunnel VLAN (inner or outer tag)
VLAN ID List	A list of the VLANs associated with this Maintenance Association or Maintenance Entity Group If you leave the VLAN ID field empty, the association is not attached to a VLAN and the VLAN type is set to *None* implicitly.
MEPID List	A comma-separated list of all the MEPs that are associated with this Maintenance Association or Maintenance Entity Group

▶ To delete a Maintenance Association (Maintenance Entity Group)

1. Access the page **SOAM ▶ CFM ▶ MA/MEG**.

   A listing of all Maintenance Associations / Maintenance Entity Groups is displayed.

2. Click the name of the Maintenance Association or Maintenance Entity Group to be deleted.

3. Click **Delete**.

***CAUTION**: Deleting a MA/MEG will also delete all instances (e.g. MEP) that use this MA/MEG.*

Setting Up Maintenance association End Points

Before setting up a MEP, you must first set up its MA/MEG. Maintenance association End Points (MEP) are discussed in IEEE 802.1ag.

▶ To set up a Maintenance association End Point

1. Access the page **SOAM ▶ CFM ▶ MEP ▶ Configuration**.

   A listing of all Maintenance association End Points is displayed.

2. Click the **Add** button to add a new MEP or click the **MEPID** of an existing MEP to edit its settings.

3. Complete the required fields, then click **Apply** .

For more information on specific parameters, refer to the following table.

Maintenance association End Point (SOAM ▶ CFM ▶ MEP ▶ Configuration)

Parameter	Description
MA/MEG Name	The name of the maintenance association (or MEG) to associate with the MEP
MEPID	Maintenance association End Point Identifier (MEPID) for this Maintenance association This value is an integer, unique to each MA, that identifies a specific MEP in CCM frames.
Port	The port used by this MEP
MEP Name	The name of the Maintenance association End Point
Active	The administrative state of the MEP: • **Checked (Yes)**: The MEP is to function normally. • **Unchecked (No)**: The MEP is to cease functioning. *Note: When deactivating a MEP, you must also deactivate all DMM instances that use this MEP. Doing so will prevent the VCX Controller from detecting unwanted alarms, such as CCM alarms.*
Primary VID VLAN	The Primary VLAN ID of the MEP. This is always one of the VLAN IDs assigned to the MEP's MA/MEG. The value 0 indicates that either the Primary VLAN ID is that of the MEP's MA/MEG, or that the MEP's MA/MEG is not associated with a VLAN ID.

▶ To delete a Maintenance association End Point

1. Access the page **SOAM ▶ CFM ▶ MEP ▶ Configuration**.

   A listing of all Maintenance association End Points is displayed.

2. Click the MEPID of the MEP to be deleted.

3. Click **Delete**.

Viewing MEP Status

▶ To view maintenance association end point (MEP) status

1. Access the page **SOAM ▶ CFM ▶ MEP ▶ Status**.

   A listing of all MEPs is displayed, along with their status codes and details.

   The total number of MEPs found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 54). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain MEPs, enter a value on which to filter, then click **Search**. You can filter by the MEP name, MEPID or the R-CCM status code value.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

For more information on specific codes, refer to the following table.

MEP Status (SOAM ▶ CFM ▶ MEP ▶ Status)

Parameter	Description
MEP Name	The name assigned to this Maintenance association End Point
MEPID	Identifier for the Maintenance association End Point
R-CCM Remote CCM	Indicates whether the MEP is not receiving CCMs from a MEP in its configured list. Possible vales are *Active (A)* or *Inactive (I)*.

9.1.2 Setting Up Delay Measurements

DMM measurements (delay and delay variation) work as follows.

A DMM frame is sent from an originating unit to one of the remote devices linked to the VCX Controller. When the DMM frame is received by the remote device, it sends a DMR to the originating unit.

Note: Receiving the DMM frame by the remote device and transmitting the DMR involve some processing time that may or may not be accounted for.

DMM measurements are measurements of network delay and network delay variation. The remote device needs to eliminate processing time in order to obtain a true measurement of the network delay and delay variation. This is accomplished by the use of two time stamps:

- **c** = Time when the DMR frame (DMM response) was transmitted by the remote device
- **d** = Time when the DMR frame was received by the originating unit

Using these time stamps, the originating unit calculates one-way delay as follows:

- **One-Way Network Delay** = d – c

▶ To configure a delay measurement reflection endpoint

1. Access the page **SOAM ▶ CFM ▶ DMM ▶ Configuration**.

   A listing of all existing Delay Measurement instances (reflectors) is displayed.

   The total number of reflectors found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain reflection endpoints, enter a value on which to filter, then click **Search**. You can filter by index value, DMM name, remote device name/serial number, or whether or not the endpoint has been enabled.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. In the **Index** column of the table, click the value associated with the endpoint for which you want to view detailed information.

For more information on specific parameters, refer to the following table.

DMM Configuration (SOAM ▶ CFM ▶ DMM ▶ Configuration)

Parameter	Description
Index	The index of the Delay measurement instance
DMM Name Name	The name of the Delay Measurement instance
Remote Device Name	The name of a remote device to associate with the current DMM reflection instance
Enable	Select this box to enable reflecting DMM frames on the remote device specified above

9.2 Using the Two-Way Active Measurement Protocol (TWAMP)

This section describes the Two-Way Active Measurement Protocol (TWAMP) function and how to set it up in your Metro Ethernet network. TWAMP packet generation provides the ability to perform one- and two-way delay and delay variation in a Layer-3 network, as well as packet loss measurements. TWAMP packets are reflected back to the sender. The VCX Controller allows TWAMP packets to be reflected through its linked remote devices.

TWAMP defines two protocols:

- TWAMP control protocol (not supported by Accedian)
- TWAMP test protocol (supported by Accedian)

TWAMP light only includes the test protocol and is supported by the remote devices' TWAMP reflection feature. When using TWAMP light, test sessions can be configured without the control protocol.

Note: This function is only to be used with TWAMP when connecting to Layer-3 TWAMP session sender devices.

9.3 Setting Up a TWAMP Reflector

The VCX Controller can be configured to reflect TWAMP packets through the remote devices linked to it. The following procedure shows you how to enable this kind of packet reflection.

▶ To set up a TWAMP reflection endpoint

1. Access the page **SOAM ▶ TWAMP ▶ Reflector ▶ Configuration**.

   A listing of all TWAMP reflection instances is displayed.

   The total number of reflectors found in the system is given in the lower-left corner of the page, as well as the index values of the items currently displayed on-screen (for example, [1-25] of 254). Use the page navigation links in the lower-right corner of the page to move between the pages of results.

2. *(Optional)* To limit the view to only certain reflection endpoints, enter a value on which to filter, then click **Search**. You can filter by the device name, current device state, UDP port, or whether or not IP match or segmented TWAMP has been enabled.

   Note: Enter an asterisk (*) as a wildcard to replace one or several characters.

3. In the **Device** column of the table, click the value associated with the endpoint you want to modify.

For more information on specific parameters, refer to the following table.

TWAMP Configuration (SOAM ▶ TWAMP ▶ Reflector ▶ Configuration)

Parameter	Description
Remote Device Name	The name of the remote device on which the TWAMP reflection instance will be active
State Enable	Select to enable the processing of TWAMP packets destined to a remote device Default value: *Disabled*
UDP Port	The UDP port on which TWAMP packets are to be reflected by the remote device Default value: *6000*
IP Match	Select to enable the processing of TWAMP packets destined to a remote device
Segmented	Select to enable the support of segmented TWAMP. Segmented TWAMP requires TWAMP packets to be forwarded,

Parameter	Description
	which means that all remote devices encountered along the way can process and reply to the same TWAMP packets. *Note: The segmented TWAMP feature is designed to extend TWAMP for multiple inline remote devices in IP agnostic mode.*

10 Testing Network Performance

The SkyLIGHT VCX Controller allows for testing network performance using traffic generation and analysis, as specified in RFC-2544, and using Service Activation Testing (SAT), as specified in standard ITU-T Y.1564.

These testing techniques are presented in the following sections:

10.1 Using RFC-2544 for Traffic Generation and Analysis

This section presents traffic generation and analysis as specified in the RFC-2544. It describes how to set this up in your Metro Ethernet network and perform end-to-end testing and monitoring. This allows you to pinpoint devices or network problems or to measure current throughput, frame delay and frame-delay variation on a specific network segment.

Advanced traffic generation and analysis capabilities allow you to perform fully automated and documented turn-up tests. The test capabilities also include out-of-service tests.

For out-of-service tests, you must pair the traffic generator with another device that loops the traffic back. When testing with *Layer-2* generic frames or *Layer-3/Layer-3* generic packets (UDP), you must configure the peer unit with a loopback that matches the test traffic, and with a swapping action on the source/destination MAC addresses, IP addresses and UDP port numbers. For IP multicast traffic you must use the RFC monitor in the remote unit.

You may use the traffic generator to generate one or two flows of test traffic and provide separate results for each flow. Each flow has specific characteristics, such as traffic type and bit rate. You have the following choices when setting up each flow:

- Layer 2 (three types), Layer 3 (two types) and IP multicast traffic
- VLAN or VLAN-in-VLAN encapsulation of test traffic
- Different traffic types, frame/packet sizes and payload patterns

10.1.1 Setting Up the Traffic Generator

You can set up the traffic generator to send up to four traffic flows, each having a different traffic type, VLAN and patterns. To view the complete list of elements that can be configured for each traffic flow, refer to the table "RFC-2544 Generator Configuration (SAT ▸ RFC-2544 ▸ Generator ▸ Configuration)"

SAT Reporting is a system feature that enables you to have RFC-2544 reports automatically pushed from the SkyLIGHT VCX Controller to a designated remote server (FTP, SFTP, TFTP or SCP). Automatically pushing test reports to the server means you can view the test results more quickly, since you do not have to manually poll the remote server to determine whether or not the test has completed execution.

For details on how to automate report uploads to a remote server, see "Setting Up SAT Reporting" on page 145.

Note: All reports are available in text or XML format.

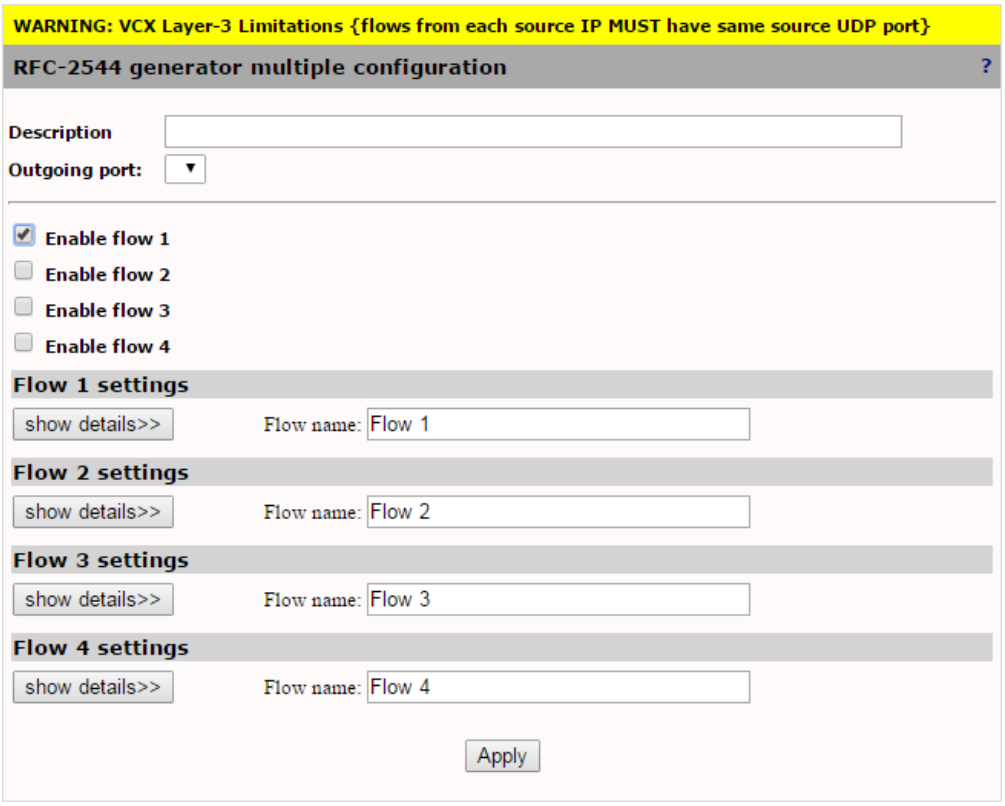
▶ To set up the RFC-2544 generator

1. Access the page **SAT ▶ RFC-2544 ▶ Generator ▶ Configuration**. An example of the display is shown in the figure below.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Note: The page content varies, depending on the traffic type you select.

SAT ▶ RFC-2544 ▶ Generator ▶ Configuration



RFC-2544 Generator Configuration (SAT ▶ RFC-2544 ▶ Generator ▶ Configuration)

Parameter	Description
Description	A description to identify the flow and its characteristics.
Outgoing Port	The port on which to send the flow(s)
Enable Flow	The flow(s) included in the test
First to Fourth Flow Header Settings	
Type	The type of test traffic: • **Layer-2**: Y.1731 LBM frames

Parameter	Description
	• **Layer-3**: UDP segments to perform a test across a multi-layered network
MAC Destination	The peer MAC address. Applies to Layer-2 and Layer-3 generic traffic only. *Note: Layer-3 generic traffic is available for the RFC-2544 traffic generator and test suite.*
Y.1731 MEG Level	The Maintenance Entity Group level Range: 0–7 *Note: Applies to Layer-2 traffic only. For details, refer to ITU-T Y.1731.*
Destination IP Address	The IP address of the remote unit interface. Applies to Layer-3 traffic only.
DSCP	The DiffServ Code Point to set in the generated packets. Applies to Layer-3 traffic only.
Source Port	The source UDP port number used to generate the UDP segment *Note: Applies to Layer-3 traffic only.*
Destination Port	The destination UDP port number that is used to generate the UDP segment *Note: Applies to Layer-3 traffic only.* *Note: You cannot set the destination port value to 8793, since this is Accedian's proprietary port number.* A port cannot be defined as the UDP port here if it is already being used for any of the following features: • Layer-3 RFC-2544 Generator • Layer-3 RFC-2544 Test Suite
TTL	The Time To Live (TTL) of the packets transmitted on the flow. *Note: Applies to layer-3 type tests only.*
Enable VLAN 1 Header	This encapsulates all frames with one VLAN header. Note: If frames with more than three VLAN tags are received by the destination NID, these frames will be discarded and frame losses will be recorded.
VLAN 1 ID	The first VLAN ID When enabled, all test frames are encapsulated with the

Parameter	Description
	specified VLAN ID.
VLAN 1 Ethernet Type	The first VLAN Ethernet type The available options are: • S-VLAN • T-VLAN • C-VLAN
VLAN 1 Priority	The first VLAN priority bits *Note: Applies only when the VLAN 1 header is enabled.*
VLAN 1 CFI	The first VLAN Canonical Format Indicator (CFI) *Note: Applies only when the VLAN 1 header is enabled.*
Enable VLAN 2 Header	Encapsulates all frames with two VLAN headers (as in *Q in Q*) VLAN1 must be enabled to use two VLAN headers. Note: If frames with more than three VLAN tags are received by the destination NID, these frames will be discarded and frame losses will be recorded.
VLAN 2 ID	The second VLAN ID. When enabled, all test frames are encapsulated with the second specified VLAN ID (inner VLAN). *Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 Ethernet Type	*Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 Priority	The second VLAN priority bits *Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 CFI	The second VLAN Canonical Format Indicator (CFI) *Note: Applies only when the VLAN 2 header is enabled.*
Flow Name	The name assigned to the flow. For reference in the **Results** section.
Traffic Type	The type of traffic may be one of the following: • **Constant**: To send frames at a specific bit rate (kbps). You need to specify the **Bit rate**. • **Burst**: To send a predefined number of frames at every period. You must specify the **Packets per Burst**. For the **Constant** traffic type, specify the bit rate (expressed in

Parameter	Description
	kbps). Supported values are: • **0 to < 12.5 Mbps**: Steps of 0.125 Mbps • **> 13 Mbps to 1 Gbps**: Steps of 1 Mbps For **Burst** traffic type, specify the number of frames to send per period (**Packets per Burst**) as well as the period, expressed in milliseconds, between the beginning of two successive bursts of frames (**Inter-Burst Gap**). You must select a **Bit Rate** that does not exceed the capacity of the outgoing port used for that test. Failure to do so will result in inaccurate results.
Size Type	Frame sizes may be **Fixed** or **Random**: • For a **Fixed** frame, specify the packet **Size**. • For **Random** frame sizes only, specify the **Minimum** and the **Maximum** values. The size of test frames will vary randomly between the minimum and maximum values you indicate. Acceptable values range from *64 bytes* to *10240 bytes*. *Note: You may need to modify your port MTU sizes in order to accommodate your selection.*
Duration Type	Duration type may be one of the following: • **Seconds**: Stops after a specified number of seconds • **Packets**: Stops after sending a specified number of packets. Value must be greater than or equal to *8* packets. Maximum of *4000000000* packets.

10.1.2 Starting the Traffic Generator and Viewing Test Results

▶ To view a summary of the traffic generator results

1. Access the page **SAT ▶ RFC-2544 ▶ Generator ▶ Results**.

   When you first enter this page, the results of the last test performed are displayed.

2. To start a new test, click **Start**.

   You can stop the test manually at any time by clicking **Stop**.

3. Click **details** of the first or second flow to view the detailed results for this flow.

For more information on these results, refer to the following table.

RFC-2544 Generator Results (SAT ▶ RFC-2544 ▶ Generator ▶ Results)

Parameter	Description
Flow Name	The name assigned to a flow
Transmit Statistics	
Transmitted Packets	Total packets transmitted by this flow for this test
Transmitted Bytes	Total bytes transmitted by this flow for this test
L1 Rate	The transmitting bit rate of Layer-1 traffic, expressed in Mbps
L2 Rate	The transmitting bit rate of Layer-2 traffic, expressed in Mbps
State Flow State	The flow's current state may be one of the following: • **Waiting**: Waiting to be started by the tester • **Failed**: The flow was deleted before the test was started • **Running**: The flow is currently running • **Stopped**: The tester stopped the flow before it completed • **Completed**: The flow reached its duration limit
Working Rate	The flow's working rate may be one of the following: • Layer-1 • Layer-2
Receive Statistics	
Received Packets	The total packets received by the generator's analysis component for this test, after being looped back by the peer device
Received Bytes	The total bytes received by this generator (analysis component) for this test
L1 Rate	The receiving bit rate of Layer-1 traffic, expressed in Mbps
L2 Rate	The receiving bit rate of Layer-2 traffic, expressed in Mbps
OOO or Duplicates	The out-of-order or duplicate frames received by this generator (analysis component)
Number of Gaps	The number of gaps contained in the numbered sequence. Each frame contains a sequence number and a timestamp to identify

Parameter	Description
	the gap.
Maximum Gap	Maximum size, expressed in frames, of the received gaps
Two-Way Delay	
Instantaneous	The two-way instantaneous delay, expressed in microseconds The delay is measured for each frame from the generator to the loopback device and back to the generator.
Average Average Delay	The average two-way packet delay, expressed in microseconds. The delay is measured for each packet from the generator to the loopback device and back to the generator (analysis).
Minimum	The minimum two-way delay, expressed in microseconds
Maximum	The maximum two-way delay, expressed in microseconds
Two-Way Delay Variation	
Instantaneous	The two-way instantaneous delay variation value, expressed in microseconds The delay variation is measured for each set of two consecutive packets from the generator to the loopback device and back to the generator.
Average Average DV	The average two-way delay variation, expressed in microseconds
Minimum	The minimum two-way delay variation, expressed in microseconds
Maximum	The maximum two-way delay variation, expressed in microseconds
Test Times	
Test Started At	The time when the test was started
Test Stopped At	The time when the test was completed or halted

10.1.3 Setting Up a Test Suite

You can run a test suite to determine whether a network section or a specific device conforms to a Service Level Agreement (SLA) or an Ethernet standard.

When configuring a test suite, you have the choice of enabling one or more of the following tests:

- Throughput
- Frame loss
- Delay
- Back-to-back

You must also set information pertaining to the remote peer (**Peer settings**) and the test frame contents. Various parameters are configurable, depending on the type of test traffic.

Refer to the table at the end of this procedure for more information on the different tests and settings.

▶ To set up a test suite

1. Access the page **SAT ▶ RFC-2544 ▶ Testsuite ▶ Configuration**.

   A summary of all test suites that have been set up is displayed.

2. Click the **Add** button to add a new test suite or click the **Name** of an existing test suite to edit its settings.

3. Select the different tests to run, complete their corresponding settings and other required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

RFC-2544 Test Suite Configuration (SAT ▶ RFC-2544 ▶ Testsuite ▶ Configuration)

Parameter	Description
Name Suite Name	The name of the test suite A maximum of 1 test suite can be created.
Description Suite Description	The description configured to identify the test suite and its characteristics
Jumbo Frame Size	The size, expressed in bytes, of the user-defined jumbo frame that will be used, if selected for the tests Default: 2000 Maximum: 10240 Example range: 1518 to 10240 *Note: The size must be less than or equal to the port's MTU.*
Binary Duration	The duration, expressed in seconds, of each trial completed during the binary search for the maximum throughput Default: 2 seconds Range: 1 to 10 seconds

Parameter	Description
Outgoing Port	The port from which to send the flow(s)
Enable Strict Failure	Select this box to enable failure on Out Of Order (OOO) or duplicate frames/packets. Out of Order frames/packets are frames/packets that are received in a different order than they were sent in. When strict failure is enabled, OOO or duplicate frames/packets will cause a test to fail, even if all frames/packets were received. When strict failure is disabled, the SkyLIGHT VCX Controller tolerates OOO and duplicate frames/packets. If all frames/packets were received, the test is marked as passed.
Enable Verbose Report	Select this box to have all tests (including any tests that failed) and executed steps appear in the test report.
Test to Run	
Enable Throughput	Select this box to enable the throughput test. The throughput test begins by determining the maximum rate at which the test settings yield no lost frames. For example, to measure the quality of a wire-speed GigE circuit, enter a **Minimum Rate** of *800 Mbps*, a **Maximum Rate** of *1000 Mbps*, a **Step Size** of *10 Mbps* and a **Binary Duration** of *2 seconds*. The VCX Controller then performs a binary search between 800 Mbps and 1000 Mbps for 2 seconds using 10 Mbps increments in order to determine the highest rate at which the test can be performed without failing. Once the maximum rate is determined, the throughput test starts executing the actual test, which involves sending frames according to selected *Frame Size* settings for the duration specified by the *Trial Duration*.
Enable Delay	Select this box to enable the delay and delay variation test. Once a wire-speed rate with no frame loss has been defined by the throughput test, the delay and delay variation test measures the latency and jitter at that specific rate. Ensure that you have entered all required parameters in the throughput settings, since some of these parameters are required by the delay and delay variation test.
Enable Frame Loss	Select this box to enable the frame loss test. The frame loss test verifies that no frames are lost when the current test settings are used. The VCX Controller starts at the maximum rate defined in the throughput settings section, then

Parameter	Description
	steps down by the value entered in the *Step Size* parameter of the *Frame Loss* settings. Two consecutive rates must have no frame loss in order to successfully pass this test. For example, if the Device Under Test (DUT) is able to perform full wire-speed at GigE, the test runs at 1000 Mbps and 980 Mbps (for a Step Size of 20 Mbps). Both tests must yield no frame loss in order to be successful, otherwise a lower rate will be tested. Ensure that you have entered all required parameters in the throughput settings section, since some of these parameters also apply to the frame loss test.
Enable Back-to-Back	Select this box to enable the back-to-back test. The back-to-back test performs a burst according to the test settings. For this test to be successful, the DUT must not lose any frames after a burst. A two-second pause is inserted after each burst. Ensure that you have entered all required parameters in the throughput settings, since some of these parameters are required by the back-to-back test.
Peer Settings	
Type	The type of test traffic may be one of the following: • **Layer-2**: Y.1731 LBM frames • **Layer-3**: UDP segments to perform a test across a multi-layered network
MAC Destination	The peer MAC address. Applies to Layer-2 and Layer-3 generic traffic only. *Note: Layer-3 generic traffic is available for the RFC-2544 traffic generator and test suite.*
Y.1731 MEG Level	The Maintenance Entity Group level Range: 0–7 *Note: Applies to Layer-2 traffic only. For details, refer to ITU-T Y.1731.*
Destination IP Address	The IP address of the remote unit interface. Applies to Layer-3 traffic only.
DSCP	The DiffServ Code Point to set in the generated packets. Applies to Layer-3 traffic only.

Parameter	Description
Source Port	The source UDP port number used to generate the UDP segment *Note: Applies to Layer-3 traffic only.*
Destination Port	The destination UDP port number that is used to generate the UDP segment *Note: Applies to Layer-3 traffic only.* *Note: You cannot set the destination port value to 8793, since this is Accedian's proprietary port number.* A port cannot be defined as the UDP port here if it is already being used for any of the following features: • Layer-3 RFC-2544 Generator • Layer-3 RFC-2544 Test Suite
TTL	This encapsulates all frames with one VLAN header. Note: If frames with more than three VLAN tags are received by the destination NID, these frames will be discarded and frame losses will be recorded.
Enable VLAN 1 Header	This encapsulates all frames with one VLAN header. Note: If frames with more than three VLAN tags are received by the destination NID, these frames will be discarded and frame losses will be recorded.
VLAN 1 ID	The first VLAN ID When enabled, all test frames are encapsulated with the specified VLAN ID.
VLAN 1 Ethernet Type	The first VLAN Ethernet type The available options are: • S-VLAN • T-VLAN • C-VLAN
VLAN 1 Priority	The first VLAN priority bits *Note: Applies only when the VLAN 1 header is enabled.*
VLAN 1 CFI	The first VLAN Canonical Format Indicator (CFI) *Note: Applies only when the VLAN 1 header is enabled.*
Enable VLAN 2	Encapsulates all frames with two VLAN headers (as in *Q in Q*)

Parameter	Description
Header	VLAN1 must be enabled to use two VLAN headers. Note: If frames with more than three VLAN tags are received by the destination NID, these frames will be discarded and frame losses will be recorded.
VLAN 2 ID	The second VLAN ID. When enabled, all test frames are encapsulated with the second specified VLAN ID (inner VLAN). *Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 Ethernet Type	*Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 Priority	The second VLAN priority bits *Note: Applies only when the VLAN 2 header is enabled.*
VLAN 2 CFI	The second VLAN Canonical Format Indicator (CFI) *Note: Applies only when the VLAN 2 header is enabled.*
Throughput Settings	
Trial Duration	The period of time over which the throughput test will run Range: 1 to 1800 seconds Default: 60 seconds
Maximum Rate	The upper bound of the rates for which to search, expressed in Mbps Range: 1 to 1000 Mbps (1 Gbps). In steps of 0.125 Mbps for rates from 0 to 12.5 Mbps, and in steps of 1 Mbps for rates greater than or equal to 13 Mbps. You must select a **Maximum Rate** that does not exceed the capacity of the outgoing port being used for the test suite. Failure to do so may produce inaccurate results. *Note: The actual transmission rate (TX rate) used during the throughput test will not necessarily match the value of the Maximum Rate parameter, since the transmission rate depends on the results obtained from the binary search algorithm.* This parameter also applies to the delay and delay variation test, as well as to the frame loss test.
Minimum Rate	The lower bound of rates for which to search, expressed in Mbps Range: 1 to 1000 Mbps (1 Gbps). In steps of 0.125 Mbps for rates from 0 to 12.5 Mbps, and in steps of 1 Mbps for rates greater than or equal to 13 Mbps.

Parameter	Description
	You must select a **Minimum Rate** that does not exceed the capacity of the outgoing port being used for the test suite. Failure to do so may produce inaccurate results. This parameter also applies to the delay and delay variation test, as well as to the frame loss test.
Step Size	The granularity of the range, expressed in Mbps Range: A value greater than zero to the maximum rate
Use Fine Stepping	Select this box to enable fine stepping in the case of low bandwidth testing (below 12 Mbps). When fine stepping is enabled, the configured **Step Size** is ignored. The step size used for the range is *125 kbps*. This parameter also applies to the delay and delay variation test, as well as to the frame loss test.
Frame Loss	The acceptable difference between measured frame losses (n x 0.1%). For example, a setting of **1** would mean a *0.1%* frame loss would be acceptable and not considered as a frame loss by the test. Default: 0, which means a target of no frame loss is tolerated when defining full throughput, i.e. losing a single frame will cause the test to fail
Frame Size Settings	Select the frame sizes to include in the test. By default, the Jumbo frame size is not selected because it is not a frame size defined by the RFC-2544 standard. *Note: The frame size you select must be smaller than the port's MTU. Selecting a higher frame size will prevent you from running the test.*
Delay and Delay Variation Settings	
Trial Duration	The period of time over which the test is run Range: 1 to 1800 seconds Default: 120 seconds The delay and delay variation test uses also the *Maximum Rate*, *Minimum Rate* and *Fine Stepping* values set in the *Throughput Settings*.
Frame Loss	The acceptable difference between measured frame losses (n x 0.1%). For example, a value of **1** would mean a *0.1%* frame loss would be acceptable and considered as no frame loss by the test.

Parameter	Description
	Default: 0, which means a target of no frame loss is tolerated when defining full throughput, i.e. losing a single frame will cause the test to fail
Frame Size Settings	Select the frame sizes to include in the test. By default, the Jumbo frame size is not selected because it is not a frame size defined by the RFC-2544 standard. *Note: The frame size you select must be smaller than the port's MTU. Selecting a higher frame size will prevent you from running the test.*
Frame Loss Settings	
Trial Duration	The period of time over which the test will run Range: 1 to 1800 seconds Default: 60 seconds The frame loss test also uses the *Maximum Rate*, *Minimum Rate* and *Fine Stepping* values set in the *Throughput Settings* section.
Step Size	The granularity of the range, expressed in Mbps
Frame Size Settings	Select the frame sizes to include in the test. By default, the Jumbo frame size is not selected because it is not a frame size defined by the RFC-2544 standard. *Note: The frame size you select must be smaller than the port's MTU. Selecting a higher frame size will prevent you from running the test.*
Back-to-Back Settings	
Trial Duration	The period of time over which the test is run Range: 1 to 10000 milliseconds Default: 2000 milliseconds
Repeat	The number of bursts to perform for each frame/packet size. A two-second pause is inserted after each burst. Default: 50 bursts Range: to 100 bursts
Frame Size Settings	Select the frame sizes to include in the test. By default, the Jumbo frame size is not selected because it is not a frame size defined by the RFC-2544 standard. *Note: The frame size you select must be smaller than the port's*

Parameter	Description
	MTU. Selecting a higher frame size will prevent you from running the test.

10.1.4 Running a Test Suite and Viewing Test Reports

Once you have set up a test suite, you can run it and view its report. Since each test is association with one test report, you have to configure a new report each time you want to run a new test. You can run a specific test suite many times as long as you configure a new report.

▶ To run a test suite

1. Access the page **SAT ▶ RFC-2544 ▶ Testsuite ▶ Reports**.

   A summary of all test suite reports is displayed. For more information on specific parameters, refer to the table at the end of this procedure.

2. Click the **Start New Testsuite** button to configure a new report.

3. Complete the required fields, then click **Run**.

For more information on specific parameters, refer to the following table.

RFC-2544 Test Suite Reports (SAT ▶ RFC-2544 ▶ Testsuite ▶ Reports)

Parameter	Description
File Name	The name assigned to the report A maximum of 2 test reports can be created.
Status	The report's current status is listed for all tests that have been created. Possible values are: • **Failed**: An error occurred during the test suite execution. • **Running**: The test suite is currently running. • **Stopped**: A user stopped the test suite during its execution. • **Completed**: The Test suite has completed.
Description	A concise description used to help identify the report
Technician Name	The name of the individual who executed the test suite
Testsuite Configuration	Select the test suite you want to run for this report.
Special Note	Any additional report-related details that were not included in the previous field

▶ To view, save or delete a test suite report

1. Access the page **SAT ▶ RFC-2544 ▶ Testsuite ▶ Report**.

   A summary of all test suite reports is displayed. For more information on specific parameters, refer to the table "RFC-2544 Test Suite Reports (SAT ▶ RFC-2544 ▶ Testsuite ▶ Reports)" on page 143.

2. Click the **Name** of an existing test suite report to view its report file or to perform other actions.

   *Note: You can click **Stop** to stop a test while it is running. You can then click either **Save** to save it on the management station as a text file or **Delete** to delete it.*

10.2 Setting Up SAT Reporting

You can set up the SkyLIGHT VCX Controller to enable the transfer of SAT test reports to a server. Once enabled, test reports are automatically transferred to the server each time a test is completed.

Test reports are available for RFC-2544 and Y.1564. All reports are available in text or XML format.

▶ To set up SAT reporting

1. Access the page **SAT ▶ Reporting**.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

SAT Reporting (SAT ▶ Reporting)

Parameter	Description
RFC-2544 Settings	
Enable Reporting	Enables or disables the transfer of RFC-2544 reports to the specified server.
Enable TXT File Transfer	Enables or disables the transfer of RFC-2544 reports in text format to the specified server.
Enable XML File Transfer	Enables or disables the transfer of RFC-2544 reports in XML format to the specified server.
File Server Configuration	
Server URL	The full URL of the server to which to send test reports **Examples**: ftp://username:password@domain.com sftp://username@192.168.10.10 tftp://192.168.1.5 scp://username@192.168.10.10:/target_directory
SCP Password	Enter the password required for SCP and SFTP transfers.

11 Managing Alarms and System Messages

This chapter describes functions related to alarms and system messages; it contains the following sections:

11.1 Managing Alarms

The SkyLIGHT VCX Controller provides alarm functions to monitor and report on the status of the unit, of the traffic performance and of other components.

11.1.1 Setting General Alarms

▶ **To set up general alarms**

1. Access the page **System ▶ Alarm ▶ General**.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Alarm Settings (System ▶ Alarm ▶ General)

Parameter	Description
Notification	
Enable LED Reporting	Enables the reporting of alarms by activating the LED on the VCX Controllerthat is appropriate and that corresponds to the severity, e.g. minor, major or critical
Enable Syslog Reporting	Enables the reporting of alarms by creating entries in the syslog
Enable SNMP Reporting	Enables the reporting of alarms via SNMP traps from Accedian's private MIB

11.1.2 Customizing Alarms

▶ **To customize an alarm**

1. Access the page **System ▶ Alarm ▶ Configuration**.

   The settings for all alarms are displayed. For more information on specific parameters, refer to the table at the end of this procedure.
2. Click the **Number** of the alarm that you want to edit.
3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Alarm Configuration (System ▶ Alarm ▶ Configuration)

Parameter	Description
Number	The unique number that identifies this alarm. This number is assigned by the SkyLIGHT VCX Controller and cannot be modified. This alarm number is composed of three fields, the module number, the instance number and the error number. The format is AA.BBBB.CC, where the parameters are as follows: • **AA**: Module number (1-99) • **BBBB**: Instance number (0001-9999). • **CC**: Error number (01-99) A module number is assigned for each alarm in the system and may be one of the following: • **1**: Port module for link down and other related alarms • **2**: *Unassigned* • **3**: *Unassigned* • **4**: *Unassigned* • **5**: *Unassigned* • **6**: *Unassigned* • **7**: System modules, such as NTP and other agents • **8**: *Unassigned* • **9**: *Unassigned* • **10**: Loss of connectivity with a remote device • **11**: *Unassigned*
Enable	Indicates whether the alarm is enabled (true) or disabled (false). If enabled, alarms are reported.
Severity	The severity of the alarm. If LED reporting is enabled on the **Alarm ▶ General** page, the Minor, Major and Critical alarms are indicated on the VCX Controller's front panel LEDs. • **Informational**: No effect on service. Provides status information.

Parameter	Description
	• **Minor**: An error condition has occurred that does not seriously affect system functionality. • **Major**: A serious degradation of service or hardware malfunction has occurred which requires immediate attention to restore system functionality. • **Critical**: A service-affecting condition has occurred that requires immediate corrective action.
Service Affecting	Alarms may be displayed as **service affecting** or **non-service affecting**.
Description	Textual description of the alarm. The description is displayed in the **Show ▸ Alarm** page.

11.1.3 Viewing Alarms

▸ To view the status of an alarm

1. Access the page **Show ▸ Alarm**.

   The alarm status is displayed.

For more information on specific parameters, refer to the following table.

Alarm Status (Show ▸ Alarm)

Parameter	Description
Status	The status LED is ON if the alarm is enabled and has been triggered
Number	The unique number identifying this alarm This number is assigned by the SkyLIGHT VCX Controller and cannot be modified. This alarm number is composed of three fields, the module number, the instance number and the error number. The format is AA.BBBB.CC, where the parameters are as follows: • **AA**: Module number (1-99) • **BBBB**: Instance number (0001-9999) • **CC**: Error number (01-99) A module number is assigned for each alarm in the system and may be one of the following:

Parameter	Description
	• **1**: Port module for link down and other related alarms • **2**: *Unassigned* • **3**: *Unassigned* • **4**: SOAM module for Continuity Check, Delay, Packet Loss and other related alarms • **5**: *Unassigned* • **6**: *Unassigned* • **7**: System modules, such as NTP and other agents • **8**: *Unassigned* • **9**: *Unassigned* • **10**: Loss of connectivity with a remote device • **11**: *Unassigned*
Presence	Indicates whether the alarm is currently present (**true**) or not (**false**)
Severity	The severity of the alarm. Possible values may be one of the following: • **Warning**: A non-service-affecting condition has occurred that required attention. • **Minor**: An error condition has occurred that does not seriously affect system functionality. • **Major**: A serious degradation of service or hardware malfunction has occurred which requires immediate attention to restore system functionality. • **Critical**: A service-affecting condition has occurred that requires immediate corrective action.
Service Affecting	Alarms may be displayed as one of the following: • **Service Affecting** (SA) • **Non-Service Affecting** (NSA)

Parameter	Description
Description	A textual description of the alarm
Message	This is displayed only when the alarm has changed status (the alarm was turned ON or OFF). The message explains why it was turned on or off, e.g. temperature was above the threshold.
Last Change	When the alarm changed status

Refer to the following table for a list of all alarms supported and their default description.

Supported Alarms: SkyLIGHT VCX Controller

Number	Default Description
Port module for link down and other related alarms In this section, BBBB = instance number (0001-9999).	
1.0001.01	link down on LOCAL-1 port
1.0002.01	link down on LOCAL-2 port
1.BBBB.06	Speed mismatch on device [device name]
SOAM module In this section, zzzz = CFM instance index.	
4.zzzz.03	Remote CCM on down MEP, MEPID <ID>, port <port name>, VID <ID>, level <#>
System modules, such as NTP	
7.0001.01	NTP client lost server communication

▶ To view the detailed status of an alarm

1. Access the page **Show ▶ Alarm**.
2. Click the alarm **Number** to view its detailed status.

For more information on specific parameters, refer to the table "Alarm Status (Show ▶ Alarm)" on page 150.

11.2 Managing Syslog Messages

The SkyLIGHT VCX Controller logs information related to system operations as Syslog Messages. You can view the syslog messages directly in the Web management interface or send the log to a remote location such as a workstation.

11.2.1 Defining Syslog Parameters

▶ To configure Syslog parameters

1. Access the page **System ▶ Agent ▶ Syslog**.

   A list of all syslog entries is displayed, with the most recent entry at the top.

   *Tip: You can update the log window with the most recent messages by clicking **Refresh**.*

2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Syslog Configuration (System ▶ Agent ▶ Syslog)

Parameter	Description
Device Facility	The device facility to log all messages using this user-defined facility instead of the default ones
Level Threshold	Logs all messages with a level greater than or equal to the selected one. For example, setting the priority threshold to **DEBUG** (lowest priority) causes all messages to be logged.
Remote Syslog Enable	Select this box to enable sending messages to a remote syslog server
Host	The IP address or domain name of the remote syslog server

11.2.2 Sending Syslog Messages to a Remote Location

You can configure the SkyLIGHT VCX Controller to send Syslog messages to a Syslog server in a remote location.

▶ **To send Syslog messages to a remote server**

1. Access the page **System ▶ Agent ▶ Syslog**.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the table "Syslog Configuration (System ▶ Agent ▶ Syslog)" above.

11.3 Managing History Files

You can manage the creation and transfer of *history files*, which are logs that contain statistics related to the services (e.g., FlowMETER) for which the history feature has been enabled.

You can also configure the SkyLIGHT VCX Controllerto transfer its history files to a server.

> *Note: The exported history CSV files may not all contain the identical range of period numbers, depending on when the given history metrics were collected. Enabling multiple categories of history metrics with many instances requires more time for processing than the length of the reporting period. Since the history files are processed sequentially, some exported files may consequently present different period numbers compared to others.*

11.3.1 Creating History Files

▶ To enable the creation of history files

1. Access the page **System ▶ Agent ▶ History**.
2. In the Local Configuration frame, select the **Enable History** box for each feature whose history you want to retain.

   > *Note: Disabling the history disables the filling; enabling the filing enables the history.*

3. In the Local Configuration frame, select the **Enable Filing** box for each feature for which you want to create history files, then enter the **Period** after which you want the data files to be collected for storage.
4. Click **Apply**.

For more information on specific parameters, refer to the following table.

History Files, Local Configuration (System ▶ Agent ▶ History)

Parameter	Description
Local Configuration	
Enable History	Select this box to allow the creation of history files, which are stored in RAM. You can access these files via the SNMP *get* command.
Enable Filing	Select this box to allow the history files to be stored locally in non-volatile memory (NVM). Storing these files protects against losing history statistics in the event of a power failure or system restart.

Parameter	Description
	If this box is not selected, the local history files for this feature are removed. Use the Scheduling and File Transfer Configuration frame on this page to have the history files *pushed* to a server. History files can be stored locally for the following features: • FlowMETER
Period (mins)	Indicate the frequency at which the history statistics will be collected, expressed in minutes. Acceptable values range from *1* and *60*.

11.3.2 Transferring History Files

▶ To enable the transfer of history files

1. Access the page **System ▶ Agent ▶ History**.
2. Ensure that filing is enabled for the appropriate history files, then click **Apply** in the Local Configuration frame. See "Creating History Files" on page 155.
3. Customize when the history files will be scheduled by completing the fields in the Scheduling section of the Scheduling and File Transfer Configuration frame.
4. Provide the URL where the file transfer server is located and the SCP password in the File Transfer section of the Scheduling and File Transfer Configuration frame.
5. Choose a Period Mode and any optional fields in the File Options section, then click **Apply** in the Scheduling and File Transfer Configuration frame.

For more information on specific parameters, refer to the following table.

History Files, Scheduling and Files Transfers (System ▶ Agent ▶ History)

Parameter	Description
Scheduling and File Transfer Configuration	
Enable Scheduler	Select this box to have the SkyLIGHT VCX Controller transfer its history buckets' report files to a server, whose details are configured below. *Note: Report files will only be generated for the services whose Enable Filing box in the Local Configuration frame is enabled.*
Scheduled Hours	Indicate when to transfer the history buckets by making a selection from the list. Press the CTRL key to select more than one item. *Note: Finer granularity is possible using the **Hourly Minutes** or **Periodic Minutes** field, in combination with the **Schedule Offset** field.*
Scheduling Mode	Make a selection from the drop-down list to indicate the type of interval to define for history bucket file transfers: • **Hourly**: Allows you to select file transfers on the quarter-hours • **Periodic**: Allows you to choose from a wider range of interval values for file transfers Both interval types are described below.

Parameter	Description
Hourly Minutes	Use this feature to set the scheduling to trigger every 15 minutes, either right on the hour or at the 00:15, 00:30 and 00:45 marks. Any value combination is valid, provided at least one box is selected and *Hourly* is selected in the drop-down list above the boxes.
Periodic Minutes	Make a selection from the drop-down list to set the scheduling trigger interval value. **Example**: • If a unit has 3:00 and 15:00 selected in the *Scheduled Hours* list, plus 20 selected in the *Periodic Minutes* drop-down list, reports are generated at 3:00, 3:20, 3:40, 15:00, 15:20 and 15:40. Any value is valid, provided that *Periodic* is selected in the drop-down list above the boxes.
Schedule Offset	Use this field to offset the scheduling by the number of minutes you specify. • **Hourly**: Acceptable values range from *0* to *14* • **Periodic**: Acceptable values range from *0* to (*Periodic Minutes - 1*) This field enables you to generate reports as often as four times per hour, at any minute thereof. When a large number of units are set to generate report files, the offset feature can be used to spread the load on the network and servers. **Examples**: • If a unit has 3:00 and 15:00 selected in the *Scheduled Hours* list, plus 00:00 and 00:30 selected in the *Hourly Minutes* with a *Schedule Offset* of 0 minutes, reports are generated at 3:00, 3:30, 15:00 and 15:30. • If a unit has all hours selected in the *Scheduled Hours*, plus 00:15 and 00:45 in the *Hourly Minutes* with a *Schedule Offset* of 4 minutes, reports are generated at the 19th and 49th minute of every hour. • If a unit has 3:00 selected in the *Scheduled Hours* list, plus 10 selected in the *Periodic Minutes* with a *Schedule Offset* of 2 minutes, reports are generated at 3:02, 3:12, 3:22, 3:32, 3:42 and 3:52.

Parameter	Description
Random Offset	Enter a value in this field to generate a random offset, expressed in seconds, ranging between 0 and the specified value. This random offset is added to the *Schedule Offset*. Adding a random offset allows multiple units set to generate reports at the same time for the same destination to be randomly offset from one another, thus relieving the load created by several concurrent connections. *Note: The combined value of the schedule offset and random offset cannot exceed 15 minutes (900 seconds) in hourly mode or the value of Periodic Minutes when in periodic mode. If the sum of the schedule offset and random offset exceeds the specified limit, the random offset value is automatically adjusted to the highest possible value.*
File Transfer	
Server URL	Enter the full URL of the server to which the history bucket files will be sent once retrieved. **Examples**: http://domain.com ftp://username:password@domain.com sftp://username@192.168.10.10 tftp://192.168.1.5 scp://username@192.168.10.10:/target_directory
SCP Password	Enter the password required for SCP and SFTP transfers.
File Options	
Period Mode	Indicate which periods to include in the reports by selecting one of the available options: • **All Available Periods**: All the periods that are available on the VCX Controller are used to generate the reports, up to a fixed maximum number of periods. • **New Periods Since Last File Transfer**: All the periods that have been generated since the previous report. If **Include Periods From Previous Incomplete Transfers** is selected, the periods from a previous report that could not be properly generated or sent to the server are also included. • **Fixed Number of Periods**: All the periods available, up to the maximum number of periods specified in **Number of Periods**

Parameter	Description
	Note: Enabling "All Available Periods" mode when more than 1000 policies or 1000 bandwidth regulators have been activated can lead to prolonged, significant CPU usage. The same behavior may be observed when the remote server is unreachable for an extended period of time.
Options	You can exercise greater control over how the reports are generated: • **Include Periods From Previous Incomplete Transfers**: When selected, any periods contained in a report that could not be properly generated or sent to the server are also included in the current report. If not selected, only the periods since the previous report are included in the current report.

11.4 Managing the SNMP Agent

You can configure an SNMP agent so that it provides an interface to an SNMP-based management system (for *get* and *set* commands). The SNMP agent also allows the SkyLIGHT VCX Controller to send SNMP traps to a receiver. The receiver is usually used to monitor the conditions of many units.

11.4.1 Enabling the SNMP Agent

▶ To enable the SNMP agent

1. Access the page **System ▶ Agent ▶ SNMP**.
2. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

SNMP Agent (System ▶ Agent ▶ SNMP)

Parameter	Description
Enable Agent	Enables the VCX Controller's SNMP agent
Use Host Name as System Name	Uses host's name as system-name
SNMP System Name	The name to identify the VCX Controller. By convention, this is the node's fully-qualified domain name.
Contact Information	Contact information for the VCX Controller (typically an email address)
System Location	Physical location of the VCX Controller
Agent UDP Port	UDP port that the SNMP agent uses for all IPv4 interfaces *Note: Changing this value restarts the SNMP agent.*
Read-Only Community	The community string to control read-only access to the VCX Controller
Read-Write Community	The community string to control read/write access to the VCX Controller
Enable Authentication Trap Generation	Enables the VCX Controller to generate a trap when authentication to the agent fails
Enable Link Trap Generation	Enables trap generation when link status changes Map to the generic traps *2* (1.3.6.1.6.3.1.1.5.3 linkDown) and *3* (1.3.6.1.6.3.1.1.5.4 linkUp).

11.4.2 Setting Up the SNMP Trap Receivers

You can configure the SkyLIGHT VCX Controller to send SNMP traps to different notification receivers. The notification receiver is usually used to monitor conditions of many units.

The VCX Controller can be configured to send SNMP v1 traps to one or two receivers, and to send SNMP SMTPv2c traps to up to ten receivers.

Using the **Auto** trap receiver, you can also configure the VCX Controller to send SNMP traps (v1 or v2c) to other compatible notification receivers. With the **Auto** trap receiver, the IP address of the compatible notification receiver is automatically updated when the receiver connects to the VCX Controller and sends the appropriate CLI commands. Refer to the *CLI Command Manual* for information on the CLI command.

▶ To configure the SNMP trap receiver information

1. Access the page **System ▶ Agent ▶ Traps**.

   A listing of all current SNMP Trap receiver information is displayed.

2. Click the **ID** of the trap receiver you want to edit.

3. Complete the required fields, then click **Apply**.

For more information on specific parameters, refer to the following table.

Trap Receivers (System ▶ Agent ▶ Traps)

Parameter	Description
Type	The type of SNMP Trap Receiver may be either **SNMPv1** or **SNMPv2c**.
ID	ID number of the trap receiver *Note: The Auto trap receiver is configurable via the CLI only.*
State	Enable this box to have the VCX Controller send SNMPv1 or SNMPv2c traps to a specified notification receiver.
Enable Trap	Enables the VCX Controller to send SNMPv1 or SNMPv2c traps to a specified notification receiver
Notification Receiver Host Name	The IP address or host name of the device that receives SNMP traps and/or notifications The VCX Controller sends a **Cold Start** trap when starting up.
Community String Community	The community string required to send traps to the notification receiver
Host UDP Port	The UDP port used by the VCX Controller to send traps to the

Parameter	Description
UDP Port	notification receiver The well-known SNMP trap port *162* is used by default.