Extreme SLX-OS RESTCONF Guide, 20.6.3

Supporting ExtremeRouting and ExtremeSwitching
SLX 9740, SLX 9640, SLX 9540, SLX 9250, SLX 9150,
Extreme 8820, Extreme 8720, and Extreme 8520

9038955-00 Rev AA
November 2024

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/about-extreme-networks/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

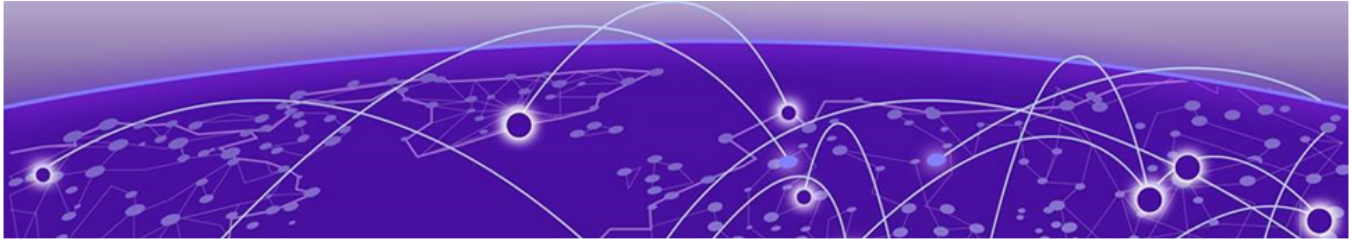


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as Extreme Networks switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

Current Product Documentation
Release Notes
Hardware and Software Compatibility for Extreme Networks products
Extreme Optics Compatibility
Other Resources such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the Open Source Declaration page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the Extreme Networks Training page.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

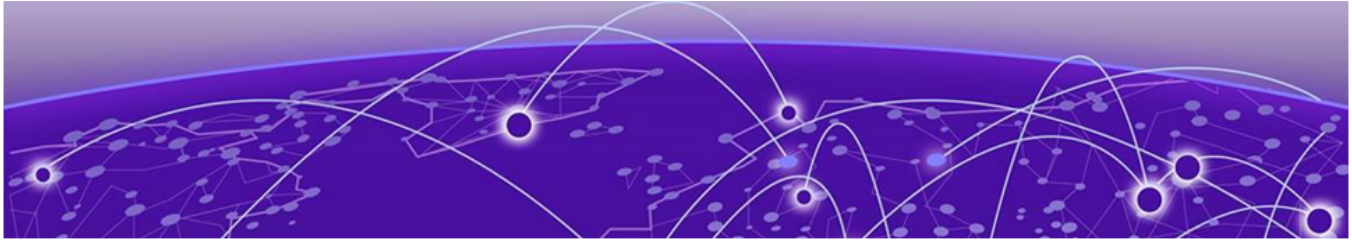
Send Feedback

The User Enablement team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at documentation@extremenetworks.com.

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



About This Document

What's New in this Document

This document is released with the SLX-OS 20.6.3 software release. The following changes were made to this document for this release.

Table 4: Summary of changes

Feature	Description	Described in
management-security	Added new RESTCONF.	management-security on page 62
username	Updated to reflect that the command can now configure the **root** account.	username on page 105

For additional information, refer to the *Extreme SLX-OS Release Notes* for this version.

Supported Hardware

For instances in which a topic or part of a topic applies to some devices but not to others, the topic specifically identifies the devices.

SLX-OS 20.6.3 supports the following hardware platforms.

- Extreme 8820
- Extreme 8720
- Extreme 8520
- ExtremeSwitching SLX 9540
- ExtremeSwitching SLX 9250
- ExtremeSwitching SLX 9150

- ExtremeRouting SLX 9740
- ExtremeRouting SLX 9640

Note

All configurations and software features that are applicable to SLX 9150 and SLX 9250 devices are also applicable for the Extreme 8520 and Extreme 8720 devices respectively.

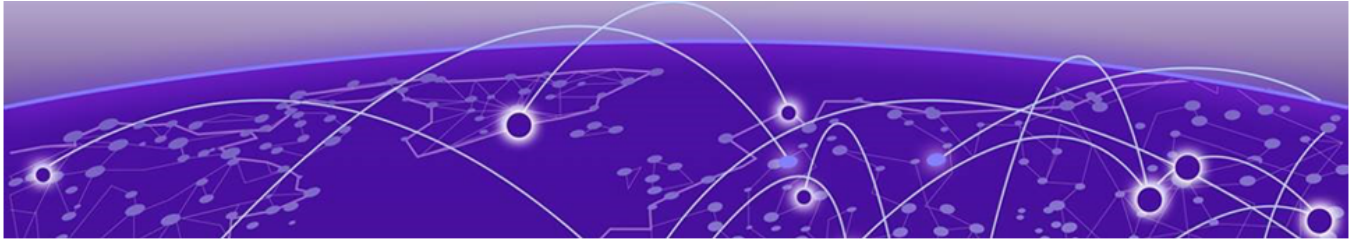
All configurations and software features that are applicable to SLX 9740 devices are also applicable for the Extreme 8820 devices.

The "Measured Boot with Remote Attestation" feature is only applicable to the Extreme 8520, Extreme 8720, and Extreme 8820 devices. It is not supported on the SLX 9150 and SLX 9250 devices.

Note

Although many software and hardware configurations are tested and supported for this release, documenting all possible configurations and scenarios is beyond this document's scope.

For information about other releases, see the documentation for those releases.



Extreme SLX-OS RESTCONF

About RESTCONF

Based on RFC8040, RESTCONF defines a Hypertext Transfer Protocol (HTTP)-based protocol using Transport Layer Security (TLS) protocol for configuring data defined in a YANG model by using the datastore concepts defined in NETCONF. RESTCONF uses HTTP methods to provide CRUD operations on a conceptual datastore containing YANG-defined data, which is compatible with a server that implements NETCONF data stores.

SLX RESTCONF supports all the operations such as GET, HEAD, OPTIONS, POST, PUT, PATCH, and DELETE method to retrieve the details about the configuration data, YANG schema, and the operational-state data.

The following feature items of the RESTCONF support are different from the existing REST API support.

- RESTCONF uses the Hyper Text Transfer Protocol Secure (HTTPS) protocol .
- The *tailf:cli-drop-node-name* of the container node defined in the YANG is present in both the URI and the payload, because the abstraction of the RESTCONF protocol mandates that datastore must be same. The content of the abstract copied from the RESTCONF protocol is mentioned below.

> This document describes an HTTP-based protocol that provides a programmatic interface for accessing data defined in YANG, using the datastores defined in NETCONF.

- The name of the YANG node is present in the URI and the payload instead of the *alt-name*.
- There is a key representation in the URI for the LIST element.
- There is the module namespace representation in the URI.
- There is the module namespace representation in the Payload.
- The **Resource-Depth** header is specified as the query parameter **depth** in the URI. It specifies the number of nested levels returned in a response for a GET method on API datastores. A "400 Bad Request" status-line will be returned if it used for other methods or resource types.
  - The first nest level will be the requested data node.
  - The value of the "depth" parameter will be either an integer between 1 and 65535, or the string "unbounded". The default **depth** value is unbounded.
  - For example, the below URL will retrieve all child resources of the interface, with the "depth" parameter set to the default value "unbounded".

    ```
    GET /restconf/data/brocade-interface:interface?depth=unbounded
    ```
- The **content** query parameter is used to differentiate between the configuration and the operational-state data.
- The *with-default* query parameter is used with the value **trim** or **report-all-tagged** to get the configuration data without default values.
- The Media Type mentioned in the **Accept** header has been changed.

Before you begin

Before you can use the Extreme SLX-OS RESTCONF, obtain a username and password for accessing SLX-OS through the RESTCONF. By default, RESTCONF is enabled on Extreme SLX-OS devices. You cannot disable it.

Logging in and out

You can log in to the device by entering the username and password or the session ID provided by the switch after authenticating the initial request from the client.

If the authentication is successful, the response header "Authentication-Token" is sent to the client. From then, client applications can use this token and send it to the server

for the authentication for further access to the server by using the same persistent connection. The client applications use this token to obtain further access to the server using the persistent connection.

The following is an example of an Authentication-token.

```
HTTP/1.1 201 Created
 Date: Wed, 02 Mar 2018 22:46:15 GMT
 Server: SLX-OS WWW
 Authentication-Token: TEM5Wk59XV5xRFxOdVtydF9kWDZwd2hHRGV6Q0B0NXk=
 Location: http://localhost/rest/config/running/router/mpls
 Cache-control: private, no-cache, must-revalidate, proxy-revalidate
 Content-Length: 0
 Content-Type: text/html

* Connection #0 to host 10.24.12.135 left intact
```

There is no expiry for the authentication token or the user session. There is expiry for the HTTP session only, which is 180 seconds. The client will timeout if the server does not respond within 180 seconds. This also applies to the Authentication-token expiry.

For single persistent connection, there must be only one token. When the same token is reused, you can have maximum number of 100 requests in a persistent connection.

To log out from the device, you must delete the session created using the DELETE operation. The URI for deleting a session is http:// host:port/rest/session/<session-id>.

Base URI

The Base URI for the RESTCONF API is: */restconf/*.

The base URI /restconf contains three child resources. The YANG tree representation is:

```
+--rw restconf
      +--rw data
      +--ro operations
      +--ro yang-library-version
```

Basic authentication to a REST endpoint

Verify and obtain the base URI of the RESTCONF API and then create the URI as shown in the below example.

```
curl -v -X GET -u admin:password https://10.20.192.65:80/restconf/

root@XMC:~/firmware/images$ curl -v -X GET -u admin:password http://10.20.192.66:80/rest
Note: Unnecessary use of -X or --request, GET is already inferred.
*   Trying 10.20.192.66...
* TCP_NODELAY set
* Connected to 10.20.192.66 (10.20.192.66) port 80 (#0)
* Server auth using Basic with user 'admin'
> GET /rest HTTP/1.1
> Host: 10.20.192.66
> Authorization: Basic YWRtaW46cGFzc3dvcmQ=
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: 2019-12-27 10:39:54
< Server: SLX-OS Wave WWW
```

```
< Authentication-Token: QDtEdkMzfHJKUEhZYGkyZE5sLz40fG5CfVNnWlJjRl8=
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Type: application/vnd.base.resource+xml
< Content-Length: 3548
<

<rest xmlns="http://brocade.com/ns/rest" xmlns:y="http://brocade.com/ns/rest" y:self="/
rest">

  <config y:self="/rest/config">
    <running y:self="/rest/config/running"/>
  </config>

  <operational-state y:self="/rest/operational-state"/>
  <operations y:self="/rest/operations">
    <get-maint-mode-status y:self="/rest/operations/get-maint-mode-status"/>
    <user-session-info y:self="/rest/operations/user-session-info"/>
    <get-arp y:self="/rest/operations/get-arp"/>
    <show-clock y:self="/rest/operations/show-clock"/>
    <get-contained-in-ID y:self="/rest/operations/get-contained-in-ID"/>
    <fwdl-status y:self="/rest/operations/fwdl-status"/>
    <activate-status y:self="/rest/operations/activate-status"/>
    <firmware-download y:self="/rest/operations/firmware-download"/>
    <firmware-commit y:self="/rest/operations/firmware-commit"/>
    <firmware-restore y:self="/rest/operations/firmware-restore"/>
    <firmware-download-sanity y:self="/rest/operations/firmware-download-sanity"/>
    <show-firmware-version y:self="/rest/operations/show-firmware-version"/>
    <reload y:self="/rest/operations/reload"/>
    <set-http-application-url y:self="/rest/operations/set-http-application-url"/>
    <get-vlan-brief y:self="/rest/operations/get-vlan-brief"/>
    <get-interface-switchport y:self="/rest/operations/get-interface-switchport"/>
    <get-ip-interface y:self="/rest/operations/get-ip-interface"/>
    <get-interface-detail y:self="/rest/operations/get-interface-detail"/>
    <get-media-detail y:self="/rest/operations/get-media-detail"/>
    <get-port-channel-detail y:self="/rest/operations/get-port-channel-detail"/>
    <get-portchannel-info-by-intf y:self="/rest/operations/get-portchannel-info-by-intf"/>
    <get-lldp-neighbor-detail y:self="/rest/operations/get-lldp-neighbor-detail"/>
    <get-mac-acl-for-intf y:self="/rest/operations/get-mac-acl-for-intf"/>
    <get-mac-address-table y:self="/rest/operations/get-mac-address-table"/>
    <get-netconf-client-capabilities y:self="/rest/operations/get-netconf-client-
capabilities"/>
    <show-ntp y:self="/rest/operations/show-ntp"/>
    <bna-config-cmd y:self="/rest/operations/bna-config-cmd"/>
    <bna-config-cmd-status y:self="/rest/operations/bna-config-cmd-status"/>
    <show-raslog y:self="/rest/operations/show-raslog"/>
    <show-support-save-status y:self="/rest/operations/show-support-save-status"/>
    <show-system-info y:self="/rest/operations/show-system-info"/>
    <get-system-uptime y:self="/rest/operations/get-system-uptime"/>
    <show-system-monitor y:self="/rest/operations/show-system-monitor"/>
    <clear-tm-voq-stat-ing-all-egr-all y:self="/rest/operations/clear-tm-voq-stat-ing-all-
egr-all"/>
    <clear-tm-voq-stat-ing-all-egr-ifname y:self="/rest/operations/clear-tm-voq-stat-ing-
all-egr-ifname"/>
    <clear-tm-voq-stat-slot-id-egr-all y:self="/rest/operations/clear-tm-voq-stat-slot-id-
egr-all"/>
    <clear-tm-voq-slot-id-egress-port-name y:self="/rest/operations/clear-tm-voq-slot-id-
egress-port-name"/>
    <get-tunnel-info y:self="/rest/operations/get-tunnel-info"/>
    <get-tunnel-statistics y:self="/rest/operations/get-tunnel-statistics"/>
    <get-last-config-update-time y:self="/rest/operations/get-last-config-update-time"/>
    <get-last-config-update-time-for-xpaths y:self="/rest/operations/get-last-config-
update-time-for-xpaths"/>
    <get-stp-brief-info y:self="/rest/operations/get-stp-brief-info"/>
    <get-stp-mst-detail y:self="/rest/operations/get-stp-mst-detail"/>
```

```
  </operations>

</rest>
* Connection #0 to host 10.20.192.66 left intact

from the rest reply user can derive the URI for any REST endpoint
curl -v -X GET -u admin:password http://10.20.192.65:80//rest/config/running -H "Accept:
application/
vnd.configuration.resource+xml"
```

Limitations

The REST Commands for **show-ha** and **show-slots** are not supported.

Data

The datastore resource is a collection of configuration data and state data nodes. This mandatory resource represents the combined configuration and state data resources that can be accessed by a client. If the datastore resource represented by the */restconf/data* subtree is retrieved, the datastore and its contents are returned by the server. The datastore is represented by a node named "data". All methods are supported on data.

YANG-library version

This leaf identifies the revision date of the *ietf-yang-library* YANG module supported by the server. Both GET and SET methods are supported.

Operations resource

An operation resource represents an RPC operation defined with the YANG "rpc" statement or a data-model-specific action defined with a YANG "action" statement. The statement is invoked using a POST method on the operation resource.

Use the GET Method on the /restconf/operations to check the list of RPCs it supports.

The following example uses the POST operation to retrieve the operation resource statement:

```
root@admin11:~# curl -v -k -X POST -H "Accept: application/yang-data+xml" -d "<show-
system-monitor></show-system-monitor>"
-u admin:password https://10.20.192.67:443/restconf/operations/show-system-monitor
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.20.192.67...
* Connected to 10.20.192.67 (10.20.192.67) port 443 (#0)
* found 148 certificates in /etc/ssl/certs/ca-certificates.crt
* found 614 certificates in /etc/ssl/certs
* ALPN, offering http/1.1
* SSL connection using TLS1.2 / ECDHE_RSA_AES_128_GCM_SHA256
*      server certificate verification SKIPPED
*      server certificate status verification SKIPPED
*      common name: 10.20.199.211 (does not match '10.20.192.67')
*      server certificate expiration date OK
*      server certificate activation date OK
*      certificate public key: RSA
*      certificate version: #3
```

```
*       subject: C=IN,ST=TN,L=CHN,O=HCL,OU=SQA,CN=10.20.199.211
*       start date: Wed, 26 Jun 2019 10:57:22 GMT
```

Transport protocol requirements

RESTCONF requires the following transport protocols.

- The RESTCONF server is supported over HTTPS without the TLS. To support data integrity and confidentiality, RESTCONF requires HTTPS.
- RESTCONF supports the "https" URI scheme, and SLX-OS uses the IANA assigned default port 443.
- The X.509v3 based certificate is used for establishing the connection between server and client.
- The X.509 certificate must be used by the client to verify the integrity of the server's TLS certificate. The RESTCONF client must check the identity of the server according to Section 6 of [RFC6125].
- The RESTCONF server must authenticate client access to any protected resource. If the RESTCONF client is not authenticated, the server must send an HTTP response with "401 Unauthorized". The error-tag value "access-denied" is used in this case.

The following is an HTTPS configuration on an SLX device.

```
on SLX:
crypto key label mykey rsa modulus 2048
crypto ca trustpoint myca
keypair mykey
end

crypto ca authenticate <trustpoint-name> cert-type <commoncert|https> directory <dir-
name> file <file-name>
host <host-name/ip> protocol <SCP|FTP> user <user-name>
crypto ca enroll myca common brocade country US directory /root/vishu host <server ip>
locality SJ organization Brocade
orgunit Eng protocol SCP state CA user root password pass

On Linux CA:
============
cd  <your directory>

openssl ca -policy policy_anything -extensions server_cert -out 10.25.164.147.pem -config
openssl.cnf
-infiles <slx mgmt ip>.csr

From the CA host, find out the certificate creation time.  The time on the switch must be
later than this time,
or the installation will not work:
date;
openssl x509 -noout -text -in <slx mgmt ip>.pem | grep 'Not Before'

On  SLX:
===========
To adjust the time on the switch, run the following command.  You might need to adjust
for the time zone:
clock set yyyy-mm-ddThh:mm:ss

crypto ca import myca certificate directory <your directory> host <server ip> protocol
SCP user root file <slx mgmt ip>.pem
password pass
```

```
copy running-config startup-config
show crypto key mypubkey
show crypto ca trustpoint
show crypto ca certificates
show running-config crypto key
show running-config crypto ca
```

URI

The uniform resource information (URI) identifies the resource. The resources are represented with URIs in the following format.

```
/restconf/<path>? <query>
```

- restconf: the entry point of the URI in the device, and the root of the API configured on the device is discovered by getting the "/.well-known/host-meta" resource.
- path: the target resource URI, which is used for identifying the resource being accessed by the HTTP operation.
- query: the query parameter lists with the form of "name=value" pairs. Most query parameters like (depth) are optional to implement by the server and optional to use by the client. Any reserved characters must be percent-encoded, according to RFC3986.

Operations

The HTTP methods are used for manipulating the resource defined in the YANG model for the CRUD operations. You must employ appropriate access control mechanisms to limit what operations can be allowed by a user.

POST Method

The POST method is sent by the client to create a data resource or invoke an operation resource. The server uses the target resource type to determine how to process the request. It is supported for all the resource types. Use the POST method to create the top-level configuration data resource or to create a child data resource. You can use the POST method to invoke RPC operation. The message-body or the payload in the POST method contain the resource to be created. When the creation is successful, "201 Created" status line is returned and there is no response message-body.

To create a top-level resource, use the following example.

```
curl -v -X POST -d "<mpls />" -u admin:password https://<> /restconf/data/brocade-
mpls:mpls-config/router
-H "Content-Type: application/yang-data+xml"
```

Response body

```
< HTTP/1.1 201 Created
< Date: Wed, 02 Nov 2016 22:46:15 GMT
< Server: SLX-OS WWW
< Authentication-Token: TEM5Wk59XV5xRFxOdVtydF9kWDZwd2hHRGV6Q0B0NXk=
< Location: http://localhost/rest/config/running/router/mpls
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Length: 0
< Content-Type: text/html
```

```
<
* Connection #0 to host 10.24.12.135 left intact
```

If the data resource already exists, the POST request fails and a "409 Conflict" status-line is returned. The error-tag value "resource-denied" is used in this case.

```
curl -v -X POST -H "Content-Type: application/yang-data+json" -d "{\"mpls\": {}}
-u admin:password https://<> /restconf/data/brocade-mpls:mpls-config/router -k
```

In case of a conflict, you receive the following response.

```
< HTTP/1.1 409 Conflict
< Date: Thu, 16 Feb 2017 20:21:37 GMT
< Server: SLX-OS WWW
< Authentication-Token: ZjlLUzswdkY9XkZbNUVoOmwzVFdoUkhtWF1Lc0NsWH0=
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Length: 62
< Content-Type: text/json

  {
  "error": {
    "-xmlns": "urn:ietf:params:xml:ns:yang:ietf-restconf",
    "error-type": "protocol",
    "error-tag": "resource-denied",
    "error-message": "Data resource already exists"
  }
}
```

The following example invokes an RPC operation.

```
curl -v -k -X POST -H "Accept: application/yang-data+xml" -d "<show-firmware-version></
show-firmware-version>"
-u admin:password https://10.20.192.65:443/restconf/operations/show-firmware-version
Note: Unnecessary use of -X or --request, POST is already inferred.
*   Trying 10.20.192.65...
* TCP_NODELAY set
* Connected to 10.20.192.65 (10.20.192.65) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=IN; ST=TN; L=CHN; O=HCL; OU=SQA; CN=10.20.192.65
*  start date: Dec 26 12:00:30 2019 GMT
*  expire date: Dec 25 12:00:30 2020 GMT
*  issuer: C=IN; ST=TN; L=CHN; O=HCL; OU=SQA; CN=10.20.192.65;
emailAddress=dpanneerselvam@extreme.com
*  SSL certificate verify result: self signed certificate in certificate chain (19),
continuing anyway.
* Server auth using Basic with user 'admin'
> POST /restconf/operations/show-firmware-version HTTP/1.1
> Host: 10.20.192.65
> Authorization: Basic YWRtaW46cGFzc3dvcmQ=
```

```
> User-Agent: curl/7.58.0
> Accept: application/yang-data+xml
> Content-Length: 47
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 47 out of 47 bytes
< HTTP/1.1 200 OK
< Date: Fri, 27 Dec 2019 10:46:10 GMT
< Server: SLX-OS WWW
< Authentication-Token: VG5OY3dwTmgvTDFadVpeeVBna1U5ZExcVl9Fb1R7aHE=
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Length: 1169
< Content-Type: application/yang-data+xml
< Vary: Accept-Encoding
< Pragma: no-cache
<
<output xmlns='urn:brocade.com:mgmt:brocade-firmware-ext'>
  <show-firmware-version>
    <os-name>SLX-OS Operating System Software</os-name>
    <os-version>20.1.1</os-version>
    <copy-right-info>Copyright (c) 1995-2019 Extreme Networks, Inc.</copy-right-info>
    <build-time>Thu Dec 26 11:10:42 2019
</build-time>
    <firmware-full-version>20.1.1_bld85</firmware-full-version>
    <control-processor-vendor> GenuineIntel</control-processor-vendor>
    <control-processor-chipset> Intel(R) Xeon(R) CPU D-1527 @ 2.20GHz</control-processor-
chipset>
    <control-processor-cpucores> 4 cores</control-processor-cpucores>
    <control-processor-microcode> 0x7000017</control-processor-microcode>
    <control-processor-memory>31653 MB</control-processor-memory>
    <node-info>
      <slot-no>0</slot-no>
      <node-instance-no>1</node-instance-no>
      <node-type>type-mm</node-type>
      <firmware-version-info>
        <application-name>SLX-OS</application-name>
        <primary-version>20.1.1_bld85</primary-version>
        <secondary-version>20.1.1_bld85</secondary-version>
      </firmware-version-info>
    </node-info>
  </show-firmware-version>
</output>
* Connection #0 to host 10.20.192.65 left intact
```

PUT Method

The PUT method is sent by the client to create or replace the target data resource. The target resource for PUT method for data creation is the new resource. Both data and datastore is supported for PUT method. A request message-body must be present, representing the new data resource, else the server returns "400 Bad Request" status-line. The error-tag value "invalid-value" is used in this case.

When new data resource is created, PUT method respond as "201 Created" as shown below .

```
curl -v -X PUT -d "<lsp-metric>20</lsp-metric>" -u admin:password
https://10.24.12.133:443/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-
holder/lsp=lsp1/lsp-metric
```

Response body

```
HTTP/1.1 201 Created
      Date: Mon, 23 Apr 2016 17:04:00 GMT
      Server: example-server
      Last-Modified: Mon, 23 Apr 2016 17:04:00 GMT
```

When the same data resource is updated, PUT method respond as "204 No Content" as shown below.

```
curl -v -X PUT -d "<lsp-metric>22</lsp-metric>" -u admin:password
https://10.24.12.133:443/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-
holder/lsp=lsp1/lsp-metric
```

Response body

```
HTTP/1.1 204 No Content
      Date: Mon, 23 Apr 2016 17:04:00 GMT
      Server: example-server
      Last-Modified: Mon, 23 Apr 2016 17:04:00 GMT
```

PATCH Method

The PATCH method is used for creating or updating the child resource. Here, only the mere PATCH method is supported. A request message-body must be present, representing the new data resource, otherwise the server returns "400 Bad Request" status-line. The error-tag value "invalid-value" is used in this case. The target resource must be the parent of the child resource to be created.

For Leaflist case, you must not use this method to change the key values of the leaf list instance.

```
curl -v -X PATCH -d "<policy><retry-time>{uint32}</retry-time></policy>" -u
admin:password
http://10.24.12.135:443/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-
holder/mpls/policy
-H "Accept: application/yang-data+xml"
```

Response body

```
HTTP/1.1 204 No Content
      Date: Mon, 23 Apr 2016 17:04:00 GMT
      Server: example-server
      Last-Modified: Mon, 23 Apr 2016 17:04:00 GMT
```

If you try to PATCH a request which is not available, a Bad Request status line is returned and the error tag as invalid-value is used.

```
curl -v -X PATCH -d <policy3><retry-time>{uint32}</retry-time></policy3>"
-u admin:password http://10.24.12.135:443/restconf/data/brocade-mpls:mpls-config/router/
mplsmpls-cmds-holder/mpls/policy3/
-H "Accept: application/yang-data+xml"
```

Response body

```
< HTTP/1.1 400 Bad Request
< Date: 2017-02-16 20:53:01
< Server: SLX-OS Wave WWW
< Authentication-Token: fGVXWXlHYEo7Yl52W1YzRTBXVztTb3BvamltUDZPY0c=
< Cache-control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Type: text/html
< Content-Length: 0
< Connection: close
<
```

```
<error xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
    <error-type>protocol</error-type>
    <error-tag>invalid-value</error-tag>
    <error-message>Data resource does not exists</error-message>
  </error>
```

DELETE Method

The DELETE method is used to delete the target resource. If the DELETE request succeeds, a "204 No Content" status-line is returned. If the target resource represents a configuration leaf-list or list data node, it must represent a single YANG leaf-list or list instance.

```
curl -v -X DELETE -u admin:password
https://<>/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-holder/mpls/
policy
-H "Accept: application/yang-data+xml"
```

```
HTTP/1.1 204 No Content
      Date: Mon, 23 Apr 2016 17:49:40 GMT
      Server: example-server
```

If a DELETE request is sent for unconfigured data resource. Then the server responds as "Not found.

```
curl -v -X DELETE -u admin:password
https://<>/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-holder/mpls/
policy
-H "Accept: application/yang-data+xml"
```

Response body

```
< HTTP/1.1 404 Not Found
< Server:
< Date: Thu, 27 Apr 2017 09:18:11 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Content-Length: 0
< Content-Type: text/html
< Pragma: no-cache
```

If a DELETE request is sent for data resource which is unknown to server, it responds as "Bad Request" and a bad-element error-tag is shown below.

```
curl -v -X DELETE -u admin:password
https://<>/restconf/data/brocade-mpls:mpls-config/router/mpls/mpls-cmds-holder/mpls/
policy123
-H "Accept: application/yang-data+xml"
```

Response body

```
HTTP/1.1 400 Bad Request
      Date: Mon, 23 Apr 2016 17:49:40 GMT
      Server: example-server

   <error xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf">
    <error-type>protocol</error-type>
    <error-tag>bad-element</error-tag>
    <error-message>Data resource does not exists</error-message>
    </error>
```

XML representation

A resource is represented as an XML element which contains the values of the resource (if any) with child elements to represent the sub resources. An XML representation of a resource is used in both the request payload and in the response.

The XML attribute, "xmlns" is mentioned in the representation. This attribute has the name of the YANG module of the resource specified in the representation.

For example, the below XML representation is for the interface "ethernet" resource which contain the child list element route-map "policy" as sub-resources.

```
<Ethernet xmlns="http://brocade.com/ns/rest/brocade-interface">
  <name>2/12</name>
    ...
    ...
    ...
    <ip xmlns="http://brocade.com/ns/rest/brocade-ip-policy">
    <policy>
      <route-map>
        <route-map-name>testmap</route-map-name>
      </route-map>
    </policy>
  </ip>
  ...
  ...
</Ethernet>
```

The utf-8 character set is used for the XML message encoding. A message is encoded for the following special characters.

Special Character	Encoded Character	Description of the Special character
<	<	less than
>	>	greater than
&	&	ampersand
'	'	apostrophe
"	"	quotation mark

JSON representation

SLX-OS supports JSON format to represent the resource. This section provides information on the JSON representation for the YANG elements.

- The YANG elements in the resource models are be mapped into JSON elements for the proper serialization.
- A leaf element is mapped into a single key-value pair. The key and the value are separated by a colon.

- A container element is mapped into a JSON object. Thus, the equivalent representation of a container starts with a left curly bracket and ends with a right curly bracket. The elements within the container are separated a comma.
- A list element is mapped into a JSON array. Thus, the equivalent representation of the list starts with a left square bracket and ends with a right square bracket. The instances of the list element are separated by a comma.

The following is an example of JASON representation.

```
{
"sflow": {
  "enable": "true",
  "collector": [
    {
    "collector-ip-address": "1.1.1.1",
    "collector-port-number": "6343",
    "use-vrf": "mgmt-vrf",

  },
    {
    "collector-ip-address": "1.2.3.4",
    "collector-port-number": "23",
    "use-vrf": "mgmt-vrf",
         }
  ],
  "polling-interval": "12",
  "sample-rate": "32",
 }
}
```

Media types

Media types the form of the data contained within a resource representation.

There are two media to identify the different kinds of resources. It is specified in the Accept and Content-Type header's value for the request and in the response respectively.

Table 5: Media types

Media type	Resources
application/yang-data+xml	Represents the data resource derived from a YANG module in the XML format.
application/yang-data+json	Represents any data resource derived from a YANG module in the JSON format.

Capabilities

The HTTP methods are used for manipulating the resource defined in the YANG model for the CRUD operations. You must employ appropriate access control mechanisms to limit what operations can be allowed by a user.

The RESTCONF protocol capability URIs are present in the container "/restconf-state/capabilities" defined in the ietf-restconf-monitoring module. The server must include a

"capability" URI leaf-list entry for the "defaults" mode or the optional query parameters used by the server. The server must include a "capability" leaf-list entry for each optional query parameter that it supports. The name and the supported URIs are as follows.

```
GET /restconf/data/ietf-restconf-monitoring:restconf-state/capabilities  HTTP/1.1
  Host: example.com
  Accept: application/yang.data+xml


HTTP/1.1 200 OK
   Date: Mon, 23 Apr 2012 17:02:00 GMT
   Server: example-server
   Cache-Control: no-cache
   Pragma: no-cache
   Last-Modified: Sun, 22 Apr 2012 01:00:14 GMT
   Content-Type: application/yang.data+xml

<capabilities xmlns="urn:ietf:params:xml:ns:yang:ietf-restconf-monitoring">
    <capability>urn:ietf:params:restconf:capability:depth:1.0</capability>
    <capability>urn:ietf:params:restconf:capability:with-defaults:1.0</capability>
    <capability>urn:ietf:params:restconf:capability:defaults:1.0?basic-mode=trim</
capability>
```

Schema resources

Retrieval of the YANG modules is supported. The leaf "schema" must be present in the associated "module" list entry. To retrieve a YANG module, you must first needs to get the URL for retrieving the schema, which is stored in the "schema" leaf.

The client can get the URL to retrieve the schema. When the client responds the URL, the corresponding YANG can be obtained.

```
GET /restconf/data/ietf-yang-library:modules-state/module=
       brocade-interface,2015-04-04/schema HTTP/1.1
   Host: 10.24.12.109
  Accept: application/yang-data+xml
```

The server responds with following URL.

```
HTTP/1.1 200 OK
   Date: Mon, 23 Apr 2012 17:01:00 GMT
   Server: example-server
   Content-Type: application/yang-data
  <?xml version="1.0" encoding="UTF-8" ?>
  <ietf-yang-library:schema>http://10.11.12.109/restconf/yang-modules/brocade-interface/
2015-04-04
  </ietf-yang-library:schema\>
```

To get the YANG schema, use the following.

```
GET http://10.24.12.109/restconf/yang-modules/ brocade-interface/2015-04-04
   HTTP/1.1
   Host: 10.11.12.109
  Accept: application/yang
```

The server responds with following URL.

```
HTTP/1.1 200 OK
      Date: Thu, 11 Feb 2016 11:10:31 GMT
      Server: 10.24.12.109
```

```
      Content-Type: application/yang

module brocade-interface {
    namespace "urn:brocade.com:mgmt:brocade-interface";
    prefix "brocade-interface";

    // contents of YANG module deleted for this example...
    ...
    ...
}
```

Yang module retrieval

The "ietf-yang-library" module provides the information about the YANG modules and submodules defined in the SLX-OS. All YANG modules and submodules must be identified in the YANG module library.

- **modules**: This mandatory container holds the identifiers for the YANG data model modules supported by the server.
- **modules/module**: This mandatory list contains one entry for each YANG data model module supported by the server. There must be an instance of this list for every YANG module that is used by the server.

This ietf-yang-library module is defined in the RFC7895 . The YANG tree diagram for ietf-yang-library.

```
+--ro modules-state
      +--ro module-set-id    string
      +--ro module* [name revision]
         +--ro name                   yang:yang-identifier
         +--ro revision               union
         +--ro schema?                inet:uri
         +--ro namespace              inet:uri
         +--ro feature*               yang:yang-identifier
         +--ro deviation* [name revision]
         |  +--ro name        yang:yang-identifier
         |  +--ro revision    union
         +--ro conformance-type       enumeration
```

Query parameter

Each RESTCONF operation allows one or more query parameters to be present in the request URI. The specific parameters that are allowed depends on the resource type, and sometimes the specific target resource used, in the request.

- Query parameters can be given in any order.
- Each parameter can appear at most once in a request URI. They are optional to implement by the server and optional to use by the client
- If more than one instance of a query parameter is present, then a "400 Bad Request" status-line MUST be returned by the server.
- A default value may apply if the parameter is missing.
- Query parameter names and values are case-sensitive

- A server MUST return an error with a '400 Bad Request' status-line if a query parameter is unexpected.
- The contents of the any query parameter value MUST be encoded according to RFC3986. Any reserved characters MUST be percent-encoded, according to RFC3986.

The following are the query parameter which will be supported in this release.

- Depth
- Content
- With-Default

Depth

- The "depth" parameter is used to specify the number of nest levels returned in a response for a GET method.
- The first nest-level will be the requested data node itself.
- The value of the "depth" parameter will be either an integer between 1 and 65535, or the string "unbounded". "unbounded" is the default.
- This parameter will be only allowed for GET methods on API, datastore, and data resources
- A "400 Bad Request" status-line will be returned if it used for other methods or resource types
- To retrieve all the child resources, the "depth" parameter should be set to the default value "unbounded".
- If an unsupported value is used, the RESTCONF server must return an <rpc-error> response with an 'invalid-value' error-tag.

For example, the below mentioned URL retrieves all the child resources of the “interface”, with the default value "unbounded" set to param “depth”.

```
GET /restconf/data/brocade-interface:interface?depth=unbounded
```

Content

- This query parameter will be used to select config and non-config data resources to be retrieved.
- This will be supported only on GET methods on data store and data resources.
- A "400 Bad Request" status-line is returned if used for other methods or resource types.
- The content is mandatory and the value can be either config or non-config.
- If an unsupported value is used, the RESTCONF server MUST return an <rpc-error> response with an 'invalid-value' error-tag.

You must mention the value of the content as “config” in the URI to retrieve the configuration data.

```
GET /restconf/data/interface?content=config
```

With Default

The "with-defaults" parameter is used to specify how information about default data nodes should be returned in response to GET requests on data resources.

- The value of the “basic-mode” will be returned as trim in the "defaults" protocol capabilities URI response to mention that default values will not be retrieved
- If an unsupported value is used, the RESTCONF server must return an <rpc-error> response with an 'invalid-value' error-tag.

When data is retrieved with a <with-defaults> parameter equal to 'trim', data nodes must not be reported if they contain the schema default value.

```
GET  /restconf/data/interfaces/interface=eth1?with-defaults=trim   HTTP/1.1
Host: 10.24.12.77
Accept: application/yang.data+json
```

This is the server responds.

```
HTTP/1.1 200 OK
   Date: Mon, 23 Apr 2012 17:01:00 GMT
   Server: SLX-OS WWW
   Content-Type: application/yang.data+json
   {
     "example:interface": [
       {
         "name" : "eth1",
         "status" : "up"
       }
     ]
   }
```

Root resource discovery

The RESTCONF client can determine the root of the RESTCONF API by sending the request to the server using the URI /.well-known/host-meta as follows:

```
curl -v -X GET -u admin:password https://<>/.well-known/host-meta
```

The following is the response of the request.

```
<data xmlns=’http://docs.oasis-open.org/ns/xri/xrd-1.0’>
 <Link rel='restconf' href='/restconf'/>
</data>
```

The response contains the "restconf" link relation returned by the server. The client can use the path "/restconf" as the RESTCONF entry point, prepend it to any subsequent request to a RESTCONF resource.

Error Reporting and Response Messages

In SLX-OS, an HTTP status code reports success or failure for RESTCONF operation. The error information is returned for "4xx" and "5xx" class of status code.

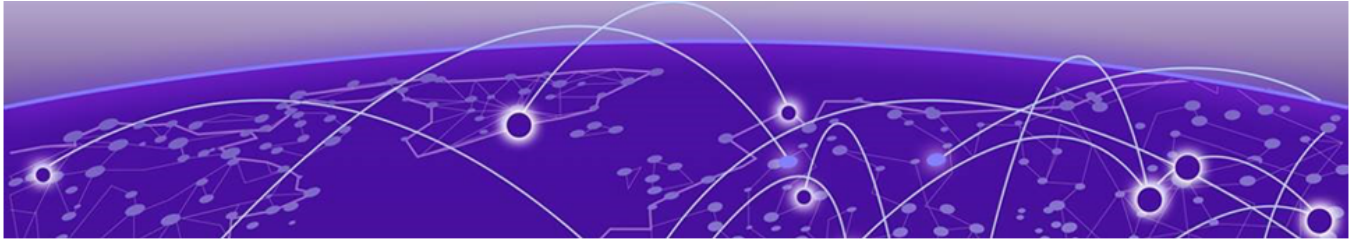
The following table shows the supported are the error-tag with status -code .

Status Code	Error Tag
Invalid-value	400
unknown-element	400
operation-not-supported	404 or 501
operation-failed	412 or 500
Access-denied	401 or 403
Data-exists	409
Unknown-namespace	400
Bad-element	400
Unknown-element	400
Malformed-message	400
Missing-attribute	400
Unknown-attribute	400
Bad-attribute	400
data-exists	409
In-use	409

When an error occurs for a request message on any resource type, and the status code that is returned is in the "4xx" range, the server sends a response message-body containing the information described by the "yang-errors". The Content-Type of this response message is a subtype of application/yang-data.

The following is an example of an error message.

```
HTTP/1.1 401 Not Found
 Date: Tue, 2 Aug 2016 17:11:00 GMT
 Server: SLX-OS WWW
 Content-Type: application/yang-data+json
  {
        "ietf-restconf:errors": {
          "error": [
           {
              "error-type": " application",
              "error-tag": "unknown-element",
              "error-message": "Element not found"
            }
          ]
        }
   }
```



Configuration RESTCONFs

aaa/accounting

Configures, modifies, or retrieves login or command accounting configuration.

Resource URIs

URI	Description
/restconf/data/brocade-aaa:aaa-config/accounting	Login or command accounting.
/restconf/data/brocade-aaa:aaa-config/accounting/commands	Enables or disabled command accounting.
/restconf/data/brocade-aaa:aaa-config/aaa/accounting/exec	Enables or disables login accounting.

PUT URIs	Payload	Description
/restconf/data/brocade-aaa:aaa-config/aaa/accounting/exec/defaultacc/start-stop/server-type	<server-type>{acc_srv_type}</server-type>	Enables login accounting.
/restconf/data/brocade-aaa:aaa-config/aaa/accounting/commands/defaultacc/start-stop/server-type	<server-type>{acc_srv_type}</server-type>	Enables command accounting.

Parameters

server-type

Specifies server for accounting. Possible values are:

None

Disables login accounting.

tacacs+

Configures to use TACACS+ server.

radius

Configures to use radius server.

exec

Login accounting.

default

Sends the logged information to the default server.

start-stop

Sends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background.

server-type

Specifies server for accounting : tacas+ or radius

Usage Guidelines

GET, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-aaa:aaa-config/accounting

Request Body

None

Response Body

```
<aaa-config xmlns="urn:brocade.com:mgmt:brocade-aaa">
                <aaa>
                    <accounting>
                        <exec>
                            <defaultacc>
                                <start-stop>
                                    <server-type/>
                                </start-stop>
                            </defaultacc>
                        </exec>
                    </accounting>
                </aaa>
            </aaa-config>
```

aaa/authentication

Configures, retrieves, and modifies AAA login sequence.

Resource URIs

URI	Description
/restconf/data/brocade-aaa:aaa-config/aaa/authentication	Configures AAA login sequence.

GET URIs	Description
/restconf/data/brocade-aaa:aaa-config/aaa/authentication	Configures AAA login sequence.
/data/brocade-aaa:aaa-config/aaa/authentication/login	Specifies the type of server that will be used for authentication, authorization, and accounting (AAA) on the device. The local server is the default.
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/first	Configures the primary source of authentication.
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/second	Configures the secondary source of authentication.

PATCH URIs	Payload	Description
/data/brocade-aaa:aaa-config/aaa/authentication/login	<login><first>{enumeration}</first></login>	Configures the order of sources for login and sets the primary source of authentication.

PUT URIs	Payload	Description
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/first	<first>{enumeration}</first>	Configures the order of sources for login and sets the primary source of authentication.
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/second	<second>{enumeration}</second>	Configures the order of sources for login and sets the secondary source of authentication.

DELETE URIs
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/first
/restconf/data/brocade-aaa:aaa-config/aaa/authentication/login/second

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/data/brocade-aaa:aaa-config/aaa/authentication

Request Body

None

Response Body

```
<aaa-config xmlns="urn:brocade.com:mgmt:brocade-aaa">
                <aaa>
                    <authentication>
                        <login>
                            <second/>
                        </login>
                    </authentication>
                </aaa>
            </aaa-config>
```

The following example uses the PUT option to configure AAA login sequence.

URI

http://host:443/data/brocade-aaa:aaa-config/aaa/authentication/login/first

Request Body

```
<first>radius</first>
```

Response Body

None

The following example uses the DELETE option to remove AAA login sequence.

URI

http://host:443/data/brocade-aaa:aaa-config/aaa/authentication/login/first

Request Body

None

Response Body

None

acl-policy

Configures, modifies, or retrieves ACL configuration.

Resource URIs

URI	Description
/restconf/data/brocade-acl-policy:acl-policy	Configures ACL policy.

GET URIs	Description
/config/restconf/data/brocade-acl-policy:acl-policy	Configures ACL policy.
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/allow-conflicting-rules	Allows conflicting rules in a ACL table.
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/allow-duplicate-rules	Allows duplicate rules in a ACL table.

PUT URIs	Payload	Description
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/allow-conflicting-rules	<allow-conflicting-rules>true</allow-conflicting-rules>	Allows conflicting rules in a ACL table.
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/acl-policy/allow-duplicate-rules	<allow-duplicate-rules>true<allow-duplicate-rules>	Allows duplicate rules in a ACL table.

DELETE URIs
/config/restconf/data/brocade-acl-policy:acl-policy
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/allow-conflicting-rules
/restconf/data/brocade-acl-policy:acl-policy/global-acl-policy-conf-cmds/allow-duplicate-rules

Parameters

allow-conflicting-rules

Allows conflicting rules in a ACL table.

allow-duplicate-rules

Allows duplicate rules in a ACL table.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to display whether duplicate rules are allowed.

URI

http://host:443/restconf/data/brocade-acl-policy:acl-policy/allow-conflicting-rules

Request Body

None

Response Body

```
<acl-policy xmlns="urn:brocade.com:mgmt:brocade-acl-policy">
                <global-acl-policy-conf-cmds>
                    <allow-conflicting-rules/>
                </global-acl-policy-conf-cmds>
            </acl-policy>
```

The following is an example PATCH operation to allow duplicate rules in a ACL table.

URI

http://host:443/restconf/data/brocade-acl-policy:acl-policy/allow-conflicting-rules

Request Body

```
<allow-conflicting-rules />
```

Response Body

None

The following is an example of the DELETE operation to remove the ACL policy.

URI

http://host:443/restconf/data/brocade-acl-policy:acl-policy

Request Body

None

Response Body

None

arp

Configures, modifies, or retrieves Address Resolution Protocol (ARP).

Resource URIs

URI	Description
/restconf/data/brocade-arp:arp-entry	Address Resolution Protocol (ARP).

GET URIs	Description
/restconf/data/brocade-arp:arp-entry=%arp--ip-address%	Retrieves Address Resolution Protocol (ARP) configuration information.

DELETE URIs
/restconf/data/brocade-arp:arp-entry=%arp--ip-address%

Parameters

arp-ip-address

Specifies the IP address of the ARP entry.

mac-address-value

Specifies the MAC address in HHHH.HHHH.HHHH format.

interfacename

Specifies the interface to use.

Usage Guidelines

GET, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following is an example of the DELETE operation to remove the ARP configuration.

URI

http://host:443/restconf/data/brocade-arp:arp-entry=%arp--ip-address%

Request Body

```
<arp-entry operation="delete" xmlns="urn:brocade.com:mgmt:brocade-arp">
                <arp-ip-address>%req_val%</arp-ip-address>
            </arp-entry>
```

Response Body

None

bridge-domain

Configures a bridge domain.

Resource URIs

URI	Description
/restconf/data/brocade-bridge-domain:bridge-domain	Configures a bridge domain.

GET URIs	Description
/restconf/data/brocade-bridge-domain:bridge-domain	Retrieves a bridge domain configuration information.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/vc-id-num	Retrieves information about a virtual circuit with the specified ID.
/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/peer=%peer-ip%/load-balance	Retrieves load-balancing details.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/peer=%peer-ip%/cos	Sets the cos value in the range 0 to 7.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/statistics	Configures statistics.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/pw-profile-name	Sets the Pw-profile name. The maximum size is 64.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/bpdu-drop-enable	Enables bpdu-drop functionality.
/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/local-switching	Configures local switching.

POST URIs	Payload	Description
/restconf/data/brocade-bridge-domain:bridge-domain	<bridge-domain><bridge-domain-id>{req_val}</ bridge-domain-id><bridge-domain-type>{req_val}</	Configures a bridge domain.

POST URIs	Payload	Description
	bridge-domain-type></bridge-domain>	
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%	<peer><peer-ip>{req_val}</peer-ip></peer>	Configures bridge domain peer.
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/logical-interface	<ethernet><lif-bind-id>{req_val}</lif-bind-id></ethernet>	Configures logical interface.
restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/logical-interface/port-channel=%pc-lif-bind-id%	<port-channel><pc-lif-bind-id>{req_val}</pc-lif-bind-id></port-channel>	Configures logical interface as port-channel.

DELETE URIs
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/vc-id-num
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/description
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/peer=%peer-ip%
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/statistics
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/router-interface=%router-ve%
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/router-interface=%router-ve%/disallow-oar-ac
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/logical-interface
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/logical-interface/ethernet=%lif-bind-id%
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/logical-interface/port-channel=%pc-lif-bind-id%
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/pw-profile-name
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/bpdu-drop-enable

DELETE URIs
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/local-switching
/restconf/data/brocade-bridge-domain:bridge-domain=%bridge-domain-id%,%bridge-domain-type%/mac-address

Parameters

bridge-domain-id

The bridge domain ID.

bridge-domain-type

The bridge domain type.

peer

Specifies the peer.

peer-ip

The peer IP address.

load-balance

Specifies load balancing.

lsp

Specifies the LSP.

logical-interface

Specifies the logical interface.

pw-profile

Specifies the PW-profile.

bpdu-drop-enable

Specifies the BPDU drop enable feature.

local-switching

Specifies local switching.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http:/host:443/restconf/data/brocade-bridge-domain:bridge-domain

Request Body

None

Response Body

```
<bridge-domain xmlns="urn:brocade.com:mgmt:brocade-bridge-domain">
    <bridge-domain-id>%req_val%</bridge-domain-id>
    <bridge-domain-type>%req_val%</bridge-domain-type>
</bridge-domain>
```

The following example uses the POST option to configure a bridge domain.

URI

http:/host:443/restconf/data/brocade-bridge-domain:bridge-domain

Request Body

```
<bridge-domain xmlns="urn:brocade.com:mgmt:brocade-bridge-domain">
                <bridge-domain-id>%req_val%</bridge-domain-id>
                <bridge-domain-type>%req_val%</bridge-domain-type>
                <description/>
            </bridge-domain>
```

Response Body

None

The following example uses the DELETE option to remove a bridge domain.

URI

http:/host:443/restconf/data/brocade-bridge-domain:bridge-domain

Request Body

None

Response Body

None

clock

Configures, modifies, or retrieves system time zone.

Resource URIs

URI	Description
/restconf/data/brocade-clock:clock-sa	Configure system time zone.

GET URIs	
/restconf/data/brocade-clock:clock-sa/clock	Configure System Timezone
/restconf/data/brocade-clock:clock-sa/clock/timezone	Timezone region or city. Regions are Africa, America, Antarctica, Arctic, Asia, Atlantic, Australia, Europe, Indian, and Pacific.

PATCH URIs	Payload	Description
/restconf/data/brocade-clock:clock-sa	<clock><timezone>(string)</timezone></clock>	Modifies or updates the system time zone.

PUT URIs	Payload	Description
/restconf/data/brocade-clock:clock-sa/clock/timezone	<timezone>(string)</timezone>	Modifies or updates the system time zone.

DELETE URIs	Payload	Description
/restconf/data/brocade-clock:clock-sa/clock/timezone	<timezone>(string)</timezone>	Deletes the system time zone.

Parameters

timezone

Specifies the local clock time zone.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-clock:clock-sa/clock/timezone

Request Body

None

Response Body

```
<clock-sa xmlns="urn:brocade.com:mgmt:brocade-clock">
                <clock>
                    <timezone/>
                </clock>
```

control-plane

Configures, modifies, or retrieves control plane configuration.

Resource URIs

URI	Description
/restconf/data/brocade-control-plane:control-plane	Control plane configuration.
/restconf/data/brocade-control-plane:control-plane/ipv6	IPv6 Control plane configuration.
/data/brocade-control-plane:control-plane/ipv6/subnet-rate-limit	Configure the rate limit for the subnet
/restconf/data/brocade-control-plane:control-plane/ipv6/subnet-rate-limit/cbr	Configures the CBR.

Parameters

cir

Specifies rate value. The range is from 0 to 100000.

cbr

Specifies the burst value in Kbytes. The range is from 1 to 64.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:80restconf/data/brocade-control-plane:control-plane

Request Body

None

Response Body

```
control-plane xmlns="urn:brocade.com:mgmt:brocade-control-plane">
                <ipv6>
                    <subnet-rate-limit>
                        <cbr/>
                    </subnet-rate-limit>
```

```
                </ipv6>
            </control-plane>>
```

The following example uses the DELETE option to remove the control plane configuration.

URI

http://host:443/restconf/data/brocade-control-plane:control-plane

Request Body

None

Response Body

None

delete configuration

Deletes the prefix-independent-convergence configuration.

Resource URIs

URI	Description
<base_URI>/config/running/cluster/no prefix-independent-convergence	Deletes the prefix-independent-convergence.

Parameters

delete configuration

Deletes prefix-independent-convergence.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:80/rest/config/running/cluster/prefix-independent-convergence

Request Body

None

Response Body

```
http://<srvrip>:80/rest/config/running/prefix-independent-convergence
```

display running-configuration

Displays running configuration for prefix-independent-convergence.

Resource URIs

URI	Description
<base_URI>/config/running/cluster/do show running-config prefix-independent-convergence	Displays running configuration for prefix-independent-convergence.

Parameters

display running-configuration

Displays running configuration for prefix-independent-convergence.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:80/rest/config/running/cluster/prefix-independent-convergence

Request Body

None

Response Body

```
http://<srvrip>:80/rest/config/running/prefix-independent-convergence
```

dot1x

Configures, retrieves, and modifies 802.1X authentication.

Resource URIs

URI	Description
/restconf/data/brocade-dot1x:dot1x	Configures 802.1X authentication.

GET URIs	Description
/restconf/data/brocade-dot1x:dot1x	IEEE 802.1X port-based access control.
/restconf/data/brocade-dot1x:dot1x/enable	Enables global port authentication.
/restconf/data/brocade-dot1x:dot1x/test	Configures 802.1X readiness check.
/restconf/data/brocade-dot1x:dot1x/timeout	Configures timeout for dot1x readiness check

PATCH URIs	Payload	Description
/restconf/data/brocade-dot1x:dot1x	<dot1x><enable>(enumeration)</enable></dot1x>	Configures IEEE 802.1X port-based access control and enables global port authentication.
/restconf/data/brocade-dot1x:dot1x/test	<test><timeout>{dot1x-readinesstest-timeout-interval}</timeout></test>	Configures timeout for dot1x readiness check.

PUT URIs	Payload	Description
/restconf/data/brocade-dot1x:dot1x/enable	<enable>(enumeration)</enable>	Enables global port authentication.
/restconf/data/brocade-dot1x:dot1x/timeout	<timeout>{dot1x-readinesstest-timeout-interval}</timeout>	Configures timeout for dot1x readiness check.

DELETE URIs
/restconf/data/brocade-dot1x:dot1x/enable
/restconf/data/brocade-dot1x:dot1x/timeout

Parameters

test timeout

Specifies the readiness test interval value in seconds. Valid values range from 1 through 65535. The default readiness test interval is 10 seconds.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-dot1x:dot1x

Request Body

None

Response Body

```
<dot1x xmlns="urn:brocade.com:mgmt:brocade-dot1x">
                        <timeout>
                            <tx-period>%dot1x-tx-timeout-interval%</tx-period>
                        </timeout>
                    </dot1x>
```

The following example uses the PATCH option to configure dot1x.

URI

http://host:443/restconf/data/brocade-dot1x:dot1x

Request Body

```
<dot1x><enable>true</enable></dot1x>
```

Response Body

None

The following example uses the DELETE option to remove dot1x.

URI

http://host:443/restconf/data/brocade-dot1x:dot1x/enable

Request Body

None

Response Body

None

ip/access-list

Configures, modifies, or retrieves the Internet Protocol (IP) access list configuration.

Resource URIs

URI	Description
/restconf/data/brocade-ip-access-list:ip-acl	The Internet Protocol configuration.
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard	Standard IP ACL configuration.
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/extended	Extended IP ACL configuration.

POST URIs	Payload	Description
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list	<standard><name>{acl-name}</name></standard>	Configures a standard ACL.
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list	<extended><name>{acl-name}</name></extended>	Configures an extended ACL.

DELETE URIs
/restconf/data/brocade-ip-access-list:ip-acl
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard=%name%
/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/extended=%name%
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-ip-access-list:ip-acl-interface
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-ip-access-list:ip-acl-interface/ip/access-group=%ip-access-list%,%ip-direction%
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-ip-access-list:ip-acl-interface/ip/access-group=%ip-access-list%,%ip-direction%/traffic-type
/restconf/data/brocade-interface:interface/port-channel=%name%/brocade-ip-access-list:ip-acl-interface
/restconf/data/brocade-common-def:routing-system/brocade-interface:interface/ve=%name%/brocade-ip-access-list:ip-acl-interface
/restconf/data/brocade-common-def:routing-system/brocade-interface:interface/ve=%name%/brocade-ip-access-list:ip-acl-interface/ip/access-group=%ip-access-list%,%ip-direction%

Parameters

name

Specifies the IPv4 access list name.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the access list configurations.

URI

http://host:443/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard=%name%

Request Body

None

Response Body

```
<ip-acl xmlns="urn:brocade.com:mgmt:brocade-ip-access-list">
                <ip>
                    <access-list>
                        <standard>
                            <name>%req_val%</name>
                        </standard>
                    </access-list>
                </ip>
            </ip-acl>
```

The following example uses the POST option to configure a standard access list.

URI

http://host:443/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard=%name%

Request Body

```
<standard >
    <name>std10</name>
</standard>
```

Response Body

None

The following example uses the DELETE option to remove a standard access list.

URI

http://host:443/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard=%name%

Request Body

None

Response Body

None

ipv6/access-list

Configures, modifies, or retrieves the Internet Protocol version 6 (IPv6) access list configuration.

Resource URIs

URI	Description
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6	The Internet Protocol configuration.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard	Standard IP ACL configuration.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%	Sequence number configuration.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended	Extended IP ACL configuration.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%	Sequence number configuration.

GET URIs	Description
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%//src-host-ip	Retrieves the source host IP of a specific standard ACL with a sequence ID.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%/src-mask	Displays whether count is enabled for a standard ACL.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%//count	Displays whether count is enabled for a specific standard ACL.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%//log	Displays whether log is configured for a specific standard ACL.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%//copy-sflow	Sends matching inbound packets to the sFlow collector.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended%name%/seq=%seq-id%//sport-number-lt-tcp	s-port numbers less than or equal to Transmission Control Protocol (TCP).
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//sport-number-gt-tcp	s-port numbers greater than or equal to Transmission Control Protocol (TCP).

GET URIs	Description
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//sport-number-eq-neq-udp	All TCP or User Datagram Protocol (UDP) port numbers except the s-port number.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//sport-number-lt-udp	s-port numbers less than or equal to User Datagram Protocol (UDP).
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//sport-number-gt-udp	s-port numbers greater than or equal to User Datagram Protocol (UDP).
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//vlan	Displays the VLAN interface to which the ACL is bound.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%//count	Displays whether count is enabled for an extended ACL.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%/log	Displays whether log is configured for an extended ACL.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%/seq=%seq-id%/mirror	Mirrors packets matching the rule.

POST URIs	Payload	Description
/config/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list	<standard><name>{name}</name></standard>	Configures a standard IPv6 access list.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%	<seq><seq-id>{seq-id}</seq-id><action>{enumeration}</action><src-host-any-sip>{sip-cid})</src-host-any-sip></seq>	Configures the parameters of a standard IPv6 access list.
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list	<extended><name>{name}</name></extended>	Configures an extended IPv6 access list.

DELETE URIs
/restconf/data/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%
/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/extended=%name%

Parameters

name

Specifies the IPv6 access list name.

seq

Specifies the sequence number.

seq-id

Specifies the sequence number for the rule.

action

Specifies the action to be performed. Supported actions are **deny**, **hard-drop**, and **permit**. Configuring deny drops traffic. Configuring hard-drop force drops traffic. Configuring permit allows traffic.

src-host-any-sip

Specifies any source host IP address.

src-host-ip

Specifies the source host IP address.

count

Enables the counting of the packets matching the rule.

log

Packets matching the filter are sent to the CPU and a corresponding log entry is generated by enabling the logging mechanism. This parameter is only available with permit and deny.

protocol-type

The type of protocol used.

dst-host-any-dip

Specifies any destination host IP address.

dst-host-ip

Specifies the destination host IP address.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the source host IP address.

URI

http://host:443/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%/src-host-ip

Request Body

None

Response Body

```
<ipv6-acl xmlns="urn:brocade.com:mgmt:brocade-ipv6-access-list">
                <ipv6>
                    <access-list>
                        <standard>
                            <name>%req_val%</name>
                        </standard>
                    </access-list>
                </ipv6>
            </ipv6-acl>
```

The following example uses the POST option to configure a standard access list (rest1).

URI

http://host:443/restconf/data/brocade-ipv6-access-list:ipv6-acl/ipv6/access-list/standard=%name%/seq=%seq-id%/src-host-ip

Request Body

```
<standard><name>rest1</name></standard>
```

Response Body

None

The following example uses the DELETE option to remove a standard access list.

URI

http://host:443/restconf/data/brocade-ip-access-list:ip-acl/ip/access-list/standard=%name%

Request Body

None

Response Body

None

management-security

Resource URIs

URI	Description
<base_URI>/restconf/data/brocade-crypto:management-security	Sets and retrieves the supported TLS version on the device for both scenarios where the device acts as a server or as a client.

GET URIs	Description
<base_URI>/restconf/brocade-crypto:management-security/ssl-profile/server/tls	Retrieves the current TLS support configuration for the server.
<base_URI>/restconf/brocade-crypto:management-security/ssl-profile/client/tls	Retrieves the current TLS support configuration for the client.

POST URIs	Payload	Description
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/server/tls	<min-version>{1.1|1.2|1.3}<min-version>	Specifies the configuration of minimum supported TLS version when the device acts as a Server.
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/client/tls	<min-version>{1.1|1.2|1.3}<min-version>	Specifies the configuration of minimum supported TLS version when the device acts as a client.

PATCH URIs	Payload	Description
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/server/tls	<min-version>{1.1|1.2|1.3}<min-version>	Specifies the configuration of minimum supported TLS version when the device acts as a Server.
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/client/tls	<min-version>{1.1|1.2|1.3}<min-version>	Specifies the configuration of minimum supported TLS version when the device acts as a client.

Delete URIs

Delete URIs
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/server/tls/min-version
<base_URI>/restconf/data/brocade-crypto:management-security/ssl-profile/client/tls/min-version

server

The TLS version to use when the device is considered a Server.

client

The TLS version to use when the device is considered a client.

min-version

The minimum TLS version supported by the device in the particular mode.

Usage Guidelines

GET, POST, PUT, PATCH, and DELETE operations are supported.

Examples

The following example uses the GET option to retrieve the current TLS version when the device is a client.

URI

http://host:443/restconf/data/brocade-crypto:management-security/ssl-profile/client

Request Body

None

Response Body

```
<tls>
    <min-version>
        1.2
    </min-version>
<tls>
```

The following example uses the PUT option to set the TLS version to version 1.3 when the device is considered a server.

URI

http://host:443/restconf/data/brocade-crypto:management-security/ssl-profile/server

Request Body

```
<tls>
    <min-version>
        1.3
    </min-version>
<tls>
```

Response Body

None

node

Penalizes all links originating from the node IP address.

Resource URIs

URI	Description
/restconf/data/brocade-node:node-id	Penalizes all links originating from the node IP address..

POST URIs	Payload	Description
/restconf/data/brocade-node:node-id=%node-id%	<node-id>	Configures sFlow collector.

DELETE URIs
/restconf/data/brocade-node:node-id=%node-id%

Parameters

node-id

Specifies the the node ID.

Usage Guidelines

GET, POST, and DELETE operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-node:node-id=%node-id%

Request Body

None

Response Body

None

The following example uses the DELETE option to remove the sFlow sampling rate.

URI

http://host:443/restconf/data/brocade-node:node-id=%node-id%

Request Body

None

Response Body

None

ntp

Configures, modifies, or retrieves NTP commands.

Resource URIs

URI	Description
/restconf/data/brocade-ntp:ntp	Configures NTP.

GET URIs	Description
/restconf/data/brocade-ntp:ntp	Displays NTP configuration.
/restconf/data/brocade-ntp:ntp/authentication-key	Displays authentication key.
/restconf/data/brocade-ntp:ntp/server	Displays NTP server information.

POST URIs	Payload	Description
/restconf/data/brocade-ntp:ntp/server	<server><ip>(ip-address)</ip><use-vrf>(vrf-name)</use-vrf></server>	Configures NTP server.
/crestconf/data/brocade-ntp:ntp/authentication-key	<authentication-key><keyid>(unit32)</keyid><md5>{string}</md5></authentication-key>	Configures authentication key and MD5 message-digest algorithm.
/restconf/data/brocade-ntp:ntp/server	<server><ip>(ip-address)</ip><use-vrf><key>(unit32)</key></server>	Configures NTP server key.
/restconf/data/brocade-ntp:ntp/disable	<all> | <server>	Disables the NTP server/client mode. Disabling the NTP server/client mode does not remove the configuration.

POST URIs	Payload	Description
/restconf/data/brocade-ntp:ntp/authenticate	<key-id-1 > <key-id-2> <key-id-n>	This command enables or disables the NTP authentication at global level. If the authentication is enabled, the NTP packets from servers, peers, clients not having MAC is dropped. Only those servers/peers configured with key authentication is considered for time synchronization. Client requests only with authentication is served, whose key-IDs match with one of the trusted key-IDs.
/restconf/data/brocade-ntp:ntp/master	< key key-id > < use-vrf vrf-name >	Configures the device as an authoritative NTP Server. ntp master enables device to use its own clock to synchronize with peers/clients. This command is not effective, if the NTP is enabled in client-only mode. .
/restconf/data/brocade-ntp:ntp/server	<ipv4 | ipv6 > <vrf name >	Specifies or adds an NTP server IP address and optionally associates an authentication key to the server.
/restconf/data/brocade-ntp:ntp/trusted-key	<key-id-1 > <key-id-2> <key-id-n>	Configures additional subset of trusted key-IDs which can be used for NTP and client authentication. The keys configured for server/peer is implicitly considered as part of trusted keys.
/restconf/data/brocade-ntp:ntp/peer	<ipv4 | ipv6 > <vrf name >	Configures the NTP peers and specify the peers to synchronize the system clock. Maximum 8 NTP peers can be configured

DELETE URIs

DELETE URIs
/restconf/data/brocade-ntp:ntp/server
/restconf/data/brocade-ntp:ntp/authentication-key
//restconf/data/brocade-ntp:ntp/source-ip

Parameters

authentication-key

Configures authentication key parameters.

server

Configures NTP server parameters.

ip

Configures the source ip to be used for NTP.

keyid

Specifies authentication key ID. Valid range is from 0 to 65535.

use-vrf

Specifies the VRF to be used.

key

Specifies the key.

md5

Specifies a string for the MD5 message-digest algorithm. The string can be a maximum of 15 ASCII characters.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-ntp:ntp/server

Request Body

None

Response Body

```
<server y:self="restconf/data/brocade-ntp:ntp/server/10.1.1.2%2Cmgmt-vrf">
    <ip>10.1.1.2</ip>
    <use-vrf>mgmt-vrf</use-vrf>
  </server>
```

The following example uses the POST option to configure authentication-key.

URI

http://host:443/restconf/data/brocade-ntp:ntp/authenticate

Request Body

```
<authentication-key>
  <keyid>50</keyid>
  <md5>{teesting}</md5>
</authentication-key>
```

Response Body

The following example uses the DELETE option to remove NTP configuration.

URI

http://host:443/restconf/data/brocade-ntp:ntp/server

Request Body

None

Response Body

prefix-independent-convergence

Configures prefix-independent-convergence.

Resource URIs

URI	Description
<base_URI>/config/running/prefix-independent-convergence	Configures prefix-independent-convergence.

Parameters

prefix-independent-convergence

Configures prefix-independent-convergence.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://<srvrip>:80/rest/config/running/prefix-independent-convergence

Request Body

None

Response Body

```
http://<srvrip>:80/rest/config/running/prefix-independent-convergence
```

router/isis

Configures IS-IS protocol.

Resource URIs

URI	Description
/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis	Configures IS-IS protocol.

GET URIs	Description
/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis	Enables IS-IS.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/net=%net-cmd%	Defines NSAP address.
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-check/auth-check	Authenticate incoming PDUs for LSPs, CSNP, and PSNP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-check/auth-check-level1	Authenticate incoming PDUs for Level-1 LSPs, CSNP, and PSNP.
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-check/auth-check-level1/auth-check-level1-disable	Disables authentication of incoming PDUs for Level-1 LSPs, CSNP, and PSNP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-check/auth-check-level2	Authenticate incoming PDUs for Level-2 LSPs, CSNP, and PSNP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-check/auth-check-level2/auth-check-level2-disable	Disables the authenticate incoming PDUs for Level-2 LSPs, CSNP, and PSNP.
estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-mode	Define authentication mode.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-mode/md5	HMAC-MD5 authentication.

GET URIs	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-mode/md5/auth-mode-md5-level1	Authentication mode for Level-1 LSPs, CSNP, and PSNP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-mode/md5/auth-mode-md5-level2	Authentication mode for Level-2 LSPs, CSNP, and PSNP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-key	Define authentication key
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-key/auth-key-level1-str	Auth-key for Level-1 ISIS Router
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/auth-key/auth-key-level2-str	Auth-key for Level-2 ISIS Router
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/csnp-interval	Rate of transmission of CSNPs
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/disable-inc-stct-spf-opt	Disables Incremental Shortcut SPF Optimizations; resorts to Full SPF
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/disable-incremental-spf-opt	Disables Incremental SPF Optimizations; resorts to Full SPF
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/disable-partial-spf-opt	Disables Partial SPF Optimizations; resorts to Full SPF
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/fast-flood	Defines the number of LSPs to be flooded before SPF Run
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/fast-flood/fast-flood-value	The number of LSPS to be flooded before SPF Run. Range is 1-15; default is 4

GET URIs	Description
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes//graceful-restart	Enables the ISIS graceful restart capability
/estconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes//graceful-restart/helper-disable	Disables Helper Mode
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/hostname	Integrated IS-IS dynamic hostname
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/hostname/disable	Disables integrated IS-IS dynamic hostname
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/is-type	Define inter-area/intra area operation mode
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/log	Enable Logging IS-IS activities
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/log /adjacency	Logging Adjacency Changes
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/log /invalid-lsp-packets	Logging Invalid LSP Packets
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/lsp-gen-interval	Minimum interval between regenerating same LSP
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/lsp-interval	Rate of transmission of LSPs
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/lsp-refresh-interval	LSP refresh interval
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/max-lsp-lifetime	Maximum LSP lifetime

GET URIs	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/nonstop-routing	Enables the ISIS nonstop routing capability
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/partial-spf-interval	Partial SPF Calculation Timers
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/partial-spf-interval/pspf-max-hold-time	Max hold time (msec) between two PSPF calculations. Range is 0-120000. Default is 5000.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/partial-spf-interval/pspf-init-delay	Initial delay (msec) between receiving a LSP change to PSPF calculation. Range is 0-120000. Default is 2000.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/partial-spf-interval/pspf-hold-time	Hold time (msec) between two PSPF calculations. 0-120000. Default is 5000
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/retransmit-interval	Time between retransmission of LSP.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/set-debug	Enabling isis debug configuration.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/set-debug/nsr	Sets NSR debug.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/set-overload-bit	Configures a device to signal other devices not to use it as an intermediate hop in their shortest path first (SPF) calculations if an IS's resources are overloaded and are preventing the IS from properly performing IS-IS routing.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/set-overload-bit/on-startup	Set overload-bit only temporarily on reboot.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/spf-interval/level-1	SPF calculation Timers

GET URIs	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributess/reverse-metric	Configure IS-IS reverse metric at the router level.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/reverse-metric/reverse_metric_tlv	Configure reverse metric TLV.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/reverse-metric/tlv-type	Configure reverse metric TLV type.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/reverse-metric/rev-metric-val	Configure IS-IS reverse metric value.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/reverse-metric/whole-lan	Change metric for whole LAN.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes/reverse-metric/te-def-metric	Update TE default metric sub-tlv.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family	Enter Address Family command mode.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4	IPv4 address Family.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/unicast	IPv4 unicast address Family.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/metric-style	Use narrow or wide metric type.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/metric-style/wide	Use new style of TLVs to carry wider metric.

GET URIs	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/metric-style/wide/level1	Level-1 only.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/metric-style/wide/metric-style-wide-level2	Level-2 only.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/summary-address=%summary-ip%,%summary-ip-mask%	Configure Integrated IS-IS address summaries
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/summary-address=%summary-ip%,%summary-ip-mask%/summary-ip-level2	Configure Integrated IS-IS address summaries.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/ldp-sync	Enable LDP-SYNC on all eligible ISIS interfaces.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/ldp-sync/hold-down	Length (in seconds) of hold-down timer. Range is 1-65535.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/default-link-metric	Default Link Metric.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/default-link-metric/level1	Default Link Metric for Level-1.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/default-link-metric/level2	Default Link Metric for Level-2.

GET URIs	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/af-common-attributes/default-information-originate	Controls origination of default route.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/af-common-attributes/default-information-originate/default-information-originate-route-map	Uses route map.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes/af-common-attributes	Configures attributes for IPv4 address family.
</restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv6-unicast/af-ipv6-attributes/af-common-attributes	Configures attributes for IPv6 address family.

POST URIs	Payload	Description
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-isis:interface-eth-isis-conf/intf-isis/interface-isis	<interface-auth-key><interface-auth-key-level>%enumeration%</interface-auth-key-level><interface-auth-key-str>%string%</interface-auth-key-str></interface-auth-key>	Configures IS-IS Protocol (ISIS).
/rrestconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder	<net><net-cmd>{net-cmd}</net-cmd></net>	Define NSAP address
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes	<fast-flood-value> {unit32} < /fast-flood-value >	Define number of LSPs to be flooded before SPF Run

POST URIs	Payload	Description
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes	<spf-interval><spf-interval-level>level-1</spf-interval-level><spf-interval-max-hold-time>{unit32}</spf-interval-max-hold-time><spf-interval-initial-delay>{unit32}</spf-interval-initial-delay><spf-interval-hold-time>{unit32}</spf-interval-hold-time></spf-interval>	SPF calculation Timers.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv4-unicast/af-ipv4-attributes	<summary-address><summary-ip>{inet:ipv4-address}</summary-ip><summary-ip-mask>{inet:ipv4-address}</summary-ip-mask><Level-1>{enumeration}</Level-1></summary-address>	Configures Integrated IS-IS address summaries.
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/address-family/ipv4/af-ipv6-unicast/af-ipv6-attributes	<summary-prefix><summary-prefix-ipv6>{common-def:ipv6-address-prefix}</summary-prefix-ipv6><Level-1>true</Level-1></summary-prefix>	Configure Integrated IS-IS address summaries

DELETE URIs
/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis
/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis/int-router-isis/interface-ip-router-isis
/restconf/data/brocade-interface:interface/ethernet=%name%/ipv6/brocade-isis:intf-ipv6-router-isis
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder
/restconf/data/brocade-common-def:routing-system/router/brocade-isis:isis/router-isis-cmds-holder/router-isis-attributes

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/rrestconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis/int-router-isis

Request Body

None

Response Body

The following is an example of the POST operation to configure an IS-IS network entity title (NET) for the routing process.

URI

http://host:443/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis/int-router-isis

Request Body

```
<net><net-cmd>01.1111.1111.1111.00</net-cmd></net>
```

Response Body

None

The following is an example of the DELETE operation to remove IS-IS configuration.

URI

http://host:443/restconf/data/brocade-interface:interface/ethernet=%name%/ip/brocade-isis:intf-router-isis/int-router-isis

Request Body

None

Response Body

None

rmon

Configures, modifies, or retrieves Remote Monitoring Protocol (RMON) information.

Resource URIs

URI	Description
/restconf/data/brocade-rmon:rmon	Remote Monitoring Protocol (RMON).

GET URIs	Description
/restconf/data/brocade-rmon:rmon	Remote Monitoring Protocol (RMON).
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%/event-description	Retrieves event description.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%/log	Retrieves logged events.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%/event-owner	Retrieves event owner identity.
/restconf/data/brocade-rmon:rmon/alarm-entry=%alarm-index%/alarm-owner	Retrieves alarm owner identity.

POST URIs	Payload	Description
/restconf/data/brocade-rmon:rmon	<event><event-index>(int32)</event-index></event>	Configures RMON event.
/restconf/data/brocade-rmon:rmon	<alarm><alarm-index>(int32)</alarm-index><snmp-oid>(string)</snmp-oid><interval>(int32)</interval><type>(string)</type><rising-threshold>(unit32)</rising-threshold><event>(int32)</event></alarm>	Configures RMON alarm.

PATCH URIs	Payload	Description
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<event><description>(string)</description></event>	Configures RMON event description.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<event><log>(string)</log></event>	Configures event log.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<event><trap>(string)</trap></event>	Configures event trap.

PATCH URIs	Payload	Description
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<event><owner>(string)</owner></event>	Configures event owner.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<alarm><snmp-oid>(string)</snmp-oid><interval>(int32)</interval><type>(string)</type><rising-threshold>(unit32)</rising-threshold><event>(int32)</event></alarm>	Configures RMON alarm.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<alarm><falling-threshold>(uint32)</falling-threshold><event>(int32)</event></alarm>	Configures alarm falling threshold.
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%	<alarm><owner>(string)</owner></alarm>	Configures alarm owner.

DELETE URIs
/restconf/data/brocade-rmon:rmon/event-entry=%event-index%
/restconf/data/brocade-rmon:rmon/alarm-entry=%alarm-index%
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-rmon:rmon/collection/ether-stats-entry=%ether-stats-index%
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-rmon:rmon/collection/history-control-entry=%history-control-index%

Parameters

alarm-index

Configures RMON alarm. The range is from 1 to 65535.

rising-threshold

Configures rising threshold. The range is from 0 to 4294967295.

falling-threshold

Configures falling threshold. The range is from 0 to 4294967295.

snmp-oid

Configures SNMP OID.

interval

Configures alarm sample interval.

event-index

Configures RMON event. The range is from 1 to 65535.

Usage Guidelines

GET, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-rmon:rmon/event-entry=%event-index%/event-description

Request Body

None

Response Body

```
 <rmon xmlns="urn:brocade.com:mgmt:brocade-rmon">
                <event-entry>
                    <event-index>%req_val%</event-index>
                    <event-community/>
                </event-entry>
            </rmon>
```

The following example uses the POST option to configure alarm.

URI

http://host:443/restconf/data/brocade-rmon:rmon

Request Body

```
<alarm>
  <alarm-index>100</alarm-index>
  <snmp-oid>1.3.6.1.2.1.16.1.1.1.5.65535</snmp-oid>
  <interval>10</interval>
  <type>absolute</type>
  <rising-threshold>10000</rising-threshold>
  <event>100</event>
</alarm>
```

Response Body

None

The following example uses the DELETE option to remove RMON event.

URI

http://host:443/restconf/data/brocade-rmon:rmon/event-entry=%event-index%/event-description

Request Body

None

Response Body

None

sflow

Configures, modifies, or retrieves sFlow configuration.

Resource URIs

URI	Description
/rest/config/running/sflow	sFLow configuration.

GET URIs	Description
/restconf/data/brocade-sflow:sflow	Retrieves sFLow configuration.
/restconf/data/brocade-sflow:sflow/agent-address	Retrieves sFLow agent-ID address.
/restconf/data/brocade-sflow:sflow/enable	Retrieves if sFlow is enabled globally or not.
/config/running/sflow/source-interface	Retrieves sFlow source IP interface.
/restconf/data/brocade-sflow:sflow/agent-address/agent-interface-name	Retrieves the sFlow interface information.
/restconf/data/brocade-sflow:sflow/collector=%collector-ip-address%,%collector-port-number%,%use-vrf%	Retrieves sFlow collector configuration.
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/polling-interval	Retrieves interface counter polling interval details.
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/sample-rate	Retrieves interface sampling rate.
/restconf/data/brocade-sflow:sflow/update-destination-mac	Retrieves the state of Update Destination MAC for routed packets feature.

POST URIs	Payload	Description
/restconf/data/brocade-sflow:sflow	<collector><collector-ip-address>{inet:ip-address}</collector-ip-address><collector-port-number>{uint32}</collector-port-number><use-vrf>{common-def:vrf-name}</use-vrf></collector>	Configures sFlow collector.

PATCH URIs	Payload	Description
	<sflow><enable>true</enable></sflow>	Enables sFlow.

PATCH URIs	Payload	Description
/restconf/data/brocade-sflow:sflow		
/restconf/data/brocade-sflow:sflow/agent-address/agent-interface-name	<source-interface><interface-type>{source-interface-type}</interface-type><interface-name>{loopback:intf-loopback-port-type}</interface-name></source-interface>	Confiugres sFlow source interface.
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/polling-interval	<sflow><polling-interval>{uint32}</polling-interval></sflow>	Configures sFlow polling interval.
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/sample-rate	<sflow><sample-rate>{uint32}</sample-rate></sflow>	Configures sFlow sampling rate.

PUT URIs	Payload	Description
/restconf/data/brocade-sflow:sflow	<sflow><enable>true</enable></sflow>	Enables sFlow.
/restconf/data/brocade-sflow:sflow/agent-address/agent-interface-name	<source-interface><interface-type>{source-interface-type}</interface-type><interface-name>{loopback:intf-loopback-port-type}</interface-name></source-interface>	Confiugres sFlow source interface.
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/polling-interval	<sflow><polling-interval>{uint32}</polling-interval></sflow>	Configures sFlow polling interval.

PUT URIs	Payload	Description
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/sample-rate	<sflow><sample-rate>{uint32}</sample-rate></sflow>	Configures sFlow sampling rate.
/restconf/data/brocade-sflow:sflow/update-destination-mac	<sflow><update-destinationmac/></sflow>	Configures sFlow Update Destination MAC for routed packets.

DELETE URIs
/restconf/data/brocade-sflow:sflow/enable
/restconf/data/brocade-sflow:sflow/agent-address
/restconf/data/brocade-sflow:sflow/source-interface
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/polling-interval
/restconf/data/brocade-interface:interface/ethernet=%name%/brocade-sflow:sflow/sample-rate
/restconf/data/brocade-sflow:sflow/update-destination-mac

Parameters

collector-ip-address

Specifies the IP address of the sFlow collector.

collector-port-number

Specifies the port number used by the sFlow collector. The value can range from 1 through 65535.

use-vrf

VRF to use for sending data to the collector (default = mgmt-vrf).

source-ip

Specifies the source IP address to use.

polling-interval

Specifies polling interval value. The value can range from 1 through 65535. The default value is 20.

sample-rate

Specifies sampling rate value. The value can range from 1 through 16000000 (for SLX 9740 and Extreme 8820) and from 1 to 100000 for all other devices. The default value is 2048.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:80/rest/config/running/sflow/enable

Request Body

None

```
<sflow xmlns=""urn:brocade.com:mgmt:brocade-sflow"" xmlns:y=""http://brocade.com/ns/
rest"" y:self=""/rest/config/running/sflow"">
  <enable>true</enable>
  <source-interface y:self=""/rest/config/running/sflow/source-interface"">
  </source-interface>
  <collector y:self=""/rest/config/running/sflow/collector/34.1.1.2%2C6343%2Cvrf2"">
    <collector-ip-address>34.1.1.2</collector-ip-address>
    <collector-port-number>6343</collector-port-number>
    <use-vrf>vrf2</use-vrf>
  </collector>
  <collector y:self=""/rest/config/running/sflow/collector/112.1.1.2%2C6343%2Cdefault-
vrf"">
    <collector-ip-address>112.1.1.2</collector-ip-address>
    <collector-port-number>6343</collector-port-number>
    <use-vrf>default-vrf</use-vrf>
  </collector>
  <collector y:self=""/rest/config/running/sflow/collector/172.22.12.83%2C6343%2Cmgmt-
vrf"">
    <collector-ip-address>172.22.12.83</collector-ip-address>
    <collector-port-number>6343</collector-port-number>
    <use-vrf>mgmt-vrf</use-vrf>
  </collector>
  <collector y:self=""/rest/config/running/sflow/collector/
fdd1:a123:b123:c123:34:1:1:2%2C6622%2Cvrf2"">
    <collector-ip-address>fdd1:a123:b123:c123:34:1:1:2</collector-ip-address>
    <collector-port-number>6622</collector-port-number>
    <use-vrf>vrf2</use-vrf>
  </collector>
  <collector y:self=""/rest/config/running/sflow/collector/
fdd1:a123:b123:c123:112:1:1:2%2C6343%2Cdefault-vrf"">
    <collector-ip-address>fdd1:a123:b123:c123:112:1:1:2</collector-ip-address>
    <collector-port-number>6343</collector-port-number>
    <use-vrf>default-vrf</use-vrf>
  </collector>
  <polling-interval>44</polling-interval>
  <sample-rate>456</sample-rate>
</sflow>
```

The following example uses the POST option to configure sFlow collector.

URI

http://host:80/rest/config/running/sflow

Request Body

```
<collector>
  <collector-ip-address>fdd1:a123:b123:c123:112:1:1:2</collector-ip-address>
  <collector-port-number>6343</collector-port-number>
```

```
   <use-vrf>default-vrf</use-vrf>
</collector>
```

None

The following example uses the DELETE option to remove the sFlow sampling rate.

URI

http://host:80/rest/config/running/sflow/sample-rate

Request Body

None

None

topology-group

Configures topology VLAN group for L2 protocols.

Resource URIs

URI	Description
/brocade-topology-group:topology-group	Configures topology vlan group for L2 protocols.

GET URIa	Description
/restconf/data/brocade-topology-group:topology-group	Retrieves topology group configuration details.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%	Retrieves information for a particular topology group.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%}/master-vlan	Retrieves information about master VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan	Retrieves information about member VLAN.

POST URIs	Payload	Description
restconf/data/brocade-topology-group:topology-group	<topology-group><topology-group-id>(unit32)</topology-group-id></topology-group>	Configures topology group.

PATCH URIs	Payload	Description
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%}/master-vlan	<master-vlan>(unit32)</master-vlan>	Configures master VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan	<member-vlan><add>(unit32)</add></member-vlan>	Adds member VLAN.

PATCH URIs	Payload	Description
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan	<member-vlan><remove>(unit32)</remove></member-vlan>	Removes member VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan-remove	<remove>(unit32)</remove>	Removes member VLAN.

PUT URIs	Payload	Description
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%}/master-vlan	<master-vlan>(unit32)</master-vlan>	Configures master VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan	<member-vlan><add>(unit32)</add></member-vlan>	Adds member VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-bridge-domain/member-bridge-domain-add	<add>(unit32)</add>	Removes member VLAN.
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan-remove	<remove>(unit32)</remove>	Removes member VLAN.

DELETE URIs
/restconf/data/brocade-topology-group:topology-group=%topology-group-id%

Parameters

group-id

Specifies topology group ID.

member-vlan

Configures member VLANs.

master-vlan

Configures master VLANs.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/restconf/data/brocade-topology-group:topology-group=%topology-group-id%/member-vlan

Request Body

```
<topology-group>
  <topology-group-id>1</topology-group-id>
</topology-group>
```

Response Body

None

The following example uses the DELETE option to remove Topology group master VLAN.

URI

http://host:443/restconf/data/brocade-topology-group:topology-group=%topology-group-id%

Request Body

None

Response Body

None

threshold-monitor

Configures the various threshold-monitor parameters.

Resource URIs

URI	Description
<base_URI>/config/running/threshold-monitor	Configure Threshold Monitoring parameters.

GET URIs	Description
<base-uri>/config/running/threshold-monitor/hardware-resources	Retrieves the global values for *count* and *interval*. These constraints can be summarized as *Generate a maximum of {count} messages in {interval} units of time.*
<base-uri>/config/running/threshold-monitor/bfd-sessions	Retrieves the configuration for monitoring BFD sessions.
<base-uri>/config/running/threshold-monitor/ecmp	Retrieves the configuration for monitoring ECMP Table resource utilization.
<base-uri>/config/running/threshold-monitor/host	Retrieves the configuration for monitoring Host Table resource utilization.
<base-uri>/config/running/threshold-monitor/lif	Retrieves the configuration for monitoring LIFs
<base-uri>/config/running/threshold-monitor/mac-table	Retrieves the configuration for monitoring MAC Table resource utilization.
<base-uri>/config/running/threshold-monitor/nexthop	Retrieves the configuration for monitoring Nexthop Table resource utilization.
<base-uri>/config/running/threshold-monitor/route	Retrieves the configuration for monitoring Route Table resource utilization.
<base-uri>/config/running/threshold-monitor/vxlan-tunnel	Retrieves the configuration for monitoring the number of open VXLAN Tunnels.
<base-uri>/config/running/threshold-monitor/acl	Retrieves the configuration for monitoring the various ACL resource usage.
<base-uri>/config/running/threshold-monitor/acl/ip-in	Retrieves the configuration for monitoring the number of available filters for IPv4 Ingress ACLs.
<base-uri>/config/running/threshold-monitor/acl/ip-out	Retrieves the configuration for monitoring the number of available filters for IPv4 Egress ACLs.
<base-uri>/config/running/threshold-monitor/acl/ipv6-in	Retrieves the configuration for monitoring the number of available filters for IPv6 Ingress ACLs.
<base-uri>/config/running/threshold-monitor/acl/ipv6-out	Retrieves the configuration for monitoring the number of available filters for IPv6 Egress ACLs.

GET URIs	Description
<base-uri>/config/running/threshold-monitor/acl/mac-in	Retrieves the configuration for monitoring the number of available filters for MAC Ingress ACLs.
<base-uri>/config/running/threshold-monitor/acl/mac-out	Retrieves the configuration for monitoring the number of available filters for MAC Egress ACLs.

PUT URIs	Payload	Description
<base_URI>/config/running/threshold-monitor/hardware-resources	<hardware-resources> <count>{max-number-of-generated-events}</count> <interval>{time-interval-in-seconds}</interval> </hardware-resources>	Configures the global values for the count and interval. When configured, these constraints can be summarized as: *Generate a maximum of {max-number-of-generated-events} messages in {time-interval-in-seconds} units of time.*
<base_URI>/config/running/threshold-monitor/bfd-session	<bfd-session> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </bfd-session>	Configures the monitoring of BFD Sessions.
<base_URI>/config/running/threshold-monitor/ecmp	<ecmp> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </ecmp>	Enables monitoring of ECMP Table resource utilization.
<base_URI>/config/running/threshold-monitor/host	<host> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </host>	Enables monitoring of Host Table resource utilization.
<base_URI>/config/running/threshold-monitor/lif	<lif> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </lif>	Enables monitoring of LIFs.
<base_URI>/config/running/threshold-monitor/mac-table	<mac-table> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </mac-table>	Enables monitoring of MAC Table resource utilizations.

PUT URIs	Payload	Description
<base_URI>/config/running/threshold-monitor/nexthop	<nexthop> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </nexthop>	Enables monitoring of Nexthop table entries and table's resource utilization.
<base_URI>/config/running/threshold-monitor/route	<route> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </route>	Enables monitoring of Route table entries and table's resource utilization.
<base_URI>/config/running/threshold-monitor/vxlan-tunnel	<vxlan-tunnel> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </vxlan-tunnel>	Enables monitoring of the number of open VXLAN Tunnels.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ip-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ip-in> </acl>	Enables monitoring of the available filters when configuring IP Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ip-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ip-out> </acl>	Enables monitoring of the available filters when configuring IP Egress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ipv6-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ipv6-in> </acl>	Enables monitoring of the available filters when configuring IPv6 Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ipv6-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ipv6-out> </acl>	Enables monitoring of the available filters when configuring IPv6 Egress ACLs.

PUT URIs	Payload	Description
<base-uri>/config/running/threshold-monitor/alc	<acl> <mac-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <mac-in> </acl>	Enables monitoring of the available filters when configuring MAC Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <mac-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <mac-out> </acl>	Enables monitoring of the available filters when configuring MAC Egress ACLs.

PATCH URIs	Payload	Description
<base_URI>/config/running/threshold-monitor/hardware-resources	<hardware-resources> <count>{max-number-of-generated-events}</count> <interval>{time-interval-in-seconds}</interval> </hardware-resources>	Configures the global values for the count and interval. When configured, these constraints can be summarized as: *Generate a maximum of {max-number-of-generated-events} messages in {time-interval-in-seconds} units of time.*
<base_URI>/config/running/threshold-monitor/bfd-session	<bfd-session> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </bfd-session>	Configures the monitoring of BFD Sessions.
<base_URI>/config/running/threshold-monitor/ecmp	<ecmp> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </ecmp>	Enables monitoring of ECMP Table resource utilization.
<base_URI>/config/running/threshold-monitor/host	<host> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </host>	Enables monitoring of Host Table resource utilization.
<base_URI>/config/running/threshold-monitor/lif	<lif> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </lif>	Enables monitoring of LIFs.

PATCH URIs	Payload	Description
<base_URI>/config/running/threshold-monitor/mac-table	<mac-table> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </mac-table>	Enables monitoring of MAC Table resource utilizations.
<base_URI>/config/running/threshold-monitor/nexthop	<nexthop> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </nexthop>	Enables monitoring of Nexthop table entries and table's resource utilization.
<base_URI>/config/running/threshold-monitor/route	<route> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </route>	Enables monitoring of Route table entries and table's resource utilization.
<base_URI>/config/running/threshold-monitor/vxlan-tunnel	<vxlan-tunnel> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> </vxlan-tunnel>	Enables monitoring of the number of open VXLAN Tunnels.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ip-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ip-in> </acl>	Enables monitoring of the available filters when configuring IP Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ip-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ip-out> </acl>	Enables monitoring of the available filters when configuring IP Egress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ipv6-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ipv6-in> </acl>	Enables monitoring of the available filters when configuring IPv6 Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <ipv6-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <ipv6-out> </acl>	Enables monitoring of the available filters when configuring IPv6 Egress ACLs.

PATCH URIs	Payload	Description
<base-uri>/config/running/threshold-monitor/alc	<acl> <mac-in> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <mac-in> </acl>	Enables monitoring of the available filters when configuring MAC Ingress ACLs.
<base-uri>/config/running/threshold-monitor/alc	<acl> <mac-out> <high-limit>{high-limit-value}</high-limit> <low-limit>{low-limit-value}</low-limit> <actions>{action}</actions> <mac-out> </acl>	Enables monitoring of the available filters when configuring MAC Egress ACLs.

Delete URIs
<base-uri>/config/running/threshold-monitor/hardware-resources
<base-uri>/config/running/threshold-monitor/hardware-resources/count
<base-uri>/config/running/threshold-monitor/hardware-resources/interval
<base-uri>/config/running/threshold-monitor/bfd-sessions
<base-uri>/config/running/threshold-monitor/ecmp
<base-uri>/config/running/threshold-monitor/host
<base-uri>/config/running/threshold-monitor/lif
<base-uri>/config/running/threshold-monitor/mac-table
<base-uri>/config/running/threshold-monitor/mac-table
<base-uri>/config/running/threshold-monitor/nexthop
<base-uri>/config/running/threshold-monitor/route
<base-uri>/config/running/threshold-monitor/vxlan-tunnel
<base-uri>/config/running/threshold-monitor/acl
<base-uri>/config/running/threshold-monitor/acl/ip-in
<base-uri>/config/running/threshold-monitor/acl/ip-out
<base-uri>/config/running/threshold-monitor/acl/ipv6-in
<base-uri>/config/running/threshold-monitor/acl/ipv6-out
<base-uri>/config/running/threshold-monitor/acl/mac-in
<base-uri>/config/running/threshold-monitor/acl/mac-out

Parameters

count *max-number-of-generated-events*

Configures the maximum number of events that are generated for the configured time interval. The range is 1-60 events. The default is 4 events.

interval *interval-in-seconds*

Specifies the time interval during which events are generated. The range is 30-900 seconds. The default value is 30 seconds.

high-limit *high-limit-value*

Configures the upper threshold limit of the monitored event that will trigger the configured action.

low-limit *low-limit-value*

Configures the lower threshold limit of the monitored event that will trigger the configured action.

action [*none* | *raslog* | *snmp* | *all*]

Specifies the action to be taken when a threshold is crossed. The values supported are `all`, `none`, `raslog`, and `snmp`. Default is `all`.

all

RASLOG and SNMP trap will be sent when the threshold is crossed.

none

No action will be taken when the threshold is crossed.

raslog

Only RASLOG will be sent when the threshold is crossed.

snmp

SNMP traps will be sent when the threshold is crossed.

Usage Guidelines

GET, PUT, PATCH, and DELETE operations are supported.

Examples

The following example uses the PATCH option to update the configuration details.

URI

http://host:80/rest/config/running/threshold-monitor

```
curl -v -X PATCH -d
"<mac-table><high-limit>95</high-limit><low-limit>80</low-limit><actions>raslog</actions>
<count>2</count><interval>60</interval></mac-table>"
curl -v -X PATCH -d
"<bfd-session><high-limit>85</high-limit><low-limit>60</low-limit><actions>snmp</actions>
<count>2</count><interval>60</interval></bfd-session>"
curl -v -X PATCH -d
"<vxlan-tunnel><high-limit>95</high-limit><low-limit>90</low-limit><actions>all</actions>
<count>2</count><interval>60</interval></vxlan-tunnel>"
curl -v -X PATCH -d
"<lif><high-limit>65</high-limit><low-limit>50</low-limit><actions>all</actions>
<count>2</count><interval>60</interval></lif>"
 curl -v -X PATCH -d
"<hardware-resources><count>90</count><interval>60</interval></hardware-resources>"
```

tpvm

Configures the various TPVM parameters.

Resource URIs

URI	Description
<base_URI>/config/running/tpvm	Configure TPVM parameters.

PUT URIs	Payload	Description
<base_URI>/config/running/tpvm/TPVM/interface/management/ipv6	<ipv6><dhcpv6>true</dhcpv6></ipv6>	Configures enabling DHCP for assigning IPv6 address for the management interface (eth0) of the TPVM.
<base_URI>/config/running/tpvm/TPVM/interface/management/ipv6	<ipv6-params><ipv6addr><ipv6-address-and-mask></ipv6addr><gw><gw-ipv6-address> </gw></ipv6-params>	Configures the IPv6 address and gateway for the management interface (eth0) of the TPVM.
<base_URI>/config/running/tpvm/TPVM/dns	<dns> <dns-params><primary-server><ipv6-address> </primary-server><secondary-server><ipv6-address> </secondary-server><domain>domain-name</domain> </dns-params> </dns>	Configures the primary and secondary DNS servers for the management interface (eth0) of the TPVM. Also configures the domain name.
<base_URI>/config/running/tpvm/TPVM/ntp	<ntp> <server><host-name></server><server><ipv4-address></server> <server><ipv6-address></server>	Configures the NTP servers for use with this TPVM instance. Up to 5 NTP servers can be configured. NTP servers can be configured as IPv4 or IPv6 address formats or as FQDNs.
<base_URI>/config/running/tpvm/TPVM/trusted-peer	<trusted-peer><pwless> <ipv6><ipv6-address></ipv6><password><password></password></pwless><sudo-user><sudo-user-account></sudo-user> </trusted-peer>	Configures the trusted peer and sets its access credentials.

PUT URIs	Payload	Description
<base_URI>/config/running/tpvm/TPVM/ldap/ca-cert/import	<import> <protocol></protocol-to-use> <user><user-name></user> <ldap-password><password></ldap-password> <ldap-host><hostname:ip-address></ldap-host> <directory><remote-directory></directory> <filename><cert-file-name></filename> </import>	Imports a particular certificate from a remote LDAP server.
<base_URI>/config/running/tpvm/TPVM/ldap/ldap-server/ldap-server-options	<ldap-server> <host><hostname:ip-address></host> <port><port-number></port> </ldap-server>	Configures a LDAP server using either its FQDN or using its IPv4 or IPv6 address.

PUT URIs	Payload	Description
<base_URI>/config/running/tpvm/upgrade	<upgrade> <protocol><protocol-to-use></protocol> <user><user-name></user> <password><password></password> <host><host-ip-address></host> <directory><remote-directory></directory> <filename><image-file-name></filename> </upgrade>	Configures the parameters to upgrade TPVM.
<base_URI>/config/running/tpvm/download	<download> <protocol><protocol-to-use></protocol> <user><user-name></user> <password><password></password> <host><host-ip-address></host> <directory><remote-directory></directory> <filename><image-file-name></filename>	Configures the parameters to download a TPVM image file.

Parameters

ipv6params

ipv6addr *ipv6-address-and-mask*

The IPv6 address and mask to be configured on the management interface (eth0) of the TPVM.

gw *gw-ipv6-address*

The IPv6 address of the default gateway.

dns

dns-params

primary-server *ipv6-address*

The IPv6 address of the primary DNS server.

secondary-server *ipv6-address*

The IPv6 address of the secondary DNS server.

domain *domain-name*

The domain of this instance of TPVM.

ntp

server *host-name*

The hostname of a NTP server.

server *ipv4-address*

The IPv4 address of a NTP server

server *ipv6-address*

The IPv6 address of a NTP server

trusted-peer

pwless

ipv6 *ipv6-address*

The IPv6 address of the trusted-peer.

password *password*

The password for the trusted-peer device.

sudo-user *sudo-user-account*

The account used to become the SUDO user on the trusted-peer device.

upgrade

protocol *protocol-to-use*

The protocol to use to access the remote download server.

user *user-name*

The account used to access the remote download server.

password *password*

The password for the account used to access the remote download server.

host *host-ip-address*

The IP address of the remote download server which contains the TPVM image.

directory *remote-directory*

The directory on the remote download server where the TPVM image is stored.

filename *image-file-name*

The filename of the TPVM image.

import

protocol *protocol-to-use*

The protocol to use to access the remote LDAP server.

user *user-name*

The account used to access the remote LDAP server.

ldap-password *password*

The password for the account used to access the remote LDAP server.

ldap-host *hostname:ip-address*

The FQDN hostname or IPv4/IPv6 address of the remote LDAP server which contains the certificate.

directory *remote-directory*

The directory on the remote LDAP server where the certificate is stored.

filename *cert-file-name*

The filename of the certificate to be downloaded.

ldap-server

host *hostname:ip-address*

The FQDN hostname or IPv4/IPv6 address of the remote LDAP server.

port *port-number*

The port number on which the LDAP server can be found.

download

protocol *protocol-to-use*

The protocol to use to access the remote download server.

user *user-name*

The account used to access the remote download server.

password *password*

The password for the account used to access the remote download server.

host *host-ip-address*

The IP address of the remote download server which contains the TPVM image.

directory *remote-directory*

The directory on the remote download server where the TPVM image is stored.

filename *image-file-name*

The filename of the TPVM image.

Usage Guidelines

PUT and PATCH operations are supported.

Examples

The following example shows the setting of the DHCPv6 option for IPv6 address assignment to the management interface of the TPVM.

URI

http://host:80/rest/config/running/tpvm

```
curl -v -X PATCH
-d "<ipv6><dhcpv6>true</dhcpv6></ipv6>"
-u admin:password http://10.20.246.30:80/rest/config/running/tpvm/TPVM/interface/
management/ipv6 -k -v
```

The following example shows manual assignment of IPv6 address to the management interface of the TPVM.

```
 curl -v -X PATCH
-d "<ipv6-params><ipv6addr>23::54/24</ipv6addr><gw>12:23::5:32</gw></ipv6-params<"
-u admin:password http://10.20.246.30:80/rest/config/running/tpvm/TPVM/interface/
management/ipv6/ -k -v
```

The following example shows the configuration of a trusted peer.

```
 curl -v -X PATCH
-d "<pwless><ipv6>12:3::65:76</ipv6><password>welcome123</password></pwless>"
-u admin:password http://10.20.246.30:80/rest/config/running/tpvm/TPVM/trusted-peer/ -k -v

curl -v -X PATCH -d "<trusted-peer><sudo-user>extrenetwo</sudo-user></trusted-peer>" -u
admin:password http://10.20.246.30:80/rest/config/running/tpvm/TPVM/trusted-peer/ -k -v

admin:password http://10.20.246.30:80/rest/config/running/tpvm/TPVM/interface/management/
ipv6/ -k -v
```

username

Manages username and other related settings for the system default accounts, *root*, *admin*, *user*, and other user created accounts.

Resource URIs

URI	Description
/rest/config/running/data/username	Username configuration and management.

POST URIs	Payload	Description
/rest/config/running/data/username	<name> <{name}> </name> <password> <{password}> </password> <role> <{role}> </role>	Configures the username, password, and role for a user account. The system default accounts, *root*, *admin*, *user*, and user defined accounts can be configured.

DELETE URIs
/rest/config/running/data/username

Usage Guidelines

POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Parameters

`name`

The name of the user account being configured. Can be one of the system default accounts, *root*, *admin* and *user*. User created accounts can also be manged through this REST call.

`password`

The password for the account being managed.

`role`

The role of the account being managed.

Examples

The following example configures the system default *admin* account for the device.

URI

http://host:80/rest/config/running/username

Request Body

```
<name>
    admin
</name>
<password>
    passwordadmin
</password>
<role>
    admin
</role>
```

Response Body

None

vrf

Configures, modifies, or retrieves VRF configurations.

Resource URIs

URI	Description
/restconf/data/brocade-vrf:vrf	VRF configurations.

GET URIs	Description
/restconf/data/brocade-vrf:vrf	VRF configurations.
/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast	Retrieves IPv4 address family configurations.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast/max-route	Retrieves IPv4 address family max route.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ipv6/unicast	Retrieves IPv6 address family configurations.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ipv6/unicast/max-route	Retrieves IPv6 address family max route.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast/import	Imports a map.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast/export	Exports a map.
/restconf/data/brocade-vrf:vrf=%vrf-name%/ip/vrf-router-id	Retrieves IP route details.

POST URIs	Payload	Description
/restconf/data/brocade-vrf:vrf	<vrf>(name)</vrf>	Configures VRF.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ipv4	<unicast />	Configures unicast IPv4 address family.
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family//ipv6	<unicast />	Configures unicast IPv6 address family.

PUT URIs	Payload	Description
/restconf/data/brocade-vrf:vrf=%vrf-name%/ip/vrf-router-id	<router-id>(ip-address)</router-id>	Configures IP route.
/restconf/data/brocade-vrf:vrf=%vrf-name%/	<max-route>(unit32)</max-route>	Configures unicast IPv4 address family max-route.

PUT URIs	Payload	Description
address-family/ip/unicast/ max-route		
/restconf/data/brocade-vrf:vrf=%vrf-name%/ address-family/ipv6/ unicast/max-route	<max-route>(unit32)</max-route>	Configures unicast IPv6 address family max route.

DELETE URIs
/restconf/data/brocade-vrf:vrf=%vrf-name%
/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ip/unicast/max-route
/restconf/data/brocade-vrf:vrf=%vrf-name%/address-family/ipv6/unicast

Parameters

vrf-name

Specifies the VRF name.

rd

Specifies the ASN number.

max-route

Specifies the maximum number of routes.

router-id

Specifies IP address.

Usage Guidelines

GET, POST, PUT, PATCH, DELETE, OPTIONS, and HEAD operations are supported.

Examples

The following example uses the GET option to retrieve the configuration details.

URI

http://host:443/rrestconf/data/brocade-vrf:vrf

Request Body

None

Response Body

```
<vrf xmlns="urn:brocade.com:mgmt:brocade-vrf">
                <vrf-name>%req_val%</vrf-name>
                <address-family>
                    <ip>
                        <unicast>
                            <max-route/>
                        </unicast>
                    </ip>
                </address-family>
            </vrf>
```

The following is an example of the POST operation to add a VRF.

URI

http://host:443/restconf/data/brocade-vrf:vrf

Request Body

```
<vrf>vrf1</vrf>
```

Response Body

None

The following is an example of the DELETE operation to remove a VRF.

URI

http://host:443/restconf/data/brocade-vrf:vrf/vrf-name

Request Body

None

Response Body

None