Cisco Nexus Data Broker Configuration Guide, Release 2.0

First Published: September 30, 2014

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1

Cisco Nexus Data Broker Overview

This chapter contains the following sections:

About Cisco Nexus Data Broker

Visibility into application traffic has traditionally been important for infrastructure operations to maintain security, troubleshooting, and compliance and perform resource planning. With the technological advances and growth in cloud-based applications, it has become imperative to gain increased visibility into the network traffic. Traditional approaches to gain visibility into network traffic are expensive and rigid, making it difficult for managers of large-scale deployments.

Cisco Nexus Data Broker with Cisco Nexus Switches provides a software-defined, programmable solution to aggregate copies of network traffic using Switched Port Analyzer (SPAN) or network Test Access Point (TAP) for monitoring and visibility. As opposed to traditional network taps and monitoring solutions, this packet-brokering approach offers a simple, scalable and cost-effective solution that is well-suited for customers who need to monitor higher-volume and business-critical traffic for efficient use of security, compliance, and application performance monitoring tools.

With the flexibility to use a variety of Cisco Nexus Switches and the ability to interconnect them to form a scalable topology provides the ability to aggregate traffic from multiple input TAP or SPAN ports, and replicate and forward traffic to multiple monitoring tools which may be connected across different switches. Combining the use of Cisco Plug-in for OpenFlow and the Cisco One Platform Kit (onePK) agent to communicate to the switches, Cisco Nexus Data Broker provides advance features for traffic management.

Cisco Nexus Data Broker provides management support for multiple disjointed Cisco Nexus Data Broker networks. You can manage multiple Cisco Nexus Data Broker topologies that may be disjointed using the same application instance. For example, if you have 5 data centers and want to deploy an independent Cisco Nexus Data Broker solution for each data center, you can manage all 5 independent deployments using a single application instance by creating a logical partition (network slice) for each monitoring network.

Cisco Nexus Data Broker provides the following:

- A scalable topology for TAP and SPAN port aggregation.
- Support for Q-in-Q to tag input source TAP and SPAN ports.
- Symmetric load balancing.

- Rules for matching monitoring traffic based on Layer 1 through Layer 4 information.
- The ability to replicate and forward traffic to multiple monitoring tools.
- Time stamping using Precision Time Protocol (PTP).
- Packet truncation beyond a specified number of bytes to discard payload.
- Reaction to changes in the TAP/SPAN aggregation network states.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory using RADIUS or TACACS for authentication, authorization, and accounting (AAA) functions.
- End-to-end path visibility, including both port and flow level statistics for troubleshooting.
- Robust Representational State Transfer (REST) API and a web-based GUI for performing all functions
- Support for Cisco Plug-in for Open Flow, version 1.0 and Cisco One Platform Kit (onePK), version 1.3.0.

With Cisco Nexus Data Broker, you can:

- Classify Switched Port Analyzer (SPAN) and Test Access Point (TAP) ports.
- Add monitoring devices to capture traffic.
- Filter which traffic should be monitored.
- Redirect packets from a single or multiple SPAN or TAP ports to multiple monitoring devices through delivery ports.
- Restrict which users can view and modify the monitoring system.
- Connect to Cisco onePK agents for which Cisco onePK devices have been configured.
- Configure these additional features, depending upon the type of switch:
    - Set VLAN ID on Cisco Nexus 3000 and 3100 Series switches.
    - Symmetric load balancing on Cisco Nexus 3100 Series switches.
    - Q-in-Q on Cisco Nexus 3000 and 3100 Series switches.
    - Timestamp tagging and packet truncation on Cisco Nexus 3500 Series switches.

Supported Web Browsers

The following web browsers are supported for Cisco Nexus Data Broker:

- Firefox 18.x and later versions
- Chrome 24.x and later versions

Note JavaScript 1.5 or a later version must be enabled in your browser.

Guidelines and Limitations

Cisco Nexus Data Broker runs in a Java Virtual Machine (JVM). As a Java-based application, Cisco Nexus Data Broker can run on any x86 server. For best results, we recommend the following:

- One 6-core CPU at 2 GHz or higher.
- A minimum of 8 GB of memory.
- A minimum of 40 GB of free hard disk space must be available on the partition where you will be installing the Cisco Nexus Data Broker application.
- A 64-bit Linux distribution with Java, such as the following:
  - Ubuntu Linux
  - Red Hat Enterprise (RHEL) Linux
  - Fedora Linux
- Java Virtual Machine 1.7.x
- A $JAVA_HOME environment variable in your profile set to the path of the JVM.

CHAPTER 2

Deploying Cisco Nexus Data Broker

This chapter contains the following sections:

Installing Cisco Nexus Data Broker

Installing or Upgrading the Cisco Nexus Data Broker Software

Important There is no direct upgrade path from Cisco XNC Monitor Manager Release 1.0 to Cisco Nexus Data Broker Release 2.0. If you have Cisco XNC Monitor Manager Release 1.0 installed and you want to update to Cisco Nexus Data Broker Release 2.0, you must first upgrade to Cisco XNC Monitor Manager Release 1.5. See the *Cisco Extensible Network Controller Deployment Guide, Release 1.5* for the procedure.

- To complete a new installation of Cisco Nexus Data Broker, see Installing the Cisco Nexus Data Broker Software, on page 6.
- To upgrade Cisco XNC Monitor Manager Release 1.5 or Release 1.6 to Cisco Nexus Data Broker Release 2.0, see Upgrading the Application Software, on page 7.

Installing the Cisco Nexus Data Broker Software

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 If prompted, enter your Cisco.com username and password to log in.

Step 5 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

Step 6 Download the Cisco Nexus Data Broker application bundle.

Step 7 Create a directory in your Linux machine where you plan to install Cisco Nexus Data Broker.
For example, in your Home directory, create `CiscoNDB`.

Step 8 Copy the Cisco Nexus Data Broker zip file into the directory that you created.

Step 9 Unzip the Cisco Nexus Data Broker zip file.
The Cisco Nexus Data Broker software is installed in a directory called `xnc`. The directory contains the following:

- `runxnc.sh` file—The file that you use to launch Cisco Nexus Data Broker.
- `version.properties` file—The Cisco Nexus Data Broker build version.
- `captures` directory—The directory that contains output dump files from analytics run in Cisco Nexus Data Broker.

  Note The `captures` directory is created after you execute the Cisco Nexus Data Broker analytics tool.

- `configuration` directory—The directory that contains the Cisco Nexus Data Broker initialization files.

  This directory also contains the `startup` subdirectory where configurations are saved.

- `bin` directory—The directory that contains the following script:
  - `xnc` file—This script contains the Cisco Nexus Data Broker common CLI.
- `etc` directory—The directory that contains profile information.
- `lib` directory—The directory that contains the Cisco Nexus Data Broker Java libraries.
- `logs` directory—The directory that contains the Cisco Nexus Data Broker logs.

  Note The `logs` directory is created after the Cisco Nexus Data Broker application is started.

- `plugins` directory—The directory that contains the OSGi plugins.
- `work` directory—The webserver working directory.

  Note The `work` directory is created after the Cisco Nexus Data Broker application is started.

Upgrading the Application Software

You can use the **upgrade** command to upgrade a Cisco XNC Monitor Manager Release 1.5 or Release 1.6 installation to Cisco Nexus Data Broker Release 2.0. This upgrade is called an in-place upgrade, which means that the product bits are replaced. A backup archive is created to restore your original installation, if necessary.

When you execute the **upgrade** command, the installation and the configuration are upgraded. However, any changes you made to the shell scripts or configuration files, for example, `runxnc.sh` and `config.ini`, are overwritten. After you complete the upgrade process, you must manually reapply your changes to those files.

Before You Begin

- If you have upgraded from Cisco XNC Monitor Manager Release 1.5 to Cisco XNC Monitor Manager Release 1.6, reset the password, start the controller and save the configuration using the **Save** button at the top of the menu bar in the Cisco XNC Monitor Manager GUI.
- Stop all controller instances that use the Cisco XNC Monitor Manager 1.5 or 1.6 installation. This will avoid conflicts with the file system, which is updated during upgrade.
- If you are using high availability clustering, stop all application instances in the cluster to ensure that there are no inconsistencies.
- Back up your `config.ini` and `runxnc.sh` files.

Important You should manually backup your `config.ini` and `runxnc.sh` files before upgrading, because the backup process does not back them up for you. If you do not backup your files before upgrading, any changes you made will be lost.

Step 1 In a web browser, navigate to Cisco.com.

Step 2 Under **Support**, click **All Downloads**.

Step 3 In the center pane, click **Cloud and Systems Management**.

Step 4 In the right pane, click **Network Controllers and Applications**, and then click **Cisco Nexus Data Broker.**

Step 5 Download the Cisco Nexus Data Broker Release 2.0 application bundle.

Step 6 Create a temporary directory in your Linux machine where you plan to upgrade to Cisco Nexus Data Broker. For example, in your `Home` directory, create `CiscoNDB_Upgrade`.

Step 7 Extract the Cisco Nexus Data Broker Release 2.0 zip file into the temporary directory that you created.

Step 8 Navigate to the `xnc` directory that was created when you installed the Cisco XNC Monitor Manager Release 1.5 or 1.6 software.

Step 9 Stop all running release 1.5 or release 1.6 processes.

Step 10 Backup your release 1.5 or release 1.6 installation using your standard backup procedures.

Step 11 Navigate to the `xnc/bin` directory in the temporary directory that you created for the Cisco Nexus Data Broker Release 2.0 upgrade software.

Step 12 Upgrade the application by entering the **./xnc upgrade --perform --target-home** {*xnc_directory_to_be_upgraded*} **[--verbose] [--backupfile** {*xnc_backup_location_and_zip_filename*}**]** command.

You can use one of the following options:

Option	Description
--perform --target-home {*xnc_directory_to_be_upgraded*}	Upgrades the Cisco XNC Monitor Manager installation to Cisco Nexus Data Broker.
--perform --target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Upgrades the Cisco XNC Monitor Manager installation to Cisco Nexus Data Broker and creates a backup .zip file in the directory path that you set. **Note** You must provide the name of the backup file and the .zip extension.
--rollback --target-home {*xnc_directory_to_be_upgraded*}	Rolls back to the previous Cisco XNC Monitor Manager installation.
--rollback --target-home {*xnc_directory_to_be_upgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*}	Rolls back to the previous Cisco XNC Monitor Manager installation using the backup file in the absolute path that you set.
--verbose	Displays detailed information to the console. This option can be used with any other option and is disabled by default.
--validate --target-home {*xnc_directory_to_be_upgraded*}	Validates the installation.
./xnc help upgrade	Displays the options for the **upgrade** command.

Step 13 Navigate to the `xnc` directory where you originally installed Cisco XNC Monitor Manager.

Step 14 Start the application processes that you previously stopped.

Note Press Ctrl–F5, or press the Cmd, Shift, and R keys simultaneously when you access Cisco Nexus Data Broker through a web UI following an upgrade.

Step 15 If you have any upgrade-related issues, perform the following tasks:

a) Stop all application processes.

b) Navigate to the temporary directory that you created in Step 6.

c) Enter the **./xnc upgrade --rollback --target-home** {*xnc_directory_to_be_downgraded*} **--backupfile** {*xnc_backup_location_and_zip_filename*} **[--verbose]** command.

d) Restart the application processes.

Note Press Ctrl–F5, or press the Cmd, Shift, and R keys simultaneously when you access Cisco XNC Monitor Manager through a web UI following a rollback.

Starting the Application

Step 1 (Optional) Navigate to the `xnc/bin` directory.

Step 2 (Optional) Change the default password supplied with Cisco Nexus Data Broker by entering the **./xnc reset-admin-password [--wait-seconds** {*wait_time*} **--password** {*password*}**]** command.
The {*password*} variable resets the administrator password to the value that you specify by restarting the user manager. The {*wait_time*} is the number of seconds to wait while the user manager restarts. The minimum {*wait_time*} value is 5 seconds and the maximum is 60 seconds.

Note
- The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one nonalphanumeric character.
- If you leave the password blank, it is reset to the factory default of "admin".
- Each time that you reset the administrative password, make sure that the new password meets these requirements or you will not be able to log in to Cisco Nexus Data Broker.

Step 3 Navigate to the `xnc` directory and start Cisco Nexus Data Broker by entering the **./runxnc.sh** command.
You can use one of the following options:

Option	Description
no option	Starts Cisco Nexus Data Broker with the **-start** option.
-jmx	Enables Java Management Extensions (JMX) remote access on the Cisco Nexus Data Broker JVM, which can be used to troubleshoot performance issues.
-jmxport *port_number*	Enables JMX remote access on the specified JVM port.
-debug	Enables debugging on the Cisco Nexus Data Broker JVM.
-debugsuspend	Suspends the Cisco Nexus Data Broker startup until a debugger is connected.
-debugport *port_number*	Enables debugging on the specified JVM port.
-start	Starts Cisco Nexus Data Broker and provides Secure Shell (SSH) access on port 2400. **Note** The SSH server can be accessed by any Cisco Nexus Data Broker user with the network-administrator role.
-start *port_number*	Starts Cisco Nexus Data Broker and provides SSH access to the controller on the specified port number. **Note** The SSH server can be accessed by any Cisco Nexus Data Broker user with the network-administrator role. The valid range of values for *port_num* is 1024 through 65535.
-stop	Stops Cisco Nexus Data Broker.
-status	Displays the status of Cisco Nexus Data Broker.

Option	Description
-console	Starts Cisco Nexus Data Broker with the OSGi console.
-help	Displays the options for the **./runxnc.sh** command.
-tls	Enables TLS secure connections between Cisco Nexus Data Broker and OpenFlow or onePK switches. To enable TLS, start the controller by entering the **./runxnc.sh -tls -tlskeystore** *keystore_file_location* **-tlstruststore** *truststore_file_location* command.

Verifying That the Application is Running

Step 1 Open a command window where you installed Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc` directory that was created when you installed the software.

Step 3 Verify that the application is running by entering the **./runxnc.sh -status** command.
The controller outputs the following, which indicates that the controller is running the Java process with PID 21680:

```
Controller with PID:21680 -- Running!
```

What to Do Next

Connect the switches to the controller. For more information, see the configuration guide for your switches.

CHAPTER 3

Managing TLS Certificate, KeyStore, and TrustStore Files

This chapter contains the following sections:

About the TLS Certificate, KeyStore, and TrustStore Files

Note To support onePK devices, all connections to Cisco Nexus Data Broker that use onePK or OpenFlow agents require Transport Layer Security (TLS).

Enabling the TLS connections between Cisco Nexus Data Broker and the OpenFlow or onePK switches requires TLS KeyStore and TrustStore files. The TLS KeyStore and TLS TrustStore files are password protected.

Cisco Nexus 3000, 3100, and 3500 Series switches require additional credentials, including Private Key, Certificate, and Certificate Authority (CA).

- The TLS KeyStore file contains the private key and certificate information used by Cisco Nexus Data Broker.

- The TLS TrustStore file contains the Certification Authority (CA) certificates used to sign the certificates on the connecting switches.

If TLS connections are required in your Cisco Nexus Data Broker implementation, all of the connections in the network must be TLS encrypted, and you must run Cisco Nexus Data Broker with TLS enabled (see Starting the Application with TLS Enabled , on page 19). After Cisco Nexus Data Broker is started with TLS, you must run the TLS KeyStore password configuration command (see Providing the TLS KeyStore and TrustStore Passwords, on page 20) to provide the passwords for Cisco Nexus Data Broker to unlock the KeyStore files.

Preparing to Generate the TLS Credentials

OpenFlow and Cisco onePK switches require cryptographic configuration to enable TLS.

Caution Self-signed certificates are appropriate only for testing in small deployments. For additional security, as well as more granular controls over individual certificate use and revocation, you should use certificates generated by your organization's Certificate Authority. In addition, you should never use the keys and certificates generated by this procedure in a production environment.

Before You Begin

Ensure that OpenSSL is installed on the Linux host where these steps will be performed.

Step 1 Create a TLS directory, and then navigate to it:
mkdir -p TLS

cd TLS

Step 2 Create three directories under `mypersonalca` and two prerequisite files:
mkdir -p mypersonalca/certs

mkdir -p mypersonalca/private

mkdir -p mypersonalca/crl

echo "01" > mypersonalca/serial

touch mypersonalca/index.txt

Step 3 Create the CA configuration file (ca.cnf).
The following is an example of the content of the ca.cnf file:

```
[ ca ]
default_ca = mypersonalca

[ mypersonalca ]
#
# WARNING: if you change that, change the default_keyfile in the [req] section below too
# Where everything is kept
dir = ./mypersonalca

# Where the issued certs are kept
```

```
certs = $dir/certs

# Where the issued crl are kept
crl_dir = $dir/crl

# database index file
database = $dir/index.txt

# default place for new certs
new_certs_dir = $dir/certs

#
# The CA certificate
certificate = $dir/certs/ca.pem

# The current serial number
serial = $dir/serial

# The current CRL
crl = $dir/crl/crl.pem

# WARNING: if you change that, change the default_keyfile in the [req] section below too
# The private key
private_key = $dir/private/ca.key

# private random number file
RANDFILE = $dir/private/.rand

# The extentions to add to the cert
x509_extensions = usr_cert

# how long to certify for
default_days = 365

# how long before next CRL
default_crl_days= 30

# which md to use; people in comments indicated to use sha1 here
default_md = sha1

# keep passed DN ordering
preserve = no

# Section names
policy = mypolicy
x509_extensions = certificate_extensions

[ mypolicy ]
# Use the supplied information
commonName = supplied
stateOrProvinceName = optional
countryName = optional
emailAddress = optional
organizationName = optional
```

```
organizationalUnitName = optional

[ certificate_extensions ]
# The signed certificate cannot be used as CA
basicConstraints = CA:false

[ req ]
# same as private_key
default_keyfile = ./mypersonalca/private/ca.key

# Which hash to use
default_md = sha1

# No prompts
prompt = no

# This is for CA
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer
string_mask = utf8only
basicConstraints = CA:true
distinguished_name = root_ca_distinguished_name
x509_extensions = root_ca_extensions

[ root_ca_distinguished_name ]
# EDIT THOSE
commonName = Controller
stateOrProvinceName = Mass
countryName = US
emailAddress = root_ca_userid@cisco.com
organizationName = Cisco

[ root_ca_extensions ]
basicConstraints = CA:true
```

What to Do Next

Create the TLS certificate file.

Creating the TLS Private Key, Certificate, and Certification Authority

Before You Begin

Complete the steps in Preparing to Generate the TLS Credentials, on page 12.

Step 1 Generate the TLS private key and Certification Authority (CA) files by entering the **openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -out mypersonalca/certs/ca.pem -outform PEM -keyout mypersonalca/private/ca.key** command.
This step generates the TLS private key in PEM format with a key length of 2048 bits, and the CA file.

Step 2 Generate the certificate key and certificate request files by entering the **openssl req -newkey rsa:2048 -keyout cert.key -keyform PEM -out cert.req -outform PEM** command.
This step generates the controller key (cert.key) and certificate request (cert.req) files in PEM format.

Important You must specify a PEM pass phrase that is 4 to 1024 alphanumeric characters in length, for example, cisco123.

You must also specify a common name in this step to complete Step 3. An example of a common name is the hostname of the server where Cisco Nexus Data Broker is running.

Step 3 Generate the certificate file by entering the **openssl ca -batch -notext -in cert.req -out cert.pem -config ca.cnf** command.
This step generates the certificate (cert.pem) file in PEM format using the certificate request (cert.req) and the certificate configuration (ca.cnf) files as inputs, and creates the certificates file (cert.pem) as output.
The following is an example of the console response:

```
Using configuration from ca.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'AU'
stateOrProvinceName   :ASN.1 12:'Some-State'
organizationName      :ASN.1 12:'Internet Widgits Pty Ltd'
commonName            :ASN.1 12:'localhost'
```

What to Do Next

Generate and import the certificate files on your Cisco Nexus 3000, 3100, or 3500 Series switches.

Configuring the Cryptographic Keys on the Switch

Before You Begin

Create the TLS certificate.

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch(config)# **ip domain-name** *domain-name*	Configures the domain name for the switch.
Step 2	switch(config)# **crypto key generate rsa label myKey2 exportable modulus 2048**	Generates the cryptographic key.
Step 3	switch(config)# **crypto ca trustpoint myCA**	Enters the trustpoint configuration mode and installs the trustpoint file on the switch.
Step 4	switch(config-trustpoint)# **rsakeypair myKey2**	Installs the key files on the switch.
Step 5	switch(config-trustpoint)# **exit**	Exits trustpoint configuration mode.
Step 6	switch# **show crypto ca trustpoints**	(Optional) Verifies creation of the trustpoint files.
Step 7	switch# **show crypto key mypubkey rsa**	(Optional) Verifies creation of the key files.
Step 8	From the console, enter the **cat mypersonalca/certs/ca.pem** command.	Displays the certificate file on the machine hosting the generated TLS certificates.
Step 9	switch(config)# **crypto ca authenticate myCA**	Copies the CA certificate (`ca.pem`) to the switch to use as input. **Note** When copying the CA certificate, include the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`. End the input with a line that contains only `END OF INPUT`.
Step 10	switch(config)# **crypto ca enroll myCA**	Generates the certificate request on the switch.
Step 11	From the console, enter the **openssl ca -in n3k-cert.req -out newcert.pem -config ./ca.cnf** command.	Copies the certificate request from the switch to the file `n3k-cert.req` on your Linux machine, and then uses it to generate the switch certificate.
Step 12	switch(config)# **crypto ca import myCA certificate**	Copies the certificate (`newcert.pem`) to the switch.
Step 13	From the console, enter the **cat newcert.pem** command.	Displays the certificate on the Linux console.
Step 14	switch# **show crypto ca certificates**	Displays the certificates on the switch.

What to Do Next

Enable TLS for Cisco onePK and OpenFlow switches.

Enabling TLS for onePK and OpenFlow Switches

Before You Begin

- Create the TLS certificate.
- Configure the cryptographic keys on the switch.

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch(config)# **onep**	Enters onePK configuration mode on the switch.
Step 2	switch(config-onep)# **transport type tls**	Enables TLS for onePK switches.
Step 3	switch# **exit**	Exits onePK configuration mode.
Step 4	switch# **show onep status**	(Optional) Displays the onePK configuration.
Step 5	switch(config)# **openflow**	Enters OpenFlow agent configuration mode on the switch.
Step 6	switch(config-ofa)# **switch 1**	Enters OpenFlow agent configuration mode for switch 1.
Step 7	switch(config-ofa)# **tls trust-point local myCA remote myCA**	Enables TLS certificate authority on the switch.
Step 8	switch(config-ofa-switch)# **pipeline** {*201*/*203*}	Configures the pipeline. **Note** Set the pipeline to **201** for Cisco Nexus 3000 and 3100 Series switches. This is the default value, and only expert users should set the number to any value other than 201. Set the pipeline to **203** for Cisco Nexus 3500 Series switches. This is the default value, and only expert users should set the number to any value other than 203.
Step 9	switch(config-ofa-switch)# **controller ipv4** {*A.B.C.D*} **port 6653 vrf management security tls**	Enables TLS for OpenFlow switches. *A.B.C.D* is the IP address of the controller. **Note** For more information about configuring TLS for OpenFlow (Cisco Nexus 3000, 3100, or 3500 Series switches), see the configuration guide for the switches in your environment.

What to Do Next

Create the TLS KeyStore file.

Creating the TLS KeyStore File

Note The TLS KeyStore file should be placed in the `configuration` directory of Cisco Nexus Data Broker.

Before You Begin

Complete the steps in Configuring the Cryptographic Keys on the Switch.

Step 1 Copy `cert.key` to `xnc-privatekey.pem`.
This command copies the `cert.key` file that was generated in the "Creating the TLS Private Key, Certificate, and Certificate Authority" section. This file contains the Cisco Nexus Data Broker private key.

Step 2 Copy `cert.pem` to `xnc-cert.pem`.
This command makes a copy of the `cert.pem` file that was generated in the "Creating the TLS Private Key, Certificate, and Certificate Authority" section. This file contains the Cisco Nexus Data Broker certificate.

Step 3 Create the `xnc.pem` file, which contains the private key and certificate, by entering the **cat xnc-privatekey.pem xnc-cert.pem > xnc.pem** command.

Step 4 Convert the PEM file `xnc.pem` file to the file `xnc.p12` file by entering the **openssl pkcs12 -export -out xnc.p12 -in xnc.pem** command.

Step 5 Enter a password at the prompt.
Note This is the Export password. Use the same password that you entered in Step 2 of "Creating the TLS Private Key, Certificate, and Certification Authority". The password must contain at least 6 characters, for example, **cisco123**. You must use the same password for this step and for Step 7.
The `xnc.pem` file is converted to a password-protected .p12 file.

Step 6 Convert the `xnc.p12` to a Java KeyStore (tlsKeyStore) file by entering the **keytool -importkeystore -srckeystore xnc.p12 -srcstoretype pkcs12 -destkeystore tlsKeyStore -deststoretype jks** command.
This command converts the `xnc.p12` file to a password-protected tlsKeyStore file

Step 7 Enter a password at the prompt.
Note Use the same password that you entered in Step 5.

Creating the TLS TrustStore File

Note The TLS TrustStore file should be placed in the application configuration directory.

Step 1 Copy the `mypersonalca/certs/ca.pem` file to `sw-cacert.pem`.

Step 2 Convert the `sw-cacert.pem` file to a Java TrustStore (tlsTrustStore) file by entering the **keytool -import -alias swca1 -file sw-cacert.pem -keystore tlsTrustStore** command.

Step 3 Enter a password at the prompt.
The `sw-cacert.pem` file is converted into a password-protected Java TrustStore (tlsTrustStore) file.

Note The password must be at least six characters long, for example, **cisco123**.

Step 4 If the switches in your network use more than one CA certificate, repeat Step 1 through Step 3 for each CA certificate required.

Starting the Application with TLS Enabled

Before You Begin

- Generate and import certificate files on the switches.
- Enable TLS on the OpenFlow or onePK switches.
- Create and deploy TLS KeyStore and TLS TrustStore files for the Cisco Nexus Data Broker application.
- Make sure that the TLS KeyStore (tlsKeyStore) and TLS TrustStore (tlsTrustStore) files are located in the `./configuration` directory.

Step 1 From the console, start Cisco Nexus Data Broker by entering the **./runxnc.sh -tls -tlskeystore ./configuration/tlsKeyStore -tlstruststore ./configuration/tlsTrustStore** command.

Note You will not see any network elements until you provide the TLS KeyStore and TrustStore passwords as described in the next section.

Step 2 Cisco Nexus Data Broker is started with TLS enabled.

Providing the TLS KeyStore and TrustStore Passwords

The TLS KeyStore and TrustStore passwords are sent to the Cisco Nexus Data Broker so that it can read the password-protected TLS KeyStore and TrustStore files.

Step 1 Open a command window where you installed Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc/bin` directory.

Step 3 Provide the TLS KeyStore and TLS TrustStore passwords by entering the **./xnc config-keystore-passwords** [**--user** {*user*} **--password** {*password*} **--url** {*url*} **--verbose --prompt --keystore-password** {*keystore_password*} **--truststore-password** {*truststore_password*}] command.
Enter the following information:

- The Cisco Nexus Data Broker username {*user*}—The user name.
- The Cisco Nexus Data Broker password {*password*}—The password for the user. For example, the default admin password is admin.
- The Cisco Nexus Data Broker web URL {*url*}—The web URL of the application. For example, the default URL is `https://Nexus_Data_Broker_IP:8443` or `http://Nexus_Data_Broker_IP:8080`.

  Note Use caution when using HTTP, because this will send your password to the controller in clear text.

- The TLS KeyStore password {*keystore_password*}—The TLS KeyStore password.
- The TLS TrustStore password {*truststore_password*}—The TLS TrustStore password.

CHAPTER 4

Logging in and Managing Cisco Nexus Data Broker

This chapter contains the following sections:

Configuring Cisco Nexus Data Broker

Configuring High Availability Clusters

Cisco Nexus Data Broker supports high availability clustering in active/active mode with up to five controllers. To use high availability clustering with Cisco Nexus Data Broker, you must edit the `config.ini` file for each instance of Cisco Nexus Data Broker.

Before You Begin

- All IP addresses must be reachable and capable of communicating with each other.
- All switches in the cluster must connect to all of the controllers.
- All controllers must have the same HA clustering configuration information in the `config.ini` files.
- All controllers must have the same information in the `xnc/configuration/startup` directory.

- If using cluster passwords, all controllers must have the same password configured in the `xncjgroups.xml` file. See Password Protecting the High Availability Clusters, on page 22.

Step 1 Ensure that Cisco Nexus Data Broker is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 4 Use any text editor to open the `config.ini` file.

Step 5 Locate the following text:

```
# HA Clustering configuration (colon-separated IP addresses of all controllers that are part of the
 cluster.)
# supernodes=<ip1>:<ip2>:<ip3>:<ipn>
```

Step 6 Remove the comments on the # supernodes line, and replace <ip1>:<ip2><ip3>:<ipn> with the IP addresses for each instance of Cisco Nexus Data Broker in the cluster. You can enter from two to five IP addresses.

Example:

```
# HA Clustering configuration (colon-separated IP addresses of all controllers that are part of the
 cluster.)
supernodes=10.1.1.1:10.2.1.1:10.3.1.1:10.4.1.1:10.5.1.1
```

Step 7 Save the file and exit the editor.

Step 8 Repeat Step 3 through Step 7 for each instance of Cisco Nexus Data Broker in the cluster.

Step 9 Restart Cisco Nexus Data Broker.

Password Protecting the High Availability Clusters

You can password protect your HA clusters with the `xncjgroups.xml` file. This file must be exactly the same for each instance of Cisco Nexus Data Broker.

Step 1 Ensure that Cisco Nexus Data Broker is not running on any of the instances in the cluster.

Step 2 Open a command window on one of the instances in the cluster.

Step 3 Navigate to the `xnc/configuration` directory.

Step 4 Use any text editor to open the `xncjgroups.xml` file.

Step 5 Locate the following text:

```
<!-- <AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH> -->
```

Step 6 Remove the comments from the AUTH line.

Example:

```
<AUTH auth_class="org.jgroups.auth.MD5Token" auth_value="ciscoXNC" token_hash="MD5"></AUTH>
```

Step 7 (Optional) Change the password in the auth_value attribute.

By default, the cluster is protected with the password "ciscoXNC". You can change this password to whatever value you want, if you make the same change on all machines in the cluster.

Step 8 Save the file and exit the editor.

Step 9 Repeat Step 4 through Step 8 for each instance of Cisco Nexus Data Broker in the cluster.

Step 10 Restart Cisco Nexus Data Broker.

Editing the Configuration Files for Cisco Nexus Switches

The following configuration settings can improve scalability when connecting to Cisco Nexus 3000 or 3100 Series switch.

Step 1 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 2 Use any text editor to open the `config.ini` file.

Step 3 Update the following parameters:

Name	Predefined Value	Default Value	Recommended Value
of.messageResponseTimer	10000	2000	60000
of.switchLivenessTimeout	—	60500	120500
of.flowStatsPollInterval	120	10	240
of.portStatsPollInterval	300	5	240
of.descStatsPollInterval	—	60	240
of.barrierMessagePriorCount	50	100	50
of.discoveryInterval	—	300	300
of.discoveryTimeoutMultiple	—	2	2

Note Predefined values are the values that Cisco includes in the `config.ini` file that is shipped with Cisco Nexus Data Broker. A em dash ("—") in this column of the table means that unless you explicitly update the value, the default value will be used.

Step 4 Save the file and exit the editor.

Step 5 Restart Cisco Nexus Data Broker.

Configuring User Roles for Edge Ports

To manage which edge ports a Cisco Nexus Data Broker application user can use for creating rules for edge ports, you must modify the App-User role settings in the `config.ini` file to enable role-based access control (RBAC) for application users. After you make your changes and restart Cisco Nexus Data Broker, note these restrictions:

- Cisco Nexus Data Broker App-User role users will be able to create rules only for source ports which are part of the resource group or groups assigned to that role .
- Only Cisco Nexus Data Broker App-Admin role users will be able create rules with no source.

To enable RBAC for the App-User role, follow these steps:

Step 1 Open the `config.ini` file for editing.

Step 2 Locate the line `# Enforce restriction on edge/tap ports user can capture (default false).`

Step 3 Remove the comment character from the following line:
`monitor.strictAuthorization=true`

Step 4 Save your work and close the file.

Step 5 If Cisco Nexus Data Broker is running, restart the application to enable the change.

Logging in to the Cisco Nexus Data Broker GUI

You can log into the Cisco Nexus Data Broker using HTTPS. The default HTTPS web link for the Cisco Nexus Data Broker GUI is `https://Nexus_Data_Broker_IP:8443/monitor`.

Note You must manually specify the https:// protocol in your web browser. The controller must also be configured for HTTPS.

You can log also into the Cisco Nexus Data Broker using HTTP. The default HTTP web link for the Cisco Nexus Data Broker GUI is `http://Nexus_Data_Broker_IP:8080/monitor`.

Note Use caution if you log in with HTTP, because passwords and other sensitive data will be sent in clear text.

Step 1 In your web browser, enter the Cisco Nexus Data Broker web link.

Step 2 On the launch page, do the following:

a) Enter your username and password.

The default username and password is admin/admin.

b) Click **Log In**.

Cisco Nexus Data Broker GUI Overview

The Cisco Nexus Data Broker GUI contains the following areas and panes:

- A menu bar across the top of the window that provides access to the main categories of information in Cisco Nexus Data Broker.
- A topology map on the right that displays a visual representation of your network.
- Several panes with additional views and information about the selected category.

The menu bar contains the following items:

- The **Online help** button—Provides access to the online help for the current page.
- A **Save** button—Enables you to save any additions or changes you make in Cisco Nexus Data Broker.

Note You should always click **Save** after making any configuration changes.

- A **Northbound API** button—Enables you to view northbound API content in a new browser tab, and displays the content and calls.
- The administrative management (**Admin**) drop-down list—Provides access to different tasks, as follows:
  - **Management**—Provides access to manage devices, flows, users, slices, Administration, Authorization, and Authentication (AAA) configuration, view the OSGi console, view cluster information, and to troubleshoot your network.
  - **Settings**—Provides access to create user roles and resource groups, and to assign devices to resource groups.
  - **Logout**—Logs you out of Cisco Nexus Data Broker.

Topology Tools

The left side of the topology pane contains a zoom slider that allows you increase or decrease the size of the topology diagram. You can also increase or decrease the size of the topology diagram by scrolling up or down, respectively, with your mouse wheel.

You can move the entire topology diagram, a single topology element, or a node group. To move the diagram, an element, or a node group, click it and drag it.

To view information about a node or an edge port, hover over the node or edge port icon with your mouse. The information displayed depends on the device you choose.

To view information about a path, hover over the path in the topology diagram.

To view information about a filter, hover over the **Name** of the filter in the **Configure Filters** tab.

Pane Resizing

You can resize the panes in the GUI display by clicking the pane resize grippers as follows:

- To increase or decrease the height of either of the left or right bottom pane, click the pane resize grippers at the top of the pane, and then drag up or down with your mouse.
- To collapse either the lower right or lower left pane, hover over the pane resize grippers at the top of the pane until a double-ended arrow is displayed, and then click your mouse once.
- To restore a collapsed pane, hover over the pane resize grippers at the bottom of the pane until a double-ended arrow is displayed, and then click your mouse once.
- To increase or decrease the width of the two left panes at the same time, click the pane resize grippers at the top of the pane, and then drag left or right with your mouse.

Saving Configuration Changes

You should periodically save the configuration changes that you make in Cisco Nexus Data Broker. Any unsaved configuration changes in Cisco Nexus Data Broker will be lost if you stop the application.

On the menu bar, click **Save**.

CHAPTER 5

Managing Devices

This chapter contains the following sections:

Adding a Node Name

Adding user-friendly node names helps you to identify nodes in the topology diagram.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 3 Click the link for the node that you want to rename in the **Node Name** column.

Step 4 In the **Update Node Information** dialog box, complete the following fields:

Name	Description
Node ID field	The unique identifier for a network element, such as an OpenFlow switch.

Name	Description
Node Name field	The name that you want to assign to the node. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
Tier drop-down list	Choose the tier property for the network element. This can be one of the following: • **Unknown** • **Access** • **Distribution** • **Core**
Operation Mode drop-down list	Choose how the traffic is handled based on the flows. This can be one of the following: • **Allow reactive forwarding—**No default flows are programmed. How traffic that does not match a flow is treated depends upon the switch implementation. • **Proactive forwarding only—**The following default flows are programmed on the switch: ◦ Punt Address Resolution Protocol (ARP) packets. ◦ Punt Link Layer Discovery Protocol (LLDP) packets. ◦ Drop all other traffic.

Step 5 Click **Save**.

Viewing Expanded Nodes Information

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 3 Click the icon in the top right corner.

Step 4 The **Nodes Learned** dialog box displays these nonconfigurable fields:

Name	Description
Node Name field	The name assigned to the node.
Node ID field	The ID of the node.
Tier Name field	The tier that you selected for the node.
MAC Address field	The MAC address of the node.
Ports field	The ports accessible on the node.

Step 5 Click the **X** in the upper right corner of the dialog box to close it.

Viewing the Ports List

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 3 Click the **Ports** link for a node.

Step 4 The **Ports List** dialog box displays all of the ports for the specified node.

Step 5 Click the **X** in the upper right corner of the dialog box to close it.

Adding onePK Devices

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **onePK** tab.

Step 3 Click **Add onePK Device**.

Step 4 In the **Add onePK Device** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.

Name	Description
Username field	The name of the user assigned to the device. **Note** The username that the admin enters in order to connect to the Cisco onePK agent.
Password field	The password of the user assigned to the device. **Note** This is the password that the admin enters in order to connect to the Cisco onePK agent.

Step 5 Click **Add onePK Device**.
The node configuration is added. When a physical device is associated with the address that you entered, a success message is displayed. The address is displayed in blue in the **Network Element Address** list of **onePK Devices** on the **onePK** tab.
When there is no physical device associated with the address that you entered, no connection is made, and a connection timed out error message is displayed. The address is grayed out in the **Network Element Address** list of **onePK Devices** on the **onePK** tab.

Removing onePK Devices

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **onePK** tab.

Step 3 In the **onePK Devices** list, check the check box next to each device that you want to remove, or check the top check box to remove all onePK Devices.

Step 4 Click **Remove onePK Device**.

Step 5 In the **Remove onePK Device** confirmation dialog box, click **Remove onePK Device**.

Adding a Node Group

A node group allows you to visually group nodes in the Cisco Nexus Data Broker topology diagram. Node groups do not create links between nodes.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 3 Click **Add Group**.

Step 4 In the **Add Node Group** dialog box, complete the following field:

Name	Description
Name field	The name that you want to give the node group. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 Click **Add Group**.
The name of the group displays in the list of node groups.

What to Do Next

Add nodes to the node group.

Adding Nodes to a Node Group

Adding nodes to a node group visually associates the nodes with the node group in the topology diagram. Node groups are highlighted in different colors in the diagram.

Note If you add a node that already belongs to a node group to a new node group, it is automatically removed from the first node group and added to the new node group.

Before You Begin

Add a node group.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 3 Click the name of the node group to which to want to add nodes in the **Node Groups** list.

Step 4 Add nodes to the group by doing one of the following:

- Click one or more nodes in the topology diagram, and then click **Add to group <group name>** in the topology diagram.
- Click the **Nodes in Group** tab, and then do the following:

a) In the **Add Nodes to Group - <group name>** dialog box, choose one or more nodes from the drop-down list.
b) Click **Add to group**.

The nodes display in the **Nodes in Group - <group name>** list on the **Nodes in Group** tab, and in the node group in the topology diagram.

Removing Nodes from a Node Group

Before You Begin

Add nodes to a node group.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 3 Click the name of the node group from which to want to remove nodes in the **Nodes Groups** list.

Step 4 To remove nodes from the group, do one of the following:

- Click a node group in the topology diagram, and then:

a) Click the node you want to remove from the group.
b) Click **Remove from group – <group-name>** in the topology diagram.

- Click the **Nodes in Group** tab, and then:

a) Check the check box next to the node or nodes you want to remove in the list of **Nodes in Group <group name>**, or check the top check box in the list to select all nodes in the group for removal.
b) Click **Remove Nodes from <group-name>** .

Step 5 In the **Remove Nodes** confirmation dialog box, click **Remove**.

Removing a Node Group

Removing a node group disassociates the nodes added to it from the node group, and the node group is no longer displayed in the topology diagram.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 3 In the **Node Groups** list, check the check box next to the name of the node group you want to remove, or check the top check box to select all node groups for removal.

Step 4 Click **Remove Group**.

Step 5 In the **Remove Group** confirmation dialog box, click **Remove Group**.
The node group is removed and no longer displays in the topology diagram.

Adding a Gateway IP Address

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 3 Click **Add Gateway IP Address**.

Step 4 In the **Add Gateway IP Address** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the gateway IP address. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
Gateway IP Address/Mask field	The IP address and subnet mask of the default gateway in the following format: *IP_Address/Subnet_Mask* **Note** • If your deployment includes only OpenFlow traffic, the gateway IP address can be set to the same IP address used as the default gateway for the host systems on that subnet. • If your deployment includes OpenFlow and non-OpenFlow traffic, the gateway IP address must be set to an unused IP address on that subnet.

Step 5 Click **Save**.

Removing a Gateway IP Address

Before You Begin

Add one or more gateway IP addresses.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 3 Check the check box next to the name of each gateway IP address you want to remove, or check the top check box to remove all gateway IP address entries.

Step 4 Click **Remove Gateway IP Address**.

Step 5 In the **Remove Gateway IP Address** confirmation dialog box, click **Remove Gateway IP Address**.

Adding Ports

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 3 Click **Add Ports**.

Step 4 In the **Add Ports** dialog box, complete the following fields:

Name	Description
Gateway Name drop-down list	The name of the gateway address to which you want to bind the port.
Node ID drop-down list	The node that contains the port that you want to bind to the gateway address.
Select Port drop-down list	The port that you want to bind to the gateway address.

Step 5 Click **Save**.

CHAPTER 6

Configuring Ports and Devices

This chapter contains the following sections:

About Cisco Nexus Data Broker Port Types

Cisco Nexus Data Broker enables you to configure different port types. All configured ports are displayed in the **Configured Ports** table on the **Port Types** tab.

Edge Ports

Edge ports are the ingress ports where traffic enters the monitor network. Cisco Nexus Data Broker supports the following edge ports:

- TAP ports—For incoming traffic connected to a physical tap wire.
- SPAN ports—For incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Configuring an edge port is optional.

Delivery Ports

Delivery ports are the egress ports where the traffic exits the monitor network. These outgoing ports are connected to external monitoring devices. When you configure a monitoring device in Cisco Nexus Data Broker, you can associate a name and an icon to the monitoring device.

Configured devices are displayed in the **Monitor Devices** table on the **Devices** tab. The icon appears in the topology diagram with a line that connects it to the node.

VLAN Double Tagging

Cisco Nexus Data Broker enables you to configure a switch port as an edge port and specify a VLAN for that port. When you configure the VLAN ID, and the connection to the Cisco onePK agent is up, Cisco Nexus Data Broker programs the Cisco Nexus 3000 or 3100 Series switch so that all packets received in that port are VLAN tagged, and the VLAN ID is the one configured on the edge port. If the packets received in that port are already VLAN-tagged frames, they get double-tagged, and the outermost VLAN tag contains the VLAN ID that is associated with the configured edge port.

Configuring a Port Type

Step 1 In the topology diagram, click the node for which you want to configure a port.
The **Ports** area of the sidebar displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click **Click to configure** under the port identifier of the port that you want to configure.

Step 3 From the **Select a port type** drop-down list, choose one of the following:

- **Edge Port-SPAN**
- **Edge Port-TAP**
- **Monitoring Device**

Edge Port-SPAN—Creates an edge port for incoming traffic connected to an upstream switch that is configured as a SPAN destination.

Edge Port-TAP—Creates an edge port for incoming traffic connected to a physical TAP port.

Monitoring Device—Creates a monitoring device for capturing traffic and configures the corresponding delivery port.

Step 4 (Optional) In the **Port Description** field, enter a port description.
The port description can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 (Optional) Enter a VLAN ID.
The port is configured as dot1q to preserve any production VLAN information.

Step 6 Click **Submit**.

Removing a Port Type Configuration

Before You Begin

- At least one port type must be configured.
- The port type configuration that you want to remove must not be used in a rule. If it is, you must either modify or remove the rule before you can remove the port type configuration.

Step 1 From the **Port Types** tab, choose one of the following:

- The top checkbox to select all **Configured Ports** for removal.
- The check box next to the name of only the configured port or ports that you want to remove.

Step 2 Above the list of **Configured Ports**, click **Remove Port Configuration**.

Step 3 In the **Remove Port Configuration** confirmation dialog box, click **Remove Port Configuration**.
The port configurations are removed.

Configuring a Monitoring Device

Step 1 In the topology diagram, click the node for which you want to configure a monitoring device.
The **Port Types** tab displays the list of ports available to configure for that node.

Step 2 In the list of ports for the node, click **Click to configure** under the port identifier of the port that you want to configure.

Step 3 From the **Select a port type** drop-down list, click **Add Monitoring Device**.

Step 4 In the **Add Device** dialog box, complete the following fields:

Name	Description
Device Name field	The name that you want to use for the monitoring device. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** You can change the device name after the monitoring device has been added.

Name	Description
Icons selection	The choice of icons, with the first one selected by default. Choose any icon to use for the monitoring device. **Note** You can change the icon after the monitoring device has been added.

Step 5 Click **Submit**.

Removing A Monitoring Device

Before You Begin

- At least one monitoring device must be configured for the port.
- The monitoring device that you want to remove must not be used in a rule. If it is, you must either modify or remove the rule before you can remove the monitoring device.

Step 1 Click the **Devices** tab.

Step 2 In the **Device Name** list, choose one of the following:

- The top checkbox to select all monitoring devices for removal.
- The checkbox next to the name of only the monitoring device or devices you want to remove.

Step 3 Above the **Device Name** list, click **Remove Monitoring Devices**.

Step 4 In the **Remove Monitoring Devices** confirmation dialog box, click **Remove Devices**.

Configuring a Root Node

A root node is automatically selected by Cisco Nexus Data Broker. If the defined root node is too far from the source switches, you can manually configure a different switch. We recommend that you choose a switch with edge ports as your new root node.

Note Root node changes do not take effect until you save the configuration.

Step 1 From the **Root** tab, click **Configure Root Node**.

Step 2 In the **Configure Root Node** dialog box, choose a node from the drop-down list.

Step 3 Click **Configure Root Node**.
The **Configured Root Node** is displayed the **Root** tab, and below it the **Current Root Node**, if any.

Step 4 Click **Save** in the menu bar.
The root node addition or change is saved.

Cisco onePK Agent

The Cisco onePK plug-in for Cisco Nexus Data Broker communicates with onePK devices through a onePK agent on the device. To support onePK device functions in Cisco Nexus Data Broker, the application must be connected to the onePK agent. The agent is the mediator between Cisco Nexus Data Broker and onePK-enabled devices that are configured in Cisco Nexus Data Broker.

To secure communication between Cisco Nexus Data Broker onePK-enabled devices, you must configure Transport Layer Security (TLS) in Cisco Nexus Data Broker. See the *Cisco Nexus Data Broker Configuration Guide, Release 2.0* for detailed procedures.

Connecting to a onePK Agent

You must connect to a onePK agent to support additional functionality in Cisco Nexus Data Broker, including symmetric load balancing, Q-in-Q, timestamp tagging, and packet truncation.

Step 1 In the topology diagram, click the node to which you wish to connect a onePK agent.

Step 2 In the sidebar, click **Click to enable addtional functionality**.

Step 3 In the **Connect to onePK agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 4 Click **Submit**.

Symmetric Load Balancing

Cisco Nexus Data Broker enables you to configure symmetric load balancing settings on the egress port channels. Load balancing settings are based on Layer 2 source MAC and destination IP addresses, or Layer 2, Layer 3, or Layer 4 source and destination ports. When you configure symmetric load balancing for all the port-channel interfaces on the switch, all the traffic from specific sources and destinations in both directions always flows on the same port-channel member link.

Note Symmetric load balancing in Cisco Nexus Data Broker is available only for Cisco Nexus 3100 Series switches.

Configuring Symmetric Load Balancing

Before You Begin

- Configure a onePK agent for the node.
- Configure and provision TLS on the switches.

Step 1 In the topology diagram, click the node for which you wish to configure symmetric load balancing.

Step 2 In the side bar, from the **Symmetric Load Balancing** drop-down list, choose one of the following:

- **SOURCE_DESTINATION_IP—**source and destination IP address (includes Layer 2)
- **SOURCE_DESTINATION_IP_ONLY—**source and destination IP addresses only
- **SOURCE_DESTINATION_PORT—**source and destination TCP/UDP port (includes Layer 2 and Layer 3)
- **SOURCE_DESTINATION_PORT_ONLY—**source and destination TCP/UDP port only

Step 3 Click **Submit**.

Configuring Q-in-Q

Note The ability to configure Q-in-Q is available only for Cisco Nexus 3000 and 3100 Series switches. Q-in-Q is automatically enabled when you configure a VLAN ID for an edge port, if the VLAN ID is maintained on the edge port.

Step 1 In the topology diagram, click the node for which you wish to configure Q-in-Q.

Step 2 In the side bar, configure an edge port and set a VLAN ID on that edge port.

Step 3 Click **Enable QinQ**.

Step 4 In the **Connect to onePK Agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 5 Click **Submit**.

Configuring Packet Truncation

Note Packet truncation can only be configured on Cisco Nexus 3500 Series switches.

Before You Begin

- Configure a onePK device.
- Connect to the onePK agent.

Step 1 In the topology diagram, click the node for which you wish to configure packet truncation.

Step 2 In the side bar, click the port for which you want to configure packet truncation.

Step 3 From the **Select a port type** drop-down list, choose one of the following:

- **Edge Port-SPAN**

- **Edge Port-TAP**

Step 4 (Optional) In the **Port Description** field, enter a port description.
The port description can contain between 1 and 256 alphanumeric characters, including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 5 (Optional) Enter a VLAN ID.
The port is configured as dot1q to preserve any production VLAN information.

Step 6 In the **Enable Packet Truncation** field, enter the truncated packet length that you want, in bytes.

Note It is recommended that you enter a minimum of 64 bytes, in multiples of 4.

Step 7 Click **Submit**.
The port configuration is saved, and the number of bytes for truncated packets is displayed in the label **TRUNC=<bytes>** beside the port name.

Configuring Timestamp Tagging

Note Timestamp tagging can only be configured on Cisco Nexus 3500 Series switches.

Before You Begin

- Configure a delivery device on the node.
- Configure a onePK device.

Step 1 In the topology diagram, click the node for which you wish to configure timestamp tagging.

Step 2 In the side bar, configure a delivery device.

Step 3 In side bar, click **Click to enable additional functionality**.

Step 4 In the **Connect to onePK Agent** dialog box, complete the following fields:

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The username of the user that you want to assign to the device.
Password field	The password of the user that you want to assign to the device.

Step 5 Check the check box next to **Enable Timestamp Tagging**.

Step 6 Click **Submit**.
The port is displayed in the **Port** list with the label **TS-Tag**.

CHAPTER 7

Filtering Flows

This chapter contains the following sections:

About Cisco Nexus Data Broker Networks

A Cisco Nexus Data Broker network consists of one or more Cisco Nexus 3000, 3100, or 3500 Series switches with Cisco Plug-in for OpenFlow dedicated for connecting multiple spanned ports and network taps from the production network infrastructure. Cisco Nexus Data Broker programs the switches using the OpenFlow protocol. Cisco Nexus Data Broker filters the packets that travel the network and delivers them to a pool of connected monitoring devices.

About Forwarding Path Options

Cisco Nexus Data Broker supports the following forwarding path options:

- Multipoint-to-Multipoint—With the Multipoint-to-Multipoint (MP2MP) forwarding path option, both the ingress edge port where SPAN or TAP traffic is coming into the monitor network and the egress delivery ports are defined. Cisco Nexus Data Broker uses the delivery ports to direct traffic from those ingress ports to one or more devices.
- Any-to-Multipoint—With the Any-to-Multipoint (A2MP) forwarding path option, the ingress edge port of the monitor network is not known, but the egress delivery ports are defined. Cisco Nexus Data Broker automatically calculates a loop-free forwarding path from the root node to all other nodes using the Single Source Shortest Path (SSSP) algorithm.

About Filters and Rules

Filters

In Cisco Nexus Data Broker, you can use a filter to define the Layer 2 (L2), Layer 3 (L3), and Layer 4 (L4) criteria used to filter traffic. Traffic that matches the criteria in the filter is routed to the delivery ports and from there to the attached monitor devices.

Rules

You can use rules to associate filters to configured monitor devices. You can configure rules with or without a source. Rules with a source node and port use the Multipoint-to-Multipoint forwarding path option. Rules without a source port on a node use the loop-free Any-to-Multipoint forwarding path option.

When a rule is configured with the Deny option, the ingress edge ports may or may not be defined. Cisco Nexus Data Broker drops traffic on the specified ingress edge port(s) or on all nodes if no ingress edge ports are defined.

Each rule has a priority that can be configured. Rules with a higher priority are given precedence over those with a lower priority.

Rules can be created and saved without installing them. After they are saved, installation can be toggled on and off in the Cisco Nexus Data Broker GUI.

Adding a Filter

Step 1 On the **Configure Filters** tab, click **Add Filter**.

Step 2 In the **Filter Description** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Name field	The name of the filter. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Predefined EtherTypes** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format. If you choose **Predefined EtherTypes**, all predefined Ethernet types contained in the `config.in` file are associated with the rule, and you should not configure any other parameters. **Note** If you do configure any other parameters along with **Predefined EtherTypes**, then click **Save Rule**, an error message will be displayed.

Name	Description
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** • You cannot enter a range of IPv6 addresses in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** • You cannot enter a range of IPv6 addresses in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Step 5 In the **Layer 4** section of the **Add Filter** dialog box, complete the following fields:

Name	Description
Source Port drop-down list	Choose the source port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose **Enter Source Port**, enter either a single port number or a range of source port numbers. **Note** • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose **Enter Destination Port**, enter either a single port number or a range of destination port numbers. **Note** • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Step 6 Click **Add Filter**.

Editing a Filter

Before You Begin

You must add a filter before you can edit it.

Note You cannot change the filter **Name** in the **Edit Filter** dialog box.

Step 1 On the **Configure Filters** tab, click the **Edit** button next to the **Name** of the filter that you want to edit.

Step 2 In the **Edit Filter** dialog box, edit the following fields:

Name	Description
Name field	The name of the filter. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Predefined EtherTypes** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format. If you choose **Predefined EtherTypes**, all predefined Ethernet types contained in the `config.in` file are associated with the rule, and you should not configure any other parameters. **Note** If you do configure any other parameters along with **Predefined EtherTypes**, then click **Save Rule**, an error message will be displayed.

Name	Description
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Edit Filter** dialog box, edit the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** • You cannot enter a range of IPv6 addresses in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** • You cannot enter a range of IPv6 addresses in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Cloning a Filter

Before You Begin

You must add at least one filter before you can clone a filter.

Step 1 On the **Configure Filters** tab, click **Clone** next to the **Name** of the filter that you want to clone.

Step 2 In the **Filter Description** section of the **Clone Filter** dialog box, complete the following fields:

Name	Description
Name field	The name of the filter. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed once you have saved it.
Bidirectional check box	Check this box if you want the filter to capture traffic information from a source IP, source port, or source MAC address to a destination IP, destination port, or destination MAC address, and from a destination IP, destination port, or destination MAC to a source IP, source port, or source MAC address.

Step 3 In the **Layer 2** section of the **Clone Filter** dialog box, complete the following fields:

Name	Description
Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value displayed is IPv4, or you can choose one of the following: • **IPv6** • **ARP** • **LLDP** • **Predefined EtherTypes** • **Enter Ethernet Type** If you choose **Enter Ethernet Type** as the type, enter the Ethernet type in hexadecimal format. If you choose **Predefined EtherTypes**, all predefined Ethernet types contained in the `config.in` file are associated with the rule, and you should not configure any other parameters. **Note** If you do configure any other parameters along with **Predefined EtherTypes**, then click **Save Rule**, an error message will be displayed.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic. You can enter a single VLAN ID, a range of VLAN ID values, or comma-separated VLAN ID values and VLAN ID ranges, for example, 1-4,6,8,9-12.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 4 In the **Layer 3** section of the **Clone Filter** dialog box, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. This can be one of the following: • The host IP address, for example, 10.10.10.10 • An IPv4 address range, for example, 10.10.10.10-10.10.10.15 • The host IP address in IPv6 format, for example, 2001::0 **Note** • You cannot enter a range of IPv6 addresses in the **Source IP Address** field. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 source IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.
Destination IP Address field	The destination IP address of the Layer 3 traffic. This can be one of the following: • The destination IP address. For example, 10.10.10.11 • An IPv4 address range, for example, 10.10.11.10-10.10.11.15 • The destination IP address in IPv6 format, for example, 2001::4 **Note** • You cannot enter a range of IPv6 addresses in the **Destination IP Address** field. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 4 source or destination ports. • If you configure a range of Layer 3 destination IP addresses, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Protocol drop-down list	Choose the Internet protocol of the Layer 3 traffic. This can be one of the following: • **ICMP** • **TCP** • **UDP** • **Enter Protocol** If you choose **Enter Protocol** as the type, enter the protocol number in decimal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. Only the Differentiated Services Code Point (DSCP) values are used.

Step 5 In the **Layer 4** section of the **Clone Filter** dialog box, complete the following fields:

Name	Description
Source Port drop-down list	Choose the source port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Source Port** If you choose **Enter Source Port**, enter either a single port number or a range of source port numbers. **Note** • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 source ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Name	Description
Destination Port drop-down list	Choose the destination port of the Layer 4 traffic. This can be one of the following: • **FTP (Data)** • **FTP (Control)** • **SSH** • **TELNET** • **HTTP** • **HTTPS** • **Enter Destination Port** If you choose **Enter Destination Port**, enter either a single port number or a range of destination port numbers. **Note** • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 3 IP source or destination addresses. • If you configure a range of Layer 4 destination ports, you cannot configure ranges of Layer 2 VLAN identifiers.

Step 6 Click **Clone Filter**.
The new filter is created and is displayed in the **Filters** list.

Deleting a Filter

You can delete a filter that has associated rules, resulting in removal of all the rules at the same time.

Step 1 On the **Configure Filters** tab, check the check box next to filter or filters that you want to delete, and then click **Remove Filters**.
When filters have rules associated with them, this information is displayed in the **Remove Filters** dialog box.

Step 2 In the **Remove Filters** dialog box, click **Remove Filters**.

Adding a Rule

Before You Begin

- Add a filter to be assigned to the rule.
- Configure a monitoring device (optional).
- Configure an edge port or multiple edge ports (optional).

Step 1 On the **Apply Filters** tab, click the **Add Rule** button.

Step 2 In the **Add Rule** dialog box, complete the following fields in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The **Rule Name** cannot be modified after the rule is saved.
Filter drop-down list	Choose the filter that you want to assign to the rule.
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, complete the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same filter for **Allow Filters** that you choose for **Traffic Drop Filters**.
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.

Field	Description
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes next to their names.
Traffic Drop Filters drop-down list	Choose a filter to use to drop matching traffic. **Note** You cannot choose the same filter for **Traffic Drop Filters** that you choose for **Allow Filters**.

Step 4 (Optional) In the **Assign Source Ports** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 5 Do one of the following:

- Click **Save Rule** to save the rule, but not to install it until later.
- Click **Install Rule** to save the rule and install it at the same time.

Modifying a Rule

Before You Begin

You must add a rule before you can modify it.

Step 1 On the **Apply Filters** tab, click the **Edit** button next to the **Name** of the rule that you want to modify.

Step 2 In the **Modify Rule** dialog bog you can modify the **Rule Priority** in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. **Note** The **Rule Name** cannot be modified after the rule is saved.
Rule Filter drop-down list	The filter applied to the rule. **Note** The **Rule Filter** cannot be modified after the rule is saved.
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, modify the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same rule for **Allow Filters** that you choose for **Traffic Drop Filters**.
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes next to their names.
Traffic Drop Filters drop-down list	Choose a filter to use to drop matching traffic. **Note** You cannot choose the same rule for **Traffic Drop Filters** that you choose for **Allow Filters**.

Step 4 In the **Assign Source Ports** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.

Field	Description
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 5 Click **Submit**.

Cloning a Rule

Before You Begin

Add at least one rule.

Step 1 On the **Apply Filters** tab, click **Clone Rule** next to the **Name** of the rule in the **Rules** list.

Step 2 In the **Clone Rule** dialog box, complete the following fields in the **Rule Details** area:

Field	Description
Rule Name field	The name of the rule. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The **Rule Name** cannot be modified after the rule is saved.
Filter drop-down list	Choose the filter that you want to assign to the rule.
Priority field	The priority that you want to set for the rule. The default is 100, and the valid range of values is 0 through 10000.

Step 3 In the **Actions** area, complete the following fields:

Field	Description
Allow Filters drop-down list	Choose a filter to use to allow matching traffic. **Note** You cannot choose the same filter for **Allow Filters** that you choose for **Traffic Drop Filters**.

Field	Description
Set VLAN field	The VLAN ID that you want to set for the rule.
Strip VLAN at delivery port check box	Check this box to strip the VLAN tag from the packet before it reaches the delivery port. **Note** The **Strip VLAN at delivery port** action is only valid for rules with a single edge port and one or more delivery devices for a single, separate node.
Destination Devices list	The monitoring devices that you want to associate with the filter. You can choose one or more devices by checking the boxes next to their names.
Traffic Drop Filters drop-down list	Choose a filter to use to drop matching traffic. **Note** You cannot choose the same filter for **Traffic Drop Filters** that you choose for **Allow Filters**.

Step 4 (Optional) In the **Assign Source Ports** area, complete the following fields:

Field	Description
Select Source Node drop-down list	Choose the source node that you want to assign. **Note** If you do not choose a source node, the any-to-multipoint loop-free forwarding path option is used, and traffic from all nondelivery ports is evaluated against the filter.
Select Source Port drop-down list	Choose the port on the source node that you want to assign. **Note** Only edge ports can be used as source ports.

Step 5 Do one of the following:

- Click **Save Cloned Rule** to save the rule, but not to install it until later.
- Click **Install Cloned Rule** to save the rule and install it at the same time.

Viewing Flow Statistics for a Rule

Cisco Nexus Data Broker enables you to view flow statistics for a rule that you have configured.

Before You Begin

- Add a filter.

- Configure a rule that uses the filter.
- Configure an edge port or multiple edge ports (optional).
- Configure a monitoring device (optional).

Step 1 On the **Apply Filters** tab, click the **Name** of the rule for which you want to display flow information.
The **Rule Path** dialog box is displayed. It provides the following information:

Name	Description
Edge Ports pane	The edge ports associated with the rule.
Topology pane	The nodes associated with the rule.
Devices pane	The delivery devices associated with the rule.

Step 2 Do one of the following:

- To view flow statistics for the entire topology, click **Flow Statistics**.
- To view flow statistics for an edge port, a node, or a device, click the appropriate icon in the **Rule Path** dialog box.

The **Flow Statistics** for a rule dialog box is displayed. It provides the following detail about the rule:

Name	Description
In Port field	Input port(s) from which traffic is matched. An asterisk ("*") indicates any input port.
DL Drc field	Source MAC address to be matched for incoming traffic. An asterisk ("*") indicates any source MAC address.
DL Dst field	Destination MAC address to be matched for incoming traffic. An asterisk ("*") indicates any destination MAC address.
DL Type field	Ethertype to be matched for incoming traffic. For example, "IPv4" or "IPv6" is used for all IP traffic types.
DL VLAN field	VLAN ID to be matched for the incoming traffic. An asterisk ("*") indicates any VLAN ID.
VLAN PCP field	VLAN priority to be matched for the incoming traffic. An asterisk ("*") is almost always displayed in this field.
NW Src field	IPv4 or IPv6 source address for the incoming traffic. An asterisk ("*") indicates any source address based on IPv4 or IPv6 Ethertypes.

Name	Description
NW Dst field	IPv4 or IPv6 destination address for the incoming traffic. An asterisk ("*") indicates any destination address based on IPv4 or IPv6 Ethertypes.
NW Proto field	Network protocol to be matched for the incoming traffic. For example, "6" indicates the TCP protocol.
TP Src field	Source port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
TP Dst field	Destination port associated with the network protocol to be matched for the incoming traffic. An asterisk ("*") indicates any port value.
Adtions field	Output action to be performed for the traffic matching the criteria specified, for example, "OUTPUT = OF|2".
Byte Count field	Aggregate traffic volume shown in bytes that match the specified flow rule.
Packet Count field	Aggregate traffic volume shown in packets that match the specified flow rule.
Duration Seconds field	The amount of time, in milliseconds, that the specific flow rule has been installed in the switch.
Idle Timeout field	The amount of time, in milliseconds, that the flow can be idle before it is removed from the flow table.
Priority field	The priority assigned to the flow. Flows with higher priority numbers take precedence.

Step 3 Click **Close** to close the **Flow Statistics** dialog box.

Step 4 Click **Close** to close the **Rule Path** dialog box.

Deleting a Rule

Step 1 Navigate to the **Apply Filters** tab.

Step 2 Check the check box for the rule or rules that you want to delete.

Step 3 Click **Remove Rules**.

CHAPTER 8

Managing Roles and Resources

This chapter contains the following sections:

About Cisco Data Broker Users

Cisco Nexus Data Broker uses roles and levels to manage user access. One of the following levels can be assigned to each role that you create:

- **App-Administrator—**Has full access to all Cisco Nexus Data Broker resources.
- **App-User—**Has full access to resources that are assigned to his resource group and resources that are created by another user who has similar permissions.

Each role is assigned to one or more groups, which are collections of resources. Group resources are non-Inter Switch Link (ISL) ports that are specifically assigned to that group. After you have created a group, you can assign that group to a role.

Creating a Role

Step 1 In the menu bar, click the **Admin** drop-down list, and choose **Settings**.

Step 2 On the **Roles** tab, click **Add Role**.

Step 3 In the **Add Role** dialog box, complete the following fields:

Field	Description
Name field	The name of the role. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
Level drop-down list	Choose the level that you want to assign to the role. This can be one of the following: • **App-Administrator—**Has full access to all Cisco Nexus Data Broker resources. • **App-User—**Has full access to resources that are assigned to his resource group and resources that are created by another user who has similar permissions.

Step 4 Click **Submit**.

Configuring a Role to Access Multiple Disjoint Networks

Multiple disjoint networks are the virtual networks that you create when you create network slices in the Cisco Nexus Data Broker application. Roles can be configured to permit role-based access to multiple Cisco Nexus Data Broker disjoint networks.

For example, if you have two networks, the first named **dev** and the second named **prod**, the network administrator can create a user that has access to both networks but with difference privileges for each network. The access level for network **dev** can be assigned as **App-Admin**, and the access level for network **prod** can be assigned as **App-User**.

The App-Admin privilege provides the ability to create, edit, and delete his or other roles' rules and filters on the assigned network, in this case, dev. The App-User privilege provides the ability to create, edit, and delete rules and filters owned by this role only on the assigned network, in this case, prod. The application user role can create, edit, or delete rules and filters only for the disjoint network or networks to which the role has been

assigned. In addition, the application user role can view and apply filters created by the application administrator, but cannot edit or delete them.

Step 1 Log in to the Cisco Nexus Data Broker network with the Network-Admin role username and password.

Step 2 Ensure that you are in the **dev** network.

Step 3 On the menu bar, choose **Settings** from the **Admin** drop-down list .

Step 4 Click **Add Role**.

Step 5 In the **Name** field of the **Add Role** dialog box, enter the name for the role, for example, NDB-role-dev.
The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 6 From the **Level** drop-down list, choose **App-Administrator**.

Step 7 Click **Submit**.

Step 8 On the menu bar, choose the **prod** network from the network drop-down list.

Step 9 Repeat Steps 3 and 4 for the **prod** network.

Step 10 In the **Name** field of the **Add Role** dialog box, enter NDB-role-prod.

Step 11 From the **Level** drop-down list, choose **App-User**.

Step 12 Click **Submit**.

Step 13 Assign **allPorts** to role MM-role-prod under the **Assign** tab.
The role NDB-role-dev now has App-Administrator permissions to the network **dev** and the role NDB-role-prod has App-User permissions to network **prod**.

You can now create a user that has both of these application roles.

Note Press Ctrl+F5, or Cmd+Shift+R, simultaneously, when switching between networks with different access levels.

Removing a Role

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 In the **Roles** table on the **Roles** tab, click the role that you want to remove.

Step 3 In the **Remove Roles** confirmation dialog box, click **Remove**.

Creating a Resource Group

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Groups** tab, click **Add Group**.

Step 3 In the **Add Resource Group** dialog box, enter the name that you want to use for the resource group.
The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 4 Click **Submit**.

What to Do Next

Add resources to the group.

Adding Resources to a Resource Group

Before You Begin

Create a resource group.

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Groups** tab, choose the group to which you want to add resources.

Step 3 Choose a node in the topology diagram.

Step 4 In the **Add Ports to Group** dialog box, choose the ports that you want to add to the group.

Step 5 Click **Submit**.

Step 6 Repeat Step 3 through Step 5 for all of the ports that you want to add.

Step 7 Remove a resource, or multiple resources, by choosing one or more ports in the **Group Detail** table, and then clicking **Remove Ports**.

Step 8 In the **Remove Ports** dialog box, click **Remove**.

What to Do Next

Assign the resource group to a role.

Assigning a Group to a Role

Before You Begin

- Create a role.
- Create a resource group.

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 Click the **Assign** tab.

Step 3 Click **Assign** next to the role for which you want to assign a group.

Step 4 In the **Configure Role** dialog box, complete the following fields:

Field	Description
Assign Group field	The groups that you want to assign to the role. You can choose one or more groups to assign. **Note** You cannot assign a group to a role with the App-Administrator level.
Unassign Group field	The groups that you want to unassign from the role. You can choose one or more groups to unassign. **Note** You cannot unassign the allPorts group from a role with the App-Administrator level.

Step 5 Click **Apply**.

Unassigning a Group

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 Click the **Assign** tab.

Step 3 Click **Assign** next to the role for which you want to unassign a group.

Step 4 In the **Configure Role** dialog box, choose a port in the **Unassign Group** drop-down list.

Step 5 Click **Apply**.

Removing a Group

The following groups cannot be removed:

- The default **allPorts** group
- Any group that has been assigned to a role.

Step 1 From the **Admin** drop-down list, choose **Settings**.

Step 2 On the **Groups** tab, choose the group or groups that you want to remove.

Step 3 Click **Remove Groups**.

Step 4 In the **Remove Resource Groups** confirmation dialog box, click **Remove**.

CHAPTER 9

Managing Flows

This chapter contains the following sections:

About Flow Programming

With Cisco Nexus Data Broker, you can configure individual flows in each network device. Flows are identified based on Layer 1 through Layer 4 criteria. After the flow is identified, you can specify the actions to be performed on the packets that match the flow specification. The criteria for matching and actions varies depending upon the switch. Possible actions are as follows:

- Dropping or forwarding the packet to one or more interfaces.
- Setting the VLAN ID and priority of the packets.
- Modifying the source and destination MAC addresses of the packets.
- Modifying the source and destination IP addresses of the packets.

All flows that you create are listed in the **Flow Entries** table on the **Flows** tab. Flows become active when you install them in the device.

Adding a Flow Entry

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Flows**, and then click the **Flow Entries** tab.

Step 3 Click **Add Flow Entry**.

Step 4 In the **Flow Description** area of the **Add Flow Entry** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the flow. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** You cannot change the name of the flow entry after it is saved.
Node drop-down list	Choose the ID or node name for the device. **Note** The node you choose cannot be changed one you save the flow entry.
Input Port drop-down list	Choose the port on the node where traffic enters the flow.
Priority field	The priority that you want to apply to the flow. The default priority is 500. Flows with a higher priority are given precedence over flows with a lower priority. **Note** The priority is considered only when all of the Layer 2, Layer 3, and Layer 4 match fields are equal.
Hard Timeout field	The amount of time in milliseconds for the flow to be installed before it is removed from the flow table.
Idle Timeout field	The amount of time in milliseconds that the flow can be idle before it is removed from the flow table.
Cookie field	An identifier added to the flow. Cookies are specified by the controller when the flow is installed and are returned as part of each flow status and flow expired message.

Step 5 In the **Layer 2** area, complete the following fields:

Name	Description
Ethernet Type field	The Ethernet type for the Layer 2 traffic. The Ethernet type for IPv4, in hexadecimal format, is displayed by default. Either accept the default value, or enter one of the following, in hexadecimal format: • **IPv6** • **ARP** • **LLDP**
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.

Name	Description
Source MAC Address field	The source MAC address for the Layer 2 traffic.
Destination MAC Address field	The destination MAC address for the Layer 2 traffic.

Step 6 In the **Layer 3** area, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic. **Note** The format of the source IP address must match the Ethernet type that you entered in the **Ethernet Type** field for Layer 2.
Destination IP Address field	The destination IP address of the Layer 3 traffic. **Note** The format of the destination IP address must match the Ethernet type that you entered in the **Ethernet Type** field for Layer 2.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. **Note** Only the DSCP bits are supported on Cisco Nexus 3000 Series switches.

Step 7 In the **Layer 4** area, complete the following fields:

Name	Description
Source Port field	The source port of the Layer 4 traffic.
Destination Port field	The destination port of the Layer 4 traffic.
Protocol field	The Internet protocol number of the Layer 4 traffic. Enter the IP protocol number in decimal, hexadecimal, or octal format.

Step 8 In the **Actions** area, select one or more actions:

- **Drop**
- **Loopback**
- **Flood**
- **Software Path**
- **Hardware Path**
- **Controller**
- **Add Output Ports**
- **Set VLAN ID**

- **Set VLAN Priority**
- **Strip VLAN Header**
- **Modify Datalayer Source Address**
- **Modify Datalayer Destination Address**
- **Modify Network Source Address**
- **Modify Network Destination Address**
- **Modify ToS Bits**
- **Modify Transport Source Port**
- **Modify Transport Destination Port**
- **Flood All**
- **Enqueue**
- **Set VLAN CFI**
- **Push VLAN**
- **Set EtherType**

Step 9 Do one of the following:

- Click **Install Flow** to install the flow into the device.
- Click **Save Flow** to save the flow to the **Flow Entries** table but not install the flow in the flow table of the device.

Viewing Flow Details

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Flows**, and then click the **Flow Entries** tab.

Step 3 Locate the flow that you want to view.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 4 In the **Flow Overview** area of the **Flow Detail** tab, perform one of the following tasks:

- Click **Remove Flow** to remove the flow from the **Flow Entries** table.
- Click **Edit Flow** to edit the flow in the flow table of the device.
- Click **Uninstall Flow** to remove the flow from the flow table of the device.

CHAPTER 10

Troubleshooting

This chapter contains the following sections:

About Troubleshooting

Cisco Nexus Data Broker includes a variety of tools that you can use to troubleshoot your network connections. From the **Troubleshoot** tab, you can do the following:

- View all of the nodes in the network.
- View detailed information about the ports for each node in the network.
- View detailed information about the flows for each node in the network.
- View when the nodes were discovered by in the **Uptime** tab.
- View detailed information about TIF policies in the **Policy Analyzer** tab.
- Run analytics on selected flows and TIF policies.

Viewing Flow and Port Detail Statistics

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

Step 3 In the **Existing Nodes** tab, locate the node for which you want to view statistics.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 4 Perform one of the following tasks:

- Click **Flows** to view detailed information about all flows programmed on the node.
- Click **Ports** to view detailed information about all ports of the node.

Note The statistics are updated every 120 seconds.

Viewing Inconsistent Controller Flows or Inconsistent Node Flows

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 In the menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

Step 3 From the **Select a node** drop-down list, choose a node.
The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows**, if any, next to each type.

Step 4 Click either **Inconsistent Controller Flows** or **Inconsistent Node Flows** to view details for any inconsistent flows.
Details are displayed in the **Statistics** tab.

What to Do Next

Fix inconsistent controller flows or inconsistent node flows.

Exporting Inconsistent Flow Details

In order to view and save inconsistent controller or inconsistent node flow details for reference, you can export them to a comma-delimited file.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 In the menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

Step 3 Choose a node from the **Select a node** drop-down list.
The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows** next to each type.

Step 4 Choose either **Inconsistent Controller Flows** or **Inconsistent Node Flows**.
The list of **Inconsistent Controller Flows** or **Inconsistent Node Flows** is displayed in the **Statistics** tab.

Step 5 Check the check box next to one or more inconsistent flows, or check the check box at the top of the list to choose all flows in the list.

Step 6 Click **Export All**, and then click **Export Flow Details**.

Step 7 Save the inconsistent flow detail information as a `.csv` file that you can open later for analysis.

Fixing Inconsistent Flows

Note When you fix an inconsistent controller flow, the flow is installed on the switch. When you fix an inconsistent node flow, the flow is removed from the switch, because the controller is the authoritative source of flow information.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 In the menu bar, choose**Troubleshoot**, and then click the **Flow Check** tab.

Step 3 Choose a node from the **Select a node** drop-down list.
The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows** next to each type.

Step 4 Click either **Inconsistent Controller Flows** or **Inconsistent Node Flows**.
The list of **Inconsistent Controller Flows** or **Inconsistent Node Flows** is displayed in the **Statistics** tab.

Step 5 Check the check box next to one or more inconsistent flows, or check the check box at the top of the list to choose all flows in the list.

Step 6 Click **Fix Inconsistent Flows**.

Step 7 In the **Fix Flows** confirmation dialog box, click **Fix Inconsistent Flows**.

The **Flow Check** tab redisplays **Inconsistent Controller Flows** and **Inconsistent Node Flows** with the updated number of each type.

Note If you chose all inconsistent flows in Step 4, the number displayed is 0.

SDN Analyzer

The SDN Analyzer downloads packet capture (pcap) files for the interface that you select. The individual pcap files are consolidated into one zip file.

By default, the SDN Analyzer captures 5 pcap files with 100 MB of network data each. If more than the set amount of data is captured, the earlier data is overwritten. You can change the amount of data collected in the `config.ini` file.

Using the SDN Analyzer

The SDN Analyzer captures packets that come to Cisco Nexus Data Broker and outputs the results to a zip file. The location of the zip file depends upon your browser settings.

Before You Begin

You must have root privileges on the server that is running Cisco Nexus Data Broker to run the SDN Analyzer.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 On the menu bar, click **Troubleshoot**, and then click the **SDN Analyzer** tab.

Step 3 Click the interface that you want to view, and then click **Start Analyzer**.

Step 4 When you have finished collecting data, click **Stop Analyzer**.

Changing the Default Values for the SDN Analyzer

Step 1 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 2 Use any text editor to open the `config.ini` file.

Step 3 Locate the following parameters:

- troubleshoot.fileSize = 100
- troubleshoot.number = 5

Step 4 Change the files as appropriate. We recommend that you use a file size of no more than 100mb, and increase the number of pcap files.

Step 5 Save the file and exit the editor.

Step 6 Restart Cisco Nexus Data Broker.

CHAPTER 11

Managing Slices

This chapter contains the following sections:

About Slice Manager

The Slice Manager provides a way for you, as a network administrator, to partition networks into many logical networks. This feature allows you to create multiple disjoint networks and assign different roles and access levels to each one. Each logical network can be assigned to departments, groups of individuals, or applications. Multiple disjoint networks can be managed using the Cisco Nexus Data Broker application.

The Slice Manager creates slices based on the following criteria:

- Network devices—The devices that can be used in the slice.

  Network devices can be shared between slices.

- Network device interfaces—The device interfaces that can be used in the slice.

  Network device interfaces can be shared between slices.

- Flow Specification—A combination of source and destination IP, protocol, and source and destination transport ports used to identify the traffic that belongs to the slice.

  Flow specifications can be assigned to different slices if the associated network devices and interfaces are disjointed.

Note You can also use VLAN IDs to segregate the slice traffic.

Slices must be created by a Cisco Nexus Data Broker user with the Network Administrator role. After creation, the slices can be managed by a user with the Slice Administrator role.

Slices can overlap if each slice has at least one unique attribute. For example, a slice can share the same physical switches and ports, but be differentiated by the type of traffic it receives.

Adding a Slice

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **Slices**.

Step 3 From the **Admin** drop-down list, choose **Slices**.

Step 4 On the **Slices** tab, click **Add Slice**.

Step 5 In the **Add Slice** dialog box, complete the following fields:

Name	Description
Slice Name field	The name that you want to assign to the slice. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), vertical bar (|), or at sign (@). **Note** The slice name cannot be changed once it is saved.
Static VLAN field	The static VLAN that you want to assign to the slice.

Step 6 Click **Add Slice**.

Adding Nodes and Ports to a Slice

Before You Begin

You must have created a slice before you can add nodes and ports.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **Slices**.

Step 3 From the **Admin** drop-down list, choose **Slices**.

Step 4 On the **Slices** tab, choose the slice for which you want to add entries.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 5 In the topology diagram, click a node that you want to add to the slice.

Step 6 In the **Add Slice Entry** dialog box, choose the port or ports that you want to add to the slice.

Step 7 Click **Add Entry**.

Step 8 Repeat Step 3 through Step 5 for each node and port that you want to add to the slice.

Adding a Flow Specification

Before You Begin

Create a slice before you add a flow specification.

Note Be default, a flow specification is bidirectional.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **Slices**.

Step 3 From the **Admin** drop-down list, choose **Slices**.

Step 4 On the **Flow Spec** tab, choose the slice for which you want to add a flow specification.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 5 On the **Detail** tab, click **Add Flow Spec**.

Step 6 In the **Add Flow Spec** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to use for the flow specification. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
VLAN field	The VLAN ID or the range of VLAN IDs that you want to use for the flow specification.
Source IP field	The source IP address that you want to use for the flow specification.
Destination IP field	The destination IP address that you want to use for the flow specification.
Protocol field	The IP protocol number in decimal format that you want to use for the flow specification.
Source Port field	The source port that you want to use for the flow specification.

Name	Description
Destination Port field	The destination port that you want to use for the flow specification.

Step 7 Click **Add Flow Spec**.

CHAPTER 12

Administrative Tasks

This chapter contains the following sections:

About AAA Servers

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). Cisco Nexus Data Broker uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with an AAA server.

Remote authentication and authorization is supported using the AAA server. To authenticate each user, Cisco Nexus Data Broker uses both the login credentials and an attribute-value (AV) pair that assigns the authorized role for the user as part of the user administration. After successful authentication, the Cisco AV pair is returned to Cisco Nexus Data Broker for resource access authorization.

Adding an AAA Server

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **AAA**.

Step 3 From the **Admin** drop-down list, choose **AAA**.

Step 4 In the **AAA Configuration** dialog box, click **Add Server**.

Step 5 In the **Add AAA Server** dialog box, complete the following fields:

Name	Description
Server Address field	The IP address of the AAA server.
Server Secret field	The shared secret configured on the AAA server.
Protocol drop-down list	Choose the protocol for the AAA server. This can be one of the following: • **Radius+** • **TACACS+**

Step 6 Click **Save**.

What to Do Next

If you chose RADIUS as the protocol for the AAA server, you need to configure user authentication for RADIUS.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format.

In the RADIUS server, configure the Cisco av-pair attribute for a user as follows:

```
shell:roles="Network-Admin Slice-Admin"
```

Viewing an AAA Server

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **AAA**.

Step 3 From the **Admin** drop-down list, choose **AAA**.

Step 4 In the **AAA Configuration** dialog box, click a server address.

Step 5 After viewing the server information in the **Remove AAA Configuration** dialog box, click **Close.**

Step 6 In the **AAA Configuration** dialog box, click **Close.**

Users and Roles

Cisco Nexus Data Broker uses users and roles to manage user access. You can assign more than one role to a user. This can be one of the following:

- **Network Administrator—**Provides full administrative privileges to all applications.
- **Network Operator—**Provides read-only privileges to all applications.
- **Application User—**Provides privileges that are defined in the specified application.
- **Slice User—**Provides access to a specified slice.

Each user is assigned a role, which determines the permissions that they have. Slice users are assigned to both a role and a slice. The Admin user with the Network Administrator role is created by default when you install Cisco Nexus Data Broker.

Viewing User Information

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **Users**.

Step 3 From the **Admin** drop-down list, choose **Users**.

Step 4 In the **User Management** dialog box, you can do the following:

- View a list of usernames and the roles assigned to each user.
- Click an existing user to delete the user or change the password for the user.
- Click **Add User** to create a new user.

Step 5 When you are finished, click **Close**.

Adding a User

After creating a user, you can change the password, but you cannot change the roles assigned to the user.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **Users**.

Step 3 From the **Admin** drop-down list, choose **Users**.

Step 4 In the **User Management** dialog box, click **Add User**.

Step 5 In the **Add User** dialog box, complete the following fields:

Name	Description
Username field	The name that you want to assign to the user. A username can be between 1 and 32 alphanumeric characters and contain any special character except a period ("."), forward slash ("/"), pound sign ("#"), percent sign ("%"), semicolon (";"), question mark ("?"), or backslash ("\").
Password field	The password for the user. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one nonalphanumeric character.
Choose Role(s) drop-down list	Choose the role that you want to assign to the user. You can assign more than one role. This can be one of the following: • **Network Administrator—**Provides full administrative privileges to all applications. • **Network Operator—**Provides read-only privileges to all applications. • **Application User—**Provides privileges that are defined in the specified application. • **Slice User—**Provides access to a specified slice.
Role Name field	If you chose **Application User**, enter the name that you want to assign to the role.
Slices drop-down list	If you chose **Slice User**, choose the slice that you want to assign to the user.

Name	Description
Slice Role drop-down list	If you chose **Slice User**, choose the role that you want to assign to the user. This can be one of the following: • **Administrator—**Provides full administrative privileges to the specified slice. • **Operator—**Provides read-only privileges to the specified slice.
Assign button	Assigns a role to the user.

Step 6 Click **Add User**.

Step 7 In the **User Management** dialog box, click **Close.**

Changing the Password for an Existing User

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **AAA**.

Step 3 From the **Admin** drop-down list, choose **Users**.

Step 4 In the **User Management** dialog box, click the user that you want to modify.

Step 5 In the **Manage User** dialog box, click **Change Password**.

Step 6 In the **Change Password** dialog box, enter the new password in the **New Password** and in the **Verify New Password** fields.

Step 7 Click **Submit**.

Step 8 Click **Close** in the **Manage User** dialog box.

Step 9 Click **Close** in the **User Management** dialog box.

Deleting a User

If you are signed in as a particular user, you cannot delete that user.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **Users**.

Step 3 From the **Admin** drop-down list, choose **Users**.

Step 4 In the **User Management** dialog box, click the user that you want to modify.

Step 5 In the **Edit User** dialog box, click **Remove User**.

Step 6 In the **User Management** dialog box, click **Close**.

Viewing Cluster Management Information

Note The cluster management dialog boxes are read-only.

Before You Begin

You must have configured high availability clustering in order to view the cluster management information. See Configuring High Availability Clusters, on page 21.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **AAA**.

Step 3 From the **Admin** drop-down list, choose **Clusters**.
The **Cluster Management** dialog box lists the IP addresses of all of the Cisco Nexus Data Broker instances in the cluster. Clusters can be denoted by one of the following icons:

- The ***** icon indicates the cluster node that is currently being viewed.
- The **C** icon indicates that the cluster node is the coordinator.

Step 4 In the **Cluster Management** dialog box, choose a cluster.
The **Connected Nodes** dialog box lists all of the nodes in the selected cluster.

Step 5 In the **Connected Nodes** dialog box, click **Close.**

Step 6 In the **Cluster Management** dialog box, click **Close.**

Viewing the OSGi Console

You can view all of Cisco Nexus Data Broker bundles that comprise the application by viewing the OSGi Web Console.

Note This procedure does not provide a step-by-step guide to everything you can do in the OSGi Web Console for **Cisco XNC Bundles** list. It guides you in opening the OSGi Web Console and viewing bundle information.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From management **Admin** drop-down list, choose **OSGi**.

Step 3 From the **Admin** drop-down list, choose **OSGi**.
A new browser tab opens.

Step 4 Enter your username and password, and then press **Enter**.
The **Cisco – XNC Bundles** list is displayed. In this page you can view all of the active packages, filter on the package name to specify bundle names, and complete other tasks.

Step 5 When you are finished viewing the list, close the **Cisco – XNC Bundles** browser tab.

Viewing the Northbound API Content

You can view all of Cisco Nexus Data Broker northbound API content for the application by opening a browser tab using the **Northbound API** tool (book icon) in the menu bar.

Step 1 From the menu bar, click the **Northbound API** button.
A new browser tab (Swagger UI) is opened and the complete list of northbound API content used in Cisco Nexus Data Broker is displayed.

From this tab, you can do the following:

- Show or hide the operations for an API.
- List the operations for an API.
- Expand the operations for an API.

Step 2 When you are finished viewing northbound API content, close the browser tab.

System Management

The system management features in Cisco Nexus Data Broker enable you to download and save the configuration files for your system, or upload and restore the configuration files for your system. You can also download log files.

Downloading the System Log Files

You can download log files for Cisco Nexus Data Broker to use for analysis. Log files are saved as a .zip archive.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **System**.
The **System Administration** dialog box is displayed.

Step 3 Click **Download Logs**.
A dialog box opens in the browser prompting you to either open or save the .zip file.

Step 4 Do one of the following:

- Save the archive to a location of your choosing, for example, `home/ndbconfig`.
- Open the archive to view the contents, and then save it.

Downloading the System Configuration Files

You can download the system configuration files for Cisco Nexus Data Broker to save them in case you need to restore the system after an upgrade or other change. System configuration files are saved in a zipped archive.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **System**.
The **System Administration** dialog box is displayed.

Step 3

Step 4 Click **Download Configuration**.
A dialog box opens in the browser prompting you to either open or save the file.

Step 5 Do one of the following:

- Save the archive to a location of your choosing, for example, `home/ndbconfig`.

- Open the archive to view the contents, and then save it.

Uploading the System Configuration Files

You can upload the saved system configuration files for Cisco Nexus Data Broker to restore the Cisco Nexus Data Broker application in the case of a failure or other event. After restoring you configuration, you will need to restart Cisco Nexus Data Broker.

Before You Begin

You must download the system configuration files and save them in a zipped archive.

Step 1 From the **Admin** drop-down list, choose **Management**.

Step 2 From the management **Admin** drop-down list, choose **System**.
The **System Administration** dialog box is displayed.

Step 3 Click **Upload Configuration**.

Step 4 Navigate to the location of the file `configuration_startup.zip`.

Step 5 Click on the archive file.
The system configuration is uploaded and the browser displays a message informing you that you need to restart the server.

Step 6 Restart the server, and then log back in to the Cisco Nexus Data Broker GUI.

Backing Up or Restoring the Configuration

The backup and restore commands allow you to back up your Cisco Nexus Data Broker configurations and restore them.

Step 1 Open a command window where you installed Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 3 Back up the configuration by entering the **./xnc config --backup** command.
The **--backup** option creates a backup archive (in .zip format) of the startup configuration in the current `xnc` distribution. The backup archive is stored in `{xncHome}/backup/`. A new archive is created each time that the backup command is entered using a filename with the current timestamp.

Step 4 Restore the configuration by entering the **./xnc config --restore --backupfile** {*zip_filename*} command.
The **--restore** option restores the startup configuration of the current `xnc` distribution from an existing backup archive. The restore action requires the absolute path of the backup archive.

Step 5 If you are restoring a configuration, stop and restart Cisco Nexus Data Broker for the restored configuration to take effect.

Recovering the Administrative Password

The Cisco Nexus Data Broker network administrator user can return the administrative password to the factory default.

Note The software may or may not be running when this command is used. If the it is not running, the password reset takes effect the next time that it is run.

Step 1 Open a command window where you installed Cisco Nexus Data Broker.

Step 2 Navigate to the `xnc/bin` directory that was created when you installed the software.

Step 3 Reset the administrative password by entering the **./xnc reset-admin-password** [**--wait-seconds** {*wait_time*} **--password** {*password*}] command.
Resets the admin password to the default or specified password by restarting the user manager.

- The **wait-seconds** is the length of time, in seconds, to wait for the user manager to restart. The minimum is 5 seconds and the maximum is 60 seconds.
- The **password** is the administrative password.

Note
- The password must be from 8 to 256 characters, contain both uppercase and lowercase characters, and have at least one number and one nonalphanumeric character.
- If you leave the password blank, it is reset to the factory default of "admin".
- Each time that you reset the administrative password, make sure that the new password meets these requirements or you will not be able to log in to Cisco Nexus Data Broker.

Uninstalling the Application Software

Before You Begin

Ensure that your Cisco Nexus Data Broker application is stopped before proceeding.

Step 1 Navigate to the directory where you created the Cisco Nexus Data Broker installation.
For example, if you installed the software in `Home/CiscoNDB`, navigate to the `Home` directory.

Step 2 Delete the `CiscoNDB` directory.