Extreme™
Customer-Driven Networking

Extreme SLX-OS
Network Packet Broker Configuration Guide,
17s.1.01

Supporting the ExtremeSwitching SLX 9140 and SLX 9240 Switches

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Extreme technical documentation.

Notes, cautions, and warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential

hazards.

NOTE
A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

DANGER
A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used to highlight specific words or phrases.

Format	Description
bold text	Identifies command names.
	Identifies keywords and operands.
	Identifies the names of GUI elements.
	Identifies text to enter in the GUI.
italic text	Identifies emphasis.
	Identifies variables.
	Identifies document titles.
`Courier font`	Identifies CLI output.

Format	Description
	Identifies command syntax examples.

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

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

Extreme resources

Visit the Extreme website to locate related documentation for your product and additional Extreme resources.

White papers, data sheets, and the most recent versions of Extreme software and hardware manuals are available at www.extremenetworks.com. Product documentation for all supported releases is available to registered users at www.extremenetworks.com/support/documentation.

Document feedback

Quality is our first concern at Extreme, and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you.

You can provide feedback in two ways:

- Use our short online feedback form at http://www.extremenetworks.com/documentation-feedback-pdf/
- Email us at internalinfodev@extremenetworks.com

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Contacting Extreme Technical Support

As an Extreme customer, you can contact Extreme Technical Support using one of the following methods: 24x7 online or by telephone. OEM customers should contact their OEM/solution provider.

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

- GTAC (Global Technical Assistance Center) for immediate support
  - Phone: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact.
  - Email: support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- GTAC Knowledge – Get on-demand and tested resolutions from the GTAC Knowledgebase, or create a help case if you need more guidance.
- The Hub – A forum for Extreme customers to connect with one another, get questions answered, share ideas and feedback, and get problems solved. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
- Support Portal – Manage cases, downloads, service contracts, product licensing, and training and certifications.

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

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

About This Document

What's new in this document

This document is the first version of the *Extreme SLX-OS Network Packet Broker Configuration Guide*, for Extreme SLX-OS 17s.1.01.

On October 30, 2017, Extreme Networks, Inc. acquired the data center networking business from Brocade Communications Systems, Inc. This document has been updated to remove or replace references to Brocade Communications, Inc. with Extreme Networks, Inc., as appropriate.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Extreme Networks, Inc. for this SLX-OS release, documenting all possible configurations and scenarios is beyond the scope of this document.

The following hardware platforms are supported by this release:

- ExtremeSwitching SLX 9140
- ExtremeSwitching SLX 9240

    NOTE
    Some of the commands in this document use a slot/port designation. Because the SLX 9140 and the SLX 9240 do not contain line cards, the slot designation must always be "0" (for example, 0/1 for port 1).

Network Packet Broker

NPB overview

A Network Packet Broker (NPB) provides a collection of monitoring tools with access to traffic across the network.

When you configure and reboot an SLX-OS device into NPB mode, it can function as a Network Packet Broker.

The SLX-OS NPB implementation includes the following features:

* Aggregation: Traffic on multiple ingress interfaces is aggregated and forwarded on a single egress interface ("many to one"), to one monitoring tool.
* Replication: Traffic on a single ingress interface is replicated and forwarded on multiple egress interfaces ("one to many"), to multiple monitoring tools.
* Load Balancing: Aggregation and replication traffic is load-balanced across the members of an egress port-channel interface.
* Timestamping: With Precision Time Protocol (PTP) accuracy, ingress and egress timestamps aid analysis of congestion and security issues. For details, refer to the "Precision Time Protocol (PTP)" section of the *Extreme SLX-OS Management Configuration Guide for SLX 9140 and SLX 9240*.

The following table indicates which interface types are supported for the aggregation, replication, load balancing, and timestamping features:

TABLE 1 Ingress and egress interface types

Feature	Ingress interfaces	Egress interfaces
Aggregation	Multiple physical, port-channel, or mixed interfaces	One physical or port-channel interface
Replication	One physical or port-channel interface	A TVF domain, including multiple physical, port-channel, or mixed interfaces
Load Balancing	Not supported	One port-channel interface
Timestamping	Physical and port-channel interfaces	Physical and port-channel interfaces

Route maps under NPB

A route map is a container for one or more numbered permit or deny stanzas; each stanza contains a sequence of statements.

Evaluation of route maps consists of a list scan, from the lowest-numbered stanza to the highest-numbered stanza. Within each stanza, statements are evaluated in order. The following are among the technologies that use route maps:

- BGP and OSPF protocols. For details, refer to the *Extreme SLX-OS Layer 3 Routing Configuration Guide for SLX 9140 and SLX 9240*.
- Policy-based routing (PBR) (Not supported)
- Network Packet Broker (NPB)

Route-map syntax and evaluation vary with the technology. However, "match" statements are common to all route-map implementations. Upon a match, the actions specified in the match statement and in the remaining statements of that stanza are implemented. The list scan ends without examining higher-numbered stanzas.

Route-map "set" statements are also supported for the mentioned technologies. Upon a match, set statements perform an action on the matched traffic. The action varies with the technology. The following table compares route-map features and functionality for the various technologies.

TABLE 2 Route-map comparison

Feature	NPB	BGP	PBR (Not supported)
Traffic routing or forwarding	Yes	Yes	Yes
Traffic redistribution	No	Yes	No
Route-attribute modification	No	Yes	No
Stanzas	One or more permit or deny stanzas	One or more permit or deny stanzas	One or more permit or deny stanzas
Match statements	One or more **match { mac | ip | ipv4 } address acl** statements	One or more supported **match** statements	One or more **match { ip | ipv4 } address acl** statements
Set statements (Supported only in permit stanzas)	**set interface** or **set next-hop-tvf-domain**	0, 1, or multiple **set** statements	0, 1, or multiple **set** statements
Continue statements	No	0 or 1 **continue** statements	No
Interfaces	Physical and port-channel interfaces	Device-level	Layer 3 interfaces

NPB configuration guidelines

Follow these guidelines when implementing Network Packet Broker (NPB):

- NPB requires a license. For details, refer to the *Extreme SLX-OS Software Licensing Guide for SLX 9140 and SLX 9240*.
- A system reboot is required when moving from default system mode to NPB mode and conversely.
- Most Layer 2 and Layer 3 configurations are not supported in NPB mode. Although implementing them does not generate error messages, do not configure them in NPB mode.

- Only one route map can be applied per interface as NPB policy. However, that route map can have multiple stanzas.
- You can apply a given route map on multiple interfaces.
- The only supported match statements are **match { mac | ip | ipv6 } address acl** statements. Other match statements are ignored.
- The only supported set statements are **set interface** and **set next-hop-tvf-domain**. Other set statements are ignored.
- If a stanza does not contain a match statement, "match any" is implied.
- The only supported egress interfaces are physical interfaces, port-channel interfaces, and TVF domains.
- If a physical interface is part of a port-channel, a **set interface** statement on that interface is ignored.

Forwarding priority guidelines

The following guidelines determine forwarding priority in an NPB route-map:

- In general, forwarding priority is determined by the first match in the lowest-numbered stanza. For exceptions, refer to Priority among Layer 2 and Layer 3 match acl statements on page 14.
- The order in which the egress interfaces are configured is also the order for configuring forwarding.
- If a route map has multiple egress interfaces, the first egress interface ready for forwarding is used.
  - A physical interface is considered ready for forwarding if its link is up.
  - Port-channels and TVF domains are considered ready if at least one member port link is up.
- If the current egress interface loses its Ready status, then the next configured egress interface that is ready for forwarding is used.
- If a Down egress interface becomes Ready and if it has higher priority than the currently selected egress interface, the higher priority egress interface replaces it.
- If none of the configured egress interfaces are ready, the traffic is dropped.

Stanza and ACL permit and deny keywords

Both route-map stanzas and access-control lists (ACLs) have **permit** and **deny** keywords.

Both NPB and PBR route-maps contain **match { mac | ip | ipv4 } address acl** statements. However, permit and deny rules in ACLs applied to route maps function differently than rules in the security ACLs discussed in the *Extreme SLX-OS Security Configuration Guide for SLX 9140 and SLX 9240*:

- In security ACLs, permit rules allow packets and deny rules drop packets.
- In ACLs applied to PBR route-maps, permit and deny rules specify criteria for route-map decisions.
- In ACLs applied to NPB route-maps, permit and deny rules are mechanisms to exclude certain traffic flows from set statements.

The following table describes the interactions between route-map permit and deny stanzas; and permit and deny rules in ACLs applied to those stanzas by **match { mac | ip | ipv4 } address acl** statements.

TABLE 3 Route-map stanza and ACL permit and deny interactions

Stanza	ACL rule	Resulting TCAM action
Permit	Permit	The **set** statement or statements are applied.

TABLE 3 Route-map stanza and ACL permit and deny interactions (continued)

Stanza	ACL rule	Resulting TCAM action
Permit	Deny	Packets that match a **deny** keyword are denied from using the stanza **set** statement: • NPB: The packet is dropped. • PBR: The packet is routed as normal.
Deny	Permit	No action is taken: • NPB: The packet is dropped. • PBR: The packet is routed as normal.
Deny	Deny	If there are no subsequent matches, the packet is forwarded.

Priority among Layer 2 and Layer 3 match acl statements

In general, forwarding priority is determined by the first match in the lowest-numbered stanza. However, there are exceptions to this priority, if a route map contains match statements from both of the following groups:

- Layer 2: **match mac address acl**
- Layer 3: **match ip address acl** and **match ipv6 address acl**

Priority among Layer 2 and Layer 3 **match acl** statements is as follows:

- If the match within one ACL is on a permit rule and the match in the other ACL is on a deny rule, the permit match is accepted and the deny match is ignored.
- If both matches are on permit rules, the Layer 3 match is accepted and the Layer 2 match is ignored.
- If there are both IPv4 and IPv6 matches, the first match in the lowest-numbered stanza is accepted and other matches are ignored.

Basic NPB configuration

This section includes elements common to all SLX-OS NPB implementations

Setting NPB as the system mode

Before enabling Network Packet Broker (NPB), you must set NPB as the system mode.

Accessing NPB mode requires a license. For details, refer to the *Extreme SLX-OS Software Licensing Guide for SLX 9140 and SLX 9240*.

1. Enter **configure terminal** to access global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter **hardware** to access hardware configuration mode.

   ```
   device(config)# hardware
   ```

3. Enter **system-mode npb** to change the system mode to NPB.

```
device(config-hardware)# system-mode npb
%Warning: To activate the new system-mode config, please reboot the system using 'reload system'.
```

To return to default system mode from NPB system mode, enter **system-mode default** rather than **system-mode npb**.

4. Enter **end** to access privileged EXEC mode.

```
device(config-hardware)# end
```

5. To reboot the system, effecting the system mode change, enter **reload system**.

```
device# reload system
Warning: This operation will cause the chassis to reboot and requires all existing telnet,
secure telnet and SSH sessions to be restarted.
Unsaved configuration will be lost.
Please run `copy running-config startup-config` to save the current configuration if not done
already.
Are you sure you want to reboot the chassis [y/n]?
```

6. Press **y** and then **Enter**.

Creating ACLs for NPB

For NPB traffic aggregation and traffic replication, an access-control list (ACL) is required.

1. Enter **configure terminal** to access global configuration mode.

```
device# configure terminal
```

2. Enter the **{ mac | ip | ipv6 } access-list** command to create an ACL.

```
device# ip access-list standard aclNPB_01
```

3. Create one or more permit or deny rules.

```
device(conf-ipacl-std)# permit host 192.1.1.1 count
```

> NOTE
> A **deny** rule specifies that a matching packet is "denied" from using the **set** statement. For details, refer to NPB overview on page 11.

Aggregating traffic from interfaces

This task aggregates and forwards traffic from multiple interfaces to a single, physical egress interface.

1. Configure an ACL, as described in Creating ACLs for NPB on page 15.

```
device(config)# ip access-list standard aclNPB_01
device(conf-ipacl-std)# permit host 192.1.1.1 count
device(conf-ipacl-std)# exit
device(config)#
```

2. Configure a route map that contains the relevant **match { mac | ip | ipv6 } address acl** command.

```
device(config)# route-map npb_map1 permit 1
device(config-route-map-npb_map1/permit/1)# match ip address acl acl_2
```

> **NOTE**
> For a MAC ACL, use the **match mac address acl** command. For an IPv6 ACL, use the **match ipv6 address acl** command.

3. Specify the route-map egress physical interface.

```
device(config-route-map-npb_map1/permit/1)# set interface ethernet 0/5
device(config-route-map-npb_map1/permit/1)# exit
```

4. Apply the route map to the ingress interfaces.

   • Physical interfaces

```
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# npb policy route-map npb_map1
```

   • Port-channel interfaces

```
device(config)# interface port-channel 10
device(config-Port-channel-10)# npb policy route-map npb_map1
```

The following example configures ingress traffic from Ethernet 0/1 and port-channel 100 to egress Ethernet 0/5.

```
device# configure terminal
device(config)# route-map npb_map permit 10
device(config-route-map-npb_map/permit/10)# match ip address acl acl_2
device(config-route-map-npb_map/permit/10)# set interface ethernet 0/5
device(config-route-map-npb_map/permit/10)# exit
device(config)# interface ethernet 0/1
device(conf-if-eth-0/1)# npb policy route-map npb_map
device(conf-if-eth-0/1)# exit
device(config)# interface port-channel 100
device(config-Port-channel-100)# npb policy route-map npb_map
```

Replication to multiple interfaces

Traffic on an ingress interface is replicated and forwarded on multiple egress interfaces, usually to multiple monitoring tools.

The replication ingress-interface is one physical or port-channel interface.

Multiple physical and port-channel egress interfaces are supported. However, you first need to associate such interfaces with a Transparent VLAN flooding (TVF) domain. You then use a route map to designate that TVF domain as egress. Ingress traffic is replicated, and forwarded by way of the TVF to the egress interfaces that you specified.

Transparent VLAN flooding

Transparent VLAN flooding (TVF) forwards packets without any form of CPU intervention, including MAC learning and MAC destination lookups.

This implementation of TVF has the following attributes:

   • Traffic is distributed in hardware to all members of the TVF domain.
   • Because this feature does not use any MAC address entries in the CAM, it is useful when MAC address entries need to be conserved.

- You can create as many as 4096 TVF domains.

- Domain members can be tagged and untagged ports. There is no software limitation on the number of member ports.

- You can mix and match ports with different speeds.

- At the TVF domain level, load balancing does not occur. If you need load balancing, associate a port-channel with the TVF domain, which balances the loads among the interfaces included in the port-channel.

- CPU intervention is not required, enabling line-rate traffic forwarding.

Creating TVF domains

This task creates one or more Transparent VLAN flooding (TVF) domains.

1. Enter **configure terminal** to access global configuration mode.

    ```
    device# configure terminal
    ```

2. Enter the **tvf-domain** command, specifying one of the valid formats.

    - To create one TVF domain, specify an integer from 1 through 4096.

        ```
        device(config)# tvf-domain 10
        ```

    - To specify a range of TVF domains, insert a hyphen (-) between the beginning and ending integers.

        ```
        device(config)# tvf-domain 20-30
        ```

    - To specify individual domains and ranges of domains, separate them with commas (for example, 1,5-7,55).

        ```
        device(config)# tvf-domain 1,5-7,55
        ```

3. Enter **exit** to return to global configuration mode.

    ```
    device(config-tvf-domain-10)# exit
    device(config)#
    ```

Assigning a TVF domain to a physical egress interface

This task assigns a TVF domain to a physical egress interface.

1. Enter **configure terminal** to access global configuration mode.

    ```
    device# configure terminal
    ```

2. Enter the **interface ethernet** command to access interface configuration mode.

    ```
    device(config)# interface ethernet 0/5
    ```

3. Enter the **tvf-domain** command, specifying one of the valid formats.
   - To assign one TVF domain to the interface, specify its integer ID.

     ```
     device(conf-if-eth-0/5)# tvf-domain add 10
     ```

   - To assign a range of TVF domains to the interface, insert a hyphen (-) between the beginning and ending integers.

     ```
     device(conf-if-eth-0/5)# tvf-domain add 20-30
     ```

   - To assign individual domains and ranges of domains, separate them with commas (for example, 1,5-7,55).

     ```
     device(conf-if-eth-0/5)# tvf-domain add 1,5-7,55
     ```

   - To assign all defined TVF domains to the interface, enter **tvf-domain all**.

     ```
     device(conf-if-eth-0/5)# tvf-domain all
     ```

   - To assign all defined TVF domains to the interface—except for those specified—enter the **tvf-domain except** option.

     ```
     device(conf-if-eth-0/5)# tvf-domain except 1,2,4-7
     ```

Assigning a TVF domain to a port-channel egress interface

This task assigns a TVF domain to a port-channel egress interface.

1. Enter **configure terminal** to access global configuration mode.

   ```
   device# configure terminal
   ```

2. Enter the **interface port-channel** command to access port-channel configuration mode.

   ```
   device(config)# interface port-channel 10
   ```

3. Enter the **tvf-domain** command, specifying one of the valid formats.
   - To assign one TVF domain to the interface, specify its integer ID.

     ```
     device(config-Port-channel-10)# tvf-domain add 10
     ```

   - To assign a range of TVF domains to the interface, insert a hyphen (-) between the beginning and ending integers.

     ```
     device(config-Port-channel-10)# tvf-domain add 20-30
     ```

   - To assign individual domains and ranges of domains, separate them with commas (for example, 1,5-7,55).

     ```
     device(config-Port-channel-10)# tvf-domain add 1,5-7,55
     ```

   - To assign all defined TVF domains to the interface, enter **tvf-domain all**.

     ```
     device(config-Port-channel-10)# tvf-domain all
     ```

   - To assign all defined TVF domains to the interface—except for those specified—enter the **tvf-domain except** option.

     ```
     device(config-Port-channel-10)# tvf-domain except 1,2,4-7
     ```

Replicating traffic to multiple interfaces

This task replicates traffic entering an interface to multiple egress interfaces.

1. Create needed TVF domains, as described in Creating TVF domains on page 17.

   ```
   device# configure terminal
   device(config)# tvf-domain 10
   device(config-tvf-domain-10)# exit
   ```

2. Assign TVF domains to the egress interfaces.

   • Physical interfaces (For details, refer to Assigning a TVF domain to a physical egress interface on page 17.)

   ```
   device(config)# interface ethernet 0/5
   device(conf-if-eth-0/5)# tvf-domain add 10
   ```

   • Port-channel interfaces

   ```
   device(config)# interface port-channel 10
   device(config-Port-channel-10)# tvf-domain add 10
   ```

3. Configure an ACL, as described in Creating ACLs for NPB on page 15.

   ```
   device(config)# ip access-list standard aclNPB_01
   device(conf-ipacl-std)# permit host 192.1.1.1 count
   device(conf-ipacl-std)# exit
   ```

4. Configure a route map that contains the relevant **match { mac | ip | ipv6 } address acl** command.

   ```
   device(config)# route-map npb_map1 permit 1
   device(config-route-map-npb_map1/permit/1)# match ip address acl acl_2
   ```

5. Specify the TVF domain that contains the egress interfaces for the replicated traffic.

   ```
   device(config-route-map-npb_map1/permit/1)# set next-hop-tvf-domain 5
   ```

6. Apply the route map to the ingress interface.

   • Physical interface

   ```
   device(config)# interface ethernet 0/2
   device(conf-if-eth-0/2)# npb policy route-map npb_map1
   ```

   • Port-channel interface

   ```
   device(config)# interface port-channel 10
   device(config-Port-channel-10)# npb policy route-map npb_map1
   ```

The following example replicates traffic entering an interface to multiple egress interfaces.

```
device# configure terminal
device(config)# tvf-domain 10
device(config-tvf-domain-10)# exit
device(config)# interface ethernet 0/5
device(conf-if-eth-0/5)# tvf-domain add 10
device(conf-if-eth-0/5)# exit
device(config)# interface port-channel 10
device(config-Port-channel-10)# tvf-domain add 10
device(config-Port-channel-10)# exit
device(config)# route-map npb_map1 permit 1
device(config-route-map-npb_map1/permit/1)# match ip address acl acl_2
device(config-route-map-npb_map1/permit/1)# set next-hop-tvf-domain 5
device(config-route-map-npb_map1/permit/1)# exit
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# npb policy route-map npb_map1
```

Forwarding traffic to a port-channel

For load balancing, this task forwards traffic entering an interface to a port-channel.

1. Configure an ACL, as described in .

   ```
   device# configure terminal
   device(config)# ip access-list standard aclNPB_01
   device(conf-ipacl-std)# permit host 192.1.1.1 count
   device(conf-ipacl-std)# exit
   ```

2. Configure a route map that contains the relevant **match { mac | ip | ipv6 } address acl** command.

   ```
   device(config)# route-map npb_map1 permit 1
   device(config-route-map-npb_map1/permit/1)# match ip address acl aclNPB_01
   ```

3. Specify the egress port-channel interface.

   ```
   device(config-route-map-npb_map1/permit/1)# set interface port-channel 10
   device(config-route-map-npb_map1/permit/1)# exit
   ```

4. Apply the route map to a single ingress interface:

   • Physical interface

   ```
   device(config)# interface ethernet 0/2
   device(conf-if-eth-0/2)# npb policy route-map npb_map1
   ```

   • Port-channel interface

   ```
   device(config)# port-channel 5
   device(config-Port-channel-10)# npb policy route-map npb_map1
   ```

The following example forwards traffic entering a physical interface to a port-channel.

```
device# configure terminal
device(config)# ip access-list standard aclNPB_01
device(conf-ipacl-std)# permit host 192.1.1.1 count
device(conf-ipacl-std)# exit
device(config)# route-map npb_map1 permit 1
device(config-route-map-npb_map1/permit/1)# match ip address acl aclNPB_01
device(config-route-map-npb_map1/permit/1)# set interface port-channel 10
device(config-route-map-npb_map1/permit/1)# exit
device(config)# interface ethernet 0/2
device(conf-if-eth-0/2)# npb policy route-map npb_map1
```

NPB show commands

There are several show commands that display Network Packet Broker (NPB) information, as listed in the following table.

TABLE 4 NPB show commands in the *Command Reference*

Command	Description
show route-map	Displays configuration details of all route maps, of a specified route map, or of the route map applied to an interface.
show running-config tvf-domain	Displays configuration details of one or all TVF domains.