

IP Routing Protocol-Independent Commands

This chapter contains the following sections:

- accept-lifetime, on page 2
- directed-broadcast, on page 4
- ip policy route-map, on page 5
- ip redirects, on page 7
- ip route, on page 8
- ip routing, on page 10
- key-string, on page 11
- key (key chain), on page 12
- key chain, on page 14
- send-lifetime, on page 16
- show ip protocols, on page 18
- show ip route, on page 19
- show ip route summary, on page 20
- show key chain, on page 21

accept-lifetime

To set the time period during which the authentication key on a key chain is received as valid, use the a**ccept-lifetime** command inkey chain key configuration mode. To revert to the default value, use the **no** form of this command.

Syntax

accept-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no accept-lifetime

Parameters

- ***start-time***—Beginning time that the key specified by the key command is valid to be received. The syntax can be either of the following:
  - *hh*:*mm*:*ss Month date year*
  - *hh*:*mm*:*ss date Month year*
  - *hh*—hours (0-23)
  - *mm*—minutes (0-59)
  - *ss*—seconds (0-59)
  - *Month*—first three letters of the month
  - date—date (1-31)
  - year—year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

- **infinite**—Key is valid to be received from the *start-time* value on.
- ***end-time***—Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
- **duration** *seconds*—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default time period during which the authentication key is valid for authenticating incoming packets is set to **Forever**.

The definition of **Forever** is: the starting time is January 1, 2000, and the ending time is infinite.

Command Mode

Key Chain Key Configuration mode

User Guidelines

The switch checks **Time-of-Date** again a value of the *start-time* argument *regardless if* **Time-of-Date** is not set by management or by SNTP because of the default value of Time-of-Date always is an passed time.

If validation of the value of the *start-time* argument was passed and the *end-time* argument is configured and its value is **infinite** the key is considered as actual *regardless if* **Time-of-Date** is not set by management or by SNTP.

If **Time-of-Date** is not set by management or by SNTP and if the *end-time* argument is configured with a value differing from **infinite** or the **duration** parameter is configured, the key is considered as expired.

If **Time-of-Date** is set by management or by SNTP, the switch checks **Time-of-Date** again a value of the *end-time* argument or of the **duration** parameter.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called keychain1. The key named string1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named string2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)#  ip rip authentication key-chain keychain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain keychain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string string1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string string2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
```

directed-broadcast

Use the **directed-broadcast** IP Interface Configuration mode command to enable the translation of a directed broadcast to physical broadcasts. Use the **no** form of this command to disable this function.

Syntax

directed-broadcast

no directed-broadcast

Default Configuration

Translation of a directed broadcast to physical broadcasts is disabled. All IP directed broadcasts are dropped.

Command Mode

IP Configuration mode

Example

The following example enables the translation of a directed broadcast to physical broadcasts.

```
switchxxxxxx(config)# interface ip 192.168.1.1
switchxxxxxx(config-ip)# directed-broadcast
```

ip policy route-map

To enable policy routing on an interface and identify a route map, use the **ip policy route-map** command in Interface Configuration mode. To disable policy routing, use the **no** form of this command.

Syntax

ip policy route-map *map-tag*

no ip policy route-map

Parameters

- ***map-tag***—Name of the route map to use for policy routing.

Default Configuration

No policy routing occurs on the interface.

Command Mode

Interface Configuration mode

User Guidelines

Use the **ip policy route-map** command to enable policy routing on an interface. The actual policy routing will take a place if an IP address is defined on the interface.

The IP packets matched to the route-map conditions specified by the route map with the *map-tag* name will take a route depended on the action of the matched ACL:

- **permit**—The route specified by the set command Policy routing.
- **deny**—The route specified by the IP Forwarding table (regular routing).
- Name of the route map to use for policy routing.

The IP packets that are not matched, will be forwarded using the obvious shortest path.

IP policy routing on a Layer 2 interface is performed only when IP interface is defined, its status is UP, and the next hop is reachable. If the IP policy routing is not applied then the matched IP packets will be forwarded using the obvious shortest path.

Note. Of course, like in the case of regular IP Routing Policy Based IP Router routes only MAC "tome" IP frames. IP policy routing cannot be configured on an interface together with the following features:

- VLAN ACL

Example

The following example shows how to configure policy routing:

```
switchxxxxxx(config)# ip access-list extended pr-acl1
switchxxxxxx(config-ip-al)# permit tcp any any 156.12.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
```

```
switchxxxxxx(config)# ip access-list extended pr-acl2
switchxxxxxx(config-ip-al)# permit tcp any any 156.122.5.0 0.0.0.255 any
switchxxxxxx(config-ip-al)# exit
switchxxxxxx(config)# route-map pbr 10
switchxxxxxx(config-route-map)# match ip address access-list pr-acl1
switchxxxxxx(config-route-map)# set ip next-hop 56.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# route-map pbr 20
switchxxxxxx(config-route-map)# match ip address access-list pr-acl2
switchxxxxxx(config-route-map)# set ip next-hop 50.1.1.1
switchxxxxxx(config-route-map)# exit
switchxxxxxx(config)# interface vlan 1
switchxxxxxx(config-if)# ip policy route-map pbr
switchxxxxxx(config-if)# exit
```

ip redirects

Use the **ip redirects** command in IP Interface Configuration mode to enable the sending of ICMP redirect messages to re-send a packet through the same interface on which the packet was received. To disable the sending of redirect messages, use the **no** form of this command.

Syntax

ip redirects

no ip redirects

Default Configuration

The sending of ICMP redirect messages is enabled.

Command Mode

IP Configuration mode

Example

The following example disables the sending of ICMP redirect messages on IP interface 1.1.1.1 and re-enables the messages on IP interface 2.2.2.2:

```
switchxxxxxx(config)# interface ip 1.1.1.1
switchxxxxxx(config-ip)# no ip redirects
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# interface ip 2.2.2.2
switchxxxxxx(config-ip)# ip redirects
switchxxxxxx(config-ip)# exit
```

ip route

To establish static routes, use the **ip route** command in global configuration mode. To remove static routes, use the **no** form of this command.

Syntax

ip route *prefix* {*mask* | */prefix-length*} {{*ip-address* [**metric** *value*]} | **reject-route**}

no ip route *prefix* {*mask* | */prefix-length*} [*ip-address*]

Parameters

- ***prefix***—IP route prefix for the destination.
- ***mask***—Prefix mask for the destination.
- ***/ prefix-length***—Prefix mask for the destination.Specifies the number of bits that comprise the IP address prefix. The prefix length must be preceded by a forward slash (/). (Range: 0–32)
- ***ip-address***—IP address of the next hop that can be used to reach that network.
- **metric** *value*—Metric of the route. The default metric is 4 for the Next Hop on an In-Band interface and 2 for the Next Hop on OOB. Range: 1–255.
- **reject-route**—Stopping routing to the destination network.

Default Configuration

No static routes are established.

Command Mode

Global Configuration mode

User Guidelines

Use the **no ip route** command without the i*p-address* parameter to remove all static routes to the given subnet.

Use the **no ip route** command with the *ip-address* parameter to remove only one static route to the given subnet via the given next hop.

Example 1—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using mask:

```
switchxxxxxx(config)# ip route 172.31.0.0 255.255.0.0 172.31.6.6 metric 2
```

Example 2—The following example shows how to route packets for network 172.31.0.0 to a router at 172.31.6.6 using prefix length :

```
switchxxxxxx(config)# ip route 172.31.0.0 /16 172.31.6.6 metric 2
```

Example 3—The following example shows how to reject packets for network 194.1.1.0:

```
switchxxxxxx(config)# ip route 194.1.1.0 255.255.255.0 reject-route
```

Example 4—The following example shows how to remove all static routes to network 194.1.1.0/24:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24
```

Example 5—The following example shows how to remove one static route to network 194.1.1.0/24 via 1.1.1.1:

```
switchxxxxxx(config)# no ip route 194.1.1.0 /24 1.1.1.1
```

ip routing

To enable IP routing, use the **ip routing** command in global configuration mode. To disable IP routing, use the **no** form of this command.

Syntax

ip routing

no ip routing

Parameters

This command has no arguments or keywords.

Default Configuration

IP routing is enabled.

Command Mode

Global Configuration mode.

User Guidelines

Use the command to enable IP Routing.

The switch supports one IPv4 stack on in-band interfaces and the OOB port.

The IP stack is always running on the OOB port as an IP host regardless whether IP routing is enabled. The switch blocks routing between in-band interfaces and the OOB interface. In the case when there are two best routes - one via an in-band and one via the OOB port, the switch will use the route via the OOB port.DHCP Relay and IP Helper cannot be enabled on the OOB port. Routing protocols cannot be enabled on the OOB port. The IP subnet defined on the OOB port is not redistributed to routing protocols running on in-band interfaces.

Example

The following example enables IP routing:

```
switchxxxxxx(config)# ip routing
```

key-string

To specify the authentication string for a key, use the **key-string** command in key chain key configuration mode. To remove the authentication string, use the **no** form of this command.

Syntax

key-string *text*

no key-string

Parameters

- ***text***—Specifies the authentication string. The string can contain from 1 to 16 characters.

Default Configuration

No key exists.

Command Mode

Key Chain Key Configuration mode

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# version 2
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# exit
```

key (key chain)

To identify an authentication key on a key chain, use the **key** command in key-chain configuration mode. To remove the key from the key chain, use the **no** form of this command.

Syntax

key *key-id*

no key *key-id*

Parameters

- ***key-id***—Identification number of an authentication key on a key chain. The range of keys is from 1 to 255. The key identification numbers need not be consecutive. The scope of a key identification number is the key chain where the key is defined.

Default Configuration

No key exists on the key chain.

Command Mode

Key-Chain Configuration mode

User Guidelines

It is useful to have multiple keys on a key chain so that the software can sequence through the keys as they become invalid after time, based on the **accept-lifetime** and **send-lifetime** key chain key command settings.

Each key has its own key identifier, which is stored locally. The combination of the key identifier and the interface associated with the message uniquely identifies the authentication algorithm and authentication key in use. Only one authentication packet is sent, regardless of the number of valid keys. The software starts looking at the lowest key identifier number and uses the first valid key.

If the last key expires, authentication will be finished with error.

To remove all keys, remove the key chain by using the **no key chain** command.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key 1
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
```

```
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

key chain

To enable authentication for routing protocols, identify a group of authentication keys by using the **key chain** command in global configuration mode. To remove the key chain, use the **no** form of this command

Syntax

key chain *name-of-chain*

no key chain *name-of-chain*

Parameters

- ***name-of-chain***—Name of a key chain. The chain-name may have from 1 to 32 characters. A key chain must have at least one key and can have up to 256 keys.

Default Configuration

No key chain exists.

Command Mode

Global Configuration mode

User Guidelines

You must configure a key chain with keys to enable authentication.

Although you can identify multiple key chains, we recommend using one key chain per interface per routing protocol. Upon specifying the key chain command, you enter **key-chain** configuration mode.

Example

The following example configures a key chain named chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or a discrepancy in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 2011 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 2011 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
```

```
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
```

send-lifetime

To set the time period during which an authentication key on a key chain is valid to be sent, use the **send-lifetime** command in Key Chain Key configuration mode. To revert to the default value, use the **no** form of this command.

Syntax

send-lifetime *start-time* {**infinite** | *end-time* | **duration** *seconds*}

no send-lifetime

Parameters

- ***start-time***—Beginning time that the key specified by the **key** command is valid to be received. The syntax can be either of the following:
  - *hh*:*mm*:*ss Month date year*
  - *hh*:*mm*:*ss date Month year*
  - *hh*—hours (0-23)
  - *mm*—minutes (0-59)
  - *ss*—seconds (0-59)
  - *Month*—first three letters of the month
  - date—date (1-31)
  - year—year (four digits)

The default start time and the earliest acceptable date is January 1, 2000.

- **infinite**—Key is valid to be received from the *start-time* value on.
- ***end-time***—Key is valid to be received from the *start-time* value until the *end-time* value. The syntax is the same as that for the *start-time* value. The *end-time* value must be after the *start-time* value. The default end time is an infinite time period.
- **duration** *seconds*—Length of time (in seconds) that the key is valid to be received. The range is from 1 to 2147483646.

Default Configuration

The default time period during which the authentication key is valid for authenticating incoming packets is set to forever.

Forever (the starting time is January 1, 2000, and the ending time is infinite)

Command Mode

Key Chain Key Configuration mode

User Guidelines

Specify a *start-time* value and one of the following values: **infinite** *end-time*, or **duration** *seconds*.

A key is considered as expired if Time-of-Date is not set by management or by SNTP.

If the last key expires, authentication will be finished with error.

Example

The following example configures a key chain called chain1. The key named key1 will be accepted from 1:30 p.m. to 3:30 p.m. and be sent from 2:00 p.m. to 3:00 p.m. The key named key2 will be accepted from 2:30 p.m. to 4:30 p.m. and be sent from 3:00 p.m. to 4:00 p.m. The overlap allows for migration of keys or discrepancies in the set time of the router. There is a 30-minute leeway on each side to handle time differences:

```
switchxxxxxx(config)# router rip
switchxxxxxx(config-rip)# network 172.19.1.1
switchxxxxxx(config-rip)# exit
switchxxxxxx(config)# interface ip 172.19.1.1
switchxxxxxx(config-ip)# ip rip authentication mode md5
switchxxxxxx(config-ip)# ip rip authentication key-chain chain1
switchxxxxxx(config-ip)# exit
switchxxxxxx(config)# key chain chain1
switchxxxxxx(config-keychain)# key 1
switchxxxxxx(config-keychain-key)# key-string key1
switchxxxxxx(config-keychain-key)# accept-lifetime 13:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 14:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# key 2
switchxxxxxx(config-keychain-key)# key-string key2
switchxxxxxx(config-keychain-key)# accept-lifetime 14:30:00 Jan 25 1996 duration 7200
switchxxxxxx(config-keychain-key)# send-lifetime 15:00:00 Jan 25 1996 duration 3600
switchxxxxxx(config-keychain-key)# exit
switchxxxxxx(config-keychain)# exit
```

show ip protocols

To display the parameters and current state of the active IP routing protocol processes, use the **show ip protocols** command in user EXEC or privileged EXEC mode.

Syntax

show ip protocols [**summary**]

Parameters

- **summary**—Displays the configured routing protocol process names.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

The information displayed by the **show ip protocols** command is useful in debugging routing operations.

Example 1. The following is sample output from the **show ip protocols** command, showing active routing protocols:

```
switchxxxxxx# show ip protocols
IP Routing Protocol is "rip"
Interfaces  IP Addresses
VLAN 1    12.1.1.1
VLAN 1    150.23.12.2
VLAN 11   1.1.1.1
```

Example 2. The following is sample output from the **show ip protocols** command with the **summary** keyword:

```
switchxxxxxx# show ipv6 protocols summary
IP Routing Protocol is "rip"
```

show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

Syntax

show ip route [**address** *ip-address* {*mask* [**longer-prefixes**]} [*protocol* | **static** | **rejected** | **icmp | connected**]

Parameters

- **address** *ip-address*—IP address about which routing information should be displayed.
- ***mask***—The value of the subnet mask.
- **longer-prefixes**—Specifies that only routes matching the IP address and mask pair should be displayed.
- ***protocol***—The name of the origin of the protocol to be displayed. Use one of the following arguments:
- **rip**—Displays routes added by RIP
- **connected**—Displays connected routes.
- **icmp**—Displays routes added by ICMP Direct.
- **rejected**—Displays rejected routes.
- **static**—Displays static routes.

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Use this command without parameters to display the whole IPv4 Routing table.

Use this command with parameters to specify required routes.

Example 1. The following is sample output from the **show ip route** command when IP Routing is not enabled:

```
switchxxxxxx# show ip route
Maximum Parallel Paths: 1 (1 after reset)IP Forwarding: disabled
Codes: > - best, C - connected, S - static, I - ICMP
IP Routing Table - 5 entries
Code IP Route Distance/ Next Hop Last Time Outgoing
 Metric IP Address Updated Interface
------ ------------------- ----------- --------------- ------------- ------------
S 10.10.0.0/16 1/2 10.119.254.244 00:02:22 vlan2
S> 10.10.0.0/16 1/1 10.120.254.244 00:02:22 vlan3
S> 10.16.2.0/24 1/1 10.119.254.244 00:02:22 vlan2
C> 10.119.0.0/16 0/1 0.0.0.0 vlan2
C> 10.120.0.0/16 0/1 0.0.0.0 vlan3
```

show ip route summary

Use the **show ip route summary** command in User EXEC or Privileged EXEC mode to display the current contents of the IP routing table in summary format.

Syntax

show ip route summary

Command Mode

User EXEC mode

Privileged EXEC mode

User Guidelines

Example

The following is sample output from the show **ip route summary** command:

```
switchxxxxxx# show ip route summary
IP Routing Table Summary - 90 entries
35 connected, 25 static, 12 RIP
Number of prefixes:
/16: 16, /18: 10, /22: 15, /24: 15, /28: 2, /30: 12
```

show key chain

To display authentication key information, use the **show key chain** command in Privileged EXEC mode.

Syntax

show key chain [*name-of-chain*]

Parameters

- ***name-of-chain***—Name of the key chain to display, as named in the key chain command.

Default Configuration

Information about all key chains is displayed.

Command Mode

Privileged EXEC mode

Example 1. The following is sample output from the **show key chain** command when the current time of date is defined:

```
switchxxxxxx# show key chain
Current Time of Date is Feb 8 2011
Accept lifetime is configured to ignore
Key-chain trees:
key 1 -- text "chestnut"
accept lifetime (always valid) - (always valid) [valid now]
send lifetime (always valid) - (always valid) [valid now]
key 2 -- text "birch"
accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)
send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)[valid now]
```

Example 2. The following is sample output from the **show key chain** command when the current time of date is not defined:

```
switchxxxxxx# show key chain
Current Time of Date is not defined
Accept lifetime is ignored
Key-chain trees:
key 1 -- text "chestnut"
accept lifetime (always valid) - (always valid) [valid now]
send lifetime (always valid) - (always valid) [valid now]
key 2 -- text "birch"
accept lifetime (00:00:00 Dec 5 2010) - (23:59:59 Dec 5 2010)
send lifetime (06:00:00 Dec 5 2010) - (18:00:00 Dec 5 2016)
```