High Availability Command Reference

This chapter describes commands to configure high availability.

crashdump-timeout

To set the longest time that the newly active fabric card waits before reloading the previously active fabric card, use the **crashdump-timeout** command in redundancy mode. To reset the default time that the newly active fabric card waits before reloading the previously active fabric card, use the **no** form of this command.

crashdump-timeout [*mm* | *hh:mm*]

Syntax Description

mm	(Optional) Time, in minutes, that the newly active fabric card waits before reloading the previously active fabric card. The range is from 5 to 1080 minutes.
hh:mm	(Optional) Time, in hours and minutes, that the newly active fabric card waits before reloading the previously active fabric card. The range is from 5 minutes to 18 hours.

Command Default

The default timeout for this command is 5 minutes.

Command Modes

Redundancy mode (config-red)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Use this command to specify the length of time that the newly active fabric card waits before reloading the previously active fabric card.

Examples

The following example shows how to set the time before the previously active fabric card is reloaded.

```
Router(config-red)# crashdump-timeout 10
```

network area

To define the interfaces on which Open Shortest Path First (OSPF) protocol runs and to define the area ID for those interfaces, use the **network area** command in router configuration mode. To disable OSPF routing for the interfaces, use the **no** form of this command.

network *ip-address wildcard-mask* **area** *area-id*
no network *ip-address wildcard-mask* **area** *area-id*

Syntax Description

ip-address	IP address.
wildcard-mask	Wild card mask address.
area-id	Area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. To associate areas with IP subnets, specify a subnet address as the value of the *area-id* argument.

Command Default

This command is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

The *ip-address* and *wildcard-mask* arguments together enable one or multiple interfaces to be associated with a specific OSPF area using a single command. To associate areas with IP subnets, specify a subnet address as the value of the *area-id* argument.

Examples

The following example shows how to initialize OSPF routing process 109, and defines four OSPF areas.

```
Router(config)# interface TenGigabitEthernet4/1
Router(config-if)# ip address 209.165.200.225 255.255.255.0
Router(config)# router ospf 109
Router(config-router)# network 209.165.200.226 0.0.0.255 area 10.9.50.0
Router(config-router)# network 209.165.200.227 0.0.255.255 area 2
Router(config-router)# network 209.165.200.228 0.0.0.255 area 3
Router(config-router)# network 0.0.0.0 255.255.255.255 area 0
```

Related Commands

Command	Description
router ospf	Configures an OSPF routing process.

nsf cisco

To enable Cisco Nonstop Forwarding (NSF) operations on a router that is running the Open Shortest Path First (OSPF) protocol, use the **nsf cisco** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf cisco [**enforce global** | **helper** [**disable**]]
no nsf cisco [**enforce global** | **helper** [**disable**]]

Syntax Description

enforce global	(Optional) Cancels Cisco NSF restart on all the interfaces when neighboring networking devices that are not NSF-aware are detected on any interface during the restart process.
helper	(Optional) Configures Cisco NSF helper mode.
disable	(Optional) Disables Cisco NSF helper mode.

Command Default

Cisco NSF restarting mode is disabled but helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables Cisco NSF on an OSPF router. When the Cisco NSF is enabled on a router, the router is Cisco NSF capable and will operate in restarting mode.

By default, neighboring Cisco NSF-aware routers operate in NSF helper mode during a graceful restart. To disable Cisco NSF helper mode on a Cisco NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on a Cisco NSF-aware router, use the **no nsf cisco helper disable** command.

If neighbors that are not Cisco NSF-aware are detected on a network interface during a Cisco NSF graceful restart, restart is aborted only on that interface and continues on other interfaces. To cancel restart for the entire OSPF process when neighbors that are not Cisco NSF-aware are detected during restart, configure this command with the **enforce global** keywords.

Examples

The following example shows how to enable Cisco NSF restarting mode on a router. This example causes the Cisco NSF restart to be canceled for the entire OSPF process if neighbors that are not Cisco NSF-aware are detected on any network interface during the restart.

```
Router(config)# router ospf 24
Router(config-router)# nsf cisco enforce global
```

Related Commands

Command	Description
nsf ietf	Enables IETF NSF.

nsf ietf

To configure Internet Engineering Task Force (IETF) Nonstop Forwarding (NSF) operations on a router that is running Open Shortest Path First (OSPF), use the **nsf ietf** command in router configuration mode. To return to the default, use the **no** form of this command.

nsf ietf [**restart-interval** *seconds* | **helper** [**disable** | **strict-lsa-checking**]]
no nsf ietf [**restart-interval** | **helper** [**disable** | **strict-lsa-checking**]]

Syntax Description

restart-interval *seconds*	(Optional) Specifies length of the graceful restart interval, in seconds. The range is from 1 to 1800. The default value is 120 seconds.
helper	(Optional) Configures IETF NSF helper mode.
disable	(Optional) Disables helper mode on an IETF NSF-aware router.
strict-lsa-checking	(Optional) Enables strict link-state advertisement (LSA) checking for helper mode.

Command Default

IETF NSF graceful restart mode is disabled but the helper mode is enabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command enables IETF NSF on an OSPF router. When IETF NSF is enabled on a Cisco router, the router is IETF NSF-capable and will operate in restarting mode.

By default, neighboring IETF NSF-aware routers operate in IETF NSF helper mode during a graceful restart. To disable IETF NSF helper mode on an IETF NSF-aware router, use this command with the **disable** keyword. To reenable helper mode after explicitly disabling helper mode on an IETF NSF-aware router, use the **no nsf ietf helper disable** command.

Strict LSA checking enables a router in IETF NSF helper mode to terminate the graceful restart process if it detects a changed LSA that would cause flooding during the graceful restart process. Configure strict LSA checking on IETF NSF-aware and IETF NSF-capable routers but it is effective only when the router is in helper mode.

Examples

The following example shows how to enable IETF NSF restarting mode on a router and changes the graceful restart interval from default (120 seconds) to 200 seconds:

```
Router(config)# router ospf 24
Router(config-router)# nsf ietf restart-interval 200
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF.

router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

router ospf *process-id*
no router ospf *process-id*

Syntax Description

process-id	Identification parameter internally used for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.

Command Default

OSPF routing process is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

You can specify multiple OSPF routing processes in each router.

Examples

The following example shows how to configure an OSPF routing process and assign a process number of 109.

```
Router(config)# router ospf 109
```

Related Commands

Command	Description
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

show cef nsf

To display the current Cisco Nonstop Forwarding (NSF) state of Cisco Express Forwarding on both the active and standby fabric cards, use the **show cef nsf** command in privileged EXEC mode.

show cef nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the **show cef nsf** command is entered before a switchover occurs, no switchover activity is reported. After a switchover occurs, enter the **show cef nsf** command to display details about the switchover as reported by the newly active fabric card.

Examples

The following is a sample output from the **show cef nsf** command.

```
Router# show cef nsf

Last switchover occurred: 00:01:30.088 ago
Routing convergence duration: 00:00:34.728
FIB stale entry purge durations:00:00:01.728 - Default
00:00:00.088 - Red
Switchover
Slot Count Type Quiesce Period
1 2 sso 00:00:00.108
2 1 rpr+ 00:00:00.948
3 2 sso 00:00:00.152
5 2 sso 00:00:00.092
6 1 rpr+ 00:00:00.632
No NSF stats available for the following linecards:4 7
```

Related Commands

Command	Description
show cef state	Displays the state of Cisco Express Forwarding on a networking device.

show cef state

To display the state of Cisco Express Forwarding on a networking device, use the **show cef state** command in privileged EXEC mode.

show cef state

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following example shows how to verify that Cisco Express Forwarding is Cisco NSF capable.

```
Router# show cef state

CEF Status:
RP instance
common CEF enabled
IPv4 CEF Status:
CEF enabled/running
dCEF enabled/running
CEF switching enabled/running
universal per-destination load sharing algorithm, id 7E0E20AE
RRP state:
I am standby RRP: no
RF Peer Presence: yes
RF Peer Comm reached: yes
RF Peer Config done: yes
RF Progression blocked: unblocked (blocked for 00:00:00.588)
Redundancy mode: sso(3)
CEF NSF sync: enabled/running
CEF ISSU Status:
FIBHWIDB broker
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
FIBIDB broker
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
FIBHWIDB Subblock broker
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
FIBIDB Subblock broker
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
Adjacency update
```

```
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
IPv4 table broker
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
CEF push
Slot(s): 3 5 40 (0x10000000028) (grp 0x37003204) - Not ISSU aware.
```

Related Commands

Command	Description
show cef nsf	Displays the current Cisco NSF state of Cisco Express Forwarding on both the active and standby fabric cards.

show ip ospf

To display general information about Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in user EXEC or privileged EXEC mode.

show ip ospf [*process-id*]

Syntax Description

process-id	(Optional) Process ID. If this argument is included, the information for the specified routing process is included.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf** command.

```
Router# show ip ospf 1

Routing Process "ospf 1" with ID 40.40.40.40
Start time: 00:01:08.623, Time elapsed: 1d00h
Supports only single TOS(TOS0) routes
Supports opaque LSA
```

Related Commands

Command	Description
show ip ospf neighbor	Displays OSPF neighbor information on a per-interface basis.
show ip ospf nsf	Displays IP OSPF NSF state information.

show ip ospf neighbor

To display Open Shortest Path First (OSPF) neighbor information on a per-interface basis, use the **show ip ospf neighbor** command in privileged EXEC mode.

show ip ospf neighbor [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

interface-type interface-number	(Optional) Type and number associated with a specific OSPF interface.
neighbor-id	(Optional) Neighbor hostname or IP address in A.B.C.D format.
detail	(Optional) Displays all the neighbors in detail.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf neighbor** command showing a single line of summary information for each neighbor.

```
Router# show ip ospf neighbor
```

```
Neighbor ID    Pri    State       Dead Time   Address       Interface
10.199.199.137 1     FULL/DR      0:00:31   192.168.80.37
TenGigabitEthernet 4/1
172.16.48.1    1     FULL/DROTHER 0:00:33   172.16.48.1
TenGigabitEthernet 4/2
```

The following is sample output from the **show ip ospf neighbor detail** command.

```
Router# show ip ospf neighbor detail
```

```
Neighbor 45.45.45.45, interface address 5.5.5.1
    In the area 0 via interface TenGigabitEthernet5/1
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 5.5.5.2 BDR is 5.5.5.1
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:39
    Neighbor is up for 00:00:57
    Index 3/3, retransmission queue length 0, number of retransmission 0
```

```
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 45.45.45.45, interface address 2.2.2.1
    In the area 0 via interface TenGigabitEthernet4/4
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 2.2.2.1 BDR is 2.2.2.2
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:37
    Neighbor is up for 00:03:54
    Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
Neighbor 45.45.45.45, interface address 1.1.1.1
    In the area 0 via interface TenGigabitEthernet5/3
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 1.1.1.2 BDR is 1.1.1.1
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR)
    Dead timer due in 00:00:38
    Neighbor is up for 00:00:59
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf nsf	Displays IP OSPF NSF state information.

show ip ospf nsf

To display IP Open Shortest Path First (OSPF) Nonstop Forwarding (NSF) state information, use the **show ip ospf nsf** command in user EXEC or privileged EXEC mode.

show ip ospf nsf

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>), Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is sample output from the **show ip ospf nsf** command.

```
Router# show ip ospf

Routing Process "ospf 1" with ID 192.168.2.1 and Domain ID 0.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Non-Stop Forwarding enabled, last NSF restart 00:02:06 ago (took 44 secs)
Area BACKBONE(0)
Number of interfaces in this area is 1 (0 loopback)
Area has no authentication
SPF algorithm executed 3 times
```

Related Commands

Command	Description
show ip ospf	Displays general information about OSPF routing processes.
show ip ospf neighbor	Displays OSPF neighbor information on a per-interface basis.

show issu capability

To display the In-Service Software Upgrade (ISSU) capability of a client, use the **show issu capability** command in user EXEC or privileged EXEC mode.

show issu capability {**entries** | **groups** | **types**} [*client_id*]

Syntax Description

entries	Displays a list of capability types and dependent capability types that are included in a single capability entry. Types within an entry can also be independent.
groups	Displays a list of capability entries based on the priority order (in the order that they are negotiated in a session).
types	Displays an ID that identifies a particular capability.
client_id	(Optional) Client registered to the ISSU infrastructure. To obtain a list of client IDs, use the **show issu clients** command.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

ISSU capability is a functionality where an ISSU client can support and is required to interoperate with peers. When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following example is a sample output of the **show issu capability types** command displaying the ISSU capability types for the IP host ISSU client (clientid=2082):

```
Router# show issu capability types 2082
```

```
Client_ID = 2082,  Entity_ID = 1 :
    Cap_Type = 0
```

Related Commands

Command	Description
show issu	Displays software upgrade information.
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu clients

To list the current ISSU clients, that is, the applications and protocols on the network supported by ISSU, use the **show issu clients** command in user EXEC or privileged EXEC mode.

show issu clients

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

To implement the ISSU versioning functionality, a client must first register its client capability, and client message information with the ISSU infrastructure during system initialization.

The **show issu clients** command lists all the ISSU clients currently operating in the network, along with their Client ID numbers and the number of entities each client contains.

Examples

The following is a sample output of the **show issu clients** command displaying the ISSU clients:

```
Router# show issu clients

 Client_ID = 1101,  Client_Name = ISSU NGXP CARD OIR client,  Entity_Count
 = 1
 Client_ID = 1102,  Client_Name = ISSU NGXP HAL RM Client,  Entity_Count
 = 1
 Client_ID = 1104,  Client_Name = ISSU NGXP MTM client,  Entity_Count =
1
 Client_ID = 1105,  Client_Name = ISSU NGXP PBMGR client,  Entity_Count
= 1
 Client_ID = 1106,  Client_Name = ISSU NGXP CIM IPC client,  Entity_Count
 = 1
 Client_ID = 1107,  Client_Name = ISSU NGXP rep IPC client,  Entity_Count
 = 1
 Client_ID = 1108,  Client_Name = ISSU NGXP l2pt IPC client,  Entity_Count
 = 1
 Client_ID = 1109,  Client_Name = ISSU NGXP mtm IPC client,  Entity_Count
 = 1
 Client_ID = 1110,  Client_Name = ISSU NGXP QOS IPC client,  Entity_Count
 = 1
 Client_ID = 1111,  Client_Name = ISSU NGXP PB IPC client,  Entity_Count
```

```
 = 1
 Client_ID = 1112,  Client_Name = ISSU NGXP RM IPC client,  Entity_Count
 = 1
 Client_ID = 1113,  Client_Name = ISSU NGXP igmp_sn IPC client,
Entity_Count = 1
```

Related Commands

Command	Description
show issu capability	Displays the ISSU capability of a client.
show issu entities	Displays the ISSU entity information.
show issu negotiated	Displays results of a negotiation that occurred concerning message versions or client capabilities.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu comp-matrix

To display information regarding the ISSU compatibility matrix, use the **show issu comp-matrix** command in user EXEC or privileged EXEC mode.

show issu comp-matrix {**negotiated** | **stored**}

Syntax Description

negotiated	Displays negotiated compatibility matrix information.
stored	Displays stored compatibility matrix information.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Before attempting an ISSU, check the compatibility level between the Cisco Carrier Packet Transport (CPT) software versions on the active and the standby fabric cards. ISSU will not work if the two versions are incompatible. Use the **show issu comp-matrix** command with the **negotiated** keyword to display information on the negotiation of the compatibility matrix data between two software versions on a given system. Use the **show issu comp-matrix** command with the **stored** keyword to display stored compatibility matrix information.

Examples

The following example is a sample output of the **show issu comp-matrix negotiated** command displaying negotiated compatibility matrix information:

```
Router#  show issu comp-matrix negotiated
```

```
 Cid     Eid      Sid     pSid    pUid      Compatibility

=======================================================
  2       1       262151  3       1         COMPATIBLE
  3       1       262160  5       1         COMPATIBLE
  4       1       262163  9       1         COMPATIBLE
  5       1       262186  25      1         COMPATIBLE
  7       1       262156  10      1         COMPATIBLE
  8       1       262148  7       1         COMPATIBLE
  9       1       262155  1       1         COMPATIBLE
  10      1       262158  2       1         COMPATIBLE
```

```
11      1       262172  6       1       COMPATIBLE
100     1       262166  13      1       COMPATIBLE
110     113     262159  14      1       COMPATIBLE
200     1       262167  24      1       COMPATIBLE
2002    1       -       -       -       UNAVAILABLE
2003    1       262185  23      1       COMPATIBLE
2004    1       262175  16      1       COMPATIBLE
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu sessions	Displays ISSU session information for a specified client.

show issu endpoints

To display the ISSU endpoint information, use the **show issu endpoints** command in user EXEC or privileged EXEC mode.

show issu endpoints

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

Endpoint is an execution unit within a redundancy domain. The ISSU infrastructure communicates between the two endpoints to establish a session and perform session negotiation for ISSU clients.

Examples

The following is a sample output of the **show issu endpoints** command displaying ISSU endpoints:

```
Router# show issu endpoints
```

```
My_Unique_ID = 5/0x5,  Client_Count = 71
This endpoint communicates with 2 peer endpoints :
        Peer_Unique_ID  CAP   VER  XFORM ERP  Compatibility
          3/0x       3    1     2     1   3      Not same
          4/0x       4    1     2     1   3       Same

Shared Negotiation Session Info :
   Nego_Session_ID = 95
   Nego_Session_Name = shared nego session
   Transport_Mtu = 4096
   Ses_In_Use = 2
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu entities

To display information about entities in one or more ISSU clients, use the **show issu entities** command in user EXEC or privileged EXEC mode.

show issu entities [*client-id*]

Syntax Description

client-id	(Optional) Identification number of a single ISSU client.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

An entity is a logical group of sessions that possess some common attributes. Enter a Client_ID to view information only about entities of a client. If a Client_ID is not specified, the command displays all the entities of the ISSU clients known to the device.

If the Client_ID number is not known, use the **show issu clients** command to display the current list of clients with their names and ID numbers.

Examples

The following example is a sample output of the **show issu entities** command displaying the entity information for a specific ISSU client:

```
Router# show issu entities 1106
```

```
Client_ID = 1106 :
    Entity_ID = 1,  Entity_Name = ISSU NGXP CIM IPC entity:
       MsgType MsgGroup CapType CapEntry CapGroup
        Count    Count   Count   count    Count
          26       1       1       1        1
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

Command	Description
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu fsm

To display the ISSU finite state machine (FSM) information corresponding to an ISSU session, use the **show issu fsm** command in user EXEC or privileged EXEC mode.

show issu fsm [*session_id*]

Syntax Description

session_id	(Optional) Session ID corresponding to an ISSU session.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Examples

The following is a sample output of the **show issu fsm** command displaying and verifying the ISSU state:

```
Router# show issu fsm 55
```

```
 Session_ID = 55 :
  FSM_Name          Curr_State      Old_State       Error_Reason
  FSM_L1            TRANS           P_VER           none
  FSM_L2_HELLO      EXIT            RCVD            none
  FSM_L2_A_CAP      A_INIT          unknown         none
  FSM_L2_P_CAP      P_EXIT          P_REQ           none
  FSM_L2_A_VER      A_INIT          unknown         none
  FSM_L2_P_VER      P_EXIT          P_VER_REQ       none
  FSM_L2_TRANS      COMP            COMP            none
Current FSM is FSM_L2_TRANS
Session is compatible
Negotiation started at 2d23h, duration is 0.052 seconds
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

Command	Description
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu message

To display checkpoint messages for a specified ISSU client, use the **show issu message** command in user EXEC or privileged EXEC mode.

show issu message {**groups** | **types**} [*client_id*]

Syntax Description

groups	Displays information on the message group supported by the specified client.
types	Displays information on all the message types supported by the specified client.
client_id	(Optional) Specifies a Client ID.

Command Default

If client ID is not specified, displays message groups or message types information for all the clients registered to the ISSU infrastructure.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

ISSU messages are synchronized data (also known as checkpoint data) sent between two endpoints.

When an ISSU-aware client establishes its session with a peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following is a sample output of the **show issu message groups** command displaying message groups for Client_id 2082:

```
Router# show issu message groups 2082
```

```
Client_ID = 2082,  Entity_ID = 1 :
   Message_Group = 1 :
                  Message_Type = 1,  Version_Range = 1 ~ 1
                  Message_Type = 2,  Version_Range = 1 ~ 1
                  Message_Type = 3,  Version_Range = 1 ~ 1
                  Message_Type = 4,  Version_Range = 1 ~ 1
                  Message_Type = 5,  Version_Range = 1 ~ 1
```

```
                    Message_Type = 6,  Version_Range = 1 ~ 1
                    Message_Type = 8,  Version_Range = 1 ~ 1
                    Message_Type = 9,  Version_Range = 1 ~ 1
                    Message_Type = 10,  Version_Range = 1 ~ 1
                    Message_Type = 11,  Version_Range = 1 ~ 1
                    Message_Type = 12,  Version_Range = 1 ~ 1
                    Message_Type = 13,  Version_Range = 1 ~ 1
                    Message_Type = 14,  Version_Range = 1 ~ 1
                    Message_Type = 15,  Version_Range = 1 ~ 1
                    Message_Type = 16,  Version_Range = 1 ~ 1
                    Message_Type = 17,  Version_Range = 1 ~ 1
                    Message_Type = 18,  Version_Range = 1 ~ 1
                    Message_Type = 19,  Version_Range = 1 ~ 1
                    Message_Type = 20,  Version_Range = 1 ~ 1
                    Message_Type = 21,  Version_Range = 1 ~ 1
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.

show issu negotiated

To display the session negotiation details about the ISSU message version or client capabilities, use the **show issu negotiated** command in user EXEC or privileged EXEC mode.

show issu negotiated {**version** | **capability**} *session-id*

Syntax Description

version	Displays the results of a negotiation about versions of the messages exchanged during the specified session, between the active and standby endpoints.
capability	Displays the results of a negotiation about the capabilities of the client application for the specified session.
session-id	Number used by the ISSU to identify a particular communication session between the active and the standby devices.

Command Default

Displays negotiated capability or version information for all the ISSU sessions.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

If the session_ID number is not known, enter the **show issu sessions** command. It will display the session_ID.

Examples

The following example is a sample output of the **show issu negotiated version** command displaying results of a negotiation about message versions.

```
Router# show issu negotiated version 55
```

```
Session_ID = 55 :
    Message_Type = 1,  Negotiated_Version = 1,  Message_MTU = 24
    Message_Type = 2,  Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 3,  Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 4,  Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 5,  Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 6,  Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 8,  Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 9,  Negotiated_Version = 1,  Message_MTU = 16
```

```
    Message_Type = 10, Negotiated_Version = 1,  Message_MTU = 788
    Message_Type = 11, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 12, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 13, Negotiated_Version = 1,  Message_MTU = 32
    Message_Type = 14, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 15, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 16, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 17, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 18, Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 19, Negotiated_Version = 1,  Message_MTU = 1380
    Message_Type = 20, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 21, Negotiated_Version = 1,  Message_MTU = 12
    Message_Type = 22, Negotiated_Version = 1,  Message_MTU = 48
    Message_Type = 23, Negotiated_Version = 1,  Message_MTU = 2360
    Message_Type = 24, Negotiated_Version = 1,  Message_MTU = 16
    Message_Type = 25, Negotiated_Version = 1,  Message_MTU = 20
    Message_Type = 26, Negotiated_Version = 1,  Message_MTU = 8008
    Message_Type = 27, Negotiated_Version = 1,  Message_MTU = 12
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu message types	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu sessions	Displays detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible.

show issu sessions

To display detailed information about a particular ISSU client, including whether the client status for the impending software upgrade is compatible, use the **show issu sessions** command in user EXEC or privileged EXEC mode.

show issu sessions *client-id*

Syntax Description

client-id	Identification number used by the ISSU for the client.

Command Default

Displays session information for all the clients registered to the ISSU infrastructure.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

A session is bidirectional and a reliable connection that is established between two endpoints. Sync-data and negotiation messages are sent to the peer endpoint through a session.

When an ISSU-aware client establishes its session with the peer, an ISSU negotiation takes place. The ISSU infrastructure uses the registered information to negotiate the capabilities and the message version to be used during the session.

Examples

The following is a sample output of the **show issu sessions** command:

```
Router# show issu sessions 1106
```

```
Client_ID = 1106,  Entity_ID = 1 :

*** Session_ID = 55,  Session_Name = NGXP CIM IPC :

      Peer      Peer    Negotiate  Negotiated    Cap       Msg      Session
    UniqueID     Sid      Role       Result    GroupID  GroupID  Signature
        3          56   PASSIVE   COMPATIBLE     1        1          0
                              (policy)

   Negotiation Session Info for This Message Session:
        Nego_Session_ID = 55
        Nego_Session_Name = NGXP CIM IPC
        Transport_Mtu = 0
```

```
         Compat_Result: raw_result =   COMPATIBLE,  policy_result =
COMPATIBLE


 *** Session_ID = 107,  Session_Name = NGXP CIM IPC :

       Peer     Peer   Negotiate  Negotiated   Cap      Msg     Session
     UniqueID    Sid     Role       Result   GroupID  GroupID  Signature
         4         79   PASSIVE   COMPATIBLE    1        1         0
                              (policy)

    Negotiation Session Info for This Message Session:
         Nego_Session_ID = 107
         Nego_Session_Name = NGXP CIM IPC
         Transport_Mtu = 0
         Compat_Result: raw_result =   COMPATIBLE,  policy_result =
COMPATIBLE
```

Related Commands

Command	Description
show issu clients	Lists the current ISSU clients, that is, the applications and protocols on the network supported by the ISSU.
show issu message	Displays the formats, versions, and maximum packet size of ISSU messages supported by a particular client.
show issu negotiated	Displays the results of a negotiation that occurred concerning message versions or client capabilities.

show redundancy

To display current or historical status and related information on planned or logged handovers, use the **show redundancy** command in privileged EXEC mode.

show redundancy [**clients** | **config-sync** | **counters** | **domain** | **history** | **idb-sync-history** | **interlink** | **states** | **switchover** | **trace**]

Syntax Description

clients	(Optional) Displays the redundancy-aware client application and protocol list.
config-sync	(Optional) Displays redundancy configuration synchronization status.
counters	(Optional) Displays redundancy-related operational measurements.
domain	(Optional) Displays information about the redundancy domain.
history	(Optional) Displays past status and related information about logged handovers.
idb-sync-history	(Optional) Displays redundancy Interface Descriptor Blocks (IDB) synchronization history.
interlink	(Optional) Displays interlink utilization.
states	(Optional) Displays redundancy-related states.
switchover	(Optional) Displays the switchover counts, the uptime since active, and the total system uptime.
trace	(Optional) Displays redundancy trace.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
9.3.0	This command was introduced.

Usage Guidelines

This command displays the redundancy configuration mode of the fabric card. This command also displays information about the number of switchovers, system uptime, processor uptime, and redundancy state, and reasons for any switchovers.

Examples

The following is a sample output from the **show redundancy** command.

```
Router# show redundancy
```

```
Redundant System Information :
------------------------------
       Available system uptime = 18 hours, 44 minutes
       Switchovers system experienced = 1
       Standby failures = 0
       Last switchover reason = active unit failed

       Hardware Mode = Duplex
       Configured Redundancy Mode = SSO
       Operating Redundancy Mode = SSO
       Maintenance Mode = Disabled
       Communications = Up

Current Processor Information :
-------------------------------
        Active Location = slot 5
        Current Software state = ACTIVE
        Uptime in current state = 10 minutes
        Image Version = Cisco IOS Software, ONS NGXP Software
(NGXP-ADVIPSERVICES-M), Experimental Version
        15.1(20110216:101154) [ios_ngxp_dev-georgeti-ios_ngxp_dev.pkg
100]
        Copyright (c) 1986-2011 by Cisco Systems, Inc.
        Compiled Wed 16-Feb-11 16:59 by georgeti
        Configuration register = 0x101

Peer Processor Information :
----------------------------
        Standby Location = slot 4
        Current Software state = STANDBY HOT
        Uptime in current state = 8 minutes
        Image Version = Cisco IOS Software, ONS NGXP Software
(NGXP-ADVIPSERVICES-M), Experimental Version
        15.1(20110215:170703) [ios_ngxp_dev-sathk-ngxp_Feb16th 109]
        Copyright (c) 1986-2011 by Cisco Systems, Inc.
        Compiled Wed 16-Feb-11 15:12 by sathk
        Configuration register = 0x101 (will be 0x8001 at next reload)
```

The following is a sample output from the **show redundancy states** command.

```
Router# show redundancy states
```

```
     my state = 13  -ACTIVE
     peer state = 8 -STANDBY HOT
     Mode = Duplex
     Unit ID = 4

    Redundancy Mode (Operational) = SSO
    Redundancy Mode (Configured)  = SSO
    Redundancy State              = SSO
    Manual Swact = enabled
```

```
    Communications = Up

    client count = 47
    client_notification_TMR = 30000 milliseconds
    keep_alive TMR = 9000 milliseconds
    keep_alive count = 0
    keep_alive threshold = 10
    RF debug mask = 0x0
```

The following is a sample output from the **show redundancy history** command.

```
Router# show redundancy history
```

```
00:00:12 client added: Redundancy Mode RF(29) seq=60
00:00:12 client added: IfIndex(139) seq=61
00:00:12 client added: CHKPT RF(25) seq=68
00:00:12 client added: NGXP Platform RF(4500) seq=76
00:00:12 client added: NGXP CardIntf Mgr RF(4505) seq=77
00:00:12 client added: Event Manager(77) seq=84
00:00:12 client added: Network RF Client(22) seq=109
00:00:12 client added: XDR RRP RF Client(71) seq=135
00:00:12 client added: CEF RRP RF Client(24) seq=136
00:00:12 client added: RFS RF(520) seq=157
00:00:12 client added: Config Sync RF client(5) seq=159
```

The following is a sample output from the **show redundancy switchover history** command.

```
Router# show redundancy switchover history
```

```
Index  Previous  Current  Switchover         Switchover
       active    active   reason             time
-----  --------  -------  ----------------   --------------------
   1       4        5     active unit failed 10:58:11 PDT Wed Jun 7 2000
```