Configuring Transports

This module provides information about Nonstop Routing (NSR), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP) transports on Cisco ASR 9000 Series Aggregation Services Routers .

If you have specific requirements and need to adjust the NSR, TCP, or UDP values, refer to the *Transport Stack Commands on IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*.

Note For a complete description of the transport configuration commands listed in this module, refer to the *Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Command Reference* publication.

Feature History for Configuring NSR, TCP, UDP, and UDP RAW Transports on the Cisco ASR 9000 Series Router

Release	Modification
Release 3.7.2	This feature was introduced.
Release 6.3.3	XIPC Queue Drop Detection and Correction feature was introduced for TCP.

Prerequisites for Configuring NSR, TCP, UDP, Transports

The following prerequisites are required to implement NSR, TCP, UDP, Transports:

You must be in a user group associated with a task group that includes the proper task IDs. The command reference guides include the task IDs required for each command. If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Information About Configuring NSR, TCP, UDP Transports

To configure NSR, TCP, and UDP transports, you must understand the following concepts:

NSR Overview

Nonstop Routing (NSR) is provided for Open Shortest Path First (OSPF) and Label Distribution Protocol (LDP) protocols for the following events:

- Route Processor (RP) failover
- Process restart for either OSPF, LDP, or TCP
- In-service software upgrades (ISSU)

In the case of the RP failover, NSR is achieved by for both TCP and the applications (OSPF or LDP).

NSR is a method to achieve High Availability (HA) of the routing protocols. TCP connections and the routing protocol sessions are migrated from the active RP to standby RP after the RP failover without letting the peers know about the failover. Currently, the sessions terminate and the protocols running on the standby RP reestablish the sessions after the standby RP goes active. Graceful Restart (GR) extensions are used in place of NSR to prevent traffic loss during an RP failover but GR has several drawbacks.

You can use the **nsr process-failures switchover** command to let the RP failover be used as a recovery action when the active TCP or active LDP restarts. When standby TCP or LDP restarts, only the NSR capability is lost till the standby instances come up and the sessions are resynchronized but the sessions do not go down. In the case of the process failure of an active OSPF, a fault-management policy is used. For more information, refer to *Implementing OSPF on Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

TCP Overview

TCP is a connection-oriented protocol that specifies the format of data and acknowledgments that two computer systems exchange to transfer data. TCP also specifies the procedures the computers use to ensure that the data arrives correctly. TCP allows multiple applications on a system to communicate concurrently, because it handles all demultiplexing of the incoming traffic among the application programs.

Any IP protocol other than TCP or UDP is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

UDP Overview

The User Datagram Protocol (UDP) is a connectionless transport-layer protocol that belongs to the IP family. UDP is the transport protocol for several well-known application-layer protocols, including Network File System (NFS), Simple Network Management Protocol (SNMP), Domain Name System (DNS), and TFTP.

Any IP protocol other than TCP, UDP, is known as a RAW protocol.

For most sites, the default settings for the TCP, UDP, and RAW transports need not be changed.

During external port scanning on ports 19 and 20, the UDP packets dropped by Nmap tool without sending an ICMP response, cause uncertainty in identifying the true state of the ports. The port states can be open, closed, or filtered.

Due to no response from the target system, the port states might misclassify as open instead of a closed or filtered state, and can lead to a false-positive situation.

Table 1: UDP port availability for Applications

Platform	Start of Range	End of Range	Availability
Cisco IOS XR 64-bit Operating System	15000	57344	Available
Cisco IOS XR 64-bit Operating System	57345	65535	Reserved
Cisco IOS XR 32-bit Operating System	15000	65535	Available

How to Configure Failover as a Recovery Action for NSR

This section contains the following procedure:

Configuring Failover as a Recovery Action for NSR

This task allows you to configure failover as a recovery action to process failures of active instances.

When the active TCP or the NSR client of the active TCP terminates or restarts, the TCP sessions go down. To continue to provide NSR, failover is configured as a recovery action. If failover is configured, a switchover is initiated if the active TCP or an active application (for example, LDP, OSPF, and so forth) restarts or terminates.

For information on how to configure MPLS Label Distribution Protocol (LDP) for NSR, refer to the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers*.

For information on how to configure NSR on a per-process level for each OSPF process, refer to the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Note Before performing this procedure, enable RP isolation using the **isolation enable** command for improved troubleshooting. Without enabling RP isolation, the failing process will not generate the logs required to find the root cause of the failure.

SUMMARY STEPS

1. **configure**
2. nsr process-failures switchover
3. **commit**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**configure**	
Step 2	nsr process-failures switchover **Example:** `RP/0/RSP0/CPU0:router(config)# nsr process-failures switchover`	Configures failover as a recovery action for active instances to switch over to a standby route processor (RP) to maintain nonstop routing (NSR.
Step 3	**commit**	

XIPC Tail Drop Detection and Correction for TCP

Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Extended IPC (XIPC) Tail drop is one of the more commonly used congestion avoidance mechanisms. Tail drop treats all traffic equally and does not differentiate between classes of service. Queues fill during periods of congestion. When the output queue is full and tail drop is in effect, packets are dropped until the congestion is eliminated and the queue is no longer full.

This feature introduces XIPC as a new policer, and culprit session falls into this bucket and is policed heavily. This feature improves the serviceability of the XIPC queues owned by TCP. To perform this, the TCP monitors and identifies the sessions that are receiving more data. TCP revisits the statistics at regular intervals, and based on the data, it decides whether the sessions need to be policed or added to default policer rate. Therefore, other sessions are given a fair chance to use the XIPC queue, and high-data sessions are throttled down at hardware.

To detect the culprit session, TCP internal queue size is considered along with rate-limit. If the overall queue size reaches the threshold value and per session rate-limit value is exceeded then the culprit sessions in that queue are detected.

After applying the dynamic policer, culprit sessions may flap. As per the TCP dumpfiles and logs, this is an expected behavior. If a culprit BGP session has aggressive timers (KA 3 sec and Hold timer 9 sec), even then the sessions may flap and we may not verify the LPTS packet drops using the **show lpts** commands.

TCP Configurations to Enable XIPC Tail Drop

The following configuration enables XIPC tail drop on TCP:

```
RP/0/0/CPU0:Router (config)# tcp num-thread Ingress-threads-TCP max-threads
RP/0/0/CPU0:Router (config)# pak-rate tcp stats-start [rate-limit packet rate | max-pkt-size
 max-pkt-size-value max-pak-rate max-pak-rate-value]
```

Verification

The following example displays the statistics of TCP packet rate.

```
RP/0/RSP0/CPU0:Router# show tcp pak-rate stats

       PR -  Number of packets in 30 sec (display, if more than Rate-limit)
       MPR - Maximum size packets in 30 sec (display, if more than Maximum packet rate)

         Time         Foreign Address    Local Address     VRF          PR        MPR
-------------------------------------------------------------------------------------------

 Nov 19 15:56:08.464   6.6.13.7:179       6.6.13.6:23898    0x60000000  18767      1502
 Nov 19 15:56:08.464   6.6.1.7:46922      6.6.1.6:179       0x60000000  107802     8932
```

Note

- These are the culprit session information and applied LPTS dynamic policer on these sessions.
- Using default BGP timers (60 sec KA and 180 sec hold timer expiry) and show commands, we can observe the number of packets received in the last 30 sec.
- After applying policer, if the number of packets received are less than the configured packet rate, after 85 sec, above details will be removed from the show command.

The following example verifies the sessions statistics at XIPC policer-index level and per-session level.

```
RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                    Accept Drop
XIPC  97  Local  1000  9600   3912960      368661   01234567

RP/0/RSP0/CPU0:Router# show lpts pifib hardware police location 0/3/cPU0 | i XIPC
                                    Accept Drop
  XIPC  97  Local  1000  9600      0          0       01234567
```

Note Statistics are cleared when last session under this policer index is removed.

The following example verifies the sessions statistics at XIPC policer and also provides the entries present in the hardware.

```
 RP/0/RSP0/CPU0:Router# show lpts pifib hardware entry statistics location 0/3/cpu0 | i
6.6.1.7,
                                                        Accept/Drop
1754   IPV4 default     TCP    any       LU(30)     4021290/456698  any, 179 6.6.1.7,
46922
2584   IPV4 default     TCP    any       LU(30)       0/0           any, 179 6.6.1.7,
any
```

Additional References

The following sections provide references related to configuring NSR, TCP, and UDP transports.

Related Documents

Related Topic	Document Title
the Cisco ASR 9000 Series Router Transport Stack commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Transport Stack Commands in the IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router MPLS LDP commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*MPLS Label Distribution Protocol Commands in the MPLS Command Reference for Cisco ASR 9000 Series Routers*
the Cisco ASR 9000 Series Router OSPF commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*OSPF Commands in the Routing Command Reference for Cisco ASR 9000 Series Routers*
MPLS Label Distribution Protocol feature information	*Implementing MPLS Label Distribution Protocol in the MPLS Configuration Guide for Cisco ASR 9000 Series Routers*
OSPF feature information	*Implementing OSPF in the Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
—	To locate and download MIBs, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport