New and Changed Information

This chapter contains the following sections:

New and Changed Information

The following table provides an overview of the significant changes to this guide for the current release. The table does not provide a list of all the exhaustive changes made to the configuration guide or of the new features in this release.

Feature	Description	Added or Changed in Release	Where Documented
SSH	Added new SSH commands to configure support for legacy SSH security algorithms, message authentication codes (MACs), key types, and ciphers.	7.0(3)I7(3)	Configuring Legacy SSH Algorithm Support
uRPF	Added support for the 3164Q, 31128PQ, 3232C, and 3264Q switches and the Cisco Nexus 3100 platform switches in N9K mode.	7.0(3)I7(3)	Guidelines and Limitations for Unicast RPF
802.1X	Added the support to the 802.1X protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports.	7.0(3)I7(1)	Configuring 802.1X
IPv6 First-Hop Security	Added the support for the IPv6 First-Hop Security features.	7.0(3)I7(1)	Configuring IPv6 First-Hop Security

New and Changed Information

Feature	Description	Added or Changed in Release	Where Documented
Unicast RPF	Introduced this feature for the Cisco Nexus 3132Q-V, 31108PC-V, and 31108TC-V switches.	7.0(3)I7(1)	Guidelines and Limitations for Unicast RPF Configuring Unicast RPF
Configuring rate limits	Added a new chapter titled Configuring Rate Limits.	7.0(3)I6(1)	Configuring Rate Limits
Port Security with vPC	Added guidelines and limitations for Port Security on vPCs.	7.0(3)I5(2)	Guidelines and Limitations for Port Security on vPCs
Port Security with vPC	Added configuration example for Port Security in a vPC domain.	7.0(3)I5(2)	Configuration Examples for Port Security in a vPC Domain
Port Security	Added a new chapter titled Configuring Port Security.	7.0(3)I5(1)	Configuring Port Security
X.509v3 Authentication for SSH	Added configuration steps and example for X509v3 certificate based SSH authentication	7.0(3)I5(1)	Configuring X.509v3 Certificate-Based SSH Authentication
SSH	Changed the default value of the **show ssh key** command to display the fingerprint in SHA256 format by default and added the **md5** option if you want to see the fingerprint in MD5 format.	7.0(3)I4(6)	Generating SSH Server Keys
CoPP	Changed the police CIR rate range to start with 0 to initiate a packet drop.	7.0(3)I4(1)	Configuring a Control Plane Policy Map
AAA	Added the ability to log successful and failed login attempts.	7.0(3)I4(1)	Logging Successful and Failed Login Attempts
IP ACLs	Enabled access control entry (ACE) information to be displayed in the output of the **show logging ip access-list cache** command.	7.0(3)I4(1)	Configuring IPv4 ACL Logging

Feature	Description	Added or Changed in Release	Where Documented
ACE with SMAC or DMAC	OpenFlow is now handled by the POLICY_MGR process and tap-aggregation is handled by the ACLMGR process. Due to this enhancement, OpenFlow specific options are not available for tap-aggregation. Therefore, you cannot create an ACE with SMAC or DMAC.	7.0(3)I2(1)	Guidelines and Limitations for ACLs
HTTP method match enhancement	As an enhancement to HTTP method match, the tcp-option-length option has been added to the ACE syntax to specify the length of the TCP options header in the packets.	7.0(3)I2(1)	Guidelines and Limitations for ACLs Configuring ACL Using HTTP Methods to Redirect Requests
Enabling PIM to get the packets on the copp-s-igmp queue.	The PIM_IGMP class-id is set on the port only when PIM is enabled. Since there is no need to punt IGMP packets to the CPU on the Layer 3 ports when PIM is not enabled, you have to configure feature pim and enable PIM on the port to get the packets on the copp-s-igmp queue.	7.0(3)I2(1)	Guidelines and Limitations for CoPP
The same MAC address is permitted in the static DHCP binding across multiple IP and ports.	The same MAC address is permitted in the static DHCP binding across multiple IP and ports whereas in releases prior to 7.0(3)I2(1), the unsupported DHCP static binding configuration is rejected with an error.	7.0(3)I2(1)	Guidelines and Limitations for DHCP Snooping
uRPF	Added support for Cisco Nexus 3100 platform switches in N3K mode.	7.0(3)I2(1)	Configuring Unicast RPF

New and Changed Information