Oracle® Communications IP Service Activator

Cisco IOS Cartridge Guide

Release 7.2

E47722-01

October 2013

ORACLE®

Oracle Communications IP Service Activator Cisco IOS Cartridge Guide, Release 7.2

E47722-01

Contents

4 Device Configuration

5 Cisco Cartridge Configuration Utility

6 Cisco Pre-checks and Post-checks

A Options Framework

Preface

The *IP Service Activator Cisco IOS Cartridge Guide* provides detailed technical information about Oracle Communications IP Service Activator features, device configuration information, and sample device configuration for Cisco IOS devices.

Audience

This guide is intended for network managers and technical consultants responsible for implementing IP Service Activator within a network that uses the Cisco devices.

Related Documents

For more information, see the following documents in the IP Service Activator Release documentation set:

- *IP Service Activator Installation Guide*
- *IP Service Activator System Administrator's Guide*

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Cisco IOS Cartridge Overview and Features

This chapter outlines the tasks involved in installing the Oracle Communications IP Service Activator Cisco IOS cartridge and IP Service Activator support for Cisco devices.

The following tables list the features and services supported by the IP Service Activator Cisco IOS cartridge.

Cartridge Overview

IP Service Activator cartridges enable you to support your existing services, emerging services, and business needs. The cartridges operate in conjunction with the IP Service Activator core product.

Installing the Cartridge

For cartridge installation procedures, see *IP Service Activator Installation Guide*.

Installing Configuration Policies

IP Service Activator supports extensible configuration policies that are seen through the graphical user interface (GUI). Each configuration policy includes one CFG file and one or more zipped HTML files.

For the configuration policy installation procedure, see *IP Service Activator Installation Guide*.

For more information on configuration policies, interface policy registration and interface/sub-interface creation, see IP Service Activator online Help.

General IP Service Activator Features

Table 1–1 lists the support for general IP Service Activator features on the Cisco IOS cartridge. Please note that not including a option is the same as having it set to the default value

Table 1–1 General IP Service Activator Features

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Configuration Protocol Support	Telnet	Yes

Table 1–1 (Cont.) General IP Service Activator Features

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Configuration Protocol Support	Secure Shell (SSH)	Yes
Configuration Protocol Support	Simple Network Management Protocol (SNMP)	No
Configuration Protocol Support	Vendor Proprietary	No
Device Discovery	SNMP	Yes
Device Discovery	Discovery Module	No
Device Configuration	Configuration Audit	Yes
Device Configuration	Command Re-issue	Yes
Device Configuration	Auto ID Migration	Yes
Device Configuration	Save Running Configuration	Yes
Device Configuration	Configuration Version	Yes
Device Configuration	Configuration Options	Yes
Device Configuration	Synonyms	Yes
Device Configuration	Command Thresholding	Yes
Device Configuration	Threshold Activated Configuration Control	Yes
Supported Services	Transparent local area network (LAN) service	No
Supported Services	Interface Configuration Management	Yes
Supported Services	Quality of Service (QoS)	Yes
Supported Services	Layer 3 Multi Protocol Label Switching (MPLS) Virtual Private Network (VPN)	Yes
Supported Services	Point-to-Point Circuit Cross Connect (CCC)	No
Supported Services	Point-to-Point Virtual Leased Line (VLL) Martini	Yes
Supported Services	Virtual Private LAN Service (VPLS)	No
Supported Services	Service Assurance Agent (SAA)	Yes
Supported Services	Netflow	Yes
Supported Services	Dynamic User VPN	No
Supported Services	IPsec	Yes
Supported Services	Label Switched Path (LSP)	Yes
Supported Services	Virtual LAN (VLAN)	Yes
Supported Services	Base Configuration Policies	Yes
Supported Services	Layer 2 QoS	Yes
Supported Services	Service Group	Yes

Table 1–1 (Cont.) General IP Service Activator Features

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Supported Services	QoS Attachment	Yes
Supported Services	Virtual Routing and Forwarding (VRF) Route Maps	Yes
Supported Services	VRF and IP Multicast	Yes
Supported Services	Virtual Customer Edge (CE)	Yes
Supported Services	VPN and IP Multicast Module	Yes
Supported Services	Configuration Template Manager	Yes
Supported Services	QoS with Hierarchical Queuing Framework	Yes
Supported Services	QoS on aggregation services routers (ASR) devices	Yes
Configuration Management	Configuration Archiving and Versioning	Yes
Configuration Management	Configuration Restore	Yes
Configuration Management	Service Configuration Auditing	Yes
Configuration Management	Service Configuration Traceability	Yes
Configuration Management	Service Repair	Yes
Configuration Management	Real-time Configuration Change Tracking	Yes
SDK	Service Cartridge Software Development Kit (SDK)	Yes
SDK	Configuration Policy SDK	Yes

Layer 3 MPLS VPN

Table 1–2 lists the Layer 3 MPLS VPN support on the Cisco IOS cartridge.

Note: iBGP peering should be configured manually.

Table 1–2 Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Layer 3 MPLS VPN Support	**Layer 3 MPLS VPN Support**	Yes
Topology	Mesh	Yes
Topology	Hub and Spoke	Yes
Topology	Management	Yes
Addressing	Public IP (IPv4 and IPv6)	Yes
Addressing	Private IP (IPv4 and IPv6)	Yes
Addressing	Unnumbered	Yes
Addressing	Interface Description	Yes

Table 1–2 (Cont.) Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
VFR Table	VRF Export Map Reference	Yes
VFR Table	VRF Import Map Reference	Yes
VFR Table	VRF DHCP Helper	No
VFR Table	VRF Description	Yes
VFR Table	VRF Label	No
VFR Table	VRF Route Targets	Yes
VFR Table	VRF Table Name	Yes
VFR Table	VRF Route Distinguisher	Yes
VFR Table	VRF Route Limit (Max Routes)	Yes
VFR Table	External Border Gateway Protocol (EBGP) Multipath Load Sharing	Yes
VFR Table	Enhanced Interior Gateway Routing Protocol (EIGRP) Multipath Load Sharing	No
VFR Table	Internal Border Gateway Protocol (IBGP) Multipath Load Sharing	Yes
VRF Table	EBGP and IBGP (EIBGP) Multipath Load Sharing	Yes
VFR Table	IBGP Unequal-cost	Yes
VFR Table	VRF Import (Max Paths)	Yes
VFR Table	VRF Target	No
VFR Table	VRF Reduction	Yes
VFR Table	Force Install	Yes
VFR Table	Shareable	Yes
VFR Table	Open Shortest Path First (OSPF) Router ID	Yes
VFR Table	Interface-less VRF	Yes
Routing Options	Routing Options	No
Routing Options	Autonomous Systems (AS)	No
Routing Options	Autonomous System Number (ASN) Loops	No
Routing Options	Independent Domain	No
Routing Options	Load Balancing	No
Routing Options	IPv4 Multipath	No
Routing Options	IPv4 Multipath Unequal Cost	No
Routing Options	IPv4 Multipath External and Internal Border Gateway Protocol (BGP) Paths	No
Routing Options	IPv6 Multipath	No
Routing Options	IPv6 Multipath Unequal Cost	No

Table 1–2 (Cont.) Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Routing Options	IPv4 Multipath External and Internal Border Gateway Protocol (BGP) Paths	No
Static Routing	Static Routing	Yes
Static Routing	Static Global Routes	Yes
Static Routing	Static Local Routes (Redistribution)	Yes
Static Routing	Static Permanent Routes	Yes
Static Routing	Static Tag Value	Yes
Static Routing	Static Next Hop IP Address (IPv4 and IPv6)	Yes
Static Routing	Static Next Hop Interface	Yes
Static Routing	Static Next Hop IP and Interface	Yes
Static Routing	Static Route to Null0	Yes
BGP	BGP Network Statements (IPv4 and IPv6)	Yes
BGP	BGP Aggregate Statements (IPv4 and IPv6)	Yes
eBGP	eBGP	Yes
eBGP	EBGP AS override	Yes
eBGP	EBGP Site of Origin	Yes
eBGP	Remove Private AS	Yes
eBGP	EBGP Update Source	Yes
eBGP	EBGP Multihop	Yes
eBGP	EBGP Allow AS in	Yes
eBGP	EBGP Provider Edge (PE)-Customer Edge (CE) MD5 Authentication	Yes
eBGP	EBGP Local AS	Yes
eBGP	EBGP Advertise Address Family (IPv4 and IPv6)	Yes
eBGP	EBGP Local AS No Prepend	Yes
eBGP	EBGP Neighbor Description	Yes
eBGP	EBGP Soft Reconfiguration	Yes
eBGP	EBGP Router as Next Hop	Yes
eBGP	EBGP Neighbor weight	Yes
eBGP	EBGP Filters	Yes
eBGP	EBGP Default route	Yes
eBGP	EBGP Prefix Limit (IPv4 and IPv6)	Yes

Table 1–2 (Cont.) Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
eBGP	EBGP Prefix Limit Restart (IPv4 and IPv6)	Yes
eBGP	EBGP Prefix Filters	Yes
eBGP	EBGP Standard Community Attributes	Yes
eBGP	EBGP Extended Community Attributes	Yes
eBGP	EBGP Timers	Yes
eBGP	Keep Alive	Yes
eBGP	Hold Timer	Yes
eBGP	EBGP Neighbor Advertisement Interval	Yes
eBGP	EBGP Inbound Route Map	Yes
eBGP	EBGP Neighbor Site of Origin (SOO)	Yes
eBGP	External Route Map	Yes
eBGP	Generated Route Map	Yes
eBGP	EBGP Local Preference	Yes
eBGP	EBGP Site of Origin Route Map	Yes
eBGP	Route Map Name	Yes
eBGP	EBGP Outbound Route Map	Yes
eBGP	External Route Map	Yes
eBGP	EBGP Route Dampening	Yes
eBGP	Redistribution into BGP	Yes
eBGP	BGP Redistribution Metric and Policy from Connected	Yes
eBGP	BGP Redistribution Metric and Policy from Static	Yes
eBGP	BGP Redistribution Metric and Policy from Routing Information Protocol (RIP)	Yes
eBGP	BGP Redistribution Metric and Policy from OSPF	Yes
eBGP	BGP Redistribution Metric and Policy from EIGRP	Yes
eBGP	Default Route	Yes
eBGP	EBGP Neighbour Transport Connection Mode Active/Passive	Yes
eBGP	EBGP Neighbour Transport PathMTUDiscovery	Yes
eBGP	EBGP Neighbour Transport Single Session/MultiSession	Yes

Table 1–2 (Cont.) Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
eBGP	EBGP Neighbour	Yes
eBGP	EBGP Log Updown	Yes
OSPF	OSPF	Yes
OSPF	Area	Yes
OSPF	OSPF Area Type	Yes
OSPF	OSPF not-so-stubby area (NSSA) Type 7 Redistribution	Yes
OSPF	OSPF Maximum Paths	Yes
OSPF	OSPF Cost	Yes
OSPF	OSPF Process ID	Yes
OSPF	OSPF BGP Redistribution Tag	Yes
OSPF	OSPF Distribute in Filter	Yes
OSPF	OSPF Distribute out Filter	Yes
OSPF	OSPF shortest Path First (SPF) Throttling	Yes
OSPF	OSPF MD5 Authentication	Yes
OSPF	OSPF Summary Addresses	Yes
OSPF	Suppress Advertise	Yes
OSPF	Tag Value	Yes
OSPF	Redistribution into OSPF	Yes
OSPF	OSPF Redistribution Metric and Policy from Connected	Yes
OSPF	OSPF Redistribution Metric and Policy from Static	Yes
OSPF	OSPF Redistribution Metric and Policy from RIP	Yes
OSPF	OSPF Redistribution Metric and Policy from BGP	Yes
OSPF	OSPF Redistribution Metric and Policy from EIGRP	Yes
OSPF	Default Route	Yes
RIP	RIP	Yes
RIP	RIP Ignore Routes from Source	Yes
RIP	RIP Passive Interface	Yes
RIP	Redistribution into RIP	Yes
RIP	RIP Redistribution Metric and Policy from Connected	Yes
RIP	RIP Redistribution Metric and Policy from Static	Yes
RIP	RIP Redistribution Metric and Policy from OSPF	Yes

Table 1–2 (Cont.) Layer 3 MPLS VPN Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
RIP	RIP Redistribution Metric and Policy from BGP	Yes
RIP	RIP Redistribution Metric and Policy from EIGRP	Yes
RIP	Default Route	No
EIGRP	EIGRP	Yes
EIGRP	EIGRP Device ASN	Yes
EIGRP	EIGRP Site ASN	Yes
EIGRP	EIGRP Site of Origin	Yes
EIGRP	EIGRP Route Map Name for SOO	Yes
EIGRP	EIGRP MD5 Authentication	Yes
EIGRP	EIGRP Maximum Paths	Yes
EIGRP	EIGRP Redistribution	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from Connected	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from Static	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from BGP	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from OSPF	No
EIGRP	EIGRP Redistribution Metrics and Policy from RIP	Yes

Virtual CE

Table 1–3 lists the Virtual CE support on the Cisco IOS cartridge.

Table 1–3 Virtual CE

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Addressing	Public IP (IPv4 and IPv6)	Yes
Addressing	Private IP (IPv4 and IPv6)	Yes
Addressing	Unnumbered	Yes
Addressing	Interface Description	Yes
VRF Table	VRF Export Map Reference	No
VRF Table	VRF Import Map Reference	No
VRF Table	VRF DHCP Helper	No
VRF Table	VRF Description	Yes
VRF Table	VRF Label	No
VRF Table	VRF Route Targets	Yes

Table 1–3 (Cont.) Virtual CE

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
VRF Table	VRF Table Name	Yes
VRF Table	VRF Route Distinguisher	Yes
VRF Table	VRF Route Limit (Max Routes)	Yes
VRF Table	EIBGP Multipath Load Sharing	No
VRF Table	EBGP Multipath Load Sharing	Yes
VRF Table	EIGRP Multipath Load Sharing	Yes
VRF Table	IBGP Multipath Load Sharing	No
VRF Table	IBGP Unequal-cost	No
VRF Table	VRF Import (Max Paths)	Yes
VRF Table	VRF Target	Yes
VRF Table	VRF Reduction	No
VRF Table	Force Install	No
VRF Table	Shareable	No
VRF Table	OSPF Router ID	Yes
VRF Table	Interface-less VRF	
Static Routing	Static Global Routes	No
Static Routing	Static Local Routes (Redistribution)	No
Static Routing	Static Permanent Routes	Yes
Static Routing	Static Tag Value	Yes
Static Routing	Static Next Hop IP Address	Yes
Static Routing	Static Next Hop Interface	Yes
Static Routing	Static Next Hop IP and Interface	Yes
Static Routing	Static Route to Null0	Yes
BGP	BGP Network Statements	Yes
BGP	BGP Aggregate Statements	Yes
eBGP	EBGP AS override	Yes
eBGP	EBGP Site of Origin	Yes
eBGP	Remove Private AS	Yes
eBGP	EBGP Update Source	Yes
eBGP	EBGP Multihop	Yes
eBGP	EBGP Allow AS in	Yes
eBGP	EBGP PE-CE MD5 Authentication	Yes
eBGP	EBGP Local AS	Yes
eBGP	EBGP Local AS No Prepend	Yes
eBGP	EBGP Neighbor Description	Yes
eBGP	EBGP Soft Reconfiguration	Yes

Table 1–3 (Cont.) Virtual CE

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
eBGP	EBGP Router as Next Hop	Yes
eBGP	EBGP Neighbor weight	Yes
eBGP	EBGP Filters	Yes
eBGP	EBGP Default route	Yes
eBGP	EBGP Prefix Limit	Yes
eBGP	EBGP Prefix Limit Restart	Yes
eBGP	EBGP Prefix Filters	Yes
eBGP	EBGP Standard Community Attributes	Yes
eBGP	EBGP Extended Community Attributes	Yes
eBGP	EBGP Timers	Yes
eBGP	Keep Alive	Yes
eBGP	Hold Timer	Yes
eBGP	EBGP Neighbor Advertisement Interval	Yes
eBGP	EBGP Inbound Route Map	Yes
eBGP	External Route Map	Yes
eBGP	Generated Route Map	No
eBGP	EBGP Local Preference	No
eBGP	EBGP Site of Origin Route Map	No
eBGP	EBGP Neighbor Site of Origin	No
eBGP	Route Map Name	No
eBGP	EBGP Outbound Route Map	Yes
eBGP	External Route Map	Yes
eBGP	EBGP Route Dampening	No
eBGP	Redistribution into BGP	Yes
eBGP	BGP Redistribution Metric and Policy from Connected	Yes
eBGP	BGP Redistribution Metric and Policy from Static	Yes
eBGP	BGP Redistribution Metric and Policy from RIP	Yes
eBGP	BGP Redistribution Metric and Policy from OSPF	Yes
eBGP	BGP Redistribution Metric and Policy from EIGRP	Yes
eBGP	Default Route	No
OSPF	OSPF Area Type	Yes

Table 1–3 (Cont.) Virtual CE

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
OSPF	OSPF NSSA Type 7 Redistribution	Yes
OSPF	OSPF Maximum Paths	Yes
OSPF	OSPF Cost	Yes
OSPF	OSPF BGP Redistribution Tag	Yes
OSPF	OSPF Distribute in Filter	Yes
OSPF	OSPF Distribute out Filter	Yes
OSPF	OSPF SPF Throttling	Yes
OSPF	OSPF MD5 Authentication	Yes
OSPF	OSPF Summary Addresses	Yes
OSPF	Suppress Advertise	Yes
OSPF	Tag Value	Yes
OSPF	Redistribution into OSPF	Yes
OSPF	OSPF Redistribution Metric and Policy from Connected	Yes
OSPF	OSPF Redistribution Metric and Policy from Static	Yes
OSPF	OSPF Redistribution Metric and Policy from RIP	Yes
OSPF	OSPF Redistribution Metric and Policy from BGP	Yes
OSPF	OSPF Redistribution Metric and Policy from EIGRP	Yes
OSPF	Default Route	No
OSPF	Capability VRF-Lite	Yes
RIP	RIP Ignore Routes from Source	Yes
RIP	RIP Passive Interface	Yes
RIP	Redistribution into RIP	Yes
RIP	RIP Redistribution Metric and Policy from Connected	Yes
RIP	RIP Redistribution Metric and Policy from Static	Yes
RIP	RIP Redistribution Metric and Policy from OSPF	Yes
RIP	RIP Redistribution Metric and Policy from BGP	Yes
RIP	RIP Redistribution Metric and Policy from EIGRP	Yes
RIP	Default Route	No
EIGRP	EIGRP Device ASN	Yes
EIGRP	EIGRP Site ASN	Yes

Table 1–3 (Cont.) Virtual CE

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
EIGRP	EIGRP Site of Origin	Yes
EIGRP	EIGRP Route Map Name for SOO	Yes
EIGRP	EIGRP MD5 Authentication	Yes
EIGRP	EIGRP Maximum Paths	Yes
EIGRP	EIGRP Redistribution	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from Connected	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from Static	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from BGP	Yes
EIGRP	EIGRP Redistribution Metrics and Policy from OSPF	No
EIGRP	EIGRP Redistribution Metrics and Policy from RIP	Yes
SAA	IPv4 Destination Address	Yes
SAA	IPv6 Destination Address	Yes
SAA	IPv4 Source Address	Yes
SAA	IPv6 Source Address	Yes
SAA	VRF aware	Yes

Note that for Virtual CE, static routing, BGP Networks, and BGP Aggregate addresses support IPv4 and IPv6 addresses.

Layer 2 VLL

Table 1–4 lists the Layer 2 VLL support on the Cisco IOS cartridge.

Table 1–4 Layer 2 VLL Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Martini Point-to-Point	Asynchronous Transfer Mode (ATM) AAL5	Yes
Martini Point-to-Point	ATM Cell	Yes
Martini Point-to-Point	Ethernet	Yes
Martini Point-to-Point	Ethernet VLAN	Yes
Martini Point-to-Point	Frame	Yes
Martini Point-to-Point	Port Based	No
Martini Point-to-Point	Port and VLAN Tagged	No

Label Switched Path

Table 1–5 lists the Label Switched Path (LSP) support on the Cisco IOS cartridge.

Note: Interior Gateway Protocol (IGP) metric ranges are as follows: Absolute: 1 to 4294967295; Relative: -10 to 10 (IGP metric ranges).

Table 1–5 LSP Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
LSP Module	Yes
Primary Tunnel	Yes
Backup Tunnel	Yes
Bypass Tunnel	No
Setup Priority	Yes
Hold Priority	Yes
Affinity	Yes
IGP Metric	Yes
Fast Reroute	Yes
Record Route	Yes
Label Distribution Protocol (LDP) Enabled	Yes

Note that for LSP, the Address Family accepts IPv4 and IPv6 addresses.

Quality of Service

Table 1–6 lists the Quality of Service (QoS) support on the Cisco IOS cartridge.

Table 1–6 QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Layer 3 QoS Support	**Layer 3 QoS Support**	Yes
Access Rule Support	Access Rule Support	Yes
Access Rule Support	Inbound Access Rule Support	Yes
Access Rule Support	Outbound Access Rule Support	Yes
Access Rule Support	Logging	Yes
Access Rule Support	Suppress Management Traffic Terms	Yes
Access Rule Support	Named Access Control List (ACL) Support	Yes
Access Rule Support	Numbered ACL Support (IPv4 only)	Yes
Access Rule Support	Guarantees Supported	No
Access Rule Support	Limits Supported	No
Access Rule Support	Access Rule Classification Criteria	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Access Rule Support	Access Rule Classification Based on Source IPv4 Address	Yes
Access Rule Support	Access Rule Classification Based on Destination IPv4 Address	Yes
Access Rule Support	Access Rule Classification Based on Source IP Port	Yes
Access Rule Support	Access Rule Classification Based on Source IPv6 Address	Yes
Access Rule Support	Access Rule Classification Based on Destination IP Port	Yes
Access Rule Support	Access Rule Classification Based on IP Protocol	Yes
Access Rule Support	Access Rule Classification Based on DiffServ Codepoints	Yes
Access Rule Support	Access Rule Classification Based on IPv4 Precedence Codepoints	Yes
Access Rule Support	Access Rule Classification Based on IPv4 Type of Service (TOS) Codepoints	No
Access Rule Support	Access Rule Classification Based on URL	No
Access Rule Support	Access Rule Classification Based on Multipurpose Internet Mail Extensions (MIME) Type	No
Access Rule Support	Access Rule Classification Based on Application protocol	No
Access Rule Support	Access Rule Classification Based on Application Type	No
Access Rule Support	Access Rule Classification Based on Domain Name	Yes
Access Rule Support	Access Rule Classification Based on 802.1p User Priority	No
Access Rule Support	Access Rule Classification based on MPLS EXP Value	Yes
Access Rule Support	Access Rule Classification Based on Transmission Control Protocol (TCP) Flag Values	Yes
Access Rule Support	Access Rule Classification Based on Internet Control Message Protocol (ICMP) Flag Values	Yes
Access Rule Support	Access Rule Classification Based on Fragments	Yes
Access Rule Support	Access Rule Classification Based on Input Interface Traffic	Yes
Access Rule Support	Access Rule Classification Based on VLAN Traffic	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Access Rule Support	Access Rule Classification Based on Port Traffic	Yes
Access Rule Support	Access Rule Classification Based on Sub Application	Yes
Traffic Classification Rules	Traffic Classification Rules	Yes
Traffic Classification Rules	Inbound Traffic Classification Rule Support	Yes
Traffic Classification Rules	Outbound Traffic Classification Rule Support	Yes
Traffic Classification Rules	Named ACL Support	Yes
Traffic Classification Rules	Traffic Classification Rule Criteria	Yes
Traffic Classification Rules	Traffic Classification Based on Source Media Access Control (MAC) Address	Yes
Traffic Classification Rules	Traffic Classification Based on Destination MAC Address	Yes
Traffic Classification Rules	Traffic Classification Based on Source IPv4 Address	Yes
Traffic Classification Rules	Traffic Classification Based on Destination IPv4 Address	Yes
Traffic Classification Rules	Traffic Classification Based on Source IPv6 Address	Yes
Traffic Classification Rules	Traffic Classification Based on Destination IPv6 Address	Yes
Traffic Classification Rules	Traffic Classification Based on Source IP Port	Yes
Traffic Classification Rules	Traffic Classification Based on Destination IP Port	Yes
Traffic Classification Rules	Traffic Classification Based on IP Protocol	Yes
Traffic Classification Rules	Traffic Classification Based on All DiffServ Code Points	Yes
Traffic Classification Rules	Traffic Classification Based on IPv4 Precedence Codepoints	Yes
Traffic Classification Rules	Traffic Classification Based on IPv4 TOS Codepoints	No
Traffic Classification Rules	Traffic Classification Based on URL	Yes
Traffic Classification Rules	Traffic Classification Based on MIME Type	Yes
Traffic Classification Rules	Traffic Classification Based on Application Protocol	Yes
Traffic Classification Rules	Traffic Classification Based on Application Type	No

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Traffic Classification Rules	Traffic Classification Based on Domain Name	No
Traffic Classification Rules	Traffic Classification Based on 802.1p User Priority	No
Traffic Classification Rules	Traffic Classification Based on MPLS EXP Value	Yes
Traffic Classification Rules	Traffic Classification Based on TCP Flag Bits	Yes
Traffic Classification Rules	Traffic Classification Based on ICMP Flag Values	Yes
Traffic Classification Rules	Traffic Classification Based on Fragments	Yes
Traffic Classification Marketing	Traffic Classification Marking	Yes
Traffic Classification Marketing	Marking DiffServ Code Points	Yes
Traffic Classification Marketing	Marking IPv4 IP Precedence	Yes
Traffic Classification Marketing	Marking IPv4 TOS	No
Traffic Classification Marketing	Marking 802.1p User Priority	No
Traffic Classification Marketing	Marking: MPLS Experimental Bit	Yes
Traffic Classification Marketing	Marking: Topmost MPLS Experimental Bit	Yes
Traffic Classification Marketing	Discard Class	Yes
Traffic Classification Marketing	Trust Type	Yes
Traffic Policing Rules	Traffic Policing Rules	Yes
Traffic Policing Rules	Inbound Traffic Policing Rule Support	Yes
Traffic Policing Rules	Outbound Traffic Policing Rule Support	Yes
Traffic Policing Rules	Policing Rule: Named ACL Support	Yes
Traffic Policing Rules	Policing Rule Classification Criteria	Yes
Traffic Policing Rules	Policing Classification Based on Source MAC Address	No
Traffic Policing Rules	Policing Classification Based on Destination MAC Address	No
Traffic Policing Rules	Policing Classification Based on Source IPv4 Address	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Traffic Policing Rules	Policing Classification Based on Destination IPv4 Address	Yes
Traffic Policing Rules	Policing Classification Based on Source IP Port	Yes
Traffic Policing Rules	Policing Classification Based on Destination IP Port	Yes
Traffic Policing Rules	Policing Classification Based on IP Protocol	Yes
Traffic Policing Rules	Policing Classification Based on All DiffServ Code Points	Yes
Traffic Policing Rules	Policing Classification Based on IPv4 Precedence Codepoints	Yes
Traffic Policing Rules	Policing Classification Based on IPv4 TOS Codepoints	No
Traffic Policing Rules	Policing Classification Based on URL	No
Traffic Policing Rules	Policing Classification Based on MIME Type	No
Traffic Policing Rules	Policing Classification Based on Application Protocol	No
Traffic Policing Rules	Policing Classification Based on Application Type	No
Traffic Policing Rules	Policing Classification Based on Domain Name	No
Traffic Policing Rules	Policing Classification Based on 802.1p User Priority	No
Traffic Policing Rules	Policing Classification Based on MPLS EXP Value	Yes
Traffic Policing Rules	Policing Classification Based on TCP Flags	Yes
Traffic Policing Rules	Policing Classification based on ICMP Flag Values	Yes
Traffic Policing Rules	Policing Classification Based on Fragments	Yes
Traffic Policing Rules	Policing Rule Marking Actions	Yes
Traffic Policing Rules	Policing: Marking DiffServ Code Points	Yes
Traffic Policing Rules	Policing: Marking IP Precedence	Yes
Traffic Policing Rules	Policing: Marking IPv4 TOS	No
Traffic Policing Rules	Policing: Marking 802.1p User Priority	No
Traffic Policing Rules	Policing: Marking: MPLS Experimental Bit	Yes
Traffic Policing Rules	Policing: Marking Topmost MPLS Experimental Bit	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Standard Per Hop Behaviour (PHB) Support	Standard PHB Group Support	Yes
Standard PHB Group Support	PHB Weighted Round Robin (WRR)	No
Standard PHB Group Support	PHB WRR Inbound	No
Standard PHB Group Support	PHB WRR Outbound	No
Standard PHB Group Support	PHB Priority Queuing (PQ)	No
Standard PHB Group Support	PHB Priority Queuing Inbound	No
Standard PHB Group Support	PHB Priority Queuing Outbound	No
Standard PHB Group Support	PHB Weighted Fair Queuing (WFQ)	Yes
Standard PHB Group Support	PHB WFQ Inbound	Yes
Standard PHB Group Support	PHB WFQ Outbound	Yes
Standard PHB Group Support	PHB WFQ Class-based Queuing Support	Yes
Standard PHB Group Support	PHB WFQ Discard Eligibility Marking	Yes
Standard PHB Group Support	PHB WFQ PQ Percentage Bandwidth Support	Yes
Standard PHB Group Support	PHB WFQ Low Priority Queue Percentage Bandwidth Support	Yes
Standard PHB Group Support	PHB WFQ Per-queue Weighted Random Early Detection (WRED) Support	Yes
Standard PHB Group Support	PHB WFQ Per-queue Tail Drop Limits	Yes
Standard PHB Group Support	PHB Congestion Avoidance: WRED	Yes
Standard PHB Group Support	PHB Inbound WRED	Yes
Standard PHB Group Support	PHB Outbound WRED	Yes
Standard PHB Group Support	PHB WRED: Differentiated Services Code Point (DSCP) Support	Yes
Standard PHB Group Support	PHB WRED: IPv4 Precedence	Yes
Standard PHB Group Support	PHB WRED: IPv6 Precedence	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Standard PHB Group Support	PHB WRED: Parameters	Yes
Standard PHB Group Support	PHB WRED: Min Threshold	Yes
Standard PHB Group Support	PHB WRED: Max Threshold	Yes
Standard PHB Group Support	PHB WRED: Max Threshold with units [Bytes or Milliseconds or Default (no units)]	Yes
Standard PHB Group Support	PHB WRED: Weight Factor	Yes
Standard PHB Group Support	PHB WRED: Exponential Weight Constant	Yes
Standard PHB Group Support	PHB: Explicit Congestion Notification	Yes
Standard PHB Group Support	PHB Rate Limiting	No
Standard PHB Group Support	PHB Inbound Rate Limiting	No
Standard PHB Group Support	PHB Outbound Rate Limiting	No
Standard PHB Group Support	PHB Rate Limit Average	No
Standard PHB Group Support	PHB Rate Limit Burst Rate	No
Standard PHB Group Support	PHB Rate Limit Burst Interval	No
Standard PHB Group Support	PHB Frame Relay Fragmentation (FRF)	Yes
Standard PHB Group Support	PHB FRF.12	Yes
Standard PHB Group Support	PHB Frame Relay Traffic Shaping (FRTS)	Yes
Standard PHB Group Support	PHB FRTS - committed information rate (CIR)	Yes
Standard PHB Group Support	PHB FRTS - MINCir	Yes
Standard PHB Group Support	PHB FRTS -committed burst (BC)	Yes
Standard PHB Group Support	PHB FRTS - excess burst (BE)	Yes
Standard PHB Group Support	PHB Inbound CIR	Yes
Standard PHB Group Support	PHB Inbound MINCIR	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Standard PHB Group Support	PHB Inbound BC	Yes
Standard PHB Group Support	PHB Inbound BE	Yes
Standard PHB Group Support	PHB backward explicit congestion notification (BECN)	Yes
Standard PHB Group Support	PHB forward explicit congestion notification (FECN	Yes
Standard PHB Group Support	PHB Frame Relay Hold-Queue Depth	Yes
Standard PHB Group Support	PHB ATM Traffic Shaping	Yes
Standard PHB Group Support	PHB Outbound ATM Traffic Shaping	Yes
Standard PHB Group Support	PHB Inbound ATM Traffic Shaping	Yes
Standard PHB Group Support	PHB ATM Service Classes	Yes
Standard PHB Group Support	PHB ATM Service Class - unspecified bit rate (UBR)	No
Standard PHB Group Support	PHB ATM Service Class - constant bit rate (CBR)	Yes
Standard PHB Group Support	PHB ATM Service Class - real time (RT) variable bit rate (VBR)	Yes
Standard PHB Group Support	PHB ATM Service Class - non-real time (NRT) VBR	Yes
Standard PHB Group Support	PHB ATM Service Class - available bit rate (ABR)	No
Standard PHB Group Support	PHB ATM Service Class - Virtual Circuit (VC)-Class Map Generation	Yes
Standard PHB Group Support	PHB ATM Service Class - VC-Class Map Explicit Naming	Yes
Standard PHB Group Support	PHB ATM Hold-Queue Depth	Yes
Standard PHB Group Support	PHB ATM TX-Ring Limit Support	Yes
Standard PHB Group Support	PHB ATM Queue-depth Support	Yes
MQC-PHB Support	MQC-PHB Support	Yes
MQC-PHB Support	MQC-PHB Classification Criteria	Yes
MQC-PHB Support	Traffic Classification Explicit ACL Number Specification	Yes
MQC-PHB Support	Traffic Classification Explicit ACL Name Specification	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
MQC-PHB Support	Traffic Classification Based on Source MAC Address	Yes
MQC-PHB Support	Traffic Classification Based on Destination MAC Address	Yes
MQC-PHB Support	Traffic Classification Based on Source IPv4 Address	Yes
MQC-PHB Support	Traffic Classification Based on Source IPv6 Address	Yes
MQC-PHB Support	Traffic Classification Based on Destination IPv4 Address	Yes
MQC-PHB Support	Traffic Classification Based on Destination IPv6 Address	Yes
MQC-PHB Support	Traffic Classification Based on Source IP Port	Yes
MQC-PHB Support	Traffic Classification Based on Destination IP Port	Yes
MQC-PHB Support	Traffic Classification Based on IP Protocol	Yes
MQC-PHB Support	Traffic Classification Based on All IPv4 DiffServ Code Points	Yes
MQC-PHB Support	Traffic Classification Based on All IPv6 DiffServ Code Points	Yes
MQC-PHB Support	Traffic Classification Based on URL	Yes
MQC-PHB Support	Traffic Classification Based on MIME Type	Yes
MQC-PHB Support	Traffic Classification Based on Application Protocol	Yes
MQC-PHB Support	Traffic Classification Based on MPLS EXP Value	Yes
MQC-PHB Support	Traffic Classification Based on ATM Cell Loss Priority	Yes
MQC-PHB Support	Traffic Classification - Nested Class Map	Yes
MQC-PHB Support	Traffic Classification Match Any Support	Yes
MQC-PHB Support	Traffic Classification Exclude Option	Yes
MQC-PHB Support	Traffic Classification Based on TCP Flag Bits	Yes
MQC-PHB Support	Traffic Classification Based on ICMP Flag Values	Yes
MQC-PHB Support	Traffic Classification Based on IP Precedence	Yes
MQC-PHB Support	Traffic Classification Based on Fragments	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
MQC-PHB Support	Traffic Classification Routing Table Protocol (RTP) Protocol Port	Yes
MQC-PHB Support	Compound Traffic Classification	Yes
MQC-PHB Support	Low Latency Queuing (LLQ)	Yes
MQC-PHB Support	LLQ Inbound	Yes
MQC-PHB Support	LLQ Outbound	Yes
MQC-PHB Support	LLQ Absolute Bandwidth Support	Yes
MQC-PHB Support	LLQ Percentage Bandwidth Support	Yes
MQC-PHB Support	LLQ Percentage Remaining Bandwidth Support	No
MQC-PHB Support	LLQ Device Default Bandwidth	Yes
MQC-PHB Support	LLQ Burst Support	Yes
MQC-PHB Support	Class Based Weighted Fair Queue (CBWFQ)	Yes
MQC-PHB Support	CBWFQ Inbound	No
MQC-PHB Support	CBWFQ Outbound	Yes
MQC-PHB Support	CBWFQ Absolute Bandwidth Support	Yes
MQC-PHB Support	CBWFQ Percentage Bandwidth Support	Yes
MQC-PHB Support	CBWFQ Remaining Percentage Bandwidth Support	Yes
MQC-PHB Support	CBWFQ Remaining Percentage Bandwidth with Overhead accounting	Yes
MQC-PHB Support	CBWFQ Remaining Percentage Bandwidth with Overhead accounting on ATM	No
MQC-PHB Support	CBWFQ Queue Limit Support	Yes
MQC-PHB Support	Fair-queue Flow Queue-limit Default	Yes
MQC-PHB Support	Fair-queue Flow Queue-limit Limit	Yes
MQC-PHB Support	Class Based Fair Queuing (CBFQ) Max Reserved Bandwidth	Yes
MQC-PHB Support	MQC-PHB Default WFQ	Yes
MQC-PHB Support	MQC-PHB Default WFQ Inbound	No
MQC-PHB Support	MQC-PHB Default WFQ Outbound	Yes
MQC-PHB Support	MQC-PHB Default Reserved Bandwidth Control	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
MQC-PHB Support	MQC-PHB Single Rate Policing	Yes
MQC-PHB Support	MQC-PHB Single Rate Policing Inbound	Yes
MQC-PHB Support	MQC-PHB Single Rate Policing Outbound	Yes
MQC-PHB Support	MQC-PHB Single Rate Policing Absolute Rate	Yes
MQC-PHB Support	MQC-PHB Single Rate Policing Percent Rate	Yes
MQC-PHB Support	Default Committed Bust Size (CBS)	Yes
MQC-PHB Support	Default Excess Burst Size (EBS)	Yes
MQC-PHB Support	MQC-PHB Two Rate Policing	Yes
MQC-PHB Support	MQC-PHB Two Rate Policing Inbound	Yes
MQC-PHB Support	MQC-PHB Two Rate Policing Outbound	Yes
MQC-PHB Support	MQC-PHB Two Rate Policing Absolute Rate	Yes
MQC-PHB Support	MQC-PHB Two Rate Policing Percent Rate	Yes
MQC-PHB Support	MQC-PHB Policing Actions	Yes
MQC-PHB Support	MQC-PHB Policing: Drop	Yes
MQC-PHB Support	MQC-PHB Policing: Set IP Precedence	Yes
MQC-PHB Support	MQC-PHB Policing: Set DiffServ Code Points	Yes
MQC-PHB Support	MQC-PHB Policing: Set MPLS Exp	Yes
MQC-PHB Support	MQC-PHB Policing: Set FR DE	Yes
MQC-PHB Support	MQC-PHB Policing: Set ATM CLP	No
MQC-PHB Support	MQC-PHB Policing: Set Policed Dscp	Yes
MQC-PHB Support	MQC-PHB Shaping Support	Yes
MQC-PHB Support	MQC-PHB Shaping: Inbound	No
MQC-PHB Support	MQC-PHB Shaping: Outbound	Yes
MQC-PHB Support	MQC-PHB Shaping: Default Shaping	Yes
MQC-PHB Support	MQC-PHB Shaping: Shape Average	Yes
MQC-PHB Support	MQC-PHB Shaping: Shape Average with Overhead accounting	Yes

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
MQC-PHB Support	MQC-PHB Shaping: Shape Average with Overhead accounting on ATM	No
MQC-PHB Support	MQC-PHB Shaping: Shape Peak	Yes
MQC-PHB Support	MQC-PHB Shaping: Default Bc	Yes
MQC-PHB Support	MQC-PHB Shaping: Default Be	Yes
MQC-PHB Support	MQC-PHB Maximum Number of Shaping Buffers	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS Support	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS Inbound	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS Outbound	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS MINCir	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS BECN	Yes
MQC-PHB Support	MQC-PHB Shaping: FRTS FECN	Yes
MQC-PHB Support	MQC-PHB Marking Support	Yes
MQC-PHB Support	MQC-PHB Marking Inbound	Yes
MQC-PHB Support	MQC-PHB Marking Outbound	Yes
MQC-PHB Support	MQC-PHB Marking: DiffServ Code Point Support	Yes
MQC-PHB Support	MQC-PHB Marking: MPLS Experimental Bit Support	Yes
MQC-PHB Support	MQC-PHB Marking TopMost MPLS EXP Support	Yes
MQC-PHB Support	MQC-PHB Marking Frame Relay Discard Eligibility Bit Support	Yes
MQC-PHB Support	MQC-PHB Marking ATM Cell Loss Priority Support	Yes
MQC-PHB Support	MQC-PHB Marking IP Precedence	Yes
MQC-PHB Support	MQC-PHB Marking IPv4 TOS	No
MQC-PHB Support	MQC-PHB Marking IPv4 Discard Class	Yes
MQC-PHB Support	MQC-PHB Marking Trust Type	Yes
MQC-PHB Support	MQC-PHB Congestion Avoidance	Yes
MQC-PHB Support	MQC-PHB Congestion Avoidance Queue-limit with units [Bytes or Milliseconds or Default (no units)]	Yes
MQC-PHB Support	MQC-PHB Inbound Congestion Avoidance	No

Table 1–6 (Cont.) QoS Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
MQC-PHB Support	MQC-PHB Outbound Congestion Avoidance	No
MQC-PHB Support	Tail Drop Limit	Yes
MQC-PHB Support	Tail Drop Default	Yes
MQC-PHB Support	MQC-PHB WRED Device Default Parameters	No
MQC-PHB Support	MQC-PHB WRED IP Precedence Support	Yes
MQC-PHB Support	MQC-PHB WRED DSCP Support	Yes
MQC-PHB Support	MQC-PHB Nesting Support	Yes
MQC-PHB Support	MQC-PHB Inbound Nesting	Yes
MQC-PHB Support	MQC-PHB Outbound Nesting	Yes
MQC-PHB Support	MQC-PHB Header Compression	Yes
MQC-PHB Support	MQC-PHB RTP Header Compression Support	Yes
MQC-PHB Support	MQC-PHB TCP Header Compression Support	No
MQC-PHB Support	MQC-PHB with Hierarchical Queuing Framework Support	Yes

Layer 2 QoS

Table 1–7 lists the Layer 2 QoS support on the Cisco IOS cartridge.

Table 1–7 Layer 2 QoS Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
catOSPolicingRule Configuration Policy	No
Policing Rule IP Classification Criteria	No
Classification Based on Trust Type	No
Classification Based on DiffServ Code Point	No
Classification Based on Source IPv4 Address	No
Classification Based on Destination IPv4 Address	No
Policing Rule MAC Classification Criteria	No
Classification Based on Trust Type	No
Classification Based on DiffServ Code Point	No
Classification Based on Source MAC Address	No
Classification Based on Destination MAC Address	No
Policing Rule IPX Classification Criteria	No
Classification Based on Trust Type	No

Table 1–7 (Cont.) Layer 2 QoS Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
Classification Based on DiffServ Code Point	No
Classification Based on Source MAC Address	No
Classification Based on Destination MAC Address	No
Classification Based on Protocol	No
Classification Based on Source IPX Address	No
Classification Based on Destination IPX Address	No
rate-limit Configuration Policy	No
qosCosAttachment Configuration Policy	Yes

Service Assurance

Table 1–8 lists the Service Assurance (SA) support on the Cisco IOS cartridge.

Table 1–8 Service Assurance Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
Service Assurance Probe	Yes
Service Assurance Probe Types	Yes
ICMP Echo Probe	Yes
User Datagram Protocol (UDP) Jitter Probe	Yes
TCP Connect Probe	Yes
UDP Echo Probe	Yes
ICMP Jitter Probe	No
VoIP UDP Jitter Probe	No
RTP-based VoIP Probe	No
VoIP Gatekeeper Delay Monitoring	No
VoIP Call Setup (Post Dial Delay) Monitoring	No
HTTP Probe	No
ICMP Path Echo Probe	No
ICMP Path Jitter Probe	No
FTP Probe	No
DNS Probe	No
Dynamic Host Configuration Protocol (DHCP) Probe	No
Data Link Switching (DLSW) + Probe	No
SA Probe Transmission Parameters	Yes
SA Probe Timeout	Yes
SA Probe Frequency	Yes
SA Probe Lifetime	Yes

Table 1–8 (Cont.) Service Assurance Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
SA Probe Request Size	Yes
SA Destination Port	Yes
SA Source Port	Yes
SA Probe Source IP Address	Yes
SA DSCP	Yes
SA Probe Destination IP Address	Yes
SA Packets in Sequence	Yes
SA Inter-packet Interval	Yes
SA Probe Reaction Configuration	Yes
SA Reaction Configuration - Supported Threshold Types	Yes
Immediate	Yes
Average	Yes
Consecutive	Yes
Never	Yes
X of Y	Yes
SA Reaction Configuration - Supported Action Types	Yes
Trigger	Yes
Trap	Yes
SNA Nmvt	Yes
External System IP	Yes
SA Probe History	Yes
Lives Kept	Yes
Filter	Yes
Buckets	Yes
SA MD5 Support	No
SA Probe Numbering	Yes
SA Explicitly Specified Probe Identifiers	No
SA Auto-generated Probe Identifiers	Yes
SA Probe Checks	Yes
SA Error Checking	Yes
SA Connect Checking	Yes
SA Timeout Checking	Yes
rtrResponder Configuration Policy	Yes

Netflow

Table 1–9 lists the Netflow support on the Cisco IOS cartridge.

Table 1–9 Netflow Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
Measurement Parameters	No
Collect NetFlow Statistics	No
NetFlow Cache Entries	Yes
NetFlow Active Timeout	Yes
NetFlow Inactive Timeout	Yes
NetFlow Aggregation	Yes
NetFlow Aggregation Schemes	Yes
NetFlow Autonomous System Aggregation Scheme	Yes
NetFlow Destination Prefix Aggregation Scheme	Yes
NetFlow Prefix Aggregation Scheme	Yes
NetFlow Protocol Port Aggregation Scheme	Yes
NetFlow Source Prefix Aggregation Scheme	Yes
NetFlow Aggregation Cache Entries	No
NetFlow Aggregation Active Timeout	No
NetFlow Aggregation Inactive Timeout	No
NetFlow Aggregation Export Destinations	No
NetFlow Export Version	No
NetFlow Export Source	No
NetFlow Export Destinations	No
NetFlow Ingress Accounting on Interface	No
Sampled NetFlow	No
Sampled NetFlow on Interface	No
Sampled NetFlow Packet Interval	No
Collect Committed Access Rate (CAR) QoS Management Information Base (MIB) Statistics	No
Collect Juniper Cost of Service (CoS) MIB Statistics	No
Collect MIB2 Statistics	No
collectorParameters Configuration Policy	Yes
Cisco Netflow FlowCollector	Yes
InfoVista Netflow	Yes
netflowParameters Configuration Policy	Yes
NetFlow Cache	Yes
NetFlow Active Timeout	Yes
NetFlow Inactive Timeout	Yes
NetFlow Aggregation	Yes

Table 1–9 (Cont.) Netflow Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
NetFlow Aggregation Schemes	Yes
NetFlow Autonomous System Aggregation Scheme	Yes
NetFlow Destination Prefix Aggregation Scheme	Yes
NetFlow Prefix Aggregation Scheme	Yes
NetFlow Protocol Port Aggregation Scheme	Yes
NetFlow Source Prefix Aggregation Scheme	Yes

VRF and IP Multicast

Table 1–10 lists the VRF and IP Multicast support on the Cisco IOS cartridge.

Table 1–10 VRF and IP Multicast Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
multicastDevice Configuration Policy	Yes
multicastInterface Configuration Policy	Yes
multicastAutoRp Configuration Policy	Yes
multicastBootstrapRp Configuration Policy	Yes
multicastVrf Configuration Policy	Yes

VRF Route Maps

Table 1–11 lists the VRF Route Maps support on the Cisco IOS cartridge.

Table 1–11 VRF Route Maps Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
bgpRoutePolicy Configuration Policy	Yes
vrfRoutePolicy Configuration Policy	Yes

Interface Configuration Management

Table 1–12 lists the Interface Configuration Management support on the Cisco IOS cartridge.

Table 1–12 Interface Configuration Management Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Backup Interface	Backup Interface Policy	Yes
Channelized Interface Creation	E1 Channelized Interface	Yes
Channelized Interface Creation	E1 Controller	Yes
Channelized Interface Creation	E3 Controller	Yes

Table 1–12 (Cont.) Interface Configuration Management Support

Area	IP Service Activator Feature	Supported on Cisco IOS Cartridge
Channelized Interface Creation	E3 Channelized Interface	Yes
Channelized Interface Creation	Synchronous Transport Module level-1 (STM1) Channelized Interface	Yes
Channelized Interface Creation	STM1 Controller	Yes
Channelized Interface Creation	T1 Channelized Interface	Yes
Channelized Interface Creation	T1 Controller	Yes
Channelized Interface Creation	T3 Channelized Interface	Yes
Channelized Interface Creation	T3 Controller	Yes
Cisco	Cisco Ethernet Port	Yes
Cisco	Cisco Universal Interface	Yes
Dialer List	DialerList	Yes
DLSW	DLSW	Yes
DLSW	DLSW Device	Yes
DLSW	DLSW Ethernet Interface	Yes
DLSW	DLSW Token Ring Interface	Yes
HSRP	Hot Standby Router Protocol (HSRP)	Yes
Interface Creation	Basic Rate Interface (BRI)	Yes
Interface Creation	Dialer Interface	Yes
Interface Creation	Loopback Interface	Yes
Interface Creation	Multilink Interface	Yes
Interface Creation	Virtual Template Interface	Yes
Interface Decoration	POS Interface	Yes
Interface Decoration	Serial Interface	Yes
Multicast Interface	Multicast Interface	Yes
PPP Multilink	PPP Multilink	Yes
SGBP	Stack Group Bidding Protocol (SGBP)	Yes
SubInterface Creation	ATM Subinterface	Yes
SubInterface Creation	Frame Relay Interface	Yes
SubInterface Creation	VLAN Sub Interface	Yes

Note that all supported interface configuration management configuration policies support IPv4 and IPv6 addresses.

Base Configuration Policies

Table 1–13 lists the Base Configuration Policies support on the Cisco IOS cartridge.

Table 1–13 Base Configuration Policies Support

IP Service Activator Feature	Supported on Cisco IOS Cartridge
banners Configuration Policy	Yes
ipPools Configuration Policy	Yes
keyChains Configuration Policy	Yes
prefixListEntries Configuration Policy	Yes
snmpCommunities Configuration Policy	Yes
snmpHosts Configuration Policy	Yes
staticRoutes Configuration Policy	Yes
userAuth Configuration Policy	Yes
userData Configuration Policy (provided for generic data model annotation only)	No

Cisco Hardware and Software

For the most up-to-date information about the supported Cisco devices contact Oracle Global Customer Support (GCS). For Oracle GCS contact information, see *IP Service Activator Installation Guide*.

Operating Systems

For complete information about the operating systems supported for the Cisco IOS cartridge, see *IP Service Activator Installation Guide*.

2

Handling a Cisco IOS Upgrade

This chapter explains the steps you need to perform before and after upgrading the Cisco IOS.

Prerequisites

Before performing the Cisco IOS upgrade, complete the following tasks for the device you are upgrading:

1. It is recommended that you resolve as many concretes as possible that are in a conflict or disabled state. Keep a record of those which you can resolve.
2. Run an audit to determine whether IP Service Activator and the device configuration are synchronized. If there are missing commands, consider re-issuing them to clean up the audit. Preserve the audit output.

   For more information on viewing audit logs, see the discussion about audit trails in *IP Service Activator System Administrator's Guide*.
3. Stop all provisioning on the device.
4. Unmanage the device.

Upgrading the Cisco IOS

For instructions on upgrading the Cisco IOS, see the Cisco documentation.

Post-upgrade Tasks

After performing the Cisco IOS upgrade, complete the following tasks for the device you have upgraded:

1. Reset the device capabilities:
   a. Right-click the device and select **Properties**.
   b. Select the **Capabilities** property page.
   c. Click **Reset Device Capabilities**.
   d. In the confirmation popup, click **Yes**.
   e. Click **OK** and then **Commit**.
2. Rediscover the device:
   a. Right-click the device.
   b. Select **Discover**.

3. Verify that the new IOS version was picked up by IP Service Activator:
   a. Right-click the device.
   b. Select **Properties**.

      The **Description** field displays the new IOS version.
4. Manage the device and set it to offline test mode:
   a. Right-click the device and select **Properties**.
   b. Select the **Management** property page.
   c. Select **Offline Maintenance** on the **Command Delivery** list.
   d. Right-click the device and select **Manage**.
   e. Click **OK** and then **Commit**.

      You can access the audit log at the following location to confirm commands were processed in offline maintenance mode:

      /opt/OracleCommunications/IPServiceActivator/AuditTrails/npCisco.audit.log

      For more information on checking an audit trail log for a cartridge, see *IP Service Activator System Administrator's Guide*.

      The audit log must be empty. If there are rejected concretes in step 1 of the "Prerequisites" (based on the reason for rejection), you can view commands. These commands configure the service for the concrete and are related to rejected concretes. If so, you can continue.

      If there are other commands, refer to the options documentation, and confirm that all the concretes used in installation are not in conflict. You must check if the capabilities were fetched correctly. If not, it may be because, the registry was not set up correctly to point to the specific capabilities file.

      If you view commands for non-rejected concretes, check the options. Review the options and see if there is an entry that controls the behavior you view. It is possible that the MIPSA registry entry you made for Device/IOS combination is not being applied. You must check the Network Processor logs to assist you in tracking this down.

      Note: Ideally for every new Device/IOS combination, you must perfect the Network Processor configuration on a lab system, and then apply the changes to the live system once it is debugged. To access the Network Processor logs to confirm processing of the configuration after managing the device:

      /opt/OracleCommunications/IPServiceActivator/logs/networkprocessor.log

      ---

When you manage the device in offline maintenance mode, the following message appears in the **Current Faults** pane for concretes associated with the managed device:

```
Changes to configuration were attempted while in an Offline Mode; some
configuration has not been applied to the device
```

You can safely ignore this message.

5. Change the command delivery mode for the device to online:

   Right-click the device, select **Command Delivery**, select **Online**, then select **Commit**. IP Service Activator will retry sending any rejected configuration.

6. Run an audit to verify that IP Service Activator and the device configuration are synchronized:

   a. Right-click the device and select **Properties**.

   b. Select the **Audit/Migrate** property page.

   c. Click the **Initiate Audit** button.

   d. When the audit is finished, click **Detach Audit**. Then right-click in the new window that appears, choose **Select All** and copy-paste the text to another application or file.

      The device is ready for provisioning through IP Service Activator.

      Compare this audit with the audit generated in the "Prerequisites" step. Use similar steps as given above to reconcile any new discrepancies.

Note: If the audit fails and the post-upgrade audit results show discrepancies between the IP Service Activator configuration and the device configuration, you must verify and update the Cisco IOS options using the IP Service Activator Cisco IOS Cartridge configuration utility. This tool shows you the options available for your device and IOS combination. For more information, see "Cisco Cartridge Configuration Utility". For more information about Device Audit Color Codes, see IP Service Activator online Help. For additional help, you can contact Oracle Global Customer Support.

3

Handling a Card Replacement

This chapter explains the steps you need to perform to replace a card in a Cisco device.

Prerequisites

Before you replace a card in a Cisco device, you will need to do the following:

1. Remove the roles, if you are using the GUI, or unlink the roles, if you are using the OSS Integration Manager (OIM), from all interfaces and sub-interfaces located on the card to be removed.
2. Make sure the operation completes on the device and run device Audit to ensure that all services have been removed from target interfaces (located on card to replace).

Replacing the Card

Proceed with the card replacement according to the vendor's procedure.

Post-replacement Tasks

After you replace a card in a Cisco device, you will need to do the following:

1. When the device is back to normal operation with the new card, re-discover the device.
2. Set roles as required on the interfaces and sub-interfaces located on the new card and proceed with normal provisioning.

4

Device Configuration

This chapter details the authentication methods supported on Oracle Communications IP Service Activator Cisco IOS cartridge and describes the required manual pre-configuration to support various options and services.

Supported Authentication Methods

The IP Service Activator Cisco IOS cartridge supports the following authentication methods on all devices:

- Telnet with TACACS+
- Telnet with Named User
- Telnet with Anonymous
- SSH with password authentication
- SSH with keyed authentication

> **Note:** Anonymous without enable is invalid for Cisco.

Manual Pre-configuration

This section describes the manual pre-configuration required by the Cisco IOS cartridge to support various options and services.

Configuring SNMP

SNMP must be enabled on all routers for the IP Service Activator discovery process to work. Ensure the following line is included in the configuration:

```
snmp-server community community-name RO
```

> **Note:** Setup SNMP for the IP Service Activator discovery process using a community name (typically *public*). You can set the authentication as required. As a best practice make the Community read-only. The network discovery process uses a default community of *public;* you will need to amend the appropriate SNMP parameter in the **Discovery** dialog if you set a different read community on the devices.

Configuring SSH

To use SSH authentication, you need to configure an SSH server on the device.

The device must have a hostname and domain-name.

In configuration mode, enter the following commands:

```
crypto key generate rsa
```

You are prompted for a modulus size for the key. The default is 512, but Cisco recommends the use of a minimum modulus size of 1024 bits.

```
ip ssh time-out 120
ip ssh authentication-retries 3
```

> **Note:** On later versions of IOS, SSH is configured automatically when the device is booted. For more information, see the Cisco documentation.

Mandatory Manual Configuration for MPLS VPNs

Before using IP Service Activator to set up VPNs, some manual configuration of routers is required. The following pre-configuration is required for each device role.

PE Routers

On all PE (gateway) routers in the core VPN, you should ensure the following configuration is present:

IP Addresses

IP addresses must be correctly assigned. IPv4 and IPv6 addresses are supported.

Loopback Interfaces

A loopback interface must be set up and allocated an IP address.

Configuring MPLS

Cisco Express Forwarding (CEF) or Distributed CEF (dCEF) is a prerequisite for label switching. The relevant Cisco commands are:

```
ip cef
ip cef distributed
```

For IPv6:

```
ipv6 cef
```

MPLS must be enabled on all appropriate interfaces. On each of the appropriate interfaces, enable MPLS using one of the following commands:

On IOS 12.1 or earlier:

```
(config-if)tag-switching ip
```

On IOS 12.2:

```
(config-if)mpls ip
```

> **Note:** The `mpls ip` command is a new syntax for the `tag-switching ip` command, so in the running-config you will still see `tag-switching ip`.

On 7200, 7500, and 12000 series routers running IOS 12.2, you also need to run the following command to enable LDP:

```
(config)mpls label switching protocol
```

IPv6 Routing

You must manually enable IPv6 routing to be able to configure the router for IPv6 routing. The relevant Cisco command is:

```
ipv6 unicast-routing
```

IGP

A suitable IGP (such as OSPF, IS-IS, or EIGRP) must be implemented in order to distribute IP routes in the core. The IGP for PE-CE communication is configured by IP Service Activator.

Note that OSPFv3 and RIPng are not supported for IPv6.

P Routers

On all P routers in the core VPN, the following manual configuration is required.

IP Addresses

IP addresses must be correctly assigned.

Loopback Interfaces

It is recommended that a loopback interface be set up and allocated an IP address.

Configuring MPLS

CEF or Distributed CEF is a prerequisite for label switching. The relevant Cisco commands are:

```
ip cef
ip cef distributed
```

For IPv6:

```
ipv6 cef
```

MPLS must be enabled on all appropriate interfaces. On each of the appropriate interfaces, enable MPLS using one of the following commands:

On IOS 12.1 or earlier:

```
(config-if)tag-switching ip
```

or, on IOS 12.2:

```
(config-if)mpls ip
```

> **Note:** The `mpls ip` command is a new syntax for the `tag-switching ip` command, so in the running-config you will still see `tag-switching ip`.

On 7200, 7500, and 12000 series routers running IOS 12.2, you also need to run the following command to enable Label Distribution Protocol (LDP):

```
(config)mpls label switching protocol
```

IPv6 Routing

You must manually enable IPv6 routing to be able to configure the router for IPv6 routing. The relevant Cisco command is:

```
ipv6 unicast-routing
```

IGP

An Interior Gateway Protocol (IGP), such as OSPF, IS-IS, or EIGRP must be implemented in order to distribute IP routes. These are required for creating Label Switched Paths (LSPs).

CE Routers

The CE (access) routers at customer sites are not configured to control routing by IP Service Activator, since they may not be under the control of the network service provider. Therefore they need to be manually configured. You need to ensure the following are set up:

- BGP, RIP, OSPF, or static routing must be configured in order to advertise reachability information between the CE and the PE.
- It is recommended that a loopback interface be set up on each CE router.

Optional Pre-configuration for MPLS VPNs

You can manually pre-configure routers with data which provide specific operational requirements for MPLS VPNs. IP Service Activator is able to incorporate the following pre-configured data into the device configuration.

Pre-defined VRF Tables

You can manually configure VRF tables on a PE router. When a pre-defined VRF table exists on a device, IP Service Activator can treat it in three different ways:

- IP Service Activator has no control of the VRF table or its contents.
- IP Service Activator has control of the VRF table and preserves its contents.
- IP Service Activator has control of the VRF table and removes its contents.

You can specify the amount of control IP Service Activator has over a VRF table by setting certain site-specific values (on the **VRF** property page of the Site dialog box).

Restrictions

- **VRF Table Name**: The name of a user-defined VRF table must be unique on the device. It may consist of up to a maximum of 30 alphanumeric and underscore characters.
- **VRF Table Description**: The description of a pre-defined VRF table can only be changed on the device. If the description is changed on the device, the description will not be affected by a propagated configuration update. If you want to transfer control of the VRF table description to IP Service Activator, you must manually delete its description field from the VRF table on the device.
- **Adding Route Targets and External Features**: It is possible to manually add route targets and parameters (for example, parameters that cannot be configured by IP Service Activator) to a pre-defined VRF table that is controlled by IP Service Activator. However, these parameters are preserved only until IP Service Activator either deletes the VRF table or merges it into another one. This normally occurs if

you change the property settings of the relevant site, in which case the manually added route targets and parameters are no longer required.

External Inbound and Outbound BGP Route-maps

You can choose to implement externally defined inbound and outbound BGP route-maps on a per-interface basis, or have IP Service Activator generate route-maps.

Specifying an external route map will result in the following command being configured within the ipv4-vrf level:

```
neighbor <ip-address> route-map <map-name> in|out
```

where the neighbor ip-address and map-name are taken from the **Route Map** property page on the Site dialog box.

> **Note:** Use a naming scheme different from IP Service Activator's for external inbound and outbound route-maps. IP Service Activator will remove route-maps with the same naming as those which it generates when the device is unmanaged and re-managed.

Pre-defined VRF Import Maps

You can manually pre-define import maps for VRFs on a PE router.

A VRF Import Map allows the site to selectively import routes learned elsewhere.

> **Note:** If different import maps are provisioned against different interfaces in a site, the site will be provisioned using multiple VRFs since only a single VRF import map applies to a VRF.

As well, VRF reduction will not occur between sites with different provisioned import (or export) maps. VRF sharing occurs only if both sites have no import maps, or have the same import maps.

A manually defined import map can be assigned to a VRF table (on the**VRF Export** property page of the Site dialog box).

Import map names longer than the maximum supported by the device are truncated.

Pre-defined VRF Export Maps

You can manually pre-define export maps for VRFs on a PE router. The export map only allows those routes in the VRF table whose route prefixes match those specified in the export map to be advertised to other PE routers. The exported routes are tagged with an RT value specified by the export map.

A manually defined export map can be assigned to a VRF table (on the **VRF Export** property page of the Site dialog box).

Export map names longer than the maximum supported by the device are truncated.

Configuring an Export Map

The following commands provide an example of configuring an export map.

```
access-list 1 permit 128.1.1.1
```

Defines access list 1 which accepts routes with IP address 128.1.1.1

```
access-list 2 permit any
```

Defines access list 2 which accepts any routes

```
route-map export-map-name permit sequence-number
match ip address 1
set extcommunity rt 100:94
```

Export map `export-map-name` attaches route target 100:94 to routes specified in access list 1. The `sequence-number` identifies the order in which the route-map is implemented.

```
route-map export-map-name permit sequence-number
match ip address 2
set extcommunity rt 100:26
```

Export map `export-map-name` attaches route target 100:26 to routes specified in access list 2. The `sequence-number` must be a higher value than the preceding sequence-number.

If an export map is used by a management VPN, the spoke sites are not required to export route targets. To prevent management spoke sites exporting route targets, set **Spoke** to **None** for the spoke site's export policy route target on the **MPLS** property page in the VPN dialog box, or alternatively, use the pre-defined export map configuration shown in the following example:

```
export map 'ExpMapCust#1'
route-target export 1:1111
route-target export 1:1394
route-target export 1:1614
```

where `ExpMapCust#1` is a pre-defined export map used by both management and customer VPN sites; `1:1111` is the route target of the management hub site, `1:1394` and`1:1614` are the route targets of the customer sites in the VRF table of each spoke site.

```
ip access-list extended ExpMap_Mng
deny ip 192.168.65.0.0.0.0.255 any
deny ip 20.20.20.0.0.0.0.255 any
permit ip any any
```

where `deny ip 192.168.65.0.0.0.0.255 any` rejects matching routes to the management hub site, `deny ip 20.20.20.0.0.0.0.255 any` rejects routes to the customer LAN, `permit ip any` any accepts all other routes.

```
route-map ExpMapCust#1 permit 10
match ip address ExpMap_Mng
set extcommunity rt 1:1394 1:1614
```

Export map `ExpMapCust#1` attaches route targets `1:1394` and`1:1614` to routes permitted by access list `extended ExpMap_Mng`. Note that the management hub site route target `1:1111` is not attached to these routes.

Pre-defined Prefix List Filters

When eBGP is used as the CE-PE protocol, the number of routes that are received from, or sent to, a CE router can be selectively reduced using a manually pre-defined prefix list installed on the neighboring PE router. Routes whose prefixes match those in the prefix list will either be allowed or rejected by the PE router depending on their designation in the prefix list. You need to specify in the user interface that the prefix

list is required to only filter routes that are either incoming (CE to PE) or outgoing (PE to CE).

A pre-defined prefix list can be used instead of an access list for configuring a pre-defined export map described in "Pre-defined VRF Export Maps".

Creating a Prefix List

You can configure a prefix list using the commands described below in router configuration mode. You can apply a pre-configured prefix list filter to a site by entering the name of the prefix list in the **Prefix filters In** or **Out** fields on the **EBGP Advanced** property page of the Site dialog box.

If a route prefix received by the PE matches a prefix in the prefix list, that prefix will either be accepted or rejected depending on whether the entry is designated as **permit** or **deny**. The following conditions also apply:

- A prefix is denied if it cannot be matched with any prefixes in the prefix list.
- If a prefix matches several prefixes in the prefix list, the prefix with the lowest sequence value is used.

This command adds a single entry to a prefix list:

```
ip prefix-list list-name [seq sequence-value] deny|permit prefix|prefix-length [ge ge-value] [le le-value]
```

Sequence values are automatically generated by default. You only need to specify a sequence value if the automatic generation of sequence values is disabled. For more information, see "Sequence Values".

You must specify either **deny** or **permit** for the specified prefix to be either allowed or rejected by the PE router.

`ge` and `le` values specify a prefix length range, where:

prefix length < `ge-value` <= `le-value` <= 32.

Examples: `198.0.0.0/8 ge 16 le 16` specifies all prefixes in the range 198.0.0.0/8 to 198.0.0.0/16.

`198.0.0.0/0 ge 16 le 24` specifies all prefixes in the range 198.0.0.0/16 to 198.0.0.0/24.

If only the `ge-value` is specified, the prefix range is from `ge-value` to 32.

If only the `le-value` is specified, the prefix range is from the `prefix-length-value` to `le-value`.

Sequence Values

Sequence values are generated automatically by default, but generation can be disabled using:

```
no ip prefix-list sequence-number
```

Sequence values are, by default, automatically generated in increments of 5, so that the first list entry has a value of 5 and the next entry has a value of 10 and so on.

Examples of Configuring a Prefix List

Deny routes with prefixes 196.0.0.0/8 and prefix lengths greater than 25 up to 32 in network 192/8:

```
ip prefix-list filter1 deny 192.0.0.0/8 ge 25
```

Deny all routes in Class A network 22/8 by specifying prefix lengths from /8 to /32:

```
ip prefix-list filter1 deny 22.0.0.0/8 le 32
```

Deny routes with prefixes 100.70.1/ with prefix lengths from /24 to /25:

```
ip prefix-list filter1 deny 100.70.1.0/24 ge 25
```

Permit route 36.0.0.0/8:

```
ip prefix-list filter1 36.0.0.0/8
```

Permit routes with prefix lengths of 8 to 24; make list entry sequence value 5:

```
ip prefix-list filter1 seq 5 permit 0.0.0.0/0 ge 8 le 24
```

Manually Pre-configured Multi-AS VPNs

You can use IP Service Activator to manage manually pre-configured multi-AS VPNs.

When managing multi-AS VPNs with IP Service Activator, the domain-level property **Configure iBGP Peering** must be deselected in the user interface. For more information, see *IP Service Activator VPN User's Guide*.

PE Routers in the Same AS

iBGP peering must be manually pre-configured between PE routers that reside in the same AS.

For example:

```
router bgp 65057
  no synchronization
  no auto-summary
  neighbor 10.52.0.1 remote-as 65057
  neighbor 10.52.0.1 update-source 10.52.20.1

  address-family vpnv4 unicast
    neighbor 10.52.0.1 activate
    neighbor 10.52.0.1 next-hop-self
    neighbor 10.52.0.1 send-community extended
  exit
```

Inter-AS PE routers

eBGP peering must be manually pre-configured between PE routers where each PE router resides in a different AS.

For example:

```
router bgp 65057
  no synchronization
  no auto-summary
  neighbor 10.52.0.1 remote-as 65056
  neighbor 10.52.0.1 ebgp-multihop
  neighbor 10.52.0.1 update-source 10.52.20.1

  address-family vpnv4 unicast
    neighbor 10.52.0.1 activate
    neighbor 10.52.0.1 next-hop-self
    neighbor 10.52.0.1 send-community extended
  exit
```

To configure the necessary functionality on the device, see the Cisco documentation: http://www.cisco.com/cisco/web/psa/default.html

Mandatory Manual Pre-configuration for Layer 2 Martini VPNs

Before configuring Layer 2 Martini VPNs, ensure that devices are preconfigured as described in this section.

Specify Label Distribution Protocol on Interfaces for Martini L2 Connections

Specify the LDP on each interface to be used for a Layer 2 Martini connection. If you do not specify LDP, tag distribution protocol (TDP) is used instead.

Log into the PE router and enter: `mpls label protocol ldp`

Assign Label Distribution Protocol Router IDs to the PE Routers

To assign LDP router IDs to the PE routers, perform the following steps. Both PE routers require a loopback address that you can use to create a virtual circuit between the routers.

1. Enter interface configuration mode: `interface loopback0`

   Note: The LDP router ID must be configured with a 32-bit mask to ensure proper operation of MPLS forwarding between PE routers.

2. Assign an IP address to the loopback interface: `ip address <ip-address>`
3. Assign the loopback IP address as the router ID: `mpls ldp router-id loopback0 force`

   Note: This command forces the loopback interface to be the LDP router ID on each PE router. Without *force*, the router can assign a different router ID, thereby preventing the establishment of virtual circuits between PE routers.

5

Cisco Cartridge Configuration Utility

This chapter describes the Oracle Communications IP Service Activator Cisco IOS cartridge configuration utility and explains how to use it.

About the Cisco Cartridge Configuration Utility

The Cisco cartridge configuration utility is a command line tool that is installed with the Cisco IOS cartridge, and provides the ability to automatically generate options and registry files for your Cisco devices.

You can run the Cisco cartridge configuration utility to generate a CSV (comma-separated values) file containing entries for all the Cisco devices and IOS combinations in your IP Service Activator database. You can then run the Cisco cartridge configuration utility again to generate the options files for your devices. The Cisco cartridge configuration utility reads the options from the master options CSV file and matches them to your device and IOS combinations.

The Cisco cartridge configuration utility will create an options xml file for each device and IOS version. The tool can be run with a different parameter to generate a registry file that will use the newly generated options files. The necessary procedures are provided in this section, and cover the tasks listed in the task checklist.

The **cartridgeConfigurationTool.sh** script is the executable file used to invoke commands in the Cisco cartridge configuration utility.

Task Checklist

The following list displays the suggested order of tasks for using the Cisco cartridge configuration utility:

1. Retrieving a List of Device Type and IOS Version Combinations
2. Generating the Registry File
3. Generating Multiple Options Files and/or Generating a Single Options File
4. Generating Capabilities Files

Using the Cisco Cartridge Configuration Utility: General Commands

The Cisco cartridge configuration utility is installed with the IP Service Activator Cisco IOS cartridge. Following is the syntax of a list of device type and IOS version combinations:

Navigate to the *IP_SERVICE_ACTIVATOR_HOME* **/bin** directory.

For example:

```
bin/cartridgeConfigurationTool.sh -help
```

Table 5–1 displays general usage commands for the Cisco cartridge configuration utility.

Table 5–1 Commands for Cisco Cartridge Configuration Utility

Command	Description
-generateCapabilitiesFiles	Generates an initial set of capabilities files.
-generateOptionsInDir	Generates the complete set of options in the output directory.
-generateOptionsZip	Generates the complete set of options.
-generateRegistry	Generates the **MIPSA_registry.xml** file.
-generateSingleOptionsFile	Generates a single options file.
-help	Displays help text for the Cisco cartridge configuration utility.
-output	Sets the output filename or directory.
-queryActiveDeviceTypesAndIOS	Queries IP Service Activator for active Cisco device and IOS data.

Retrieving a List of Device Type and IOS Version Combinations

Using the **cartridgeConfigurationTool.sh** executable file in the Cisco cartridge configuration utility, you can retrieve a list of device type and IOS version combinations from the Policy Server database.

To retrieve a list of device type and IOS version combinations:

1. Navigate to the *IP_SERVICE_ACTIVATOR_HOME* directory.
2. Execute one of the following commands:

```
bin/cartridgeConfigurationTool.sh -queryActiveDeviceTypesAndIOS db [host_name
port sid user_name password] [proxyagent] [-output output_filename]
OR
bin/cartridgeConfigurationTool.sh -queryActiveDeviceTypesAndIOS oim [hostname
port username password] [proxyname] [-output output_filename]
```

Table 5–2 Commands to Retrieve Device TypOe and IOS Version Combinations

Where	Is
db	Used to query data directly from the database.
oim	Used to query data via the IP Service Activator Integration Manager.
hostname	The database (db) or IP Service Activator naming service (oim) host name or IP address.
port	The database (db) or IP Service Activator naming service (oim) port number. (Optional).
sid	The database (db) SID.
username	The database (db) or IP Service Activator (oim) username.
password	The database (db) or IP Service Activator (oim) password.

Table 5–2 (Cont.) Commands to Retrieve Device TypOe and IOS Version Combinations

Where	Is
proxyagent	Used to restrict the device query to devices managed by the specified proxy agent (optional).
output_filename	The device IOS data output file (optional) that will be created in *IP_SERVICE_ACTIVATOR_HOME* directory

For example:

```
bin/cartridgeConfigurationTool.sh -queryActiveDeviceTypesAndIOS oim localhost 2809
orchestream orchestream -output device_ios.csv
```

Multi-valued List Options

The cartridge configuration tool can generate options for multivalued lists. An entry in the CSV provided as the base (cisco_options.csv) includes values for the option `cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.hardwareList`. The multiple values for this option will be separated by "\" (single back slash) so that running the script (cartridgeConfigurationTool.sh on UNIX or Solaris and cartridgeConfigurationTool.bat on Windows) generates options XML with the multiple values provided.

The following is an example of the format of the CSV entry:

```
cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.hardwareList,Cisco
7600,12.*\(.*\)SXE,12.2(18)SXE,,7600-SIP-200\7600-SIP-400\7600-SIP-600,Cisco service policy direct reference on frame-relay - Hardware list
```

For this example, the output generated in the generated XML will be as follows:

```
<cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.hardwareList>

<base:item>7600-SIP-200</base:item>

<base:item>7600-SIP-400</base:item>

<base:item>7600-SIP-600</base:item>

</cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.hardwareList>
```

Generating the Registry File

Using the **cartridgeConfigurationTool.sh** executable file in the Cisco cartridge configuration utility, you can generate the **MIPSA_registry.xml** file with your set of device type and IOS version combinations.

For more information on cartridge capabilities management and the registry, see *IP Service Activator System Administrator's Guide*.

To generate the registry file:

1. Navigate to the *IP_SERVICE_ACTIVATOR_HOME* directory.
2. Execute the following command:

   ```
   bin/cartridgeConfigurationTool.sh -generateRegistry device_ios_data package
   default|series|device|deviceios [-output output_filename]
   ```

Table 5–3 Commands to Generate the Registry File

Where	Is
device_ios_data	The csv file of the device type and IOS version pairs that were generated in the procedure. For more information, see "Retrieving a List of Device Type and IOS Version Combinations".
package	The package prefix for the generated options and capabilities files. This translates to an output directory. You can specify a multi-level destination sub-directory hierarchy by providing multiple sub-directory names separated by "." characters. The target directory will be created below the output directory for the registry file.
default	Used to generate all capabilities references to **cisco_default.xml**.
series	Used to generate capabilities references for each device series - for example: **cisco_3600.xml.**
device	Used to generate capabilities references for each device type - for example: **cisco_3640.xml.**
deviceios	Used to generate capabilities references for each device IOS combination - for example: **cisco_3640-12.2(13)T.xml**.
output_filename	The name of the output registry file.

For example:

```
bin/cartridgeConfigurationTool.sh -generateRegistry device_ios.csv
com.oracle.ipsa series -output MIPSA_registry.xml
```

The **MIPSA_registry.xml** file is saved in the *IP_SERVICE_ACTIVATOR_HOME* directory.

3. Update the MIPSA registry file to include the new IOS/device combinations. For information on how to include the new IOS/device combinations, see the discussion about creating or editing a cartridge registry file in *IP Service Activator System Administrator's Guide*.
4. Copy the generated registry file to the following directory: *IP_SERVICE_ACTIVATOR_HOME***/Config/networkProcessor**

Note: If you need to re-generate the **MIPSA_registry.xml** file by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completion. When you reload the registry, the Network Processor reloads its configuration files. The path for the reload registry script is *IP_SERVICE_ACTIVATOR_HOME***/bin**. To reload the registry, execute the following command:

```
npAdmin.sh reload_registry
```

Understanding Registry File Behavior

An entry in the **MIPSA_registry.xml** file matches a device if *all* of the following conditions are met:

- `driverType` is equal to the Device Driver value from the Device Type entry on the **Topology** tab in the IP Service Activator GUI.
- `deviceType` matches the Model, s/w Vn value from the Device Type entry on the **Topology** tab in the IP Service Activator GUI if `useRegex` is turned off.

- `osVersion` appears as a substring in the **Description** field on the **Device** property page in the IP Service Activator GUI if `useRegex` is turned off.

If multiple entries in the **MIPSA_registry.xml** file match a given device, the first entry (the one listed first in the file) is used.

Regular expression matching is not supported for the **driverType** field. However, it can be enabled for the **deviceType** and **osVersion** fields by including the `useRegex` attribute as follows:

```
<deviceType useRegex="true" >Cisco 26[0-9][0-9]</deviceType>
<osVersion useRegex="true" >12.2(1[45])T</osVersion>
```

See the sample **MIPSA_registry.xml** file below for examples of the values mentioned above.

Sample Registry File Entry

The following is a sample MIPSA registry file entry:

```
<!-- Cisco 2611 -->
<cartridgeUnit>
<name>com.oracle.ipsa.cu1.2611.12.2(15)T16</name>
<driverType>cisco</driverType>
<deviceType>Cisco 2611</deviceType>
<osVersion>12.2(15)T16</osVersion>
<smToDmQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/sm2dm.xq</sm
ToDmQuery>
<dmValidation>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/dmValidatio
n.xq</dmValidation>
<dmMigration>com/metasolv/serviceactivator/cartridges/cisco/xquerylib/dmMigration.
xq</dmMigration>
<dmToCliQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/annotatedDm
2Cli.xq</
dmToCliQuery>
<capabilities>com/oracle/ipsa/capabilities/cisco_2600.xml</capabilities>
<options>com/oracle/ipsa/options/Cisco_2611-12.2(15)T16.xml</options>
<errorMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/errorMessag
es.xml</
errorMessages>
<warningMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/warningMe
ssages.xml</warningMessages>
<successMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/successMe
ssages.xml</successMessages>
</cartridgeUnit>
```

Generating Multiple Options Files

Using the **cartridgeConfigurationTool.sh** executable file in the Cisco cartridge configuration utility, you can generate a complete set of options configuration files for your Cisco device types and IOS versions.

For more information on cartridge capabilities management and option files, see *IP Service Activator System Administrator's Guide*.

To generate multiple options files:

1. Navigate to the *IP_SERVICE_ACTIVATOR_HOME*/**lib/java-lib/cartridges/cisco** directory.
2. Execute the following command:

   ```
   bin/cartridgeConfigurationTool.sh -generateOptionsZip options_filename device_
   ```

```
ios_data package -output output_zipfile
```

Table 5–4 Commands to Generate Multiple Options Files

Where	Is
options_filename	The path to the master options configuration data (**cisco_options.csv)**.
device_ios_data	The csv file of the device type and IOS version pairs that was generated in the procedure. For more information, see "Retrieving a List of Device Type and IOS Version Combinations".
package	The package prefix for options files. This translates to an output directory. You can specify a multi-level destination sub-directory hierarchy by providing multiple sub-directory names separated by "." characters. The target directory will be created below the output directory for the registry file.
output_zipfile	The file name of the output zip file.

For example:

```
bin/cartridgeConfigurationTool.sh -generateOptionsZip Config/cisco_options.csv
device_ios.csv com.oracle -output cisco_options.zip
```

The **cisco_options.zip** file is saved in *IP_SERVICE_ACTIVATOR_HOME*.

3. Load the updated options by doing one of the following:
   - Extract the **cisco_options.zip** file to the *IP_SERVICE_ACTIVATOR_HOME*/**Config/networkProcessor** directory. The new options will be dynamically picked up from the classpath if you use the `reload_registry` command.
   - Shut down and restart the Network Processor. The updated options will be reloaded from the **options.zip** file.

Note: If you need to re-generate options by running this procedure again at a later time, you must re-start the Network Processor after completing this procedure.

Generating a Single Options File

Using the **cartridgeConfigurationTool.sh** executable file in the Cisco cartridge configuration utility, you can generate a single options file for a specific Cisco device type and IOS version.

For more information on cartridge capabilities management and option files, see *IP Service Activator System Administrator's Guide*.

To generate a single options files:

1. Navigate to the *IP_SERVICE_ACTIVATOR_HOME* directory.
2. Execute the following command:

```
bin/cartridgeConfigurationTool.sh -generateSingleOptionsFile options_filename
"device_type" "ios_version" [-output "output_filename"]
```

Table 5–5 Commands to Generate a Single Options File

Where	Is
options_filename	The path to the master options configuration data file (**cisco_options.csv**).
device_type	The Cisco device type entered between quotation marks.
ios_version	The Cisco IOS version entered between quotation marks.
output_filename	The name of the output XML file entered between quotation marks.

For example:

```
bin/cartridgeConfigurationTool.sh -generateSingleOptionsFile Config/cisco_
options.csv "Cisco 3640" "12.2(13)T4" -output "cisco_options_3640_
12.2(13)T4.xml"
```

The generated file is saved in the *IP_SERVICE_ACTIVATOR_HOME* directory.

3. Copy the output xml file to the following directory:

   IP_SERVICE_ACTIVATOR_HOME/**Config/networkProcessor/com/oracle/ipsa/options**

> **Note:** If you need to re-generate options by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completing this procedure. When you reload the registry from *IP_SERVICE_ACTIVATOR_HOME*/**bin**, the Network Processor reloads its configuration files. To reload the registry, execute the following command:
>
> ```
> npAdmin.sh reload_registry
> ```

Generating Capabilities Files

Using the **cartridgeConfigurationTool.sh** executable file in the Cisco cartridge configuration utility, you can generate an initial set of capabilities files based on the default cartridge capabilities.

Note that only new (missing) capabilities files are generated - existing files are not modified.

For more information on cartridge capabilities management, see *IP Service Activator System Administrator's Guide*.

To generate capabilities files:

1. Navigate to the *IP_SERVICE_ACTIVATOR_HOME* directory.
2. Execute the following command:

   ```
   bin/cartridgeConfigurationTool.sh -generateCapabilitiesFiles device_ios_data
   package default|series|device|deviceios [-output output_dir]
   ```

Table 5–6 Commands to Generate Capabilities Files

Where	Is
device_ios_data	The csv file of the device type and IOS version pairs that was generated in the procedure. For more information, see "Retrieving a List of Device Type and IOS Version Combinations".

Table 5–6 (Cont.) Commands to Generate Capabilities Files

Where	Is
package	The package prefix for capabilities files. This translates to an output directory. You can specify a multi-level destination sub-directory hierarchy by providing multiple sub-directory names separated by "." characters. The target directory will be created below the output directory for the registry file.
default	Used to generate the capabilities file **cisco_default.xml**.
series	Used to generate the capabilities files for each device series - for example: **cisco_3600.xml**.
device	Used to generate the capabilities files for each device type - for example: **cisco_3640.xml**.
deviceios	Used to generate the capabilities files for each device IOS combination - for example: **cisco_3640-12.2(13)T.xml**.
output_directory	The directory where the capabilities package and files are to be created (optional) - if you do not specify a directory, IP Service Activator will use the current directory.

For example:

```
bin/cartridgeConfigurationTool.sh -generateCapabilitiesFiles device_ios.csv
com.oracle series -output ./Config/networkProcessor
```

The Cisco cartridge configuration utility creates the capabilities file and places it in a package directory structure in the following directory:

*IP_SERVICE_ACTIVATOR_HOME***/Config/networkProcessor/com/oracle/ipsa/capabilities**

Note: If you need to re-generate the capabilities files by running this procedure again at a later time, you must re-start the Network Processor or reload the registry after completing this procedure. When you reload the registry from *IP_SERVICE_ACTIVATOR_HOME***/bin**, the Network Processor reloads its configuration files. To reload the registry, execute the following command:

```
npAdmin.sh reload_registry
```

6

Cisco Pre-checks and Post-checks

This chapter describes the pre-checks and post-checks that can be run and explains how to install, enable, and disable them. It also describes the behavior of the individual pre-checks and post-checks for the Cisco IOS cartridge.

About Pre-checks and Post-Checks

Pre-checks look for existing configuration on a device when you commit a configuration. This prevents disruption of existing services.

Pre-checks also determine if the Oracle Communications IP Service Activator configuration will create conflicts with an existing configuration, during creation of a new service instance by IP Service Activator. In case a conflict is detected, the operation is aborted and an error message generated.

The post-checks look for the configuration after it has been applied on a device. Post-checks determine if an IP Service Activator configuration is really configured on the device or silently rejected by that device, after an IP Service Activator creates a new service instance. An error message is generated if the device silently rejects the configuration, and the applied configuration is rolled back.

Post-checks can validate successful application of a configuration beyond the simple validation offered by the device response during command issue.

Installing Pre-checks and Post-checks

The standard pre-checks and post-checks are installed when IP Service Activator is installed. For more information, see *IP Service Activator Installation Guide*.

Enabling/disabling Pre-checks and Post-checks

Pre-checks and post-checks can be enabled and disabled using the **standard.properties** file. The file is located in the following directory:

Config/networkProcessor/com/metasolv/serviceactivator/cartridges/cisco/pre_check/standard.properties.txt

To disable a particular pre-check or post-check, change its value to **false**, as shown in the example below. The value **true** indicates an enabled pre-check or post-check.

```
<checkProperties xmlns="http://www.metasolv.com/ serviceactivator/checkproperties"
>
    <preCheckRouteMap>true</preCheckRouteMap>
    <preCheckClassMap>true</preCheckClassMap>
    <preCheckPolicyMap>true</preCheckPolicyMap>
```

```
    <preCheckNamedAcl>true</preCheckNamedAcl>
    <preCheckVrf>true</preCheckVrf>
    <preCheckCryptoMap>true</preCheckCryptoMap>
    <preCheckConfigVersion>false</preCheckConfigVersion>
    <preCheckRouterIOSUpgrade>false</preCheckRouterIOSUpgrade>
    <preCheckPolicer>true</preCheckPolicer>
</checkProperties>
```

Individual Pre-checks and Post-checks

Table 6–1 outlines the behavior of the individual pre-checks and post-checks for the Cisco IOS cartridge.

Table 6–1 Pre-checks and Post-checks

Name	Behavior	Default
Pre-checks		
preCheckRouteMap	Raises a fault when a route map with the specified name exists. It is a VPN service precheck.	On
preCheckClassMap	Raises a fault when a class map with the specified name exists. It is a QOS service precheck.	On
preCheckPolicyMap	Raises a fault when a policy map with the specified name exists. It is a QOS service precheck.	On
preCheckCryptoMap	Raises a fault when a crypto map with the specified name and sequence exists. It is an IPsec service precheck.	On
preCheckNamedAcl	Raises a fault when an ACL with the specified name exists. It is a QoS service precheck.	On
preCheckVrf	Raises a fault when a VRF with the specified name exists. It is a VPN service precheck.	On
preCheckRouterIOSUpgrade	Raises a fault when router IOS version does not match the version from the last device discovery.	Off
preCheckConfigVersion	Raises a fault when the IP Service Activator and the router configuration versions do not match.	Off
preCheckPolicer	Raises a fault when an aggregate policer with the specified name exists. It is a Layer 2 QOS service precheck.	On

Table 6–1 (Cont.) Pre-checks and Post-checks

Name	Behavior	Default
preCheckMlsQos	Raises a fault when MLS QoS is disabled. It is a Layer 2 QoS service precheck.	Off
preCheckVlanVtpModeServer	Raises a fault when the user tries to add a VLAN with value greater than 1005 while router runs in VTP Server mode. It is a VLAN service precheck.	On
preCheckVlanVtpModeClient	Raises a fault when the user tries to add or modify a VLAN while router runs in VTP Client mode. This pre-check, looks for any VLAN operations involving adding new VLAN, and modifying or deleting any existing VLAN. If enabled, it takes over pre-checking transactions of the preCheckVlanVtpModeServer pre-check, for the extended VLAN range with IDs above 1005. It is a VLAN service pre-check.	Off
preCheckInterfaceMediaType	Raises faults in the following scenarios: ■ Interface media type is RJ45 and speed is being set to default or nonegotiate value. ■ Interface media type is not RJ45 and speed is not being set to default or nonegotiate value. **Note**: This pre-check is only invoked when a user tries to set GigabitEthernet interface Speed value through ciscoEthernePortCharacteristics configuration policy.	On
preCheckVlanIdSync	Raises a fault when VLAN IDs on trunk interface is not the subset of VLAN IDs being configured through IP Service Activator. It is a vlanInterface configuration policy specific pre-check.	On
preCheckOspfProcessId	Raises a fault when Ospf process-id being configured through IP Service Activator already exists on the device. It is an Ospf routing protocol specific pre-check.	On

Table 6–1 (Cont.) Pre-checks and Post-checks

Name	Behavior	Default
preCheckInterfaceOspfMessageDigestKeyId	Raises a fault when Ospf md5 authentication key-id already exists on the interface or sub-interface on which ospf routing protocol with md5 authentication is being configured. It is an ospf routing protocol specific pre-check.	On
preCheckMsdpConnectSourceOriginatorIdInterface	Raises a fault when msdp originator-id interface or msdp connect-source interface being configured through IP Service Activator does not exist on the device. It is Multicast Source Discovery Protocol specific pre-check.	On
preCheckMulticastRegisterSourceInterface	Raises a fault when the interface configured for pim register-source in Multicast Device configuration policy does not exist on the device.	Off
Post-checks		
postChecksEnabled	It is a global flag that enables or disables post-checks.	Off
postCheckIntfServicePolicyInput	Raises a fault when interface Service policy in input direction is silently rejected by a device. **Note**: For QoS policies containing the bandwidth, priority, random-detect, queue-limit, and shaping some IOS of 3500 switches silently reject configuration if it is applied in input direction.	Off

A

Options Framework

This appendix outlines the options framework in the Oracle Communications IP Service Activator Cisco IOS cartridge.

The options framework controls the configuration style for different device type and IOS operating system version combinations. These options are registered by the cartridge in the **MIPSA_registry.xml** file. A sample file is displayed below:

```
<?xml version="1.0" encoding="UTF-8"?>
<cartridgeUnits xmlns="http://www.metasolv.com/serviceactivator/networkprocessor
/cartridgemanager/">

  <!-- Cisco 7206VXR -->
  <cartridgeUnit>
    <name>com.oracle.cu1.7206VXR.12.4(11)T3</name>
    <driverType>cisco</driverType>
    <deviceType>Cisco 7206VXR</deviceType>
    <osVersion>12.4(11)T3</osVersion>
    <smToDmQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/sm2dm.
xq</smToDmQuery>
    <dmValidation>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/dmVal
idation.xq</dmValidation>
    <dmMigration>com/metasolv/serviceactivator/cartridges/cisco/xquerylib/dmMigr
ation.xq</dmMigration>
    <dmToCliQuery>com/metasolv/serviceactivator/cartridges/cisco/units/cu1/annot
atedDm2Cli.xq</dmToCliQuery>
    <capabilities>com/oracle/capabilities/cisco_7200.xml</capabilities>
    <options>com/oracle/options/Cisco_7206VXR-12.4(11)T3.xml</options>
    <errorMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/error
Messages.xml</errorMessages>
 <warningMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/war
ningMessages.xml</warningMessages>
    <successMessages>com/metasolv/serviceactivator/cartridges/cisco/messages/suc
cessMessages.xml</successMessages>
  </cartridgeUnit>

</cartridgeUnits>…
```

The *options* entry references an option configuration file with the path relative to *SERVICEACTIVATOR_HOME* **/Config/networkProcessor**.

In this example, the **Cisco_7206VXR-12.4(11)T3.xml** file is located in the following directory:

*IP_SERVICE_ACTIVATOR_HOME***/Config/networkProcessor/com/oracle/options**

A sample file is displayed below:

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!--
 - Oracle IP Service Activator Cisco Cartridge Options
 - Device: Cisco 7206VXR
 - IOS: 12.4(11)T3
 -->
<base:options xsi:type="CartridgeOptions"
xmlns="http://www.metasolv.com/serviceactivator/cisco/options"
xmlns:base="http://www.metasolv.com/se
rviceactivator/options" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<cartridge.cisco.qos.mapClassNamingStrategy>auto</cartridge.cisco.qos.mapClassNami
ngStrategy>

<cartridge.cisco.qos.mapclass.framerelay.mincir.in.validation>sameAsOut</cartridge
.cisco.qos.mapclass.framerelay.mincir.in.validation>
   <cartridge.cisco.qos.atmQosOnPvc>vcClass</cartridge.cisco.qos.atmQosOnPvc>
</base:options>
```

Configuration Options

Table A–1 details the configuration options for the Cisco IOS cartridge. For the options files to be valid, you must enter the options definitions in the order below. The default value is used if an option is not defined.

Note: Changing the value of an option for a device that has existing configurations provisioned by IP Service Activator could result in the configurations being removed and re-added using the new configuration style.

Table A–1 Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.mapClassNamingStrategy	auto	■ auto ■ concatenation ■ phbname	Cisco Map Class Naming Strategy The Frame Relay map class naming strategy: ■ auto (default) - auto generate the name ■ concatenation - creates the map-class name by concatenating the names of all PHB groups (PHB, or MQC, or both) applied to the interface, both inbound and outbound. For example, if two PHB groups called FRTSPHBgroup and MQCOut are applied to an interface, the `map-class` command would be as follows: `map-class frame-relay FRTSPHBGroup-MQCOut` ■ phbname - name the map-class after one of the PHB and MQC PHB groups that contribute to the map-class. Take the name from the following list in the specified order: - PHB group (if it exists) - outbound MQC PHB group (if it exists) - inbound MQC PHB group
cartridge.cisco.qos.mapclass.framerelay.mincir.in.validation	sameAsOut	■ sameAsOut ■ noValidation	Cisco Map Class Frame Relay mincir in validation Defines the type of validation for the Frame Relay mincir in value: ■ sameAsOut (default) - the mincir in value needs to be equal to the mincir out value. ■ noValidation - no validation will be done for the mincir in value.
cartridge.cisco.qos.atmQosOnPvc	vcClass	■ vcClass ■ direct	Cisco ATM QOS on PVC Defines how QOS is provisioned on ATM PVCs: ■ vcClass (default) - use the VC class. ■ direct - provision directly on PVC.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.trafficShapingOnFRInterface	mapClass	■ policyMap ■ mapClass ■ dts	Cisco Traffic Shaping on Frame Relay Interface Defines how traffic shaping is provisioned on Frame Relay interfaces: ■ policyMap - use a policy map. ■ mapClass (default) - use a map class. ■ dts - use distributed traffic shaping (7500 series).
cartridge.cisco.qos.suppressRateLimitAcl	false	■ false ■ true	Cisco Suppress Rate Limit ACL Indicates whether the access group in the `rate-limit` command should be suppressed when no classification is used.
cartridge.cisco.qos.ratePoliceFormat	multiLine	■ multiLine ■ singleLine	Cisco Rate Policing Format Indicates which command format to use: ■ singleLine - use single line format. ■ multiLine (default) - use multiple line format. ■ This option is only applicable for Single-Rate policing
cartridge.cisco.qos.policymap.police.twoRate.lineFormat	multiLine	■ multiLine ■ singleLine	Cisco Two-Rate Policing Format Indicates which command format to use: ■ singleLine - use single line format. ■ multiLine (default) - use multiple line format. ■ This option is only applicable for Two-Rate policing
cartridge.cisco.qos.policymap.police.defaultCBSValue	-1	xs:integer	Cisco Police CBS Default Value for 'Absolute' rate-type Indicates the Committed Burst Size to use when the default check box is checked in the **MQC PHB Group Police** tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the CBS value is not configured when the `police` command is issued. This value is read in case of 'Absolute' rate-type only.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.police.percent.defaultCBSValue	-1	xs:integer	Cisco Police CBS Default Value for 'Percent' rate-type Indicates the Committed Burst Size to use when the default check box is checked in the **MQC PHB Group Police** tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the CBS value is not configured when the `police` command is issued. This value is read in case of 'Percent' rate-type only. The range is 1-2000.
cartridge.cisco.qos.policymap.police.defaultEBSValue	-1	xs:integer	Cisco Police EBS Default Value for'Absolute' rate-type Indicates the Excess Burst Size to use when the default check box is checked in the **MQC PHB Group Police** tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the EBS value is not be configured when the `police` command is issued. This value is read in case of 'Absolute' rate-type only.
cartridge.cisco.qos.policymap.police.percent.defaultEBSValue	-1	xs:integer	Cisco Police EBS Default Value for 'Percent' rate-type Indicates the Excess Burst Size to use when the default check box is checked in the **MQC PHB Group Police** tab. The value must be greater than -1 in order to take effect. If a negative value is specified, the EBS value is not be configured when the `police` command is issued. This value is read in case of 'Percent' rate-type only.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.classmap.dscpMatchEnhanced	false	■ true ■ false	Cisco Class Map Match IP DSCP Enhanced Indicates which command format to use: ■ true: match dscp [IPv4 and IPv6 packets] ■ false: match ip dscp [IPv4 packets only] This option also applies during strict aggregation. This option only applies when an address type of 'IPv4' is selected. For an address type selection of 'IPv6', 'match dscp' will be used. Use of the 'ip' keyword specifies that the match is for IPv4 packets only. The absence of the 'ip' keyword, which is supported on device/IOS combinations supporting IPv6, specifies that the match is on both IPv4 and IPv6 packets.
cartridge.cisco.qos.classmap.precedenceMatchEnhanced	false	■ true ■ false	Cisco Class Map Match IP Precedence Enhanced Indicates which command format to use: ■ true: match precedence [IPv4 and IPv6 packets] ■ false: match ip precedence [IPv4 packets only] This option also applies during strict aggregation. This option only applies when an address type of 'IPv4' is selected. For an address type selection of 'IPv6', 'match dscp' will be used. Use of the 'ip' keyword specifies that the match is for IPv4 packets only. The absence of the 'ip' keyword, which is supported on device/IOS combinations supporting IPv6, specifies that the match is on both IPv4 and IPv6 packets.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.classmap.tosType	object-model	■ object-model ■ dscp ■ precedence	Cisco Class Map TOS Type Indicates the TOS to use when issuing the classmap command of `match [dscp | precedence]`: ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the ClassMap_ DscpMatch setting in the CDD mechanism file. ■ precedence: precedence marking is used. This option is ignored when using strict aggregation.
cartridge.cisco.qos.classmap.existWithEmptyMatchCriteria	true	■ true ■ false	Cisco Class Map Exists with Empty Match Criteria Indicates whether the device allows a class map to exist without any match criteria: ■ true: class maps can exist without any match criteria. ■ false: class maps cannot exist without any match criteria. If the value is set to **false**, you must ensure that a modification to the class map does not result in all of its match criteria being removed. In some cases, you may need to remove the service policy from the interface in order for the operation to be successful.
cartridge.cisco.qos.classmap.isPerPortPerVlanSupported	false	■ true ■ false	Cisco Support for the Per Port Per Vlan Qos Indicates whether the device support the per port per vlan Qos. true: support per port per vlan false: per port per vlan is not supported If the value is set to 'true', special care is taken to ensure that a modification to the class map does not result in interface service policy being removed automatically by the device. In some cases, the service policy may also need to be removed from, and added back to, the interface in order for the operation to succeed.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.classmap.matchany.isSupported	true	■ true ■ false	Cisco Catalyst Switches Support for the Match Any Command Indicates if the `match any` command is supported for class map configurations: ■ true: create the class map with a `match any` statement. ■ false: create the class map without a `match any` statement. Strict aggregation does not change the behavior of this option. Changing this value changes support for `match any` commands.
cartridge.cisco.qos.classmap.match.isAggregateVlanSupported	true	■ true ■ false	Cisco Support for aggregating the Match vlan commands with more than two VLAN IDs. Indicates if the aggregation of match vlan commands with more than two VLAN IDs is supported for class map configurations. ■ true: create the aggregated `match vlan` command with more than two VLAN IDs. ■ false: create the `match vlan` command by distributing `match vlan` commands with maximum two VLAN IDs per `match` statement. Changing this value will change the support for aggregation of `match vlan` commands.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.classmap.matchCosSupport.hardwareList			Cisco Support for MQCPHB "match cos" command. The support for Match Cos command is hardware dependent on some IOS. For example, 12.2SX. On other IOS versions its not. This option will take care of both cases. For hardware dependent supporting devices, list of items will be populated in this option based on entries for hardware types made in option csv file. For hardware independent supporting devices, no item would be populated and existence of the option element would validate the support of Match Cos command. Example: <cartridge.cisco.qos.classmap.matchCosSupport.hardwareList> <base:item>7600-SIP-200</base:item> <base:item>7600-SIP-400</base:item> <base:item>4--VIP2-50--PA-2E3</base:item> </cartridge.cisco.qos.classmap.matchCosSupport.hardwareList> Where <base:item> contains the hardware type which supports the Cos Traffic type (or "match cos" command).
cartridge.cisco.qos.classmap.matchCosInner.isSupported	false	▪ true ▪ false	Indicates whether the "match cos inner" command is supported on the device. true - COS Inner traffic type is supported on the device false(default) - COS Inner traffic type is not supported on the device
cartridge.cisco.qos.policymap.fairqueue.isSupported	true	▪ true ▪ false	Cisco Support for the Fair-Queue Command Indicates if the `fair-queue` command is supported for policy map configurations: ▪ true: create the policy map with a `fair-queue` statement. ▪ false: no ACL reference; `fair-queue` statements are used in the policy map. Changing this value changes support for `fair-queue` commands.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.setDscpEnhanced	false	■ true ■ false	Cisco Policy Map Set IP DSCP Enhanced Indicates which command format to use: ■ true: set dscp [IPv4 and IPv6 packets] ■ false: set ip dscp [IPv4 packets only] ■ To set DSCP values for IPv4 packets only, use the 'ip' keyword. Without the 'ip' keyword, set DSCP values for both IPv4 and IPv6 packets. The absence of the 'ip' keyword is supported on device/IOS combinations supporting IPv6.
cartridge.cisco.qos.policymap.setPrecedenceEnhanced	false	■ true ■ false	Cisco Policy Map Set IP Precedence Enhanced Indicates which command format to use: ■ true: set precedence [IPv4 and IPv6 packets] ■ false: set ip precedence [IPv4 packets only] ■ To set precedence values for IPv4 packets only, use the 'ip' keyword. Without the 'ip' keyword, set precedence values for both IPv4 and IPv6 packets. The absence of the 'ip' keyword is supported on device/IOS combinations supporting IPv6.
cartridge.cisco.qos.policymap.setTosType	object-model	■ object-model ■ dscp ■ precedence	Cisco Policy Map Set TOS Type Indicates which type of packet marking to use in the `policy-map` command: ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the PolicyMap_SetDscp setting in the CDD mechanism file. ■ precedence: precedence marking is used
cartridge.cisco.multicast.distributedSwitching	unsupported	■ unsupported ■ mandatory ■ optional	Cisco Muticast Routing Distributed Keyword Indicates whether multicast distributed switching is mandatory, optional, or not supported on the device.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.defaultWREDType	dscp	■ dscp ■ precedence	Cisco Default WRED Type for Policy Map Indicates which WRED type to use by default in policy map configuration mode: ■ dscp: issues the command `random-detect dscp-based` ■ precedence: issues the command `random-detect precedence`
cartridge.cisco.qos.policymap.wredType	object-model	■ object-model ■ dscp ■ precedence	Cisco WRED Type for Policy Map Indicates which packet marking to use in policymap WRED commands (MQC WRED in IP Service Activator): ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the PolicyMap_DiffservCompliantWred setting in the CDD mechanism file. ■ precedence: precedence marking is used.
cartridge.cisco.qos.policymap.wredRemoveWithType	false	■ true ■ false	Cisco WRED Type Removal Command Variation for Policy Map Indicates which command format to use to remove random-detect [dscp-based | precedence]: ■ true: the `no random-detect` dscp-based or "no random-detect precedence" command will be issued as appropriate ■ false: the `no random-detect` command will be issued without the wred type
cartridge.cisco.qos.phbwfq.dropStrategy.wredType	object-model	■ object-model ■ dscp ■ precedence	Cisco Drop Strategy as WRED for PHB WFQ Indicates which packet marking to use in policymap random detect commands (phb wfq in IP Service Activator): ■ object-model: object model decides packet marking. ■ dscp: uses dscp marking ■ precedence: uses precedence marking

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.phbwfq.dropStrategy.defaultWREDType	dscp	■ dscp ■ precedence	Cisco Drop Strategy as defaultWRED for PHB WFQ Indicates which packet marking to use in policymap random detect commands (phb wfq in IP Service Activator): ■ dscp: issues the command `random-detect dscp-based` ■ precedence: issues the command `random-detect precedence`
cartridge.cisco.qos.policymap.wredDscpGsrBug	false	■ true ■ false	Cisco Generate Extra Random-Detect Command for Dscp Indicates whether to issue an extra `random-detect` command for DSCP based policy maps. This can be used for devices that have problems with the normal `random-detect` command sequence, such as GSRs running IOS 12.0(*)S: ■ true: an extra `random-detect` command is issued - `random-detect` and `random-detect dscp-based` ■ false: the `random-detect dscp-based` command is issued
cartridge.cisco.qos.interface.wredType	object-model	■ object-model ■ dscp ■ precedence	Cisco Interface WRED Type Indicates which packet marking to use in interface WRED commands (PHB WRED in IP Service Activator): ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the Wred_ DiffservCompliantWred setting in the CDD mechanism file. ■ precedence: precedence marking is used.
cartridge.cisco.qos.car.setTosType	object-model	■ object-model ■ dscp ■ precedence	Cisco CAR Set TOS Type Indicates which type of packet marking to set in the `rate limit` command (policing rule in IP Service Activator): ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the Car_SetDiffServ setting in the CDD mechanism file. ■ precedence: precedence marking is used.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.acl.numbered.tosType	object-model	■ object-model ■ dscp ■ precedence	Cisco Numbered ACL TOS Type Indicates which type of packet marking to use in the `numbered ACL` command: ■ object-model: packet marking will be decided by the object model. ■ dscp: dscp marking will be used, similar to the NumberedAcl_Dscp setting in the CDD mechanism file. ■ precedence: precedence marking will be used.
cartridge.cisco.qos.acl.named.tosType	object-model	■ object-model ■ dscp ■ precedence	Cisco Named ACL TOS Type Indicates which type of packet marking to use in the `named ACL` command: ■ object-model: packet marking is dictated by the object model. ■ dscp: dscp marking is used, similar to the NamedAcl_Dscp setting in the CDD mechanism file. ■ precedence: precedence marking is used.
cartridge.cisco.qos.acl.isDscpSupported	true	■ true ■ false	Cisco support for dscp in IPv4 access list Indicates whether dscp is supported in the IPv4 access list.
cartridge.cisco.qos.acl.protocolFor94	nos	■ nos ■ ipinip	Cisco protocol name for protocol no. 94 Indicates whether to send ipinip or nos for protocol 94.
cartridge.cisco.qos.policymap.police.tosType	object-model	■ object-model ■ dscp ■ precedence	Cisco Policy Map Police TOS Type Indicates which type of police action you select for MQC policing: ■ object-model: the police action is decided by the object model. ■ dscp: the *set-dscp-transmit* action is used. ■ precedence: the *set-prec-transmit* action is used.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.police.roundoffCIRValue	false	■ true ■ false	Cisco CIR and PIR (in TR policing) Value is Rounded Up Indicates whether the device rounds the CIR and PIR (in TR policing) value upwards in `police or mls qos aggregate-policer` commands. If the value is set to **true**, the cartridge rounds the CIR value upwards. It uses the 'cartridge.cisco.qos.policymap.police.roundoffCIRFactor' option in order to determine the nearest multiple to round towards.
cartridge.cisco.qos.policymap.police.roundoffCIRFactor	8000	■ 500 ■ 8000	Cisco Multiple Used when Rounding CIR and PIR (in TR policing) Values This value indicates the multiple that the device uses when rounding up CIR and PIR (in TR policing) values in `police or mls qos aggregate-policer` commands. The cartridge rounds the CIR and PIR (in TR policing) value upwards to the nearest multiple of the specified value. The 'cartridge.cisco.qos.policymap.police.roundoffCIRValue' option must be set to **true** in order for this value to take effect.
cartridge.cisco.qos.policymap.police.SRsingleLine.percentAndTimeBasedSyntax.isSupported	false	■ true ■ false	Cisco Support for percentage and time-based syntax on single-rate police Indicates whether the percentage and time based syntax to be followed for single-rate police command in single-line. If this value is set to 'true' along with ratePoliceFormat set to 'singleLine', then syntax for 'percent' rate-type single-rate police will be 'police cir percent percentage [burst-in-msec] [bc conform-burst-in-msec ms] [be peak-burst-in-msec ms] [conform-action action] [exceed-action action [violate-action action]]]'d-action action [violate-action action]]]'

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.police.cisco10000SeriesSyntax.isSupported	false	■ true ■ false	Cisco Support for the Police percentage and time based syntax for 10k series Indicates whether the percentage and time based syntax for 10k series is to be followed for the police command. If this value is set to 'true', then syntax for percent type SR(single-line, depending on percentAndTimeBasedSyntax option value)/TR police will be 'police cir percent percentage [burst-in-msec] [bc conform-burst-in-msec ms] [pir percentage] [be peak-burst-in-msec ms] [conform-action action] [exceed-action action] [violate-action action]'ed-action action] [violate-action action]'
cartridge.cisco.qos.policymap.police.violateAction.isSupported	true	■ true ■ false	Cisco Support for the Police Violate Action Indicates whether the `violate-action` parameter is supported for the `police` command. If this value is set to **false**, then the `violate-action` parameter is not issued.
cartridge.cisco.qos.policymap.police.exceedAction.isSupported	true	■ true ■ false	Cisco Support for the Police Exceed Action Indicates whether the `exceed-action` parameter is supported for the `police` command. If this value is set to **false**, then the `exceed-action` parameter is not issued.
cartridge.cisco.qos.policymap.police.conformAction.isSupported	true	■ true ■ false	Cisco Support for the Police Conform Action Indicates whether the `conform-action` parameter is supported for the `police` command. If this value is set to **false**, then the `conform-action` parameter is not issued.
cartridge.cisco.qos.rateLimitWithMplsAction	set-mpls-exp	■ set-mpls-exp-imposition ■ set-mpls-exp	Cisco Rate Limit MPLS Action Indicates which MPLS Action to use: ■ set-mpls-exp-imposition: use mpls imposition ■ set-mpls-exp (default): use multiple line format

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.sendAllShapeRates	false	■ true ■ false	Cisco Shape Rates Indicates which command format to use: ■ For Average shaping: shape average {cir} or shape average {cir} {cir*4ms} {cir*4ms} eg. shape average 56000 or shape average 56000 224 224 shape average {cir} {bc} or shape average {cir} {bc} {bc} eg. shape average 56000 28000 or shape average 56000 28000 28000 ■ For Peak Shaping: shape peak {cir} or shape peak {cir} {cir*4ms} {cir*4ms} eg. shape peak 16000 or shape peak 16000 64 64 shape peak {cir} {bc} or shape peak {cir} {bc} {bc} eg. shape peak 56000 28000 or shape peak 56000 28000 28000
cartridge.cisco.qos.atmHoldQueue.maximum	1024	4 to 2048	Cisco QOS ATM Hold Queue Depth Maximum Value Defines the maximum value for the ATM Hold Queue Depth. A fault is raised if the ATM Hold Queue Depth is greater than the specified value.
cartridge.cisco.qos.atmHoldQueue.minimum	5	4 to 2048	Cisco QOS ATM Hold Queue Depth Minimum Value Defines the minimum value for the ATM Hold Queue Depth. A fault is raised if the ATM Hold Queue Depth is less than the specified value.
cartridge.cisco.qos.atmPvcVciRange.maximum	1023	0 to 65535	Cisco QOS ATM PVC VCI Maximum Value Defines the maximum value for the ATM PVC VCI. A fault is raised if the ATM PVC VCI is greater than the specified value.
cartridge.cisco.qos.atmPvcVciRange.minimum	0	0 to 65535	Cisco QOS ATM PVC VCI Minimum Value Defines the minimum value for the ATM PVC VCI. A fault is raised if the ATM PVC VCI is less than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.frHoldQueue.maximum	1024	1 to 2048	Cisco QOS FR Hold Queue Depth Maximum Value Defines the maximum value for the Frame Relay Hold Queue Depth. A fault is raised if the Frame Relay Hold Queue Depth is greater than the specified value.
cartridge.cisco.qos.frHoldQueue.minimum	1	1 to 2048	Cisco QOS FR Hold Queue Depth Minimum Value Defines the minimum value for the Frame Relay Hold Queue Depth. A fault is raised if the Frame Relay Hold Queue Depth is less than the specified value.
cartridge.cisco.qos.mlsQos.enable	false	▪ true ▪ false	Cisco Support for the `mls qos` command Indicates whether the `mls qos` command can be used to enable QoS for the device.
cartridge.cisco.qos.policerAggregateSyntax.isSupported	false	▪ true ▪ false	Cisco Support for the `policer aggregate` command syntax Indicates whether the `policer aggregate` command can be used to enable QoS for the device.
cartridge.cisco.qos.aggregatePolicer.commandSyntax	mls_qos_aggregate		Cisco Support for the `named aggregate policer` command syntax Indicates which command syntax to use when defining the aggregate policer. Changing this value will change the command syntax for all aggregate policers.
cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRValue	true	▪ true ▪ false	Cisco CIR Value is Rounded Up Indicates whether the device rounds the CIR value upwards in `rare-limit output/input access-group` commands. If the value is set to **true**, then the cartridge will round the CIR upwards. The cartridge will use the "cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRFactor" option in order to determine the nearest multiple to round towards.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRFactor	8000	■ 500 ■ 8000	Cisco Multiple Used when Rounding CIR Values Indicates the multiple which the device uses when rounding up CIR values in `rate-limit output/input access-group` commands. The cartridge will round the CIR value upwards to the nearest multiple of the specified value. The "cartridge.cisco.qos.policingRule.rateLimit.roundoffCIRValue" option must be set to **true** for this value to take effect.
cartridge.cisco.qos.encapsulateNamesWithQuotes	true	■ true ■ false	Indicates whether the double-quotes supported around classmap,policymap,policer names. If this value is set to 'false', then the names are not encoded in double quotes.
cartridge.cisco.saa.icmpEcho.sourceIpAddress.isSupported	true	■ true ■ false	Cisco Support for the SAA ICMP Echo Operation Source IP Address. Indicates whether the Source IP Address configuration is supported for SAA ICMP Echo operations. A fault is raised if this value is set to **false** and a source IP address is set for an ICMP Echo operation.
cartridge.cisco.saa.tos.isSupported	true	■ true ■ false	Cisco Support for SAA ToS Indicates whether the ToS configuration is supported for SAA operations. A fault is raised if this value is set to **false** and a ToS value is set for an SAA operation.
cartridge.cisco.saa.rtr.schedule.forever.isSupported	true	■ true ■ false	Cisco Support for SAA Rtr-Schedule Lifetime Forever Indicates whether the `life forever` parameter is supported for the `rtr schedule` command. If the value is set to **true**, then the `life forever` parameter is used whenever the lifetime value is set to **Default**. **Note:** The default is **true** for devices with IOS version 12.1 and 12.2. For devices with IOS version 12.0, the default is **false**.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.verifyErrorEnable.isSupported	true	■ true ■ false	Cisco Support for SAA Verify-Error-Enable with Error Checking Indicates whether the `verify-error-enable` parameter is supported for the `rtr reaction-configuration` command. A fault is raised if this value is set to **false** and error checking is enabled. **Note:** The default value is **false** for IOS version 12.0. For IOS version 12.2 the default value is **true**.
cartridge.cisco.saa.tcp.requestDataSize.isSupported	true	■ true ■ false	Cisco Support for SAA TCP Connect Operation Request Data Size Indicates whether the `request-data-size` command is supported for SAA TCP Connect operations. A fault is raised if this value is set to **false** and a request size is set for a TCP Connect operation.
cartridge.cisco.saa.action.nmvt.isSupported	true	■ true ■ false	Cisco Support for SAA Threshold Action-Type Nmvt Indicates whether the *nmvt* threshold action-type is supported for the SAA `rtr reaction-configuration` command. A fault is raised if this value is set to **false** and the action type is set to **nmvt**.
cartridge.cisco.saa.rtr.reactionConfig.multipleMonitorElementsAllowed	false	■ true ■ false	Cisco SAA Rtr Reaction-Configuration Multiple Monitor Elements Allowed Indicates whether multiple monitor parameters are allowed for the SAA `rtr reaction-configuration` command. The monitor elements include the `connection-loss-enable`, `timeout-enable`, and `verify-error-enable` parameters. If the value is set to **true**, then multiple monitor elements are configured in a single `rtr reaction-configuration` command.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.jitter.maxInterval	0	xs:integer	Cisco SAA Jitter Operation Maximum Interval Value Indicates the maximum allowable Jitter interval value. The Jitter interval value is calculated by multiplying the number of packets by the inter-packet interval. A value of **0** means that there is no maximum on the device. A fault is raised if the Jitter interval is greater than the specified value.
cartridge.cisco.saa.removeProbeTwice	false	■ true ■ false	Cisco SAA RTR Probe to be Removed Twice Indicates whether to send the `no rtr {probe-id}` command twice in order to remove the RTR Probe. If the value is set to **true**, then the `no rtr {probe-id}` command is sent twice whenever it is used.
cartridge.cisco.saa.rtr.thresholdType.average.isSupported	true	■ true ■ false	Cisco Support for SAA Threshold-Type Average Indicates whether the `threshold-type average` parameter is supported for the SAA `rtr reaction-configuration` command. A fault is raised if this value is set to **false** and the threshold type is set to **average**.
cartridge.cisco.saa.rtr.thresholdType.consecutive.isSupported	true	■ true ■ false	Cisco Support for SAA Threshold-Type Consecutive Indicates whether the `threshold-type consecutive` parameter is supported for the SAA `rtr reaction-configuration` command. A fault is raised if this value is set to **false** and the threshold type is set to **consecutive**.
cartridge.cisco.saa.rtr.commandSyntax	rtr	■ rtr ■ Ip sla monitor ■ Ip sla	Cisco SAA RTR Command Syntax Indicates which command syntax to use when provisioning SAA RTR configurations. Changing this value will change the command syntax for all future SAA RTR configurations.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.icmpEcho.commandSyntax	type echo protocol ipIcmpEcho	■ type echo protocol ipIcmpEcho ■ icmp-echo	Cisco SAA Icmp Echo Command Syntax Indicates which command syntax to use when provisioning SAA Icmp Echo configurations. Changing this value will change the command syntax for all future SAA Icmp Echo operations.
cartridge.cisco.saa.udpEcho.commandSyntax	type udpEcho	■ type udpEcho ■ udp-echo	Cisco SAA UDP Echo Command Syntax Indicates which command syntax to use when provisioning SAA UDP Echo configurations. Changing this value will change the command syntax for all future SAA UDP Echo operations.
cartridge.cisco.saa.tcpConnect.commandSyntax	type tcpConnect	■ type tcpConnect ■ tcp-connect	Cisco SAA TCP Connect Command Syntax Indicates which command syntax to use when provisioning SAA TCP Connect configurations. Changing this value will change the command syntax for all future SAA TCP Connect operations.
cartridge.cisco.saa.jitter.commandSyntax	type jitter	■ type jitter ■ udp-jitter	Cisco SAA Jitter Command Syntax Indicates which command syntax to use when provisioning SAA Jitter configurations. Changing this value will change the command syntax for all future SAA Jitter operations.
cartridge.cisco.saa.bucketOfHistoryKept.commandSyntax	buckets-of-history-kept	■ buckets-of-history-kept ■ history buckets-kept	Cisco SAA History-Buckets Command Syntax Indicates which command syntax to use when provisioning SAA History-Buckets configurations. Changing this value will change the command syntax for all future SAA History-Buckets operations.
cartridge.cisco.saa.filterForHistory.commandSyntax	filter-for-history	■ filter-for-history ■ history filter	Cisco SAA History-Filter Command Syntax Indicates which command syntax to use when provisioning SAA History-Filter configurations. Changing this value will change the command syntax for all future SAA History-Filter operations.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.livesOfHistoryKept.commandSyntax	lives-of-history-kept	■ lives-of-history-kept ■ history lives-kept	Cisco SAA History-Lives-Kept Command Syntax Indicates which command syntax to use when provisioning SAA History-Lives-Kept configurations. Changing this value will change the command syntax for all future SAA History-Lives-Kept operations.
cartridge.cisco.saa.vrfName.commandSyntax	vrf		Cisco SAA VRF-aware Command Syntax Indicates which command syntax to use when provisioning SAA VRF-aware configurations. Changing this value will change the command syntax for all future SAA VRF-aware operations.
cartridge.cisco.saa.icmpEcho.requestDataSize.minimum	0	0 to 65535	Cisco SAA ICMP Echo Request-Data-Size Minimum Value Indicates the minimum allowable value for the `request-data-size` command in SAA ICMP Echo operations. A fault is raised if the request size is less than the specified value.
cartridge.cisco.saa.icmpEcho.requestDataSize.maximum	65535	0 to 65535	Cisco SAA ICMP Echo Request-Data-Size Maximum Value Indicates the maximum allowable value for the `request-data-size` command in SAA ICMP Echo operations. A fault is raised if the request size is greater than the specified value.
cartridge.cisco.saa.udpEcho.requestDataSize.minimum	4	4 to 8192	Cisco SAA UDP Echo Request-Data-Size Minimum Value Indicates the minimum allowable value for the `request-data-size` command in SAA UDP Echo operations. A fault is raised if the request size is less than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.udpEcho.requestDataSize.maximum	8192	4 to 8192	Cisco SAA UDP Echo Request-Data-Size Maximum value Indicates the maximum allowable value for the `request-data-size` command in SAA UDP Echo operations. A fault is raised if the request size is greater than the specified value. **Note:** Devices with IOS versions 12.0 and 12.2 support maximum value of 1500 as default, whereas devices with IOS versions 12.4 and above support default value of 8192.
cartridge.cisco.saa.tcpConnect.requestDataSize.minimum	0	0 to 65535	Cisco SAA TCP Connect Request-Data-Size Minimum Value Indicates the minimum allowable value for the `request-data-size` command in SAA TCP Connect operations. A fault is raised if the request size is less than the specified value.
cartridge.cisco.saa.tcpConnect.requestDataSize.maximum	65535	0 to 65535	Cisco SAA TCP Connect Request-Data-Size Maximum Value Indicates the maximum allowable value for the `request-data-size` command in SAA TCP Connect operations. A fault is raised if the request size is greater than the specified value.
cartridge.cisco.saa.icmpEcho.frequency.minimum	0	0 to 604800	Cisco SAA ICMP Echo Frequency Minimum Value Indicates the minimum allowable frequency value for SAA ICMP Echo operations. A fault is raised if the period setting is less than the specified value.
cartridge.cisco.saa.icmpEcho.frequency.maximum	604800	0 to 604800	Cisco SAA ICMP Echo Frequency Maximum Value Indicates the maximum allowable frequency value for SAA ICMP Echo operations. A fault is raised if the period setting is greater than the specified value.
cartridge.cisco.saa.udpEcho.frequency.minimum	0	0 to 604800	Cisco SAA UDP Echo Frequency Minimum Value Indicates the minimum allowable frequency value for SAA UDP Echo operations. A fault is raised if the period setting is less than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.udpEcho.frequency.maximum	604800	0 to 604800	Cisco SAA UDP Echo Frequency Maximum Value Indicates the maximum allowable frequency value for SAA UDP Echo operations. A fault is raised if the period setting is greater than the specified value.
cartridge.cisco.saa.tcpConnect.frequency.minimum	0	0 to 604800	Cisco SAA TCP Connect Frequency Minimum Value Indicates the minimum allowable frequency value for SAA TCP Connect operations. A fault is raised if the period setting is less than the specified value.
cartridge.cisco.saa.tcpConnect.frequency.maximum	604800	0 to 604800	Cisco SAA TCP Connect Frequency Maximum Value Indicates the maximum allowable frequency value for SAA TCP Connect operations. A fault is raised if the period setting is greater than the specified value.
cartridge.cisco.saa.jitter.frequency.minimum	0	0 to 604800	Cisco SAA Jitter Frequency Minimum Value Indicates the minimum allowable frequency value for SAA Jitter operations. A fault is raised if the period setting is less than the specified value.
cartridge.cisco.saa.jitter.frequency.maximum	604800	0 to 604800	Cisco SAA Jitter Frequency Maximum Value Indicates the maximum allowable frequency value for SAA Jitter operations. A fault is raised if the period setting is greater than the specified value.
cartridge.cisco.saa.timeout.minimum	0	0 to 604800000	Cisco SAA Timeout Minimum Value Indicates the minimum allowable timeout value for SAA operations. A fault is raised if the timeout setting is less than the specified value. **Note**: The default value is **1** for IOS version 12.0. For 12.4 version the default value is set as **0**.
cartridge.cisco.saa.timeout.maximum	604800000	0 to 604800000	Cisco SAA Timeout Maximum Value Indicates the maximum allowable timeout value for SAA operations. A fault is raised if the timeout setting is greater than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.liveOfHistoryKept.minimum	0	0 to 25	Cisco SAA History-Lives-Kept Minimum Value Indicates the minimum allowable History Lives Kept value for SAA operations. A fault is raised if the lives kept setting is less than the specified value.
cartridge.cisco.saa.liveOfHistoryKept.maximum	2	0 to 25	Cisco SAA History-Lives-Kept Maximum Value Indicates the maximum allowable History Lives Kept value for SAA operations. A fault is raised if the lives kept setting is greater than the specified value.
cartridge.cisco.saa.bucketsOfHistoryKept.minimum	1	1 to 60	Cisco SAA History-Buckets Minimum Value Indicates the minimum allowable History Buckets value for SAA operations. A fault is raised if the history bucket setting is less than the specified value.
cartridge.cisco.saa.bucketsOfHistoryKept.maximum	60	1 to 60	Cisco SAA History-Buckets Maximum Value Indicates the maximum allowable History Buckets value for SAA operations. A fault is raised if the history bucket setting is greater than the specified value.
cartridge.cisco.saa.jitter.numOfPackets.minimum	1	1 to 60000	Cisco SAA Jitter Num-Packets Minimum Value Indicates the minimum allowable number of packets value for SAA Jitter operations. A fault is raised if the *Packets in sequence* setting is less than the specified value.
cartridge.cisco.saa.jitter.numOfPackets.maximum	60000	1 to 60000	Cisco SAA Jitter Num-Packets Maximum Value Indicates the maximum allowable number of packets value for SAA Jitter operations. A fault is raised if the *Packets in sequence* setting is greater than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.jitter.InterpacketInterval.minimum	1	1 to 60000	Cisco SAA Jitter Interpacket-Interval Minimum Value Indicates the minimum allowable interpacket interval value for SAA Jitter operations. A fault is raised if the interpacket interval setting is less than the specified value.
cartridge.cisco.saa.jitter.InterpacketInterval.maximum	60000	1 to 60000	Cisco SAA Jitter Interpacket-interval Maximum Value Indicates the maximum allowable interpacket interval value for SAA Jitter operations. A fault is raised if the interpacket interval setting is greater than the specified value.
cartridge.cisco.saa.tos.hexaDecimalValue	false	■ true ■ false	Cisco SAA Send TOS Value in Hexadecimal Indicates whether the TOS value should be sent in hexadecimal format. If the value is set to **true**, the TOS value is sent in hexadecimal format. If the value is set to **false**, the TOS value is sent in decimal format.
cartridge.cisco.saa.requestDataSize.configureDefault	false	■ true ■ false	Cisco SAA Request Data Size Configure Default Indicates whether the `request-data-size` command should be issued for SAA operations when the request size is set to **Default**. ■ true - the command is issued when the request size is set to **Default**. ■ false - the command is not issued when the request size is set to **Default**. The following request sizes are used when the value is set to **true**: ■ TCP Connect - 1 ■ UDP Echo - 16 ■ ICMP Echo - 28 ■ Jitter - 32

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.thresholdFalling.configureDefault	false	■ true ■ false	Cisco SAA Threshold Falling Configure Default Indicates whether the `threshold-falling` parameter should be issued for SAA operations when the Threshold Falling value is set to **Default**. If this option is set to **true**, the `threshold-falling` value is set to 5000 milliseconds. If this option is set to **false**, the `threshold-falling` parameter is not configured.
cartridge.cisco.saa.reactionConfig.isOldSyntaxSupported	false	■ true ■ false	Cisco SAA Support for Old Syntax for Reaction Configuration Indicates whether the device supports the old syntax for the SAA `reaction-configuration` command. A fault is raised if this value is set **false** and an attempt is made to use the old syntax via the "cartridge.cisco.saa.reactionConfig.useOldSyntax" option.
cartridge.cisco.saa.reactionConfig.useOldSyntax	false	■ true ■ false	Cisco SAA Use the Old Syntax for Reaction Configuration Indicates whether the old syntax should be used when issuing the `reaction-configuration` command for SAA operations. If the value is set to **true**, the old syntax is used for the `reaction-configuration` command.
cartridge.cisco.netflow.secondaryIpPort.isSupported	true	■ true ■ false	Cisco Support for NetFlow Secondary Destination IP Address and Port Indicates whether a secondary destination IP address and port can be set for NetFlow configurations. A fault is raised if this value is set to **false** and an attempt is made to configure a secondary IP address.
cartridge.cisco.netflow.samplingModePacketInterval.isConfigured	false	■ true ■ false	Cisco NetFlow Cache Sampling Mode Configuration Indicates whether the sampling mode should be configured on the device for NetFlow configurations. If this value is set to **true**, the following command is issued as part of the NetFlow configuration: `ip flow-sampling-mode packet-interval 10`

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.netflow.mainCache.cacheEntriesConfiguration.isSupported	true	■ true ■ false	Cisco Support for NetFlow Version Cache Size Indicates whether the device supports cache entries for NetFlow configurations. A fault is raised if this value is set to **false** and the cache value is greater than zero.

cartridge.cisco.netflow.routeCacheSampled.isConfigured	false	■ true
		■ false
			Cisco NetFlow Cache Sampled Mode Configuration
			Indicates whether Sampled NetFlow should be enabled on the interface.
			If the value is set to **true**, the Sampled NetFlow is enabled via the `sampled` parameter:
			`ip route-cache flow sampled`
			If the value is set to **false**, the normal NetFlow is enabled as follows:
			`ip route-cache flow`

cartridge.cisco.netflow.ipFlowAtInterfaceLevel.isSupported	false	■ true ■ false	Cisco NetFlow Configuration Indicates whether ip flow command is supported on a specific device. If the value is set to true, the `ip flow` command is sent instead of `ip route-cache flow`. If the value is set to false, then refer to routeCacheSampled option to determine the correct command.
cartridge.cisco.netflow.inactiveTimeout.immediately.isSupported	false	■ true ■ false	Cisco Support for NetFlow Inactive timeout Immediately Indicates whether inactive flow timeout immedialtely is supported. **Note**: If the value is set to **true** the command `ip flow-cache timeout inactive 0` is configured. Fault is raised for the devices that do not support 0 - Timeout immediately
cartridge.cisco.ppp.multilink.fragment.useDisableFlag	false	■ true ■ false	Cisco Support for PPP Multilink Fragment Disable Indicates if *ppp multilink fragment disable* needs to be sent instead of *no ppp multilink fragmentation*. Changing this value alters the command used to disable ppp multilink fragmentation on the router.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.policeWithMplsAction	SetMplsExpTransmit	■ SetMplsExpTransmit ■ SetMplsExpImpositionTransmit	Cisco Police MPLS Action Indicates which MPLS action to use in the police command when the marking value is less than 8: ■ SetMplsExpTransmit (default) - the `set-mpls-exp-transmit` parameter is used. ■ SetMplsExpImpositionTransmit - the `set-mpls-exp-imposition-transmit` parameter is used.

cartridge.cisco.qos.interface.defaultWREDType	precedence	■ dscp
		■ precedence
			Cisco Default WRED Type for Interface
			Indicates which WRED type to use by default in interface configuration mode.
			■ dscp - the following command is issued:
			`random-detect dscp-based`
			■ precedence - the following command is issued:
			`random-detect`

cartridge.cisco.vpn.vrf.vrfRoutePolicy.suppressExportRouteTargets	false	■ true ■ false	Cisco VRF Route Policy Export Route Target Suppression Indicates whether export route target suppression is enabled: ■ true - suppression is enabled, so any route target values specified in the **VPN Target** field of associated VRF Route Policy configuration policies is suppressed (i.e. the `route-target export` statement is not configured in the VRF for these route targets). ■ false - suppression is not enabled, so all export route targets will be added to the VRF.
cartridge.cisco.vpn.vrf.defaultVrfFormat	ip_vrf	ip_vrf mp_vrf	Cisco VRF Format Indicates the format of the VRF in the case that an IPv4 private address is present in the VRF: ip_vrf: VRF would be in the form `ip_vrf***` mp_vrf: (multiprotocol VRF) VRF would be in the form `vrf definition`

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description

cartridge.cisco.qos.classmap.useAclForMatchAny	false	■ true
		■ false
			Cisco Use ACL Instead of Match Any in Class Map
			Indicates whether an ACL should be used instead of the `match any` statement in the class map for classification groups with the **Match Any** option selected:
			■ true - an ACL is referenced in the class map via the `match access-group` command:
			`class-map match-any map-name match access-group name acl-name`
			■ false - the `match any` statement is used in the class map:
			`class-map match-any map-name match any`
			This option is ignored when using strict aggregation, so the `match any` statement will be used in the class-map.
			This option only applies when the **Match Any** option is selected in the classification group.

cartridge.cisco.qos.classmap.useIPv6AclForMatchAny	false	■ true
		■ false
			Cisco Use IPv6 ACL Instead of Match Any in Class Map
			Indicates whether an ACL should be used instead of the `match any` statement in the class map for classification groups with the **Match Any** option selected:
			■ true - an ACL is referenced in the class map via the `match access-group` command:
			`class-map match-any map-name match access-group name acl-name`
			■ false - the `match any` statement is used in the class map:
			`class-map match-any map-name match any`
			This option is ignored when using strict aggregation, so the `match any` statement will be used in the class-map.
			This option only applies when the **Match Any** option is selected in the classification group.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.interface.suppressNoIPv6Enable	false	■ true ■ false	Specifies whether `no ipv6 enable` command should be issued or not when all the ipv6 addresses which are configured through IP Service Activator are removed. ■ true - `no ipv6 enable` command will be suppressed and not sent to the device. ■ false - `no ipv6 enable` command will be sent to the device. If this value is **false**, then remaining devices support flowcontrol either with send or receive command apart from 2900XL and 3500XL series switches.
cartridge.cisco.qos.classmap.useAclForMatchNotDscp	false	■ true ■ false	Cisco Use ACL Instead of "match not dscp" in Class Map Indicates whether an ACL should be used instead of the "match not dscp" statement in the class map for classification groups with the exclude option selected and the traffic type is dscp marking. true: an ACL will be referenced in the class mpa via the `match access-group` command: class-map match-any map-name match access-group name acl-name false: the `match not dscp` statement will be used in the class map: class-map match-any map-name match not dscp ... The option is ignored when using strict aggregation. This option only applies when the exclude option is selected and the traffic type is dscp marking in the classification.
cartridge.cisco.qos.policymap.queuelimit.lowLimit	1	xs:integer	Cisco QOS Congestion Avoidance Queue Limit Minimum Value Indicates the minimum allowable value for the congestion avoidance queue limit. A fault is raised if the queue limit is less than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.queuelimit.highLimit	8192000	xs:integer	Cisco QOS Congestion Avoidance Queue Limit Maximum Value Indicates the maximum allowable value for the congestion avoidance queue limit. A fault is raised if the queue limit is greater than the specified value.
cartridge.cisco.qos.policymap.llq.defaultCOS	true	■ true ■ false	Cisco LLQ Support for Default Class of Service Indicates whether the LLQ MQC action is supported when using the default class of service. A fault is raised if this value is set to **false** and LLQ is selected as an action for the default class of service.
cartridge.cisco.qos.policymap.llq.defaultWFQ	false	■ true ■ false	Cisco LLQ Support for Default WFQ Indicates whether the LLQ and Default WFQ actions can both be selected in a single MQC PHB group. A fault is raised if this value is set to **false** and both the LLQ and Default WFQ actions are selected.
cartridge.cisco.qos.mapclass.fragment.lowLimit	16	xs:integer	Cisco FRTS FRF.12 Fragment Size Minimum Indicates the minimum allowable value for the FRTS FRF.12 fragment size. A fault is raised if the fragment size is less than the specified value.
cartridge.cisco.qos.frts.concurrentPolicy	allTargets	■ allTargets ■ subOrInterface	Cisco FRTS Concurrent Policy Application Indicates whether an FRTS policy can be applied to different targets concurrently: ■ allTargets (default) - the service policy can be applied to multiple targets. ■ subOrInterface - the service policy can not be applied to multiple targets. A fault is raised if the value is set to **subOrInterface** and an FRTS policy is concurrently applied on a main interface and one of its subinterfaces.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.policymap.congestion.allowedMqcAction	shapingCbwfq	■ shapingCbwfq ■ cbwfq	Cisco Other MQC Actions Allowed with Congestion Indicates which other MQC actions are allowed in conjuction with congestion: ■ shapingCbwfq (default) - shaping and CBWFQ are both allowed when congestion is selected. ■ cbwfq - only CBWFQ is allowed when congestion is selected. A fault is raised if the value is set to **cbwfq** and the Congestion, CBWFQ, and Shape actions are all selected on an MQC PHB group.
cartridge.cisco.qos.interface.frtsCommand	true	■ true ■ false	Cisco Support for the Frame-Relay Traffic-Shaping Command Indicates whether the device supports the `frame-relay traffic-shaping` command on Frame Relay interfaces: ■ true - the `frame-relay traffic-shaping` command is issued. ■ false - the `frame-relay traffic-shaping` command is not issued.
cartridge.cisco.qos.policymap.shaping.basic	true	■ true ■ false	Cisco Support for Default Shaping Indicates whether the device supports default shaping for MQC PHB groups. A fault is raised if this value is set to **false** and default shaping is selected.
cartridge.cisco.qos.policymap.shaping.peak	true	■ true ■ false	Cisco Support for Peak Shaping Indicates whether the device supports peak shaping for MQC PHB groups. A fault is raised if this value is set to **false** and peak shaping is selected.
cartridge.cisco.qos.policymap.shaping.average	true	■ true ■ false	Cisco Support for Average Shaping Indicates whether the device supports average shaping for MQC PHB groups. A fault is raised if this value is set to **false** and average shaping is selected.
cartridge.cisco.qos.policymap.shaping.maxbuffers	true	■ true ■ false	Cisco Support for Shaping Buffers Indicates whether the device supports the shaping buffers setting for MQC PHB groups. A fault is raised if this value is set to **false** and the shaping buffers value is greater than zero.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.mapclass.supportsFrtsHoldQDepth	true	■ true ■ false	Cisco Support for FRTS Hold Queue Depth Indicates whether the device supports the FRTS `frame-relay holdq` command. A fault is raised if this value is set to **false** and the FRTS hold queue depth is greater than zero.
cartridge.cisco.qos.mapclass.deployOnInterface	false	■ true ■ false	Cisco Support for FRF command on interface Indicates if the frame-relay fragmentation should be applied directly to the interface or put in the mapClass. This option should only be used on routers supporting the `frame-relay fragment` command under the interface context.
cartridge.cisco.qos.interface.supportsAtmHoldQDepth	true	■ true ■ false	Cisco Support for ATM Hold Queue Depth Indicates whether the device supports the ATM `vc-hold-queue` command. A fault is raised if this value is set to **false** and the ATM hold queue depth is greater than zero.
cartridge.cisco.vlan.isSwitchportCommandSupported	true	■ true ■ false	Cisco Support for the Switchport Command Indicates whether the device supports the `switchport` command for placing an interface into Layer 2 mode. ■ true - the `switchport` command is used. ■ false - the `switchport mode` command is used.
cartridge.cisco.vlan.isNonegotiateSupported	true	■ true ■ false	Cisco Support for the Switchport No Negotiate Command Indicates whether the device supports the `switchport nonegotiate` command. A fault is raised if this value is set to **false** and the **No Negotiate** value is set for a VLAN interface.
cartridge.cisco.vlan.isQinqSupported	true	■ true ■ false	Cisco Support for 802.1Q Traffic Indicates whether the device supports the `dot1q-tunnel` parameter for the `switchport mode` command. A fault is raised if this value is set to **false** and the qinq VLAN ID is set for a VLAN interface.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description

cartridge.cisco.vlan.defaultEncapsulation	true	■ true
		■ false
			Cisco Default Switchport Trunk Encapsulation
			Indicates whether the default encapsulation should be restored when removing the trunk encapsulation.
			■ true - the following command is issued when removing encapsulation:
			`default switchport trunk encapsulation`
			■ false - the following command is issued when removing the encapsulation:
			`no switchport trunk encapsulation`

cartridge.cisco.vlan.isSwitchportEncapsulationSupported	true	■ true ■ false	Cisco Support for Switchport Trunk Encapsulation Indicates whether the device support the `switchport trunk encapsulation` command. true - the `switchport trunk encapsulation` command is sent if the encapsulation is configured. false - the encapsulation configuration is ignored, no command is sent.
cartridge.cisco.vlan.allowAdditionalVlanIds	false	■ true ■ false	Cisco Configure Additional VLAN IDs Indicates whether VLAN IDs 1 and 1002-1005 should be configured in addition to the IDs specified in the VLAN Interface configuration policy for tagged VLANs. ■ true - VLAN IDs 1 and 1002-1005 are configured in addition to the values you specify. ■ false - only the VLAN ID values you specify are configured.
cartridge.cisco.vlan.accessVlanId.minimum	1	1 to 4094	Cisco Untagged VLAN ID Minimum Value Indicates the minimum allowable VLAN ID value for untagged VLANs. A fault is raised if the VLAN ID is less than the specified value.
cartridge.cisco.vlan.accessVlanId.maximum	4094	1 to 4094	Cisco Untagged VLAN ID Maximum Value Indicates the maximum allowable VLAN ID value for untagged VLANs. A fault is raised if the VLAN ID is greater than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.allowedVlanId.minimum	1	1 to 4094	Cisco Tagged VLAN ID Minimum Value Indicates the minimum allowable VLAN ID value for tagged VLANs. A fault is raised if the VLAN ID is less than the specified value.
cartridge.cisco.vlan.allowedVlanId.maximum	4094	1 to 4094	Cisco Tagged VLAN ID Maximum Value Indicates the maximum allowable VLAN ID value for tagged VLANs. A fault is raised if the VLAN ID is greater than the specified value.
cartridge.cisco.vlan.vlanIds.isDuplicateAllowed	true	■ true ■ false	Cisco Tagged VLAN IDs Validation on Duplicates Indicates if the VLAN ID duplication in VLAN IDs is allowed for tagged VLANs. A fault is raised if the application is not allowed when duplication happens.
cartridge.cisco.vlan.mgmtVlanInterface.validate	false	■ true ■ false	Cisco Management VLAN Interface Validation on missing Indicates if validation is needed for missing mgmtVlanInterface. A fault is raised if the mgmtVlanInterface is missing when this option is set to **true**.
cartridge.cisco.vlan.vlanDefinition.isReduced	false	■ true ■ false	Cisco VLAN Definition Reduction Indicates if VLAN reduction is needed for the vlanDefinition. A fault is raised if this option is **false** and there are duplicate VLAN IDs on one interface.
cartridge.cisco.vlan.mtu.minimum	576	576 to 18190	Cisco VLAN MTU Minimum Value Indicates the minimum allowable VLAN MTU value. A fault is raised if the MTU value is less than the specified value.
cartridge.cisco.vlan.mtu.maximum	18190	576 to 18190	Cisco VLAN MTU Maximum Value Indicates the maximum allowable VLAN MTU value. A fault is raised if the MTU value is greater than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.commandSyntax	vlan	■ vlan ■ vlan database	Cisco VLAN Command Syntax Indicates whether VLANs are provisioned in global configuration mode or in VLAN configuration mode. ■ vlan - provisioning is done in global configuration mode via the `conf t` command. ■ vlan database - provisioning is done in VLAN configuration mode via the `vlan database` command.
cartridge.cisco.vlan.audit.adjacentVlanIdsSeparator	comma	■ comma ■ hyphen	Cisco Consecutive VLAN IDs Separator Indicates which separator to use when configuring two consecutive VLAN IDs. ■ comma - the IDs are separated by a comma: vlan 3,4 ■ hyphen - the IDs are separated by a hyphen: vlan 3-4 This value should be set according to the format displayed by the device so that audits can compare the values correctly. This option is only used when provisioning VLANs in global configuration mode. It is ignored if VLAN configuration mode is being used. For more information, see the description of the option: "cartridge.cisco.vlan.commandSyntax"
cartridge.cisco.vlan.portChars.flowControlSend.isSupported	true	■ true ■ false	Cisco Support for the Flow Control Send Command Indicates whether the device supports the `flowcontrol send` command in interface configuration mode. This command is used when configuring an interface to send pause frames. A fault is raised if this value is set to **false** and the Flow Control Send value is set in the Cisco Ethernet Port Characteristics configuration policy.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.portChars.flowControl.isSupported	true	■ true ■ false	Cisco Support for the Flow Control Command Indicates whether the device supports the `flowcontrol` command in interface configuration mode. A fault is raised if this value is set to **false** and any Flow Control values are set in the Cisco Ethernet Port Characteristics configuration policy.
cartridge.cisco.vlan.portChars.xlflowControl.isSupported	false	■ true ■ false	Cisco 2900XL and 3500XL series switches support flowcontrol symmetric and asymmetric Indicates flowcontrol or flowcontrol asymmetric or flowcontrol symmetric command is accepted on this XL series switches. If this value is **true**, then these XL series switches support flowcontrol with symmetric or asymmetric command. If this value is **false**, then remaining devices support flowcontrol either with send or receive command apart from 2900XL and 3500XL series switches.
cartridge.cisco.vlan.portChars.portStormControl.isSupported	true	■ true ■ false	Cisco Support for the Storm Control Command Indicates whether the device supports the `storm-control` command in interface configuration mode. A fault is raised if this value is set to **false** and the 3500 Storm Control values are set in the Cisco Ethernet Port Characteristics configuration policy.
cartridge.cisco.vlan.portChars.mlsQosTrustType.isSupported	true	■ true ■ false	Cisco Support for the Mls Qos Trust Command Indicates whether the device supports the `mls qos trust` command in interface configuration mode. A fault is raised if this value is set to **false** and the Trust Type value is set in the Cisco Ethernet Port Characteristics configuration policy.
cartridge.cisco.vlan.portChars.stormControlThreshold.isSupported	true	■ true ■ false	Cisco Support for Storm Control Threshold Indicates whether the device supports the `storm-control` command in interface configuration mode. A fault is raised if this value is set to **false** and the Storm Control threshold is set in the Cisco Ethernet Port Characteristics configuration policy.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.portChars.isDuplexDependentOnSpeed	true	▪ true ▪ false	Cisco Dependency Between Duplex and Speed Indicates whether the configuration of the `duplex` command is dependent on the `speed` command being issued beforehand. If this value is set to **true**, then the Speed value in the Cisco Ethernet Port Characteristics configuration policy must be set to any value besides **auto** whenever a Duplex value is set. Otherwise, a fault is raised.
cartridge.cisco.vlan.portChars.spanningTreeRootGuard.isOldSyntaxSupported	false	▪ true ▪ false	Cisco Support for the Old Syntax of the Spanning Tree Guard Configuration Indicates whether the configuration of the spanning-tree guard mode should be done using the old syntax: ▪ true - the old syntax is used: `spanning-tree` *`mode`* `guard` ▪ false - the new syntax is used: `spanning-tree guard` *`mode`*
cartridge.cisco.vlan.portChars.udldEnable	false	▪ true ▪ false	Cisco XL series switches support udld enable Indicates `udld port aggressive` command is accepted as udld enable on this XL series switches. If this value is **true**, then XL series switches support udld enable command. If this value is **false**, then remaining devices support udld port aggressive command apart from XL series switches.
cartridge.cisco.vlan.portChars.srrQueueBandwidthShape.isSupported	false	▪ true ▪ false	Cisco srr-queue bandwidth shape Indicates that through ciscoEthernetPortCharacteristics policy `srr-queue bandwidth shape` command is supported [through SRR queue bandwidth shape] only for Cisco 3750G and Cisco 3750ME switches. The `srr-queue bandwidth shape` commands will be generated only if the value is **true**.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.portChars.mdixAuto.isSupported	false	■ true ■ false	Cisco MDIX-Auto Indicates that through ciscoEthernetPortCharacteristics policy `mdix auto` command is supported [through Auto-MDIX] only for Cisco 3750G switch. The `mdix auto` commands will be generated only if the value is **true**.
cartridge.cisco.vlan.portChars.speed.nonegotiate.isSupported	true	■ true ■ false	Cisco Speed Nonegotiate Support Indicates that through ciscoEthernetPortCharacteristics policy `speed nonegotiate` is supported [through Port Negotiation (GBIC only)] for all devices, except for Cisco 3508G XL and 3512XL with IOS (12.0(5)WC9a). If this value is **false**, then the command will be sent as either *negotiation auto* or *no negotiation auto*.
cartridge.cisco.vlan.portChars.defaultSpeed.isSupported	true	■ true ■ false	Cisco Default Speed Support Indicates that through ciscoEthernetPortCharacteristics policy `default speed` is supported [through Port Negotiation (GBIC only)]. If this value is **false**, the command will be sent as *no speed nonegotiation*.
cartridge.cisco.vlan.portChars.negotiation.isSupported	false	■ true ■ false	Cisco Negotiation Support Indicates that through ciscoEthernetPortCharacteristics policy `negotiation` command is supported [through Port Negotiation (GBIC only)] only for Cisco 3508G XL and 3512XL with IOS (12.0(5)WC9a). If this value is **true**, then the command will be sent as either *negotiation auto* or *no negotiation auto*.
cartridge.cisco.vpn.ospf.spfthrottle.commandSyntax	timers throttle spf	■ timers throttle spf ■ timers spf	Cisco VPN OSPF SPF Throttling Command Syntax Indicates which command syntax to use when provisioning VPN OSPF SPF Throttling configurations. Changing this value will change the command syntax for all future VPN OSPF SPF Throttling configurations.
cartridge.cisco.vpn.ospf.maximumPath.minimum	1	1 to 16	Cisco ospf maximum-path Minimum Value Defines the minimum value for the maximum-path. A fault is raised if the maximum-path is less than the specified value.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vpn.ospf.maximumPath.maximum	16	1 to 16	Cisco ospf maximum-path Maximum Value Defines the maximum value for the maximum-path. A fault is raised if the maximum-path is greater than the specified value.
cartridge.cisco.controller.au4tug3.isSupported	true	■ true ■ false	Cisco StmlChannelizedSerialInterface Policy, controller au-4-tug-3 Support This is deprecated. Please use cartridge.cisco.controller.au4tug3.variant. Indicates that `au-4-tug-3` command is not supported on 3500 and 3600 devices with IOS 12.0 (14) S and 12.2 (15) T. If this value is **true**, `au-4-tug-3` command is supported.
cartridge.cisco.controller.au4tug3.variant	au4default		Cisco Stm1ChannelizedSerialInterface Policy, controller au-4-tug-3 Support Indicates that au-4-tug-3 command is not supported on 3500 and 3600 devices with IOS 12.0(14) S and 12.2(15)T.
cartridge.cisco.interface.chooseDescFromWhenConflictOccurs	default	■ default ■ configPolicy ■ site	Cisco Method for Choosing the Interface Description Specifies which interface description to use when multiple conflicting descriptions are found: ■ default - No conflict detection is performed. This means that the conflicting descriptions may overwrite each other. ■ configPolicy - Use the value specified in the subinterface creation configuration policy. ■ site - Use the value specified in the VPN site.
cartridge.cisco.interface.suppressNoIPv6Enable	false	■ true ■ false	Suppress removal of IPv6 enablement on an Interface Specifies whether `no ipv6 enable` command should be issued or not when all the ipv6 addresses which are configured through IP Service Activator are removed. ■ false - `no ipv6 enable` command will be sent to the device. ■ true - `no ipv6 enable` command will be suppressed and not sent to the device.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.interface.supportMaxReservedBandwidthAtPVC	false		Support for Max Reserved Bandwidth at ATM PVC level Indicates whether to support the `max-reserved-bandwidth` command at ATM PVC.
cartridge.cisco.interface.plSerial.fairQueueSupport	NotSupported		Set Fair Queue Flag on plSerial Interface Indicates whether to support `no fair-queue` on plSerial Interface.
cartridge.cisco.interface.stm1Channelized.fairQueueSupport	NotSupported		Set Fair Queue Flag on stm1Channelized Interface Indicates whether to support `no fair-queue` on stm1Channelized Interface.
cartridge.cisco.interface.e1Channelized.fairQueueSupport	NotSupported		Set Fair Queue Flag on e1Channelized Interface Indicates whether to support `no fair-queue` on e1Channelized Interface.
cartridge.cisco.interface.holdQueueRemoveWithLength	false	■ true ■ false	Cisco hold-queue removal command variation.Indicates which command format to use to remove hold-queue <Queue Length> [in | out] true - the "no hold-queue <Queue Length> [in | out]" command will be issued. false - the "no hold-queue [in | out]" command will be issued.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.global.cddBehavior.isSupported	false		Global option: support CDD behavior Specifies whether CDD behavior is supported with the combination of existing option. This option works in the following scenario currently: 1) acl with precedence codepoint command 2) match dscp/precedence or acl dscp/precedence intelligence false - the commands generated can be different from CDD commands true - the commands generated should be the same as CDD commands when all of the CDD mechanisms match cisco options and there's no NP specific options. 3) QoS reduction false - reduction applies to both user-named and auto-named QoS configurations true - reduction applies to auto-named QoS configurations only, the same as CDD does. Impact: The 'no auto-summary' command is normally issued as part of the address-family command. However, for some routers and IOS combinations, it is not desirable to issue this command, but preserve the preconfigured command, which is 'auto-summary'
cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.hardwareList			Cisco service policy direct reference on frame-relay - Hardware list List of hardware types that require direct service policy reference on frame-relay and do not support frame-relay map-class references. Each list item is a string representing the vendor-specific model name identifier.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList	none	List of strings representing the network module name which is the substring of the Hardware description available on ATM interfaces supporting "queue-depth"(italics) command.For example,NM-1A-T3/E3	List of network modules that require queue-depth(italics) command on ATM PVC targets and do not support tx-ring(italics) command. Each item in the list is a string representing the network module name which is the substring of the Hardware description available on ATM interfaces. For example, the entry in the options file is as follows: <cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList> <base:item>NM-1A-T3/E3</base:item> <base:item>NM-2A-T3/E3</base:item> </cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList>
cartridge.cisco.saa.vrfAware.isSupported	false		Cisco VRF-aware SAA Indicates whether to issue the following command: true - issue the vrf vrfName command false - do not issue the command Impact: The 'vrf vrfName' command is either issued as part of the RTR command or IP SLA. as part of the RTR command or IP SLA.
cartridge.cisco.multicast.ssmMapping.isSupported	false		Cisco Support for Multicast SSM Mapping Indicates whether device supports Multicast SSM Mapping: true - Command for SSM Mapping would be generated if user configures SSM Mapping using multicastDevice configuration policy. false - A fault will be raised if user configures SSM Mapping using multicastDevice configuration policy.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.multicast.msdp.isSupported	true		Cisco Support for MSDP Indicates whether device supports MSDP: true - Command for MSDP would be generated if user configures MSDP using multicastDevice configuration policy. false - A fault will be raised if user configures MSDP using multicastDevice configuration policy.
cartridge.cisco.multicast.msdp.cacheSaState.isSupportedByDefault	true		Cisco Support for MSDP Cache SA State Indicates whether device supports MSDP Cache SA State by default: true - A fault Fault will be raised that 'Cache SA state is supported by default on this device.' false - Command for enabling Cache SA State would be configured to the device.
cartridge.cisco.qos.mqcPhb.cosInnerMarkingSupport.hardwareList			Cisco MQCPHB CosInner Marking Support - Hardware list List of hardware types that supports Cos Inner Marking Each list item is a string representing the vendor-specific model name identifier. Example: <cartridge.cisco.qos.mqcPhb.cosInnerMarkingSupport.hardwareList> <base:item>7600-SIP-200</base:item> <base:item>7600-SIP-400</base:item> <base:item>4--VIP2-50--PA-2E3</base:item> </cartridge.cisco.qos.mqcPhb.cosInnerMarkingSupport.hardwareList> Where <base:item> contains the hardware type which supports the Cos Inner Marking.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.mqcPhb.cosMarkingSupport.hardwareList			Cisco Support for MQCPHB Cos Marking The support for Cos Marking is hardware dependent on some IOS versions (for example, 12.2SX). On other IOS versions its not. This option will take care of both cases. For hardware dependent supporting devices, a list of items would be populated in this option based on entries for hardware types made in an option csv file. For hardware independent supporting devices, no item would be populated and existence of the option element would validate the support of Cos Marking. For hardware dependent supporting devices: <cartridge.cisco.qos.mqcPhb.cosMarkingSupport.hardwareList> <base:item>4--VIP2-50--PA-2CE1/PRI -balanced</base:item> <base:item>7600-SIP-200</base:item> <base:item>7600-SIP-400</base:item> <base:item>4--VIP2-50--PA-2E3</base:item> </cartridge.cisco.qos.mqcPhb.cosMarkingSupport.hardwareList> Where <base:item> contains the hardware type which supports the Cos Marking. For hardware independent supporting devices: <cartridge.cisco.qos.mqcPhb.cosMarkingSupport.hardwareList/> In this case just the presence of this empty option in the option xml file will provision the Cos marking on the device.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.vlan.portChar.disableEnableInterface	false		Cisco IOS Interface Disable and Enable Specify whether the interface is disabled before any ethernet port characteristic changes: true - disable the interface before any ethernet port characteristics changes. If the interface is enabled and any ethernet port characteristics has been changed then disable the interface before the changes and re-enable it. If the interface is disabled and any ethernet port characteristics has been changed then the characteristics changes will be made and interface will remain disabled. false(default) - do not disable the interface before any ethernet port characteristics changes.
cartridge.cisco.qos.frameRelay.servicePolicyDirectReference.useServicePolicyOnMainInterface	false		Cisco service policy used on frame-relay main interface Indicates wheather a map class or a service policy will be used on a main interface: false (default) - a map class will be used on the main interface true -a service policy will be used on the main interface
cartridge.cisco.qos.policymap.defaultWREDWeightFactorConstant	true		Cisco default WRED WeightFactor Constant for Policy Map Indicates whether to configure default WRED WeightFactor constant 9: true - configure default WRED WeightFactor constant 9 false - do not configure default WRED WeightFactor constant 9 Impact: Set this option to false while migrating from Cisco Device Driver to NetworkProcessor Cisco Cartridge. This will prevent NetworkProcessor to configure default WRED WeightFactor constant 9, since the Device Driver does not configure the same.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.routing.allowNoAutoSummary	true		Cisco Routing Allow NoAutoSummary Indicates whether to issue the following command: true - issue the no auto-summary command false - do not issue the command Impact: The 'no auto-summary' command is normally issued as part of the address-family command. However, for some routers and IOS combinations, it is not desirable to issue this command, but preserve the preconfigured command, which is 'auto-summary'.
cartridge.cisco.routing.allowDefaultBgpAddressFamilyVrf	true		Allow default address-family vrf in router bgp configuration mode Indicates whether to allow or suppress the following command when empty: true - allow an address-family vrf command containing only default configuration in router bgp configuration mode false - suppress the address-family vrf command in router bgp configuration mode when it contains only default configuration Impact: The 'address-family vrf' command in router bgp configuration mode is normally issued even if the address-family contains only default commands. However, for some devices and IOS combinations, the device does not show an address-family vrf command configured with only default configuration in router bgp configuration mode.

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.bgpce.ipv4.configurationMode	Router		BGPce config policy IPv4 configuration Indicates whether to issue ipv4 neighbor/network/redistribute commands in router configuration mode or address-family configuration mode: Router - issues commands under "router bgp .." command Address-Family - issues commands under "address-family ipv4" command (which is under "router bgp .." command) Impact: Certain IOS combinations put the ipv4 neighbor/network/redistribute commands by default under "address-family ipv4" configuration mode even though issued under "router bgp..". Audit would fail in such cases. Set the "Address-Family" mode in such case.
cartridge.cisco.qos.device.hqf.isSupported	false		Cisco Hierarchical Queuing Framework support on device Indicates whether HQF is supported on device or not: true - HQF is supported on the device. All the validations (or) the new commands supported on HQF will be enabled (or) available to use. false (default) - HQF is not supported on the device
cartridge.cisco.qos.device.isASR	false		Cisco option specifying ASR device or not Indicates whether the device is ASR device or not: true - Device is ASR. All the validations (or) the new commands supported on ASR devices will be enabled (or) available to use. false (default) - Device is not ASR

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.alias.vrf.allowAliasIpVrf	true		Sends "alias vrf"command in all cases Indicates whether to allow or suppress the following command when empty: true - allow an alias ip vrf command in case the vrf format is IP_VRF. Else alias vrf command is sent. false - The alias vrf command is always sent regardless of VRF format. Impact: Either alias ip vrf or alias vrf is sent based on the VRF format (IP_VRF or MP_VRF respectively) However, for some devices and IOS combinations, the device does not support alias ip vrf command.Instead the alias vrf command should be sent
cartridge.cisco.exec.disableTerminalMonitor	false		Cisco Disable Terminal Monitor Set this option to true to disable debug command output and system error messages for the IPSA terminal session. Impact: true - "terminal no monitor command will be issued before configuring the device false - by default terminal no monitor is not issued
cartridge.cisco.routing.allowNoSynchronization	true		Cisco Routing Allow NoSynchronization Indicates whether to issue the following command: true - issue the no synchronization command false - do not issue the command Impact: The 'no synchronization' command is normally issued as part of "address-family" command. However, for some routers and IOS combinations, it is not desirable to issue this command, but preserve the preconfigured command, which is 'synchronization'.
cartridge.cisco.qos.device.hqf.isSupported	false	■ true ■ false	Cisco Hierarchical Queuing Framework support. Indicates if device supports HQF or not. true - device supports HQF and all the validations of HQF are applicable. false - device does not support HQF

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.qos.device.isASR	false	▪ true ▪ false	Cisco ASR device. Indicates if device is ASR or not. true - device is ASR all the validations of ASR device are applicable. false - device is not ASR
cartridge.cisco.qos.policymap.defaultWREDWeightFactorConstant	false	▪ true ▪ false	Cisco default WRED WeightFactor Constant for Policy Map. Indicates whether to configure default WRED WeightFactor constant 9. true - configure default WRED WeightFactor constant 9 false - do not configure default WRED WeightFactor constant 9
cartridge.cisco.routing.allowDefaultBgpAddressFamilyVrf	true	▪ true ▪ false	Allow default address-family vrf in router bgp configuration mode. Indicates whether to allow or suppress the following command when empty. true - allow an address-family vrf command containing only default configuration in router bgp configuration mode. false - suppress the address-family vrf command in router bgp configuration mode when it contains only default configuration
cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList	None	List of strings representing the network module name which is the substring of the Hardware description available on ATM interfaces supporting queue-depth command. For Example: NM-1A-T3/E3 NM-2A-T3/E3	List of network modules that require queue-depth command on ATM PVC targets and do not support tx-ring command. Each item in the list is a string representing the network module name which is the substring of the Hardware description available on ATM interfaces. For Example: The entry in the options file is as follows: <cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList> <base:item>NM-1A-T3/E3</base:item> <base:item>NM-2A-T3/E3</base:item> </cartridge.cisco.qos.atmPvc.queueDepthSupport.hardwareList>
cartridge.cisco.saa.vrfAware.isSupported	false	▪ true ▪ false	Indicates whether to issue the following command. true - issue the "vrf vrfName" command false - do not issue the command

Table A–1 (Cont.) Configuration Options

Option	Default Value	Possible Values	Description
cartridge.cisco.saa.vrfName.commandSyntax	vrf	■ vrfName ■ vrf	Indicates which command syntax to use when provisioning SAA VRF-aware configurations. Changing this value will change the command syntax for all future SAA VRF-aware operations.
cartridge.cisco.qos.encapsulateNamesWithQuotes	true	■ true ■ false	Indicates whether the IOS supports quotes around the names such as classmap,policymap,and aggregate policer. If the option is set to false, these names will be sent without encoding in quotes, and a validation error will be raised if there are spaces in the names.
cartridge.cisco.vpn.vrf.configureRouteTargetsInVrfContext	true	■ true ■ false	Indicates whether route targets are configured in VRF context, or in both IPv4 and IPv6 address families, when the AddressFamily is set to IPv4+IPv6 in the GUI. true: route targets are configured in VRF context when the AddressFamily is set to IPv4+IPv6 in the GUI false: route targets are configured in both IPv4 and IPv6 address families when the AddressFamily is set to IPv4+IPv6 in the GUI. This option applies only for MP VRF.