Configuring SDM Templates

Information About SDM Templates

You can use SDM templates to configure system resources to optimize support for specific features, depending on how your device is used in the network. You can select a template to provide maximum system usage for some functions.

Cisco Catalyst 9600 Series Switches support the following templates:

- Core
- SDA
- NAT
- Distribution

After you change the template and the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before you enter the **reload** privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

SDM Templates and Switch Stacks

In a switch stack, all stack members must use the same SDM template that is stored on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

You can use the **show switch** privileged EXEC command to see if any stack members are in SDM mismatch mode.

How to Configure SDM Templates

Setting the SDM Template

Follow these steps to use the SDM template to maximize feature usage:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**sdm prefer** { **core** | **nat** | **sda** | **distribution** } **Example:** `Device(config)# sdm prefer nat`	Specifies the SDM template to be used on the switch. The keywords have these meanings: • **core** —Sets the Core template. • **nat** —Maximizes the NAT configuration on the switch. • **sda** —Sets the SDA template. • **distribution** —Sets the Distribution template. **Note** The **no sdm prefer** command and a default template is not supported.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.
Step 5	**reload** **Example:** `Device# reload`	Reloads the operating system. After the system reboots, you can use the **show sdm prefer** privileged EXEC command to verify the new template configuration. If you enter the **show sdm prefer** command before

	Command or Action	Purpose
		you enter the reload privileged EXEC command, the **show sdm prefer** command shows the template currently in use and the template that will become active after a reload.

Monitoring and Maintaining SDM Templates

Command	Purpose
show sdm prefer	Displays the SDM template in use.
reload	Reloads the switch to activate the newly configured SDM template.

Note The SDM templates contain only those commands that are defined as part of the templates. If a template enables another related command that is not defined in the template, then this other command will be visible when the **show running config** command is entered. For example, if the SDM template enables the **switchport voice vlan** command, then the **spanning-tree portfast edge** command may also be enabled (although it is not defined on the SDM template).

If the SDM template is removed, then other such related commands are also removed and have to be reconfigured explicitly.

Configuration Examples for SDM Templates

Examples: Displaying SDM Templates

The following example output shows the core template information:

```
Device# show sdm prefer core
This is the Core template.
  Security Ingress IPv4 Access Control Entries*:       7168  (current) - 7168  (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:   5120  (current) - 5120  (proposed)
  Security Egress IPv4 Access Control Entries*:        7168  (current) - 7168  (proposed)
  Security Egress Non-IPv4 Access Control Entries*:    8192  (current) - 8192  (proposed)
  QoS Ingress IPv4 Access Control Entries*:            5632  (current) - 5632  (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:        2560  (current) - 2560  (proposed)
  QoS Egress IPv4 Access Control Entries*:             6144  (current) - 6144  (proposed)
  QoS Egress Non-IPv4 Access Control Entries*:         2048  (current) - 2048  (proposed)
  Netflow Input Access Control Entries*:               1024  (current) - 1024  (proposed)
  Netflow Output Access Control Entries*:              1024  (current) - 1024  (proposed)
  Flow SPAN Input Access Control Entries*:             512   (current) - 512   (proposed)
  Flow SPAN Output Access Control Entries*:            512   (current) - 512   (proposed)
  Number of VLANs:                                     4094
  Unicast MAC addresses:                               32768
  Overflow Unicast MAC addresses:                      768
  Overflow L2 Multicast entries:                       2304
```

```
  L3 Multicast entries:                              32768
  Overflow L3 Multicast entries:                     768
  Ipv4/Ipv6 shared unicast routes:                   212992
  Overflow shared unicast routes:                    1536
  Policy Based Routing ACEs / NAT ACEs:              3072
  Tunnels:                                           2816
  LISP Instance Mapping Entries:                     512
  Control Plane Entries:                             1024
  Input Netflow flows:                               32768
  Output Netflow flows:                              32768
  SGT/DGT (or) MPLS VPN entries:                     32768
  SGT/DGT (or) MPLS VPN Overflow entries:            768
  Wired clients:                                     2048
  MACSec SPD Entries:                                256
  MPLS L3 VPN VRF:                                   1024
  MPLS Labels:                                       45056
  MPLS L3 VPN Routes VRF Mode:                       209920
  MPLS L3 VPN Routes Prefix Mode:                    32768
  MVPN MDT Tunnels:                                  1024
  L2 VPN EOMPLS Attachment Circuit:                  1024
  MAX VPLS Bridge Domains :                          1000
  MAX VPLS Peers Per Bridge Domain:                  128
  MAX VPLS/VPWS Pseudowires :                        16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cl
```

The following example output shows the NAT template information:

```
Device# show sdm prefer nat
This is the NAT template.
  Security Ingress IPv4 Access Control Entries*:       7168  (current) - 7168  (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:   5120  (current) - 5120  (proposed)
  Security Egress IPv4 Access Control Entries*:        3072  (current) - 3072  (proposed)
  Security Egress Non-IPv4 Access Control Entries*:    5120  (current) - 5120  (proposed)
  QoS Ingress IPv4 Access Control Entries*:            2560  (current) - 2560  (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:        1536  (current) - 1536  (proposed)
  QoS Egress IPv4 Access Control Entries*:             3072  (current) - 3072  (proposed)
  QoS Egress Non-IPv4 Access Control Entries*:         1024  (current) - 1024  (proposed)
  Netflow Input Access Control Entries*:               1024  (current) - 1024  (proposed)
  Netflow Output Access Control Entries*:              1024  (current) - 1024  (proposed)
  Flow SPAN Input Access Control Entries*:             512   (current) - 512   (proposed)
  Flow SPAN Output Access Control Entries*:            512   (current) - 512   (proposed)
  Number of VLANs:                                     4094
  Unicast MAC addresses:                               32768
  Overflow Unicast MAC addresses:                      768
  Overflow L2 Multicast entries:                       2304
  L3 Multicast entries:                                32768
  Overflow L3 Multicast entries:                       768
  Ipv4/Ipv6 shared unicast routes:                     212992
  Overflow shared unicast routes:                      1536
  Policy Based Routing ACEs / NAT ACEs:                15872
  Tunnels:                                             1792
  LISP Instance Mapping Entries:                       1024
  Control Plane Entries:                               1024
  Input Netflow flows:                                 32768
  Output Netflow flows:                                32768
  SGT/DGT (or) MPLS VPN entries:                       32768
  SGT/DGT (or) MPLS VPN Overflow entries:              768
  Wired clients:                                       2048
  MACSec SPD Entries:                                  256
  MPLS L3 VPN VRF:                                     1024
  MPLS Labels:                                         45056
  MPLS L3 VPN Routes VRF Mode:                         209920
  MPLS L3 VPN Routes Prefix Mode:                      32768
  MVPN MDT Tunnels:                                    1024
```

```
  L2 VPN EOMPLS Attachment Circuit:                    1024
  MAX VPLS Bridge Domains :                            1000
  MAX VPLS Peers Per Bridge Domain:                    128
  MAX VPLS/VPWS Pseudowires :                          16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli
```

The following example output shows the SDA template information:

```
Device# show sdm prefer sda
This is the SDA template.
  Security Ingress IPv4 Access Control Entries*:       2048  (current) - 2048  (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:   3072  (current) - 3072  (proposed)
  Security Egress IPv4 Access Control Entries*:        16384 (current) - 16384 (proposed)
  Security Egress Non-IPv4 Access Control Entries*:    6144  (current) - 6144  (proposed)
  QoS Ingress IPv4 Access Control Entries*:            5632  (current) - 5632  (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:        2560  (current) - 2560  (proposed)
  QoS Egress IPv4 Access Control Entries*:             6144  (current) - 6144  (proposed)
  QoS Egress Non-IPv4 Access Control Entries*:         2048  (current) - 2048  (proposed)
  Netflow Input Access Control Entries*:               1024  (current) - 1024  (proposed)
  Netflow Output Access Control Entries*:              1024  (current) - 1024  (proposed)
  Flow SPAN Input Access Control Entries*:             512   (current) - 512   (proposed)
  Flow SPAN Output Access Control Entries*:            512   (current) - 512   (proposed)
  Number of VLANs:                                     4094
  Unicast MAC addresses:                               32768
  Overflow Unicast MAC addresses:                      768
  Overflow L2 Multicast entries:                       2304
  L3 Multicast entries:                                32768
  Overflow L3 Multicast entries:                       768
  Ipv4/Ipv6 shared unicast routes:                     212992
  Overflow shared unicast routes:                      1536
  Policy Based Routing ACEs / NAT ACEs:                2048
  Tunnels:                                             2816
  LISP Instance Mapping Entries:                       2048
  Control Plane Entries:                               1024
  Input Netflow flows:                                 32768
  Output Netflow flows:                                32768
  SGT/DGT (or) MPLS VPN entries:                       32768
  SGT/DGT (or) MPLS VPN Overflow entries:              768
  Wired clients:                                       2048
  MACSec SPD Entries:                                  256
  MPLS L3 VPN VRF:                                     1024
  MPLS Labels:                                         45056
  MPLS L3 VPN Routes VRF Mode:                         209920
  MPLS L3 VPN Routes Prefix Mode:                      32768
  MVPN MDT Tunnels:                                    1024
  L2 VPN EOMPLS Attachment Circuit:                    1024
  MAX VPLS Bridge Domains :                            1000
  MAX VPLS Peers Per Bridge Domain:                    128
  MAX VPLS/VPWS Pseudowires :                          16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli
```

The following example output shows the distribution template information:

```
Device# show sdm prefer distribution
This is the Distribution template.
  Security Ingress IPv4 Access Control Entries*:       7168  (current) - 7168  (proposed)
  Security Ingress Non-IPv4 Access Control Entries*:   5120  (current) - 5120  (proposed)
  Security Egress IPv4 Access Control Entries*:        7168  (current) - 7168  (proposed)
  Security Egress Non-IPv4 Access Control Entries*:    8192  (current) - 8192  (proposed)
  QoS Ingress IPv4 Access Control Entries*:            5632  (current) - 5632  (proposed)
  QoS Ingress Non-IPv4 Access Control Entries*:        2560  (current) - 2560  (proposed)
  QoS Egress IPv4 Access Control Entries*:             6144  (current) - 6144  (proposed)
```

```
  QoS Egress Non-IPv4 Access Control Entries*:         2048  (current) - 2048  (proposed)
  Netflow Input Access Control Entries*:               1024  (current) - 1024  (proposed)
  Netflow Output Access Control Entries*:              1024  (current) - 1024  (proposed)
  Flow SPAN Input Access Control Entries*:             512   (current) - 512   (proposed)
  Flow SPAN Output Access Control Entries*:            512   (current) - 512   (proposed)
  Number of VLANs:                                     4094
  Unicast MAC addresses:                               81920
  Overflow Unicast MAC addresses:                      768
  Overflow L2 Multicast entries:                       2304
  L3 Multicast entries:                                16384
  Overflow L3 Multicast entries:                       768
  Ipv4/Ipv6 shared unicast routes:                     114688
  Overflow shared unicast routes:                      1536
  Policy Based Routing ACEs / NAT ACEs:                3072
  Tunnels:                                             2816
  LISP Instance Mapping Entries:                       1024
  Control Plane Entries:                               1024
  Input Netflow flows:                                 49152
  Output Netflow flows:                                49152
  SGT/DGT (or) MPLS VPN entries:                       32768
  SGT/DGT (or) MPLS VPN Overflow entries:              768
  Wired clients:                                       2048
  MACSec SPD Entries:                                  256
  MPLS L3 VPN VRF:                                     1024
  MPLS Labels:                                         45056
  MPLS L3 VPN Routes VRF Mode:                         112640
  MPLS L3 VPN Routes Prefix Mode:                      32768
  MVPN MDT Tunnels:                                    1024
  L2 VPN EOMPLS Attachment Circuit:                    1024
  MAX VPLS Bridge Domains :                            1000
  MAX VPLS Peers Per Bridge Domain:                    128
  MAX VPLS/VPWS Pseudowires :                          16384
Ipv4/Ipv6 Direct and Indirect unicast routes share same space
* values can be modified by sdm cli
```

Examples: Configuring SDM Templates

```
Device(config)# sdm prefer distribution
Device(config)# exit
Device# reload
  Proceed with reload? [confirm]
```

Additional References for SDM Templates

Related Documents

Related Topic	Document Title
For complete syntax and usage information for the commands used in this chapter.	*Command Reference (Catalyst 9600 Series Switches)*

Feature History for SDM Templates

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature	Feature Information
Cisco IOS XE Gibraltar 16.11.1	SDM Template	Standard SDM templates can be used to configure system resources to optimize support for specific features.

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.