IPv6 Support on Switch Virtual Interface

This document provides an overview of the switch virtual interface (SVI) for Cisco1000 Series and Cisco 4000 Series Integrated Services Routers.

- Information About IPv6 Support on Switch Virtual Interface, on page 1
- Configuration Examples for IPv6 Support on Switch Virtual Interface, on page 5

Information About IPv6 Support on Switch Virtual Interface

Overview of the Switch Virtual Interface

Cisco offers different flavors of integrated switching modules for the modular Cisco 1000 and 4000 Series Integrated Services Routers: the Cisco 4-Port Gigabit Ethernet Switch modules with Next-Generation WAN Interface Cards (NGWIC), 16- and 36-port Cisco EtherSwitch modules, the Cisco EtherSwitch 4-port and 9-port high-speed WAN interface cards (HWICs), the Cisco EtherSwitch service modules, and the Enhanced Cisco EtherSwitch service modules.

The integrated switch ports for the fixed-configuration Integrated Services Routers and the switch ports on the HWICs/NGWICs do not natively support Layer 3 addresses or Layer 3 features. They must be assigned to a SVI and use a VLAN interface for Layer 3 features. SVI represents a logical Layer 3 interface on a switch. In addition to basic routing, SVI can be used to support additional features for the network that the SVI represents.

Cisco IOS Software Features Supported by Switch Virtual Interface

The table lists the Cisco IOS Software features supported by SVI and summarized the typical use of these features. Please refer to the Feature Navigator Tool to check whether a specific platform supports a specific feature.

Table 1: Cisco IOS Software Features Supported by SVI

Cisco IOS Software Feature	SVI Use Scenario	SVI Support Status
Routing Features		

Cisco IOS Software Feature	SVI Use Scenario	SVI Support Status
Routing Protocols	Interconnects Layer 3 networks using protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, and Enhanced Interior Gateway Routing Protocol (EIGRP) configured under SVI	Yes
IP Version 6 (IPv6)	Provides IPv6 support	Yes (Gibraltar 16.12)
Network Address Translation (NAT)	Translates public IP addresses to private address pools, and private addresses to public IP addresses; SVI is typically used as a NAT inside interface	Yes
Dynamic Host Configuration Protocol (DHCP)	• DHCP server feature: Dynamically assigns private IP addresses to devices connected to the switch ports • DHCP client feature: Allows the SVI to receive a dynamically assigned IP address	Yes
Hot Standby Routing Protocol (HSRP)	Supports redundancy and high availability with a secondary device connected to the LAN with SVI, using HSRP	Yes
Virtual Router Redundancy Protocol (VRRP)	Supports redundancy and high availability with a secondary device connected to the LAN with SVI, using VRRP	Yes
Gateway Load Balancing Protocol (GLBP)	Supports redundancy and high availability with a secondary device connected to the LAN with SVI, using GLBP	Yes
Policy-Based Routing (PBR)	Creates policy maps for routing decisions and QoS settings	Yes
Point-to-Point Protocol (PPP) over Ethernet (PPPoE)	Provides PPPoE client support for a device (such as a DSL modem) connected to the switch port; typically used when the SVI is the only interface available to provide backup using the external device	Yes
Multicast	Provides multicast support for clients connected to the switch ports	No
VPN Routing and Forwarding (VRF)	Associates a VRF instance with an SVI to map VLANs to different logical or physical VPN WAN connections	Yes
Layer 2 Tunnel Protocol Version 3 (L2TPv3)	Provides LAN extension between remote sites; SVI is used as the Layer 2 tunnel termination point	Yes (17.2 or later)
Ethernet over MPLS (EoMPLS)	Provides Ethernet extension between remote sites; SVI interface used as the EoMPLS pseudowire attachment circuit	No
Security Features		

Cisco IOS Software Feature	SVI Use Scenario	SVI Support Status
IP Security (IPsec)	• Supports Easy VPN remote as the inside interface • Provides IPsec tunnel termination on the SVI; typically used when SVI is the only interface available to provide backup WAN connection with an external device (such as a DSL modem)	Yes
Generic Routing Encapsulation (GRE)	Provides GRE tunnel termination on the SVI;, typically used when SVI is the only interface available to provide backup WAN connection with an external device (such as a DSL modem)	Yes
Firewall	Provides Firewall support for VLANs	No
Intrusion Prevention System (IPS)	Provides IPS support for VLANs	Yes
IP access control lists (ACLs)	Provides packet filtering to control network traffic and restrict the access of users and devices to the network	Yes
Network Admission Control (NAC)	Enforces NAC of endpoint devices connected to the VLAN	No
Auth-proxy	Authenticates inbound and outbound users connected to the VLAN	No
Quality-of-Service (QoS) Features		
Classification with standard and extended access list	Provides QoS classification with standard and extended access lists	No
Classification with IP type of service (ToS): IP precedence, differentiated services code point (DSCP), or destination address	Provides QoS classification with IP ToS bits	No
Classification with Network-Based Application Recognition (NBAR) with TCP	Provides QoS classification with NBAR TCP traffic	No
Class-based marking	Provides QoS marking based on user-defined traffic class with DSCP and IP precedence values	No
Policing	Limits the input or output transmission rate on SVI and specifies traffic handling policies when the traffic either conforms to or exceeds the specified rate limits	No
Committed Access Rate	Limits the input or output transmission rate on SVI	No
Class-Based Traffic Shaping	Provides Generic Traffic Shaping based on user defined traffic class	No

Cisco IOS Software Feature	SVI Use Scenario	SVI Support Status
Generic-Traffic Shaping	Limits the transmission rate of data to match the speed of the remote, target interface and helps ensure that the traffic conforms to policies contracted for it	No
Weighted Random Early Detection (WRED)	Provides early detection of congestion and differentiated performance characteristics for different classes of service	No
Class-Based Weighted Fair Queue (CBWFQ)	Allocates bandwidth based on user-defined traffic class	No
Low-Latency Queue (LLQ)	Provides strict priority queuing with CBWFQ to allow delay-sensitive data such as voice to be dequeued and sent first, giving delay-sensitive data preferential treatment over other traffic	No
Hierarchical QoS	Using a modular QoS command-line interface (CLI) in a hierarchical structure, provides a high degree of granularity for QoS policies and helps meet complex service-level agreement (SLA) requirements	No
EVC under SVI	-	Yes (16.9.1)
NBAR on SVI	-	Yes (17.2)

Additional Information for IPv6 Support on Switch Virtual Interface

SVI on Cisco Integrated Services Routers is designed to provide basic Layer 3 functions for the Layer 2 switch ports that belong to a specific VLAN. The SVI does not provide the same feature set and functions as the integrated Layer 3 Ethernet ports of the integrated services routers and should not be used to entirely replace the Layer 3 Ethernet ports. Customer who need additional Layer 3 Ethernet ports for their Integrated Services Routers may consider the use of 1- and 2-Port Fast Ethernet High-Speed WIC for modular ISR platforms. The guidelines presented in this document summarize feature support considerations for an Integrated Services Router deployment that uses SVIs.

For more information, please refer to the following links:

• Cisco 4-Port and 8-Port Gigabit Ethernet Switch NIM

• Cisco IOS Security Configuration Guide:
http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_book09186a008049e249.html

• Cisco IOS Quality-of-Service Solutions Configuration Guide:
http://www.cisco.com/en/US/partner/products/ps6441/products_configuration_guide_book09186a008065c7a1.html

Configuration Examples for IPv6 Support on Switch Virtual Interface

Easy VPN Remote and NAT

Easy VPN Remote and NAT

http://www.cisco.com/en/US/technologies/tk583/tk372/technologies_white_paper09186a00801fdef9.shtml

Example: DHCP

```
! SDM Default Configuration
! The default startup configuration file for Cisco Router and Security Device Manager (SDM)
! DO NOT modify this file; it is required by SDM as is for factory defaults
! Version 1.0
!
hostname yourname
!
logging buffered 51200 warnings
!
username cisco privilege 15 secret 0 cisco
!
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool sdm-pool
import all
network 10.10.10.0 255.255.255.248
default-router 10.10.10.1
lease 0 2
!
no ip domain lookup
ip domain-name yourdomain.com
!
interface FastEthernet2
no ip address
no shutdown
!
interface FastEthernet3
no ip address
no shutdown
!
interface FastEthernet4
no ip address
no shutdown
!
interface FastEthernet5
no ip address
no shutdown
!
interface FastEthernet6
no ip address
no shutdown
!
```

```
interface FastEthernet7
no ip address
no shutdown
!
interface FastEthernet8
no ip address
no shutdown
!
interface FastEthernet9
no ip address
no shutdown
!
interface Vlan1
description $ETH-SW-LAUNCH$$INTF-INFO-FE 2$
ip address 10.10.10.1 255.255.255.248
ip tcp adjust-mss 1452
!
ip http server
ip http access-class 23
ip http secure-server
ip http authentication local
ip http timeout-policy idle 60 life 86400 requests 10000
!
access-list 23 permit 10.10.10.0 0.0.0.7
!
banner login ^
----------------------------------------------------------------------
Cisco Router and Security Device Manager (SDM) is installed on this device.
This feature requires the one-time use of the username "cisco" with the password "cisco".
The default username and password have a privilege level of 15.
Please change these publicly known initial credentials using SDM or the IOS CLI.
Here are the Cisco IOS commands.
username <myuser> privilege 15 secret 0 <mypassword>
no username cisco
Replace <myuser> and <mypassword> with the username and password you want to use.
For more information about SDM please follow the instructions in the QUICK START
GUIDE for your router or go to http://www.cisco.com/go/sdm
----------------------------------------------------------------------
^
!
no cdp run
!
!
line con 0
login local
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet
transport input telnet ssh
line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet
transport input telnet ssh
!
! End of SDM default config file
end
```

Example: QoS Marking

```
Current configuration: 2002 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 1841-SVI-DUT
!
boot-start-marker
boot-end-marker
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
class-map match-all non-critical-traffic
match access-group name ACL2
class-map match-all PREC-5
match ip precedence 5
class-map match-all critical-traffic
match access-group name ACL1
class-map match-all DSCP-AF
match dscp af21
!
!
policy-map mark-traffic
class crtical-traffic
set ip dscp cs5
class non-critical-traffic
set ip precedence 2
!
interface FastEthernet0/0
ip address 20.0.0.2 255.255.255.0
speed 100
full-duplex
!
interface FastEthernet0/1
ip address 202.82.33.153 255.255.255.252
shutdown
duplex auto
speed auto
!
interface FastEthernet0/0/0
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
duplex full
speed 100
!
interface Vlan1
```

```
ip address 10.0.0.2 255.255.255.0
service-policy input mark-traffic
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip http server
no ip http secure-server
!
ip access-list standard ACL
ip access-list standard ACL1
permit 10.0.0.100
!
ip access-list extended ACL2
permit ip host 10.0.0.1 host 20.0.200.1
!
control-plane
!
line con 0
exec-timeout 0 0
privilege level 15
line aux 0
line vty 0 4
exec-timeout 0 0
login
!
scheduler allocate 20000 1000
end
```

Example: PBR

```
interface FastEthernet0/0/0
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
duplex full
speed 100
!
interface Vlan1
ip address 10.0.0.2 255.255.255.0
ip policy route-map PBR
!
route-map PBR permit 10
match ip address ACL2
set ip precedence critical
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.0.0.1
!
ip http server
no ip http secure-server
!
ip access-list standard ACL
ip access-list standard ACL1
permit 10.0.0.100
!
ip access-list extended ACL2
permit ip host 10.0.0.1 host 20.0.200.1
```

```
!
control-plane
!
```

Example: PBR