

Cisco ISR4000 Series Integrated Services Routers Bridge Domain Configuration Guide

Contents

[Introduction](#)

[Components Used](#)

[Restrictions for Bridge Domain Interfaces](#)

[Summary Steps](#)

[Detailed Steps](#)

[Network Diagram](#)

[Configurations](#)

[Assigning a MAC Address](#)

[Verifying Bridge Domain Interface Configuration](#)

[DETAILED STEPS](#)

[Technical Assistance](#)

Introduction

A bridge domain must include a set of logical interfaces that participate in Layer 2 learning and forwarding. You can optionally configure a VLAN identifier and a routing interface for the bridge domain to also support Layer 3 IP routing.

The Cisco ISR 4000 Series Integrated Services Routers support the bridge domain interface (BDI) feature for packaging Layer 2 Ethernet segments into Layer 3 IP.

Bridge domain interface supports the following features:

- IP termination
- Layer 3 VPN termination
- Address Resolution Protocol (ARP), G-ARP, and P-ARP handling
- MAC address assignment

Prior to configuring a bridge domain interface, you must understand the following concepts:

- Ethernet Virtual Circuit Overview
- Bridge Domain Interface Encapsulation
- Assigning a MAC Address
- Support for IP Protocols
- Support for IP Forwarding
- Packet Forwarding
- Bridge Domain Interface Statistics

Components Used

The information in this document is based on ISR 4000 router

Restrictions for Bridge Domain Interfaces

The following are the restrictions pertaining to bridge domain interfaces:

Only 4096 bridge domain interfaces are supported per system.

For a bridge domain interface, the maximum transmission unit (MTU) size can be configured between 1500 and 9216 bytes. Bridge domain interfaces support only the following features:

- IPv4 Multicast
- QoS marking and policing. Shaping and queuing are not supported
- IPv4 VRF
- IPv6 unicast forwarding
- Dynamic routing such as BGP, OSPF, EIGRP, RIP, ISIS, and STATIC
- Hot Standby Router Protocol (HSRP) from IOS XE 3.8.0 onwards.
- Virtual Router Redundancy Protocol (VRRP) from IOS XE 3.8.0 onwards.
- Bridge domain interfaces do not support the following features:
- PPP over Ethernet (PPPoE)
- Bidirectional Forwarding Detection (BFD) protocol
- Netflow
- QoS
- Network-Based Application Recognition (NBAR) or Advanced Video Coding (AVC)
- MPLS TE built over BDI interface is not supported and Blackholed.

Summary Steps

1. enable
2. configure terminal
3. interface BDI interface number
4. encapsulation encapsulation dot1q <first-tag> [second-dot1q <second-tag>]
5. Do one of the following:
 - ip address ip-address mask
 - ipv6 address { X:X:X:X link-local | X:X:X:X / prefix [anycast | eui-64] | autoconfig [default] }
6. mac-address { mac-address }
7. no shut
8. interface GigabitEthernet interface number
9. no ip address
10. service instance [number] ethernet
11. encapsulation dot1q <first-tag>
12. bridge-domain <number>

Detailed Steps

	Command or Action	Purpose
Step 1	configure terminal Router# configure terminal	Enters global configuration mode.
Step 2	interface BDI {interface number} Router(config-if)# interface BDI3	Specifies a bridge domain interface on a Cisco IOS Series Integrated Services Router.
Step 3	encapsulation encapsulation dot1q <first-tag> [second-dot1q <second-tag>] Router(config-if)# encapsulation dot1Q 1 second-dot1q 2	Defines the encapsulation type. The example shows how to define dot1q as the encapsulation type.
Step 4	Do one of the following: ip address ip-address mask ipv6 address {X:X:X:X link-local X:X:X:X/prefix [anycast / eui-64] / autoconfig [default] } Router(config-if)# ip address 100.1.1.1 255.255.255.0 Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64	Specifies either the IPv4 or IPv6 address for the bridge domain interface.

Step 6

match security-group destination tag *sgt-number*
Router(config-route-map)# match security-group destination tag 150

Configures the value for security-group destination security tag.

Step 6

mac address {*mac-address*}
Router(config-if)# mac-address 1.1.1

Specifies the MAC address for the bridge domain interface.

Step 7

no shut
Router(config-if)# no shut

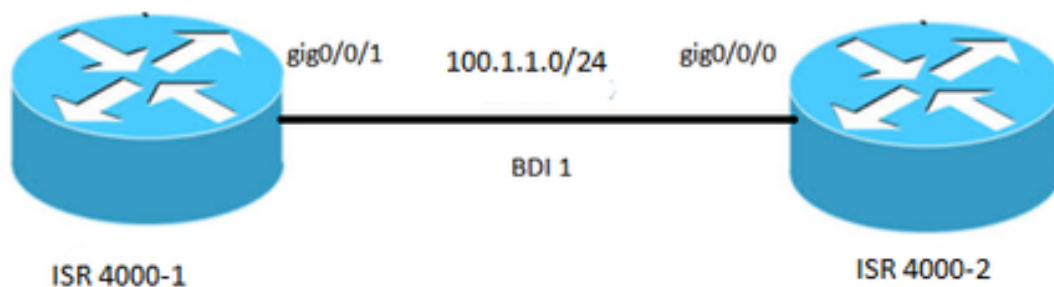
Enables the bridge domain interface.

Step 8

shut
Router(config-if)# shut

Disables the bridge domain interface on the Cisco 4000 Series Integrated Services Router.

Network Diagram



Configurations

ISR 4000-1

```
interface BDI1
mac-address 0001.0001.0001
ip address 100.1.1.1 255.255.255.0
encapsulation dot1Q 100
end
!
interface GigabitEthernet0/0/1
no ip address
negotiation auto
service instance 100 ethernet
encapsulation dot1q 100
bridge-domain 1
no shut
!
```

ISR 4000-2

```
interface BDI1
mac-address 0002.0002.0002
ip address 100.1.1.2 255.255.255.0
encapsulation dot1Q 100
end
!
interface GigabitEthernet0/0/0
no ip address
negotiation auto
service instance 100 ethernet
encapsulation dot1q 100
bridge-domain 1
no shut
!
```

Assigning a MAC Address

All the bridge domain interfaces on the Cisco ISR 4000 chassis share a common MAC address. The first bridge domain interface on a bridge domain is allocated a MAC address. Thereafter, the same MAC address is assigned to all the bridge domain interfaces that are created in that bridge domain.

Verifying Bridge Domain Interface Configuration

DETAILED STEPS

Step 1 show interfaces bdi

Displays the configuration summary of the corresponding BDI.

```
Router# showlik interfaces bdi 1
BDI1 is up, line protocol is up
Hardware is BDI, address is 0001.0001.0001 (bia 00c8.8bee.5993)
Internet address is 100.1.1.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation 802.1Q VLAN, Vlan ID 100, loopback not set
Keepalive not supported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:06:07, output 00:00:50, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
30 packets input, 3366 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
87 packets output, 22568 bytes, 0 underruns
0 output errors, 0 interface resets
0 unknown protocol drops
0 output buffer failures, 0 output buffers swapped out
```

Step 2 show platform software interface fp active name

Displays the bridge domain interface configuration in a Forwarding Processor.

```
Router# show platform software interface fp active name bdi 1
```

```
Name: BDI1, ID: 8, QFP ID: 9, Schedules: 4096
Type: BDI, State: enabled, SNMP ID: 4, MTU: 1500
IP Address: 100.1.1.1
IPv6 Address: ::
Flags: ipv4
ICMP Flags: unreachable, no-redirects, no-info-reply, no-mask-reply
ICMP6 Flags: unreachable, no-redirects
SMI enabled on protocol(s): UNKNOWN
Authenticated-user:
FRR linkdown ID: 65535
Bridge-domain ID: 1
BDI FLAG: 0
vNet Name: , vNet Tag: 0, vNet Extra Information: 0
Dirty: unknown
AOM dependency sanity check: PASS //signifies that the BDI hardware programming is correct.
AOM Obj ID: 109
```

Step 3 show platform hardware qfp active interface if-name

Displays the bridge domain interface configuration in a data path.

```
Router# show platform hardware qfp active interface if-name BDI1
```

```
General interface information
Interface Name: BDI1
Interface state: VALID
Platform interface handle: 8
QFP interface handle: 9
Rx uidb: 32761
Tx uidb: 32759
Channel: 0
Interface Relationships
```

```
BGPPA/QPPB interface configuration information
Ingress: BGPPA/QPPB not configured. flags: 0000
Egress : BGPPA not configured. flags: 0000
```

```
ipv4_input enabled.
ipv4_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.
```

Features Bound to Interface:

```
2 GIC FIA state
65 PUNT INJECT DB
69 cpp_l2bd_svr
41 icmp_svr
43 ipfrag_svr
44 ipreass_svr
Protocol 0 - ipv4_input
FIA handle - CP:0x56432e2146c0 DP:0xead8fc80
IPV4_INPUT_DST_LOOKUP_ISSUE (M)
IPV4_INPUT_ARL_SANITY (M)
IPV4_INPUT_DST_LOOKUP_CONSUME (M)
IPV4_INPUT_FOR_US_MARTIAN (M)
IPV4_INPUT_LOOKUP_PROCESS (M)
IPV4_INPUT_IPOPTIONS_PROCESS (M)
IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x56432e213fb8 DP:0xead9d100
IPV4_VFR_REFRAG (M)
IPV4_OUTPUT_L2_REWRITE (M)
IPV4_OUTPUT_FRAG (M)
BDI_VLAN_TAG_ATTACH
BDI_LAYER2_LOOKUP_GOTO
LAYER2_BRIDGE
BDI_OUTPUT_GOTO_OUTPUT_FEATURE
IPV4_OUTPUT_DROP_POLICY (M)
DEF_IF_DROP_FIA (M)
Protocol 8 - layer2_input
FIA handle - CP:0x56432e214d80 DP:0xead83080
LAYER2_INPUT_SIA (M)
LAYER2_INPUT_LOOKUP_PROCESS (M)
LAYER2_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 9 - layer2_output
FIA handle - CP:0x56432e214000 DP:0xead9c880
BDI_VLAN_TAG_ATTACH
BDI_LAYER2_LOOKUP_GOTO
LAYER2_BRIDGE
BDI_OUTPUT_GOTO_OUTPUT_FEATURE
LAYER2_OUTPUT_DROP_POLICY (M)
DEF_IF_DROP_FIA (M)
Protocol 14 - ess_ac_input
FIA handle - CP:0x56432e2140d8 DP:0xead9af00
PPPOE_GET_SESSION
ESS_ENTER_SWITCHING
PPPOE_HANDLE_UNCLASSIFIED_SESSION
DEF_IF_DROP_FIA (M)
```

Step 4 debug platform hardware qfp feature

```
Router# debug platform hardware qfp active feature l2bd client all
```

The selected CPP L2BD Client debugging is on.

Step 5 platform trace runtime process forwarding-manager module

Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Forwarding Manager process.

```
Router(config)# platform trace runtime slot F0 bay 0 process forwarding-manager module interfaces level info
```

Step 6 platform trace boottime process forwarding-manager module interfaces

Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Route Processor Forwarding Manager process during bootup.

```
Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max
```

Technical Assistance

Description

The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.

Link

<http://www.cisco.com>