

# Contents

Introduction .....	1
Prerequisites .....	1
Example: Configuring link layer attack protection .....	2
Network configuration .....	2
Analysis .....	3
Applicable hardware and software versions.....	3
Restrictions and guidelines .....	5
Procedures .....	5
Configuring Device B .....	5
Configuring Device A .....	5
Configuring Device C .....	6
Verifying the configuration .....	6
Configuration files .....	7
Example: Configuring ARP attack protection .....	8
Network configuration .....	8
Applicable hardware and software versions.....	9
Procedures .....	11
Verifying the configuration .....	11
Configuration files .....	12
Example: Configuring network layer attack protection .....	12
Network configuration .....	12
Applicable hardware and software versions.....	12
Restrictions and guidelines .....	14
Procedures .....	15
Verifying the configuration .....	15
Configuration files .....	15
Example: Configuring transport layer attack protection .....	16
Network configuration .....	16
Applicable hardware and software versions.....	16
Procedures .....	17
Verifying the configuration .....	17
Configuration files .....	18

# Introduction

This document provides configuration examples of link layer attack protection, ARP attack protection, network layer attack protection, and transport layer attack protection, as defined in [Table 1](#).

**Table 1 Attack protection types**

Attack protection types		Description
Link layer attack protection	MAC address attack protection	Prevents the attack of packets with different source MAC addresses or VLANs by configuring the maximum number of MAC addresses that an interface can learn.
	STP packet attack protection	Provides protection measures such as BPDU guard, root guard, loop guard, and TC-BPDU guard.
ARP attack protection	ARP source suppression	Prevents IP attack packets from fixed sources.
	ARP black hole routing	Prevents IP attack packets from sources that are not fixed.
	ARP active acknowledgement	Prevents user spoofing.
	Source MAC-based ARP attack detection	Prevents ARP packet attacks from the same source MAC.
	ARP packet source MAC consistency check	Prevents attacks from ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.
Network layer attack protection	uRPF check	Protects a network against source spoofing attacks.
	TTL attack protection	Prevents an attack by disabling sending ICMP time exceeded messages.
Transport layer attack protection	SYN flood attack protection	Enables the server to return a SYN ACK message when it receives a TCP connection request, without establishing a half-open TCP connection.

## Prerequisites

The configuration examples in this document were created and verified in a lab environment, and all the devices were started with the factory default configuration. When you are working on a live network, make sure you understand the potential impact of every command on your network.

This document assumes that you have basic knowledge of attack protection.

# Example: Configuring link layer attack protection

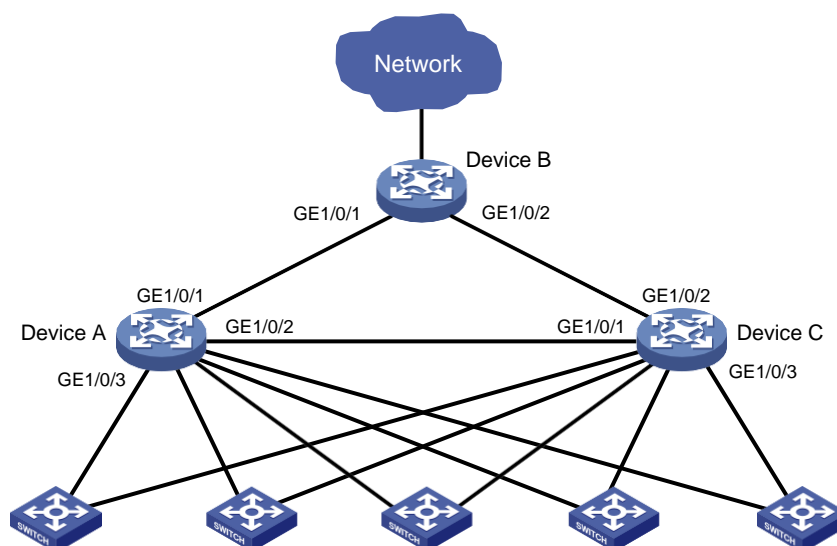
## Network configuration

As shown in Figure 1, Device A, Device B, and Device C run MSTP. Device B acts as the root bridge, and GigabitEthernet 1/0/1 on Device C is blocked.

Configure the following features to prevent link layer attacks:

- Configure root guard on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 of Device B for Device B to act as the root bridge.
- Configure loop guard on GigabitEthernet 1/0/2 of Device C to prevent temporary loops. The loop guard feature keeps the port in **Discarding** state in all MSTIs when it receives noBPDU.
- Configure BPDU guard on ports at the access side of Device A and Device C. The BPDU guard feature prevents the ports from performing spanning tree calculations when it receives forged BPDUs with a higher priority.
- Enable TC-BPDU guard on Device A, Device B, and Device C. The TC-BPDU guard feature prevents a large number of TC-BPDUs from affecting the network in a short time.
- Set the maximum number of MAC addresses that can be learned by ports at the access side of Device A and Device C. This configuration protects the devices from a large number of attack packets that have different source MAC addresses. The attack packets might cause a large MAC table and low forwarding performance.
- Configure broadcast and multicast suppression on the designated ports of Device B and all ports on Device A and Device C. When incoming broadcast or multicast traffic exceeds the threshold (6400 pps), an interface discards broadcast or multicast packets until the traffic drops below the threshold.

Figure 1 Network diagram



# Analysis

For the ports at the access side of Device A and Device C to rapidly transit to the forwarding state, use the **stp edged-port** command to configure these ports as edge ports.

This example uses GigabitEthernet 1/0/3 to illustrate the configuration on the ports at the access side on Device A and Device C.

## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Restrictions and guidelines

When you configure link layer attack protection, follow these restrictions and guidelines:

- On a port, the loop guard feature is mutually exclusive with the root guard feature or the edge port setting.
- Do not configure the loop guard feature on ports at the access side. Otherwise, the ports stay in **Discarding** state in all MSTIs because they cannot receive BPDUs.

## Procedures

### Configuring Device B

# Specify IP addresses for interfaces. (Details not shown.)

# Configure root guard on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
<DeviceB> system-view
```

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

```
[DeviceB-if-range] stp root-protection
```

```
[DeviceB-if-range] quit
```

# Configure TC-BPDU guard.

```
[DeviceB] stp tc-protection
```

```
[DeviceB] stp tc-protection threshold 10
```

# Configure broadcast and multicast suppression on GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2.

```
[DeviceB] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

```
[DeviceB-if-range] broadcast-suppression pps 6400
```

```
[DeviceB-if-range] multicast-suppression pps 6400
```

```
[DeviceB-if-range] quit
```

## Configuring Device A

**# Specify IP addresses for interfaces. (Details not shown.)**

**# Configure STP BPDU guard.**

```
<DeviceA> system-view
```

```
[DeviceA] stp bpdu-protection
```

**# Configure GigabitEthernet 1/0/3 as an edge port.**

```
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] stp edged-port
```

```
[DeviceA-GigabitEthernet1/0/3] quit
```

**# Configure TC-BPDU guard.**

```
[DeviceA] stp tc-protection
```

```
[DeviceA] stp tc-protection threshold 10
```

**# Set the maximum number of MAC addresses that GigabitEthernet 1/0/3 can learn.**

```
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] mac-address max-mac-count 1024
```

```
[DeviceA-GigabitEthernet1/0/3] quit
```

**# Configure broadcast and multicast suppression on all ports.**

```
[DeviceA] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
```

```
[DeviceA-if-range] broadcast-suppression pps 6400
```

```
[DeviceA-if-range] multicast-suppression pps 6400
```

```
[DeviceA-if-range] quit
```

## Configuring Device C

```
# Specify IP addresses for interfaces. (Details not shown.)
# Configure STP BPDU guard.
<DeviceC> system-view
[DeviceC] stp bpdu-protection

# Configure GigabitEthernet 1/0/3 as an edge port.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] stp edged-port
[DeviceC-GigabitEthernet1/0/3] quit

# Configure loop guard on GigabitEthernet 1/0/2.
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] stp loop-protection
[DeviceC-GigabitEthernet1/0/2] quit

# Configure TC-BPDU guard.
[DeviceC] stp tc-protection
[DeviceC] stp tc-protection threshold 10

# Set the maximum number of MAC addresses that GigabitEthernet 1/0/3 can learn.
[DeviceC] interface gigabitethernet 1/0/3
[DeviceC-GigabitEthernet1/0/3] mac-address max-mac-count 1024
[DeviceC-GigabitEthernet1/0/3] quit

# Configure broadcast and multicast suppression on all ports.
[DeviceC] interface range gigabitethernet 1/0/1 to gigabitethernet 1/0/3
[DeviceC-if-range] broadcast-suppression pps 6400
[DeviceC-if-range] multicast-suppression pps 6400
[DeviceC-if-range] quit
```

## Verifying the configuration

```
# Verify that the edge ports go down after they receives STP BPDUs. (Details not shown.)
# Bring the edge ports up by using the undo shutdown command. (Details not shown.)
# Verify that the bridge ID of Device B does not change and that the STP topology remains stable
after STP BPDUs with higher priority are sent to Device B. (Details not shown.)
```

# Verify that the devices do not refresh the FIB table frequently and that no serious packet loss occurs after a large number of TC BPDUs are sent to the devices. (Details not shown.)

# Verify that the uplink ports are not flooded after a large number of broadcasts are sent to the edge ports on device A and Device C. (Details not shown.)

## Configuration files



### IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

- Device A:

```
#
stp bpdu-protection
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
port link-mode bridge
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
port link-mode bridge
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/3
port link-mode bridge
mac-address max-mac-count 1024
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
```

- Device B:

```
#
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
port link-mode bridge
stp root-protection
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
port link-mode bridge
stp root-protection
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
```

- Device C:

```
#
stp bpdu-protection
stp tc-protection threshold 10
#
interface GigabitEthernet 1/0/1
port link-mode bridge
stp root-protection
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/2
port link-mode bridge
stp loop-protection
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
interface GigabitEthernet 1/0/3
port link-mode bridge
stp edged-port
mac-address max-mac-count 1024
broadcast-suppression pps 6400
multicast-suppression pps 6400
#
```

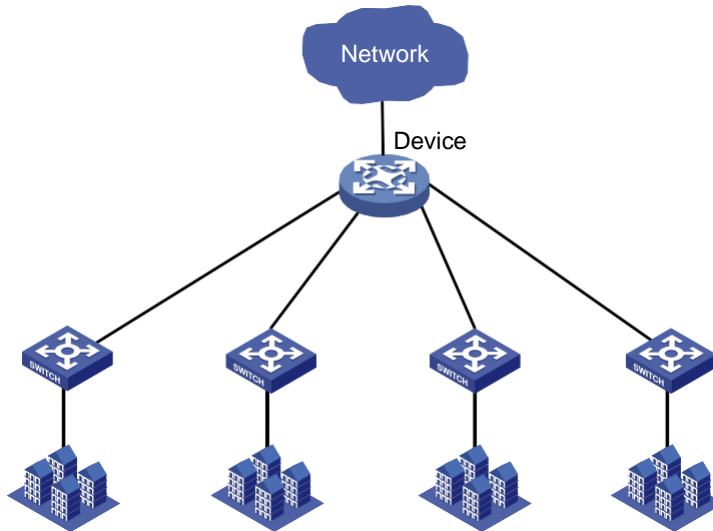
## Example: Configuring ARP attack protection

### Network configuration

As shown in [Figure 2](#), the device is the gateway for the internal network. Configure ARP attack protection on the device to prevent ARP attacks.



**Figure 2 Network diagram**



## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Procedures

# Specify IP addresses for interfaces. (Details not shown.)

# Enable ARP source suppression.

```
<Device> system-view
[Device] arp source-suppression enable
```

# Configure the device to accept a maximum of 8 unresolvable packets per source IP address in 5 seconds.

```
[Device] arp source-suppression limit 8
```

# Enable ARP black hole routing to prevent unresolvable IP packet attacks.

```
[Device] arp resolving-route enable
```

# Enable ARP active acknowledgment to prevent user spoofing.

```
[Device] arp active-ack enable
```

# Configure source MAC-based ARP attack detection to prevent ARP packet attacks from the same source MAC.

```
[Device] arp source-mac filter
[Device] arp source-mac threshold 25
```

```
# Enable ARP packet source MAC address consistency check to prevent attacks from ARP packets
with different source MAC addresses in the Ethernet header and in the message body.
```

```
[Device] arp valid-check enable
```

## Verifying the configuration

1. Verify that ARP attack protection functions on the device:
  - # Send ARP attack packets to the device. (Details not shown.)
  - # Verify that the CPU usage does not surge. (Details not shown.)
2. Verify that each ARP attack protection feature functions on the device (this example uses the ARP source suppression feature):
  - # Send the device 20 forged packets with the same source IP address and unresolvable destination IP addresses. (Details not shown.)
  - # Verify that the device stops resolving the packets after receiving 8 forged packets within 5 seconds. (Details not shown.)
  - # Verify the ARP source suppression configuration.

```
[Device] display arp source-suppression
```

```
ARP source suppression is enabled
```

```
Current suppression limit: 8
```

```
Current cache length: 16
```

## Configuration files

---

### ❗ IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

---

```
#
arp valid-check enable
arp source-mac filter
arp source-mac threshold 25
arp active-ack enable
arp source-suppression enable
arp source-suppression limit 8
#
```

# Example: Configuring network layer attack protection

## Network configuration

As shown in [Figure 3](#), Device A is the gateway for the internal network. To protect Device A against IP packet attacks from internal and external networks, configure the following network layer attack protection features:

- Configure strict uRPF check to prevent source address spoofing attacks.
- Disabling sending ICMP time exceeded messages. The device will not be flooded by ICMP time exceeded messages when receiving a large number of packets with TTL set to 1.

**Figure 3 Network diagram**



## Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 3570 switch series	Release 11xx
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx

SC 3170 switch series	Not supported
SC 3130 switch series	Not supported

# Restrictions and guidelines

When you configure network layer attack protection, follow these restrictions and guidelines:

- After you disable sending ICMP time exceeded messages, the tracer feature will not be available.
- Enabling the uRPF check feature halves the route capacity of the switch.
- The uRPF check feature cannot be enabled if the number of existing routes exceeds half of the route capacity on the switch. This mechanism prevents route loss, which can cause packet loss.

## Procedures

# Specify IP addresses for interfaces. (Details not shown.)

# Enable strict uRPF check.

```
[DeviceA] ip urpf strict
```

# Disable sending ICMP time exceeded messages. Sending ICMP time exceeded messages is disabled by default.

```
[DeviceA] undo ip ttl-expires enable
```

## Verifying the configuration

1. Verify that Device A can prevent source address spoofing attacks:

# Verify that Device A can filter out packets with forged source IP addresses. (Details not shown.)

# Verify the uRPF configuration.

```
[DeviceA] display ip urpf
```

Global uRPF configuration information:

```
Check type: strict
```

2. Verify that TTL attack protection functions on Device A:

# Enable ICMP debugging by executing the **debugging ip icmp** command on Device A. (Details not shown.)

# Use a PC to send packets in which the TTL is 1 to Device A. (Details not shown.)

# Verify that Device A does not display any debugging information and that the PC does not receive any ICMP time exceeded messages. (Details not shown.)

# Enable sending ICMP time exceeded messages and send packets in which the TTL is 1 to Device A. (Details not shown.)

# Verify that Device A responds with ICMP time exceeded messages.

```
<DeviceA> *Aug 14 16:43:31:068 2016 NM-3 SOCKET/7/ICMP: Slot=2;
```

```
Time(s):1371221011 ICMP Output:
```

```
ICMP Packet: src = 6.0.0.1, dst = 202.101.0.2
```

```
type = 11, code = 0 (ttl-exceeded)
```

```
Original IP: src = 202.101.0.2, dst = 192.168.0.2
```

```
proto = 253, first 8 bytes = 00000000 00000000
```

# Configuration files



## IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```
#  
ip urpf strict  
#
```

# Example: Configuring transport layer attack protection

## Network configuration

As shown in [Figure 4](#), the device is the gateway for the internal network. Configure SYN Cookie protection on the device to protect against SYN flood attacks. With this feature enabled, the device responds to a SYN packet with a SYN ACK packet without establishing a TCP semi-connection. The device establishes a TCP connection only when it receives an ACK packet from the sender.

**Figure 4 Network diagram**



# Applicable hardware and software versions

The following matrix shows the hardware and software versions to which this configuration example is applicable:

Hardware	Software version
SC 5525 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 5520 switch series	Release 63xx, Release 65xx, Release 6615Pxx, Release 6628Pxx
SC 3170 switch series	Release 11xx
SC 3130 switch series	Release 63xx

## Procedures

# Specify IP addresses for interfaces. (Details not shown.)

# Enable SYN Cookie.

```
<Device> system-view
```

```
[Device] tcp syn-cookie enable
```

## Verifying the configuration

# Verify that the device does not have any TCP semi-connections. The state "SYN\_RECEIVED" represents semi-connections.

```
[Device] display tcp
```



```

*: TCP connection with authentication
Local Addr:port      Foreign Addr:port    State      Slot  PCB
0.0.0.0:21           0.0.0.0:0            LISTEN     1     0xffffffffffffff9
d
0.0.0.0:23           0.0.0.0:0            LISTEN     1     0xffffffffffffff9
f
192.168.2.88:23      192.168.2.79:2197    ESTABLISHED 1     0xffffffffffffffa
3
192.168.2.88:23      192.168.2.89:2710    ESTABLISHED 1     0xffffffffffffffa
2
192.168.2.88:23      192.168.2.110:50199  ESTABLISHED 1     0xffffffffffffffa
5

```

## Configuration files



### IMPORTANT:

Support for the **port link-mode bridge** command depends on the device model.

```

#
tcp syn-cookie enable
#

```