

Layer 2 Security Features on Cisco Catalyst Layer 3 Fixed Configuration Switches Configuration Example

Document ID: 72846

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

Configure

- Network Diagram
- Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard

Verify

Troubleshoot

Related Information

Introduction

This document provides a sample configuration for some of the Layer 2 security features, such as port security, DHCP snooping, dynamic Address Resolution Protocol (ARP) inspection and IP source guard, that can be implemented on Cisco Catalyst Layer 3 fixed configuration switches.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Catalyst 3750 Series Switch with version 12.2(25)SEC2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with these hardware:

- Cisco Catalyst 3550 Series Switches
- Cisco Catalyst 3560 Series Switches
- Cisco Catalyst 3560–E Series Switches
- Cisco Catalyst 3750–E Series Switches

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Similar to routers, both Layer 2 and Layer 3 switches have their own sets of network security requirements. Switches are susceptible to many of the same Layer 3 attacks as routers. However, switches and Layer 2 of the OSI reference model in general, are subject to network attacks in different ways. These include:

- **Content Addressable Memory (CAM) Table Overflow**

Content Addressable Memory (CAM) tables are limited in size. If enough entries are entered into the CAM table before other entries are expired, the CAM table fills up to the point that no new entries can be accepted. Typically, a network intruder floods the switch with a large number of invalid source Media Access Control (MAC) addresses until the CAM table fills up. When that occurs, the switch floods all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub. If the intruder does not maintain the flood of invalid–source MAC addresses, the switch eventually times out older MAC address entries from the CAM table and begins to act like a switch again. CAM table overflow only floods traffic within the local VLAN so the intruder only sees traffic within the local VLAN to which he or she is connected.

The CAM table overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port. The specification of MAC addresses on switch ports is far too unmanageable a solution for a production environment. A limit of the number of MAC addresses on a switch port is manageable. A more administratively scalable solution is the implementation of dynamic port security at the switch. In order to implement dynamic port security, specify a maximum number of MAC addresses that will be learned.

- **Media Access Control (MAC) Address Spoofing**

Media Access Control (MAC) spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker. When a single frame is sent with the source Ethernet address of the other host, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic, it does not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

Use the port security feature to mitigate MAC spoofing attacks. Port security provides the capability to specify the MAC address of the system connected to a particular port. This also provides the ability to specify an action to take if a port security violation occurs.

- **Address Resolution Protocol (ARP) Spoofing**

ARP is used to map IP addressing to MAC addresses in a local area network segment where hosts of the same subnet reside. Normally, a host sends out a broadcast ARP request to find the MAC address

of another host with a particular IP address, and an ARP response comes from the host whose address matches the request. The requesting host then caches this ARP response. Within the ARP protocol, another provision is made for hosts to perform unsolicited ARP replies. The unsolicited ARP replies are called Gratuitous ARP (GARP). GARP can be exploited maliciously by an attacker to spoof the identity of an IP address on a LAN segment. This is typically used to spoof the identity between two hosts or all traffic to and from a default gateway in a "man-in-the-middle" attack.

When an ARP reply is crafted, a network attacker can make his or her system appear to be the destination host sought by the sender. The ARP reply causes the sender to store the MAC address of the network attacker's system in the ARP cache. This MAC address is also stored by the switch in its CAM table. In this way, the network attacker has inserted the MAC address of his or her system into both the switch CAM table and the ARP cache of the sender. This allows the network attacker to intercept frames destined for the host that he or she is spoofing.

Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems are required as well as static ARP entries. Another solution that can be used to mitigate various ARP-based network exploits, is the use of DHCP snooping along with dynamic ARP inspection. These Catalyst features validate ARP packets in a network and permit the interception, logging, and discarding of ARP packets with invalid MAC address to IP address bindings.

DHCP snooping filters trusted DHCP messages in order to provide security. Then, these messages are used to build and maintain a DHCP snooping binding table. DHCP snooping considers DHCP messages that originate from any user-facing port that is not a DHCP server port as untrusted. From a DHCP snooping perspective, these untrusted user-facing ports must not send DHCP server type responses, such as DHCP OFFER, DHCP ACK, or DHCP NAK. The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch. The DHCP snooping binding table does not contain information about hosts interconnected with a trusted interface. An untrusted interface is an interface configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network. The DHCP snooping binding table can contain both dynamic and static MAC address to IP address bindings.

Dynamic ARP inspection determines the validity of an ARP packet based on the valid MAC address to IP address bindings stored in a DHCP snooping database. Additionally, dynamic ARP inspection can validate ARP packets based on user-configurable access control lists (ACLs). This allows for the inspection of ARP packets for hosts that use statically configured IP addresses. Dynamic ARP inspection allows for the use of per-port and VLAN Access Control Lists (VACLs) to limit ARP packets for specific IP addresses to specific MAC addresses.

- **Dynamic Host Configuration Protocol (DHCP) Starvation**

A DHCP starvation attack works by the broadcast of DHCP requests with spoofed MAC addresses. If enough requests are sent, the network attacker can exhaust the address space available to the DHCP servers for a period of time. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. With the placement of a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Because DHCP responses typically include default gateway and DNS server information, the network attacker can supply his or her own system as the default gateway and DNS server. This results in a man-in-the-middle attack. However, the exhaust of all of the DHCP addresses is not required to introduce a rogue DHCP server.

Additional features in the Catalyst family of switches, such as the DHCP snooping, can be used to help guard against a DHCP starvation attack. DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. The binding table contains information such as the MAC address, IP address, lease time, binding type, VLAN number and the interface information that corresponds to the local untrusted interfaces of a switch. Untrusted messages are those received from outside the network or firewall. Untrusted switch interfaces are ones that are configured to receive such messages from outside the network or firewall.

Other Catalyst switch features, such as IP source guard, can provide additional defense against attacks such as DHCP starvation and IP spoofing. Similar to DHCP snooping, IP source guard is enabled on untrusted Layer 2 ports. All IP traffic is initially blocked, except for DHCP packets captured by the DHCP snooping process. Once a client receives a valid IP address from the DHCP server, a PACL is applied to the port. This restricts the client IP traffic to those source IP addresses configured in the binding. Any other IP traffic with a source address other than the addresses in the binding is filtered.

Configure

In this section, you are presented with the information to configure the Port Security, DHCP Snooping, Dynamic ARP Inspection and IP Source Guard security features.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

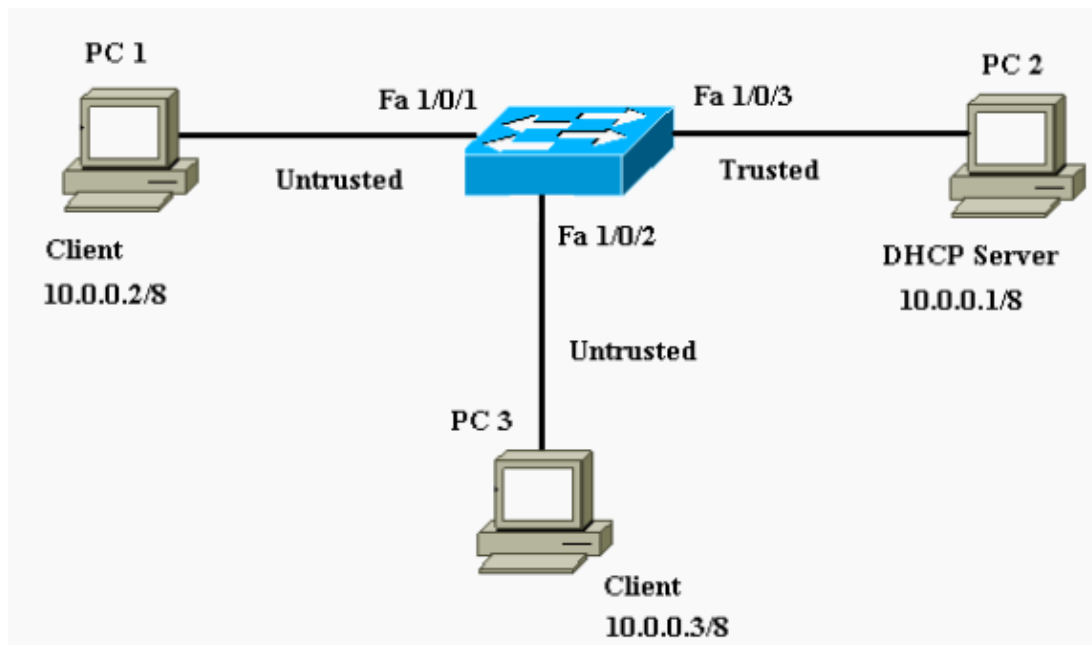
The configurations of the Catalyst 3750 Switch contain these:

- Port Security
- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard

Network Diagram

This document uses this network setup:

- PC 1 and PC 3 are clients connected to the switch.
- PC 2 is a DHCP server connected to the switch.
- All ports of the switch are in the same VLAN (VLAN 1).
- DHCP server is configured to assign IP addresses to the clients based on their MAC addresses.



Port Security

You can use the port security feature to limit and identify MAC addresses of the stations allowed to access the port. This restricts input to an interface. When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses. If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port. If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station that attempts to access the port is different from any of the identified secure MAC addresses, a security violation occurs. Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged. By default, the port shuts down when the maximum number of secure MAC addresses is exceeded.

Note: When a Catalyst 3750 Switch joins a stack, the new switch receives the configured secure addresses. All dynamic secure addresses are downloaded by the new stack member from the other stack members.

Refer to Configuration Guidelines for the guidelines on how to configure port security.

Here, the port security feature is shown configured on the FastEthernet 1/0/2 interface. By default, the maximum number of secure MAC addresses for the interface is one. You can issue the **show port-security interface** command in order to verify the port security status for an interface.

Port Security	
Cat3750# show port-security interface fastEthernet 1/0/2	
Port Security	: Disabled
Port Status	: Secure-down
Violation Mode	: Shutdown
Aging Time	: 0 mins
Aging Type	: Absolute
SecureStatic Address Aging	: Disabled
Maximum MAC Addresses	: 1
Total MAC Addresses	: 0
Configured MAC Addresses	: 0
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0000.0000.0000:0
Security Violation Count	: 0

```

/--- Default port security configuration on the switch.

Cat3750#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat3750(config)#interface fastEthernet 1/0/2
Cat3750(config-if)#switchport port-security
Command rejected: FastEthernet1/0/2 is a dynamic port.

/--- Port security can only be configured on static access ports or trunk ports.

Cat3750(config-if)#switchport mode access

/--- Sets the interface switchport mode as access.

Cat3750(config-if)#switchport port-security

/--- Enables port security on the interface.

Cat3750(config-if)#switchport port-security mac-address 0011.858D.9AF9

/--- Sets the secure MAC address for the interface.

Cat3750(config-if)#switchport port-security violation shutdown

/--- Sets the violation mode to shutdown. This is the default mode.

Cat3750#

/--- Connected a different PC (PC 4) to the FastEthernet 1/0/2 port
/--- to verify the port security feature.

00:22:51: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa1/0/2,
          putting Fa1/0/2 in err-disable state
00:22:51: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,
          caused by MAC address 0011.8565.4B75 on port FastEthernet1/0/2.
00:22:52: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/2,
          changed state to down
00:22:53: %LINK-3-UPDOWN: Interface FastEthernet1/0/2, changed state to down

/--- Interface shuts down when a security violation is detected.

Cat3750#show interfaces fastEthernet 1/0/2
FastEthernet1/0/2 is down, line protocol is down (err-disabled)

/--- Output Suppressed.

/--- The port is shown error-disabled. This verifies the configuration.

/--- Note: When a secure port is in the error-disabled state,
/--- you can bring it out of this state by entering
/--- the errdisable recovery cause psecure-violation global configuration command,
/--- or you can manually re-enable it by entering the
/--- shutdown and no shutdown interface configuration commands.

Cat3750#show port-security interface fastEthernet 1/0/2
Port Security           : Enabled
Port Status             : Secure-shutdown
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type              : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses   : 1
Total MAC Addresses     : 1

```

Configured MAC Addresses	: 1
Sticky MAC Addresses	: 0
Last Source Address:Vlan	: 0011.8565.4B75:1
Security Violation Count	: 1

Note: Same MAC addresses should not be configured as secure and static MAC address on different ports of a switch.

When an IP phone is connected to a switch through the switchport configured for voice VLAN, the phone sends untagged CDP packets and tagged voice CDP packets. So the MAC address of the IP phone is learned on both the PVID and the VVID. If the appropriate number of secure addresses are not configured, you can get an error message similar to this message:

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred,  
caused by MAC address 001b.77ee.eeee on port GigabitEthernet1/0/18.  
PSECURE: Assert failure: psecure_sb->info.num_addrs <= psecure_sb->max_addrs:
```

You must set the maximum allowed secure addresses on the port to two (for IP phone) plus the maximum number of secure addresses allowed on the access VLAN in order to resolve this issue.

Refer to [Configuring Port Security](#) for more information.

DHCP Snooping

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch. When a switch receives a packet on an untrusted interface and the interface belongs to a VLAN that has DHCP snooping enabled, the switch compares the source MAC address and the DHCP client hardware address. If the addresses match (the default), the switch forwards the packet. If the addresses do not match, the switch drops the packet. The switch drops a DHCP packet when one of these situations occurs:

- A packet from a DHCP server, such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet, is received from outside the network or firewall.
- A packet is received on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match.
- The switch receives a DHCPRELEASE or DHCPDECLINE broadcast message that has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received.
- A DHCP relay agent forwards a DHCP packet, which includes a relay-agent IP address that is not 0.0.0.0, or the relay agent forwards a packet that includes option-82 information to an untrusted port.

Refer to [DHCP Snooping Configuration Guidelines](#) for the guidelines on how to configure DHCP snooping.

Note: For DHCP snooping to function properly, all DHCP servers must be connected to the switch through trusted interfaces.

Note: In a switch stack with Catalyst 3750 Switches, DHCP snooping is managed on the stack master. When a new switch joins the stack, the switch receives DHCP snooping configuration from the stack master. When a member leaves the stack, all DHCP snooping bindings associated with the switch age out.

Note: In order to ensure that the lease time in the database is accurate, Cisco recommends that you enable and configure NTP. If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Rogue DHCP servers can be mitigated by DHCP snooping features. The **ip dhcp snooping** command is issued in order to enable DHCP globally on the switch. When configured with DHCP snooping, all ports in the VLAN are untrusted for DHCP replies. Here, only the FastEthernet interface 1/0/3 connected to the DHCP server is configured as trusted.

```

DHCP Snooping

Cat3750#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat3750(config)#ip dhcp snooping

!--- Enables DHCP snooping on the switch.

Cat3750(config)#ip dhcp snooping vlan 1

!--- DHCP snooping is not active until DHCP snooping is enabled on a VLAN.

Cat3750(config)#no ip dhcp snooping information option

!--- Disable the insertion and removal of the option-82 field, if the
!--- DHCP clients and the DHCP server reside on the same IP network or subnet.

Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip dhcp snooping trust

!--- Configures the interface connected to the DHCP server as trusted.

Cat3750#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is disabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----                -
FastEthernet1/0/3        yes          unlimited

!--- Displays the DHCP snooping configuration for the switch.

Cat3750#show ip dhcp snooping binding
MacAddress                IPAddress          Lease(sec)  Type           VLAN  Interface
-----                -
00:11:85:A5:7B:F5        10.0.0.2          86391      dhcp-snooping  1     FastEtheret1/0/1
00:11:85:8D:9A:F9        10.0.0.3          86313      dhcp-snooping  1     FastEtheret1/0/2
Total number of bindings: 2

!--- Displays the DHCP snooping binding entries for the switch.

Cat3750#

!--- DHCP server(s) connected to the untrusted port will not be able
!--- to assign IP addresses to the clients.

```

Refer to Configuring DHCP Features for more information.

Dynamic ARP Inspection

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from

certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before it updates the local ARP cache or before it forwards the packet to the appropriate destination
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

In non-DHCP environments, dynamic ARP inspection can validate ARP packets against user-configured ARP ACLs for hosts with statically configured IP addresses. You can issue the **arp access-list** global configuration command in order to define an ARP ACL. ARP ACLs take precedence over entries in the DHCP snooping binding database. The switch uses ACLs only if you issue the **ip arp inspection filter vlan** global configuration command in order to configure the ACLs. The switch first compares ARP packets to user-configured ARP ACLs. If the ARP ACL denies the ARP packet, the switch also denies the packet even if a valid binding exists in the database populated by DHCP snooping.

Refer to Dynamic ARP Inspection Configuration Guidelines for the guidelines on how to configure dynamic ARP inspection.

The **ip arp inspection vlan** global configuration command is issued in order to enable dynamic ARP inspection on a per-VLAN basis. Here, only the FastEthernet interface 1/0/3 connected to the DHCP server is configured as trusted with the **ip arp inspection trust** command. DHCP snooping must be enabled in order to permit ARP packets that have dynamically assigned IP addresses. See the DHCP Snooping section of this document for DHCP snooping configuration information.

```
Dynamic ARP Inspection
Cat3750#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Cat3750(config)#ip arp inspection vlan 1

!--- Enables dynamic ARP inspection on the VLAN.

Cat3750(config)#interface fastEthernet 1/0/3
Cat3750(config-if)#ip arp inspection trust

!--- Configures the interface connected to the DHCP server as trusted.

Cat3750#show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

Vlan    Configuration      Operation  ACL Match      Static ACL
----    -
1       Enabled             Active
Vlan    ACL Logging           DHCP Logging
----    -
1       Deny                  Deny
```

```
!--- Verifies the dynamic ARP inspection configuration.
```

```
Cat3750#
```

Refer to Configuring Dynamic ARP Inspection for more information.

IP Source Guard

IP source guard is a security feature that filters traffic based on the DHCP snooping binding database and on manually configured IP source bindings in order to restrict IP traffic on non-routed Layer 2 interfaces. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor. IP source guard prevents IP/MAC spoofing.

You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. A port ACL is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

You can configure IP source guard with source IP address filtering, or with source IP and MAC address filtering. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table.

Note: IP source guard is supported only on Layer 2 ports, which includes access and trunk ports.

Refer to IP Source Guard Configuration Guidelines for guidelines on how to configure IP source guard.

Here, IP source guard with source IP filtering is configured on the FastEthernet 1/0/1 interface with the **ip verify source** command. When IP source guard with source IP filtering is enabled on a VLAN, DHCP snooping must be enabled on the access VLAN to which the interface belongs. Issue the **show ip verify source** command in order to verify the IP source guard configuration on the switch.

IP Source Guard

```
Cat3750#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Cat3750(config)#ip dhcp snooping
Cat3750(config)#ip dhcp snooping vlan 1

!--- See the DHCP Snooping section of this document for
!--- DHCP snooping configuration information.

Cat3750(config)#interface fastEthernet 1/0/1
Cat3750(config-if)#ip verify source

!--- Enables IP source guard with source IP filtering.

Cat3750#show ip verify source
Interface  Filter-type  Filter-mode  IP-address      Mac-address      Vlan
-----  -
-----  -
-----  -
-----  -
-----  -
```

```
Fa1/0/1    ip          active    10.0.0.2          1
!--- For VLAN 1, IP source guard with IP address filtering is configured
!--- on the interface and a binding exists on the interface.
Cat3750#
```

Refer to Understanding IP Source Guard for more information.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Securing Networks with Private VLANs and VLAN Access Control Lists](#)
- [LAN Product Support](#)
- [LAN Switching Technology Support](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 17, 2007

Document ID: 72846
