

# IP Source Guard

## Ethernet Switch

ZyNOS 4.0

## Support Notes

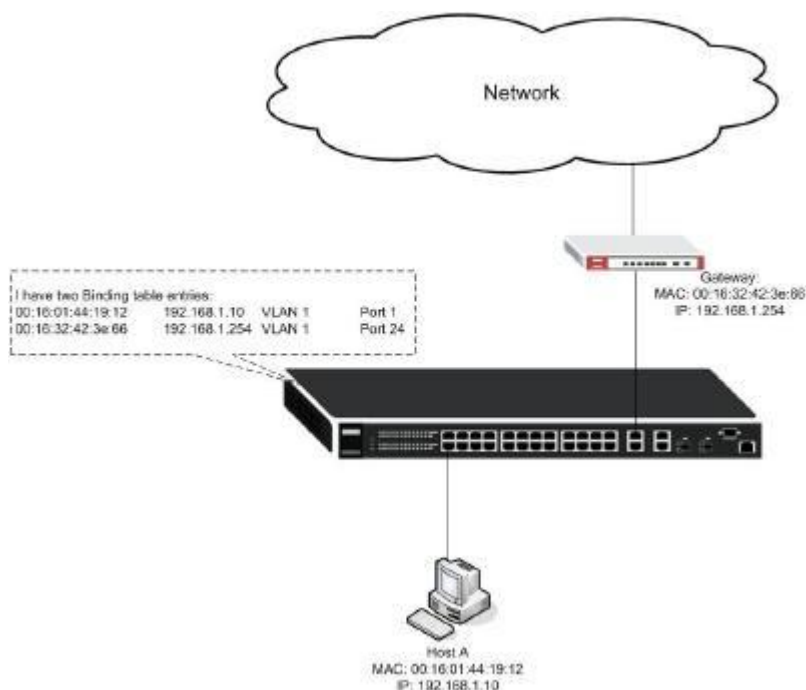
Version 4.0

July 2011



## Overview of IP Source Guard

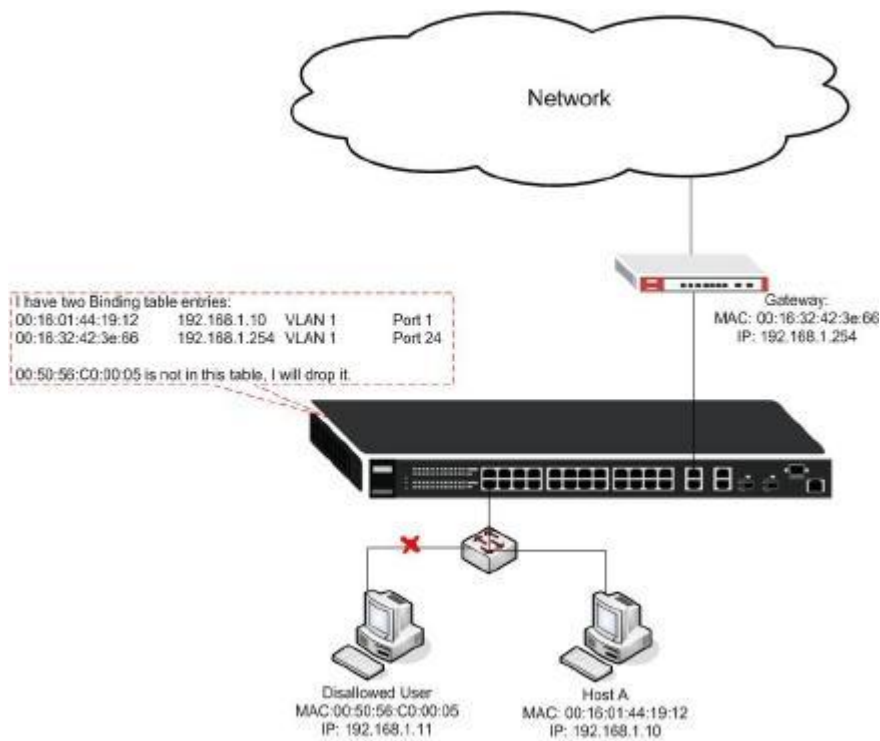
IP Source Guard is a new feature in ZyNOS 3.80. It allows the switch to identify who has the permission to access the network. Furthermore, device can check the binding of MAC address, IP address, VLAN tag, and ingress port of packets. Had any parameter be mismatching, the packet will be dropped. The below scenario is an example:



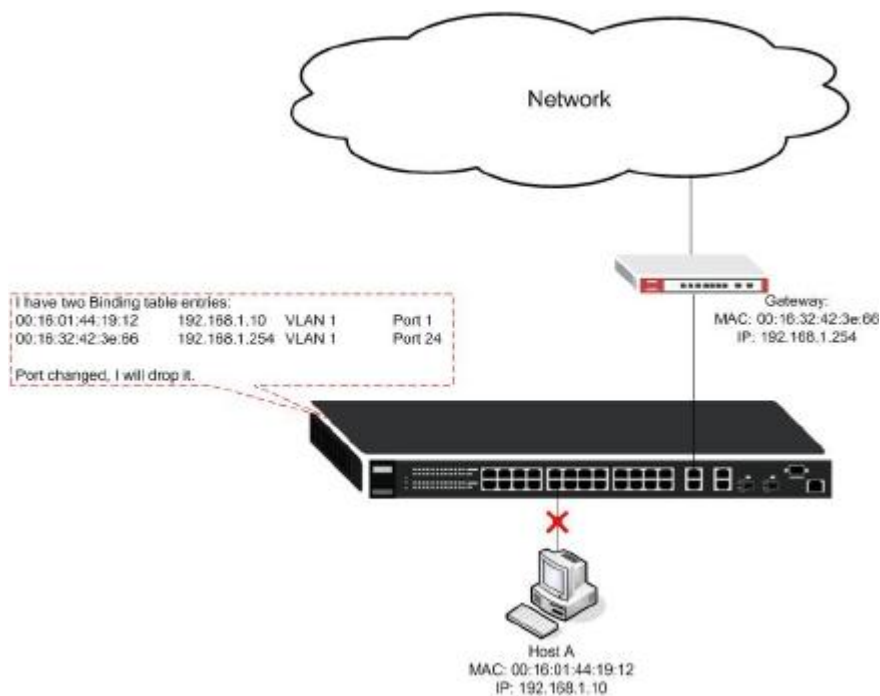
Host A has its own static IP address, MAC address, and the switch knows which Host A has connected and what VLAN this port belongs to.

IP Source Guard can filter packets in the below scenarios:

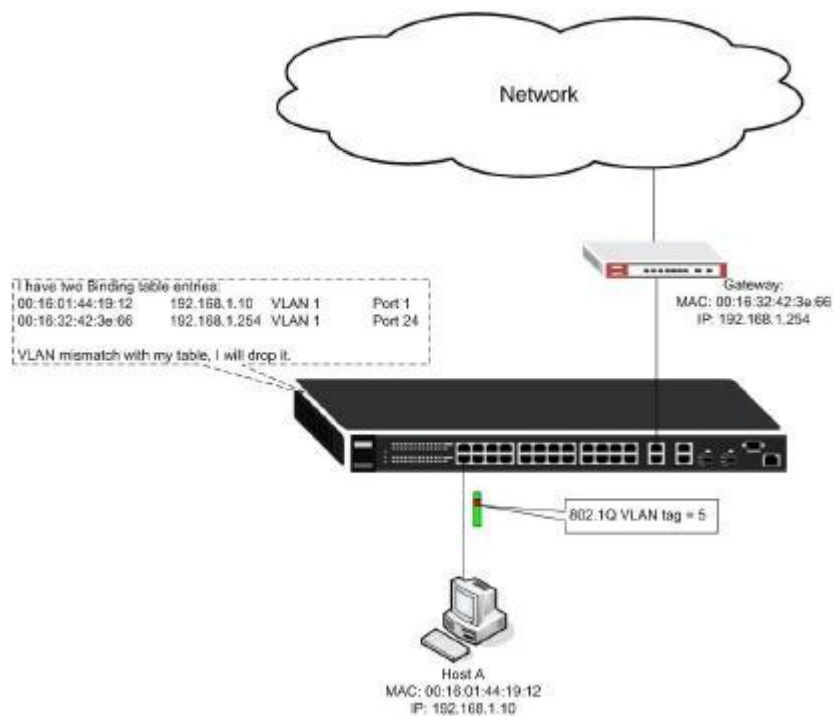
1. If unauthorized user connects to an external switch, IP Source Guard will drop packets coming from the user. IP or MAC address mismatching.



2. If Host A changes the connecting port, the switch will drop packets coming from Host A. port mismatching.



3. If the VLAN tag is different from the table of switch. The packets from Host A will be dropped because of the mismatching of VLAN.



## Scenario

Here we'd like to demonstrate a situation with a port changing. Consider the scenario below:

Figure 1

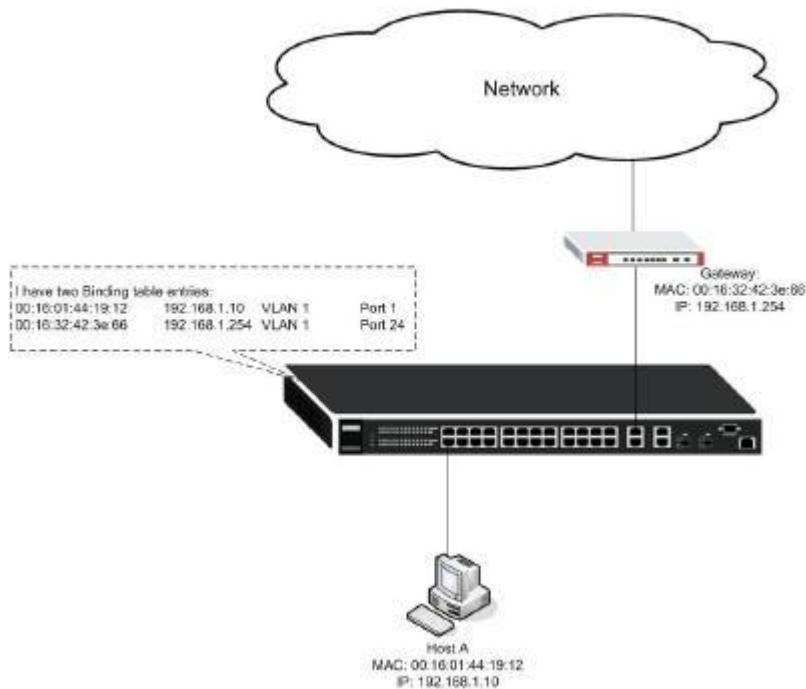
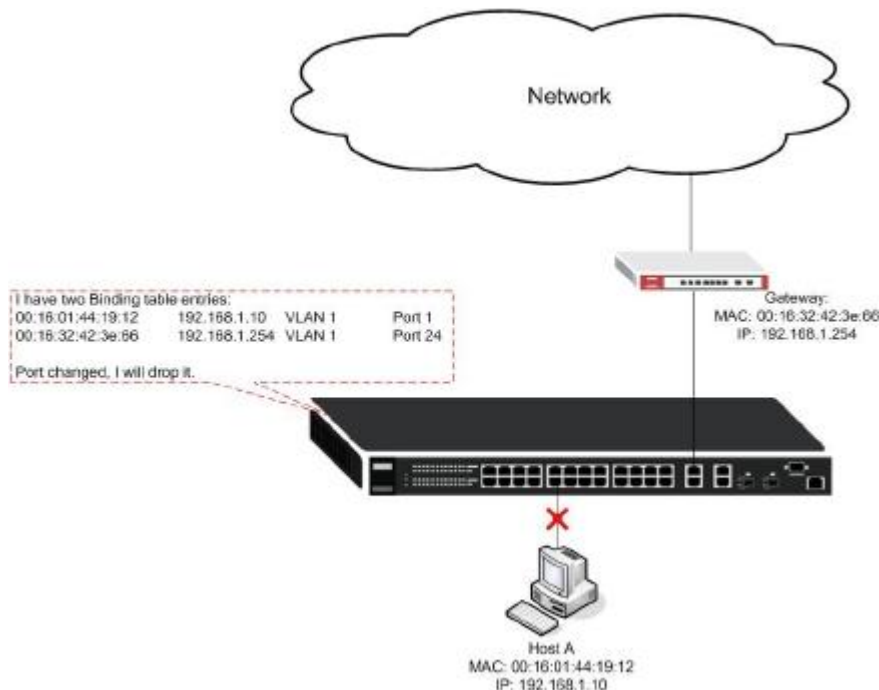


Figure 2



In this example, Host A and Gateway are connected to port 1 and port 26 (Figure 1). Administrator builds a static binding of Host A and Gateway. If any of the two devices

changes its connecting port, the packets will be dropped by the switch.

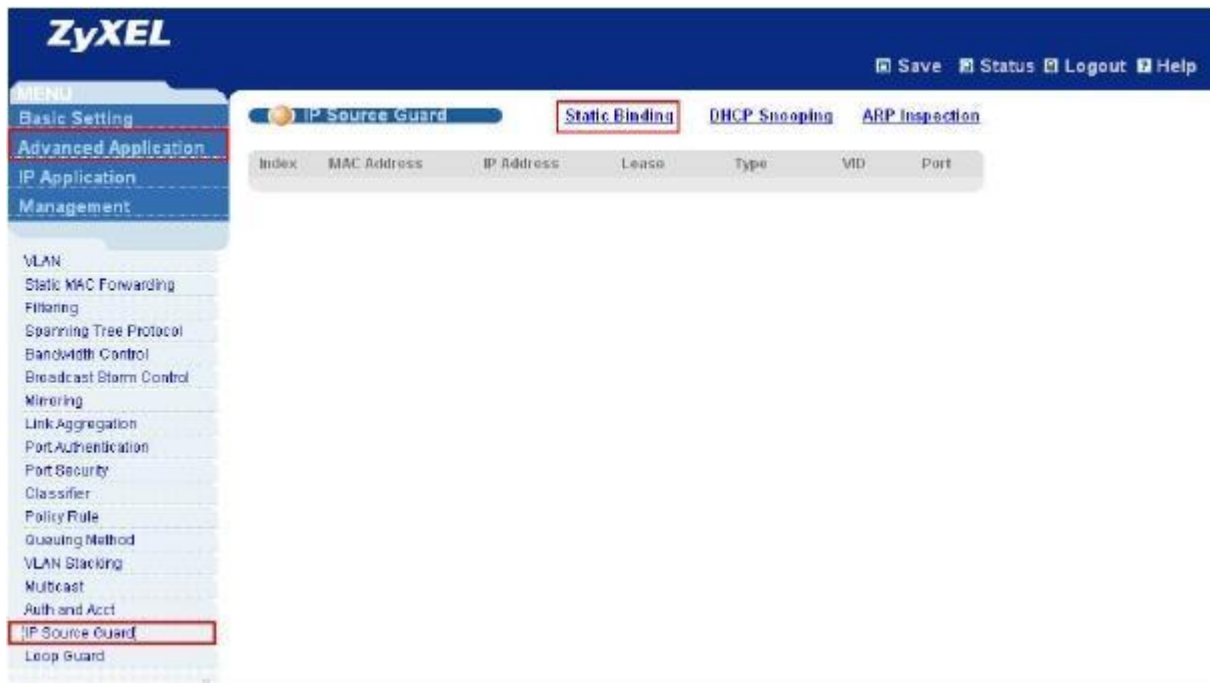
## Configuration using the Web GUI

1. Connect the MGMT port to a PC or Notebook using the RJ45 Cable.
2. By default, the MGMT IP address of the out-band port is 192.168.0.1/24
3. Set your NIC to 192.168.0.100/24
4. Open an Internet browser (e.g. IE) and enter <http://192.168.0.1> into the URL field.
5. By default, the username for the administrator is “admin” and the password is “1234”.
6. After successfully logging in, you will see a screen similar to the one below.

The screenshot shows the ZyXEL Web GUI interface. On the left is a menu with options: MENU, Basic Setting, Advanced Application, IP Application, and Management. The 'Advanced Application' option is highlighted. On the right, the 'Port Status' table is displayed, showing details for ports 1 through 10. The table includes columns for Port, Name, Link, State, PD, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, and Up Time.

Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		1000M/F	FORWARDING	Off	Disabled	1116	1476	0	29.787	8.825	1:17:32
2	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8	Down		STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9	Down		STOP	-	Disabled	819	10239	0	0.0	0.0	0:00:00
10	Down		STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00

7. Click “**Advanced Application**” → “**IP Source Guard**” → “**Static Binding**” to go to the “**IP Source Guard Static Binding**” page.



8. In the “**IP Source Guard Static Binding**” page, set the MAC, IP, VLAN, and Port binding then click “**Add**”. Below is an example of binding the Gateway to port 26.

The screenshot shows the 'IP Source Guard Static Binding' configuration form. It has a title bar with 'IP Source Guard Static Binding' and a 'IPSG' link. The form contains the following fields:

- MAC Address:** 00 : 00 : e8 : 89 : 8b : b7
- IP Address:** 192.168.1.254
- VLAN:** 1
- Port:** ☒ 26 ☐ Any

At the bottom of the form are three buttons: 'Add', 'Cancel', and 'Clear'.

9. Then we continue to add a new binding of Host A.



**IP Source Guard Static Binding**
IPSG

MAC Address	00 : 16 : 01 : 44 : 19 : 12
IP Address	192.168.1.10
VLAN	1
Port	<input checked="" type="radio"/> 1 <input type="radio"/> Any

Add Cancel Clear

10. After creating the static binding, we need to configure the ARP inspection. Because IP Source Guard filters packets based on the ARP packets before a session was established. After the ARP was inspected, then the switch decides if it will forward the following packets like ICMP, TCP.

Click **“Advanced Application”** **“IP Source Guard”** **“ARP Inspection”** then click **“Configure”** to enter the “ARP Inspection Configure” page.

[Save](#) [Status](#) [Logout](#) [Help](#)

**MENU**  
[Basic Setting](#)  
[Advanced Application](#)  
[IP Application](#)  
[Management](#)  


---

[VLAN](#)  
[Static MAC Forwarding](#)  
[Filtering](#)  
[Spanning Tree Protocol](#)  
[Bandwidth Control](#)  
[Broadcast Storm Control](#)  
[Mirroring](#)  
[Link Aggregation](#)  
[Port Authentication](#)  
[Port Security](#)  
[Classifier](#)  
[Policy Rule](#)  
[Queuing Method](#)  
[VLAN Stacking](#)  
[Multicast](#)  
[Auth and Act](#)  
[IP Source Guard](#)  
[Loop Guard](#)

**IP Source Guard**
Static Binding
DHCP Snooping
ARP Inspection

Index	MAC Address	IP Address	Lease	Type	VID	Port
1	00:16:01:44:18:12	192.168.1.11	Infinity	static	1	1
2	ca:00:01:19:00:00	192.168.1.254	Infinity	static	1	24

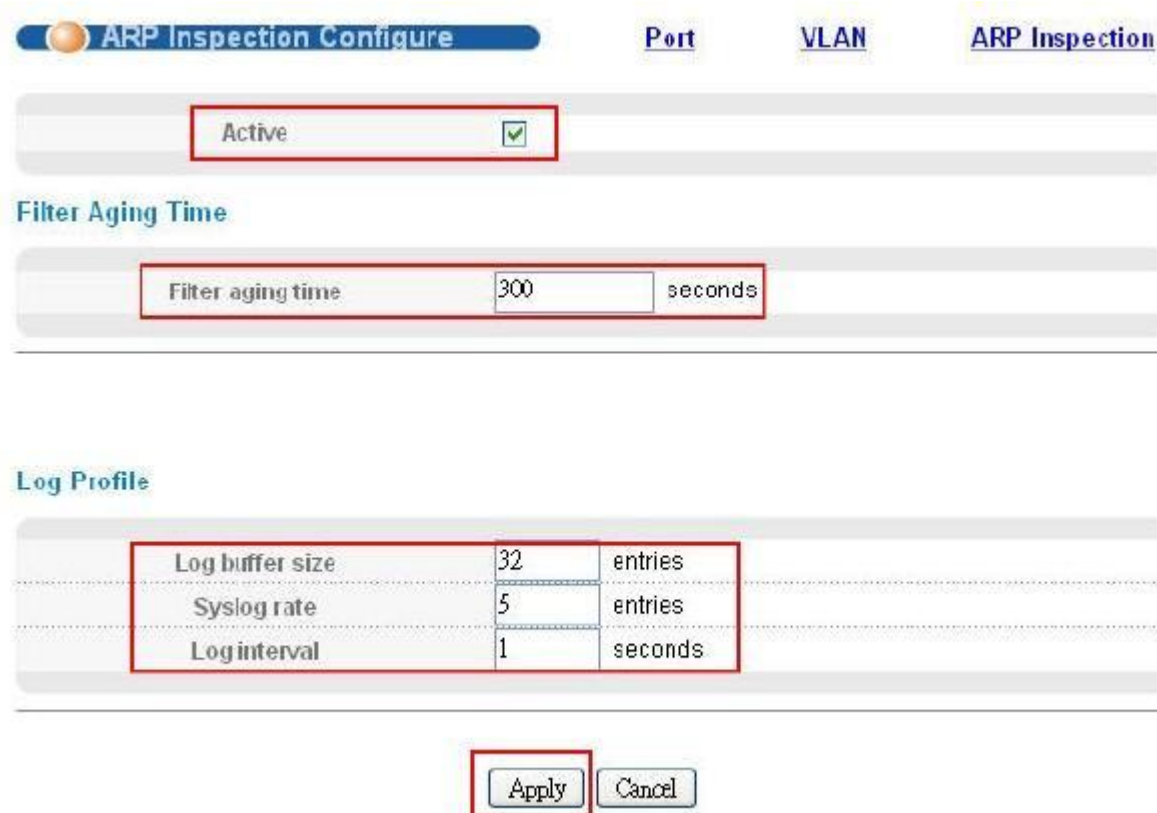


The screenshot shows the 'ARP Inspection Status' page. At the top, there are four tabs: 'ARP Inspection Status' (selected), 'VLAN Status', 'Log Status', and 'Configure' (highlighted with a red box). To the right of these tabs is an 'IPSG' link. Below the tabs, it says 'Total number of filters – 0'. There is a table with the following columns: Index, MAC Address, VID, Port, Expiry (sec), Reason, and Delete. The table contains one row with asterisks (\*) in the first six columns and a checkbox in the 'Delete' column. Below the table are 'Delete' and 'Cancel' buttons.

Index	MAC Address	VID	Port	Expiry (sec)	Reason	Delete
*	*	*	*	*	*	<input type="checkbox"/>

Buttons: Delete, Cancel

11. Check the “**Active**” checkbox, enter the “**Filter Aging Time**” and “**Log Profile**” value on the “**ARP Inspection Configure**” page. You can leave “**Filter Aging Time**” and “**Log Profile**” value by default. Click “**Apply**”



The screenshot shows the 'ARP Inspection Configure' page. At the top, there are four tabs: 'ARP Inspection Configure' (selected), 'Port', 'VLAN', and 'ARP Inspection'. Below the tabs, there is a section for 'Active' with a checkbox that is checked (highlighted with a red box). Below this is a section for 'Filter Aging Time' with a text input field containing '300' and the unit 'seconds' (highlighted with a red box). Below that is a section for 'Log Profile' with a table containing three rows: 'Log buffer size' with value '32' and unit 'entries', 'Syslog rate' with value '5' and unit 'entries', and 'Log interval' with value '1' and unit 'seconds' (the entire table is highlighted with a red box). At the bottom, there are 'Apply' and 'Cancel' buttons (the 'Apply' button is highlighted with a red box).

Active ☒

Filter Aging Time

Filter aging time 300 seconds

Log Profile

Log buffer size	32	entries
Syslog rate	5	entries
Log interval	1	seconds

Buttons: Apply, Cancel

12. Click “**VLAN**” to open the “**ARP Inspection VLAN Configure**” page.

ARP Inspection Configure

Port

VLAN

ARP Inspection

Active

☒

Filter Aging Time

Filter aging time

300

seconds

Log Profile

Log buffer size	32	entries
Syslog rate	5	entries
Log interval	1	seconds

Apply

Cancel

13. There are two parts in the “**ARP Inspection VLAN Configure**” page. The upper part is used to show the list of VLAN setting and the lower part is used to configure which VLAN the ARP Inspection was implemented.

Here we enter “1” as the “**Start VID**” and “5” as the “**End VID**”. Click “**Apply**”

ARP Inspection VLAN Configure

Configure

VLAN

Start VID 1

End VID 5


Apply

VID	Enabled	Log
*	No <input type="button" value="v"/>	None <input type="button" value="v"/>

Apply

Cancel

Then the lower part will show each VLAN’s configuration. Since we use VLAN 1 as Host A’s VLAN, we need to enable it on VLAN 1.

 **ARP Inspection VLAN Configure**

[Configure](#)

VLAN	Start VID <input style="width: 50px;" type="text"/>	End VID <input style="width: 50px;" type="text"/>
------	---	---

VID	Enabled	Log
*	No <input type="button" value="v"/>	None <input type="button" value="v"/>
1	Yes <input type="button" value="v"/>	All <input type="button" value="v"/>
2	No <input type="button" value="v"/>	All <input type="button" value="v"/>
3	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>
4	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>
5	No <input type="button" value="v"/>	Deny <input type="button" value="v"/>

Apply

14. After step 13, the Static Binding is successfully configured.

## Configuration using the CLI

```
vlan 1 name 1
    normal ""
    fixed 1-10
    forbidden ""
    untagged 1-10
    ip address 192.168.1.1 255.255.255.0
exit
interface route-domain 192.168.1.1/24
exit
ip source binding 00:16:01:44:19:12 vlan 1 192.168.1.11 interface port-channel 1
ip source binding 00:16:32:42:3e:66 vlan 1 192.168.1.254 interface port-channel 26
ip address 192.168.0.1 255.255.255.0
arp inspection vlan 1 logging all
arp inspection vlan 1
arp inspection
```