Table of Contents

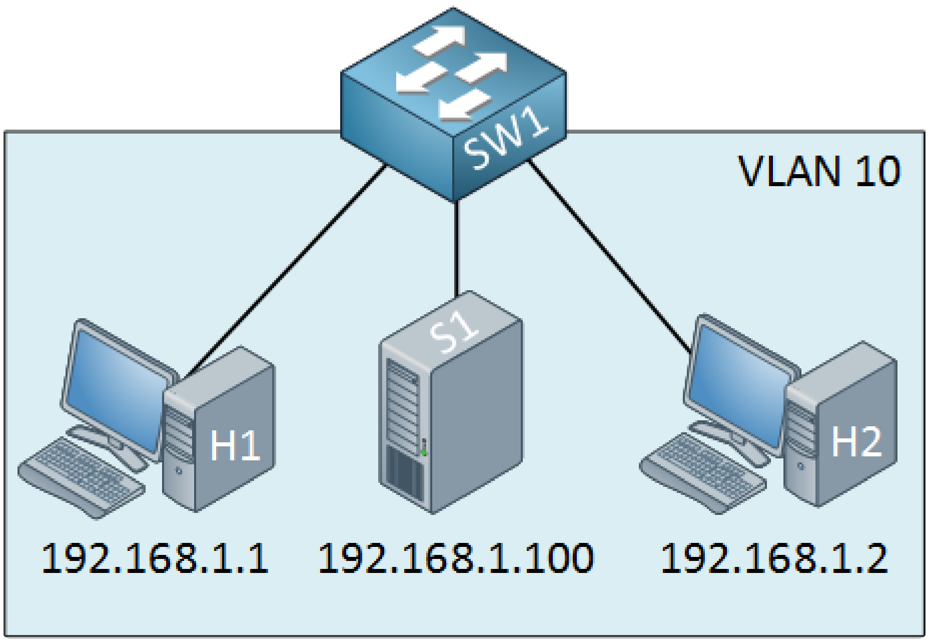
CCIE Routing & Switching

You are here: Home » Cisco » CCIE Routing & Switching

VLAN Access-List (VACL)

★★★★★ 10 votes

VLAN access-lists (VACL) are very useful if you want to filter traffic within the VLAN. Let me give you an example:



Let's say I want to make sure that the two computers are unable to communicate with the server. You could use port-security to filter MAC addresses but this isn't a very safe method.

I will show you how to configure a VACL so that the two computers won't be able to reach the server. First we have to create an access-list:

```
SW1(config)#access-list 100 permit ip any host 192.168.1.100
```

First step is to create an extended access-list. Traffic from any source to destination IP address 192.168.1.100 should match my access-list. This might look confusing to you because your gut will tell you to use "deny" in this statement…don't do it though, use the permit statement!

```
SW1(config)#vlan access-map NOT-TO-SERVER 10
SW1(config-access-map)#match ip address 100
SW1(config-access-map)#action drop
SW1(config-access-map)#vlan access-map NOT-TO-SERVER 20
SW1(config-access-map)#action forward
```

Next step is to create the VACL. Mine is called "NOT-TO-SERVER".

• Sequence number 10 will look for traffic that matches access-list 100. All traffic that is permitted in access-list 100 will match here. The action is to drop this traffic.
• Sequence number 20 doesn't have a match statement so everything will match, the action is to forward traffic.

As a result all traffic from any host to destination IP address 192.168.1.100 will be dropped, everything else will be forwarded.

```
SW1(config)#vlan filter NOT-TO-SERVER vlan-list 10
```

Last step is to apply the VACL to the VLANs you want. I apply mine to VLAN 10. Let's see if this works or not…

```
C:Documents and SettingsH1>ping 192.168.1.100

Pinging 192.168.4.4 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.4.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

H1 is no longer able to reach the server.

You can use VACLs to do some cool stuff, maybe you want to block IPv6 traffic for all hosts within a VLAN:

```
SW1(config)#mac access-list extended NO-IPV6
SW1(config-ext-macl)#permit any any 0x86DD 0x000
```

First I'll create a MAC access-list that filters on ethertypes. 0x86DD is the ethertype for IPv6 traffic.

```
SW1(config)#vlan access-map BLOCK-IPV6 10
SW1(config-access-map)#match mac address NO-IPV6
SW1(config-access-map)#action drop
SW1(config-access-map)#vlan access-map BLOCK-IPV6 20
SW1(config-access-map)#action forward
```

• Sequence number 10 will match traffic that is defined in MAC access-list "NO-IPV6". It will match on Ethernet frames with ethertype 0x86DD as defined in the MAC access-list. The action is to drop traffic.
• Sequence number 20 does not have a match statement so everything will match. The action is to forward traffic.

As a result IPv6 traffic will be dropped and all other traffic will be forwarded.

```
SW1(config)#vlan filter BLOCK-IPV6 vlan-list 20
```

Don't forget to enable it on an interface. I'll activate it on VLAN 20 this time. That's all there is to it, I hope this lesson has been helpful.

Rate this Lesson:

★★★★★

« Previous Lesson
AAA Authentication on Cisco Switch

Next Lesson »
DHCP Snooping

Home › Forums › VLAN Access-List (VACL)

This topic contains 19 replies, has 8 voices, and was last updated by Rene Molenaar 7 months, 4 weeks ago.

Viewing 15 posts - 1 through 15 (of 19 total)
1 2 →

- Author
  Posts | Subscribe
- December 4, 2014 at 02:27 #10976 Reply

geoff o
Member

Hi, just getting ready for CCNP Switch .

I was wondering how do you edit / update VACLs ?
Do you need to use text editor like standard ?
Reload switch ?

Examples of changing requirements say add new server 192.168.1.101

December 5, 2014 at 12:43 #10977 Reply

Rene Molenaar
Keymaster

Hi Geoff,

You can edit the access-list, no problem at all. I'm not 100% sure if it will be active right away or if you need to remove + add the VACL again before it is applied. If you want to know, I can try it and let you know the results.

Rene

October 13, 2015 at 06:38 #18826 Reply

Ronie S
Participant

Hi Rene,

I was trying to use the VACL with mac access-list to prevent traffic from Computer A to Computer B. Both computer are connected directly to the Swtich A as follow,

Switch A

Computer A	Computer B
IP- 192.168.1.1	IP-192.168.1.2
MAC – 0023.2343.5678	MAC- 0023.2343.5679

****

Configuration on Switch A,

```
mac access-list extended test

permit any host 0023.2343.5679

vlan access-map test1 10

match mac address test

action drop

vlan access-map test1 20

action forward

vlan filter test1 vlan-list 1 (knowing all switch ports are in default vlan 1)
```

****

Testing

Once I tried to ping from computer A to B, the ping request timed out for 5 times and after 5 times, ping started to reply successfully for 8 times and blocked 5 times again. Keep rotating like that.

****

Do you know what I am missing ? Please suggest me. Thank you in advance.

Best Regards,

Ronie

October 14, 2015 at 16:06 #18870 Reply

Frades
Participant
wow, similar to route-map. awesome!

i have a question, on the 1st sentence you said that we can prevent both computers from communicating with server by using "port security". could you elaborate on how port-security will filter the traffic of computers going to server?

October 23, 2015 at 15:53 #19162 Reply

Rene Molenaar

Keymaster
@Ronie I just did some testing and I'm also seeing strange results when using a mac access-list to filter MAC addresses. I used two routers and one 3560 switch. When I apply the vlan filter, the routers are still able to ping each other until I clear their ARP tables. Once I do that, they are unable to reach each other anymore since some of the ARP packets get filtered.

I would expect all traffic that matches one of the MAC addresses to be filtered but for whatever reason, it's acting weird.
@Frades you can use port security to set a limit to the number of MAC addresses or you can use it as a MAC address filter. The last option will do the job but it's not very secure, MAC addresses are easy to spoof.

December 7, 2015 at 22:54 #20124 Reply

Hamood R
Participant
Rene,

Great lesson however I have question. When we applied filter to certain VLAN in the example it is VLAN 10. It means all traffic from VLAN 10 will be blocked? Please clarify.

Thanks

Hamood

December 9, 2015 at 21:50 #20155 Reply

Rene Molenaar
Keymaster
Hi Hamood,

It will be applied to all traffic in VLAN 10 yes, depending on what you configured on the access-list.

Rene

January 19, 2016 at 15:41 #21125 Reply

Hans d

Participant
Hi Rene,

I have some weird results when I try to configure a vlan access-map:

```
DSW1(config)#vlan access-map ?
```

```
DSW1(config)#vlan access-map
Command rejected: Bad VLAN list - character #1 is a non-numeric
character ('a').
```

When I copy and past your commands, it returns a “Invalid character detected”
I’ve tried this on a switch running SW version 12.1 and 15.0, both do the same.

Any ideas?

Regards,

Hans de Roode

January 19, 2016 at 16:59 #21128 Reply

Rene Molenaar
Keymaster
Hi Hans,

What device/IOS are you using? It seems it doesn’t know the vlan access-map command. Instead it thinks you want to create a VLAN called ‘a’ (first letter it finds) which returns an error since VLANs can only have numbers.

Here’s the output of a switch:

```
Switch(config)#vlan ?
  WORD           ISL VLAN IDs 1-4094
  access-log     Configure VACL logging
  access-map     Create vlan access-map or enter vlan access-map command
mode
  accounting     VLAN accounting configuration
  configuration  vlan feature configuration mode
  filter         Apply a VLAN Map
  group          Create a vlan group
  internal       internal VLAN
```

Above you can see it supports vlan access-maps.

```
Switch(config)#vlan access-map ?
  WORD  Vlan access map tag
```

```
Switch(config)#vlan access-map TEST
Switch(config-access-map)#
```

Rene

January 20, 2016 at 02:37 #21140 Reply

Hans d
Participant
Hi Rene,
I’m using 2950 SW version 12.1 and a IE200 with SW version 15.0, and no access-map command.
I just tried a IE3000 and that one has the access-map command.

Problem solved, it’s model related.

Thank you for your help.
Regards,
Hans de Roode.

March 5, 2016 at 12:00 #22543 Reply

Jie C
Participant
Private vlan can also achieve the same goal isn’t it. What could be different from the design point of view?

March 5, 2016 at 12:04 #22544 Reply

Jie C
Participant
seems like vacl is more flexible when comes with specific traffic requirements. Thanks Rene

March 6, 2016 at 12:43 #22549 Reply

Rene Molenaar
Keymaster
Hi Jie,

Private VLANs allow you to restrict traffic between VLANs or when you use the isolated VLAN, it prevents hosts within the VLAN from communicating with each other (similar to the protected port).

The VLAN access-list allows you to filter specific traffic within a VLAN.

Rene

March 29, 2016 at 17:09 #23027 Reply

Jason W
Participant
Rene, Do you have a lesson on Port ACLs (PACL)?

March 30, 2016 at 19:38 #23046 Reply

Rene Molenaar
Keymaster
Hi Jason,

Not yet but let me show you something here. a Port ACL is a standard, excended or MAC access-list that is applied to a L2 switchport. For example:

```
Switch(config)#ip access-list extended PERMIT_EVERYTHING
Switch(config-ext-nacl)#permit ip any any

Switch(config)#interface GigabitEthernet 0/1
Switch(config-if)#ip access-group PERMIT_EVERYTHING in
```

Or if you want to filter MAC addresses:

```
Switch(config)#mac access-list extended SOURCE_MAC
Switch(config-ext-macl)#permit host fa16.3e0d.b11f any

Switch(config)#interface GigabitEthernet 0/2
Switch(config-if)#mac access-group SOURCE_MAC in
```

Rene

- Author
  Posts

Viewing 15 posts - 1 through 15 (of 19 total)
1 2 →
Reply To: VLAN Access-List (VACL)

b i link b-quote del img ul ol li code close tags ¶

Please put configurations in between `backticks` or use the CODE button.
To place inline images, please use a image share service (such as TinyPic or Imgur) and use the IMG button!

□ Notify me of follow-up replies via email

Maximum file size allowed is 2048 KB.

Attachments:
Choose File No file chosen
Add another file

Submit

About NetworkLessons.com

Hello There! I'm René Molenaar (CCIE #41726), Your Personal Instructor of Networklessons.com. I'd like to teach you everything about Cisco, Wireless and Security. I am here to Help You Master Networking!

Read my story

Social Fans

14,351 FANS	8,735 FOLLOWERS	1,589 SUBSCRIBERS

Highest Rated Lessons

MPLS Layer 3 VPN Configuration
★★★★★ (35 votes)

Cisco Portfast Configuration
★★★★★ (27 votes)

Introduction to DMVPN
★★★★★ (21 votes)

EIGRP Router ID
★★★★★ (20 votes)

How to configure OSPF Virtual Link
★★★★★ (19 votes)

New Lessons

Voice VLAN

Introduction to Wireless LAN

Network Topologies

Broadcast Domain

Collision Domain

Disclaimer

Privacy Policy

Support

VLAN Access-List (VACL) written by Rene Molenaar average rating 4.7/5 - 10 user ratings