CCNPv7 SWITCH

Chapter 10 Lab 10-2, Securing VLANs

Modifikovaný: PS 2017-06-11

Topology



Objectives

* Secure the staff VLAN from the student VLAN.
* Secure the staff VLAN when temporary staff personnel are used.
* Secure the server farm using private VLANs.

POZN: modifikácia -> najprv RACL, VACL, potom private vlan

Background

In this lab, you will configure the network to protect the VLANs using router ACLs, VLAN ACLs, and private VLANs. First, you will secure the new server farm (Host C) by using private VLANs. Service providers use private VLANs to separate different customers’ traffic while utilizing the same parent VLAN for all server traffic. The private VLANs provide traffic isolation between devices, even though they might exist on the same VLAN.

You will then secure the staff VLAN from the student VLAN by using a RACL, which prevents traffic from the student VLAN from reaching the staff VLAN. This allows the student traffic to utilize the network and Internet services while keeping the students from accessing any of the staff resources.

Lastly, you will configure a VACL that allows a host on the staff network to be set up to use the VLAN for access but keeps the host isolated from the rest of the staff machines. This machine is used by temporary staff employees.

**Note:** This lab uses Cisco Catalyst 3560 and 2960 switches running Cisco IOS 15.0(2) IP Services and LAN Base images, respectively. The 3560 and 2960 switches are configured with the SDM templates “dual-ipv4-and-ipv6 routing” and “lanbase-routing”, respectively. Depending on the switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab. Catalyst 3650 switches (running any Cisco IOS XE release) and Catalyst 2960-Plus switches (running any supported Cisco IOS image) can be used in place of the Catalyst 3560 switches and the Catalyst 2960 switches.

Required Resources

* 2 switches (Cisco 2960 with the Cisco IOS Release 15.0(2)SE6 C2960-LANBASEK9-M image or comparable)
* 2 switches (Cisco 3560 with the Cisco IOS Release 15.0(2)SE6 C3560-ipservicesK9-M image or comparable)
* 4 PCs
* Ethernet and console cables

Step 1: Load and verify the configurations from lab 10-1.

1. Verify that the configurations from Lab 10-1 are loaded on the devices by issuing the show vtp status command. The output should show that the current VTP domain is SWPOD, and VLANs 100 and 200 should be represented in the number of existing VLANs. The output from switch ALS1 is shown as an example. If the switches are not configured properly, erase the startup config, delete the vlan.dat file, and load the configurations saved at the end of lab 10-1.

**Note**: If you are loading the configurations from Lab 10-1, they do not include VLAN and VTP commands. You must first configure ALS1 and ALS2 as VTP clients and then create VLANs 100 (staff) and 200 (student) and the VTP domain name on DLS1. Refer to Lab 10-1 for assistance if necessary.

ALS1# **show vtp status**

VTP Version capable : 1 to 3

VTP version running : 2

VTP Domain Name : SWPOD

VTP Pruning Mode : Disabled

VTP Traps Generation : Disabled

Device ID : 0017.95d1.8b80

Configuration last modified by 172.16.1.3 at 3-1-93 01:39:36

Feature VLAN:

--------------

VTP Operating Mode : Client

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

Configuration Revision : 3

MD5 digest : 0xAE 0xEB 0x3A 0xEB 0x28 0x23 0x1D 0x85

0x7E 0x8C 0x70 0x56 0x03 0x70 0x29 0xB2

Will VLAN information be stored in NVRAM when this device is rebooted? Explain.

1. Issue the show vlan command on DLS1. The student and staff VLANs should be listed in the output of this command.

DLS1# **show vlan brief**

VLAN Name Status Ports

---- ------------------------------- --------- -----------------------------

1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4

Fa0/5, Fa0/6, Fa0/13, Fa0/14

Fa0/15, Fa0/16, Fa0/17, Fa0/18

Fa0/19, Fa0/20, Fa0/21, Fa0/22

Fa0/23, Fa0/24

Gi0/1, Gi0/2

99 Management

100 staff active

200 student active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

How many of these VLANs are present by default?

1. Issue the show interfaces trunk command on each switch. If trunking was configured properly in Labs 10-1, Fast Ethernet 0/7–0/12 should be in trunking mode on all switches.

DLS1# **show interfaces trunk**

Port Mode Encapsulation Status Native vlan

Fa0/7 on 802.1q trunking 666

Fa0/8 on 802.1q trunking 666

Fa0/9 on 802.1q trunking 666

Fa0/10 on 802.1q trunking 666

Fa0/11 on 802.1q trunking 666

Fa0/12 on 802.1q trunking 666

Port Vlans allowed on trunk

Fa0/7 1-4094

Fa0/8 1-4094

Fa0/9 1-4094

Fa0/10 1-4094

Fa0/11 1-4094

Fa0/12 1-4094

Port Vlans allowed and active in management domain

Fa0/7 1,99,100,200

Fa0/8 1,99,100,200

Fa0/9 1,99,100,200

Fa0/10 1,99,100,200

Fa0/11 1,99,100,200

Port Vlans allowed and active in management domain

Fa0/12 1,99,100,200

Port Vlans in spanning tree forwarding state and not pruned

Fa0/7 1,100,200

Fa0/8 1,100,200

Fa0/9 1,100,200

Fa0/10 1,100,200

Fa0/11 1,100,200

Fa0/12 1,100,200

What is the native VLAN for these trunk ports?

1. Issue the show standby brief command on DLS2.

DLS2# **show standby brief**

P indicates configured to preempt.

|

Interface Grp Pri P State Active Standby Virtual IP

Vl99 1 100 P Standby 172.16.99.3 local 172.16.99.1

Vl100 1 100 P Standby 172.16.100.3 local 172.16.100.1

Vl200 1 150 P Active local 172.16.200.3 172.16.200.1

For which VLANs is DLS2 the active router?

DLS2 is the active router for VLAN 200

What is the priority of the current root bridge for VLAN 200?

Based on the output of the **show spanning-tree** command, the priority is 24776.

Step 2: Configure Routed ACLs between VLANs.

Configure router access control lists (RACLs) to separate the student and staff VLANs. The staff VLAN (100) can access the student VLAN (200), but the student VLAN does not have access to the staff VLAN for security purposes.

1. To deny the student subnet, use an extended IP access list on DLS1 and DLS2, and assign the access list to the appropriate VLAN interfaces using the **ip access-group** *acl-num*{**in** | **out**} command.

DLS1(config)# **access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 established**

DLS1(config)# **access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 echo-reply**

DLS1(config)# **access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255**

DLS1(config)# **access-list 100 permit ip any any**

DLS1(config)# **interface vlan 200**

DLS1(config-if)# **ip access-group 100 in**

DLS2(config)# **access-list 100 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 established**

DLS2(config)# **access-list 100 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 echo-reply**

DLS(config)# **access-list 100 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255**

DLS2(config)# **access-list 100 permit ip any any**

DLS2(config)# **interface vlan 100**

DLS2(config-if)# **ip access-group 100 in**

DLS2(config)# **interface vlan 200**

DLS2(config-if)# **ip access-group 100 in**

1. Check the configuration using the show ip access-list and show ip interface vlan *vlan-id* commands.

DLS1# **show access-lists**

Extended IP access list 100

10 permit tcp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 established

20 permit icmp 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255 echo-reply

30 deny ip 172.16.200.0 0.0.0.255 172.16.100.0 0.0.0.255

40 permit ip any any

DLS1# **show ip interface vlan 100**

Vlan100 is up, line protocol is up

Internet address is 172.16.100.3/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.2

Outgoing access list is not set

Inbound access list is 100

<output omitted>

1. After the access list has been applied verify the configuration in one of the following ways. Option 1 using real hosts is preferred.

Connect host PC-A to ALS1 port Fa0/5 in staff VLAN 100 and assign it IP address 172.16.100.15/24 with default gateway 172.16.100.1. Connect host PC-B to ALS2 port Fa0/5 in student VLAN 200 and assign it IP address 172.16.200.15/24 with default gateway 172.16.200.1. Ping the staff host from the student host. This ping should fail. Then ping the student host from the staff host. This ping should succeed.

What does a U signify in the output of the ping command?

The U signifies unreachable. This means that when the ping was getting routed, there was some point where a router did not have a route to the destination or that the packets were getting dropped (for example, through an access list).

Step 3: Configure VACLs.

Configure the network so that the temporary staff host cannot access the rest of the staff VLAN, yet still be able to use the default gateway of the staff subnet to connect to the rest of the network and the ISP. You can accomplish this task by using a VLAN ACL (VACL).

Konfigurácia bude na DLS12 aj DLS2.

1. Temporary staff host bude PC na ALS1 s už danou IP adresou172.16.100.15/24. Zároveň preraď PC na ALS2 do vlan 100 a priraď mu IP adresu 172.168.100.16/24 s IP DG 172.16.100.1
2. Configure an access list on DLS1 and DLS2 too, called temp-host using the ip access-list extended name command. This list defines the traffic between the host and the rest of the network. Then define the traffic using the permit ip host ip-address subnet wildcard-mask command. Note that you must be explicit about what traffic to match -- this isn't a traffic *filtering* ACL, it is a traffic *matching* ACL. If you were to leave the second line of the example below out, pings would work.

DLS1(config)# **ip access-list extended temp-host**

DLS1(config-ext-nacl)# **permit ip host 172.16.100.15 172.16.100.0 0.0.0.255**

DLS1(config-ext-nacl)# **permit icmp host 172.16.100.15 172.16.100.0 0.0.0.255**

1. The VACL is defined using a VLAN access map. Access maps are evaluated in a numbered sequence. To set up an access map, use the vlan access-map map-name seq# command. The following configuration defines an access map named block-temp, which uses the match statement to match the traffic defined in the access list and denies that traffic. You also need to add a line to the access map that allows all other traffic. If this line is not added, an implicit deny catches all other traffic and denies it.

DLS1(config)# **vlan access-map block-temp 10**

DLS1(config-access-map)# **match ip address temp-host**

DLS1(config-access-map)# **action drop**

DLS1(config-access-map)# **vlan access-map block-temp 20**

DLS1(config-access-map)# **action forward**

DLS1(config-access-map)# **exit**

1. Define which VLANs the access map should be applied to using the vlan filter map-name vlan-list vlan-ID command.

DLS1(config)# **vlan filter block-temp vlan-list 100**

1. Verify the VACL configuration using the show vlan access-map command on DLS1.

DLS1# **show vlan access-map**

Vlan access-map "block-temp" 10

Match clauses:

ip address: temp-host

Action:

drop

Vlan access-map "block-temp" 20

Match clauses:

Action:

forward

1. From HOST na ALS1, try to ping to HOST on ALS2 (172.16.100.201). The ping should not be successful.

Step 4: Configure private VLANs.

Private VLANs are an option when you have multiple devices in the same broadcast domain, but need to prevent them from communicating from each other. A good example is in a server farm where the servers do not need to receive other server's broadcast traffic.

In a sense, Private VLANs allow you to sub-divide the layer 2 broadcast domain. You are able to associate a primary VLAN with multiple secondary VLANs, while using the same IP address space for all of the devices. In this construct, the secondary VLANs can only communicate with the primary VLAN. The secondary VLANs are restricted from directly communicating with each other.

Secondary VLANs are defined as one of two types; either COMMUNITY or ISOLATED. A secondary community VLAN allows the hosts within the VLAN to communicate with one another and the primary VLAN. A secondary isolated VLAN does not allow hosts to communicate with others in the same isolated VLAN. They can only communicate with the primary VLAN.

A primary VLAN can have multiple secondary community VLANs associated with it, but only one secondary isolated VLAN.

1. The first step is to configure the switches for the primary VLAN. Based on the topology diagram, VLAN 150 will be used for the new server farm. On VTP server DLS1, add VLAN 150, name the VLAN **server-farm** and exit vlan config mode. Also configure DLS1 as the root bridge for VLANs 150, 151, and 152.

DLS1(config)# **vlan 150**

DLS1(config-vlan)# **name server-farm**

DLS1(config-vlan)# **exit**

DLS1(config)# **spanning-tree vlan 150-152 root primary**

Once this is complete, verify that VLAN 150 is preset in the database at DLS2

* + 1. Configure interface VLAN 150 at DLS1 and DLS2:

DLS1(config)# **interface vlan 150**

DLS1(config-if)# **ip address 172.16.150.1 255.255.255.0**

DLS2(config)# **interface vlan 150**

DLS2(config-if)# **ip add 172.16.150.2 255.255.255.0**

1. Configure both switches in transparent mode for VTP using the vtp mode transparent global configuration command. This is required to use PVLANs with VTP version 2.

DLS1(config)# **vtp mode transparent**

Setting device to VTP TRANSPARENT mode.

DLS2(config)# **vtp mode transparent**

Setting device to VTP TRANSPARENT mode.

1. Configure DLS1 and DLS2 to contain the new PVLANs. Secondary PVLAN 151 is an isolated VLAN used for Fast Ethernet port 0/6, while secondary PVLAN 152 is used as a community PVLAN for Fast Ethernet ports 0/18–0/20. Configure these new PVLANs in global configuration mode. You also need to associate these secondary VLANs with primary VLAN 150.

DLS1(config)# **vlan 151**

DLS1(config-vlan)# **private-vlan isolated**

DLS1(config-vlan)# **exit**

DLS1(config)# **vlan 152**

DLS1(config-vlan)# **private-vlan community**

DLS1(config-vlan)# **exit**

DLS1(config)# **vlan 150**

DLS1(config-vlan)# **private-vlan primary**

DLS1(config-vlan)# **private-vlan association 151,152**

DLS2(config)# **vlan 151**

DLS2(config-vlan)# **private-vlan isolated**

DLS2(config-vlan)# **exit**

DLS2(config)# **vlan 152**

DLS2(config-vlan)# **private-vlan community**

DLS2(config-vlan)# **exit**

DLS2(config)# **vlan 150**

DLS2(config-vlan)# **private-vlan primary**

DLS2(config-vlan)# **private-vlan association 151,152**

1. The **private-vlan mapping** interface configuration command permits PVLAN traffic to be switched through Layer 3. Normally you would include all the secondary VLANs to allow for HSRP to work, but for this example we will leave VLAN 151 off of DLS2 so we can demonstrate the isolation of VLAN 151. Configure these commands for interface VLAN 150 on DLS1 and DLS2.

DLS1(config)# **interface vlan 150**

DLS1(config-if)# **private-vlan mapping 151-152**

DLS1(config-if)# **end**

DLS2(config)# **interface vlan 150**

DLS2(config-if)# **private-vlan mapping 151-152**

DLS2(config-if)# **end**

1. Verify the creation of the secondary PVLANs and their association with the primary VLAN using the show vlan private-vlan command. Note that no ports are currently associated with these VLANs. This is expected behavior.

DLS1#**show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

150 151 isolated

150 152 community

DLS2# **show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- -----------------------------------------

150 151 isolated

150 152 community

Will hosts assigned to ports on private VLAN 151 be able to communicate directly with each other?

No. In an isolated VLAN, all ports can communicate only with ports in the primary VLAN and not each other.

**Konfig community VLAN**

1. On ALS1, configure interface FastEthernet 0/ so it is in private-vlan host mode and has association to VLAN 150

ALS(config)# **interface fastethernet 0/5**

ALS1(config-if)# **switchport mode private-vlan host**

ALS1(config-if)# **switchport private-vlan host-association 150 152**

ALS1(config-if)# **exit**

1. Use the show vlan private-vlan command and note that the ports configured are currently associated with these VLANs.

ALS1#**show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- ------------------------------------------

150 151 isolated

150 152 community Fa0/6

1. On ALS2, configure the Fast Ethernet ports that are associated with the server farm private VLANs. Fast Ethernet port 0/5 is used for the secondary community PVLAN 152. The switchport mode private-vlan host command sets the mode on the interface and the switchport private-vlan host-association primary-vlan-id secondary-vlan-id command assigns the appropriate VLANs to the interface. The following commands configure the PVLANs on DLS2.

ALS2(config)# **interface fastethernet 0/5**

ALS2(config-if)# **switchport mode private-vlan host**

ALS2(config-if)# **switchport private-vlan host-association 150 152**

ALS2(config-if)# **exit**

Over

1. Use the show vlan private-vlan command and note that the ports configured are currently associated with these VLANs.

DLS2# **show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- -----------------------------------------

150 151 isolated

150 152 community Fa0/6

1. Over konektivitu, PC na PC, pC na DLS1/2

**Konfig izolovanej VLAN**

1. On ALS2, configure the Fast Ethernet ports that are associated with the server farm private VLANs. Fast Ethernet port 0/5 is used for the secondary isolated PVLAN 151, and ports 0/18–0/20 are used for the secondary community VLAN 152. The switchport mode private-vlan host command sets the mode on the interface and the switchport private-vlan host-association primary-vlan-id secondary-vlan-id command assigns the appropriate VLANs to the interface. The following commands configure the PVLANs on DLS2.

DLS2(config)# **interface fastethernet 0/5**

DLS2(config-if)# **switchport mode private-vlan host**

DLS2(config-if)# **switchport private-vlan host-association 150 151**

DLS2(config-if)# **exit**

DLS2(config)# **interface range fa0/18 - 20**

DLS2(config-if-range)# **switchport mode private-vlan host**

DLS2(config-if-range)# **switchport private-vlan host-association 150 152**

As servers are added to Fast Ethernet 0/18–20, will these servers be allowed to hear broadcasts from each other? Explain.

1. Use the show vlan private-vlan command and note that the ports configured are currently associated with these VLANs.

DLS2# **show vlan private-vlan**

Primary Secondary Type Ports

------- --------- ----------------- -----------------------------------------

150 151 isolated Fa0/5

150 152 community Fa0/18, Fa0/19, Fa0/20

1. Over konektivitu, PC na PC, pC na DLS1/2