



Romel Cabling ▾



Home

Home > My courses > 121 - ITSP2B > 14 Protecting the Switch Infrastructure > Lesson Proper for Week 14

Lesson Proper for Week 14

PRIVATE VLANs TRUNKING VULNERABILITIES PORT SECURITY

Let's consider a scenario where we need to create a huge number of VLANs. If we do not have enough subnets to accommodate the VLANs, we won't be able to create the VLANs. Hence, from a scalability perspective, we need to create VLANs that can still be part of the same subnet. This can be fulfilled by using the concept of private VLANs.

WHAT IS A PRIVATE VLAN?

Private VLAN is a security concept that is used primarily in data centers or server farms where multiple servers from different organizations are connected together.

There may be a situation where Team A may be placing two servers, Team B would be placing another two servers, and Team C has one server, all in the same physical data center space. Obviously, Team A would to isolate their network traffic from the other teams and vice versa. This would improve their security and privacy.

We may realize at this point that to fulfill this requirement, we can create three VLANs on the switch connected to the three teams' devices. And for communication purposes, each VLAN has to be associated with a subnet. But if instead of three, there a hundred VLAN requirements, we may need to accommodate a hundred subnets, which in most cases can cause a scalability issue.

Hence to fulfill the requirement, we can go for private VLANs where we associate all the users connected to a group of switches under a single VLAN. So basically the isolation happens within a single VLAN that addresses the scalability factor of using multiple subnets.

Private VLANs can be sub-categorized into two VLANs:

- Primary VLAN



- Secondary VLAN

In private VLANs, we also come across three port types:

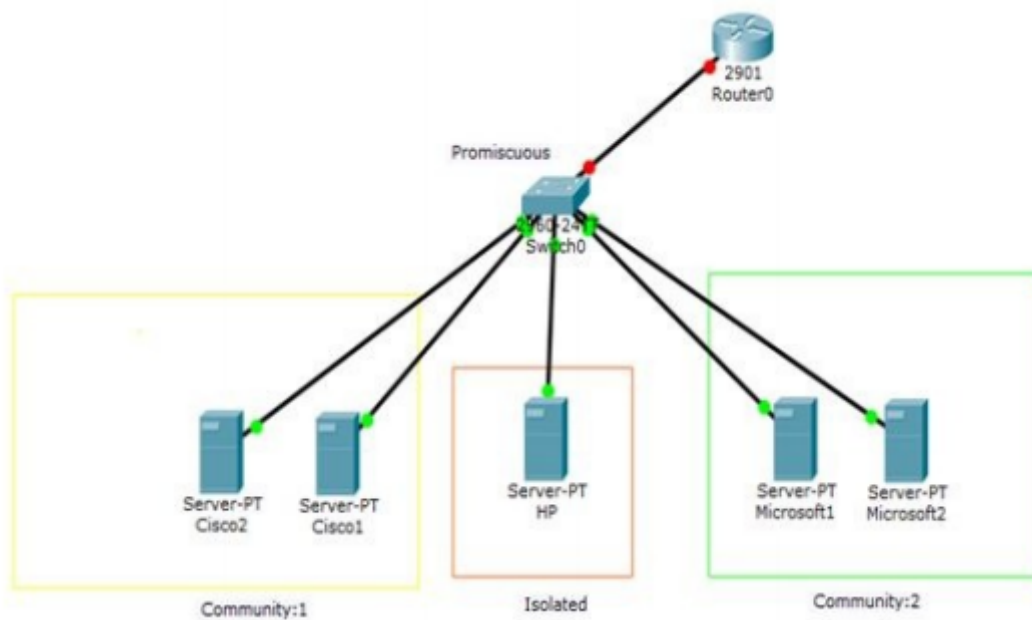
- Promiscuous
- Community
- Isolated

Generally, the primary VLAN is associated with the promiscuous port and the secondary VLAN can be used for community and isolated ports. Let's break it down.

The primary VLAN is the single VLAN that maps a group of ports under one single, private VLAN domain. Multiple secondary VLANs can be associated with the primary VLAN. The point to be noted is that the primary VLAN only would be transparent to the external world operations, such as inter-VLAN routing.

Secondary VLANs can be created for community ports and isolated ports. So what are the functionalities of these ports? Community ports are the ports that can talk to their community ports as well as the promiscuous port but not with isolated ports. Isolated ports can only communicate with the promiscuous port. Promiscuous ports are the ports that can communicate with all ports.

Let's explain that with an illustration:



In this example, we can see that the data center switch is connecting three different organizations servers, namely Cisco, HP, and Microsoft.

Since Cisco and Microsoft have two servers each, they would like to create two community VLANs so that the Cisco servers can talk to each other and avoid communication with other servers. We can expect a similar requirement for the Microsoft servers.

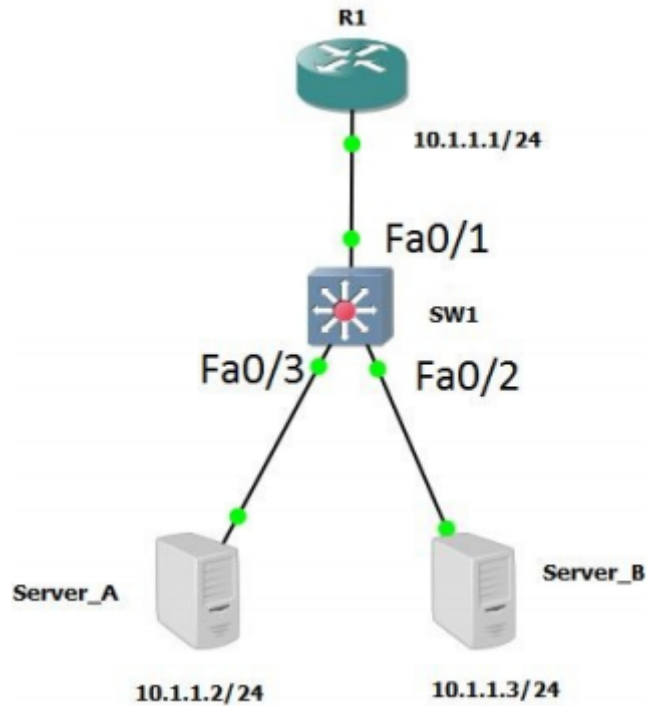
Since HP has a single server, there is no need for the server to talk to other servers. Hence HP can be associated with an isolated VLAN so that it can only communicate with the promiscuous port.



As all the users need to talk to the external world, which is through the default gateway, the switch port connected to the router should be configured as a member of the primary VLAN, which is the promiscuous port.

Private VLAN lab

In this lab, an isolated private VLAN would be created to allow two servers owned by two different organizations within the same IP range to communicate with their default gateway, but not with each other:



Before starting the private VLAN configuration, it is mandatory to configure the VTP mode as transparent. Recall that VTP is a protocol that is used to synchronize the VLAN databases on all switches. But since private VLANs are not carried by VTP, it is better to configure the mode as transparent as that would be used for local VLANs:

```
| SW1(config)# vtp mode transparent
```

Private VLANs have to be created before associating to a port, just like normal VLANs. Upon creating the VLANs, the type (isolated, community, or primary) should be provided. We are creating an isolated VLAN, 201, and mapping it to the primary VLAN, 200:



```

SW1(config)# vlan 201
SW1(config-vlan)# private-vlan isolated
SW1(config-vlan)# vlan 200
SW1(config-vlan)# private-vlan primary
SW1(config-vlan)# private-vlan association 201

```

Our completed VLAN configuration looks like this:

```

vlan 200
  private-vlan primary
  private-vlan association 201
!
vlan 201
  private-vlan isolated

```

Next, we configure the respective interfaces to be associated with the primary and isolated VLANs. The uplink port to the router would be set to the promiscuous mode, with the primary VLAN mapped to the secondary VLAN:

```

SW1(config)# interface f0/1
SW1(config-if)# switchport mode private-vlan promiscuous
SW1(config-if)# switchport private-vlan mapping 200 201

```

The two server ports will be configured in host mode wherein they would be identified as isolated VLAN ports with the 201 VLAN 201 defined:

```

SW1(config)# interface f0/3
SW1(config-if)# switchport mode private-vlan host
SW1(config-if)# switchport private-vlan host-association 200 201
SW1(config-if)# interface f0/2
SW1(config-if)# switchport mode private-vlan host
SW1(config-if)# switchport private-vlan host-association 200 201

```

At this point, our private VLAN configuration is complete. We can verify private VLAN interface assignments with the `show vlan private-vlan` command:

```

SW1# show vlan private-vlan

```

Primary	Secondary	Type	Ports
200	201	isolated	Fa0/1, Fa0/3, Fa0/2

```

SW1# show interface status

```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	10/100BaseTX	connected	200	a-full	a-100	10/100BaseTX
Fa0/2		connected	200,201	a-full	a-100	10/100BaseTX
Fa0/3		connected	200,201	a-full	a-100	10/100BaseTX
Fa0/4	10/100BaseTX	notconnect	1	auto		auto

The `show interface switchport` command is used for verifying private VLAN details per interface.

Finally, we can check whether the router can communicate with both servers, which should be successful but the servers should not communicate directly with one another:

```

R1# ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
R1# ping 10.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Server_A# ping 10.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

```



An Access Control List (ACL) is used to filter incoming or outgoing network traffic of an interface, whether it's on a Cisco Router or Adaptive Security Appliance (ASA). Without Access Control List (ACL) any type of network traffic will be allowed to flow freely between networks/interfaces and this can be a security flaw.

Access Control List is a hierarchical set of statements that have matching criteria and an action that is triggered once the matching criteria are fulfilled. If the packet's detail does not match the first line, it moves to the second line, and so on until it gets a match. If none of the lines matches the packet's detail, the packet gets dropped. This is because of the inherent characteristic of an ACL, which is called **implicit deny**.

Ideally, an Access Control List would be configured on Layer 3 devices and would be applied on Layer 3 interfaces for inspection to happen when the packet moves from one network to another. When there is a requirement for an access list to work within the same VLAN, that is where we can use the concept of the VLAN access list.

VLAN ACLs (VACLs)

VLAN ACLs (VACLs) can be used for intra-VLAN traffic filtering. For example, if within VLAN 2, a PC is not supposed to ping a server that is also on the same VLAN, but the rest of the users in VLAN 2 can be allowed, then a VACL can be implemented for VLAN 2 alone.

Steps for configuring VACL:

The following are the steps to configure VACL:

1. Create a normal access list on the switch that matches your source IP and destination IP. As usual, this can be fulfilled using a standard Access Control List or an extended access list:

```
Switch(config)# access-list <acl no> <permit| deny> <protocol> <source ip>  
<source wildcard mask><operator> <source port number><destination ip>  
<destination wildcard mask><operator><destination port number>
```

2. Create a VLAN access map. This is basically having two statements: *match* and *action*. Match is to match the ACL, and action is to either permit or deny the traffic that matches the ACL:

```
Switch(config)#vlan access-map <VACL Name> <Sequence No>  
Switch(config-access-map)#match ip address <ACL number>  
Switch(config-access-map)#action <permit|drop>
```

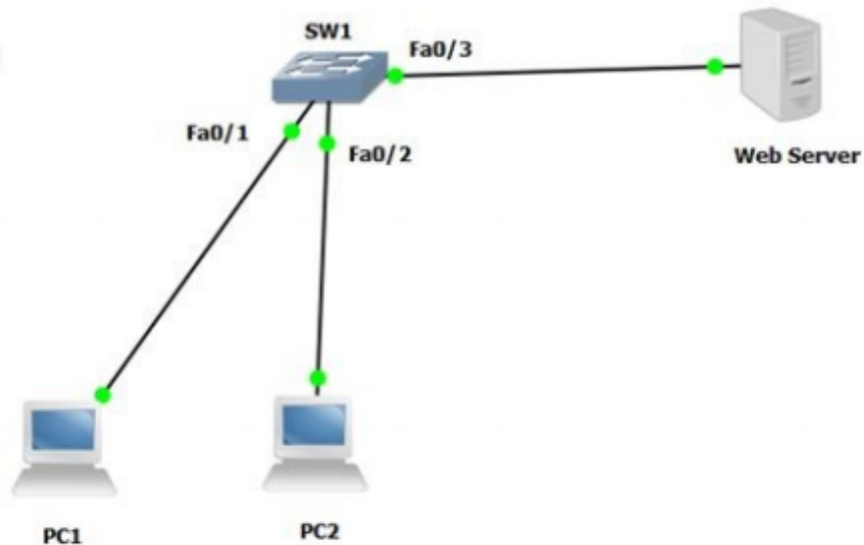
3. Associate this VLAN access list with the VLAN so that this would be used for inspection only on that VLAN:

```
Switch(config)#vlan filter <VACL Name> vlan-list <vlan id>
```

One important point to note is that the access list used in step 1 is used only for matching the IP address. It is only in step 2 that the VACL filters the traffic based on the match. The permit in the ACL is identifying the IP addresses to be matched. If there is a deny statement in the ACL, then the corresponding IP address would not be matched by the VACL:



PC1:10.1.1.1/24
PC2:10.1.1.2/24
Web Server:10.1.1.3/24



The objective of this lab is to allow us block **PC1** from accessing the web server and allowing **PC2** to access the Server. All the hosts are in VLAN 15:

```
| Sw1(config)#access-list 100 permit ip host 10.1.1.1 host 10.1.1.3
```

Access list 100 is created to match the traffic from PC1 to the web server:

```
| Sw1(config)#vlan access-map BLOCKPC1 10
| Sw1(config-access-map)#match ip address 100
| Sw1(config-access-map)#action drop
| Sw1(config)#vlan access-map BLOCKPC1 20
| Sw1(config-access-map)#action permit
```

A VACL named BLOCKPC1 is created. The first line matches the 100 ACL and the matched traffic would be dropped. Hence, if the switch receives a packet with a source address of 10.1.1.1 and a destination address of 10.1.1.3, the packet would be dropped. The second line of the VACL is an implicit permit that allows all other traffic that is not matched by ACL 100 to be forwarded. Ultimately, the PC2 traffic to the server would be allowed by the second line of the VACL:



In the step 3, the VACL named BLOCKPC1 is applied to a VLAN filter so that the traffic inspection can happen for only the VLAN 15 subnet.

As a final verification, PC1, when trying to reach the web server for any traffic, would not be allowed and PC2 would be allowed to access the server.

Thus, by implementing VACL, we are able to apply an inspection policy on a per-VLAN basis.

Trunking-related attacks

DTP is a common Layer 2 protocol that is used to negotiate a switch port to take a role as an access or a trunk link. There are two modes that are used in DTP for the negotiation process:



- **Dynamic desirable:** This mode negotiates the other side of the port to form a trunk link by sending out DTP frames. If the other side is manually configured as the access mode, then the port negotiates to form an access link. On all other combinations, this mode should be able to form a trunk link.
- **Dynamic auto:** This mode negotiates the other side of the port to form an access link ideally. But when it connects with dynamic desirable on the other side of the port, it would form a trunk as dynamic desirable is more powerful than dynamic auto.

Now, most of the Cisco switches have the factory default switch port mode settings as either dynamic desirable or dynamic auto. If an administrator leaves the switch port default settings then there is a vulnerability, that is, if an unauthorized user connects to one of the unused ports and generates an unsolicited DTP frame, the user might end up becoming a trunk. Ideally, the attacker would like to do this to identify the different VLAN traffic running on the production as well as to launch further attacks on the production network.

VLAN Hopping

This is one of the VLAN-related attacks that can be executed. The objective behind this attack is that the attacker wants to move from the given VLAN to a new VLAN where the intended victim is placed. This can be evoked by using a concept called **double-tagging**.

◀ Preliminary Activity for Week 14

Jump to...



Analysis, Application, and Exploration for Week 14 ▶



Navigation

Home



Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B



Participants



Grades

General

01 Exploring Security Threats

02 Delving into Security Toolkits

03 Intrusion Prevention System

04 Understanding Security Policies I

05 Understanding Security Policies II

06 - Preliminary Examination

07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

09 Implementing the AAA Framework

10 Implementing the AAA Framework: Implementing A...

11 Securing the Control and Management Planes


12 - Midterm Examination

13 Protecting Layer 2 Protocols


14 Protecting the Switch Infrastructure


 Preliminary Activity for Week 14

 **Lesson Proper for Week 14**

 Analysis, Application, and Exploration for Week 14

 Generalization for Week 14

 Evaluation for Week 14

 Assignment for Week 14

15 Exploring Firewall Technologies I

16 Exploring Firewall Technologies II

17 Cisco ASA

121 - WEB101 / CCS3218

Courses



Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.



COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment



visit www.bcp.edu.ph

Enrollment registration is now Ongoing





For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.

"Be trained to be the best,
Be linked to success"

 bcp-inquire@bcp.edu.ph  (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

