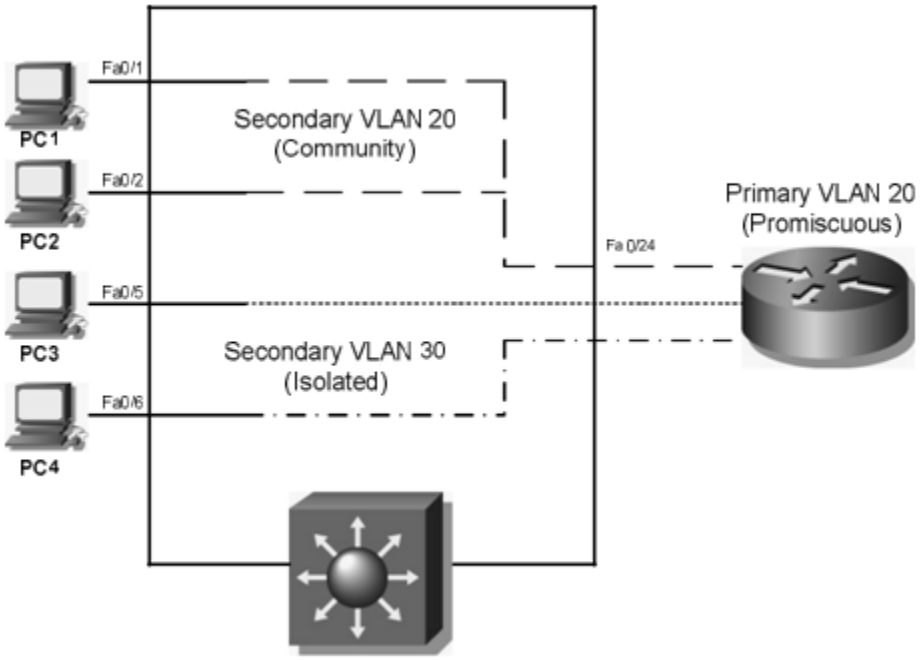
Infrastructure Security

LAB – Thực hiện Private VLAN



1. Mô tả

Trong nhiều trường hợp, các thiết bị có thể nằm trong cùng một VLAN do cùng chung một vị trí đặt máy. Vấn đề bảo mật là một trong những yếu tố khác trong thiết kế VLAN: các thiết bị khác nhau trong các VLAN khác nhau không nhận broadcast. Thêm vào đó, việc chia các máy tính ra các VLAN khác nhau sẽ dẫn đến yêu cầu dùng router hoặc các switch đa lớp giữa các subnet và các kiểu thiết bị này thường có thêm nhiều chức năng bảo mật. Trong một vài trường hợp, nhu cầu tăng tính bảo mật bằng cách tách các thiết bị bên trong một VLAN gây khó khăn trong việc quản lý địa chỉ IP. Tính năng private VLAN của Cisco giúp giải quyết vấn đề này. Private VLAN cho phép một switch tách biệt các máy tính như thể các máy tính này trên các VLAN khác nhau trong khi vẫn dùng duy nhất một IP subnet. Một tình huống phổ biến để triển khai private VLAN là trong phòng trung tâm dữ liệu (data center) của các nhà cung cấp dịch vụ. Nhà cung cấp dịch vụ có thể cài đặt một router và một switch. Sau đó, nhà cung cấp dịch vụ sẽ gắn các thiết bị từ các khách hàng khác nhau vào cùng một switch. Private VLAN cho phép nhà cung cấp dịch vụ dùng một subnet duy nhất cho cả tòa nhà, cho các cổng khác nhau của khách hàng sao cho nó không thể giao tiếp trực tiếp trong khi vẫn hỗ trợ tất cả các khách hàng trong một switch duy nhất.

Một private VLAN bao gồm các đặc điểm sau:

- Các cổng cần giao tiếp với tất cả các thiết bị khác.

- Các cổng cần giao tiếp với nhau và với các thiết bị khác, thường là router.
- Các cổng giao tiếp chỉ với những thiết bị dùng chung.

Để hỗ trợ những nhóm cổng trên, một private VLAN bao gồm một VLAN chính gọi là Primary VLAN và một hoặc nhiều VLAN phụ gọi là Secondary VLAN. Các cổng trong primary VLAN được gọi là Promiscuous có nghĩa là nó có thể gửi và nhận khung với bất kỳ cổng nào khác, kể cả với những cổng được gán vào secondary VLAN. Các thiết bị được truy cập chung, chẳng hạn như router hay server thường được đặt vào trong primary VLAN. Các cổng khác, chẳng hạn như các cổng của khách hàng sẽ gắn vào một trong những secondary VLAN

Có thể hình dung primary VLAN có tác dụng chuyên chở các lưu lượng dữ liệu của máy tính nằm trong các secondary VLAN ra ngoài. Secondary VLAN chia ra làm 2 loại: Isolated VLAN và Community VLAN.

- Isolated: bất kì cổng của switch nào gắn vào isolated VLAN sẽ chỉ có thể giao tiếp với primary VLAN mà thôi, không thể giao tiếp với các secondary VLAN khác. Thêm vào đó, nếu các máy tính thuộc cùng một isolated VLAN cũng không thể giao tiếp được với nhau mặc dù chúng cùng nằm trong một VLAN. Các máy tính này chỉ có thể giao tiếp với primary VLAN để đi ra khỏi local subnet mà thôi. Các máy tính nằm trong isolated VLAN hoàn toàn cô lập, ngoại trừ với máy tính trong primary VLAN.
- Community: các cổng của switch gắn vào community VLAN có thể nói chuyện được với nhau và với primary VLAN, nhưng đối với các secondary VLAN khác thì không được.

Tất cả secondary VLAN phải được kết hợp với một primary VLAN. Private VLAN là một loại VLAN đặc biệt nên nó chỉ có ý nghĩa cục bộ trên một switch mà thôi. Switch nào cấu hình private VLAN thì chỉ có switch đó mới có các VLAN này thôi. Giao thức VTP sẽ không quảng bá thông tin về private VLAN cho các switch khác. Khi cấu hình private VLAN thì chúng ta cũng bị yêu cầu phải thực hiện chế độ VTP transparent.

Đối với private VLAN định nghĩa ra 2 loại cổng: Promiscuous và Host. Promiscuous là cổng của switch kết nối với gateway. Quy tắc của private VLAN không áp dụng cho loại cổng này. Cổng này có thể giao tiếp với các loại primary VLAN hay secondary VLAN mà không bị giới hạn nào cả. Máy tính kết nối với cổng của switch thuộc loại isolated VLAN hay community VLAN. Cổng community chỉ có thể giao tiếp với cổng promiscuous hoặc các cổng khác nằm trong cùng một community VLAN. Đối với các máy tính nằm trong isolated VLAN thì cũng không giao tiếp được với nhau, mà chỉ có thể giao tiếp với cổng promiscuous mà thôi.

Thực hiện Private VLAN với yêu cầu:

- Tạo 3 VLAN:

+ Vlan 10: Vlan Primary.

+ Vlan 20: Vlan Secondary (Community).

+ Vlan 30: Vlan Secondary (Isolated).

- Tạo cổng:

+ Interface fa0/24: Promiscuous

+ Interface fa0/1 – fa0/5: Thuộc Vlan 20

+ Interface fa0/6 – fa0/10: Thuộc Vlan 30

Tất cả PC và router cùng mạng.

2. Cấu hình

Private VLAN chỉ được cấu hình khi switch là VTP transparent:

```
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```

Định nghĩa primary Vlan:

```
Switch(config)#vlan 10 Switch(config-vlan)#private-vlan primary
```

Định nghĩa community Vlan:

```
Switch(config)#vlan 20 Switch(config-vlan)#private-vlan community
```

Định nghĩa isolated Vlan:

```
Switch(config)#vlan 30 Switch(config-vlan)#private-vlan isolated
```

Kết hợp Vlan 20, 30 với Vlan 10:

```
Switch(config)#vlan 10
Switch(config-vlan)#private-vlan association 20,30
```

Định nghĩa cổng promiscuous:

```
Switch(config)#interface fa0/24
Switch(config-if)#switchport mode private-vlan promiscuous
Switch(config-if)#switchport private-vlan mapping 10 20,30
```

Định nghĩa cổng host cho Vlan 10, 20:

```
Switch(config)#interface range fa0/1 - 5
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 10 20
```

Định nghĩa cổng host cho Vlan 10, 30:

```
Switch(config)#interface range fa0/6 - 10
```

```
Switch(config-if-range)#switchport mode private-vlan host
Switch(config-if-range)#switchport private-vlan host-association 10 30
```

Trong trường hợp cần giao tiếp lớp 3 với những Vlan khác:

```
Switch(config)#interface vlan 10 Switch(config-if)#private-vlan mapping 20,30
```

3. Cấu hình đầy đủ

Switch

```
Building configuration...
Current configuration : 2332 bytes !
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
private-vlan primary
private-vlan association 20,30
!
vlan 20
private-vlan community
!
vlan 30
private-vlan isolated
!
!
```

```
interface FastEthernet0/1
switchport private-vlan host-association 10 20 switchport mode private-vlan
host
!
interface FastEthernet0/2
switchport private-vlan host-association 10 20 switchport mode private-vlan
host
!
interface FastEthernet0/3
switchport private-vlan host-association 10 20 switchport mode private-vlan
host
!
interface FastEthernet0/4
switchport private-vlan host-association 10 20 switchport mode private-vlan
host
!
interface FastEthernet0/5
switchport private-vlan host-association 10 20 switchport mode private-vlan
host
!
interface FastEthernet0/6
switchport private-vlan host-association 10 30 switchport mode private-vlan
host
!
interface FastEthernet0/7
switchport private-vlan host-association 10 30 switchport mode private-vlan
host
!
interface FastEthernet0/8
switchport private-vlan host-association 10 30
switchport mode private-vlan host
!
interface FastEthernet0/9
switchport private-vlan host-association 10 30 switchport mode private-vlan
host
!
```

```
interface FastEthernet0/10
switchport private-vlan host-association 10 30 switchport mode private-vlan
host
!
.....


!
interface FastEthernet0/24
switchport private-vlan mapping 10 20,30 switchport mode private-vlan
promiscuous !
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
no ip address
!
interface Vlan10
no ip address
private-vlan mapping 20,30
!
ip classless
ip http server
ip http secure-server
!
control-plane
!
line con 0
line vty 5 15
!
end
```

4. Kiểm tra

PC1 có thể giao tiếp với PC2 và router.

PC3 và PC4 không thể giao tiếp với nhau nhưng có thể giao tiếp với router.

```
Switch# sh interfaces fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 10 (VLAN0010) 20 (VLAN0020)
30 (VLAN0030)
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
10 (VLAN0010) 20 (VLAN0020) 30 (VLAN0030)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Switch# sh interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
```

```
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 10 (VLAN0010) 20 (VLAN0020)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
10 (VLAN0010) 20 (VLAN0020)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Switch# sh interfaces fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 10 (VLAN0010) 30 (VLAN0030)
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
10 (VLAN0010) 30 (VLAN0030)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Switch#sh vlan
VLAN  Name  Status      Ports
----  ------------------      ---------   -------------------------------
1     default     active      Fa0/11, Fa0/12, Fa0/13, Fa0/14
                  Fa0/15, Fa0/16, Fa0/17, Fa0/18
                  Fa0/19, Fa0/20, Fa0/21, Fa0/22
10    VLAN0010    active      Fa0/23, Gi0/1, Gi0/2
20    VLAN0020    active
30    VLAN0030    active
1002  fddi-default      act/unsup
1003  token-ring-default      act/unsup
```

```
1004  fddinet-default   act/unsup
1005  trnet-default     act/unsup
.....
Primary Secondary Type  Ports
------- --------- ----------- ---------------------------------
10    20    community   Fa0/1, Fa0/2, Fa0/3, Fa0/4,
                  Fa0/5, Fa0/24
10    30    isolated    Fa0/6, Fa0/7, Fa0/8, Fa0/9,
                  Fa0/10, Fa0/24
```