سیسکو به پارسی

آشنایی با Protected Port و Private VLAN

نوشته:

شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

انجمن سیسکو به پارسی http://forum.shafagh.com

Protected Port

چگونه روی سوییچ ارتباط مستقیم دو Interface با هم را ببندیم؟

به عبارت دیگر این دو یا چند پورت نتوانند با هم صحبت کنند اما با بقیه یا یک پورت خاص بتوانند Packet رد و بدل کنند...

در سوییچ سیسکو دو راه برای این کار وجود دارد:
Protected Port و Private VLAN

راه حل اول ساده تر است...
در مورد Private VLAN بعدا صحبت خواهیم کرد... برای Protected Port روی سوییچ به مثال زیر توجه کنید:

چهار پورت در یک VLAN داریم. سه پورت اول باید بتوانند با پورت چهارم ارتباط داشته اما یکدیگر را نبینند:

```
interface FastEthernet0/1
switchport protected
interface FastEthernet0/2
switchport protected
interface FastEthernet0/3
switchport protected
```

Cisco in Persian

روی پورت چهارم تنظیمی لازم نیست...
پورتهایی که Protected هستند با هم نمیتوانند صحبت کنند به همین سادگی.

```
Switch#sh interfaces fa 0/7 switchport
Name: Fa0/7
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
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: 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 associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL

Protected: true
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
Switch#
Switch#
```

Cisco in Persian

Private VLAN

فکر کنید سرورهای شما در Subnet ی به آدرس ۱۹۲.۱۶۸.۱.۰ قرار دارند و Firewall 192.168.1.1 است.

سرور های ۱۹۲.۱۶۸.۱.۲ و ۱۹۲.۱۶۸.۱.۳ باید همدیگر را دیده و به فایروال وصل شوند از طرفی ۱۹۲.۱۶۸.۱.۴ و ۱۹۲.۱۶۸.۱.۵ را نبینند این دو سرور آخری نیز باید ارتباط با هم داشته باشند به علاوه ارتباط با فایروال. یک سری سرور هم دارید که از ۱۹۲.۱۶۸.۱.۱۰ تا ۱۹۲.۱۶۸.۱.۳۰ تنها باید به فایروال صحبت کنند اما با هم نه.

راه حل ساده ای در مطلب قبلی ارائه کردیم (Protected Port) برای این مثال پیچیده جوابگو نیست.

اگر بخواهیم VLAN برای هر دسته سرور یا هر سرور بسازیم که کار طاقت فرسایی است چون در مقابل بایدSubnetting انجام دهیم و فایروال نیز باید پورتی در هر VLAN از جنس همان IP داشته باشد.

اگر بخواهیم از ACL یا Access-List استفاده کنیم مساله مدیریت آن سخت و پیچیده میشود... راه حل خوب راه حلی است که دست به IP ها و آدرسینگ لایه ۳ نزنیم و روی پورت ها گروه بندی تعریف کنیم. یکسری پورت مثل فایروال با همه صحبت کند... یک سری داخل گروه خود و سری دیگر با هیچ کس صحبت نکنند (غیر از فایروال(

هدف از PVLAN تفکیک لایه ای شبکه است به طوری که بهAddress ها دست نزنیم اما پورت ها تنها به پورت های خاص دسترسی داشته باشند...

از کاربرد های PVLAN در Data Center ها و شبکه های Hosting است ... سرور های متعددی را اجاره میدهند که سرورها تنها باید به روتر و Gateway یا Firewall شبکه دسترسی داشته باشند و در عین حال لازم نیست به هر سرور یک IP Subnet جداگانه اختصاص دهیم و Routing برقرار کنیم یا VLAN های متعدد را به Firewall و Gateway شبکه Trunk کنیم بلکه در لایه دو دستگاه ها را از هم جدا میکنیم.

کل این شبکه جدا شده می شود یک.Private VLAN

سه نوع Private VLAN داریم که در یک پیاده سازی ممکن است از هر سه نوع استفاده کنیم:

Primary VLAN

این VLAN در واقع در برگیرنده کل VLAN های داخل Private VLAN است و درون آن پورت های Promiscuous یا بی طرف نظیر روترو Firewall که باید جوابگوی همه باشند قرار میگیرند.

Cisco in Persian

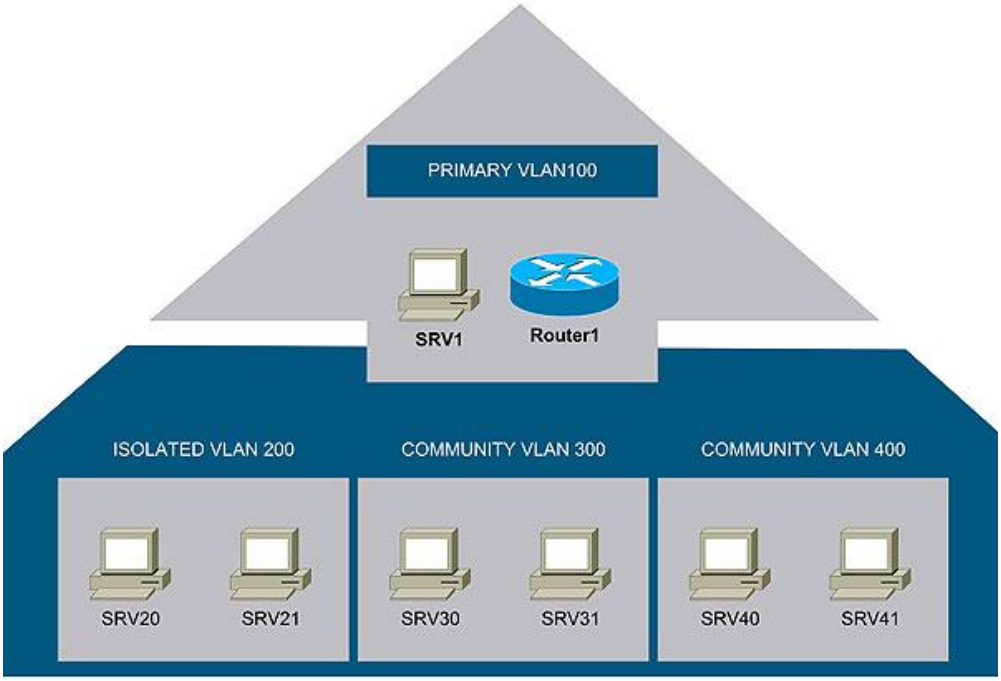
Isolated VLAN و Community VLAN دو نوع دیگر از سه نوع PVLAN می باشند که به آن Secondary VLAN میگوییم:

Isolated VLAN

برای قرار دادن پورت هایی است که با هیچ کس نتوانند ارتباط برقرار کنند غیر از.Promiscuous Port

Community VLAN

در این VLAN پورت ها با هم می توانند صحبت کنند اما با Community دیگر و پورت های داخلIsolated نمیتوانند ارتباط برقرار کرده و مثل همیشه با Promiscuous میتوانند صحبت کنند.



PRIVATE VLAN

Cisco in Persian

در شکل بالا سرور ۲۱ تنها به روتر و سرور ۱ دسترسی دارد. سرور ۲۰ هم نمیتواند ۲۱ را ببیند. از این رو یک Isolated برای هر PVLAN کافیست.

اما سرور ۳۰ به سرور ۳۱ و به روتر و سرور ۱ دسترسی دارد اما نمیتواند سرورهای ۴۰ و ۴۱ را ببیند چون در Community دیگر قرار دارند...

تنظیم PVLAN

تنظیم Private VLAN به سادگی ۴ قدم زیر انجام میگردد:

قدم اول

برای تنظیم PVLAN سوییچ را بصورت VTP Transparent تنظیم میکنیم:

```
vtp mode transparent
```

قدم دوم

VLANها را تعریف میکنیم.

```
!
vlan 100
  private-vlan primary
  private-vlan association 200,300
!
vlan 200
  private-vlan isolated
!
vlan 300
  private-vlan community
!
```

قدم سوم

پورت ها را درون VLAN ها قرار میدهیم. میتوانیم برای Switch نیز یک SVI داخل PVLAN ساخته تا ترافیک لایه ۳ را به بیرون هدایت کند.

```
interface Vlan100
 ip address 192.168.100.2 255.255.255.0
 private-vlan mapping 200,300


interface FastEthernet0/11
 switchport private-vlan mapping 100 200,300
 switchport mode private-vlan promiscuous
!
interface FastEthernet0/12
 switchport private-vlan host-association 100 200
 switchport mode private-vlan host
!
interface FastEthernet0/13
 switchport private-vlan host-association 100 200
 switchport mode private-vlan host
!
interface FastEthernet0/14
 switchport private-vlan host-association 100 300
 switchport mode private-vlan host
!
interface FastEthernet0/15
 switchport private-vlan host-association 100 300
 switchport mode private-vlan host
```

Cisco in Persian

قدم چهارم

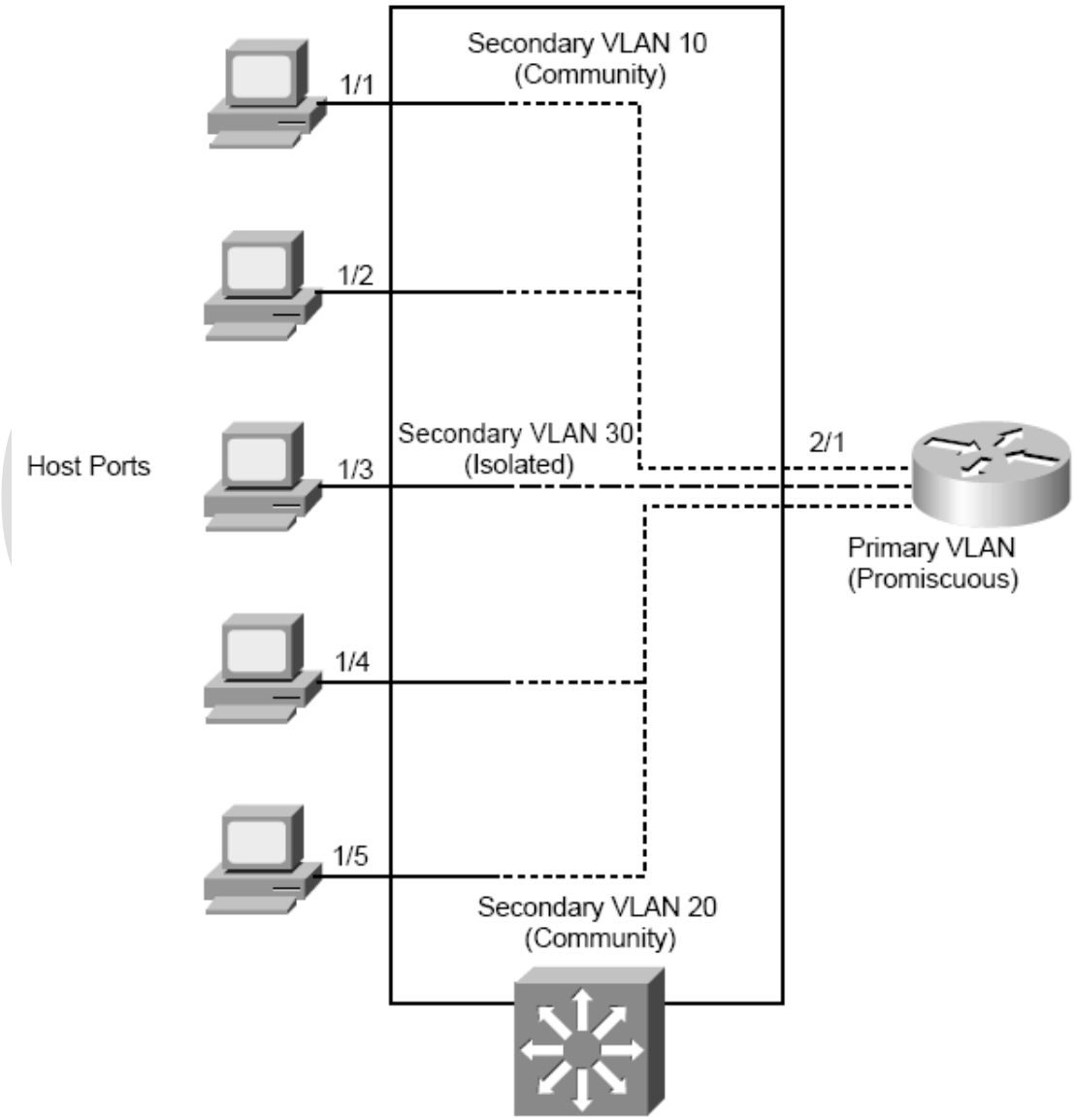
از درستی تنظیمات خود اطمینان حاصل میکنیم:

```
Switch#sh vlan private-vlan

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------
100     200       isolated          Fa0/11, Fa0/12, Fa0/13
100     300       community         Fa0/11, Fa0/14, Fa0/15


Switch#sh vlan private-vlan type

Vlan Type
---- -----------------
100  primary
200  isolated
300  community
```

Cisco in Persian

خلاصه

در یک VLAN ممکن است همه پورت ها با یکدیگر کاری نداشته باشند و تنها با روتر ارتباط برقرار کنند مثل یک Server Block در Hosting یا مثلا یک Service Provider که همه مشترکین را در یک VLAN نگاه میدارد اما در لایه دو میخواهد آنها را از هم جدا سازد.



تنظیم نمونه:

```
vlan 10
private-vlan community
!
vlan 20
private-vlan community
!
vlan 30
private-vlan isolated
!
vlan 100
private-vlan primary
private-vlan association 10,20,30
!
Switch(config)# interface range fastethernet 1/1 – 1/2
Switch(config-if)# switchport private-vlan host-association 100 10

Switch(config)# interface range fastethernet 1/4 – 1/5
Switch(config-if)# switchport private-vlan host-association 100 20

Switch(config)# interface fastethernet 1/3
Switch(config-if)# switchport private-vlan host-association 100 30


Switch(config)# interface fastethernet 2/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 100 10,20,30
```

Cisco in Persian