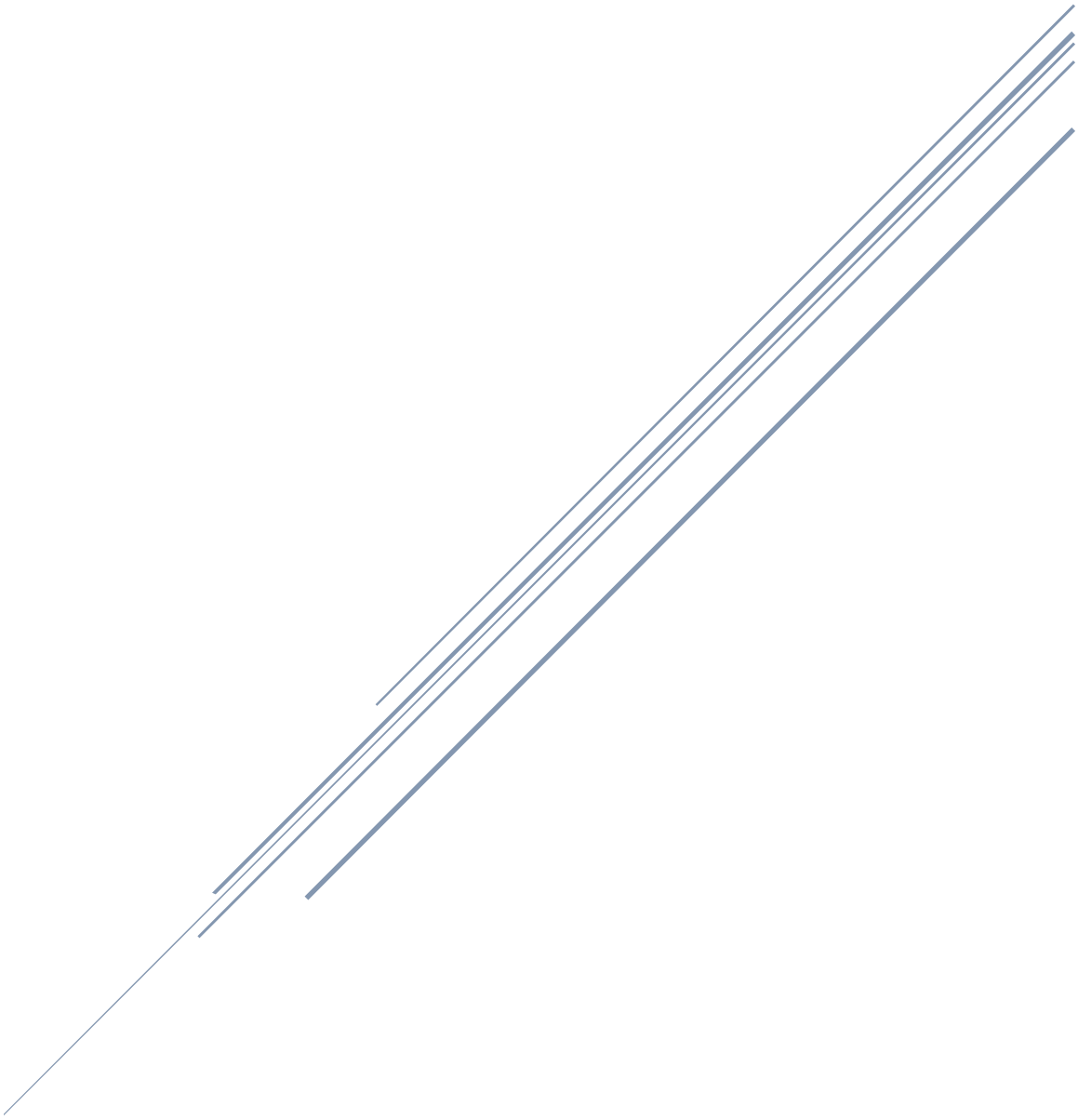
# CCIE ROUTNG & SWITCHING

Part-1



Ehsan Hosseini
ehsan.h95@gmail.com

**Blueprint topics covered in this chapter:**

This chapter covers the following subtopics from the Cisco CCIE Routing and Switching written exam blueprint. Refer to the full blueprint in Table I-1 in the Introduction for more details on the topics covered in each chapter and their context within the blueprint.

- Ethernet
- Speed
- Duplex
- Fast Ethernet
- Gigabit Ethernet
- SPAN, RSPAN, and ERSPAN
- Virtual Switch System (VSS)
- IOS-XE

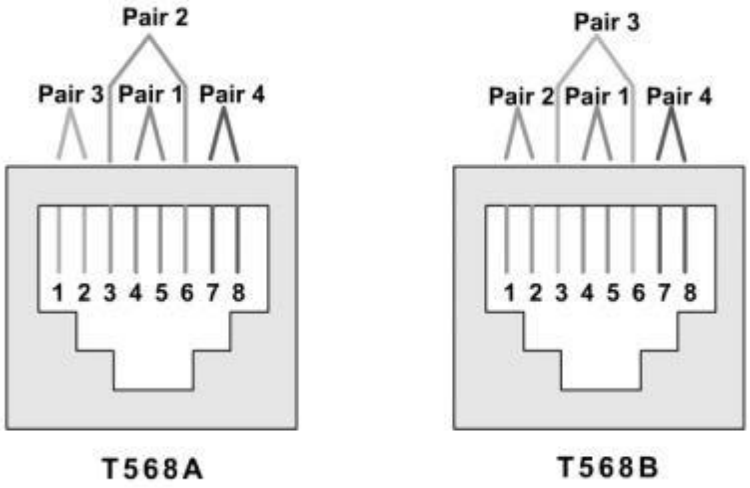
به نام خدا

## CHAPTER 1

# Ethernet Basic

### Ethernet Layer 1: Wiring, Speed, and Duplex

در cabling اترنت دو استادارد وجود دارد. این دو استاندارد نخوه چیدمان کابل را در سوکت RJ45 مشخص می کند.




این دو استاندارد جهت افزایش بهترین سرعت در لینک می باشد. بسته به اینکه نوع ارتباط چگونه باشد از یکی از دو نوع Straight-through و یا Cross-Over استفاده می کنیم.

در ارتباط از پین ها استفاده می شود.پین های 1و2 برای ارسال و 3و6 برای دریافت استفاده می شود.

نحوه استفاده باید جوری باشد که وقتی فرستنده از روی پین send ارسال میکند، گیرنده باید بر روی پین receive دریافت کند.

موقع استفاده باید متوجه بود که آیا دستگاه خصوصیتی به نام reverse circuit را دارد یا نه.(که اکثر Switchهای امروزی این قابلیت را دارند).به این صورت که وقتی روی دریافت را روی پین sendخود داشته باشد آنرا روی پین Receive ارسال می کند.این قابلیت در روترها وجود ندارد.می توان اینطور نتیجه گرفت که اگر دو دستگاه reverse circuit داشته باشند یا هر دو نداشته باشند از کابل Cross-Over استفاده میکنیم و اگر یکی از آنها این خصوصیت را داشته و دیگری نداشته باشد از Straight-through استفاده می شود.

**Table 1-2** *Ethernet Cabling Types*

Key Topic

| Type of Cable | Pinouts | Key Pins Connected |
|---|---|---|
| Straight-through | T568A (both ends) or T568B (both ends) | 1 – 1; 2 – 2; 3 – 3; 6 – 6 |
| Cross-over | T568A on one end, T568B on the other | 1 – 3; 2 – 6; 3 – 1; 6 – 2 |

در جدول بالا هر دو نوع را با شماره پین های آن مشاهده می کنید.

اما مروزه در اکثر پورت ها در سوئیچ ها خصوصیتی وجود دارد به اسم Auto-MDIX (automatic medium-dependent interface crossover) که که خود اینترفیس تشخیص می دهد بسته به نوع مدیا آیا باید reverse circuit را انجام دهد یا خیر.بنابراین بر روی پورت های که قابلیت Auto-MDIX وجود دارد، مهم نیست که از چه نوع کابلی استفاده کنید.

## Auto-negotiation, Speed, and Duplex

وقتی دو pc یا سوئیچ رو به وصل میکنیم باید speed در دو سر لینک یکسان باشد،در غیر اینصورت پورت up نمی شود، و اگر duplex یکسان نباشد یکی از طرفین پکت ها را discard می کند،و همانطور که میدانید Ethernet سرعت های مختلفی دارد. قابلیت Auto-negotiation در دوسر لینک این speed&duplex را توافق می کند. نحوه توافق دو طرف برای speed به وسیله Fast Link Puleses(FLP) می باشد،که از طریق ارسال این پالس ها با مقدار clock خود در این پالس به سرعت clock طرف مقابل پی برده و بر سر سرعت توافق کنند. این نکته هم مهم است که تواق سرعت کاملا فیزیکی می باشد و به وسیله ارسال سیگنال می باشد و توافق بر سر duplex با ارسال پکت می باشد.

## CSMA/CD

در لینک های Ethernet هم امکان collision وجود دارد. هم در لینک های dedicate و هم در shared .

زمانی که از لینک shared استفاده می کنیم(مثل اتصال به Hub)،باید از مکانیزمی جهت جلوگیری از collision استفاده کرد،و اگر اتفاق افتاد بتواند آنرا شناسایی کند. نحوه کار این مکانیزم به صورت زیر است.

1- وقتی پورتی قصد ارسال داشته باشد روی پین receive خود گوش می کند که کسی ارسال نداشته باشد.
2- در صورت مثبت بودن وضعیت شروع به ارسال می کند.
3- بعد از ارسال شروع به گوش دادن می کند که آیا collision رخ داده است یا خیر.
4- در هنگام ارسال یک کپی از محتوای ارسالی به پین receive خود نیز ارسال می کند،اگر همان باشد که ارسال کرده یعنی collision رخ نداده. ولی اگر کسی دیگر نیز ارسال داشته باشد چیزی که روی پین خود دریافت می کند متفاوت خواهد بود.
5- زمانی که collision رخ می دهد یک jamming signal ارسال میشود وه به دیگران اطلاع میدهد.اگر کسی دچار collision شده باشد مدت زمانی تصادفی صبر می کند و دوباره کار خود را انجام می دهد.

## Collision Domains and Switch Buffering

Collision Domain به مجموعه ای از اینترفیس های اترنت که احتمال collision در آن وجود دارد می گویند.اگر اینترفیسی احتمال collision در آن وجود نداشته باشد،خود اینترفیس یک collision domain مستقل را تشکیل میدهد.

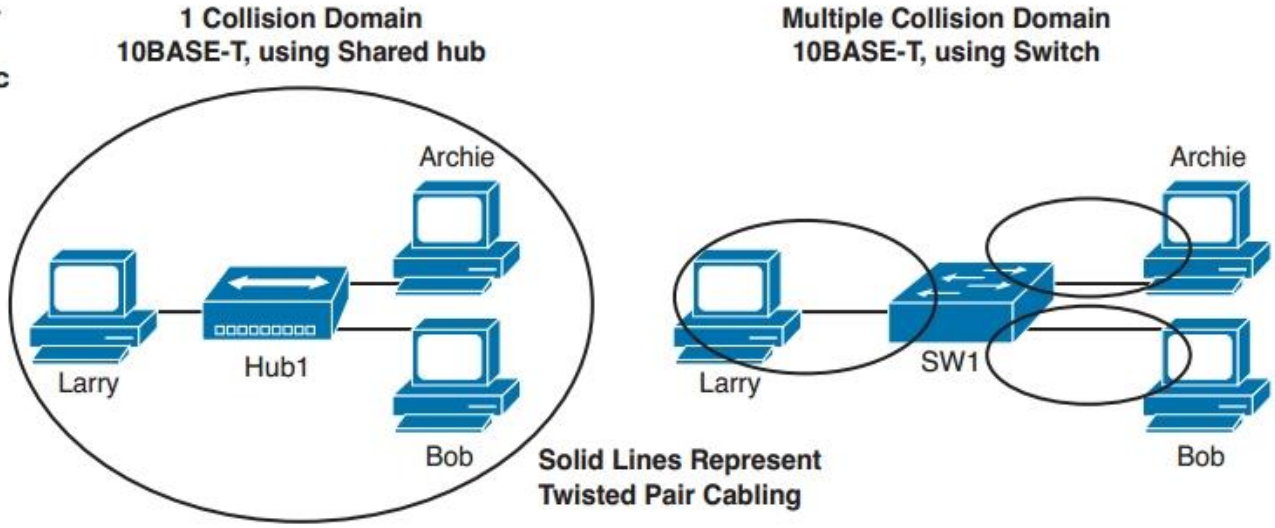



**Figure 1-2** *Collision Domains with Hubs and Switches*

وقتی پورتی از سوئیچ به Hub وصل میشود باید half-duplex باشد.با اینکار CSMA/CD نیز فعال میشود.

## Basic Switch Port Configuration

سناریو زیر را در نظر بگیرید:

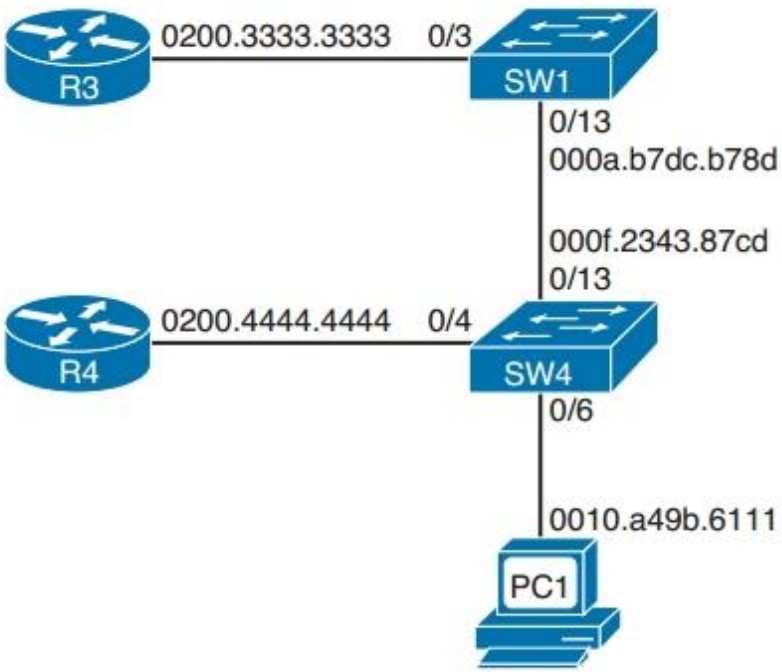



**Figure 1-3** *Simple Switched Network with Trunk*

با استفده از دستور زیر می توان نوع duplex،میزان speed، reliability ، نوع encapsulation، mac و... را مشاهده کرد.

```
switch1# show interface fa 0/13
FastEthernet0/13 is up, line protocol is up
  Hardware is Fast Ethernet, address is 000a.b7dc.b78d (bia 000a.b7dc.b78d)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s
! remaining lines omitted for brevity
! Below, Switch1's interface connecting to Switch4 is configured for 100 Mbps,
! HDX. Note that IOS rejects the first duplex command; you cannot set duplex until
! the speed is manually configured.
```

در شکل زیر سعی شده که duplex عوض شود،ولی همانطور که می بینید این دستور قبل اجرا نیست،زیرا برای تغییر duplex ابتدا باید speed را عوض کرد.

```
switch1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
switch1(config)# int fa 0/13
switch1(config-if)# duplex half
Duplex will not be set until speed is set to non-auto value
switch1(config-if)# speed 100
```

در شکل زیر نمایش پیغام عدم تطابق duplex در دو طرف مدیا را می توانید مشاهده کنید.در این سناریو یک طرف half و طرف دیگر full-duplexمی باشد.

طرف full همزمان هم امکان send و هم receive را دارد،ولی طرفی که half می باشد در زمان ارسال امکان دریافت نیز برایش وجود دارد(بخاطر duplex طرف مقابل که full است)،پس امکان collision به وجود می آید.

**Example 1-1** *Manual Setting for Duplex and Speed, with Mismatched Duplex (Continued)*

Key Topic

```
02:40:49: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/13
(not full duplex), with Switch1 FastEthernet0/13 (full duplex).
! Above, CDP messages have been exchanged over the link between switches. CDP
! exchanges information about Duplex on the link, and can notice (but not fix)
! the mismatch.
```

## Ethernet Layer 2: Framing and Addressing

همانطور که می دانید encapsulation های مختلفی برای Ethernet وجود دارد که در شکل زیر آمده است.

**Figure 1-4** *Ethernet Framing Options*

Key Topic

**Ethernet (DIX) and Revised (1997) IEEE 802.3**

| 8 | 6 | 6 | 2 | Variable | 4 |
|---|---|---|---|---|---|
| Preamble | Dest. Address | Source Address | Type/ Length | Data | FCS |

**Original IEEE Ethernet (802.3)**

| 7 | 1 | 6 | 6 | 2 | 1 | 1 | 1-2 | Variable | 4 |
|---|---|---|---|---|---|---|---|---|---|
| Preamble | SD | Dest. address | Source address | Length | DSAP | SSAP | Control | Data | FCS |
| 802.3 | | | | | 802.2 | | | | 802.3 |

**IEEE 802.3 with SNAP Header**

| 7 | 1 | 6 | 6 | 2 | 1 | 1 | 1-2 | 3 | 2 | Variable | 4 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Preamble | SD | Dest. address | Source address | Length | DSAP | SSAP | Control | OUI | TYPE | Data | FCS |
| 802.3 | | | | | 802.2 | | | SNAP | | | 802.3 |

در تمامی این encapsulation ها دو قسمت sub layer وجود دارد.

Mac: مشخصات آدرس فرستنده گیرندهء فریم در آن وجود دارد.

LLC:مشخصات خود پکتی است که در اترنت ،انکپسوله شده است را مشخص میکند،مثل اینکه نوع پکت ip است یا ipx یا ....

**در DIX**

Preamble: برای مشخص کردن شروع فریم و همچنین sync کردن clock بین دو طرف.

FCS: frame check sequence است که برای error detection استفاده می شود.

Type: نوع دیتا را مشخص میکند.

Length: طول فریم را مشخص می کند.

**در original IEEE :**

CD: شروع فریم

Preamble: sync کردن clock بین دو طرف.

DSAP: نوع پکت در مقصد

SSAP: نوع پکت در مبدا

Control: برای این است که از Ethernet هم در connection less و هم connection oriented استفاده شود.(این فیلد عملا کاربردی ندارد،برای همین در سال 1997 دوباره از اترنت dix استفاده شد)

## Switching and Bridging Logic

مکانیزم های سوئیچینگ را در مثال زیر می توان مشاهده کرد.

**Table 1-7** *LAN Switch Forwarding Behavior*

Key Topic

| Type of Address | Switch Action |
|---|---|
| Known unicast | Forwards frame out the single interface associated with the destination address |
| Unknown unicast | Floods frame out all interfaces, except the interface on which the frame was received |
| Broadcast | Floods frame identically to unknown unicasts |
| Multicast | Floods frame identically to unknown unicasts, unless multicast optimizations are configured |

وقتی سوئیچ ترافیکی را دریافت کند که مقصد آن را بداند،آنرا روی پورت مورد نظر میفرستد.

اگر ترافیکی را بیگرد که unicast باشد ولی مقصد آنرا نداند،آنرا روی همه پورت ها flood می کند.

ترافیک دریافتی broadcast را مانند unknown unicast روی همه پورت ها flood می کند.

در صورت دریافت ترافیک multicast اگر روی سوئیچ multicast switching فعال باشد آنرا روی پورت های مورد نظر ارسال می کند،در غیر اینصورت مانند unknown unicast رفتار می کند.

به صورت پیشفرض وقتی سوئیچ اولین فریم را روی یک اینترفیس دریافت کند،source mac آنرا بر روی اینترفیس خود map می کند.مثال نشان می دهد که روی چه پورتی چه mac address هایی learn شده است.

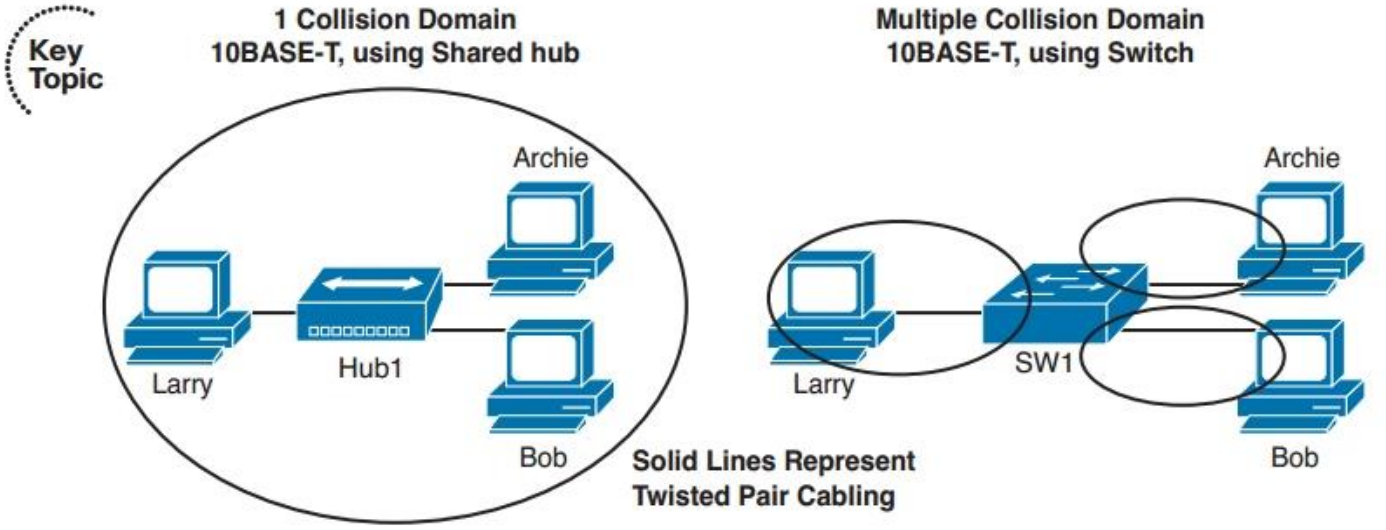



**Figure 1-2** *Collision Domains with Hubs and Switches*

**Example 1-2** *Command Output Showing MAC Address Table Learning*

```
Switch1# show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   1    000f.2343.87cd    DYNAMIC     Fa0/13
   1    0200.3333.3333    DYNAMIC     Fa0/3
   1    0200.4444.4444    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 3
! Above, Switch1's MAC address table lists three dynamically learned addresses,
! including Switch4's FA 0/13 MAC.
! Below, Switch1 pings Switch4's management IP address.
```

در صورتی که macaddressی را یاد نگرفته باشد،کافیست 1 بار آنرا ping کرده و دوباره mac-table را بررسی کنیم.

```
Switch1# ping 10.1.1.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
! Below Switch1 now knows the MAC address associated with Switch4's management IP
! address. Each switch has a range of reserved MAC addresses, with the first MAC
! being used by the switch IP address, and the rest being assigned in sequence to
! the switch interfaces - note 0xcd (last byte of 2nd address in the table above)
! is for Switch4's FA 0/13 interface, and is 13 (decimal) larger than Switch4's
! base MAC address.
Switch1# show mac-address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       ----        -----
   1    000f.2343.87c0    DYNAMIC     Fa0/13
   1    000f.2343.87cd    DYNAMIC     Fa0/13
   1    0200.3333.3333    DYNAMIC     Fa0/3
   1    0200.4444.4444    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 4
! Not shown: PC1 ping 10.1.1.23 (R3) PC1's MAC in its MAC address table
-------------------------------------------
```

در شکل بالا همانطور که مشاهده می کنید سوئیچ یک روی پورت 0/13 خود دو mac-address متفاوت را learn کرده است.اما علت چیست؟

در mac-address اول که به c0 ختم می شود، mac خود سوئیچ به حساب می آید (manageable). و mac دوم که به cd ختم می شود mac-address پورت SW4 0/13 می باشد.در واقع مقدار decimal مربوط به شماره پورت به صورت hexadecimal در انتهای mac قرار میگیرد. و مقدار 13 decimal (شماره پوت) برابر است با مقدار d در hexadecimal .

به صورت پیش فرض یک mac-address بعد از 300 ثانیه از mac address table در صورت عدم دریافت فریم،پاک می شود.با دستور زیر هم می توان این زمان را مشاهده کرد.

```
switch4# show mac-address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

برای تغییر این زمان برای یک vlan خاص می توان از دستور زیر استفاده کرد.

**SW1(config)#mac address-table aging-time 100 vlan 1**

در این مثال میزان aging-time برای vlan 1 را به 100 ثانیه کاهش دادیم.

و اگر بخواهیم بفهمیم که یک mac خاص روی کدام اینترفیس learn شده از دستور زیر استفاده می کنیم.

```
switch4# show mac-address-table address 0200.3333.3333
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0200.3333.3333    DYNAMIC     Fa0/13
Total Mac Addresses for this criterion: 1
```

## SPAN, RSPAN, and ERSPAN

توسط این مکانیزم ها می توان روی سوئیچ،کپی ترافیک یک یا چند پورت و یا Vlan را به یک پورت خاص انتقال دهید.که برای اهدافی نظیر monitoring، troubleshooting ویا جهت ارسال به سیستم تشخیص و جلوگیری از نفوذ (IPS/IDS) استفاده می شود.

در SPAN ترافیکی می خواهیم از آن کپی تهیه کنیم به پورتی بر روی همان سوئیچ ارسال می شود.

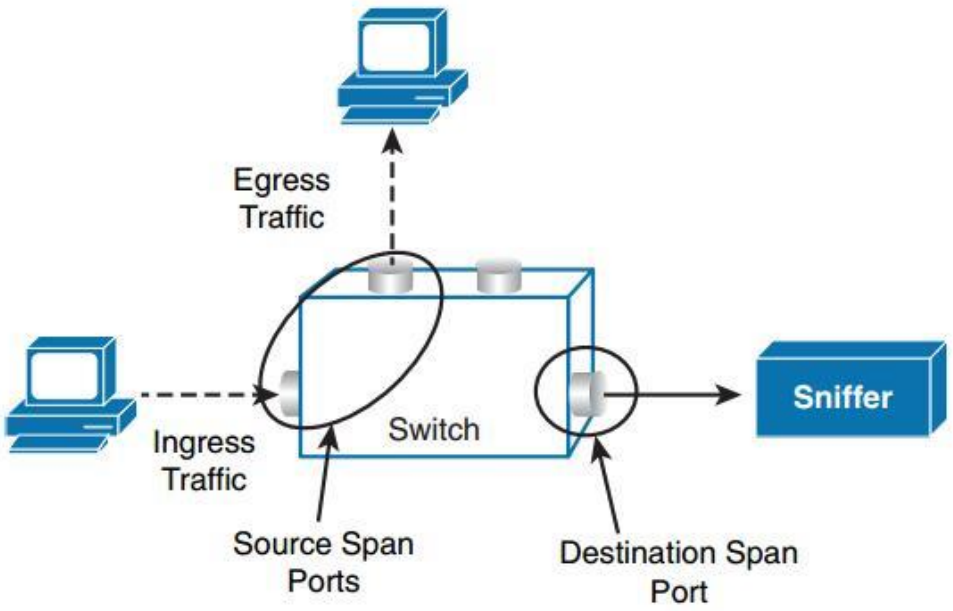



**Figure 1-7** *SPAN Topology*

در RSPAN (Remote SPAN) ترافیک روی یک سوئیچ وارد می شود،و می توان روی هر سوئیچی در شبکه این ترافیک را دریافت کرد.

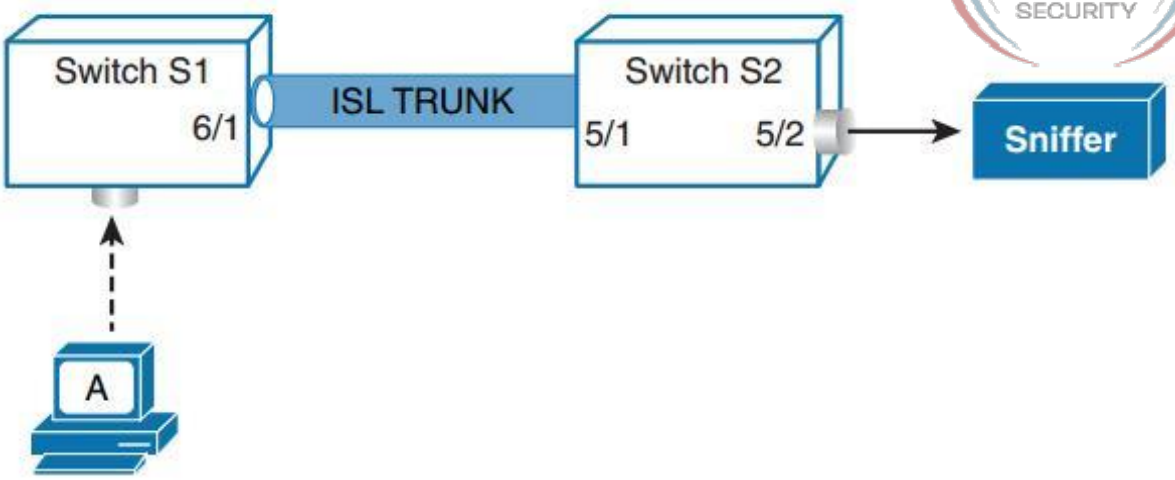



**Figure 1-8** *RSPAN Topology*

ERSPAN (Encapsulating Remote SPAN) درست مانند RSPAN عمل می کند،با این تفاوت که از نوعی تانل Encapsulation Routing برای ارسال ترافیک کپی شده استفاده می کند.

در زیر به محدودیت ها و شرط های پورت مقصد در SPAN,RSPAN,ERSPAN می پردازیم.

- وقتی یک پورت را به عنوان پورت مقصد پیکربندی میکنید،تمام پیکربندی قبلی آن پاک می شود.ولی اگر روی آن SPAN پیکربندی کرده باشید،بعد از پاک کردن دستورات SPAN،دستورات قبلی باز خواهند گشت.
- وقتی پورتی را که عضوی از Etherchannel بوده است را به پورت مقصد تبدیل کنید،آن پورت از عضویت Etherchannelخارج می شود.و اگر یک routed port باشد،کانفیگ SPAN روی آن override می شود.
- پورت مقصد از port security, 802.1x authentication, private VLAN پشتیبانی نمی کند.در واقع SPAN/ RSPAN با 802.1x نا سازگار می باشند.
- پورت مقصد از پروتکل های لایه 2 مانند VTP,DTP,STP,CDP پشتیبانی نمی کند.

در زیر به شرایط کارکرد SPAN,RSPAN,ERSPAN را بررسی می کنیم.

- پورت مبدا می تواند یک یا چند پورت و همینطور یک یا چند VLAN باشد،اما نمی تواند ترکیبی از آنها باشد.
- تا 64 پورت برای SPAN Session روی یک سوئیچ میتواند تعریف کرد که به هر Session باید یک Destination Port تعریف شود.
- پورت لایه 2 یا 3 یک سوئیچ می تواند به عنوان پورت مبدا یا مقصد برای SPAN تعریف شود.
- مواظب بار سنگین بر روی پورت مقصد در SPAN باشید.یک پورت 100Mg می تواند تا 10Mg بر روی پورت مقصد overload بر جا بگذارد. و حتی این میزان تا 100Mg می تواند افزایش پیدا کند،اگر پورت مبدا یک VLAN باشد.پس اگر ترافیک چند پورت را به یک پورت مقصد ارسال می کنید باید مواظب overload پورت مقصد باشید.
- یک Source Port نمی تواند یک Destination Port هم باشد و یا بالعکس.
- به ازای هر تعداد Source Port تنها می توان یک Destination Portداشت.

- یک پورت Trunk نیز می تواند به عنوان یک پورت مبدا برای Span یا RSPAN استفاده شود.در این حالت ترافیک تمام Vlanها روی لینک مانیتور می شوند.برای محدود کردن این مانیتورینگ می توان از دستور **filter vlan** استفاده کرد.
- ترافیکی که از دیگر vlan ها route می شوند،امکان ارسال به پورت مقصد را ندارند.

در SPAN,RSPAN,ERSPAN هم ترافیک سه نوع ترافیک پشتیبانی می شود.ترافیک ورودی،ترافیک خروجی،هر دو.

به صورت پیش فرض SPAN حالت هر دو، را پشتیبانی می کند.ولی می توان آنرا طوری پیکربندی کرد که فقط ترافیک ورودی یا فقط ترافیک خروجی را مانیتور کند.به نکات زیر توجه کنید:

- وقتی ترافیکی از یک پورت مبدا وارد شود،قبل از اینکه پارامترهای VACL,ACL,QOS روی آن تاثیر بگذارند،یک کپی از آن به پورت مقصد ارسال می شود.
- وقتی ترافیک از یک پورت مبدا خارج شود،بعد از تاثیر گذاشتن پارامترهای VACL,ACL,QOS یک کپی از آن به پورت مقصد ارسال می شود.یعنی احتمال دارد مقادیری از پکت ها مانیتور نشوند.
- وقتی ترافیک های یک Source Port را مانیتور می کنید،ترافیک های کنترلی در لایه 2 مانند CDP,spanning-tree BPDUs,VTP,DTP,PAgp frames مانیتور نمی شود.برای کپی گرفتن از این اطلاعات باید از دستور **encapsulation replicate** استفاده شود.

## SPAN Configuration

یک مثال ساده از کانفیگ SPAN را در زیر مشاهده می کنید.

**Example 1-3** *Basic SPAN Configuration Example*

```
MDF-ROC1# configure terminal
MDF-ROC1(config)# monitor session 1 source interface fa0/12
MDF-ROC1(config)# monitor session 1 destination interface fa0/24
```

در این مثال ترافیک هایی که دریافت یا ارسال می شوند،یک کپی از آن به پورت fa0/24 ارسال می شود.

حال مثال پیچیده تری از SPAN را مشاهده کنید.

**Example 1-4** *Complex SPAN Configuration Example*

```
MDF-ROC3# config term
MDF-ROC3(config)# monitor session 11 source interface fa0/18 rx
MDF-ROC3(config)# monitor session 11 source interface fa0/9 tx
MDF-ROC3(config)# monitor session 11 source interface fa0/19
MDF-ROC3(config)# monitor session 11 filter vlan 1 - 3 , 229
MDF-ROC3(config)# monitor session 11 destination interface fa0/24 encapsulation
  replicate
```

در این مثال ترافیک وارد شده از fa0/18 ،ترافیک خارج شده از fa0/9،و هر دو ترافیک ورودی و خروجی پورت fa0/19 ،به پورت fa0/24 (Trunk Port)ارسال می شود.همانطور که مشخص است،ترافیک vlanهای 1,2,3,299 روی لینک فیلتر شده است.

## RSPAN Configuration

به مثال زیر توجه کنید:

**Example 1-5** *RSPAN Configuration Example*

```
IDF-SYR1# config term
IDF-SYR1(config)# vlan 199
IDF-SYR1(config-vlan)# remote span
IDF-SYR1(config-vlan)# exit
IDF-SYR1(config)# monitor session 3 source vlan 66 - 68 rx
IDF-SYR1(config)# monitor session 3 destination remote vlan 199
!Now moving to IDF-SYR2:
IDF-SYR2# config term
IDF-SYR2(config)# vlan 199
IDF-SYR2(config-vlan)# remote span
IDF-SYR2(config-vlan)# exit
IDF-SYR2(config)# monitor session 23 source vlan 9 rx
IDF-SYR2(config)# monitor session 23 source vlan 11
IDF-SYR2(config)# monitor session 23 destination remote vlan 199
!Now moving to MDF-SYR9
MDF-SYR9# config term
MDF-SYR9(config)# vlan 199
MDF-SYR9(config-vlan)# remote span
MDF-SYR9(config-vlan)# exit
MDF-SYR9(config)# monitor session 63 source remote vlan 199
MDF-SYR9(config)# monitor session 63 destination interface fa0/24
MDF-SYR9(config)# end
```

در شکل بالا روی هر سه سوئیچ vlan 199 را به عنوان remote span vlan تعریف می کنیم.این vlan باید روی تمام پورت های trunk در مسیر اجازه رد شدن داشته باشد.(allowed)

در سوئیچ اول ترافیک ورودی از vlan 66-68 ،به vlan 199 (remote vlan) ارسال می شود.

در سوئیچ دوم ترافیک ورودی از vlan 9 و ترافیک ورودی و خروجی از vlan 11 به vlan 199 ارسال می شود.

و نهایتا در سوئیچ سوم ترافیک vlan 199 را به پورت fa0/24 جهت مانیتورینگ ارسال می کنیم.

یک نکته را باید به خاطر بسپارید. اینکه چون vlan 199 واقعا وجد ندارد، روی لینکها prune می شود.و باید آنرا به صورت دستی از حالت prune خارج کرد.یا اگر allowed نیست باید روی لینک اجازه عبور به آن داده شود.

## ERSPAN Configuration

**Example 1-6** *ERSPAN Configuration Example*

```
ASR1002(config)# monitor session 1 type erspan-source
ASR1002(config-mon-erspan-src)# source interface gig0/1/0 rx
ASR1002(config-mon-erspan-src)# no shutdown
ASR1002(config-mon-erspan-src)# destination
ASR1002(config-mon-erspan-src-dst)# erspan-id 101
ASR1002(config-mon-erspan-src-dst)# ip address 10.1.1.1
ASR1002(config-mon-erspan-src-dst)# origin ip address 172.16.1.1
```

```
!Now for the configuration of the Catalyst 6500
SW6509(config)# monitor session 2 type erspan-destination
SW6509(config-mon-erspan-dst)# destination interface gigabitEthernet2/2/1
SW6509(config-mon-erspan-dst)# no shutdown
SW6509(config-mon-erspan-dst)# source
SW6509(config-mon-erspan-dst-src)# erspan-id 101
SW6509(config-mon-erspan-dst-src)# ip address 10.1.1.1
```

در این مثال روتر ASR 1002 ترافیک ورودی روی پورت gig0/1/0 را به پورت gig2/2/1 سوئیچ 6509 ارسال می کند.این ترافیک توسط سوئیچ 6509 که توسط روتر در GRE کپسوله شده، مانیتور می شود.مانیتورینگی که در پورت GE2/2/1 وجود دارد،کل فریم اترنت را (L2-L7) خواهد دید.

ERSPAN در IOS-XE قابل پیاده سازی است که در روترهای سری ASR1000 وجود دارد.و همچنین در سری Catalyst 6500 , 7600 نیز پشتیبانی می شود.

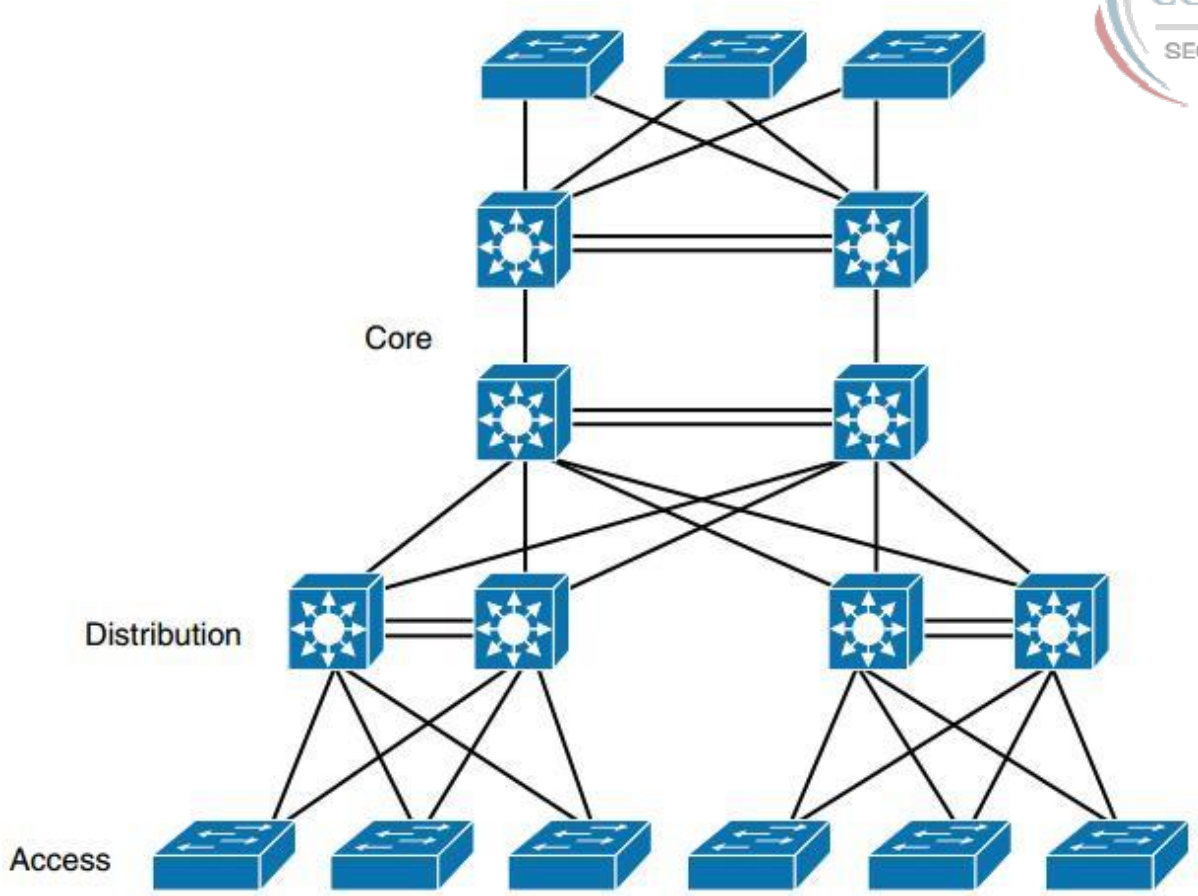
برای بررسی عملکرد SPAN,RSPAN,ERSPAN از دستور زیر می توان استفاده کرد.

**Example 1-7** *ERSPAN Verification Example*

```
ASR1002# show monitor session 1
Session 1
---------
Type                    : ERSPAN Source Session
Status                  : Admin Enabled
Source Ports            :
   RX Only            : Gi0/1/0
Destination IP Address : 10.1.1.1
MTU                    : 1464
Destination ERSPAN ID : 101
Origin IP Address     : 172.16.1.1
```

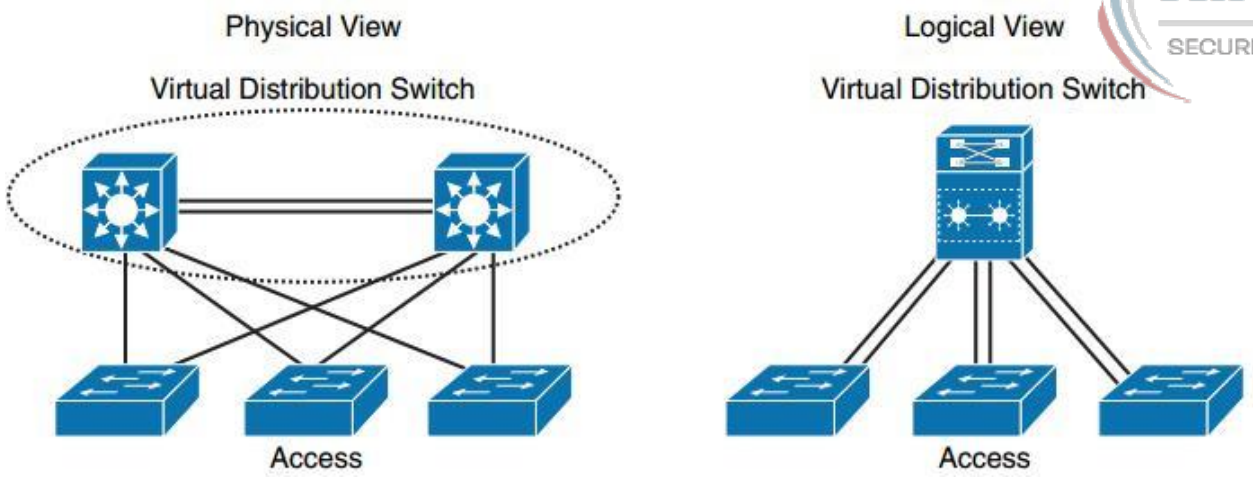
## Virtual Switch System

تمام شبکه های امروزی نیاز به دو مفهوم **Availability** و **Reliability** در دستگاه ها،ارتباطات و سرویس ها دارند.که در لایه دو شبکه می توان مانند شکل زیر این **redundancy** را ایجاد کرد.




ایجاد توپولوژی برای فراهم کردن **redundancy** باعث پیچیدگی در طراحی و عملکرد شبکه می شود.

متدی که می تواند بر این پیچیدگی چیره شود **Virtual Switching System (VSS)** نام دارد. سیسکو این تکنولوژی را برای ساده کردن مدیریت و تنظیمات شبکه های سوییچینگ ایجاد کرد.این تکنولوژی در سوئیچ های سیسکو سری **6500** و **4500** وجود دارد.شکل زیر نحوه عملکرد **VSS** را در لایه **Core** از دو دیدگاه فیزیکی و منطقی کاملا واضح نمایش می دهد.




می توان دو سوئیچ را از طریق پورت های 10G به صورت یک Stack به هم وصل و یک سوئیچ واحد جهت تنظیم در شبکه قرار داد.از مزایای ایجاد یک سوئیچ مجازی مدیریت آسان تر و کاهش در تعداد Adjacency در شبکه می باشد.زیرا به جای دو سوئیچ،یک سوئیچ واحد دیده می شود.

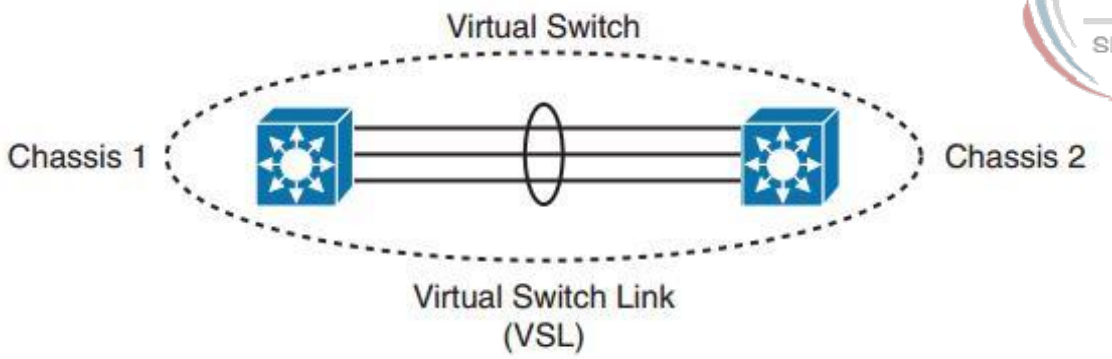
از دیگر مزایای این کار علاوه بر افزونگی(Redundancy)،Load-Balancing با استفاده از Port-Channel می باشد.در طراحی های قبلی شبکه ایجاد Ether Channel به خاطر ارتباط یک سوئیچ لایه Access با دو سوئیچ لایه Core مجاز نبود.اما از آنجا که در این توپولوژی سوئیچ Access در واقع به یک سوئیچ Core به وسیله دو لینک متصل می باشد،انجام این کار به سادگی می باشد.

## VSS Active and VSS Standby Switch

- **VSS Active:** سوییچ اصلی در **VSS** را بعنوان **Active** میشناسیم. کار این سوییچ مدیریت **VSS** است. این سوییچ **Control Plane** سوییچ **VSS** است و نقش مدیریت و اجرای پروتکل های لایه دو و سه را بعهده دارد. حتی مدیریت برق، کارت ها، کنسول و **Management Plane** بعهده این سوییچ است
- **VSS Standby:** وظیفه سوئیچ Standby چک کردن وضعیت VSS Active است تا در زمان نیاز در نقش Active ظاهر شود.اما در عین حال مشغول forward کردن ترافیک شبکه است و تنها ترافیک کنترلی را به Active ارجاع می دهد

## Virtual Switch Link

در VSS جهت ارتباط بین دو سوئیچ از VSL (Virtual Switch Link) استفاده می شود.از VSL جهت انتقال ترافیک کنترلی و دیتا بین دو سوئیچ استفاده می شود،که مجموعه ای است از لینک های Gig که تشکیل یک Port-Channel را می دهد.ساختار VSL به گونه ای است که Control Traffic و Management Traffic با اولویت بالاتری روی لینک ارسال می شود.




## Multichassis EtherChannel (EMC)

یک VSS می تواند تا 512 عدد EtherChannel را پیاده سازی کند.از آنجا که دو Channel برای ایجاد VSL (هر کدام روی یک شاسی) استفاده می شود،این تعداد در عمل به 510 عدد تغییر می کند که همین مقدار نیز بیش از نیاز های شبکه امروزی می باشد.

همانطور که گفته شد MEC به EtherChannel ی گفته می شود که بین سوئیچ مجازی متشکل از دو سوئیچ مجازی و یک دستگاه دیگر نظیر سوئیچ Access ایجاد می شود.ار آنجا که سوئیچ مجازی متشکل از دو سوئیچ است،در واقع این Channel به صورت فیزیکی بین سه دستگاه ایجاد شده و منجر به Load-Balancing و Failover در ارتباط با سوئیچ مجازی می گردد.

در زیر نمونه ای از تنظیمات EMC را می توانید ببینید:

## Access switch:

```
interface GigabitEthernet1/1/1
channel-group 10 mode on
!
interface GigabitEthernet1/1/2
channel-group 10 mode on
```

## Core switch:

```
interface Port-channel10
switchport
!
interface GigabitEthernet1/3/17
switchport
channel-group 10 mode on
!
interface GigabitEthernet2/3/17
switchport
channel-group 10 mode on
```

## Verify:

**6500SW1#sh etherchannel summary**
Number of channel-groups in use: 3
Number of aggregators: 3

Group Port-channel Protocol Ports
——+———-+———+————————————–
10 Po10(SU) - Gi1/3/17(P) Gi2/3/17(P)
100 Po100(RU) - Te1/5/4(P) Te1/6/4(P)
200 Po200(RU) - Te2/5/4(P) Te2/6/4(P)

**Switch12#sh etherchannel summary**
Number of channel-groups in use: 1
Number of aggregators: 1

Group Port-channel Protocol Ports
——+———-+———+————————————–
10 Po10(SU) - Gi1/1/1(P) Gi1/1/2(P

## VSS Configuration

برای تنظیم VSS نیاز به Supervisor مخصوص دارید.علاوه بر آن به Line Cardها و IOS که از VSS پشتیبانی کند وجود دارد.برای تست کارت های دستگاه و تطبیق سازگاری آنها می توان از دستور زیر استفاده کرد:

**6500SW#switch convert check vss-capable**

*This is a VSS capable switch.*

*VSL ports can be configured in slot: 4,5,6*

سوئیچ های 6500 بصورت پیش فرض به عنوان سوئیچ های Stand-alone یا منفرد عمل می کنند،پس باید آنها را برای VSS توسط چند قدم زیر تنظیم کرد:

1. از اجرای NFS و SSO که روش های Redundancy بین Supervisorها هستند مطمئن شوید.
2. شماره Domain و Virtual Switch را تنظیم کنید.
3. روی هر شاسی Port-Channel با شماره پورت خود را تنظیم نمایید.
4. شاسی را از حالت stand-alone به حالت Virtual Switch تبدیل کنید.

حال دستورات این چهار مرحله را در زیر مشاهده کنید:

Step1:

```
6500SW1(config)#redundancy
6500SW1(config-red)#mode sso
!
```

Step2:

```
6500SW1(config)#switch virtual domain?
Virtual switch domain number

6500SW1(config)#switch virtual domain 100
Domain ID 100 config will take effect only
after the exec command ‘switch convert mode virtual’ is issued

6500SW1(config-vs-domain)#switch 1
6500SW1(config-vs-domain)#exit

…

6500SW2(config)#switch virtual domain 100
Domain ID 100 config will take effect only
after the exec command ‘switch convert mode virtual’ is issued

6500SW2(config-vs-domain)#switch 2
6500SW2(config-vs-domain)#exit
```

Step3:

```
6500SW1(config)#int port-channel 100
6500SW1(config-if)#switch virtual link 1
6500SW1(config-if)#no shutdown
6500SW1(config-if)#exit
6500SW1(config)#int te5/4
6500SW1(config-if)#channel-group 100 mode on
6500SW1(config-if)#no shutdown
6500SW1(config)#int te6/4
6500SW1(config-if)#channel-group 100 mode on
6500SW1(config-if)#no shutdown

…

6500SW2(config)#int port-channel 200
6500SW2(config-if)#switch virtual link 2
6500SW2(config-if)#no shutdown
6500SW2(config-if)#exit
6500SW2(config)#int te5/4
6500SW2(config-if)#channel-group 200 mode on
```

```
6500SW2(config-if)#no shutdown
6500SW2(config)#int te6/4
6500SW2(config-if)#channel-group 200 mode on
6500SW2(config-if)#no shutdown
```

Step4:

```
6500SW1#switch convert?
Check check if this switch and its modules are VSS capable or not
mode mode keyword virtual or standalone

6500SW1#switch convert mode?
Stand-alone stand-alone switch

virtual virtual switch

6500SW1#switch convert mode virtual

This command will convert all interface names
to naming convention “interface-type switch-number/slot/port”,
save the running config to startup-config and
reload the switch.

NOTE: Make sure to configure one or more dual-active detection methods
once the conversion is complete and the switches have come up in VSS mode.

Do you want to proceed? [Yes/no]: yes
Converting interface names
Building configuration…
Saving converted configuration to bootflash: …
Destination filename [startup-config.converted_vs-20110705-214318]?

*** — SHUTDOWN NOW —
```

از تطبیق **PFC mode** بین دو سوییچ مطمئن شوید تا در زمان نیاز **SSO** بتواند بدرستی عمل کند:

```
6500SW1#show platform hardware pfc mode
PFC operating mode: PFC3C
```

حال پس از Reboot تنظیمات سوییچ را بررسی میکنید. دو سوییچ بصورت واحد در یک configuration روی سوییچ activeدیده میشوند.

برای Verification نیز از دستور زیر استفاده می کنیم تا از صحیح بودن Configuration مطمئن شویم.

```
6500SW1#show switch virtual
Switch mode : Virtual Switch
```

Virtual switch domain number : 100
Local switch number : 1
Local switch operational role: Virtual Switch Active
Peer switch number : 2
Peer switch operational role : Virtual Switch Standby

6500SW1#show switch virtual role

Switch Switch Status Preempt Priority Role Session ID
Number Oper(Conf) Oper(Conf) Local Remote
————————————————————————
LOCAL 1 UP FALSE(N ) 100(100) ACTIVE 0 0
REMOTE 2 UP FALSE(N ) 100(100) STANDBY 4004 1462
In dual-active recovery mode: No

6500SW1#show switch virtual link
VSL Status: UP
VSL Uptime: 43 minutes
VSL SCP Ping: Pass
VSL ICC Ping : Pass
VSL Control Link : Te1/5/4

6500SW1#show switch virtual link port-channel
Flags: D – down P – bundled in port-channel
I – stand-alone s – suspended
H – Hot-standby (LACP only)
R – Layer3 S – Layer2
U – in use N – not in use, no aggregation
f – failed to allocate aggregator

M – not in use, no aggregation due to minimum links not met
m – not in use, port not aggregated due to minimum links not met
u – unsuitable for bundling
d – default port

w – waiting to be aggregated

Group Port-channel Protocol Ports
——+———-+———+————————-
100 Po100(RU) - Te1/5/4(P) Te1/6/4(P)
200 Po200(RU) - Te2/5/4(P) Te2/6/4(P)

**Blueprint topics covered in this chapter:**

This chapter covers the following subtopics from the Cisco CCIE Routing and Switching written exam blueprint. Refer to the full blueprint in Table I-1 in the Introduction for more details on the topics covered in each chapter and their context within the blueprint.

- VLANs
- VLAN Trunking
- VLAN Trunking Protocol (VTP)
- PPP over Ethernet (PPPoE)

CHAPTER 2

# Virtual LANs and VLAN Trunking

## Virtual LANs

اولین موضوع در این فصل،Broadcast Domain می باشد.مفهوم Broadcast Domain چیست؟

در بیانی ساده می توان اینطور تعریف کرد که دستگاه های که Broadcast همدیگر را دریافت می کنند در یک Broadcast-Domain قرار دارند.برای مثال کامپوتر هایی که به یک یا چند hub متصل هستند،در یک Broadcast-Domain می باشند.در جند سوئیچ نیز اگر چند کامپیوترهایی وصل باشند،آنها نیز Broadcast packet یکدیگر را دریافت می کنند.اما در صورتی که در بین سوئیچ ها یک روتر وجود داشته باشد،دیگر آنها در یک Broadcast-Domain یکسان نیستند،زیرا روتر اجازه عبور پکت های broadcast را نمی دهد.

Broadcast می تواند مخرب باشد،به این شکل که یک کامپوترهای زیادی، Broadcast Packet را ارسال کنند،این کار می تواند عملکرد شبکه را مختل کند.

برای کاهش حجم پکت های Broadcast،از مفهومی به نام VLAN استفاده می شود.تعدادی از اینترفیس ها را عضو یک VLAN کرده و تشکیل یک Broadcast-Domain مستقل را می دهیم.

وقتی کامپوتر ها را در پورت های یک سوئیچ را در چند VLAN مختلف قرار می دهیم،آنها دیگر نمی توانند از طریق لایه 2 با هم ارتباط داشته باشند.و برای ارتباط آنها از روتر استفاده می شود.به همین خاطر باید Vlanهای مختلف رنج IP مختلف استفاده شود.ولی اگر رنج یکسان استفاده شد،می توان از Proxy IP استفاده کرد. که این کار مرسوم نمی باشد.

ولی می شود کل شبکه که در یک vlan قرار داد و به آنها رنج IPهای مختلف داد.در این حالت می توان برای ارتباط آنها اگر gateway یکی باشد،از secondary IP روی روتر استفاده کرد.که البته این کار هم مرسوم نمی باشد.

## Virtual LANs

با انجام دادن دو عمل زیر می توان چندین Broadcast-Domain در شبکه راه انداخت.

1. بر روی سوئیچ Vlan را تعریف می کنیم.
2. پورت مورد نظر خود را عضو Vlan دلخواه می کنیم.

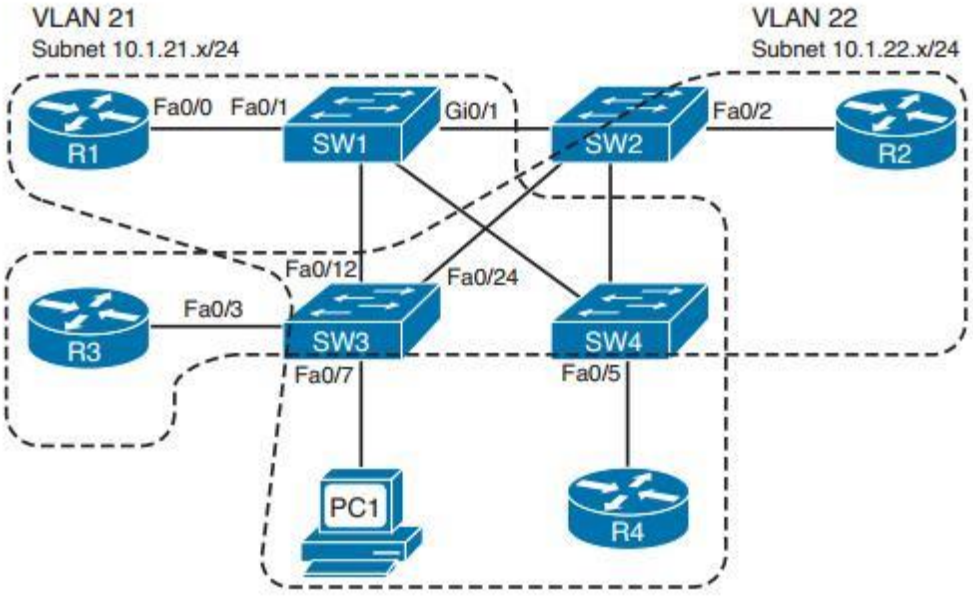
حال با دو روش ایجاد Vlan آشنا می شویم.

## Using VLAN Database Mode to Create VLANs

تعداد کل Vlanها **4095** می باشد.که به دو دسته **standard** و **extended** تقسیم می شوند.

ساخت vlan در محیط **vlan-database** محدود به رنج نرمال(standard) یعنی 1-1005 می شود.

در شکل زیر می بینید که شبکه به دو broadcast-domain تقسیم شده است.




در شکل زیر متوجه می شوید که همه پورت ها در vlan 1 قرار گرفته اند.به جز پورت 0/24 , 0/12 که trunk می باشند.

```
! Below, note that Fa0/12 and Fa0/24 are missing from the list, because they have
! dynamically become trunks, supporting multiple VLANs.

Switch3# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
```

برای ایجاد vlan در vlan database وارد محیط enable شده،و بعد از وارد کردن دستور vlan database،وارد محیط vlan database می شویم.بعد،مانند شکل vlanخود را تعریف می کنیم.

```
Switch3# vlan database
Switch3(vlan)# vlan 21
VLAN 21 added:
    Name: VLAN0021
```

در محیط vlan database می توان از دو دستور برای مشاهده وضعیت vlan استفاده کرد.

دستور اول :

```
Switch3(vlan)# show current
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No
```

با این دستور می توان وضعیت وضعیت save شده را نشان می دهد.که همانطور که می بینید vlan 21 که در بالا تعریف شده وجود ندارد.زیرا هنوز آنرا ذخیره نکردیم.

دستور دوم:

```
Switch3(vlan)# show proposed
  VLAN ISL Id: 1
    Name: default
    Media Type: Ethernet
    VLAN 802.10 Id: 100001
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
    Remote SPAN VLAN: No

  VLAN ISL Id: 21
    Name: VLAN0021
    Media Type: Ethernet
    VLAN 802.10 Id: 100021
    State: Operational
    MTU: 1500
    Backup CRF Mode: Disabled
```

این دستور وضعیت جاری و save نشده را نمایش می دهد.می بینید که vlan 21 نیز در خروجی این دستور مشخص است.

در محیط vlan database سه دستور دیگر نیز وجود دارد:

```
Switch3(vlan)# ?
VLAN database editing buffer manipulation commands:
  abort   Exit mode without applying the changes
  apply   Apply current changes and bump revision number
  exit    Apply changes, bump revision number, and exit mode
  no      Negate a command or set its defaults
  reset   Abandon current changes and reread current database
  show    Show database information
  vlan    Add, delete, or modify values associated with a single VLAN
  vtp     Perform VTP administrative functions.
```

**Abort**: بدون save کردن از محیط vlan database خارج می شود.

**Apply**: vlan را save می کند.

**Reset**: vlan را save نمی کند ولی از محیط vlan database خارج نمی شود.

حتی در هنگام تعریف vlan نیز میتوان به آن نام داد.

```
Switch3(vlan)# vlan 22 name ccie-vlan-22
VLAN 22 added:
    Name: ccie-vlan-22
```

در این محیط کلیدهای z^ مانند دستور abort عمل می کند.

با دستور زیر نیز می توان اینترفیس را عضو vlan کرد:

```
Switch3(config-if)# int fa 0/7
Switch3(config-if)# switchport mode access
Switch3(config-if)# switchport access vlan 21
Switch3(config-if)# ^Z
```

و روش دوم ایجاد vlan در محیط Configuration می باشد.

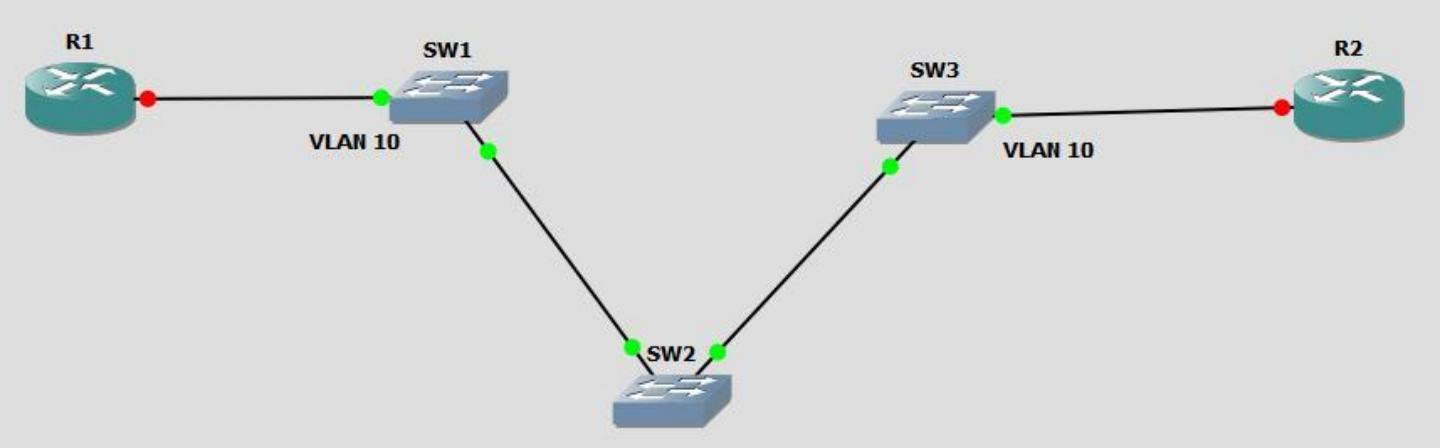
به شکل زیر دقت کنید،وقتی قبل از تعریف یک vlan،اینترفیسی را عضو آن کنیم،آن vlan بلافاصله ساخته می شود.

```
Switch3(config)# int fa 0/8
Switch3(config-if)# switchport mode access
Switch3(config-if)# switchport access vlan 31
% Access VLAN does not exist. Creating vlan 31
```

ولی در شکل زیر vlan 32 به صورت دیگر ساخته شده است:

```
Switch3(config)# vlan 32
Switch3(config-vlan)# name ccie-vlan-32
Switch3(config-vlan)# ^Z
```

در اینترفیسی از سوئیچ عضو vlan خاصی شده یا سوئیچ در مسیر عبور ترافیک vlan خاصی است،باید آن vlan روی سوئیچ تعریف شود.




مثلا در شکل بالا دو روتر 1و2 در vlan 10 قرار دارند.با اینکه هیچ پورتی از سوئیچ دو عضو vlan 10 نیست،ولی چون ترافیک این vlan از این مسیر عبور می کند،پس باید vlan 10 روی این سوئیچ نسز تعریف شود.

## Modifying the Operational State of VLANs

Vlanها می توانند دارای دو حالت باشند.حالات active و suspended، که این دو حالت در هر دو مُد vlan-database و Configuration mode می توانند مشخص شوند،که به صورت پیش فرض وقتی Vlanی ساخته شود state آن active می باشد.

در حالت suspend ترافیک آن vlan اجازه عبور نخواهند داشت.اما در active اجازه رد شدن دارند.

یک Vlan به دو راه می تواند suspend شود:

1. از طریق VTP به در سراسر Domain.

2. به صورت local روی سوئیچ بدون انتقال به سایر سوئیچ ها از طریق VTP

دستور **state suspend** در هر دو مُد vlan database و configuration mode می تواند مورد استفاده قرار گیرد.

Suspend کردن یک Vlan به صورت locally که همان Shutdown کردن یک Vlan به صورت local نیز نامیده می شود،با دستور **shutdown** انجام می شود،که تنها این دستور را می توان در Configuration mode اجرا کرد. مفهوم shutdown در vlan و Interface Vlan متفاوت می باشد و نباید اشتباه کنید.

ولی اگر دستور state suspend را وارد کنیم،در کل دامنه vlan به حالت suspend می رود.

حال اگر یک vlan که suspend شده را بخواهیم به صورت locally، active کنیم،باید از دستور no shutdown در configuration mode و در vlan context استفاده کنیم.

و اگر بخواهیم آنرا در کل domain به حالت active تغییر دهیم باید از دستور **vlan** *vlan-number* **state active** در مُد vlan-database استفاده کرد.

برای درک بهتر مطلب از چند مثال استفاده می کنیم:


در مثال بالا روی هر دو سوئیچ vlanهای 10,20,30,40,50 را می سازیم،و vtp domain را به CCIE تغییر می دهیم.

```
SW1(config)#vtp domain CCIE
Changing VTP domain name from NULL to CCIE
SW1(config)#vlan 10,20,30,40,50
SW1(config-vlan)#ex
```

اگر روی هر دو سوئیچ اطلاعات vlanها را مشاهده کنیم نتیجه زیر خواهد بود:

```
SW1(config)#do show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et0/0, Et0/1, Et0/2, Et0/3
                                                Et1/0, Et1/1, Et1/2, Et1/3
                                                Et2/0, Et2/1, Et2/2, Et2/3
                                                Et3/0, Et3/1, Et3/2, Et3/3
                                                Et4/0, Et4/1, Et4/2, Et4/3
                                                Et5/0, Et5/1, Et5/2, Et5/3
                                                Et6/0, Et6/1, Et6/2, Et6/3
                                                Et7/0, Et7/1, Et7/2, Et7/3
                                                Et8/0, Et8/1, Et8/2, Et8/3
                                                Et9/0, Et9/1, Et9/2, Et9/3
                                                Et10/0, Et10/1, Et10/2, Et10/3
                                                Et11/0, Et11/1, Et11/2, Et11/3
                                                Et12/0, Et12/1, Et12/2, Et12/3
                                                Et13/0, Et13/1, Et13/2, Et13/3
                                                Et14/0, Et14/1, Et14/2, Et14/3
                                                Et15/0, Et15/1, Et15/2, Et15/3
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
50   VLAN0050                         active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

تمام vlanهای ساخته شده در حالت active می باشند.

حال روی سوئیچ یک vlan 10 را به صورت locally به حالت suspend در می آوریم.

```
SW1(config-vlan)#vlan 10
SW1(config-vlan)#shutdown
SW1(config-vlan)#exit
```

نتیجه را رو هر دو سویچ می بینیم:

```
10   VLAN0010                         act/lshut
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
```

```
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
```

تصویر اول مربوط به سوئیچ یک و تصویر دوم مربوط به سوئیچ دوم می باشد.می بینید که در سوئیچ اول به صورت -locally shutdownنمایش داده می شود.

حال می خواهیم vlan 20 را به صورت globally به حالت suspend ببریم.

```
SW1(config)#end
SW1#
*Mar 29 21:50:35.025: %SYS-5-CONFIG_I: Configured from console by console
SW1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW1(vlan)#vlan 20 state suspend
VLAN 20 modified:
    State SUSPENDED
SW1(vlan)#apply
APPLY completed.
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#
```

در ادامه وضعیت vlan 20 را در هر دو سوئیچ خواهیم دید:

```
10   VLAN0010                         act/lshut
20   VLAN0020                         suspended
30   VLAN0030                         active
40   VLAN0040                         active
```

نتیجه در هر دو سوئیچ به صورت بالا خواهد بود.

برای active کردن یک vlan ،یکی از دو راه زیر را انجام می دهیم:

```
SW1#vlan database
% Warning: It is recommended to configure VLAN from config mode,
  as VLAN database mode is being deprecated. Please consult user
  documentation for configuring VTP/VLAN in config mode.

SW1(vlan)#vlan 20 state active
VLAN 20 modified:
    State ACTIVE
SW1(vlan)#
```

یا

```
SW1(config)#vlan 20
SW1(config-vlan)#state active
```

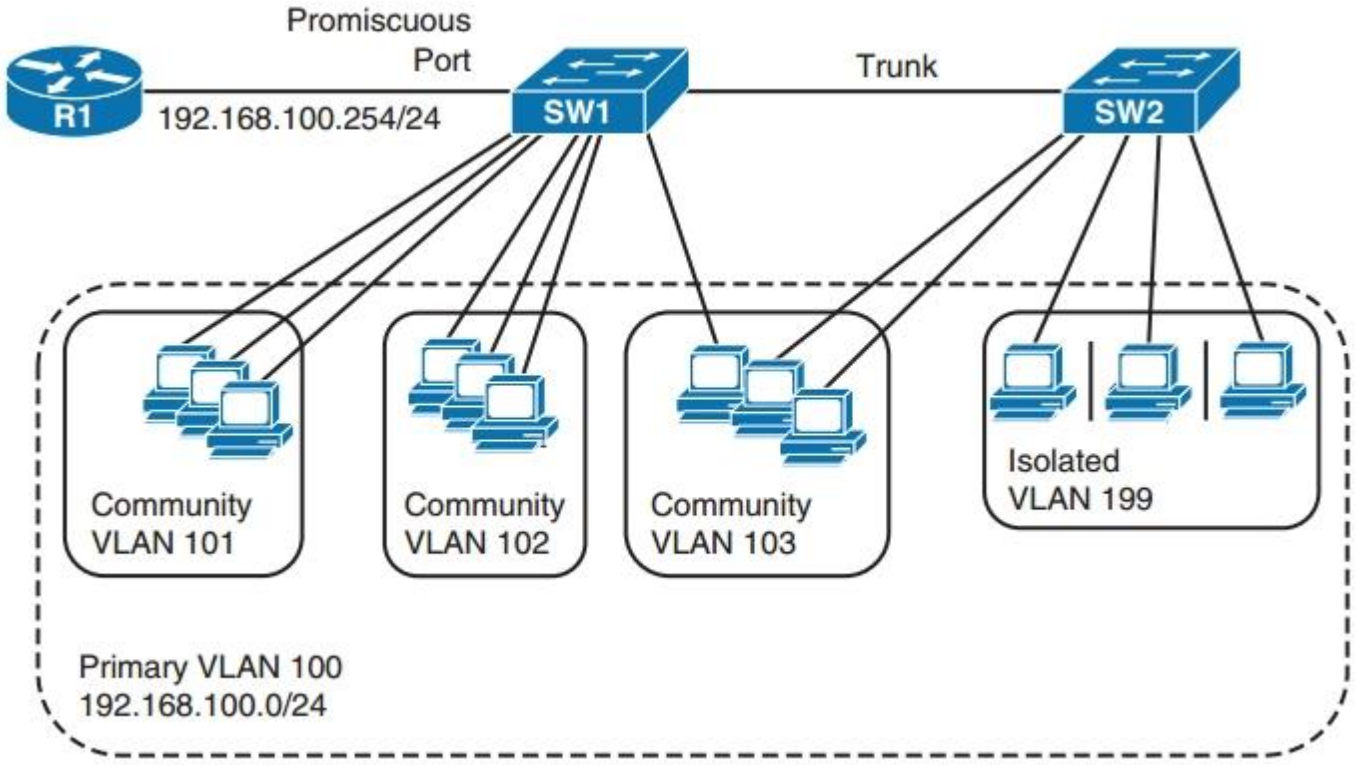
# Private VLAN

قبلا یا گرفتیم که برای ایجاد امنیت و مدیریت راحت تر، vlanهای می ساختیم و پورت ها را عضو vlanهای مختلف می کردیم.در این حالت برای اینکه vlanهای مختلف با هم ارتباط داشته باشند باید از روتر استفاده می کردند.به vlanها رنج های مختلف IP می دادیم.حال نیاز داریم که بعضی از سرورها باهم ارتباط نداشته باشند و به شبکه سرویس ارائه دهند. چه باید کرد؟

یا مثلا در service provider که در ازای هر مشتری خود یک پورت از سوئیچ را برای مشتری در نظر می گیرد.برای اینکه امنیت را بین مشتری های خود حفظ کند نباید اجازه ارتباط آنها را باهم بدهد.پس هر پورت را باید در یک vlan مجزا با رنج IP مجزا قرار دهد.

برای مشکلات بالا رها بسیار ساده تری به نام Private Vlan وجود دارد.با Private VLAN می توان بر ارتباطات یک vlan مدیریت داشت.

شکل زیر را ببینید:




در این تمام کامپوتر های متصل به سوئیچ یک و دو عضو یک vlan اصلی به نام Primary Vlan هستند.برای مدیریت ارتباط در یک vlan باید از مفهومی به نام Secondary/sub Vlan استفاده کنیم.با اینکار می توانیم در درون یک vlan اصلی به نام primary vlan سیستم های مختلف را عضو secondary vlan کنیم.

Secondary Vlan دارای دو نوع می باشد.

1. Community: در این نوع vlan ،سیستم های که عضو یک vlan باشند می توانند باهم ارتباط داشته ولی با دیگر vlanها نمی توانند ارتباط ایجاد کنند.ولی می توانند primary vlan را ببینند.

2. Isolated: دراین نوع vlan هیچ سیستمی نمی تواند با هیچ سیستم دیگری ارتباط داشته باشد.حتی با سیستم هایی که با هم در یک Isolated Vlan باشد.

در شکل بالا کاملا شخص است که سیستمی که در community Vlan 101 است،تنها می تواند سیستم های عضو این Community را ببیند و نمی تواند با سیستمی در Community Vlan 102 ارتباط داشته باشد.

اما سیستم های که در Isolated VLAN 199 هستند با هیچکس نمی توانند در ارتباط باشند.و تنها می توانند با Primary Vlan ارتباط داشته باشند.

همانطورکه در شکل می بینید یکی از پورتهای سوئیچ به R1 (gateway) متصل میباشد.این پورت که نام آن Promiscuous می باشد،تنها پورتی در شبکه است که همه سیستم های Private Vlan می توانند با این پورت ارتباط داشته باشند و از طریق این پورت از شبکه ارتباط داشته باشند.

در private Vlan یک primary vlan وجود دارد و n عدد Secondary vlan.یک Secondary Isolated، و تعداد n-1، Community.

یک نکته دیگر در خصوص Private Vlan وجود دارد و آن این است که اگر از VTP v3 استفاده نمی کنید،باید VTP Mode در تمام سوئیچ ها باید Transparent باشد.

در زیر نحوه کانفیگ دستورات Primary Vlan و Secondary Vlan را می بینید.

```
AccessSw(config)# vlan 199
AccessSw(config-vlan)# name Isolated
AccessSw(config-vlan)# private-vlan isolated
AccessSw(config-vlan)# vlan 101
AccessSw(config-vlan)# name Community1
AccessSw(config-vlan)# private-vlan community
AccessSw(config-vlan)# vlan 102
AccessSw(config-vlan)# name Community2
AccessSw(config-vlan)# private-vlan community
AccessSw(config-vlan)# vlan 103
AccessSw(config-vlan)# name Community3
AccessSw(config-vlan)# private-vlan community
AccessSw(config-vlan)# vlan 100
AccessSw(config-vlan)# name Primary1
AccessSw(config-vlan)# private-vlan primary
AccessSw(config-vlan)# private-vlan association 101-103,199
AccessSw(config-vlan)# exit
```

دستورات Secondary vlan,community Vlan , Promiscuous:

```
AccessSw(config)# interface range fa0/1 - 3
AccessSw(config-if-range)# switchport mode private-vlan host
AccessSw(config-if-range)# switchport private-vlan host-association 100 101
AccessSw(config-if-range)# interface fa0/13
AccessSw(config-if)# switchport mode private-vlan promiscuous
AccessSw(config-if)# switchport private-vlan mapping 100 101-103,199
```

برای Verification نیز از دستور زیر می توان استفاده کرد:

```
AccessSw(config)# interface range fa0/1 - 3
AccessSw(config-if-range)# switchport mode private-vlan host
AccessSw(config-if-range)# switchport private-vlan host-association 100 101
AccessSw(config-if-range)# interface fa0/13
AccessSw(config-if)# switchport mode private-vlan promiscuous
AccessSw(config-if)# switchport private-vlan mapping 100 101-103,199
```

اگر از یک SVI به عنوان gateway برای Secondary Vlanهایی که در Primary Vlan 100 هستند می خواهید استفاده کنید از دستور زیر باید استفاده کنید:

```
AccessSw(config-if)# interface Vlan100
AccessSw(config-if)# private-vlan mapping 101-103,199
AccessSw(config-if)# ip address 192.168.100.254 255.255.255.0
```

# VLAN Trunking: ISL and 802.1Q

پورت trunk پورتی است که اجازه عبور چندین vlan را می دهد.درست برعکس پورت access که تنها اجازه عبور ترافیک یک vlan را می دهد.برای ارتباط سوئیچ ها با یکدیگر از پورت trunk استفاده می شود،و برای اتصال یک سوئیچ با یک روتر بسته به شرایط هم می شود از trunk و هم از access استفاده کرد.

## ISL and 802.1Q Concepts

برای ایجاد یک لینک Trunk باید از یکی از پروتکل های ISL یا 802.1Q استفاده کرد.که با هم تفاوت هایی دارند.

ISL قبلا فقط از رنج vlan normal-range را میکرد،ولی در حال حاضر هم normal و هم Extended را پشتیبانی می کند. 802.1Q نیز از هر دو رنج VLAN پشتیبانی می کند.

ISL برای cisco است ولی 802.1Q استاندارد IEEE می باشد.

در لینک های trunk چون ترافیک چندین vlan عبور می کند،باید مشخص شود که هر ترافیک برای کدام vlan است.برای اینکار ISL از encapsulation استفاده می کند که یک 26header بایتی به پکت اضافه می کند15 بیت آن شماره vlanمی باشد،بعلاوه 4بایت trailer جدید که در مجموع 30بایت به فریم اضافه می کند.ولی 802.1Q یک 4header بایتی به اضافه می کند که به آن TAG می گویند.این tag دقیقا بعد از فیلد source-address قرار می گیرد.از این 4بایت ، 2 بایت آن مقدار 0x8100 مقدار دهی می شود که نشان دهنده 802.1Q می باشد، و در 2بایت بعدی 12 بیت آن به عنوان شماره tag در نظر گرفته می شود.

در ISL مفهومی به نام native vlan وجود ندارد، ولی 802.1Q از آن پشتیبانی می کند.

Native Vlan به vlanی گفته می شود که هنگام عبور از لینک trunk به آن tag نمی خورد.مثلا در سمت دیگر لینک اگر Deviceی باشد که تگ را نفهمد می توان در این سمت فریم را بدون تگ ارسال کرد.که پیش فرض آن vlan 1 است.

**Table 2-3** *Comparing ISL and 802.1Q*

| Feature | ISL | 802.1Q |
|---|---|---|
| VLANs supported | Normal and extended range[1] | Normal and extended range |
| Protocol defined by | Cisco | IEEE |
| Encapsulates original frame or inserts tag | Encapsulates | Inserts tag |
| Has a concept of native VLAN | No | Yes |

در شکل زیر تفاوت فریم در ISL و 802.1Q را مشاهده می کنید:

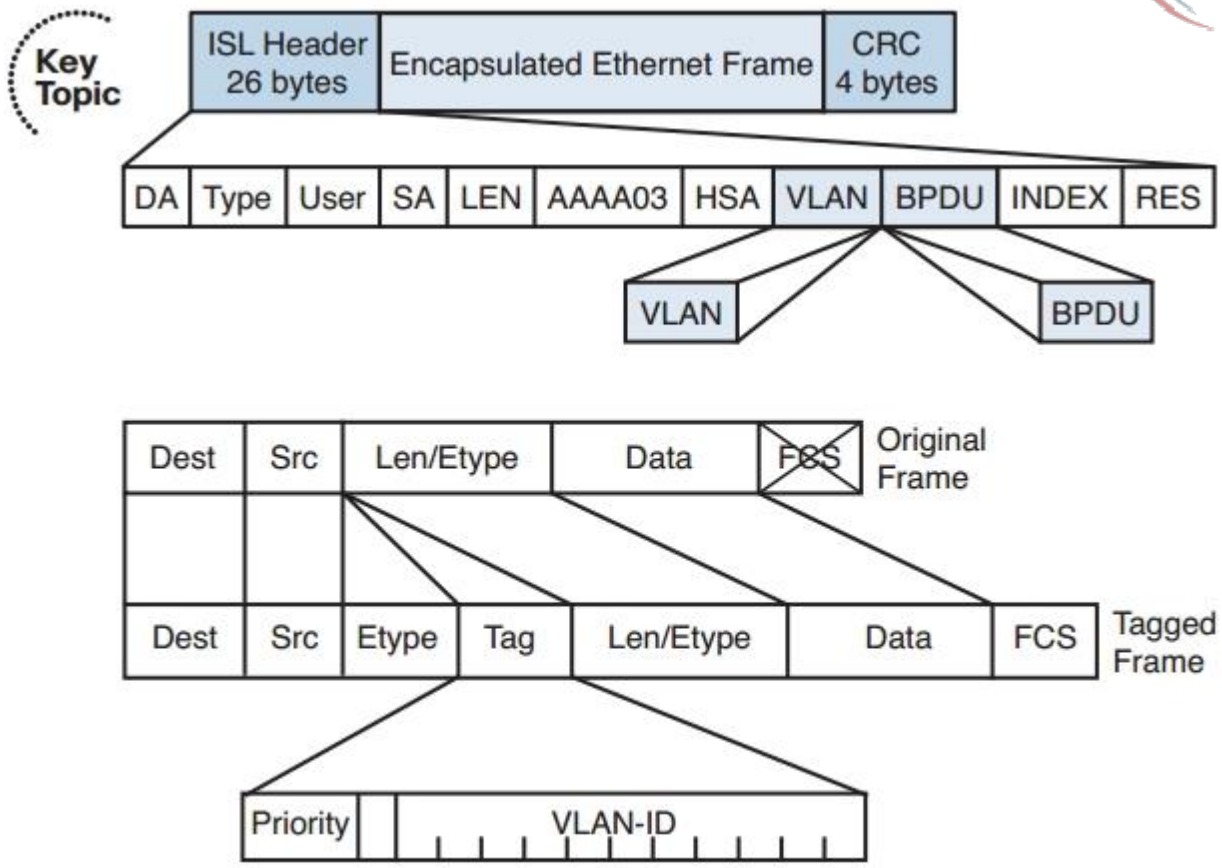



**Figure 2-4** *ISL and 802.1Q Frame Marking Methods*

ذکر یک نکته نیز ضروری است که اگر بخواهیم در 802.1q مانند ISL همه vlanها tag داشته باشند و native vlan وجود نداشته باشد باید از دستور **vlan dot1q tag native** استفاده کنیم.

## ISL and 802.1Q Configuration

سوئیچ را می توان به دو صورت dynamic و static تبدیل به trunk کرد.برای اینکه به صورت dynamic ، trunk شود از پروتکلی به نام DTP(Dynamic Trunking Protocol) استفاده می شود.این پروتکل مخصوص سیسکو است و بر روی سوئیچ های سیسکو استفاده می شود.

برای اینکه یک پورت را access کنیم از دستور **switchport mode access** استفاده میکنیم. و بعد با دستور **switchport access vlan** ***vlan-number*** آن پورت را عضو یک vlan می کنیم.

برای اینکه یک لینک را به صورت دستی trunkکنیم از دستور **switchport mode trunk** استفاده می کنیم. اما روی سوئیچ سیسکو به صورت پیشفرض مد لینک یا dynamic desirable است یا dynamic auto.در واقع روی پورت، پروتکل DTP شروع به صحبت با طرف دیگر لینگ می کند و بعد تصمیم می گیرد که trunk شود یا access. و بعد آن برای encapsulation نیز مذاکره می کند،مبنی بر اینکه 802.1Q باید trunk شوند یا ISL. اگر هر دو طرف ISL را پشتیبانی کنند، نوع encapsulation، ISL می شود.ولی اگر طرف مقابل پاسخ ندهد یا DTP را پشتیبانی نکند، پورت به در مُد access می ماند.

اما تفاوت Dynamic Desirable با Dynamic Auto در چیست؟

اگر پورت Desirable باشد شروع به مذاکره (negotiation) با طرف مقابل می کند، و اگر پورت Auto باشد منتظر می ماند تا طرف مقابل شروع به negotiation کند. بدیهی است که اگر هر دو طرف در حالت Auto باشند هیچ وقت آن لینک trunk نمی شود.

در شکل زیر دستورهای Trunking را مشاهده کنید:

Key Topic

**Table 2-4** *VLAN Trunking–Related Commands*

| Command | Function |
|---|---|
| switchport \| no switchport | Toggle defining whether to treat the interface as a switch interface (**switchport**) or as a routed interface (**no switchport**) |
| switchport mode ... | Sets DTP negotiation parameters |
| switchport trunk ... | Sets trunking parameters if the interface is trunking |
| switchport access ... | Sets nontrunking-related parameters if the interface is not trunking |
| show interfaces trunk | Summary of trunk-related information |
| show interfaces *type number* trunk | Lists trunking details for a particular interface |
| show interfaces *type number* switchport | Lists both trunking and nontrunking details for a particular interface |

با دستور no switchport می توان یک پورت لایه 2 را تبدیل به یک پورت لایه 3 کرد و به آن IP داد.و با switchport می توان پورت لایه 3 را به لایه 2 تبدیل کرد.

با دستور switch mode می توان چگونگی trunk شدن را تعیین کرد.

swtichport mode dynamic desirable : این لینک شروع به negotiation با طرف مقابل می کند.

swtichport mode dynamic auto: این لینک منتظر negotiation از طرف مقابل می ماند.

Switchport mode trunk : با این دستور مُد لینک را صراحتا trunk تعیین می کنیم.

Switchport mode access : این دستور مُد لینک را access می کند.

Switchport trunk encapsulation: با این دستور می توان نوع پروتکل مشخص کرد.(ISL , 802.1Q)

Show interface trunk: این دستور پورت های trunk نمایش می دهد.

Show interface *type number* trunk: جزئیات Trunking یک پورت را نشان می دهد.

Show interface *type number* switchport: جز مربوط به trunking و nontrunking یک پورت را نشان می دهد.

شکل زیر را در ببینید:

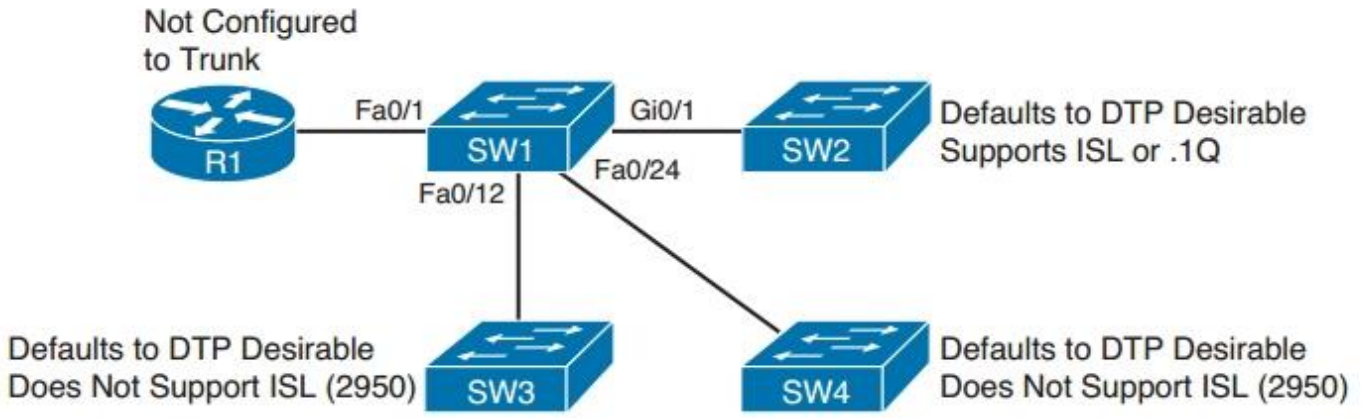



**Figure 2-5** *Trunking Configuration Reference for Example 2-6*

خروجی دستور زیر را روی سوئیچ یک را نیز مشاهده کنید:

```
Switch1# show int fa 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: dynamic desirable
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 private-vlan host-association: none
Administrative private-vlan mapping: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001

Protected: false
Unknown unicast blocked: disabled
Unknown multicast blocked: disabled

Voice VLAN: none (Inactive)
Appliance trust: none
```

Switchport: لایه پورت را نشان می دهد.اگر enable باشد پورت لایه 2 است،در غیر اینصورت پورت لایه 3 می باشد.

Administrative Mode: مُدی که روی پورت کانفیگ شده است را نمایش می دهد.در اینجا dynamic desirable است.

Operational Mode: عملکرد واقعی پورت را نشان می دهد که در اینجا access است.

Administrative trunking Encapsulation: نوع encapsulation که کانفیگ شده است را نشان می دهد، که در اینجا negotiate را نشان می دهد.یعنی نوع آن اعلام نشده و وظیفه تعیین آن با DTP است.

Operational trunking Encapsulation: نوع encapsulation جاری را نشان می دهد که در اینجا native است، زیرا اصلا trunk وجود ندارد.

Negotiation of Trunking: نشان می دهد که آیا DTP فعال است یا خیر.

حال دستور زیر را مشاهده کنید:

```
Switch1# show int gig 0/1 trunk
Port        Mode         Encapsulation  Status        Native vlan
Gi0/1       desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Gi0/1       1,21-22

Port        Vlans in spanning tree forwarding state and not pruned
Gi0/1       1,21-22
```

در این خروجی مُد لیک را Desirable، نوع encapsulation را n-isl (یعنی negotiate شده) و در status وضعیت لینک را که trunk است نشان می دهد.

Vlans allowed on trunk: لیست شماره vlanهایی که از لینک اجازه عبور دارند.

Vlans allowed and active in….: لیست vlanهای مجاز به عبور و آنها که عبور میکند را نشان می دهد.

Vlans in spanning tree forwarding…: لیست vlanهای که اجازه عبور دارن و active هستند ولی prune نیستند.

به صورت پیش فرض همه vlanها روی لینک trunk،allowed هستند،ولی اگر بخواهیم جلوی ورود ترافیک خاصی را بگیریم از دستور زیر استفاده می کنیم:

```
SW1(config-if)#switchport trunk allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list
```

می توان لیستی از vlan را وارد کرد.

add: می توان به لیست قبلی vlan جدیدی به لیست اضافه کرد.

all: همه vlanها اجازه ورود پیدا می کنند.

Except: همه vlanها جز آنها که در لیست وارد می کنیم.

None: هیچ vlanی.

Remove: vlan خاصی را از لیست حذف می کند.

دستور زیر نیز تمام پورت های trunk را با مشخصات آنها نشان می دهد:

```
Switch1# show int trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/12      desirable    n-802.1q       trunking      1
Fa0/24      desirable    n-802.1q       trunking      1
Gi0/1       desirable    n-isl          trunking      1

Port        Vlans allowed on trunk
Fa0/12      1-4094
Fa0/24      1-4094
Gi0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/12      1,21-22
Fa0/24      1,21-22
Gi0/1       1,21-22

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/12      1,21-22
Fa0/24      1,21-22
Gi0/1       1,21-22
```

همانطور که قبلا نیز گفتیم پروتکل DTP به صورت پیش فرض فعال است، و اگر بخواهیم آنرا disable کنیم از دستور زیر استفاده می کنیم:

**#Switchport nonegotiation**

اگر DTP را disable کردید،باید روی هر لینک به صورت دستی access یا trunk بودن آنرا مشخص کنید.این کار برای لینک های access توصیه می شود.

وقتی nonegotiate را فعال می کنید،باید نوع encapsulation را قبل از اینکه مُد را trunk تعیین کنید،مشخص کنید.

برای مشاهده عملکرد DTP به صورت global یا به ازای یک اینترفیس خاص از دستورهای زیر استفاده می کنیم:

**#Show dtp**

**#Show dtp interface f0/0**

در شکل زیر نیز چگونگی trunk شدن یا نشدن یک لینک را نشان می دهد که کاملا واضح است:

**Table 2-5** *Trunking Configuration Options That Lead to a Working Trunk*

| Configuration Command on One Side[1] | Short Name | Meaning | To Trunk, Other Side Must Be |
|---|---|---|---|
| switchport mode trunk | Trunk | Always trunks on this end; sends DTP to help other side choose to trunk | On, desirable, auto |
| switchport mode trunk; switchport nonegotiate | Nonegotiate | Always trunks on this end; does not send nor process DTP messages (good when other switch is a non-Cisco switch) | On |
| switchport mode dynamic desirable | Desirable | Sends DTP messages indicating dynamic mode with preferred trunking, and trunks if negotiation succeeds | On, desirable, auto |
| switchport mode dynamic auto | Auto | Sends DTP messages indicating dynamic mode with preferred access, and trunks if negotiation succeeds | On, desirable |
| switchport mode access | Access | Never trunks; can send a single DTP message when entering the access mode to help other side reach same conclusion, ceases to send and process DTP messages afterward | (Never trunks) |
| switchport mode access; switchport nonegotiate | Access (with nonegotiate) | Never trunks; does not send or process DTP messages | (Never trunks) |

با توجه با تصویر زیر اگر بخواهیم روی روتر routing داشته باشیم باید اطلاعات چندین vlan از روی لینک trunk رد شود.

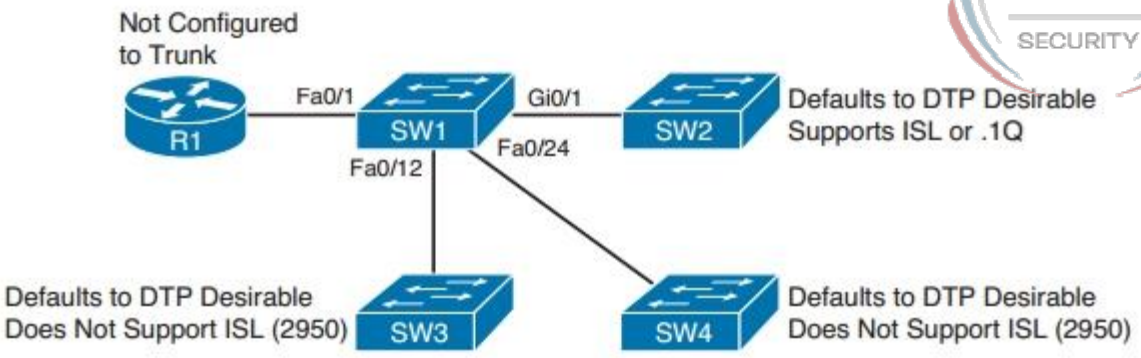



**Figure 2-5** *Trunking Configuration Reference for Example 2-6*

چون روتر DTP پشتیبانی نمی کند بهتر است روی سوئیچ DTP را disable کنیم،و به صورت دستی لینک را trunk می کنیم.سپس روی روتر به ازای هر vlan یک subinterface می سازیم و در آن encapsulation برای آن vlan را تعریف می کنیم.

```
Router1(config)# interface fa0/0
Router1(config-if)# no shutdown
Router1(config-if)# interface fa0/0.1
Router1(config-subif)# encapsulation isl 21
Router1(config-subif)# ip address 10.1.21.1 255.255.255.0
Router1(config-subif)# interface fa0/0.2
Router1(config-subif)# encapsulation isl 22
Router1(config-subif)# ip address 10.1.22.1 255.255.255.0
```

حال اگر بخواهیم یک vlan بدون tag روی لینک رد شود چه باید کرد؟

در سوئیچ بر روی لینک مورد نظر دستور **switchport trunk native vlan** *vlan-number* وارد می کنیم.

در روی رئتر به دو طریق می توان این کار را کرد،یکی اینکه روی subinterface دستور **encapsulation dot1q** *vlan-number* **native** را وارد کنیم یا اینکه IP آن را به خود اینترفیس بدهیم ، در این صورت نیز بدون tag ارسال می شود.

```
Router1(config)# interface fa0/0
Router1(config-if)# ip address 10.1.21.1 255.255.255.0
Router1(config-if)# no shutdown
Router1(config-if)# interface fa0/0.2
Router1(config-subif)# encapsulation dot1q 22
Router1(config-subif)# ip address 10.1.22.1 255.255.255.0
```

## 802.1Q-inQ Tunneling

موقعی که دو شبکه Ethernet بخواهند از طریق provider با هم ارتباط داشته باشند و ترافیک vlanهای یکدیگر را داشته باشند، درService Provider از این پروتکل جهت برقراری ارتباط لایه دو استفاده می شود. به این سرویس Metro Ethernet می گویند. برای این نوع سرویس دهی راه حل هایی وجود دارد مانند VPLS,EoMPLS,802.1Q-in-Q که دو مورد اول مربوط به دوره CCIE Service Provider می باشد، و فقط به 802.1Q-in-Q می پردازیم.

برای انتقال vlanها باید ارتباط provider با customer به صورت لایه دویی باشد نه با پروتکلIP.تا این انتقال انجام شود.

حال فرض کنیم که customer از provider برای انتقال ترافیک vlan 10 استفاده می کند.تا اینجا مشکلی نیست.مشکل از زمانی آغاز می شود که یک customer دیگر قصد ارسال ترافیک را داشته باشد،و آن customer نیز vlan 10 داشته و قصد ارسال ترافیک آن vlan را داشته باشد.

برای حل این مشکل، service provider از مکانیزمی به نام Double-Tagging استفاده می کند.یعنی به ازای هر مشتری یک tag جدید به فریم اضافه می کند.

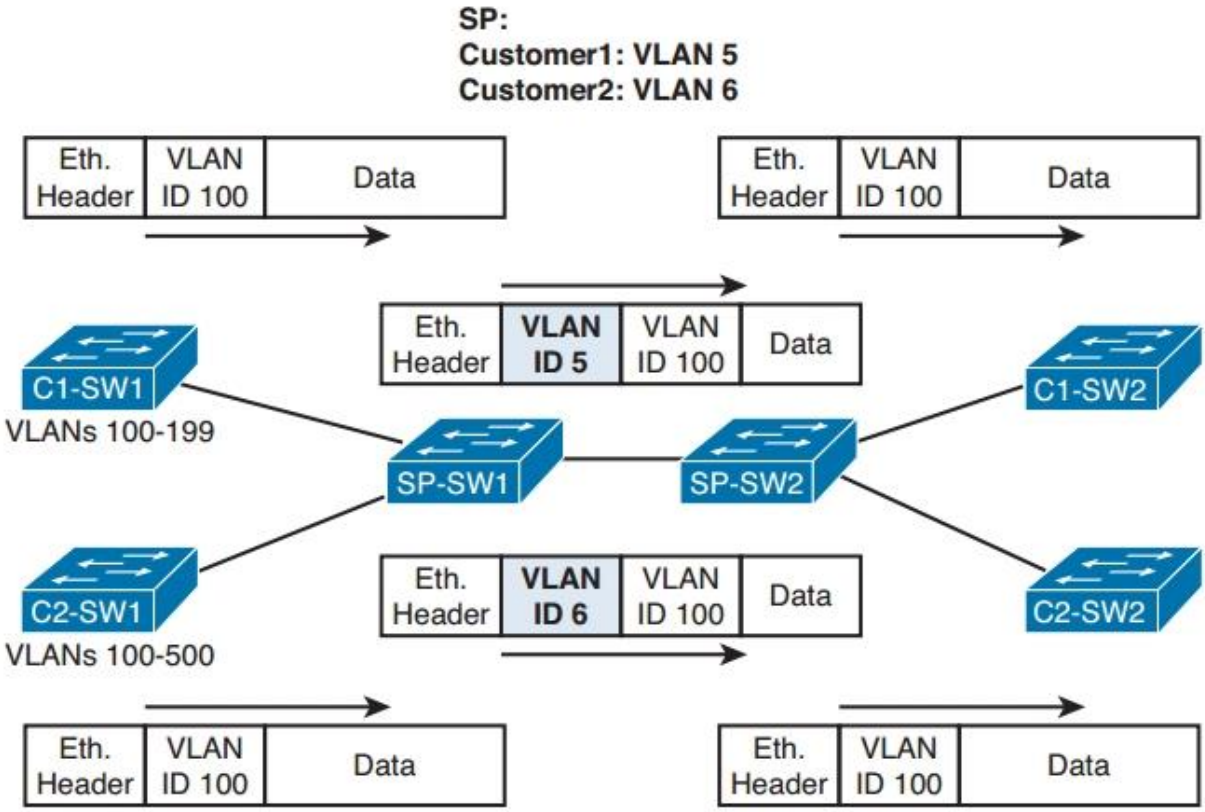



**Figure 2-6** *Q-in-Q: Basic Operation*

در تصویر بالا برای customer 1 از tag 5 و برای customer 2 از tag 6 استفاده می کند.این فریم ها با همراه با tag دوم در شبکه provider منتقل می شوند،و قبل از اینکه فریم بخواهد

در زیر نحوه کانفیگ 802.1Q-in-Q را مشاهده می کنید:

```
SP-SW1(config)# vlan dot1q tag native
SP-SW1(config)# system mtu 1504 ! Applies to 100Mbps interfaces
SP-SW1(config)# system mtu jumbo 1504 ! Applies to 1Gbps and 10Gbps interfaces
!
SP-SW1(config)# vlan 5
SP-SW1(config-vlan)# name Customer1
SP-SW1(config-vlan)# exit
SP-SW1(config)# vlan 6
SP-SW1(config-vlan)# name Customer2
SP-SW1(config-vlan)# exit
```

خط اول داشتن tag را برای همه vlanها اجباری می کند. اما در خط دوم و سوم مقدار MTU را به 1504 افزایش داده است.

MTU ( Maximum Transmission Unit ) ، نهایت سایز یک پکت یت فریم را مشخص می کند.مقدار پیش فرض آن 1500 byte بایت است.ولی در مثال بالا بخاطر tag دوم 4 byte دیگر به حجم فریم افزوده می شود.پیش برای جلوگیری از Fragmentation مقدار MTU را 1504 افزایش می دهیم.

اما تفاوت خط دوم همانطور که در توضیح آن نیز مشخص است در دوع اینترفیس می باشد که با توجه به نوع اینترفیس باید یکی از دو دستور بالا را به کار برد.

```
SP-SW1(config)# interface FastEthernet0/1
SP-SW1(config-if)# switchport mode dot1q-tunnel
SP-SW1(config-if)# switchport access vlan 5

SP-SW1(config-if)# l2protocol-tunnel cdp
SP-SW1(config-if)# l2protocol-tunnel lldp
SP-SW1(config-if)# l2protocol-tunnel stp
SP-SW1(config-if)# l2protocol-tunnel vtp
```

در شکل بالا اجازه عبور ترافیک های مدیریتی لایه 2 نیز از روی شبکه service provider نیز داده شده است.

# VLAN Trunking Protocol

هدف از ایجاد VTP، یک مدیریت متمرکز بر روی سوئیچ ها جهت ایجاد،حذف،تغییر Vlanها در سطح یک Domain، و همچنین کاهش بار ترافیک Vlanها در سطح سبکه می باشد.یعنی دیگر لازم نیست که vlanها را روی همه سوئیچ ها به صورت دستی وارد کنید،بلکه روی یک سوئیچ وارد کرده و به دیگر سوئیچ ها اعمال می شود.VTP که یک پروتکل لایه دو می باشد، اطلاعاتی در باره VLANها از قبیل VLAN ID, VLAN Name, VLAN Type را به سوئیچ های همسایه خود ارسال می کند. پکت های VTP حتما باید روی لینک Trunk منتقل شوند،زیرا VTP روی لینک Access،Advertise نمی شود.

ابتدا بهتر است با مفهومی به نام VTP Domain آشنا شوید.VTP Domain به محدوده ای گفته می شود که اطلاعات مربوط به VTP آن دامنه تنها در سطح همان دامنه ارسال می شوند و از آن خارج می شوند.به عنوان مثال اگر در سطح شبکه خود دو VTP Domain داشته باشید،اطلاعات یک دامنه به دامنه دیگر ارسال نمی شود.در واقع بدون تنظیم domain-name پروسه VTP اصلا شروع به کار نمی کند.

VTP دارای سه ورژن می باشد.ابتدا در مورد ورژن های 1و2 صحبت می کنیم.در این ورژن ها VTP در سه مُد متفاوت کار می کند.

1. Server
2. Client
3. Transparent

Server: در این مد سوئیچ اجازه ساخت،حذف و تغییر در Vlan را دارد.سوئیچی که در مُد Server باشد می تواند Vlanها را به دیگر سوئیچ ها اعلان (Advertise) کند.این اعلان از طریق لینک Trunk به دیگر سویچ ها فرستاده می شود.وقتی سوئیچ دیگر این Advertisement را دریافت می کند،Vlanها را نصب می کند.در واقع این سوئیچ هم قابلیت Advertising و هم Listening را دارد.در این مُد اطلاعات در فایلی به نام vlan.dat در flash ذخیره می شوند.پیشنهاد می شود که در شبکه حداقل دو VTP Server برای Redundancy داشته باشید.

Client: سوئیچی که در Client Mode کانفیگ شود درست مانند سرور عمل می کند،با این تفاوت که توانایی ساخت،حذف و تغییر در Vlanها را ندارد.ولی می تواند هم Advertisement داشته باشد، و هم به اطلاعات VTPارسال شده از سوی دیگر سوئیچ ها گوش دهد تا در صورت نیاز آنها را نصب کند. در این مُد نیز مانند سرور اطلاعات در فایلی به نام vlan.dat در flash ذخیره می شوند.

Transparent: در این مد Vlanها به صورت locally ساخته می شوند.یعنی اطلاعات advertise شده توسط دیگر سوئیچ ها را نصب نمی کند،ولی آنها را برای دیگر Switchها Forward می کند.یک تفاوت در vtp v1 , v2 در این مُد وجود دارد، و آن اینکه در VTP v1 اگر پکتی که دریافت می شد مربوط به همان دامین سوئیچ نبود،سوئیچ آنرا رد (Relay) نمی کرد.که در VTP v2 این محدودیت برداشته شد.یادمان باشد که VTP را نمی شود Disable کرد،و به جای آن می توان از Transparent mode استفاده کرد.ولی در VTP ورژن 3 این مشکل برطرف شده و می توان آنرا off کرد که در ادامه آنرا توضیح خواهم داد.اطلاعات vlan در این مُد هم در فایل vlan.dat و هم در NVRAM ذخیره می شوند.

## VTP Process and Revision Number

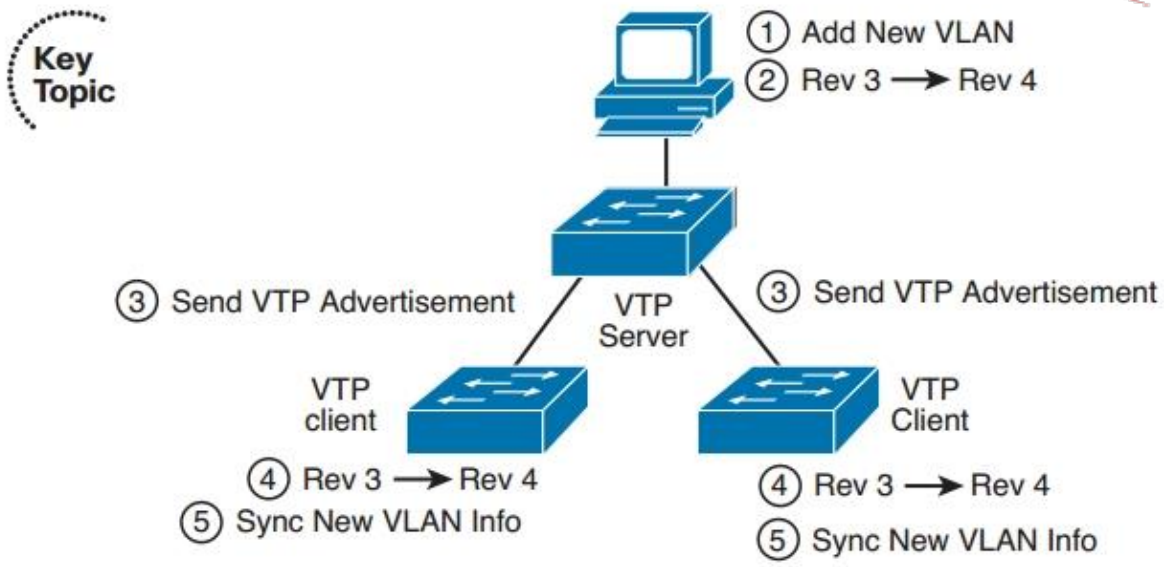



**Figure 2-7** *VTP Revision Number Basic Operation*

Revision Number در واقع یک Sequence number برای دیتابیس VTP می باشد.این شماره همراه با پکت VTP برای دیگران ارسال می شود.این شماره به صورت هربار تغییر در دیتابیس vlan،به صورت incremental یکی به آن افزوده می شود.وقتی سوئیچی یک پکت VTP دریافت کند،ابتدا Revision number آنرا چک می کند.اگر مقدار آن بیشتر از مقدار خودش بود،updateها را نصب میکند.اگر این مقدار مساوی بود پیغام را رد می کند،و اگر مقدار آن کوچکتر بود به فرستنده پکت اطلاع می دهد و خودش پیغام جدید برای نصب به فرستنده می فرستد.اما مشکلی که ممکن است در VTP پیش بیاید این است که مکن است سوئیچ یک پکت با revision number بالاتر را وارد شبکه کنیم،اینکار باعث می شود که که دیگر سوئیچها دیتابیس خود را به اشتباه update کنند.برای جلوگیری از این کار قبل از وارد کردن سوئیچ به شبکه،یکبار مُد آنرا به Transparent تغییر داد،زیرا مقدار Revision Number در مُد Transparent همیشه صفر است.

دستور زیر می تواند اطلاعاتی از VTP در اختیارتان قرار دهد:

```
Switch1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCIE-domain
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0023.ea41.ca00
Configuration last modified by 10.1.1.3 at 9-9-13 13:31:46
Local updater ID is 10.1.1.1 on interface Vl1 (lowest numbered VLAN interface
  found)
```

```
Feature VLAN:
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 7
Configuration Revision            : 2
MD5 digest                        : 0x0E 0x07 0x9D 0x9A 0x27 0x10 0x6C 0x0B
                                    0x0E 0x35 0x98 0x1E 0x2F 0xEE 0x88 0x88
```

در خروجی دستور بالا همانطور که مشخص است می توانید VTP mode, VTP version, Revision Number, VTP Pruning،تعداد vlanهای موجود و ..... را مشاهده کنید.

با دستور زیر می توانید Domain name به VTP اختصاص دهید.

```
Switch3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch3(config)# vtp domain CCIE-domain
Changing VTP domain name from NULL to CCIE-domain
```

در حالت پیش فرض نام دامنه برابر با Null می باشد.و برای اینکه سوئیچ ها بتوانند برای هم پکت VTP ارسال کنند باید نام دامنه آنها یکسان باشد.در غیر اینصورت پیغام DOMAINMISMATCH را خواهید دید.

اگر بخواهیم ورژن VTP را عوض کنیم می توان از دستور **vtp version** *version-number* استفاده کرد.م این نکته را باید به خاطر داشته باشیم که در یک دامنه،باید ورژن VTP روی همه سوئیچ ها یکسان باشد.

و برای تغییر مُد یک سوئیچ از دستور **vtp mode {server|client|Transparent}** استفاده کرد.

دستور دیگری نیز برای Authentication در VTP بین سوئیچ ها وجود دارد.دستور vtp password *password* که به وسیله آن می توان یک پسورد برای امنیت بین سوئیچ ها تعیین کرد.این پسوردها به صورت هش md5 بین سوئیچ ها منتقل می شوند. ولی اگر روی خود سوئیچ دستور **show vtp password** وارد کنید می توانید این پسورد را ببینید.برای جلوگیری از اینکار باید **service password-encryption** را روی سوئیچ فعال کنیم.

در VTP v1,2 از چهار نوع پیغام استفاده می شود:

1. Summary Advertisement
2. Subset Advertisement
3. Advertisement Request
4. Join

**Summary Advertisement**: این پیغام توسط VTP server , client هر پنج دقیقه ارسال می شود.و همچنین بعد از هر تغییر در vlan database توسط server نیز ارسال می شود.این پیغام اطلاعاتی در مورد vtp domain- name،revision number،هویت آخرین update کننده،time Stamp مربوط به آخرین Update، MD5 password و تعداد subset advertisementها. این پیغام vlan-database را advertise نمی کند.

**Subset Advertisement**: این پیغام که توسط vtp server, client زمانی که تغییری در vlan data-base رخ دهد ایجاد می شود.همچنین این پیغام حاوی تمام محتوی vlan-database می باشد.یک پیغام subset advertisement می تواند چند vlan-database را در خود نگه دارد.

**Advertisement Request**: این پیغام نیز هم توسط server و هم client می تواند ارسال شود،که با این ارسال از همسایه خود درخواست بخش یا کل vlan-database را می کند.این پیغام زمانی ارسال می شود که یک client ، restart شود،یا وقتی یک مُد یک سوئیچ client شود، و یا اینکه یک Server یا client یک پیغام Summary advertisement دریافت کند که مقدار revision number آن بزرگتر از revision خودش باشد.

**Join**: این پیغام زمانی توسط server و client هر 6 ثانیه ارسال می شود که VTP Pruning فعال باشد.توسط این پیغام مشخص می کنید که ترافیک کدام vlan را باید دریافت کند و کدام را نباید دریافت کند.در واقع اعلام می کند کدام vlan ، active و کدامیک unused می باشد.

## VTP Pruning

وقتی vtp را روی سوئیچ ها فعال می کنیم،اطلاعات مربوط به تمام vlanها در شبکه Advertise می شود، و تمام سوئیچ ها این اطلاعات را دریافت می کنند.حال فرض کنید سوئیچی vlanی را در دیتابیس خود دارد که هیچکدام از پورت هایش عضو آن vlan نیستند.چه اتفاقی می افتد؟آن سوئیچ با اینکه هیچ پورتی در عضویت آن vlan ندارد،ولی تمام ترافیک مربوط به آن vlan را روی لینک trunk خود دریافت می کند.در اینجاست که VTP Pruning به کار می آید.

وقتی روی سوئیچی pruning را فعال می کنیم،آن سوئیچ فقط درخواست ترافیکی را می کند که یا پورتی از خودش عضو آن vlan باشد،یا در مسیر عبور ترافیک برای آن vlan باشد.اما سوئیچ چگونه این کار را انجام می دهد؟

وقتی روی سوئیچ pruning را فعال می کنید،سوئیچ از روی لیستی به نام Eligible List درخواست خود ر ارسال می کند.این لیست به صورت پیش فرض از شماره‌vlanهای 2 تا 1001 را در خود دارد.بعد از فعال شدن pruning این لیست edit می شود و vlanهای غیر ضروری از آن حذف می شود.دستور فعال سازی pruning را در زیر مشاهده می کنید.وقتی این دستور روی Server فعال شود،در کل شبکه pruning اجرا می شود.

#vtp pruning

برای تغییر در این لیست نیز می توان از دستور زیر استفاده کرد.

```
IOU1(config-if)#sw tr pruning vlan ?
  WORD    VLAN IDs of the allowed VLANs when this port is in trunking mode
  add     add VLANs to the current list
  except  all VLANs except the following
  none    no VLANs
  remove  remove VLANs from the current list
```

می توان در دستور بالا یک رنج vlan را مشخص کرد،و یا برای اضافه کردن یک vlan از دستور add استفاده کرد تا vlan جدید به لیست اضافه شود.و برای حذف کردن یک vlan از گزینه remove استفاده کنیم.گزینه none هیچ vlanی را دربر نمی گیرد، و با گزینه except میتوان همه vlanها به جز vlanهای جدید را در لیست قرار داد.

## Normal-Range and Extended-Range VLANs

در Extended-Range, vtp در vtp منتقل نمی شوند.و اصلا در این مد قابل کانفیگ نیستند. فقط در سوئیچ های با مُد Transparent قابل کانفیگ می باشند. در جدول زیر رنج همه Vlanها را مشاهده می کنید.

Key Topic

**Table 2-8** *Valid VLAN Numbers, Normal and Extended*

| VLAN Number | Normal or Extended? | Can Be Advertised and Pruned by VTP Versions 1 and 2? | Comments |
|---|---|---|---|
| 0 | Reserved | — | Not available for use |
| 1 | Normal | No | On Cisco switches, the default VLAN for all access ports; cannot be deleted or changed |
| 2–1001 | Normal | Yes | — |
| 1002–1005 | Normal | No | Defined specifically for use with FDDI and TR translational bridging |
| 1006–4094 | Extended | No | — |
| 4095 | Reserved | No | Not available for use |

در جدول زیر نیز محل قرارگیری vlanها در مُدهای مختلف را مشاهده می کنید.

Key Topic

**Table 2-9** *VLAN Configuration and Storage for VTPv1 and VTPv2*

| Function | When in VTP Server Mode | When in VTP Transparent Mode |
|---|---|---|
| Normal-range VLANs can be configured from | Both VLAN database and configuration modes | Both VLAN database and configuration modes |
| Extended-range VLANs can be configured from | Nowhere—cannot be configured | Configuration mode only |
| VTP and normal-range VLAN configuration commands are stored in | vlan.dat in Flash | Both vlan.dat in Flash and running configuration[1] |
| Extended-range VLAN configuration commands are stored in | Nowhere—extended range not allowed in VTP server mode | Running configuration only |

همانطور که مشخص است extended-range برای مُد transparent در NVRAM قرار می گیرد ولی normal-range هم در NVRAM و هم در فایل vlan.dat در flash ذخیره می شود.

ولی برای مُد server، extended-range اصلا کانفیگ نمی شود،پس ذخیره هم نمی شود،standard-range در فایل vlan.dat در flash ذخیره می گردد.

و نکته آخر اینکه اگر یک سوئیچ transparent را که اطلاعات NVRAM و vlan.dat یکسان نداشته باشد،سوئیچ از vlan.dat استفاده می کند و اولیت این فایل بیشتر است.

## VTP version 3

VTP v3 آخرین ورژن از VTP می باشد که که نسبت به ورژن های یک و دو تغییراتی داشته و مشکلاتی که در ورژن های قبلی موجود بود را بهبود بخشیده است.در این ورژن مواردی مانند Extended Vlans،Private Vlans و MST Configuration نیز advertise می شودند،که در vtp v1,2 این امکان وجود نداشت.

در VTP v1,2 وقتی یک سوئیچ client و یا server با Revision number بالاتر وارد شبکه می شد،دیتابیس خود را به دیگر سوئیچ ها می داد و این یک مشکل امنیتی محسوب می شد.اما این مشکل در VTP v3 با مفهومی به نام Primary-Server حل شده است.در این ورژن، primary server تنها سوئیچی است که می تواند در کل دامنه vlan-database را ارسال کند.دیگر server, clientها تنها در صورتی vlan-database خود رابه اشتراک می گذارند که بر سر دو پارامتر domain-name و شناسهء primary-server به توافق برسند.شناسه primary-server همان base-mac address سوئیچ primary می باشد. شوئیچ Primary تنها سوئیچی است که اجازه تغییرات در vlan-database را به مدیر شبکه می دهد.

دیگر سوئیچ های Server در شبکه را Secondary Server می نامند.برعکس VTP v1,2،در این ورژن Secondary اجازه تغییر در vlan-database را به administrator نمی دهد.بلکه آنها فقط وظیفه primary-server را معرفی می دهند. Clientها نیز اجازه تغییر در database را ندارند.هم client و هم secondaryها یک کپی از vlan-database از primary server را در خود نگه می دارند و آنها را به همسایه های خود می دهند اگر با vtp-domain و شناسه primary server به توافق برسند.یعنی در vtp v3 نیز میتواند یک سوئیچ با revision-number بالاتر database خود ر ابه دیگر سوئیچ ها بدهد در صورتی که vtp-domain،primary server identity و vtp password خود را با دیگر سوئیچ ها یکی کند.

اگر بین دو و یا بیشتر از سوئیچ های server و یا client، شناسه primary server یکسان نباشد Conflict رخ می دهد. وقتی بین سوئیچ ها Conflict رخ دهد آنها database خود را با هم sync نمی کنند،حتی اگر باقی پارامترها در بین آنها یکسان باشد.این مفهوم از گسترش دیگر vlan-database ها در شبکه جلوگیری می کند.زیرا تنها primary-server اجازه تغییر در database را دارد و سوئیچ های که با primary-identity موافق باشند فورا آن database را shareمی کند. وقتی سوئیچی از شبکه خارج می شود،می تواند vlan-database خود را تغییر دهد. و خود را به عنوان primary server می داند،البته تا زمانی که به شبکه متصل نیست.وقتی به شبکه برگردد متوجه میشود که primary identity خود با دیگر همسایه ها یکسان نیست،در این صورت حتی اگر revision number بالاتری نیز داشته باشد توسط همسایه ها پذیرفته نمی شود. VTP v3 را می توان روی یک لینک خاص یا به صورت globally از کار انداخت.

## VTP version 3 Configuration

باید تعیین ورژن VTP v3 ابتدا باید domain-name را معرفی کنیم.اینکار جهت آغاز پروسه vtp در ورژن 1،2 نیز ضروری می باشد.سپس روی تمام سوئیچ ها باید ورژن را به 3 تغییر دهیم.

```
Switch3(config)# vtp version 3
Switch3(config)#
Sep  9 15:49:34.493: %SW_VLAN-6-OLD_CONFIG_FILE_READ: Old version 2 VLAN configura-
  tion file detected and read OK.  Version 3
    files will be written in the future.
```

تعریف مُد client و server نیز مانند ورژن یک و دو است:

```
Switch3(config)# vtp mode client
Setting device to VTP Client mode for VLANS.
```

سپس روی سوئیچی که هنوز primary نشده می خواهیم یک vlan ایجاد کنیم.اجازه اینکار داده نخواهد شد،مگر اینکه با دستور vtp primary در EXEC مُد آنرا تعریف کنیم.مانند شکل زیر:

```
Switch1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch1(config)# vlan 23
VTP VLAN configuration not allowed when device is not the primary server for vlan
  database.
Switch1(config)# do vtp primary
This system is becoming primary server for feature vlan
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
Switch1(config)#
Sep  9 17:06:59.332: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: 0023.ea41.ca00 has become
  the primary server for the VLAN VTP feature
```

یکی دیگر از قابلیت های VTP v3 گزینه hidden برای پسورد می باشد.با این کار حتی اگر روی خود سوئیچ نیز دستور show vtp password نیز وارد شود باز هم پسورد اصلی قابل مشاهده نیست.

```
Switch1(config)# vtp password S3cr3tP4ssw0rd hidden
Setting device VTP password
Switch1(config)# do show vtp password
VTP Password: 8C70EFBABDD6EC0300A57BE402409C48
```

در شکل زیر می بینید که یک سوئیچ دیگر به خاطر یکسان نبودن پسورد نمی تواند primary شود.

```
Switch2(config)# do vtp primary
This system is becoming primary server for feature vlan
Enter VTP Password: <entering 8C70EFBABDD6EC0300A57BE402409C48>
Password mismatch
```

## PPPoE Configuration

PPPoE( Point-to-Point over Ethernet) یک پروتکل برای اتصال چند کامپوتر در یک شبکه LAN از طریق مودم می باشد.این پروتکل همانطور که ار نامش پیداست encapsulation فریم های ppp را در داخل فریم های اترنت انجام می هد.این پروتکل امکان ایجاد چندین session را روی یک client فراهم می کند.

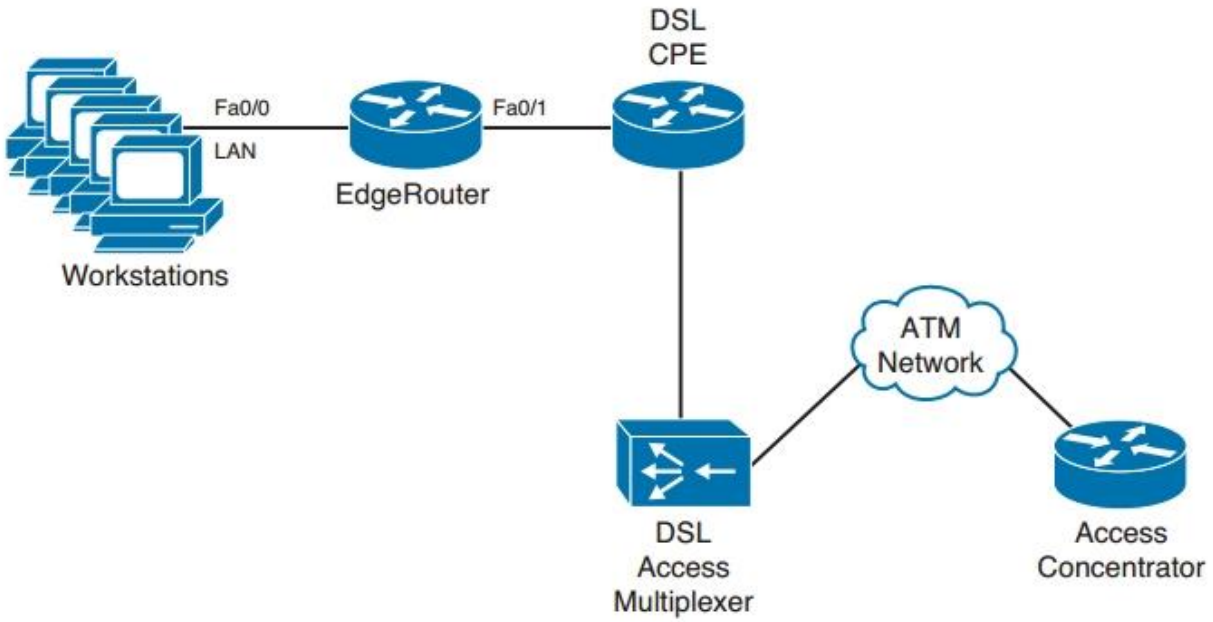



**Figure 2-8** *PPPoE Topology for Example 2-12*

در شکل بالا PPPoE Client روی EdgeRouter راه اندازی میشود و به ISP متصل می شود و به این صورت شبکه LAN پشت روتر نیز از اینترنت بهره مند می شوند.

نحوه پیکربندی PPPoE Client را روی روتر در شکل زیر ببینید:

```
EdgeRouter(config)# interface fa0/0
EdgeRouter(config-if)# no shutdown
EdgeRouter(config-if)# ip address 192.168.100.1 255.255.255.0
EdgeRouter(config-if)# ip nat inside
EdgeRouter(config)# interface fa0/1
EdgeRouter(config-if)# no shutdown
EdgeRouter(config-if)# pppoe-client dial-pool-number 1
EdgeRouter(config-if)# exit
EdgeRouter(config)# interface dialer1
EdgeRouter(config-if)# mtu 1492
EdgeRouter(config-if)# ip tcp adjust-mss 1452
EdgeRouter(config-if)# encapsulation ppp
EdgeRouter(config-if)# ip address negotiated
EdgeRouter(config-if)# ppp chap hostname Username@ISP
EdgeRouter(config-if)# ppp chap password Password4ISP
EdgeRouter(config-if)# ip nat outside
```

```
EdgeRouter(config-if)# dialer pool 1
EdgeRouter(config-if)# exit
EdgeRouter(config)# ip nat inside source list 1 interface dialer1 overload
EdgeRouter(config)# access-list 1 permit 192.168.100.0 0.0.0.255
EdgeRouter(config)# ip route 0.0.0.0 0.0.0.0 dialer1
```

**Blueprint topics covered in this chapter:**

This chapter covers the following subtopics from the Cisco CCIE Routing and Switching written exam blueprint. Refer to the full blueprint in Table I-1 in the Introduction for more details on the topics covered in each chapter and their context within the blueprint.

- Spanning Tree Protocol
  - 802.1D STP
  - 802.1w RSTP
  - 802.1s MST
  - Loop Guard
  - Root Guard
  - EtherChannel Misconfiguration Guard
  - BPDU Guard and BPDU Filter
  - UDLD
  - Bridge Assurance
- EtherChannel
- Troubleshooting Complex Layer 2 Issues

# Spanning Tree Protocol

## 802.1D Spanning Tree Protocol and Improvements

شبکه های Ethernet(لایه دو) امکان loop وجود دارد.درست مانند لایه سه.ممکن در است در شبکه Ethernet چند مسیر برای یک ترافیک Broadcast وجود داشته باشد و در صورت عبور ترافیک از همه مسیرها loop در شبکه به وجود می آید که منجر به Broadcast Storm می شود. که باعث پر شدن Bandwidth در شبکه و Process در سوئیچ های شبکه می شود.پروتکل Spanning Tree برای جلوگیری از loop در لایه دو می باشد.و به وسیله ایجاد یک ساختار درختی برای توپولوژی، یک مسیر loop free ایجاد می کند.اگر نحوه کار STP را توضیح دهیم اینگونه است که الگوریتمی به نام STA در شبکه اجرا می شود که به وسیله آن یک نقطه اصلی را در شبکه تعیین می کند به نام Root Bridge می گویند و سپس هر سوئیچ تنها یک مسیر برای رسیدن به Root برمی گزیند و پورت هایی که باعث ایجاد loop می شوند را به حالت Block تغییر می دهد.در ادامه توضیحات کامل را خواهم داد.

در پروسه STP سه عمل اصلی انجام می شود:

1. انتخاب Root Bridge
2. تعیین Root Port برای هر سویئچ
3. انتخاب Designated Port به ازای هر سگمنت.

### Elect the Root Bridge

در شبکه سوئیچی که کمترین Bridge-ID را داشته باشد به عنوان Root Bridge شناخته می شود.اما Bridge ID چیست؟

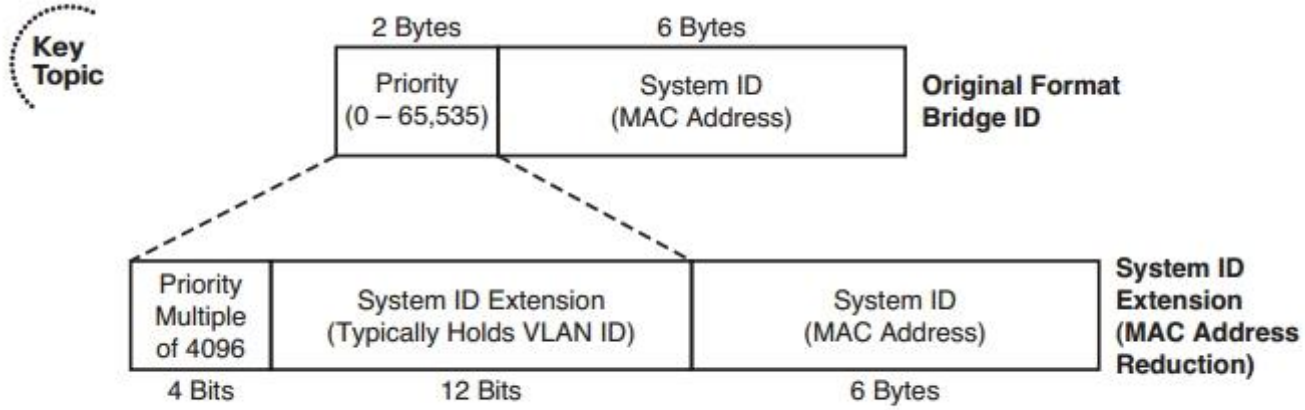



**Figure 3-2** *IEEE 802.1D STP Bridge ID Formats*

در original format Bridge ID همانطور که می بینید از ترکیب دو فیلد Priority و System ID(base mac address) ، باعث ایجاد Bridge ID می شود.مقدار Priority می تواند از 0 تا 65535 باشد. هر سوئیچی که مقدار priority آن کمتر باشد به عنوان Root Bridge انتخاب می شود. و در صورت اینکه مساوی باشد از base mac address استفاده می شود که در هر سوئیچ یک مقدار منحصر با فرد و یا unique است.

اما در فرمت بعدی که System ID Extension نام دارد کمی تغییر به وجود آمد.در این فرمت فیلد priority تبدیل به فیلد مجزا شده است.priority از 0 شروع می شود و تا مقدار 65535 به صورت مقدار 4096 تایی به آن اضافه می شود. System ID نیز همان مقدار vlan می باشد.

در هر دو فرمت اولویت با مقدار priority می باشد.هر چه این مقدار کمتر باشد اولویت سوئیچ برای Root شدن نیز بیشتر می شود.ذکر این نکته نیز مهم است که فرمت دوم برای برای +PVST می باشد.در ادامه تضیح خواهم داد.

## Determining the Root Port

وقتی در توپولوژی Root Bridge مشخص شد،تمام سوئیچ ها شروع به محاسبه برای بهترین مسیر برای رسیدن به Root می کنند. پورتی که بهترین مسیر را تا Root بداند، به عنوان Root Port انتخاب می شود.حال به چگونگی اینتخاب بهترین مسیر می پردازیم.

وقتی سوئیچی Root شد شروع به ارسال BPDU در بازه زمنی هر 2ثانیه می کند.به BPDU ، STP Hello گفته می شود. این پکت با Cost 0 برای همسایه ها ارسال می شود. وقتی سوئیچی این پکت را دریافت می کند میزان Cost لینکی روی آن دریافت کرده را با مقدار Cost پکت جمه می کند و مقدار جدید را در پکت قرار می دهد،و مقادیر forwarding Switch's Bridge ID, forwarder's port priority, forwarder's port number با مقادیر خود عوض کرده و سپس به همسایه های خود ارسال می کند به جز پورت هایی که Block هستند. بهترین مسیر از محاسبه مجموع Costها با Cost خود اینترفیس تعیین می شود.مقدار Cost پیش فرض از روی bandwidth لینک محاسبه می شود. در شکل زیر مقدار Cost برای لینک های مختلف را ببینید:

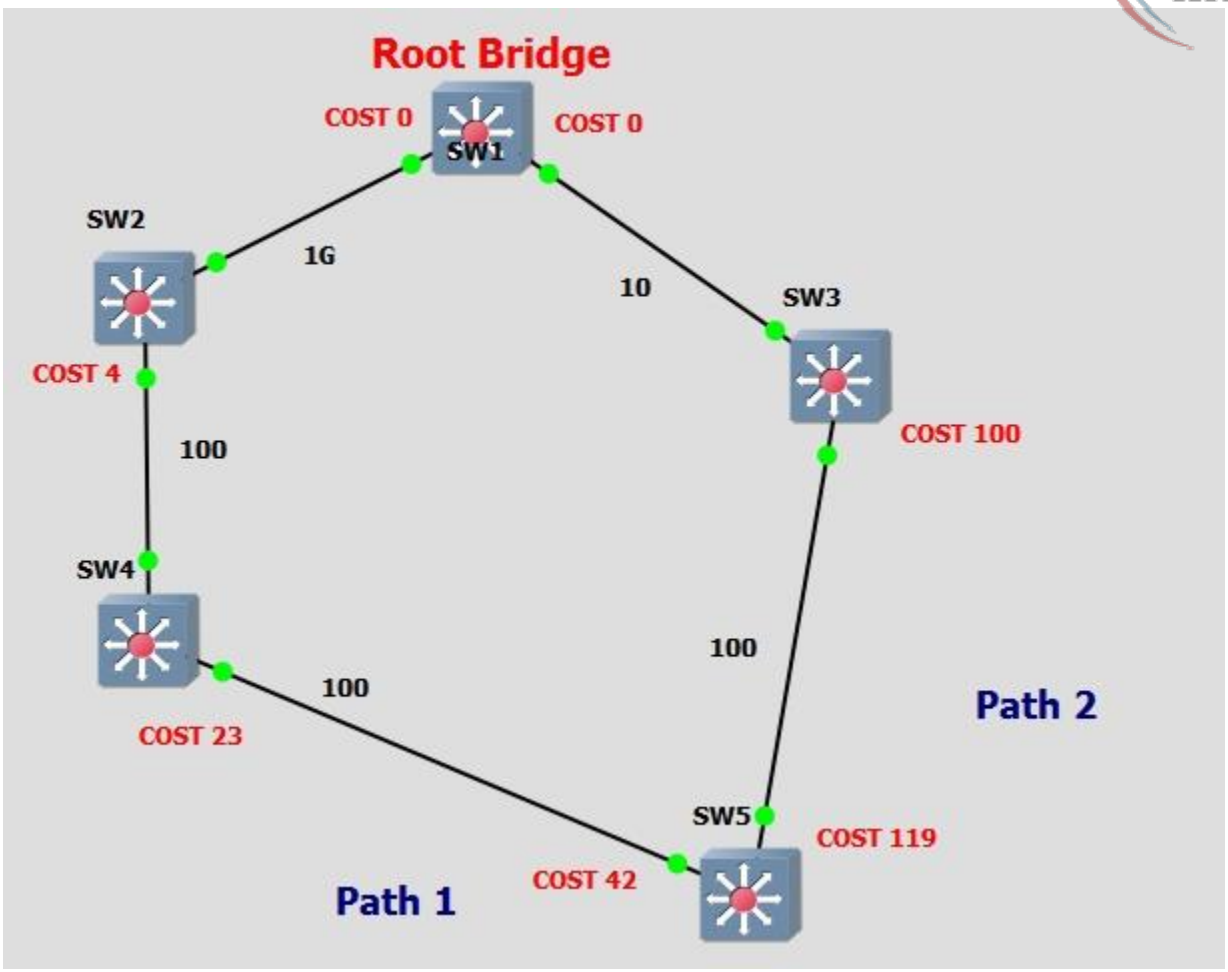
**Table 3-3** *Default Port Costs According to IEEE 802.1d*

Key Topic

| Speed of Ethernet | Original IEEE Cost | Revised IEEE Cost |
|---|---|---|
| 10 Mbps | 100 | 100 |
| 100 Mbps | 10 | 19 |
| 1 Gbps | 1 | 4 |
| 10 Gbps | 1 | 2 |

پس میتوان اینطور نتیجه گرفت که هر چه مقدار Bandwidth یک لینک بیشتر باشد، میزان Cost آن پایین تر می شود، و هرچه Costپائین تر باشد مسیر مناسب تر است.

در زیر با یک مثال ساده این مثال را بیشتر توضیح خواهم داد:




همانطور که در شکل بالا مشاهده می کنید، SW5 از دو مسیر می تواند Root Bridge را ببیند.سپس با محاسبه مقدار Cost بر اساس پهنای باند لینک ها، مسیر 1 را انتخاب می کند.زیرا مقدار مجموع Cost محاسبه شده از مسیر 1 برابر با 42 و مسیر 2 مقدار Cost 119 را دارد. دیگر سوئیچ ها نیز به همین صورت Root Port خود را مشخص می کنند.

یک نکته را باید به خاطر داشته باشید که Root Port، فقط BPDU دریافت می کند و ارسال آن به عهده Designated Port می باشد که در ادامه به توضیح آن نیز خواهم پرداخت. در زیر شکل خود کتاب را نیز مشاهده می کنید:

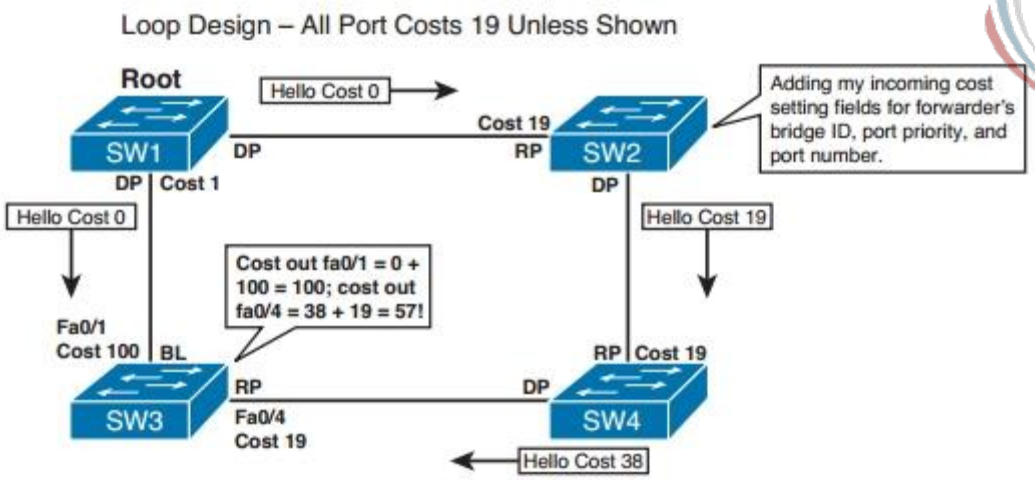



**Figure 3-3** *Calculating STP Costs to Determine RPs*

در شرایط بالا سوئیچ روی هر پورت خود Costهای متفاوتی را دریافت می کرد.حال فرض کنیم سوئیچ روی دو پورت خود BPDU با Cost برابر دریافت کند.در این شرایط از پارامترهای زیر برای انتخاب Root Port استفاده می کند:

1. Bridge ID کمتر فرستنده.
2. Port Priority کمتر فرستنده.(به صورت پیش فرض Priority پورت ها 128 می باشد که قابل تغییر هستند.)
3. شماره پورت کمتر.

دو شرط آخر تنها در موقعی استفاده می شود که فرستنده یک سوئیچ باشد که با دو لینک متصل می باشد.


## Determining Designated Port

از دید STP در هر سگمنت باید یک Designated Port وجود داشته باشد.وظیفه Designated Port ارسال PBDU است. در واقع در یک سگمنت، طرفی که Hello BPDU با Cost کمتر را ارسال می کند به عنوان Designated Port انتخاب می شود.پس می توان به این نتیجه رسید که تمام پورت های سوئیچ Designated هستند.

این بخش را با مثال کتاب توضیح خواهم داد:

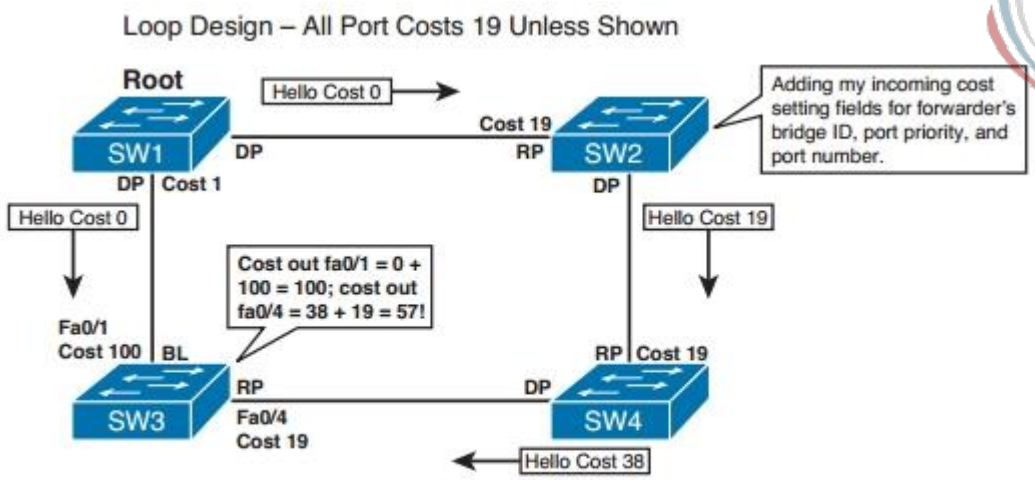



**Figure 3-3** *Calculating STP Costs to Determine RPs*

در سگمنت بین دو سوئیچ 3 و 4،هر دو برای هم Hello BPDU ارسال می کنند،ولی سوئیچ 3 با Cost 100 و سوئیچ 4 با Cost 38 ارسال می کند. بعد از مقایسه سوئیچ چهار پورت خود را Designated در این سگمنت مشخص می کند.و اگر Costها نیز با هم برابر بودند، Neighbor Bridge ID مقایسه می شود.و در صورت برابر بودن آنها Port Priority همسایه و اگر آن هم برابر بود شماره پورت همسایه مقایسه می شود.

و در انتها تعریف Block Port.پورتی که نه Root Portاست و نه Designated Port به حالت Block Port می باشد. این همان پورتی است که در صورت ارسال ترافیک باعث بروز Loop در شبکه می شود.روی این نوع پورت BPDU دریافت می شود،ولی ارسال نمی شود.

## Converging to a New STP Topology

با استفاده از STP شبکه به صورت loop free و Stable می شود. ولی وقتی شبکه از حالت Stable خارج شود چه اتفاقی می افتد؟ STP چگونه شبکه را به حالت Stable در می آورد؟

ابتدا تعریفی از Stable از دیدگاه STP را می گوییم:

1. Root Switch در بازه هر دو ثانیه (Hello Timer) Hello BPDU ارسال می کند.
2. تمام سوئیچ ها این BPDUها را روی Root Port خود دریافت می کنند.
3. بعد از تغییر forwarder's port priority, forwarder's port number، از روی Designated Port خود آنرا ارسال می کنند.
4. روی پورت Block، BPDU دریافت می شود ولی از آن ارسال نمی شود.

حال اگر یکی از شرایط بالا عوض شود،مانند عدم دریافت BPDU و یا دریافت BPDU با مشخصات جدید، آن وقت شبکه از حالت Stable خارج گشته است.در این زمان Convergence, STP را آغاز می کند.

شکل زیر را در نظر بگیرید:

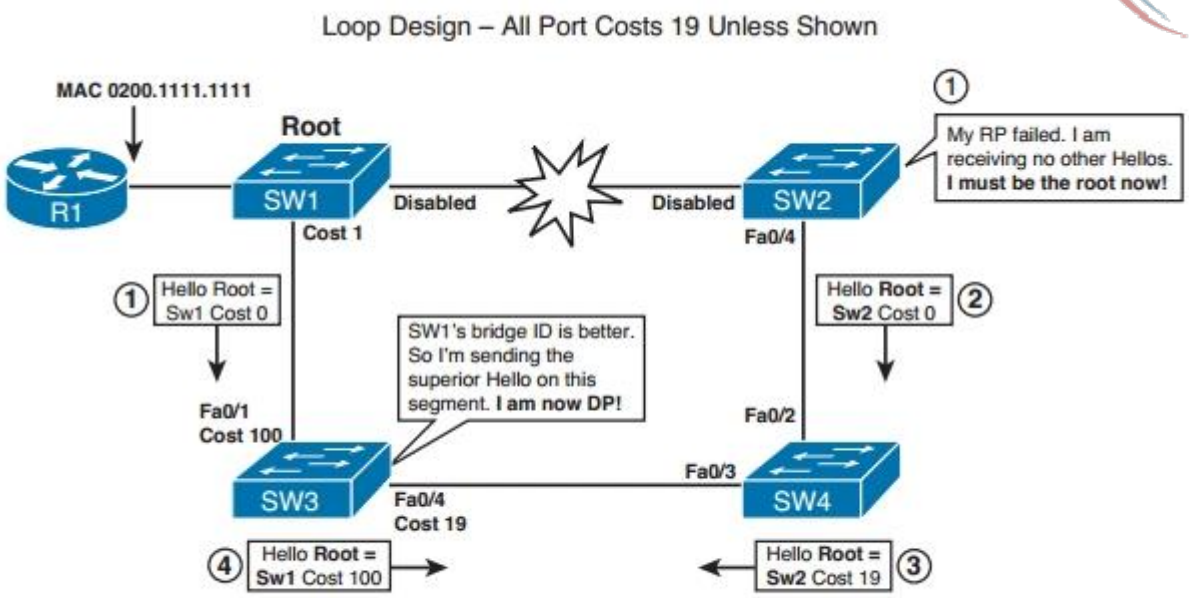



**Figure 3-4** *Reacting to the Loss of Link Between SW1 and SW2*

در شکل بالا لینک بین سوئیچ های یک و دو قطع می شود.سوئیچ 2 بعد از 20 ثانیه که از Root Bridge هیچ BPDUی دریافت نکرد،اینطور فکر میکند که Root Bridge از مدار خارج شده و سپس خود را Root معرفی می کند و شروع به ارسال BPDU با مشخصه جدید برای سوئیچ 4 می کند. (به آن 20 ثانیه که از Root هیچ BPDUی دریاف نشد، -maxage timer می گویند که 10 برابر Hello Timer است).

سپس سوئیچ 4 BPDU از سوئیچ 2 دریافت می کند،متوجه طریق مشخصات Root در BPDU دریافتی می شود، ولی چون تنها Root Port آن به سوئچ 2 است،آنرا از طریق Designated port(f0/3) آنرا به سوئیچ 3 می دهد.

حال BPDU از طرف سوئیچ 4 به سوئیچ 3 می رسد.سوئیچ 3 که از روی هر دو پورت خود Hello PBDU دریافت می کند متوجه تغییر می شود. روی پورت Block خود BPDUی که دریافت می کند دارای bridge ID بهتری است.سپس پورت Block خود را به Root Port ، و Root port خود را به Designated port تبدیل میکند.

سوئیچ 4 که حالا از طرف سوئیچ 3 ، BPDU با bridge ID بهتری دریافت می کند، Designated port خود را به Root port ، و Root port خود را به Designated port تبدیل میکند. و BPDU گرفته شده از سوئیچ 3 را به سوئیچ 2 ارسال می کند.

سوئیچ 2 ، BPDU با Bridge ID را از سوئیچ 4 دریافت دریافت می کند،و دیگر خود را به عنوان Root معرفی نمی کند، و پورت f0/4 خود را به Root Port تبدیل می کند و دیگر BPDU ارسال نمی کند.

## Topology Change Notification and Updating the CAM

بعد از اینکه STP در شبکه دوباره محاسبات خود را انجام داد و Convergence انجام شد،مشکلی پیش می آید که مربوط به CAM(Content Addressable Memory) می باشد. برای توضح بیشتر باز هم شکل قبل را مثال می زنیم.

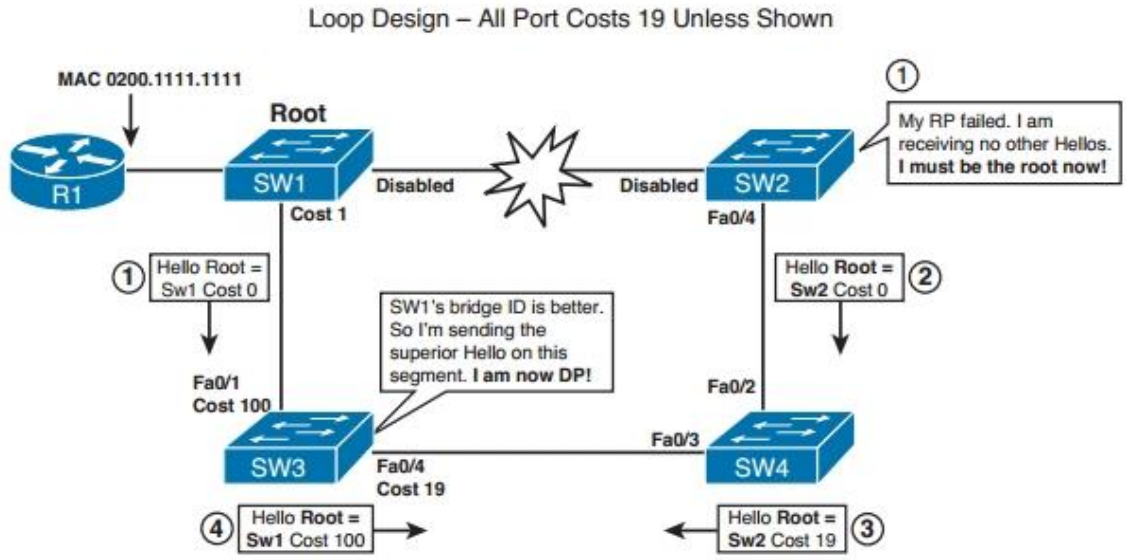
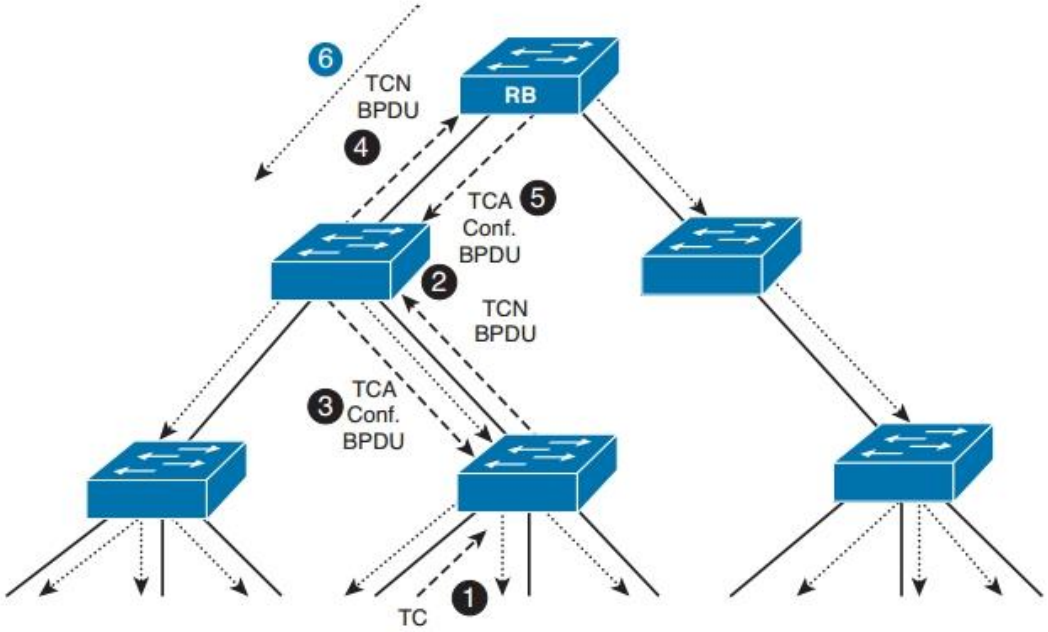



**Figure 3-4** *Reacting to the Loss of Link Between SW1 and SW2*

در این شکل قبل از Convergence سوئیچ 3 برای mac-address 0200.1111.1111 ، پورت خروجی را f0/4 می دانست.در حالی که بعد از Convergence باید این پورت از روی f0/1 یاد گرفته شود.

در این حالت سوئیچ پیغامی را به نام TCN BPDU مبنی بر این اشتباه به روی Root Port خود ارسال می کند.سوئیچ بالاتر که این پیام را میگیرد آنرا از طریق Root Port خود ارسال می کند و یک ACK به سوئیچ فرستنده می دهد.این کار تا زمانی که پیام به سوئیچ Root برسد ادامه دارد. سوئیچ Root نیز BPDU را برای تمام سوئیچ های شبکه ارسال می کند و در آن بیت TCN را set می کند.همه سوئیچ ها بعد از دریافت این پیغام تایمر CAM Table خود را از 300 ثانیه به 15 کاهش می دهند.و در این زمان مسیرهای صحیح در CAM table قرار می گیرند.



## Transitioning from Blocking to Forwarding

زمانی که در Convergence در STP رخ می دهد و یک توپولوژی مجدد Stable به وجود می آید،بعضی از پورت ها که در وضعیت Block بودند تبدیل به Designated یا Root پورت می شوند و باید در حالت Forwarding باشند. ولی این تبدیل به صورت آنی نیست و یک بازه زمانی را دربر می گیرد. در بازه ،پورت ابتدا باید دو حالت Listening و Learning را بگذراند و سپس وارد حالت Forwarding شود.هریک از این حالت ها 15 ثانیه زمان می گیرد که به آن Forward Delay می گویند.البته تغییر حالت از Forwarding به Blocking سریع و آنی انجام می شود.

در شکل زیر حالت های مختلف یک پورت را می بینید و مشاهده می کنید که در چه حالت های دیتا ارسال می شود،یا در چه حالت هایی Mac-addressها learn می شود و پایدار بودن یا نبودن هر حالت را می بینید:

Key Topic

**Table 3-4** *IEEE 802.1D Spanning Tree Interface States*

| State | Forwards Data Frames? | Learns Source MACs of Received Frames? | Transitory or Stable State? |
|---|---|---|---|
| Blocking | No | No | Stable |
| Listening | No | No | Transitory |
| Learning | No | Yes | Transitory |
| Forwarding | Yes | Yes | Stable |
| Disabled | No | No | Stable |

## Per-VLAN Spanning Tree and STP over Trunks

در 802.1D(Common STP) برای تمام vlanها در کل توپولوژی تنها یک ساختار وجود دارد.یعنی تنها یک instance به ازای کل Vlanها در شبکه اجرا می شود و تنها یک مسیر فعال در شبکه وجود دارد.

اما PVST توسط سیسکو برای حل این مشکل به وجود آمد.با +PVST می توان به ازای هر vlan یک instance در شبکه اجرا می کند.یعنی به ازای هر vlan یک ساختار متفاوت ایجاد می شود.یک Root Bridge متفاوت. با اینکار می توان از تمام

لینکهای شبکه استفاده کرد. مثلا لینکی که برای یک Vlan در حالت Block است، برای Vlan دیگر می تواند Forward باشد.

برای مثال به شکل زیر نگاه کنید:

هیچ لینکی در شبکه زیر برای هر دو VLAN در حالت Block نیست.اما تنها مشکلی که PVST دارد این است که 802.1Q را پشتیبانی نمی کند و فقط از ISL پشتیبانی می کند.زیرا استاندارد نیست. اما سیسکو این مشکل را حل کرده و بر روی سوئیچ های سیسکو می توان از آن استفاده کرد.

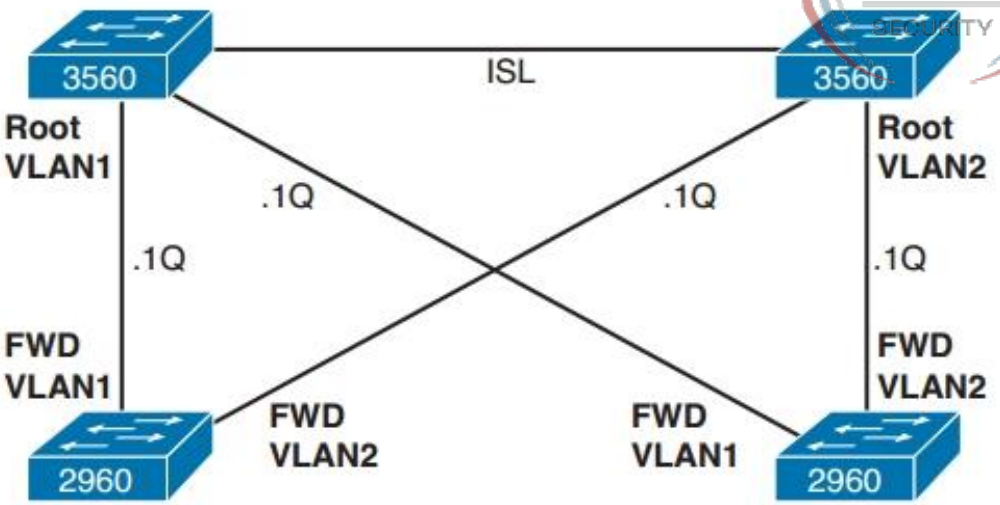
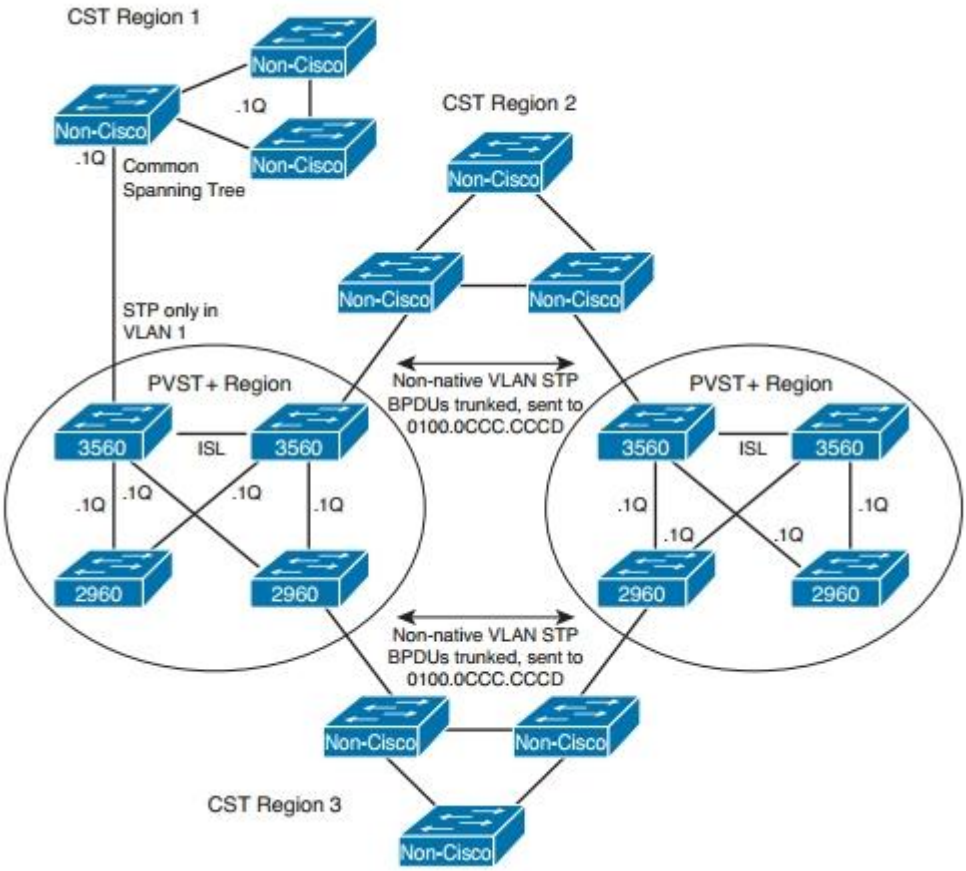



**Figure 3-6** *Operation of PVST+ for Better Load Balancing*

اما در سوئیچ های غیر سیسکو باید از Common Spanning Tree استفاده کرد. که همنطور که در شکل زیر نیز می بینید می توان ترکیبی از هر دو را داشت:



آدرس 0100.0CCC.CCCD که در شکل بالا مشاهده می کنید destination mac addressی هست که در PVST+ برای ارسال BPDU به ازای هر vlan ارسال می شود.این mac address برای شبکه های غیر سیسکویی به معنی unknown unicast می باشد و به این صورت دو شبکه PVST+ از طریق یک شبکه CST با هم ارتباط برقرار می کنند.

## STP Configuration and Analysis

در مثال زیر بخشی از کانفیگ STP را خواهید دید، و دستورات Verify برای STP را نیز خواهید دید:

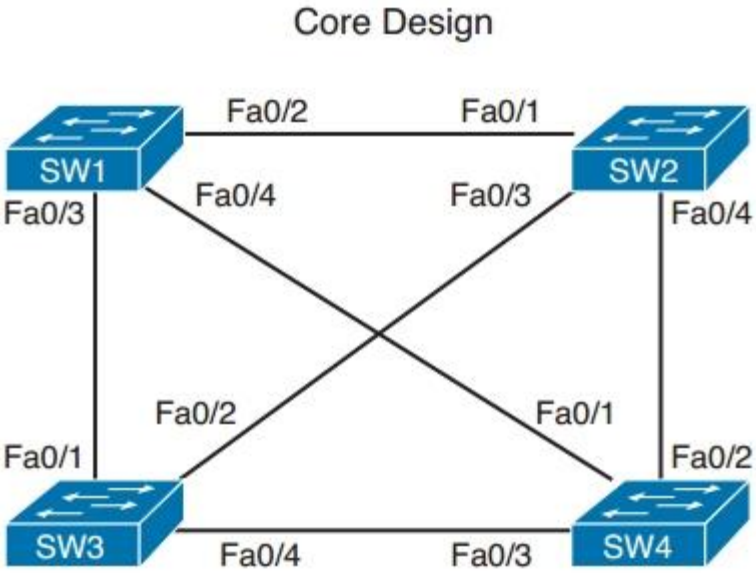



**Figure 3-10** *Network Used with Example 3-1*

در شکل زیر دستور show spanning-tree root را در سوئیچ یک مشاهده می کنید:

```
SW1# sh spanning-tree root

                                        Root    Hello Max Fwd
Vlan                Root ID          Cost    Time  Age Dly  Root Port
---------------- -------------------- --------- ----- --- ---  ------------
VLAN0001         32769 000a.b7dc.b780         0     2   20  15
VLAN0011         32779 000a.b7dc.b780         0     2   20  15
VLAN0012         32780 000a.b7dc.b780         0     2   20  15
VLAN0021         32789 000a.b7dc.b780         0     2   20  15
VLAN0022         32790 000a.b7dc.b780         0     2   20  15
```

در ستون Root ID مشاهده می کنید که Root Bridge برای همه vlanها یکی است.یعنی یک سوئیچ برای همه Vlanها نقش Root Bridge را بازی می کند.اگر به ستون Cost دقت کنید، متوجه می شوید که این مقدار برای همه Vlanها صفر است.پس می توان اینگونه نتیجه گیری کرد که سوئیچ یک به عنوان Root Bridge برای همه Vlanها می باشد.

همچنین می توان مقادیر کنترلی را در سه ستون Hello time,Max age,Forward delay مشاهده کرد. که مقادیر پیش فرض هستند.

با دستور زیر می توان مشخصات Root Bridge برای یک Vlanخاص را با جزویات مشاهده کرد.میزان Priority برابر است با 32769.مقدار پیش فرض 32768 می باشد،اما چون برای Vlan 1 است عدد یک نیز با آن جمع می شود.اگر priority برای Vlan 2 را می دیدیم مقدار آن 2+32768 یعنی 32770 م بود. و در ادامه نیز مشاهده می کنید که به صراحت بیان شده که این سوئیچ برای Vlan 1، نقش Root را دارد.

```
SW1# sh spanning-tree vlan 1 root detail
  Root ID     Priority    32769
              Address     000a.b7dc.b780
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

در شکل زیر، سوئیچ دو با کاهش مقدار Priority ، به عنوان Root جدید خود را معرفی می کند. اما یادمان باشد که میزان Priority باید مضربی از 4096 باشد. و در ادامه نیز می بینیم که حال سوئیچ دو برای Vlan 1 نقش Root bridge را دارد و MAC سوئیچ دو به عنوان Root سوئیچ نشان داده می شود. و میزان Priority نیز به 28673 تغیر کرده است:

```
SW2(config)# spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096

SW2(config)# spanning-tree vlan 1 priority 28672
SW2(config)# ^Z
SW2# sh spanning-tree vlan 1 root detail
VLAN0001
  Root ID     Priority    28673
              Address     0011.92b0.f500
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

سپس در سوئیچ دو دستور زیر را وارد می کنیم.با این دستور مقدار Priority برای همه Vlanها مشخص می شود:

```
SW2# sh spanning-tree root priority
VLAN0001         28673
VLAN0011         32779
VLAN0012         32780
VLAN0021         32789
VLAN0022         32790
```

سپس روی سوئیچ سه دستور زیر را وارد کی میکنیم و متوجه می شویم که سوئیچ سه برای vlan 1 ، mac سوئیچ دو و Priority تعیین شده توسط آن را می بیند:

```
SW3# sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    28673
              Address     0011.92b0.f500
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

می بینید که سوئیچ سه BPDU مربوط به این VLAN را با Cost 19 از روی پورت fa0/2 دریافت می کند.

```
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Altn BLK 19        128.1    P2p
Fa0/2            Root FWD 19        128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/13           Desg FWD 100       128.13   Shr
```

در شکل نیز می بینید که سوئیچ سه پورت fa0/2 خود را به خاطر Cost کمتر به عنوان Root Port در نظر گرفته و پورت fa0/1 نیز به عنوان Alternate port در نظر گرفته که در وضعیت Blocking قرار دارد.اما چرا fa0/4 را به عنوان Alternate Portدر نظر گرفته است؟زیرا Sender Bridge ID از روی پورت fa0/1 کمتر از fa0/4 است.پورت fa0/4 نیز به عنوان Designated Port در حالت Forwarding می باشد. در ستون بعدی نیز مقدار Priority برای پورت ها را می بینید که به صورت پیش فرض 128 است. در ستون آخر نیز نوع پورت را می بینید که Point-to-Point هستند و اگر share باشند یعنی به Hub وصل هستند.

حال روی پورت fa0/3 در سوئیچ سه، مقدار Cost را افزایش داده،ببینید چه اتفاقی می افتد:

```
SW3# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)# int fa 0/2
SW3(config-if)# spanning-tree vlan 1 cost 100
```

میزان Cost را برای vlan 1 روی Root port سوئیچ سه افزایش داده است.حال اگر روی سوئیچ سه دستور زیر را وارد کنیم موتجه می شویم که مقادیر Root Port و Alternate Port تغییر کرده:

```
SW3# sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    28673
              Address     0011.92b0.f500
              Cost        38
              Port        1 (FastEthernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     000e.837b.3100
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 15

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/1            Root LIS 19        128.1    P2p
Fa0/2            Altn BLK 100       128.2    P2p
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/13           Desg FWD 100       128.13   Shr
```

همانطور که می بینید fa0/2 در حالت Alternate و پورت fa0/1 در نقش Root Port و در وضعیت Listening می باشد.

برای اینکه یک سویچ را Root کینم باید priority آن را تغییر دهیم.ولی جور دیگر نیز می توان این کار را انجام داد. در سوئیچ های سیسکو می تان با استفاده ار یک ماکرو این کار را انجام داد. این ماکرو به شکل زیر است:

**Spanning-tree vlan** *vlan-number* **root {primary|secondary}**

وقتی این دستور را همراه با primary برای هر vlanی وارد می کنیم میزان priority پیش فرض که 32768 است را به 24576 تغییر می دهد.ولی اگر سوئیچی مقدار priority آن کمتر از 24576 باشد،سوئیچی که این دستور را وارد می کند priorityخود را به میزان 4096 تا کمتر از Root Priority تغییر می دهد.

و اگر در سوئیچی از secondary استفاده کنیم،آن سوئیچ به عنوان backup برای primary در نظر گرفته می شود،و در صورت از مدار خارج شدن سوئیچ primary اصلی، تبدیل به primary شود.با این دستور priority سوئیچ secondary به 28672 تغییر می کند، و این یک مقدار ثابت است و و مانند primary به priority دیگر شوئیچ ها نگاه نمی کند.

در انتهای دستور **spanning-tree vlan** *vlan-number* **root {primary|secondary}** می توان از دستور **diameter** نیز استفاده کرد.این مقدار با عمق شبکه تنظیم می گردد.یعنی مقادیر **hello-time** و **dead-interval** را با توجه به عمق شبکه تعیین می کند.

## Rapid Spanning Tree Protocol

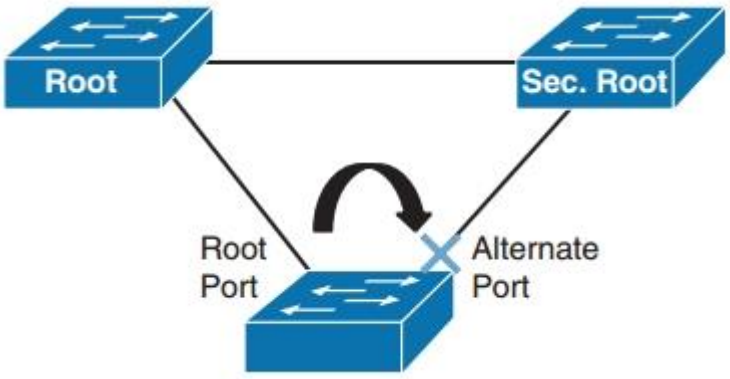
802.1w یا همان Rapid Spanning Tree Protocol (RSTP) برای کاهش زمان همگرایی STP به وجود آمد.این پروتکل با STP است و می تواند در کنار آن کار کند. این پروتکل برای بهبود عملکرد در لایه دو تغییراتی را در خصوصیات پورت های خود داشته است.خصوصیاتی نظیر وضعیت های پورت،نقش های پورت و انواع پورت. وضعیت پورت در RSTP از 5 به 3 کاهش یافته است.در 802.1D STP پنج مرحله Disabled,Blocking,Listening,Learning,Forwarding وجود داشت که در 802.1W RSTP این وضعیت ها به Discarding,learning,Forwarding تغیر کرده است. وضعیت های Discarding , Forwarding وضعیت های پایدار یا Stable هستند و Learning یک وضعیت گذرا یا Transitory می باشد. و البته در RSTP دو نقش به پورت ها اضافه شده است،یکی Alternate Root Port و دیگری Backup Designated Port می باشد. در شکل زیر می توانید وضعیت های STP با کدام وضعیت در RSTP برابر است.

| STP State (802.1D) | RSTP State (802.1w) |
|---|---|
| Disabled | Discarding |
| Blocking | Discarding |
| Listening | Discarding |
| Learning | Learning |
| Forwarding | Forwarding |

در RSTP زمان max age از 20 ثانیه به 6 ثانیه کاهش یافته است.یعنی برابر با عدم دریافت تنها 3 Hello BPDU. و البته همانطور که در شکل بالا مشاهده می کنید حالت موقتی Listening در RSTP نیز حذف شده است. و دیگر غابلیت آن نیز وچود PortFast , UplinkFast,BackboneFast به عنوان استاندارد در RSTP می باشد.

در RSTP دو نقش جدید نیز افزوده شده است، یکی Alternate Port که به عنوان جایگزین Root Port عمل می کند، و Backup Port که به عنوان جایگزین برای Designated Port در Shared segment استفاده می شود.

Alternate Port با از بین رفتن Root Port سریع جایگزین آن می شود، و از زیاد شدن زمان همگرایی را به حداقل می رساند. که در شکل زیر می بینید :




درست مانند UplinkFast در 802.1D STP.

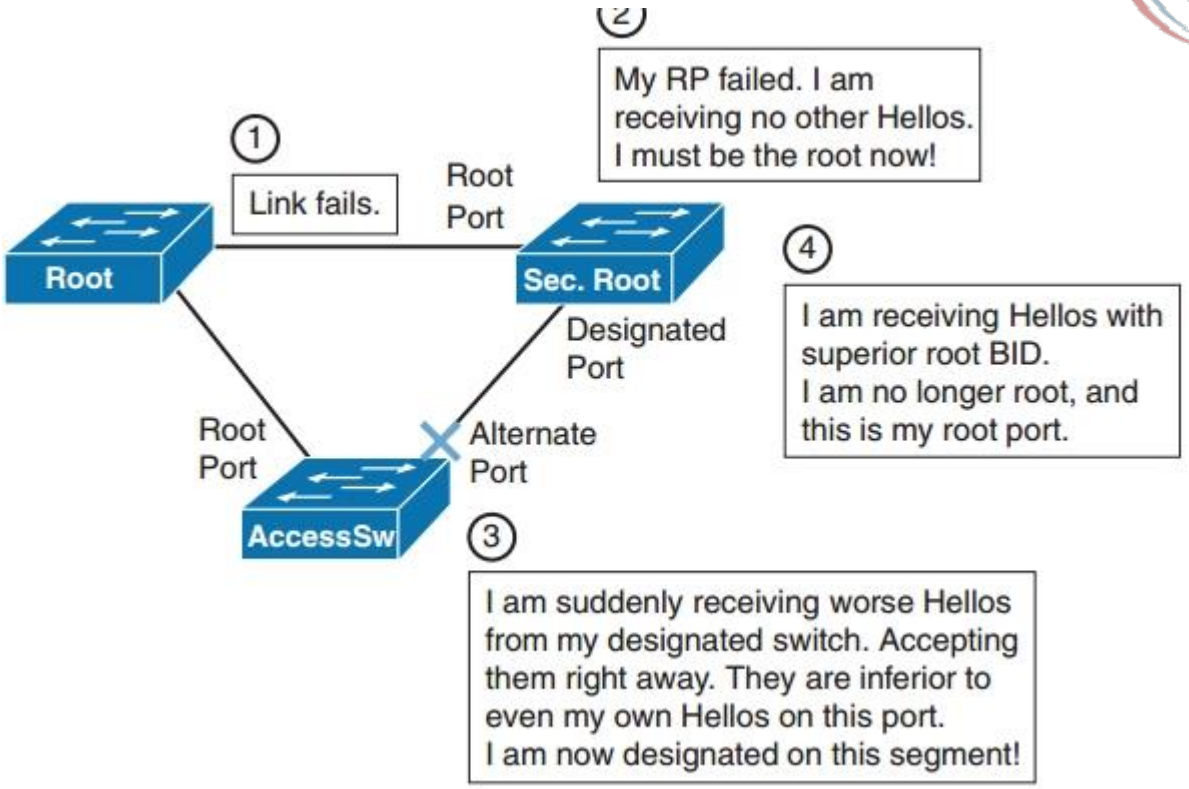
سه نوع پورت در RSTP وجود دارد:

1. Point to Point: پورتی یک سوئیچ را به سوئیچ دیگر وصل می کند.
2. Shared: پورتی که به یک Hub متصل باشد.
3. پورتی که به عنوان Access کارکند و به یک دستگاه مثل کامپیوتر متصل است.باید روی این پورت ها port fast ایجاد شود،زیرا در موقع تغییر توپولوژی ، این لینک ها ترافیک را Discard می کنند.

کار اصلی RSTP روی پورت Point to Point برای بهبود زمان همگرایی می باشد. یک سوئیچ هنگام مذاکره با سوئیچ همسایه اگر Half Duplex باشد متوجه می شود که پورت خود به یک Hub متصل شده است.زیرا hub نمی تواند Full Duplex را پشتیبانی کند.

اگر بخواهیم یک پورت به در حالت Point to Point باشد از دستور **spanning-tree link-type point-to-point** استفاده می کنیم.

در شکل زیر می بینیم که وقتی یک سوئیچ ارتباط خود را با Root از دست می دهد چه اتفاقی می افتد:




همانطور که می بینید وقتی لینک سوئیچ Sec.Root ارتباطش با Root قطع می شود،دیگر BPDU را از آن دریافت نمی کند، پس اینطورنتیجه می گیرد که Root از بین رفته و حالا خودش باید Root شود.سپس به همسایه خود نیز این خبر را می دهد،وقتی AccessSw این BPDU از روی Alternate Port خود دریافت می کند متوجه می شود که این یک Inferior BPDU است،زیرا او همچنان از طریق Root Port خود با Root در ارتباط است و از آن BPDU می گیرد.سپس BPDU مربوط به Root را به Sec.Root ارسال می کند. وقتی سوئیچ Sec.Root این BPDU را دریافت می کند، متوجه می شود که یک Superior BPDU دریافت کرده و دیگر خود را به عنوان Root معرفی نمی کند و پورت در دریافت کننده را به Root Port تبدیل می کند.

در مثال بالا دو نوع BPDU را تعریف کردیم که در زیر به توضیح هر کدام پداخته شده است:

1. Inferior BPDU: وقتی یک سوئیچ ارتباط خود با Root را از دست بدهد، شروع به ارسال این پیغام می کند و در آن خود را به عنوان Root معرفی می کند.
2. Superior BPDU: این پیغام توسط سوئیچی ارسال می شود که Bridge ID بهتری نسبت به Root داشته باشد، و می خواهد Root شود.این پیغام می تواند مشکلاتی نیز داشته باشد که به آن ها نیز خواهیم پرداخت.

## Rapid Per-VLAN Spanning Tree Plus (RPVST+)

RPVST می تواند به ازای هر vlan به صورت مجزا کار کند.یعنی برای هر Vlan یک ساختار و ریشه مجزا وجود داشته باشد. و مانند RSTP دارای مشخصات یکسانی است. نظیر زمان همگرایی، رفتار Hello Packet،انتخاب Root Bridge، وضعیت پورت ها و ....

پیاده سازی +RPVST بسیار ساده است، کافیست در محیط Global دستور زیر را وارد کنید:

**Spanning-tree mode rapid-pvst**

برای Edge-port ها نیز همانطور که قبلا گفته شد از دستور **spanning-tree portfast** در زیر اینترفیس استفاده می کنیم،یا در محیط global از دستور **spanning-tree portfast default** استفاده کنیم.

## Multiple Spanning Trees: IEEE 802.1s

در +RPVST و یا +PVST می توانستیم به ازای هر Vlan یک Root جدید و در نتیجه یک ساختار مجزا برای آن Vlan ایجاد کنیم. این کار باعث می شد که بتوانیم از تمام لینک های شبکه بتوانیم استفاده کنیم. این کار اگر تعداد vlanها کم باشد بسیار می تواند مفید باشد. اما در صورت زیاد بودن vlanها می تواند عملکرد شبکه و کارایی سوئیچ ها را مختل کند.زیرا به ازای هر vlan یک ساختار مجزا ایجاد خواهد شد و root هر vlan پیغام های مخصوص خود را در شبکه ارسال می کند. در MST مانند PVST می توان چند پروسه STP با Root مختلف در توپولوژی ایجاد کرد. برعکس +PVST که برای هر vlan یک پروسه STP را اجرا می کند.در MST یک instance ایجاد می شود و سپس هر تعداد vlan به آن تخصیص داده می شود.مثلا کل vlanها را به دو instance تخصیص داد، و بعد برای فقط آن دو instance در شبکه پروسه STP را اجرا کرد.یک Root برای یک Instance و یک Root برای Instance دیگر.

در شبکه به سوئیچ های که MST را اجرا می کنند، MST region می گویند.که می توان کل و یا تعدادی از سوئیچ ها باشند.

به نحوه پیاده سازی MST دقت کنید:

```
SW1(config)# spanning-tree mst configuration
SW1(config-mst)# name CCIE
SW1(config-mst)# revision 1
SW1(config-mst)# instance 1 vlan 1-500
SW1(config-mst)# instance 2 vlan 501-1000
SW1(config-mst)# instance 3 vlan 1001-2047
SW1(config-mst)# instance 4 vlan 2048-4094
```

ابتدا باید دستور **spanning-tree mode mst** را وارد کرد تا بتوان MST را پیکربندی کرد. با اجرای این دستور به مد MST Configuration وارد می شویم.

سپس یک نام را به آن اختصاص می دهیم. و سپس با دستور بعدی یک revision number به آن می دهیم. در خطوط بعدی نیز instanceها همراه با vlanهای آنها مشخص می شود.در MST می توان تا 15 عدد vlan تعیین کرد.و در هر instance باید رنج vlanهای مورد نظر را وارد کنیم. دقت داشته باشید که مقادیر name و revision number و instanceها در یک region باید باهم یکسان باشد.

اما در MST مفهوم دیگری به نام **IST(Internal Spanning-tree)** وجود دارد. IST برای ارتباط MST با شبکه های غیر MST است که مقدار instance آن نیز صفر می باشد و با CST(common spanning-tree) با همسایه های خود ارتباط برقرار می کند. به شکل زیر دقت کنید:

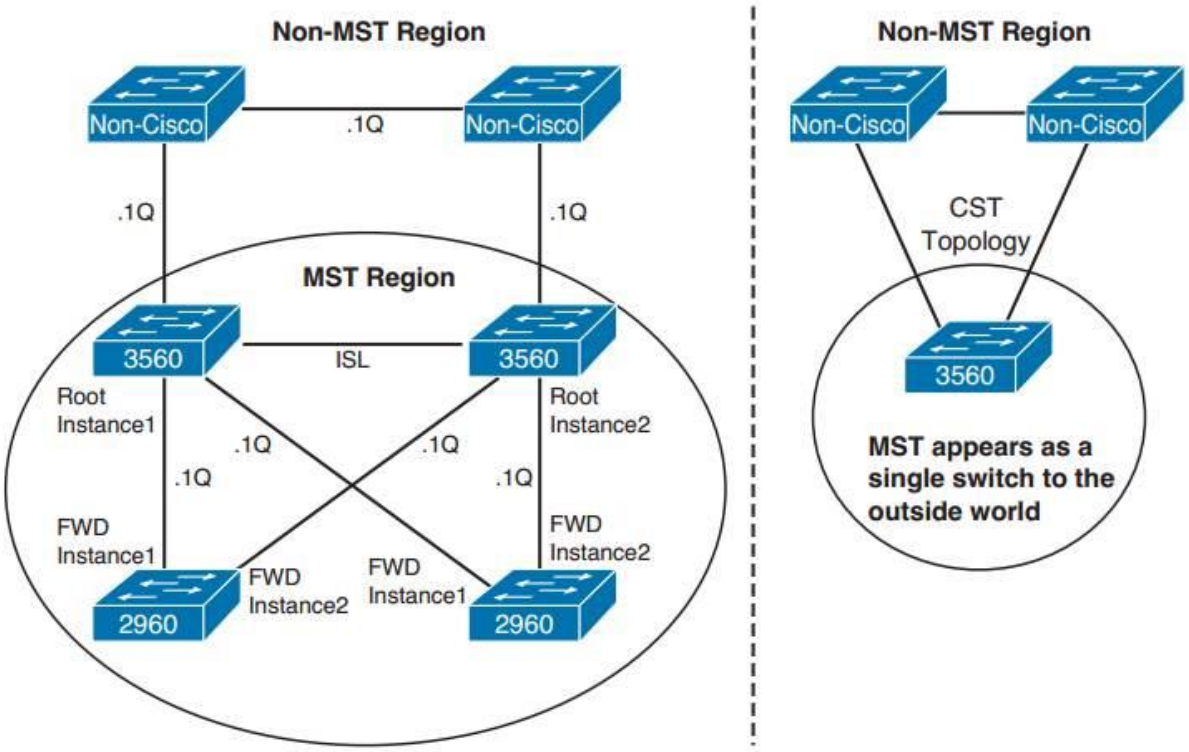



**Figure 3-14** *MST Operations*

در قسمت سمت چپ همانطور که مشخص است چهار سوئیچ پایینی در یک MST Region به دو سوئیچ غیر سیسکو متصل است. در MST دو instance وجود دارد که برای هر instance یک root مجزا اختصاص داده شده است.

اما در شکل سمت چپ از نظر سوئیچ های غیر سیسکویی که توانایی پیاده سازی MST را ندارند، کل شبکه MST به صورت یک سوئیچ دیده می شود و از طریق CST با آن ارتباط برقرار می کند.

با دستور **show current** می توان وضعیت فعلی MST را مشاهده کرد. اگر از محیط MST config خارج نشده باشید چیزی نمایش داده نمی شود و با خروج از این مد کانفیگ apply می شود.

```
SW1(config-mst)# show current
Current MST configuration
Name      []
Revision  0     Instances configured 1

Instance  Vlans mapped
--------  ----------------------------------------------------------------------
0         1-4094
----------------------------------------------------------------------------
```

اگر در مد MST config باشید و دستور **show pending** را وارد کنید می توانید دستورهایی که هنوز apply نشده را نیز مشاهده کنید.

```
SW1(config-mst)# show pending
Pending MST configuration
Name      [CCIE]
Revision  1     Instances configured 5

Instance  Vlans mapped
--------  ----------------------------------------------------------------------
0         none
1         1-500
2         501-1000
3         1001-2047
4         2048-4094
```

بعد از اینکه از محیط MST خارج شدید می توانید با دستور **show spanning-tree mst configuration** نیز می توان از چگونگی پیکربندی MST مطلع شد.

برای تعریف **Priority , Cost , Port Priority , root primary/secondary** مانند دیگر مدهای STP عمل می کنیم با این تفاوت که بجای **vlan** از **mst** *instance-number* استفاده می کنیم. مثلا برای تعریف یک سوئیچ به عنوان root primary برای یک یا چند instance از دستور **spanning-tree mst 1-3 root primary** استفاده می کنیم.

اگر در یک MST region سوئیچ ها از vtp version3 پشنیبانی کنند، می توان از آن برای همسان کردن (synchronization) کانفیگ MST بین سوئیچ ها استفاده کرد. و در این صورت سوئیچ هایی که MST region configuration یکسانی داشته باشند عضو یک MST region می شوند.

```
SW1(config)#vtp domain CCIE
Changing VTP domain name from NULL to CCIE
SW1(config)#vtp version 3
SW1(config)#vtp mode server mst
Setting device to VTP Server mode for MST.
SW1(config)#do vtp primary mst
This system is becoming primary server for feature  mst
No conflicting VTP3 devices found.
Do you want to continue? [confirm]
SW1(config)#
*May 13 18:05:47.189: %SW_VLAN-4-VTP_PRIMARY_SERVER_CHG: aabb.cc00.0100 has become the primary server for the MST VTP feature
SW1(config)#
```

## Protecting and Optimizing STP

در این بخش می خواهیم در مورد ابزارهای جهت حفاظت از STP در مقابل مشکلات و حملات مطرح کنیم.

## PortFast Ports

این ابزار بر روی پورت های access مورد استفاده قرار می گیرد زمان تغییر وضعیت یک پورت به forward را کاهش می دهد. بر روی این پورت حالت های **learning(Forward Delay) و listening** وجود ندارد.یعنی پورتی که به کلاینت متصل باشد، 30 ثانیه در زمان رسیدن به حالت forward صرفه جویی می کند. اگر در یک PC از طریق DHCP بخواهد IP دریافت کند به دلیل میزان زمان forward delay دچار مشکل می شود، ولی با portfast می توان از وقوع چنین مشکلاتی نیز جلوگیری کرد.

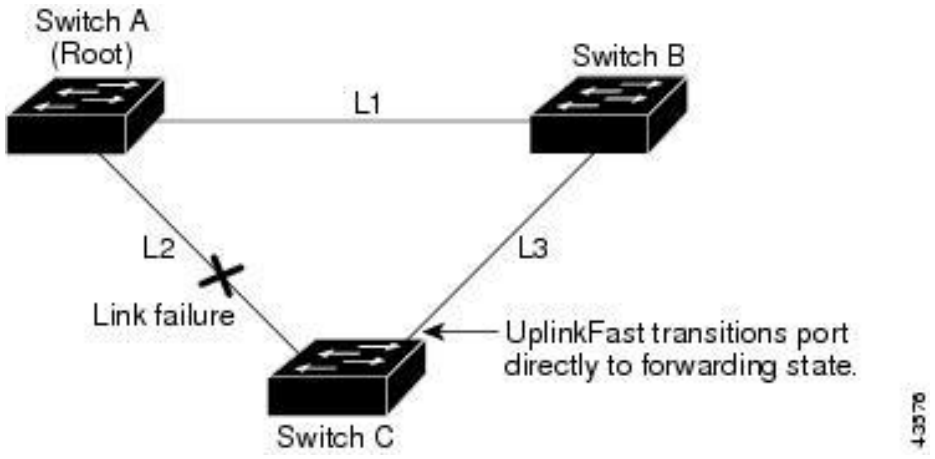
این دستور را یا می توان مستقیم زیر اینترفیس وارد کرد مانند **spanning-tree portfast** یا اینکه به صورت globally به این شکل نوشت: **spanning-tree portfast default**.در حالت دوم تنها روی پورت های access عمل می کند. و اگر روی پورتی که access بود و قصد اجرای portfast را روی آن نداشتیم ، می توانیم از دستور **spanning-tree portfast disable** استفاده کنیم و portfast را از روی آن پورت مشخص غیر فعال کنیم.

اگر روی یک پورت access که به یک سرور یا روتر متصل است و می خواهید روی آن نیز portfast فعال شود از دستور **spanning-tree portfast traunk** استفاده می کنید.

## UplinkFast and BackboneFast

در کتاب CCIE v5 به موضوعاتی نظیر uplinkfast و backboneFast اشاره نشده ولی بخاطر اهمیت موضوع در این کتاب گنجانده شده است.

تعریف uplinkfast را با توجه به شکل زیر انجام می دهیم:




در شکل بالا Switch A به عنوان Root شناخته شده است، و Switch C دو مسیر برای رسیدن به Root دارد که مسیر L2 را ترجیح می دهد. اما اگر پورت ارتباط Switch C به هر دلیلی با Switch A از روی این لینک قطع شود، لینک L3 که در وضعیت Block است باید به حالت forward برود. که این تبدیل حالت نیاز به سپری شدن زمان برای دو حالت Leastening و Learning دارد.

Uplinkfast از هدر رفتن این زمان (30 ثانیه) جلوگیری کرده و زمان همگرایی را کاهش می دهد.

Uplinkfast روی سوئیچ access باید کانفیگ شود. یعنی حتی اگر access هم نباشد بعد از اجرای این دستور تبدیل به سوئیچ access می شود. به این صورت که priority سوئیچ را به 49152 تغییر می دهد و به مقدار cost هر پورت 3000 اضافه می کند تا مطمئن شود که این سوئیچ به عنوان root یا transit عمل نمی کند.

و برای اینکه نیاز به ارسال TCN در شبکه نباشد ، خود سوئیچ شروع به ارسال MACهای مربوط به پورت های access خود به یک آدرس multicast برای دیگر سوئیچ ها می کند. یعنی با source-mac سیستم های متصل به پورت های acces به destination-mac برای آدرس multicast می کند.

دستور اجرای UplinkFast نیز به صورت global روی سوئیچ access است.

**Spanning-tree uplinkfast**

## BackboneFast

در مثال بالا دیدیم که یک سوئیچ Access مستقیما به سوئیچ root وصل بود و بعد از قطعی لینک بلافاصله پورت block وارد وضعیت forward می شد. اما اگر سوئیچ access به وسیله یک سوئیچ دیگر به سوئیچ root متصل باشد و لینک در سوئیچ بالاتر به سوئیچ root قطع شود، سوئیچ access باید مدت زمان Max-age را سپری کند، که برابر است با زمان دریافت 10 عدد BPDU، یعنی 20 ثانیه.

مکانیزم کارکرد BackboneFast به این صورت است که سوئیچ وقتی یک BPDU را دیافت نکند بلافاصله به سوئیچ بالاتر خود پیغامی را تحت عنوان RLQ(Root Link Query) می فرستد و از سوئیچ بالاتر خود درباره Root سوال می کند. اگر سوئیچ بالاتر ارتباطش با Root به صورت مستقیم باشد و قطع شده باشد به سوئیچ پائین خود می گوید که ارتباطش با Root قطع شده است، و اگر ارتباط آن به وسیله یک سوئیچ دیگر باشد ، یک پیغام RLQ به سوئیچ لابتر خود می فرستد. به این وسیله سوئیچی که BPDU دریافت نکرده متوجه می شود که آیا لینکی که به سمت Root است قطع شده است یا خیر. اما یادمان نباشد که BackboneFast را باید روی همه سوئیچ های شبکه اجرا کنیم. دستور backbonefast نیز باید به صورت global نوشته شود.

**Spanning-tree backbonefast**

## Root Guard, BPDU Guard , and BPDU Filter: Protecting Access Ports

لینک های access برای اتصال به دستگاه های end-user می باشد. برای همین روی این لینک ها portfast را فعال می کنیم تا زمان forward-delay را سپری نکند و پورت مستقیم به حالت forward برود. اما اگر به هریک از پورت های access یک سوئیچ متصل شود، می تواند باعث ایجاد Loop در شبکه شود. حتی می تواند یک مشکل امنیتی به وجود آورد. به این صورت که یک سوئیچ به BID کوچیکتر به پورت وصل شود و به عنوان root شناخته شود. با اینکار تمام ترافیک STP به سمت این سوئیچ ارسال می شود. که دستور آن روی پورت access به صورت **spanning-tree bpduguard enable** می باشد. و اگر بخواهیم روی تمام پورت های access این خصوصیت فعال باشد باید به صورت global دستور **spanning-tree portfast bpduguard default** استفاده شود. و اگر بخواهیم این خصوصیت را از روی پورتی برداریم از دستور **spanning-tree bpdiguard disable** استفاده می کنیم.

اما وقتی روی پورت access به همراه portfast دستور BPDU Guard را وارد کنیم، اگر روی آن پورت یک سوئیچ متصل شود و اقدام به ارسال BPDU کند، به محض اینکه سوئیچ روی پورت خود BPDU دریافت کند، وضعیت آن پورت error disable تبدیل می شود. و اینکار مانع ایجاد Loop می شود.

وقتی روی یک پورت access، Root Guard را فعال کنیم،این پورت در مقابل BPDUهای با BID بهتر محافظت می کند. اگر روی این پورت یک سوئیچ به BID بهتر متصل شود، پورت به حالت root- inconsistent می رود. در این حالت هیچ فریمی دریافت یا ارسال نمی شود تا زمانی که Superior BPDU دریافت نشود.این زمان در STP برابر با Max-age- message می باشد و در RSTP برابر است با زمان عدم دریافت 3 عدد hello . Root Guard را می توان به ازای پورت فعال کرد که ار دستور **spanning-tree guard root** روی هر اینترفیس استفاده می کنیم. و برای دیدن اطلاعات پورت هایی که در وضعیت root-inocondidtent قرار دارند از دستور **show spanning-tree inconsistentports** استفاده می کنیم.

و اما BPDU Filter که مرتبط با توقف و ارسال BPDU روی یک پورت Access می باشد و رفتار آن بسته نوع فعال کردن آن متفاوت است.

وقتی دستور **spanning-tree portfast bpdufilter default** را به صورت global وارد کنید،روی تمام پورت های accessی که portfast روی فعال شده باشد، اجرا می شود. بهد از اجرای آن ، پورت ها شروع به ارسال PBDU در هر 2ثانیه می کنند، و اگر به ازای ارسال 10 BPDU جوابی از طرف مقابل دریافت نکند، ارسال BPDU را قطع می کند. در واقع بعد از ارسال یازده BPDU (یکی در زمان بالا آمدن پورت و ده تا در زمان های Hello interval). و سپس در صورت عدم دریافت پاسخ ارسال BPDU را متوقف می کند. ولی پورت همچنان آمادگی دریافت BPDU را دارد، چه در زمان ارسال 10 عدد BPDU و چه بعد از آن. و اگر BPDUی را دریافت کند، BPDU Fliter روی آن پورت غیر فعال می شود. و پورت شروع به ارسال و دریافت BPDU طبق روال STP می کند. و اگر بخواهیم روی پورت خاصی این خصوصیت را غیر فعال کنیم از دستور **spanning-tree bpdufilter disable** روی آن پورت استفاده می کنیم.

و اگر به صورت local روی یک پورت دستور **spanning-tree bpdufilter enable** را فعال کنیم، ارسال و دریافت BPDUها متوقف خواهد شد.

نوع استفاده از BPDU filter به نوع پیکربندی آن دارد. اگر آن را global کانفیک کنید، بعد از گذشت زمان تعریف شده در صورتی که BPDU دریافت نکند یعنی device مقابل قادر به مکالمه از طریق STP نیست و ارسال BPDU کار بیهوده ای می باشد. و اگر از طرف مقابل BPDU دریافت کند، BPDU Filter روی آن پورت غیر فعال می شود و تا زمانی که ورت down و بعد up نشود غیر فعال خواهد ماند.

اگر روی یک پورت به صورت local کانفیگ شود، هیچ BPDUی ارسال نمی شود و در صورت دریافت آن را Drop می کند. از اینکار برای تبدیل شبکه به چند دامین STP استفاده می شود.در این حالت STP روی آن پورت کارکردی ندارد و نمی تواند جلوی Loop را در شبکه بگیرد، و این وظیفه مدیر شبکه است تا بتواند جلوی Loop را در این شرایط بگیرد.

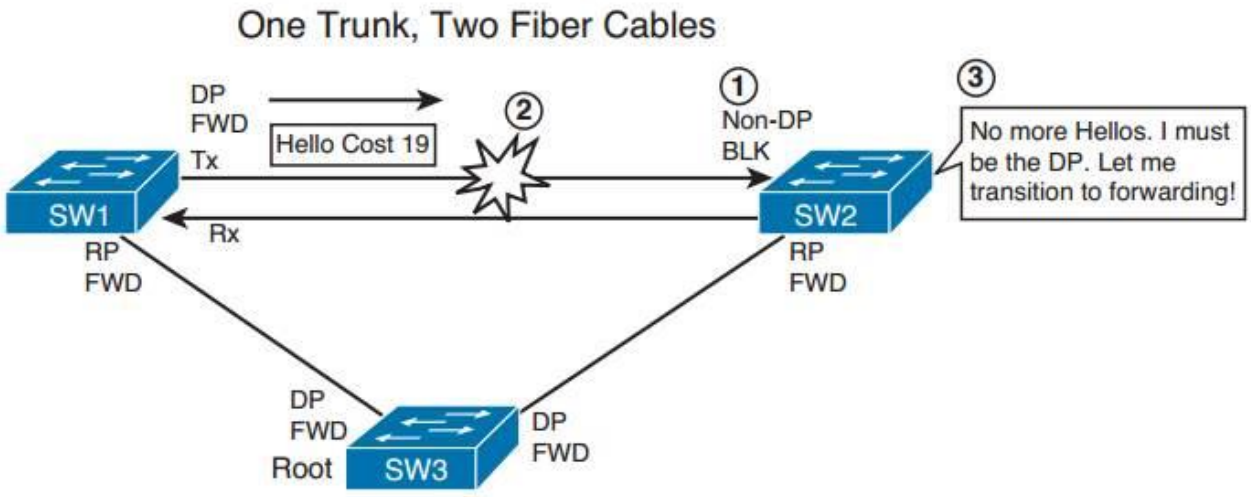
دو نوع BPDU وجود دارد که می تواند مشکل ساز باشند:

1. **Inferior BPDU:** این BPDU زمانی ارسال می شود که یک سوئیچ به Root خود دسترسی نداشته باشد،در این صورت خود را Root معرفی می کند.

2. **Superior BPDU:** این BPDU را سوئیچی ارسال می کند که BID بهتری نسبت به Root فعلی داشته باشد و در حالت خود را Root معرفی می کند. اما مشکل ساز بودن این BPDU که در تعریف Root Guard نیز گفته شد می تواند این صورت باشد که این BPDU از طرف سوئیچی باشد که از عمد در شبکه قرار گرفته و قصد Root شدن را دارد.

## Protecting Against Undirectional Link Issues

گاهی ممکن است ارتباط بین دو سوئیچ یک طرفه شود. که می تواند به دلیل cabaling متفاوت در دو سر لینک یا قطع یک core در فیبر نوری و یا مشکل در GBIC(GigaBit Interface Convertor) باشد که ارتباط یک طرفه می شود. یعنی یکی از طرفین متوجه این قطعی نمی شوند. مثلا روی یک لینک ارسال دارد می کند ولی طرف مقابل دریافتی ندارد.این در حالتی هست که لینک connected نمایش داده می شود. به شکل زیر دقت کنید:




در شکل بالا سوئیچ 3 ، root می باشد، و لینک سوئیچ دو به سمت سوئیچ یک bloack است. اگر این لینک یک طرفه شود ، سوئیچ دو دیگر روی آن لینک BPDU دریافت نمی کند و وضعیت پورت را designated تغییر می دهد و پورت در حالت forwarding قرار می گیرد. به همین صورت یک Loop ایجاد می شود. اما UDLD این یک طرفه شدن را به وسیله ارسال و دریافت UDLD Message در بازه 15 ثانیه و عدم دریافت پاسخ در 3 تا 15 ثانیه تشخیص می دهد و مانع از ایجاد Loop می شود.

UDLD در دو مد کار می کند:

1. **UDLD Normal:** در این حالت در صورتی که متوجه شود پورت پاسخی را دریافت نمی کند،بخشی که برای ارسال استفاده می شود را به حالت error disable می برد.
2. **UDLD Aggressive:** در این حالت بعد از عدم دریافت پاسخ از سه UDLD Message، روی آن پورت به فاصله یک ثانیه هشت پیغام UDLD دیگر نیز ارسال می کند، که در صورت عدم دریافت پاسخ هر دو مسیر را به حالت error disableمی برد.

برای UDLD از دستور **udld {enable | aggressive}** استفده می کنیم که این دستور روی تمام لینک های فیبر اثر می گذارد. و برای فعال کردن روی دیگر لینک ها روی آن اینترفیس از دستور **udld port [aggressive]** استفاده می کنیم.اگر aggressive را وارد نکنید از مد normal استفاده می کند. برای غیر فعال کردن udld روی یک لینک فیبر از **no udld enable** و روی دیگر پورت ها از **no udld port** زیر اینترفیس استفاده می کنیم.

اما اگر دلیل این یک طرفه شدن به دلیل عدم دریافت BPDU نباشد، واقعا Loop اتفاق می افتد. در این شرایط از Loop Guard استفاده می شود. در loop guard اگر روی پورت block هیچ BPDUی دریافت نشود، آن پورت به حالت Loop-Inconsistent می رود و هیچ ترافیکی ارسال و دریافت نمی شود. و به محض دریافت BPDU پورت از این حالت خارج می شود.

از دستور **spanning-tree global-default loopguard enable** به صورت global و از دستور **spanning-tree guard loop** در زیر اینترفیس برای فعال کردن Loop Guard استفاده می شود.

برای غیر فعال کردن آن نیز باید زیر اینترفیس از دستور **no spanning-tree guard loop** استفاده کنیم.