CCNP : Switch

Cisco Certified Network Professional

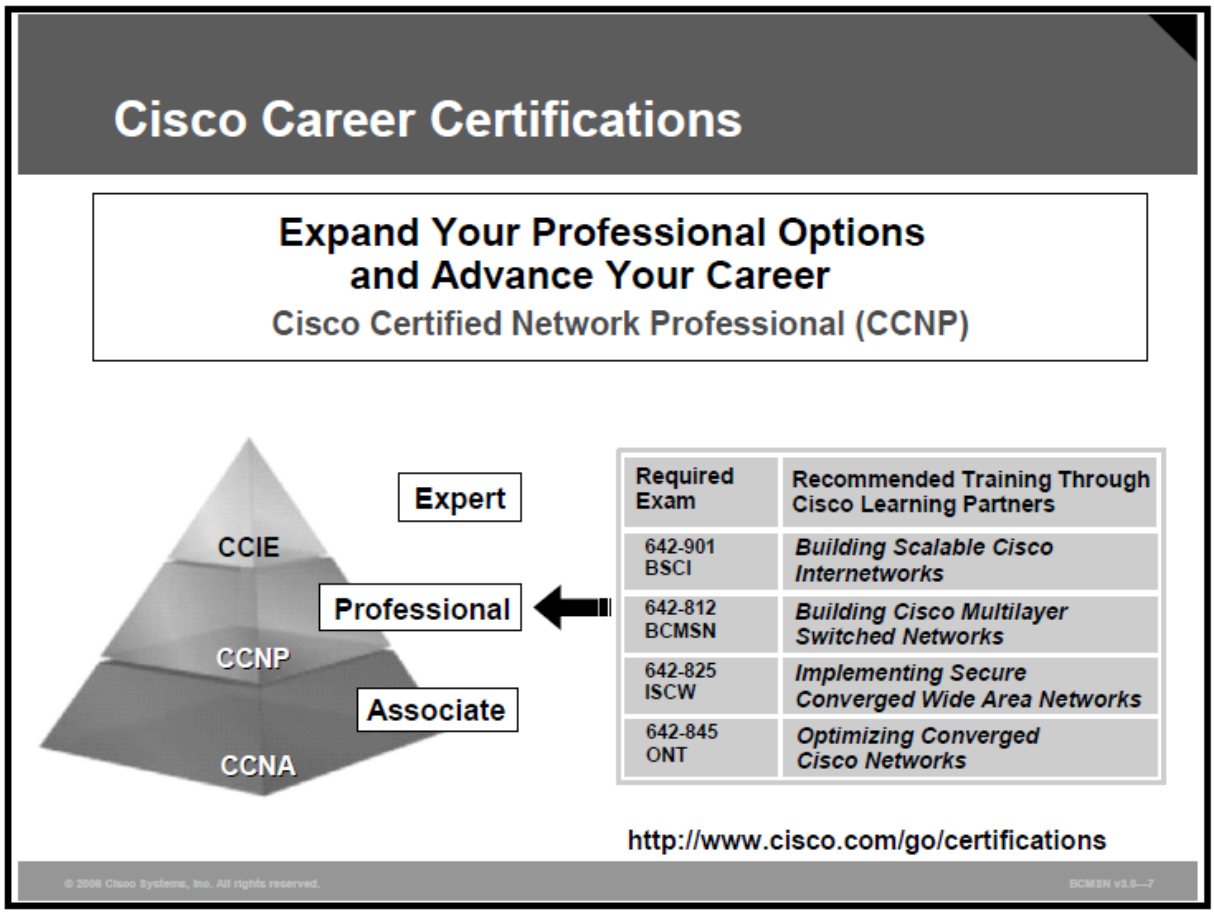
Study Guide

Engineer SHOWAN KOLIJI

مهندس شوان کلیجی

Email : **Kolijis@yahoo.com**

Koliji_Cisco@yahoo.com



CCNP Switch

Cisco Certified Network Professional

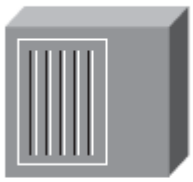
: Switch Operation

سوئیچ از نظر ظاهری شباهت زیادی به هاب Hub دارد با این تفاوت که قیمت آن از Hub گران تر است . سوئیچ بسیار هوشمندتر و کاراتر از یک Hub عمل می کند . Hub در هنگام دریافت یک بسته آن را از تمام پورت هایش عبور می دهد ولی سوئیچ ترافیک را روی کل پورت های خود Forward نمی کند بلکه MAC Address بسته را بررسی می کند و بر اساس آن آدرس بسته را به پورتی ارسال می کند که کامپیوتر گیرنده اطلاعات متصل می باشد .

در شبکه های LAN قدیمی که از Hubها استفاده می شد از مکانیسم خاصی به نام CSMA/CD که نحوه ارسال و دریافت فریم ها را کنترل می کرد استفاده می شد . به دلیل استفاده تمامی کامپیوترها از پهنای باند مشترک ، در صورتی که یکی از دستگاه ها اقدام به ارسال فریمی نماید ، دیگران تنها باید منتظر دریافت آن فریم بوده و نمی توانند در این زمان اقدام به ارسال اطلاعات به سمت دستگاه های دیگر نمایند . اگر دو دستگاه به صورت همزمان اطلاعاتی را ارسال کنند تصادم یا Collision رخ خواهد داد که به این شرایط Half – Duplex اطلاق می شود . کلیه دستگاه های متصل به یک Hub عضوی از یک Collision Domain هستند .

سوئیچ عملیات ارسال فریم را بر اساس MAC گنجانده شده در داخل فریم لایه 2 انجام می دهد و وسعت گسترش Collision Domain بسیار محدود است یعنی هر پورت سوئیچ و کامپیوتری که مستقیما با آن در تماس است در داخل یک Collision Domain جداگانه قرار دارند . تمامی دستگاه های متصل به پورت های سوئیچ به صورت Full – Duplex عمل می نمایند یعنی کلیه دستگاه ها همزمان می توانند اقدام به ارسال و دریافت اطلاعات نمایند . فریم های معیوب و بد توسط سوئیچ به دستگاه های دیگر ارسال نمی شود . سوئیچ می تواند ترافیک Broadcast را محدود به یک حجم خاصی نماید .

تفاوت سوئیچ با هاب :



Hub

- Collision : CSMA/CD
- Half – Duplex
- Bandwidth Sharing
- Error Propagation
- High Traffic
- Security Treatment

Switch

- No Collision
- Full – Duplex
- No Bandwidth Sharing
- No Error Propagation
- Low Traffic
- No Security Treatment

Switch Layer 2 :

حالت هایی که سوئیچ بسته ها را Flood می کند :

- Unknown Unicast MAC – Address
- Broadcast : MAC : FFFF.FFFF.FFFF
- Multicast (Default)

جدول MAC – Table :

در زمان ارتباطات کامپیوترها با سوئیچ در داخل سوئیچ جدولی ایجاد و کامل خواهد شد به نام MAC – Address – Table که این جدول شامل کلیه آدرس های MAC – Address کامپیوترها و تجهیزات شبکه ای می باشد که به پورت های سوئیچ متصل می باشند . مقادیر داخل جدول به صورت Dynamic بروزرسانی (Update) خواهد شد . با کامل شدن این جدول سوئیچ بر اساس اطلاعات داخل این جدول بسته ها را به مقصد ارسال خواهد کرد .

در سوئیچ به دو روش زیر جدول MAC – Table پر خواهد شد :

- **Static**

با دستور زیر MAC – Address دستگاه های مورد نظر را به صورت Static وارد می کنیم :

Switch (config) # MAC – Address – Table Static H.H.H VLAN vlan-id Interface type mod/num

- **Dynamic**

در این حالت سوئیچ ، MAC – Address هر دستگاهی که اقدام به ارسال بسته ای بکند را به صورت Dynamic در جدول MAC – Table خود Learn می کند . در این حالت Learning از طریق Source MAC صورت می گیرد و Forwarding از طریق Destination MAC .

دستور دیدن جدول MAC – Table :

Switch # Show MAC – Address – Table [Dynamic | Static] [VLAN vlan-id] [Interface type mod/num] [Address MAC – Address]

دستور پاک کردن جدول MAC سوئیچ :

Switch # Clear MAC – Address Dynamic [VLAN vlan-id] [Interface type mod/num] [Address MAC – Address]

این دستور فقط MACهایی که به صورت Dynamic ذخیره شده اند را پاک می کند .

نکته :

زمان Update جدول MAC – Table در سوئیچ 300 ثانیه می باشد و قابل تغییر است .

دستور تغییر زمان Update جدول MAC – Table :

Switch (config) # MAC – Address – Table aging – time Seconds

دستور دیدن زمان Update جدول MAC – Table :

Switch # Show MAC – Address – Table aging – time

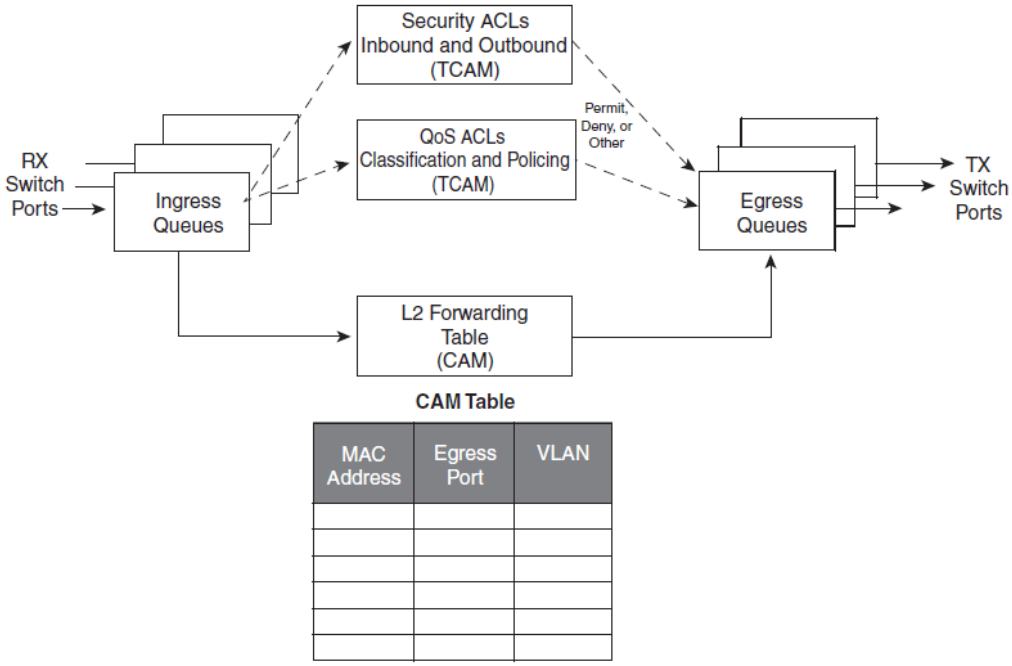
نکته :

در صورتی که اطلاعاتی توسط یک سوئیچ دریافت شود که مقصد آن در لیست MAC – Table موجود نباشد ، سوئیچ آن بسته را به کلیه پورت های خود ارسال خواهد کرد . مانند یک هاب عمل می کند .

دستور دیدن جدول TCAM :

Switch # Show Controller TCAM

CAM Table : Content Addressable Memory Table



: CAM Table

تمامی سوئیچ های کاتالیست سیسکو از جدول CAM برای L2 Switching استفاده می کنند . زمانی که فریمی توسط سوئیچ دریافت می شود ، آدرس Source Mac آن در داخل جدول CAM به ثبت خواهد رسید . در حالت کلی شماره پورت دریافت کننده فریم ، شماره VLAN آن و نیز زمان دریافت در مقابل آدرس MAC در داخل جدول CAM به ثبت خواهد رسید . در واقع جدول CAM Table همان جدول MAC Table است که به صورت سخت افزاری در سوئیچ قرار داده شده است تا سرعت پردازش را بالا ببرد . اطلاعات هر دو جدول یکسان است .

نکته :

زمانی که یک فریم توسط پورتی از سوئیچ دریافت می شود ، فریم مزبور در داخل Ingress Queueها مربوط به پورت دریافت کننده قرار می گیرند (همانگونه که در شکل صفحه قبل مشاهده می کنید) هر Queue می تواند چندین فریم در حال انتظار باشد و همچنین سطح متفاوتی از اولویت را می توان بر روی هر کدام از Queueها اختصاص داد . پورت های سوئیچ را می توان به گونه ای تنظیم کرد که فریم های حساس به زمان ، مانند ترافیک صوت و تصویر را زودتر از دیگر فریم ها پردازش و ارسال نماید .

همانگونه که در شکل صفحه قبل مشاهده می کنید اگر بر روی سوئیچ Security ACLs و QoS ACLs نوشته شده باشد ، اگر فریمی از پورتی وارد سوئیچ شود (Ingress Queueها) همزمان با هر سه یعنی Security ACLs و QoS ACLs و CAM Table بررسی می شود و بعد ارسال خواهد شد . هیچ کدام بر دیگری اولویت ندارند چون برای هر کدام از آنها یک سخت افزار اختصاص داده شده است .

نکته :

فریم ها که قبلا در صف های Ingress Queueها قرار داشتند بعد از بررسی توسط سخت افزارهای Security ACLs و QoS ACLs و CAM Table در صف های دیگری قرار می گیرند که مربوط به پورت خروجی است و Egress Queueها نام دارند .

MLS : MultiLayer Switch

سوئیچ های کاتالیست سیسکو از دو نوع مختلف پروسه MLS پشتیبانی می کنند که عبارتند از Route Caching که روش قدیمی تر بوده و Topology – Based که متد جدیدتری می باشد .

- Route Caching

در این متد نیاز به استفاده از هر دوی Route Processor (RP) و Switch Engin (SE) وجود دارد بدین ترتیب که اولین پاکت هر کدام از جریان های ترافیکی باید از داخل RP با جدول Routing Table چک می شود و مقصد یا پورت خروجی آن مشخص می شود . سپس SE نتیجه این عملیات را دریافت کرده و یک میانبر در داخل جدول MLS خود به ثبت می رساند و از این به بعد پاکت های بعدی مربوط به همان جریان نیازی به عبور از RP ندارند و از طریق اطلاعات میانبر ثبت شده در داخل جدول MLS و توسط SE به مقاصد خود ارسال خواهند شد . این روش سرعت بالایی دارد و در سوئیچ های قدیمی استفاده می شد .

- Topology – Based

در این متد از یک سخت افزار منحصر به فرد استفاده می شود بدین ترتیب که سوئیچ از روی اطلاعات مربوط به جدول Routing یک دیتابیس جداگانه ایجاد کرده و آن را در داخل یک سخت افزار مخصوص قرار می دهد . پاکت های دریافت شده توسط سوئیچ با بررسی این دیتابیس به مقاصد خود ارسال می شوند که به دلیل انحصاری بودن این سخت افزار برای هدایت پیام ها ، سرعت انجام کل پروسه بسیار بیشتر از متد قبلی است . محتویات این دیتابیس کاملا با جدول Routing یکسان بوده و به محض بروز تغییری در جدول Routing این جدول نیز به روز خواهد شد. این متد در سیسکو به نام (CEF) Cisco Express Forwarding نامیده می شود .

FIB Table : Forwarding Information Base

جدول FIB از روی جدول Routing ایجاد می گردد که این جدول نیز به صورت سخت افزاری می باشد. فقط یک رکورد اضافی نسبت به جدول Routing دارد که Next – Hop MAC – Address است . که در آن MAC Addressهایی را ذخیره می کند که پاکت ها باید به آنها ارسال شود یعنی خودش قبلا ARP زده و MAC آنها را به دست آورده است و ذخیره کرده تا سرعت ارسال بسته ها بالا رود . چون در حالت Forwarding فریم ها تغییر می کنند با یک قسمت سخت افزاری به نام L3 Frame Rewrite این کار را انجام می دهد . در سوئیچ ها برای پردازش پاکت هایی که به صورت نرمال می باشند و هدف از آنها Forwarding می باشد از این سخت افزار استفاده می شود ولی برای پاکت هایی که باید پاسخی را دریافت کنند مانند بسته های ARP نمی توانند از این سخت افزار استفاده کنند بلکه از نرم افزار سوئیچ ها استفاده می کنند .

در زیر جدول FIB و جدول CAM را مشاهده می کنید :

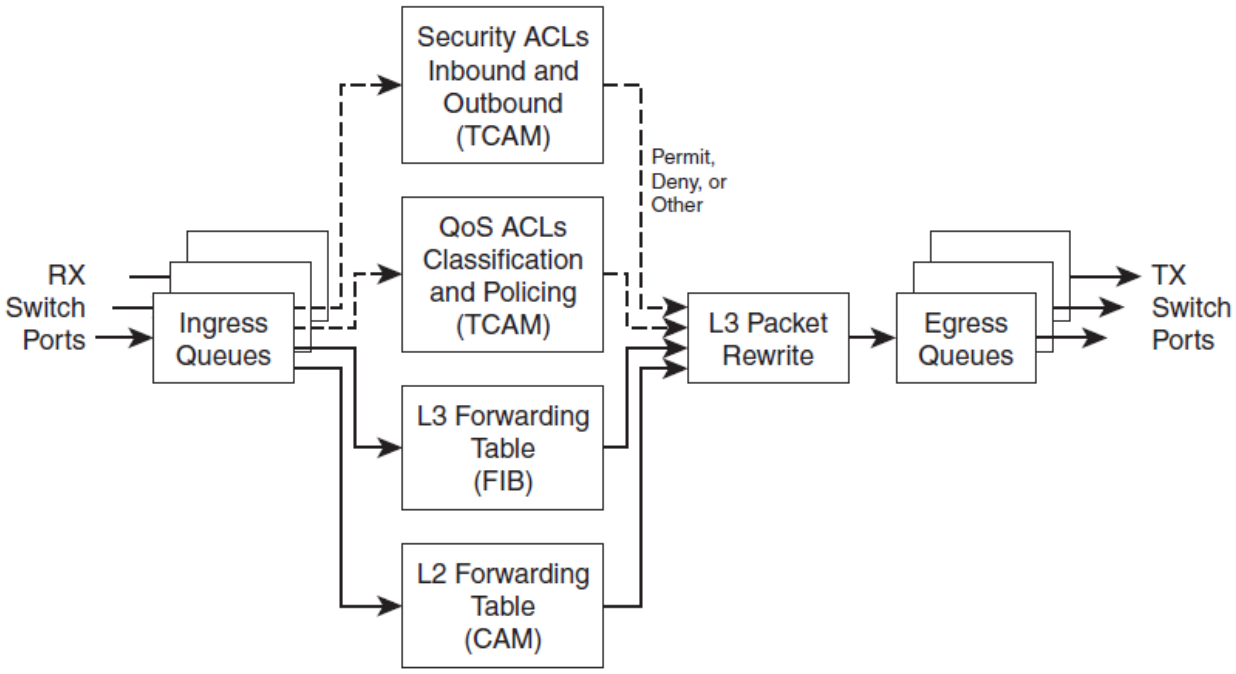
CAM Table

MAC Address	Egress Port	VLAN

FIB Table

IP Address	Next-Hop IP Addr	Next-Hop MAC Addr	Egress Port

TCAM Table : Ternary Content – Addressable Memory Table



ACLها برای بررسی و کنترل ترافیک مورد استفاده قرار می گیرند . هر ACL از یک یا چندین قانون یا ACL Entry (ACE) تشکیل شده است که دستگاه ها باید به ترتیب اولویت این قوانین را در مورد هر پاکت مورد بررسی قرار دهند . در سوئیچ های Multilayer پروسه بررسی ACLها توسط سخت افزار انجام می پذیرد . به عبارتی دیگر ، سوئیچ های Multilayer تنها با یک بار مراجعه به جداول موجود در TCAM خود می توانند پیام ها را با تمامی قوانین مربوط به Security ACLها و یا QoS ACLها مقایسه نمایند . حتی برخی از سوئیچ ها دارای بیش از یک TCAM بوده و بنابراین عملیات بررسی پیام ها در هر دو جهت ورودی و خروجی به صورت همزمان با عملیات L2 / L3 Forwarding صورت می گیرد . جدول TCAM دارای دو بخش زیر است :

- Feature Manager (FM) : بعد از ایجاد یک ACL و مشخص شدن قوانین ، FM باعث می شود تا تمامی این قوانین به صورت مجتمع در داخل حافظه TCAM قرار بگیرد تا سوئیچ تنها با یک بار مراجعه به این جدول قادر به بررسی تمامی پیام ها با قوانین باشد.
- Switching Database Manager (SDM) : در مورد برخی از سوئیچ های سیسکو می توانید حافظه TCAM را به پارتیشن های مختلف تقسیم بندی کنید که SDM وظیفه مدیریت پارتیشن ها را بر عهده دارد .

: Switch Port Configuration

استاندارد Ethernet :

استاندارد Ethernet در حدود سال 1980 با نام استاندارد IEEE 802.3 پایه ریزی شد. این استاندارد در گذشته دارای سرعتی معادل 10 Mbps و با استفاده از کابل های Coaxial و Twisted Pair شکل گرفت. امروزه شبکه های اترنت بسیار محبوب هستند و پیشرفت قابل توجهی در آنها به وقوع پیوسته است . شبکه اترنت امروزی گسترش یافته و با تجهیزات آن با سرعت های 100 Mbps و 1 Gbps و 10 Gbps در دسترس می باشند .

معرفی انواع استانداردهای Ethernet :

- **10Base 2**

در این استاندارد طول کابل می تواند 185 متر باشد که از کابل های Coaxial نوع Thinnet استفاده می شود و حداقل طول کابل بین دو کامپیوتر 0.5 متر می باشد . از کابل های Thinnet در شبکه هایی با توپولوژی Bus استفاده می شود .

- **10Base 5**

در این استاندارد طول کابل می تواند 500 متر باشد که از کابل های Coaxial نوع Thicknet (ضخیم) استفاده می شود و حداقل طول کابل بین دو کامپیوتر 2.5 متر می باشد.

- **10Base T**

در این استاندارد طول کابل می تواند 100 متر باشد که از کابل های Twisted Pair استفاده می شود و T در این عبارت حرف اول Twisted Pair می باشد که از نوع UTP CAT3 استفاده می شود ولی از کابل STP و سایر کابل های UTP هم می توان در این استاندارد استفاده کرد و در این توپولوژی از هاب یا سوئیچ استفاده می شود . همچنین در این استاندارد هر کامپیوتر با یک کابل Twisted Pair به هاب یا سوئیچ متصل می شود .

- **100Base TX**

این استاندارد به نام IEEE 802.3u یا FastEthernet شناسایی می شود. طول کابل می تواند 100 متر باشد و از کابل های Twisted Pair از نوع UTP CAT5 ، CAT6 ، 5e استفاده خواهد شد و از دو رشته کابل برای تبادل اطلاعات استفاده می شود .

100Base FX

در این استاندارد بیشتر از کابل فیبرنوری Multimode استفاده می شود . طول کابل می تواند 412 متر باشد و برای اتصال در این استاندارد بیشتر از کانکتورهای نوع ST و SC استفاده خواهد شد .

1000Base T

این استاندارد به نام IEEE 802.3ab شناسایی می شود. طول کابل می تواند 100 متر باشد و از کابل های Twisted Pair از نوع UTP CAT5 ، CAT6 ، CAT 5e و کانکتور RJ – 45 استفاده می شود و از چهار جفت سیم برای تبادل اطلاعات استفاده می شود .

1000Base SX

این استاندارد به نام IEEE 802.3z یا GigabitEthernet شناسایی می شود. در این استاندارد از دو نوع کابل فیبرنوری Multimode با قطر هسته 62,5 میکرون که حداکثر طول سیم برابر با 220 متر و قطر هسته 50 میکرون که حداکثر طول سیم برابر با 550 متر می باشد استفاده می شود.

1000Base LX

این استاندارد به نام IEEE 802.3z یا GigabitEthernet شناسایی می شود. در این استاندارد از کابل فیبرنوری Single Mode با قطر هسته 9 میکرون استفاده می شود و طول کابل می تواند 10 کیلومتر باشد.

Ethernet 10 Gbps

این استاندارد به نام IEEE 802.3ae شناسایی می شود و طول کابل می تواند 40 کیلومتر باشد. ارتباط در این استاندارد کاملا دو طرفه همزمان یا Full Duplex می باشد و می توان در شبکه های LAN و MAN و WAN استفاده نمود .

10GBase SR

این استاندارد امکان دسترسی به سرعت GigabitEthernet 10 را از طریق فیبرنوری نوع MultiMode با منبع نور لیزر با طول موج کوتاه 850 نانومتر برای مسافت 300 متر را خواهد داد .

10GBase LR

این استاندارد امکان دسترسی به سرعت GigabitEthernet 10 را از طریق فیبرنوری نوع Single Mode با منبع نور لیزر با طول موج بلند 10310 نانومتر برای مسافت 10 کیلومتر را خواهد داد .

10GBase ER

این استاندارد امکان دسترسی به سرعت 10 GigabitEthernet را از طریق فیبرنوری نوع Single Mode با منبع نور لیزر با طول موج بلند 1550 نانومتر برای مسافت 40 کیلومتر را خواهد داد.

10GBase SW

این استاندارد امکان دسترسی به سرعت 10 GigabitEthernet را از طریق فیبرنوری نوع MultiMode با منبع نور لیزر با طول موج 850 نانومتر برای مسافت 300 متر را خواهد داد .

10GBase LW

این استاندارد امکان دسترسی به سرعت 10 GigabitEthernet را از طریق فیبرنوری نوع Single Mode برای مسافت 10 کیلومتر را خواهد داد و در شبکه های SONET استفاده خواهد شد .

10GBase EW

این استاندارد امکان دسترسی به سرعت 10 GigabitEthernet را از طریق فیبرنوری نوع Single Mode با منبع نور لیزر با طول موج بلند 1550 نانومتر برای مسافت 40 کیلومتر را خواهد داد و در شبکه های SONET استفاده خواهد شد .

10GBase T

این استاندارد امکان دسترسی به سرعت 10 GigabitEthernet را از طریق کابل UTP برای مسافت 100 متر خواهد داشت . شبیه استاندارد FastEthernet می باشد با این تفاوت که در این استاندارد سرعت 10 Gbps پشتیبانی خواهد شد .

پیکربندی مربوط به پورت های سوئیچ :

برای وارد شدن به محیط پیکربندی یک پورت باید دستور زیر را در محیط Global اجرا کنیم :

Switch (config) # Interface Type module / number

Switch (config – if) #

Type :

در قسمت type نوع اینترفیس را مشخص می کنیم مثلا : Ethernet یا Fastehhernet یا Gigabitethernet یا ...

Number :

در قسمت num شماره port یا اینترفیس مورد نظر نوشته می شود .

شماره اینترفیس در سوئیچ از 0/1 شروع می شود .

دو نوع سوئیچ داریم :

- Fixed : سوئیچ هایی که ماژول های توکار دارند و نمی توان به آنها ماژول اضافه کرد و چون فقط یک ماژول دارد همیشه قسمت Module آن صفر است .
- Modular : سوئیچ های بزرگی که تعداد ماژول های بیشتری دارند و می توان ماژول به آنها اضافه کرد و باید حتما در قسمت Module شماره ماژول ذکر شود .

روشن یا خاموش کردن یک اینترفیس :

Switch (config) # interface Type module / number

خاموش یا غیرفعال می شود

Switch (config – if) # Shutdown

روشن یا فعال می شود

Switch (config – if) # No Shutdown

فرمان نمایش دادن وضعیت یک Port یا اینترفیس :

Switch # show interface Type module / number

فرمان نمایش دادن وضعیت تمام Portها :

Switch # show interface status

فرمان تغییر نام برای هر Pore :

توضیحی می باشد که برای هر اینترفیس می توان نوشت و برای مدیریت بهتر اینترفیس ها از آن استفاده می شود .

Switch (config) # interface Type module / number

Switch (config – if) # Description name

دستور انتخاب چند پورت :

سه روش وجود دارد :

روش اول برای انتخاب اینترفیس های غیر متوالی :

Switch (config) # Inteface range type num type num …

مثال :

Switch (config) # Inteface range Fastethernet 0/1 Fastethernet 0/3 Fastethernet 0/6 …

Switch (config – Range – if) #

روش دوم برای انتخاب اینترفسی های متوالی :

Switch (config) # Inteface range type num – num

مثال :

Switch (config) # Inteface range Fastethernet 0/1 – 5

Switch (config – Range – if) #

روش سوم برای انتخاب اینترفیس های متوالی و غیر متوالی (ترکیبی) :

Switch (config) # Inteface range Fastethernet 0/1 , Fastethernet 0/3 – 7 , Gigabitethernet 0/2

Switch (config – Range – if) #

استفاده از یک Macro برای انتخاب اینترفیس ها در زمان های دلخواه و فراخوانی آنها :

تعریف Macro :

Switch (config) # Define Inteface – range macro – name Type mod/num , Type mod/num …

فراخوانی Macro :

Switch (config) # Inteface range Macro macro – name

: Speed

سرعت انتقال یک بیت در زمان

سرعت اینترفیس ها در انتقال یک بیت :

Ethernet 10 mbps : IEEE 802.3

FastEthernet 100 mbps : IEEE 802.3u

GigabitEthernet 1000 mbps : IEEE 802.3z , IEEE 802.3ab

TenGigabitEthernet 10000 mbps : IEEE 802.3ae

فرمان تغییرسرعت یک اینترفیس :

Switch (config – if) # Speed { 10 | 100 | 1000 | Auto }

نکته :

اگر دو سوئیچ را به یکدیگر وصل کنیم باید سرعت هر دو طرف پورت (اینترفیس های هر دو سوئیچ) برابر باشند , بهتر است از Auto استفاده کنیم و دو سوئیچ با توافق هم از بالاترین سرعت ممکن برای انتقال داده استفاده میکنند .

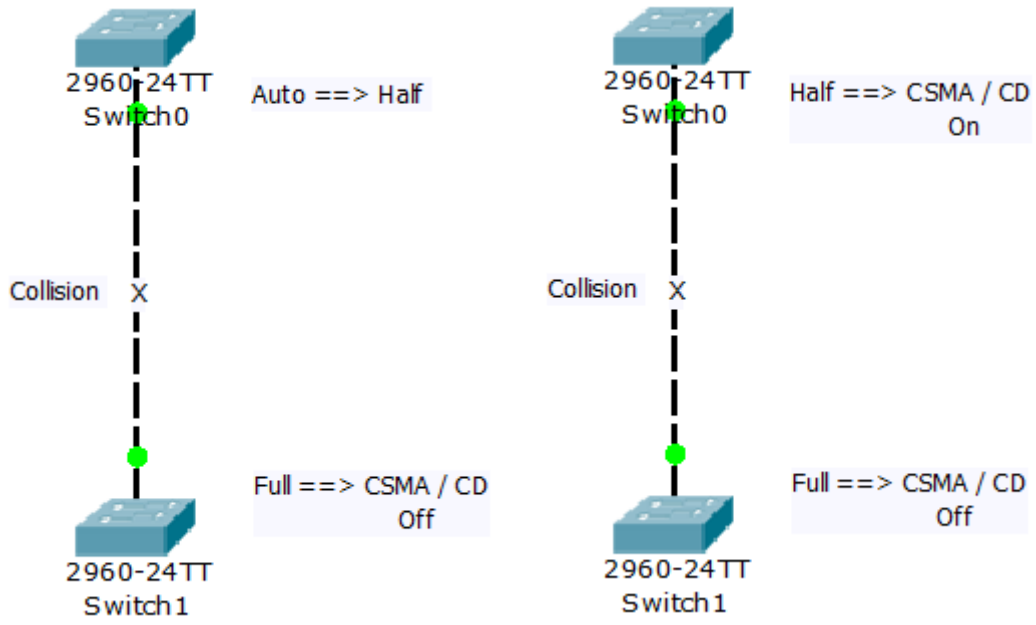
تنظیم Duplex اینترفیس :

Switch (config – if) # Duplex { Half | Full | Auto }

نکته :

در شبکه بسته های کوچکتر از 64 byte یعنی error . وقتی Runt Error که باید بین (64 – 1518 byte) باشد کمتر از 64 byte باشد یعنی احتمالا مشکل Duplex در شبکه وجود دارد و شبکه سرعت پایینی دارد .

همیشه باید Duplex را در حالت Full تنظیم کنیم مگر در حالتی خاص مثلا سوئیچ را به یک Hub وصل کنیم .



در هر دو حالت Collision رخ میدهد . در حالتی که یکی از سوئیچ ها در حالت Full و دیگری در حالت Auto باشد چون سوئیچ 1 جواب سوئیچ 0 را نمی دهد که Duplex را در حالت auto است یا نه , پس سوئیچ 0 خود را در حالت کمتر قرار می دهد یعنی حالت Half و چون یک طرف پورت Half و طرف دیگر حالت Full است collision رخ می دهد .

پیش فرض حالت Duplex در سوئیچ Auto است .

نکته :

بهتر است تنظیمات جاهای حساس شبکه را همیشه به صورت Static وارد کنیم یعنی در حالت پیش فرض ها قرار ندهیم .

مدیریت خطاهای مربوط به پورت های سوئیچ :

سوئیچ های کاتالیست سیسکو توانایی شناسایی اتوماتیک خطاهای مربوط به پورت های خود را دارند . در صورتی که یک خطا در مورد یکی از پورت های سوئیچ روی دهد ، پورت مزبور در وضعیت غیرفعال قرار می گیرد تا مدیر شبکه بعد از بررسی خطا اقدام به فعال سازی دستی آن نماید . همچنین در بعضی مواقع خود سوئیچ نیز می تواند بعد از گذشت مدت زمان اندکی اقدام به فعال کردن پورت غیرفعال شده بکند .

شناسایی اتوماتیک خطاها :

سوئیچ های کاتالیست سیسکو توانایی شناسایی اتوماتیک خطاهای مربوط به پورت های خود را دارند . در صورت یافت شدن خطایی در روی پورت ، وضعیت آن به صورت errdisable قرار گرفته و عملکرد پورت نیز غیرفعال خواهد شد . این رفتار سوئیچ را می توان کنترل نمود تا تنها نوع خاصی از خطا باعث غیرفعال شدن یک پورت گردد. برای این کار از دستور زیر استفاده می کنیم :

Switch (config) # [no] errdisable detect cause [all | cause – name]

به جای متغیر cause – name می توانید نام مربوط به یک خطا را بنویسید . در حالت کلی انواع پارمترهایی که می توان به جای متغیر فوق قرار داد عبارتند از :

- All : تایپ این پارامتر باعث می شود تا سوئیچ در قبال تمامی خطاهای ممکن از خود واکنش انجام دهد .
- Arp – inspection : اشاره به خطاهای مربوط به پروسه Dynamic ARP inspection دارد.
- BPDU Guard : تایپ این پارامتر باعث می شود تا در صورتی که یک پورت PortFast اقدام به دریافت پیام BPDU نماید ، سوئیچ اقدام به شناسایی یک خطا نماید .
- Channel – Misconfig : اشاره به خطاهای مربوط به EtherChannel دارد .

- DHCP – Rate – Limit : اشاره به خطاهای مربوط به DHCP Snooping دارد .
- DTP – Flap : در صورتی که وضعیت trunking از یک نوع به نوع دیگر تغییر می یابد ، سوئیچ یک پیام خطا تولید خواهد کرد .
- GBIC – invalid : در صورت استفاده از ماژول های مشکل دار GBIC و SFP سوئیچ یک پیام خطا خواهد داد .
- Llpower : اشاره به خطاهای مربوط به ویژگی PoE دارد .
- L2 ptguard : اشاره به خطاهای مربوط به تونل های ایجاد شده در سطح لایه 2 دارد .
- Link – Flap : در صورتی که وضعیت Link state یک پورت به صورت Flapping بوده و به صورت متناوب مابین Up و Down متغیر باشد سوئیچ یک پیام خطا مبنی بر آن تولید خواهد کرد .
- Loopback : اشاره به خطاهای مربوط به قرارگیری یک پورت در وضعیت Loop back دارد .
- Pagp – Flap : در صورتی که پورت EtherChannel دارای تنظیمات صحیح نباشد ، سوئیچ یک پیام خطا تولید خواهد کرد .
- Psecure – Violation : اشاره به خطاهای ایجاد شده در قبال استفاده از ویژگی های امنیتی در روی پورت ها (Port Security) دارد .
- Root Guard : در صورتی که پیام BPDU مربوط به سوئیچ Root از یک پورت نامربوط دریافت گردد ، پیام خطایی مبنی بر آن تولید خواهد شد .
- security – Violation : اشاره به خطاهای مربوط به ویژگی Port Security دارد .
- Storm – Control : در صورت افزایش کانترهای مربوط به ویژگی Storm Control یک پیام خطا تولید خواهد شد .
- UDLD : در صورت قرارگیری یک پورت در وضعیت Unidirectional یک پیام خطا نشان داده می شود .
- Unicast – Flood : باعث فعال شدن تشخیص خطا در مورد پروسهUnicast Flood Blocking می شود .
- VMPS : تایپ این پارامتر باعث می شود تا سوئیچ اقدام به شناسایی خطاهای مربوط به سرویس VMPS نماید .

برای نمایش errdisable دستور زیر را اجرا می کنیم :

Switch # Show errdisable Detect

دستور نمایش دلایلی که باعث errdisable شدن پورت گردیده است :

Switch # Show errdisable Recovery

در حالت پیش فرض هیچ کدام Recovery نمی شوند .

میتوانیم سوئیچ را به گونه ای پیکربندی کنید که خود به صورت اتوماتیک اقدام به فعال کردن پورت غیرفعال گردد . برای انجام این کار باید در ابتدا دلیل قرارگیری یک پورت در وضعیت errdisable که می خواهید بعد از بروز آن دوباره به صورت اتوماتیک فعال گردد را در دستور زیر مشخص سازید :

Switch (config) # Errdisable Recovery cause [all | cause – name]

در صورتی که سوئیچ را مجبور کرده باشید که بعد از بروز یک خطای خاص اقدام به فعال سازی اتوماتیک پورت معیوب نماید ، پورت یاد شده به صورت پیش فرض به مدت 300 ثانیه در وضعیت بلوکه قرار گرفته و سپس توسط سوئیچ فعال خواهد شد . برای تغییر این مدت زمان می توانید از دستور زیر استفاده کنید :

Switch (config) # Errdisable Recovery Interval second

به جای متغیر second می توانید اعداد 30 الی 86400 را بنویسید .

مثال : دستوراتی که برای فعال شدن دوباره پورت هایی که توسط ویژگی Port Security بعد از مدت 1 ساعت لازم است :

Switch (config) # Errdisable Recovery cause Psecure – Violation

Switch (config) # Errdisable Recovery Interval 3600

برای مشاهده لیست تمامی پورت هایی که در وضعیت Errdisable قرار گرفته اند و دلایل مربوطه از دستور زیر استفاده می کنیم :

Switch # Show Interface Status Errdisable

VLAN and Trunks

Virtual LAN : VLAN

: VLAN

تمامی پورت های یک سوئیچ در یک محیط Broadcast Domain قرار دارد . این بدان معنی است که تمامی Deviceهایی که به این سوئیچ متصل هستند همگی در یک LAN قرار دارند , بنابراین می توانند براحتی به یکدیگر دسترسی داشته باشند.

قرارگیری تمامی منابع شبکه مانند Serverها , کاربران , اینترنت در یک LAN واحد مشکلاتی را به دنبال دارد . نتیجه آن :

1. ترافیک بالا
2. امنیت پایین

به عبارتی در چنین شبکه ای نمی توان مدیریت روی ترافیک و امنیت داشت . در حالی که اگر یک Broadcast Domain را به چندین Broadcast Domain تفکیک کنیم , ترافیک کاهش و محلی شده و دسترسی ها محدود می شود .

در واقع با تبدیل کردن یک LAN به چندین LAN یا همان VLAN نتایج زیر حاصل می شود :

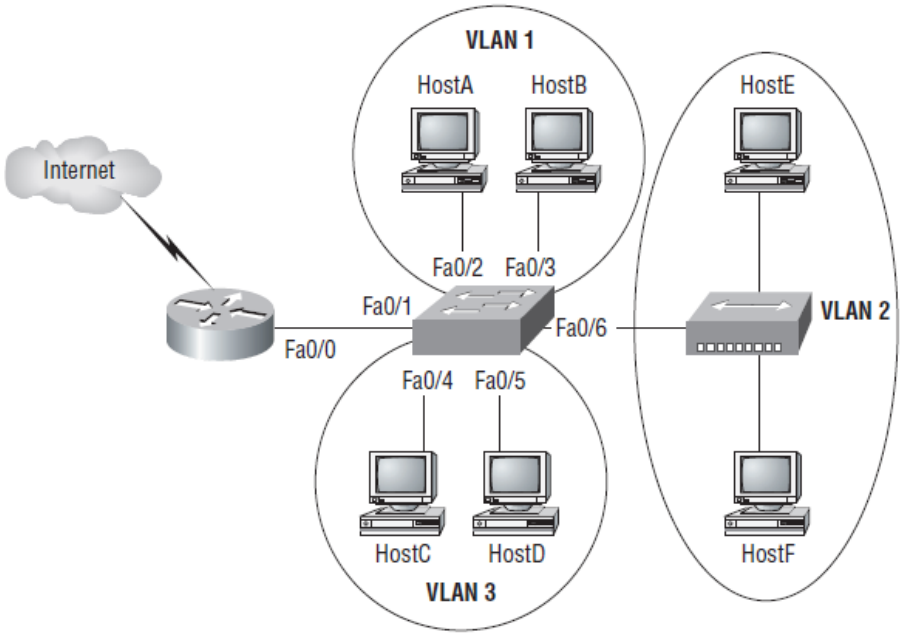
- کوچک شدن Broadcast Domain
- کاهش و محلی شدن ترافیک
- محدود کردن سطح دسترسی

فرض کنید تعدادی کامپیوتر در یک LAN قرار داشته باشند . بنابراین همه این کامپیوترها به راحتی با یکدیگر ارتباط دارند . اما در صورتی که یک LAN را به چندین VLAN تبدیل کنیم , کامپیوترهایی که در یک VLAN هستند نمی توانند با VLANهای دیگر ارتباط برقرار کنند .

تعریف و ساخت VLAN در لایه دوم از مدل OSI امکان پذیر می باشد .

در یک سوئیچ بین 0 تا 4095 عدد VLAN می توان درست کرد . VLANهای 0 و 4095 رزرو شده هستند و نمی توان از این دو استفاده کرد . تعداد و شماره VLANهایی را که می توانیم از آنها استفاده کنیم بین 1 تا 1005 است که به آنها استاندارد می گویند . از 1006 تا 4094 را Extand می گویند و در سوئیچ های

Transparent استفاده می شوند. از 1002 تا 1005 را نمیتوانیم استفاده کنیم به آنها VLANهای Token Ring و FDDI می گویند .



دستور ساخت VLAN :

Switch (config)# VLAN vlan – id

Switch (config - Vlan)# Name name

تعریف نام برای VLAN اختیاری است ، اگر نام تعریف نکیم به صورت اتوماتیک سوئیچ یک نام به VLAN اختصاص می دهد . مثلا اگر VLAN 2 را تعریف کنیم و نامگذاری نکنیم خود سوئیچ نامی را به صورت زیر به آن VLAN اختصاص داده می شود :

Default = VLAN xxxx : VLAN 0002

دستور نمایش VLANها :

Switch # Show VLAN

Switch # Show VLAN Brief

مثالی از دستور Show VLAN :

Verifying VLAN Configuration with the show vlan Command

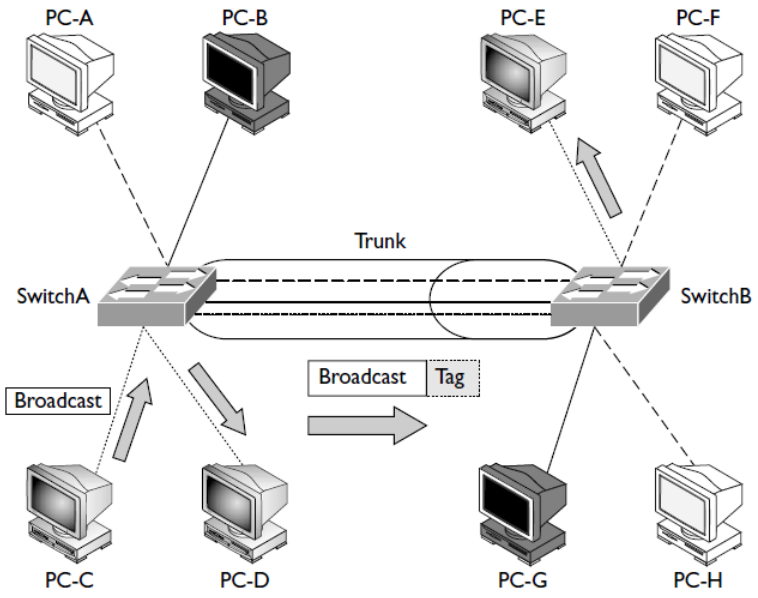
```
Switch#
show vlan
VLAN  Name                              Status    Ports
----  --------------------------------  ------    --------------------------------
1     default                           active    Gi1/1, Gi1/2, Gi3/20, Gi4/20
2     Engineering                       active    Gi4/2, Gi4/3, Gi4/4, Gi4/5
                                                  Gi4/6, Gi4/7, Gi4/8, Gi4/9
                                                  Gi4/10, Gi4/11, Gi4/12
101   Marketing                         active    Gi2/5, Gi2/6, Gi2/7, Gi2/8
                                                  Gi2/9, Gi2/10, Gi2/11, Gi2/12
                                                  Gi2/13, Gi2/14, Gi2/15, Gi2/16
                                                  Gi2/17, Gi2/18
```

نکته :

VLAN 1 غیر قابل تغییر نام است و حذف نمی شود و به صورت پیش فرض تعریف شده است و در حالت اول همه اینترفیس ها در VLAN 1 قرار دارند .

انواع Port از نظر ترافیک VLANها :

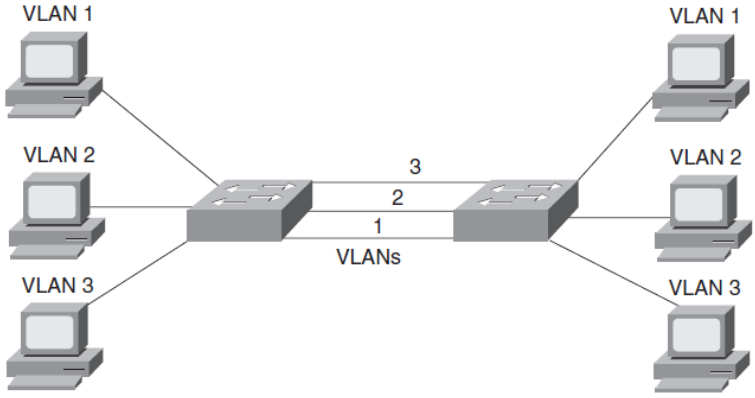
- Access : پورت هایی که فقط ترافیک یک VLAN را از خود عبور می دهند.
- Trunk : پورت هایی که محدود به ترافیک یک VLAN نیستند و ترافیک همه VLANها را از خود عبور می دهند .



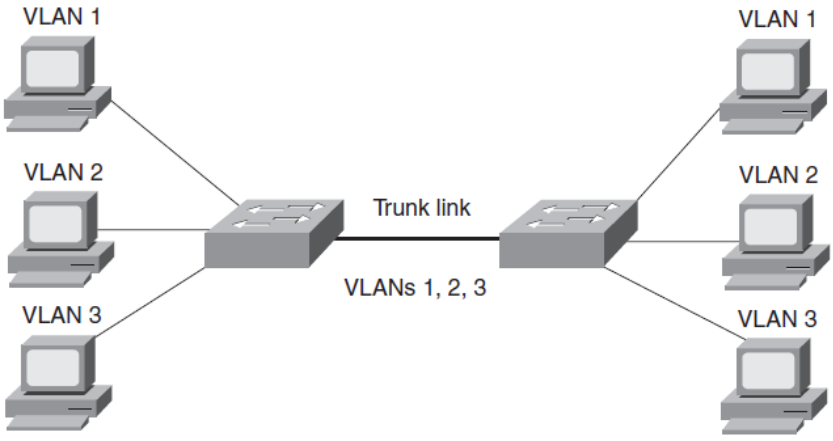
در شکل بالا PCهای همرنگ در یک VLANقرار دارند .

وقتی که PC – C که با PC – D و PC – E در یک VLAN قرار دارند می خواهد برای PC – E بسته Data بفرستد اول به سوئیچ A میرسد و سوئیچ بسته را گرفته و به آن Tag میچسباند که این بسته متعلق به VLAN خاکستری است و ارسال میکند به سوئیچ B از طریق پورتی که در حالت Trunk قرار دارد . سوئیچ B بسته را دریافت میکند و به قسمت Tag آن نگاه می کند و میبیند که متعلق به VLAN خاکستری است پس در VLAN خاکستری آن را منتشر میکند (این در حالتی است که MAC کامپیوتر E هنوز Learn نشده باشد) پس به PC – E می رسد . قبل از ارسال به VLAN خاکستری باید سوئیچ B بسته را که دریافت کرد Tag آن را بعد از خواندن از بسته جدا کند و بعد ارسال کند .

به شکل های زیر دقت کنید ، مشاهده می کنید که برای ارتباط بین هر VLAN باید یک پورت Access اختصاص دهیم . در این شرایط با افزایش تعداد VLANها ، تعداد اتصالات فیزیکی و مستقل مورد نیاز برای متصل کردن سوئیچ ها به یکدیگر افزایش خواهد یافت .



در چنین وضعیتی است که بهره گیری از یک اتصال Trunk می تواند باعث آسانی کار گردد . تصویر پایین نحوه استفاده از یک اتصال Trunk به جای تمامی اتصالات فیزیکی دیگر را نشان می دهد که وظیفه انتقال اطلاعات مربوط به VLANهای مختلف را بر عهده دارد :



نکته : پورت هایی که PC به سوئیچ متصل می شود را access تعریف میکنیم و پورت بین سوئیچ ها را باید حتما Trunk تعریف کنیم .

دستور قرار دادن پورت در VLAN :

```
Switch ( config ) # Interface   type   mod/num
Switch ( config – if ) # Switchport   mode   access
Switch ( config – if ) # Switchport  Access   VLAN   vlan-id
```

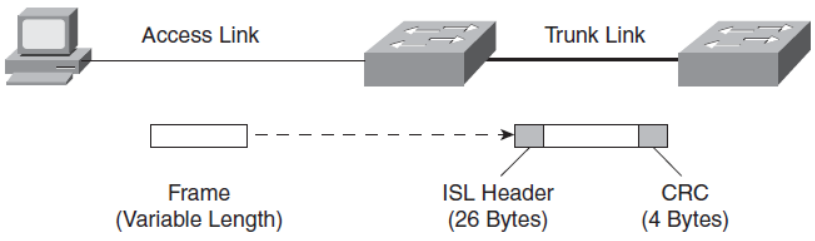
مثال :

```
Switch ( config ) # Interface   FastEthernet  0/1
Switch ( config – if ) # Switchport   mode   access
Switch ( config – if ) # Switchport  Access   VLAN  2
```

با این دستور پورت 0/1 در VLAN 2 قرار می گیرد .

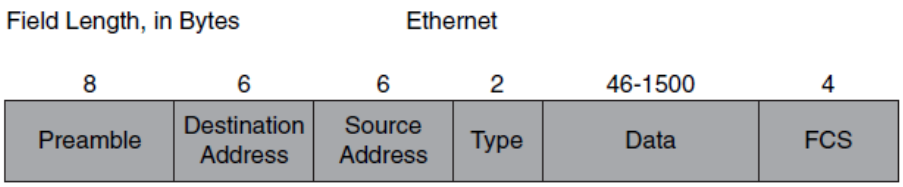
پروتکل های VLAN در اتصالات Trunk :

1. ISL (Inter Switch Link) یک روش Encapsulation مخصوص Deviceهای سیسکو است . Framing مخصوص به خود دارد . Native VLAN ندارد .

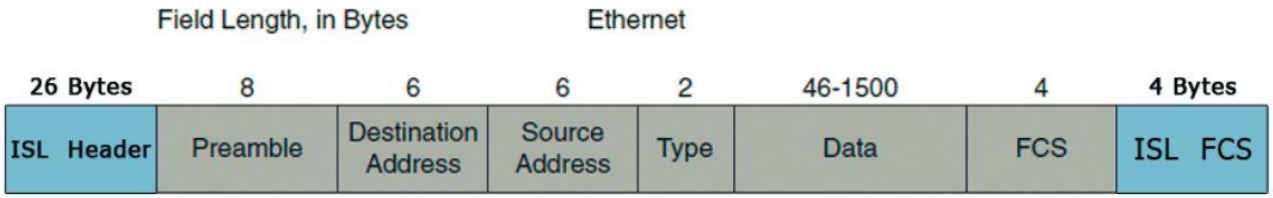


ISL Frame Identification

شکل الف :

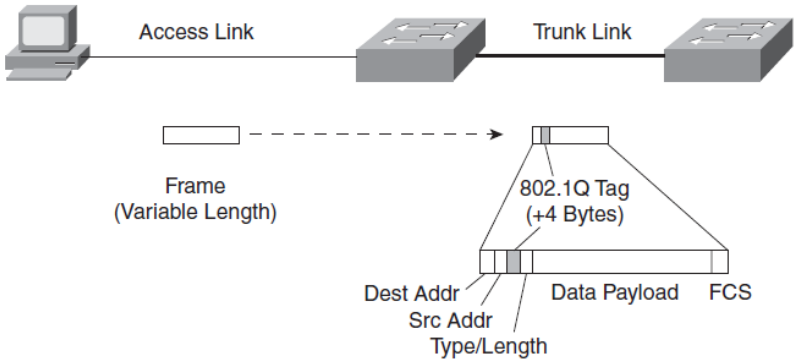


شکل ب :

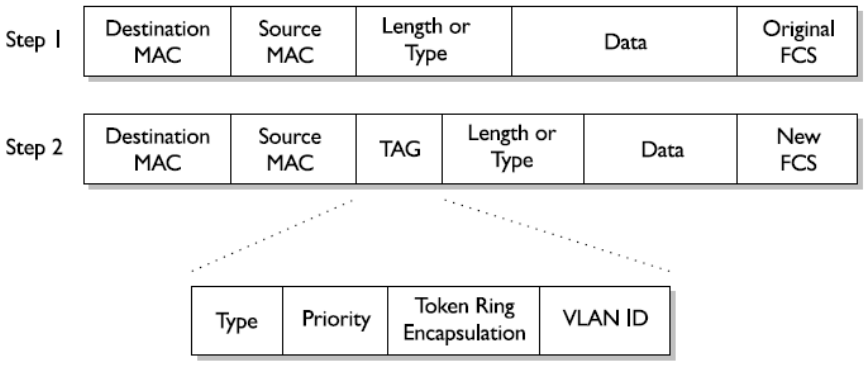


پروتکل ISL فریم ارسالی که به صورت شکل الف است را بعد از Tag به صورت شکل ب تغییر می دهد یعنی به اول فریم ISL Header به اندازه 26 بایت و به آخر فریم FCS ISL به اندازه 4 بایت را اضافه می کند و بعد ارسال می کند .

2. پروتکل IEEE 802.1Q یک پروتکل بین المللی است و همه شرکت ها از آن استفاده می کنند . Framing مخصوص به خود دارد و Native VLAN را دارد .



IEEE 802.1Q Frame-Tagging Standard



این پروتکل فریم اصلی که در شکل با Step 1 مشخص شده می گیرد و با Tag زدن به آن مثل فریم Step 2 که 4 byet است و حاوی شماره VLAN است را تغییر می دهد و ارسال می کند.

نکته :

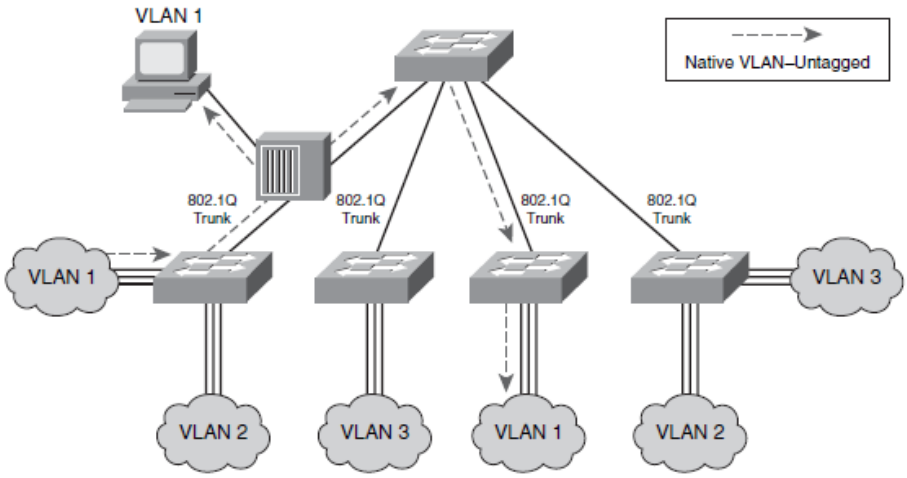
ISL بر 802.1Q اولویت دارد . پورت های Trunk که از متد ISL استفاده می کنند ، فریم هایی تا اندازه 1548 byte را اجازه می دهند که عبور کند و پورت های Trunk که از متد 802.1Q استفاده می کنند ، فریم هایی تا اندازه 1522 byte را اجازه می دهند که عبور کند.

دستورات تنظیم VLAN :

```
Switch ( config ) # Interface   type   mod/num
Switch ( config – if ) # Switchport  trunk  encapsulation { ISL | Dot1Q }
Switch ( config – if ) # Switchport   mode   trunk
```

Native VLAN :

برای کنترل ارسال و دریافت ترافیک سوئیچ ها مورد استفاده قرار میگیرد. اگر بخواهیم فریم های یک VLAN را Tag نزنیم از Native VLAN استفاده می کنیم . چون اگر این کار را نکنیم منجر به افزایش Overhead روی پورت Trunk می شود .



در شکل بالا VLAN 1 را Native VLAN تنظیم کرده ایم (البته VLAN 1 به صورت پیش فرض Native VLAN است) تا فریم های ارسالی در این VLAN را Tag نزند . حتما باید دو طرف پورت یک پروتکل داشته باشد و باید تعیین کنیم چه پروتکلی باشد .

پروتکل 802.1Q از Native VLAN پشتیبانی می کند و به کمک فرمان زیر روی پورت Trunk فعال می شود :

Switch (config) # Interface type mod/num

Switch (config – if) # Switchport trunk native VLAN vlan – number

دستوری که ترافیک یک یا چند VLAN را از یک پورت در حالت Trunk مجاز می کند و برچسب (Tag) می زند :

Switch (config – if) # Switchport trunk Allowed VLAN vlan – range

در VLAN – Range می توانیم از 3 حالت زیر استفاده کنیم :

1. 2 , 4 , 5
2. 2 – 5
3. 2 – 5 , 10 – 15

دستور حذف یک VLAN از بقیه VLAN های یک پورت :

Switch(config – if)#Switchport trunk Allowed VLAN Remove vlan-id

دستور اضافه کردن یک VLAN به بقیه VLAN های یک پورت :

Switch (config – if)# Switchport trunk Allowed VLAN add vlan-id

دستوری که همه VLAN ها را مجاز میکند :

Switch (config – if) # Switchport trunk Allowed VLAN ALL

دستوری که همه VLAN ها را مجاز میکند بغییر از چند Vlan :

Switch (config – if)#Switchport trunk Allowed VLAN except vlan-id

دستوری که هیچکدام از VLAN ها را مجاز نمیکند :

Switch (config – if) # Switchport trunk Allowed VLAN none

برای مشاهده وضعیت Trunk Port به صورت خلاصه از دستور زیر استفاده می کنیم :

Switch # Show Interface type mod/num Trunk

مثال :

Determining Switch Port Trunking Status

```
Switch# show interface gigabitethernet 2/1 trunk
Port       Mode          Encapsulation  Status         Native vlan
Gi2/1      on            802.1q          trunking      1

Port       Vlans allowed on trunk
Gi2/1      1-4094

Port       Vlans allowed and active in management domain
Gi2/1      1-2,526,539,998,1002-1005

Port       Vlans in spanning tree forwarding state and not pruned
Gi2/1     1-2,526,539,998,1002-1005
```

برای مشاهده وضعیت پورت های Trunk از دستور زیر استفاده می کنیم :

Switch # Show Interface Trunk

Dynamic Trunking Protocol

DTP :

این پروتکل بررسی می کند آیا اینترفیس های سوئیچ باید Trunk شوند یا نه و اگر بشود با چه پروتکلی Trunk شوند . فقط Device های شرکت سیسکو این پروتکل را دارند .

دستور اعمال DTP :

Switch (config – if) # Switchport mode { Access | Trunk | Dynamic Auto | Dynamic Desirable }

Mode های DTP :

1. **Access** : اگر یک طرف پورت در حالت Access باشد به طرف دیگر پورت پیشنهاد نمی دهد .
2. **Trunk** : در این حالت پورت می گوید من Trunk هستم و پیشنهاد Trunk بودن را به طرف دیگر پورت می دهد .
3. **Dynamic Auto** : در این حالت پورت پیشنهاد نمی دهد ولی اولین پورتی که پیشنهاد دهد را قبول می کند .
4. **Dynamic Desirable** : در این حالت پورت هم پیشنهاد می دهد هم اولین پیشنهادی که طرف دیگر پورت بدهد را قبول می کند .

switch A / switch B	Access	Trunk	Dynamic Auto	Dynamic Desirable
Access	Access	**X**	Access	Access
Trunk	**X**	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Access	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk

پیش فرض پورت ها Dynamic Auto یا Dynamic Desirable است .

Administrativ Mode :

به چهار حالتی که کاربر وارد می کند یعنی (Access Dynamic Desirable , Dynamic Auto , Trunk ,) که در بالای جدول نوشته شده می گویند .

Operational Mode :

به دو حالت داخل جدول یعنی (Access , Trunk) که DTP تعیین می کند یعنی Modeهایی که DTP برای پورت ها تعیین می کند می گویند .

نکته :

وقتی در یک mode باشیم که یک طرف پورت در حالت Access باشد و طرف دیگر در حالت Trunk باشد , این حالت بدترین حالت است چون هیچ کدام از طرفین پورت حالت خود را تغییر نمی دهند تا هر دو طرف در یک حالت access یا Trunk قرار گیرند .

نکته :

بسته های پروتکل DTP مرتبا در بین سوئیچ های شبکه در حال رفت و آمد است . هر 30 ثانیه یک بسته فرستاده می شود و این کار باعث ارسال بسته های اضافی DTP در مدار و کاهش سرعت شبکه می شود .

دستور خاموش کردن DTP :

Switch (config – if) # Switchport Nonegotiate

این دستور را در حالتی می توانیم وارد کنیم که Switchport Mode دو طرف یک پورت را به حالت (Static) دستی Trunk کرده باشیم.

بهتر است در شبکه دستور switchport Mode را برای سوئیچ های اصلی به صورت دستی وارد کنیم و دستور Nonegotiate را در آن سوئیچ ها وارد کنیم . برای سوئیچ های معمولی در شبکه زیاد لازم نیست این کار را بکنیم .

دستور Show های DTP :

Switch # Show interface type mod/num switchport

Switch # Show DTP

مثال : در زیر مثالی از اجرای دستور switchport fastethernet 0/2 Show interface را مشاهده می کنید :

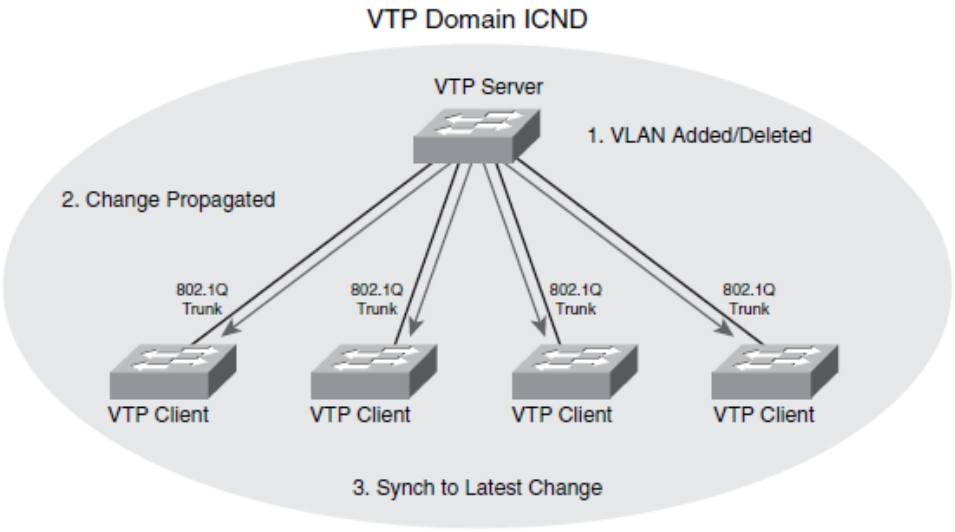
```
Switch# show interface fastethernet 0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto

Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
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
Switch#
```

VLAN Trunking Protocol



: VTP

طرح مدیریت گروهی سوئیچ ها را معرفی می کند . بنابراین VTP با تعریف کردن یک ناحیه که شامل تعدادی سوئیچ می باشد و تعریف Client و Server در این شبکه , تغییرات را روی Server اعمال می کند و سپس به اطلاع سوئیچ های دیگر می رساند . مخصوص دستگاه های سیسکو است .

: VTP Domain

ناحیه ای که شامل تعدادی سوئیچ بوده به طوری که هر سوئیچ اطلاعات مربوط به VLAN خود را با بقیه سوئیچ ها به اشتراک می گذارد .هر سوئیچ تنها می تواند عضو یک VTP Domain باشد و سوئیچ هایی که در VTP Domain های متفاوتی هستند نمی توانند اطلاعات مربوط به VLANهایشان را با یکدیگر به اشتراک بگذارند.

: VTP Advertisement

هر کدام از سوئیچ های سیسکو در VTP Domain اطلاعات مربوط به VLAN ها را به کمک VTP Advertisement از سوئیچ های مجاورش که از طریق پورت Trunk به آنها متصل است دریافت می کند. VTP Advertisementها به صورت فریم های Multicast در VTP Domain ارسال می شوند. لینک بین دو سوئیچ باید به صورت Trunk تعریف شود تا VTP Advertisementها قادر به انتقال باشند.

VTP Messages

If you use a client/server configuration for VTP, these switches can generate three types of VTP messages:

- Advertisement request
- Subset advertisement
- Summary advertisement

VTP Advertisementها به 3 فرم در یک VTP Domain منتشر می شوند :

Summary Advertisement :

اطلاعاتی هستند که هر 300 ثانیه توسط VTP Server به بقیه سوئیچ ها در VTP Domain ارسال می شود و شامل اطلاعات مربوط به VLAN Database می باشد .

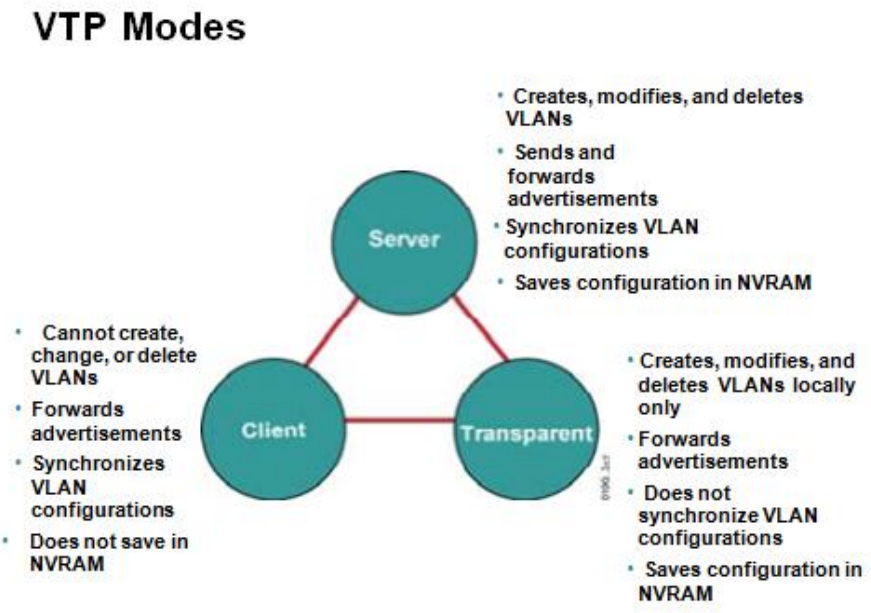
Subset Advertisement :

اطلاعاتی هستند که توسط Server هنگام رخ دادن تغییر در تنظیمات VLANها ارسال می شود و شامل اطلاعات VLAN Database و وضعیت هر کدام از VLANها می باشد.

Advertisement Request :

اطلاعاتی هستند که توسط VTP Clientها از VTP Server درخواست می شوند.

Modeهای مختلف پروتکل VTP :



در یک VTP Domain هر کدام از سوئیچ ها می بایست در یکی از Mode های زیر ایفای نقش کنند :

- Server Mode
- Client Mode
- Transparent Mode

در واقع VTP Mode مشخص می کند که هر کدام از سوئیچ ها چگونه در اطلاع رسانی در مورد VLANها و عملکرد VTP نقش خواهد داشت .

Server Mode :

سوئیچی که در این Mode قرار میگیرد دارای توانایی کامل در ایجاد , حذف و تغییر VLAN و مدیریت Domain خواهد بود . تمام سوئیچ ها به صورت پیش فرض در این Mode قرار دارند.

Client Mode :

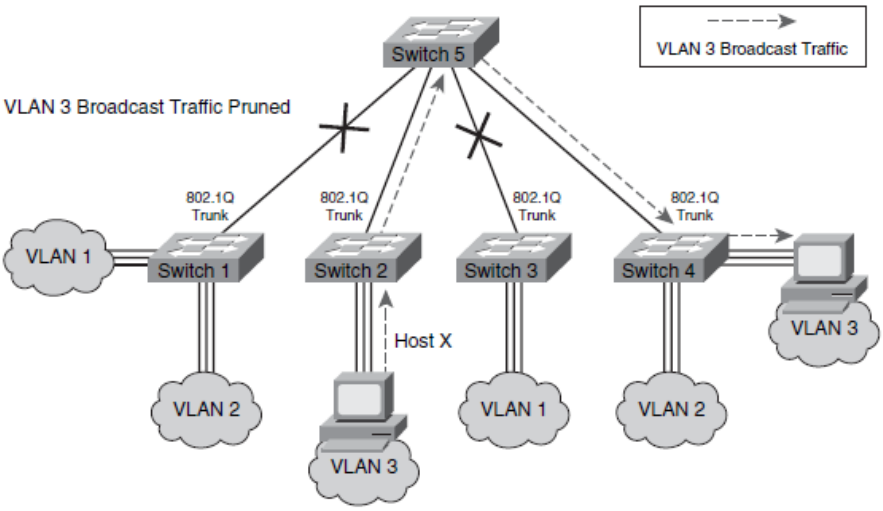
سوئیچی که در این Mode قرار می گیرد قادر به حذف یا اضافه یا تغییر VLAN نخواهد بود . سوئیچی که در این Mode قرار میگیرد به تغییراتی که توسط سوئیچ های دیگر گزارش می شود گوش می دهد و این تغییرات را روی خود اعمال می کند .

Transparent Mode :

سوئیچی که در این Mode قرار می گیرد به عنوان یک عضو خنثی عمل میکند . اطلاعاتی که در مورد VTP از سوئیچ های مجاور دریافت می کند را بدون اینکه روی خود اعمال کند از طریق پورت Trunk به سوئیچ های مجاورش ارسال می کند . قادر به حذف و اضافه کردن VLAN می باشد اما این تغییرات را به دیگر سوئیچ ها ارسال نمی کند .

VTP PRUNING :

همانطور که می دانید Broadcastای که یک سوئیچ دریافت می کند از تمام پورتهایش به بیرون ارسال می کند . این باعث افزایش ترافیک بیهوده بر این کانال می کند. VTP Pruning می گوید که فریم های Broadcast در یک VLAN به سوئیچ هایی تحویل داده شود که پورتی در آن VLAN داشته باشند . در نتیجه ترافیک بیهوده روی کانال ارتباطی Trunk تحمیل نخواهد شد .



تنظیم پروتکل VTP بر روی سوئیچ :

- تعیین نام VTP Domain

نام Domain را برای سوئیچ تعریف می کنیم . سوئیچ هایی که VTP Domain یکسان داشته باشند میتوانند اطلاعات مربوط به VLANها را با یکدیگر به اشتراک بگذارند . برای بار اول اگر Domain name را از Server تعیین کنیم روی همه سوئیچ های دیگر اعمال می شود چون domain همه Null است . ولی برای بار دوم یا بیشتر باید تک تک domain همه را وارد کنیم :

```
Switch ( config ) # Vtp  Domain  domain – name
```

- تعیین VTP Mode

سوئیچ ها به صورت پیش فرض Server Mode هستند . به کمک فرمان زیر می توان Mode vtp را تغییر دهیم :

```
Switch ( config ) # Vtp  Mode { Server | Client | Transparent }
```

- تعیین VTP Version

VTP دارای 3 ورژن 1 و 2 و 3 است . که ورژن 3 را ساپورت نمی کند و ورژن 2 , Takenring را ساپورت می کند ولی ورژن 1 ساپورت نمی کند .در ورژن 1 باید برای سوئیچ های Transparent حتما Domain name را تعریف کنیم ولی در ورژن 2 لازم نیست :

```
Switch ( config ) # Vtp  Version { 1 | 2 }
```

تعیین VTP Password

در یک VTP Domain با مشخص شدن VTP Server هر سوئیچ دیگری که Client Mode باشد اطلاعات مربوط به VLAN ها را از VTP server می گیرند . حال در صورتی که نخواهید هر کسی به راحتی بتواند سوئیچ خود را وارد شبکه کند و اطلاعات مربوط به VLANها را دریافت کند یا خرابکاری کند می بایست پس از انجام Authentication و یکسان بودن پسورد اطلاعات مربوط به VLAN را دریافت کند . از متد MD5 استفاده می کند با دستور زیر پسورد را Set می کنیم:

```
Switch ( config ) # Vtp  Password  password
```

فعال کردن VTP Pruning

```
Switch ( config ) # Vtp  Pruning
```

نکته :در یک شبکه حتما باید اول لینک بین سوئیچ ها را در حالت Trunk قرار داد بعد VTP را اجرا کرد. یعنی اول DTP اجرا شود بعد VTP .

بررسی عملکرد VTP روی سوئیچ :

```
Switch #Show  Vtp  Password
Switch #Show  Vtp  Status
Switch #Show  Vtp  Counters
```

مثال :

show vtp counters *Reveals VTP Message and Error Counters*

```
Switch# show vtp counters
VTP statistics:
Summary advertisements received    : 1
Subset advertisements received     : 2
Request advertisements received    : 1
Summary advertisements transmitted : 1630
Subset advertisements transmitted  : 0
Request advertisements transmitted : 4
Number of config revision errors   : 0
Number of config digest errors     : 0
Number of V1 summary errors        : 0

VTP pruning statistics:

Trunk            Join Transmitted Join Received      Summary advts received from
                                                     non-pruning-capable device
---------------- ---------------- ---------------- ------------------------------
Gi0/1                82352            82931            0
Switch#
```

Check کردن بسته های VTP توسط سوئیچ ها :

وقتی سوئیچ سرور بسته VTP را می فرستد همراه این بسته یک بسته VTP دیگری را که با رمز خود Hash شده می فرستد (این کار را با متد Massag Digest 5) انجام می دهد . سوئیچ Client هر دو بسته را دریافت می کند و بسته اصلی که حاوی اطلاعات VTP است را با رمز خود با استفاده از متد MD5 , Hash می کند و اگر نتیجه Hash خود با Hash فرستاده شده از سوئیچ Server برابر باشد بسته اصلی VTP را روی خود اعمال می کند و اگر برابر نباشد بسته را دور می اندازد .

Revision Number :

هر وقت در شبکه یک بسته VTP از طریق سرور ارسال شود و clientها آن را دریافت کنند و بر روی خود اعمال کنند یک واحد به Revision Number همه اضافه می شود .

Revision Numberها به دو صورت اضافه می شوند :

1. Topology Change : تغییر در ساختار VLAN شبکه به وسیله سرور .
2. هر 300 ثانیه یک بار بسته VTP در شبکه توسط سرور ارسال می شود .

سوئیچ ها وقتی بسته ای را دریافت می کنند قسمت Revision Number بسته را با قسمت Revision Number خود مقایسه می کنند اگر مساوی بود تغییرات را روی خود اعمال نمی کنند یعنی قبلا اعمال کرده اند ولی اگر بیشتر باشد آن وقت تغییرات را انجام می دهند و یک واحد به Revision Number خود می افزایند .

نکته مهم :

اگر یک شبکه داشته باشیم و بعدا بخواهیم یک سوئیچ دیگری به این شبکه اضافه کنیم باید حتما Revision Number آن را صفر کنیم چون اگر Revision Number سوئیچ بیشتر از مقدار Revision number شبکه باشد دستورات خود را به کل شبکه ارسال می کند و سوئیچ های دیگر وقتی Revision Number بسته

ارسالی را با Revision Number خود مقایسه می کنند و می بینند که بیشتر است , دستورات را روی خود اعمال می کنند و شبکه بهم ریخته می شود و خراب می شود .

چگونه Revision Number را در سوئیچ صفر کنیم :

1. VTP domain name را یک بار تغییر می دهیم
2. VTP Mode را یک بار عوض می کنیم

با این دو روش در هر دو حالت Revision Number صفر می شود و میتوانیم به شبکه وصل کنیم.

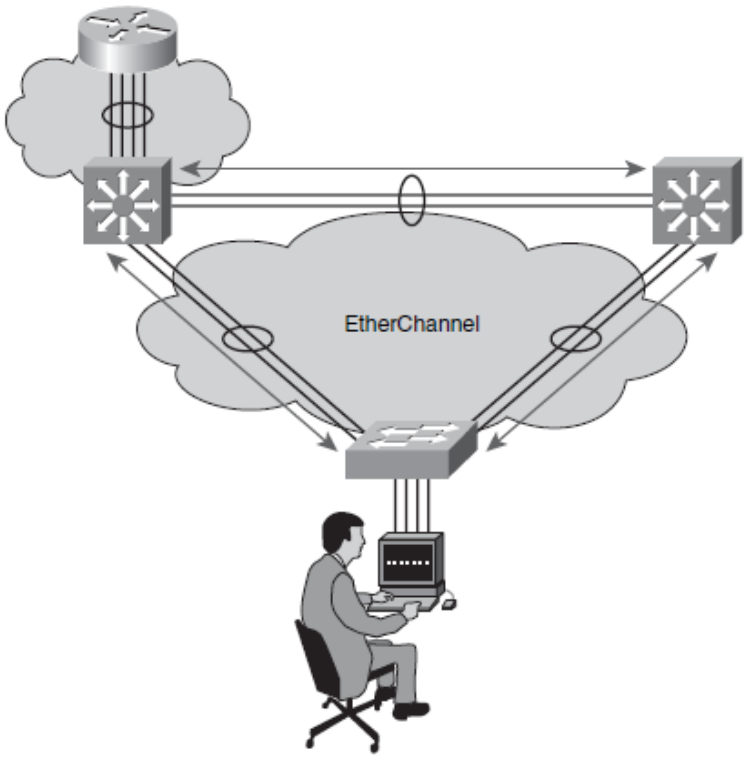
فایل Vlan.dat :

در حافظه Flash همه تنظیمات و اطلاعات مربوط به VLANهای شبکه را در خود ذخیره می کند. در سوئیچ های Server و Client در حافظه Flash ذخیره می شوند ولی در سوئیچ های Transparent در حافظه Running – config ذخیره می شود .

برای دیدن محتویات فایل Vlan.dat در سوئیچ هایی که Server و Client هستند باید اول Mode آنها را تغییر دهیم به Transparent و بعد در حافظه Running – config می توانیم محتویات فایل را ببینیم.

Aggregating Switch Links

EtherChannel



Etherchannel توانمندی می باشد که اجازه می دهد چندین پورت فیزیکی سوئیچ در یک گروه منطقی قرار گیرند که به منظور دسترسی به پهنای باند بالاتر و ایجاد تحمل خطا در اتصالات بین سوئیچ ها استفاده می شود که به شما اجازه خواهد داد از مجموعه پهنای باند اتصالات فیزیکی که در گروه منطقی قرار دارند استفاده کنید .

در گروه Etherchannel می توانیم از پورت های FastEthernet و GigabitEthernet استفاده کنید که میزان پهنای باند بین سوئیچ ها افزایش یابد . می توانیم دو یا چهار یا هشت پورت فیزیکی را داخل یک گروه قرار دهیم . مهم نیست که پورت ها به ترتیب و پشت سر هم انتخاب شوند . همه پورت های شرکت کننده باید دارای سرعت و Duplex مساوی و Enable و فعال باشد .

Etherchannel دارای 2 پروتکل PAgP و LACP است که با یکدیگر سازگار نمی باشند و باید در دو طرف یک لینک از یک پروتکل (یا PAgP و یا LACP) استفاده کرد . باید پورت ها همه یا در حالت Access یا در حالت Trunk باشند .

پروتکل های مدیریت اتصالات Etherchannel :

PAgP : Port Aggregation Protocol

یک پروتکل انحصاری مربوط به شرکت سیسکو می باشد . در صورتی می توان از این پروتکل استفاده نماییم که تجهیزات دو طرف اتصال شما سیسکو باشد .

LACP : Link Aggregation Control Protocol

این پروتکل توسط همه شرکتها پشتیبانی می شود و اگر تجهیزات شما از شرکت های متفاوتی باشند می توان از این پروتکل استفاده کرد . در این پروتکل می توان تا 16 پورت را در یک باندر جای داد ولی 8 تای آن Active است اگر یکی از پورت ها قطع شود به صورت اتوماتیک یکی دیگر از پورت ها فعال می شود .

Mode های پروتکل های PAgP و LACP :

EtherChannel Modes

Mode	Protocol	Description
auto	PAgP	Passively listens for PAgP queries from a Cisco device configured with either *desirable* or *on*. By default the interface is not part of a channel.
desirable	PAgP	Generates PAgP queries to form a channel, but by default is not part of a channel.
on	PAgP & LACP	Generates PAgP queries and assumes the port is part of a channel.
active	LACP	Enables a channel if the other side responds to its LACP messages.
passive	LACP	Passively listens for LACP messages to form a channel from an active port.

برای پروتکل PAgP دستورات زیر را در دو طرف لینک وارد می کنیم:

Configuring a PAgP EtherChannel

To configure switch ports for PAgP negotiation (the default), use the following commands:

```
Switch(config)# interface type mod/num
Switch(config-if)# channel-protocol pagp
Switch(config-if)# channel-group number mode {on | {{auto | desirable}
  [non-silent]}}
```

Auto : در این مد هیچ پیام PAgP از طرف اینترفیس ارسال نمی شود ولی آماده پاسخ گویی به پیام های PAgP از سوئیچ مقابل می باشد و قادر به آغاز PAgP Negotiation نیست.

Desirable : در این مد اینترفیس پیام های PAgP را ایجاد و به طرف سوئیچ مقابل ارسال می کند و قادر به آغاز PAgP Negotiation می باشد .

On : این مد باعث فعال شدن Etherchannel بر روی اینترفیس ها می شود بدون ارسال هیچ پیام PAgP .

Non – Silent : به صورت پیش فرض در حالت Silent قرار دارد یعنی اگر بعد از مدت 15 ثانیه از دستگاه مقابل هیچ پیام PAgP دریافت نکرد به صورت اتوماتیک Etherchannel فعال می شود و اگر از پارامتر Non – Silent استفاده کنیم ، اگر از دستگاه مقابل هیچ پیام PAgP دریافت نکند به هیچ وجه Etherchannel فعال نمی شود .

PAgP

Switch B / Switch A	Auto	Desirable	On
Auto	NO	YES	NO
Desirable	YES	YES	NO
On	NO	NO	YES

برای پروتکل LACP دستورات زیر را در دو طرف لینک وارد می کنیم:

Configuring a LACP EtherChannel

To configure switch ports for LACP negotiation, use the following commands:

```
Switch(config)# lacp system-priority priority
Switch(config)# interface type mod/num
Switch(config-if)# channel-protocol lacp
Switch(config-if)# channel-group number mode {on | passive | active}
Switch(config-if)# lacp port-priority priority
```

Lacp system – Priority :

دستور اول باعث اختصاص یک Priority به کل یک سوئیچ می گردد . مقدار این پارامتر به صورت پیش فرض برابر با 32768 بوده اما می توانید از اعداد 1 الی 65535 استفاده کنید . هر سوئیچ که Lacp system – Priority کمتری نسبت به سوئیچ های دیگر داشته باشد آن سوئیچ از اولویت بالاتری برخوردار بوده و نقش تصمیم گیرنده در تشکیل ارتباط Etherchannel را برعهده خواهد گرفت . در صورتی

که Lacp system – Priority همه سوئیچ ها با هم برابر باشد ، سوئیچی که دارای کوچکترین آدرس MAC باشد در نقش فوق ظاهر می شود .

Active :

در این مد اینترفیس پیام های LACP را ایجاد و به طرف سوئیچ مقابل ارسال می کند و قادر به آغاز PAgP Negotiation می باشد .

Passive :

در این مد هیچ پیام LACP از طرف اینترفیس ارسال نمی شود ولی آماده پاسخگویی به پیام های LACP از سوئیچ مقابل است و قادر به آغاز PAgP Negotiation نمی باشد .

On :

این مد باعث فعال شدن Etherchannel بر روی اینترفیس ها می شود بدون ارسال هیچ پیام LACP .

Lacp Port – Priority :

می توانید پورت بیشتری از حد مجاز را برای قرار گرفتن در داخل اتصال Etherchannel تعیین کنید که در این صورت ، پورت های مازاد بر 8 در وضعیت Standby قرار خواهند گرفت . با استفاده از این دستور می توانید تعیین کنید کدام یک از پورت ها به عنوان پورت اصلی در تشکیل ارتباط Etherchannel شرکت کنند و کدام یک از آنها در حالت Standby قرار گیرند . مقدار این پارامتر به صورت پیش فرض برابر با 32768 بوده اما می توانید از اعداد 1 الی 65535 استفاده کنید . در صورتی که Lacp Port – Priority همه پورت ها با هم برابر باشد ، پورت هایی که شماره آنها در روی سوئیچ کمتر از دیگران باشد به عنوان پورت ها اصلی انتخاب می شوند .

Switch B / Switch A	Passive	Active	On
Passive	NO	YES	NO
Active	YES	YES	NO
On	NO	NO	YES

LACP

دستورات نمایش وضعیت Etherchannel :

Switch # Show { PAgP | LACP } Neighbor

Switch # Show Etherchannel

Switch # Show Etherchannel Load – balance

Switch # Show Etherchannel Port – channel

Switch # Show Etherchannel Summary

مثال :

show etherchannel summary *Command Output*

```
Switch# show etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SU)         PAgP       Fa0/41(P)   Fa0/42(P)   Fa0/43   Fa0/44(P)
                                  Fa0/45(P)   Fa0/46(P)   Fa0/47(P)   Fa0/48(P)
```

پیکربندی Load Balancing در روی اتصالات Etherchannel :

برای انجام این کار از دستور زیر استفاده می کنیم :

Switch (config) # Port Channel load – balance method

جدول زیر نشان دهنده متدهایی است که می توانید به جای متغیر method از آنها استفاده کنید که به صورت پیش فرض متد src – dst – ip مورد استفاده قرار می گیرد .

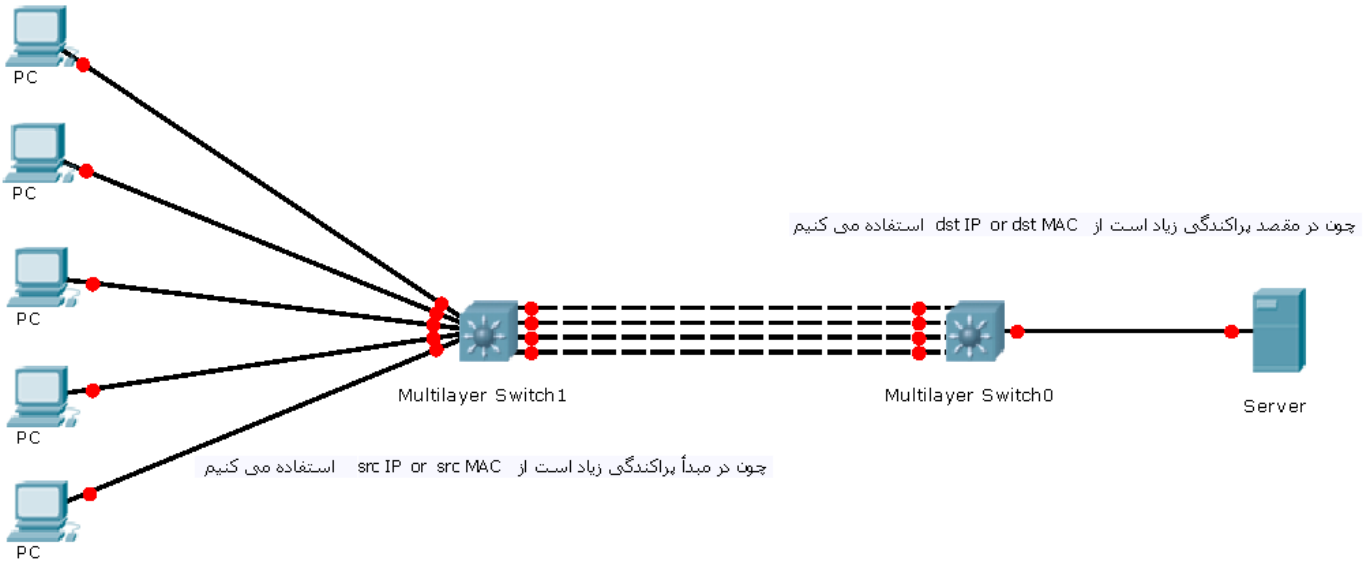
Types of EtherChannel Load-Balancing Methods

***method* Value**	**Hash Input**	**Hash Operation**	**Switch Model**
src-ip	Source IP address	bits	All models
dst-ip	Destination IP address	bits	All models
src-dst-ip	Source and destination IP address	XOR	All models
src-mac	Source MAC address	bits	All models
dst-mac	Destination MAC address	bits	All models
src-dst-mac	Source and destination MAC	XOR	All models
src-port	Source port number	bits	6500, 4500
dst-port	Destination port number	bits	6500, 4500
src-dst-port	Source and destination port	XOR	6500, 4500

نکته مهم :

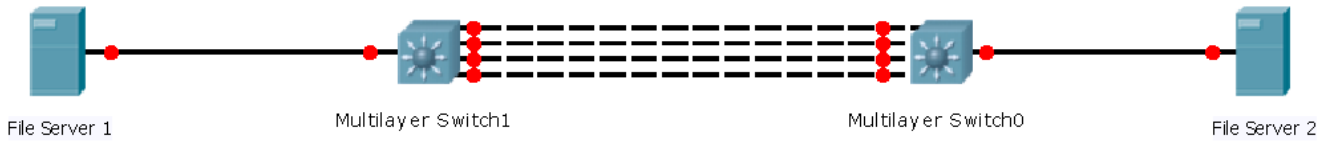
اگر پراکندگی در مقصد زیاد باشد از متدهایی که dst هستند استفاده می کنیم و اگر پراکندگی در مبدأ زیاد باشد از متدهایی که src هستند استفاده می کنیم و اگر پراکندگی در هر دو صرف زیاد باشد از متدهایی که dst و src هستند استفاده می کنیم . IP اولویت دارد بر MAC .

به شکل زیر دقت کنید :



در همچنین سناریوهایی method سوئیچ های دو طرف با هم فرق می کند . در Switch 0 از متدهای Dst IP و Dst MAC استفاده می شود چون پراکندگی در مقصد زیاد است ولی در Switch 1 از متدهای Src IP و Src MAC استفاده می شود چون پراکندگی در مبدأ زیاد است .

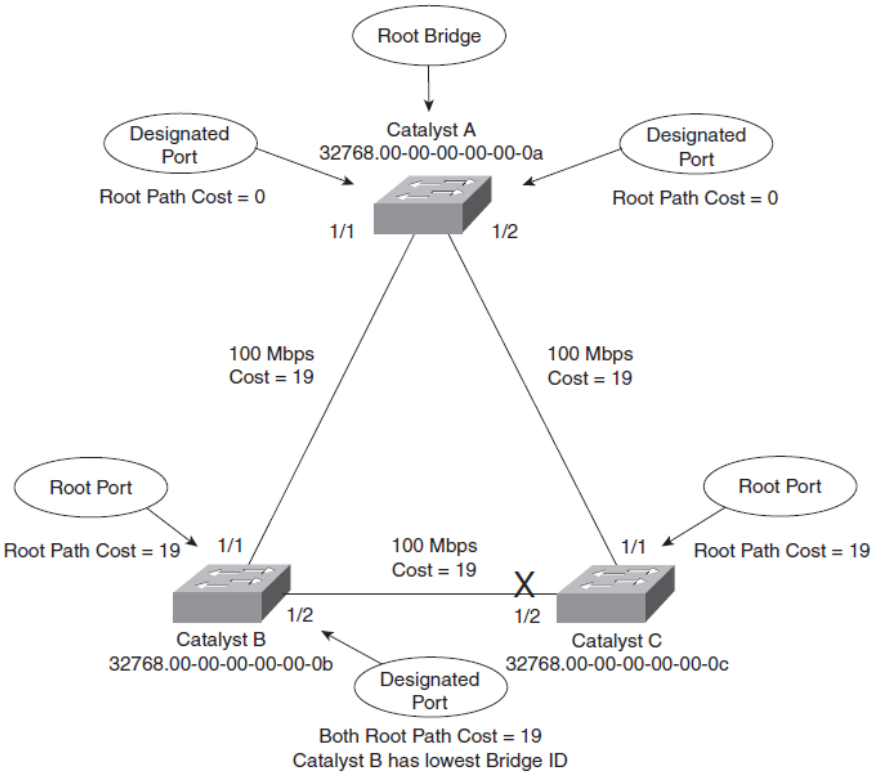
به شکل زیر دقت کنید :



در همچنین سناریوهایی چون تعداد MAC و IP در دو طرف یکی است پس فقط از یک پورت ارسال می شود . باید در این حالت از متد Src – Port یا Dst – Pore استفاده کنیم چون هر برنامه شماره پورت اختصاصی دارد و نسبت به آن شماره از متدها استفاده می شود .

Traditional Spanning Tree Protocol

Spanning – Tree Protocol



: STP

وظیفه اصلی STP جلوگیری از رخ دادن Loop و متوقف کردن Loop رخ داده شده در لایه 2 می باشد . در واقع این کار را با Shutdown کردن لینک های اضافی انجام میدهد . تمام سوئیچ های سیسکو با ورژن IEEE 802.1D کار می کنند .

STP با بکار بردن Spanning – Tree Algorithm یا همان STA , توپولوژی شبکه را به صورت درخت درآورده و سپس با غیر فعال کردن مسیرهای اضافی که منجر به رخ دادن Loop در شبکه شده اند , Loop رخ داده شده را مهار می کند . در شبکه انتخاب Root (ریشه) خیلی مهم است .

این پروتکل در 3 مرحله کار خود انجام می دهد :

1. Elect Root Bridge Per Network
2. Select Root Port Per Switch
3. Select designated Port Per Link (segment)

Bridge ID :

BID ملاک شناسایی یک سوئیچ در STP می باشد . در واقع مشخصه ای است که یک سوئیچ به کمک آن در میان سوئیچ های دیگر شناخته می شود .

BID : Bridge Priority + MAC Address

Priority :

عددی است برابر با 32768 که روی سوئیچ سیسکو به صورت پیش فرض Set شده است و قابل تغییر نیز است , عددی بین 0 تا 65535 را می توانیم انتخاب کنیم . در سوئیچ به صورت زیر نمایش داده می شود :

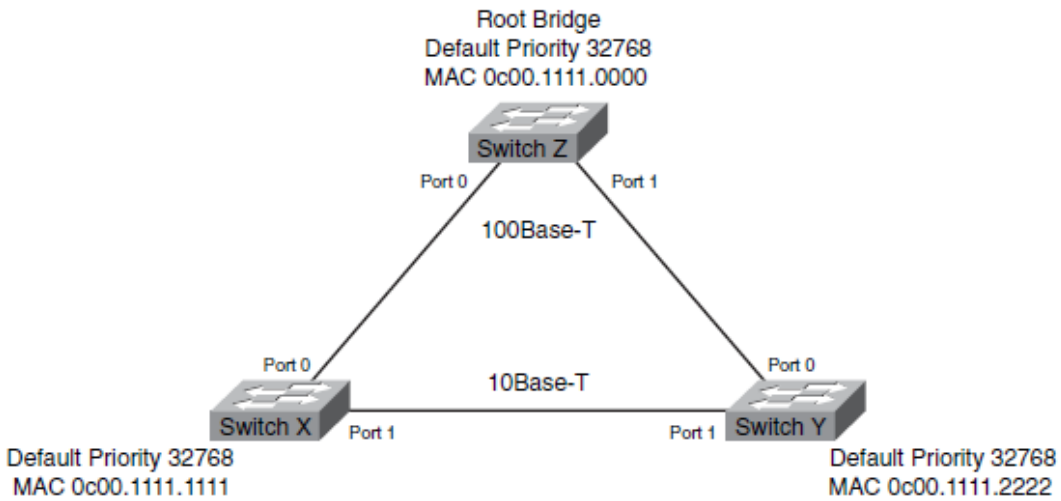
Bridge ID : 32768 : MAC Address

Root Bridge :

BID های سوئیچ های شبکه با هم مقایسه می شوند و سوئیچی که دارای پایین ترین BIDباشد به عنوان Root Bridge انتخاب می شود .

نکته : اولین معیار برای مقایسه , Priority می باشد . سوئیچی که پایینترین Priority را داشته باشد Root Bridge انتخاب می شود .

اگر Priority همه سوئیچ ها با هم برابر باشد در این حالت سوئیچی که دارای پایین ترین MAC Address باشد به عنوان Root Bridge انتخاب می شود .



در شکل فوق چون priority همه سوئیچ ها برابر است و MAC سوئیچ Z از همه پایین تر است پس به عنوان Root Bridge انتخاب می شود .

BPDU : Bridge Protocol Data Unit

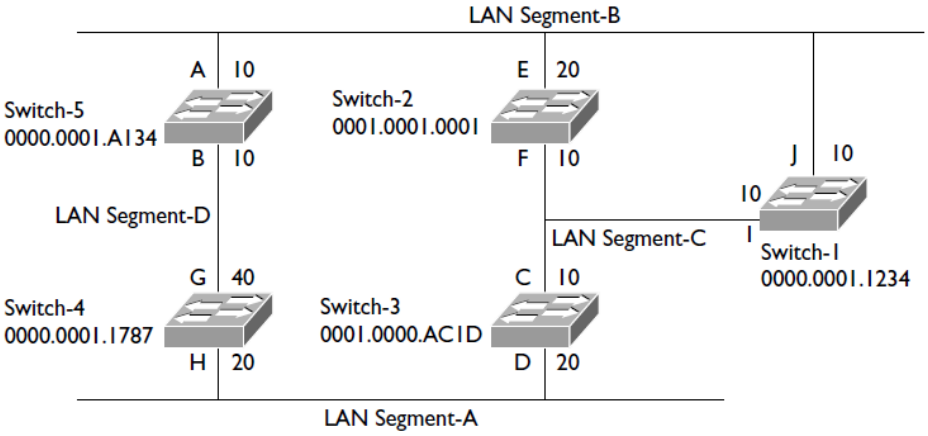
فریمی است که سوئیچ ها به کمک آن با هم تبادل اطلاعات می کنند , به کمک این فریم با یکدیگر صحبت می کنند و خود را به دیگران معرفی می کنند تا در نهایت بتوانند در شبکه Root Bridge را انتخاب کنند . همچنین هر گونه تغیراتی که بابت تغییر توپولوژی رخ دهد با این فریم ها به هم اطلاع می دهند .

در پروتکل STP دو نوع BPDU به شرح زیر خواهیم داشت :

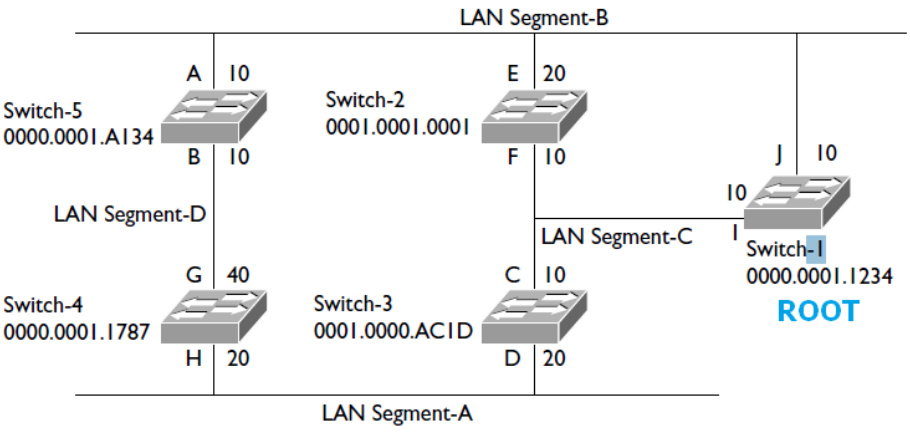
- Configuration BPDU : شامل اطلاعاتی برای شناخت توپولوژی لایه 2 و محاسبات پروتکل STP می باشد .
- TCN BPDU : این نوع BPDUها جهت اعلام تغییرات در توپولوژی شبکه استفاده می شود.

مراحل STP :

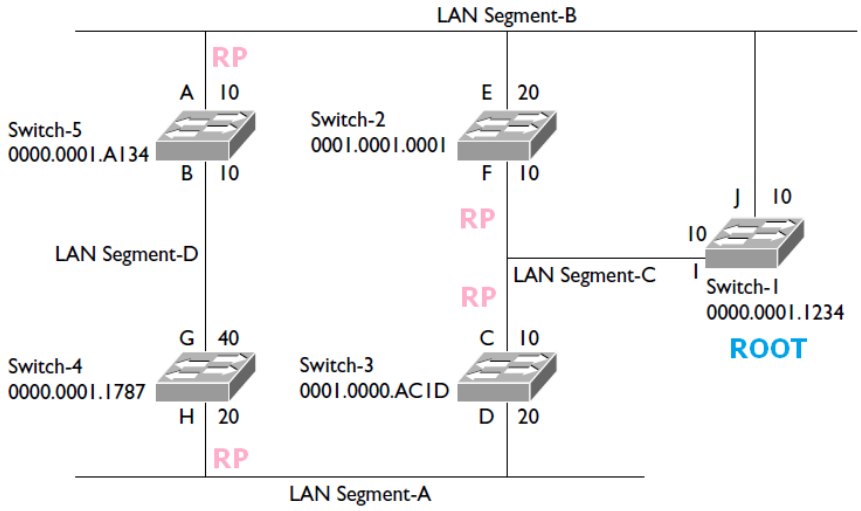
به شکل زیر توجه کنید :



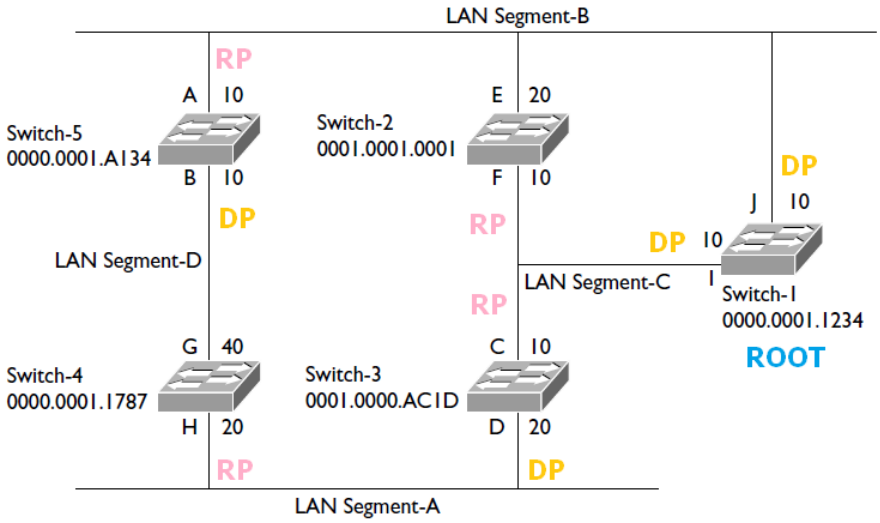
مرحله اول : Root Bridge انتخاب می شود



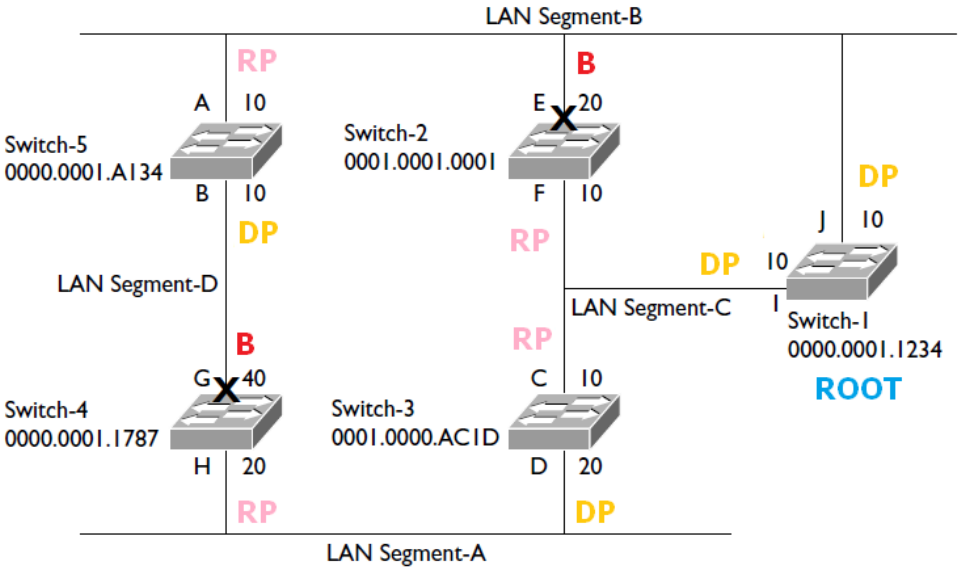
مرحله دوم : Root Port انتخاب می شود



مرحله سوم : Designated Port مشخص می شود



مرحله چهارم : لینک های Block تعیین و Shutdown می شوند



Root Port :

پورتی از سوئیچ که دارای کمترین Cost تا Root Bridge است . پورتی است که BPDU با کاست کمتری دریافت بشود .

Designated Port :

پورتی از سوئیچ که به عنوان پورت Forwarding انتخاب می شود . در این حالت پورت قابلیت ارسال و دریافت اطلاعات را خواهد داشت . پورتی است که BPDU با کاست کمتری روی آن ارسال می شود .

Block :

لینک هایی که نه RP و نه DP باشد یا پورتی که دارای Cost بیشتری در مقایسه با RP باشد Block شده و مانع از رخ دادن Loop می شود . زمانی که یکی از پورت ها قطع شود این پورت وصل می شود .

نکته :

اگر COST برابر باشد به Sender Bridge ID نگاه می کند که کدام بهتر است یعنی کدام کمتر باشد آن را RP تعیین می کند .اگر هم Cost هم Sender Bridge ID برابر باشند به Sender Port ID نگاه می کند هر کدام کمتر باشد آن را RP تعیین می کند .

تمامی پورت هایی که به Root Bridge متصل هستند به عنوان DP انتخاب می شوند.

Cost نسبت عکس با Bandwidth دارد . این بیانگر آن است که با افزایش پهنای باند , Cost کم می شود .

در شروع شبکه هر سوئیچ یک فریم BPDU به شرح زیر تهیه و ارسال می کند:

1. Root Bridge " Bridge ID "
2. Sender Bridge " Bridge ID "
3. Root Path Cost
4. Sender Port ID

وقتی که Root Bridge یک شبکه مشخص شد از آن به بعد فقط او فریم های BPDU را می فرستد .

جدول STP Path Cost :

STP Path Cost

Link Bandwidth	Old STP Cost	New STP Cost
4 Mbps	250	250
10 Mbps	100	100
16 Mbps	63	62
45 Mbps	22	39
100 Mbps	10	19
155 Mbps	6	14
622 Mbps	2	6
1 Gbps	1	4
10 Gbps	0	2

تغییر Root Path Cost :

دستور تغییر Cost اینترفیس در پروسه Spanning – tree :

Switch (config – if)# Spanning – tree [VLAN vlan – id] Cost [Cost]

دستور نمایش Cost اینترفیس در پروسه Spanning – tree :

Switch # Show Spanning – tree Interface type mod/mod [Cost]

مثال :

برای نمونه مقدار STP Cost پیش فرض مربوط به یک پورت Gigabit Ethernet برابر با 4 بوده اما می توان مقدار آن را با استفاده از دستور زیر در VLAN 10 به 2 تغییر داد :

Switch (config – if)# Spanning – tree VLAN 10 Cost 2

همانطور که در زیر مشاهده می کنید پورت Gigabit Ethernet 0/1 به عنوان Trunk تعیین شده و ترافیک مربوط به VLANهای 1 و 10 و 20 را از خود عبور می دهد . در این شرایط می توان مقدار Cost این پورت در مورد تمامی VLANها را به ترتیب مشاهده کرد :

Displaying STP Port Cost Values on an Interface

```
Switch# show spanning-tree interface gigabitEthernet 0/1
Vlan                Role Sts Cost       Prio.Nbr Type
------------------- ---- --- ---------- -------- --------------------------------
VLAN0001            Root FWD 4          128.1    P2p
VLAN0010            Desg FWD 2          128.1    P2p
VLAN0020            Root FWD 4          128.1    P2p
```

نکته :

Cost زمانی افزایش پیدا می کند که وارد اینترفیس سوئیچ شود نه خارج .

تغییر مقدار Port ID :

STP Port ID : Port priority . Port #

Priority عددی است بین 0 تا 255 که پیش فرض 128 است . این شناسه برابر با 16 بیت بوده که 8 بیت آن مربوط به Priority پورت و 8 بیت دیگر نیز برابر با شماره آن می باشد .

مثال : شماره پورت Gigabit Ethernet 3/16 برابر با 128.144 می باشد .

دستور تغییر priority برای تغییر Sender Root Port :

Switch (config – if)# Spanning – tree [VLAN vlan – id] Port – Priority [priority]

این دستور را باید در روی اینترفیسی که BPDU ارسال می کند وارد کنیم تا در هنگام فرستادن BPDU مقدار Sender Root Port را با مقدار جدید به سوئیچ دیگر ارسال کند.

دستور نمایش priority اینترفیس در پروسه Spanning – tree :

Switch # Show Spanning – tree Interface type mod/mod [priority]

مثال : مقدار priority پیش فرض مربوط به یک پورت Gigabit Ethernet 3/16 برابر با 128 بوده اما می توان مقدار آن را با استفاده از دستور زیر در VLANهای 10 و 100 برابر با 64 تغییر داد :

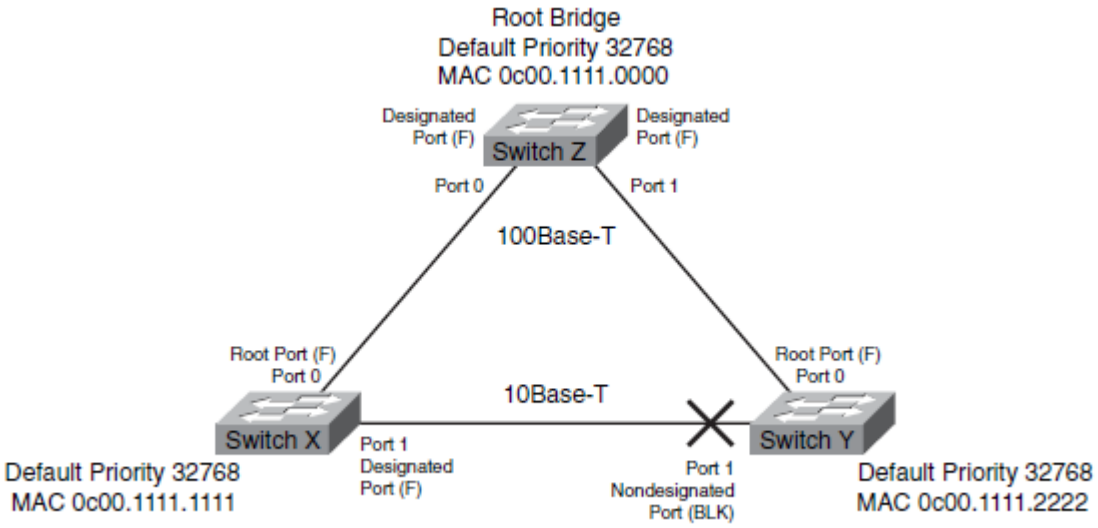
Switch (config – if)# Spanning – tree VLAN 10 , 100 Port – Priority 64

همانطور که در زیر مشاهده می کنید پورت Gigabit Ethernet 3/16 به عنوان Trunk تعیین شده و ترافیک مربوط به VLANهای 10 و 100 و 200 را از خود عبور می دهد . در این شرایط می توان مقدار priority این پورت در مورد VLANهای 10 و 100 را که به 64 تغییر یافته مشاهده کرد :

Confirming STP Port Priority Values After Configuration

```
Switch# show spanning-tree interface gigabitEthernet 3/16
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0010         Desg FWD 4           64.144  Edge P2p
VLAN0100         Desg FWD 4           64.144  Edge P2p
VLAN0200         Desg FWD 4          128.144  Edge P2p
Switch#
```

مثال :



فریم های BPDU که سوئیچ های شبکه شکل فوق به هم می فرستند :

BPDU Switch Z → Switch X

- Switch Z
- Switch Z
- 0
- 128 . 0

BPDU Switch Z → Switch Y

- Switch Z
- Switch Z
- 0
- 128 . 1

BPDU Switch X

- Switch Z
- Switch X
- 19
- 128 . 1

BPDU Switch Y

- Switch Z
- Switch Y
- 19
- 128 . 1

دستور مانیتورینگ :

Switch # Show Spanning – tree Summary

Switch # Show Spanning – tree [Root | Bridge]

نکته :

در خروجی دستور Show Spanning – tree در قسمت بالای آن مشخصات Root Bridge و در قسمت وسط مشخصات خود سوئیچ و در قسمت پایین مشخصات پورت ها را نمایش می دهد .

دستور فعال و غیرفعال کردن Spanning – tree :

Switch (config) # [No] Spanning – tree VLAN vlan – id

با اجرا کردن دستور پایین Spanning – tree را روی اینترفیس دلخواه فعال یا غیرفعال می کنیم :

Switch (config) # Interface type mod / mod

Switch (config – if) # [No] Spanning – tree VLAN vlan – id

تغییر Root Bridge :

- روش اول :

کم کردن Priority یک سوئیچ :

Switch (config) # Spanning – tree VLAN vlan – id Priority 0 – 65535

مثال :

Switch (config) # Spanning – tree VLAN 1 Priority 4096

- روش دوم :

روی سوئیچی که می خواهیم Root Bridge باشد این دستور را وارد می کنیم :

Switch (config) # Spanning – tree VLAN vlan – id Root Primary

این دستور را در سوئیچ دوم می زنیم تا اگر Root Bridge اول قطع شد این Root Bridge شود :

Switch (config) # Spanning – tree VLAN vlan – id Root Secondary

زمان های STP :

STP Timers

Timer	Function	Default Value
Hello	Interval between configuration BPDUs.	2 seconds
Forward Delay	Time spent in Listening and Learning states before transitioning toward Forwarding state.	15 seconds
Max Age	Maximum length of time a BPDU can be stored without receiving an update. Timer expiration signals an indirect failure with designated or root bridge.	20 seconds

Hello – Time : فاصله زمانی مربوط به ارسال پیام های Configuration BPDU از طریق سوئیچ Root را نشان می دهد و به صورت پیش فرض برابر با 2 ثانیه می باشد .

Forward – Time : مقدار زمانی را نشان می دهد که یک پورت در وضعیت های Listening و Learning قرار می گیرد و به صورت پیش فرض برای هر کدام از این وضعیت ها برابر با 15 ثانیه می باشد .

Max – Age : مقدار زمانی را نشان می دهد که یک سوئیچ بعد از دریافت پیام BPDU اقدام به حذف آن می نماید و به صورت پیش فرض برابر با 20 ثانیه می باشد .

تغییر زمان های STP :

فقط بر روی Root Bridge زمان ها را تغییر می دهیم . چون فقط او بسته های BPDU ارسال می کند .

Manually Configuring STP Timers

Use one or more of the following global configuration commands to modify STP timers:

```
Switch(config)# spanning-tree [vlan vlan-id] hello-time seconds
Switch(config)# spanning-tree [vlan vlan-id] forward-time seconds
Switch(config)# spanning-tree [vlan vlan-id] max-age seconds
```

نکته :

اگر در دستورات بالا پارامتر [VLAN vlan – id] را تعیین کنیم فقط در آن VLAN تعیین شده زمان ها تغییر می کنند و اگر این پارامتر را ننویسیم تغییر زمان ها بر روی همه VLANها اعمال می شود .

تغییر مقادیر زمان های STP به روش اتوماتیک :

تغییر مقادیر مربوط به زمان های STP نیاز به محاسبه دقیق و مد نظر گرفتن پارامترهایی مانند سایز شبکه یا Diameter دارد .

شکل کلی دستور به صورت زیر است :

Switch (Config) # Spanning – tree VLAN vlan – list Root { Primary | Secondary } [Diameter diameter] [Hello – Time hello – time]

با اجرای دستور فوق و تعیین سایز شبکه با استفاده از پارامتر diameter مقدار این زمان ها به صورت اتوماتیک و با توجه فرمول های مشخص شده در استاندارد IEEE 802.1D محاسبه وتعیین خواهد شد . diameter اشاره به عمق شبکه دارد و بیان کننده تعداد سوئیچ هایی است که مابین سوئیچ Root Bridge و انتهای هر مسیر قرار دارند . در صورتی که از اجرای پارامتر hello – time خودداری کنید ، مقدار آن به صورت پیش فرض برابر با 2 ثانیه قرار خواهد گرفت .

برای مثال فرض کنید که شبکه ای کوچک متشکل از سه سوئیچ می باشد که به صورت یک مثلث با یکدیگر در ارتباط می باشند . خروجی دستور زیر مقدار زمان های فعلی STP را در مورد VLAN 100 نشان داده است :

Displaying the STP Timer Values in Use

```
Switch# show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol ieee
  Root ID     Priority    100
              Address     000c.8554.9a80
              This bridge is the root
              Hello  Time  2  sec  Max  Age  20  sec  Forward  Delay 15  sec

  Bridge ID   Priority    100    (priority 0 sys-id-ext 100)
              Address     000c.8554.9a80
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time 300
[output omitted]
```

نکته :

به دلیل آنکه طولانی ترین مسیر در توپولوژی فرضی ما از 3 سوئیچ تشکیل شده ، بنابراین این شبکه بسیار کوچکتر از توپولوژی نمونه است که توسط طراحان STP برای تعیین مقدار زمان های STP مد نظر قرار داده شده بود .بدین ترتیب که استاندارد IEEE 802.1D فرض را بر آن گذاشته است که شبکه نمونه از 7 عدد سوئیچ در هر مسیر تشکیل شده است . از این رو در شبکه فوق می توانید مقدار diameter را برابر با 3 قرار دهید تا بدین ترتیب زمان Convergence یا همگرایی STP بهبود یابد . در چنین شبکه ای می توان مقدار زمان hello را نیز برابر با 1 ثانیه قرار داد . در این صورت اجرای دستور زیر مقدار زمان های STP را به صورت اتوماتیک و بر حسب مقدار پارامتر diameter محاسبه خواهد کرد :

Switch (config) # Spanning – tree VLAN 100 Root Primary Diameter 3 Hello – Time 1

برای مشاهده تغیرات به خروجی دستور زیر نگاه کنید :

Confirming STP Timer Configuration Changes

```
Switch# show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol ieee
  Root ID     Priority    100
              Address     000c.8554.9a80
              This bridge is the root
              Hello  Time  1  sec  Max  Age  7  sec  Forward  Delay  5  sec

  Bridge ID   Priority    100    (priority 0 sys-id-ext 100)
              Address     000c.8554.9a80
              Hello Time   1 sec  Max Age  7 sec  Forward Delay  5 sec
              Aging Time 300
```

همانطور که در بالا مشاهده می کنید مقدار زمان های Hello Time برابر با 1 ثانیه و Max Age برابر با 7 ثانیه و Forward Delay برابر با 5 ثانیه به صورت اتوماتیک تعیین شده است .

وضعیت پورت ها در STP :

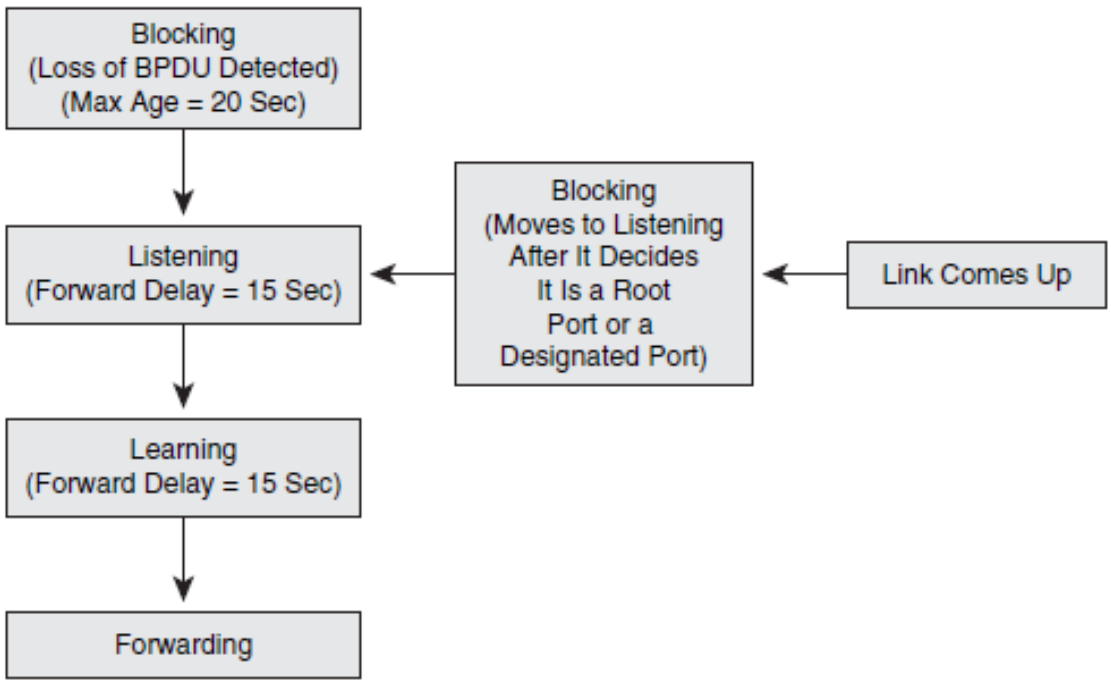
1. **Disable** : در این حالت پورت نه فریمی را دریافت میکند نه ارسال . پورت به صورت دستی غیرفعال شده .

2. **Blocking** : وقتی سوئیچ را روشن می کنیم پورت ها در حالت blocking قرار دارند و هیچ فریمی را ارسال یا دریافت نمی کنند . در این حالت پورت ها فقط به BPDU ها گوش می دهند تا بتوانند در مورد وضعیت بعدی خود تصمیم بگیرند .

3. **Listening** : در این حالت هر سوئیچ با توجه به BPDUهایی که می شنود Root bridge را انتخاب می کند . بنابراین اگر به این پورت فریمی وارد شود که حاوی MAC Address جدیدی باشد در MAC Table خود ذخیره نمی کند .

4. **Learning** : بعد از سپری شدن مدت زمان Listening پورت تغییر وضعیت داده و وارد حالت Learning می شود . در این حالت سوئیچ تمامی مسیرهای موجود در شبکه و مسیرهای فاقد Loop را شناسایی می کند .

5. **Forwarding** : بعداز اینکه Root Port و Designated Port بودن یک پورت مشخص شد در مرحله Forwarding پورت قادر به ارسال و دریافت فریم می باشد .



مثال زیر نشان دهنده قرارگیری یک پورت در وضعیت های مختلف می باشد :

```
*Mar 16 14:31:00 UTC: STP SW: Fa0/1 new disabled req for 1 vlans
Switch(config)# interface fastethernet 0/1
Switch(config-if)#no shutdown
Switch(config-if)#^-Z
*Mar 16 14:31:00 UTC: STP SW: Fa0/1 new blocking req for 1 vlans
```

مثال فوق نشان می دهد که یک پورت در ابتدا در وضعیت Disabled قرار دارد . بعد از فعال سازی پورت مزبور ، اجرای دستور Interface fastethernet 0/1 و Show Spanning – Tree در پایین نشان داده است که وضعیت آن تغییر یافته است .

مرحله اول : پورت در وضعیت Listening قرار می گیرد :

```
Switch# show spanning interface fastethernet 0/1

Vlan             Port ID                    Designated                 Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID             Prio.Nbr
---------------- ------------ ------------- -------------------------- --------
VLAN0001         128.1           19 LIS         0 32769 000a.f40a.2980 128.1

*Mar 16 14:31:15 UTC: STP SW: Fa0/1 new learning req for 1 vlans
```

مرحله دوم : پورت در وضعیت Learning قرار می گیرد :

```
Switch# show spanning interface fastethernet 0/1
Vlan             Port ID                    Designated                 Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID             Prio.Nbr
---------------- ------------ ------------- -------------------------- --------
VLAN0001         128.1           19 LRN         0 32768 00d0.5849.4100  32.129

*Mar 16 14:31:30 UTC: STP SW: Fa0/1 new forwarding req for 1 vlans
```

مرحله سوم : پورت در وضعیت Forwarding قرار می گیرد :

```
Switch# show spanning interface fastethernet 0/1

Vlan             Port ID                    Designated                 Port ID
Name             Prio.Nbr      Cost Sts     Cost Bridge ID             Prio.Nbr
---------------- ------------ ------------- -------------------------- --------

VLAN0001        128.1           19 FWD         0 32768 00d0.5849.4100  32.129
```

جدول زیر خصوصیات پورت را در وضعیت های مختلف نمایش می دهد :

	BPDU Send	BPDU Listening	MAC_Address Learning	Data Forwarding
Block	NO	YES	NO	NO
Listening	YES	YES	NO	YES
Learning	YES	YES	NO	NO
Forwarding	YES	YES	YES	YES

نکته :

پورتی که Block است قطع نیست ولی از Loop جلوگیری می کند یعنی خاموش است ولی فریم های BPDU را دریافت می کند .

نکته : مراحلی که یک پورت از حالت Block به حالت Forwarding تغییر وضعیت می دهد :

Blocking Port → Listening (15 sec) → Learning (15 sec) → Forwarding

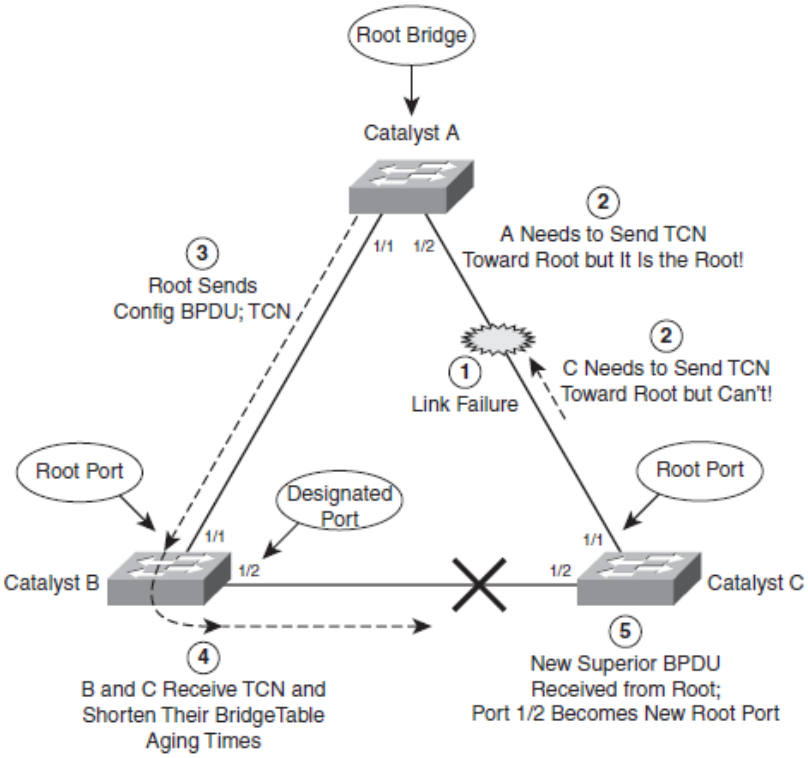
تغییر در توپولوژی STP :

سوئیچ های شبکه در هنگام مشاهده شبکه یک تغییر در توپولوژی اقدام به ارسال پیام های TCN BPDU می نمایند .در حقیقت تنها زمانی یک سوئیچ اقدام به ارسال پیام TCN می نماید که یک پورت در وضعیت Forwarding قرار گرفته و یا از Forwarding یا Learning به Blocking تغییر وضعیت دهد . بعد از بروز تغییرات فوق ، پیام TCN BPDU از طریق پورت root دستگاه به سمت سوئیچ root ارسال خواهد شد تا دستگاه مزبور از بروز تغییری در توپولوژی لایه 2 آگاه گردد .لازم به ذکر است که نوع تغییر در داخل پیام TCN BPDU گنجانده نشده و دریافت این پیام توسط سوئیچ root تنها دلیل بر بروز یک تغییر در توپولوژی لایه 2 می باشد .

به انواع مختلفی از تغییراتی که در شبکه روی میدهند و واکنش STP در قبال آنها خواهیم پرداخت .

STP Topology Change Kind :

- Direct Topology Change (تغییرات مستقیم) :



شکل صفحه قبل نشان دهنده یک توپولوژی است که از لحاظ پروتکل STP در وضعیت پایدار قرار گرفته است . در این نقطه است که اتصال مابین دستگاه های A و C دچار مشکل می شود . ادامه این پروسه به صورت زیر خواهد بود :

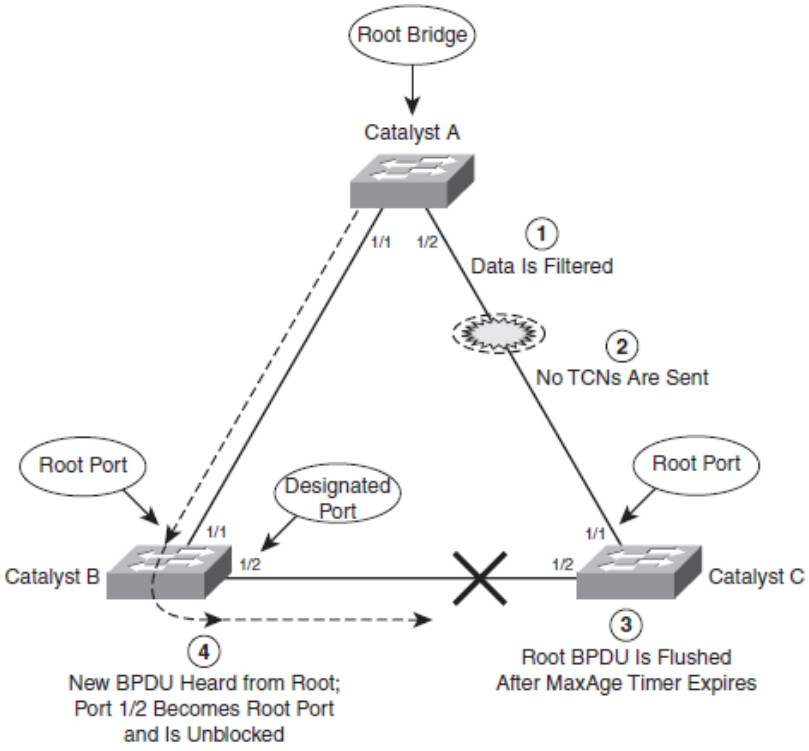
1. مرحله اول : سوئیچ C بروز ایرادی در ارتباط برقرار شده از طریق پورت 1/1 را شناسایی می کند . از سویی دیگر سوئیچ A نیز بروز ایراد در ارتباط برقرار شده از طریق پورت 1/2 خود را شناسایی می کند .
2. مرحله دوم : پورت 1/1 در روی دستگاه C به عنوان Root Port انتخاب شده بود و به همین جهت این دستگاه اطلاعات BPDU دریافت شده از طریق Root Bridge را که در حافظه خود نگه داشته بود ، از حافظه خود پاک می کند . معمولا در این شرایط سوئیچ C سعی خواهد کرد که یک پیام TCN BPDU از طریق Root Port خود به سمت دستگاه Root Bridge ارسال نماید که انجام چنین کاری در این سناریویی به دلیل معیوب بودن Root Port امکان پذیر نخواهد بود . همچنین بدون استفاده از ویژگی های پیشرفته تری مانند Up Link Fast ، سوئیچ C از وجود مسیر جایگزین دیگری به سمت Root Bridge نیز آگاه نیست . از سویی دیگر ، سوئیچ A نیز بروز ایرادی در ارتباط برقرار شده از طریق پورت 1/2 خود را شناسایی کرده و به دلیل آنکه خود این سوئیچ در نقش Root Bridge انتخاب شده است ، بنابراین نیازی به ارسال پیام های TCN BPDU وجود ندارد .

3. مرحله سوم : دستگاه A که به عنوان Root Bridge ایفای نقش می کند ، یک پیام Configuration BPDU ایجاد خواهد کرد که مقدار فیلد TCN آن تغییر یافته و نشان دهنده بروز یک تغییر در توپولوژی می باشد . این پیام از طریق پورت 1/1 ارسال شده و در طی مسیر توسط سوئیچ های دیگر دریافت می شود . بدین ترتیب هر سوئیچ بعد از دریافت ، آن را برای سوئیچ های پایین دستی خود نیز هدایت می نماید تا کل دستگاه ها یک کپی از پیام فوق را در اختیار داشته باشند .

4. مرحله چهارم : سوئیچ های B و C این پیام TCN را دریافت می نمایند و با دریافت این پیام مدت زمان عمر مربوط به داده های جدول CAM را به 15 ثانیه (برابر با مقدار زمان Forward Delay) کاهش می دهند .

5. مرحله پنجم : دستگاه C دوباره منتظر دریافت پیام های ارسالی از سوئیچ Root Bridge خواهد ماند . این بار پیام های مزبور توسط پورت 1/2 مربوط به سوئیچ C دریافت خواهد شد که قبلا در وضعیت Blocking قرار داشت . از این رو سوئیچ C پورت 1/2 خود را به عنوان Root Port جدید انتخاب کرده و وضعیت آن را از Listening به Learning و سپس به Forwarding تغییر می دهد .

Indirect Topology Change (تغییرات غیر مستقیم) :



در شکل فوق مشاهده می کنید که ایرادی در اتصال سوئیچ های A و C باعث تأثیرپذیری غیر مستقیم سوئیچ های مزبور شده است . بدین ترتیب که اتصال مزبور در روی دستگاه های A و C به صورت " UP " گزارش شده اما عاملی مانند یک فایروال مابین این اتصال قرار گرفته و باعث شده است که ترافیک انتقالی از این اتصال دچار مشکل شده یا فیلتر گردد .

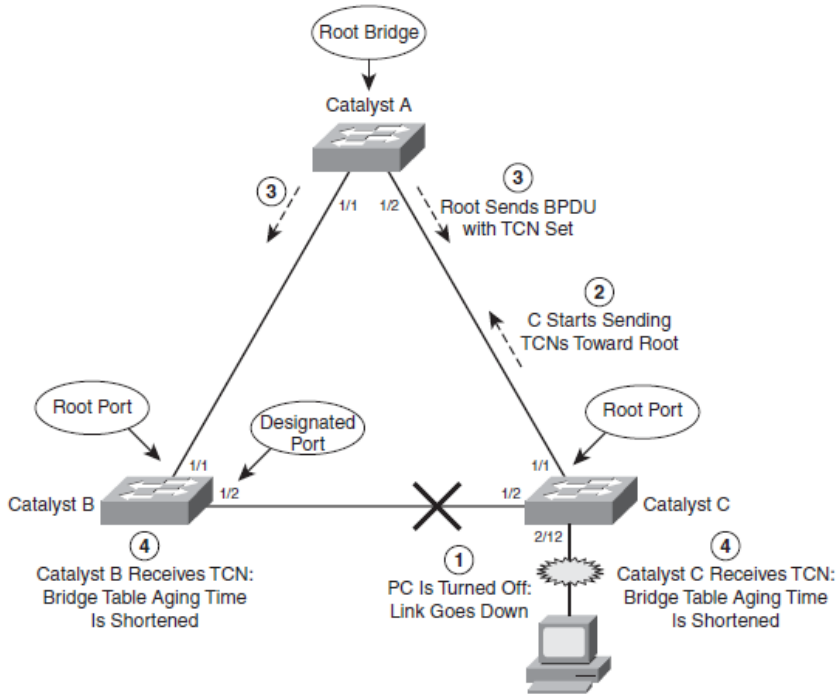
پروتکل STP با استفاده از زمان ها یا timerهای تعیین شده قادر به شناسایی این نوع از مشکلات غیر مستقیم است . کل این پروسه را می توان به صورت زیر تشریح کرد :

1. مرحله اول : با اینکه سوئیچ های A و C اتصال مزبور را به صورت UP گزارش میکنند ، اما به دلیل مشکلی در این اتصال ، هیچ ترافیکی مابین دستگاه های فوق مبادله نمیشود .
2. مرحله دوم : به دلیل آنکه سوئیچ ها هیچ گونه ایرادی در اتصال مشاهده نکرده و وضعیت آن را به صورت UP گزارش میکنند ، بنابراین هیچ پیام TCN نیز ایجاد و ارسال نخواهد شد .
3. مرحله سوم : سوئیچ C هم تا به حال اطلاعات مربوط به بهترین BPDU دریافت شده از سوئیچ Root Bridge که از طریق پورت 1/1 دریافت شده بود را در حافظه خود نگه داشته است . اما در این شرایط هیچ پیام BPDU از سوئیچ Root Bridge توسط پورت مزبور دریافت نمی شود . بعد از گذشت مدت زمان Max – age و به دلیل دریافت نشدن پیام BPDU جدید که باعث تمدید اعتبار پیام های قبلی گردد ، سوئیچ C اطلاعات مربوط به BPDU مزبور را از حافظه خود پاک میکند. در این صورت سوئیچ C منتظر دریافت پیام های BPDU مربوط به سوئیچ Root Bridge از تمامی پورت های خود خواهد ماند .
4. مرحله چهارم : سوئیچ C پیام Configuration BPDU مربوط به سوئیچ Root Bridge را از طریق پورت 1/2 دریافت می کند . بعد از انجام محاسبات ، این پورت به عنوان Root Port جدید انتخاب کرده و وضعیت آن را از Blocking به Listening سپس Learning و در انتها به Forwarding تغییر می دهد .

نکته :

هر سوئیچی که یک قطعی را تشخیص دهد یک پیام TCN از طریق همه پورت هایش حتی پورتی که در حالت Blocking قرار دارد را به Root Bridge می فرستد تا به او بگوید که در شبکه قطعی رخ داده است و در آن لحظه Root Bridge بسته های TC را به همه سوئیچ های شبکه ارسال می کند و اطلاع می دهد که قطعی روی داده است و مدت زمان Update جدول CAM خود را که پیش فرض 300 ثانیه است را به 15 ثانیه کاهش دهند تا مرحله Learning که 15 ثانیه است رخ دهد و MAC جدید را در جدول خود ذخیره کنند و مسیر جدید را برای Forwarding انتخاب کنند . در انتها بعد از 35 ثانیه (که شامل مدت زمان Max – age + Forward – time است) دوباره زمان Update سوئیچ ها به 300 ثانیه برمی گردد .

Insignificant Topology Change (تغییرات نامربوط) :



در شکل فوق مشاهده می کنید که این بار یک دستگاه کامپیوتر به پورت 2/12 سوئیچ C متصل شده است . در این شرایط خاموش و روشن شدن کامپیوتر یا پورت 2/12 باعث خواهد شد تا این سوئیچ تغییر یاد شده را در قالب پیام های TCN به سمت سوئیچ Root Bridge ارسال کند .

برای درک این پروسه مراحل را به ترتیب بیان می کنیم :

1. مرحله اول : کامپیوتر متصل به پورت 2/12 سوئیچ C خاموش می شود . این کار باعث خواهد شد که پورت مزبور نیز در وضعیت Down قرار گیرد .
2. مرحله دوم : سوئیچ C پیام TCN را از طریق پورت 1/1 خود که به عنوان Root Port ایفای نقش می نماید ، به سمت سوئیچ Root Bridge ارسال می کند .
3. مرحله سوم : سوئیچ Root Bridge یک پیام Ack به سمت سوئیچ C ارسال کرده و سپس یک پیام Configuration BPDU با مقدار فیلد TCN تغییر یافته برای تمامی سوئیچ های شبکه ارسال می کند . این کار باعث خواهد شد تا تمامی سوئیچ های غیر Root Bridge از بروز تغییری در جایی از شبکه مطلع شوند .

4. مرحله چهارم : سوئیچ های B و C پیام ارسالی از سوئیچ Root Bridge را دریافت کرده و مدت زمان عمر داده های موجود در جدول CAM خود را کاهش میدهند . این باعث خواهد شد تا اطلاعاتی که اخیرا Update نشده اند از داخل جدول حذف شده و تنها آدرس هایی در آن باقی بمانند که به صورت متمادی اقدام به ارسال اطلاعات می نمایند . این کاهش عمر آدرس های واقع در جدول CAM به صورت پیش فرض به مدت 35 ثانیه (مدت زمان Max – age + Forward – time است) ادامه خواهد داد .

نکته : در قطعی های مستقیم 30 ثانیه طول می کشد ولی در قطعی های غیر مستقیم 50 ثانیه طول می کشد که پورت از حالت Blocking به حالت Forwarding تغییر حالت دهد .

مستقیم	غیرمستقیم
Detect = 0 s	Detect = 20 s
Listening = 15 s	Listening = 15 s
Learning = 15 s	Learning = 15 s
Time = 30 s	Time = 50 s

Spanning – Tree Extend System – id :

برای اینکه یک سوئیچ را به عنوان Root Bridge تعیین کنید ، از یکی از دو متد زیر استفاده کنید :

- مقدار Priority مربوط به سوئیچ را با عددی کمتر از دستگاه های دیگر قرار دهید تا سوئیچ یاد شده در حین پروسه انتخاب دستگاه Root Bridge به این عنوان برگزیده شود . برای این کار دستور زیر را وارد می کنیم :

Switch (config) # Spanning – tree VLAN vlan – list Priority bridge – priority

در این دستور متغیر bridge – priority اشاره به مقدار Priority سوئیچ دارد که به صورت پیش فرض برابر با 32768 بوده اما می توان از عددی در رنج 0 الی 65535 استفاده کرد . در صورتی که ویژگی System – id Extend در وضعیت فعال باشد ، مقدار پیش فرض این متغیر برابر با 32768 بعلاوه شماره VLAN خواهد بود . به صورت دقیق تر عدد مزبور برابر با یکی از مضرب های 4096 در رنج 0 الی 61440 خواهد بود .

- مجبور کردن یک سوئیچ به اعمال تغییرات بر روی تنظیمات STP به گونه ای که به عنوان دستگاه Root Bridge برگزیده شود . تایپ دستور زیر باعث اجرای اتوماتیک برخی از دستورات دیگر می گردد . برای نمونه مقدار Priority مربوط به سوئیچ توسط مدیر تعیین نشده ولی اجرای این دستور دستگاه را مجبور می کند در پی هماهنگی با سوئیچ های دیگر موجود در داخل یک VLAN یا مجموعه ای از آنها مقدار Priority خود را برابر با عددی کمتر از بقیه تعیین نماید که نتیجه این کار ، انتخاب شدن آن به عنوان Root Bridge مورد نظر خواهد بود .

Switch (config) # Spanning – tree VLAN vlan – list Root { Primary | Secondary }

در صورتی که از پارامتر Primary استفاده شود ، سوئیچ سعی خواهد کرد که خود را در نقش دستگاه Root Bridge فعال قرار دهد . اما در صورتی که از پارامتر Secondary استفاده شود ، سوئیچ سعی خواهد کرد که خود را در نقش دستگاه Root Bridge ثانویه انتخاب کند .

استفاده از اتصالات ثانویه و ویژگی Redundancy :

متدهای دیگری نیز وجود دارد که با استفاده از آنها می توانید مقدار زمان همگرایی یا Convergence شبکه را در هنگام بروز ایرادی در آن کاهش دهید . این پارامترها که مختص سیسکو می باشند عبارتند از :

- Port Fast
- Uplink Fast
- Backbone Fast

روش های فوق به جای اعمال تغییر در زمان های STP باعث تخصیص نقش ویژه ای بر روی برخی از پورت ها شده و بدین ترتیب باعث افزایش زمان همگرایی یا Convergence شبکه می شوند .

سازمان استاندارد IEEE نیز پروتکل STP را بهبود داده و بدین ترتیب نسخه پیشرفته تری از آن را معرفی کرده است که به نام IEEE 802.1w یا (RSTP) Rapid Spanning Tree Protocol نامیده می شود .

Port – Fast :

مختص دستگاه های سیسکو است که باعث می شود مراحل Listening و Learning روی اینترفیس های Access صورت نگیرد و زودتر فعال شود . به صورت نرمال در زمان اتصال PC به پورت یک سوئیچ که بر روی آن پروتکل STP فعال می باشد زمانی معادل 30 ثانیه طول می کشد که پورت سوئیچ متصل به PC در وضعیت Forwarding قرار گیرد . در این مدت 30 ثانیه PC قادر به برقراری ارتباط نخواهد بود . با استفاده از توانمندی Port – Fast بر روی پورت های سوئیچ که در حالت Access قرار دارند و به PC یا سایر دستگاه هایی که ایجاد Loop نمی کنند متصل می باشند می توانند بعد از اتصال به سوئیچ بلافاصله در وضعیت Forwarding قرار گیرند .

به صورت پیش فرض ویژگی Port – Fast در روی تمامی پورت های سوئیچ در وضعیت غیرفعال قرار دارد . می توانید با دستور زیر این ویژگی را بر روی تمامی پورت های Access سوئیچ فعال نمایید :

Switch (config) # Spanning – tree Pore – Fast default

برای فعال یا غیرفعال کردن ویژگی فوق در روی یک پورت خاص می توان از دستور زیر استفاده کرد :

Switch (config – if) # [No] Spanning – tree Pore – Fast

نکته : حتما Port – Fast روشن شود .

برای مشاهده وضعیت ویژگی Port – Fast می توانید از دستور زیر استفاده کنید :

Switch # Show Spanning – tree Interface type mod/mod Port - Fast

برای نمونه مثال زیر نشان می دهد که پورت Fast Ethernet 0/1 عضوی از VLAN 10 بوده و ویژگی Port – Fast در روی آن نیز فعال گشته است .

You can display the current PortFast status with the following command:

```
Switch# show spanning-tree interface type mod/num portfast
```

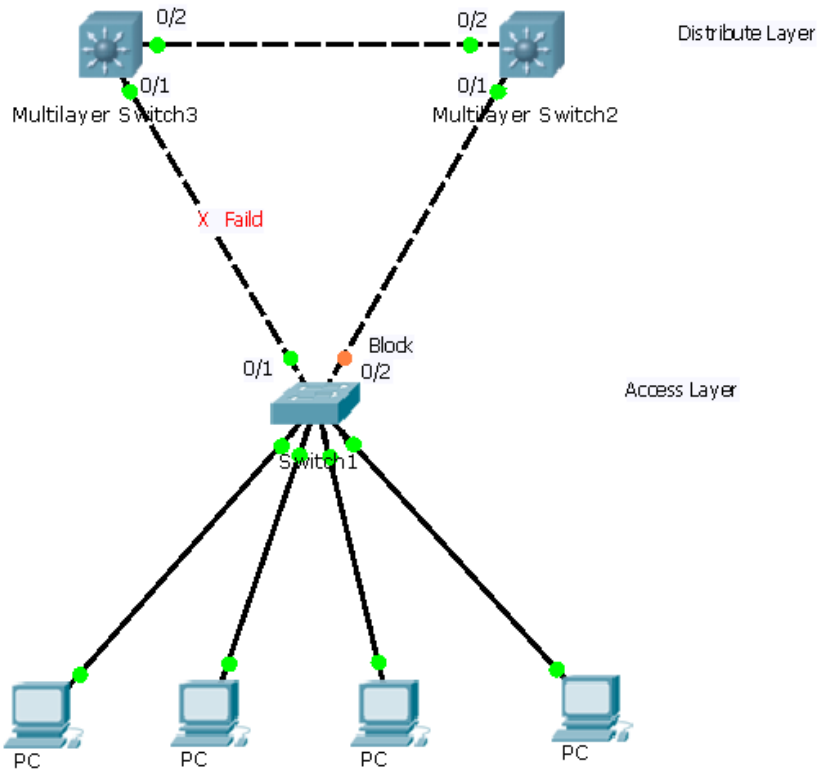
For example, the following output shows that port Fast Ethernet 0/1 supports only access VLAN 10 and has PortFast enabled:

```
Switch# show spanning-tree interface fastethernet 0/1 portfast
VLAN0010          enabled
Switch#
```

Uplink Fast :

فرض کنید که به قصد در اختیار داشتن ویژگی Redundancy ، یک سوئیچ در لایه Access با استفاده از دو اتصال فیزیکی مجزا به دو سوئیچ در لایه Distribute متصل شده است . در حالت عادی یکی از این اتصال ها به عنوان اتصال اصلی و در وضعیت فعال بوده و دیگری به عنوان اتصال جایگزین و غیرفعال می باشد . در این صورت بروز ایرادی در اتصال اصلی باعث خواهد شد تا بعد از سپری شدن حداکثر 50 ثانیه ، اتصال دوم برای انتقال اطلاعات مورد استفاده قرار گیرد و این مدت زمان زیادی است که شبکه قطع باشد. برای رفع این مشکل از ویژگی Uplink Fast بر روی سوئیچ های لایه Access استفاده می کنیم که باعث خواهد شد در صورت بروز ایرادی در اتصال Root Port ، سوئیچ بلافاصله اقدام به استفاده از پورتی که در وضعیت Blocking دارد نماید.

به شکل زیر توجه کنید :



همانگونه که در شکل صفحه قبل مشاهده می کنید ، اگر ویژگی Uplink Fast بر روی سوئیچ 1 که در لایه Access قرار دارد را فعال کنیم وضعیت Listening پورت ها را حذف می کند و در صورت بروز مشکل برای پورت root ، سریعا پورت Black را وصل و در وضعیت Forwarding قرار می دهد که سوئیچ 2 بتواند MAC کامپیوترهایی که به سوئیچ 1 متصل هستند را از طریق پورت 0/1 خود دریافت کند تا در جدول CAM خود ذخیره کند این کار را با استفاده از ارسال پیام های Dummy Multicast به سمت آدرس ثابت 0100.0ccd.cdcd انجام می گیرد . سوئیچ 2 نمی تواند از طریق پورت 0/2 خود این MACها را دریافت کند زیرا لینکی که به سوئیچ 1 و 3 وصل است دچار مشکل شده است .

می توانید با دستور زیر این ویژگی را بر روی تمامی پورت های سوئیچ و همچنین کلیه VLANهای موجود فعال نمایید :

Switch (config) # Spanning – tree Uplinkfast [Max – Update – Rate packets – per – second]

نکته : سوئیچ با در نظر گرفتن مقدار پارامتر Max – Update – Rate اقدام به ارسال پیام های Multicast Dummy می نماید . مقدار پیش فرض این پارامتر برابر با 150 پاکت بر ثانیه می باشد اما می توانید از عدد 0 الی 65535 استفاده کنید .

برای مشاهده وضعیت مربوط به STP Uplink Fast می توانید از دستور زیر استفاده کنید. نمونه ای از اجرای آن نیز در زیر نشان داده شده است :

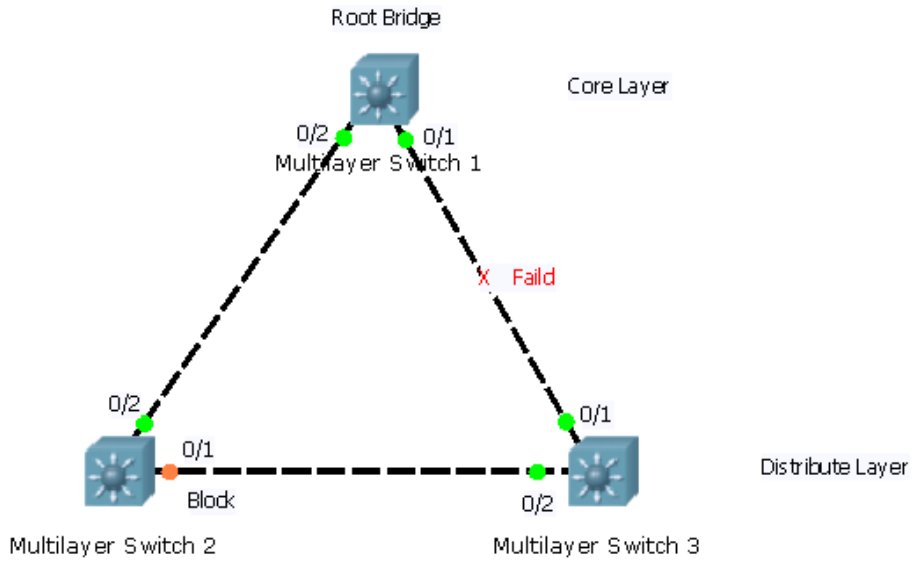
```
Switch# show spanning-tree uplinkfast
UplinkFast is enabled
Station update rate set to 150 packets/sec.
UplinkFast statistics
Number of transitions via uplinkFast (all VLANs)            : 2
Number of proxy multicast addresses transmitted (all VLANs)  : 52

Name                   Interface List
---------------------- --------------------------------
VLAN0001               Gi0/1(fwd)
VLAN0010               Gi0/1(fwd)
VLAN0100               Gi0/1(fwd)
Switch#
```

Backbone Fast :

ویژگی Backbone Fast بر روی سوئیچ هایی که در لایه های Core و Distribiute قرار دارند مورد استفاده قرار می گیرد . با فعال کردن این ویژگی بر روی سوئیچ ها ، مدت زمان Max Age را در هنگام قطعی پورت حذف می کنند و فقط مراحل Listening و Learning رخ خواهد داد .

به شکل زیر دقت کنید :



همانگونه که در بالا مشاهده می کنید پورت 0/1 بین دو سوئیچ 1 و 3 قطع شده است و سوئیچ 3 نمی تواند از طریق پورت 0/1 خود به سوئیچ 1 ترافیک بفرستد . سوئیچ 3 به محض اطلاع از این موضوع ، پیامی به سوئیچ 2 مبنی بر اینکه " من Root Bridge هستم " را ارسال می کند . سوئیچ 2 قبل از اینکه قبول کند که سوئیچ 3 ، Root Bridge شده است پیامی به سوئیچ 1 نام (Root Link Query) RLQ مبنی بر اینکه " آیا هنوز Root Bridge هستی ؟ " را ارسال می کند . وقتی که سوئیچ 1 پاسخ داد که Root Bridge هستم آنگاه سوئیچ 2 به سوئیچ 3 اعلام می کند که هنوز سوئیچ 1 در نقش Root Bridge قرار دارد ، پس پورت خود را که در حالت Block قرار دارد با حذف زمان Max Age به وضعیت Forwarding تغییر می دهد که در نهایت سوئیچ 3 از طریق این پورت می تواند با Root Bridge در ارتباط باشد .

می توانید با دستور زیر این ویژگی را بر روی سوئیچ فعال نمایید :

```
Switch ( config ) # Spanning – tree  Backbonefast
```

برای مشاهده وضعیت مربوط به Backbone Fast می توانید از دستور زیر استفاده کنید. مثالی از اجرای آن نیز در زیر نشان داده شده است :

```
Switch# show spanning-tree backbonefast
BackboneFast is enabled
Switch#
```

همانطور که در خروجی دستور بالا مشاهده می کنید ویژگی Backbone Fast بر روی سوئیچ مورد نظر فعال (Enabled) شده است .

نکته :

اگر یک پورت را بخواهیم برای وصل شدن به یک PC آماده کنیم با اجرا کردن دستور زیر سه کار را به صورت اتوماتیک بر روی آن پورت انجام می دهد . اول پورت را در حالت Access قرار می دهد ، دوم ویژگی Port Fast را بر روی آن فعال می کند ، سوم ویژگی Aggrigation را بر روی آن پورت خاموش می کند :

Switch (config - if) # Switch – Port Host

Types of STP

انواع پروتکل STP :

سیسکو و سازمان استاندارد IEEE هر دو به صورت مستقل اقدام به ارائه نسخه هایی متفاوت از پروتکل STP کرده اند که قابلیت مقیاس پذیری آن به صورت چشمگیری افزایش یافته است و همچنین زمان Convergence یا همگرایی شبکه نیز بهبود پیدا کرده است . نسخه های دیگر پروتکل STP عبارتند از :

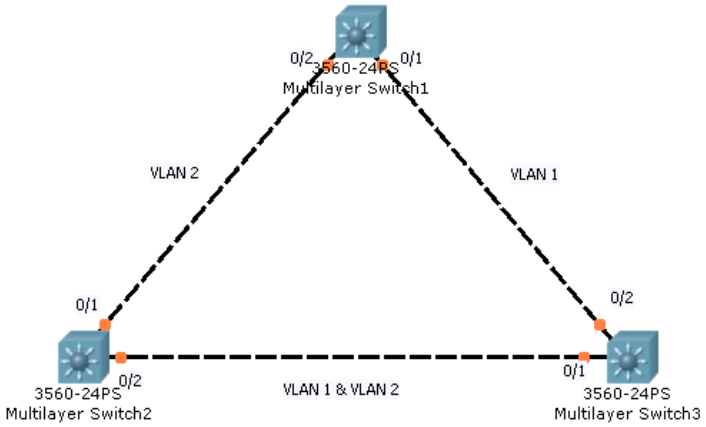
Common Spanning Tree (CST) :

این ورژن از پروتکل IEEE 802.1Q استفاده می کند یعنی تمام لینک ها در حالت Trunk قرار دارند و ارسال اطلاعات تمامی VLANها از طریق این نوع از اتصالات صورت می گیرد . به ازای همه VLANها یک STP فعال است . تمامی پیام های CST BPDU از طریق اتصالات Trunk و با استفاده از Native VLAN و به صورت Untagged منتقل می شوند . در این ورژن امکان در اختیار داشتن ویژگی Load Balancing را نخواهیم داشت .

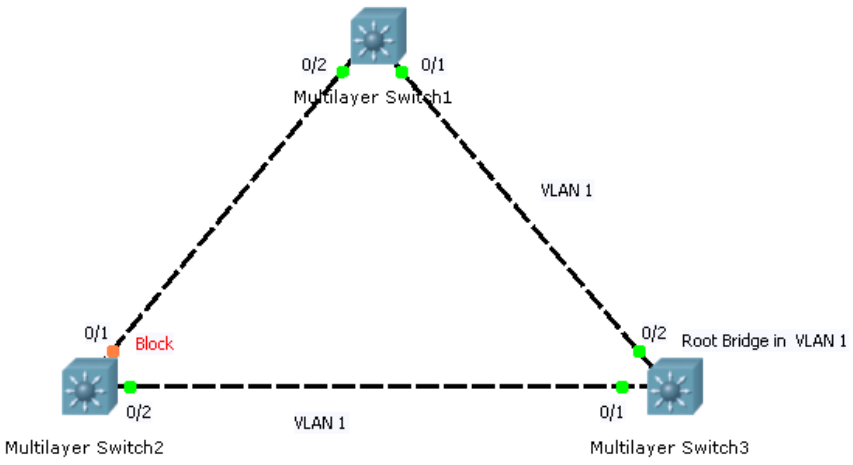
Per – VLAN Spanning Tree (PVST) :

سیسکو این نسخه از STP را ارائه داده است به نام PVST نامیده می شود که در آن ، یک پروسه مجزا از پروتکل STP به ازای هر یک از VLANها در شبکه اجرا می گردد . در این شرایط می توان پروتکل STP را به صورت مستقل در مورد تک تک VLANها پیکربندی کرد که نتیجه آن ، بهبود کارایی هر VLAN خواهد بود . در این حالت امکان در اختیار داشتن ویژگی Load Balancing را خواهیم داشت . به دلیل آنکه پروتکل PVST توسط سیسکو معرفی شده است ، بنابراین برای استفاده از آن باید اتصال Trunk را با بهره گیری از پروتکل ISL ایجاد نمود .

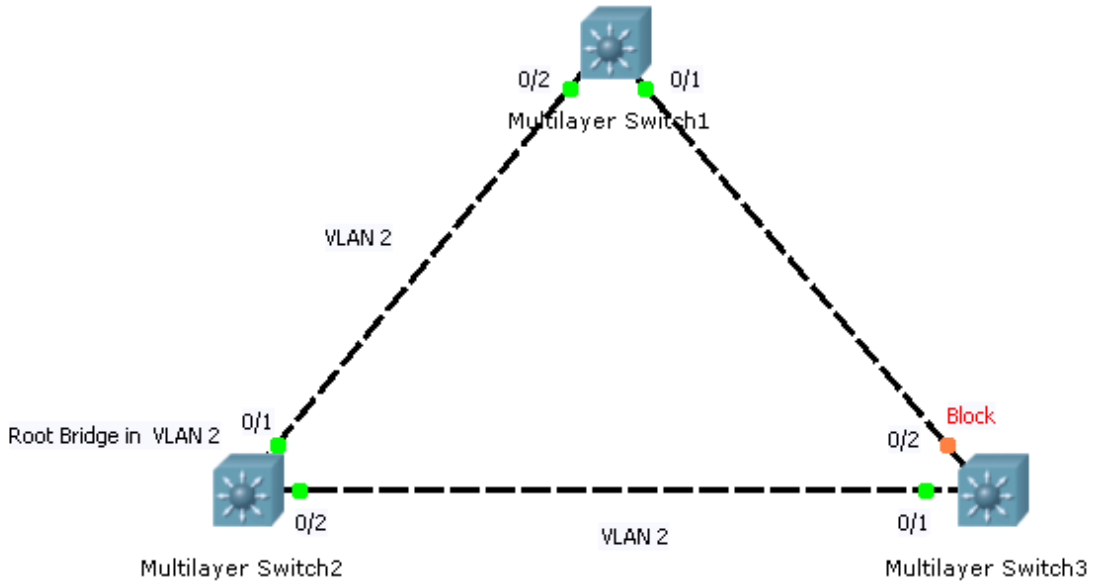
به شکل توجه کنید :



همانطور که در شکل بالا مشاهده می کنید از ورژن PVST استفاده شده است . در این سناریو که دارای دو VLAN می باشد از دو پروسه STP برای هر VLAN یک پروسه استفاده شده است و در پروسه STP که در VLAN 1 کار می کند سوئیچ 3 در نقش Root Bridge کار می کند و پورت 0/1 سوئیچ 2 در وضعیت Block قرار دارد . اما در پروسه STP که در VLAN 2 کار می کند سوئیچ 2 در نقش Root Bridge کار می کند و پورت 0/2 سوئیچ 3 در وضعیت Block قرار دارد . عملا هیچ کدام از پورت ها خاموش نیستند چون پورتی که در یک VLAN در وضعیت Block قرار دارد در VLAN دیگر در وضعیت Forwarding قرار دارد . برای درک بیشتر به شکل های زیر نگاه کنید :



در شکل صفحه قبل پروسه STP را در VLAN 1 مشاهده می کنید . با توجه به شکل متوجه می شوید که سوئیچ 3 در نقش Root Bridge کار می کند و بر روی پورت هایی که با VLAN 1 مشخص شده اند عمل Forwarding صورت می گیرد و پورت 0/1 سوئیچ 2 در وضعیت Block قرار دارد .



اما در شکل فوق پروسه STP را در VLAN 2 مشاهده میکنید . با توجه به شکل متوجه می شوید که سوئیچ 2 در نقش Root Bridge کار می کند و بر روی پورت هایی که با VLAN 2 مشخص شده اند عمل Forwarding صورت می گیرد و پورت 0/2 سوئیچ 3 در وضعیت Block قرار دارد .

Per – VLAN Spanning Tree Plus (PVST +) :

سیسکو نسخه ای دیگر از STP را به صورت اختصاصی معرفی کرده است که توانایی تعامل با CST را داشته و به نام PVST + نامیده می شود . این ورژن همان PVST است با این تفاوت که هم از پروتکل ISL و هم از پروتکل 802.1Q پشتیبانی می کند . در حقیقت پروتکل PVST + به عنوان یک مترجم ، پیام های CST را به PVST و بالعکس ترجمه می کند . در حال حاضر از این ورژن در سوئیچ ها به صورت پیش فرض استفاده می شود .

Protecting the Spanning Tree Protocol Topology

محافظت از ساختار شبکه در سطح لایه 2 :

سوئیچ ها به منظور اجرای STP از پیام های BPDU استفاده می کنند . در شبکه انتخاب سوئیچ Root Bridge و محل قرارگیری آن از اهمیت بالایی برخوردار بوده به همین خاطر انتخاب دستی Root Bridge در اختیار مدیران قرار داده شده است . تصور نمایید که سوئیچی ناشناخته به محلی از شبکه متصل شده و در پی داشتن پارامترهای مناسب تر سعی در کسب نقش Root Bridge از سوئیچ های فعلی را داشته باشد . در پاسخ به این مشکل سیسکو دو ویژگی امنیتی در روی سوئیچ های خود تعبیه کرده است که با عناوین Root Guard و BPDU Guard نامیده می شود .

ویژگی Root Guard :

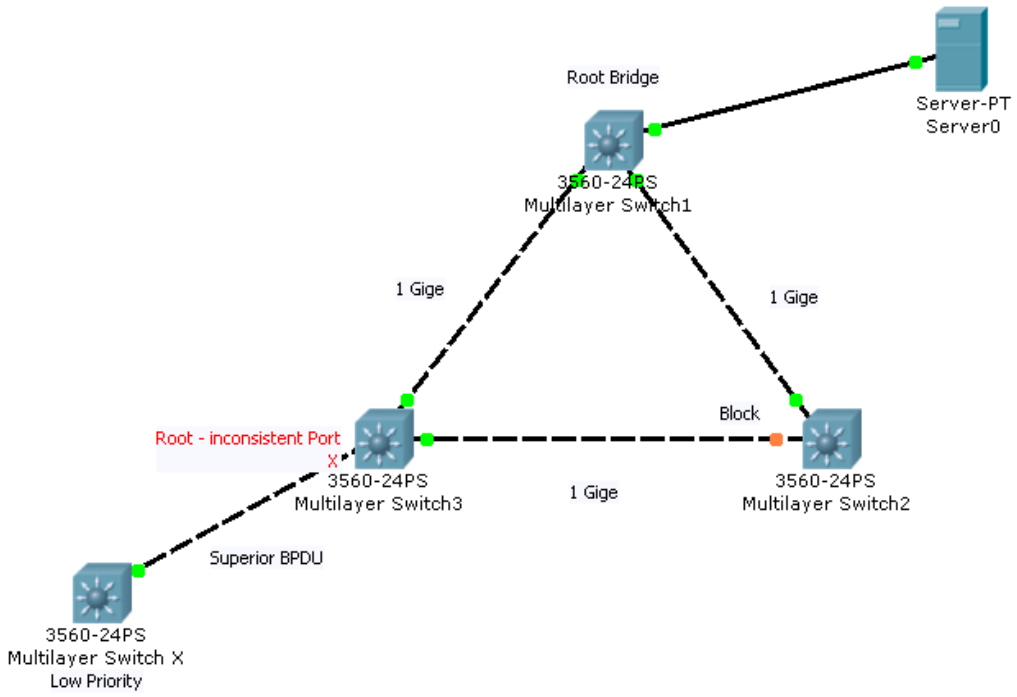
ویژگی Root Guard به منظور کنترل مکان قرارگیری سوئیچ Root Bridge در شبکه تهیه و ارائه شده است . بر حسب قانون تمامی سوئیچ ها از BID مربوط به سوئیچی که به عنوان Root Bridge انتخاب می شوند آگاهی دارند . بدین ترتیب در صورت فعال کردن این ویژگی بر روی یک پورت ، در صورتی که پورت مزبور یک پیام BPDU با شرایط بهتر دریافت نماید ، تغییری در تصور خود از سوئیچ Root Bridge اعمال نکرده و در حقیقت از بزگزیده شدن سوئیچ ارسال کننده این پیام به عنوان Root Bridge جلوگیری به عمل می آورد . در این شرایط پورت دریافت کننده این پیام در وضعیت Root – inconsistent قرار می گیرد و بنابراین انتقال هر نوع ترافیک کاربران از این پورت امکان پذیر نخواهد بود . پورتی که در این وضعیت قرار خواهد گرفت تنها قادر به دریافت پیام های BPDU خواهد بود .

برای فعال سازی ویژگی Root Guard می توان از دستور زیر استفاده کرد :

```
Switch ( config - if ) # Spanning – tree    guard root
```

به صورت پیش فرض ویژگی Root Guard بر روی تمامی پورت های سوئیچ غیرفعال می باشد .

به شکل زیر دقت کنید :



همانگونه که در شکل بالا مشاهده می کنید سوئیچ X با priority کمتر نسبت به سوئیچ Root Bridge می خواهد در نقش Root Bridge جدید ظاهر شود . ولی چون ویژگی Root Guard را بر روی تمام پورت های سوئیچ های شبکه که در حالت Access قرار دارند فعال کرده ایم به محض اینکه سوئیچ X که به یکی از پورت های سوئیچ 3 متصل است ، پیام Superior BPDU (یعنی پیام BPDU که نشان دهنده یک سوئیچ Root Bridge جدید باشد) را ارسال کند ، سوئیچ 3 آن پورتی را که این پیام را از آن دریافت کرده را در حالت Root – inconsistent قرار می دهد و بنابراین انتقال هر نوع ترافیک از این پورت امکان پذیر نخواهد بود .

با اجرای دستور زیر می توان لیستی از پورت هایی که در وضعیت Root – inconsistent قرار دارند را مشاهده کرد :

Switch # Show Spanning – tree inconsistentports

ویژگی BPDU Guard :

ویژگی BPDU Guard برای محافظت از پورت هایی که ویژگی Port Fast در روی آنها فعال شده ارائه گشته است . تصور کنید پورتی که ویژگی Port Fast در روی آن فعال شده است را به اشتباه به یک سوئیچ متصل کنیم . در این صورت احتمال بروز چرخه یا Loopهای لایه 2 در روی این پورت وجود دارد ، همچنین احتمال آن است که سوئیچ متصل شده به این پورت سعی در انتخاب خود به عنوان دستگاه Root Bridge جدید داشته باشد نیز وجود خواهد داشت .

اگر پورتی که ویژگی BPDU Guard در روی آن فعال شده است اقدام به دریافت هر نوع BPDU نماید وضعیت خود را به errdisable تغییر خواهد داد. در این حالت پورت مزبور تمامی ترافیک های انتقالی از خود را بلوکه کرده و در حقیقت در وضعیت Shut Down قرار می گیرد . برای برطرف کردن این وضعیت هم می توان پورت را به صورت دستی فعال نمود و یا روشی را پیکربندی نمود که بعد از سپری شدن مدت زمان معلومی این کار به صورت اتوماتیک انجام گیرد .

با دستور زیر ویژگی BPDU guard را بر روی همه اینترفیس هایی که ویژگی Port Fast نیز بر روی آنها فعال شده است ، فعال می کنیم :

Switch (config) # Spanning – tree Portfast bpduguard Default

با دستور زیر ویژگی BPDU guard را بر روی اینترفیس مورد نظر فعال و غیرفعال می کنیم :

Switch (config - if) # [No] Spanning – tree bpduguard enable

بروز اختلال در دریافت پیام های BPDU :

عملکرد پروتکل STP به ارسال و دریافت پیام های BPDU توسط سوئیچ ها وابسته است . بنابراین ارسال متناوب پیام های BPDU توسط سوئیچ Root Bridge برای زیر نظر گرفتن هر گونه تغییر در توپولوژی شبکه ضروری است . تصور کنید که یک سوئیچ از دریافت پیام های BPDU عاجز باشد . در شرایط عادی معمولا یک سوئیچ چنین پدیده ای را به عنوان بروز یک خطا در دستگاه های همسایه در نظر گرفته و بنابراین اقدام به اجرای دوباره الگوریتم STP خواهد کرد که در نتیجه آن ، پورت دیگری که هم اکنون در وضعیت بلوکه قرار دارد ، به عنوان Root Port برگزیده خواهد شد .

در شرایطی که دریافت نکردن پیام های BPDU توسط سوئیچ در نتیجه بروز ایرادی در کار دستگاه همسایه نبوده و یا هیچ تغییر خاصی در توپولوژی شبکه روی نداده باشد که باعث ممانعت از ارسال پیام های BPDU به سمت سوئیچ یاد شده گردد ، این تصور سوئیچ و عکس العمل آن برای اجرای دوباره پروتکل STP در هنگام دریافت نکردن پیام های BPDU باعث بروز چرخه یا Loop خواهد شد .

به منظور برطرف کردن چنین مشکلاتی ، سیسکو دو ویژگی دیگر را معرفی کرده است که عبارتند از :

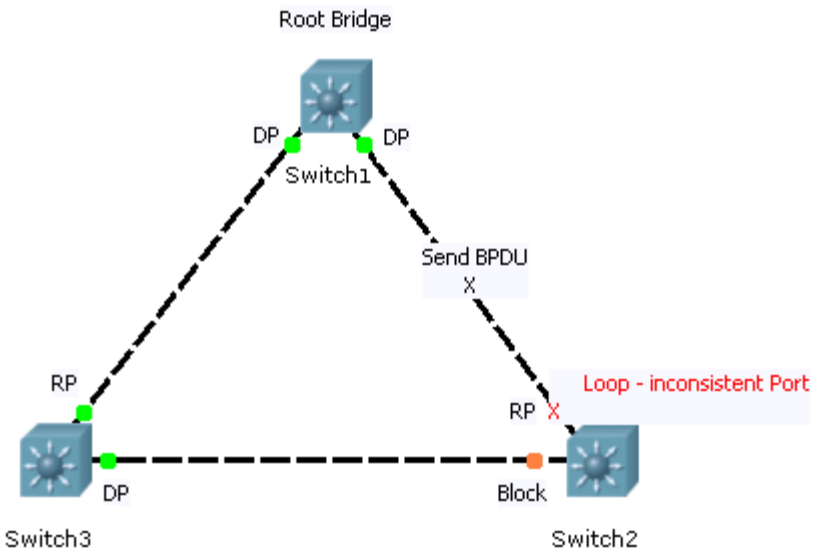
- Loop Guard
- Unidirectional Link Detection (UDLD)

ویژگی Loop Guard :

تصور داشته باشید که پورتی از سوئیچ در وضعیت Blocking قرار دارد و تا زمانی که پیام های BPDU را دریافت می کند ، در وضعیت Blocking باقی خواهد ماند . در صورتی که این پورت به هر دلیلی نتواند پیام های BPDU را دریافت کند ، اطلاعات مربوط به آخرین پیام BPDU دریافت شده توسط پورت مزبور تا سپری شدن زمان Max Age در حافظه دستگاه باقی می ماند . بعد از گذشت زمان Max Age ، سوئیچ اقدام به حذف این اطلاعات کرده و فرض را بر آن می گذارد که نیازی به قرار داشتن پورت یاد شده در وضعیت Blocking وجود ندارد . در این شرایط سوئیچ ، پورت مزبور را در پروسه عادی STP شرکت داده و آن را تا ورود به مرحله Forwarding ادامه می دهد و این کار باعث بروز Loop می شود .

برای جلوگیری از بروز این شرایط می توان از ویژگی Loop Guard استفاده کرد . این ویژگی وضعیت دریافت پیام های BPDU توسط پورت هایی که Designated نیستند را زیر نظر دارد . یعنی تا زمانی که این پورت ها ، پیام های BPDU را دریافت کنند ، اجازه در پیش گرفتن رفتار پیش فرض خود را خواهند داشت . اما در صورتی که پیام های BPDU را دریافت نکنند ، پورت مزبور را در وضعیت Loop – inconsistent قرار می دهد که در نتیجه این کار از بروز چرخه یا Loop جلوگیری به عمل می آورد . بعد از ورود یک پورت به وضعیت Loop – inconsistent ، اگر باز هم پورت مزبور قادر به دریافت پیام های BPDU باشد ، ویژگی Loop Guard آن را در پروسه عادی STP شرکت خواهد داد یعنی فعال سازی پورت مزبور به صورت اتوماتیک صورت می گیرد .

به شکل زیر توجه کنید :



همانگونه که در شکل بالا مشاهده می کنید اگر به هر دلیلی پیام های BPDU که سوئیچ 1 به سوئیچ 2 ارسال می کند دچار مشکل شده و سوئیچ 2 نتواند این پیام ها را دریافت کند ، آنگاه سوئیچ 2 بعد از طی شدن زمان Max Age آخرین پیام دریافتی ، فرض را بر آن میگذارد که دیگر نیازی به Block نگه داشتن پورت خود نمی باشد در نتیجه آن پورت را در وضعیت Forwarding قرار می دهد و این کار باعث بروز Loop

می شود . برای رفع این مشکل از ویژگی Loop Guard استفاده می کنیم که در این حالت پورت RP سوئیچ 2 که پیام های BPDU را دریافت نمی کند را در وضعیت Loop – inconsistent قرار می دهد و خاموش می کند تا با تغییر وضعیت پورت Block از بروز Loop جلوگیری کند .

به صورت پیش فرض این ویژگی در روی تمامی پورت های سوئیچ در وضعیت غیرفعال قرار دارد .

با دستور زیر ویژگی Loop Guard را بر روی همه پورت های سوئیچ فعال می کنیم :

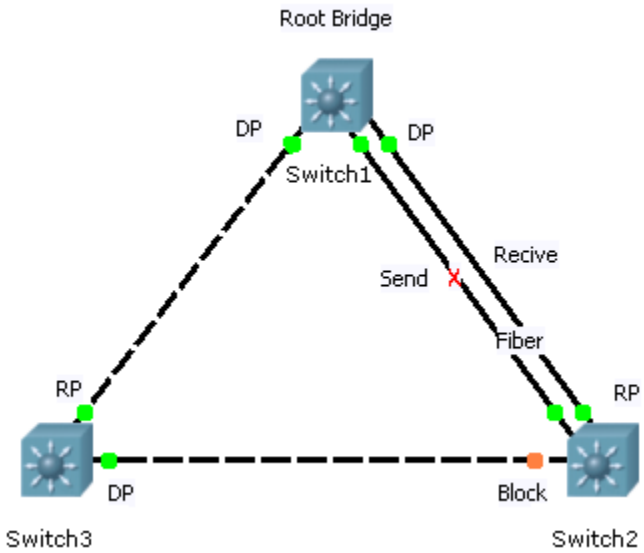
Switch (config) # Spanning – tree loopguard Default

با دستور زیر ویژگی Loop Guard را بر روی اینترفیس مورد نظر فعال و غیرفعال می کنیم :

Switch (config - if) # [No] Spanning – tree guard loop

ویژگی UDLD :

هدف از ایجاد اتصالات مابین دستگاه ها ، فراهم کردن امکان ارسال و دریافت اطلاعات مابین آنها در هر دو جهت می باشد . در صورتی که ایرادی در این اتصال فیزیکی روی دهد ، دستگاه ها آن را شناسایی کرده و قطع بودن ارتباط را گزارش می دهند . به شکل زیر دقت کنید :



با توجه به شکل صفحه قبل مشاهده می کنید که سوئیچ 1 و سوئیچ 2 به وسیله فیبر نوری با یکدیگر در ارتباط هستند. یکی از کابل ها برای Send و کابل دیگر برای Recive استفاده می شود و در این صورت مثلا اگر لینک send قطع شود و سوئیچ 2 پیام های BPDU را نتواند دریافت کند ولی از طریق لینک Recive با سوئیچ 1 در ارتباط است . بروز این پدیده باعث بروز مشکل در توپولوژی STP می شود ، زیرا یکی از دستگاه های شرکت کننده در ارتباط قادر به دریافت پیام های BPDU نخواهد بود و بروز این پدیده در نهایت

باعث ایجاد Loop می شود و همچنین دستگاه مزبور از اینکه تصور اشتباهی از پدیده مزبور داشته است ، مطلع نخواهد شد .

برای جلوگیری از بروز این مشکل می توان از یک ویژگی مخصوص سیسکو به نام UDLD استفاده کرد . این ویژگی پورت های دو سوی اتصال را بررسی می کند تا از اینکه هر دو انتها قادر به ارسال و دریافت اطلاعات می باشند اطمینان حاصل نماید . برای انجام این کار یک طرف اتصال به صورت متناوب اقدام به ارسال فریم های UDLD کرده و انتظار دریافت پاسخ آن از دستگاه موجود در سوی دیگر اتصال را خواهد داشت .

در صورتی که یک طرف اتصال قادر به ارسال پاسخ در قبال دریافت پیام های UDLD نبوده و یا به هر دلیل ، این پیام ها به دست دستگاه فرستنده نرسد ، اتصال مزبور به عنوان Unidirectional یا یکطرفه در نظر گرفته خواهد شد .

پیام های UDLD در فاصله زمانی ثابت توسط دستگاه ها ارسال می شوند که مقدار پیش فرض آن برابر با 15 ثانیه است . ویژگی UDLD بعد از سه بار ارسال متناوب پیام های UDLD و دریافت نکردن پاسخ ، اتصال مزبور را به عنوان Unidirectional شناسایی می نماید .

ویژگی UDLD دارای دو نوع عملکرد مختلف می باشد :

- **Normal mode** : در این شرایط بعد از شناسایی اتصالات Unidirectional یا یکطرفه ، عملکرد عادی پورت مزبور ادامه خواهد یافت فقط یک پیام syslog مبنی بر این واقعه نشان داده خواهد شد .
- **Aggressive mode** : در این وضعیت ویژگی UDLD سعی در برقراری دوباره اتصال خواهد داشت . بدین ترتیب که پیام های UDLD در هر ثانیه 1 بار و حداکثر 8 پیام به سمت دستگاه مقابل فرستاده می شود . در صورتی که هیچ کدام از این 8 پیام با پاسخی از دستگاه موجود در سوی دیگر اتصال روبرو نشود ، پورت متصل به این اتصال در وضعیت errdisable قرار می گیرد .

به صورت پیش فرض این ویژگی در روی تمامی پورت های سوئیچ در وضعیت غیرفعال قرار دارد .

با دستور زیر ویژگی UDLD را بر روی همه پورت های فیبرنوری سوئیچ فعال می کنیم :

Switch (config) # UDLD { Enable | Aggressive | Message Time seconds}

به منظور تعیین فاصله زمانی مربوط به ارسال پیام های UDLD از دستور Message Time استفاده می کنیم . مقدار این پارامتر باید در رنج 7 الی 90 ثانیه قرار داشته باشد . مقدار پیش فرض آن در برخی از سوئیچ ها برابر با 7 ثانیه و در برخی از مدل ها برابر با 15 ثانیه می باشد .

با دستور زیر ویژگی UDLD را بر روی اینترفیس مورد نظر فعال و غیرفعال می کنیم :

Switch (config - if) # UDLD { Enable | Aggressive | Disable }

نکته :پورت هایی که به وسیله ویژگی UDLD در وضعیت errdisable قرار گرفته ، برای فعال سازی دوباره آن باید دستورهای زیر را اجرا کنیم :

Switch (config - if) # Shutdown

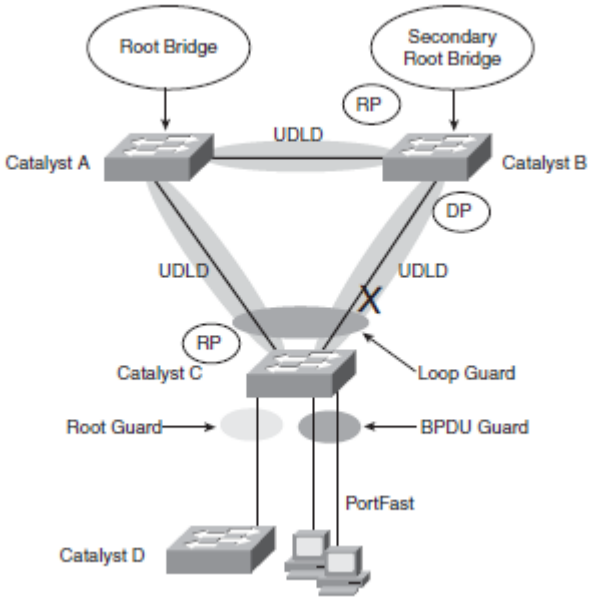
Switch (config - if) # No Shutdown

Switch # UDLD Reset

برای مشاهده وضعیت مربوط به ویژگی UDLD می توانید از دستور زیر استفاده کنید.

Switch # Show UDLD type mod/num

شکل زیر نشان می دهد که ویژگی های فوق در کجای سناریو استفاده می شود :



ویژگی BPDU Filtering :

به صورت پیش فرض پروتکل STP در روی تمامی پورت های یک سوئیچ فعال بوده و از بروز Loop یا چرخه های لایه 2 جلوگیری می کند . پیام های BPDU نیز از طریق تمامی پورت ها ، شامل پورت های Port Fast ارسال می گردند .

توصیه می شود که پروتکل STP را در روی تمامی پورت های سوئیچ در وضعیت فعال نگه دارید اما در شرایط خاص مثلا روی پورت هایی که Port Fast روی آنها فعال است می توان با جلوگیری از ارسال پیام های BPDU از طریق یک پورت ، پروتکل STP را در روی همان اینترفیس غیرفعال ساخت .

به صورت پیش فرض این ویژگی در روی تمامی پورت های سوئیچ در وضعیت غیرفعال قرار دارد .

با دستور زیر ویژگی BPDU Filtering را بر روی همه پورت های سوئیچ که Port Fast روی آنها فعال است ، فعال می کنیم :

```
Switch ( config ) # Spanning – Tree Portfast  bpdufilter  Default
```

نکته :

در صورتی که هیچ کدام از پورت های دستگاه به صورت Port Fast پیکربندی نشده باشد ، اجرای دستور فوق بی نتیجه خواهد بود .

با دستور زیر ویژگی BPDU Filtering را بر روی اینترفیس مورد نظر فعال و غیرفعال می کنیم :

```
Switch ( config - if ) # Spanning – Tree   bpdufilter { Enable | Disable }
```

Advanced Spanning Tree Protocol

نسخه های جدیدتر پروتکل STP

پروتکل RSTP :

پروتکل قدیمی STP با استاندارد 802.1D دارای مشکلاتی از جمله طولانی بودن زمان Convarge می باشد ، که این زمان در پروتکل STP با استاندارد 802.1D معادل 30 تا 50 ثانیه می باشد .

بر همین اساس سازمان استانداردسازی IEEE ورژن جدیدی از پروتکل STP را ارائه دادند که به نام Rapid Spanning Tree Protocol (RSTP) نامیده شده است . پروتکل RSTP از استانداردIEEE 802.1W از الگوریتم STA که برگرفته از عبارت Algorithm Spanning Tree می باشد استفاده خواهد کرد .

نقش پورت ها در RSTP :

- Root Port : هر کدام از سوئیچ ها یکی از پورت های خود را که مسیری مناسبتر برای دسترسی به دستگاه Root Bridge را نشان می دهد به عنوان Root Port بر می گزینند.
- Designated Port : در صورتی که بیش از یک سوئیچ به یک سگمنت لایه 2 متصل شده باشد ، تنها یکی از این سوئیچ ها برای ارسال اطلاعات مربوط به آن سگمنت به سمت قسمت های دیگر شبکه و سگمنت های دیگر مورد استفاده قرار خواهد گرفت . این پورت به نام Designated Port نامیده می شود .
- Alternate Port : علاوه بر Root Port ، هر کدام از سوئیچ ها یک پورت دیگر خود را که بعد از Root Port به عنوان مناسبترین مسیر برای دسترسی به دستگاه Root Bridge است را به عنوان Alternate Port برمی گزینند .
- Backup Port :به عنوان جایگزینی برای Designated Port می باشد . در صورتی که پورت Designated Port مربوط به یک سگمنت لایه 2 و یا اتصال متصل به آن معیوب گردد ، Backup Port بلافاصله جایگزین آن خواهد شد .

وضعیت پورت ها در RSTP :

- ⊡ Discarding : در این وضعیت تمامی پیام های دریافتی بلوکه می شوند . همچنین هیچ آدرس MAC جدیدی در داخل جدول CAM دستگاه به ثبت نمی رسد . در حقیقت این وضعیت برابر با ترکیب Blocking ، Listening و Disable در پروتکل STP می باشد .
- ⊡ Learning : در این وضعیت پیام های دریافتی بررسی شده و در صورت نیاز آدرس MAC آنها در جدول CAM به ثبت می رسد . اما هیچ گونه ترافیکی از طریق پورت ها انتقال نخواهد یافت .
- ⊡ Forwarding : در این مرحله پورت ها اقدام به دریافت و بررسی پیام های ورودی کرده و در صورت نیاز اقدام به ثبت آنها در جدول CAM می کنند . همچنین در این وضعیت دیتای کاربران نیز به مقاصد خود هدایت می شوند .

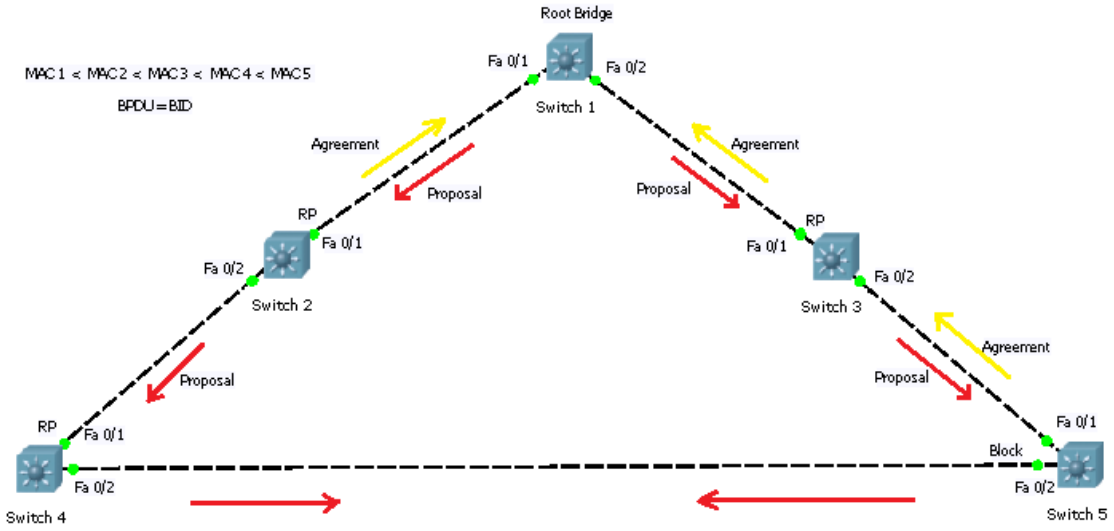
انواع پورت در RSTP :

- Edge Port : اشاره به پورتی در روی سوئیچ دارد که در نقاط مرزی شبکه قرار داشته و بنابراین به کامپیوترها متصل می باشند . در پروتکل STP ، پورت های Port Fast این وظیفه را بر عهده داشتند . در پروتکل RSTP نیز می توان پورت هایی که به دستگاه هایی فاقد توانایی ایجاد Loop متصل می باشند را به عنوان پورت Edge یا Port Fast نامید .
- Root Port : اشاره به پورتی روی سوئیچ دارد که به عنوان بهترین مسیر دسترسی به دستگاه Root Bridge می باشند . هر کدام از سوئیچ ها تنها مجاز به انتخاب یک پورت خود به عنوان Root Port هستند .

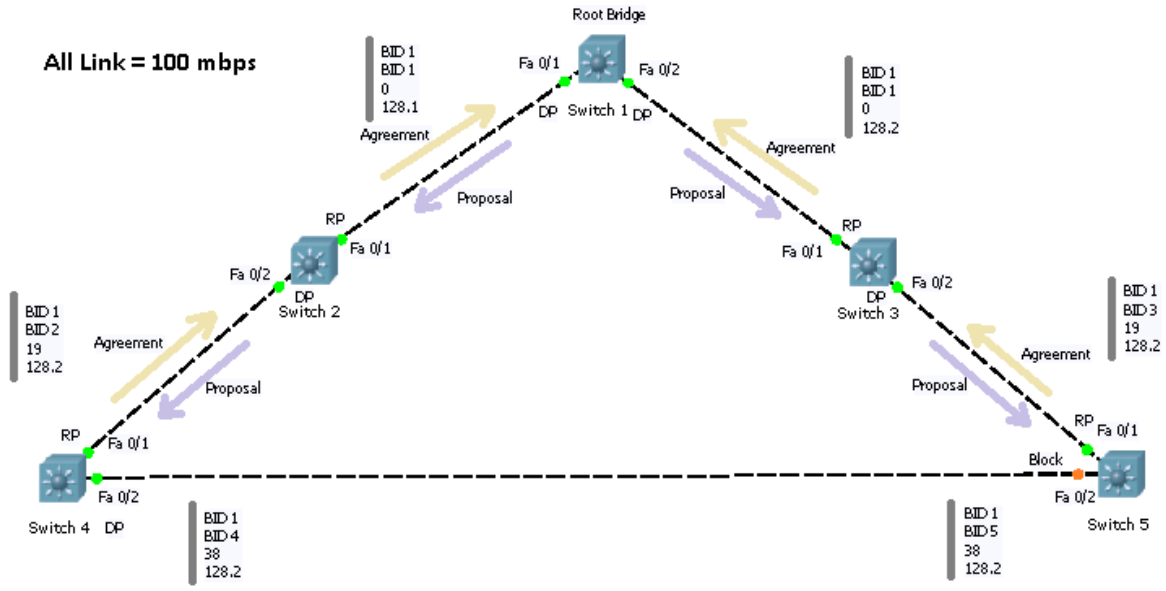
- Point – to – Point : اشاره به پورتی در روی سوئیچ دارد که به یک سوئیچ دیگر متصل شده و به عنوان Designated Port انتخاب گردد . در این شرایط برخلاف استفاده از تایمرهای مختلف ، سوئیچ های همسایه اقدام به انجام یک گفتگو (Handshake) با یکدیگر خواهند کرد تا وضعیت نهایی پورت های یاد شده تعیین گردد . در این شرایط پیام های BPDU در قالب پیام های Proposal و Agreement مابین دستگاه های مرتبط توسط این پورت ها منتقل می شود . بدین ترتیب که یکی از سوئیچ ها اقدام به برگزیدن یک پورت خود به عنوان Designated می کند که در صورت موافقت سوئیچ همسایه ، پورت مزبور به صورت قطعی به عنوان Designated انتخاب خواهد شد .

برای درک بیشتر به اشکال زیر توجه کنید :

شکل نخست سناریو :



شکل نهایی سناریو :

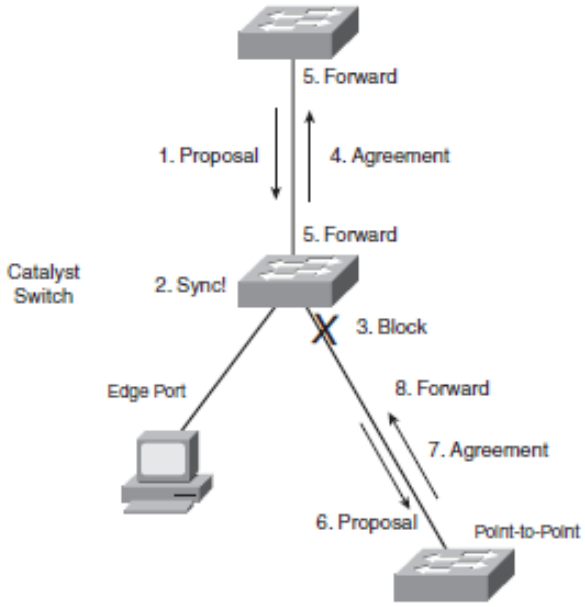


پروسه Synchronization :

یک سوئیچ برای انجام Synchronization باید وضعیت همه پورت های خود را تعیین نماید . پورت های غیر Edge در ابتدا در وضعیت Discarding قرار می گیرند . با آغاز مبادله پیام های BPDU ، امکان شناسایی سوئیچ Root Bridge وجود دارد . در صورتی که یک پورت اقدام به دریافت پیام های Superior BPDU کند ، پورت مزبور به عنوان Root Port برگزیده خواهد شد .

در حقیقت هر یک از سوئیچ ها برای تعیین وضعیت پورت های خود اقدام به انجام یک handshake به نام Agreement – Proposal Handshake می نمایند . تمامی سوئیچ ها فرض را بر آن می گذارند که دارای پورت Designated در روی خود می باشند که در نتیجه آن ، پیام Proposal را از طریق خود ارسال خواهند کرد .

زمانی که یک سوئیچ پیام Proposal دریافت می کند ، مراحل زیر طبق شکل زیر روی خواهد داد :



- مرحله اول : در صورتی که سوئیچ ارسال کننده پیام Proposal دارای Superior BPDU باشد ، سوئیچ دریافت کننده متوجه خواهد شد که دستگاه همسایه دارای پورت Designated در روی خود بوده و بنابراین پورت دریافت کننده BPDU در روی خود را در نقش Root Port قرار می دهد .
- مرحله دوم : اما سوئیچ قبل از انجام هر کاری باید ارتباط خود را با قسمت های دیگر توپولوژی قطع کرده و بنابراین خود را با شرایط موجود وفق دهد . یعنی می توان گفت سوئیچ باید خود را با توپولوژی موجود Synchronize نماید .
- مرحله سوم : تمامی پورت های غیر Edge سوئیچ بلافاصله در وضعیت Discarding قرار می گیرند تا امکان بروز چرخه یا Loop وجود نداشته باشد .

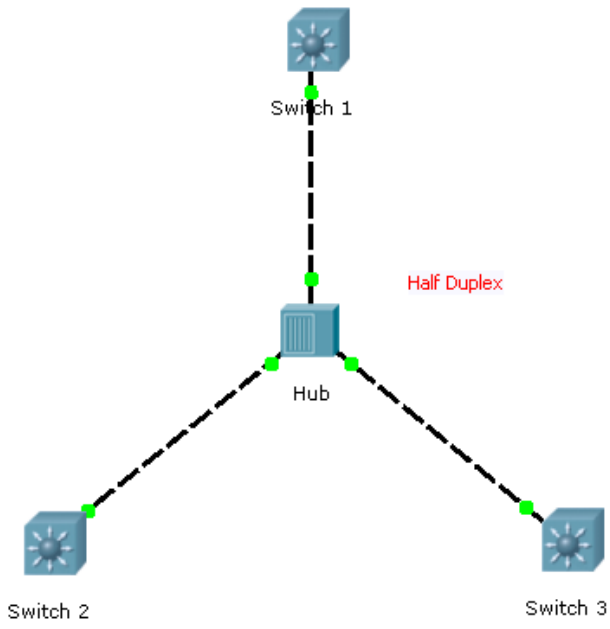
- مرحله چهارم : یک پیام Agreement برای سوئیچ ارسال کننده Proposal فرستاده شده و بدین ترتیب سوئیچ Local موافقت خود را با انتخاب شدن پورت ارسال کننده Proposal در نقش DP اعلام می دارد .
- مرحله پنجم : پورت Root بلافاصله در وضعیت Forwarding قرار می گیرد . در این صورت امکان تبادل اطلاعات مابین سوئیچ ارسال کننده Proposal و دستگاه Local وجود خواهد داشت .
- مرحله ششم : در این مرحله تمامی پورت های غیر Edge دستگاه Local که در وضعیت Discarding قرار گرفته اند نیز به نوبه خود اقدام به ارسال پیام Proposal به همسایه خود خواهد کرد .
- مرحله هفتم : سوئیچ های دریافت کننده پیام Proposal نیز همین پروسه را تکرار کرده و در نتیجه آن ، پیام Agreement خود را برای دستگاه فرستنده پیام Proposal می فرستند .
- مرحله هشتم : پورت ارسال کننده Agreement بلافاصله در وضعیت Forwarding قرار می گیرد .

برای اینکه نوع پورت یا Link Type را در روی یک پورت برابر با Edge Port قرار دهید ، از دستور زیر استفاده می کنیم :

Switch (config – if) # Spanning – Tree Portfast

RSTP فقط روی پورت هایی که نوع آنها برابر با Point – to – Point باشد کار می کند . همچنین به صورت پیش فرض در صورتی که یک پورت در وضعیت Full Duplex عمل نماید ، نوع پورت یا Link Type در روی آن برابر با Point – to – Point قرار خواهد گرفت . اما در صورت نیاز این کار را می توان به صورت دستی نیز انجام داد .

برای نمونه به شکل زیر توجه کنید :



همانطور که مشاهده می کنید در این حالت پورت های بین سوئیچ در حالت Half Duplex قرار دارند و برای اینکه بتوانیم پروتکل RSTP را پیکربندی کنیم باید به صورت دستی نوع پورت یا Link Type در روی آنها را برابر با Point – to – Point قرار دهیم .

با دستور زیر می توانیم به صورت دستی نوع پورت یا Link Type در روی پورت را برابر با Point – to – Point قرار دهیم :

Switch (config – if)# Spanning – Tree Link-Type Point – to – Point

Max – age time در پروتکل RSTP برابر با 6 ثانیه می باشد و سرعت همگرایی بهبود بخشیده شده است . به ازای هر VLAN یک نمونه RSTP وجود دارد و به همین خاطر هنوز مشکل ترافیکی که به علت ارسال بسته های BPDU در هر VLAN حل نشده است.

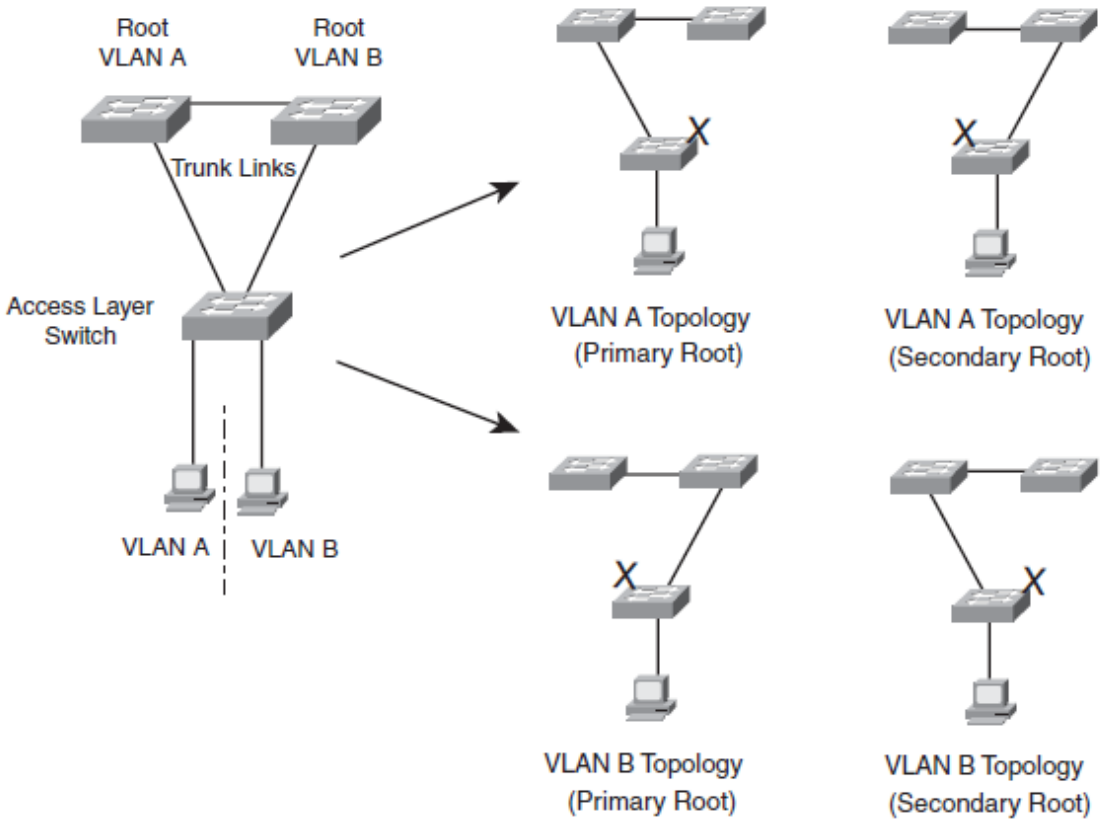
دستور فعال کردن Rapid PVST+ به صورت زیر است :

Switch (config – if)# Spanning – Tree Mode Rapid – PVST

پروتکل (MST) Multiple Spanning Tree :

پروتکل MST با استاندارد IEEE 802.1S به منظور کاهش تعداد پروسه های STP و حل مشکل ترافیک ایجاد شده در VLANها ، به تعدادی که واقعا مورد نیاز توپولوژی می باشد طراحی و معرفی شده است . بدین ترتیب مدیر شبکه می تواند صرفنظر از تعداد VLAN و تنها با تکیه بر تعداد توپولوژی ممکن ، اقدام به تعیین دستی تعداد پروسه STP مورد نیاز نماید .

ایده ای که در پشت این پروتکل وجود دارد آن است که بتوان تعدادی از VLANها را مجبور به استفاده از یک پروسه STP نمود . با توجه به شکل زیر ، به دلیل وجود دو مسیر ممکن از سوئیچ لایه Access به سوئیچ های بالادستی ، وجود تنها دو پروسه STP کافی خواهد بود . در این شرایط پروسه اول STP می تواند از اتصال uplink اول استفاده کرده و اتصال دوم را بلوکه کند و پروسه STP دوم نیز می تواند به صورت برعکس عمل نماید .



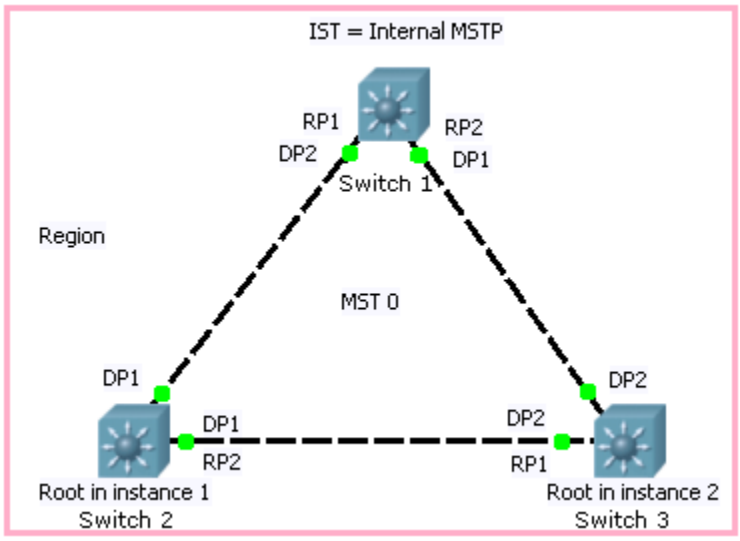
در نتیجه در شکل فوق می توان VLAN A را مجبور به استفاده از پروسه STP اول و VLAN B را مجبور به استفاده از پروسه دوم STP نمود .

MST Region :

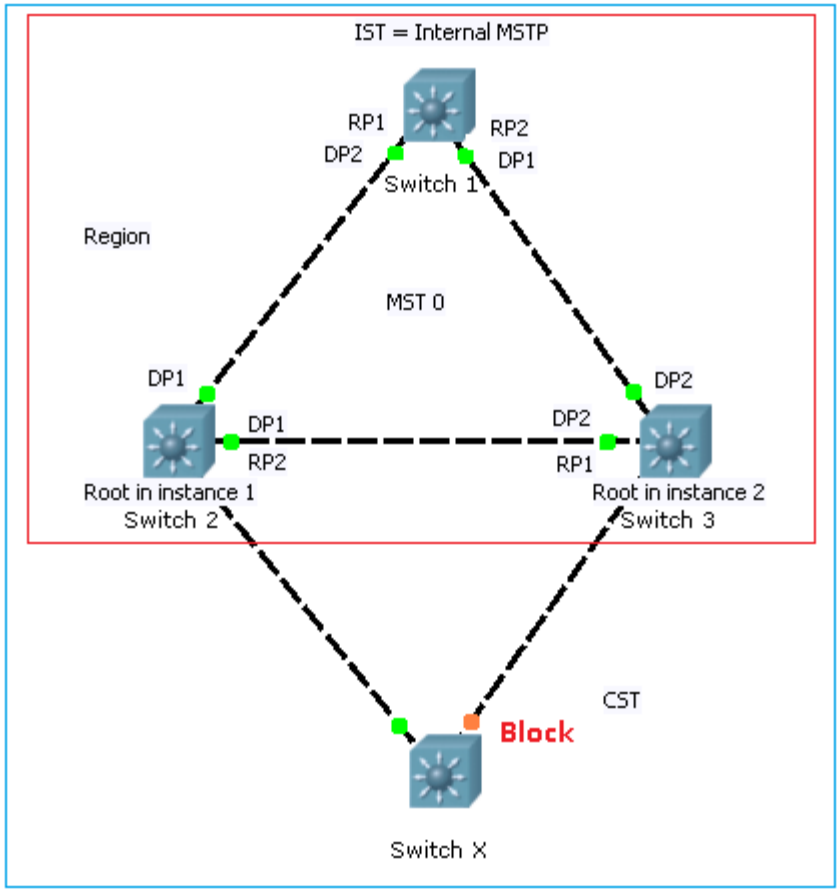
سوئیچ هایی که برای استفاده از MST پیکربندی شده اند ، از اینکه سوئیچ های همسایه خود از کدام نسخه STP استفاده می کنند نیز آگاهی خواهند داشت . این کار با قرار دادن سوئیچ های مختلف در داخل یک MST Region میسر می شود . دستگاه های واقع در داخل یک MST Region از پارامترهای خاص یکسانی استفاده می کنند . این پارامترها که مقدار آنها باید در روی سوئیچ های واقع در داخل یک MST Region یکسان باشد عبارتند از :

- MST Configuration Name : حداکثر برابر با 32 کاراکتر
- MST Configuration Revision Number : برابر با 0 الی 65535
- MST Instance – to – VLAN Mapping Table : حداکثر برابر با 4096

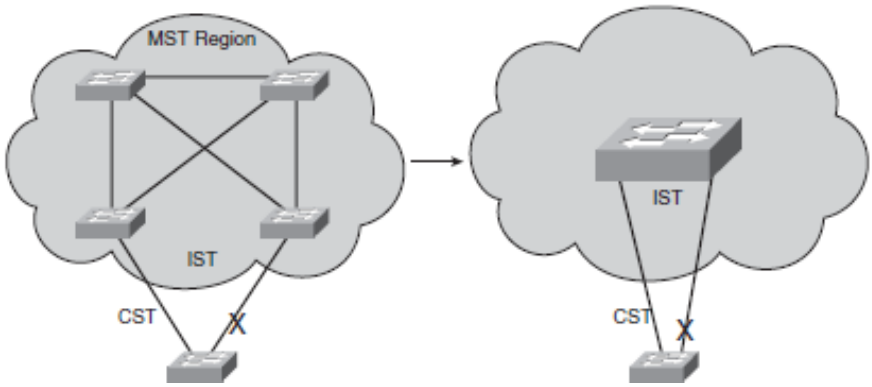
در صورتی که دو سوئیچ از مقدار مساوی به ازای پارامترهای فوق برخوردار باشند ، عضوی از یک MST Region واحد و در غیر این صورت ، متعلق به دو MST Region متفاوت خواهند بود . شکل صفحه بعد نشان می دهد که سوئیچ ها در یک MST Region قرار دارند و دو نمونه MST در این سناریو وجود دارد :



همانطور که در بالا مشاهده می کنید تمام سوئیچ هایی که در یک MST Region قرار دارند در واقع به عنوان یک سوئیچ مجازی بزرگ عمل کرده و با دیگر قسمت های شبکه که خارج از MST Region می باشند ، در یک پروسه CST واحد شرکت می نماید . در این شرایط پروتکل CST که در کل توپولوژی اجرا می شود ، نیازی به آگاهی از اینکه در داخل MST Region چه نوع پروتکلی مورد استفاده قرار گرفته نداشته و کل MST Region را به عنوان یک سوئیچ مجازی بزرگ در نظر می گیرد که شبیه به دیگر سوئیچ های خارج از MST Region قصد شرکت در الگوریتم STP دارد . شکل زیر ایده فوق را نشان می دهد :



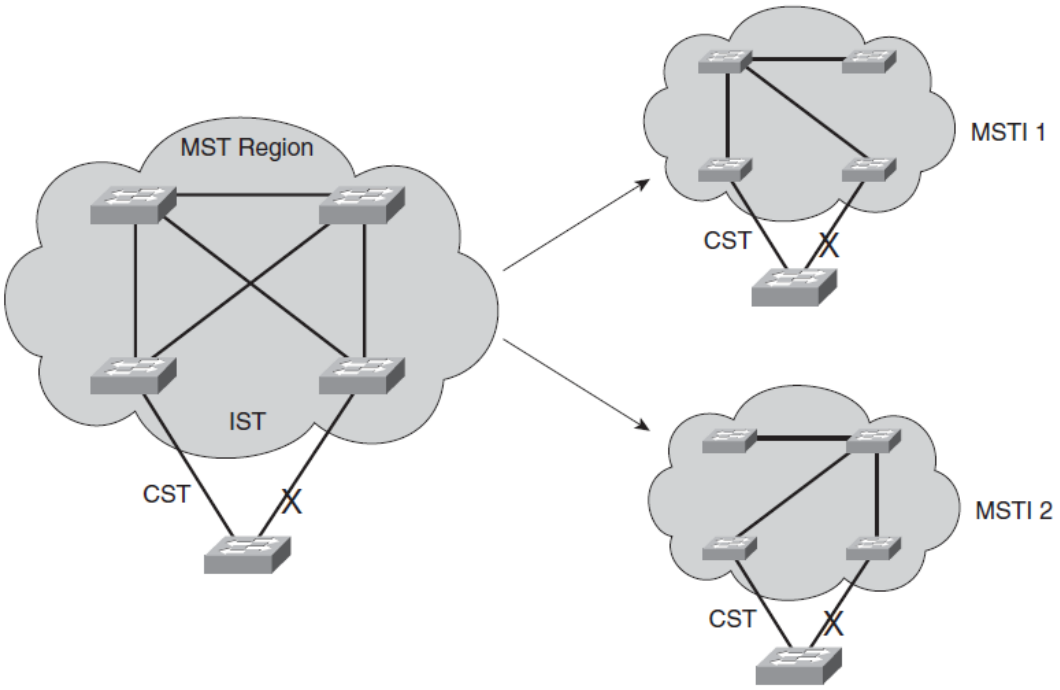
در شکل صفحه قبل یک MST Region را مشاهده می کنید که شامل سوئیچ های مختلف و اتصالات مابین آنهاست . همچنین سوئیچ X در خارج از این MST Region نیز وجود دارد که توسط اتصالات 802.1Q با MST Region در تماس بوده و بنابراین از CST بهره می گیرد و کل سوئیچ های داخل MST Region را به عنوان یک سوئیچ مجازی بزرگ در نظر می گیرد .مانند شکل زیر :



پروسه های MST یا MST instances :

همانطور که گفته شد با استفاده از پروتکل MST می توان گروهی از VLANها را مجبور به استفاده از یک پروسه یا instance واحد STP نمود . در داخل یک MST Region می توان پروسه های مختلفی از MST را تعریف کرد که به هر کدام از این پروسه ها یک MST instance اطلاق می شود . دستگاه های سیسکو حداکثر توانایی پشتیبانی از 16 عدد MST instance در داخل هر MST Region را دارند .

شکل زیر نشان می دهد که چگونه می توان در داخل یک MST Region اقدام به تعریف MST instanceهای مختلف نمود :



توجه داشته باشید که در داخل MST Region هم اکنون سه پروسه مختلف از STP در حال اجرا هستند که عبارتنداز :

- MSTI 1
- MSTI 2
- IST

پیکربندی مربوط به MST :

برای پیکربندی MST در روی یک سوئیچ مراحل زیر را باید انجام بدیم :

Step 1. Enable MST on the switch:

```
Switch(config)# spanning-tree mode mst
```

Step 2. Enter the MST configuration mode:

```
Switch(config)# spanning-tree mst configuration
```

Step 3. Assign a region configuration name (up to 32 characters):

```
Switch(config-mst)# name name
```

Step 4. Assign a region configuration revision number (0 to 65,535):

```
Switch(config-mst)# revision version
```

Step 5. Map VLANs to an MST instance:

```
Switch(config-mst)# instance instance-id vlan vlan-list
```

Step 6. Show the pending changes you have made:

```
Switch(config-mst)# show pending
```

Step 7. Exit the MST configuration mode; commit the changes to the active MST region configuration:

```
Switch(config-mst)# exit
```

دستور مشاهده فعال یا غیر فعال بودن پروتکل MST بر روی یک سوئیچ :

Switch # Show Spanning – Tree MST

در جدول زیر به ترتیب دستورات << انتخاب سوئیچ Root و اختصاص یک Priority بر روی سوئیچ و تعیین مقدار Cost مربوط به یک پورت و تعیین مقدار Priority مربوط به یک پورت و تعیین مقدار MST timerها >> نوشته شده است :

MST Configuration Commands

Task	Command Syntax
Set root bridge (macro).	Switch(config)# spanning-tree mst *instance-id* root {primary | secondary} [diameter *diameter*]
Set bridge priority.	Switch(config)# spanning-tree mst *instance-id* priority *bridge-priority*
Set port cost.	Switch(config)# spanning-tree mst *instance-id* cost *cost*
Set port priority.	Switch(config)# spanning-tree mst *instance-id* port-priority *port-priority*
Set STP timers.	Switch(config)# spanning-tree mst hello-time *seconds* Switch(config)# spanning-tree mst forward-time *seconds* Switch(config)# spanning-tree mst max-age *seconds*

مثال :

Switch (config) # Spanning – Tree Mode MST

Switch (config) # Spanning – Tree MST Configuration

Switch (config – mst) # Instance 1 VLAN 1 – 4

Switch (config – mst) # Name CCNP

Switch (config – mst) # Revision 4

Switch (config) # Spanning – Tree MST 1 Root Primary

Multilayer Switching

Inter VLAN Routing

به منظور فراهم ساختن امکانی برای انتقال ترافیک مربوط به یک VLAN به یک VLAN دیگر باید از یک دستگاه لایه 3 استفاده کنید . چندین سال قبل این وظیفه برعهده روترها بود که از طریق اتصالات فیزیکی یا مجازی اقدام به هدایت ترافیک مربوط به یک VLAN به سمت VLANهای دیگر می نمود . به صورت کلی این پروسه با عنوان Inter VLAN Routing خوانده می شود .

سوئیچ های Multilayer می توانند هم در سطح لایه 2 عمل کرده و عملیات Switching را انجام دهند و هم در سطح لایه 3 فعالیت کرده و پروسه Routing را بر عهده دارد . همانند روترها می توان یک آدرس IP بر روی پورت های یک سوئیچ Multilayer تخصیص داد . همچنین در صورت ایجاد یک پورت مجازی در روی دستگاه می توان آدرس IP مورد نظر را بر روی آن اختصاص داد . این نوع اینترفیس های مجازی به عنوان Switched Virtual Interface (SVI) نامیده می شوند . به یاد داشته باشید که این آدرس به عنوان Default Gateway تمامی دستگاه های متصل به آن اینترفیس یا SVI قرار خواهد گرفت .

وضعیت و عملکرد یک پورت وابسته به دستور Switchport است . برای مشاهده اطلاعات مورد نیاز در این باره می توانید از دستور زیر استفاده کرد :

Switch # Show Interface type mod/num Switchport

در صورتی که در خروجی این دستور عبارت Enabled را مشاهده کنید نشان دهنده فعال بودن Switchport بوده و بنابراین پورت در سطح لایه 2 عمل می کند . اما وجود عبارت Disabled بیانگر آن است که پورت مزبور در سطح لایه 3 فعالیت می کند .

در زیر مثالی از اجرای این دستور را مشاهده می کنید :

```
Switch# show interface gigabitethernet 0/1 switchport
Name: Gi0/1
Switchport: Disabled
Switch#
```

در صورتی که یک پورت سوئیچ در سطح لایه 3 فعالیت می کند ، می توانید با استفاده از دستور زیر آن را در سطح لایه 2 قرار داد :

Switch (config) # Interface type mod/num

Switch (config – if) # Switchport

در صورتی که یک پورت سوئیچ در سطح لایه 2 فعالیت می کند ، می توانید با استفاده از دستور زیر آن را در سطح لایه 3 قرار داد :

Switch (config) # Interface type mod/num

Switch (config – if) # No Switchport

با اجرا کردن دستور فوق بر روی پورت می توانیم یک آدرس IP به آن اختصاص دهیم و عمل Routing را پیکربندی کنیم .

سوئیچ های Multilayer به صورت پیش فرض عمل Routing را انجام نمی دهند باید دستور زیر را روی سوئیچ های Multilayer اجرا کنیم تا به عنوان یک Router عمل کنند و پروسه Routing را انجام دهند :

Switch (config) # IP Routing

بعد از دستور فوق می توانیم Inter VLAN Routing را پیکربندی کنیم :

Switch (config) # Interface VLAN vlan – id

Switch (config – if) # IP Address ip – address wildcard mask

مثال :

```
Switch ( config ) # IP Routing
Switch ( config ) # Interface  VLAN  100
Switch ( config – if ) # IP  Address  192.168.1.1 255.255.255.0
Switch ( config – if ) # No Shutdown
Switch ( config ) # Interface  Vlan  200
Switch ( config – if ) # IP Address  192.168.2.2  255.255.255.0
Switch ( config – if ) # No Shutdown
Switch ( config ) # Interface  Vlan  300
Switch ( config – if ) # IP Address  192.168.3.2  255.255.255.0
Switch ( config – if ) # No Shutdown
```

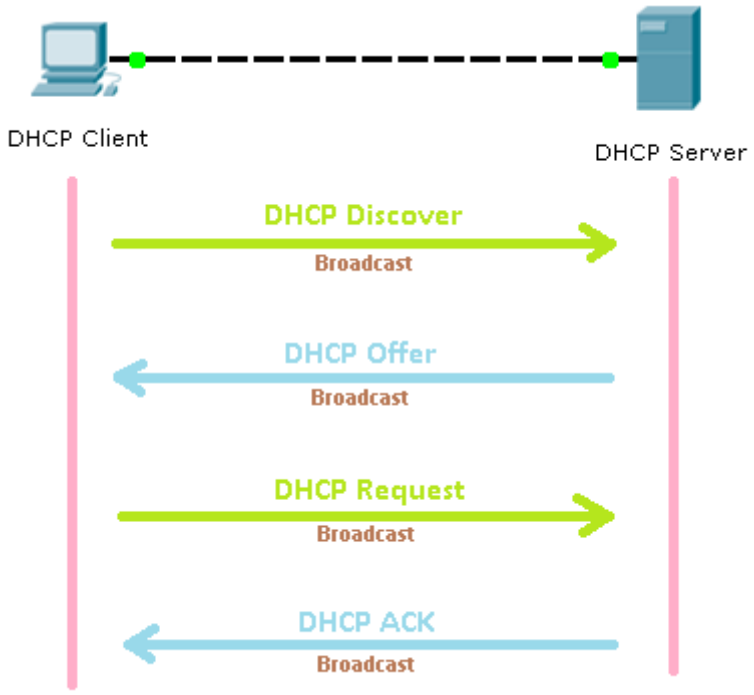
Dynamic Host Configuration Protocol (DHCP)

استفاده از DHCP در سوئیچ های Multilayer :

پروتکل DHCP امکان تخصیص اتوماتیک اطلاعات از جمله آدرس IP و ماسک و آدرس Default Gateway بر روی کلاینت هایی که از این پروتکل پشتیبانی می کنند را فراهم ساخته است . این پروتکل در استاندارد RFC 2131 تعریف شده و بر اساس یک مدل Client / Server عمل می کند . بدین ترتیب دستگاه هایی که نیاز به دریافت اطلاعات دارند به نام DHCP Client و دستگاه های ارائه دهنده این اطلاعات نیز با عنوان DHCP Server نامیده می شوند .

تصور نمایید کلاینتی که دارای هیچ نوع آدرس IP در روی خود نمی باشد را به یک شبکه متصل کرده ایم . در این صورت دستگاه مزبور باید اطلاعات مورد نیاز خود را از DHCP Server دریافت نماید .

به شکل زیر دقت کنید :



در حالت کلی مراحل انجام گرفته در شکل صفحه قبل به صورت زیر خواهد بود :

- **مرحله اول** : DHCP Client یک پیام DHCP Discover را به صورت Broadcast در شبکه منتشر خواهد کرد . این پیام به منظور شناسایی سرورهای DHCP ارسال شده و آدرس MAC مربوط به DHCP Client نیز در آن گنجانده می شود .
- **مرحله دوم** : در صورتی که یک DHCP Server در شبکه موجود باشد ، این پیام را دریافت کرده و در قبال آن یک پیام DHCP Offer می فرستد . این پیام شامل اطلاعاتی نظیر آدرس IP و ماسک و آدرس Default Gateway و موارد دیگر خواهد بود . آدرس IP مربوط به DHCP Server نیز در داخل پیام مزبور گنجانده می شود تا هویت دستگاه ارسال کننده پیام مشخص گردد . به علت اینکه DHCP Client فعلا دارای آدرس IP برای خود نمی باشد ، این پیام نیز در قالب Broadcast ارسال خواهد شد .
- **مرحله سوم** : بعد از آنکه DHCP Client پیام مزبور را دریافت نموده و تمایل به استفاده از اطلاعات مورد نظر داشته باشد پیام DHCP Request را خواهد فرستاد . به علت آنکه DHCP Client مزبور هنوز به صورت رسمی شروع به استفاده از آدرس فوق نکرده است ، بنابراین این پیام نیز به صورت Broadcast فرستاده می شود .

مرحله چهارم : DHCP Server بعد از دریافت پیام DHCP Request از Client اقدام به ارسال پاسخ خود به نام DHCP ACK کرده و با این کار با درخواست Client مبنی بر استفاده از اطلاعات یاد شده موافقت می کند . این پیام نیز به صورت Broadcast فرستاده می شود .

نکته :

فقط روی سوئیچ های Multilayer می توانیم DHCP Server را راه اندازی کنیم .

پیکربندی DHCP Server در روی سوئیچ Multilayer :

configure a DHCP server:

```
Switch(config)# ip dhcp excluded-address start-ip end-ip
Switch(config)# ip dhcp pool pool-name
Switch(config-dhcp)# network ip-address subnet-mask
Switch(config-dhcp)# default-router ip-address [ip-address2] [ip-address3] ...
Switch(config-dhcp)# lease {infinite | {days [hours [minutes]]}}
Switch(config-dhcp)# exit
```

مثال :

Switch (config) # IP DHCP Excluded – Address 192.168.1.1 192.168.1.10
Switch (config) # IP DHCP Pool Cisco
Switch (config – dhcp) # Network 192.168.1.0 255.255.255.0
Switch (config – dhcp) # Default – Router 192.168.1.1
Switch (config – dhcp) # DNS – Server 192.168.1.2
Switch (config – dhcp) # Lease infinite
Switch (config – dhcp) # Exit

بعد از اجرا کردن دستورات فوق VLAN مورد نظر را روشن یا فعال می کنیم و به آن آدرس Default Gateway را بدهیم .
دستور اول برای اینکه آدرس هایی را که نمی خواهیم به Clientها اختصاص بدهد را مشخص می کنیم .
دستور دوم برای تعریف یک مخزن از یک Range آدرس IP می باشد . برای هر Range از آدرس IPهای موجود در شبکه باید یک مخزن یا Pool تعریف کنیم تا هر VLAN یک مخزن برای آدرس دهی داشته باشد .

برای مشاهده آدرس های تخصیص داده شده توسط سرور DHCP می توانید از دستور زیر استفاده کنید :

```
Switch # Show  IP  DHCP  Binding
```

پیکربندی DHCP Relay :

همانطور که گفته شد ، روش صحیح در پیکربندی DHCP آن است که سرور DHCP در داخل یک VLAN قرار داشته باشد . اما به منظور پشتیبانی از Clientهای واقع در VLANهای دیگر باید سوئیچ Multilayer را به عنوان DHCP Relay پیکربندی کنید تا درخواست های دریافت شده از Clientهای واقع در VLANهای دیگر توسط سوئیچ دریافت و به سمت سرور DHCP ارسال گردد .

در ابتدا نیاز به پیکربندی یک SVI برای هر یک از VLANها دارید . این SVI به عنوان Default Gateway مربوط به همان VLAN خواهد بود و باید در نقش DHCP Relay عمل نماید .

سپس با دستور IP Helper – Address ، آدرس دقیق سرور DHCP را بعد از آن مشخص می کنیم :

```
Switch ( config – if ) # IP  Helper – Address  ip – dhcp
```

مثال :

```
Switch ( config ) # Interface  VLAN  4

Switch ( config – if ) # IP  Address  192.168.1.1  255.255.255.0

Switch ( config – if ) # IP Helper – Address  192.168.199.4

Switch ( config – if ) # Exit
```

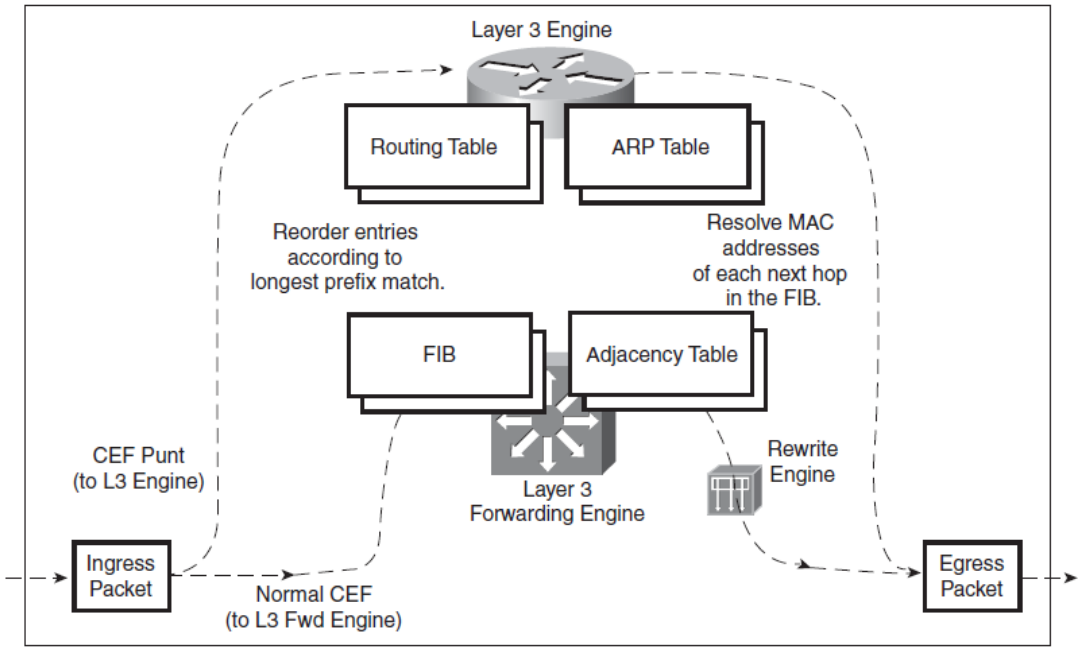
در مثال فوق آدرس 192.168.199.4 مربوط به آدرس DHCP Server شبکه می باشد .

پروسه CEF در سوئیچ های Multilayer :

سویئچ های سیسکو با تکیه بر متدهای مختلفی می توانند ترافیک را در سطح لایه 3 و 4 بررسی کرده و آنها را به مقاصد خود هدایت کنند . نسل فعلی سوئیچ های Multilayer کاتالیست از یک متد خاص به نام Cisco Express Forwarding (CEF) برای این کار استفاده می کنند . این ویژگی در ابتدا برای استفاده در روی روترها و به منظور هدایت هرچه سریعتر اطلاعات ارائه گشت . اما مدتی بعد سیسکو آن را برای استفاده در روی سوئیچ های Multilayer خود نیز گسترش داد .

همانطور که در شکل زیر مشاهده می کنید ، یک سوئیچ Multilayer مبتنی بر CEF دارای دو قسمت مجزا به شرح زیر می باشد :

- **Layer – 3 Engin** : عملیات Routing را بر حسب جدول Routing انجام می دهد .
- **Layer – 3 Forwarding Engin** : این قسمت با دریافت اطلاعات از Layer – 3 Engin عملیات هدایت اطلاعات به سمت مقاصد خود را انجام می دهد .



Packet Flow Through a CEF-Based Multilayer Switch

در این روش از چند مرحله زیر برای بالا بردن سرعت استفاده می شود :

- **مرحله اول** : اطلاعات مربوط به جدول (FIB) Forwarding Information Base کاملا از روی اطلاعات جدول Routing ایجاد می شود . جدول FIB به صورت سخت افزاری در روی سوئیچ قرار دارد و چون تنها یک کار خاص را انجام می دهد سرعت پردازش را بالا میبرد. مثلا اگر یک پاکت وارد سوئیچ شود قسمت Dst IP آن پاکت در جدول FIB همزمان با تمام رکوردهای داخل این جدول مقایسه می شود و آن را در کمترین زمان پیدا کرده و به طرف مقصد Forward می کند .

مرحله دوم : در این مرحله تمام اطلاعات داخل جدول Arp table که MAC دستگاه های متصل به روتر یا سوئیچ Multilayer در آن ذخیره شده را در یک قسمت سخت افزاری دیگر به نام Adjacency Table دانلود می کند و برای مدتی در جدول خود نگه می دارد تا اگر FIB Table مسیر خروجی را پیدا کرد ، از قبل آدرس MAC مقصد خروجی را برای آن بسته آماده نگه داشته تا سرعت ارسال بالا رود .

مرحله سوم : وقتی که اینترفیس از طریق FIB Table و آدرس MAC مقصد از طریق Adjacency Table پیدا و تعیین شد ، چون مقادیر Src MAC و Dst MAC و TTL و FCS و Check sum بسته مورد نظر تغییر خواهد کرد باید چسباندن و کندن اطلاعات نیز سریع انجام شود که به وسیله یک سخت افزار دیگر به نام Packet Rewrite Engine این کارها در اسرع وقت انجام می پذیرد .

برای مشاهده محتویات جدول FIB می توانید از دستور زیر استفاده کند :

Switch # Show IP CEF [VLAN vlan – id] [type mod/num] [Detail]

مثال زیر اطلاعات مربوط به VLAN 101 را در داخل جدول FIB نشان می دهد :

Displaying FIB Table Entries for a Specified VLAN

```
Switch# show ip cef vlan 101
Prefix              Next Hop            Interface
10.1.1.0/24         attached            Vlan101
10.1.1.2/32         10.1.1.2            Vlan101
10.1.1.3/32         10.1.1.3            Vlan101
Switch#
```

برای مشاهده محتویات جدول Adjacency می توانید از دستور زیر استفاده کند :

Switch # Show Adjacency [VLAN vlan – id] [type mod/num] [Summary | Detail]

مثال زیر جدول Adjacency را نشان می دهد :

Displaying the Total Number of Known Adjacencies

```
Switch# show adjacency summary
Adjacency Table has 106 adjacencies
  Table epoch: 0 (106 entries at this epoch)
  Interface                 Adjacency Count
  Vlan99                    21
  Vlan101                   3
  Vlan102                   1
  Vlan103                   47
  Vlan104                   7
  Vlan105                   27
Switch#
```

برای مشاهده موارد CEF Glean از دستور زیر استفاده می کنیم :

Switch # Show IP CEF Adjacency Glean

مثال :

Displaying Adjacencies in the CEF Glean State

```
Switch# show ip cef adjacency glean
Prefix              Next Hop            Interface
10.1.1.2/32         attached            Vlan101
127.0.0.0/8         attached            EOBC0/0
[output omitted]
Switch# show ip arp 10.1.1.2
Switch# show ip cef 10.1.1.2 255.255.255.255 detail
10.1.1.2/32, version 688, epoch 0, attached, connected
0 packets, 0 bytes
  via Vlan101, 0 dependencies
    valid glean adjacency
Switch#
```

رکوردهایی که هنوز آدرس MAC آنها پیدا نشده را Glean می گویند .

دستور مشاهده بسته هایی که CEF آنها را Drop کرده است :

Switch # Show CEF Drop

مثال :

```
Switch# show cef drop
CEF Drop Statistics
Slot  Encap_fail  Unresolved Unsupported     No_route      No_adj   ChkSum_Err
RP       8799327           1       45827      5089667          32            0
Switch#
```

دستور مشاهده تعداد و دلیل Forward نشدن بسته ها :

Switch # Show CEF Not – CEF – Switched

مثال :

```
Switch# show cef not-cef-switched
CEF Packets passed on to next switching layer
Slot  No_adj  No_encap  Unsupp'ted  Redirect  Receive  Options  Access  Frag
RP    3579706        0           0         0 41258564        0       0     0
Switch#
```

انواع متدهای CEF :

Acceleraterd CEF (aCEF) :

در این حالت فقط Routeهایی که بیشتر مورد استفاده قرار می گیرند در CEFها دانلود می شود و بقیه Routeهای دیگر که کمتر مورد استفاده قرار می گیرند در قسمت نرم افزاری یعنی Routing Table ذخیره می شوند . در این حالت به جای استفاده از یک دستگاه Forwarding Engine متمرکز ، از چندین دستگاه Forwarding Engine استفاده می شود .

Distributed CEF (dCEF) :

در این حالت همه Routeهای که داخل Routing Table در CEFها دانلود می شود و پردازش می کند . در این حالت نیز به جای استفاده از یک دستگاه Forwarding Engine متمرکز ، از چندین دستگاه Forwarding Engine استفاده می شود .

در بعضی از سوئیچ ها می توان CEF را غیرفعال کرد . این کار را با دستور زیر بر روی اینترفیس مورد نظر انجام می دهیم :

در برخی از سوئیچ ها از این دستور استفاده می کنیم :

Switch (config – if) # No IP CEF

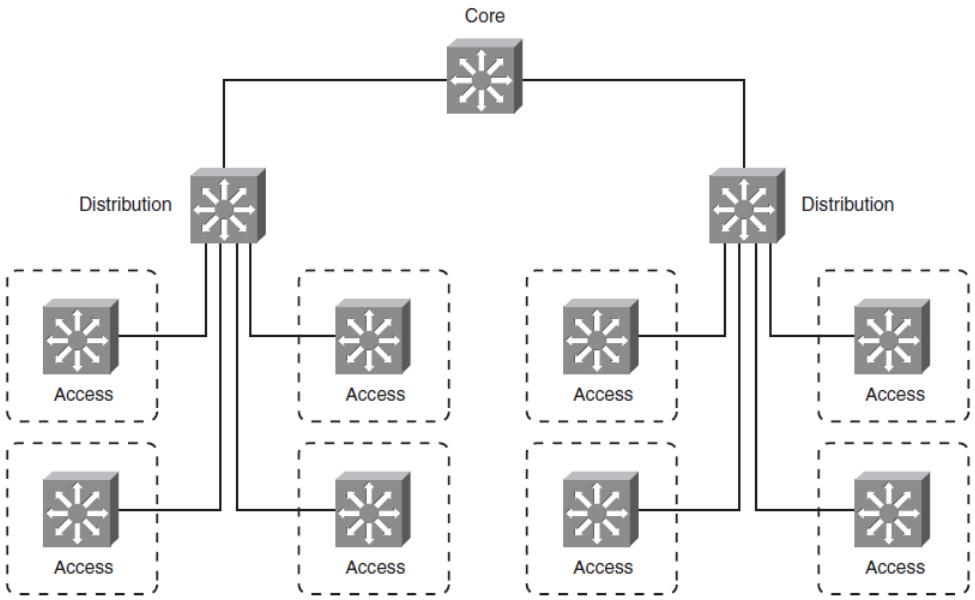
در برخی از سوئیچ ها از این دستور استفاده می کنیم :

Switch (config – if) # No IP Route – Cashe CEF

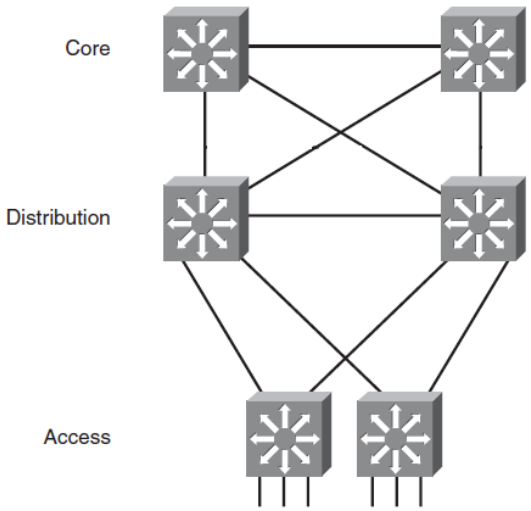
Enterprise Compus Network Design

طراحی شبکه :

در گذشته شبکه ها را به صورت شکل زیر طراحی و پیاده سازی می کردند . البته سرورها به سوئیچ لایه Core متصل بودند . ولی با مشاهده این شکل متوجه خواهید شد اگر به هر دلیلی یکی از لینک های مابین سوئیچ های لایه Distribution و سوئیچ Core قطع شود ارتباط بین دو شبکه موجود قطع خواهد شد و این ناشی از طراحی بد شبکه است .



برای رفع اینگونه مشکل ها بهتر است که طراحی شبکه ها را طوری انجام دهیم که در لایه Core از دو سوئیچ استفاده شود و ارتباط بین آنها و سوئیچ های لایه Distribution را به صورت Full Mesh برقرار کنیم . به شکل زیر توجه کنید :



همانطور که در شکل صفحه قبل مشاهده می کنید اگر لینکی دچار مشکل شود ارتباط سوئیچ های لایه های مختلف شبکه با هم قطع نمی شود از یک لینک دیگر استفاده می شود .

بر اساس مکان قرارگیری سرویس های شبکه و فاصله آنها از کاربران انتهایی ، جریانات ترافیکی مربوط به شبکه ها را می توان در سه گروه عمده قرار داد که به شرح زیر است :

- **Traffic Local** : این نوع ترافیک در لایه Access رد و بدل می شود چون در یک VLAN یا دارای یک Subnet هستند .
- **Traffic Remote** : این نوع ترافیک در بین چند VLAN حرکت می کند یعنی از لایه Access به لایه Distribution رفته و برمی گردد.
- **Traffic Enterprice** : ترافیکی که در کل شبکه حرکت می کند یعنی از لایه Access به لایه Distribution رفته و و از آنجا به لایه Core رفته و برمیگردد .

سوئیچ های لایه **Access** :

این لایه معمولا در تماس مستقیم با کاربران انتهایی قرار دارد . سوئیچ های لایه Access ارتباط کاربران در سطح لایه 2 را فراهم می سازد یعنی Forwarding را بر اساس آدرس MAC انجام می دهند . سوئیچ های لایه Access دارای ویژگی های زیر هستند :

- دارا بودن تعداد پورت زیاد
- هزینه کم برای هر پورت
- در اختیار داشتن پورت های پرسرعت برای دسترسی به لایه های بالاتر (Uplink Fast)
- قابلیت پشتیبانی از VLANها ، QoS و فیلتراسیون ترافیک
- توانایی بهره گیری از چندین اتصال Uplink برای در اختیار دادن ویژگی Redundancy

سوئیچ های لایه **Distribution** :

این لایه وظیفه برقراری ارتباط مابین لایه Access و لایه Core را در یک شبکه Campus بر عهده دارد . لایه مزبور معمولا به عنوان مرز یک شبکه در سطح لایه 3 به شمار می رود که انتقال اطلاعات مابین VLANها را امکان پذیر می سازد . سوئیچ های لایه Distribution دارای ویژگی های زیر هستند :

- توانایی دریافت ترافیک از چندین سوئیچ لایه Access
- قابلیت هدایت سریع پیام ها در سطح لایه 3
- قابلیت پشتیبانی از VLANها ، QoS و فیلتراسیون ترافیک و امنیت شبکه
- توانایی بهره گیری از اتصالات پرسرعت به سمت لایه های Access و Core

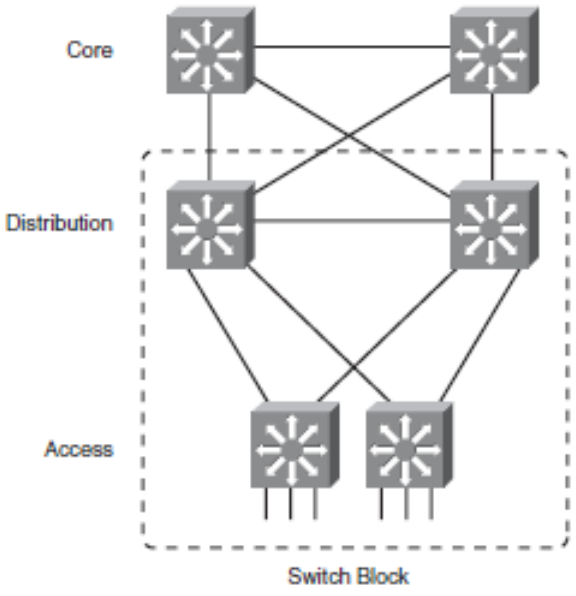
سوئیچ های لایه **Core** :

این لایه به عنوان ستون فقرات و یا Backbone شبکه نامیده می شود . این لایه وظیفه برقراری ارتباط مابین سوئیچ های لایه Distribution را برعهده دارد . دستگاه های این لایه باید هدایت ترافیک در بالاترین سرعت ممکن را داشته باشد . به دلیل آنکه دستگاه های واقع در این لایه باعث انتقال حجم عظیمی از ترافیک می شود نباید روی این سوئیچ ها Policy و Security اعمال کنیم چون باعث کاهش سرعت شبکه می شود . سوئیچ های لایه Core دارای ویژگی های زیر هستند :

- توانایی هدایت بسیار سریع پیام ها در سطح لایه 3
- قابلیت پشتیبانی از ویژگی پیشرفته QoS

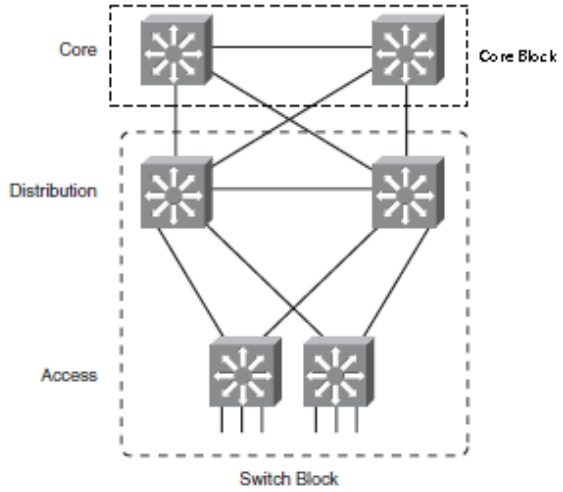
Switch Block :

به مجموعه ای از سوئیچ های لایه Access و لایه Distribution که در یک منطقه قرار دارند (یک یا دو سوئیچ در هر لایه) گفته می شود .



Core Block :

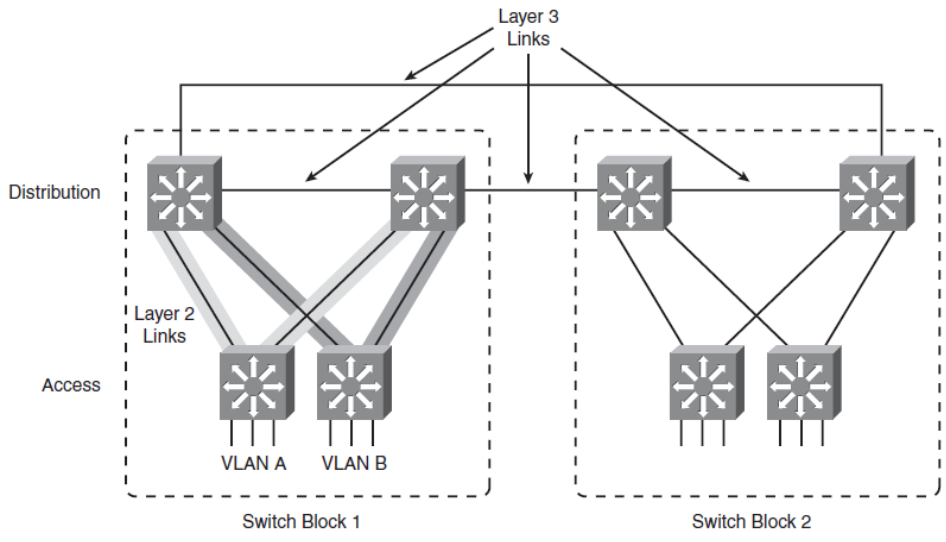
به یک یا دو سوئیچ لایه Core که در یک مجموعه قرار دارند گفته می شود .



Collapsed Core :

در این نوع از طراحی از سوئیچ های لایه Core استفاده نمی شود که اینگونه طراحی بیشتر در سازمان هایی پیاده سازی می شود که یا هزینه ایجاد لایه Core مستقل را نداشته یا به دلیل برخورداری از Userهای کم نیازی به انجام آن ندارند . در چنین شرایطی وظایف لایه Core را نیز سوئیچ های لایه Distribution انجام می دهند .

شکل زیر نشان دهنده سناریوی سادهای از این نوع طراحی می باشد :

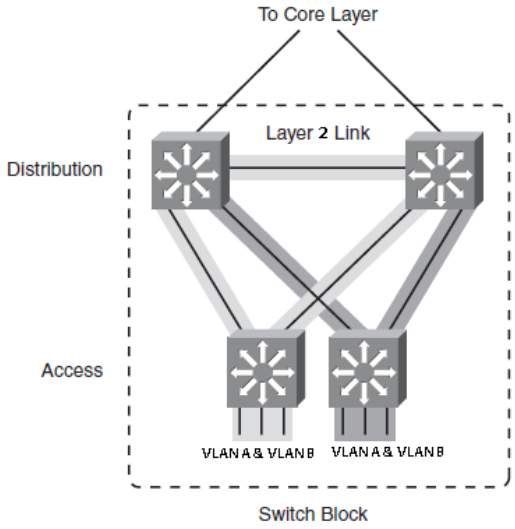


Collapsed Core Design

همانطور که در شکل فوق مشاهده می کنید ارتباطات مابین سوئیچ های لایه Distribution از نوع لایه 3 خواهند بود و ارتباطات مابین سوئیچ های لایه Distribution و لایه Access از نوع لایه 2 خواهند بود .

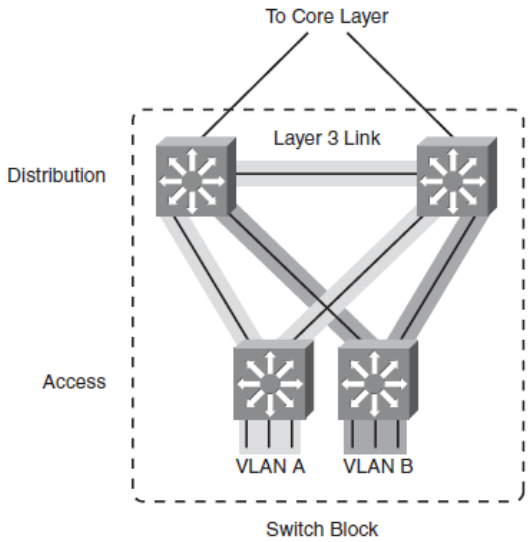
انواع ساختار در Switch Block :

حالت اول : به شکل زیر توجه کنید :



همانطور که در سناریوی فوق مشاهده می کنید در این حالت باید از پروتکل RSTP استفاده کرد و لینک مابین دو سوئیچ لایه Distribution باید از نوع لایه 2 باشد تا بین PCهایی که در یک VLAN قرار دارند در دو طرف ، ارتباط برقرار باشد .

حالت دوم : به شکل زیر توجه کنید :

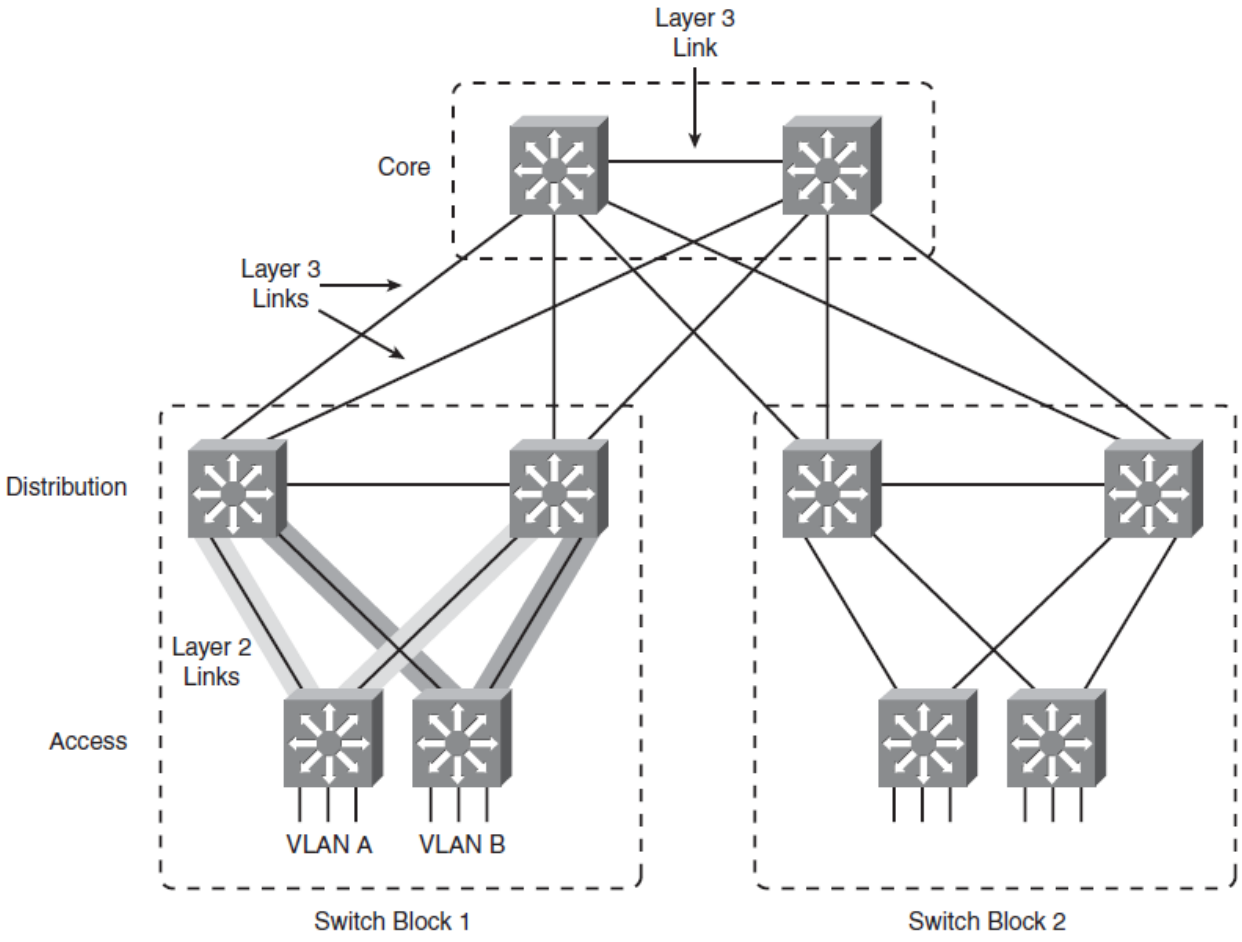


همانطور که در سناریوی فوق مشاهده می کنید در این حالت باید از پروتکل RPVST استفاده کرد و لینک مابین دو سوئیچ لایه Distribution باید از نوع لایه 3 باشد . در این حالت می توانیم از ویژگی Inter VLAN Routing استفاده کنیم . این نوع طراحی از بهترین روش های طراحی می باشد .

یکی از سوئیچ های لایه Distribution را در نقش Root Bridge و سوئیچ دیگر این لایه را در نقش Root Secondary قرار می دهیم .

Dual Core Design :

یک لایه Core به صورت Dual Core طراحی شده است که وظیفه برقراری ارتباط مابین دو یا چند Switch Block را بر عهده داشته و ویژگی Redundancy را نیز در اختیار ما قرار می دهد . شکل زیر نشان دهنده سناریوی سادهای از این نوع طراحی می باشد . مشاهده می فرمایید که لایه Core به عنوان ماژول جداگانه ای باعث برقراری ارتباط مابین Switch Blockها شده است :



Dual Core Design

در سناریوهای Dual Core از دو سوئیچ یکسان برای در اختیار داشتن Redundancy استفاده می شود . در چنین شرایطی هر کدام از سوئیچ های Distribution مربوط به هر Switch Block با استفاده از دو اتصال مجزا به هر یک از سوئیچ های Core متصل میگردند . همچنین سوئیچ های لایه Core نیز با استفاده از یک اتصال لایه 3 با یکدیگر در ارتباط خواهند بود .

Layer 3 High Availability

: Router Redundancy

سوئیچ های Multilayer می توانند به عنوان Default Gateway عمل کرده و باعث برقراری ارتباط کلاینت های واقع در یک شبکه یا یک VLAN با محیط خارج بشود . در این صورت کلاینت ها ترافیک خود به مقصد محیط خارج را به سمت آدرس IP مربوط به SVI و یا پورت لایه 3 در روی سوئیچ خواهد فرستاد . به منظور افزایش Availability در شبکه باید روشی را به کار برد تا بروز ایرادی در کار یک Default Gateway باعث قطعی ارتباط یک شبکه یا VLAN با محیط خارج نگردد . برای رسیدن به این هدف از سه پروتکل زیر که First – Hop Redundancy Protocol (FHRP) نامیده می شوند استفاده می کنیم :

: Hot Standby Router Protocol (HSRP)

HSRP یک پروتکل اختصاصی شرکت سیسکو می باشد که بر روی روترها و سوئیچ های Multilayer شرکت سیسکو پشتیبانی می شود . در این پروتکل تعدادی روتر در یک گروه مجازی قرار خواهند گرفت . در این حالت یکی از روترها که Priority بالاتری دارد به عنوان روتر فعال انتخاب خواهد شد که به Active Router معروف می باشد . در داخل این گروه یک روتر دیگر به عنوان پشتیبان Active Router انتخاب خواهد شد و این روتر در وضعیت Standby قرار خواهد داشت .

سایر روترهای داخل گروه HSRP در وضعیت Listen HSRP قرار دارند و این روترها به صورت مرتب با ارسال پیام های HSRP Hello وضعیت فعالیت Active Router را تحت نظر خواهند گرفت .

کلیه روترهای داخل یک HSRP Group دارای یک IP Address و MAC Address مجازی خواهند بود که این آدرس به عنوان Default Gateway برای کلیه کامپیوترهای یک Subnet در نظر گرفته خواهد شد . هر گروه HSRP با یک شماره شناسایی خواهد شد که این شماره عددی است بین 0 تا 255 که به صورت اختیاری تعیین خواهد شد .

در یک گروه HSRP روتری که بالاترین Priority را داشته باشد به عنوان Active Router تعیین خواهد شد . Priority عددی بین 0 تا 255 خواهد بود که به صورت پیش فرض این مقدار بر روی روترهای شرکت سیسکو 100 تعیین شده است . در صورتی که روترهای داخل یک گروه HSRP دارای Priority مساوی باشند روتری که دارای بالاترین IP Address می باشد به عنوان Active Router در آن گروه تعیین خواهد شد .

روترها در پروتکل HSRP دارای وضعیت های مختلفی به شرح زیر می باشند :

- **Initial :** در این حالت هنوز پروسه HSRP بر روی Router آغاز نشده است .
- **Learn :** در این حالت Router از Virtual IP Address آگاهی نخواهد داشت و منتظر دریافت این اطلاعات از Active Router خواهد بود .
- **Listen :** در این حالت Router از IP Address و MAC Address مربوط به Virtual Router آگاهی خواهد داشت و این روتر یک Active Router یا یک Standby Router نمی باشد .
- **Speak :** در این حالت Router اقدام به ارسال پیام های HSRP Hello خواهد کرد و در پروسه انتخاب Active Router شرکت خواهد کرد .
- **Standby :** در این حالت روتر به عنوان یک Standby Router انتخاب خواهد شد و اقدام به مانیتور کردن Active Router خواهد کرد و در صورتی که Active Router دچار مشکل شود این روتر نقش Active Router را برعهده خواهد گرفت .
- **Active :** در این حالت روتر تبدیل به Active Router خواهد شد و این روتر تنها روتری می باشد که داخل گروه HSRP قادر به Forward کردن اطلاعات می باشد .

نکته :

چون سوئیچ های Multilayer نیز کار روتر را انجام می دهند و پروسه Routing را انجام می دهند پس از این به بعد اگر از کلمه روتر استفاده شد به غیر از روترهای اصلی منظور سوئیچ های Multilayer نیز می باشد .

نکته مهم :

کلیه روترهای داخل گروه HSRP باید در یک Subnet یا عضو یک VLAN باشند .

نکته :

همانطور که می دانید هر کدام از پورت های Ethernet روتر دارای یک آدرس MAC برای خود هستند که این آدرس MAC متناظر با آدرس IP آن اینترفیس قرار خواهد گرفت . به همین ترتیب روتر مجازی HSRP نیز دارای یک آدرس MAC برای خود است که در فرمت 0000.0c07.acXX خواهد بود . به جای علامت های XX شماره مربوط به گروه HSRP در مبنای 16 قرار داده می شود . برای نمونه آدرس MAC مربوط به HSRP Group 1 برابر با 0000.0c07.ac01 و آدرس MAC مربوط به HSRP Group 16 برابر با 0000.0c07.ac10 خواهد بود .

HSRP Timer :

در پروتکل HSRP روتر Active پیام های Hello را به سمت روتر Standby ارسال می کند در حقیقت روتر Standby با تحت در نظر گرفتن این پیام های Hello فعالیت روتر Active را مانیتور خواهد کرد . در پروتکل HSRP به صورت پیش فرض پیام های Hello هر 3 ثانیه یکبار از روتر Active به سمت روتر Standby ارسال خواهد شد . پیام های Hello به سمت یک مقصد Multicast که برابر با 224.0.0.2 است ارسال می شوند . در این بین پورت UDP 1985 مورد استفاده قرار خواهد گرفت .

زمان دیگری در پروتکل HSRP به نام Hold time مورد استفاده قرار خواهد گرفت که این زمان به صورت پیش فرض 10 ثانیه است . در صورتی که روتر Standby مدت زمان 10 ثانیه پیام Hello را از روتر Active دریافت نکند فرض بر از کار افتادن روتر Active گذاشته خواهد شد و روتر Standby تبدیل به روتر Active خواهد شد .

دستورات پیکربندی HSRP :

Switch (config) # Interface type mod/num

Switch (config – if) # Standby group Priority priority

دستور تعریف IP مجازی :

Switch (config – if) # Standby group IP virtual – IP

دستور تغییر زمان های HSRP :

Switch (config – if) # Standby group Timers [msec] Hello [msec] Holdtime

این کار باید بر روی تمام روترهای عضو یک گروه HSRP انجام پذیرد .

دستور انتخاب روتر Active به صورت دستی :

Switch (config – if) # Standby group Preempt [Delay [Minimum seconds] [Reload seconds]]

دستور Authentication در پروتکل HSRP :

روش اول :

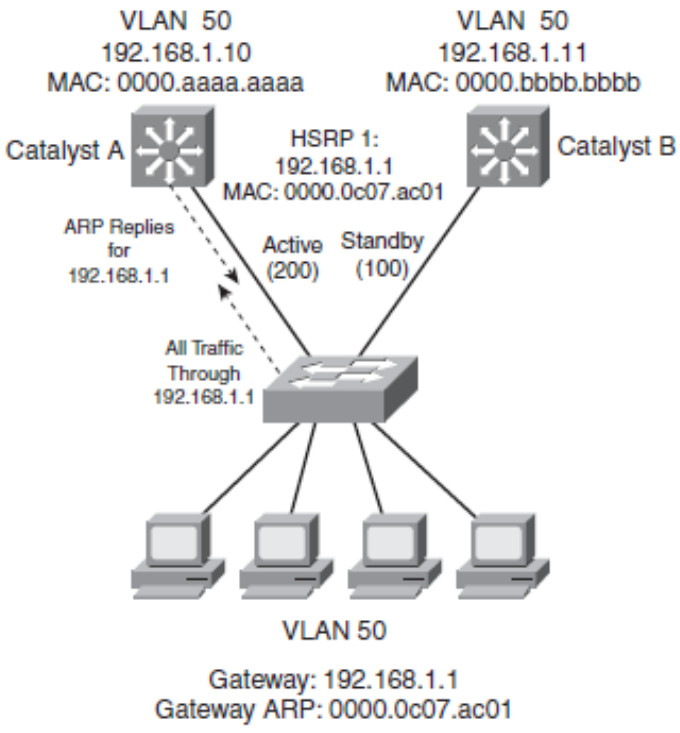
```
Switch ( config – if ) # Standby  group  Authentication  string
```

روش دوم :

```
Switch ( config – if ) # Standby  group Authentication  MD5 Key – String
[ 0 | 7 ]  string
```

مثال :

شکل زیر نشان دهنده یک توپولوژی می باشد که در آن اقدام به استفاده از دو سوئیچ Multilayer کرده و همچنین یک گروه HSRP با شماره برابر با 1 و آدرس IP برابر با 192.168.1.1 در روی آنها ایجاد کرده ایم . سوئیچ A به دلیل در اختیار داشتن Priority بالاتر در نقش Active بوده و بنابراین به درخواست های ARP رسیده از کلاینت ها پاسخ خواهد داد . در این بین سوئیچ B در وضعیت Standby قرار داشته و بنابراین به پیام های ارسال شده به مقصد 192.168.1.1 پاسخ نخواهد داد . از این رو تنها سوئیچ A و اتصالات منتهی به آن برای انتقال ترافیک شبکه مورد استفاده قرار خواهند گرفت :



همانطور که در شکل فوق مشاهده می کنید تمام ترافیک کامپیوترهای VLAN 50 از طریق سوئیچ A انتقال داده می شود . اگر دقت کنید Default Gateway همه کامپوترها برابر با آدرس IP مجازی قرار داده شده است و آدرس MAC برای ARP برابر با 0000.0c07.ac01 است که 01 آن برابر با شماره گروه HSRP است .

در زیر پیکربندی مربوط به هر سوئیچ A را مشاهده می کنید :

Configuring an HSRP Group on a Switch

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# standby 1 priority 200
CatalystA(config-if)# standby 1 preempt
CatalystA(config-if)# standby 1 ip 192.168.1.1
```

دستورات بالا مربوط به سوئیچ A می باشد . پیکربندی مربوط به سوئیچ B نیز دقیقا با سوئیچ A یکسان بوده با این تفاوت که دستور تعیین Priority در سوئیچ A برابر با 200 بوده و در روی سوئیچ B برابر با 100 که همان مقدار پیش فرض است .

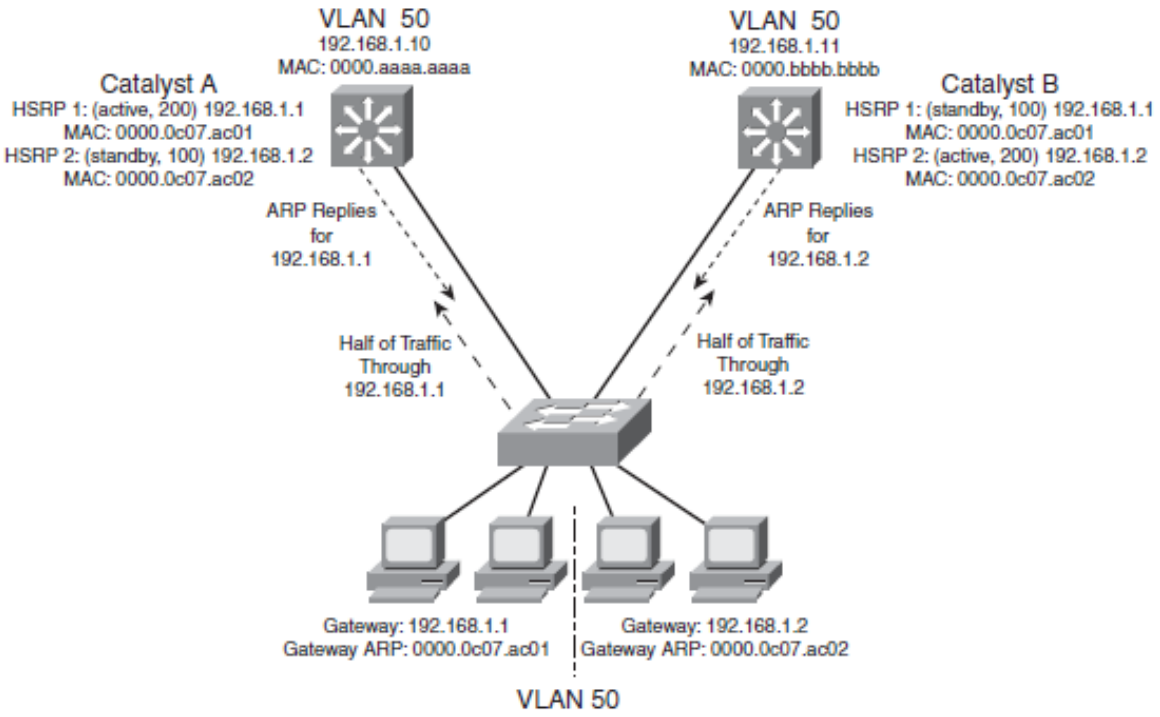
انجام Load Balancing در پروتکل HSRP :

همان سناریوی قبلی را در نظر بگیرید ، چون یکی از سوئیچ ها در حالت Active قرار دارد پس همه کلاینت ها ترافیک خود را به سمت سوئیچ Active خواهند فرستاد و سوئیچ دیگر و اتصالات آن تا زمان بروز ایرادی در کار سوئیچ Active مورد استفاده قرار نخواهد گرفت .

انجام Load Balancing و ارسال ترافیک به سمت هر دو دستگاه واقع در لایه Distribution با استفاده از یک گروه HSRP غیر ممکن است . پس برای انجام این کار باید دو گروه HSRP تعریف کنیم و یک سوئیچ را در گروه HSRP 1 در نقش سوئیچ Active قرار دهیم و در گروه HSRP 2 در نقش سوئیچ Standby قرار دهیم و سوئیچ دیگر را در گروه HSRP 1 در نقش سوئیچ Standby قرار دهیم و در گروه HSRP 2 در نقش سوئیچ Active قرار دهیم . در این حالت دو روتر مجازی HSRP و در نتیجه دو آدرس IP متفاوت به عنوان Default Gateway در اختیار خواهیم داشت .

شکل صفحه بعد همین سناریو را نمایش داده است . در این مثال سوئیچ A به عنوان Active در مورد گروه اول (192.168.1.1) و Standby در مورد گروه دوم (192.168.1.2) تعیین شده است .در این بین سوئیچ B به عنوان Active در مورد گروه دوم و Standby در مورد گروه اول عمل خواهد کرد .

در ادامه کار باید نیمی از کلاینت ها را برای استفاده از گروه اول به عنوان Default Gateway و نیمی دیگر را برای بهره گیری از گروه دوم به عنوان Default Gateway پیکربندی کرد .



در زیر پیکربندی مربوط به هر دو سوئیچ را مشاهده می کنید :

Configuring Load Balancing Between HSRP Groups

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# standby 1 priority 200
CatalystA(config-if)# standby 1 preempt
CatalystA(config-if)# standby 1 ip 192.168.1.1
CatalystA(config-if)# standby 1 authentication MyKey
CatalystA(config-if)# standby 2 priority 100
CatalystA(config-if)# standby 2 ip 192.168.1.2
CatalystA(config-if)# standby 2 authentication MyKey
```

```
CatalystB(config)# interface vlan 50
CatalystB(config-if)# ip address 192.168.1.11 255.255.255.0
CatalystB(config-if)# standby 1 priority 100
CatalystB(config-if)# standby 1 ip 192.168.1.1
CatalystB(config-if)# standby 1 authentication MyKey
CatalystB(config-if)# standby 2 priority 200
CatalystB(config-if)# standby 2 preempt
CatalystB(config-if)# standby 2 ip 192.168.1.2
CatalystB(config-if)# standby 2 authentication MyKey
```

برای مشاهده وضعیت مربوط به گروه های HSRP و اینترفیس های مربوطه از دستور زیر استفاده می کنیم :

Switch # Show Standby [Brife] [VLAN vlan – id] [type mod/num]

اجرای این دستور در روی سوئیچ A در سناریوی قبل نتیجه زیر را در برخواهد داشت :

Displaying the HSRP Router Role of a Switch: CatalystA

```
CatalystA# show standby vlan 50 brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active addr      Standby addr     Group addr
Vl50        1   200  P Active   local            192.168.1.11     192.168.1.1
Vl50        2   100    Standby  192.168.1.11     local            192.168.1.2
CatalystA#
CatalystA# show standby vlan 50
Vlan50 - Group 1

  Local state is Active, priority 200, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.248
  Virtual IP address is 192.168.1.1 configured
  Active router is local
  Standby router is 192.168.1.11 expires in 9.860
  Virtual mac address is 0000.0c07.ac01
  Authentication text "MyKey"
  2 state changes, last state change 00:11:58
  IP redundancy name is "hsrp-Vl50-1" (default)
Vlan50 - Group 2
  Local state is Standby, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 1.302
  Virtual IP address is 192.168.1.2 configured
  Active router is 192.168.1.11, priority 200 expires in 7.812
  Standby router is local
  Authentication text "MyKey"
  4 state changes, last state change 00:10:04
  IP redundancy name is "hsrp-Vl50-2" (default)
CatalystA#
```

مثال زیر اجرای دستور فوق را در روی سوئیچ B نشان می دهد :

Displaying the HSRP Router Role of a Switch: CatalystB

```
CatalystB# show standby vlan 50 brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active addr      Standby addr     Group addr
Vl50        1    100    Standby  192.168.1.10     local            192.168.1.1
Vl50        2    200  P Active   local            192.168.1.10     192.168.1.2
CatalystB#
CatalystB# show standby vlan 50
Vlan50 - Group 1

  Local state is Standby, priority 100
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 0.980
  Virtual IP address is 192.168.1.1 configured
  Active router is 192.168.1.10, priority 200 expires in 8.128
  Standby router is local
  Authentication text "MyKey"
  1 state changes, last state change 00:01:12
  IP redundancy name is "hsrp-Vl50-1" (default)
Vlan50 - Group 2
  Local state is Active, priority 200, may preempt
  Hellotime 3 sec, holdtime 10 sec
  Next hello sent in 2.888
  Virtual IP address is 192.168.1.2 configured
  Active router is local
  Standby router is 192.168.1.10 expires in 8.500
  Virtual mac address is 0000.0c07.ac02
  Authentication text "MyKey"
  1 state changes, last state change 00:01:16
CatalystB#
```

همانطور که در خروجی دستور مشاهده می کنید سوئیچ B در گروه 1 در حالت Standby قرار دارد و در گروه 2 در نقش Active فعال است .

: Virtual Router Redundancy Protocol (VRRP)

این پروتکل شبیه به پروتکل HSRP بوده اما توسط سازمان استاندارد IETF و در سند RFC 2338 معرفی شده است . در این پروتکل نیز چندین روتر در یک گروه مجازی معروف به گروه VRRP قرار خواهند گرفت و به کلیه روترهای قرار گرفته در این گروه یک آدرس IP و یک MAC Address اختصاص داده خواهد شد . در پروتکل VRRP در داخل گروه مجازی VRRP یک روتر در نقش روتر اصلی یا روتر Master و سایر روترها در نقش روتر پشتیبان یا Backup قرار خواهند داشت . در این پروتکل تنها روتر Master قادر به ارسال ترافیک به مقصد خواهد بود .

در این پروتکل روتری که بالاترین Priority را داشته باشد به عنوان روتر اصلی یا روتر Master انتخاب خواهد شد که مقدار پیش فرض آن 100 است اما می توان عددی بین 0 الی 254 را نیز انتخاب کرد . آدرس MAC مربوط به روتر مجازی VRRP در فرمت 0000.5e00.01XX می باشد که متغیر XX اشاره به شماره گروه VRRP در مبنای 16 دارد .

روتر Master با ارسال پیام هایی به نام Advertisement به مقصد یک آدرس Multicast ، یعنی 244.0.0.18 به کلیه روترهای داخل گروه VRRP وضعیت خود را اعلام خواهد کرد . پیام های Advertisement به صورت پیش فرض هر 1 ثانیه یکبار ارسال خواهد شد .

برای پیکربندی VRRP از دستورات زیر استفاده می کنیم :

Switch (config – if) # VRRP group Priority level

Switch (config – if) # VRRP group IP virtual – IP

Switch(config – if)# VRRP group Timers Advertisement [msec] interval

Switch (config – if) # No VRRP group Preempt

Switch (config – if) # VRRP group Preempt [Delay seconds]

Switch (config – if) # VRRP group Authentication string

دستور مجبور کردن روتر به کسب مقدار Advertisement Timer از دستگاه Master :

Switch (config – if) # VRRP group Timers Learn

این بار سناریوی Load Balancing در پروتکل HSRP را در مورد VRRP مطرح می کنیم . در این حالت پیکربندی مربوط به سوئیچ های A و B به ترتیب زیر خواهد بود :

Configuring Load Balancing with VRRP

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# vrrp 1 priority 200
CatalystA(config-if)# vrrp 1 ip 192.168.1.1

CatalystA(config-if)# vrrp 2 priority 100
CatalystA(config-if)# no vrrp 2 preempt
CatalystA(config-if)# vrrp 2 ip 192.168.1.2
```

```
CatalystB(config)# interface vlan 50
CatalystB(config-if)# ip address 192.168.1.11 255.255.255.0
CatalystB(config-if)# vrrp 1 priority 100
CatalystB(config-if)# no vrrp 1 preempt
CatalystB(config-if)# vrrp 1 ip 192.168.1.1
CatalystB(config-if)# vrrp 2 priority 200
CatalystB(config-if)# vrrp 2 ip 192.168.1.2
```

برای مشاهده وضعیت مربوط به VRRP در روی یک یا چند اینترفیس از دستور زیر استفاده می کنیم :

Switch # Show VRRP [Brife]

مثال زیر نمونه ای از اجرای دستور فوق را در روی سوئیچ های A و B نشان می دهد :

Displaying Switch Roles for VRRP Load Balancing

```
CatalystA# show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vlan50             1   200 3218        Y  Master  192.168.1.10    192.168.1.1
Vlan50             2   100 3609           Backup  192.168.1.11    192.168.1.2
CatalystA#
CatalystB# show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Vlan50             1   100 3609           Backup  192.168.1.10    192.168.1.1
Vlan50             2   200 3218        Y  Master  192.168.1.11    192.168.1.2
CatalystB#
```

Gateway Load Balancing Protocol (GLBP) :

پروتکل GLBP یک پروتکل اختصاصی شرکت سیسکو می باشد . این پروتکل علاوه بر تحمل خطا امکان تعادل بار بین چندین روتر در یک گروه GLBP را فراهم می کند . در پروتکل GLBP چندین روتر در یک گروه GLBP قادر به ارسال همزمان ترافیک به سمت مقصد خواهند بود . در صورت ارسال بسته های اطلاعاتی توسط کامپیوترها به سمت IP Address مجازی گروه GLBP ، کلیه روترهای داخل گروه به صورت همزمان بسته ها را به مقصد ارسال خواهند کرد . پروتکل GLBP بر روی سوئیچ های سری 4500 و سری 6500 سیسکو پشتیبانی خواهند شد . در این پروتکل حداکثر تا 1024 عدد اینترفیس قادر خواهند بود در یک گروه GLBP قرار گیرند .

پروتکل GLBP بر خلاف دو پروتکل قبل ، نیازی به آنکه برخی از کلاینت ها از یک آدرس Default Gateway و برخی دیگر از یک آدرس Default Gateway دیگر استفاده کنند وجود نداشته و همگی آنها تنها از یک آدرس Default Gateway یکسان برخوردار خواهند بود . در این صورت کلاینت ها درخواست های ARP خود را برای این روتر مجازی ارسال کرده و آدرس MAC مربوط به یکی از دستگاه های واقع در گروه GLBP برای آن فرستاده می شود . نتیجه آن خواهد بود که تمامی کلاینت ها از یک آدرس IP به عنوان Default Gateway استفاده کرده اما از MACهای مختلفی برای دسترسی به همان IP استفاده خواهند کرد .

Active Virtual Gateway (AVG) :

از بین تمامی روترهای واقع در داخل یک گروه GLBP یک روتر به عنوان AVG برگزیده خواهد شد . در این انتخاب مقدار Priority بالا و یا در صورت یکسان بودن آن ، IP بزرگتر مد نظر قرار داده می شود . روتر AVG مسئول ارسال پاسخ در قبال تمامی درخواست های ARP کلاینت ها است . روتر AVG بر روی هر کدام از روترهای عضو گروه GLBP اقدام به تخصیص یک آدرس MAC مجازی خواهد کرد . در این بین حداکثر 4 عدد آدرس MAC مجازی می تواند در داخل یک گروه GLBP قرار داشته باشد .

Active Virtual Forwarder (AVF) :

تمامی روترهای عضو یک گروه GLBP می توانند توسط دستگاه AVG به عنوان دستگاه AVF تعیین شوند که در این صورت یک آدرس MAC مجازی نیز بر روی آنها اختصاص داده خواهد شد . فرمت این آدرس MAC به صورت 0007.b4XX.XXYY می باشد که 6 بیت ابتدایی قسمت XXXX برابر با صفر و 10 بیت بقیه برابر با شماره گروه GLBP خواهد بود . همچنین YY نیز بیان کننده شماره مربوط به روتر AVF است .

تمامی روترهای عضو یک گروه GLBP باید وضعیت یکدیگر را زیر نظر بگیرند تا در هنگام بروز ایرادی در کار یکی از آنها روتری دیگر جایگزین آن گردد . برای انجام این کار روتر AVG اقدام به ارسال پیام های متناوب Hello

برای تمامی دیگر روترهای عضو گروه کرده و منتظر دریافت پاسخ از سوی آنها می ماند . به صورت پیش فرض این پیام ها هر 3 ثانیه یکبار ارسال می شوند .در صورتی که در خلال مدت زمان Holdtime که برابر با 10 ثانیه است پاسخی از سوی AVG دریافت نگردد ، دستگاه مورد نظر به صورت معیوب در نظر گرفته خواهد شد . به صورت پیش فرض روتر AVG از پیام های Hello برای شناسایی روترهای AVF معیوب نیز استفاده می کند .

پیکربندی GLBP :

Switch (config – if) # GLBP group Priority level

دستور تعریف آدرس IP مجازی پروتکل GLBP :

Switch (config – if) # GLBP group IP virtual – IP

دستور تغییر مقدار زمان های پروتکل GLBP :

Switch (config – if) # GLBP group Timers [msec] Hello [msec] Holdtime

اگر به هر دلیلی سوئیچ AVG غیرفعال شود و سوئیچ دیگری جایگزین آن شود و دوباره بعد از مدتی سوئیچ AVG فعال شود نمی تواند به صورت پیش فرض دوباره در نقش سوئیچ AVG ظاهر شود حتی اگر مقدار Priority آن نیز بالاتر باشد . با وارد کردن دستور زیر سوئیچ دوباره می تواند در نقش سوئیچ AVG ظاهر شود :

Switch (config – if) # GLBP group Preempt [Minimum Delay seconds]

همانطور که می دانید در یک گروه GLBP فقط 4 عدد سوئیچ AVF می توانند در این نقش ظاهر شوند . برای انتخاب این چهار سوئیچ از پارامتری به نام Weight استفاده می کنیم که به صورت پیش فرض در تمام سوئیچ ها برابر با 100 می باشد و می توان عددی بین 1 الی 254 را قرار داد. هر سوئیچ Weight بالاتری داشته باشد در انتخاب AVF شرکت داده می شود .

برای انجام این کار باید سه مرحله زیر را انجام دهیم :

در ابتدا نیاز به مشخص کردن پورت هایی داریم که باید ویژگی Tracking در روی آنها فعال گردد . به منظور انجام این کار باید یک گروه برای قرار دادن این اینترفیس ها در داخل آن ایجاد کنیم . نام مربوط به گروه مزبور به جای متغیر abject – number در دستور زیر می نویسیم که مقدار آن عددی بین 1 الی 500 خواهد بود . نوع مربوط به پروسه Tracking را نیز می توان توسط یکی از پارامترهای Line – protocol و IP Routing تعیین کرد . بدین ترتیب که دستور Line – protocol اشاره به وضعیت لایه 2 داشته و IP Routing نیز اشاره به وضعیت لایه 3 و پروتکل Routing فعال شده در روی آن پورت دارد .

Switch (config) # Track abject – number Interface type mod/num { Line – protocol | IP Routing }

در مرحله بعد باید مقدار کاهش پارامتر Weight در هنگام بروز ایرادی در روی پورت های Track شده را مشخص کرد . در صورتی که در وضعیت پورت مشخص شده در دستور Track تغییری رخ داده و کارکرد آن مختل شود ، مقدار Weight مربوط به دستگاه برابر با عدد تعیین شده بعد از دستور Decrement کاهش خواهد یافت .

Switch (config – if) # GLBP group Weighting Track abject – number [Decrement value]

در مرحله سوم باید مقدار Weight مربوط به روتر GLBP را تعیین کرد . همچنین باید در این مرحله مقدار حداقل و حداکثری را برای Weight مشخص نمود . همانطور که گفته شد در صورتی که مقدار Weight به زیر حداقل تعیین شده برسد ، نقش AVF از دستگاه گرفته خواهد شد :

Switch (config – if) # GLBP group Weighting Maximum [Lower value] [Upper value]

اگر یکی از AVFها قطع شود تا مدت زمان Redirect که برابر با 600 ثانیه می باشد ، سوئیچ AVG هم آدرس MAC آن سوئیچ قطع شده را برمی گرداند و هم به جای او Forwarding را انجام می دهد بعد تا مدت 14400 ثانیه فقط Forwarding را به جای او انجام می دهد و آدرس MAC او را نمی فرستد . اگر بعد از گذشت 14400 ثانیه سوئیچ AVF باز وصل نشود ، سوئیچ AVG ارتباط را قطع می کند و هیچ کاری را به جای او انجام نمی دهد .

Redirect → 600 s

Time – out → 14400 s

Time < 600 s → Send MAC + Forwarding

600 s < Time < 14400 s → Forwarding

Time > 14400 s → Faild

دستور تغییر مقدار Redirect و Time – out :

Switch (config – if) # GLBP group Timers Redirect redirect timeout

متد Load Balancing در پروتکل GLBP :

همانطور که می دانید روتر AVG حداکثر تا 4 عدد روتر AVF را در داخل یک گروه GLBP انتخاب کرده و بر روی هر یک از آنها یک آدرس MAC مجازی اختصاص می دهد . همچنین روتر AVG تنها روتری است که قادر به دریافت درخواست های ARP از کلاینت ها و ارسال MAC مربوط به یکی از روترهای AVF به آنهاست . به این صورت دستگاه AVG با کنترل آدرس های MAC فرستاده شده به کلاینت ها می تواند عملیات Load Balancing را کنترل کند .

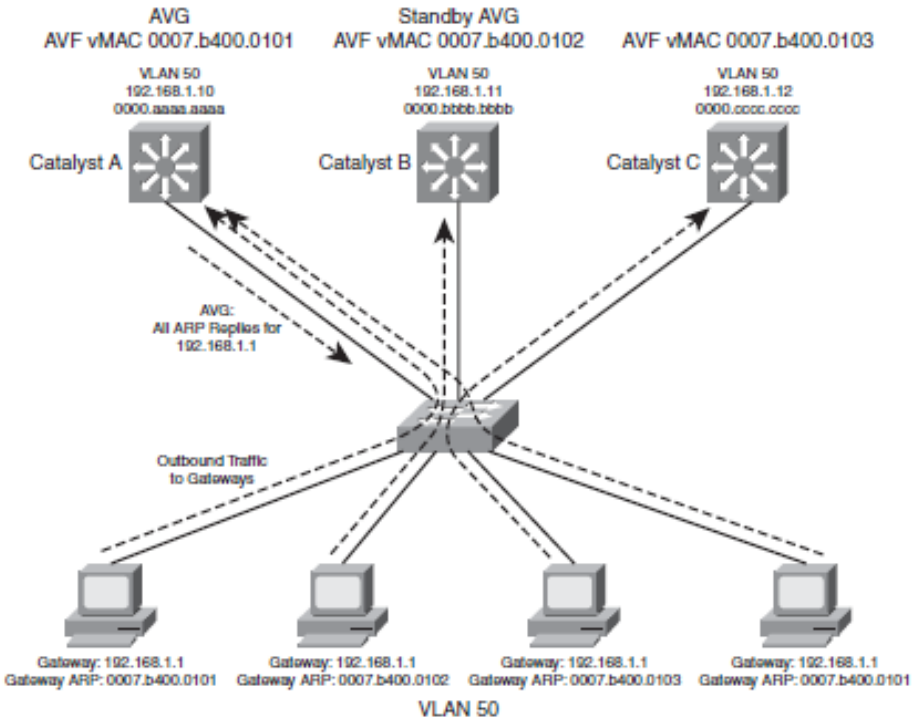
در حالت کلی 3 روش زیر برای انجام Load Balancing در پروتکل GLBP وجود دارد که عبارتند از :

- **Round Robin :** آدرس های MAC مجازی مربوط به روترهای AVF به ترتیب (چرخشی) به کلاینت های ارسال کننده درخواست ARP فرستاده می شود . این وضعیت به صورت پیش فرض نیز مورد استفاده قرار می گیرد .
- **Weighted :** در این متد مقدار Weight است که حجم ترافیک ارسال شده به سمت هر کدام از VAFها را تعیین می کند . در صورتی که مقدار Weight مربوط به یک روتر AVF بیشتر باشد ، آدرس MAC مجازی مربوط به آن به کلاینت های بیشتری فرستاده شده و بنابراین کاربران بیشتری از آن دستگاه به عنوان Default Gateway استفاده می کنند .
- **Host Dependent :** در این متد هر کدام از کلاینت هایی که اقدام به ارسال یک درخواست ARP کرده اند ، یک آدرس MAC مجازی از AVG دریافت کرده و به صورت همیشگی از همان روتر AVF به عنوان Default Gateway استفاده می کند .

برای تعیین متد Load Balancing می توانید از دستور زیر بر روی روتر AVG استفاده کنید :

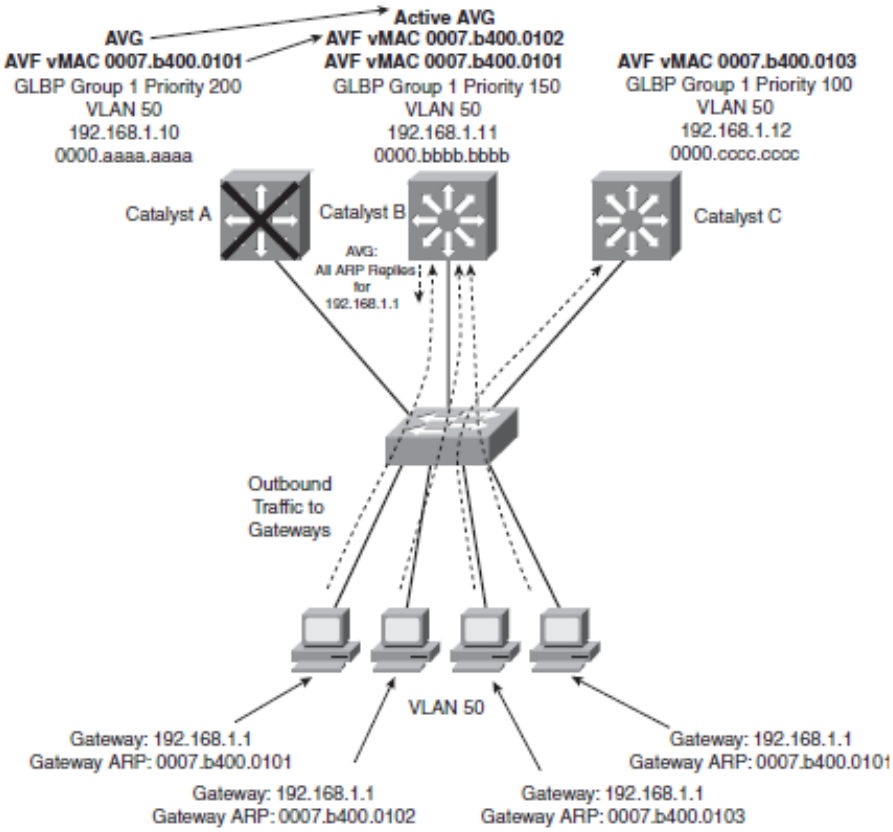
Switch (config – if) # GLBP group Load Balancing [Round – Robin | Weighted | Host – Dependent]

شکل صفحه بعد نشان دهنده مثالی است که در آن 3 سوئیچ Multilayer در داخل یک گروه GLBP قرار گرفته اند . در این بین سوئیچ A به عنوان روتر AVG انتخاب شده و آدرس روتر مجازی GLBP نیز برابر با 192.168.1.1 تعیین شده است . در این صورت تمامی پیام های ARP مربوط به کلاینت ها تنها توسط سوئیچ A دریافت و پردازش خواهد شد . سوئیچ های B و C نیز به عنوان دو دستگاه AVF عمل می کنند .



همانطور که در شکل بالا مشاهده می کنید متد Load Balancing مورد استفاده شده در این مثال برابر با Round Robin بوده و بنابراین سوئیچ A در هنگام ارسال پاسخ به درخواست های ARP کلاینت ها ، آدرس MAC مجازی مربوط به سوئیچ های AVF را به ترتیب در داخل پیام های ARP Reply خواهد گنجاند .

شکل زیر نشان دهنده عکس العمل روترهای GLBP در هنگام معیوب شدن دستگاه AVG فعلی است .



قبل از بروز ایراد ، روتر A به دلیل دارا بودن مقدار بالاتری از Priority در نقش AVG عمل کرده ولی بعد از معیوب شدن این دستگاه و بر اساس مقدار Priority ، سوئیچ B به همین نقش انتخاب می شود . در این شرایط سوئیچ B به عنوان AVG مسئول دریافت درخواست های ARP و ارسال یکی از آدرس های MAC مجازی به سمت کلاینت ها خواهد بود . در نتیجه این کار ، تمامی کلاینت هایی که قبل از خراب شدن دستگاه A از آن به عنوان Default Gateway استفاده می کردند ، حالا نیز می توانند ترافیک خود را دوباره به سمت همان IP (یعنی 192.168.1.1) و همان MAC (یعنی 0007.b400.0102) ارسال کنند .

با توجه به این سناریو پیکربندی مربوط به سوئیچ های A و B و C به ترتیب زیر خواهد بود :

Configuring GLBP Load Balancing

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# glbp 1 priority 200
CatalystA(config-if)# glbp 1 preempt
CatalystA(config-if)# glbp 1 ip 192.168.1.1
```

```
CatalystB(config)# interface vlan 50
CatalystB(config-if)# ip address 192.168.1.11 255.255.255.0
CatalystB(config-if)# glbp 1 priority 150
CatalystB(config-if)# glbp 1 preempt
CatalystB(config-if)# glbp 1 ip 192.168.1.1
```

```
CatalystC(config)# interface vlan 50
CatalystC(config-if)# ip address 192.168.1.12 255.255.255.0
CatalystC(config-if)# glbp 1 priority 100
CatalystC(config-if)# glbp 1 ip 192.168.1.1
```

برای بررسی عملکرد GLBP می توانید از دستور Show GLBP [Brief] استفاده کنید .

مثال زیر نمونه ای از اجرای این دستور را بر روی سوئیچ های A و B و C نشان می دهد :

```
CatalystA# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
V150        1    -   200 Active   192.168.1.1     local           192.168.1.11
V150        1    1   7   Active   0007.b400.0101  local           -
V150        1    2   7   Listen   0007.b400.0102  192.168.1.11    -
V150        1    3   7   Listen   0007.b400.0103  192.168.1.12    -
CatalystA#
```

```
CatalystB# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
V150        1    -   150 Standby  192.168.1.1     192.168.1.10    local
V150        1    1   7   Listen   0007.b400.0101  192.168.1.10    -
V150        1    2   7   Active   0007.b400.0102  local           -
V150        1    3   7   Listen   0007.b400.0103  192.168.1.12    -
CatalystB#
```

```
CatalystC# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router


V150        1    -   100 Listen   192.168.1.1     192.168.1.10    192.168.1.11
V150        1    1   7   Listen   0007.b400.0101  192.168.1.10    -
V150        1    2   7   Listen   0007.b400.0102  192.168.1.11    -
V150        1    3   7   Active   0007.b400.0103  local           -
CatalystC#
```

Redundant Switch Supervisors :

سوئیچ هایی مانند مدل های 4500R و سری 6500 می توانند حاوی دو عدد Supervisors در داخل شاسی های خود باشند . در این شرایط اولین Supervisors که سریعتر بوت شود در نقش فعال (Active) قرار گرفته و Supervisors دیگر به عنوان جایگزین (Backup) آن انتخاب خواهد شد . Supervisors فعال بلافاصله بعد از بوت دستگاه شروع به کار خواهد کرد . در حقیقت تمامی عملیات Switching توسط این Supervisors صورت خواهد گرفت . اما Supervisors دیگر که در وضعیت Standby قرار دارد تنها تا یک مرحله خاص بوت شده و منتظر معیوب شدن Supervisors فعال باقی می ماند .

برای پیکربندی ویژگی Redundancy در مورد دو Supervisors می توان از Modeهای مختلفی استفاده کرد . نوع Mode مورد استفاده برای انجام این کار نحوه برقراری ارتباط دو Supervisors و تبادل اطلاعات مابین آنها را تعیین خواهد کرد .

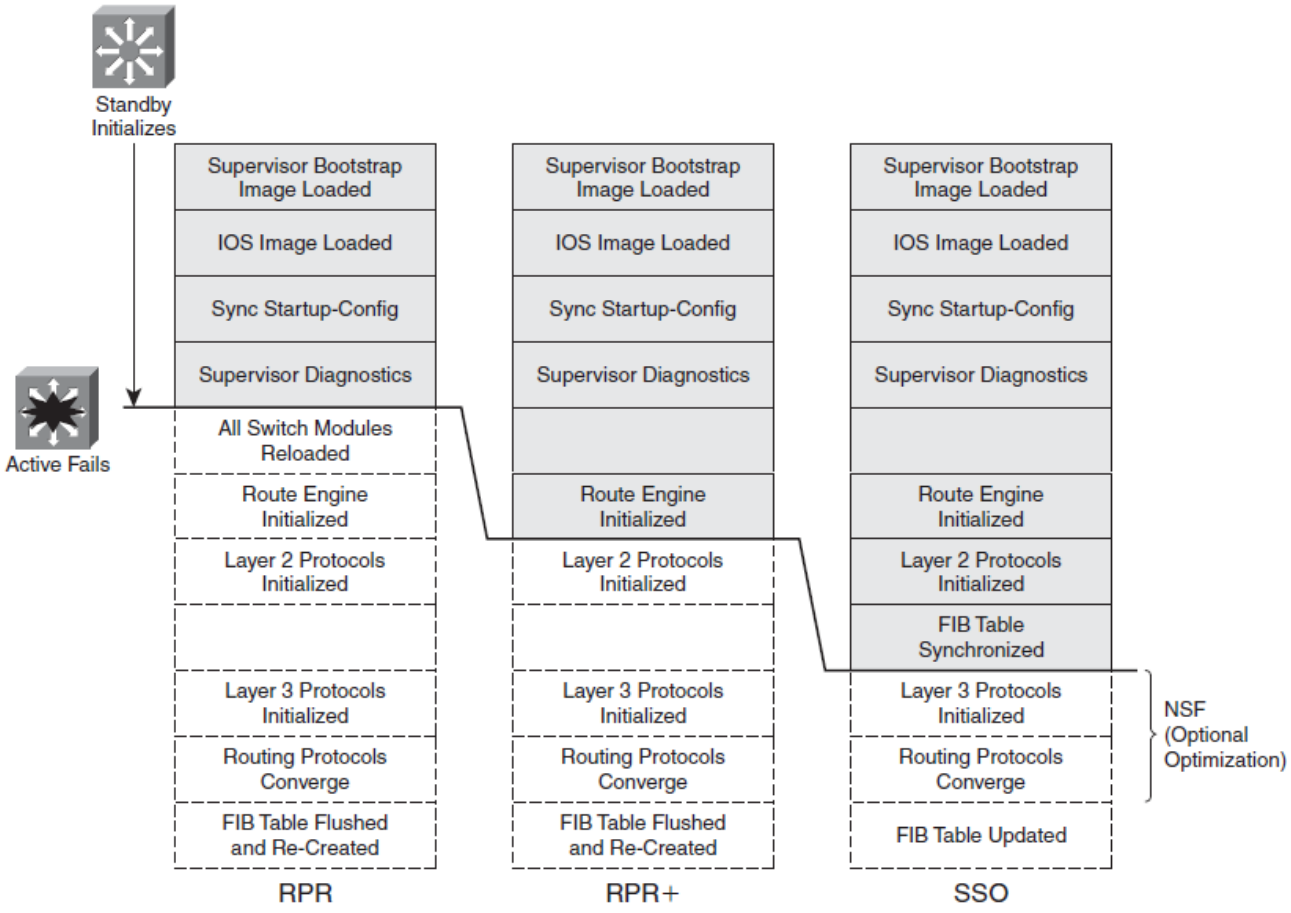
در حالت کلی انواع Modeهای مربوط به پیکربندی ویژگی Redundancy در روی سوئیچ های کاتالیست سیسکو به صورت زیر است :

- **Route Processor Redundancy (RPR)** : در این حالت Supervisors ثانویه به صورت ناقص بوت شده و اگر Supervisors فعال معیوب گردد ، Supervisors دوم تمامی دیگر ماژول های نصب شده در روی سوئیچ را ریست کرده و سپس نقش فعال را بر عهده خواهد گرفت . در این حالت مدت زمان پوشش دادن خطا کمتر از 2 دقیقه می باشد .

- **Route Processor Redundancy Plus (RPR +)** : در این حالت Supervisors ثانویه بوت و Route Engine آن نیز شناسایی شده و در مدار قرار می گیرد . اما Supervisors مزبور نخواهد توانست به صورت فعال در پروسه های Routing و Switching شرکت نماید . در نتیجه در صورت بروز ایرادی در Supervisors فعال ، Supervisors دوم می تواند پروسه بوت خود را کامل کرده و بدون تاثیرگذاری در دیگر ماژول ها فعالیت خود را آغاز کند . در این حالت مدت زمان پوشش دادن خطا کمتر از 30 ثانیه می باشد .

- **Stateful Switchover (SSO)** : در این حالت Supervisors ثانویه به صورت کامل بوت شده و Route Engine و Switch Engine آن نیز شناسایی و در مدار قرار می گیرد . حتی در این بین محتویات فایل های running – config و startup – config نیز مابین دو Supervisors مبادله شده و قرار گرفتن دستگاه جدید در مدار در کمتر از 1 ثانیه انجام می پذیرد .

در شکل زیر مراحلی که به صورت پررنگ تر نشان داده شده است بیانگر مراحلی هستند که در هر کدام از Redundancy Modeها توسط Standby Supervisors طی می شود . مشاهده می نمایید که در متد SSO یک Standby Supervisors مراحل کمی تا بوت کامل فاصله داشته اما در مورد RPR این فاصله بیشتر از متدهای دیگر است .



Standby Supervisor Readiness as a Function of Redundancy Mode

برای تعیین متدهای مورد استفاده Redundancy می توانید از دستور زیر استفاده کنید :

Switch (config) # Redundancy

Switch (config – Red) # Mode { RPR | RPR – Plus | SSO }

دستوری که نشان می دهد که سوئیچ مورد نظر از چه متدی استفاده کرده و در چه وضعیتی قرار دارد از دستور زیر استفاده می کنیم :

Switch (config) # Show Redundancy States

مثال زیر نشان می دهد که سوئیچ از متد + RPR استفاده می کند . همچنین با نگاه کردن به عبارت my State می توان دریافت که دومین Supervisors (که با Unit ID برابر با 2 نشان داده شده است) در وضعیت Active قرار دارد . اما Supervisors بعدی در وضعیت Standby و HOT قرار دارد . بدین معنی که بوت آن وابسته به Redundancy Mode بوده و به محض وجود امکان این پروسه تکمیل خواهد شد :

Verifying Supervisor Module Redundancy Mode and State

```
Router# show redundancy states
        my state = 13 -ACTIVE
      peer state = 8  -STANDBY HOT
            Mode = Duplex
            Unit = Secondary

         Unit ID = 2

Redundancy Mode (Operational) = Route Processor Redundancy Plus
Redundancy Mode (Configured)  = Route Processor Redundancy Plus
      Split Mode = Disabled
   Manual Swact = Enabled
 Communications = Up

   client count = 11
 client_notification_TMR = 30000 milliseconds
           keep_alive TMR = 9000 milliseconds
         keep_alive count = 1
    keep_alive threshold = 18
            RF debug mask = 0x0
Router#
```

Securing Switch Access

: Port Security

تجهیزات سیسکو توانمندی پیشرفته ای را به نام Port security پشتیبانی می کنند که قابلیت افزایش امنیت را روی پورتهای سوئیچ به شما خواهد داد که این افزایش امنیت مخصوصا بر روی سوئیچ های لایه Access که کامپیوترهای کاربران به آن متصل میباشند , اهمیت بیشتری دارد .

Port security به شما این امکان را می دهد که قادر باشید کنترل کاملی روی دستگاه هایی که به سوئیچ متصل می شود داشته باشید .

مثلا شما می توانید توانمندی Port security را روی پورت FastEthernet 0/1 سوئیچ فعال کنید و اجازه بدهید فقط PC 1 قادر به برقراری ارتباط با این پورت باشد و سایر کامپیوترها قادر به برقراری ارتباط با پورت FastEthernet 0/1 را نداشته باشند . در صورتی که کامپیوتر یا هر Device دیگری غیر از PC 1 قصد استفاده از پورت FastEthernet 0/1 را داشته باشند , قادر به برقراری ارتباط با این پورت نباشند . در پیکربندی Port security می توانید تعیین کنید در صورتی که دستگاهی غیر از PC 1 قصد ارتباط با پورت FastEthernet 0/1 را داشته باشد این پورت Shutdown و غیر فعال شود .

Port security برای شناسایی کامپیوترها و تعیین مجاز بودن یا غیر مجاز بودن آن کامپیوتر برای استفاده از پورت از MAC Addresss آن کامپیوتر یا Device استفاده می کنند .

روی پورت هایی می توانیم امنیت برقرار کنیم که پورت ها Access باشند .

پیکربندی Port security :

Switch (config) # Interface type mod/num

Switch (config – if) # Switchport Mode Access

Switch (config – if) # Switchport Port – Security

Switch (config – if) # Switchport Port – Security Maximum number

Switch (config – if) # Switchport Port – Security MAC – Address mac-address

Switch (config – if) # Switchport Port – Security Violation Mode

مثال برای پورت 0/1 :

Switch (config) # interface fastethernet 0/1

Switch (config – if) # Switchport Mode Access

Switch (config – if) # Switchport Port – Security

Switch (config – if) # Switchport Port – Security Maximum 1

Switch (config – if) # Switchport Port – Security MAC – Address aaaa.1111.abab

Switch (config – if) # Switchport Port – Security Violation Shutdown

mode در قسمت Violation سه حالت زیر را دارد :

- **Shutdown** : در این حالت اگر تخلف در شبکه بر روی پورت انجام شود پورت خاموش یا غیر فعال می شود و در حالت errdisable قرار می گیرد .
- **Restrict** : در این حالت پورت در همان وضعیت فعال باقی می ماند اما پاکت های ارسالی از آدرس های MAC غیر مجاز را بلوکه می کند . در این بین تعداد پاکت های ارسالی از آدرس های MAC غیر مجاز شمارش شده و یک SNMP Trap و همچنین یک Log Message نیز ایجاد و فرستاده می شود .
- **Protect** : در این حالت پورت در همان وضعیت فعال باقی می ماند اما پاکت های ارسالی از آدرس های MAC غیر مجاز را بلوکه می کند . در این بین هیچ اطلاعاتی ثبت نشده و پیام خطایی نیز نمایش داده نمی شود .

زمانی در شبکه تخلف ایجاد شود پورت Shutdown می شود و پیغام Error – Disable را می دهد .برای برطرف کردن این پیام اول باید ارتباط PC که تخلف کرده را قطع کنیم , بعد PC اصلی را وصل می کنیم و بعد دوباره پورت را روشن می کنیم با دستورات زیر :

Switch (config)# Interface type mod/num

Switch (config)# shutdown

Switch (config)# No shutdown

نکته : وقتی در یک شبکه یک Hub به یک سوئیچ وصل باشد و یک PC به همان Hub وصل شده باشد و در تنظیمات Port – security همان پورتی که Hub به سوئیچ وصل شده تعداد Maximum را 2 تعریف کنیم اولین PC که به Hub وصل شود MAC آن در جای خالی MAC – Address – Table سوئیچ ذخیره می شود و تا زمانی که سوئیچ خاموش و روشن نشود این MAC از حافظه پاک نمی شود .

با فرمان زیر در Port security خود سوئیچ به صورت دینامیک پورت ها را Learn می کند یعنی با توجه به مقدار Maximum که تعریف کرده ایم MAC کامپیوترهایی را که برای اولین بار به پورت وصل می شوند ذخیره می کند :

Switch (config – if) # Switchport Port – Security MAC – Address sticky

MAC – Addressهایی را که به صورت Dynamic , Learn کرده ایم با دستور زیر پاک می شوند :

Switch # Clear Port – security Dynamic

MAC - Addressهایی را که به صورت Static , Learn کرده ایم با دستور زیر پاک می شوند :

Switch # Clear Port – security Static

Showهای Port – security :

Switch # Show Port – security

Switch # Show Port – Security – Address

Switch # Show Port – security interface type mod/num

Switch # Show Port – security Status err – disable

مثال زیر نمونه ای از اجرای دستور فوق است :

Displaying Summary Information for Ports in the Errdisable State

```
Switch# show interfaces status err-disabled
Port      Name               Status       Reason
Gi0/11    Test port          err-disabled psecure-violation
Switch#
TIP
When a port is moved to the errdisable state, you must either manually cycle it
or configure the switch to automatically re-enable ports after a prescribed delay.
To manually cycle a port and return it to service, use the following commands:
Switch(config)# interface type mod/num
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
```

مثال زیر نمونه ای از اجرای دستور Show Port – Security است :

Displaying Port Security Status Summary Information

```
Switch# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
     Gi0/11              5            1                  0         Restrict
     Gi0/12              1            0                  0         Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 6176
Switch#
```

Port – Based Authentication :

سویئچ های کاتالیست سیسکو قادر به پشتیبانی از ویژگی Port – Based Authentication هستند که ترکیبی از Port Security و AAA Authentication بوده و مبتنی بر استاندارد IEEE 802.1x می باشد . بعد از فعال شدن این ویژگی تا زمانی که هویت کلاینت ارسال کننده اطلاعات مورد تایید قرار نگرفته است ، هیچ ترافیکی از طریق پورت انتقال داده نخواهد شد . اما در صورت تایید هویت ، کلاینت می تواند به صورت عادی از پورت سوئیچ استفاده کند .به منظور بهره گیری از ویژگی فوق ، سوئیچ و کلاینت هر دو باید توانایی پشتیبانی از 802.1x و پروتکل (EAPOL) Extensible Authentication Protocol Over LANs را داشته باشند . پروتکل IEEE 802.1x در سطح لایه 2 عمل می نماید . زمانی که پورت سوئیچ وجود یک کلاینت را شناسایی می کند ، وضعیت در ابتدا به صورت Unauthenticated یا همان بلوکه باقی خواهد ماند تا کلاینت هویت خود را به اطلاع سوئیچ برساند . کلاینت تنها در صورتی قادر به برقراری ارتباط با سوئیچ IEEE 802.1x است که دارای نرم افزاری با قابلیت پشتیبانی از IEEE 802.1x باشد . در شرایطی که پورت سوئیچ در وضعیت Unauthenticated قرار گرفته است ، به جز ترافیک مربوط به پروتکل IEEE 802.1x هیچ ترافیکی قادر به عبور از پورت مزبور نخواهد بود .

پیکربندی پروتکل IEEE 802.1x :

برای بررسی هویت کلاینت ها می توان از یک یا چند سرور خارجی RADIUS استفاده کرد .

برای پیکربندی پروتکل IEEE 802.1x مراحل زیر را طی می کنیم :

- **مرحله اول :** فعال کردن AAA در روی سوئیچ

Switch (config) # AAA New – Model

- **مرحله دوم :** تعیین سرورهای RADIUS خارجی

Switch (config) # Radius – Server Host { hostname | ip – address } [Key string]

- **مرحله سوم :** متد مورد استفاده در Authentication را مشخص می کنیم

Switch (config) # AAA Authentication Dot 1x Default Group Radius

- **مرحله چهارم :** فعال کردن 802.1x روی سوئیچ

Switch (config) # Dot 1x System – Auth – Control

- **مرحله پنجم :** هر کدام از پورت هایی را که قرار است از این ویژگی استفاده کنند پیکربندی می کنیم

Switch (config) # Interface type mod/num
Switch (config – if) # Dot 1x Port – Control { Force – Authorized | Force – Unauthorized | Auto }

Force – Authorized : در این حالت پورت مزبور هیچ نوع بررسی در مورد هویت کلاینت های متصل انجام نداده و تمامی کلاینت ها می توانند از پورت استفاده کنند .
Force – Unauthorized : در این حالت هویت هیچ کدام از کلاینت های متصل مورد تأیید قرار نگرفته و بنابراین پورت مزبور به صورت همیشگی در وضعیت بلوکه باقی خواهد ماند .
Auto : در این صورت هویت کلاینت ها توسط پروتکل 802.1x مورد بررسی قرار می گیرد و در صورت موفقیت آمیز بودن کار ، وضعیت پورت به authenticated تغییر می یابد .

- **مرحله ششم :** امکان اتصال چندین کلاینت از طریق هر کدام از پورت ها :

Switch (config – if) # Dot 1x Host – Mode Multi – Host

در مثال زیر دو سرور Radius به آدرس های 10.1.1.1 و 10.1.1.2 پیکربندی شده است :

Configuring 802.1x Port-Based Authentication

```
Switch(config)# aaa new-model
Switch(config)# radius-server host 10.1.1.1 key BigSecret
Switch(config)# radius-server host 10.1.1.2 key AnotherBigSecret
Switch(config)# aaa authentication dot1x default group radius
Switch(config)# dot1x system-auth-control
Switch(config)# interface range FastEthernet0/1 - 40
Switch(config-if)# switchport access vlan 10
Switch(config-if)# switchport mode access
Switch(config-if)# dot1x port-control auto
```

شناسایی و حذف حمله های Spoofing :

DHCP Snooping :

همانطور که می دانید یک سرور DHCP می تواند برخی از اطلاعات مورد نیاز کاربران ، مانند آدرس IP و آدرس سرورهای DNS و Defalut gateway و نام Domain و موارد دیگر را در اختیار کلاینت ها قرار دهد . تصور کنید که یک فرد هکر اقدام به قرار دادن یک سرور DHCP غیر مجاز در شبکه کرده است . در این صورت پیام های DHCP Request ارسالی از کلاینت ها توسط این سرور نیز قابل دریافت خواهد بود . بدین ترتیب پاسخ پیام توسط این سرور DHCP غیرمجاز برای کلاینت ارسال خواهد شد و کلاینت در صورت دریافت آن ، آدرس اعلام شده توسط سرور DHCP را به عنوان Defalut gateway خواهد شناخت .
نتیجه بروز چنین شرایطی آن خواهد بود که پیام های ارسالی از کلاینت ها به جای ارسال به سمت Defalut gateway اصلی به سمت کامپیوتر فرد هکر فرستاده خواهد شد . این فرد می تواند بعد از دریافت و بررسی محتویات پیام ها آنها را به سمت Defalut gateway اصلی بفرستد اما در این میان به تمامی اطلاعات شبکه دسترسی پیدا کرده است .

شرکت سیسکو در سوئیچ های کاتالسیت خود از توانمندی به نام DHCP Snooping جهت افزایش امنیت در برابر حمله DHCP Server Spoofing پشتیبانی می کند که برای مقابله به حمله DHCP Server Spoofing پورت های سوئیچ در دو وضعیت به شرح زیر قرار خواهند گرفت :

- **Trusted :**

پورت سوئیچ که در وضعیت Trusted قرار دارد قادر به دریافت پیام های DHCP Offer ، DHCP ACK خواهد بود .

- **Untrusted :**

پورت سوئیچ در وضعیت Untrusted قادر به دریافت پیام های DHCP Discover ، DHCP Request خواهد بود . پورتی که در وضعیت Untrusted قرار دارد قادر به دریافت پیام های DHCP Offer ، DHCP ACK نخواهد بود و در صورت دریافت این پیام ها پورت Shutdown خواهد شد .

نکته :
همه اینترفیس ها به صورت پیش فرض در وضعیت Untrusted قرار دارند . پورت سوئیچ که به DHCP Server متصل می باشد باید در وضعیت Trusted و سایر پورت ها در وضعیت Untrusted قرار گیرند .

پیکربندی DHCP Snooping :

Switch (config) # IP DHCP Snooping

Switch (config) # IP DHCP Snooping VLAN vlan – id [vlan – id]

Switch (config) # Interface type mod/num

Switch (config – if) # IP DHCP Snooping Trust

به صورت پیش فرض تعداد پیام های DHCP دریافت شده توسط پورت های Untrusted از اهمیت برخوردار نبوده اما در صورتی که می خواهید این تعداد را محدود به عدد خاصی کنید ، از دستور زیر استفاده می کنید :

Switch (config) # Interface type mod/num

Switch (config – if) # IP DHCP Snooping Limit Rate rate

به جای متغیر می توانید از رنج 1 الی 2048 استفاده کنید . همچنین واحد شمارش این متغیر نیز پاکت بر ثانیه می باشد .

سوئیچ ها را می توان برای استفاده از DHCP Option – 82 نیز پیکربندی کرد . در این صورت سوئیچ پیام های DHCP Request دریافتی از پورت های Untrusted را بررسی کرده و آدرس MAC و ID مربوط به پورت را در داخل فیلد Option – 82 قرار می دهد . در نتیجه این پیکربندی ، DHCP Request مزبور به سمت سرور DHCP مجاز ارسال خواهد شد :

Switch (config) # [No] IP DHCP Snooping Information Option

برای مشاهده وضعیت DHCP Snooping و اطلاعات مربوطه از دستور زیر استفاده می کنیم :

Switch # Show IP DHCP Snooping [Binding]

برای مثال فرض کنید که می خواهیم دو پورت fast 0/35 و fast 0/36 که عضوی از VLAN 104 می باشند را به عنوان Untrusted تعیین کرده و حداکثر تعداد پیام های DHCP دریافتی از آنها را برابر با 3 قرار دهیم . در این بین به دلیل آنکه سرور DHCP مجاز ما متصل به پورت giga 0/1 می باشد ، این پورت باید به عنوان Trusted تعیین گردد .

مثال زیر نحوه پیکربندی سوئیچ را نشان می دهد :

DHCP Snooping Configuration

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 104
Switch(config)# interface range fastethernet 0/35 - 36
Switch(config-if)# ip dhcp snooping limit rate 3
Switch(config-if)# interface gigabitethernet 0/1
Switch(config-if)# ip dhcp snooping trust
```

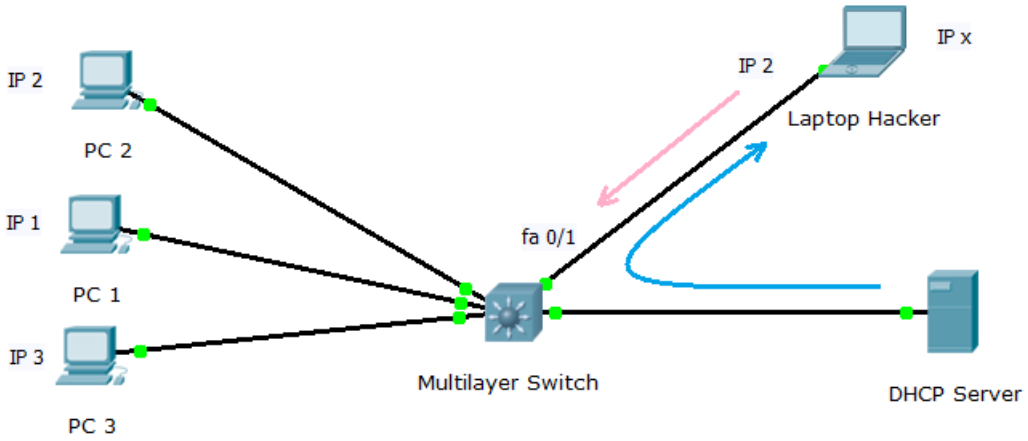
به خروجی دستور IP DHCP Snooping Show در این مثال توجه کنید :

DHCP Snooping Status Display

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
104
Insertion of option 82 is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
FastEthernet0/35             no          3
FastEthernet0/36             no          3
GigabitEthernet0/1           yes         unlimited
Switch#
```

IP Source Guard :

در حالت عادی هر کدام از کامپیوترها در هنگام ارسال اطلاعات ، آدرس IP خود را به عنوان Source IP در داخل پیام قرار می دهند . حال اگر یک فرد هکر آدرس IP خود را مخفی کند و از آدرس IP یک کامپیوتر دیگر استفاده کند می تواند به تمامی اطلاعات ردوبدل شده دستیابی پیدا کند . برای مثال به شکل زیر توجه کنید ، شخص هکر آدرس IP خود را (IP x) مخفی کرده و با استفاده از آدرس IP کامپیوتر 2 (یعنی IP 2) به DHCP Server پیام می فرستد و درخواست اطلاعات می کند و در مقابل DHCP Server به درخواست مزبور پاسخ می دهد و اطلاعات را در اختیار آن می گذارد و شخص هکر می تواند با استفاده از این اطلاعات و آدرس IP کامپیوتر 2 در شبکه خرابکاری کند .



سوئیچ های کاتالیست سیسکو می توانند از یک ویژگی به نام IP Source Guard برای شناسایی حملاتی شبیه به مورد فوق استفاده کنند . همانطور که می دانید سوئیچ های لایه 2 آدرس های MAC مربوط به دستگاه های متصل به پورت های خود را در داخل جدول CAM به ثبت میرسانند . ویژگی IP Source Guard از اطلاعات جمع آوری شده توسط ویژگی DHCP Snooping استفاده کرده و بدین ترتیب از آدرس های MAC متناظر با آدرس های IP کلاینت ها آگاه می شود (زیرا ویژگی DHCP Snooping آدرس های MAC و IP متناظر با آنها را در داخل جدولی به ثبت می رساند) . در این صورت پاکت های دریافت شده توسط یک پورت به صورت زیر مورد بررسی قرار می گیرد :

- آدرس Source IP مربوط به پیام باید برابر با آدرس IP کسب شده توسط ویژگی DHCP Snooping و یا آدرسی که به صورت دستی تعیین گشته است باشد .
- آدرس Source MAC مربوط به پیام باید برابر با آدرس MAC کسب شده توسط ویژگی DHCP Snooping باشد .

Switch (config) # Interface type mod/num

Switch (config – if) # IP Verify Source [Port – Security]

در مورد کامپیوترهایی که از DHCP استفاده نمی کنند و به صورت دستی به آنها آدرس IP و غیره را داده ایم باید با دستور زیر این اطلاعات را در داخل جدول DHCP Snooping Binding قرار دهیم :

Switch (config) # IP Source Binding mac – address VLAN vlan – id ip – address Interface type mod/num

به منظور مشاهده وضعیت مربوط به ویژگی IP Source Guard از دستور زیر استفاده می کنیم :

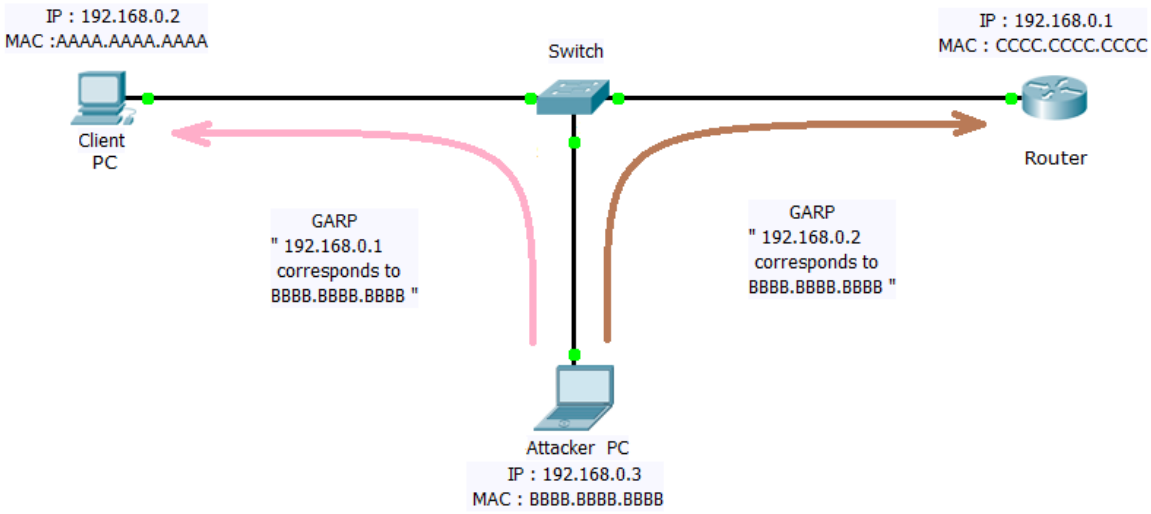
Switch # Show IP Verify Source [Interface type mod/num]

به منظور مشاهده محتویاتی که به صورت دستی یا دینامیک در داخل جدول DHCP Snooping Binding قرار گرفته اند از دستور زیر استفاده می کنیم :

Switch # Show IP Source Binding [mac – address] [DHCP – Snooping | Static] [VLAN vlan – id] [ip – address] [Interface type mod/num]

Dynamic ARP Inspection (DAI) :

معمولا دستگاه ها در هنگام ارسال اطلاعات به سمت مقاصد خود در صورت اطلاع نداشتن از آدرس MAC دستگاه Next – Hop ، از پروتکل ARP استفاده می کنند . در این صورت پیام ARP Request ارسال شده و آدرس MAC گنجانده شده در داخل پیام های ARP Reply در داخل جدول ARP به ثبت می رسد . این پروسه در شرایط عادی بسیار خوب انجام شده و به نتیجه خواهد رسید . اما فرض کنید که یک فرد هکر دستگاه خود را به شبکه متصل کرده و پیام های ARP Request کلاینت ها را دریافت و پاسخ ARP Reply را به سمت آنها ارسال کند .



در تصویر بالا مشاهده می کنید که آدرس PC برابر با 192.168.0.2 و آدرس Default Gateway آن برابر با 192.168.0.1 می باشد . حال Hacker در پاسخ به پرسش ARP کامپیوتر PC برای آگاهی از MAC Address مربوط به Default Gateway یک پاسخ ARP جعلی با MAC Address خود به سمت PC ارسال خواهد کرد . در این حالت هکر MAC Address کامپیوتر خود را به عنوان Default Gateway به سمت PC ارسال خواهد کرد و PC در جدول ARP Cache خود این آدرس جعلی را به عنوان Default Gateway قرار می دهد . در این صورت کلیه بسته هایی که باید به سمت Default Gateway اصلی ارسال شوند به سمت کامپیوتر هکر ارسال خواهد شد و هکر بعد از دریافت بسته هایی که قرار نبود به دست او برسد آنها را بررسی کرده و اطلاعات مورد نظر را بدست خواهد آورد . فرد هکر در نهایت بسته ها را به سمت مقصد صحیح خود ارسال می کند و چیزی که در این بین اتفاق افتاده است ، از دید دیگر کلاینت ها مخفی خواهد ماند.

این نوع حملات به نام ARP Poisoning یا ARP Spoofing نامیده می شوند . سوئیچ های کاتالیست سیسکو با استفاده از ویژگی (Dynamic ARP Inspection (DAI می توانند از بروز حملاتی شبیه به این ممانعت به عمل آورند . شبیه به DHCP Snooping ، ویژگی DAI نیز پورت های سوئیچ را به صورت Trusted و Untrusted طبقه بندی می کند . بدین ترتیب سوئیچ مجبور خواهد بود تا تمامی پیام های ARP دریافت شده از طریق پورت های Untrusted را مورد بررسی قرار دهد . زمانی که یک پورت Untrusted پیام

ARP را دریافت می کند ، آدرس MAC و IP مربوط به آن را با اطلاعات صحیح بدست آمده مقایسه می کند . در صورتی که اطلاعات گنجانده شده در داخل پیام های ARP Reply مغایر با اطلاعات صحیح بوده و یا با موارد موجود تداخل داشته باشد ، پاکت مزبور از بین رفته و یک پیام Log نشان داده خواهد شد .

پیکربندی (Dynamic ARP Inspection (DAI :

Switch (config) # IP ARP Inspection VLAN vlan – range

Switch (config) # Interface type mod/num

Switch (config – if) # IP ARP Inspection Trust

در صورتی که کامپیوترهایی با آدرس های استاتیک داشته باشیم می توانید از ترکیب دستورات زیر استفاده کنید :

Switch (config) # ARP Access – List acl – name

Switch (config – nacl) # Permit IP Host sender – ip MAC Host sender – mac [Log]

Switch (config – nacl) # Exit

Switch (config) # IP ARP Inspection Filter arp – acl – name VLAN vlan – range [static]

برای حصول اطمینان از اینکه آیا پیام ARP Reply واقعا از سوی آدرسی که در داخل آن قرار داده شده است ارسال شده یا نه ، می توان دستور زیر را اجرا کرد :

Switch (config) # IP ARP Inspection Validate { [src – mac] [dst – mac] [ip] }

Securing With VLANs

: Vlan Access – List (VACL)

پاکت هایی که در داخل یک VLAN مانده و به سمت VLANهای دیگر فرستاده نمی شوند را نمی توان با استفاده از ACLهای عادی تحت کنترل درآورد . زیرا این اطلاعات از یک پورت سوئیچ به پورتی دیگر ارسال نمی شوند یعنی داخل یک VLAN قرار دارد و از یک VLAN به VLAN دیگر نمی رود و بنابراین نمی توان یک ACL را بر روی آنها اعمال کرد .در این بین VACLها را می توان برای در اختیار داشتن همین امکان مورد استفاده قرار داد . با اینکه VACLها متفاوت از RACLها یا همان ACLهای معمولی می باشند ، اما با استفاده از آنها نیز می توان ترافیک مورد نظر را بلوکه کرده و یا امکان انتقال آنها را فراهم ساخت .

باید یک نقشه از VLAN را تعریف کنیم . دستورات زیر برای تعریف نقشه VLAN مورد استفاده قرار می گیرند :

Switch (config) # VLAN Access – Map map – name [sequence – number]

Switch (config – access – map) # Match IP – Address { Acl – name | Acl – number }

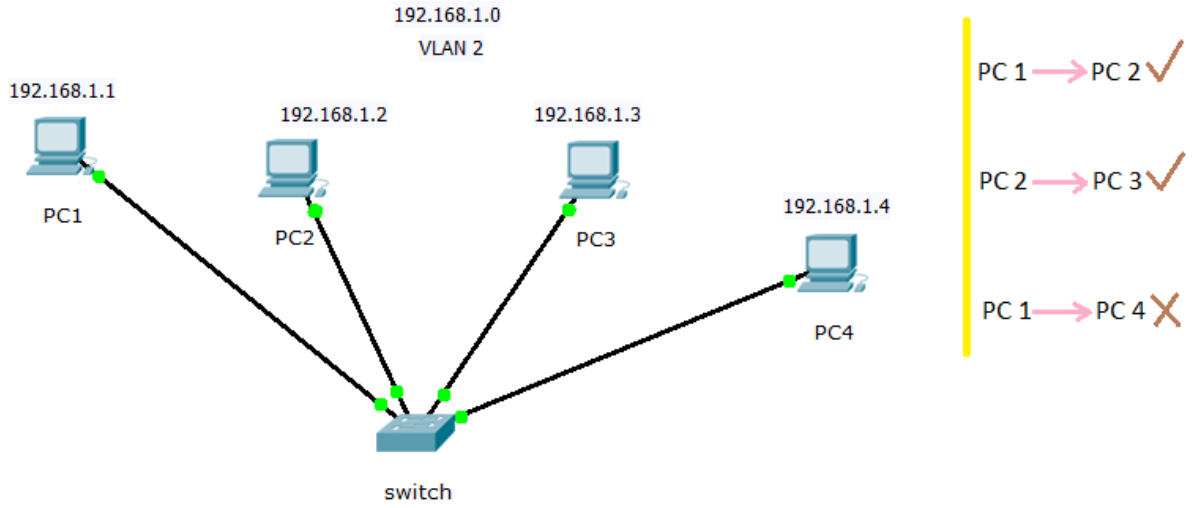
Switch (config – access – map) # Action { Forward | Drop | Redirect type mod/num }

اگر از پارامتر Redirect در دستور فوق استفاده کنیم سوئیچ ترافیک ورودی را که برای اینترفیس خاصی آمده را به اینترفیسی که در دستور Redirect تعیین کرده ایم ارسال می کند و یک پیام می گذارد .

در نهایت باید VACL را در مورد یک VLAN خاص فعال سازیم . این کار با اعمال دستور زیر انجام می گیرد :

Switch (config) # VLAN Filter map – name VLAN – List vlan – list

مثال : با توجه به شکل زیر دستورات را می نویسیم :



اول Access – List را می نویسیم :

Switch (config) # Access – List 100 Permit IP Host 192.168.1.1 Host 192.168.1.2

Switch (config) # Access – List 101 Permit IP Host 192.168.1.1 Host 192.168.1.4

Switch (config) # Access – List 102 Permit IP Host 192.168.1.2 Host 192.168.1.3

Access – Map را می نویسیم تا نقشه VLAN را ترسیم کنیم :

Switch (config) # VLAN Access – Map Cisco 10

Switch (config – access – map) # Match IP – Address 100

Switch (config – access – map) # Action Forward

Switch (config – access – map) # Exit

Switch (config) # VLAN Access – Map Cisco 20

Switch (config – access – map) # Match IP – Address 101

Switch (config – access – map) # Action Drop

Switch (config – access – map) # Exit

```
Switch ( config ) # VLAN  Access – Map  Cisco  30
Switch ( config – access – map ) # Match  IP – Address  102
Switch ( config – access – map ) # Action  Forward
Switch ( config – access – map ) # Exit
Switch ( config ) # VLAN  Access – Map  Cisco  40
Switch ( config – access – map ) # Action  Drop
Switch ( config – access – map ) # Exit
```

حال VACL را بر روی VLAN 2 اعمال می کنیم :

```
Switch ( config ) # VLAN  Filter  Cisco  VLAN – List  2
```

دستور مشاهده VACL :

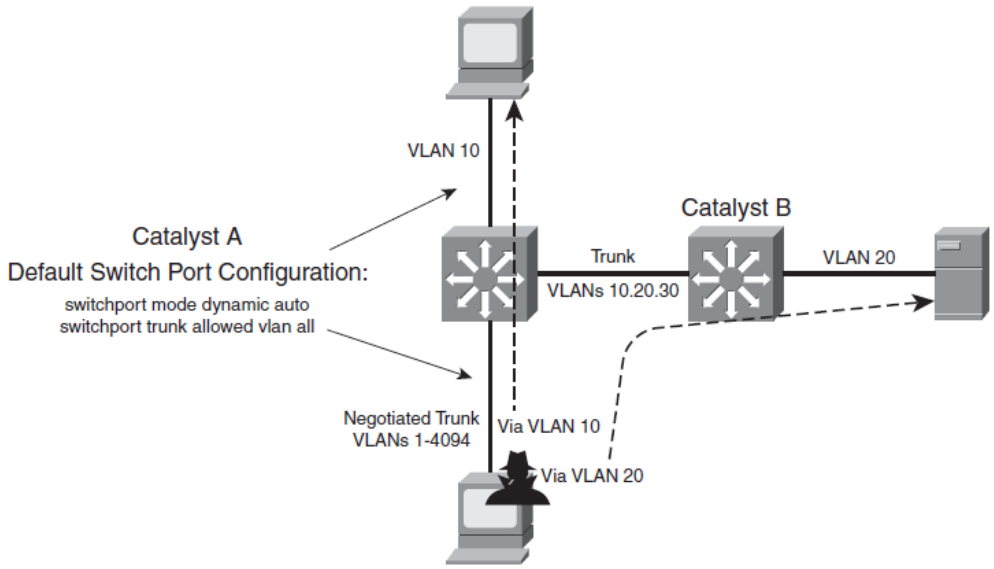
```
Switch # Show  VLAN  Access – Map
```

امن کردن اتصالات Trunk :

سوئیچ های سیسکو می توانند با استفاده از پروتکل DTP اقدام به ایجاد اتوماتیک اتصالات Trunk با یکدیگر نمایند . با اینکه بهره گیری از این پروتکل می تواند بار مدیریتی شبکه را کاهش دهد ، اما امکان سوء استفاده افراد خرابکار از آن را نیز فراهم می سازید . به صورت پیش فرض وضعیت این پروتکل در روی پورت های سوئیچ برابر با Auto قرار داده شده است . که در این شرایط ، اگر سوئیچی دیگر درخواست خود مبنی بر ایجاد اتصال Trunk را برای پورت مزبور ارسال نماید ، اتصال trunk مابین آن دو پورت به صورت اتوماتیک برقرار خواهد شد .

در شرایط عادی هر کدام از پورت های سوئیچ که در وضعیت Access قرار دارند به یک کامپیوتر متصل می باشند . اگر فردی خرابکار در پشت یکی از کامپیوترها قرار داشته باشد و با استفاده از نرم افزارهای خاصی ، می تواند از پروتکل DTP و وضعیت پیش فرض پورت های سوئیچ سوء استفاده کند و درخواست

خود مبنی بر ایجاد اتوماتیک اتصال Trunk را برای پورت سوئیچ بفرستد . در چنین شرایطی می توان اینگونه بیان کرد که کامپیوتر مزبور خود را به جای یک سوئیچ قرار داده است .



An Example of Switch Spoofing to Gain Access to a Trunk

بعد از برقراری اتصال trunk ، فرد هکر می تواند تمامی اطلاعات مربوط به کلیه VLANهایی که مجاز به استفاده از اتصال trunk هستند را دریافت کند . همچنین می تواند ترافیک مورد نظر خود را به سمت همه VLANها ارسال کند . شکل صفحه قبل این سناریو را نشان می دهد .

برای پیش گیری از وقوع این نوع از حملات می توان پورت های سوئیچ که به کامپیوترها متصل می شود را به صورت دستی در حالت Access قرار دهیم و تمامی پورت های آزاد سوئیچ را غیرفعال کنیم تا امکان متصل شدن هیچ دستگاهی به آنها وجود نداشته باشد .

پیکربندی پورت های سوئیچ به حالت Access :

Switch (config) # Interface type mod/num

Switch (config – if) # Switchport Access VLAN vlan – id

Switch (config – if) # Switchport Mode Access

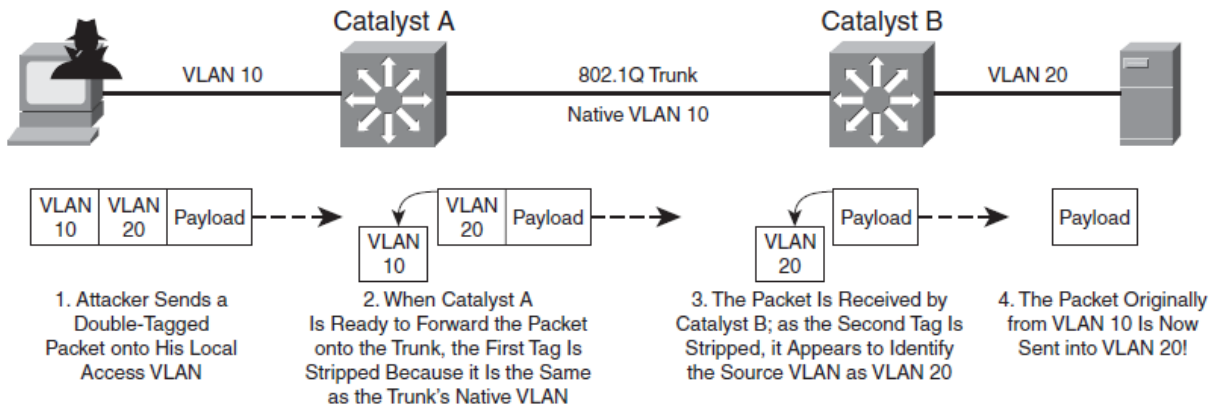
دستور نمایش وضعیت پورت :

Switch # Show Interface type mod/num Switchport

VLAN Hopping :

در این نوع از حملات فرد هکر اقدام به دستکاری 802.1q tagها نموده و بدین ترتیب شماره VLAN گنجانده شده در داخل فریم ها را با شماره مورد نظر خود تعویض می نماید . در نتیجه این کار ، سوئیچ دریافت کننده پیام فرض را بر آن خواهد گذاشت که این پیام از یک VLAN دیگر ارسال شده است که در حقیقت چنین نیست .

شکل زیر مکانیسم انجام این حمله را نشان داده است :



VLAN Hopping Attack Process

در این مثال فرد هکر در داخل VLAN 10 قرار داشته و پیام هایی به صورت Double Tagged (یعنی عملیات 802.1q tagging دو بار بر روی فریم انجام شده است) ایجاد و ارسال می کند . در حقیقت این فرد هکر به یک اتصال trunk متصل نشده است اما به منظور فریب دادن سوئیچ طوری وانمود می کند که دارای یک اتصال trunk با سوئیچ می باشد .

در این حالت اولین Tag شماره VLAN 20 می باشد که مقصد است اما دومین Tag حاوی شماره مربوط به VLAN 10 است که فرد هکر در آن قرار دارد . در این حالت سوئیچ A بعد از دریافت این فریم از سوی هکر ، اقدام به هدایت آن از طریق پورت trunk خواهد کرد . اما به دلیل آنکه شماره VLAN 10 واقع در اولین Tag برابر با Native VLAN مربوط به اتصال trunk است بنابراین سوئیچ A قبل از هدایت فریم در اتصال trunk این tag را از روی فریم برخواهد داشت .

سوئیچ A با انجام این کار تصور می کند که فریم مزبور دیگر دارای tag نیست در حالی که فریم یاد شده باز هم از یک tag دیگر برخوردار می باشد . در سوی دیگر سوئیچ B این پیام را دریافت کرده و با بررسی tag آن متوجه می شود که این پیام باید از طریق VLAN 20 به مقصد خود هدایت شود . اما می دانید که این tag توسط فرد هکر در داخل فریم گنجانده شده است . در نتیجه این پروسه پیام ها به مقصدی که مورد نظر فرد هکر بود فرستاده خواهد شد .

کاملا واضح است که دلیل بروز این نوع حملات استفاده از Native VLAN های بدون tag است . برای جلوگیری از بروز این نوع از حملات باید یکی از دو روش زیر را در مورد اتصالات trunk اعمال کنید :

- شماره Native VLAN را برابر با یکی از VLANهای آزاد که مورد استفاده ای ندارد قرار دهید . این کار باید بر روی هر دو دستگاه که در برقراری اتصال trunk شرکت دارند انجام شود .

- روش دیگر مجبور کردن سوئیچ به tag دار کردن فریم های مربوط به Native VLAN است .

برای مجبور ساختن سوئیچ به tag دار کردن فریم های مربوط به Native VLAN در روی تمامی اتصالات trunk از دستور زیر استفاده می کنیم :

```
Switch ( config ) # VLAN  dot 1q  Tag Native
```

: Private VLAN (PVLAN)

با استفاده از ویژگی Private VLAN و بدون نیاز به استفاده از روتر می توانید دستگاه های واقع در داخل یک VLAN را به نواحی ایزوله مختلفی تقسیم کنید .

به عنوان مثال فرض کنید که یک ISP چندین مشتری خود را در داخل یک VLAN قرار داده است که همگی آنها از یک Default Gateway یکسان که در داخل شبکه ISP قرار دارد بهره خواهند گرفت . اما بدیهی است که ترافیک داخلی مربوط به هر کدام از این مشتری ها نباید به سمت مشتری دیگر ارسال شود و همچنین این ترافیک نباید برای سرور واقع در شرکت ISP نیز فرستاده شود .

با کمک Private VLANها می توان این مشکلات را برطرف کنید . در حقیقت هر کدام از VLANهای معمولی می توانند به صورت مجازی به چند ناحیه ایزوله از یکدیگر (Sub – VLAN) تبدیل شوند که به هر کدام از این نواحی Secondary VLAN گفته می شود . بدین ترتیب تمامی دستگاه های واقع در داخل یک Secondary VLAN قادر به برقراری ارتباط با پورت های واقع در Primary VLAN (مانند پورت روتر) بوده اما توانایی این کار را در رابطه با Secondary VLANهای دیگر ندارد . انواع مختلف یک Secondary VLAN به ترتیب زیر است :

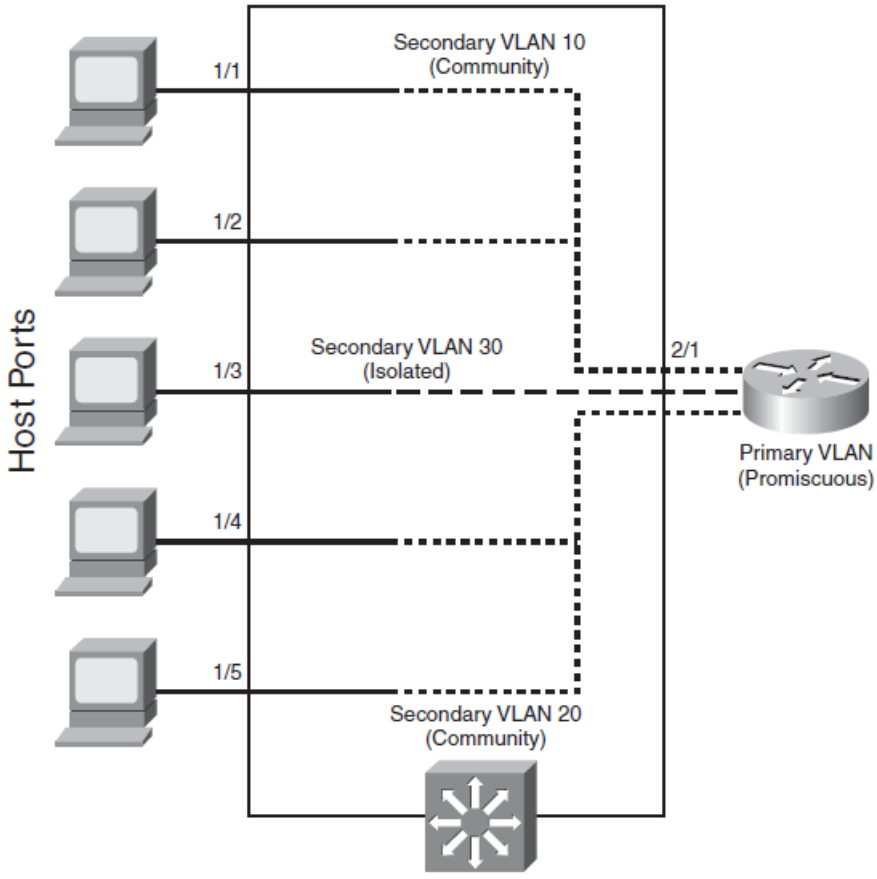
- **Isolated** : در صورتی که پورتی از سوئیچ در داخل یک Isolated VLAN قرار گرفته باشد ، قادر به دسترسی به پورت های واقع در Primary VLAN بوده اما ارتباطی مابین این پورت با دیگر Secondary VLAN ها برقرار نخواهد کرد .

- **Community** : تمامی پورت هایی که در داخل یک Community VLAN قرار گرفته باشند ، قادر به ارتباط با یکدیگر و Primary VLAN بوده اما ارتباطی مابین این پورت با دیگر Secondary VLANها برقرار نخواهد کرد .

بعد از تعیین کردن نوع هر پورت فیزیکی باید ارتباط آن با دیگر پورت هایی که در سناریوی PVLAN مورد استفاده قرار خواهند گرفت را مشخص سازید . در حالت کلی هر پورت را باید در یکی از انواع زیر تعریف کرد :

- **Promiscuous** : این پورت سوئیچ معمولا به یک روتر و یا فایروال متصل می شود . پورت مزبور باید توانایی ارسال و دریافت پیام های لایه 2 از تمامی پورت های داخل Primary VLAN را داشته باشد .
- **Host** : این پورت معمولا به یک دستگاه کامپیوتر یا هر نوع host دیگر متصل می شوند که هر پورت Host می تواند به یکی از انواع Isolated یا Community وجود داشته باشد .

شکل زیر مثال ساده ای از ارتباط مابین انواع پورت ها در سناریوی PVLAN را نشان می دهد . مشاهده می فرمایید که برخی از کامپیوترها به Community VLAN متصل شده و در این بین یک کامپیوتر نیز به یک Isolated VLAN وصل شده است .



Private VLAN Functionality Within a Switch

پیکربندی (Private VLAN (PVLAN :

در ابتدا اقدام به ایجاد یک یا چند Secondary VLAN مورد نیاز خواهیم کرد :

```
Switch ( config ) # VLAN  vlan – id
Switch ( config – vlan ) # Private – VLAN  { Isolated | Community }
```

در مرحله دوم باید یک Primary VLAN را ایجاد نماییم . Primary VLAN در واقع همان VLAN اصلی می باشد که قرار است با استفاده از ویژگی PVLAN به نواحی (Sub – VLAN) مختلف تقسیم شود . دستورات زیر برای تعریف یک Primary VLAN مورد استفاده قرار می گیرد :

```
Switch ( config ) # VLAN  vlan – id
Switch ( config – vlan ) # Private – VLAN  Primary
Switch ( config – vlan ) # Private – VLAN  Association  { Secondary – VLAN – list
| Add  Secondary – VLAN – list  |  Remove  Secondary – VLAN – list }
```

تعیین نقش هر پورت در PVLAN :

در ابتدا با استفاده از دستور زیر نقش هر پورت در یک PVLAN را مشخص نمایید :

```
Switch ( config ) # Interface  type  mod/num
Switch ( config – if ) # Switchport  Mode  Private – VLAN  { Host | Promiscuous }
```

هر کدام از پورت های Host که دستور فوق در روی آنها اجرا شده است را باید متناظر با Secondary – VLAN و Primary VLANهای مربوطه قرار دهید . برای این کار از دستور زیر استفاده می کنید :

```
Switch ( config – if ) # Switchport  Private – VLAN  Host – Association  Primary
– VLAN – id  Secondary – VLAN – id
```

اما در مورد پورت های Promiscuous که دستور صفحه قبل در روی آنها اجرا شده است باید اقدام به پیکربندی Mapping نمایید . برای این کار از دستور زیر استفاده می کنید :

Switch (config – if) # Switchport Private – VLAN Mapping Primary – VLAN – id Secondary – VLAN – id | { Add Secondary – VLAN – list } | { Remove Secondary – VLAN – list }

مثال : به همان شکل دو صفحه قبل توجه فرمایید . در مثال زیر پیکربندی PVLAN در روی سوئیچ را نشان داده ایم :

Configuring Ports with Private VLANs

```
Switch(config)# vlan 10
Switch(config-vlan)# private-vlan community
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan community
Switch(config)# vlan 30
Switch(config-vlan)# private-vlan isolated
Switch(config)# vlan 100
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 10,20,30
Switch(config-vlan)# exit
Switch(config)# interface range fastethernet 1/1 - 1/2
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 10
Switch(config)# interface range fastethernet 1/4 - 1/5
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 20
Switch(config)# interface fastethernet 1/3
Switchconfig# switchport private-vlan host
Switch(config-if)# switchport private-vlan host-association 100 30

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

دستور مانیتورینگ :

Switch # Show VLAN Private – VLAN

متناظر قرار دادن Secondary – VLANها با Primary – VLAN :

در هنگام استفاده از سوئیچ های لایه 3 و پورت های SVI در روی آنها نیاز به انجام مراحل دیگری نیز داریم . فرض کنید که در روی یک سوئیچ اقدام به ایجاد یک Primary – VLAN با شماره 200 کرده ایم . همچنین این سوئیچ دارای یک پورت SVI با آدرس IP مخصوص به خود در داخل VLAN 200 بوده که در عملیات routing شرکت می نماید . در مثال زیر اقدام به ایجاد isolated VLAN 40 و community VLAN 50 کرده و آنها را متناظر با Primary – VLAN 200 قرار داده ایم :

Associating Secondary VLANs to a Primary VLAN SVI

```
Switch(config)# vlan 40
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# vlan 50
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# vlan 200
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 40,50

Switch(config-vlan)# exit
Switch(config)# interface vlan 200
Switch(config-if)# ip address 192.168.199.1 255.255.255.0
```

در این شرایط Primary – VLAN 200 می تواند ترافیک را در سطح لایه 3 انتقال داده ولی Secondary – VLANهایی که در داخل این Primary – VLAN قرار دارند اطلاعات را تنها در سطح لایه 2 انتقال خواهند داد . اما برای امکان پذیر کردن انتقال اطلاعات در سطح لایه 3 در مورد Secondary – VLANها باید اقدام به پیکربندی Mapping در روی پورت SVI نیز بکنید :

Switch (config – if) # Private – VLAN Mapping { Secondary – VLAN – id | Add Secondary – VLAN – list | Remove Secondary – VLAN – list }

در مورد مثال فوق خواهیم داشت :

Switch (config) # Interface VLAN vlan – id

Switch (config – if) # Private – VLAN Mapping 40 , 50

نکته :

باید سوئیچ در Transparent Mode قرار داشته باشد تا بتوانیم ویژگی Private – VLAN را روی آن اجرا کنیم .

Cisco Exams in Arbil

آزمون های سیسکو در اربیل (کردستان / عراق)

- ثبت نام
- رزرو هتل
- رزرو بلیط هواپیما

(برای کسب اطلاعات بیشتر با شماره زیر تماس بگیرید)

ENTRY CCENT NETWORK

ASSOCIATE CCNA NETWORK

PROFESSIONAL CCNP NETWORK

EXPERT CCIE ROUTING & SWITCHING

IRAN : +989127687757
ERBIL : +964 750 530 8221
Kolijis@Yahoo.com
Koliji_Cisco@Yahoo.com
Showan.Koliji

Network Engineer
Showan koliji
Cisco live!

Network Engineer
IRAN : +989127687757
ERBIL : +964 750 530 8221
Kolijis@Yahoo.com
Showan.Koliji

Showan koliji