شبکه های محلی مجازی

VLan

تهیه و تنظیم : محمدی

باشگاه مهندسان ایران

گروه مهندسی کامپیوتر

تابستان 88

فهرست عناوین

مقدمه	4
آشنایی با مفهوم VLAN	5
VLANها در مقایسه با Subnet ها	6
مزایای VLAN	8
اجزای VLAN	9
سویچ هایی که از VLAN پشتیبانی می کنند	12
عضویت در یک VLAN	12
روش های پیکربندی VLAN	14
انواع اتصالات VLAN	18
اتصالات Access Link	18
اتصالات Trunk	19
تعریف Trunking	19
مقدمات Trunking	20
پیکربندی یک Trunk	21
تکنولوژی های VLAN	24
ISL	24

802.1Q	26
VLAN Trunk Protocol	30
حالت های VTP	30
پیام های VTP	32
VTP pruning	35
نمونه ای از پیکربندی یک VLAN (در سوئیچ 2950)	38
منابع و ماخذ	42

مقدمه

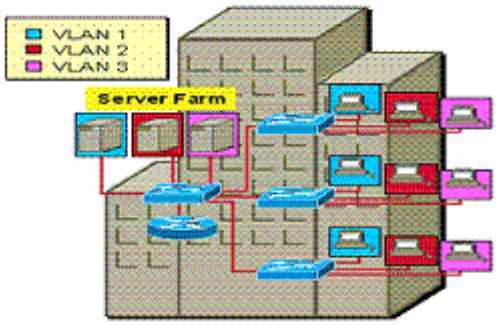
بیشترین سرمایه گذاری ها به سمت نمونه های شبکه ای سوئیچی حرکت کرده اند ، شبکه هایی که در آن کامپیوترها به پورت های تعیین شده روی سوئیچ های Ethernet ، سوئیچ های Gigabit Ethernet ، سوئیچ های ATM ، یا سایر انواع سوئیچ ها متصل شده اند .

دستگا های سوئیچ طراحی های شبکه ای را به شکلی که در آن شبکه کلی یک شبکه بزرگ مسطح (flat) است و در نقطه مقابل بسیاری از زیرشبکه هاست که به وسیله روترها به همدیگر متصل شده اند ، پشتیبانی می کنند . هر کامپیوتر می تواند با دیگری به صورت مستقیم ارتباط برقرار کند . این شبکه ها مزیت ها و معایبی دارند . یکه شبکه یکنواخت به آسانی همه سیستم ها را داخل یک Broadcast Domain به همدیگر متصل می کند ، اما وجود تنها یک Broadcast Domain زیان هایی مرتبط با امنیت ، مسایل ترافیکی شبکه ، و فقدان مدیریت محلی دارد .

Virtual LANs یا VLAN ها راهکاری برای حل این مشکلات فراهم کرده اند.

آشنایی با مفهوم VLAN

LAN مجازی که VLAN نیز نامیده می شود، زیرگروهی منطقی درون یک شبکه محلی است که به جای جابه جایی دستی کابل ها برای سیم کشی بین آنها، از طریق نرم افزار ایجاد شده است . VLAN ایستگاه های کاربری و دستگاه های شبکه را بدون توجه به سگمنت فیزیکی LAN ای که به ان متصل اشده اند ، درون یک واحد مجزا ترکیب می کند و به ترافیک اجازه می دهد به شکل کاراتری درون شبکه جریان یابد. هر VLAN در واقع یک شبکه می باشد که هر کدام از آنها ، یک Broadcast Domain جداگانه هستند .به عبارت دیگر یک VLAN شامل مجموعه ای از دستگاه هایی است که داخل یک Broadcast Domain قرار دارند می شود . یک پیام Broadcast که از یک VLAN ایجاد می شود ، به VLAN های بعدی عبور داده نخواهد شد .



مثال ساده ای از VLAN

VLAN ها در پورت سوئیچ های LAN پیاده سازی میشوند ، و معمولا راه حل های اختصاصی برای آن ارایه داده شده است . VLANها زمانی را که برای جابه جایی ، اضافه کردن و تغییرات در شبکه می شود را کاهش می دهد .

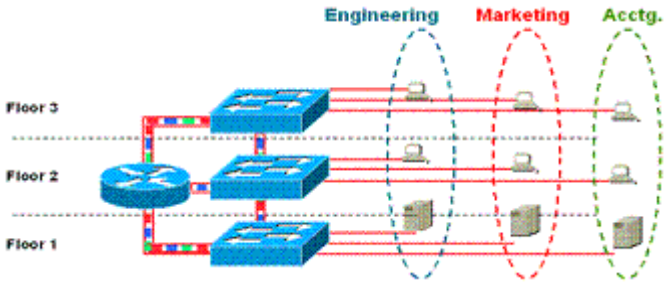
سوئیچ ها در ایجاد VLANها در جایی که امکان استفاده از روترهایی با پورت های بیشتر وجود نداشته باشد ، بسیار مفید خواهند بود .

VLANها در لایه دو عمل می کنند ، از آن جایی که هدف آنها مجزا کردن ترافیک از طریق VLANاست ، به جای استفاده از Bridge (پل) برای اتصال یک VLAN به دیگری ، به یک روتر نیاز است. روتر در لایه 3 و بالاتر پروتکل شبکه کار می کنند ، که نیازمند این است که سگمنت های لایه شبکه شناخته شوند و با VLANها هماهنگ شوند ، که این کار کمی پیچیده است . در این مقاله نگاهی کوتاه به VLANها خواهیم داشت .

VLANها در مقایسه با Subnet ها

تعریف VLAN را دیدیم . استفاده از VLAN همان هدفی را دنبال می کند که تقسیم بندی شبکه به اجزای کوچکتر و با آدرس های لایه سوم همان هدف را دنبال می کند . با این تفاوت که VLAN قابلیت انعطاف زیادی داشته و دستگاه هایی که عضو یک VLAN می باشند به صورت فیزیکی در هر جایی از یک Broadcast Domain حضور داشته باشند . این بدین معنی است که می توان یک کاربر را از یک سوئیچ به سوئیچی

دیگر البته در همان Broadcast Domain انتقال داد . بدون اینکه عضویت آن کاربر در آن VLAN از بین برود. مثلا از یک طبقه با طبقه ای دیگر . تنها محدودیت این انتقال این است که کاربر به هر قسمتی انتقال داده می شود ، باید متصل به همان شبکه لایه دوم باشد .



برداشتن مرزهای فیزیکی با استفاده از VLAN

- سیسکو ، تعداد دستگاه هایی که می توان در یک VLAN قرار داد به شکلی که کارایی شبکه پایین نیاید را تعیین کرده است . این تعداد ممکن است در دستگاه های غیر سیسکو متفاوت باشد .

تعداد دستگاه	پروتکل
500	IP
300	IPX
200	NetBIOS
200	AppleTalk
200	شبکه های دارای پروتکل های مختلط

مزایای VLAN

VLAN بسیاری از مزایای محیط اینترنت که هزینه های اجرایی را کاهش می دهند را فراهم می کند .-- اعضای یک گروه VLAN می توانند از نظر جغرافیایی پراکنده باشند ، اعضا ممکن است به جای مکان فیزیکی محل کارشان به عملکرد شغلشان یا نوع داده ای که استفاده می کنند مرتبط باشند .

- **قدرت VLAN ها از این حقیقت که افزودن ، جابه جایی ، و تغییرات می توانند به سادگی با پیکربندی یک پورت داخل یک VLAN مناسب به انجام برسند ناشی می شود . کابل کشی دوباره برای توسعه اتصال در یک محیط LAN سوئیچی ، یا پیکربندی دوباره میزبان و آدرس دهی دوباره که گران و زمان – بر هستند دیگر لازم نیستند ، چرا که مدیریت شبکه می تواند منطقا به صورت " drag and drop " کردن یک کاربر از گروه VLAN به دیگری استفاده کند .**

مدیریت و کنترل بهتر عمل broadcast – یک VLAN مشکلات مقیاس پذیری که اغلب در یک شبکه بزرگ flat یافت می شود را بوسیله شکستن یک Broadcast Domain به چندین Broadcast Domain یا گروه های VLAN حل می کند . همه ترافیک Broadcast و Multicast درون هر یک از Domain های کوچکتر جای داده می شوند .

امنیت شبکه محکم تر با تاسیس گروه های کاربری ایمن :

- **کاربران با امنیت بالاتر می توانند در یک گروه VLAN جداگانه قرار گیرند ، بنابراین اعضای غیر–گروه Broadcast های آنها را دریافت نخواهند کرد و نمی توانند با آنها ارتباط برقرار کنند .**
- **اگر ارتباط بین VLAN ای لازم است ، یک روتر می تواند اضافه شده ، و اعمال سنتی امنیتی و فیلترینگ یگ روتر می تواند به کار برده شود .**
- **سرورهای گروه کاری می توانند در مکان های ایمن و متمرکز فرار گیرند .**

مقیاس پذیری و کارایی – گروه های VLAN می توانند براساس هرگونه شرایط و معیاری تعریف شوند ؛ از این رو شما می توانید الگوهای ترافیک و کاربران وابسته و منابع یک شبکه را به صورت منطقی تعیین کنید . برای مثال ، یک مهندس که استفاده فشرده و زیاده از یک سرور شبکه ای CAD/CAM می کند می تواند داخل یک گروه VLAN جداگانه که فقط شامل مهندش و سرور است قرار داده شود . مهندس تاثیری بر باقی گروه کاری ندارد . LAN اختصاص داده شده به مهندس توان عملیاتی سرور CAD/CAM را افزایش می دهد و به کارایی باقی گروه با تاثیر نگذاشتن در کارشان کمک می کند .

اجزای VLAN

پنج جزء کلیدی درون VLAN ها وجود دارد :

سوئیچ ها –– برای تعیین عضویت VLAN . اینجا جایی است که کاربران/سیستم ها به شبکه متصل می شوند .

Trunking – برای تبادل اطلاعات VLAN درون شبکه. Trunking برای محیط های بزرگتر که شامل سوئیچ ها ، روترها ، و سرورهای متعددی هستند ضروری است .

مسیریابی چند–پروتکلی – برای پشتیبانی از ارتباطات درون–VLAN ای . به یاد داشته باشید که تا زمانی که همه اعضای درون یک VLAN هستند می توانند مستقیما با دیگری ارتباط برقرار کنند، روترها برای تبادل اطلاعات بین VLAN های متفاوت مورد نیاز هستند .

سرورها – سرورها صریحا درون محیط های VLAN لازم نیستند ؛ به هر حال ، آنها جزء اصلی درون هر VLAN هستند . درون یک محیط VLAN ریال کاربران می توانند از سرورها به روش های متفاوتی استفاده کنند . از آنجایی که VLAN ها در سراسر شبکه استفاده شده اند ، کاربران احتمالا از چندین VLAN به سرویس های آنها نیاز خواهند داشت .

Server Communication

مدیریت – برای امنیت ، اداره ، و کنترل درون یک شبکه . مدیریت و اداره موثر درون هر محیط شبکه ای کاملا ضروری است ، و برای شبکه هایی که از VLAN ها استفاده می کنند مهم تر و ضروری تر می شود . سیستم مدیریت شبکه سگمنت های منطقی درون شبکه سوئیچی را تشخیص و مدیریت می کند .

Centralized Administration

سویچ هایی که از VLAN پشتیبانی می کنند :

اگر بخواهیم چند نمونه از محصولات سیسکو که از VLAN پشتیبانی می کنند را ذکر کنیم می توانیم به :

- **Cisco Catalyst 6000, 4500, 4000 series switches that run Cisco IOS**
- **Cisco Catalyst 3750, 3750E, 3560, 3560E, 3550, 2970, 2960, 2955, 2950, and 2940 series switches**

اشاره کنیم .

علاوه بر سیسکو شرکت های دیگری نیز هستند که محصولاتی تولید می کنند که از VLAN ها پشتیبانی می کنند . برای مثال شرکت HP که سوئیچ Procurve 2524 آن از VLAN پشتیبانی می کند .

عضویت در یک VLAN

دو روش برای عضویت یک دستگاه در یک VLAN وجود دارد : استاتیک و داینامیک . این روش ها تعیین کنند نوع عملکرد سوئیچ در تخصیص پورت های خود به VLANها می باشند .در روش استاتیک ، با استفاده از دستوراتی که در Interface subcinfiguration mode اجرا می شوند. یک پورت سوئیچ را معادل یک VLAN قرار می دهیم . بنابراین هر دستگاهی که به آن پورت متصل شود ، عضو یک VLAN

خواهد بود . VLAN هایی که به این طریق ایجاد می شوند port-based VLANs نامیده می شوند .

در روش داینامیک ، عضویت یک دستگاه در یک VLAN بطور خودکار و از روی آدرس های MAC و یا ادرس IP و نیز اطلاعات مربوط به کاربر مانند نام ، گروه وابسته و غیره تعیین خواهد شد. در این روش یک سوئیچ که VMPS نامیده می شود در شبکه بکار گرفته خواهد شد که مسئول ارایه اطلاعاتی در مورد VLAN ها و دستگاه های مربوطه می باشد . یکی از سوئیچ های موجود در شبکه را به عنوان VMPS انتخاب می کنیم . سوئیچ های 1900 و 2950 قادر به ایفای نقش به عنوان VMPS نبوده ، اما سوئیچ هایی مثل مدل های Catalyst 6500 می توانند وظایف VMPS را برعهده داشته باشند . در این صورت دستگاه های 1900 و 2950 به عنوان Client عمل می کنند .و سوئیچ هایی ماند 6500 که به عنوان VMPS می باشند نیز حاوی اطلاعاتی در مورد چگونگی عضویت دستگاه های مختلف در VLAN ها خواهند بود .

روش داینامیک یک برتری مهم نسبت به روش استاتیک دارد و انهم این است که روش داینامیک ، از خصوصیت plug-and-play پشتیبانی می کند. برای مثال اگر در شبکه ای که از VLAN های داینامیک استفاده می گردد دستگاهی را از یک پورت سوئیچ به پورت سوئیچ دیگر انتقال دهیم ، پورت جدید خود را با VLAN مربوط تطبیق خواهد داد و تنها موردی که مجبور به تغییر در پیکربندی VLAN ها در روش داینامیک

خواهیم بود زمانی است که اقدام به استخدام یک نفر و یا اخراج آن کرده باشیم و یا مسئولیت کاربری تغییر کرده باشد . اما در روش استاتیک علاوه بر انجام دادن عملیات گفته شده در مورد کاربران جدید ، در مواقعی که اقدام به تغییر مکان کاربری نیز بکنیم ، مجبور به پیکربندی دوباره مربوط به VLAN آن کاربر در روی پورت جدید خواهیم بود .

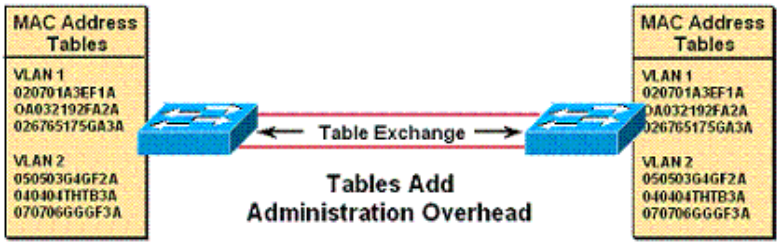
* در ادامه بحث را تحت عنوان روش های پیکربندی VLAN بیشتر بررسی می کنیم .

روش های پیکربندی VLAN

معماری های سوئیچینگ نمونه کاملی برای ایجاد VLAN ها هستند . VLAN های اولیه به صورت دستی پیکربندی می شدند ، سپس ، همچنانکه تکنولوژی VLAN بهتر درک می شد و عمومی تر می شد ، تکنیک های پیشرفته تر ی به کار برده شدند . این بخش تکنیک های متنوعی که می تواند برای ساختن VLAN استفاده شود را توصیف می کند . برای مثال ، پیشرفته ترین روش ها متکی بر پروتکل IP هستند ، اما شبکه هایی که از هر دو پروتکل های IP و پروتکل های nonroutable ، NetBIOS ، استفاده می کنند ممکن است نیاز به استفاده از روش های مبتنی بر MAC (MAC-base) پیدا کنند.

اگر بخواهیم اشاره کوتاهی به این روش ها داشته باشیم می توان به :

- **روش های پیکر بندی پورت : این روش واقعا راهی برای پیکربندی LAN های جداگانه درون یک چهارچوب یکسان است . LAN های ناشی شده به صورت تکنیکی VLAN نیستند و چون که انها به صورت پیکربندی های سیم کشی شده ای پیمربندی شده اند .**
- **MAC-Based VLANs: مدیر شبکه در اصل یک جدول ایجاد می کند که تعیین می کند چه MAC آدرسی به چه VLAN ای متعلق است . در مقایسه با روش پیکربندی پورت ، این روش قابلیت های صحیح VLAN را فراهم می کند چرا که عضویت در VLAN مستقیما به پورت خاصی از سخت افزار وابسته نیست .**



پیکربندی در نرم افزار انجام شده و یک کامپیوتر می تواند به دو یا چند VLAN متعلق باشد . بعلاوه اگر یک کامپیوتر به مکان دیگری منتقل شود ، همچنان آن کامپیوتر به همان LAN متعلق است چرا که آدرس MAC آن همراهش جابه جا شده است.

- VLAN های لایه 3 : این نوع VLAN ها اطلاعات لایه 3 را که مبتنی بر پروتکل آدرس اینترنتی است برای ساختن LAN ها استفاده می کند . یک سوئیچ لایه 3 قادر به جستجوی یک آدرس شبکه موجود در فریم داخل یک جدول است ، و فریم را بر اساس اطلاعات آدرس شبکه ای در جدول که با آدرس فریم مطابقت دارد به VLAN مناسب ارسال می کند . همانند VLAN های MAC based ، جابه جایی آسان است چرا که پورت ایستگاه کاری عضویت VLAN را تعیین می کند . به هر حال ، تکیه بر آدرس لایه 3 می تواند باعث مشکلات کارایی شود .
- IP Multicast VALNs : در این روش ، یک VLAN با عضویت در یک گروه multicast تعریف می شود . IP multicasting راهی برای یک ایستگاه کاری است تا به برخی دیگر ارسال اطلاعات داشته باشد ، اما نه به همه آنها . استفاده از این ویژگی برای ایجاد VLAN ها سودمند و قابل انعطاف است . ایستگاه های کاری که ارسال ها را دریافت می کنند به عنوان گروه multicast شناخته می شوند . multicasting ها بوسیله آدرس های IP کلاس D پیاده سازی می شوند.
- Rules-Based VLANs : برخی کمپانی ها تکنیک های پیکربندی "rules-based" را برای پیاده سازی VLAN استفاده می کنند ، که به مدیران اجازه می دهد VLAN ها را بر اساس اطلاعاتی که در بسته هایی که سوئیچ ها

دریافت و ارزیابی می کنند، ایجاد کنند . این روش عضویت در VLAN را با ایجاد قوانین در نرم افزاری که برای تعیین VLAN به کار می رود تعیین می کند . این روش انعطاف پذیری بسیار زیادی دارد ، اما تنظیم و پشتیبانی آن می تواند پیچیده باشد .

انواع اتصالات VLAN

سوئیچ ها از دو نوع اتصالات در رابطه با VLAN ها استفاده می کنند :

- Access Link
- Trunk

هنگامی که شما می خواهید VLAN ها را پیکربندی و استفاده کنید ، باید در مورد اتصالات VLAN و همچنین چگونگی پیکربندی Interface ها نیز بخوبی آگاه باشید .

اتصالات Access Link

اتصالاتی که از کارت های شبکه استاندارد و از فریم های استاندارد Ethernet استفاده می کنند ، بنام اتصالات Access Link نامیده می شوند . به عبارت دیگر ، در اتصالات Access Link فقط فریم هایی بین سوئیچ ها و طرف دیگر ارتباط ، انتقال و پردازش می شوند که از نوع 802.3 و یا Ethernet II باشند . هر یک از اتصالات Access Link می تواند فقط یک VLAN را پشتیبانی نماید . بعبارتی دیگر ، دستگاه هایی که به این نوع پورت اتصال دارند فقط در یک Broadcast Domain و یا یک VLAN قرار خواهند گرفت . برای مثال اگر ده عدد کامپیوتر را به یک هاب متصل نماییم و آن هاب را هم به یک پورت سوئیچ وصل کنیم ، تمامی ده دستگاه عضو یک VLAN خواهند بود . اما اگر بخواهیم که 6 کامپیوتر عضو یک VLAN و بقیه عضو VLAN های دیگر باشند ، باید یک عدد هاب دیگر تهیه شده و 4 دستگاه بعدی از طریق

آن هاب به پورت دیگر سوئیچ اتصال یابند . بنابراین در اتصالات Access Link هر پورت سوئیچ می تواند فقط یک VLAN را پشتیبانی کند .

اتصالات Trunk

برخلاف Access Link ، این نوع اتصالات می توانند بیش از یک عدد VLAN را از طریق یک ارتباط پشتیبانی نمایند .

آشنایی مختصری با Trunk را در اینجا خواهیم داشت .

تعریف Trunking

در شبکه های بسیار زیادی مدیران ، سوئیچینگ لایه 2 را به عنوان روش انتقال استفاده می کنند . همچنان که این شبکه ها رشد می کنند ، سرانجام شبکه به LAN مجازی یا VLAN تقسیم می شود . بعلاوه تنها تعداد محدودی پورت فیزیکی در سوئیچ های لایه دو در دسترس است . به این معنی که برای رشد یک شبکه چند سوئیچ لایه دو باید به همدیگر متصل شوند . فرایند متصل کردن یک سوئیچ به سوئیچ ، روتر ، یا سرور دیگر به عنوان Trunking شناخته می شود .

مقدمات Trunking

یک Trunk می تواند لینکی بین دو سوئیچ ، یک سوئیچ و یک روتر ، یا یک سوئیچ و یک سرور باشد . Trunk ها ترافیک را برای چند VLAN پشتیبانی می کنند و به مدیر شبکه اجازه می دهند که VLAN ها را روی چند سوئیچ گسترش دهند . علاوه براین ، یک لینک Trunk که یک سوئیچ را به یک روتر متصل می کند مسیریابی درون–VLAN ای را اجازه می دهد . (به یاد داشته باشید که میزبان های متعلق به VLAN های متفاوت تنها از طریق روتر می توانند با همدیگر ارتباط برقرار کنند .) در آخر ، اگر چندین VLAN وجود داشته باشد که باید با یک سرور خاص ارتباط برقار کنند ، یک ،Trunk بین سوئیچ و سرور می تواند برقرار شود . رایج ترین روش ، Trunking بین دو سوئیچ است ، که این روش را در اینجا مورد بحث قرار می دهیم .

از آنجایی که یک Trunk ، ترافیک ، یا فریم ها را از چندین VLAN انتقال می دهد ، سوئیچ باید روشی برای شناسایی اینکه یک فریم به کدام VLAN متعلق است داشته باشد . سیسکو از چهار روش برای شناسایی فریم پشتیبانی می کند .

1–پیوند دورن–سوئیچی سیسکو (ISL) – روش اختصاصی سیسکو که در محیط های

Fast Ethernet ، Gigabit Ethernet ، و EtherChannel بکار می رود .

2–IEEE 802.1Q – روش استاندارد صنعتی Trunking تصویب شده در IEEE، که روی Ethernet، Gigabit Ethernet، وEtherChannel استفاده می شود.

3– 802.10 – روش Trunking اختصاصی سیسکو در محیط های FDDI

4– LAN Emulation (LANE) – استاندارد IEEE برای Trunking در شبکه های ATM (حالت انتقال ناهمزمان)

با استفاده از اتصالات Trunk می توان فقط از طریق یک ارتباط فیزیکی ، ارتباط های مجازی زیادی به ازای هر VLAN ایجاد نمود که دراین صورت این تصور به وجود می آید که چند ارتباط فیزیکی مستقل وجود دارد .

پیکربندی یک Trunk

وقتی که یک Trunk را پیکربندی می کنید ، پنج حالت مختلف برای پورت سوئیچ وجود دارد :

1- auto – این حالت ، حالت پیش فرض برای پورت های Fast Ethernet وGigabit Ethernet است . در این حالت ، اگر دستگاه remote ای که پورت به آن وصل است روی حالت on، یا desirable تنظیم شده باشد یک پورت Trunk می شود .

2- on – این حالت پورت را روی حالت Trunking دائمی تنظیم می کند .

3- Off – این حالت پورت را روی حالت غیر Trunking (non-trunking) دائمی تنظیم می کند .

4- Desirable – این حالت به پورت اجازه می دهد که یک پورت Trunk شود ، اگر دستگاهی که به پورت وصل شده روی حالت desirable ، on ، یا auto تنظیم شده باشد.

5- Nonegotiate – این حالت پورت را در حالت Trunking دائمی تنظیم می کند . (این حالت پورت را از تولید فریم های پروتکل Trunking داینامیک (DTP) ممانعت می کند . فریم های DTP می توانند برای Trunking مذاکره ای (negotiate) روی Fast Ethernet و Gigabit Ethernet با استفاده از استانداردهای ISL ، IEEE 802.1Q به کار برده شوند .)

برای ایجاد یک ارتباط Trunk ، فرمان Set Trunk روی هر دو انتهای ارتباط Trunk استفده می شود . این فرمان یک Trunk را یجاد ، حالت Trunking راتنظیم می کند ، رشته VLAN هایی که از طریق این Trunk عمل انتقال را انجام می دهند را مشخص می کند ، و روش Trunking را نیز انتخاب می کند .

ترکیب این فرمان بدین شکل است :

Console> (enable) set trunk mod_num/port_num [on | off | desirable | auto | nonegotiate] vlan_range [isl | dot1q | dot10 | lane | negotiate]

* با نحوه استفاده این دستور در مثالی که در پایان آمده است بیشتر آشنا می شویم .

جدول زیر چگونگی پیکربندی دو طرف اتصال را در یک اتصال Trunk نشان می دهد .

سوئیچ remote	سوئیچ ما
On , desirable , auto	on
On , desirable , auto	desirable
On , desirable	auto
No-negatiate	No-negatiate

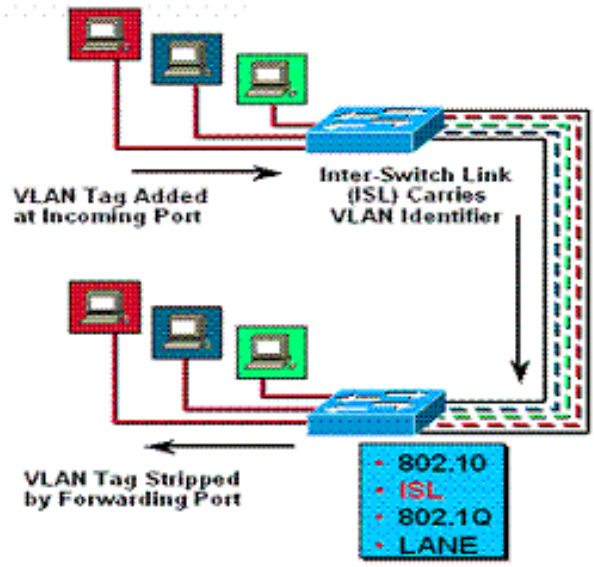
نکته مهمی که از این جدول می توان فهمید این است که در حالت "no-negatiate " پروتکل DTP به کار نرفته است . اما در حالت های "On , desirable , auto " پروتکل DTP مورد استفاده قرار گرفته است . مزیتی که پروتکل DTP دارد این است که در هنگام برقراری ارتباط Trunk این پروتکل قبل از شروع ارتباط وضعیت رو طرف را چک کرده و بنابراین اگر از تنظیمات یکسانی برخوردار نباشند ، نوع اتصال از نوع Access link خواهد بود و Trunk ایجاد نخواهد گردید . مثلا در مواقعی که یک طرف اتصال از ISL و طرف دیگر از 802.1Q پشتیبانی می کنند.

تکنولوژی های VLAN

ISL

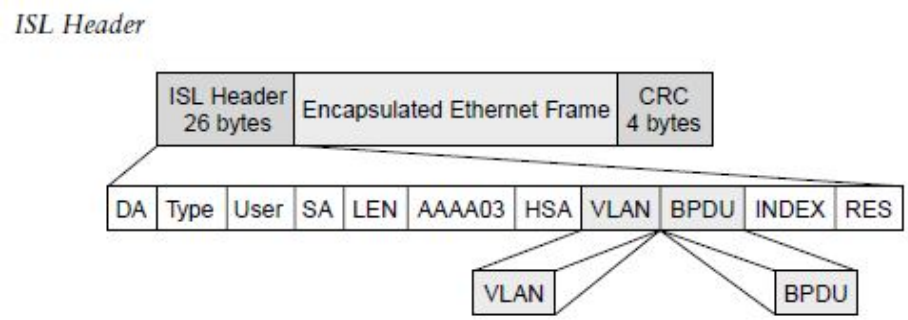
یکی از روش هایی که سیسکو برای عملیات tagging در اتصالات Trunk مورد استفاده قرار می دهد روش ISL است . این زوش در محیط های Ethernet و نیز Token Ring مورد استفاد قرار می گیرد . (به دلیل اینکه امروزه استفاده از Token Ringمحدود شده است ، این روش فقط در محیط های Ethernet بکار می رود.) بجز چند استثنا ، تمامی سوئیچ ها و روترهای سیسکو که از Trunking پشتیبانی می کنند ، قابلیت استفاده از ISL

را نیز دارا هستند . بنابراین قبل از خرید سوئیچ ها و روترها همیشه از امکانات دستگاه و پشتیبانی انها از اتصالات Trunk آگاهی لازم را بیابید.



ISL فریم اصلی Ethernet را به وسیله افزودن 26 بایت به اول و 4 بایت به آخر فریم اصلاح کرده و بنابراین فریم اصلی بین Header و Trailer قرار خواهد گرفت .

شکل زیر نحوه اصلاح فریم اصلی را برای اضافه کردن 30 بایت به آن نشان می دهد .



با توجه به اینکه حداکثر اندازه فریم Ethernet برابر با 1518 بایت است ، با افزوده شدن 30 بایت توسط ISL به فریم Ethernet اندازه آن از مقدار استاندارد بیشتر شده و بنابراین دستگاه هایی که دارای کارت های شبکه استاندارد هستند ، این فریم را یک فریم Gaint (یعنی بزرگتر از استاندارد) تشخیص داده و فریم را از بین می برند . حتی اگر اندازه فریم بزرگتر از 1518 هم بایت نشود ، باز هم کارت های شبکه استاندارد ، قادر به پردازش Header و Trailer افزوده شده نخواهند بود .

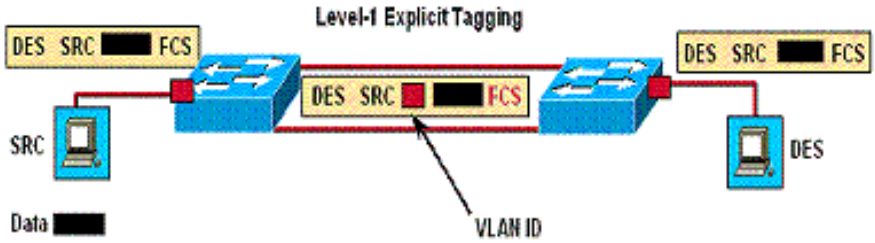
*** در اتصالات Access Link ، سوئیچ ها برای ارسال اطلاعات همیشه Header و Trailer را حذف کرده و سپس اقدام به ارسال فریم ها می کنند .**

*** از سوئیچ های سیسکو ، سوئیچ 1900 فقط از ISL و سوئیچ 2950 فقط از 802.1Q پشتیبانی می کنند.**

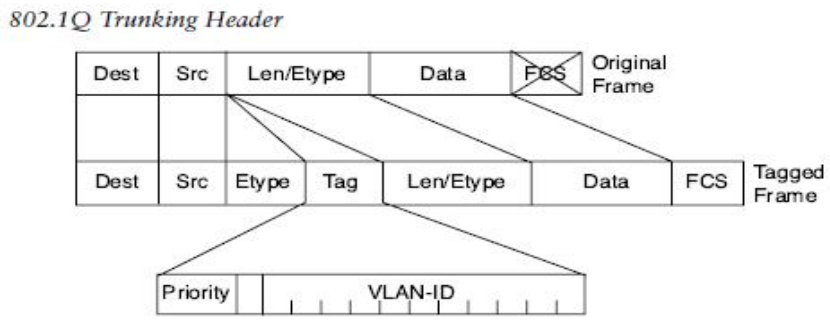
802.1Q

روش ISL چند سالی است که به وسیله استاندارد 802.1Q جایگزین شده است . مزیت این استاندارد این است که بین تولد کننده های مختلف مشترک بوده و همه دستگاه های مختلفی که توسط انها تولید می شوند از یان استاندارد پشتیبانی می کنند. در حالیکه ISL را می توان فقط در دستگاه های سیسکو بکار برد .

802.1Q که یک استاندارد IEEE ایست برای فراهم کردن تعریف VLAN و سطوح کیفیت سرویس (QoS) بوجود آمده است . چهار بایت اضافه شده به یک فریم اترنت ، حداکثر سایز فریم را از 1518 به 1522 افزایش می‌دهد. سه بیت آن برای فراهم کردن هشت سطح اولویت (QoS)استفاده شده است و 12 بیت دیگر برای شناسایی بیشتر از VLAN 4096 استفاده شده است .



البته نکته ای که وجود دارد این است که این روش 4 بایت را در داخل خود فریم اترنت جاسازی می کند ، یعنی فیلدی با عنوان tag که بعد از فیلد MAC قرار می گیرد ایجاد می کند و FCS فریم دوباره محاسبه می کند . با جاسازی 4 بایت در داخل فریم اترنت اندازه کلی فریم از 1518 بایت فراتر نخواهد رفت و بنابراین می توان این فریم ها را از طریق اتصالات Access Link نیز ارسال کرد .



802.1Q برای ساده سازی پیکربندی و مدیریت VLAN طراحی شده است .برخلاف روش ISL که تمامی فریم های Ethernet را همیشه tag می کرد ، روش 802.1Q دو روش را پیش می گیرد . یکی اینکه فریم های Ethernet بدون اینکه تغییری روی آنها اعمال شود ، ارسال می شوند . یعنی این فریم ها tag نشده و بنابراین اطلاعاتی در مورد VLAN با خود انتقال نمی دهند . در این وضعیت ، عضویت در یک VLAN خاص بوسیله پورت ها تعیین خواهد شد . مثلا هر دستگاهی که به یک پورت مخصوص اتصال داشته باشد ، عضو یک VLAN خاص خواهد بود . به این نوع VLAN ها اصطلاحا Native VLAN گفته می شود .روش دیگر هم این است که سوئیچ تمامی فریم ها را tag کرده و فقط دستگاه هایی که از استاندارد 802.1Q استفاده می کنند قادر به پردازش آنها باشند .

مزیت دیگر 802.1Q این است که هر دوی فریم های tagged و Untagged بطور همزمان می توانند در داخل یک ارتباط Trunk قرار داشته باشند .

VLAN Trunk Protocol

پروتکل VTP پروتکلی مخصوص سیسکو بوده که برای حمل اطلاعات مربوط به VLAN ها بین سوئیچ های سیسکو در اتصالات Trunk بکار می رود . این پروتکل باعث می شود که تمامی سوئیچ های شبکه دارای اطلاعات کافی در مورد تمامی VLAN های موجود باشند که نتیجه کار ، پایداری شبکه و افزایش کارایی آن خواهد بود .

برای مثال فرض کنید شبکه ای داریم که دو سوئیچ در آن وجود داشته باشد . اگر بخواهیم یک VLAN را به شبکه اضافه نماییم می توان به سادگی این عمل را به صورت دستی در روی هر دو سوئیچ جداگانه انجام داد .اما اگر تعداد سوئیچ های شبکه زیاد باشد ، مثلا 30 عدد ، در این هنگام افزودن VLAN ها در روی هر یک از سوئیچ ها کاری دشوار و وقت گیر خواهد بود . در ضمن در مواقعی که شماره یک VLAN را در یک یا چند سوئیچ به اشتباه وارد کرده باشیم و یا فراموش کنیم تنظیماتی را در روی برخی سوئیچ ها انجام دهیم ، دچار وضعیت بسیار دشوار و سردرگم کننده ای خواهیم شد .

پروتکل VTP در چنین مواقعی به کمک ما خواهد آمد و دیگر نیازی به اعمال تغییرات روی تک تک سوئیچ ها نخواهد بود . بلکه تنظیمات مربوطه در روی یک سوئیچ انجام گرفته و پروتکل VTP مسئول انتشار اطلاعات مربوط به VLAN ها و تنظیمات انجام گرفته بر روی سوئیچ های دیگر خواهد بود . همچنین در مواقعی که اقدام به افزودن یا حذف کردن یک VLAN در روی شبکه می کنیم ، این پروتکل تغییرات داده

شده را بین کل سوئیچ های شبک پخش خواهد کرد . همچنین پروتکل VTP در هنگام انتشار پیام های خود ، اشتباهاتی را که ممکن است در پیکربندی VLAN رخ داده باشد را بطور خودکار اصلاح خواهد کرد .چرا که پارامترهای مربوط به VLAN ها شامل شماره ، نام و نوع آن در هنگام انتقال به وسیله پروتکل VTP مورد بررسی قرار می گیرند .

پیام های VTP فقط از طریق اتصالات نوع Trunk منتقل می شوند . بنابرای برای استفاده از VTP باید بین سوئیچ ها اتصال Trunk ایجاد کنیم . پیام های VTP از نوع Multicast بوده و فقط دستگاه های لایه دو را تحت تاثیر قرار می دهد . بنابراین اگر روتری در بین راه وجود داشته باشد ، اجازه عبور VTP را از خود نخواهد داد .

پارامتر دیگری که در مورد VLAN ها وجود دارد ، VTP Domain است . یک Domain به گروهی از سوئیچ ها گفته می شود که دارای اطلاعات یکسانی در مورد VLAN ها هستند. یک سوئیچ فقط می تواند عضو یک VTP Domain باشد . همچنین سوئیچ ها در موقع ایجاد پیام های VTP ، نام Domain مربوطه را نیز در داخل پیام VTP جاسازی می کنند . سوئیچ هایی که این پیام ها را دریافت می کنند ، نام Domain پیام VTP را بررسی کرده و اگر شبیه نام VTP Domain خود نباشد ، پیام VTP را پردازش نخواهد کرد.

حالت های VTP (VTP modes)

هنگامی که اقدام به پیکر بندی VTP در روی سوئیچ های خود می کنیم ، سه گزینه برای انتخاب پیش رو داریم :

- Client
- Server
- Transparent

جدول زیر تفاوت های این سه mode را نشان می دهد .

Transparent	Client	Server	نوع عملیات
+	−	+	افزودن VLANها ، حذف آنها و تغییر تنظیمات مربوطه
−	−	+	توانایی ایجاد و ارسال پیام های VTP
+	+	+	توانایی منتشر کردن پیام های VTP دریافت شده
−	+	+	پذیرش تغییرات موجود در پیام های VTP
−	−	+	حالت پیش فرض دستگاه

سوئیچ هایی که در Server mode و Transparent mode تنظیم می شوند ، می توانند اقدام به ایجاد ، تغییر و یا حذف VLANها نمایند . تنها تفاوتی که بین این در

mode وجود دارد این است که تنظیمات انجام شده در روی سوئیچ های Transparent سوئیچ های دیگ شبکه را تحت تاثیر قرار نداده بلکه فقط بر روی خود آنها اعمال خواهند شد . اما سوئیچ های Server بعد از اعمال تغییرات در شبکه اقدام به انتشار آنها از طریق تمامی پورت های خود می کنند . وقتی که یک پیام VTP وارد سوئیچ Server شود ، این سوئیچ پیام رسیده را با اطلاعات خود به روز کرده و از طریق بقیه پورت های Trunk خود دوباره آنها را ارسال می کند . اما وقتی که پیام VTP به یک سوئیچ Transparent وارد می شود ، این سوئیچ پیام رسیده را دریافت کرده و آن را از طریق تمامی پورت های Trunk خود ارسال می کند.

سوئیچ Client نیز موقعی که پیام VTP را دریافت می کند ، تغییرات مربوطه را بر اساس تنظیمات موجود ر روی پیام اعمال کرده و سپس پیام را به بقیه پورت های Trunk خود انتشار خواهد داد. به عبارت دیگر در سوئیچ های Client نمی توان هیچ تغییری در پیام های VTP اعمال کرد و این سوئیچ ها همیشه اطلاعات VLAN خود را از سوئیچ های Server دیافت می کنند.

روش رایج به اینصورت است که یک سوئیچ را در شبکه در نقش Server قرار داده و بقیه را Client قرار خواهیم داد .

پیام های VTP

اگر نوع سوئیچ ها را روی Server/Client تنظیم کنیم سه نوع از پیام های VTP در شبکه مورد استفاد قرار خواهند گرفت :

- Advertisement request
- Subset advertisement
- Summery advertisement

یک پیام Advertisement request پیامی است که Client ها در هنگام بوت شدن دستگاه ایجاد کرده و اطلاعات مربوط به VLAN ها را از سوئیچ سرور خود درخواست می کنند .

سوئیچ سرور نیز جواب پیام رسیده از Client را با پیام Subset advertisement می دهد . این پیام شامل اطلاعات VLANها مانند نام، شماره، نوع و بقیه موارد مربوط می شود که سوئیچ های Client تنظیمات خود را از روی این اطلاعات انجام می دهند . پیام های Summery advertisement نیز توسط سوئیچ سرور در هر 300 ثانیه یک بار و یا به محض بروز تغییرات در شبکه ارسال می شوند که شامل اطلاعات مختصری درمورد VLANها می باشد.

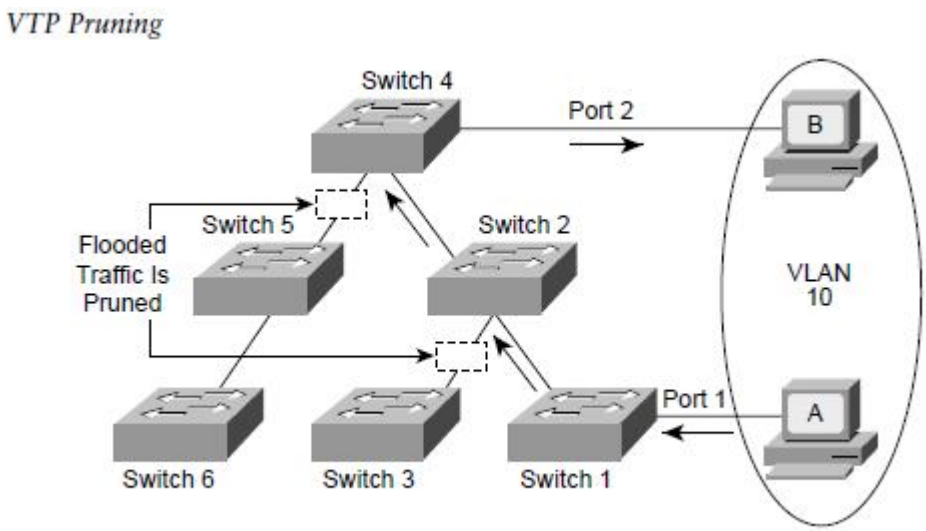
VTP pruning

به صورت پیش فرض ، یک اتصال Trunk ترافیک را برای همه VLANها حمل می کند. Broadcast ها در هر VLAN مطابق با توپولوژی جاری STP ، به همه سوئیچ های شبکه فرستاده می شوند . به هر حال ، در اکثر شبکه ها ، یک سوئیچ برای همه

VLAN ها interface ندارد ، بنابراین Broadcast ها برای VLAN هایی که interface ندارند حقیقتا پهنای باند را هدر می دهد .

VTP pruning به سوئیچ ها اجازه می دهد که از جریان یافتن Broadcast ها و unicasts های ناشناخته که هیچ پورتی را در VLAN ندارند ، به سوئیچ ها جلوگیری کنند.

شکل زیر مثالی را برای یک VTP pruning فراهم می کند .



در این شکل ، سوئیچ 1 و 4 پورت های VLAN 10 را پشتیبانی می کنند . با فعال شدن VTP pruning ، وقتی که ایستگاه A یک Broadcast می فرستد ، Broadcast تنها به سوی سوئیچی با پورت های اختصاص داده شده به VLAN 10 جریان خواهد یافت .

به عنوان یک نتیجه ، ترافیک Broadcast از ایستگاه A به سوئیچ های 3 ، 5 ، و 6 ارسال نمی شود ، چرا که ترافیک برای VLAN 10 بوسیله VTP تعیین شده ، روی لینک های سوئیچ های 2 و 4 محدود شده است. VTP pruning یکی از دو دلیل مهم

برای وادار شدن به استفاده از VTP است . علت دیگر آسان تر کردن و پایدار تربودن پیکربندی VLAN به واسطه استفاده از VTP pruning است .

VTP pruning پهنای باند در دسترس را با محدود کردن ترافیک ، که شامل Broadcast ها و .unicasts های با مقصد ناشناخته است ، افزایش می دهد .

این خصوصیت مخصوص سیسکو بوده و امکان حذف یا اضافه کردن VLANها روی اتصالات Trunk را به سوئیچ ها می دهد .

نمونه ای از پیکربندی VLANو Trunking (در سوئیچ 2950)

همه سوئیچ های سیسکو که روانه بازار می شوند ، دارای تنظیمات پیش فرضی می باشند . به طوری که شما می توانید سوئیچ های سیسکو را خریداری کرده ، دستگاه ها را با کابل کشی صحیح نصب کنید ، سوئیچ را روشن کنید ، و سپس آنها کار می کنند . تا زمانی که به بیشتر از یک VLAN نیاز ندارید -- حتی اگر شما سوئیچ ها را به یکدیگر متصل کنید، هیچ گاه نیازی به پیکربندی سوئیچ ندارید و آن به شکلی عالی کار می کند . حتی STP پیش فرض و تنظیمات trunking احتمالا بدرستی کار خواهند کرد ، اما اگر شما می خواهید از VLAN ها استفده کنید ، شما به افزودن برخی پیکربندی ها نیاز دارید .

پیکربندی VTP

یکی از اولین اعمالی که در سوئیچ ها انجام خواهد شد ، تنظیم موارد مربوط به VTP می باشد .

پیکربندی VTP در سوئیچ 2950

بسته به نسخه نرم افزاری IOS موجود در سوئیچ 2950 ، اینکار به دو نوع مختلف انجام می شود . روش قدیمی تر بجای این که در Global configuration اجرا گردد ، در privilege EXEC اجرا می شود .

در اینجا ما روش دوم پیکربندی VTP که در نسخه IOS12.1(11) EA1 و نسخه های بالاتر قابل استفاده می شود را به کار می بریم . در این روش اقدام به تنظیم موارد مربوط به VTP در Global configuration خواهیم نمود .

شکل دستورات :

```
2950(config)# vtp domain VTP_domain_name
2950(config)# vtp mode server|client|transparent
2950(config)# vtp password VTP_password
2950(config)# vtp pruning
```

بعد از پیکربندی VTP با استفاده از هر دو روش ، می توان درستی کار را با بکار بردن دستور زیر بررسی نمود :

```
2950# show vtp dtatus
VTP Version : 1
8Configuration Revision :
Maximum VLANs supported locally : 250
```

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : mygroup

VTP pruning Mode : Enabled

VTP V2 Mode : Disabled

MD5 digest : 0x54 0x80 0xA5 0x82 0x8D 0x8E 0x5F 0x94

Configuration last modified by 0.0.0.0 at 3-1-93 00:31:11

Local updater ID is 10.1.1.10 on interface Vl1

(lowest numbered VLAN interface found)

با توجه به مقدار Configuration Revision متوجه می شویم که تا به حال 8 بار

اقدام به اعمال تغییرات در پیکربندی VTP کرده ایم .

پیکربندی Trunk

چهار روش مختلف برای اتصال Trunk وجود دارد : 802.10 ، LANE ، 802.1Q ، ISL

سوئیچ 2950 فقط از 802.1Q استفاده می کند .

پیکربندی Trunk در روی سوئیچ 2950

شکل دستوری این پیکربندی به صورت زیر است :

```
2950(config)# interface type 0/port_#
2950(config-if)# switchport mode trunk|dynamic|desirable|dynamic auto |nonegatotiate
2950(config-if)# switchport trunk native vlan VLAN_#
```

برای فعال کردن اتصال Trunk در روی interface می توان از دستور Trunk استفاده کرد VLAN1 به عنوان Native VLAN در سوئیچ 2950 بوده اما می توان VLAN دیگری را به همین منظور انتخاب کرد . دستور بکار رفته چنین است :

```
2950# show interfaces type 0/port_# switchport|trunk
```

به مثال زیر توجه کنید :

```
2950#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
```

Access Mode VLAN: 0 (inactive)

Trunking Native Mode VLAN: 1 (default)

Administrative private-vlan host-association: ALL

Trunking VLANs Enabled: ALL

Pruning VLANs Enabled: 2-1001

Priority for utagged frames :0

Override vlan tag prority : false

Voice VLAN : none

در این مثال اتصال trunk فعال شده است و نوع پروتکل نیز 802.1Q می باشد . و همچنین VLAN1 به عنوان Native VLAN انتخاب شده است .

دستور زیر وضعیت trunk را نمایش می دهد .

sw1-2950#show interfaces trunk

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 1

Port Vlans allowed on trunk

Fa0/1 1-4094

Port Vlans allowed and active in management domain

Fa0/1 1-2

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1-

در این مثال می بینید که فقط یک Interface وجود دارد که از اتصال trunk استفده می کند و VLAN1 نیز به عنوان Native VLAN انتخاب شده است .

ایجاد VLAN

به طور کلی در مواقعی که اقدام به ایجاد VLAN می کنیم ، باید به موارد زیر توجه کنیم :

- **تعداد VLAN هایی که ایجاد می شوند بستگی به نوع و مدل سوئیچ بکار روفته و نسخه IOS نصب شده روی انها دارد .**
- **برخی از VLAN ها به صورت از پیش تعریف شده در روی سوئیچ ها وجود دارند ، مثل VLAN1 ، 005 و 1-002**
- **برای افزودن و یا حذف VLAN ها ، سوئیچ باید روی Server و یا Transparent تنظیم شود.**
- **نام مربوط به VLAN ها را می توان تغییر داد . اما شماره VLAN ها را نمی توان عوض کرد . تنها راه ممکن برای اینکار ، پاک کردن VLAN و ایجاد دوباره آن با شماره جدید است .**
- **تمامی Interface های روی سوئیچ در ابتدا عضو VLAN1 هستند.**
- **پروتکل های VTP ، CDP و DTP در VLAN1 فعالیت می کنند .**
- **زمانیکه دستگا های سیسکو از ISL استفاده می کنند ، PVST (Per-VLAN STP در PVST ، هر یک از VLAN های موجود دارای STP مخصوص به خود هستند.) را نمی توان به کار برد .**

- قبل از حذف هر یک از VLANها ، در ابتدا پورت های آن را به یک VLAN دیگر انتقال دهید و سپس اقدام به حذف VLAN نمایید . در غیر اینصورت ، پورت های مربوط به VLAN حذف شده همه به VLAN1 منتقل می شوند .

ایجاد و تنظیمات مربوط به VLAN ها در 2950

دستورات بکار رفته چنین خواهد بود :

2950(config)# vlan VLAN_#
2950(cnfig-vlan)# name VLAN_name

بعد از تایپ دستور VLAN وارد VLAN subconfiguration mode شده و پارامترهایی مانند نام VLAN را در داخل این قسمت تنظیم می کنیم . بعد از ایجاد VLAN مورد نظر ، نیاز به تخصیص دادن پورت های دلخواه به VLAN ذکر شده داریم . که دستورات آن به شکل زیر خواهند بود :

2950(config)# interface type 0/port_#
2950(config-if)# switchport mode access
2950(confug-if)# switchport access vlan VLAN_#

دستور اولی نوع پورت را Access Link قرار می دهد و با استفاده از دستور دوم نیز Interface دلخواه را عضو VLAN مورد نظر خواهیم نمود .

بعد از اتمام پیکربندی VLAN ها ، دستورهایی را می توان برای اطمینان از صحت مراحل انجام گرفته بکار برد .

دستور show vlan نشان دهنده لیست VLAN های موجوئ و پورت های تخصیص یافته به آنها می باشد . با نوشتن پارامتر brief در آخر دستور فوق نیز می توان اطلاعات را به صورت خلاصه تر مشاهد کرد همچنین با استفاده از دستور show interface switchport اطلاعات مخصوص به یک پورت خاص را می توان بدست آورد . برای بررسی صحت عملکرد STP از دستور زیر استفاده می کنیم :

Show spanningtree vlan VLAN_#

که سپس می توانید اطلاعات خروجی این دستور را بررسی کنید.

بعد از آشنایی مختصر با VLAN ها و ایجاد و پیکربندی آنها احتمالا با مشکلاتی روبه رو خواهید شد که برای عیب یابی VLAN ها و اتصالات Trunk مراحل و راه حل هایی وجود دارد که متاسفانه در این بحث به آنها نپرداخته ایم .

پایان!

منابع :

1–مرجع کامل CCNA مترجم و گردآورنده : دکتر حسین محسن زاده

2- **CCNA ICND Exam Certification Guide Wendell Odom Published by Cisco Press**

3- **http://www.linktionary.com**

4- **www.e-tutes.com**

5- **http://articles.techrepublic.com**

6- **www.cisco.com**

7- **www.ciscopress.com**

8- **PC Magazine**