Mahdi.Saghaei Digitally signed by Mahdi.Saghaei
DN: CN = Mahdi.Saghaei, C = IR, O = MFT ZANJAN, OU = Networking
Reason: I am the author of this document
Date: 2007.12.20 20:35:09 +03'30'

این فصل موضوع های زیر را پوشش می دهد:

- مروری بر مفاهیم شبکه های محلی مجازی (VLAN)
- انجام Trunking[1] با استفاده از ISL و 802.1Q
- پروتکل Trunking در VLAN (VTP)
- پیکربندی VLAN و Trunking

شبکه های محلی مجازی (VLAN) و عمل Trunking

مباحث شبکه های محلی مجازی و عمل trunking در آنها دو گزینه مهم در آزمون مدرک CCNA می باشند. علاوه براین ممکن است آشنایی و تسلط بر آنها در محیط کاری بسیار مهمتر و مفیدتر باشد. VLAN ها اجازه می دهند که یک سوئیچ درگاههای مختلف را در گروه بندی های متفاوت و جداگانه قرار داده و بنابراین ترافیک هر VLAN را از ترافیک VLAN های دیگر جدا کند. همچنین VLAN ها اجازه می دهند تا مهندسین شبکه بتوانند شبکه های مختلفی و جداگانه ای را بر اساس نیازهای خود طراحی و راه اندازی کنند ، بدون آنکه نیازی برای خرید سوئیچ جداگانه برای هر گروه داشته باشند. مکانیزم trunk اجازه می دهد تا هر VLAN امکان ارتباط چندین سوئیچ یا محدوده متفاوت (با ترافیک مختلف) را با یکدیگر از طریق یک ارتباط واحد اترنت فراهم نماید.

آیا من قبلا این را می دانستم؟ آزمون

هدف از این بخش و آزمون آن این است که به شما کمک کند تا متوجه شوید آیا نیازی به خواندن این فصل دارید یا خیر؟ اگر شما قصد مطالعه این فصل را دارید ، نیازی به جواب دادن به سوالات مطرح شده ذیل نخواهد بود. ۸ سوال ذیل از "بخشهای مباحث اصلی" انتخاب شده که به شما برای برنامه ریزی و هزینه کردن درست و صحیح زمان مطالعه کمک خواهد کرد.

جدول ۱-۳ مباحث اصلی مطرح شده در این فصل را ارائه داده و سوالات بخش "آیا من قبلا این را می دانستم؟" نیز با سرفصلهای مذکور مرتبط هستند.

بخش مباحث اصلی	سوالات پوشش داده شده در این فصل
مروری بر شبکه های محلی مجازی (VLAN)	۱ و ۲
انجام trunk با استفاده از ISL و 802.1Q	۳ ، ٤ و ٥
پروتکل trunking در VLAN	٦ و ۷
پیکربندی VLAN و Trunk	۸

[1] معنای لغوی Trunking یعنی کانال کشی برای تهویه و در شبکه به معنای ایجاد یک کانال ارتباطی بین شبکه های مجازی مختلف بکار می رود. برای درک بهتر این مفهوم از دیکشنری انگلیسی یا قالب PDF که در داخل CD همراه کتاب ارائه شده است ، استفاده فرمایید.

Translated by: Mahdi Saghaei

۱. در یک شبکه LAN ، کدامیک از اصطلاحات زیر بهتر از بقیه با اصطلاح VLAN برابر است؟

a. Collision Domain
b. Broadcast Domain
c. Subnet Doain
d. Single Switch
e. Trunk

۲. تصور کنید که یک سوئیچ با سه VLAN پیکربندی شده است. چه تعداد محدوده آدرس IP احتیاج خواهد بود؟ با این تصور که تمام سیستم ها در کلیه VLAN ها می خواهند از TCP/IP استفاده کنند.

a. ۰
b. ۱
c. ۲
d. ۳
e. با توجه به اطلاعات گفته شده ، چیزی نمی توان گفت.

۳. کدامیک از گزینه های زیر ، فریم اصلی اترنت را در داخل header مربوط به trunk ، پوشش گذاری می کند؟

a. VTP
b. ISL
c. 802.1Q
d. ISL و 802.1Q
e. هیچکدام

٤. کدامیک از گزینه های زیر header مربوط به trunking را به تمام VLAN ها (بجز یکی) اضافه می کند؟

a. VTP
b. ISL
c. 802.1Q
d. ISL و 802.1Q
e. هیچکدام

٥. کدامیک از گزینه های زیر اجازه ایجاد Spanning Tree به ازای هر VLAN را می دهد؟

a. VTP
b. ISL
c. 802.1Q
d. ISL و 802.1Q
e. هیچکدام

٦. کدامیک از موارد زیر اطلاعات VLAN را برای سوئیچ های همسایه انتشار می دهد؟

a. VTP
b. ISL
c. 802.1Q
d. ISL و 802.1Q
e. هیچکدام

Translated by: Mahdi saghaei

۷. کدامیک از حالتهای VTP که در زیر ذکر شده است ، اجازه می دهد که VLAN بر روی سوئیچ ایجاد گردد؟

a. Client
b. Server
c. Transparent
d. Dynamic
e. هیچکدام

۸. تصور کنید به شما اینگونه گفته شده که بر روی ارتباط اترنت سوئیچ ۱ (برای عمل trunking)به سمت سوئیچ ۲ ، پارامتر auto تنظیم شده است. حالا شما می خواهید سوئیچ ۲ را پیکربندی کنید. کدامیک از تنظیمات زیر اجازه می دهد تا مکانیزم trunking فعال شده و کار کند؟

a. Trunking فعال است.
b. Auto
c. Desirable
d. Off
e. هیچکدام

برای دسترسی به جوابها به ضمیمه A مراجعه کنید. انتخابهای پیشنهادی برای مرحله بعد شما براساس موارد زیر ارائه می گردد:

- امتیاز ٦ یا کمتر– دروس داخل فصل را بخوانید. این موارد شامل مباحث اصلی ، خلاصه مطالب اصلی و بخش سوال و جواب می شود.
- امتیاز ۷ یا ۸ – اگر شما تمایل دارید تا مباحث را بیشتر مرور کنید ، از بخش خلاصه مطالب اصلی عبور کرده و به سراغ بخش سوال و جواب بروید. در غیر اینصورت فصل بعد را برای مطالعه انتخاب کنید.

Translated by: Mahdi saghaei

مباحث اصلی

مکانیزم VTP در این فصل پس از trunking بحث شده و در انتها ، این فصل با پیکربندی VLAN پایان می پذیرد.

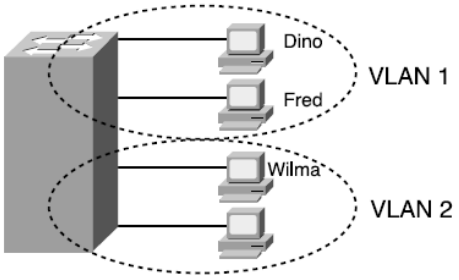
مروری بر مفاهیم شبکه های محلی مجازی (VLAN)

VLAN ها در حوزه تئوری و مفاهیم و نیز عملی نسبتا آسان هستند. در زیر گزینه های مهمی لیست شده اند که دانستن آنها قبل از شروع بحث اصلی ، کمک قابل توجهی به شما خواهد کرد:

- یک ***محدوده برخورد***[2] ، محدوده ای است که شامل مجموعه ای از کارتهای شبکه است که در صورت ارسال شدن یک فریم توسط یک کارت شبکه ، امکان برخورد با فریم ارسالی توسط یک کارت شبکه دیگر ، در همان محدوده وجود دارد.
- یک ***محدوده فراگیر***[3] ، محدوده ای است که شامل مجموعه ای از کارتهای شبکه است که در صورت ارسال فریم فراگیر توسط یک کارت شبکه ، تمام کارتهای شبکه موجود در آن محدوده ، آنرا دریافت خواهند کرد.
- یک VLAN ، بصورت ذاتی یک محدوده فراگیر است.
- VLAN ها معمولا توسط پیکربندی یک سوئیچ و قراردادن در درگاه در داخل یک VLAN خاص ساخته می شوند.
- سوئیچ های لایه ۲ ، فریمها را بین دستگاههای موجود در VLAN خود ، forward می کنند. آنها نمی توانند فریمها را بین VLAN های متفاوت forward کنند.
- یک سوئیچ لایه ۳ (سوئیچ چند لایه) یا مسیریاب بصورت ذاتی می تواند پکتها را بین VLAN ها ، مسیردهی کند.
- مجموعه ای از دستگاهها در داخل یک VLAN ، معمولا داخل یک محدوده آدرس IP یکسانی نیز هستند. دستگاههای موجود در VLAN های متفاوت ، محدوده آدرسهای IP متفاوتی نیز دارند.

تصویر ۱-۳ یک سوئیچ با دو VLAN را نمایش می دهد.Fred و Dino می توانند به یکدیگر فریم بفرستند ، اما توانایی ارسال فریم به Wilma را ندارند.

تصویر ۱-۳ شبکه ای با دو VLAN که از یک سوئیچ استفاده کرده است.



[2] ***Collision Domain***
[3] ***Broadcast Domain***

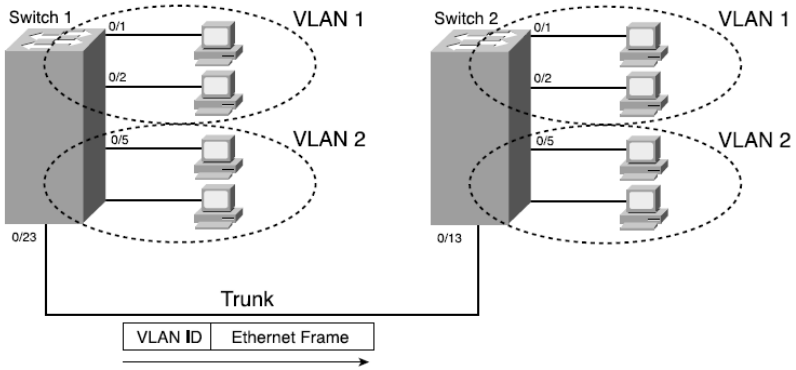
Translated by: Mahdi saghaei

بله ، مفاهیم موجود در پشت صحنه VLAN ها بسیار ساده هستند. استفاده از VLAN ها ، شما را با مفاهیم دیگری نیز که باید بدانید آشنا می کند. سپس شما در مورد Trunking در VLAN ، VTP[4] و برخی موضوع ها که به پروتکلهای لایه ۳ در هنگام استفاده از VLAN ها مربوط می شوند ، مطالبی یاد خواهید گرفت.

عمل Trunking با استفاده از ISL و 802.1q

هنگامی که شما در شبکه های دارای چندین سوئیچ بهم متصل شده از VLAN استفاده می کنید ، احتیاج خواهید داشت تا از مکانیزم trunking بین سوئیچ ها استفاده کنید. با استفاده از VLAN trunking ، هر فریم ارسالی توسط سوئیچ علامت گذاری می شود تا بدینوسیله سوئیچ دریافت کننده متوجه شود که فریم به کدام VLAN تعلق دارد. تصویر ۲-۳ مفهوم اصلی را بصورت خلاصه نمایش می دهد.

تصویر ۲-۳ *VLAN Trunking بین سوئیچ ها*



با استفاده از مکانیزم trunking ، شما می توانید چندین VLAN را که اعضای آنها بر روی بیش از سوئیچ قرار دارند ، پشتیبانی کنید. بعنوان نمونه ، زمانی که سوئیچ شماره ۱ یک فریم فراگیر[5] از دستگاهی در VLAN شماره ۱ دریافت می کند ، احتیاج دارد که آنرا بصورت فراگیر به سمت سوئیچ شماره ۲ ارسال (forward) کند. قبل از ارسال فریم ، سوئیچ شماره ۱ یک header[6] دیگر به header اصلی فریم اترنت اضافه می نماید. این header جدید شماره VLAN را داخل خود جای داده است. زمانی که سوئیچ شماره ۲ فریم را دریافت می کند ، می بیند که فریم از یک دستگاهی در VLAN شماره ۱ ارسال شده است ، بنابراین سوئیچ شماره ۲ متوجه می شود که فریم فراگیر را فقط باید بر روی رابط خود در VLAN شماره ۱ ، forward نماید.

سوئیچ های سیسکو دو نوع پروتکل مختلف را برای عمل trunking پشتیبانی می کنند. یکی ISL (Inter-Switch Link) و دیگری IEEE 802.1Q. هردوی اینها موارد اساسی trunking را تامین می کنند که در تصویر ۲-۳ نمایش داده شده است. البته تفاوتهایی هم با یکدیگر دارند که در ادامه بحث خواهد شد.

ISL

سیسکو پروتکل ISL را قبل از اینکه سازمان IEEE پروتکل trunking را استانداردسازی بکند ، ایجاد کرد. بدلیل اینکه ISL یک پروتکل اختصاصی سیسکو می باشد ، فقط بین سوئیچ های سیسکو قابل استفاده است. ISL هر فریم اصلی اترنت را بصورت کامل توسط header و trailer[7] مربوط به ISL پوشش گذاری می کند. البته فریم اصلی اترنت در داخل header و trailer مربوط به ISL بصورت دست نخورده باقی می ماند.

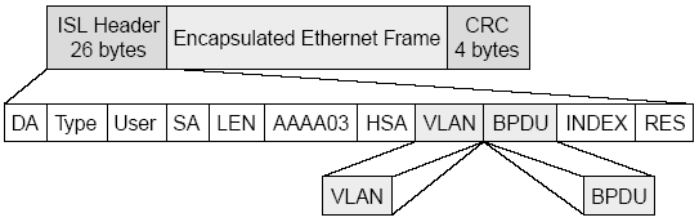
[4] VLAN Trunking Protocol
[5] Broadcast

[6] سرپیام ، قسمت ابتدایی فریم که معمولا نوع و مسیر آن را مشخص می کند.
[7] انتهای فریم ، بایت نهایی که معمولا حاوی خصوصیات داده و کنترل آن می باشد.

Translated by Ali Saghaei

تصویر ۳-۳ فریم گذاری ISL را نشان می دهد.

تصویر ۳-۳ Header متعلق به ISL



Header مربوط به ISL شامل چند فیلد بسیار مهم می شود. فیلد VLAN محلی را برای درج شماره VLAN بصورت رمزنگاری شده تامین می کند. با استفاده از علامت گذاری یک فریم توسط شماره صحیح VLAN در داخل header ، سوئیچ ارسال کننده می تواند اطمینان یابد سوئیچ دریافت کننده فریم متوجه می شود که فریم پوشش گذاری شده متعلق به کدام VLAN است. همچنین ، از فیلدهای آدرسهای مبدا و مقصد در header متعلق به ISL که دارای آدرسهای MAC سوئیچ های ارسال کننده و دریافت کننده فریم می باشند ، برای پاسخ دادن به دستگاههایی که فریم اصلی را ارسال کرده اند ، استفاده می شود. بغیر از این موارد مذکور ، جزئیات دیگر header متعلق به ISL مهم نیست.

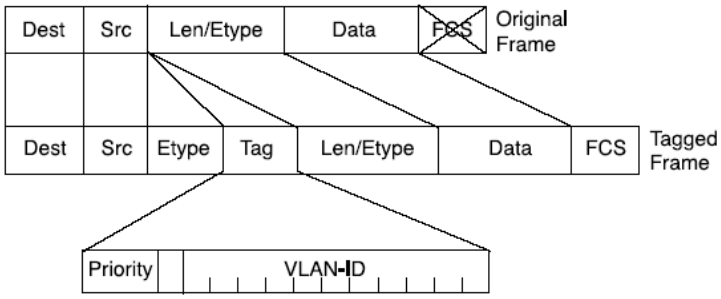
802.1Q

سازمان IEEE بسیاری از پروتکلهای مربوط به شبکه های امروزی را استانداردسازی نموده و VLAN trunking نیز از این قاعده مستثنی نیست. پس از اینکه سیسکو ISL را ایجاد کرد ، سازمان IEEE کار را بر روی استاندارد 802.1Q کامل کرد و آنرا راهی دیگر برای اجرای مکانیزم trunking تعیین نمود.

پروتکل 802.1Q یک نوع متفاوتی از header را نسبت به ISL برای علامتگذاری فریم ها با شماره VLAN استفاده می کند. در حقیقت ، 802.1Q فریم اصلی را بصورت واقعی پوشش گذاری نمی کند. بلکه ، یک header ٤ بایتی خارجی را به header اصلی اترنت اضافه می نماید. این header اضافی شامل فیلدی می شود که برای سناسایی شماره VLAN استفاده می گردد. بدلیل اینکه header اصلی تغییر پیدا کرده ، مکانیزم پوشش گذاری 802.1Q فیلد FCS اصلی را در قسمت trailer مربوط به اترنت دوباره محاسبه می کند ، این مسئله بدلیل اینکه است که FCS مبتنی بر مندرجات داخلی فریم می باشد.

تصویر ٤-۳ مکانیزم فریم سازی و header پروتکل 802.1Q مربوط به header تجدید نظر شده اترنت را نمایش می دهد.

تصویر ٤-۳ header مربوط به trunking در پروتکل 802.1Q



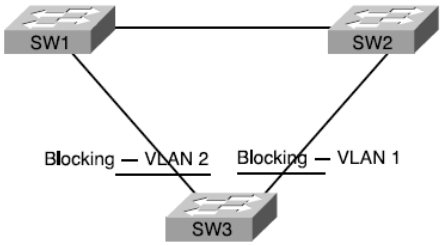
مقایسه ISL با 802.1Q

هر دو پروتکل ISL و 802.1Q عمل trunking را انجام می دهند. Header های استفاده شده در آن دو متفاوت بوده و فقط ISL بصورت واقعی فریم اصلی را پوشش گذاری می کند ، اما هر دوی آنها اجازه استفاده از شناسه VLAN (VLAN ID) به طول ۱۲ بیت را می دهند. هر دوی آنها بخوبی کار کرده و بدلیل استفاده هر دو از فیلد شماره VLAN بطول ۱۲ بیت ، یک شماره یکسان را برای VLAN ها پشتیبانی می کنند.

Translated by: Mahdi Saghaei

پروتکلهای ISL و 802.1Q دو نمونه متفاوت از Spanning Tree را برای هر VLAN پشتیبانی می کنند. نوعی که توسط ISL پشتیبانی می شود ، زودتر از 802.1Q ایجاد گردیده و بنابراین در سالهای گذشته یکی از وضعیتهای متفاوت بین این دو پروتکل trunking این بود که 802.1Q توانایی پشتیبانی از چندین Spanning Tree را نداشت. برای درک مزایای وجود داشتن چندین Spanning Tree ، تصویر ۵-۳ را بررسی کنید که یک شبکه ساده را بهمراه دو VLAN و سه سوئیچ متصل شده داخلی نشان می دهد.

تصویر ۵-۳ Spanning Tree به ازای VLAN بهمراه ISL



شما می توانید مقادیر STP را در هر VLAN بگونه ای تنظیم کنید که در هنگام فعال بودن تمام ارتباطها ، رابطهای متفاوتی در Spanning Tree های متفاوت بلوکه شوند. در تصویر ، برای جلوگیری از ایجاد حلقه ، فقط یکی از ٦ رابط متصل شده سوئیچ ها نیاز به بلوکه شدن داشته و باید block گردد. STP می تواند بگونه ای پیکربندی شود که VLAN 1 و VLAN 2 (در این مثال) رابطهای متفاوتی را بر روی سوئیچ SW3 بلوکه کنند. بنابراین ، SW3 در عمل ، پهنای باند در دسترس بر روی هر کدام از ارتباط های خود به سمت سوئیچهای دیگر را استفاده می کند. بهمین دلیل ، ترافیک داخل VLAN 1 ارتباط به سمت SW1 را استفاده کرده و ترافیک داخل VLAN 2 نیز از ارتباط به سمت SW2 استفاده می نماید. البته در صورتی که هنگام استفاده از ISL ارتباط خراب شود ، هر دو نمونه STP می توانند همگرایی کرده و مسیر را دوباره فعال کنند.

سیسکو ابزارهای STP متنوعی را برای تطبیق دادن چندین Spanning Tree ارائه می کند. ISL یک قابلیت اختصاصی سیسکو را بنام PVST+ (Per_VLAN Spanning Tree) برای پشتیبانی از چندین Spanning Tree استفاده می کند. پروتکل 802.1Q بصورت ذاتی نمی تواند از چندین Spanning Tree پشتیبانی کند ، ولی امکان انجام اینکار را با استفاده از ترکیب پروتکلهای دیگر داراست. قبلیت اختصاصی PVST+ سیسکو ، اجازه اجرای چندین مورد STP را بر روی trunk های 802.1Q می دهد. همچنین ، سازمان IEEE ویژگی جدیدی را بنام 802.1S ایجاد کرده که به 802.1Q اضافه شده و اجازه استفاده از چندین Spanning Tree را می دهد. علاوه بر این پروتکلها ، سیسکو انواع اختصاصی دیگری را هم پشتیبانی می کند.

کلیدی ترین تفاوت بین ISL و 802.1Q به خصوصیتی تحت عنوان VLAN بومی[8] مربوط می شود. پروتکل 802.1Q یک VLAN را بر روی هر trunk بعنوان VLAN بومی تعیین می کند که بصورت پیش فرض VLAN 1 می باشد. با این تعریف ، 802.1Q بصورت واقعی فریم های داخل VLAN بومی را در هنگام ارسال آنها از طریق ارتباط trunk پوشش گذاری نمی کند. هنگامی که سوئیچ موجود در طرف مقابل ارتباط ، فریم ها را در VLAN بومی دریافت کرد ، متوجه فقدان header مربوط به 802.1Q شده و متوجه می گردد که فریم مذکور بخشی از یک VLAN بومی است.

VLAN های بومی نقش بسیار مهمی را از لحاظ کاربردی ایفا می کنند. تصور کنید که شما دارای تعدادی PC هستید که به برخی از درگاههای سوئیچ متصل بوده و هیچ کدام از آنها نیز 802.1Q را نمی شناسند. شما همچنین برنامه ای برای راه اندازی ارتباطات تلفنی بر روی IP در نزدیکی PC ها دارید. تلفنهای IP یک سوئیچ داخلی دارند که شما می توانید تلفن را به کابل اترنت سوئیچ متصل کرده و سپس تلفن را به یک PC وصل کنید. این تلفنها پروتکل 802.1Q را می شناسند و بنابراین شما می توانید تلفن را در یک VLAN و PC را در یک VLAN دیگر قرار دهید. حالا شما می توانید تمام آن درگاهها را برای 802.1Q پیکربندی کنید ، بگونه ای که تمام PC ها در VLAN بومی قرار گیرند. هنگامی که یک ارتباط مستقیم با سوئیچ برقرار می شود

[8] Native VLAN

Translated by: Mahdi saghaei

، آنها بخوبی کار می کنند ، بدلیل اینکه سوئیچ هیچگونه پوشش گذاری فریم را برای VLAN بومی استفاده نمی کند. زمانی که شما یک تلفن IP بین سوئچ و PC نصب می کنید ، تلفن می تواند header های 802.1Q را شناسایی کرده و ترافیک مورد نظر را به سوئیچ ارسال و یا از آن دریافت نماید. در عین حال تلفن فقط می تواند ترافیک VLAN بومی را بین PC و سوئیچ عبور دهد.

ISL مفهومی مانند VLAN بومی را مورد استفاده قرار نمی دهد. تمام فریم ها از تمام VLAN ها برای تبادل از طریق trunk مربوط به ISL ، دارای header مخصوص ISL هستند.

جدول ۲-۳ گزینه ها و نکته های کلیدی متفاوت بین ISL و 802.1Q را بصورت خلاصه نمایش داده است.

جدول ۲-۳ مقایسه بین ISL و 802.1Q

وظیفه	ISL	802.1Q
مرکز استاندارد برای تعریف و تعیین پروتکل	اختصاصی سیسکو	سازمان IEEE
پوشش گذاری فریم اصلی	بله	خیر
اجازه استفاده از چندین Spanning Tree	بله ، با استفاده از PVST+	بله ، با استفاده از PVST+ یا 802.1S
استفاده از VLAN بومی	خیر	بله

پروتکل انجام Trunk در VLAN[9] (VTP)

سوئیچهای سیسکو یک VTP اختصاصی را برای تبادل اطلاعات پیکربندی VLAN بین سوئیچ ها استفاده می کنند. VTP یک پروتکل پیغام رسانی لایه ۲ را تعریف می کند که اجازه می دهد تا سوئیچ ها بتوانند اطلاعات پیکربندی VLAN را تبادل کرده و باعث پایدار ماندن پیکربندی VLAN در داخل شبکه شوند. بعنوان نمونه اگر شما بخواهید از 3 VLAN که نام آن accounting است استفاده کنید ، می توانید اطلاعات مورد نظر آن را بر روی یک سوئیچ پیکربندی کرده و سپس VTP می تواند آن اطلاعات را به سوئیچهای دیگر شبکه انتشار دهد. VTP می تواند عمل اضافه کردن ، حذف و تغییر نام VLAN ها را در میان چندین سوئیچ انجام داده و پیکربندی نادرست و ناسازگاری هایی که می توانند باعث ایجاد مشکل در شبکه شوند –مانند تنظیمات اشتباه در نوع VLAN و یا وجود نام تکراری VLAN – را کاهش دهد.

علاوه بر این ، VTP پیکربندی VLAN ها را ساده تر می کند. با اینکه شما هنوز در مورد نحوه پیکربندی VLAN اطلاعاتی ندارید ، برای درک بهتر VTP ، این مثال را بررسی کنید: اگر شبکه ای دارای ۱۰ سوئیچ داخلی بهم متصل شده باشد ، و بخشهای 3 VLAN بر روی آن ۱۰ سوئیچ وجود داشته باشد ، شما باید برای ساختن VLAN مذکور ، دستورات پیکربندی یکسانی را بر روی تمام ۱۰ سوئیچ انجام دهید. با استفاده از VTP شما باید 3 VLAN را فقط بر روی یک سوئیچ ساخته و سپس ۹ سوئیچ باقیمانده دیگر ، 3 VLAN را بصورت خودکار خواهند شناخت.

فرایند VTP با ساخته شدن VLAN بر روی سوئیچی بنام VTP Server شروع می گردد. تغییرات به شکل فراگیر در بین شبکه توزیع شده و انتشار می یابد. هر دو نوع VTP Client و VTP Server ها ، پیغامهای VTP را شنیده و پیکربندی خود را بر اساس آن پیغامها بروزرسانی می کنند. بنابراین VTP اجازه می دهد تا راهکارهای شبکه های سوئیچ بندی شده با کاهش دادن پیکربندی دستی مورد نیاز در شبکه ، در اندازه های وسیعی توسعه و گسترش یابند.

[9] VLAN Trunking Protocol

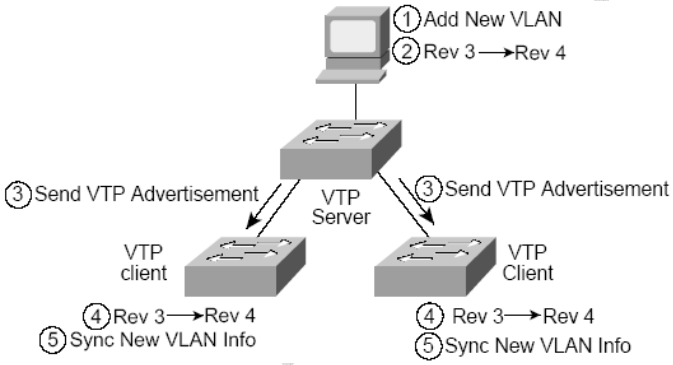
Translated by: Mahdi Saghaei

VTP چگونه کار می کند؟

VTP سیل اطلاع رسانی خود را در داخل محدوده VTP هر ۵ دقیقه یکبار و یا هر زمانی که تغییراتی که در پیکربندی VLAN رخ دهد ، پخش می کند. اطلاع رسانی و انتشار VTP شامل پیکربندی شماره ثانوی[10] ، نام های VLAN و شماره های آن و اطلاعاتی در مورد سوئیچ هایی که درگاههایی را به هر VLAN اختصاص داده اند ، می شود. با پیکربندی جزئیات بر روی یک یا تعداد بیشتری VTP Server و پخش کردن آن از طریق پیغامهای اطلاع رسانی ، تمام سوئیچ ها نامها و شماره های VLAN ها را خواهند شناخت.

یکی از مهمترین اجزای اطلاع رسانی VTP ، شماره پیکربندی ثانوی است. هر زمانی که VTP Server اطلاعات VLAN خود را اصلاح کرده و یا تغییر می دهد ، شماره پیکربندی ثانوی را ، یک رقم افزایش می دهد. سپس VTP Server پیغامهای اطلاع رسانی VTP را که شامل شماره پیکربندی ثانوی جدید می باشد ، به بیرون می فرستد. هنگامی که یک سوئیچ یک پیغام اطلاع رسانی VTP را با شماره پیکربندی ثانوی بزرگتری دریافت کرد ، پیکربندی VLAN خود را بروزرسانی می کند. تصویر ٦-٣ چگونگی عملکرد VTP را در یک شبکه سوئیچ شده ، شرح می دهد.

تصویر ٦-٣ عملکرد VTP



VTP در یکی از سه حالت زیر عمل می کند:

- حالت Server
- حالت Client
- حالت Transparent[11]

برای تبادل اطلاعات توسط VTP ، برخی سوئیچ ها بعنوان سرور و برخی دیگر بعنوان کلاینت عمل می کنند. سرورهای VTP می توانند VLAN ها را ایجاد ، حذف و یا اصلاح کرده و مقادیر پیکربندی دیگر در محدوده دامنه داخلی VTP را مدیریت نمایند. این اطلاعات ، بنوبت به کلاینتها و سرورهای VTP در همان دامنه و محدوده انتشار می یابند. سرورهای VTP پیکربندی های VLAN را در داخل NVRAM سوئیچ ذخیره می کنند ، در حالیکه در کلاینتها تمام اطلاعات پیکربندی VLAN ذخیره نمی شود. یک کلاینت VTP نه می تواند VLAN ها را ایجاد کرده ، تغییر داده و یا حذف کند و نه اینکه اطلاعات پیکربندی VLAN را در حافظه غیر فرار ذخیره کند.

بنابراین ، چرا کلاینت VTP وجود دارد ؟ خب ، اگر یک مهندس شبکه ای را طراحی و اجرا کند ، بسیار برای او راحتتر خواهد بود که پیکربندی های یک VLAN را بر روی یک سوئیچ (VTP Server) انجام داده و اطلاعات آماده را بر روی کلاینتهای VTP انتشار دهد.

جالب توجه اینکه ، برای جلوگیری از استفاده VTP جهت تبادل اطلاعات VLAN در سوئیچهای سیسکو ، شما نیازی به غیر فعال (Disable) کردن VTP ندارید. بجای آن ، شما می توانید از حالت Transparent استفاده کنید. در عین حال با استفاده از حالت Transparent در VTP بر روی برخی از سوئیچهای داخل شبکه ، سرورها و کلاینتهای VTP می توانند بصورت عادی بکار خود ادامه داده و همچنین سوئیچهای VTP که دارای حالت

[10] Configuration Revision Number

[11] شفاف ، فراگیر

Translated by saghaei

Transparent هستند ، بسادگی پیغامهای VTP را نادیده می گیرند. سوئیچی که در حالت Transparent قرار می گیرد ، مادامیکه اطلاعات پیغامهای VTP را نادیده می گیرد ، اطلاعات دریافتی VTP از سوئیچهای دیگر را از خود عبور داده و forward می کند.

یک سوئیچ که در حالت Transparent پیکربندی شده است ، می تواند VLAN ها را ایجاد ، حذف و یا اصلاح کند ، اما تغییرات به سوئیچهای دیگر موجود در دامنه فرستاده نمی شود و تغییرات فقط بر روی آن سوئیچ تاثیر می گذارد. انتخاب استفاده از حالت Transparent یک نمونه و سرمشق برای زمانی است که شبکه احتیاج دارد تا کنترلهای مدیریتی سوئیچ ها را در سطح دامنه توزیع نماید.

جدول ۳-۳ یک مرور کلی مقایسه ای را در مورد سه حالت VTP ارائه می دهد.

جدول ۳-۳ حالتهای VTP

وظیفه	حالت Server	حالت Client	حالت Transparent
سرچشمه و آغاز انتشار VTP	بله	خیر	خیر
انتشار فرایندهای دریافتی و همسان سازی اطلاعات پیکربندی VLAN با سوئیچ های دیگر	بله	بله	خیر
Forward کردن پیغامهای انتشار یافته VTP از طریق یک Trunk	بله	بله	بله
ذخیره کردن پیکربندی VLAN در NVRAM	بله	خیر	بله
توانایی ایجاد ، حذف و اصلاح VLAN ها با استفاده از دستورات پیکربندی	بله	خیر	بله

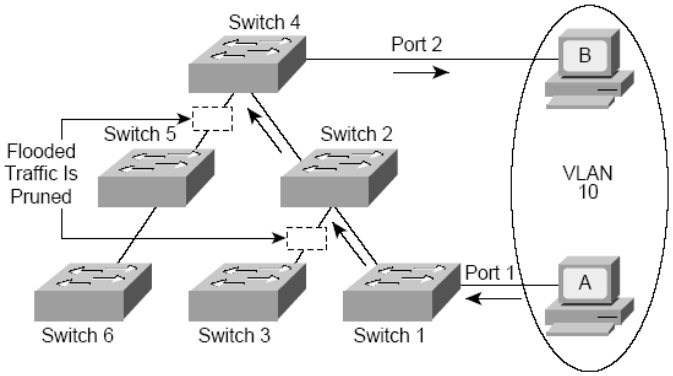
هرس کردن VTP (VTP Pruning)

بصورت پیش فرض ، یک ارتباط trunk ترافیک را به سمت تمام VLAN ها حمل کرده و انتقال می دهد. فریم های فراگیر (و فریم های منحصر بفرد با مقصد ناشناس) در هر VLAN به هر سوئیچ داخل شبکه -بر مبنای توپولوژی STP جاری- فرستاده می شوند. هرچند ، در بسیاری از شبکه ها ، یک سوئیچ در هر VLAN دارای یک رابط نیست ، بنابراین فریم های فراگیر برای VLAN هایی که دارای رابطی نیستند ، بسادگی باعث هدر رفتن پهنای باند می شوند.

VTP Pruning از جریان یافتن فریم های فراگیر و فریم های منحصر بفرد ناشناس به سمت سوئیچ هایی که دارای هیچ درگاهی در VLAN نیستند ، جلوگیری می کند. تصویر ۷-۳ مثالی از VTP Pruning را نشان می دهد.

تصویر ۷-۳ مکانیزم VTP Pruning

Translated by: Mahdi saghaei



در تصویر ۷-۳ ، سوئیچ ۱ و ٤ دارای درگاههایی در VLAN شماره ۱۰ هستند. با فعال شدن VTP Pruning ، هنگامی که کلاینت A یک فریم فراگیر ارسال می کند ، فریم مذکور فقط بسوی سوئیچهایی سرازیر می شود که درگاههایی را به VLAN شماره ۱۰ اختصاص داده اند. در نتیجه ، ترافیک فریم های فراگیر از طرف کلاینت A به سوئیچ های ۳ ، ٥ و ٦ فرستاده نمی شود. به این دلیل که ترافیک موجود برای VLAN شماره ۱۰ ، بوسیله VTP بر روی ارتباطهایی که در سوئیچهای ۲ و ٤ نشان داده شده ، هرس شده است.

هرس کرد در VTP ، با استفاده از محدود کردن جریان ترافیک که شامل فریم های فراگیر و فریم های منحصر بفرد با مقصد ناشناس می باشد، باعث افزایش پهنای باند در دسترس می شود. VTP Pruning یکی از دو عاملی است که ما را مجبور به استفاده از VTP می کند. دلیل دیگر پیکربندی راحتتر VLAN و پایدارتر کردن آن است.

پیکربندی VLAN و عمل Trunking

شما می توانید سوئیچهای سیسکو را خریده ، دستگاههای مختلف را با کابل صحیح به آن متصل کرده ، آن را روشن کنید تا کار کند. تا هنگامی که شما به بیش از یک VLAN نیازی ندارید ، احتیاجی به پیکربندی خاص بر روی سوئیچهای شبکه نخواهید داشت ، حتی بر روی تنظیمات پیش فرض STP و trunking. مگر اینکه شما تمایل به استفاده از VLAN داشته باشید که در اینصورت باید برخی از پیکربندی ها را انجام دهید.

در شبکه های واقعی ، VLAN ها گزینه ای هستند که معمولا بر روی سوئیچ ها پیکربندی می شوند. تقریبا هر شبکه ای از آن ها استفاده می کند. علاوه بر این هیچگونه راهی برای اختصاص درگاههای خاصی برای VLAN ها وجود ندارد. بهمین دلیل ، شما واقعا برای اینکه بدانید کدام درگاه در کدام VLAN قرار دارد ، نیاز به پیکربندی سوئیچ دارید.

همانگونه که انتظار داشتید ، شما می توانید VTP و trunking را پیکربندی کنید. VTP بصورت پیش فرض روشن است و عمل مذاکره trunking بصورت پیش فرض بر روی تمام درگاهها ، انجام می پذیرد. اگرچه شما ممکن است نیازی به پیکربندی VTP یا trunking نداشته باشید ، اما مطمئنا باید جهت آمادگی در آزمون ، توانایی پیکربندی VTP و trunking را داشته باشید.

جدول ٤-۳ بصورت خلاصه دستورات استفاده شده در این فصل را توضیح می دهد. در زیر آنها ، چند مثال توضیحاتی اساسی در مورد VLAN ها ، Trunking و پیکربندی VTP ارائه داده است.

جدول ٤-۳ لیست دستورات VLAN در سوئیچ ۲۹۵۰

دستور	توضیح
Vlan database	یک دستور در محیط اجرایی که کاربر را در حالت پیکربندی VLAN قرار می دهد.
Vtp {domain *domain-name* | password *password* | pruning | v2-mode | {server | client | transparent}}	مقادیر VTP را در حالت پیکربندی VLAN تعریف می کند.
Vlan *vlan-id* [name *vlan-name*]	دستور پیکربندی بانک اطلاعاتی VLAN که VLAN ها را ساخته یا

Translated by Mahdi Saghaei

	نامگذاری می کند.
Switchport mode {access | dynamic | auto | desirable} | trunk}	دستور زیرمجموعه رابط که رابط را برای عمل trunking پیکربندی می کند.
Switchport trunk {{allowed vlan *vlan-list*} | native vlan *vlan-id*} | {pruning vlan *vlan-list*}}	دستور زیرمجموعه رابط که لیست VLAN های مجاز را تصحیح می کند ، VLAN بومی 802.1Q را تعریف می کند و محدوده VLAN هایی را که عمل pruning در آن اتفاق می افتد ، تعریف می کند.
Switchport access vlan *vlan-id*	دستور زیرمجموعه رابط که بصورت ایستا یک رابط را داخل یک VLAN قرار می دهد.
Show interfaces [*interface-id* | vlan *vlan-id*] [switchport | trunk]	نمایش وضعیت trunk.
Show vlan [brief | id *vlan-id* | name *vlan-name* | *summary*]	یک دستور در محیط اجرایی که اطلاعاتی را در مورد VLAN ارائه می دهد.
Show vlan [*vlan*]	نمایش اطلاعات VLAN.
Show vtp status	اطلاعات وضعیت و پیکربندی VTP را لیست می کند.
Show spanning-tree vlan *vlan-id*	یک دستور در محیط اجرایی که اطلاعاتی را در مورد Spanning Tree متعلق به یک VLAN خاص ارائه می دهد.

پیکربندی VLAN برای یک سوئیچ

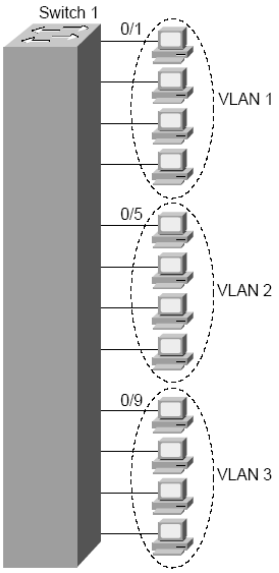
دستورات سوئیچهای ۲۹۵۰ سیسکو در پیکربندی VLAN و VTP نسبت به دستورات استفاده شده در سوئیچهای دیگر کمی تفاوت دارند. شما به محیط پیکربندی VLAN که با استفاده از اجرای دستور vlan database در محیط اجرایی وارد آن می شوید ، دسترسی خواهید داشت. بنابراین بجای استفاده از دستور configure terminal در محیط enable ، می توانید در همان محیط (enable) از دستور vlan database استفاده نمایید.

در حالت پیکربندی VLAN ، شما می توانید اطلاعات VLAN را مانند جزئیات VTP تنظیم کنید. بصورت پیش فرض ، یک سوئیچ ۲۹۵۰ حالت VTP Server را استفاده می کند ، بنابراین هر VLAN که شما پیکربندی می کنید ، در بروزرسانی های VTP شرکت داده می شود.

مثال ۱-۳ پیکربندی VLAN را در یک سوئیچ نمایش می دهد. تصویر ۸-۳ یک سوئیچ بهمراه VLAN هایی را که پیکربندی شده است ، نشان می دهد.

تصویر ۸-۳ شبکه ای با یک سوئیچ و سه VLAN

Translated by: Mahdi saghaei



مثال ۱-۳ پیکربندی VLAN بر روی یک سوئیچ ، سازگار با تصویر ۸-۳

```
Switch#vlan database
Switch(vlan)#vlan 2 name barney-2
VLAN 2 added:
    Name: barney-2
Switch(vlan)#vlan 3 name wilma-3
VLAN 3 added:
```

Translated by: Nasrali saghaei

```
    Name: wilma-3
Switch(vlan)#?
VLAN database editing buffer manipulation commands:
  abort  Exit mode without applying the changes
  apply  Apply current changes and bump revision number
  exit   Apply changes, bump revision number, and exit mode
  no     Negate a command or set its defaults
  reset  Abandon current changes and reread current database
  show   Show database information
  vlan   Add, delete, or modify values associated with a single VLAN
  vtp    Perform VTP administrative functions.

Switch(vlan)#exit
APPLY completed.
Exiting....

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fastEthernet 0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface fastEthernet 0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config)#interface range fastEthernet 0/9 - 12
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#^Z

Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                Gi0/2
2    barney-2                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
3    wilma-3                          active    Fa0/9, Fa0/10, Fa0/11, Fa0/12
```

Tran... ...aei

```
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active

Switch#show vlan id 2

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
2    barney-2                         active    Fa0/5, Fa0/6, Fa0/7, Fa0/8

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ---------------- ------------------------------------------
```

در این مثال ، کاربر کار خود را با ساختن دو VLAN جدید بنامهای barney-2 و Wilma-3 شروع می کند. سپس رابطهای ۱ تا ٤ در VLAN شماره ۱ ، رابطهای ٥ تا ۸ در VLAN شماره ۲ و رابطهای ۹ تا ۱۲ در VLAN شماره ۳ قرار داده می شوند ، همانطور که در تصویر شماره ۸-۳ پیداست. همچنین برای پیکربندی نیاز دارید تا از حالت پیکربندی VLAN استفاده کنید.

عملکرد حالت پیکربندی VLAN اندکی با حالت پیکربندی عمومی تفاوت دارد. در ابتدا ، برای ورود به حالت پیکربندی VLAN ، شما باید بجای استفاده از دستور configure terminal ، از دستور vlan database در حالت اجرایی یا همان EXEC استفاده کنید. برای اضافه کردن VLAN ها ، از دستور vlan همانطور که در تصویر بصورت vlan 2 name barney-2 و vlan 3 name Wilma-3 نشان داده شده است ، استفاده کنید. همانطور که در این مثال نشان داده شده ، دو VLAN مذکور بصورت واقعی ساخته نمی شوند ، تا هنگامی که شما پس از ساختن آنها دستور exit را استفاده کنید. قبل از اینکه پیکربندی دیگری در حالت پیکربندی VLAN اضافه کنید ، باید به سوئیچ بگویید که تغییرات را قبول کند. متوجه باشید که متن کمکی پررنگ شده که در مثال بلافاصله پس از دستور vlan نمایش داده شده است ، دلالت بر این مسئله دارد که دستور exit باعث می گردد که تغییرات ایجاد شده توسط سوئیچ مورد قبول واقع گردد ، و برعکس دستور abort باعث عدم ثبت شدن و قبول تغییرات می گردد. در مثال ، دستور exit که در هنگام خروج از حالت پیکربندی VLAN و هنگام قبول تغییرات استفاده شده ، و پیغامهای ارائه شده در زیر دستور exit ، نشان می دهد که ارائه پیغام apply completed successfully به معنای ساخته شدن موفقیت آمیز دو VLAN مورد نظر در سوئیچ می باشد.

پس از ساخته شدن VLAN ها ، حالت پیکربندی می تواند برای اختصاص هر رابط به VLAN صحیح مورد استفاده قرار گیرد. سیستم عامل ISO سیسکو ، بصورت پیش فرض هر رابط را به VLAN 1 اختصاص می دهد. بنابراین هیچ دستوری برای رابطهای fastethernet 0/1 تا fastethernet 0/4 نیاز نیست. برای چهار درگاه بعدی ، دستور switchport access vlan 2 –که در حالت زیر مجموعه رابط باید اجرا گردد– آنها را در VLAN 2 قرار می دهد (اجرای دستور switchport mode access بر روی رابطها باعث غیر فعال شدن مذاکره trunk شده و به سوئیچ می گوید که این رابطها بعنوان درگاههای دسترسی مورد استفاده قرار می گیرند ، نه برای یک ارتباط Trunk).

مثال ۱-۳ نشان می دهد که کاربر همان دستورها را برای رابطهای 0/5 تا 0/8 وارد کرده است. سیستم IOS سوئیچ اجازه می دهد که شما بیش از یک رابط را در یک لحظه (همانطور که در دستور interface range fastethernet 0/9 - 12 دیده می شود) ، پیکربندی کنید. این دستور به سوئیچ می گوید : دستورات بعدی که شما اجرا می کنید ، بر روی چهار رابط مذکور تاثیر خواهد گذاشت. بنابراین تمام چهار رابط fastethernet 0/9 تا fastethernet 0/12 ، با وارد کردن –فقط یکبار– دستور switchport access vlan 3 در VLAN 3 قرار داده می شوند.

Translated by Mahdi Shaei

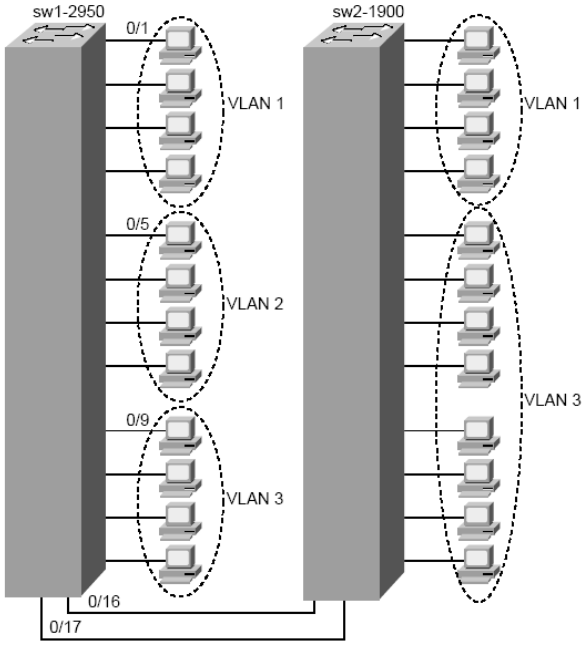
پس از بررسی پیکربندی ، شما می توانید ببینید که پیکربندی VLAN دستورات زیادی نیاز ندارد. در حقیقت ، اگر شما دستور switchport access vlan را قبل از ساختن VLAN ها در داخل حالت پیکربندی VLAN ، صادر کنید ، سوئیچ بصورت خودکار VLAN ها را ایجاد می کند. در این حالت نامهای VLAN حدس زده خواهند شد ، مانند VLAN 1 ، VLAN 2 و... .

در نهایت ، در قسمت آخر مثال ۱-۳ ، یک جفت از دستورات مهم Show لیست شده است. دستور show vlan brief یک خلاصه اجمالی از VLAN ها و رابطهای داخل هر VLAN ارائه می دهد. به بخشهای انتخاب شده مربوط به VLAN های جدید ایجاد شده ، توجه فرمایید. اگر شما به جزئیات بیشتری در مورد یک VLAN خاص احتیاج دارید ، می توانید از دستور show vlan برای لیست کردن جزئیات آن که بوسیله نام VLAN و یا شماره آن مشخص است ، دست پیدا کنید. در این حالت ، دستور show vlan id 2 ، اطلاعات مربوط به VLAN 2 را نمایش می دهد.

پیکربندی عمل Trunking در VLAN

مثال ۲-۳ همان سوئیچ مذکور در مثال قبلی را نشان می دهد ، اما با یک ارتباط trunk به سوئیچ دومی که اضافه شده و در تصویر ۹-۳ نمایش داده شده است. سوئیچ جدید یک سوئیچ سری ۱۹۰۰ است. سوئیچ ۲۹۵۰ بعنوان VTP Server با عملکرد trunking در وضعیت desirable پیکربندی شده ، و سوئیچ ۱۹۰۰ نیز یک VTP Client می باشد که با عملکرد trunking در وضعیت auto تنظیم شده است.

تصویر ۹-۳ شبکه ای با دو سوئیچ و سه VLAN



مثال ۲-۳ عمل Trunking : پیکربندی و دستورات show بر روی سوئیچ ۲۹۵۰ ، شماره ۱

Translated by Ali saghaei

```
sw1-2950#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
sw1-2950(config)#interface fastethernet 0/17
sw1-2950(config-if)#switchport mode dynamic desirable
sw1-2950(config-if)#^Z
sw1-2950#vlan database
sw1-2950(vlan)#vtp domain fred
Changing VTP domain name from NULL to fred
sw1-2950(vlan)#exit
APPLY completed.
Exiting....

sw1-2950#show vtp status
VTP Version                     : 2
Configuration Revision          : 1
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 7
VTP Operating Mode              : Server
VTP Domain Name                 : fred
```

Translated by: Mahdi Shaei

```
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : 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)

sw1-2950#show interfaces fastEthernet 0/17 switchport
Name: Fa0/17
Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: trunk
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: isl
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

sw1-2950#show interfaces fastEthernet 0/17 trunk

Port      Mode         Encapsulation  Status        Native vlan
Fa0/17    desirable    n-isl          trunking      1

Port      Vlans allowed on trunk
Fa0/17    1-4094

Port      Vlans allowed and active in management domain
Fa0/17    1-3

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/17    1-3
!
! Next command from sw2-1900
!
sw2-1900#show vlan

VLAN Name             Status     Ports
----------------------------------------
1    default          Enabled    1-12, AUI, A, B
2    barney-2         Enabled
3    wilma-3          Enabled
1002 fddi-default     Suspended
1003 token-ring-defau Suspended
1004 fddinet-default  Suspended
1005 trnet-default    Suspended
----------------------------------------
```

این مثال با پیکربندی رابط 0/17 بعنوان یک trunk آغاز می شود. اجرای دستور switchport mode dynamic desirable بر روی سوئیچ SW1 باعث می گردد که رابط مذکور کار مذاکره از طریق یک trunk را آغاز کند. مذاکره برای این است که سوئیچ بفهمد آیا عمل trunking را باید برای همه مواقع استفاده کند و همچنین آیا trunking را برای پروتکل ISL می خواهد استفاده کند یا برای 802.1Q ؟. سوئیچ SW2 (سری ۱۹۰۰) تنظیم auto را برای trunk خود استفاده می کند ، بنابراین باعث می گردد که ارتباط مذکور در حالت trunk کار کند.

گزینه های پیکربندی برای دستورات trunk بر روی سوئیچهای سیسکو ممکن است کمی گیج کننده باشد. بیشترین نمونه اشتباه در این مورد ، پیکربندی دو سمت ارتباط بصورت dynamic auto می باشد. اگر شما هر دو سمت ارتباط را بصورت auto تنظیم کنید ، trunk هرگز ایجاد نمی شود و شما نمی توانید ترافیک VLAN را از طریق ارتباط مذکور عبور دهید.

در شبکه های عادی ، شما ممکن است یک پیکربندی ساده را برای فعال کردن trunk انتخاب کنید ، بویژه به این دلیل که شما می دانید کدام درگاهها باید trunk باشند. در عین حال ، گزینه های auto و desirable به شما اجازه می دهند که بدون نیاز به ایجاد توقف در جریان ترافیک ، trunk ها را از راه دور پیکربندی نمایید.

جدول ۵-۳ گزینه های متفاوت trunking را بهمراه مفاهیم آنها بر روی سوئیچ ۲۹۵۰ ، بصورت خلاصه ارائه کرده است.

جدول ۵-۳ گزینه های پیکربندی trunk بر روی سوئیچ ۲۹۵۰ بهمراه دستور switchport mode

گزینه	توضیح	عملکرد Trunking
Access	حالت trunk را بر روی درگاه غیر فعال کرده و هیچگونه تلاشی برای عمل trunk بر روی آن رابط انجام نمی دهد.	Trunk نمی کند.
Trunk	درگاه را بصورت دائمی در حالت trunk پیکربندی کرده و با دستگاه متصل بخود مذاکره می کند برای اینکه تصمیم بگیرد آیا از ISL استفاده کند یا از 802.1Q ؟	همیشه براساس trunk عمل می کند.
Dynamic desirable	باعث می گردد که درگاه عمل مذاکره را از حالت عادی به حالت trunk تغییر دهد ، یعنی سعی می کند که با هدف ارتباط trunk مذاکره کند. درصورتی که دستگاه متصل شده به درگاه در یکی از حالتهای trunk , dynamic desirable و یا dynamic auto پیکربندی شده باشد ، مذاکره بر مبنای trunk خواهد بود. در غیر اینصورت درگاه مذکور ، یک درگاه عادی خواهد بود.	عمل trunk زمانی برقرار و اجرا می شود که دستگاه یا سوئیچ متصل شده به درگاه در یکی از حالتهای trunk ، dynamic desirable و یا dynamic auto تنظیم شده باشد.
Dynamic auto	فقط زمانی اجازه می دهد که درگاه یک ارتباط trunk برقرار کند که دستگاه متصل شده به آن ، در یکی از حالتهای dynamic desirable یا trunk تنظیم شده باشد.	عمل trunk زمانی برقرار و اجرا می شود که دستگاه یا سوئیچ متصل شده به درگاه در یکی از حالتهای dynamic desirable و یا trunk تنظیم شده باشد.

در ادامه مثال ۲-۳ ، از حالت پیکربندی VLAN برای تنظیم نام دامنه VTP با استفاده از دستور vtp domain fred استفاده شده است. سوئیچ SW1 نیازی به پیکربندی بعنوان VTP Server ندارد ، بدلیل اینکه سوئیچهای سیسکو بصورت پیش فرض VTP Server هستند. سوئیچ SW2 در داخل دامنه

Translated by: Mahdi saghaei

fred بعنوان VTP Client پیکربندی شده ، بنابراین به درستی با VTP کار می کند. همچنین SW1 احتیاج دارد تا دامنه VTP مذکور (fred) را استفاده کند. دستور show vtp نشان می دهد که سوئیچ SW1 در داخل دامنه fred بعنوان VTP Server شناخته شده است.

برای اینکه متوجه شوید آیا ارتباط بین دو رابط بصورت trunk برقرار شده یا خیر ، می توانید یکی از دستورهای show interface fastethernet 0/17 switchport یا show interface fastethernet 0/17 trunk را بر روی سوئیچ SW1 استفاده کنید. همانطور که در تصویر ۲-۳ نشان داده شده ، هر دو دستور تنظیمات پیکربندی (شامل dynamic desirable) ، وضعیت ها (وضعیت trunking که به معنی کار کردن و فعال بودن عمل trunking است) و پروتکل اجرا کننده trunk را که در این مثال ISL می باشد ، لیست می کند (سوئیچ های سری ۱۹۰۰ فقط پروتکل ISL را پشتیبانی می کنند).

با عملکرد پروتکل trunking و کارکرد صحیح vtp که باعث توزیع اطلاعات پیکربندی VLAN می شود ، سوئیچ SW2 باید در مورد VLANهای ۲ و ۳ اطلاعات لازم را فرا بگیرد. آخرین دستور در مثال ۲-۳ که از سوئیچ SW2 گرفته شده ، نشان می دهد که سوئیچ مذکور اطلاعات لازم را در مورد VLANهای barney-2 و Wilma-3 یاد گرفته است.

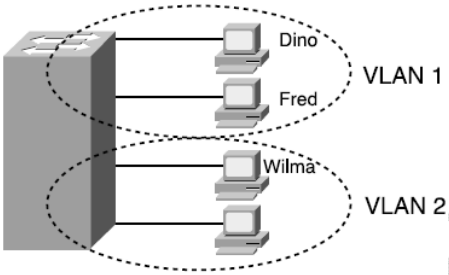
Translated by: Mahdi saghaei

خلاصه مطالب اصلی

بخش "خلاصه مطالب اصلی" مهمترین موارد این فصل را برای شما لیست می کند. با اینکه این بخش شامل تمام اطلاعات لازم برای امتحان نمی شود ، اما یک کاندیدای امتحان CCNA باید تمام جزئیات ذکر شده در بخش :خلاصه مطالب اصلی" را قبل از امتحان مطالعه کرده و با آنها آشنا باشد.

تصویر ۱۰-۳ یک ایده عمومی را برای یک VLAN نشان می دهد ، که شامل دو VLAN بهمراه دو محدوده فراگیر متفاوت می باشد.

تصویر ۱۰-۳ شبکه ای با دو VLAN که از یک سوئیچ استفاده می کنند.



جدول ٦-۳ گزینه ها و نکات کلیدی متفاوت بین ISL و 802.1Q را بصورت خلاصه نمایش می دهد.

جدول ٦-۳ مقایسه ISL و 802.1Q

وظیفه	ISL	802.1Q
سازمان استاندادری که پروتکل را تعیین می کند.	اختصاصی برای سیسکو	سازمان IEEE
پوشش گذاری فریم اصلی	بله	خیر
اجازه استفاده از چندین Spanning Tree	بله	خیر
استفاده از VLAN های بومی	خیر	بله

جدول ۷-۳ یک مرور کلی را درباره سه وضعیتVTP ارائه می کند.

جدول ۷-۳ وضعیتهای VTP

وظیفه	وضعیت Server	وضعیت Client	وضعیت Transparent
سرچشمه اطلاع رسانیVTP	بله	خیر	خیر
پردازش پیغامهای اطلاع رسانی دریافت شده و همسان سازی اطلاعات پیکربندی VLAN با سوئیچ های دیگر	بله	بله	خیر
Forward کردن پیغامهای اطلاع رسانی VTP دریافت شده از طریق ارتباط trunk.	بله	بله	بله
ذخیره پیکربندی VLAN در داخل NVRAM	بله	خیر	بله
توانایی ساخت ، اصلاح یا حذف VLANها با استفاده از دستورات پیکربندی	بله	خیر	بله

Translated by: Mahdi saghaei

جدول ۸-۳ گزینه های متفاوت Trunking را بر روی سوئیچ ۲۹۵۰ بهمراه مفاهیم آنها ارائه کرده است.

گزینه	توضیح
Access	وضعیت trunk را بر روی درگاه غیر فعال کرده و تلاشی برای برقراری ارتباط از طریق trunk بر روی رابط مذکور انجام نمی دهد.
Trunk	درگاه مورد نظر را بصورت دائمی در وضعیت trunk قرار داده و با دستگاه متصل شده مذاکره می کند تا ببیند آیا باید برای trunk از ISL استفاده یا 802.1Q ؟
Dynamic desirable	باعث می گردد که درگاه عمل مذاکره را از حالت عادی به حالت trunk تغییر دهد ، یعنی سعی می کند که با هدف ارتباط trunk مذاکره کند. درصورتی که دستگاه متصل شده به درگاه در یکی از حالتهای dynamic desirable , trunk و یا dynamic auto پیکربندی شده باشد ، مذاکره بر مبنای trunk خواهد بود. در غیر اینصورت درگاه مذکور ، یک درگاه عادی و بدون trunk خواهد بود.
Dynamic auto	فقط زمانی اجازه می دهد که درگاه یک ارتباط trunk برقرار کند ، که دستگاه متصل شده به آن ، در یکی از حالتهای dynamic desirable یا trunk تنظیم شده باشد.

Translated by: Mahdi Saghaei

سوال و جواب

با مرور این سوالات که بمراتب سخت تر هستند ، می توانید حافظه خود را بهتر تمرین داده و درک واقعی وعملی خود را نسبت به این فصل اثبات کنید. جواب این سوالات را می توانید در ضمیمه A بیابید.

برای تمرین بیشتر با سوالاتی شبیه سوالات آزمون اصلی CCNA ، مانند سوالات چند جوابی و نیز حل آنها از طریق شبیه ساز روتر ، از شبیه ساز داخل CD استفاده کنید.

۱. دامنه فراگیر را تعریف کنید.
۲. VLAN را تعریف کنید.
۳. اگر دو سوئیچ LAN سیسکو ، با استفاده از FastEthernet به یکدیگر متصل شوند ، کدامیک از پروتکلهای trunking می توانند استفاده شوند ؟ اگر فقط یک VLAN آن دو سوئیچ را پوشش دهد ، آیا احتیاجی به پروتکل trunking در VLAN وجود دارد؟
٤. VTP را تعریف کنید.
٥. سه وضعیت VTP را نام ببرید. کدامیک از وضعیت ها اجازه نمی دهد که VLAN اضافه یا اصلاح گردد؟
٦. کدامیک از دستورات سوئیچ ۲۹۵۰ عمل trunking را بر مبنای ISL بر روی درگاه fastethernet 0/12 پیکربندی می کند ؟ آیا در صورتیکه درگاه سوئیچ در انتهای دیگر ارتباط غیر فعال نشده و یا بصورتی پیکربندی شده باشد که برای ارتباط trunk مذاکره نکند ، آیا ارتباط بصورت قطعی در وضعیت trunk قرار خواهد گرفت ؟
۷. کدامیک از وضعیتهای VTP اجازه می دهد که یک سوئیچ VLANها را ایجاد کرده و آنها را به سوئیچهای دیگر انتشار دهد؟
۸. آیا تمام اعضای یک VLAN در داخل یک محدوده برخورد یکسان قرار دارند ؟ یا در داخل یک دامنه فراگیر یکسان ؟ یا هر دو؟
۹. پروتکل trunking انحصاری سیسکو بر روی اترنت کدام است؟
۱۰. عملکرد VTP Pruning را بصورت خلاصه توضیح دهید؟
۱۱. اصطلاح "یک VLAN محدوده ای فراگیر است که با یک محدوده IP برابر می باشد" را بررسی کنید. آیا شما آن را تایید می کنید ؟ یا خیر ؟ چرا ؟
۱۲. چه فیلدهایی بر روی header اترنت در هنگام استفاده از پروتکل 802.1Q اضافه شده و یا تغییر می کنند؟ شماره VLAN در کدامیک از آن فیلدها جای میگیرد؟
۱۳. توضیح دهید که یک سوئیچ در وضعیت VTP Transparent چگونه با پیغامهای VTP دریافتی از یک VTP Server رفتار می کند؟
۱٤. چه دستوری بر روی سوئیچ ۲۹۵۰ ، VLAN شماره ٥ را می سازد؟ کدام وضعیت پیکربندی مورد نیاز است؟
۱٥. کدام دستور بر روی سوئیچ ۲۹۵۰ یک رابط را در VLAN شماره ٥ قرار می دهد ؟ کدام وضعیت پیکربندی مورد نیاز است؟
۱٦. تفاوتهای اصلی فرایندهای استفاده شده در حالت پیکربندی VLAN و حالت پیکربندی عادی را توضیح دهید.
۱۷. ترکیب دستوراتی را که یک رابط را در وضعیتهای متفاوت trunking قرار می دهند ، ارائه دهید. همچنین مشخص کنید کدام دستورات هنگامی که سوئیچ طرف دیگر ارتباط گزینه auto را استفاده کرده است ، کار می کنند؟
۱۸. کدامیک از دستورات show در سوئیچ ۲۹۵۰ وضعیت پیکربندی و عملیاتی trunk را نمایش می دهد؟

Translated by: Mahdi saghaei