آموزش رایگان دوره Network+ (بخش 50)

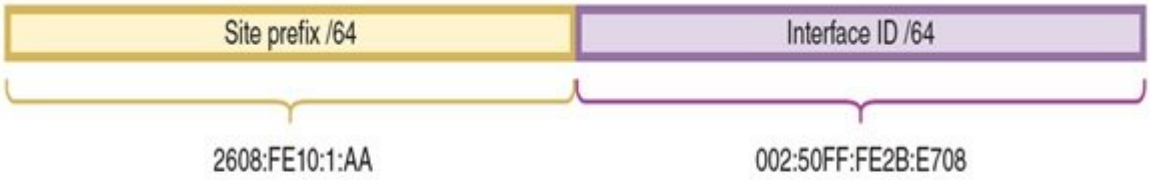
در شماره گذشته آموزش نتورک‌پلاس با جداول الگوهای زیرشبکه، الگوهای زیرشبکه با طول متغیر (VLSM) و پیاده‌سازی زیرشبکه‌ها و تقسیم زیرشبکه‌ها به شبکه‌های کوچک‌تر مطالبی آموختیم. در این شماره مبحث زیرشبکه‌های IPv6 و VLANها را آغاز خواهیم کرد.

برای مطالعه بخش چهل و نهم آموزش رایگان و جامع نتورک پلاس (Network+) اینجا کلیک کنید

زیرشبکه‌ها در IPv6

اگر به خاطر داشته باشید به شما گفتیم آدرس‌های IPv6 از 128 بیت تشکیل شده‌اند که در مقایسه با آدرس‌های 32 بیتی IPv4 طولانی‌تر هستند. این بدان معنا است که 2128 آدرس IPv6 در مقایسه با 232 آدرس IPv4 در دسترس است. با توجه به تعدد آدرس‌ها، یک ISP می‌تواند به هر یک از مشتریان خود یک زیرشبکه کامل IPv6 یا به عبارتی هزاران آدرس اختصاص دهد که در مقایسه با آدرس‌های IPv4 که باید میان تمام گره‌های یک شرکت به اشتراک گذاشته شوند رقم قابل توجهی است. در این حالت، زیرشبکه‌سازی به مدیران شبکه کمک می‌کند تا حجم زیادی از آدرس‌های IPv6 را به شکل بهتری مدیریت کنند. زیرشبکه‌سازی در IPv6 به مراتب ساده‌تر از زیرشبکه‌سازی در IPv4 است و البته تفاوت‌هایی نیز با IPv4 دارد که از آن جمله به موارد زیر می‌توان اشاره کرد:

• آدرس‌دهی IPv6 از رویکرد بدون کلاس استفاده می‌کند. در IPv6 هیچ معادلی برای شبکه‌های کلاس A، B یا C وجود ندارد. هر آدرس IPv6 فارغ از کلاس است.



• IPv6 از الگوهای زیرشبکه استفاده نمی‌کند.

• یک زیرشبکه IPv6 قادر به ارائه 18،446،744،073،709،551،616 آدرس IPv6 است.

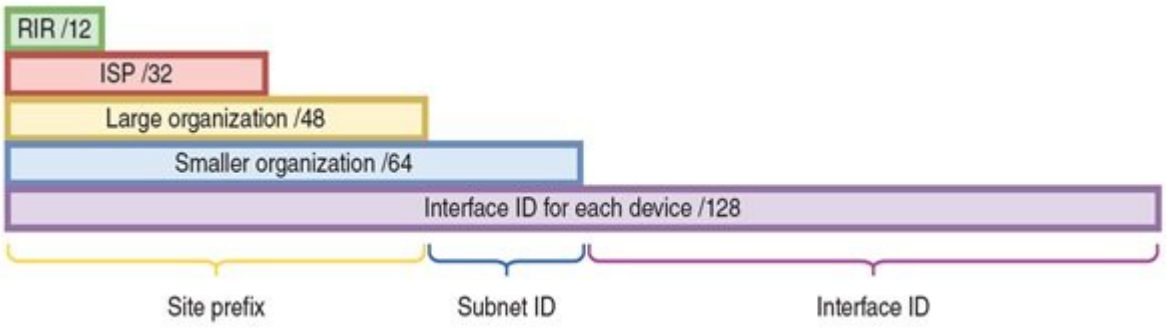
یک آدرس تک‌یاب (Unicast) یک آدرس اختصاص داده شده به یک واسط واحد در شبکه است. به شما گفتیم هر آدرس تک‌یابی می‌تواند در فرم دودویی نشان داده شود، اما بیشتر به صورت هشت بلوک متشکل از کاراکترهای چهارتایی هگزا که با دونقطه از یکدیگر ها جدا شده‌اند، نوشته می‌شود. به‌طور مثال، آدرس IPV6 زیر یک آدرس معتبر است.

2608:FE10:1:AA:002:50FF:FE2B:E708

حالا آدرس فوق را به بخش‌های زیر تقسیم می‌کنیم:

• چهار بلوک آخر که برابر با 64 بیت انتهایی هستند برای شناسایی رابط استفاده می‌شوند. (در بسیاری از شبکه‌های IPv6، این 64 بیت بر اساس نسخه IEEE-64 رابط کاربری MAC هر دستگاه است.)

• چهار بلوک اول که برابر با 64 بیت ابتدایی هستند برای شناسایی شبکه استفاده شده و پیشوند شبکه، پیشوند مکانی یا پیشوند مسیریابی سراسری نامیده می‌شوند. شکل زیر این موضوع را نشان می‌دهد.



در آدرس زیر

2608:FE10:1:AA:002:50FF:FE2B:E708

پیشوند مکانی

2608:FE10:1:AA

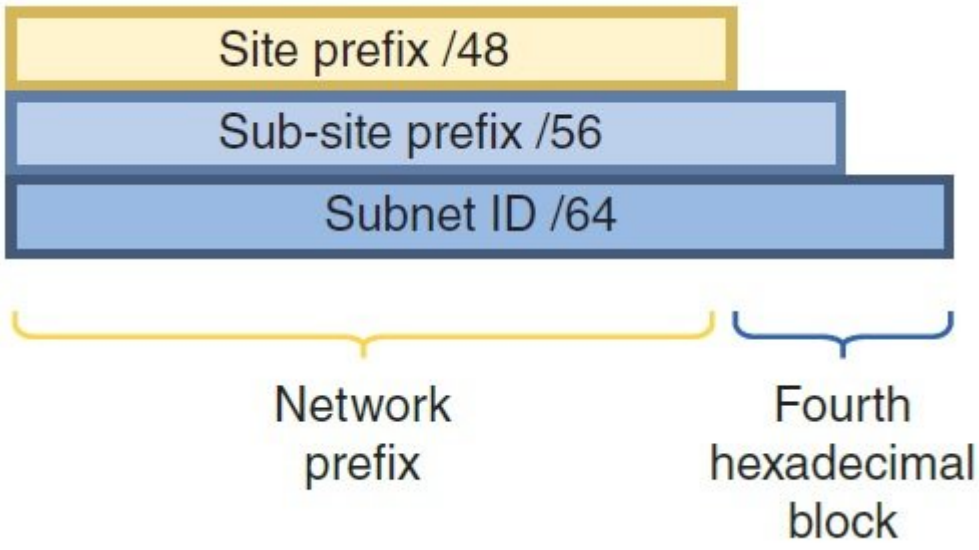
و شناسه رابط به صورت زیر است.

002:50FF:FE2B:E708

شما ممکن است پیشوندهای مکانی را به‌طور مثال به صورت زیر نیز مشاهده کنید که تعداد بیت‌هایی را نشان می‌دهند که شبکه را شناسایی می‌کنند.

2608:FE10:1:AA::/64

• چهارمین بلوک هگزادسیمال در پیشوند مکانی را می‌توان برای ایجاد زیرشبکه در مکانی تغییر داد. اجازه دهید نگاه دقیق‌تری به چگونگی شکل‌گیری این بلوک‌ها در قالب یک تصویر بزرگ داشته باشیم. در شکل زیر یک ثبت اینترنت منطقه‌ای (RIR) سرنام regional Internet registry ممکن است به یک ISP بلوکی از آدرس‌هایی که 32 بیت پیشوند مسیریابی همچون FE10::/32:2608 را به اشتراک قرار می‌دهند تخصیص دهد. ISP، به نوبه خود، ممکن است یک بلوک از آدرس‌هایی که یک پیشوند مکانی 48 بیتی یکسانی را به‌اشتراک قرار می‌دهند همچون FE10:1::/48:2608 را تخصیص دهد و مشتریان کوچک‌تر کسب‌وکار نیز ممکن است یک پیشوند مکانی 56 بیتی، همچون FE10:1:AA:://56:2608، یا یک پیشوند مکانی 64 بیتی، همچون FE10:1:AA::/64:2608 را دریافت کنند.



شناسه یک زیرشبکه، یک بلوک طولانی است که چهار کاراکتر هگزادسیمال یا 16 بیت در واحد دودویی دارد. یک سازمان با یک پیشوند مکانی /48 می‌تواند از تمام 16 بیت برای ایجاد 65،536 زیرشبکه استفاده کند. یک پیشوند مکانی / 56 می‌تواند تا 256 زیرشبکه ایجاد کند. یک پیشوند مکانی /64 تنها با یک زیرشبکه واحد حاوی بیش از 18 کوارتردسیلیون آدرس میزبانی ($۱۰^{۴۵}$) است که بیش از دو برابر مقدار تخمینی دانه‌های شن در تمام سواحل و بیابان‌های زمین است! همان‌گونه که می‌بینید، IPv6 اجازه می‌دهد تا تعداد زیادی از میزبان‌های بالقوه در یک شبکه واحد در اختیار داشته باشید.

اجازه دهید به یک شبکه فرضی با یک پیشوند مکانی FE10:1/48:2608 نگاهی داشته باشیم و ببینیم چه اتفاقی برای بلوک بعدی بیت‌ها در سطح دودویی رخ می‌دهد. در مبنای دودویی آن بلوک چهارم، شناسه زیرشبکه می‌تواند به‌طور کامل صفر

0000 0000 0000 0000

یا به‌طور کامل یک باشد.

1111 1111 1111 1111

و سپس ترکیبی از حالت‌های زیر باشد:

0001 0000 0000 0000

0010 0000 0000 0000

0011 0000 0000 0000

0100 0000 0000 0000

...

1100 1111 1111 1111

1101 1111 1111 1111

1110 1111 1111 1111

در این‌جا 65،536 هزار زیرشبکه ممکن است. یک شبکه نمونه با یک پیشوند مکانی به صورت زیر

2608:FE10:1:AA/56

می‌تواند با هشت بیت برای ایجاد 256 زیرشبکه ممکن به صورت زیر کار کند:

0000 0000

0001 0000

0010 0000

...

1101 1111

1110 1111

1111 1111

گاهی اوقات سازمان‌ها این بلوک را به زیر بلوک‌ها و شناسه‌های زیرشبکه تقسیم می‌کنند. به‌طور مثال، شکل زیر را در نظر بگیرید که بلوک Subnet ID به دو سطح مختلف مدیریت می‌شود: نیمه اول برای زیرمکان‌ها (مانند دفاتری در شهرهای مختلف) و نیمه دوم برای زیرشبکه‌هایی در هر مکانی(مانند طبقات یک ساختمان یا اداره).

برای تسلط بر مبحث محاسبه زیرشبکه ها در پروتکل IPv6 هیچ چیز بهتر از تمرین نیست. برای یادگیری نحوه محاسبه زیرشبکه‌ها نیازی نیست ریاضی را در حد استادی بلد باشید، اما برای موفقیت در آزمون **نتورک‌پلاس** باید نحوه محاسبه زیرشبکه‌ها را خوب یاد گرفته باشید.

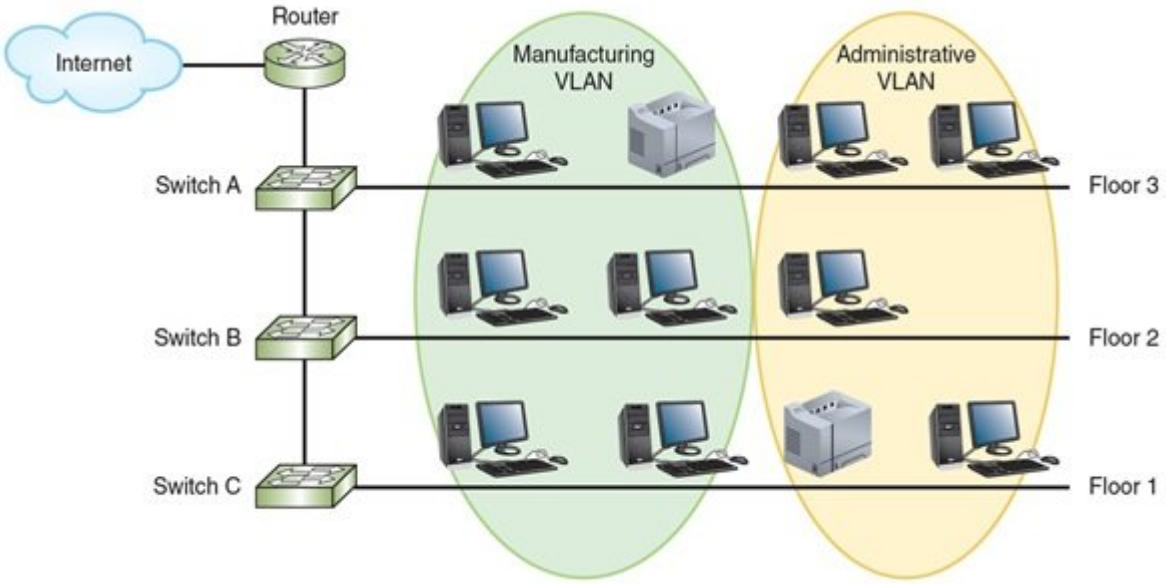
اکنون که یاد گرفتید چگونه زیرشبکه‌ها در لایه شبکه پیاده‌سازی می‌شوند و تفاوت آن‌ها در آدرس‌های IPv4 و IPv6 را مشاهده کردید، زمان آن رسیده است درباره نحوه تقسیم شبکه در لایه پیوند داده که منجر به شکل‌گیری شبکه‌های محلی مجازی (VLAN) می‌شود اطلاعاتی به دست آورید.

شبکه‌های محلی مجازی

اجازه دهید کار را با شباهت‌ها و تفاوت‌های زیرشبکه‌ها و شبکه‌های محلی مجازی شروع کنیم. یاد گرفتیم، یک گروه از آدرس‌های آی‌پی زیرشبکه می‌توانند کلاینت‌ها را روی یک شبکه بزرگ به شکل منطقی در قالب شبکه‌های کوچک‌تر سازمان‌دهی کنند. این کار اغلب با اضافه کردن روترها (یا سوییچ لایه 3) به شبکه یا با استفاده از چندین پورت روی یک روتر واحد (یا سوییچ لایه 3) انجام می‌شود. در این تکنیک با زیرشبکه‌هایی که آدرس آی‌پی موجود را سازمان‌دهی می‌کنند، شبکه‌های محلی چندگانه درون یک شبکه بزرگ‌تر ایجاد می‌شوند.

در مقابل، یک شبکه محلی مجازی (VLAN) سرنام Virtual Local Area Networks پورت‌ها را روی سوئیچ لایه 2 گروه بندی می‌کند، به طوری که مقداری از ترافیک محلی روی سوییچ مجبور می‌شوند از طریق روتر انتقال پیدا کنند تا ترافیک به یک دامنه پخشی کوچک‌تر محدود شود. همان‌گونه که از نام VLAN پیدا است، شبکه‌های محلی مجازی دامنه پخشی را از سخت‌افزار شبکه انتزاعی می‌کنند. این رویکرد شبیه به انتزاعی کردن عملکردهای محاسباتی ماشین‌های مجازی در قبال سخت‌افزار کامپیوتر است. هنگام استفاده از VLANها، محدوده دامنه پخشی را می‌توان تقریبا در هر مکانی در یک شبکه محلی فیزیکی تعریف کرد.

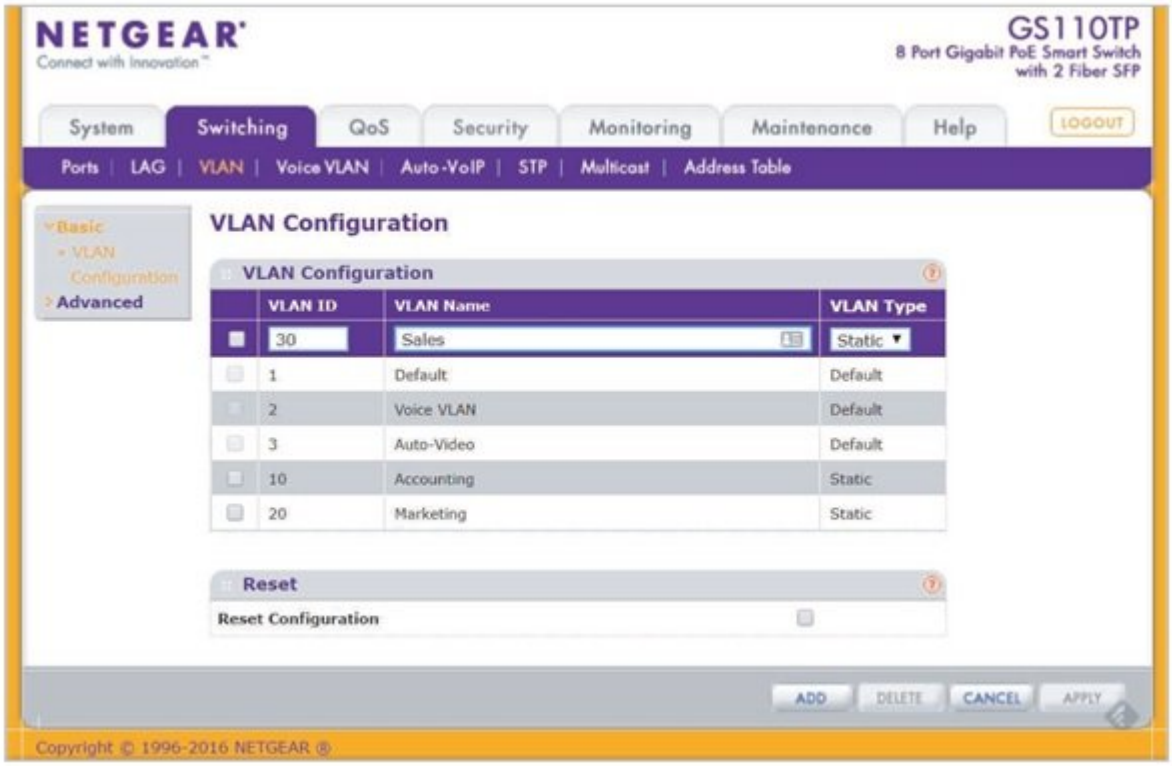
اگر به خاطر داشته باشید ابتدای مبحث زیرشبکه‌سازی مثالی زدیم که یک شبکه بزرگ در سه طبقه یک ساختمان پیاده‌سازی شده بود. به جای قرار دادن روترهای جدید در هر طبقه ساختمان، شما می‌توانید از سوییچ‌های مدیریت شده و VLAN ها برای تقسیم شبکه استفاده کنید. به‌طور مثال، فرض کنید شما شبکه را به جای آن‌که بر مبنای طبقات ساختمان تقسیم کنید بر منبای دپارتمان تقسیم می‌کنید. (شکل زیر)



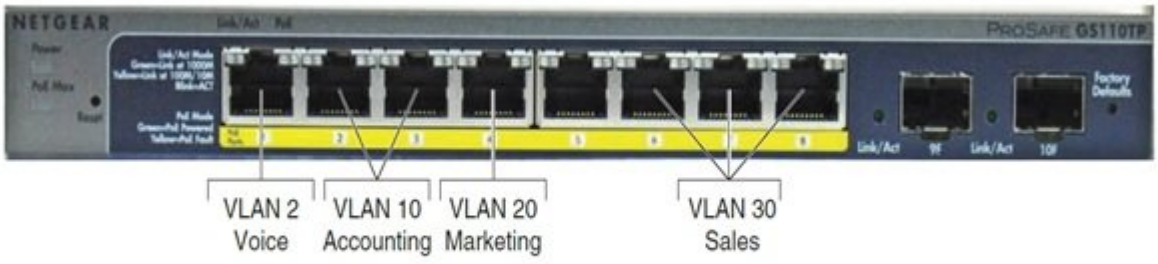
برای انجام این‌کار و در صورت لزوم سوییچ‌های مدیریتی را جایگزین سوییچ‌های اصلی می‌کنید. (ممکن است این‌کار ضرورتی نداشته باشد، زیرا بسیاری از شرکت‌ها قابلیت از پیش ساخته شده VLAN در اختیار دارند.) در مرحله بعد، شما هر میزبان را به یک VLAN خاص اختصاص می‌دهید. شما این‌کار را با پیکربندی پورت سوییچ که به هر میزبان متصل شده است کامل می‌کنید. برای آن‌که شناخت بهتری از VLAN و تفاوت آن با زیرشبکه‌ها به دست آورید پیشنهاد می‌کنم **مطلب تفاوت بین VLAN و Subnet در چیست؟** را مطالعه کنید.

سوییچ مدیریتی (Managed switch)

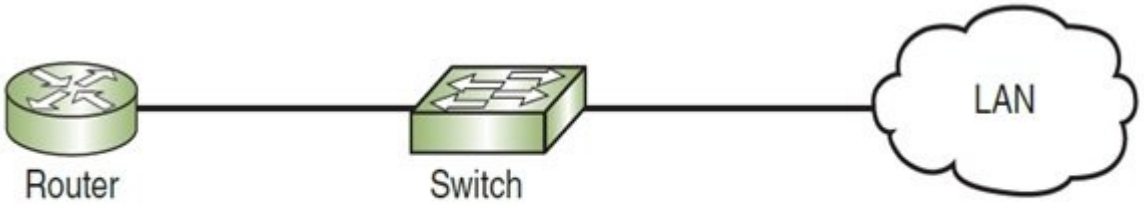
یک سوییچ غیرمدیریتی، یک مکانیزم ساده نصب را با حداقل گزینه‌های پیکربندی ارائه کرده و هیچ آدرس آی‌پی اختصاصی ندارد. سوییچ‌های غیر مدیریتی بسیار گران هستند، اما قابلیت‌های آن‌ها محدود است و نمی‌توانند از VLAN پشتیبانی کنند. در سوی دیگر، سوییچ های مدیریتی قرار دارند که می‌توان از طریق یک رابط خط فرمان یا GUI مبتنی بر وب آن‌ها را پیکربندی کرده و گاهی اوقات می‌توانند گروهی پیکربندی شوند.



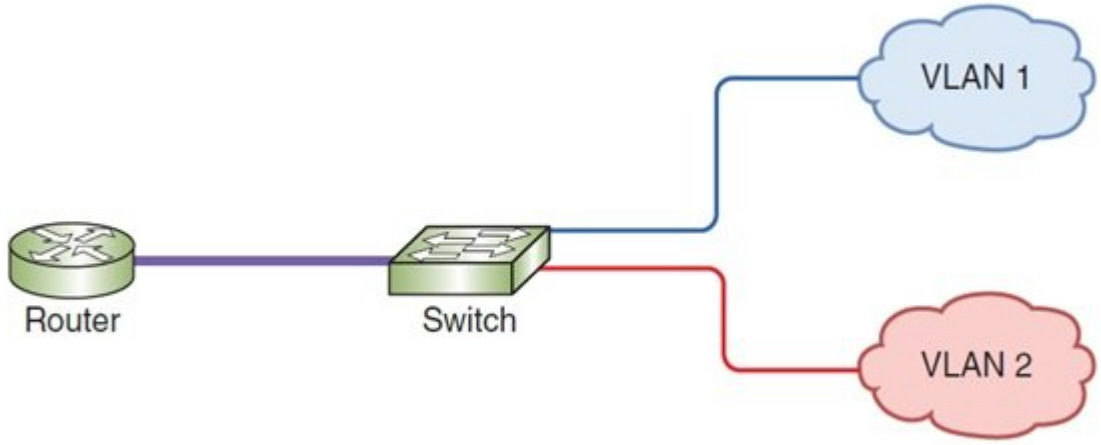
به‌طور معمول و برای مدیریت مداوم این سوییچ‌ها آدرس‌های IP به آن‌ها تخصیص داده می‌شود. VLANها می‌توانند تنها از طریق سوییچ‌های مدیریت شده که پورت‌های آن‌ها می‌توانند به گروه‌هایی تقسیم شوند، پیاده‌سازی شوند. شکل زیر پورت‌های سوییچی را نشان می‌دهد که برای VLANهای موجود در رابط مدیریت سوئیچ شکل بالا پیکربندی شده‌اند.



همان‌گونه که می‌دانید سوییچ‌ها دستگاه‌های لایه 2 هستند. (البته، سوییچ‌های لایه 3 نیز وجود دارد، اما این دستگاه‌ها نقش روترها و نه سوییچ‌ها را در لایه 3 بازی می‌کنند.) با مرتب‌سازی ترافیک بر اساس اطلاعات لایه 2، VLANها دو یا چند دامنه پخشی را از یک دامنه پخشی مجزا ایجاد می‌کنند. اجازه دهید نحوه این‌کار را مشاهده کنیم. شکل زیر عملکرد یک سوییچ عادی لایه 2 را نشان می‌دهد. این سوییچ تمامی ترافیک شبکه را روی شبکه محلی مدیریت می‌کند، مگر اینکه یک میزبان در شبکه بخواهد با یک میزبانی در شبکه دیگری ارتباط برقرار کند، در این حالت ترافیک از طریق روتر عبور می‌کند.



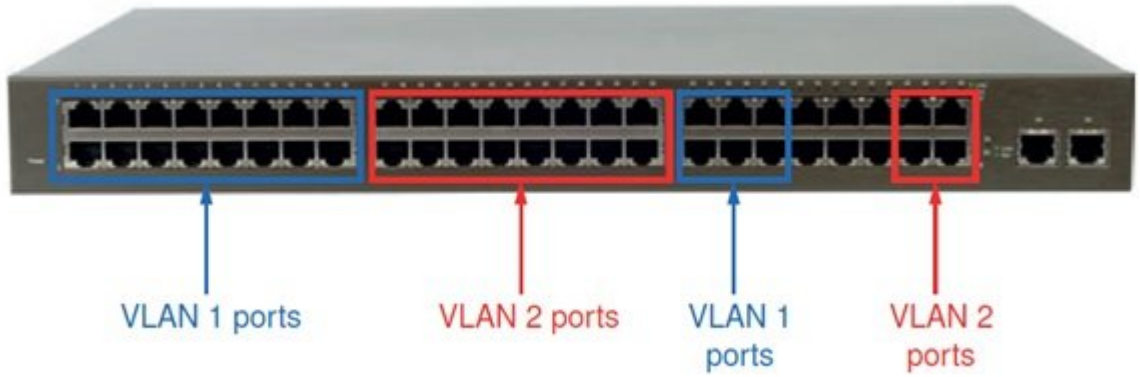
شکل زیر نشان می‌دهد که چه اتفاقی می‌افتد زمانی که پورت‌های سوییچ مدیریتی به دو پارتیشن تقسیم شده و به دو VLAN اشاره می‌کنند.



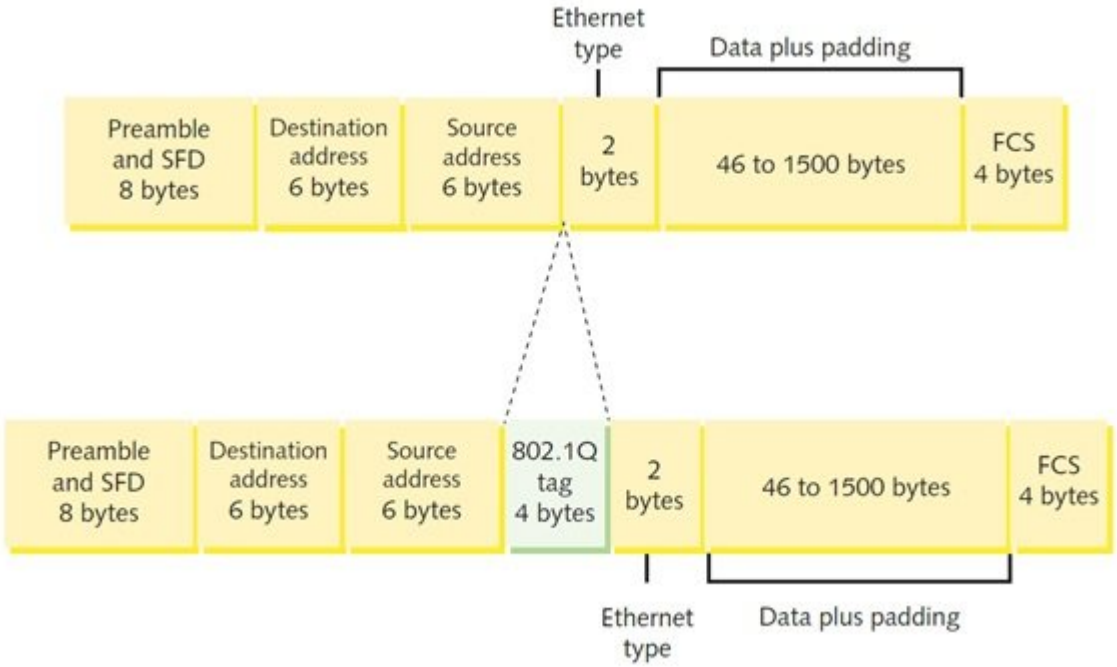
دقت کنید ترافیک درون هر VLAN هنوز هم از طریق سوییچ انتقال پیدا کرده و به دستگاه‌های دیگر در VLAN می‌رود و همچنین ترافیک به سمت میزبان‌ها در شبکه‌های دیگر هنوز از طریق روتر هدایت می‌شود. با این حال، در این

حالت ترافیک میان میزبان‌ها در VLAN 1 و VLAN 2 باید از طریق روتری که مسیریابی-بین شبکه محلی مجازی نامیده می‌شود، انجام شود. این یک پیکربندی ساده VLAN است، جایی که یک روتر به یک سوییچ که از چند VLAN پشتیبانی می‌کند، متصل می‌شود که گاهی اوقات ROAS (router on a stick) نامیده می‌شود.

نمای بصری حالتی که بالا به آن اشاره شد در دنیای واقعی شبیه به تصویر زیر است.

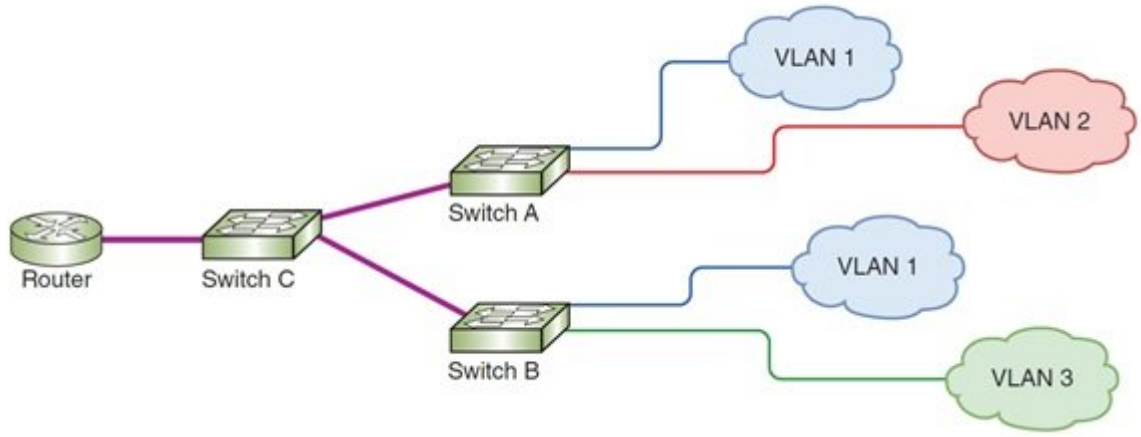


برای شناسایی این مسئله که انتقال متعلق به کدام VLAN است، سوئیچ یک تگ (tag) به فریم‌های اترنت اضافه می‌کند که پورتی که قرار است به آن برسند را مشخص می‌کند. این شناسه‌گر VLAN در استاندارد 802.1Q که استاندارد IEEE برای نحوه نمایش اطلاعات VLAN در فریم‌ها و نحوه تفسیر این اطلاعات از سوی سوییچ‌ها است مشخص شده است. توجه داشته باشید که استاندارد 802.1Q گاهی اوقات dot1q نامیده می‌شود. همچنین اطلاعات مربوط به پورت مورد نیاز این استاندارد گاهی به نام برچسب 802.1Q یا برچسب dot1q معروف است. شکل زیر نشان می‌دهد که کدام برچسب 802.1Q در سرباره فریم اترنت اضافه شده است.



برچسب تا زمانی که به یک روتر یا پورت سوئیچ متصل به دستگاه مقصد نهایی نرسد، ارسال می‌شود. در این لحظه، برچسب از فریم حذف می‌شود. اگر فریم به یک VLAN جدید هدایت شود، روتر یک تگ جدید در این نقطه اضافه می‌کند که پس از آن‌که فریم به پورت سوییچ نهایی رسید، حذف می‌شود. در اغلب موارد، نه دستگاه ارسالی و نه دستگاه دریافتی از زیرساخت VLAN اطلاعی ندارند. مشاهده کردید که یک سوییچ می‌تواند بیش از یک VLAN را پشتیبانی کند. به‌طور مشابه، یک VLAN می‌تواند پذیرای پورت‌هایی از سوی بیش از یک سوییچ باشد. فرض کنید ما

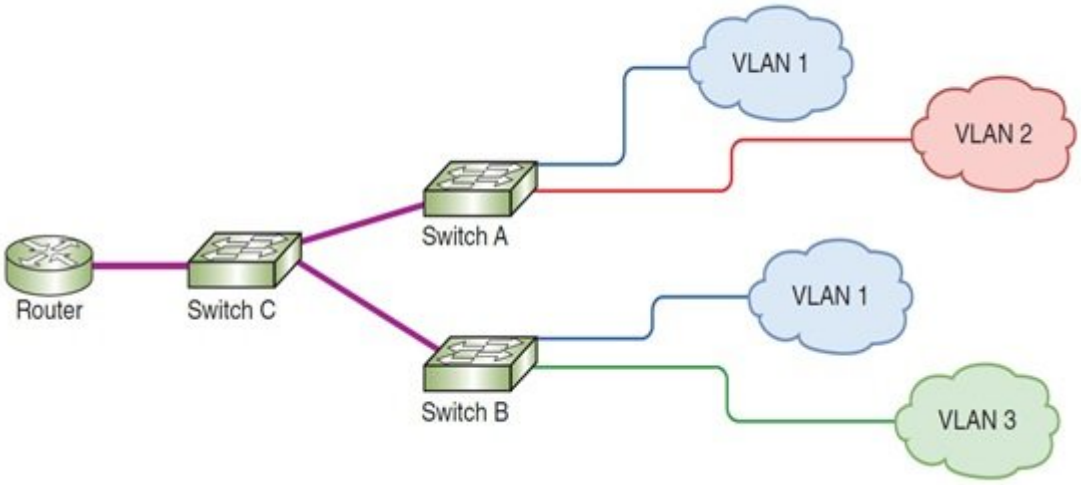
دو سوییچ دیگر را به شبکه اضافه کنیم، (شکل زیر).



پورت‌های سوییچ B در شبکه فرضی ما می‌توانند با VLANهای مشابه یا متفاوت پورت‌هایی که در سوئیچ A قرار دارد پیکربندی شوند. ترافیک از یک دستگاه روی VLAN 1 متصل به سوییچ A می‌تواند به دستگاه دیگری در VLAN 1 متصل به سوئیچ B در قالب ترافیک محلی ارسال شوند، زیرا آن‌ها در همان دامنه پخشی تعریف شده از سوی VLAN هستند. با این حال، دستگاه‌های VLAN جداگانه - حتی اگر آن‌ها به یک سوئیچ متصل باشند- نمی‌توانند بدون عبور از طریق روتر با یکدیگر صحبت کنند. بنابراین، انتقال از یک دستگاه در VLAN 1 متصل به سوئیچ B باید از طریق روتر برای رسیدن به یک دستگاه در VLAN 3، حتی اگر هر دو دستگاه به یک سوئیچ وصل شده باشند عبور کنند.

Switch Ports و Trunks

در شکل زیر سوییچ A به دستگاه‌هایی در دو VLAN و سوئیچ C متصل شده است.

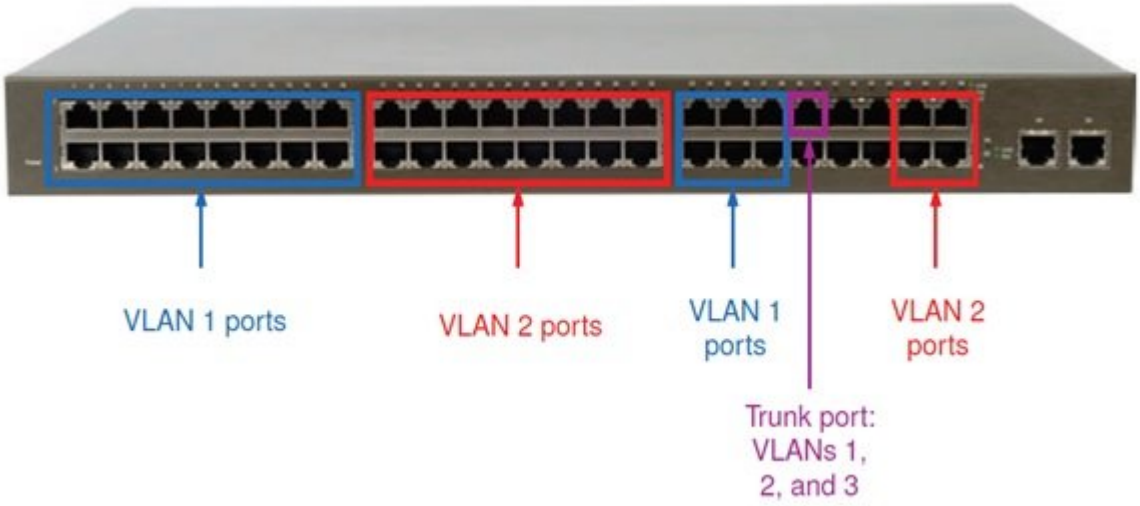


در این‌جا دو نوع متفاوت از اتصالات وجود دارند. پورت‌های متصل به دستگاه‌های کلاینت به‌طور معمول تنها برای پشتیبانی از ترافیک یک VLAN پیکربندی شده‌اند. با این حال، پورت‌هایی که به سوییچ C متصل می‌شوند باید بتوانند ترافیک را به VLAN انتقال دهند. بنابراین، هر پورت یک سوییچ که از VLANها پشتیبانی می‌کند، به عنوان یکی از دو نوع پورت VLAN به شرحی که در ادامه مشاهده می‌کنید پیکربندی می‌شود.

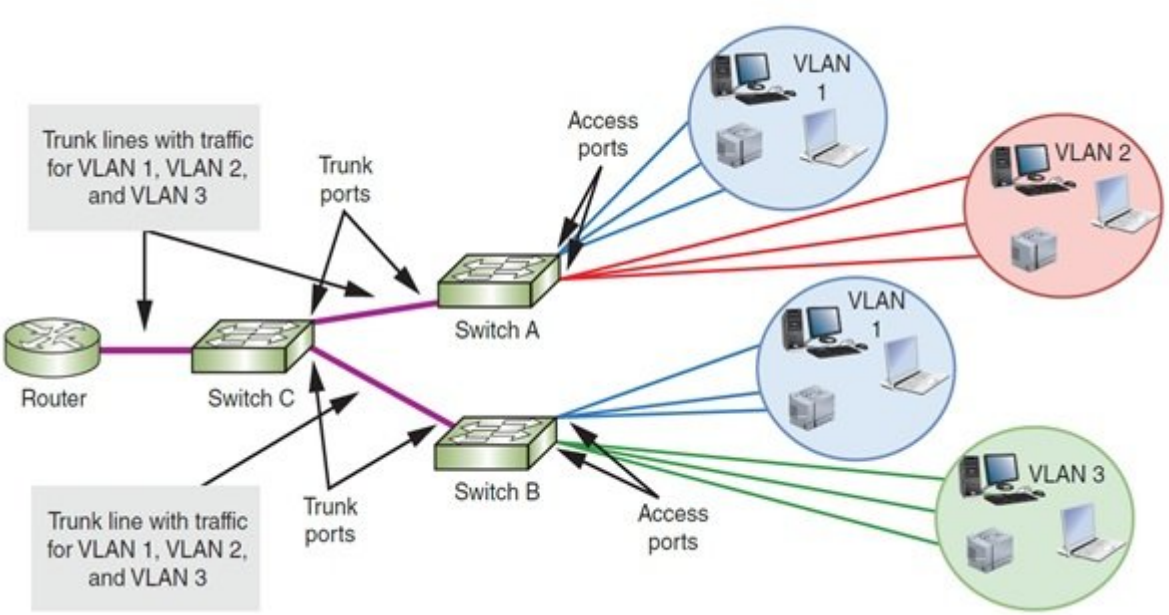
• پورت دسترسی (access port) - سوییچ را به یک نقطه پایانی، مانند یک ایستگاه کاری متصل می‌کند. کامپیوتر متصل به یک پورت دسترسی نمی‌داند متعلق به کدام VLAN است، و همچنین قادر نیست سایر VLANهای سوئیچ را تشخیص دهد.

• پورت ترانک (trunk port)- سوئیچ را به روتر یا سوئیچ دیگری (یا احتمالا یک سرور) متصل می‌کند. این رابط ترافیک چند VLAN را مدیریت می‌کند. شکل زیر خط ترانکی را نشان می‌دهد که دو پورت ترانک را به یکدیگر متصل کرده است.

یک سوییچ انفرادی می‌تواند ترافیک متعلق به چند VLAN در یک شبکه را پشتیبانی کند. این‌کار به لطف فناوری trunking انجام می‌شود. به عبارت دقیق‌تر Trunk یک اتصال فیزیکی واحد بین دستگاه‌های شبکه است که از طریق آن بسیاری از VLANهای منطقی می‌توانند داده‌ها را منتقل و دریافت کنند. شکل زیر موقعیت نسبی پورت‌های دسترسی، پورت‌های Trunk و خطوط Trunk در یک شبکه را نشان می‌دهند.



پروتکل‌های ترانکینگ تگ‌های VLAN را به فریم‌های اترنت اختصاص داده و تفسیر می‌کنند، در نتیجه نحوه مدیریت توزیع فریم‌ها از طریق یک Trunk انجام می‌شود. محبوب‌ترین پروتکل برای تبادل اطلاعات VLAN روی ترانک‌ها پروتکل VTP سرنام VLAN Trunk Protocol متعلق به شرکت سیسکو است. VTP به یک پایگاه داده VLAN روی یک سوییچ اجازه تغییر می‌دهد که این فرآیند stack master نام دارد. فرآیندی که به سوییچ اجازه می‌دهد با سایر سوییچ‌ها در شبکه در ارتباط باشد. این راهکار به مدیران شبکه اجازه می‌دهد به شکل مرکزی تمام VLANها را با اعمال تغییر روی سوئیچ واحد مدیریت کنند. برای اطلاعات بیشتر در خصوص پروتکل VTP به آدرس **Understanding VLAN Trunk Protocol** مراجعه کنید.



در شماره آینده آموزش **نتورک‌پلاس** مبحث شبکه‌های محلی مجازی را ادامه خواهیم کرد.

معرفی آموزشگاه‌های معتبر دوره نتورک پلاس در سراسر کشور

استان تهران (تهران): آموزشگاه عصر شبکه
برگزار کننده دوره‌ها بصورت حضوری و مجازی هم‌زمان
تلفن: 02188735845 کانال: @Asrehshabakeh

استان گیلان (رشت): آموزشگاه هیوا شبکه
تلفن: 01333241269 کانال: @HivaShabake

تاریخ انتشار:

25 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15267/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-%D8%B1%D8%A7%DB%8C%DA%AF%D8%A7%D9%86-%D8%AF%D9%88%D8%B1%D9%87network-%D8%A8%D8%AE%D8%B4-50