تسلط بر مفاهیم پایه شبکه منطبق با استانداردهای بین‌المللی

آموزش رایگان دوره نتورک‌پلاس، زیرشبکه‌ها و شبکه‌های محلی مجازی (بخش 47)

در شماره گذشته آموزش نتورک‌پلاس با پروتکل‌های ارسال و دریافت فایل‌ها و همچنین تا حدودی با شبکه‌های اختصاصی مجازی آشنا شدید. در این شماره قصد داریم مبحث فوق را به پایان رسانده و به سراغ شبکه‌های محلی مجازی، زیرشبکه‌ها و ماسک زیرشبکه برویم.

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

پروتکل‌هایی که در شبکه‌های اختصاصی مجازی استفاده می‌شوند

برای مطمئن شدن از این موضوع که یک شبکه اختصاصی مجازی هر نوع داده‌ای را به شکل اختصاصی روی هر نوع ارتباطی انتقال می‌دهد، پروتکل‌های ویژه‌ای برای این شبکه‌ها در نظر گرفته شده است که پروتکل‌های لایه بالاتر را کپسوله می‌کنند. فرآیندی که تونل‌زنی نام دارد. اگر به خاطر داشته باشید، به شما گفتیم میزبان‌های IPv6 می‌توانند از طریق یک شبکه IPv4 تونل‌زنی کنند، البته برعکس این قضیه نیز صادق است. همان پروسه توسط پروتکل‌های شبکه اختصاصی مجازی برای ایجاد یک اتصال مجازی یا تونل بین دو نقطه پایانی شبکه اختصاصی مجازی استفاده می‌شود. برای درک اینکه چگونه یک تونل شبکه مجازی کار می‌کند، تصور کنید یک کامیون در یک رودخانه درون یک کشتی حمل می‌شود. کامیون به دقت بارگیری می‌شود، با تسمه‌های قدرتمندی محکم بسته می‌شود و سپس از طریق مسیر رودخانه به مقصد حمل می‌شود. در مقصد، پوشش‌ها و نوارهای محافظتی برداشته شده و محموله بارگیری می‌شود. پس از اتمام بارگیری، کامیون می‌تواند در جاده‌ها مطابق با عملکردی که برای آن ترسیم شده است به کار گرفته شود. به‌طور مشابه، با پروتکل‌های تونل‌زنی شبکه اختصاصی مجازی، فریم‌ها به‌طور کامل رمزگذاری و کپسوله شده و درون بسته‌های آی‌پی معمولی و فریم‌های لایه پیوند داده‌ها قرار گرفته و انتقال داده می‌شوند. به عبارت دیگر، یک فریم در سراسر شبکه به عنوان بارداده درون فریم دیگری انتقال پیدا می‌کند. هنگامی که فریم در طرف دیگر تونل دریافت می‌شود، همانند بسته‌های دیگر درون شبکه از لایه‌های مختلف عبور کرده، به دست کاربر رسیده و به کاربر اجازه می‌دهد به منابع شبکه دسترسی پیدا کند. بیشتر پروتکل‌های تونل‌زنی در لایه پیوند داده فرآیند کپسوله کردن فریم شبکه اختصاصی مجازی را درون یک بسته لایه شبکه انجام می‌دهند، هرچند برخی از این پروتکل‌ها در لایه 3 کار می‌کنند که دسترسی به ویژگی‌ها و گزینه‌های بیشتر را امکان‌پذیر می‌کنند. از رایج‌ترین پروتکل‌های تونل‌زنی که شبکه‌های اختصاصی مجازی از آن استفاده می‌کنند به GRE، L2TP، PPTP، پروتکل متن‌باز شبکه اختصاصی مجازی و IKEv2 می‌توان اشاره کرد. هر یک از این پروتکل‌ها تعاریف خاص خود را دارند که پیشنهاد می‌کنم با صرف کمی وقت اطلاعاتی در ارتباط با آن‌ها به دست آورید.

زیرشبکه‌ها و شبکه‌های محلی مجازی

اکنون زمان آن رسیده است تا به سراغ یکی دیگر از مباحث مهم دوره **نتورک‌پلاس** برویم. زیرشبکه‌ها و شبکه‌های محلی مجازی یکی از مباحث مهم دیگر دنیای شبکه‌ها هستند که قصد داریم در شماره‌های آتی به بررسی آن‌ها بپردازیم.

تقسیم‌بندی شبکه

هنگامی که یک شبکه به چند شبکه کوچک‌تر تقسیم می‌شود، ترافیک یک شبکه از ترافیک سایر شبکه‌ها تفکیک شده و هر شبکه دامنه پخشی خاص خود را دارد. یک مدیر شبکه ممکن است به دلایل زیر ترافیک شبکه را بخش‌های کوچک‌تر تقسیم کند:

• افزایش امنیت- انتقال در دامنه‌های پخشی به هر شبکه محدود شده و در نتیجه احتمال کمی وجود دارد که هکرها یا بدافزارها از راه دور به شبکه دسترسی پیدا کنند.

• بهبود عملکرد - تقسیم‌بندی با کاهش اندازه هر دامنه پخشی ترافیک پخشی را محدود کرده و به این شکل استفاده مؤثر از پهنای باند را به همراه داشته که در نهایت بهبود عملکرد کلی شبکه را رقم خواهد زد.

• ساده‌سازی عیب‌یابی- هنگام عیب‌یابی، به جای آن‌که کل شبکه با هدف پیدا کردن خطاها و تنگناها بررسی شود، مدیر شبکه می‌تواند محدوده‌ای که باید بازرسی شود را به یک شبکه خاص و کوچک‌تر محدود کند.

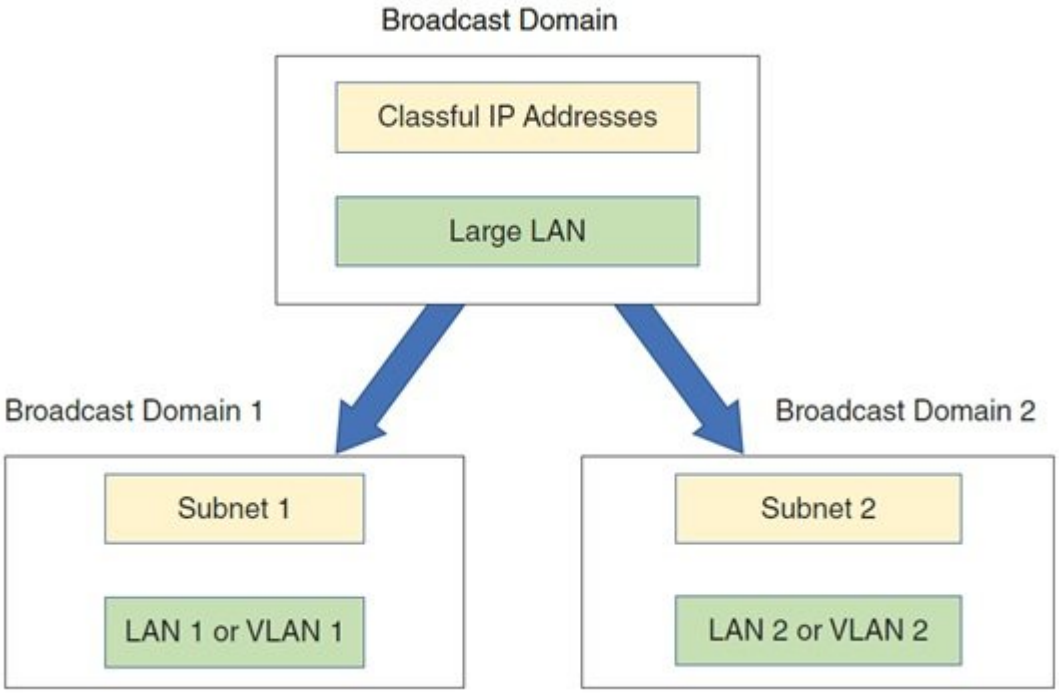
شبکه‌ها معمولا به یکی از گروه‌بندی‌های زیر تقسیم می‌شوند:

• مکان‌های جغرافیایی - به‌طور مثال، طبقه‌های یک ساختمان متصل به یک شبکه یا ساختمان‌های متصل به یک WAN

• کرانه‌های اداری- به‌طور مثال، بخش‌های حسابداری، منابع انسانی و فروش

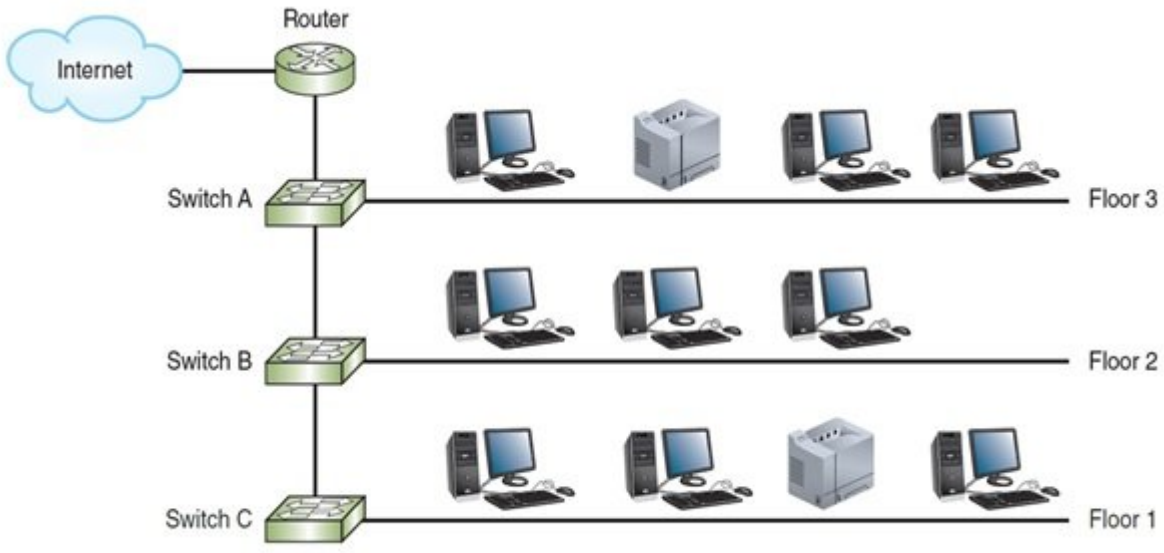
• بر مبنای دستگاه‌های مختلف - به‌طور مثال، چاپگرها، دسکتاپ‌ها، و تلفن‌های آی‌پی

با توجه به گزینه‌های مختلف تقسیم‌بندی شبکه، راه‌های مختلفی برای جدا کردن دامنه‌های پخشی در یک شبکه وجود دارد. هر رویکرد تقسیم‌بندی ملزومات خاص خود را داشته و در عین حال قابلیت‌ها و محدودیت‌های مختلفی را ارائه می‌کند. در این بین مدل OSI نیز نقش مهمی در تقسیم‌بندی شبکه بازی می‌کند. شما می‌توانید از دستگاه‌های فیزیکی در لایه 1 برای ایجاد شبکه‌های محلی جداگانه استفاده کرده، در لایه 2 شبکه‌های محلی مجازی ایجاد کنید و در لایه 3 از زیر شبکه برای سازماندهی دستگاه‌ها درون فضای آدرس آی‌پی در دسترس استفاده کنید. شکل زیر در فهم بهتر رابطه بین این مفاهیم کمک می‌کند.



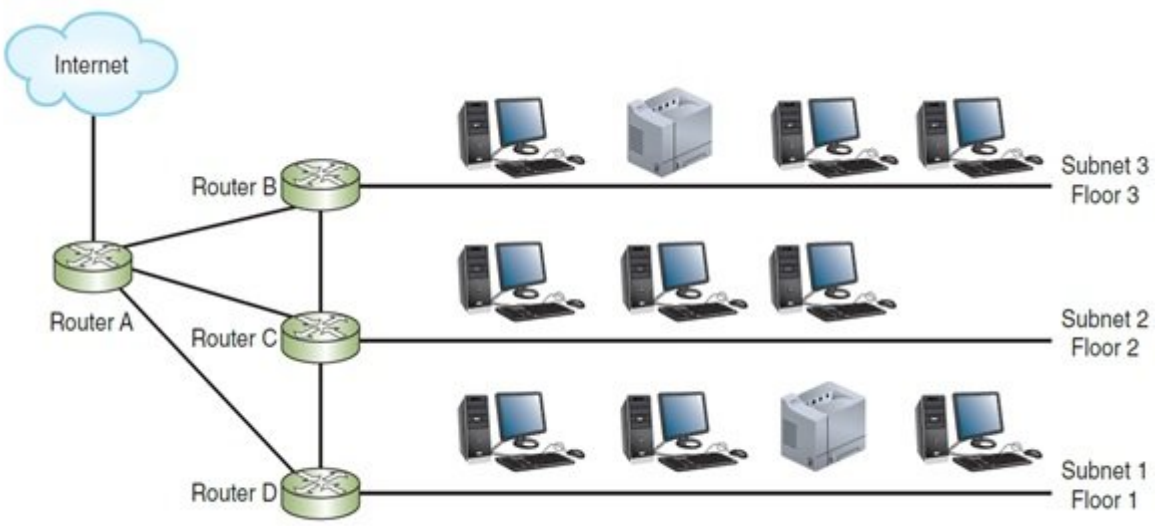
زیرشبکه‌ها

فرض کنید شبکه شرکتی از 20 یا 30 کامپیوتر و دستگاه‌های دیگر به چند صد کامپیوتر و دستگاه توسعه پیدا کرده‌اند. شبکه به عنوان یک شبکه واحد با کامپیوترهای متصل شده به چند سوئیچ لایه 2 که سوییچ‌ها به یک روتر، و سپس به اینترنت پرسرعت متصل می‌شوند کار خود را آغاز می‌کند. شکل زیر این مسئله را نشان می‌دهد.



از آنجایی که تنها یک شبکه محلی یا دامنه پخشی وجود دارد، هر میزبان در شبکه می‌تواند به‌طور مستقیم با میزبان دیگری ارتباط برقرار کرده و یک روتر به عنوان دروازه پیش‌فرض برای کل شبکه کار کند. کل شبکه دارای یک مجموعه از آدرس‌های آی‌پی، به‌طور مثال، 192.168.89.0/24، با یک ماسک زیرشبکه 255.255.255.0 است.

همانطور که شبکه بزرگ‌تر می‌شود، شما باید مدیریت بهتری بر ترافیک شبکه اعمال کنید که تکنیک تقسیم‌بندی شبکه به‌گونه‌ای که هر طبقه شبکه محلی جداگانه یا دامنه پخشی خاص خود را داشته باشد یکی از راهکارهای پیش‌رو است. یک روش برای انجام این کار، نصب یک روتر در هر طبقه است، همان‌گونه که در شکل زیر نشان داده شده است.



روترها ترافیک پخشی را به سمت جلو هدایت نمی‌کنند. شما می‌توانید یک روتر را به عنوان یک کرانه پخشی تصور کنید. اساسا روترها می‌توانند به عنوان ابزارهایی برای تقسیم ترافیک شبکه استفاده شوند. با این حال، شما همچنین باید فضای آدرس آی‌پی را در یک لایه منطقی مدیریت کنید. برای انجام این کار، نیاز به پیکربندی (یا به صورت دستی یا از طریق DHCP سرور) کلاینت‌ها در هر زیر شبکه دارید تا کلاینت‌ها بدانند چه دستگاه‌هایی عضوی از زیر شبکه آن‌ها است و چه دستگاه‌هایی به زیرشبکه تعلق ندارند. همچنین باید هر روتر را به گونه‌ای پیکربندی کنید تا اطمینان حاصل شود که روتر به عنوان گیت‌وی پیش‌فرض برای شبکه محلی کار کرده و در صورت لزوم ترافیک را به سمت به دو شبکه دیگر فوروارد کند.

در این مرحله، شما سه شبکه جداگانه و کوچک‌تر محلی (یا زیر شبکه) درون یک شبکه بزرگ‌تر دارید. با این حال، دستگاهی در زیرشبکه 2 (Subnet 2) هنوز نمی‌داند آیا دستگاه‌های Subnet 3 شبکه محلی یکسانی را به‌اشتراک قرار می‌دهند یا خیر.

چگونه می‌توان آدرس‌های آی‌پی را تقسیم کرد تا کامپیوتری در زیرشبکه 2 بتواند فرآیند انتقال داده‌ها برای دستگاه‌هایی درون زیرشبکه‌های دیگر را بر مبنای گیت‌وی پیش‌فرض ارسال کند و سعی نکند به شکل مستقیم با دستگاه‌ها ارتباط برقرار کند؟ راه‌حل این مشکل در تقسیم کردن آدرس‌های آی‌پی به سه گروه یا سه زیر شبکه نهفته است تا هر شبکه محلی یا هر طبقه در یک ساختمان آدرس‌های آی‌پی محدوده خود را داشته باشند. به این تکنیک زیرشبکه‌سازی (Subnetting) گفته می‌شود. زیرشبکه‌سازی کمک می‌کند تا مشکل مربوط به طبقه‌بندی آدرس‌ها را حل کنیم. به‌طور مثال، یک شبکه کلاس B واحد می‌تواند تا 65،534 آدرس آی‌پی داشته باشد و همه در یک شبکه محلی میزبانی شده باشند. تصور کنید یک چنین شبکه‌ای با چه چالش مدیریتی سنگینی همراه است و بدون شک عملکرد بسیار پایینی خواهد داشت. زیرشبکه‌سازی به ما کمک می‌کند تا فضای آدرس IP را به شکل بهتری مدیریت کنیم. زیرشبکه‌سازی مزایای زیر را به همراه دارد:

- اسناد شبکه ساده‌تر مدیریت می‌شوند.
- حل و فصل مشکلات ساده‌تر خواهد بود.
- روترها می‌توانند به راحتی فضای آدرس آی‌پی را مدیریت کنند تا همپوشانی آدرس‌ها رخ ندارند.
- مسیریابی در شبکه‌های بزرگ‌تر کارآمدتر خواهد بود.

ماسک زیرشبکه چگونه کار می‌کند؟

یک دستگاه از ماسک زیر شبکه برای تعیین اینکه متعلق به چه زیرشبکه یا شبکه‌ای است استفاده می‌کند. یک آدرس IPv4 دارای 32 بیت است که به دو قسمت تقسیم می‌شود. بخش شبکه که برای شناسایی شبکه استفاده شده و شناسه (Network ID) نامیده می‌شود و دیگری بخش میزبان است که برای شناسایی میزبان استفاده شده و شناسه

میزبان (host ID) نام دارد.

زمانی‌که کامپیوتری آماده ارسال اطلاعات به سمت میزبان دیگری است، ابتدا بیت‌های درون شناسه شبکه خود را با بیت‌هایی شناسایی شبکه میزبان مقصد مقایسه می‌کند. اگر بیت‌ها مطابقت داشته باشند، به معنای آن است که میزبان راه دور روی همان شبکه‌ای که کامپیوتر قصد ارسال اطلاعات را دارد قرار دارد و فرآیند انتقال به شکل مستقیم آغاز می‌شود. اگر بیت‌ها مطابقت نداشته باشند، میزبان مقصد روی شبکه دیگری قرار دارد و کامپیوتر فرآیند انتقال را به گیت‌وی پیش‌فرض در شبکه خود می‌فرستد تاگیت‌وی فرآیند ارسال به سمت شبکه درست را مدیریت کند.

چگونه کامپیوتر می‌داند چند بیت از آدرس آی‌پی خودش بیان‌گر شناسه شبکه است؟ پاسخ در ماسک زیرشبکه قرار دارد. ماسک زیر شبکه IPv4 رشته‌ای است که 32 بیت طول دارد. تعداد 1s در ماسک زیرشبکه تعداد بیت‌های آدرس آی‌پی که به شناسه شبکه تعلق دارند را تعیین می‌کند. فرض کنید یک کامپیوتر یک آدرس 192.168.123.132 و ماسک زیرشبکه 255.255.255.0 را دارد. برای شناسایی بیت‌هایی که شناسه شبکه را تشکیل می‌دهند، ابتدا این اعداد را به معادل باینری و به شرح زیر تبدیل می‌شوند:

• آدرس آی‌پی 192.168.123.132 در مبنای دودویی: (بخش قرمز رنگ شناسه شبکه در یک آدرس آی‌پی است.)

11000000.10101000.01111011.10000100

• ماسک زیرشاخه 255.255.255.0 در مبنای دودویی:

11111111.11111111.11111111.00000000

یک ماسک زیر شبکه همیشه یک سری از یک‌ها است و به دنبال آن یک سری از صفرها است. بخش 1s بخش شبکه یک آدرس آی‌پی را نشان می‌دهد و 0s بخش میزبان را نشان می‌دهد. بنابراین، بخش شناسه شبکه آدرس آی‌پی در مثال ما 24 بیت یا سه اوکت اول 192.168.123 است. بخش میزبان آخرین اوکت بوده که مقدار 132 است. با قرار دادن این مقادیر در کنار یکدیگر آدرس آی‌پی به صورت 192.168.123.132 نوشته می‌شود.

• شناسه شبکه: 192.168.123.0

• بخش میزبان: 0.0.0.132

اکنون فرض کنید این رایانه نیاز دارد با یک میزبان در 192.168.30.140 ارتباط برقرار کند. از آنجایی که شناسه‌های شبکه مطابقت ندارند (یعنی 192.168.123 با 192.168.30 مطابقت ندارد)، کامپیوتر می‌داند که میزبان راه دور در شبکه خودش نیست و انتقال را به گیت‌وی پیش‌فرض خود می‌فرستد.

هر کلاس شبکه با یک ماسک زیرشبکه پیش‌فرض به شرحی که جدول زیر نشان داده همراه است.

Default IPv4 subnet masks			
Network class	Default subnet mask (binary)	Number of bits used for network information	Default subnet mask (dotted decimal)
A	11111111 00000000 00000000 00000000	8	255.0.0.0
B	11111111 11111111 00000000 00000000	16	255.255.0.0
C	11111111 11111111 11111111 00000000	24	255.255.255.0

به‌طور مثال، در حالت پیش‌فرض، اوکت اول آدرس کلاس A اطلاعات شبکه را نشان می‌دهد. این حرف بدان معنا است که اگر شما با شبکه‌ای کار می‌کنید که میزبان با یک ماسک زیرشبکه 11111111 00000000 00000000 00000000 یا 255.0.0.0 پیکربندی شده، شما می‌دانید که شبکه از آدرس‌های کلاس A استفاده می‌کند.

نکته: اگر به یاد داشته باشید در آموزش‌های اولیه **نتورک‌پلاس** به شما گفتیم باید اطلاعات کافی در مورد مبناها و کلاس‌های مختلف شبکه درست آورد. اگر هنوز این کار را انجام نداده‌اید، در اولین فرصت به دنبال یادگیری باشید تا در پاسخ‌گویی به سوالات آزمون **نتورک‌پلاس** با مشکلی روبرو نشوید.

در شماره آینده آموزش **نتورک‌پلاس** مبحث زیرشبکه و ماسک زیرشبکه را ادامه خواهیم کرد.

تاریخ انتشار:
16 اردیبهشت 1398

نشانی منبع:
https://www.shabakeh-mag.com/networking-technology/15180/%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%87-%D9%86%D8%AA%D9%88%D8%B1%DA%A9%E2%80%8C%D9%BE%D9%84%D8%A7%D8%B3%D8%8C-%D8%B2%DB%8C%D8%B1%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7-%D9%88-%D8%B4%D8%A8%DA%A9%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%85%D8%AD%D9%84%DB%8C-%D9%85%D8%AC%D8%A7%D8%B2%DB%8C-%D8%A8%D8%AE%D8%B4-47