دانشکده برق، کامپیوتر و فناوری های پیشرفته

گروه مهندسی کامپیوتر

دستورکار آزمایشگاه شبکه‌های کامپیوتری

تهیه کنندگان:

دکتر صالح یوسفی

مهندس هما کاوند

تاریخ تنظیم:

مهرماه ۱۴۰۳

فهرست مطالب

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

آزمایش ۱

اهداف: آشنایی با محیط نرم‌افزار packet tracer و مفاهیم اولیه شبکه

تعریف شبکه‌های کامپیوتری: ارتباط فیزیکی و منطقی حداقل دو دستگاه، بر روی یک رسانه (media، بستر ارتباطی) با هدف به اشتراک گذاری منابع و انتقال داده.

سناریو ۱: می‌خواهیم با دو دستگاه یک شبکه کامپیوتری داشته باشیم.

اجزای مورد نیاز:

- دو دستگاه از میان end device
- رسانه ارتباطی

در محیط نرم‌افزار دو دستگاه را انتخاب کرده و از طریق کابل به عنوان رسانه ارتباطی این دو دستگاه را به یکدیگر متصل نمایید. اتصال دستگاه‌ها به یکدیگر به معنی اتصال کارت شبکه‌های آن‌هاست. به نوع کابلی که برای اتصال دستگاه‌ها به کار رفته است دقت کنید، اتصال دستگاه‌ها هم نوع از طریق کابل twice pair (cross) انجام می‌شود و اگر دستگاه‌ها مشابه نباشند اتصال از طریق کابل Straight انجام می‌شود. تا به اینجا شما اتصال فیزیکی دو دستگاه را انجام داده‌اید.

نکته: برای اتصال فیزیکی نیاز به آدرس فیزیکی نیز داریم که به آن MAC Address می‌گویند.

در تعریف شبکه بیان شد که اتصال فیزیکی و منطقی، برای اتصال منطقی باید برای دستگاه آدرسی منطقی تعریف کنیم که به آن IP Address گفته می‌شود. به عنوان مثال IP Address، 192.168.1.10 /24 برای دستگاه اول و 192.168.1.11 /24 برای دستگاه دوم در نظر بگیرید.

توجه: برای تعیین آدرس منطقی در محیط ویندوز بعد از اجرای دستور ncpa.cpl یا طی مسیر control panel / Network and Sharing center / change adaptor setting کلیه کارت‌های شبکه سیستم را مشاهده خواهید کرد. کارت شبکه‌ایی را که می‌خواهید برای آن IP Address تعریف کنید انتخاب کرده، راست کلیک

کرده و گزینه Properties را انتخاب نمایید. در بخش Networking، قسمت This connection uses the following items گزینه Internet Protocol Version 4 (TCP/IPv4) را انتخاب کنید و دکمه Properties را بزنید در بخش General می‌توانید IP Address برای کارت شبکه خود تعریف کنید.

بعد از اتصال فیزیکی و منطقی دو دستگاه لازم است تست کنیم که آیا اتصال برقرار است یا خیر و آیا داده‌ایی مابین این دو دستگاه مبادله خواهد شد؟

برای تست اتصال در شبکه‌هایی که از پروتکل TCP/IP استفاده می‌کنند از نرم‌افزار Ping استفاده می‌کنیم و برای بررسی بسته‌هایی که در شبکه مبادله می‌شوند می‌توانیم از نرم‌افزار Wireshark استفاده کنیم. در محیط packet tracer برای بررسی بسته‌های مبادله شده می‌توانید از قسمت simulation استفاده کنید.

سوالات و تمرینات

پروتکل ARP را به صورت کامل توضیح دهید.

پروتکل RARP را توضیح دهید.

مشخصاتی نظیرMAC Address ، طول بسته و غیره مرتبط با هر لایه را بنویسید.

آزمایش ۲

اهداف: آشنایی با دستگاه‌های Repeater، Hub، Bridge و Switch و مفاهیم Collision، Collision Domain، Broadcast و Broadcast Domain.

سناریو ۲: می‌خواهیم اتصال بیش از دو دستگاه و با مسافت‌های طولانی را داشته باشیم.

اجزای مورد نیاز:

- End device
- Repeater
- Hub
- Bridge
- Switch

در آزمایش یک، اگر فاصله دستگاه‌ها بیشتر از ۱۰۰ متر باشد چه راهکاری برای اتصال آن‌ها وجود دارد؟ در این حالت می‌توانیم از دستگاهی به نام repeater استفاده کنیم. دقت شود که دستگاه از نوع active باشد. در بازار passive repeater نام‌های مختلف دارد، برخی به آن کوپلر می‌گویند و برخی دیگر به آن barrel connector می‌گویند. حال اگر قرار باشد بیش از دو دستگاه را به یکدیگر متصل کنیم از Hub استفاده خواهیم کرد، Hub را می‌توان به صورت Multiport repeater تعریف کرد. برای سناریوهای جدید و نحوه کار Hub و repeater نیز وارد حالت simulation شده و عملکرد و بسته‌ها بررسی خواهند شد. Hub مستعد Collision است. تفاوت collision و نویز چیست؟ توپولوژی Hub همان Bus است که اولین بار توسط کمپانی زیراکس معرفی شد، امنیت آن به شدت پایین است. برای حل مشکلات Hub از وسیله‌ای به نام bridge استفاده شد که شبکه را به دو سگمنت تقسیم می‌کند و دارای MAC table است. (دستگاه‌های Hub و Bridge لایه یکی هستند.) بسته‌ها در صورتی که آدرس سگمنت مقابل را داشته باشند از Bridge عبور کرده و به سمت سگمنت دیگر می‌روند. دستگاه Hub، یک Collision domain و یک Broadcast domain است. دستگاه Bridge که بعد از آن معرفی شد، باعث می‌شود که Broadcast domain کوچکتر شود. بعد از این دستگاه‌ها سوئیچ عرضه

شد. این دستگاه لایه دومی است و تفاوت‌هایی با Bridge دارد. با استفاده از سوئیچ شما یک شبکه با توپولوژی star دارید. دلیل آنکه پورت‌ها مدتی نارنجی هستند و سپس سبز می‌شوند مبحث Spanning Tree (SPT) است.

سوالات و تمرینات

تفاوت passive repeater و active repeater در چیست؟

عملکرد Hub را به همراه مزایا و معایب آن توضیح دهید.

دستگاه‌های hub، bridge و switch را مقایسه کنید

آزمایش ۳

اهداف: آشنایی با IP Address v4

سناریو ۳: -

اجزای مورد نیاز: -

در شبکه‌هایی که از پروتکل TCP/IP استفاده می‌کنند، برای آدرس دهی منطقی از IP Address استفاده می‌شود که از این به بعد به اختصار به آن IP خواهیم گفت. این آدرس دارای دو ورژن ۴ و ۶ می‌باشد. که در این بخش به معرفی ورژن ۴ آن خواهیم پرداخت.

ویژگی‌های IP Address v4

- یک آدرس منطقی منحصر به فرد و جهانی ۳۲بیتی
- برای آدرس دهی در پروتکل‌هایی که دارای لایه شبکه هستند
- دارای دو حالت class full و class less
- در حالت class full دارای ۵ کلاس از A تا E
- مفاهیم subnetting و super netting در حالت class less
- دارای دو بخش به نام‌های Net ID و Host ID

نحوه نمایش IP

به صورت یک عدد دسیمال نقطه گذاری شده نمایش داده می‌شود. در این نماد گذاری هر عدد باینری ۳۲ بیتی به ۴ بایت ۸ بیتی مجزا تقسیم شده که توسط نقطه از یکدیگر جدا می‌شوند.

198.168.3.31

--------.--------.--------.--------

11000001.10101000 .00000011.00011111

IP = Net ID + Host ID

Subnet Mask: تعداد بیت‌هایی از IP را نشان می دهد که عضو Net ID هستند آن ها را با یک پر می‌کند و ارزش آن‌ها را با هم جمع می‌کند.

Prefix Mask: تعداد بیت‌های از IP را که عضو Net ID هستند را با یک پر می‌کند و آن ها را می‌شمارد.

به عنوان مثال IP Address 192.168.10.0 را در نظر بگیرید که ۲۴ بیت آن عضو Net ID و ۸ بیت آن عضو Host ID است. نمایش آن به صورت subnet mask و prefix به صورت زیر است

11000000.10101000.00001010.00000000

11111111.11111111.11111111.00000000

subnet Mask: 255.255.255.0

11111111.11111111.11111111.00000000

Prefix mask: 192.168.10.0 / 24

Network Address: آدرسی است که تمام بیت های بخش Host ID صفر است.

Broadcast Address: آدرسی است که تمام بیت های بخش Host ID یک است.

در شبکه **اجازه تخصیص** این دو آدرس را **نداریم**.

کلاس‌های آدرس IP

1– 126 class A: N.H.H.H
Private: 10.0.0.0 /8
128 – 191 class B: N.N.H.H
Private: 172.16-31.0.0 /16
192 – 223 class C: N.N.N.H
Private: 192.168.0.0 /24

224 – 239 class D: Multicast address

240 – 255 class E: Reserved for future use

- اگر آدرسی class A باشد باید ۸ بیت آن عضو Net ID باشد.
- اگر آدرسی class B باشد باید ۱۶ بیت آن عضو Net ID باشد.
- اگر آدرسی class C باشد باید ۲۴ بیت آن عضو Net ID باشد.

پیدا کردن رنج یک آدرسIP

به دست آوردن رنج یک IP به معنی به دست آوردن Network Address و Broadcast Address یک IP است.

۱) ابتدا prefix mask را تبدیل به subnet mask می‌کنیم.

۲) عدد ثابت ۲۵۶ را از octet متغیر subnet mask کم می‌کنیم و مقدار به دست آمده را M می‌نامیم.

۳) مضارب M را می‌نویسیم.

۴) حال octet متغیردر subnet mask و octet نظیرش در IP را در نظر می‌گیریم و نوشتن مضارب M را تا یک مقدار کمتر و یک مقدار بیشتر از آن ادامه می‌دهیم.

۵) مضارب M همیشه Network Address هستند.

۶) **یکی کمتر** از کوچکترین حد بالای octet متغیر **Broadcast Address** است.

سوالات و تمرینات

رنج IP Address های داده شده را به دست آورید.

1- 192.168.10.43 / 24

2- 200.219.0.14 /8

در یک شبکه می‌خواهیم به کاربر IP Address تخصیص دهیم، از بین موارد داده شده کدام را می‌توانیم به کاربر تخصیص دهیم؟ (با ذکر علت)

1- 192.168.0.64 /24

2- 200.200.100.127 /8

3- 192.168.10.52 /24

4- 200.100.0.16 /8

آزمایش ۴

اهداف: آشنایی با IP Address v4

سناریو ۴: -

اجزای مورد نیاز: -

در ادامه بحث IP Address v4 قصد داریم در مورد دو مبحث subnetting و super netting صحبت کنیم.

Subnetting

قرض دادن بیت های بخش Host ID به Net ID با هدف شکستن رنج بزرگ به Sub net های کوچکتر را subnetting گویند. به دو طریق می توان subnetting را انجام داد

- FLSM: با subnet Mask ثابت
  - Fixed length subnet masking
- VLSM: با subnet Mask متغیر
  - Variable length subnet masking

مزایای Subnetting

- جلوگیری از هدر رفتن IP یا بلا استفاده ماندن آن و تخصیص میزان مناسب IP به کاربران
- اختصاص آدرس IP به شرکت‌هایی که پراکندگی جغرافیایی دارند
- افزایش امنیت با انتقال نیافتن ترافیک محلی زیرشبکه‌ها
- افزایش کارایی با کاهش برخوردها

FLSM

آدرس IP را به زیر شبکه‌های مساوی تقسیم می‌کند.

به عنوان مثال آدرس IP، 200.0.0.0 /24 را به دو زیر شبکه تقسیم کنید.

200.0.0.0 /24

255.255.255.0

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	200.0.0.0 /25
0	1	1	1	1	1	1	1	200.0.0.127 /25
1	0	0	0	0	0	0	0	200.0.0.128 /25
1	1	1	1	1	1	1	1	200.0.0.255 /25

VLSM

آدرس IP، را براساس تعداد کاربران داده شده زیر شبکه می‌کند.

- رابطه زیر را در نظر می‌گیریم

$$2^n - 2 \geq x$$

- تعداد کاربران را x می‌نامیم.
- مقدار n برابر است با تعداد بیت های بخش Host ID
- محاسبه n را از بیشترین تعداد کاربران آغاز می کنیم.
- سپس براساس مقدار n، prefix mask مربوط به هر قسمت را نوشته و رنج IPهر قسمت را محاسبه می کنیم.

به عنوان مثال، تعداد کاربران زیر را در یک شبکه داریم، آدرس IP، 200.0.0.0 /24 را در اختیار داریم، از این آدرس برای آدرس دهی کاربران استفاده کنید.

تعداد کاربران	N (Host ID)
31	6
20	5
120	7
10	4

200.0.0.0 /24

- n=7 200.0.0.0 /25
- 200.0.0.127 /25
- n=6 200.0.0.128 /26
- 200.0.0.191 /26
- n=5 200.0.0.192 /27
- 200.0.0.223 /27
- n=4 200.0.0.224 /28
- 200.0.0.239 /28

Super netting or Route Summarization

- قرض دادن بیت های بخش Net ID به Host ID با هدف کاهش دادن حجم Routing table های router های شبکه را Super netting گویند.

شرط انجام Super netting

- بیت‌هایی را می توانیم از بخش Net ID به بخش Host ID قرض دهیم که **کلیه ترکیبات ۰ و ۱** آن بیت‌ها را داشته باشیم.

به عنوان مثال برای آدرس‌های IP زیر super netting را انجام دهید.

100.0.48.0 /24	100.0.00110000.0
100.0.49.0 /24	100.0.00110001.0
100.0.50.0 /24	100.0.00110010.0
100.0.51.0 /24	100.0.00110011.0
100.0.52.0 /24	100.0.00110100.0

100.0.48.0 /22

100.0.52.0 /24

سوالات و تمرینات

آدرس IP، 100.6.10.0 /24 در اختیار یک شرکت قرار دارد، کاربران این شرکت در ۴ بخش مختلف هستند و تعداد کاربر هر بخش برابر ۱۰۰، ۳۰، ۶۵ و ۸ نفر می‌باشند. برای هر بخش آدرس IP تخصیص دهید.

در یک جدول مسیریابی، برای آدرس‌های IP زیر یک مسیر یکسان وجود دارد، قصد داریم تا این جدول را خالاصه‌نویسی کنیم، خلاصه نویسی آن به چه صورت خواهد بود؟

200.82.0.53 /24

200.83.0.54 /24

200.84.0.55 /24

200.85.0.56 /24

200.86.0.57 /24

200.87.0.58 /24

آزمایش ۵

اهداف: آشنایی با محیط فیزیکی Packet tracer

سناریو ۵: اجرای یک شبکه در محیط فیزیکی نرم‌افزار و آشنایی با ماژول‌ها

اجزای مورد نیاز:

- End device
- Switch
- Wall jack
- Patch cord
- Router

تا کنون توضیحاتی که داده شده است، در قسمت محیط logical نرم‌افزار بوده است، در ادامه به محیط فیزیکی نرم‌افزار خواهیم پرداخت. قابلیت‌های محیط فیزیکی توضیح داده شود. فرض کنید در یک اداره یک اتاق با ۴ کارمند حضور دارند که می‌خواهید آن‌ها را به شبکه متصل کنید، درون رک نیز یک سوئیچ قرار داده‌اید و آن‌ها را مستقیم به سوئیچ متصل می‌کنید که نحوه این کار در نرم‌افزار توضیح داده خواهد شد. اما در محیط‌های حرفه‌ای اینگونه عمل نمی‌کنند و در اتاق‌ها از وسیله‌ای به نام keystone (wall jack) گفته می‌شود استفاده کرده و کلاینت‌ها از طریق کابل Patch cord به آن‌ها متصل می‌شوند. در محیط نرم‌افزار نیز می‌توانید این شبیه‌سازی را انجام دهید و از keystone استفاده کنید و با کمک کابل Straight که دو سر آن نیز معمولا استاندارد b است کلاینت‌ها را به جلوی keystone متصل کنید. به جای آنکه از پشت keystone مستقیم به سوئیچ متصل شود، می‌توان از patch panel استفاده کرد، اتصال به پشت patch panel داشت و از جلوی آن به پورت‌های سوئیچ اتصال برقرار کرد. این مراحل نیز در نرم‌افزار قابل شبیه‌سازی است. در rack به این نکته توجه کنید که معمولاً در استانداردهای مختلف بیان می‌شود که بین دستگاه‌ها فاصله وجود داشته باشد. برخی دستگاه‌ها rack mount هستند، برای دستگاه‌هایی که rack mount نیستند باید اصطلاحاً یک سینی زیر آن‌ها بگذاریم تا پیچ شود. حتی می‌توانید شبیه‌سازی از کابل‌هایی که درون داکت قرار می‌دهید نیز داشته باشید.

ماژول‌ها به دو دسته کلی Hot plug و non hot plug تقسیم‌بندی می‌شوند. اگر ماژولی Hot Plug باشد به این معناست که هنگامی که دستگاه روشن است شما می‌توانید آن قطعه را تعویض کنید. به عنوان نمونه سرورهای HP، اگر به عنوان مثال هارد این سرور سوخته باشد همچنان که دستگاه روشن است، می‌توانید هارد را تعویض کنید، در این حالت آن هارد اصطلاحاً Hot plug است. دسته دیگر قطعات Non Hot plug هستند، به عنوان نمونه RAM سرور را نمی‌توانید هنگامی که سرور روشن است تعویض کنید. معمولاً نرم‌افزار لیستی از ماژول‌ها دارد که می‌توانید آن‌ها را به دستگاه اضافه کنید، اگر از نوع non hot plug باشد و شما بخواهید هنگامی که دستگاه روشن است آن را تعویض نمایید، نرم‌افزار به شما پیغام خطا می‌دهد. برخی از ماژول‌های موجود شبیه‌سازی شده خود نرم‌افزار هستند که مثل در ابتدای نام آن‌ها عبارت PT قید شده است، اما برخی دیگر مواردی هستند که عیناً در دنیای واقعی وجود دارند.

ماژول‌ها ویژگی‌هایی دارند که در حین بررسی ماژول‌های هر دستگاه به آن‌ها اشاره می‌شود.

در بالاترین سطح که core محسوب می‌شود یک مسیریاب قرار می‌دهیم، (به عنوان مثال ۱۹۴۱) و در سطح دوم ۲ سوئیچ قرار می‌دهیم. و در لایه بعدی ۲ سوئیچ دیگر قرار می‌دهیم. و در لایه بعدی از end deviceها استفاده می‌کنیم. چرا از لفظ لایه استفاده کردیم؟ طراحی شبکه به صورت سلسله مراتبی است، لایه Core داریم، لایه distribution و لایه access داریم (توضیحات این سلسله مراتب بیشتر در دوره CCNP مطرح می‌شود.) این پیش‌فرض طراحی شبکه است، می‌تواند تغییر کند. کارت شبکه یکی از PCها را از fast ethernet به gig تغییر می‌دهیم (با کمک ماژول‌ها). حال می‌توان پورت این کلاینت که از نوع gig هست را به پورت gig سوئیچ متصل کنیم (دقت کنید سوئیچی باید انتخاب شود که gig ساپورت کند و در صورت نیاز ماژول آن را تغییر داد.) در لایه بعدی ابتدا ماژول‌های برق سوئیچ را به آن متصل می‌کنیم تا سوئیچ توانایی کار کردن داشته باشد. کارت شبکه سرور را نیز از طریق تغییر ماژول به gig تبدیل می‌کنیم. گاهی برای سوئیچ‌ها نمی‌توانیم ماژول اضافه کنیم در این حالت از Ether channel استفاده می‌شود. قبل از ایجاد اتصلات بین لایه

distribute و core باز هم نیاز به استفاده از ماژول‌ها داریم (این استفاده از ماژول‌ها بنا به نوع سناریویی است که در نظر گرفته‌ایم، ماژولی که اضافه کردیم SF است.) حال تخصیص IP را انجام خواهیم داد.

دستورات مربوط به تخصیص IP برای gateway در router

```
Router>en
Router#conf t
Router(config)#interface gigabitEthernet 0/1/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.1.1 255.255.255.0
```

تست کنیم که آیا یکی از کلاینت‌ها می‌تواند gateway را ping کند؟

Ping (Packet Internet or Inter-Network Groper)

از اپلیکیشن Ping برای تست ارتباطات TCP/IP استفاده می‌شود. این اپلیکیشن از یک پروتکل لایه سومی به نام ICMP استفاده می‌کند.

پیام‌های اپلیکیشن Ping

1- Destination Host Unreachable

بسته برای مقصد ارسال می‌شود، مقصد در شبکه وجود ندارد. ارتباطی بین فرستنده و گیرنده وجود ندارد. مسیر برای IP Address وجود دارد اما برای به دست آوردن MAC Address، gateway از اینترفیس مشخص شده در Routing Table، پیام ARP Replay دریافت نکرده است. (در یک VLAN نیستند، default Gateway در دسترس نیست و غیره)

2- Destination Network Unreachable

بسته Echo request ارسال می‌شود، برای Network آن بسته در یکی از routerها که بسته به اینترفیس آن وارد شده است، مسیری به آن Network در جدول Routing table وجود ندارد و بسته drop می‌شود.

3- Time Exceeded

بسته‌ایی به مسیریاب رسیده که TTL آن صفر شده است. مسیریاب بسته را drop می‌کند.

4- Transmit Failed General Failure

بسته از لایه سوم پایین‌تر نمی‌رود، به عبارت دیگر اصلا تشکیل نمی‌شود.

5- Request Time Out or No Echo Replay

این پیام به معنی آن است که IP Address مقصد با IP Address دریافت کننده بسته یکسان نیست و بسته drop می‌شود.

6- Echo replay

ابزار Tracert

از بسته‌های ICMP استفاده می‌کند و می‌توانیم با کمک آن، مسیر رفت بسته‌ها را بررسی کنیم.

نکته: Tracert سه بار هر Echo request را می‌فرستد.

سوالات و تمرینات

به لبه دیگر شبکه IP Address اختصاص دهید. از کلاینت‌های مختلف با ping شبکه را تست کنید. کلاینت‌های دیگری به شبکه اضافه کنید.

تفاوت ماژول‌های hot plug و non hot plug را توضیح دهید. هدف استفاده از ماژول‌ها چیست؟

آیا تمام دستگاه‌ها قابلیت افزوده شدن ماژول را دارند به طور کامل توضیح دهید.

چرا در این سناریو برای سوئیچ‌ها IP address اختصاص ندادیم؟

چرا اتصال سوئیچ و hub با کابل cross انجام شده است؟

تفاوت interfaceهای مسیریاب و سوئیچ در چیست؟

ساختار بسته ICMP را رسم و توضیح دهید.

آزمایش ۶

اهداف: آشنایی با تعدادی از Server ها

سناریو ۶: پیاده‌سازی تعدادی از Server ها در شبکه

اجزای مورد نیاز:

- End device
  - Server
  - PC
- Router
- Switch

قصد داریم تا بر اساس ویژگی‌های نرم‌افزار Packet Tracer به معرفی چند Server بپردازیم. در ابتدا باید به این نکته توجه داشته باشید که Server ها در دسته end device ها قرار دارند و در طراحی سه لایه‌ایی در سطح Access قرار خواهند داشت. از میان Server ها به معرفی موارد زیر می‌پردازیم.

DHCP, HTTP Server, DNS Server, NTP Server, SYS-log Server, FTP Server, TFTP Server, E-mail Server

در ابتدا چند PC، یک سوئیچ و یک مسیریاب را به عنوان شبکه انتخاب کنید و اتصالات لازم را انجام دهید.

Dynamic Host Configuration Protocol Server (DHCP Server)

این سرویس را می‌توانید به منزله استخری پر از IP Address در نظر بگیرید که به صورت پویا به دستگاه‌هایی که برای آن درخواست ارسال می‌کنند IP Address تخصیص می‌دهد. تخصیص IP Address به کاربران به سه صورت انجام می‌شود.

- Static

در این حالت admin شبکه به صورت دستی تخصیص IP Address را انجام می‌دهد به این صورت که IP Address و Subnet mask را تنظیم و set می‌کند.

نکته: تخصیص IP Address به زیر ساخت‌های شبکه (servers Routers , …) حتما به static انجام شود.

- Dynamic

تخصیص IP Address از طریق DHCP Server

هنگامی که تعداد کاربران زیاد است می‌تواند مفید باشد.

- Automatic Private IP Addressing (APIPA)

اگر کاربری به هر دلیل موفق به دریافت IP Address نشود از این طریق به خود IP Address تخصیص می‌دهد مشخصه این نوع آدرس آن است که به صورت 169.254.x.x /16 می‌باشد. این آدرس یک آدرس private محسوب می‌شود.

مشابه آزمایش ۵ دستورات مرتبط با router را وارد می‌کنیم

```
Router>en
Router # conf t
Router(config) # interface gigabitEthernet 0/1/0
Router(config-if) # no shutdown
Router(config-if) # ip address 192.168.1.1 255.255.255.0
```

برای کلاینت‌ها آدرس IP در نظر نمی‌گیریم، در قسمت تنظیمات IP برای کلاینت‌ها نوع تخصیص آدرس IP را به صورت DHCP در نظر می‌گیریم.

نکته: تا زمانی که تنظیمات DHCP را انجام نداده باشیم، آدرس کلاینت‌ها از نوع APIPA خواهند بود.

حال یک server را وارد شبکه کرده و به سوئیچ متصل کنید، در ابتدا به آن آدرس IP تخصیص دهید. از آنجا که server و زیر ساخت شبکه است به حالت Static به آن آدرس دهید و مقدار آن را 192.168.1.2 با subnet mask، 255.255.255.0 در نظر بگیرید. برای این server و سایر server های این سناریو، آدرس IP به عنوان default gateway همان آدرس IP است که به پورت مسیریاب تخصیص داده شده است و آدرس IP برای DNS server به صورت 192.168.1.3 / 24 است.

سپس از قسمت سرویس‌ها، سرویس DHCP را انتخاب و سایر تنظیمات مرتبط با آن را انجام دهید.

HTTP (Hypertext Transfer Protocol) Server

وب سرور نرم‌افزاری و سخت‌افزاری است که از HTTP و پروتکل‌های دیگر برای پاسخ به درخواست‌های کاربران از طریق شبکه جهانی وب استفاده می‌شود ، بنابراین وظیفه اصلی وب سرور نمایش محتویات وب سایت از طریق ذخیره‌سازی، پردازش و ارائه صفحات وب به کاربران است. حال از طریق گزینه سرویس‌ها تنظیمات مربوط به این سرور را انجام خواهیم داد و برای دیدن نتیجه، در یکی از کلاینت‌ها مرورگر وب را باز کرده و آدرس IP این سرور که 192.168.1.4 است را وارد کرده، مشاهده خواهید کرد که صفحه مربوطه باز خواهد شد.

DNS (Domain Name System) Server

سرور DNS همانند یک دفترچه تلفن عمل کرده و مدیریت نقشه برداری بین نام ها و اعداد را دارد، به طوری که این سرورها درخواست‌ها برای نام را به آدرس‌های IP آدرس‌ها ترجمه می‌کنند و وقتی که کاربر نام دامنه را در مرورگر وب خود می نویسد DNS مشخص می‌کند که به کدام سرور دسترسی پیدا کند . از آنجایی که ما برای سرورهای قبلی آدرس DNS را برابر با 192.168.1.3 / 24 قرار داده بودیم اکنون لازم است تا یک سرور جدید را با همین آدرس کانفیگ کنیم. برای این سرویس نیز تنظیمات آن را انجام داده و برای تست آن این بار در مرورگر نام دامنه را نوشته و نتیجه را بررسی خواهیم کرد.

NTP (Network Time Protocol) Server

استفاده از Network Time Protocol برای همگام‌سازی ساعت‌های سیستم از دسکتاپ تا سرورها به کار گرفته می‌شود، زیرا داشتن ساعت‌های هماهنگ برای بسیاری از برنامه‌ها مورد نیاز است. مجدد باید یکی از سرورها را تنظیم کنیم که به طور فرضی برای آن IP آدرس 192.168.1.5 / 24 را در نظر می‌گیریم و در قسمت سرویس‌ها NTP را انتخاب کرده، برای سادگی، قسمت Authentication را غیر فعال می‌کنیم و در تقویم تاریخ روز را انتخاب می‌کنیم. حال برای تست آن، از مسیریاب استفاده می‌کنیم، وارد مسیریاب شده و با دستور Clock Show می توانیم تاریخ و زمان را ببینیم که مقدار اشتباهی را به ما نشان می‌دهد. برای حل این مشکل

باید مشخص کنیم که کدام سرور ما ارائه سرویس NTP را بر عهده دارد و با وارد کردن دستور زیر سرور NTP خود را انتخاب می کنیم :

Router (config) # ntp server 192.168.1.5

می توانیم با دستور clock show do هم دوباره زمان را چک کنیم. اما باید بدانیم که بعد از دستور بالا ، مدت زمانی طول می کشد تا ساعت روی Router تنظیم شود و عواملی مانند:

- تاخیر شبکه بین Router و سرور NTP می‌تواند بر تنظیم ساعت تاثیر بگذارد اگر تاخیر زیاد و یا در شبکه شلوغی وجود داشته باشد ممکن است همگام‌سازی ساعت بیشتر طول بکشد .
- خود سرور NTP هم می‌تواند در پاسخ به درخواست Router تاخیر داشته باشد این می‌تواند به دلایل مختلفی مانند بارگذاری سرور ، مشکلات شبکه و غیره باشد .
- علاوه بر آن‌ها قابلیت و منابع پردازشی خود Router می‌تواند بر زمان تنظیم ساعت تاثیرگذار باشد زیرا اگر Router مشغول کارهای دیگر باشد و یا منابع محدودی داشته باشد ، ممکن است پردازش دستور NTP و به روز رسانی آن کمی زمان ببرد.

SYSLOG Server

از پروتکل SYSLOG برای ارسال گزارش‌های رویدادها استفاده می‌کنیم تا در مکانی ذخیره شده و بعدا توسط نرم‌افزار ها تجزیه و تحلیل شده و عمدتا برای عیب یابی و غیره استفاده می‌شود. برای این سرویس از IP آدرس 192.168.1.6 / 24 استفاده خواهیم کرد و در قسمت سرویس‌ها بخش SYSLOG را انتخاب و فعال می‌کنیم. در Router برای اجرای آن از دستور زیر استفاده می‌کنیم.

Router (config) # Logging host 192.168.1.6

FTP (File Transfer Protocol) Server

سرورهای FTP راه حل های نرم افزاری برای انتقال فایل‌ها در اینترنت هستند و از آن برای دو عملکرد Get و Put استفاده می‌شود یعنی فایل‌ها را از دستگاهی به سرور آپلود کنند و یا فایل ها را از سرور به دستگاه کاربر دانلود کنند. برای تنظیم این سرور از IP آدرس 192.168.1.7 /24 استفاده خواهیم کرد و در بخش سرویس

ها FTP را انتخاب خواهیم کرده، در این صفحه می توانیم برای خود یک نام و رمز برای دسترسی انتخاب کنیم و همچنین میزان دسترسی را نیز می‌توانیم محدودیت‌هایی را اعمال کنیم. برای اتصال به سرور و دسترسی به فایل ها می‌توانیم یکی از دستگاه ها را انتخاب کرده و از بخش Prompt Command می‌توانیم با دستور FTP به سرور مورد نظر خود وصل شده و فایل ها را جا به جا کنیم.

TFTP (Trivial File Transfer Protocol) Server

این پروتکل بیشتر برای انتقال فایل های کانفیگ کوتاه به Router ها و سایر دستگاه طراحی شده است و بیشتر در محیط Lan مورد استفاده قرار می‌گیرد. از FTP توسط کاربران و برای دانلود و آپلود فایل استفاده می‌شود در حالی که TFTP برای انتقال تنظیمات به دستگاه‌های شبکه استفاده می‌شود و همچنین TFTP از پروتکل UDP برای ارسال استفاده می‌کند در حالی که FTP از پروتکل TCP. هنگامی که بخواهیم اتصالی قابل اعتماد داشته باشیم از TCP استفاده می کنیم که در مرورگرهای وب، ایمیل، انتقال فایل استفاده می‌شود اما اگر بخواهیم سرعت بیشتری نسبت به اطمینان از رسیدن بسته‌ها داشته باشیم از UDP استفاده می‌کنیم. برای این آزمایش از IP آدرس 192.168.1.8 / 24 استفاده خواهیم کرد و سرویس TFTP را برای این سرور انتخاب خواهیم کرد و آن را روشن می‌کنیم و از قسمت Router برای کانفیگ آن استفاده خواهیم کرد به همین منظور به بخش CLI رفته و دستورات زیر را اجرا خواهیم کرد.

```
Router > enable
Router # copy flash : file Name
```

E-MAIL Server

سرور E-mail یک برنامه نرم‌افزاری است که برای ارسال و دریافت E-mail از آن استفاده می‌شود. برای این سرور از IP آدرس 192.168.1.9 استفاده خواهیم کرد و در سرویس ایمیل لازم است تا علاوه بر تعریف کاربران از یک دامنه هم برای ارسال و دریافت E-mail ها استفاده کنیم، دامنه ای که قبلا برای وب سایت خود تعریف کرده ایم را نیز می‌توانیم در اینجا استفاده کنیم و یک نام کاربری و رمز هم برای E-mail خود تعریف می‌کنیم. همچنین توجه داشته باشیم که هر دو پروتکل SMTP و POP3 باید فعال باشند. حال باید به دو دستگاه

پایانی رفته و در قسمت E-mail اطلاعات هر یک از کاربران را وارد کنیم برای اسم می‌توانیم هر چیزی را انتخاب کرده اما باید برای آدرس E-mail نام کاربر را با استفاده domain @ بنویسیم و IP آدرس دریافت و ارسال را هم ۱۹۲.۱۶۸.۱.۹ قرار دهیم و در آخر هم نام کاربر و رمز آن را وارد کنیم حال در هر دو دستگاه قسمت E-mail را باز کرده و از یک کامپیوتر ارسال می‌کنیم و از کامپیوتر دیگر دریافت خواهیم کرد.

جدول ۶-۱ نام برخی پروتکل‌ها و شماره پورت‌های آن را نشان می‌دهد.

جدول ۶-۱ برخی از پروتکل‌های رایج و شماره پورت آن‌ها

Protocols	Port Number
FTP	21
Telnet	23
SSH	22
SMTP	25
DNS	53
DHCP	67s, 68c
Syslog	514
Kerberos	88
RDP	3389
LDAP	389
LDAPs	636

Protocols	Port Number
POP3	110
Imap4	148
SMB	445
SMTP	25
NBT	137, 138, 159
SNMP	161
TFTP	69
NTP	123
SMTP	25
HTTP	80
HTTPs	443

سوالات و تمرینات

مزایا و معایب اختصاص IP به صورت APIPA چیست و کاربرد خاص آن را بیان کنید.

آزمایش ۷

اهداف: آشنایی با مفهوم Virtual LAN (VLAN)

سناریو ۷: شبکه‌ایی داریم که شبکه‌های محلی مجزایی دارد که همه در بستر یک شبکه واحد هستند و از سوی دیگر با محدودیت منابع مواجه هستیم

اجزای مورد نیاز:

- End device
- Switch

گاهی در یک شبکه بنا به دلایلی، چندین شبکه محلی در بستر یک شبکه واحد داریم، اما یک رنج IP address و تعداد محدودی سوئیچ و دیگر منابع را در اختیار داریم. در این حالت می‌توانیم از مفهومی به نام VLAN استفاده کنیم. به صورت پیش فرض تمام پورت‌های سوئیچ عضو VLAN 1 هستند. اگر از مفهوم VLAN استفاده کنیم، مشابه آن است که یک سوئیچ را به تعداد VLANها تکه کرده‌ایم، چرا که ترافیک هیچ‌گاه از یک valn به VLAN دیگر منتقل نمی‌شود.

نکته: یکی از مزایای استفاده از تکنیک VLAN جدا کردن Broadcast domain است.

نکته: به لحاظ تکنیکی می‌شود IP address های VLAN های مختلف را از یک رنج تخصیص داد. اما از نظر طراحی شبکه این کار را انجام ندهید. چرا؟

ترافیک از یک VLAN به VLAN دیگر تنها از طریق دستگاه‌های لایه سومی منتقل می‌شود.

ایجاد VLAN در سوئیچ

Switch (config) # VLAN number
Switch (config-VLAN) # name

با دستور show VLAN می‌توان VLANهای ایجاد شده را مشاهده کرد.

عضو کردن پورت‌های سوئیچ در VLAN

Switch (config) # interface fast 0/1

Switch (config-if) # switch port mode access VLAN number

انتخاب یک رنج پورت

Switch (config) # int range fa 0/1-10, fa 0/15, fa 0/20-5

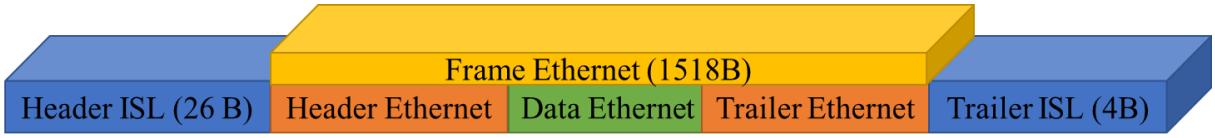
تعریف Trunk Port

همان‌طور که اشاره شد، VLAN یک مفهوم مجازی است، حال چطور همه افرادی که عضو یک VLAN اما بر روی سوئیچ‌ها مختلف پراکنده هستند بتوانند با یکدیگر در ارتباط باشند؟ باید از منظر مفاهیم لایه دومی این ارتباط برقرار شود، پس می‌توان مسئله را به این صورت بیان کرد که پورت up-link را بر روی کدام پورت و کدام VLAN قرار دهیم.

پورت Trunk به صورت پیش فرض عضو تمام VLAN ها می‌باشد، یک کپی از ترافیک تمام VLAN ها به پورت Trunk می‌رود، این پورت یک پورت خاص بر روی سوئیچ نیست، بلکه باید برای سوئیچ آن را تعریف کرد و می‌توانیم چندین پورت Trunk بر روی یک سوئیچ داشته باشیم. حال پورت Trunk چگونه تشخیص دهد که بسته‌ایی که به آن رسیده است متعلق به کدام VLAN است، دو روش برای اضافه کردن VLAN-ID به بسته وجود دارد.

۱- روش Inter Switch Link : ISL

انحصاری شرکت cisco است. فریم Ethernet در حدود ۱۵۱۸ بایت است، بسته‌هایی که بیش‌تر از ۱۵۱۸ بایت باشند به آن‌ها Giant Frame گویند و پورت‌های ethernet این بسته‌ها را drop می‌کنند، مگر آنکه توسط پورت trunk مبادله شوند. ساختار بسته را در شکل ۷-۱ مشاهده خواهید کرد.



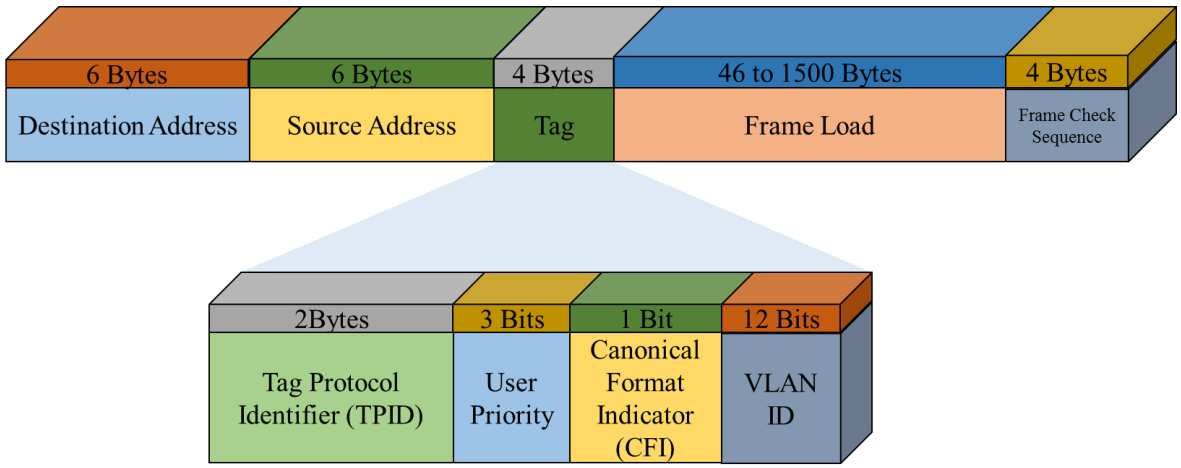
شکل ۷-۱ ساختار بسته ISL

1518 Bytes + 30 Bytes = 1548 Bytes

در این روش هدف آن است که اعلام شود بسته متعلق به کدام VLAN است.

۲- روش IEEE 802.1q یا dot 1q

روش استاندارد افزودن VLAN-ID بر روی بسته‌ها توسط پورت Trunk است.در این روش به Header فریم Ethernet، ۴ بایت اضافه می‌شود و ۱۲ بیت آن VLAN -ID است. ساختار بسته dot 1 q را در شکل ۷-۲ مشاهده می‌کنید.



شکل ۷-۲ ساختار بسته dot 1 q

نحوه تنظیم پورت Trunk

برای up شدن یک لینک trunk دو شرط لازم است.

۱- باید encapsulation دو طرف یکسان باشد (هر دو یا ISL یا 802.1q)

۲- باید Trunk mode مشخص شده باشد.

a. برای trunk mode سه حالت داریم، on، Auto و desirable است

در حالت on، پورت trunk است و به طرف دیگر پیشنهاد می‌دهد که trunk شود.

در حالت auto، پورت قابلیت trunk شدن دارد، اما تا زمانی که پیشنهادی دریافت نکند trunk نمی‌شود و پیشنهاد هم نمی‌دهد.

در حالت desirable، پورت آماده trunk شدن است هنوز trunk نشده است اما بسته پیشنهادی به طرف مقابل برای trunk شدن ارسال می‌کند.

بر مبنای توضیحات مرتبط با trunk mode، پروتکل Dynamic Trunking Protocol (DTP) را داریم، این پروتکل در مورد حالت‌های پورت‌های سوئیچ است، و جدول ۷-۱ نحوه عملکرد آن را بیان می‌کند.

جدول ۷-۱ نحوه عملکرد DTP

	Dynamic Auto	**Dynamic Desirable**	**Trunk**	**Access**
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

با توجه به شرط اول، ابتدا باید encapsulation را مشخص کنیم.

Switch (config-if) # switchport trunk encapsulation (dat1q or ISL)

این دستور معمولا برای سوئیچ‌های لایه دومی استفاده نمی‌شود.

Switch (config-if) # switchport mode trunk

Switch (config-if) # switchport mode dynamic (Auto or desirable)

این فرمان و فرمان، switchport allowed VLAN (number(s)) اختیاری و تکمیلی است.

سوالات و تمرینات

فرض کنید در یک اداره ۱۰۰ کاربر شبکه دارید که در ۴ طبقه هستند و ۱۰ نفر بخش مدیریت، ۲۰ نفر بخش HR، ۳۰ نفر بخش IT، ۲۰ نفر بخش خدمات و ۲۰ نفر بخش اداری هستند. کاربران هر بخش از یک شبکه مجزا استفاده می‌کنند و در طبقه اول تا چهارم، کارمندان ۴ بخش، HR، IT، خدمات و اداری قرار دارند و

بخش مدیریت در طبقه سوم و چهارم قرار دارند. با کمترین تجهیزات یک شبکه داخلی برای این اداره طراحی کنید. رنج آدرس IP را نیز محاسبه کنید.

آزمایش ۸

اهداف: آشنایی با مفهوم Inter VLAN Routing or Router on a Stick

سناریو ۸: شبکه‌ایی داریم که شبکه‌های محلی مجزایی دارد که همه در بستر یک شبکه واحد هستند و از سوی دیگر با محدودیت منابع مواجه هستیم.

اجزای مورد نیاز:

- End device
- Switch
- Router

همانطور که می‌دانید هر VLAN یک شبکه محلی مجازی است که تمام ویژگی‌های یک شبکه از قبیل IP Address مجزا را دارد. حال اگر بخواهیم ترافیک از یک VLAN به VLAN دیگری منتقل شود باید از مفاهیم و ابزارهای لایه سوم استفاده کنیم. برای این کار کافی است تا یک Router با اینترفیس فیزیکی یا مجازی در اختیار داشته باشیم. کاربران VLAN های مجزایی که می‌خواهیم ترافیک آن‌ها به یکدیگر منتقل شوند باید IP Address اینترفیس فیزیکی یا مجازی Router را به عنوان default gateway داشته باشند.

انواع روش‌های اتصال VLAN به Router

۱- استفاده از یک مسیریاب و با به کار گیری یک لینک اترنت بین سوئیچ و مسیریاب جهت هر VLAN

۲- استفاده از مسیریاب و برقراری ارتباط VLAN Trunk با یک سوئچ

۳- استفاده از یک سوئچ لایه سه

در حالت اول فرض کنید، تعداد VLAN هایی که قصد دارید ترافیک آن‌ها منتقل شود، ۱۰ عدد است و باید به ۱۰ اتصال مجزا بین سوئیچ و مسیریاب داشته باشیم.

از نظر شکل و توپولوژی روش دوم و سوم مشابه هستند و تنها تفاوت آن‌ها در استفاده از سوئیچ لایه سوم به جای مسیریاب می‌باشد.

استفاده از پورت Trunk کمک می‌کند تا مسیریاب از طریق یک اینترفیس منطقی (مجازی) با هر VLAN ارتباط برقرار کند. مفهوم Router on a Stick معمولا در سازمان هایی با ابعاد کوچک و متوسط که قصد دارند مسیریابی بین VLAN ها را داشته باشند پیاده سازی می‌شود. این به معنای آن است که مسیریابی در شبکه داخلی بین VLAN ها انجام خواهد شد. از یک مسیریاب استفاده خواهد شد تا بتوان به جای استفاده از سوئیچ لایه ۳، بین VLAN های مختلف، برای سرورها و داده‌های کلاینت‌ها مسیریابی انجام شود. دراین سناریویک اینترفیس فیزیکی مسیریاب را به چندین اینترفیس مجازی تبدیل خواهیم کرد (sub interface) که هر اینتفرقیس مجازی مرتبط با یک VLAN مد نظر ما می باشد، سپس مسیریاب، با تمام فریم‌هایی که با شناسه VLAN های مشخص برچسب‌گذاری شده‌اند به گونه‌ای برخورد می‌کند که گویی ورود و خروج فریم‌ها از زیر اینترفیس‌های مجازی صورت پذیرفته است.

تنظیمات سوئیچ و ساخت VLAN ها را مشابه قبل انجام می‌دهیم، پورت Trunk را ایجاد می‌کنیم. در این سناریو تنظیمات اصلی در قسمت Router باید انجام شود. برای end device های درون سناریو IP Address تخصیص می‌دهیم و برای هر مجموعه از End device هایی که متعلق به یک VLAN است یک IP Address در رنج همان IP Address به عنوان آدرس Default Gateway در نظر می‌گیریم، معمولا آدرس default gateway اولین و یا آخرین آدرس رنج آدرس می‌باشد.

پیکربندی Router on a stick در Router

```
Router(config) # interface gi 0/0
Router(config-if) # no shutdown
Router(config) # interface gi 0/0.10
Router(config-subif) # encapsulation dot1Q 10
Router(config-subif) # ip address 10.1.10.1 255.255.255.0
```

اکنون می‌توانیم با دستور show ip interface brief وضعیت اینترفیس‌های ایجاد شده و آدرس‌های IP آن‌ها را مشاهده نمود.

سوالات و تمرینات

سناریوی بخش سوالات و تمرینات جلسه قبل را در نظر بگیرید و حالا امکان مسیریابی و انتقال ترافیک بین VLAN ها را نیز به آن اضافه کنید.

آزمایش ۹

اهداف: آشنایی با مفهوم VLAN Trunking Protocol (VTP)

سناریو ۹: شبکه‌ایی داریم که شبکه‌های محلی مجزایی دارد که همه در بستر یک شبکه واحد هستند و از سوی دیگر با محدودیت منابع مواجه هستیم.

اجزای مورد نیاز:

- End device
- Switch

این پروتکل، یک پروتکل لایه دومی برای ارتباط بین سوئیچ‌ها می‌باشد. در این پروتکل، کلیه VLANها بر روی یک سوئیچ که به آن VTP Server گفته می‌شود ساخته می‌شود و توزیع VLAN ها بر عهده VTP Server قرار می‌گیرد، در این حالت سایر سوئیچ‌ها به طور معمول VTP Client خواهند بود.

در VTP چهار حالت برای سوئیچ تعریف می‌شود.

- Server
- Client
- Transparent
- off

در سوئیچی که حالت Server دارد کلیه VLAN ها ساخته شده و این سوئیچ وظیفه توزیع VLAN ها به سایر سوئیچ‌ها را بر عهده دارد، سوئیچ با حالت Client نقش دریافت کننده و انتقال دهنده بسته‌های VTP را دارد و سوئیچ Transparent از سوئیچ Server، VLAN دریافت نمی‌کند، اما بسته‌های VTP را منتقل می‌کند. لازم به ذکر است که دریافت و انتقال بسته‌ها تحت شرایط خاصی انجام می‌شود.حالت off همانند Transparent می باشد با این تفاوت که Advertisementها را ارسال نمی کند

وارد سوئیچی که می‌خواهید نقش server دارد شوید و دستور زیر را وارد کنید.

Switch (config) # vtp mode server

نکته: به طور معمول، سوئیچ‌ها حالت server دارند، اما هنگامی که می‌خواهید از VTP استفاده کنید بهتر است به طور خاص دستورات را وارد کنید.

حال تمام مسیری که قرار است بسته‌های VTP در آن منتقل شود را Trunk می‌کنیم.

نکته: برای Trunk کردن کل مسیر می‌توانید از DTP استفاده کنید.

سایر سوئیچ‌ها را در حالت Client تنظیم کنید.

Switch (config) # vtp mode client

در هنگامی که سوئیچ‌ها راه‌اندازی می‌شوند در VLAN default یا VLAN 1 قرار دارند و پارامتری به نام revision number دارند، که مقدار ابتدایی آن صفر است. این پارامتر را با اجرای دستور زیر می‌توانید مشاهده کنید.

Switch # show vtp status

بر روی سوئیچ server، ۳ عدد VLAN می‌سازیم و حال revision به عدد ۳ تغییر کرده است. حال VTP Server یک بسته update به نام VTP Advertisement را به client ها ارسال می‌کند و طی این بسته اعلام می‌کند که مقدار revision به عدد ۳ تغییر کرده است و client ها با بررسی revision متوجه تغییرات شده، و متوجه می‌شوند که یک بسته update جدید است و تغییرات را اعمال می‌کنند و بسته را اصطلاحاً به سایر پورت‌ها relay می‌کنند. بسته‌های VTP از نوع multicast لایه دومی هستند.

تنظیمات مرتبط با VTP و VLAN در running-config و startup-config ذخیره نمی‌شوند و در فایلی به نام VLAN.dat در Flash ذخیره می‌شوند و برای پاک کردن VLAN ها باید از دستور زیر استفاه کنیم.

Switch # delete flash:VLAN.dat

پس مقدار revision number نیز در VTP Server در این فایل قرار دارد. پورت‌هایی که عضو VLAN هستند در running-config قرار دارند.

فرض کنید در حال حاضر revision شبکه ۱۵ است و نیاز به یک سوئیچ دارید، یک سوئیچ از قبل در اختیار دارید، پورت trunk و دیگر موارد را تنظیم می‌کنید و سپس سوئیچ را به شبکه متصل می‌کنید و به ناگاه شبکه از بین می‌رود. دلیل این اتفاق چیست؟

دلیل آن این است که سوئیچ از قبل دارای config بوده و در فایل VLAN.dat برای revision مقدار وجود دارد و دارای تعدادی VLAN است. حال این مقدار به عنوان update به تمام سوئیچ‌ها ارسال می‌شود و پورت‌ها زرد رنگ شده و شبکه down-down می‌شود. برای جلوگیری از این مشکل باید برای شبکه و مسیر انتقال بسته VTP یک دامنه ایجاد کنیم تا VTP در آن دامنه بتواند عمل کند. پس با دستورات زیر دامنه بر روی تمام سوئیچ‌های متعلق به آن دامنه ایجاد می‌شود.

Switch (config) # vtp domain name
Switch (config) # vtp password -----

از این پس سوئیچ‌ها update هایی را تبادل می‌کنند که این مقدار را به صورت یکسان داشته باشند و در واقع عضو یک دامنه باشند.

به صورت تجربی، بهتر آن است که تنظیمات شبکه در حالت VTP را از پایین‌ترین سطح انجام دهیم.

فرض کنید، در یک شبکه از VTP استفاده کردیم، حال در این شبکه می‌خواهیم سوئیچی داشته باشیم که VLANهای مخصوص برای آن سوئیچ را تعریف کنیم و این سوئیچ در ارتباط با دیگر سوئیچ‌های شبکه است، در این حالت باید از حالت Transparent استفاده کنیم و توجه داشته باشید که دامنه و پسورد مشابه با سایر سوئیچ‌های شبکه استفاده شود.

Switch (config) # vtp mode transparent

سوالات و تمرینات

سوال آزمایش ۷ را در نظر بگیرید، برای آن از پروتکل VTP استفاده کنید و VLAN مربوط به مدیران از طریق VTP Server منتقل نشود.

آزمایش ۱۰

اهداف: آشنایی با مفهوم Port Security

سناریو ۱۰: شبکه‌ایی داریم که قصد داریم تنها کاربران خاصی قادر باشند از یک اینترفیس به شبکه وصل شوند.

اجزای مورد نیاز:

- End device
- Switch

مفهوم Port Security یک مفهوم لایه دومی است که از طریق به کار گرفتن آن تنها برای کاربران محدودی ترافیک از اینترفیس عبور خواهد کرد.

در حالت کلی Port Security در سه حالت زیر کار می کند

- Dynamic حالت معمولی که تمام MAC Address ها یاد می‌گیرد و اجازه اتصال می‌دهد.
- Static تنها به MAC Address هایی که ما تعیین می‌کنیم اجازه دسترسی می‌دهد.
- Sticky به صورت اتوماتیک MAC Address ها را ثبت می‌کند با این تفاوت که این تعداد آدرس‌ها ثبت شده محدود هستند.

پیکربندی Port Security

```
Switch (config) # int fa 0/1
Switch(config-if) # switchport mode access
```

نکته : Port Security را روی پورتی که Access است می‌توان فعال کرد

```
Switch (config-if) # switchport port-security
Switch (config-if) # switchport port-security maximum 3
```

نکته : پیش فرض مقدار یک است و تا ۱۳۲ می‌توان مقداردهی کرد.

```
Switch (config-if) # switchport port-security violation restrict
```

اگر تعداد MAC address های مورد استفاده از پورت، بیشتر از مقدار مشخص شده بیشتر شود یا MAC address غیر از MAC address مجاز از پورت استفاده کند اقدامی که برای مقابله آن درنظر گرفته شده است به صورت پیش فرض shutdown است که باعث خاموش شدن و در حالت err-disable قرار گرفتن پورت می‌شود. البته می‌توان به جای shutdown از حالت‌های دیگر مثل Protect یا restrict استفاده کرد. در حالت protect پورت را خاموش نمی‌کند و اجازه عبور را به فریم‌های مربوط به MAC address های غیر مجاز را نمی‌دهد. حالت Restrict عملکرد مشابه protect دارد با این تفاوت که log نیز تولید می‌کند.

- Protect در این حالت ترافیک مربوط به دستگاه غیر مجاز Drop می شود
- Restrict همانند حالت قبل ترافیک مربوط به دستگاه غیر مجاز Drop می شود و علاوه بر این Log نیز تولید می کند.
- Shut Down سخت گیرانه ترین حالت می باشد که با دریافت ترافیک غیرمجاز پورت مربوطه در حالت Err-Disable قرار می گیرد و پورت خاموش می شود و برای خارج کردن آن از این حالت باید وارد تنظیمات سوئیچ شد و پورت مورد نظر را خاموش و روشن کرد.

تعیین MAC Address های مجاز به دو صورت دستی و Sticky انجام می‌شود.

```
Switch(config-if) # switchport port-security mac-address BD49.FE30.3596
or
Switch (config-if) # switchport port-security mac-address sticky
```

نکته : در صورتی که بخواهیم MAC Address هایی که از طریق Sticky آنها را پیدا کرده ایم را حذف کنیم از دستورات زیر استفاده می‌کنیم

```
Switch # clear port-security all
Switch # clear port-security sticky interface fastEthernet 0/1
```

همچنین از این دستورات نیز می‌توان برای Port Security استفاده کرد.

```
Switch # show port-security
```

Switch # show port-security address

Switch # show port-security interface fa0/1

این مفهوم لایه دومی در شبکه ما در مقابل حملات زیر ایمن می‌کند.

- MAC Flooding Attack
- MAC Address Spoofing
- DHCP Starvation

همچنین از دسترسی دستگاه‌های غیر مجاز به شبکه و ایجاد مشکلات ناشی مانند سرقت اطلاعات و آلوده کردن شبکه و غیره جلوگیری می‌کند.

در صورت Shut Down شدن یک اینترفیس به دلیل نقض Port Security شما باید وارد آن اینترفیس شوید و یک بار آن را خاموش و روشن کنید.

نکته: با دستور زیر می توانید این کار را به صورت خودکار انجام دهید.

Switch(config) # errordisable recovery cause psecure-violation

Switch(config) # errordisable recovery interval <time>

مشاهده تنظیمات مربوط به Error Disable

Switch # show errordisable recovery

جدول ۱۰-۱ حالات مختلف نقض امنیت را نشان می‌دهد.

جدول ۱۰-۱

Security Violation modes

Violation Mode	Forwards Traffic	Sends Sys log Message	Displays Error Message	Increase Violation Counter	Shut Downs Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shut down	No	No	No	Yes	Yes

سوالات و تمرینات

حالت‌های مختلف Port security را بر روی پورت‌های مختلف یک سوئیچ پیاده‌سازی کنید.

آزمایش ۱۱

اهداف: آشنایی با مفهوم Spanning Tree Protocol (STP)

سناریو ۱۱: در یک شبکه چهار سوئیچ داریم که به یکدیگر متصل هستند، می‌خواهیم از ایجاد حلقه لایه دومی در ان‌ها جلوگیری نماییم.

اجزای مورد نیاز:

- Switch

پروتکلSTP ، یاSpanning Tree Protocol ، یکی از پروتکل‌های حیاتی در شبکه‌های سوئیچینگ است که برای جلوگیری از ایجاد حلقه‌ها (loops) در شبکه‌های لایه دو (Data Link Layer) مورد استفاده قرار می‌گیرد. حلقه‌ها می‌توانند منجر به ایجاد مشکلاتی از جمله طغیان بسته‌ها، کاهش کارایی شبکه و ایجاد مشکلات در ارتباطات شبکه شوند. پر.وتکل STP به‌طور خودکار شبکه را از وجود حلقه‌ها محافظت می‌کند و یک توپولوژی درختی بدون حلقه را برای شبکه ایجاد می‌کند.

تاریخچه و توسعهSTP

پروتکل STP توسط IEEE (Institute of Electrical and Electronics Engineers) به عنوان استاندارد 802.1d معرفی شد. این پروتکل ابتدا توسط Dr. Radia Perlman در دهه ۱۹۸۰ توسعه داده شد و تا کنون چندین بار مورد به‌روزرسانی قرار گرفته است.

عملکرد پروتکلSTP

مفهوم درخت پوشا(Spanning Tree)

هدف اصلی STP این است که یک درخت پوشا (Spanning Tree) را در میان همه سوئیچ‌های موجود در شبکه ایجاد کند. درخت پوشا مجموعه‌ای از لینک‌ها است که تمام سوئیچ‌ها را به هم متصل می‌کند بدون

اینکه هیچ حلقه‌ای در شبکه ایجاد شود. این درخت از یک سوئیچ به‌عنوان ریشه (Root Bridge) شروع می‌شود و به همه سوئیچ‌های دیگر متصل می‌شود.

انتخاب Bridge ریشه(Root Bridge)

هر سوئیچ در شبکه STP دارای یک Bridge ID است که شامل دو بخش زیر می‌شود:

- Bridge Priority یک مقدار ۱۶ بیتی که به‌طور پیش‌فرض ۳۲۷۶۸ است.
- MAC Address آدرس فیزیکی (MAC) سوئیچ

سوئیچی که کمترین مقدار Bridge ID را دارد به عنوان Root Bridge انتخاب می‌شود. این انتخاب به صورت خودکار انجام می‌شود و سوئیچ‌ها بر اساس Bridge ID خود در انتخاب Root Bridge شرکت می‌کنند.

انتخاب مسیرهای فعال و غیرفعال

بعد از انتخابRoot Bridge ، هر سوئیچ باید بهترین مسیر را برای رسیدن به Root Bridge انتخاب کند. این کار با محاسبه Root Path Cost انجام می‌شود که هزینه‌ای است که یک سوئیچ برای رسیدن به Root Bridge باید بپردازد. هزینه مسیر با توجه به سرعت لینک‌ها محاسبه می‌شود:

- 10 Mbps: هزینه ۱۰۰
- 100 Mbps: هزینه ۱۹
- 1Gbps: هزینه ۴
- 10Gbps: هزینه ۲

سوئیچی که کمترین Root Path Cost را دارد به عنوان Designated Bridge برای هر سگمنت انتخاب می‌شود. لینک‌هایی که توسط Designated Bridge و Root Bridge استفاده نمی‌شوند، به حالت Block در می‌آیند تا از ایجاد حلقه جلوگیری شود.

حالات پورت‌ها در STP

پورت‌های سوئیچ در STP می‌توانند در یکی از حالت‌های زیر باشند:

- Blocking در این حالت، پورت هیچ بسته‌ای را ارسال یا دریافت نمی‌کند. این حالت برای جلوگیری از حلقه‌ها استفاده می‌شود.
- Listening پورت در این حالت به دنبال BPDU ها (Bridge Protocol Data Units) است تا اطلاعات توپولوژی شبکه را به‌روزرسانی کند.
- Learning پورت در این حالت آدرس‌های MAC را یاد می‌گیرد اما هنوز داده‌ها را فوروارد نمی‌کند.
- Forwarding پورت در این حالت بسته‌ها را ارسال و دریافت می‌کند.
- Disabled پورت به‌طور دستی غیرفعال شده و هیچ بسته‌ای را ارسال یا دریافت نمی‌کند.

BPDU (Bridge Protocol Data Unit)

بسته‌های کنترلی هستند که توسط STP برای مبادله اطلاعات توپولوژی بین سوئیچ‌ها استفاده می‌شوند. دو نوع BPDU وجود دارد

- Configuration BPDU برای تعیین Root Bridge و به‌روزرسانی توپولوژی شبکه استفاده می‌شود.
- Topology Change Notification (TCN) BPDU زمانی که تغییری در توپولوژی شبکه رخ می‌دهد، ارسال می‌شود.

تغییر توپولوژی و Convergence

هرگاه تغییری در توپولوژی شبکه رخ دهد (مثلاً قطع یک لینک)، STP باید توپولوژی جدیدی را ایجاد کند. این فرآیند به عنوان Convergence شناخته می‌شود. در این حالت، سوئیچ‌ها به تبادل BPDU ها پرداخته و یک توپولوژی جدید بدون حلقه را ایجاد می‌کنند.

انواع STP و بهبودهای آن

- RSTP (Rapid Spanning Tree Protocol) - IEEE 802.1w

نسخه‌ای بهبود یافته از STP است که به عنوان استاندارد IEEE 802.1w معرفی شده است. این پروتکل سرعت Convergence را افزایش داده و زمان پاسخگویی شبکه به تغییرات توپولوژی را بهبود می‌بخشد. در RSTP ، پورت‌ها می‌توانند مستقیماً از حالت Blocking به Forwarding تغییر کنند و دیگر نیازی به گذراندن تمامی حالات STP ندارند.

- MSTP (Multiple Spanning Tree Protocol) - IEEE 802.1s

نسخه‌ای دیگر از STP است که اجازه می‌دهد چندین درخت پوشا در یک شبکه ایجاد شود. این پروتکل به هر VLAN اجازه می‌دهد که توپولوژی مخصوص به خود را داشته باشد MSTP .ترافیک شبکه را بهینه‌تر توزیع می‌کند و از منابع شبکه بهتر استفاده می‌کند.

- PVST+ (Per-VLAN Spanning Tree Plus)

نسخه‌ای اختصاصی از STP است که توسط Cisco توسعه داده شده و به ازای هر VLAN یک درخت پوشا ایجاد می‌کند. این نسخه امکان بهینه‌سازی بیشتر توپولوژی شبکه و مدیریت ترافیکVLAN ها را فراهم می‌کند.

مشکلات و چالش‌های STP

با وجود مزایایSTP ، این پروتکل دارای چالش‌ها و مشکلاتی نیز هست

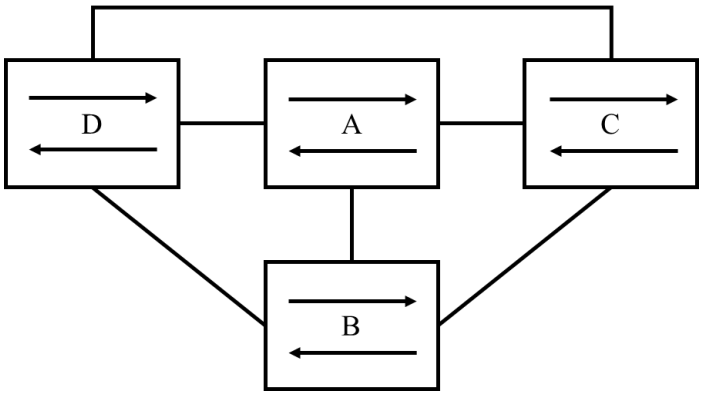
- زمان طولانیConvergence : در STP کلاسیک، زمان Convergence ممکن است چندین ثانیه طول بکشد که این می‌تواند در برخی از شبکه‌ها باعث مشکلاتی شود.
- پیکربندی پیچیده در شبکه‌های بزرگ: مدیریت و پیکربندی STP در شبکه‌های بزرگ و پیچیده ممکن است دشوار باشد و نیاز به دانش عمیقی از توپولوژی شبکه دارد.
- مشکلات احتمالی در تغییرات توپولوژی: اگر تغییرات توپولوژی به‌درستی مدیریت نشوند، ممکن است باعث بروز مشکلاتی در شبکه شود.

ملاحظات طراحی و پیاده‌سازی STP

در پیاده‌سازی STP در یک شبکه، باید موارد زیر را در نظر گرفت:

- انتخاب مناسب Root Bridge: انتخاب یک سوئیچ با پیکربندی مناسب به عنوان Root Bridge می‌تواند تأثیر زیادی در عملکرد شبکه داشته باشد.
- تنظیم Bridge Priority: تنظیم صحیح Bridge Priority برای سوئیچ‌ها می‌تواند در بهبود Convergenceو مدیریت توپولوژی شبکه موثر باشد.
- مانیتورینگ و نگهداری: مانیتورینگ مستمر وضعیت STP و نگهداری منظم شبکه می‌تواند از بروز مشکلات جلوگیری کند.

مطابق شکل ۱۱-۱ چهار سوئیچ A, B, C, D را در نظر بگیرید . این توپولوژی به صورت فیزیکی یک حلقه ایجاد می‌کند که می‌تواند باعث ایجاد مشکلاتی مانند طغیان بسته‌ها شود. برای جلوگیری از این مشکلات، از پروتکل STP استفاده می‌کنیم.



شکل ۱۱-۱ سناریو برای توضیح STP

به طور پیش‌فرض، پروتکل STP در بیشتر سوئیچ‌های مدرن فعال است. اما برای اطمینان از فعال بودن STP در سوئیچ‌ها، می‌توانید از دستور زیر استفاده کنید:

```
Switch(config)# spanning-tree vlan 1
```

این دستور STP را برای VLAN 1 فعال می‌کند. برای اطمینان از فعال بودنSTP ، می‌توانید از دستور زیر استفاده کنید:

```
Switch# show spanning-tree
```

این دستور وضعیت STP را در سوئیچ نمایش می‌دهد.

در این سناریو، می‌خواهیم سوئیچ A به عنوان Root Bridge انتخاب شود. برای این کار، باید اولویت (Priority) سوئیچ A را به یک مقدار پایین‌تر از مقادیر پیش‌فرض دیگر سوئیچ‌ها تنظیم کنیم

SwitchA(config)# spanning-tree vlan 1 priority 4096.

مقدار ۴۰۹۶ کمترین مقداری است که می‌توان برای اولویت یک سوئیچ تنظیم کرد (مقادیر پایین‌تر نشان‌دهنده اولویت بالاتر هستند). مقادیر پیش‌فرض برای سوئیچ‌های دیگر ۳۲۷۶۸ است، بنابراین با تنظیم اولویت ۴۰۹۶، سوئیچ A به احتمال زیاد به عنوان Root Bridge انتخاب خواهد شد.

بعد از انتخابRoot Bridge ، می‌توانید وضعیت پورت‌های سوئیچ‌های مختلف را بررسی کنید تا مطمئن شوید که کدام پورت‌ها در حالت Forwarding و کدام در حالت Blocking هستند. برای این کار از دستور زیر استفاده کنید.

Switch# show spanning-tree vlan 1

این دستور وضعیت STP را برای VLAN 1 نشان می‌دهد. برای هر پورت می‌توانید حالت آن را مشاهده کنید (Forwarding، Blocking، Listening، Learning)

اگر به پورت‌هایی که به کامپیوترها یا سرورها متصل هستند نیاز دارید که سریع‌تر به حالت Forwarding بروند (بدون نیاز به انتظار برای گذر از حالت‌های مختلفSTP)، می‌توانید ویژگی PortFast را فعال کنید. این ویژگی برای پورت‌هایی که مطمئن هستید هیچ حلقه‌ای در آنها وجود ندارد، مفید است.

Switch(config)# interface fastethernet 0/1
Switch(config-if)# spanning-tree portfast

این دستور ویژگی PortFast را برای پورت FastEthernet 0/1 فعال می‌کند.

برای جلوگیری از ایجاد حلقه توسط پورت‌هایی که PortFast فعال شده‌اند (اگر به اشتباه به سوئیچ دیگری متصل شوند)، می‌توانید BPDU Guard را فعال کنید. این ویژگی باعث می‌شود که اگر BPDUs در این پورت دریافت شوند، پورت به‌طور خودکار غیر فعال (shutdown) شود.

Switch(config-if)# spanning-tree bpduguard enable

برای جلوگیری از اینکه سوئیچ‌های دیگر به‌طور غیرمجاز به عنوان Root Bridge انتخاب شوند، می‌توانید ویژگی Root Guard را بر روی پورت‌هایی که به سوئیچ‌های دیگر متصل هستند فعال کنید.

Switch(config-if)# spanning-tree guard root

این دستور پورت را از تبدیل شدن به پورت Root محافظت می‌کند.

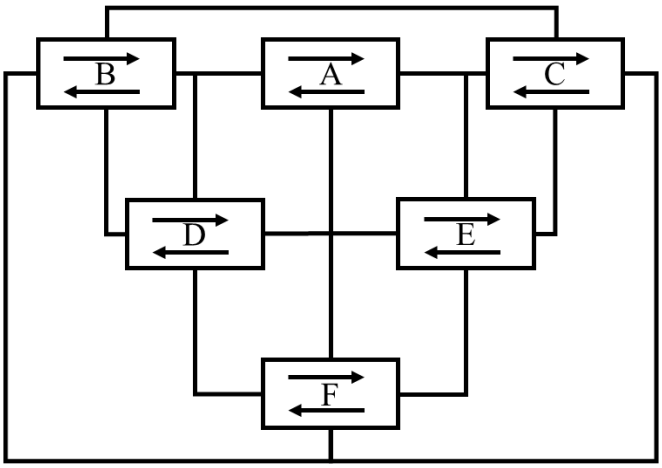
بعد از اعمال تنظیمات مختلف، می‌توانید وضعیت نهایی STP را با استفاده از دستور زیر مشاهده کنید.

Switch# show spanning-tree detail

این دستور جزئیات بیشتری از وضعیتSTP ، از جمله زمان‌هایForward Delay ، Max Age و وضعیت دقیق هر پورت را نمایش می‌دهد.

سوالات و تمرینات

شکل زیر را در نظر بگیرید با انتخاب سوئیچ یک به عنوان Root Bridge، پروتکل SPT را در این شبکه پیاده‌سازی کنید.



آزمایش ۱۲

اهداف: آشنایی با مفهوم مسیریابی و مسیریابی Static

سناریو ۱۲: می‌خواهیم بین چندین شبکه LAN با کمک مسیریاب‌ها، عمل مسیریابی را به روش Static انجام دهیم

اجزای مورد نیاز:

- Router
- سایر تجهیزات مرتبط برای پیاده‌سازی شبکه LAN

تعریف Router

یک دستگاه لایه سومی است که حداقل دارای دو اینترفیس و یک جدول Routing است، که مسیریابی بین NET ID های مختلف را انجام می‌دهد. این دستگاه در مرز شبکه قرار می‌گیرد و باید آن را در جایی قرار دهید که داده از شبکه بیرون می‌رود و یا به شبکه وارد می‌شود، به عبارت دیگر، دروازه ورود و خروج به شبکه است. این دستگاه به صورت plug & play نیست و باید تنظیم شود. دارای تنوع زیادی است و از لحاظ تعداد اینترفیس برخلاف سوئیچ اینترفیس کمتری دارد، اما این دستگاه ماژولار است و از آنجا که می‌توانید برای آن ماژول نصب کنید، می‌توانید تنوع اینترفیس داشته باشید.

تعریف Routing یا مسریابی

ورود ترافیک به اینترفیس اول مسیریاب، چک شدن آدرس مقصد در جدول routing table و خروج از اینترفیس دیگر (دوم) را گویند. (منظور از آدرس مقصد IP Address است) به عبارت دیگر، فوروارد کردم بسته از اینترفیس ورودی به اینترفیس خروجی بر اساس آدرس منطقی مقصد پس از بررسی routing table.

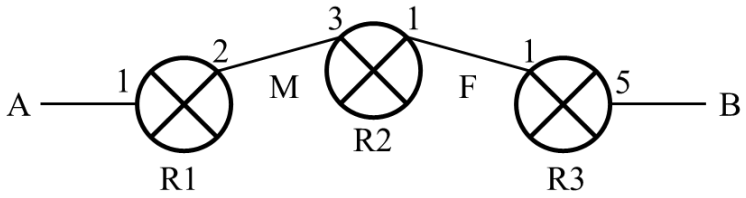
نکته: هر مسیریاب می‌تواند بسته را به همسایه خودش route کند.

مسیریاب‌ها هنگامی با هم همسایه هستند که:

۱- با یکدیگر لینک فیزیک داشته باشند

۲- آدرس IP دو سر لینک در یک رنج باشد.

در شکل ۱۲-۱، R2 و R3 با یکدیگر همسایه هستند، ۱- اتصال فیزیکی دارند. ۲- اینترفیس ۱ از R2 و اینترفیس ۱ از R3 در یک رنج آدرس IP هستند.



شکل ۱۲-۱ تعدادی Router و اتصال آن‌ها

جدول مسیریابی (Routing Table)

جدول مسیریابی مسیریاب‌های شبکه به سه روش تکمیل می‌شود.

۱- Connected: این روش به صورت خودکار است و توسط خود مسیریاب انجام می‌شود. هدف از این روش آن است تا مسیریاب شبکه‌های اطراف خود را شناسایی کند. منظور از شبکه‌های اطراف، شبکه‌هایی است که به صورت فیزیکی به مسیریاب متصل هستند. هنگامی که مسیریاب روشن می‌شود، Network Address های اینترفیس‌هایی که فیزیکی به آن‌ها وصل است را در routing table قرار می‌دهد. مسیری که به شیوه Connected آموخته شود به صورت © نمایش داده می‌شود. اما برای آن که جدول مسیریابی به این شیوه تکمیل شود آن است که: ۱- اینترفیس‌ها IP Address داشته باشند ۲- اصطلاحاً اینترفیس‌ها up-up باشند.

نکته: در جدول مسیریابی همیشه Network Address نوشته می‌شود.

روش connected لازم است، اما کافی نیست.

۲- Static: به صورت دستی و توسط مدیر (admin) شبکه نوشته می‌شود. $Destination\ Network \rightarrow Next\ Hop$ مسیری که به این شیوه آموخته می‌شود با حرف (S) نشان داده می‌شود.

نکته: اگر به صورت Static جدول مسیریابی را تکمیل می‌کنید، باید مسیر را به صورت رفت و برگشت بنویسید.

نوشتن default route: به ازای Network Address خاصی Next hop را مسیریاب خاصی در نظر نمی‌گیرند، بلکه به ازای تمامی Network Address ها به آن مسیریاب پرش می‌کنند. این مسیر در واقع یک مسیر از نوع static است

نکته: می‌توانیم چندین مسیریاب به عنوان default route داشته باشیم.

اگر در جدول مسیریابی مسیریابی default route داشته باشیم، هیچ بسته‌ایی را drop نمی‌کند.

۳- Dynamic: ساخت و نگهداری جدول routing table به صورت پویا

اجزای جدول مسیریابی

جدول مسیریابی معمولا به صورت جدول ۱۲-۱ می‌باشد.

جدول ۱۲-۱ مثالی از یک جدول مسیریابی

Network Destination	Netmask	Gateway	Interface	Metric
10.10.0.0	255.255.255.255.254	192.168.0.1	192.168.0.100	10
192.168.0.100	255.255.255.255	192.168.0.2	192.168.0.200	5
0.0.0.0	0.0.0.0	192.168.0.3	192.168.0.300	100

همانطور که در جدول ۱۲-۱ مشاهده می‌کنید جدول مسیریابی دارای بخش‌های متفاوتی است.

- Network Identifier
- Next Hop
- Metric

هزینه مربوط به استفاده از مسیر مشخص شده را نشان می دهد. این برای تعیین کارایی یک مسیر خاص بین دو نقطه در شبکه مفید است.

در جدول مسیریابی صرفاً با داشتن Network Address نمی‌توانیم تشخیص دهیم که یک رنج آدرس IP است یا یک آدرس IP به صورت منفرد. پارامتر کمکی Netmask این مشکل را رفع می‌کند. پارامتر Netmask بسیار شبیه subnet mask و با وظیفه متفاوت است. در Netmask بیت‌هایی که یک هستند به معنی آن است که نباید آن‌ها را تغییر دهیم. اما بیت‌هایی که صفر هستند به معنی آن است که می‌توانیم مقدار صفر و یک برای آن‌ها را در نظر بگیریم

مثال: آدرس IP، 10.10.0.0 با Netmask = 255.255.255.128 بیان‌گر یک رنج آدرس IP است یا یک آدرس IP منحصر به فرد؟ این آدرس معادل رنج آدرس IP به صورت 10.10.0.127 – 10.10.0.0 می‌باشد.

نکته: اینترفیس‌های خروجی و gateway حتماً باید یا به صورت لایه یکی، یا لایه دومی به هم متصل باشند.

Destination = Network Destination + Netmask
Action = Gateway + Interface

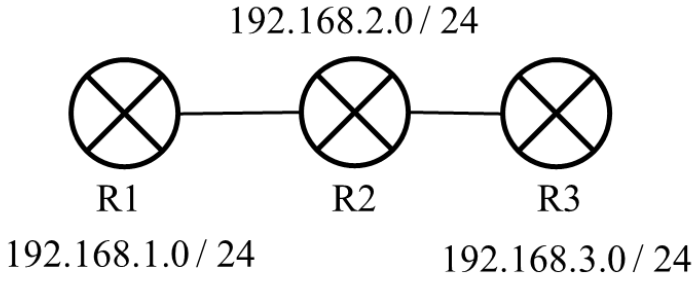
فرض کنید در یک شرکت، سه دفتر اصلی داریم که به ترتیب نام‌هایR1 ، R2، و R3 دارند. هر کدام از این مسیریاب‌ها به شبکه‌های محلی (LAN) جداگانه متصل هستند. (شکل ۱۲-۲)

آدرس IP شبکه R1: 192.168.1.0 /24

آدرس IP شبکه R2: 192.168.2.0 /24

آدرس IP شبکه R3: 192.168.3.0 /24

هدف این است که این سه مسیریاب بتوانند از طریق مسیرهای استاتیک، به یکدیگر متصل شوند و ترافیک بین این سه شبکه هدایت شود.



شکل ۱۲-۲ تصویری از مسیریاب‌های سناریو

تنظیمات اولیه مسیریاب‌ها را مطابق دستورات زیر انجام می‌دهید.

Router> enable Router# configure terminal

Router(config) # hostname R1

با این دستور نام مسیریاب را تغییر می‌دهیم.

R1(config) # interface gig0/0

R1(config-if) # ip address 192.168.1.1 255.255.255.0

R1(config-if) # no shutdown

این روند به طور مشابه برای دیگر مسیریاب‌ها انجام می‌شود.

پیکربندی مسیرهای استاتیک

Ip route “destination network address” “destination subnet mask” “next hop”

R1:

R1(config) # ip route 192.168.2.0 255.255.255.0 192.168.1.2

R1(config) # ip route 192.168.3.0 255.255.255.0 192.168.1.2

R2:

R2(config) # ip route 192.168.1.0 255.255.255.0 192.168.2.1

R2(config) # ip route 192.168.3.0 255.255.255.0 192.168.2.3

R3:

R3(config) # ip route 192.168.1.0 255.255.255.0 192.168.3.2

R3(config) # ip route 192.168.2.0 255.255.255.0 192.168.3.2

با استفاده از دستور show Ip Route می توانیم تمام مسیرها را ببینیم.

از این دستور می‌توانید ارتباط بین R1 و R3 را تست کنید.

R1# ping 192.168.3.1

در پیکربندی و استفاده از مسیرهای استاتیک، چندین نکته مهم وجود دارد که باید به آن‌ها توجه کرد.

نکات مهم در مسیریابی استاتیک

- آگاهی کامل از توپولوژی شبکه

قبل از پیکربندی مسیرهای استاتیک، باید کاملاً به توپولوژی شبکه و آدرس‌های IP آشنا باشید تا مسیرها به درستی تعریف شوند.

- تعریف مسیرهای دقیق

در تنظیم مسیرهای استاتیک، باید به دقت مسیرها و مقاصد تعریف شوند. خطا در وارد کردن آدرس مقصد یا آدرسIP، Gateway می‌تواند باعث قطع ارتباط در شبکه شود.

- تنظیم مسیرهای بازگشتی:(Return Path)

اگر دو مسیریاب بخواهند به صورت دو طرفه با یکدیگر ارتباط برقرار کنند، مسیرهای استاتیک باید در هر دو طرف تنظیم شوند. بدون مسیر بازگشتی، حتی اگر یک مسیر کار کند، ارتباط دو طرفه ممکن نخواهد بود.

- استفاده از Default Route (مسیر پیش‌فرض):

در مواقعی که تمامی ترافیک به مقصدی ناشناخته به یک Gateway مشخص هدایت می‌شود، می‌توانید از مسیر پیش‌فرض استفاده کنید

ip route 0.0.0.0 0.0.0.0 [Next-Hop IP]

این روش برای کاهش پیچیدگی در تنظیم مسیرها مفید است.

- انتخاب اولویت (Metric) مناسب

در صورتی که چندین مسیر برای یک مقصد تعریف شده باشد، می‌توان از اولویت (Administrative Distance) استفاده کرد تا مسیریاب ابتدا از مسیر مشخصی استفاده کند. مسیر با مقدار AD کمتر، اولویت بیشتری دارد. (توضیحات بیشتر در آزمایشات آتی خواهد بود)

- مدیریت دستی و نیاز به نگهداری مستمر

مسیرهای استاتیک نیاز به نگهداری و به‌روزرسانی دستی دارند، مخصوصاً در صورت تغییرات در شبکه. این مسئله برای شبکه‌های پویا اهمیت دارد.

- عیب‌یابی و نظارت مداوم

برای اطمینان از عملکرد صحیح مسیرها، از دستورات نظارتی مانند

- show ip route برای نمایش مسیرهای موجود
- Ping برای تست ارتباط.
- Traceroute برای مشاهده مسیر دقیق بسته‌ها.

- امنیت و جلوگیری از مشکلات Loop

در شبکه‌هایی که مسیرهای استاتیک استفاده می‌شوند، احتمال ایجاد حلقه‌های مسیریابی (Routing Loops) کمتر است، زیرا مسیرها به صورت دستی و کنترل‌شده تعریف می‌شوند.

- انعطاف‌پذیری کمتر در مقابل خرابی‌ها

در صورت خرابی لینک یا دستگاه در مسیر، مسیریاب به طور خودکار مسیر جایگزین پیدا نمی‌کند. بنابراین برای شبکه‌هایی که نیاز به افزونگی دارند، باید مسیرهای پشتیبان نیز به صورت استاتیک تعریف شوند.

- مستندسازی دقیق

به دلیل اینکه تمامی تغییرات باید دستی اعمال شوند، مستندسازی دقیق مسیرها و توپولوژی شبکه اهمیت ویژه‌ای دارد تا در صورت نیاز به تغییرات یا عیب‌یابی، کارها سریع‌تر انجام شود.

در مجموع، توجه به این نکات در پیکربندی مسیرهای استاتیک به حفظ پایداری و عملکرد صحیح شبکه کمک می‌کند.

مزایای مسیریابی استاتیک

- سادگی و کنترل کامل

مدیر شبکه کنترل کامل بر مسیرها دارد و می‌تواند دقیقاً مشخص کند که هر ترافیک از کدام مسیر عبور کند.

- مصرف کمتر منابع سیستمی

مسیریاب‌ها در مسیریابی استاتیک نیازی به پردازش‌های پیچیده برای محاسبه مسیر ندارند، بنابراین از منابع کمتری مانند CPU و RAM استفاده می‌کنند.

- امنیت بیشتر

به دلیل این که مسیرها به صورت دستی تنظیم می‌شوند، امکان سوءاستفاده از تغییرات غیرمجاز در مسیرها کمتر است.

- پایداری

در محیط‌هایی که توپولوژی شبکه ثابت و تغییرات کمی دارند، مسیریابی استاتیک به دلیل پایداری بالا گزینه‌ی مناسبی است.

معایب مسیریابی استاتیک

- عدم انعطاف‌پذیری

در صورت تغییر در توپولوژی شبکه (مثل اضافه شدن مسیریاب جدید یا قطع شدن لینک)، مسیرهای استاتیک باید به صورت دستی به‌روز شوند. این مسئله در شبکه‌های بزرگ کار را دشوار می‌کند.

- پیچیدگی مدیریت در شبکه‌های بزرگ

با افزایش تعداد شبکه‌ها و مسیریاب‌ها، مدیریت و نگهداری مسیرهای استاتیک زمان‌بر و پیچیده می‌شود.

- عدم توانایی در تعیین مسیرهای بهینه

مسیریابی استاتیک از الگوریتم‌های مسیریابی پویا استفاده نمی‌کند و نمی‌تواند به‌صورت خودکار بهترین و کوتاه‌ترین مسیر را انتخاب کند.

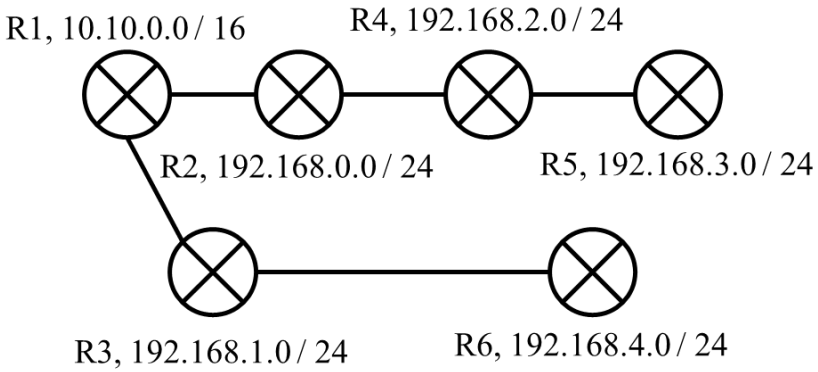
- خطر خرابی و عدم افزونگی

اگر لینک یا مسیریاب در مسیر از کار بیفتد، مسیریاب‌ها بدون پروتکل‌های مسیریابی پویا قادر به انتخاب مسیر جایگزین نیستند مگر اینکه به صورت دستی مسیرهای جدید تعریف شوند.

در کل، مسیریابی استاتیک برای شبکه‌های کوچک و پایدار که تغییرات کمی دارند مناسب است، اما در شبکه‌های بزرگ و پیچیده، استفاده از پروتکل‌های مسیریابی پویا توصیه می‌شود.

سوالات و تمرینات

شکل زیر در نظر بگیرید. مسیریابی آن را به روش استاتیک انجام دهید. این کار را طی دو مرحله انجام دهید یک بار با کمک default route (برای مسیر برگشت) و یک بار بدون در نظر گرفتن default route .



آزمایش ۱۳

اهداف: آشنایی با مفهوم پروتکل مسیریابی پویا و پروتکل مسیریابی RIP

سناریو ۱۳: می‌خواهیم بین چندین شبکه LAN با کمک مسیریاب‌ها، عمل مسیریابی را به روش RIP انجام دهیم.

اجزای مورد نیاز:

- Router
- سایر تجهیزات مرتبط برای پیاده‌سازی شبکه LAN

در آزمایش ۱۲ با مفاهیم اولیه مسیریابی و همچنین مسیریابی استاتیک آشنا شدیم، به دنبال رفع معایب این مسیریابی می‌خواهیم با مسریابی پویا آشنا شویم. ابتدا با چند اصطلاح و مفهوم دیگر آشنا شده و به سراغ روش‌های مسیریابی پویا می‌رویم، این نوع از مسیریابی دارای روش‌های متنوع با ساختارهای متفاوت هستند.

تعریف Abbreviated distance Number (AND)

پارامتر اعتماد پذیری بین روش‌های یادگیری یک مسیر

این پارامتر عددی بین ۰ تا ۲۵۵ می‌تواند داشته باشد و هرچه مقدار آن کمتر باشد به معنی آن است که اعتماد پذیری روش بیش‌تر است. اما این اعتماد پذیری بر مبنای آن است که مسیر را به چه شیوه و روشی آموخته‌ایم (به روش connected، static و غیره). اگر یک مسیر را از دو روش یاد بگیریم، روشی که دارای ADN کمتر است وارد جدول routing table خواهد شد.

مطمئن‌ترین روش یادگیری مسیر، روش Connected است و مقدار ADN آن صفر است.

بعد از روش Connected، از آنجا که مسیرهای روش Static به وسیله ادمین شبکه تعریف می‌شوند، مطمئن‌ترین روش است و ADN آن برابر یک است.

هر روش پویا، دارای ADN مجزا می‌باشد.

تعریف Metric

در آزمایش ۱۲ در جدول Routing Table مقداری به نام Metric را مشاهده کردید، اما این پارامتر چیست و به چه معناست؟ ساده‌ترین تعریفی که برای آن ارائه می‌شود، پارامتر دوری و نزدیکی به یک مسیریاب. مشابه ADN هر چه این پارامتر نیز کمتر باشد بهتر است. به این نکته دقت کنید که metric یک واحد خاص نیست و یک واحد اندازه‌گیری است، به بیان ساده، یک خط‌کش است. با این پارامتر می‌خواهیم مسافت را اندازه‌گیری کنیم. مسافت می‌تواند، فاصله، زمان، انرژی و غیره باشد.

پارامتر Metric برای Routing Protocol های متفاوت، نیز متفاوت است.

نکته: در دو سر یک لینک نمی‌توانیم دو مدل Routing Protocol مجزا اجرا کنیم، دلایل این موضوع به شرح زیر است.

۱- پارامتر متریک آن‌ها متفاوت است

۲- زبان تبلیغ مسیرهایشان متفاوت است (نحوه update کردن متفاوتی دارند)

برای انتخاب یک مسیر و قرار دادن آن در جدول Routing Table ابتدا ADN را بررسی و انتخاب می‌کنیم و سپس به سراغ متریک می‌رویم. بین چند مسیر به یک مقصد **ثابت**، با ADN و متریک مساوی، بسته‌ها به صورت Load Balance Road Robin ارسال می‌شوند و لذا تمام آن مسیرها وارد Routing Table می‌شوند.

هدف تمام Routing Protocol های مختلف، ساخت و نگهداری و به روز رسانی جدول Routing Table به صورت dynamic است.

Dynamic Routing Protocol

IGP: بین مسیریاب‌های درون یک AS کار می‌کنند.

EGP: بین مسیریاب‌های، بین AS ها کار می‌کنند.

Autonomous System (AS)

به گروهی از شبکه‌ها و مسیریاب‌ها اطلاق می‌شود که تحت مدیریت و کنترل یک سازمان یا نهاد واحد قرار دارند و از یک استراتژی مسیریابی یکسان استفاده می‌کنند. هر AS یک شناسه منحصر به فرد دارد که به آن AS Number (ASN)گفته می‌شود AS ها برای مدیریت مسیریابی اینترنت در سطح گسترده استفاده می‌شوند و به طور کلی به دو دسته تقسیم می‌شوند. AS های عمومی و خصوصی.

کاربردهای اصلیAS

- کنترل ترافیک ورودی و خروجی

ASها به یک سازمان اجازه می‌دهند تا کنترل دقیقی روی مسیرهایی که ترافیک از آن‌ها عبور می‌کند داشته باشند. برای مثال، یک شرکت ممکن است دو اتصال به اینترنت داشته باشد و بخواهد کنترل کند که ترافیک از کدام مسیر وارد یا خارج شود.

- مسیریابی در سطح اینترنت

ASها در مسیریابی اینترنتی با استفاده از پروتکل‌هایی مثل BGP (Border Gateway Protocol) (تنها پروتکل مسیریابی پویا از دسته EGP) نقش مهمی ایفا می‌کنند. هر AS می‌تواند تصمیم بگیرد که چه مسیرهایی را بهAS های دیگر تبلیغ کند و چه مسیرهایی را ازAS های دیگر بپذیرد.

ساختار و عملکردAS

هر AS معمولاً شامل چندین مسیریاب و شبکه است که همگی از یک استراتژی مسیریابی یکپارچه پیروی می‌کنند. این استراتژی‌ها می‌توانند بر اساس سیاست‌های مسیریابی سازمان تعیین شوند. به عنوان مثال، یک ISP ممکن است چندین شبکه و مسیریاب را تحت یک AS مدیریت کند و از BGP برای تبادل اطلاعات مسیریابی باAS های دیگر استفاده کند.

انواعAutonomous System

- Single-homed AS

این نوع AS تنها به یک AS دیگر متصل است و از یک اتصال برای دسترسی به اینترنت استفاده می‌کند. معمولاً سازمان‌های کوچک از این نوع ساختار استفاده می‌کنند.

- Multi-homed AS

این نوع AS به بیش از یک AS دیگر متصل است و از چندین اتصال برای دسترسی به اینترنت یا سایر شبکه‌ها استفاده می‌کند. این نوع ساختار باعث بهبود افزونگی و دسترسی‌پذیری می‌شود.

- Transit AS

این نوع AS ترافیک را بین دو یا چند AS دیگر منتقل می‌کند. یک Transit AS معمولاً نقش یک واسط را در مسیریابی اینترنتی ایفا می‌کند.

Autonomous System (ASN) Number

هر AS یک شماره منحصر به فرد دارد که توسط سازمان‌هایی مانند IANA (Internet Assigned Numbers Authority)یا RIR (Regional Internet Registry) تخصیص داده می‌شود. این شماره‌ها به دو دسته تقسیم می‌شوند:

- Public ASN برایAS هایی که به صورت عمومی به اینترنت متصل هستند و با سایرAS ها ارتباط برقرار می‌کنند.
- Private ASN برای استفاده داخلی در سازمان‌ها که نیاز به ارتباط مستقیم با اینترنت عمومی ندارند.

پروتکل‌های مسیریابی درAS

مسیریابی درون یک AS (Intra-AS Routing) و مسیریابی بینAS ها (Inter-AS Routing) با استفاده از پروتکل‌های مختلف انجام می‌شود

- Intra-AS Routing از پروتکل‌هاییماندOSPF ، EIGRP، یا RIP استفاده می‌شود.
- Inter-AS Routing از BGP برای تبادل اطلاعات مسیریابی بینAS ها استفاده می‌شود.

اهمیت AS در اینترنت

اینترنت مجموعه‌ای از هزاران AS است که با هم در تعامل هستند و با استفاده ازBGP ، اطلاعات مسیرها را تبادل می‌کنند. هر AS به عنوان یک واحد مستقل تصمیم‌گیری عمل می‌کند و سیاست‌های خود را برای مسیریابی پیاده‌سازی می‌کند. این استقلال به هر AS اجازه می‌دهد تا بهینه‌سازی‌های خاص خود را انجام دهد، مثلاً اولویت‌بندی مسیرها یا محدود کردن دسترسی به مسیرهای خاص.

چالش‌ها و مدیریت AS

- سیاست‌های مسیریابی پیچیده

هر AS ممکن است سیاست‌های خاص خود را داشته باشد که مدیریت و هماهنگی بینAS ها را پیچیده می‌کند.

- مقیاس‌پذیری

با افزایش تعدادAS ها و مسیرهای مرتبط با آن‌ها، مدیریت اطلاعات مسیریابی چالش‌برانگیزتر می‌شود.

- امنیت

اشتباه در تنظیمات BGP می‌تواند منجر به حملاتی مانند BGP Hijacking شود که می‌تواند ترافیک را به مسیرهای نادرست هدایت کند.

Interior Gateway Protocol (IGP)

- Distance Vector
  - Routing Information Protocol (RIP)
  - Interior Gateway Routing Protocol (IGRP)
- Link State
  - Open Shortest Path First (OSPF)
  - ISIS
- Balanced Hybrid
  - Enhanced Interior Gateway Routing Protocol

خواص کلی Distance Vectors

- از الگوریتم‌های مسیریابی Bellman Ford استفاده می‌کنند.
- **معمولاً** در آپدیت‌های خود subnet mask حمل نمی‌کنند (**معمولاً** class full هستند)
- دارای convergence های کندی هستند.
- از incremental update پشتیبانی نمی‌کنند و فقط full update هستند.
- نسبت به توپولوژی شبکه دید ندارند و فقط با همسایگان خود کار می‌کنند. (بر اساس شایعه کار می‌کنند)
- مستعد Loop هستند.

خواص کلی Link States

- براساس الگوریتم مسیریابی Dijkstra کار می‌کنند
- در آپدیت‌های خود subnet mask حمل می‌کنند.
- دارای convergence های سریع با مقدار عددی کم هستند
- از incremental update پشتیبانی کرده و فقط تغییرات را ارسال می‌کنند.
- نسبت به Topology Information شبکه دید دارند و بهترین مسیر را انتخاب می‌کنند
- آن‌ها Loop Free هستند

خواص کلی Balanced Hybrid

انحصاری شرکت cisco است. شامل مزایای Distance vector و Link state است (تنها مزیت DV، آن است که load کمی برای پروسس دارند). برای الگوریتم مسیریابی نیز از Diffusing Update Algorithm (DUAL) استفاده می‌کنند.

Routing Information Protocol (RIP)

به عنوان یک پروتکل مسیریابی استاندارد شناخته می‌شود. دارای ورژن‌های مختلفی است.

- RIP v1
  - در دهه ۱۹۸۰ معرفی شد.
  - از مسیریاب‌ها و پروتکل‌های مبتنی بر کلاس (classful) پشتیبانی می‌کند.
  - از Subnet پشتیبانی نمی‌کند، بنابراین برای شبکه‌هایی که نیاز به VLSM دارند، مناسب نیست.
  - آپدیت با پیام Broadcast ارسال می‌شود.
- RIP v2
  - در سال ۱۹۹۳ معرفی شد.
  - از مسیریاب‌ها و پروتکل‌های بدون کلاس (classless) پشتیبانی می‌کند.
  - از VLSM و CIDR (Classless Inter-Domain Routing) پشتیبانی می‌کند.
  - شامل Authentication برای افزایش امنیت است.
  - اطلاعات اضافی مانند Next Hop را در پیام‌های ارسالی فراهم می‌کند.
  - آپدیت با پیام Multicast ارسال می‌شود. آدرس multicast: 224.0.0.9

همچنین، نسخه‌ای از RIP به نام RIPng (RIP Next Generation) وجود دارد که برای پشتیبانی از پروتکل IPv6 طراحی شده است.

در این پروتکل، آپدیت‌ها به صورت دوره‌ایی و هر ۳۰ ثانیه منتقل می‌شود. به صورت پیش فرض، تا ۴ مسیر به مقصد یکسان با متریک مساوی، یک مسیر را وارد routing table می‌کند و بین آن‌ها Load Balance RR می‌کند، تعداد ۴ را می‌توان به ۶ افزایش داد. مسیرهایی که از طریق این پروتکل آموخته می‌شود در جدول به صورت ® نشان داده می‌شود. AND =120

در RIP، Auto Summarization به صورت پیش فرض فعال است و RIP v2 باید این قابلیت را غیر فعال کنیم (چرا؟) پارامتر محاسبه متریک RIP، Hop count است (تعداد مسیریاب‌ها را شمارش می‌کند) اگر مسیری دارای متریک ۱۶ باشد پذیرفته نمی‌شود.

فرض کنید سناریو زیر را داریم

مسیریاب R1 دارای دو شبکه داخلی 24/ 10.0.0.0 , 24/ 192.168.1.0 است.

مسیریاب R2 دارای دو شبکه داخلی 24/ 172.16.0.0 , 24/ 192.168.2.0 است.

مسیریاب R3 دارای دو شبکه داخلی 24/ 192.168.4.0 , 24/ 192.168.3.0 است.

مراحل پیکربندی RIP

ابتدا آدرس IP مناسب برای هر اینترفیس مسیریاب‌ها اختصاص می‌دهیم.سپس RIP نسخه ۲ را فعال کرده و شبکه‌ها را معرفی می‌کنیم.

R1:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.1.0
Router(config-router)# network 10.0.0.0
Router(config-router)# no auto-summary
```

R2:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.2.0
Router(config-router)# network 172.16.0.0
Router(config-router)# no auto-summary
```

R3:

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network 192.168.3.0
Router(config-router)# network 192.168.4.0
Router(config-router)# no auto-summary
```

پیکربندی RIP V1

- دستورات اصلی

Router(config)# router rip

Router(config-router)# version 1

مشخص کننده نسخه RIP

Router(config-router)# network <network-address>

مشخص کردن شبکه‌هایی که باید توسط RIP اعلام شوند

- دستورات اختیاری

Router(config-router)# passive-interface <interface>

از ارسال آپدیت‌های RIP از طریق یک اینترفیس خاص جلوگیری می‌کند.

Router(config-router)# timers basic <update-interval> <invalid> <holddown> <flush>

تنظیم تایمرهای آپدیت، نامعتبر شدن، هولد داون، و پاکسازی مسیرها.

Router(config-router)# default-information originate

اعلان مسیر پیش‌فرض (۰.۰.۰.۰) به دیگر مسیریاب‌ها

Router(config-router)# distance <distance>

تنظیم مقدار Administrative Distance

Router(config-router)# redistribute <protocol>

مسیریابی مجدد از دیگر پروتکل‌های مسیریابی

Router(config-router)# no validate-update-source

جلوگیری از بررسی منبع آپدیت‌ها

Router(config-router)# offset-list <access-list-number> <in|out> <offset> <interface>

اضافه کردن یک مقدار ثابت به metric آپدیت‌ها

پیکربندی RIP V2

- دستورات اصلی

```
Router(config)# router rip
Router(config-router)# version 2
Router(config-router)# network <network-address>
Router(config-router)# no auto-summary
```

- دستورات اختیاری

```
Router(config-router)# passive-interface <interface>
Router(config-router)# timers basic <update-interval> <invalid> <holddown> <flush>
Router(config-router)# default-information originate
Router(config-router)# distance <distance>
Router(config-router)# redistribute <protocol>
Router(config-router)# no validate-update-source
Router(config-router)# offset-list <access-list-number> <in|out> <offset> <interface>
Router(config-router)# ip rip authentication mode <text|md5>
```

فعال کردن مکانیزم احراز هویت برایRIP v2

```
Router(config-router)# ip rip authentication key-chain <key-chain-name>
```

تعیین کلید احراز هویت برایRIP v2

Loop Avoidance

پروتکل RIP از چندین مکانیزم برای جلوگیری از ایجاد حلقه‌های مسیریابی (routing loops) استفاده می‌کند. در ادامه مکانیزم‌های مختلف آن را بررسی می‌کنیم.

- محدودیت هاپ(Hop Count Limit)

پروتکل RIP از metric به نام hop count برای ارزیابی فاصله تا مقصد استفاده می‌کند.حداکثر مقدار hop countدر RIP برابر با ۱۵ است. اگر یک مسیر با hop count بیشتر از ۱۵ باشد، آن مسیر به عنوان غیرقابل دسترس (unreachable) در نظر گرفته می‌شود. این محدودیت باعث می‌شود که مسیرهای بسیار طولانی و پیچیده که احتمال ایجاد loop در آن‌ها زیاد است، مسدود شوند.

- Split Horizon

یکی از تکنیک‌های قدیمی و مؤثر برای جلوگیری از ایجاد حلقه‌های مسیریابی است.در این مکانیزم، مسیریاب از ارسال اطلاعات درباره مسیری که از یک اینترفیس یاد گرفته شده به همان اینترفیس جلوگیری می‌کند. (مسیری که از خودم یاد گرفتی برای خودم تبلیغ نکن)

- Split Horizon with Poison Reverse

Poison Reverse نسخه پیشرفته‌تر Split Horizon است.

در این تکنیک، مسیریاب به جای اینکه به‌سادگی اطلاعات مسیر را به سمت منبع ارسال نکند، به صورت فعال آن مسیر را با یک hop count برابر با ۱۶ به معنی unreachable به سمت منبع ارسال می‌کند. این کار به همه مسیریاب‌ها اطلاع می‌دهد که آن مسیر غیرقابل دسترس است و به جلوگیری از حلقه کمک می‌کند.

- Hold-Down Timer

مکانیزمی است که زمانی که مسیریاب یک مسیر را غیرقابل دسترس تشخیص می‌دهد، تا مدتی از قبول تغییرات جدید درباره آن مسیر خودداری می‌کند. این مدت زمان به مسیریاب‌ها اجازه می‌دهد تا آپدیت‌های نادرست را فیلتر کنند و به جلوگیری از حلقه‌های موقت کمک می‌کند. مقدار پیش‌فرض این تایمر در RIP معمولاً ۱۸۰ ثانیه است.

- Triggered Updates

به این معنی است که آپدیت‌های مسیریابی به صورت فوری پس از تشخیص تغییرات مهم (مثل قطع یک لینک) ارسال می‌شوند، نه اینکه منتظر چرخه آپدیت دوره‌ای 30 ثانیه‌ایی در RIP بمانند. این مکانیزم به کاهش زمان لازم برای آگاهی مسیریاب‌ها از تغییرات و جلوگیری از ایجاد حلقه‌ها کمک می‌کند.

- Route Poisoning

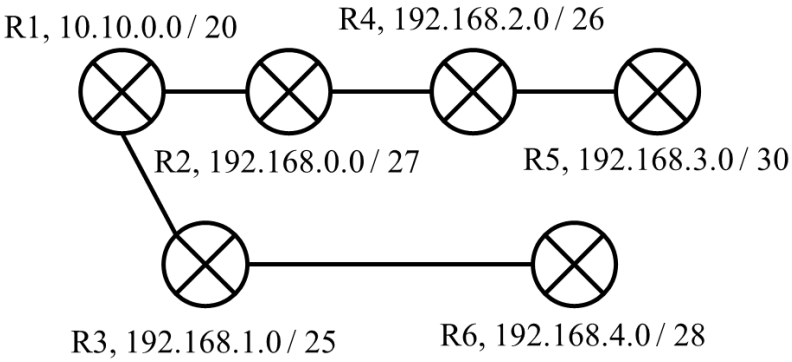
شبیه Poison Reverse است، اما به صورت کلی‌تر عمل می‌کند. وقتی یک مسیر غیرقابل دسترس می‌شود، مسیریاب آن مسیر را با metric برابر ۱۶ به همه همسایگان اعلام می‌کند تا آن‌ها بدانند که مسیر از دسترس خارج شده است.

- Garbage Collection Timer (Flush Timer)

زمانی که یک مسیر غیرقابل دسترس شناسایی می‌شود، مسیریاب تا مدتی آن مسیر را در جدول مسیریابی نگه می‌دارد اما آن را با metric برابر ۱۶ علامت‌گذاری می‌کند.این تایمر به دیگر مسیریاب‌ها فرصت می‌دهد تا آپدیت‌ها را دریافت کرده و جدول‌های خود را به‌روزرسانی کنند. پس از اتمام تایمر (که معمولاً ۲۴۰ ثانیه است)، مسیر به‌طور کامل از جدول مسیریابی حذف می‌شود.

سوالات و تمرینات

شکل زیر در نظر بگیرید. مسیریابی آن را به روش RIP انجام دهید.



آزمایش ۱۴

اهداف: آشنایی با پروتکل مسیریابی OSPF

سناریو ۱۴: می‌خواهیم بین چندین شبکه LAN با کمک مسیریاب‌ها، عمل مسیریابی را به روش OSPF انجام دهیم.

اجزای مورد نیاز:

- Router
- سایر تجهیزات مرتبط برای پیاده‌سازی شبکه LAN

در آزمایش‌های گذشته با مفهوم مسیریابی، انواع آن و پروتکل‌های مسیریابی پویا آشنا شدیم. در این آزمایش قصد داریم تا با پروتکل مسیریابی OSPF آشنا شویم.

Open Shortest Path First (OSPF)

- در دهه ۱۹۸۰ میلادی معرفی شد. اولین نسخه آن در سال ۱۹۸۹ توسط IETF (Internet Engineering Task Force) به عنوان یک پروتکل مسیریابی داخلی استاندارد منتشر شد.
  - OSPFv1: اولین نسخه از OSPF بود که در اواخر دهه ۱۹۸۰ توسعه یافت. این نسخه به دلیل محدودیت‌ها و مشکلات عملکردی به سرعت جای خود را به نسخه بعدی داد و امروزه دیگر استفاده نمی‌شود.
  - OSPFv2: این نسخه در RFC 2328 تعریف شده و همچنان برای مسیریابی در شبکه‌های IPv4 مورد استفاده قرار می‌گیرد. OSPFv2 از ویژگی‌های بهبود یافته‌ای نسبت به نسخه اول برخوردار است و امروزه به عنوان نسخه استاندارد OSPF برای شبکه‌های IPv4 کاربرد دارد.

- OSPFv3: این نسخه در RFC 5340 تعریف شده و برای مسیریابی در شبکه‌های IPv6 توسعه یافته است. OSPFv3 با توجه به تغییرات معماری در IPv6 نسبت به IPv4، ویژگی‌ها و ساختار جدیدی دارد. علاوه بر IPv6، OSPFv3 قابلیت پشتیبانی از IPv4 را نیز دارد.

- AND= 110، مسیرهایی که با OSPF آموخته می‌شوند را با حرف (O) نمایش می‌دهند.
- در حدود ۹۵٪ از OSPF به عنوان IGP استفاده می‌کنند.
- زمان Convergence بسیار سریعی دارد و با کوچکترین تغییرات همه مسیریاب‌ها به سرعت مطلع می‌شوند.
- نسبت به Topology Information شبکه به صورت جزئی اطلاع و دید کامل دارد.
- از Incremental update پشتیبانی می‌کنند. (یک link state است و تمام خواص آن را به ارث برده است)
- و به عنوان تنها IGP است که unlimited hop را پشتیبانی می‌کند.
- پارامتر متریک آن cost است که به صورت زیر محاسبه می‌شود.

$$Cost = \frac{Reference\ Bandwidth}{Interface\ Bandwidth}$$

- Reference Bandwidth: یک مقدار مرجع برای پهنای باند که در تنظیمات OSPF تعریف می‌شود. مقدار پیش‌فرض آن در بسیاری از سیستم‌ها ۱۰۰ مگابیت بر ثانیه (Mbps) است، اما می‌تواند بر اساس نیاز تغییر کند.
- Interface Bandwidth: پهنای باند واقعی رابط (Interface) شبکه که می‌تواند بر اساس نوع لینک (مانند ۱۰ Mbps، ۱۰۰ Mbps، ۱ Gbps و غیره) تنظیم شود.

مثال: اگر یک لینک با پهنای باند ۱۰۰۰ Mbps (1 Gbps) داشته باشید و مقدار مرجع پهنای باند 100 Mbps (Reference Bandwidth) باشد، هزینه‌ی این لینک به صورت زیر محاسبه می‌شود:

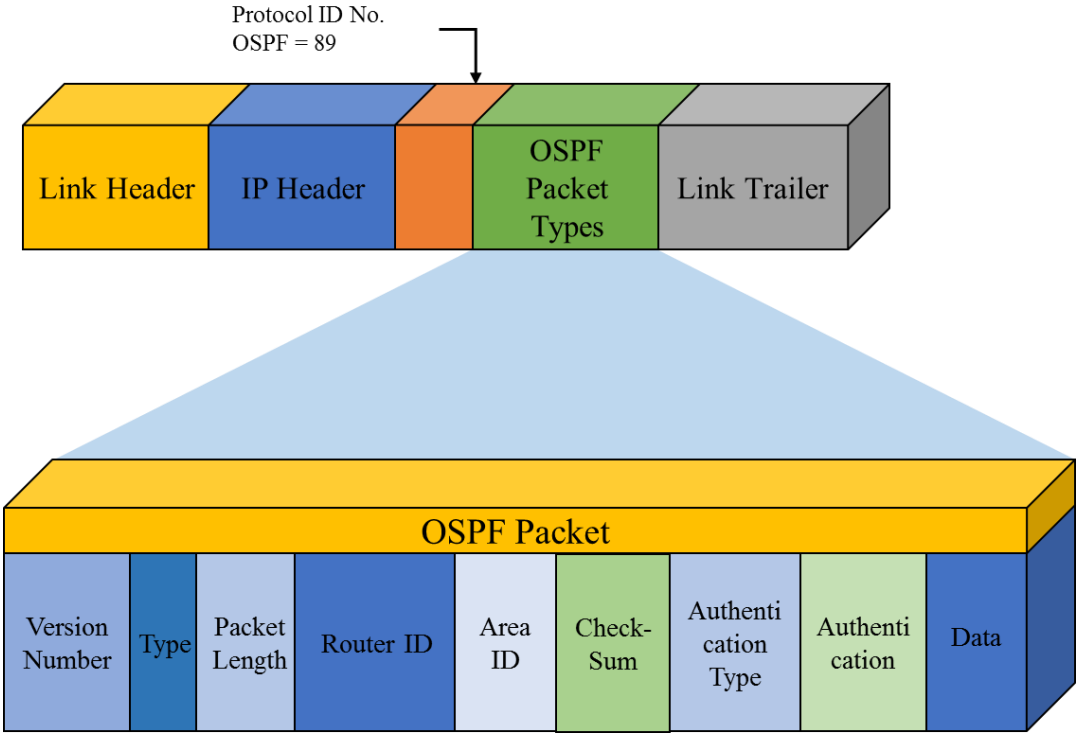
$$Cost = \frac{Reference\ Bandwidth}{Interface\ Bandwidth} = \frac{100}{1000} = 0.1$$

در OSPF، هزینه‌ها به عدد صحیح تبدیل می‌شوند، بنابراین هزینه این لینک در واقع برابر با ۱ خواهد بود (با گرد کردن به عدد صحیح).

- تنها پروتکل مسیریابی است که در آن Auto Summarization به صورت پیش فرض غیر فعال است
- این پروتکل Loop free است.

نحوه عملکرد OSPF

هنگامی که OSPF اجرا می‌شود، بر روی لینک‌های LAN هر ۱۰ ثانیه و بر روی لینک‌های WAN هر ۳۰ ثانیه برای همسایگان خود بسته‌های Hello Packet ارسال می‌کند. ساختار بسته OSPF را در شکل ۱۴-۱ مشاهده می‌کنید.



شکل ۱۴-۱ ساختار بسته OSPF

به بازه‌های ارسال بسته Hello Packet، Hello interwall گویند. از سوی دیگر Dead interwall چهار برابر Hello interwall است (بر روی لینک‌های LAN، ۴۰ ثانیه، بر روی لینک‌های WNA، ۱۲۰ ثانیه). از طریق مبادله بسته Hello Packet، هر مسیریاب، یک جدول از لیست همسایگان خود ایجاد می‌کند، که به این جدول Neighbor Table گویند و برای هر مسیریاب منحصر به فرد است.

بعد از تکمیل شدن Neighbor Table مسیریاب بسته‌هایی به نام Link State Advertisement (LSA) را با همسایگان و غیر همسایگان خود مبادله می‌کند.

پروتکل OSPF، با آدرس‌های multicast، 224.0.0.5 و 224.0.0.6 کار می‌کند.

بسته‌های LSA در واقع همان مسیرها و شبکه‌هایی هستند که هر مسیریاب در اختیار دارد و بیان دیگر همان بسته‌های update می‌باشند. و برای آن که Topology Information شبکه ایجاد شود این بسته‌ها برای کلیه مسیریاب‌ها ارسال می‌شود و لذا بعد از تبادل LSA Packet هر مسیریاب، Topology Table را ایجاد می‌کند. تا اینجای کار، هنوز هیچ مسیری وارد Routing Table نشده است.

بعد از تکمیل Topology Information هر مسیریاب با اعمال الگوریتم مسیریابی Shortest Path First (SPF) بر روی جدول Topology Information، بهترین مسیر را برای رفتن به مقاصد مختلف پیدا کرده و آن را در جدول Routing Table قرار می‌دهد.

در ادبیات OSPF، لازم است بتوانیم مسیریاب‌ها را خطاب قرار دهیم. این خطاب قرار دادن را برای جدول Neighbor Table نیاز داریم، بنابراین باید پارامتری به عنوان Router ID داشته باشیم که منحصر به فرد باشد تا OSPF از طریق آن مسیریاب‌ها را خطاب کند. در شبکه‌های TCP / IP، آدرس IP منحصر به فرد است و هم آدرس IP و OSPF هر دو در لایه سوم کار می‌کنند، پس آدرس IP می‌تواند به عنوان Router ID استفاده شود. به صورت پیش فرض بالاترین آدرس IP، اینترفیس فیزیکی مسیریاب به عنوان Router ID انتخاب می‌شود.

نکته: اگر اینترفیسی که ادمین شبکه به عنوان Router ID انتخاب کرده است، Down شود، مجدد باید تمام مراحل از ابتدا انجام شوند تا مسیریاب‌ها مجدد با یکدیگر همسایه شودند.

با توجه به نکته بیان شده، اینترفیس فیزیکی گزینه مناسبی برای Router ID نیست، به اینترفیسی نیاز داریم تا شرایط فیزیکی بر آن تأثیر نداشته باشد. حال اگر یک مسیریاب دارای Loop Back باشد، آدرس IP آن به عنوان Router ID انتخاب می‌شود حتی در صورتی که آدرس IP آن کمتر باشد. در شرایطی که دارای چندین Loop Back باشیم، آدرس IP بالاتر به عنوان Router ID انتخاب می‌شود.

نکته: اینترفیس مجازی بر روی دستگاه را Loop Back گویند. اینترفیس مجازی به صورت پیش فرض Up-Up و لایه سومی هستند.

R1 (config) # int loopback <number>
R1 (config-if) # ip address <ip address> <subnet mask>

از آنجا که این اینترفیس وابسته به سخت‌افزار نیست، نیازی به دستور no shutdown ندارد . به صورت پیش فرض up-up است.

نکته: بسته‌های LSA در صورتی ارسال می‌شوند که لینکی Up یا Down شود، که این امر نشانه Incremental Update بودن OSPF است.

در پروتکلOSPF ، دو مسیریاب زمانی Adjacent (همجوار) می‌شوند که بین آن‌ها یک رابطه همسایگی قوی و قابل اطمینان شکل گرفته باشد و این رابطه به مرحله‌ای رسیده باشد که مسیریاب‌ها بتوانند اطلاعات کامل مسیریابی (Link-State Database) را با یکدیگر تبادل کنند.

مراحل تشکیل همجواری (Adjacency)

پروتکل OSPF دارای چندین مرحله (state) برای برقراری ارتباط بین دو مسیریاب است. این مراحل به ترتیب عبارتند از

- Down State در این مرحله، مسیریاب هنوز هیچ بسته Hello از همسایه خود دریافت نکرده است.

- Init State مسیریاب بسته Hello از همسایه دریافت کرده ولی همسایه هنوز به آن پاسخ نداده است. در این مرحله، یک‌طرفه (one-way) است.
- Two-Way State زمانی که هر دو مسیریاب بسته Hello یکدیگر را دریافت و پردازش کرده‌اند و در لیست Neighbor یکدیگر قرار گرفته‌اند. در این مرحله، ارتباط به دوطرفه (two-way) تبدیل شده است. در این مرحله، مسیریاب‌ها بررسی می‌کنند که آیا باید Adjacency بین آنها برقرار شود یا خیر.
- ExStart State در این مرحله، اگر لازم باشد که دو مسیریاب Adjacency برقرار کنند) برای تبادل (Link-State Database، فرایند تبادل اطلاعات مسیریابی آغاز می‌شود. یکی از مسیریاب‌ها به عنوان Masterو دیگری به عنوان Slave انتخاب می‌شود.
- Exchange State مسیریاب‌ها اطلاعات اولیه Link-State خود را با هم مبادله می‌کنند.
- Loading State در این مرحله، مسیریاب‌ها هرگونه اطلاعات ناقص یا جدید را با یکدیگر تبادل می‌کنند.
- Full State این مرحله نهایی است که در آن مسیریاب‌ها به طور کامل Adjacency برقرار کرده‌اند و پایگاه داده‌ی Link-State خود را به طور کامل همگام کرده‌اند. این مرحله نشان‌دهنده‌ی برقراری کامل ارتباط و آماده بودن برای مسیریابی است.

برای جلوگیری از Adjacency زیاد بهتر است که به جای آن که مسیریاب‌ها دو به دو با هم Adjacent شوند، همه با یکی Adjacent شوند. مسیریابی که دیگر مسیریاب‌ها با آن Adjacent می‌شوند را Designated Router (DR) می‌گویند و برای آن که اگر مشکلی برای DR اتفاق افتاد شبکه دچار مشکل نشود یک Back up Designated Router (BDR) هم انتخاب می‌کنند.

آدرس تمام DR ها، 224.0.0.6 است، حق دسترسی به این بسته‌ها را تنها DR و BDR دارند.

آدرس تمام مسیریاب‌های OSPF، 224.0.0.5 است، همه مسیریاب‌ها حق دسترسی به این بسته را دارند.

بر روی لینک‌های Multi Access، مسیریاب‌های DR و BDR انتخاب می‌شوند.

مکانیزم انتخاب DR

مسریابی که Router ID آن از همه بالاتر باشد به عنوان DR انتخاب می‌شود، اما این فرآیند انتخاب یک مشکل دارد، چرا که مسیریابی که بالاترین Router ID را دارد، لزوماً کاراترین مسیریاب در شبکه نیست و چون همه Adjacent ها باید با این مسیریاب انجام شود باید مسیریابی به عنوان DR انتخاب شود که بالاترین Performance را در شبکه داشته باشد.

- پارامترهای کلیدی در انتخاب DR وBDR

Router Priority این پارامتر در هر مسیریاب OSPF قابل تنظیم است و مقدار پیش‌فرض آن ۱ است. اگر این مقدار ۰ تنظیم شود، مسیریاب در فرایند انتخاب DR و BDR شرکت نمی‌کند.

Router ID هر مسیریاب دارای یک شناسه منحصر به فرد است که برای شناسایی مسیریاب استفاده می‌شود. این شناسه معمولاً به صورت یک آدرس IP است.

- روند انتخاب

مرحله اول: ابتدا مسیریاب‌ها بسته‌های Hello را دریافت می‌کنند و اطلاعات موجود در آنها را تجزیه و تحلیل می‌کنند.

مرحله دوم: مسیریاب‌ها بررسی می‌کنند که آیا DR و BDR فعلی وجود دارند یا خیر. اگر DR و BDRفعلی وجود داشته باشند، مسیریاب‌های جدید به همان DR و BDR متصل می‌شوند.

مرحله سوم: اگر DR و BDR موجود نباشند (یا تازه فرایند انتخاب شروع شده باشد)، مسیریاب‌ها به ترتیب زیر عمل می‌کنند:

ابتدا مسیریاب با بالاترین Priority به عنوان DR انتخاب می‌شود.

سپس، مسیریاب با دومین Priority بالاتر به عنوان BDR انتخاب می‌شود.

اگر Priority یکسان باشد، Router ID به عنوان معیار بعدی برای انتخاب استفاده می‌شود؛ یعنی مسیریاب با بالاترین Router ID به عنوان DR و سپس مسیریاب با دومین Router ID به عنوان BDR انتخاب می‌شود.

- نحوه تغییر DR وBDR

اگر DR فعلی از کار بیفتد یا از شبکه خارج شود، BDRبه صورت خودکار به عنوان DR جدید انتخاب می‌شود و یک BDR جدید بر اساس مکانیزم فوق تعیین می‌شود. مسیریاب‌های DR و BDR جدید فقط در صورت تغییر وضعیت انتخاب می‌شوند و در شرایط عادی مسیریاب‌ها تغییر نمی‌کنند تا از نوسانات شبکه جلوگیری شود.

نکته: همیشه اولویت با مقدار Priority است. اگر یک مسیریاب با Priority بالاتر وارد شبکه شود، به عنوان DR جدید انتخاب می‌شود. مسیریاب‌های DRو BDR تا زمانی که از کار نیفتند، ثابت باقی می‌مانند تا از ایجاد نوسانات جلوگیری شود. این مکانیزم باعث می‌شود که OSPF بتواند در شبکه‌های بزرگ با ترافیک سنگین به خوبی عمل کرده و از ایجاد پیچیدگی‌های اضافی جلوگیری کند.

نکته: هر Multi Access Segment یک DR و BDR احتیاج دارد. سیسکو پیشنهاد می‌دهد، اگر مسیریابی در یک Segment، نقش DR یا BDR دارد، در Segment بعدی به عنوان DR و یا BDR انتخاب نشود. (مقدار Priority آن‌ها در Segment دیگر را صفر قرار می‌دهیم)

در پروتکلOSPF، تقسیم یک Autonomous System (AS) به چندین Area به منظور بهینه‌سازی مقیاس‌پذیری و مدیریت پیچیدگی شبکه انجام می‌شود. این بخش‌بندی به بهبود عملکرد و کاهش بار پردازشی مسیریاب‌ها کمک می‌کنند. در ادامه اصول و نکات مهم Area بندی را توضیح می‌دهیم. توجه داشته باشید که Area بندی یک نسخه از پیش تعیین شده نیست و بر اساس نیازهای پروژه و بنا بر اصول و قواعد انجام می‌شود.

تعریف Area در OSPF

یک Area مجموعه‌ای از مسیریاب‌ها و لینک‌های متصل به آن‌ها است که به عنوان یک گروه منطقی برای کاهش حجم اطلاعات مسیریابی (LSA) در شبکه استفاده می‌شود. از طریق Area بندی حوزه نفوذ Update را در AS کنترل می‌کنیم. پروتکل OSPF به روش Hierarchical Routing عمل می‌کند، جایی که Area 0

یا Backbone Area به عنوان ستون فقرات شبکه در نظر گرفته می‌شود و تمامیArea های دیگر باید به این Backboneمتصل باشند.

انواع Area ها در OSPF

- Backbone Area (Area 0)

این Area مرکزی‌ترین بخش شبکه OSPF است و همه‌یArea های دیگر باید به آن متصل شوند.

تمامی ترافیک بینArea ها از طریق Backbone عبور می‌کند.

- Standard Area (Non-Backbone Area)

به Backbone متصل می‌شوند و دارای مسیریاب‌های داخلی و لینک‌های مختلف هستند.

- Stub Area

یک نوع خاص از Area که اطلاعات مسیریابی خارجی (External Routes) را نمی‌پذیرد Stub Area .فقط مسیر پیش‌فرض (Default Route) را از Backbone دریافت می‌کند. این Area برای محیط‌هایی که ترافیک به طور عمده داخلی است و نیازی به دریافت اطلاعات مسیرهای خارجی ندارند، مناسب است.

- Totally Stubby Area

مشابه Stub Area است، با این تفاوت که حتی اطلاعات مسیریابی سایر Area ها را هم مسدود می‌کند و فقط یک مسیر پیش‌فرض دریافت می‌کند.

- Not-So-Stubby Area (NSSA)

مشابه Stub Area است، اما به مسیریاب‌های موجود در این Area اجازه می‌دهد که مسیرهای خارجی را از منابع دیگر (مثلاً RIP) وارد OSPF کنند.

طراحی سلسله مراتبی (Hierarchical) در OSPF

شبکه باید به شکلی طراحی شود که Area 0 به عنوان ستون فقرات در مرکز قرار گیرد و سایرArea ها به آن متصل باشند (حداقل با یک لینک فیزیکی به Area 0 وصل باشند). تمامی ارتباطات بینArea ها باید از طریق

Area 0 صورت گیرد. اگر Area ها به طور مستقیم به Area 0 متصل نیستند، از Virtual Link استفاده می‌شود تا اتصال منطقی با Area 0 برقرار شود.

انواع مسیریاب‌ها در OSPF بر اساس نقش در Area بندی

- Internal Router مسیریابی که تمام رابط‌های (Interfaces) آن در یک Area خاص قرار دارند.
- Backbone Router مسیریابی که حداقل یک رابط آن در Area 0 قرار دارد.
- Area Border Router (ABR) مسیریابی که بین چندین Area قرار دارد و مسئول تبادل اطلاعات بین آن‌ها است.
- Autonomous System Boundary Router (ASBR) مسیریابی که اطلاعات مسیریابی را از پروتکل‌های مسیریابی خارجی وارد OSPF می‌کند (مثلاً از RIP یا BGP).

نحوه انتخاب و طراحی Area

شبکه را به بخش‌های مجزا تقسیم کنید که هر بخش دارای کاربرد یا موقعیت جغرافیایی خاصی است. هر بخش را به عنوان یک Area مجزا در نظر بگیرید.

سعی کنید تعداد مسیریاب‌ها و لینک‌های داخل هر Area را محدود نگه دارید تا پیچیدگی و حجم اطلاعات مسیریابی کم شود. به طور کلی، توصیه می‌شود که هر Area بیش از ۵۰ مسیریاب نداشته باشد.

اگر یک بخش از شبکه دچار تغییرات مکرر می‌شود، آن را به یک Area جداگانه تبدیل کنید تا سایر بخش‌های شبکه تحت تأثیر قرار نگیرند.

مدیریت LSA ها

با تقسیم شبکه به Area ها، LSA ها درون یک Area محدود می‌شوند و باعث کاهش ترافیک OSPF و بار پردازشی مسیریاب‌ها می‌شوند. مسیریاب‌های ABR مسئول خلاصه‌سازی (Summarization) مسیرها هستند و می‌توانند اطلاعات مسیریابی بین Area ها را به شکل بهینه‌تر منتقل کنند.

مزایای استفاده از Area بندی در OSPF

- کاهش حجم اطلاعات مسیریابی: با محدود کردن LSA ها به‌Area ها، ترافیک مسیریابی در سراسر شبکه کاهش می‌یابد.
- بهبود مقیاس‌پذیری: تقسیم شبکه به Area های کوچکتر باعث می‌شود که OSPF بتواند در شبکه‌های بزرگ‌تر و پیچیده‌تر به خوبی عمل کند.
- کنترل و مدیریت بهتر: به مدیران شبکه این امکان را می‌دهد که بخش‌های مختلف شبکه را به صورت مستقل مدیریت کنند.

نکته: در ادامه به چند پیشنهاد سیسکو در طراحی Area خواهیم پرداخت.

- یک مسیریاب ABR در بیش از سه Area نباشد.
- مسیریاب ABR، DR یا BDR نباشد.
- در متن اشاره شد که بیش از ۵۰ مسیریاب در یک Area نباشد، پیشنهاد سیسکو ۶۰ است، اما تجربه مدیران شبکه عدد ۴۵ را پیشنهاد می‌دهند.

پیکربندی OSPF

فرض کنید سه مسیریاب داریم: R1، R2 و R3. این مسیریاب‌ها در دو Area مختلف (Area 0 و Area 1) قرار دارند. R1 و R2 در Area 0 (Backbone Area) و R3 در Area 1 قرار دارد. ما قصد داریم OSPF را برای این سناریو پیکربندی کنیم.

```
R1(config)# router ospf 1
```

این دستور فرآیند OSPF را فعال می‌کند و به آن یک شناسه (Process ID) می‌دهد. در این مثال، عدد ۱ به عنوان Process ID انتخاب شده است. این شناسه در یک مسیریاب خاص محلی است و بین مسیریاب‌ها یکسان بودن آن ضروری نیست.

```
R1(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

این دستور شبکه‌ای که باید تحت OSPF قرار گیرد را مشخص می‌کند. بخش 0.0.0.255 ماسک معکوس (Wildcard Mask) است که مشخص می‌کند کدام بخش از آدرس باید در نظر گرفته شود. عبارت area 0 تعیین می‌کند که این شبکه به کدام Area تعلق دارد.

R1(config-if)# ip ospf priority 100

یک دستور اختیاری، این دستور مقدار اولویت (Priority) یک مسیریاب را برای انتخاب DR/BDR تعیین می‌کند. عدد ۱۰۰ در این مثال بالاترین مقدار است که شانس این مسیریاب برای تبدیل شدن به DR را افزایش می‌دهد.

R1(config-router)# router-id 1.1.1.1

دستور اختیاری، این دستور Router ID را به صورت دستی تنظیم می‌کند. اگر این دستور تنظیم نشود، مسیریاب به صورت خودکار از بالاترین آدرس IP موجود روی اینترفیس‌های فعال استفاده می‌کند.

R1(config-if)# ip ospf hello-interval 10

دستور اختیاری، این دستور مشخص می‌کند که بسته‌های Hello هر ۱۰ ثانیه یکبار ارسال شوند.

R1(config-if)# ip ospf dead-interval 40

دستور اختیاری، این دستور مشخص می‌کند که اگر مسیریاب در مدت ۴۰ ثانیه هیچ بسته Hello از همسایه دریافت نکند، همسایه را غیرقابل دسترس فرض کند.

R1(config-if)# ip ospf cost 10

دستور اختیاری، این دستور مقدار Cost اینترفیس را به صورت دستی تنظیم می‌کند. Cost در OSPF بر اساس پهنای باند تعیین می‌شود و این دستور به شما امکان می‌دهد تا مقدار آن را به صورت دستی تغییر دهید.

R3(config-router)# area 1 stub

دستور اختیاری، این دستور مشخص می‌کند که Area 1 یک Stub Area است. اطلاعات مسیریابی خارجی (External Routes) را از سایر پروتکل‌ها نمی‌پذیرند و به جای آن فقط یک مسیر پیش‌فرض دریافت می‌کنند.

R1(config-if)# ip ospf authentication message-digest

دستور اختیاری، این دستور OSPF را برای استفاده از احراز هویت MD5 تنظیم می‌کند.

R1(config-if)# ip ospf message-digest-key 1 md5 mypassword

دستور اختیاری، این دستور کلید MD5 و رمز عبور را مشخص می‌کند که باید در بین مسیریاب‌های همسایه یکسان باشد.

R2(config-router)# area 1 range 192.168.2.0 255.255.255.0

دستور اختیاری، این دستور در یک ABR استفاده می‌شود و برای خلاصه‌سازی مسیرها به کار می‌رود. این کار باعث کاهش تعدادLSA ها و بهینه‌سازی مسیریابی بینArea ها می‌شود.

R2(config-router)# area 0 virtual-link 2.2.2.2

دستور اختیاری، این دستور یک لینک مجازی ایجاد می‌کند تا Area هایی که به طور مستقیم به Area 0 متصل نیستند، بتوانند از طریق این لینک به Backbone متصل شوند. آدرس 2.2.2.2 مربوط به Router ID مسیریاب مقصد است.

R3(config-router)# redistribute rip subnets

دستور اختیاری، این دستور مسیرهای پروتکل RIP را به OSPF وارد می‌کند. این کار توسط یک ASBR انجام می‌شود و باعث می‌شود مسیرهای خارجی (External Routes) به OSPF اضافه شوند.

دستوراتی برای مشاهده اطلاعات در خصوص مسیریابی و OSPF

Router# show ip route

این دستور جدول مسیریابی کامل مسیریاب را نمایش می‌دهد. در این جدول، اطلاعاتی درباره‌ی تمامی مسیرها از جمله مسیرهای متصل مستقیم، استاتیک، و همچنین مسیرهای یادگیری شده از پروتکل‌های مسیریابی دینامیک (مانند OSPF) وجود دارد.

Router# show ip ospf database

این دستور پایگاه داده OSPF را نمایش می‌دهد که شامل تمامیLSA های (Link-State Advertisements) دریافت‌شده و تولیدشده توسط مسیریاب است. اطلاعات در این دستور به شما کمک می‌کند تا وضعیت لینک‌ها و توپولوژی شبکه را بررسی کنید.

Router# show ip ospf neighbor

این دستور لیست همسایه‌های OSPF را نمایش می‌دهد. اطلاعاتی که در این خروجی مشاهده می‌شود شامل Router ID همسایه‌ها، وضعیت ارتباط (State)، آدرسIP و مدت زمان‌های مرتبط با بسته‌های Hello و Dead است.ستون State نشان می‌دهد که مسیریاب‌ها در چه مرحله‌ای از ارتباط (مثل 2-Way یا Full) هستند.

Router# show ip ospf interface

این دستور اطلاعات کاملی از تمامی اینترفیس‌های فعال در OSPF ارائه می‌دهد. این اطلاعات شامل آدرسIP، Area، مقدارCost ، Hello Interval، Dead Interval، و نقش اینترفیس (DR/BDR) است. همچنین تعداد همسایگان هر اینترفیس و وضعیت OSPF در آن مشخص می‌شود.

Router# show ip ospf

این دستور وضعیت کلی تنظیمات OSPF را نمایش می‌دهد. اطلاعاتی که این دستور نمایش می‌دهد شامل Process ID، Router ID، تعداد Areaها، و تنظیمات زمانی (Timers) است.

Router# show ip route ospf

این دستور فقط مسیرهای یادگیری‌شده از طریق OSPF را نمایش می‌دهد. این دستور به شما کمک می‌کند که مستقیماً مسیرهای مربوط به OSPF را ببینید و با سایر پروتکل‌ها اشتباه نگیرید.

Router# show ip ospf database router <Router-ID>

این دستور جزئیات مربوط به یک LSA خاص را نمایش می‌دهد. در اینجا، Router ID مسیریاب مورد نظر را جایگزین <Router-ID> کنید. این دستور به شما کمک می‌کند که اطلاعات دقیقی از یک مسیریاب خاص در پایگاه داده OSPF دریافت کنید.

Router# show ip ospf border-routers

این دستور مسیرهای خلاصه‌شده و تبلیغ‌شده توسط مسیریاب‌های مرزی (ABR) را نمایش می‌دهد. این خروجی شامل مسیرهایی است که بین Areaها تبادل می‌شوند.

Router# show ip ospf virtual-links

این دستور اطلاعات مربوط به لینک‌های مجازی در OSPF را نمایش می‌دهد، از جمله وضعیت ارتباط، آدرس‌های مرتبط، و تنظیمات زمانی.

Router# show ip ospf database external

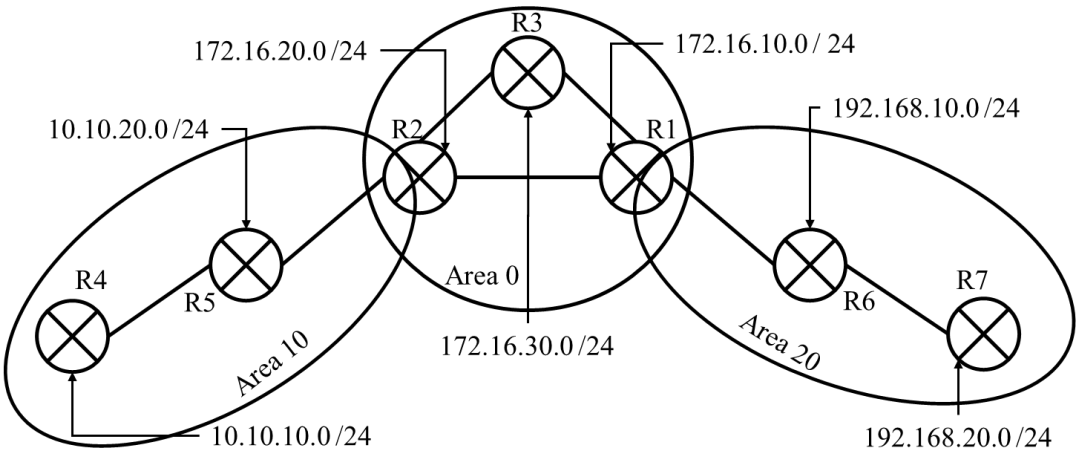
این دستور اطلاعات مربوط به LSA های خارجی که توسط ASBR ها تبلیغ می‌شوند را نمایش می‌دهد. این اطلاعات شامل مسیرهای خارجی مانند آن‌هایی که از پروتکل‌های دیگر مثل RIP یا BGP وارد OSPF شده‌اند است.

Router# show ip ospf redistribute

این دستور وضعیت و تنظیمات مسیرهای توزیع‌شده از پروتکل‌های دیگر به OSPF را نمایش می‌دهد.

سوالات و تمرینات

شکل زیر را در نظر بگیرید، پروتکل مسیریابی OSPF را برای آن اجرا کنید. کلیه دستورات را برای آن پیاده‌سازی کنید.



آزمایش ۱۵

اهداف: آشنایی با Network Address Translation (NAT)

سناریو ۱۵: در یک شبکه با آدرس IP های Private قصد ارتباط با اینترنت و خارج از محدوده آدرس IP های Private را داریم

اجزای مورد نیاز:

- Router
- Switch
- End device

ترجمه آدرس شبکه، در واقع ترجمه آدرس‌های لایه سوم است. یک مکانیزمی است که به طور گسترده در شبکه‌های Private و public برای مدیریت آدرس‌های IP و کاهش مصرف آدرس‌های IP عمومی استفاده می‌شود. این مکانیزم به طور عمده برای تبدیل آدرس‌های IP خصوصی به آدرس‌های IP عمومی و بالعکس استفاده می‌شود.

انواع NAT

- Static NAT

در این نوع ازNAT ، یک آدرس IP خصوصی به یک آدرس IP عمومی خاص و ثابت نگاشت می‌شود. این نوع NAT زمانی استفاده می‌شود که یک دستگاه درون شبکه نیاز به دسترسی دائمی به اینترنت با یک آدرس IP خاص دارد.

- Dynamic NAT

درDynamic NAT ، یک آدرس IP خصوصی به یکی از آدرس‌های IP عمومی موجود از یک رنج اختصاص داده شده نگاشت می‌شود. این روش زمانی مفید است که تعداد آدرس‌های IP عمومی کمتر از تعداد دستگاه‌های داخلی باشد.

- PAT (Port Address Translation) یا Overloading

این نوع NAT پرکاربردترین نوع است. درPAT ، چندین دستگاه با استفاده از یک آدرس IP عمومی و با متمایز کردن اتصالات از طریق شماره‌های پورت متمایز، به اینترنت دسترسی پیدا می‌کنند. این روش بهینه‌سازی مصرف آدرس‌های IP عمومی را به دنبال دارد.

مکانیزم عملکرد NAT

- تبدیل آدرس

وقتی یک بسته داده از دستگاهی در شبکه داخلی به سمت اینترنت می‌رود، مکانیزم NAT آدرس IP خصوصی آن را با آدرس IP عمومی جایگزین می‌کند.

- جدولNAT

یک جدول در مسیریاب ذخیره می‌شود که شامل نگاشت آدرس‌های IP خصوصی به آدرس‌های IP عمومی و شماره‌های پورت مرتبط با آن‌ها است. این جدول برای اطمینان از اینکه بسته‌های بازگشتی به درستی به دستگاه مبدا ارسال شوند، استفاده می‌شود.

- بازگرداندن آدرس

وقتی بسته‌ای از اینترنت به شبکه داخلی بازمی‌گردد، NAT آدرس IP عمومی را با آدرس IP خصوصی نگاشت شده جایگزین کرده و آن را به دستگاه مربوطه ارسال می‌کند.

مزایا و معایب NAT

مزایا

- حفظ آدرس‌های IP عمومی: با استفاده ازNAT ، چندین دستگاه در شبکه داخلی می‌توانند از یک آدرس IP عمومی استفاده کنند.

- افزایش امنیت: به عنوان یک دیواره امنیتی عمل می‌کند، زیرا دستگاه‌های خارجی نمی‌توانند به طور مستقیم به دستگاه‌های داخلی دسترسی پیدا کنند.
- انعطاف‌پذیری: امکان تغییر آدرس‌های IP داخلی بدون نیاز به تغییر پیکربندی شبکه خارجی وجود دارد.

معایب

- کاهش عملکرد : نیاز به پردازش اضافی دارد که ممکن است در شبکه‌های بزرگ باعث کاهش عملکرد شود.
- پیچیدگی در پیکربندی: برخی از برنامه‌ها و پروتکل‌ها با NAT سازگاری کامل ندارند و نیاز به پیکربندی خاصی دارند.
- محدودیت در Port Forwarding: در برخی مواقع، تنظیمات NAT می‌تواند باعث محدودیت در دسترسی به برخی از سرویس‌های شبکه شود.

کاربردهای NAT

- اتصال شبکه‌های خصوصی به اینترنت: به کاربران شبکه‌های خصوصی امکان می‌دهد تا از طریق یک آدرس IP عمومی به اینترنت متصل شوند.
- VPN: در شبکه‌های VPN برای اتصال ایمن از NAT استفاده می‌شود.
- Firewall: به عنوان یک لایه اضافی در دیوار آتش عمل می‌کند و از دسترسی غیرمجاز جلوگیری می‌کند.

برای درک بهتر و عملیاتی کردن NAT، سناریویی را فرض می‌کنیم که در آن شبکه‌ای با یک مسیریاب وجود دارد که قرار است به اینترنت متصل شود. در این سناریو، انواع NAT را پیاده‌سازی می‌کنیم و دستورات مربوط به هر نوع NAT را با جزئیات بررسی می‌کنیم.

فرض کنید که یک شبکه داخلی با رنج IP خصوصی 192.168.1.0 /24 داریم. این شبکه از طریق یک مسیریاب به اینترنت متصل است. مسیریاب دارای یک آدرس IP عمومی 203.113.0.1 است. ما می‌خواهیم دستگاه‌های داخلی بتوانند به اینترنت دسترسی داشته باشند.

Static NAT

تبدیل یک آدرس IP خصوصی مشخص (مثلاً 192.168.1.10) به یک آدرس IP عمومی مشخص (مثلاً 203.113.0.10).

پیکربندی اینترفیس داخلی مسیریاب

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# no shutdown
```

پیکربندی اینترفیس خارجی مسیریاب

```
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip address 203.0.113.1 255.255.255.0
Router(config-if)# no shutdown
```

تعریف NAT استاتیک

```
Router(config)# ip nat inside source static 192.168.1.10 203.0.113.10
```

تعریف اینترفیس‌هایNAT

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat inside
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat outside
```

دستور اختیاری: می‌توانید تایمر برای جدول NAT تعریف کنید.

```
Router(config)# ip nat translation timeout 3600
```

Dynamic NAT

تبدیل آدرس‌های IP خصوصی درون شبکه به آدرس‌های IP عمومی از یک رنج مشخص

تعریف رنج آدرس‌های IP عمومی

```
Router(config)# ip nat pool NAT_POOL 203.0.113.2 203.0.113.254 netmask 255.255.255.0
```

تعریف لیست دسترسی برای مشخص کردن آدرس‌های IP خصوصی که مجاز به استفاده از NAT هستند

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

پیکربندی Dynamic NAT

```
Router(config)# ip nat inside source list 1 pool NAT_POOL
```

تعریف اینترفیس‌هایNAT

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat inside
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat outside
```

دستور اختیاری، تنظیم اورلودینگ (PAT) در Dynamic NAT: اگر تعداد IP های عمومی محدود باشد، می‌توان از اورلودینگ استفاده کرد.

```
Router(config)# ip nat inside source list 1 pool NAT_POOL overload
```

PAT (Port Address Translation) یا Overloading

تعریف لیست دسترسی برای مشخص کردن آدرس‌های IP خصوصی که مجاز به استفاده از NAT هستند

```
Router(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

پیکربندی PAT با استفاده از آدرس IP عمومی مسیریاب

```
Router(config)# ip nat inside source list 1 interface gigabitEthernet 0/0 overload
```

تعریف اینترفیس‌هایNAT

```
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip nat inside
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# ip nat outside
```

دستور اختیاری، تنظیم ترجمه‌های موقت برای هر اتصال (مثلاً زمان اتمام ترجمه‌ها).

```
Router(config)# ip nat translation timeout 180
```

تست و بررسی تنظیمات NAT

نمایش ترجمه‌های NAT در حال حاضر

Router# show ip nat translations

نمایش وضعیت NAT و آمارهای مربوط به آن

Router# show ip nat statistics

IP Address + Port = Socket

در دنیای شبکه‌های کامپیوتری، Socket (سوکت) به یک ترکیب از آدرس IP و شماره پورت اشاره دارد که برای شناسایی یکتا یک اتصال یا سرویس خاص در شبکه استفاده می‌شود.

Socketچیست؟

یک نقطه انتهایی (endpoint) برای برقراری ارتباط در شبکه است. هر Socket به طور یکتا توسط ترکیب آدرس IP (نشان‌دهنده یک دستگاه یا میزبان در شبکه) و شماره پورت (نشان‌دهنده یک سرویس خاص روی آن دستگاه) شناخته می‌شود.

ساختارSocket

IP Address: یک آدرس منطقی است که دستگاه یا میزبان در شبکه را شناسایی می‌کند.

Port Number: یک شماره که به طور خاص یک برنامه یا سرویس را بر روی میزبان مشخص می‌کند.

به عنوان مثال، در یک اتصال HTTP، یک Socket می‌تواند به صورت 192.168.1.5:80 نمایش داده شود.

عملکرد Sockets

Client Socket: در سمت کلاینت برای ایجاد اتصال به سرور.

Server Socket: در سمت سرور برای گوش دادن به اتصالات ورودی از کلاینت‌ها.

در بسیاری از زبان‌های برنامه‌نویسی، از Sockets برای ارتباط بین کلاینت و سرور استفاده می‌شود. به عنوان مثال در پایتون

```
import socket

# ایجاد یک سوکت
client_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

# اتصال به سرور
client_socket.connect(('192.168.1.5', 80))
```

در این مثال، socket.AF_INET نوع خانواده آدرس که برای IPv4 استفاده می‌شود و socket.SOCK_STREAM نوع سوکت که برای پروتکل TCP استفاده می‌شود.

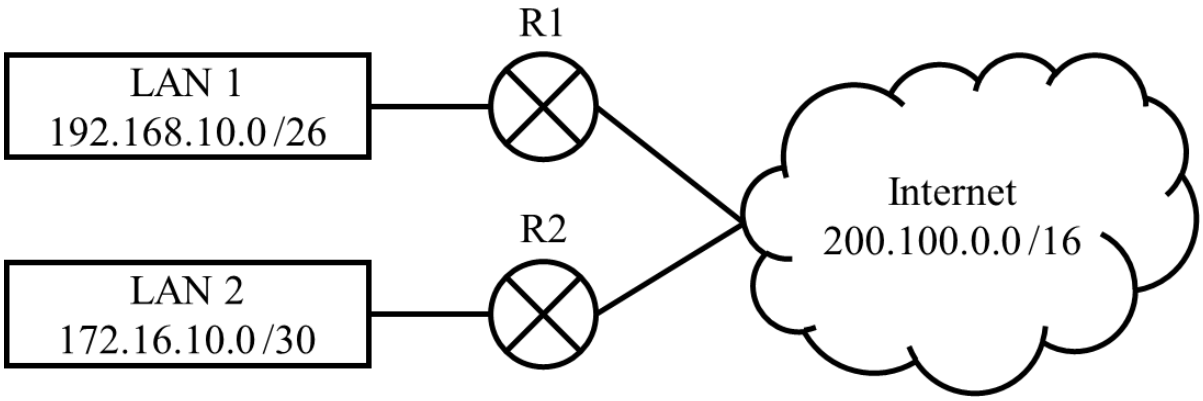
کاربردهای Socket

- ارتباطات کلاینت-سرور مانند وب سرورها و مرورگرهای وب
- ارتباطات بین فرآیندی (Inter-process Communication) در سیستم‌های توزیع شده
- استفاده در شبکه‌های بلادرنگ (Real-time Networks) مانند بازی‌های آنلاین و سیستم‌های پیام‌رسانی

ترکیب آدرس IP و شماره پورت، Socket را می‌سازد که یک مکانیزم بسیار مهم و پایه‌ای در برقراری ارتباطات شبکه‌ای است و به برنامه‌ها و دستگاه‌ها امکان می‌دهد تا به طور یکتا و مؤثر با یکدیگر در یک شبکه ارتباط برقرار کنند.

سوالات و تمرینات

شکل زیر را در نظر بگیرید، تمام انواع NAT را برای آن بنویسید. برای Static NAT حداقل ۳ مورد برای هر LAN نوشته شود.


R1
LAN 1
192.168.10.0 /26
R2
LAN 2
172.16.10.0 /30
Internet
200.100.0.0 /16

آزمایش ۱۶

اهداف: آشنایی با Telnet (Teletype Network)، Secure Shell (SSH)

سناریو ۱۶: قصد برقراری ارتباط با اجزای شبکه را از راه دور داریم.

اجزای مورد نیاز:

- Router
- Switch
- End device

یکی از اولین پروتکل‌های شبکه است که برای برقراری ارتباط از راه دور با یک دستگاه استفاده می‌شودTelnet است. این پروتکل به کاربران اجازه می‌دهد تا با استفاده از یک شبیه‌ساز ترمینال، به یک ماشین دیگر متصل شده و دستورات را اجرا کنند. با این حال، به دلیل عدم استفاده از رمزنگاری، Telnet به مرور زمان توسط پروتکل‌های امن‌تری مانند SSH جایگزین شده است. در ادامه به تشریح جزئیات استفاده از Telnet در شبکه، ویندوز و لینوکس می‌پردازم.

Telnet در شبکه‌های کامپیوتری

از پروتکل TCP برای برقراری ارتباط استفاده می‌کند و معمولاً روی پورت ۲۳ اجرا می‌شود. این پروتکل به صورت متن ساده (plaintext) ارتباط برقرار می‌کند، به این معنا که تمامی داده‌ها، از جمله نام کاربری و رمز عبور، بدون رمزنگاری ارسال می‌شوند. این موضوع Telnet را به یک پروتکل ناامن تبدیل کرده است، به خصوص در شبکه‌هایی که ترافیک توسط افراد غیرمجاز قابل شنود (sniffing) است.

با استفاده ازTelnet ، می‌توان به دستگاه‌هایی مانند مسیریاب‌ها، سوئیچ‌ها، سرورها و دیگر تجهیزات شبکه متصل شد و به آنها دسترسی داشت. در شبکه‌های امروزی، معمولاً Telnet برای پیکربندی دستگاه‌های شبکه‌ای استفاده می‌شود که هنوز از این پروتکل پشتیبانی می‌کنند.

Telnet در ویندوز

در ویندوز، Telnetبه عنوان یک کلاینت قابل استفاده است، اما این ویژگی ممکن است به صورت پیش‌فرض غیرفعال باشد. برای فعال کردن Telnet Client در ویندوز، به "Control Panel" بروید. گزینه "Programs and Features" را انتخاب کنید. روی "Turn Windows features on or off" کلیک کنید. گزینه "Telnet Client" را پیدا کنید و آن را فعال کنید.

Control Panel / Program and Features / Turn Windows features on or off / Telnet Client

پس از فعال‌سازی، می‌توانید از طریق Command Prompt به یک سرور Telnet متصل شوید.

telnet [hostname or IP address]

این دستور به شما اجازه می‌دهد که به دستگاه مقصد متصل شوید و دستورات خود را اجرا کنید.

Telnet در لینوکس

در لینوکس، Telnet معمولاً از طریق بسته‌ای به نام telnet ارائه می‌شود. اگر این بسته نصب نشده باشد، می‌توانید آن را با استفاده از مدیریت بسته (package manager) نصب کنید. به عنوان مثال، در توزیع‌های مبتنی بر Debian مانند Ubuntu:

sudo apt-get install telnet

و در توزیع‌های مبتنی بر Red Hat مانند CentOS:

sudo yum install telnet

پس از نصب، می‌توانید با دستور مشابه ویندوز به یک سرور Telnet متصل شوید:

telnet [hostname or IP address]

Telnet در MacOS

درMacOS ، Telnet به عنوان یک ابزار شبکه‌ای استفاده می‌شود که به شما امکان می‌دهد تا به صورت از راه دور به سرورها یا دستگاه‌های شبکه‌ای متصل شوید و دستورات را از طریق ترمینال اجرا کنید. با این حال،

Apple در نسخه‌های اخیرMacOS ، ابزار Telnet را به صورت پیش‌فرض حذف کرده است. در ادامه توضیح می‌دهم که چگونه می‌توانید Telnet را در MacOS نصب و استفاده کنید.

نصب Telnet درMacOS

از آنجایی که Telnet به صورت پیش‌فرض در نسخه‌های جدید MacOS موجود نیست، نیاز به نصب آن از طریق Homebrew دارید، که یک مدیر بسته محبوب در MacOS است. اگر Homebrew را نصب نکرده‌اید، ابتدا آن را نصب کنید. برای نصب Homebrew، ترمینال (Terminal) را باز کرده و دستور زیر را اجرا کنید:

```
/bin/bash -c "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/HEAD/install.sh)"
```

پس از نصب Homebrew، می‌توانید Telnet را با استفاده از دستور زیر نصب کنید:

```
brew install telnet
```

این دستور Telnet را از طریق Homebrew نصب می‌کند و آن را در دسترس قرار می‌دهد.

پس از نصب، می‌توانید با دستور مشابه ویندوز و لینوکس به یک سرور Telnet متصل شوید:

```
telnet [hostname or IP address]
```

برای پیاده‌سازی و اجرای Telnet در یک شبکه کامپیوتری، در ادامه یک سناریو را ارائه می‌دهیم. این سناریو شامل مراحل راه‌اندازی یک سرورTelnet ، اتصال کلاینت به آن، و اجرای دستورات از راه دور است.

مدیریت مسیریاب در یک شبکه محلی با استفاده از Telnet

یک مسیریاب که از پروتکل Telnet پشتیبانی می‌کند.

یک کامپیوتر (کلاینت) با سیستم عامل ویندوز، لینوکس یا MacOS که به شبکه متصل است.

دسترسی شبکه‌ای بین کامپیوتر کلاینت و مسیریاب.

اطلاعات دسترسی (نام کاربری و رمز عبور) برای ورود به مسیریاب

پیکربندی مسیریاب برای Telnet

ابتدا باید Telnet را روی مسیریاب فعال کنید.

اتصال فیزیکی به مسیریاب: برای پیکربندی اولیه، باید از طریق پورت کنسول یا SSH به مسیریاب متصل شوید.

ورود به حالت پیکربندی

```
Router> enable
Router# configure terminal
```

فعال‌سازی Telnet

```
Router(config)# line vty 0 4
```

این دستور شما را به حالت پیکربندی خط‌های مجازی ترمینال (Virtual Terminal Lines) منتقل می‌کند.

vty مخفف "Virtual Teletype" است. خطوط ۰ تا ۴ نشان‌دهنده پنج اتصال Telnet مجاز همزمان هستند.

بنابراین، شما اینجا در حال پیکربندی تنظیمات Telnet هستید.

```
Router(config-line)# login
```

این دستور باعث می‌شود که مسیریاب از کاربران درخواست کند تا هنگام اتصال به Telnet، نام کاربری و رمز عبور خود را وارد کنند. بدون این دستور، کاربران می‌توانند بدون تأیید اعتبار وارد شوند.

```
Router(config-line)# password your_password
```

این دستور رمز عبور مورد نیاز برای ورود به مسیریاب از طریق Telnet را تنظیم می‌کند. your_password را باید با رمز عبور دلخواه خود جایگزین کنید. هر کاربری که از Telnet استفاده می‌کند باید این رمز عبور را وارد کند تا اجازه دسترسی به مسیریاب را داشته باشد.

```
Router(config-line)# exit
```

این دستور شما را از حالت پیکربندی خطوط Telnet خارج می‌کند و به حالت پیکربندی جهانی (Global) برمی‌گرداند.

دستور اختیاری، اگر بخواهید ورود از راه دور به مسیریاب را محدود کنید، می‌توانید از ACL (Access Control List) استفاده کنید.

```
Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255
```

این دستور یک لیست کنترل دسترسی (ACL) با شماره ۱۰ ایجاد می‌کند که اجازه می‌دهد دستگاه‌هایی در محدوده آدرس IP 192.168.1.0 تا 192.168.1.255 به مسیریاب دسترسی داشته باشند. این لیست فقط به دستگاه‌های موجود در این شبکه محلی اجازه دسترسی می‌دهد.

```
Router(config)# line vty 0 4
Router(config-line)# access-class 10 in
```

این دستور لیست کنترل دسترسی شماره ۱۰ را به خطوط Telnet اعمال می‌کند. به این ترتیب، فقط دستگاه‌هایی که در ACL تعریف شده‌اند (192.168.1.0 /24) می‌توانند به مسیریاب از طریق Telnet متصل شوند. این کار امنیت اتصال Telnet را بهبود می‌بخشد.

```
Router(config-line)# exit
```

ذخیره پیکربندی

```
Router(config)# exit
Router# write memory
```

این دستور پیکربندی‌های فعلی را از حافظه ناپایدار (RAM) به حافظه پایدار (NVRAM) ذخیره می‌کند. این به معنای آن است که اگر مسیریاب مجدد راه‌اندازی شود، پیکربندی‌هایی که ایجاد کرده‌اید حفظ خواهند شد.

اتصال کلاینت به مسیریاب از طریق Telnet

پس از فعال‌سازی Telnet روی مسیریاب، می‌توانید از یک کامپیوتر کلاینت به آن متصل شوید.

روی ویندوز

بخش Command Prompt را باز کنید.

دستور زیر را اجرا کنید

```
telnet [IP address of router]
```

به عنوان مثال:

```
telnet 192.168.1.1
```

روی لینوکس یا MacOS

ترمینال را باز کنید.

دستور زیر را اجرا کنید.

telnet [IP address of router]

پس از اجرای دستور، از شما خواسته می‌شود که نام کاربری و رمز عبور خود را وارد کنید. اگر اعتبارسنجی موفقیت‌آمیز باشد، به کنسول مسیریاب دسترسی خواهید داشت.

اجرای دستورات مدیریتی

پس از اتصال به مسیریاب، می‌توانید دستورات مختلفی را اجرا کنید تا مسیریاب را پیکربندی یا وضعیت آن را بررسی کنید.

نمایش وضعیت اینترفیس‌ها:

Router> show ip interface brief

پیکربندی یک اینترفیس:

```
Router> enable
Router# configure terminal
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# ip address 192.168.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
Router# write memory
```

راه‌اندازی مجدد مسیریاب (با احتیاط انجام شود)

Router# reload

این دستور باعث راه‌اندازی مجدد (reboot) مسیریاب می‌شود. تمامی پیکربندی‌های ذخیره نشده از بین خواهند رفت و مسیریاب از تنظیمات ذخیره شده قبلی خود استفاده می‌کند. این دستور معمولاً برای اعمال تغییرات خاص یا پس از نصب یک به‌روزرسانی نرم‌افزاری استفاده می‌شود.

قطع اتصال از Telnet

برای خروج از جلسه Telnet ، می‌توانید دستور زیر را اجرا کنید

exit

یا کلیدهای ترکیبی [+ Ctrl را فشار داده و سپس quit را تایپ کنید.

پیکربندی سوئیچ برای Telnet

enable
configure terminal
line vty 0 4
password your_password
login
end
write memory

تنظیمات ACL برای محدود کردن دسترسی

access-list 10 permit 192.168.1.0 0.0.0.255
line vty 0 4
access-class 10 in

پیکربندی پیام خوش‌آمدگوی:

banner motd # Unauthorized access is prohibited! #

تنظیم یک پیام خوش‌آمدگویی (Message of the Day - MOTD) که هنگام ورود به دستگاه نمایش داده می‌شود. این پیام به کاربران هشدار می‌دهد که دسترسی غیرمجاز ممنوع است.

exec-timeout 5 0

تنظیم زمان انقضا برای جلسات Telnet. این دستور باعث می‌شود که اگر کاربران بدون فعالیت باشند، اتصال آنها پس از ۵ دقیقه به طور خودکار قطع شود. این می‌تواند به امنیت دستگاه کمک کند.

تعداد خطوط VTY پیش‌فرض

مسیریابها: معمولاً ۵ خط VTY به طور پیش‌فرض برای اتصال Telnet و SSH فراهم است.

سوئیچ‌ها: معمولاً ۱۶ خط VTY به طور پیش‌فرض برای اتصال Telnet و SSH فراهم است.

تغییر تعداد خطوط VTY

شما می‌توانید تعداد خطوط VTY را در تنظیمات دستگاه تغییر دهید، اما بیشتر از مقدار پشتیبانی شده توسط مدل دستگاه نمی‌توانید اضافه کنید. برای تغییر تعداد خطوط VTY، می‌توانید از دستور زیر در حالت پیکربندی استفاده کنید.

line vty 0 [N]

که در آن [N] تعداد خطوط VTY است.

برای پیاده‌سازی SSH (Secure Shell) بر روی مسیریاب و سوئیچ، شما باید تنظیمات مختلفی را انجام دهید تا اتصال امن و رمزگذاری شده فراهم شود.

پیکربندی SSH بر روی مسیریاب

ورود به حالت پیکربندی

اتصال به مسیریاب: از طریق کنسول یا Telnet به مسیریاب متصل شوید.

```
Router> enable
Router# configure terminal
```

تنظیم نام دستگاه و دامنه

نام دستگاه: نام‌گذاری دستگاه به شما کمک می‌کند تا شناسایی آسان‌تری داشته باشید.

دامنه: برای تولید کلید SSH به نام دامنه نیاز است.

```
Router(config)# hostname Router1
Router1(config)# ip domain-name example.com
```

ایجاد کلید رمزنگاری SSH

کلید SSH، تولید یک جفت کلید RSA برای استفاده در SSH.

```
Router1(config)# crypto key generate rsa
The key modulus size is 2048 bits
```

پیکربندی خطوط VTY برای SSH

تنظیمات SSH برای خطوط VTY: فقط دسترسی SSH را فعال کنید.

```
Router1(config)# line vty 0 4
```

```
Router1(config-line)# transport input ssh
Router1(config-line)# login local
Router1(config-line)# exit
```

ایجاد کاربر و تنظیم رمز عبور

کاربر و رمز عبور: ایجاد یک حساب کاربری محلی با رمز عبور برای ورود به سیستم از طریق SSH.

```
Router1(config)# username admin privilege 15 secret admin_pass
```

دستور username: ایجاد کاربر admin با رمز عبور admin_pass. با سطح دسترسی ۱۵

تنظیمات اضافی (اختیاری):

پیکربندی پیام خوش‌آمدگویی:

```
Router1(config)# banner motd # Unauthorized access is prohibited! #
```

تنظیم زمان انقضا برای جلسات SSH

```
Router1(config)# line vty 0 4
Router1(config-line)# exec-timeout 5 0
```

ذخیره پیکربندی:

```
Router1(config)# end
Router1# write memory
```

پیکربندی SSH بر روی سوئیچ

ورود به حالت پیکربندی

اتصال به سوئیچ: از طریق کنسول یا Telnet به سوئیچ متصل شوید.

```
Switch> enable
Switch# configure terminal
```

تنظیم نام دستگاه و دامنه

نام دستگاه: نام‌گذاری دستگاه برای شناسایی آسان.

دامنه: برای تولید کلید SSH به نام دامنه نیاز است.

```
Switch(config)# hostname Switch1
Switch1(config)# ip domain-name example.com
```

ایجاد کلید رمزنگاری SSH

کلید :SSH تولید یک جفت کلید RSA برای استفاده در SSH

```
Switch1(config)# crypto key generate rsa
The key modulus size is 2048 bits
```

دستور crypto key generate rsa: ایجاد کلید RSA با طول پیش‌فرض ۲۰۴۸ بیت.

پیکربندی خطوط VTY برای SSH

تنظیمات SSH برای خطوط :VTY فقط دسترسی SSH را فعال کنید.

```
Switch1(config)# line vty 0 15
Switch1(config-line)# transport input ssh
Switch1(config-line)# login local
Switch1(config-line)# exit
```

ایجاد کاربر و تنظیم رمز عبور

کاربر و رمز عبور: ایجاد یک حساب کاربری محلی با رمز عبور برای ورود به سیستم از طریق.SSH

```
Switch1(config)# username admin privilege 15 secret admin_pass
```

دستور username: ایجاد کاربر admin با سطح دسترسی ۱۵ و رمز عبور admin_pass

تنظیمات اضافی (اختیاری)

پیکربندی پیام خوش‌آمدگویی

```
Switch1(config)# banner motd # Unauthorized access is prohibited! #
```

تنظیم زمان انقضا برای جلسات SSH

```
Switch1(config)# line vty 0 15
Switch1(config-line)# exec-timeout 5 0
```

ذخیره پیکربندی

```
Switch1(config)# end
Switch1# write memory
```

با انجام این مراحل، شما می‌توانید اتصال SSH امن را برای مسیریاب و سوئیچ سیسکو پیکربندی کنید و از این طریق به مدیریت دستگاه‌ها بپردازید.

اتصال به SSH در ویندوز، MacOS، و لینوکس به روش‌های مختلفی انجام می‌شود. در ادامه به شما نشان می‌دهیم که چگونه می‌توانید از هر کدام از این سیستم‌عامل‌ها به یک سرور یا دستگاه از طریق SSH متصل شوید.

اتصال SSH در ویندوز

در ویندوز، معمولاً از نرم‌افزارهای شخص ثالث مانند PuTTY یا OpenSSH (نصب‌شده به صورت پیش‌فرض از ویندوز ۱۰ نسخه ۱۸۰۹ به بعد) استفاده می‌شود.

- استفاده از PuTTY

نصب PuTTY

PuTTY را از سایت رسمی دانلود و نصب کنید.

اجرای PuTTY

PuTTY را اجرا کنید.

در قسمت(Host Name (or IP address ، آدرس IP یا نام دامنه سرور مورد نظر خود را وارد کنید.

پورت پیش‌فرض برای SSH، ۲۲ است؛ مطمئن شوید که Connection type بر روی SSH تنظیم شده باشد.

اتصال به سرور

روی Open کلیک کنید.

یک ترمینال باز می‌شود که از شما درخواست می‌کند نام کاربری و سپس رمز عبور را وارد کنید.

- استفاده از OpenSSH

بررسی نصب OpenSSH

به Settings بروید و در قسمتApps & Features ، روی Optional Features کلیک کنید.

به دنبال OpenSSH Client بگردید؛ اگر نصب نشده باشد، می‌توانید آن را نصب کنید.

اتصال از طریق Command Prompt یا PowerShell

Command PromptیاPowerShell را باز کنید.

دستور زیر را وارد کنید

ssh username@host_ip_address

username را با نام کاربری خود و host_ip_address را با آدرس IP یا نام دامنه سرور جایگزین کنید.

پس از زدن Enter، از شما درخواست رمز عبور می‌شود.

اتصال SSH درMacOS

درMacOS ، ترمینال پیش‌فرض سیستم دارای SSH Client داخلی است و نیاز به نصب نرم‌افزار اضافی نیست.

مراحل اتصال

باز کردن Terminal

از طریق Spotlight با زدن Command + Space و تایپ کردن Terminal می‌توانید به ترمینال دسترسی پیدا کنید.

اتصال به سرور

دستور زیر را وارد کنید

ssh username@host_ip_address

username را با نام کاربری خود و host_ip_address را با آدرس IP یا نام دامنه سرور جایگزین کنید.

پس از زدن Enter، از شما درخواست رمز عبور می‌شود.

اتصال SSH در لینوکس

مانندMacOS ، لینوکس نیز به طور پیش‌فرض دارای SSH Client است و شما می‌توانید از طریق ترمینال به SSHمتصل شوید.

مراحل اتصال

باز کردن Terminal

ترمینال را باز کنید (در بیشتر توزیع‌های لینوکس با فشار دادن Ctrl + Alt + T یا جستجوی "Terminal" می‌توانید آن را باز کنید).

اتصال به سرور

دستور زیر را وارد کنید:

ssh username@host_ip_address

username را با نام کاربری خود و host_ip_address را با آدرس IP یا نام دامنه سرور جایگزین کنید.

پس از زدن Enter، از شما درخواست رمز عبور می‌شود.

اتصال SSH به یک سرور یا دستگاه از طریق ویندوز، MacOS، و لینوکس ساده است و با دستورات پایه SSH می‌توانید به راحتی ارتباط امن برقرار کنید. نرم‌افزارهای مانند PuTTY در ویندوز و استفاده از ترمینال در MacOS و لینوکس راه‌های اصلی برای انجام این کار هستند.

سوالات و تمرینات

از میان سناریوها و آزمایش‌های که تا کنون انجام داده‌اید دو مورد را به دلخواه انتخاب کنید و پیکربندی‌های مرتبط با مسیریاب‌ها و سوئیچ‌ها را از طریق ارتباط Telnet و SSH انجام دهید.