مبانی اولیه سیسکو

CCNA

CISCO CERTIFIED
CCNA
Security

جلسه ششم : انواع روتینگ پروتکل ها

✓ آموزش کامل Routing & Switching

✓ به همراه سناریو

نویسنده: مهندس امیرحسین خالقی

فهرست

پیشگفتار ۳
فصل ششم : انواع روتینگ پروتکل ها ۴
- RIP ۴
- OSPF ۵
- سناریو ۱۱

پیشگفتار

سپاس پروردگار را که این امکان را داد که تا باز بتوانیم مجموعه ای پر مطلب و پر فهم را کمتر از یک سال بنویسیم.

این کتاب با توجه به سرفصل های کتاب CCNA ICND 1 & ICND 2 برای علاقه مندان به شبکه و سیسکو نوشته شده است. در تهیه این کتاب سعی بر آن شده است تا فهم مطالب و مباحث به صورت روان و گیرا مطرح گردد.

در ابتدای کتاب سر فصل مطالب قید شده است. در انتهای هر فصل سناریویی طراحی شده که می تواند در فهم و یادگیری سریع تر شما کمک کند. توصیه می شود که این سناریو ها حتما کار شود. در انتهای کتاب به بررسی نمونه سوالات آزمون Cisco پرداخته ایم.

درصورت هرگونه مشکل در این کتاب میتوانید با ایمیل نویسنده (info@akhaleghi.ir) تماس حاصل فرمایید تا با بررسی آن بتوانیم کتابی کامل و با زبان فارسی در اختیار شما دوستان و همکاران ارجمند قرار دهیم.

در پایان از تمامی عزیزانی که ما را در تهیه و تنظیم این کتاب یاری نموده اند کمال تشکر را داریم.

باشد که موثر باشیم ....

امیرحسین خالقی

فصل ششم : انواع روتینگ پروتکل ها

در فصل قبل با روتینگ ها و نحوه کارکرد آن آشنا شدیم. دیدیم که Static Route چگونه است و چه مشکلاتی را در بر دارد. در این فصل با پروتکل های بیشتر آشنا میشویم که در ادامه به بررسی آن خواهیم پرداخت :

- RIP (Dynamic Routing Protocol)

RIP یکی از پروتکل‌های Distance Vector است که تعداد hop ها را به عنوان معیاری برای محاسبه طول یک مسیر استفاده می‌کنند. RIP نیز یکی از پروتوکل‌های IGP است یعنی عملیات مسیریابی را داخل یک سیستم مستقل واحد انجام می‌دهد، در حالی که پروتوکل‌های EGP مانند Border Gateway بین سیستم‌های مستقل مختلف کار مسیریابی را انجام می‌دهند. آخرین بهبودهایی که در RIP صورت گرفت نسخه ای از آن را با نام RIP2 ارائه داد که باعث می‌شد اطلاعات بیشتری در Packet ها جا داده شوند و ضمناً یک مکانیزم تصدیق ساده را نیز اضافه نمود. RFC 1058 (سال 1988) اولین نسخه RIP را توضیح می‌دهد. در این قسمت توانایی‌های اساسی و خصوصیات ویژه RIP را به طور خلاصه بیان می‌کنیم:

RIP پیغام‌های Routing Update را در فاصله‌های زمانی منظم و هنگامی‌که توپولوژی شبکه تغییر می‌کند ارسال می‌نماید. مسیریاب‌های RIP فقط بهترین مسیر تا مقصد (مسیر با کمترین فاصله) را نگاه می‌دارند. پس از Update کردن Routing Table ، مسیریاب فوراً به بقیه، پیغام‌های Update می‌فرستد تا آنها را از تغییر وضعیت ایجاد شده در شبکه آگاه کند. پیغام‌های Update اینچنین (که تغییری در شبکه را به بقیه اطلاع می‌دهند) مستقل از پیغام‌های Update که مسیریاب‌ها در فاصله‌های زمانی منظم ارسال می‌کنند می‌باشد.

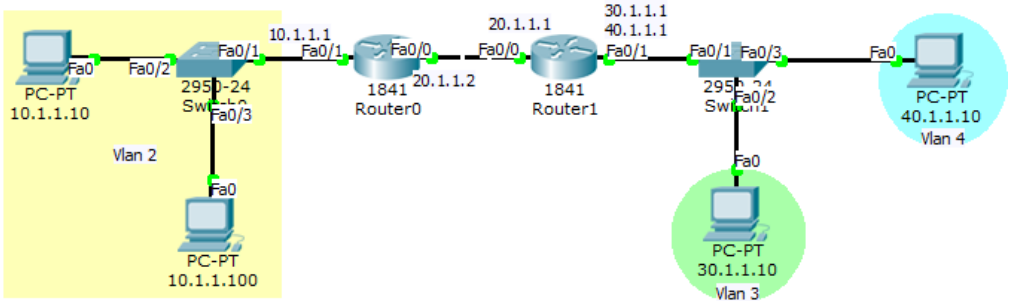
RIP تنها یک معیار برای محاسبه طول یک مسیر دارد و آن هم شمارش تعداد hop ها است. RIP از ایجاد LOOP مسیریابی بوسیله محدودیت گذاشتن روی تعداد hop هایی که می‌توانند بین Source و Dest وجود داشته باشند جلوگیری می‌کند. ماکزیمم تعداد hop در یک مسیر معتبر ۱۵ تا می‌تواند باشد، اگر یک مسیریاب پیغام Update مبنی بر ورود یک مسیریاب یا host جدید دریافت کند و این شیء جدید باعث شود که تعداد hop ها در مسیری به ۱۶ برسد آنگاه مقصد این مسیر از طرف مسیریاب، غیر قابل دسترس اعلام می‌گردد.

برای اینکه تغییرات ایجاد شده در توپولوژی شبکه هر چه سریع تر به همه اطلاع داده شود RIP یک سری قابلیت‌هایی دارد که در اغلب پروتوکل‌های دیگر نیز موجودند. به عنوان مثال RIP دارای مکانیزم Spilit Horison , Hold Down برای جلوگیری از گسترش اطلاعات نادرست مسیریابی است علاوه بر این، محدودیت hop-count که RIP قرار می‌دهد نیز از گسترش نامحدوده Loop های مسیریابی جلوگیری می‌کند.

این بار با استفاده از Rip میخواهیم روترها هم دیگر را ببینند:

همان کارهایی را که برای IP Route انجام دادیم برای Rip هم انجام میدهیم. یعنی ارتباط بین روتر و سوییچ حتما Trunk باشد. عضویت Vlan ها و ساختن Sub interface ها در روتر ، Encapsulation کردن Sub interface ها و دادن IP Address یا همان Default Gateway بر روی Sub interface ها.

با توجه به شکل زیر:



پس از اینکه به Interface های روتر ها ip دادیم میریم سراغ دستور زیر:

```
R0(config)#router rip
R0(config-router)#network 10.1.1.0
R0(config-router)#network 20.1.1.0
R0(config-router)#no auto
R0(config-router)#no auto-summary
R0(config-router)#version 1
```

در روتر ۰ دستور رو به رو را اعمال میکنیم:

```
R1(config)#router rip
R1(config-router)#network 30.1.1.0
R1(config-router)#network 40.1.1.0
R1(config-router)#network 20.1.1.0
R1(config-router)#no au
R1(config-router)#no auto-summary
R1(config-router)#ver
R1(config-router)#version 1
```

و در روتر ۱ نیز دستور روبه رو را اعمال می کنیم:

به همین سادگی تمامی PC ها همدیگر را Ping می کنند!

درخط اول با دستور Router Rip ، پروتکل Rip را فراخوانی میکنیم. سپس با استفاده از دستور Network ، IP تمام Interface ها و Sub Interface ها را به روتر نشان میدهیم.

بحث Auto Summarization :

به صورت خلاصه Summarization یا خلاصه سازی یعنی عدم ارسال سابنت مسک در هنگام Advertise کردن IP .

به صورت پیش فرض در همه روتینگ پروتکل ها فعال هست غیر از OSPF . روتری که دارای دو شبکه در یک رنج هست وقتی می خواهد آدرس شبکه را بفرستد آن را Summarize می کند و به صورت Class Full می فرستد یعنی Subnet Mask آن رامشخص نمی کند.

Auto Summarization را می توان در روتینگ پروتکل های Classless غیرفعال کرد. در روتینگ های Class full نمی توان این کار را انجام داد .اگر این قابلیت در روتینگ پروتکل هایی که به صورت پیش فرض فعال است غیرفعال نشود، در شبکه های VLSM به مشکل برمی خوریم. توصیه می شود که این قابلیت در روتینگ پروتکل هایی که به صورت پیش فرض فعال هست ، غیرفعال شود. چون بودنش دردسرساز هست. اگر بخواهیم خودمان میتوانیم به صورت دستی فعالش کنیم.

```
R1(config-router)#no auto-summary
```

– OSPF (Open Shortest Path First)

بکارگیری پروتکل RIP در شبکه های کامپیوتری بیشتر به دلیل شرایط زمان بوده است. در ده هفتاد و هشتاد حافظه و پردازنده های سریع ،گران قیمت بودند و پیاده سازی الگوریتمهای مسیریابی مبتنی بر روشهایی نظیر LS که هم به حافظه و هم به پردازندهٔ سریع نیاز دارند ، مقرون به صرفه نبود. از طرفی شبکه ها نیز آنقدر توسعه نیافته بودند که نیاز به الگوریتم های بهینه تر احساس شود. با گسترش اینترنت و توسعهٔ شبکه های خودمختار در اواخر دههٔ هشتاد ، کاستی های پروتکل RIP نمود بیشتری پیدا کرد و با سریع شدن پردازنده ها و ارزان شدن سخت افزار ، نیاز به طراحی یک پروتکل بهینه IETF، را واداشت تا در سال ۱۹۹۰،OSPF را به عنوان یک پروتکل استاندارد ارائه نماید. مسیریابهای زیادی مبتنی بر این پروتکل به بازار عرضه شده اند و احتمال می رود که در آینده تبدیل به مهمترین پروتکل مسیریابی درونی در شبکه های AS شود.

پروتکل قدرتمند و پرطرفدار OSPF یا Open Shortest Path First ، پروتکلی Link State و Open Standard است که در RFC 2328 شرح داده شده است. این پروتکل برای پیدا کردن Neighbor (همسایه) یا در واقع روترهای متصل به خود از Hello Message استفاده میکند. پیام Hello به

آدرس (AllSPF Routers) Multicast ارسال میگردد اگر در رسانه ای خاص Multicast قابل استفاده نباشد، از Unicast استفاده میکند (در این حالت آدرس همسایه باید از قبل تنظیم شده باشد).

مقایسه پروتکل OSPF با پروتکل RIP:

- ✓ این پروتکل از الگوریتم LS برای محاسبهٔ بهترین مسیر استفاده میشود و بنابراین مشکل "شمارش تا بینهایت" وجود ندارد.
- ✓ در این پروتکل معیار هزینه فقط "تعداد گام" نیست بلکه میتواند چندین معیار هزینه را در انتخاب بهترین مسیر در نظر بگیرد.
- ✓ در این پروتکل حجم بار و ترافیک یک مسیریاب در محاسبهٔ بهترین مسیر دخالت داده میشود و در ضمن در هنگام خرابی یک مسیریاب ، جداول مسیریابی سریعاً همگرا میشود.
- ✓ در این پروتکل ، فیلد Type of Service در بستهٔ IP میتواند در نظر گرفته شود و بر اساس نوع سرویس درخواستی ، برای یک بسته مسیر مناسب انتخاب گردد.
- ✓ در پروتکل OSPF تمام بسته های ارسالی برای یک مقصد خاص ، روی بهترین مسیر هدایت نمی شود بلکه درصدی از بسته ها روی مسیرهایی که از لحاظ حداقل هزینه در رتبهٔ ۲ ,۳ و ... قرار دارند ارسال میشود تا پدیدهٔ "نوسان"رخ ندهد. به این کار "موازنه بار"گفته میشود.
- ✓ در این پروتکل از مسیریابی سلسله مراتبی پشتیبانی میشود.
- ✓ در این پروتکل مسیریابها جداول مسیریابی را از دیگر مسیریابها قبول نمیکنند مگر آنکه هویت ارسال کنندهٔ آن احراز شود. به همین دلیل مسئول شبکه برای هر مسیریاب یک کلمهٔ عبور" تعیین میکند تا کاربران اخلالگر نتوانند با برنامه نویسی ، جداول مسیریابی مصنوعی تولید کرده و با ارسال آنها ، مسیریابی در شبکه را با مشکل مواجه کنند.

مبنای الگوریتم SPF بر پایه الگوریتم ریاضی است که توسط Edsger – Wybe – Dijkstra ارائه شده که با ایجاد Topology Table به ازای یک Area کار خود را انجام می دهد. هر روتر دارای زاویه دید و Perspective خود از شبکه بوده و شبکه را بصورت درختی میبیند که خود در راس آن قرار دارد و مسیرها را بصورت گراف پردازش میکند.

به ازای هر تغییر در شبکه، LSA ارسال شده و در Area به همه ارسال میشود و نهایتا پس از هر تغییر Topology Table دوباره از سر ساخته میشود.

سلسله مراتب تعیین شده برای نواحی در پروتکل OSPF:

یک شبکهٔ خودمختار (AS) به تعدادی "ناحیه" تقسیم می شود. تمام مسیریابهای درون یک ناحیه باید مسیریابهای هم ناحیه خود و هزینه ارتباط بین آنها را بدانند و در جدولی ذخیره کنند. در لحظات به هنگام سازی ، این جداول برای تمام مسیریابهای هم ناحیه ارسال خواهد شد. مسیریاب هیچ اطلاعی از وضعیت مسیریابهای درون نواحی دیگر ندارد.

درون هر ناحیه یک یا چند مسیریاب وجود دارند که ارتباط بین نواحی را برقرار میکنند ؛ به آنها ، "مسیریابهای مرزی" گفته میشود. مجموعه مسیریابهای مرزی و مسیریابهایی که در خارج از هر ناحیه نقش توزیع ترافیک بین نواحی را بر عهده دارند (بهمراه ساختار ارتباطی بین این مسیریابها) "ستون فقرات" شبکهٔ AS را تشکیل می دهد. درون ستون فقراتِ شبکهٔ AS ممکن است مسیریابهایی وجود داشته باشند که با دیگر شبکه های AS در ارتباط باشد. به این مسیریابها "دروازه های مرزی" یا BGP گفته میشود.

در پروتکل OSPF جداول زیر توسط مسیریابها "اعلان" میشود:

جدول مسیریابی محلی درون یک ناحیه : این جداول ، محتوی اطلاعاتی در مورد گراف هزینه ناحیه ای است که یک مسیریاب به آن متعلق است و توسط هر مسیریاب درون آن ناحیه، به تمام مسیریابها اعلان میشود.

جدول مسیریابی شبکه درون یک ناحیه: این جداول که محتوی اطلاعاتی در مورد مسیریابها و کانالهای بین آنها در یک شبکه است ، توسط مسیریاب های درون یک ناحیه به تمامی مسیریابها اعلان میشود.

جدول خلاصه مسیریابی مسیریابهای مرزی: این جداول محتوی اطلاعاتی خلاصه ، در مورد مسیرهای موجود در خارج از نواحی است و توسط مسیریاب های مرزی به تمامی مسیریاب های نواحی مختلف اعلان میشود.

جدول مسیریابی شبکه: این جداول محتوی اطلاعاتی در مورد مسیریاب ها و کانالهای بین آنها در خارج از شبکهٔ AS است و توسط مسیریاب های واقع بر ستون فقرات شبکهٔ AS به تمامی مسیریاب های نواحی مختلف اعلان میشود ولی فقط در مسیریاب های مرزی مورد استفاده قرار می گیرد.

انواع Area:

۱. Stub Area: این ناحیه به اطلاعات (External LSA type 5) نیازی ندارد زیرا به هر حال برای خروج از ناحیه دست به دامان ABR خود میشود. پس مسیر همیشه بدین گونه است و از طریق یک روتر خارج میشود. نکته و هدف از استفاده از این Area، Performance است. از آنجا که LSA 5 را قبول نمیکند پس LSA 4 نیز در این ناحیه بی معنی است و توسط ABR، Filter می شود. هدف صرفه جوئی در Resource ها و Memory است. که البته Stub area محدودیت های خود را نیز دارد:

- هیچ ASBR ی در ناحیه نمی توان داشت. (و مسلما هیچ Redistribution و External Route)
- Virtual Link در این Area مجاز نیست (نه در ناحیه و نه بصورت Transit)
- می توان چند ABR در این ناحیه داشت اما از آنجا که بهترین مسیر به ASBR را نمیتوان در این ناحیه فهمید، تفاوتی در انتخاب ABR برای رسیدن به ASBR وجود ندارد.
- تمام روتر ها (در Hello Message) بیت E خود را صفر ست میکنند (علامت Stub) و با روتری با E Flag برابر با یک، ارتباطی برقرار نمی کنند.

۲. Totally Stubby Area: اگر فیلتر کردن LSA 5 موجب بهبود کارایی روتر میشود، در این نوع از ناحیه حتی LSA 3 نیز Block میشود. این نوع Area توسط Cisco ارائه شده تا تنها با تزریق یک Default Route توسط ABR روتر ها تمام بسته هایی که مقصدشان داخل ناحیه نیست را به ABR بفرستند.

۳. Not So Stubby Area: یک ناحیه Stub است که بنا به دلایلی اقدام به Redistribution میکند. (مثلا ارتباط با ISP) LSA 7 در داخل ناحیه منتشر میکند. برای اعلام به نواحی دیگر به ABR میرسد. توسط ABR، اگر P bit آن LSA صفر باشد، Block میشود و اگر P Bit آن یک باشد به صورت مبدل شده به LSA 5 به بیرون از ناحیه اعلام میگردد.

۴. Backbone Area: این ناحیه بنام Area 0 مطرح میگردد و تمام نواحی از طریق این ناحیه به هم متصل میگردند. تمام LSA ها در این ناحیه مجازند غیر از نوع ۷.

۵. Standard Ordinary Area: این Area به Backbone وصل است و Stub نیست.

وضعیت های اتصال:

OSPF مسیرها را همانند پروتکل های بردار مسافت معرفی نمی کند, بلکه با استفاده از اعلان وضعیت اتصال (Link Advertisements-LSA) مسیرها را معرفی مینماید. یک اتصال (Link) فقط یک رابط (Interface) مانند اترنت (Ethernet), ویا سریال است. هر اتصال دارای ویژگی هایی شامل ناحیه OSPF که برای اتصال آن تنظیم شده, پهنای باند اتصال و پیشوند (Perfix) و ماسک زیر شبکه ثبت شده برای آن اتصال می باشد.وضعیت اتصال (Link-state) یعنی اینکه اتصال فعال یا غیر فعال است.

خصوصیات یک شبکه OSPF :

- نواحی یک یا چندگانه OSPF
- اگر از بیش از یک ناحیه استفاده شود, یک ناحیه پشتیبان (Backbone) یا ۰ باید تنظیم شود.
- تمام نواحی غیر ۰ باید به ناحیه ۰ وصل باشند.
- مسیریاب OSPF برای هر ناحیه ای که بر روی آن تنظیم می شود, یک پایگاه اطلاعاتی OSPF ایجاد می کند.
- آگهی های وضعیت اتصال (LSAs), اطلاعات مربوط به رابط های (Interface) یک مسیریاب را در سراسر ناحیه OSPF سرریز می سازند.
- پایگاه اطلاعاتی OSPF درون یک ناحیه باید قبل از اینکه یک مسیریاب , مسیرهای نصب شده در جدول مسیریابی IP را جمع بندی و محاسبه کند, هماهنگ شوند.
- الگوریتم کوتاهترین مسیر اول (Shortest Path First-SPF) در تمام پایگاه های اطلاعاتی یک مسیریاب لستفاده شده است و مسیرهای نصب شده در جدول مسیریابی IP را تعیین میکند.
- مسیرها را می توان به نواحی خلاصه کرد, نه درون نواحی.

همسایه یابی OSPF:

زمانی که OSPF بر روی یک رابط فعال می شود, مسیریاب یک بسته سلام (Hello Packet) بر روی شبکه ارسال می کند تا همسایگان خود را بیابد.در یک شبکه با چندین دسترسی (Multi-Access) بسته سلام هر ده ثانیه یکبار فرستاده می شود. در روتر وضعیت خاموش نشان دهنده این است که مسیریاب هیچ بسته سلامی (Hello Packet) را ارسال نمی کند. زمانی که OSPF بر روی یک رابط فعال شود, مسیریاب به حالت Init و یا آغازین (Initialization) تغییر وضعیت می دهد و شروع به ارسال بسته های سلام می کند. وضعیت آغازین ,همسایه های OSPF را بر روی یک اتصال (Link) شناسایی میکند. درون بسته سلام , ID مسیریاب OSPF (Router ID) نیز قرار دارد. زمانی که یک مسیریاب بسته سلامی را از یک همسایه دریافت می کند, ID مسیریاب خود را درون بسته قرار می دهد و بر روی شبکه ارسال می کند. زمانی که مسیریاب , ID مسیریاب خود را داخل بسته سلام همسایه مشاهده کند, همسایه ها در وضعیت دو طرفه (2-Way) قرار می گیرند.

در یک شبکه با چندین دسترسی (Multi-Access) یک مسیریاب (Designated Router-DR) و یک مسیریاب به عنوان پشتیبان مسیریاب اختصاصی (Backup Designated Router-BDR) انتخاب شده است. معمولا مسیریابی که بالاترین ID مسیریاب را دارد, DR و مسیریابی که پس از آن بالاترین ID را داراست BDR محسوب می شود. با توجه به انتخاب DR وBDR مهمترین مسئله تنظیم وقت است. زمانی که یک مسیریاب به عنوان DR انتخاب شد تا وقتی که از بین نرفته است DR باقی خواهد ماند. به تمام مسیریاب های یک شبکه با چندین دسترسی (Multi-Access) که DR و DBR نیستند, DROTHER گفته می شود.

تمام مسیریاب های OSPF باید با همسایه های خود تبادل اطلاعات کنند و از همسانی اطلاعات تمام مسیریاب های یک ناحیه مشخص اطمینان یابند. لزومی ندارد هر مسیریاب موجود در شبکه با چندین دسترسی اطلاعات خود را برای تمام مسیریاب های دیگر موجود در شبکه بفرستد. بنابراین هر مسیریاب, یک مسیریاب و یا LSA نوع ۱ بوجود می آورد, که وضعیت رابط های متصل به مسیریاب را مشخص می کند. تمام مسیریاب ها , LSA مسیریاب خود را به DR و BDR ارسال می کنند. DR و BDR یک شبکه یا LSA نوع ۲ را بوجود می آورد و آنرا به تمام مسیریاب های موجود در شبکه با چندین دسترسی (Multi-Access) می فرستد. در این حالت تمام مسیریاب ها به همجواری (Adjacency) کامل با DR و BDR می رسند. همجواری با DR و BDR به این معناست که هر مسیریاب بداند LSA های خود را باید به آنجا ارسال کند.

در شبکه های نقطه به نقطه (Point to Point) مفاهیم DR و BDR وجود ندارد. زیرا در آنجا فقط دو همسایه و یک اتصال نقطه به نقطه وجود دارد. مسیریاب ها در یک اتصال نقطه به نقطه یک همجواری کامل برای تبادل آگهی های وضعیت اتصال OSPF بوجود می آورند.

بررسی عملکرد OSPF:

- دستور Show IP Protocols : نشان دهنده انواع مختلف پارامترهای OSPF مانند تایمرها , فیلتر ها, metric ها, شبکه ها و اطلاعات مفید دیگر مربوط روتر مورد نظر می باشد.
- دستور Show IP Route OSPF : نشان دهنده OSPF Route های شناخته شده توسط روتر است. استفاده از این دستور یکی از بهترین روش های تشخیص امکان برقراری ارتباط بین روتر مورد نظر و بقیه شبکه می باشد. البته پارامترهای دیگری مانند OSPF Process ID را می توان در کنار دستور به کار برده و اطلاعات دلخواه را مورد بررسی قرار داد.
- دستور Show IP OSPF Interface : نشان دهنده Area های مربوط به Interface های روتر می باشد. همچنین اطلاعات دیگری مانند تایمرها (مانند hello interval) و روابط مجاورت بین روترها نیز توسط دستور فوق نمایش داده خواهند شد.
- دستور Show IP OSPF : این دستور نشان دهنده OSPF Touter ID, انواع تایمرها, تعداد دفعات اجرای الگوریتم SPF و اطلاعات مربوط به LSA ها می باشد.
- دستور Show IP OSPF Neighbor : نشان دهنده لیست روترهای همسایه, ID مربوط به روترهای DR/BDR در کنار ID و Priority مربوط به روترها و وضعیت رابطه مجاورت (Init , Exstart , Full) آنها با این روتر خواهد بود.

انواع OSPF authentication:

دو متد برای پیکربندی مکانیسم شناسایی هویت در OSPF وجود دارد که عبارتند از :

۱)Simple یا plain ۲) MD5

در صورت پیکربندی یک متد برای شناسایی هویت روترها در OSPF ،زمانی که یک روتر اقدام به دریافت پیام Update ارسال شده از روتری دیگر می نماید، هویت روتر ارسال کننده را با استفاده از یک پسورد بررسی کرده و در صورت یکسان بودن آن با پسورد تعیین شده در روی خود، پیام دریافت شده را خواهد پذیرفت. به صورت پیش فرض هیچ نوع مکانیسمی برای شناسایی هویت روترهای ارسال کننده پیام Update در پروتکل OSPF مورد استفاده قرار نمی گیرد.

پیکربندی OSPF :

Area یک مجموعه از روترها است که بوسیله Single Administrator اداره و نگهداری میشود .

روتر ناحیه مرزی که جایگزین شده بین یک Autonomous System OSPF و یک شبکه بدون OSPF که عمل میکند هر دو, OSPF و روتر پروتکل اضافه شده مانند ASBR RIP ها باید قرار داده شوند در یک ناحیه non-stub OSPF

Backbone : بخش مبنایی یک شبکه که فراهم میکند مسیر اولیه برای ترافیک فرستاده شده و راه انداخته شده از بقیه شبکه ها

Process ID : یک عدد است که برای اجرای مراحل مختلف OSPF در یک روتر صادر میشود

WildCard : یک عدد است که تعیین میکند چه مقدار IP address در OSPF استفاده میشود. Range از subnet ها را تعیین میکند wildcar برای تطبیق IP استفاده میشود. بطور مثال ip و wildcard زیر نشان میدهد range صفر تا ۲۵۵ را در wildcard آن octet که صفر است چک نمیشود و آن octet که ۲۵۵ است بدین معنی است که range یک تا ۲۵۵ را چک کند .

192.168.10.0 0.0.0.255

نحوه مسیریابی با پروتکل OSPF:

در پایان این فصل یک توپولوژی ساده را با نرم افزار شبیه سازی Packet Tracer پیاده سازی می کنیم :

ابتدا دو شبکه ایجاد می کنیم .شبکه اول با آدرس شبکه ۱۹۲,۱۶۸,۱,۰ با ماسک ۲۵۵,۲۵۵,۲۵۵,۱۹۲ و شبکه دوم با آدرس شبکه ۱۹۲,۱۶۸,۱,۶۴ با ماسک ۲۵۵,۲۵۵,۲۵۵,۱۹۲ را ایجاد می کنیم .اما چون این دو شبکه از هم مجزا هستند برای برقراری ارتباط این دو شبکه به Device هایی مانند روتر نیاز داریم .

اما نکته ای که نباید فراموش شود این است که بین این دو روتر نیز باید یک شبکه بوجود آوریم .آدرس شبکه بین روترهایمان ۱۹۲,۱۶۸,۱,۱۲۸ با ماسک ۲۵۵,۲۵۵,۲۵۵,۱۹۲ می باشد.ما روترهایمان را جهت اینکه بتوانند ارتباط برقرار کنند باید Config کنیم و بر خلاف مثال فصل اول از مسیریابی داینامیک اسفاده می کنیم پروتکلی که این مسیریابی را انجام می دهد OSPF نام دارد و ما در اینجا نحوه ی بکار اندازی پروتکل OSPF درون سیستم عامل IOS روتر تشریح می کنیم.

دستورات زیر جهت config روترهای صفر و یک بکار میروند:

```
Router0(config)#router ospf 1

Router0(config-router)#network 192.168.1.0 0.0.0.63 area 0

Router0(config-router)#network 192.168.1.128 0.0.0.63 area 0

Router0(config-router)#end
```

```
Router0(config)#router ospf 1

Router0(config-router)#log-adjacency-changes

Router0(config-router)#end

Router1(config)#router ospf 1

Router1(config-router)#network 192.168.1.64 0.0.0.63 area 0

Router1(config-router)#network 192.168.1.128 0.0.0.63 area 0

Router1(config-router)#end

Router1(config)#router ospf 1

Router1(config-router)#log-adjacency-changes

Router1(config-router)#end
```

سناریو:

حال که با مفهوم روتینگ و پروتکل های RIP و OSPF آشنا شدید مثال جلسه قبل را با این پروتکل ها پیاده سازی نمایید.