www.Prozhe.com

www.Prozhe.com

www.Prozhe.com

بسم الله الرحمن الرحیم

www.Prozhe.com

www.Prozhe.com

موسسه آموزش عالی جهاد دانشگاهی

استان اصفهان

پیاده سازی پروتکل های مسیریابی و امنیت در پروتکل های مسیریابی

پروژه دوره کارشناسی

در رشته کامپیوتر گرایش نرم افزار

توسط:

محسن مقصودی فر

استاد راهنما:

مهندس محمدرضا مصلحی

تیرماه 1392

www.Prozhe.com

www.Prozhe.com

پیشگفتار:

امروزه شبکه های کامپیوتری به قدری پیشرفت کرده اند که از چندین هزار شبکه کوچک تشکیل شده است. برای برقراری ارتباط بین این شبکه ها به یک ستون فقرات (backbone) نیازمند می باشیم. Backbone از وسایل زیادی تشکیل شده از جمله routerمی باشد که وظیفه انتقال اطلاعات را دارد. به دلیل اهمیتی که تکنیک ارسال و دریافت پیام از یک نقطه به نقطه دیگر دارد روش های مختلف انجام این کار را بررسی می کنیم و در نهایت بهترین روش را با توجه به مقیاس شبکه و هزینه ها معرفی نموده و امنیت در هر روش را مورد بررسی قرار میدهیم.

هدف از انجام این پروژه تحلیل و چگونگی کار پروتکل های مسیر یابی ،پیاده سازی پروتکل ها و در نهایت بررسی امنیت در هر یک از پروتکل ها می باشد.

توضیحات درباره فصل های این پروژه به شرح زیر است:

- فصل اول، تعریف کلی از مسیریاب و کاربرد آن در شبکه های کامپیوتری ، الگوریتم های مسیر یابی و نحو مسیریابی پروتکل های هرکدام توضیح داده شده است.
- فصل دوم، نحوه پیاده سازی پروتکل های توضیح داده شده در روتر و مثال هایی برای هرکدام انجام می دهیم.
- فصل سوم، امنیت در هریک از پروتکل های مسیر یابی جهت تبادل اطلاعات مطمئن بین روترها بررسی می شود و با مثال هایی طریقه تنظیم امنیت در آن ها را انجام می دهیم.

www.Prozhe.com

www.Prozhe.com

فهرست مطالب

عنوا ن **صفحه**

فصل اول مسیریابی بسته های IP..... 1

1-1 مسیریاب(Router):..... 1

2-1 مفهوم مسیریابی(Routing):..... 2

3-1 مقایسه مسیریابی در روتر با مسیر یابی در سوئیچ:..... 2

4-1 انواع پروتکل: 3

5-1 انواع Routeها: 3

6-1 Autonomous systems: 3

7-1 Administrative Distance: 4

8-1 Metrics: 5

9-1 Convergence Time: 6

10-1 Dynamic Route:..... 6

1-10-1 پروتکل های Distance Vector: 6

2-10-1 خواص کلی Distance Vector:..... 7

3-10-1 مشکلات مربوط به پروتکل های Distance Vector: 7

4-10-1 پروتکل های Link State: 9

5-10-1 مزیت پروتکل های Link State:..... 10

6-10-1 معایب استفاده از پروتکل های Link State:..... 10

7-10-1 پروتکل Hybrid:..... 11

فصل دوم پیاده سازی پروتکل های مسیریابی 12

1-2 Static Route: 12

1-1-2 پیکربندی Static Route:..... 12

www.Prozhe.com

www.Prozhe.com

2-2 پروتکل RIP(Routing Information Protocol): 16
2-2-1 مقایسه RIPv1 با RIPv2 : 17
2-2-2 پیاده سازی پروتکل RIPv1: 18
2-2-3 پیاده سازی پروتکل RIPv2: 21
2-2-4 عیب یابی RIP: 22
2-3 پروتکل OSPF(Open Shortest Path First): 22
2-3-1 کنترل حوزه نفوذ Update در OSPF: 23
2-3-2 انواع روتر در پروتکل OSPF: 23
2-3-3 پیدا کردن روترهای همسایه (Neighbors): 24
2-3-4 DR(Designated Router) و BDR(Backup Designated Router): 25
2-3-5 پیاده سازی پروتکل OSPF: 26
2-3-6 عیب یابی OSPF: 28
2-4 پروتکل EIGRP(Enhanced Interior Gateway Routing Protocol): 28
2-4-1 تشکیل همسایگی در پروتکل EIGRP 30
2-4-2پیاده سازی EIGRP: 31
2-4-3 عیب یابی EIGRP: 33
فصل سوم امنیت در پروتکل های مسیریابی 34
3-1 امنیت: 34
3-2 تائید هویت روتر همسایه (Neighbor Router Authentication): 35
3-3 پروتکل هایی که از Neighbor Authentication پشتیبانی می کنند: 35
3-4 چه زمانی Neighbor Authentication باید تنظیم شود؟ 35
3-5 Neighbor Authentication چگونه کار می کند؟ 36
3-5-1 Plain Text Authentication: 36
3-5-2 MD5 Authentication: 37
3-6 مدیریت زنجیره کلید(Key Chains): 37

www.Prozhe.com

www.Prozhe.com

3-7 Authentication در پروتکل RIPv2: 39
3-7-1 فعال سازی Authentication در پروتکل RIPv2: 40
3-8 فعال سازی Authentication در پروتکل EIGRP: 45
3-9 فعال سازی Authentication در پروتکل OSPF: 49

www.Prozhe.com

www.Prozhe.com

فهرست شکل ها و جدول ها

عنوا ن **صفحه**

جدول 1- 1 5
جدول 1- 2 5
شکل 1- 1 7
شکل 2- 1 13
شکل 2- 2 18
شکل 2- 3 19
شکل 2- 4 20
شکل 2- 5 27
شکل 2- 6 32
شکل 3- 1 39
شکل 3- 2 41
شکل 3- 3 45
شکل 3- 4 51

www.Prozhe.com

www.Prozhe.com

چکیده:

وظیفه مسیریاب ها انتقال اطلاعات می باشد. برای اینکه مسیریاب ها بتوانند بهترین مسیر را برای انتقال اطلاعات انتخاب کنند باید الگوریتم هایی اجرا شود تا از این طریق بهترین مسیر انتخاب شود. مجموعه مطالبی که در اختیار شما خواننده گرامی است پژوهشی در رابطه با مسیریابی در شبکه های جهانی اینترنت و بررسی الگوریتم های مسیریابی متفاوت ،تجزیه و تحلیل،نحوه پیاده سازی این الگوریتم ها ، بررسی امنیت در پروتکل های مسیر یابی و نحوه تنظیم امنیت در پروتکل های روتر می باشد.

www.Prozhe.com

www.Prozhe.com

فصل اول

مسیریابی بسته های IP

1-1 مسیریاب (Router) :

ارتباطات ما بین شبکه های LAN از طریق روتر(router) ایجاد می شود. روتر ابزاری است که ارتباطات را در سطح WAN برقرار می کند. روترها با استفاده از پروتکل های Routing بهترین مسیر ممکن برای دستیابی به مقصد را تشخیص داده و از راه Interface مربوطه، پیام را ارسال خواهند نمود.

وظایف اصلی روتر شامل موارد زیر می باشد:

- یافتن مسیر لایه سوم از یک دستگاه به یک مقصد مشخص.
- انتقال پیام ها از یک Interface به Interface دیگر به منظور هدایت آنها به مقاصد مربوطه.

درمورد وظیفه اول، روترها کارهای زیر را انجام خواهند داد:

- اطلاع در مورد روتر های دیگر متصل به شبکه و همچنین شبکه هایی که روترهای فوق با آنها در تماس می باشند.
- یافتن محل های قرارگیری روترهای مقصد
- یافتن بهترین مسیر برای دستیابی به مقصد
- ایجاد جدول Routing و به روز نگه داشتن همیشگی اطلاعات مربوطه در مورد مسیرهای ممکن برای مقاصد مختلف

برای انجام دادن وظیفه دوم، روترها باید آدرس گیرنده موجود در پیام ها را با موارد موجود در جدول Routing مقایسه کرده و Interface مربوطه را برای ارسال ترافیک مشخص کنند.

www.Prozhe.com

www.Prozhe.com

2-1 مفهوم مسیریابی(Routing):

مسیریابی فرآیندی مبتنی بر یکسری قواعد منطقی و سیاستهاست که پیچیدگی آن به سطوح و لایه های امنیت، امکان پشتیبانی همزمان از دو یا چند پروتکل و پیچیدگی ساختار و توپولوژی شبکه بستگی دارد.

انتقال داده از یک شبکه به شبکه دیگر وقتی که تنها یک مسیر واحد بین آن دو شبکه وجود دارد ساده ترین فرآیند مسیریابی است اما زمانی که بین دو شبکه چندین مسیر وجود دارد، مکانیزم پیدا کردن بهترین مسیر و همچنین اعمال معیارهای بهینگی مسیر، به الگوریتم های پویا نیاز دارد.

3-1 مقایسه مسیریابی در روتر با مسیریابی در سوئیچ:

1) روتر با توجه به آدرس مقصد و جدول مسیریابی(Routing-Table) مسیریابی میکند.
2) Routing-Table برخلاف MAC-Address-Table، به صورت اتوماتیک ایجاد نمیشود بلکه باید به صورت Static و یا توسط یکی از پروتکل های مسیریابی ایجاد شود.
3) ایجاد مسیر در جدول مسیریابی روترها، مستقل از ارسال داده می باشد. به عبارت دیگر مسیرها باید قبل از ارسال داده به صورت Static و یا توسط هریک از پروتکل های مسیریابی ایجاد شده باشد. در روترها سربار ترافیکی برای ایجاد مسیر وجود دارد.
4) روتر، مسیر Subnetهای شبکه را یاد می گیرد اما سوئیچ، مسیر تک تک نود های انتهایی را یاد می گیرد. به عبارت دیگر همه کامپیوتر های یک شبکه از یک Subnet آدرس دهی مشترک استفاده می کنند، لذا روتر نیاز دارد تا آدرس همه کامپیوتر های شبکه را یاد یگیرد. در ضمن این روش، قابلیت مسیریابی در مقیاس های بزرگ مانند اینترنت را نیز فراهم می کند. امکان مسیریابی با مکانیزم سوئیچ مسیر همه کامپیوترها را یاد می گیرد و ظرفیت حافظه و پردازش، متناسب با مقیاس اینترنت در هیچ سوئیچی وجود ندارد.
5) روتر برخلاف سوئیچ، اگر مسیر بسته دریافتی را بلد نباشد، آن را Discard می کند(دور می اندازد) و Broadcast نمی کند.
6) نکته جالب در خصوص مقایسه مسیریابی سوییچ و روتر، زمان مسیر یابی است.در سوییچ، MAC در MAC-Address-Table منحصر بفرد است و می تواند به عنوان index در MAC-Address-Table مورد استفاده قرار می گیرد.زمان پیدا کردن مسیر خروجی در جدولMAC-Address-Table، O(1) است. در حالی که در روتر، زمان مسیریابی ممکن است بالاتر باشد.

www.Prozhe.com

www.Prozhe.com

4-1 انواع پروتکل:

در لایه network دو نوع پروتکل یکی Routed Protocol و دیگری Routing Protocol وجود دارد. اصطلاح Routing protocols اشاره به پروتکل های RIP، IGRP، OSPF، EIGRP، BGP، IS-IS دارد که برای انتخاب بهترین مسیر در شبکه ها مورد استفاده قرار میگیرند. اما اصطلاح Routed protocols اشاره به پروتکل ها IP، IPX، Apple Talk دارد که به طور کلی نوع ارسال و دریافت پیام ها را تعیین کرده و طرز آدرس دهی شبکه را تعیین می نماید. هریک از پروتکل های Routed از تعدادی پروتکل Routing برای انجام وظایف خود بهره می گیرند.

5-1 انواع Routeها:

- Static
- Dynamic

یک Static Route، به صورت دستی روی دستگاه ایجاد می شود. بعبارتی روتر با بررسی Interfaceهای فعال آدرس شبکه های متصل به آنها، جدول Routing خود را تکمیل کرده و یا اینکه خود اقدام به وارد کردن آدرس مربوطه به شبکه های مقصد در داخل جدول Routing نمود.

Dynamic Route به وسیله پروتکل های Routing ایجاد می شود. پروتکل های Dynamic اینکار را با جمع آوری اطلاعاتی که در روتر های همسایه نیز به وسیله همان پروتکل ها بدست آمده، انجام خواهند داد. این پروتکل ها اطلاعات جداول Routing را که شامل آدرس های شبکه های مختلف متصل به Interfaceهای آنها می باشد را با روترهای دیگر در اشتراک گذاشته و باعث تکمیل تر شدن محتویات جدول Routing می گردند. نتیجه اینکار این است که همه روترهای شبکه در مورد همه مقاصد موجود و راههای مختلف دستیابی به آنها آگاهی کامل پیدا خواهند نمود.

6-1 Autonomous systems:

به محدوده ای از شبکه که تحت مدیریت مستقل قرار داشته باشد، AS گفته می شود.

اصطلاح IGP یا Interior Gateway Protocols اشاره به پروتکل هایی دارد که عمل Routing را در یک AS انجام می دهند.پروتکل های RIP،IGRP،OSPF،EIGRP جزو این دسته از پروتکل ها می باشند.

www.Prozhe.com

www.Prozhe.com

اصطلاح EGP یا Exterior Gateway Protocols اشاره به پروتکل هایی دارد که عمل Routing را بین چند AS انجام میدهند. امروزه پروتکل BGP یا Border Gateway Protocols جزو این دسته محسوب میشود.

برای مشخص کردن یک AS می توان آنها را به وسیله اعداد 0 الی 65535 شماره گذاری کرد.دو نوع شماره AS وجود دارد:

- Private
- Public

اگر به به محیط اینترنت که به وسیله پروتکلBGP اداره می شود دسترسی داشته باشید و بخواهید که Routeهای پروتکل BGP اینترنت را دریافت کنید، نیاز به استفاده از شماره های نوع Public خواهید داشت. اما در صورتی که شبکه داخلی خود را به چند AS مختلف تقسیم نمائید، نیاز به استفاده از شماره های Private دارید.

7-1 Administrative Distance:

روترها بهترین مسیر را برای رسیدن به مقصد انتخاب میکنند بنابراین در مواقعی که برای رسیدن به یک مقصد، اطلاعات مربوط به منابع مختلفی مورد استفاده قرار می گیرد مانند Static Route،Connected Route، یا پروتکل های Routing که روتر از بین منابع مختلف، فقط اطلاعات یک منبع را بکار می گیرد.

Administrative Distance یک روش اختصاصی سیسکو برای رتبه بندی پروتکل های و منابع Routing می باشد. برای مثال اگر در روتر دو پروتکل بطور همزمان اجرا شوند و هردو پروتکل نیز یک Route مشابه را دریافت کنند، روتر مجبور خواهد بود از یکی از این دو پروتکل استفاده کند.Administrative Distance به روتر می فهماند که کدام یک از پروتکل ها قابل اعتمادتر هستند.

پارامتر Administrative Distance عددی در رنج صفر تا 255 به هریک از پروتکل ها اختصاص داده که عدد کوچکتر نشان دهنده قابل اعتمادتر بودن پروتکل می باشد. که به صورت جدول زیر می باشد.

www.Prozhe.com

www.Prozhe.com

جدول 1-1 : Administrative distance

Administrative distance	Route Source
0	connected interface
1	Static Route
90	EIGRP
100	IGRP
110	OSPF
120	RIP

1-8 Metrics:

اگر روتر یک Route یکسان را از طریق دو منبع متفاوت، دریافت نماید، روتر برحسب مقدار Administrative Distance فقط یکی از Route ها را انتخاب خواهد کرد. اما در مواقعی که دو مسیر از یک منبع یکسان به مقصدی وجود داشته باشد، در این وضعیت از واحدی بنام Metric برای انتخاب یک Route استفاده می شود.

برخی پروتکل ها از یک Metric استفاده کرده، در حالی که برخی دیگر از مجموع چند Metric برای یافتن بهترین مسیر برای رسیدن به مقصد استفاده می کنند. جدول زیر Metric هایی که هریک از پروتکل های Routingاستفاده می کنند را نشان می دهد.

جدول 1-2 : Metrics

Metric	Routing Protocol	توضیحات
Bandwidth	EIGRP,IGRP	ظرفیت انتقال اطلاعات از طریق ارتباط،برحسب کیلوبایت بر ثانیه
Cost	OSPF	برعکس مقدار Bandwidth
Delay	EIGRP,IGRP	مدت زمان دسترسی به مقصد
Hop count	RIP	تعداد روترهایی که برای رسیدن به مقصد وجود دارد
Load	EIGRP,IGRP	مسیری که کمترین استفاده را دارد
Maximum Transmission Unit(MTU)	EIGRP,IGRP	مسیری که توانایی ارسال پیام هایی با بزرگترین ااندازه را دارد
Reliability	EIGRP,IGRP	مسیری که دارای کمترین مقدار خطاها باشد

www.Prozhe.com

www.Prozhe.com

1-9 Convergence Time:

Convergence مدت زمانی است که کل روترهای شبکه برای بدست آوردن اطلاعات مربوط به توپولوژی تمامی شبکه صرف می کنند. یعنی مدت زمانی که طول می کشد تا هر روتر کل شبکه را ببیند. این مدت زمان در پروتکل های Distance Vector بیشتر و در نتیجه همگرایی شبکه آهسته تر و در پروتکل های Link State این مدت زمان کمتر و در نتیجه همگرایی شبکه سریعتر است. بدیهی است مدت زمانی که یک شبکه به همگرایی می رسد بسیار حائز اهمیت بوده و کند بودن این فرآیند می تواند پیامدهای نامطلوبی را برای شبکه به دنبال داشته باشد.

1-10 Dynamic Route:

برخلاف Static Route که محل قرار گرفتن دستگاه گیرنده را به صورت دستی در روی روتر تنظیم می کردیم، پروتکل هایی که عمل Routing را انجام می دهند،محل قرارگیری مقاصد مختلف شبکه را با کمک اطلاعات موجود در روترهای همسایه درخواهند یافت. سه نوع پروتکل های Dynamic وجود دارد:

- Distance Vector
- Link State
- Hybrid

هریک از انواع بالا، روش متفاوتی برای یافتن بهترین مسیر تا مقصد و به اشتراک گذاشتن اطلاعات با روتر های همسایه در پیش می گیرند.

1-10-1 پروتکل های Distance Vector:

پروتکل های Distance Vector ساده ترین نوع پروتکل می باشد. این پروتکل ها برای محاسبه بهترین مسیر تا مقصد از الگوریتمی بنام Bellman-Ford استفاده می کنند.در این پروتکل ها اطلاعاتی که یک روتر دریافت می کند، از روترهای همسایه و آنها نیز به نوبه خود از روترهای همسایه خودشان دریافت می کنند و برای ارسال Update هایش از پیغام های BroadCast استفاده می کند. پروتکل های این دسته IGRP،RIP می باشد.

www.Prozhe.com

www.Prozhe.com

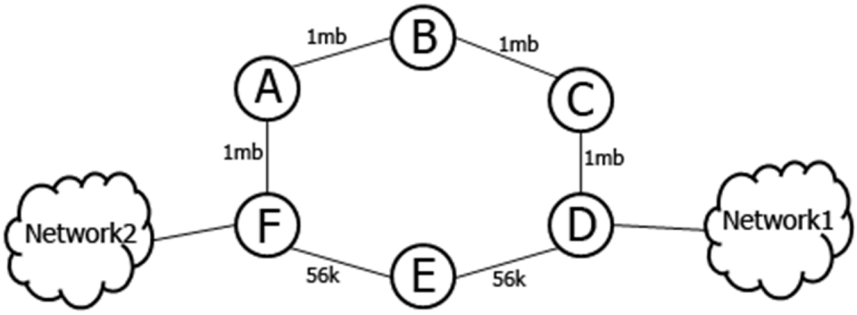
1-10-2 خواص کلی Distance Vector:

- پروتکل Distance Vector در update های خود Subnet Musk حمل نمی کند در نتیجه Classfull است.
- Full Update می باشد.

Full Update: در شبکه اگر تغییری رخ دهد همه تغییرات را ارسال می کند. به این صورت که تمام شبکه هایی که دارد را اعلام می کند.

Incremental Update: اگر در شبکه تغییری رخ دهد فقط تغییرات را ارسال می کند. برای مثال اگر شبکه ای به روتر اضافه یاکم شود، تغیرات را اعلام می کند.

- این پروتکل ها سبک هستند و به روتر فشار نمی آورند(RAM و CPU کمی دارند).
- دید به توپولوژی Information شبکه ندارند. به شکل زیر توجه کنید:



شکل 1-1: مثالی از توپولوژی Information

دو مسیر برای دو شبکه وجود دارد، مسیر d-c-b-a-f و مسیر d-e-f .

پروتکل های Distance Vector از مسیر دوم استفاده می کنند چون تعداد روتر کمتری سر راه دارند اما در صورتی که مسیر اول با سرعت بیشتر میتوان به Network2 رسید.

1-10-3 مشکلات مربوط به پروتکل های Distance Vector:

مشکل اول: زمان همگرایی(Convergence)

www.Prozhe.com

www.Prozhe.com

همانطور که قبلا گفته شد زمان همگرایی در این پروتکل ها بیشتر در نتیجه همگرایی شبکه آهسته تر است.

مشکل دوم:Loop یا چرخه لایه سوم

راه حل ها برای حل این مشکل:

محدود کردن Hop count

یکی از روش های حل مشکل شمارش نامحدود، تعریف یک حداکثر برای تعداد hopاست . پروتکل های روتینگ Distance-Vector نظیر RIP صرفا امکان افزایش تعداد hop را تا ۱۵ فراهم می نمایند . بنابراین هر چیزی که نیازمند ۱۶ hop باشد به منزله غیرقابل دسترس بودن تلقی می گردد.
بنابراین شمارش حداکثر تعداد hop ، باعث پیشگیری از گرفتار شدن بسته های اطلاعاتی در حلقه های تکرار می گردد . روش فوق با این که راه حلی قابل اعمال در شبکه است ولی قادر به حذف حلقه های روتینگ در شبکه نمی باشد و بسته های اطلاعاتی همچنان در حلقه های روتینگ گرفتار خواهند شد . ولی در مقابل این که بسته های اطلاعاتی بدون نظارت ، کنترل و بررسی در طول شبکه حرکت کنند ، حداکثر مسافتی را طی نموده و سپس از بین خواهند رفت.

Split Horizon

یکی دیگر از راه حل های برخورد با مشکل حلقه های روتینگ ، Split Horizon است. در این روش که کاهش اطلاعات نادرست و حجم عملیاتی اضافه روتینگ در یک شبکه Distance-Vector را به دنبال دارد از این اصل تبعیت می شود که اطلاعات نمی توانند در مسیری که از طریق آن دریافت شده اند مجددا ارسال گردند . به عبارت دیگر پروتکل روتینگ ، اینترفیسی را که از طریق آن بسته اطلاعاتی را دریافت کرده است بخاطر سپرده و از اینترفیس فوق برای ارسال مجدد آن استفاده نخواهد کرد.
بدین ترتیب ، روتر A از ارسال اطلاعات بهنگام شده ای که از طریق روتر B دریافت نموده است برای روتر B منع می شود.

Route poisoning

یکی دیگر از روش هایی که باعث پیشگیری از اطلاعات بهنگام شده متناقض و توقف حلقه های روتینگ می گردد ، route poisoning نامیده می شود . مثلازمانی که شبکه شماره۵ با مشکل مواجه می گردد، روتر E یک سطر را در جدول روتنیگ خود برای شبکه شماره ۵ با مقدار hop شانزده (غیرقابل دسترس بودن شبکه) درج می نماید.
با نادرست اعلام کردن مسیر رسیدن به شبکه شماره ۵ ، روتر C از بهنگام سازی اطلاعات جدول روتینگ خود

www.Prozhe.com

www.Prozhe.com

مبنی بر وجود یک مسیر برای رسیدن به شبکه شماره ۵ پیشگیری می نماید .زمانی که روتر C یک route poisoningرا از طریق روتر E دریافت می نماید ، یک poison reverse را برای روتر E ارسال می نماید تا این اطمینان ایجاد گردد که تمامی روترهای موجود در سگمنت اطلاعات مربوط به route poisoning را دریافت نموده اند.

Route poisoningو Split Horizon یک شبکه distance-vector با قابلیت اطمینان و اعتماد بیشتر را ایجاد می نمایند که در آن از بروز حلقه های تکرار پیشگیری می گردد.

Hold Down

با استفاده از hold down پیشگیری لازم در خصوص بهنگام سازی اطلاعات یک مسیر بی ثبات ، انجام می شود . با استفاده از hold down از ثبت مسیرهائی که وضعیت آنها با سرعت زیاد تغییر پیدا می نماید ، پیشگیری بعمل آمده و به آنها یک فرصت زمانی داده می شود تا وضعیت پایداری پیدا نمایند.بدین ترتیب ، به روترها اعلام می شود که برای یک بازه زمانی خاص هر گونه تغییراتی که بر روی مسیرهای حذف شده اخیر تاثیر می گذارد را محدود نمایند . با این کار از درج مسیرهای بی ثبات در سایر جداول روتینگ پیشگیری بعمل می آید.

زمانی که یک روتر اطلاعات بهنگام شده ای را از طریق یکی از همسایگان مبنی بر غیرقابل دسترس بودن یک شبکه دریافت می نماید (شبکه ای که تا پیش از این فعال بوده است) ، تایمر hold down آغاز به کار می کند . در صورتی که اطلاعات بهنگام شده جدیدی از یک همسایه دریافت شود که دارای متریک بهتری نسبت به وضعیت اولیه موجود در جدول روتینگ باشد ، hold downبرداشته شده و داده عبور داده می شود ولی اگر اطلاعات بهنگام شده ای از یک روتر همسایه دریافت گردد (قبل از اتمام مدت زمان تایمر) hold down ، که دارای متریک برابر و یا کمتر از مسیر قبلی باشد ، از اطلاعات جدید بهنگام صرفنظر و تایمر به فعالیت خود ادامه خواهد داد . بدین ترتیب زمان بیشتری برای ایجاد ثبات در شبکه قبل از آغاز فرآیند همگرائی آن فراهم می گردد.

4-10-1 پروتکل های Link State:

پروتکل های Link-State، روش دیگری را برای پیاده سازی مسیریابی به کار می برند تا بتوانند هم در انتخاب بهترین مسیر و هم در زمان همگرایی موثرتر باشد. این پروتکل ها Updateهایش را به صورت Multicast ارسال می کند و از الگوریتم Shortest Path File که توسط آقای Dijkstra ارائه شده است برای یافتن بهترین مسیر تا مقصد استفاده می کنند. در حالی که پروتکل های Distance Vector

www.Prozhe.com

www.Prozhe.com

از اطلاعات موجود در روترهای همسایه برای تکمیل کردن جدول Routing استفاده می کند. در این پروتکل ها هر روتر وضعیت لینک های متصل به خود را به کلیه روتر های AS ارسال می کند. برخلاف Distance Vector که هر روتر تنها تا روتر های همسایه را می بیند در Link-State هرروتر، اطلاعات لینک های متصل به کلیه روترهای شبکه را یاد می گیرد و با قرار دادن این اطلاعات در کنار هم، جزئیات توپولوژی شبکه را بدست می آورند وآنها در جدول دیتابیس (Database Table) نگهداری می کند.

به عبارت دیگر پروتکل های Link State کل توپولوژی شبکه و اینکه چه دستگاهی با کدام دستگاه دیگر ارتباط دارد را به یکباره در شروع کار بدست می آورند. پروتکل IS-IS،OSPF جزو این دسته می باشند.

1-10-5 مزیت پروتکل های Link State:

- این پروتکل ها قادر به محدود کردن مناطق تحت پوشش می باشد. در پروتکل های Distance Vector هر تغییری در هر قسمتی از شبکه ، بقیه قسمت های شبکه را تحت تاثیر قرار می دهد. اما در پروتکل های Link State می توان محدوده ای را که تحت تاثیر قرار خواهد گرفت را مشخص نمود.
- استفاده از پیام های Multicast برخلاف Broadcast در این پروتکل ها همچنین در صورت بروز هر تغییری در شبکه، فقط قسمت های تغییر یافته منتقل خواهند شد(Incremental)
- پروتکل های Link State عمل Routing را در مورد آدرس های بدون کلاس نیز انجام می دهند(Classless)
- در این پروتکل ها Loop یا چرخه های لایه سوم در جدول Routing وارد نخواهد شد.
- ترافیک کم آن از دیگر مزایای این پروتکل ها می باشد.

1-10-6 معایب استفاده از پروتکل های Link State:

این پروتکل ها باعث مصرف شدن زیاد منابع شبکه مثل پردازنده وRAM می شوند. این پروتکل ها فقط زمانی عمل می کنند که پیام های متناوب Update را در بازه زمانی تعیین شده دریافت نمایند.

www.Prozhe.com

www.Prozhe.com

1-10-7 پروتکل Hybrid:

EIGRP پروتکل انحصاری شرکت CISCO می باشد وتنها روی روتر های کمپانی CISCO قابل اجرا است. این پروتکل، مبتنی بر روش Distance Vector است اما از ایده های Link-state نیز در آن بکار گرفته شده است. از آنجایی که این پروتکل از مزایای هر دو روش بهره برده است، روش Hybrid(ترکیبی) نیز گفته می شود.

www.Prozhe.com

www.Prozhe.com

فصل دوم

پیاده سازی پروتکل های مسیریابی

2-1 Static Route:

زمانی که یک آدرس در داخل جدول Routing اضافه میکنیم، در واقع یک Static Route را ایجاد کرده ایم. استفاده از این روش در شبکه هی کوچکتر عمومیت دارد. در شبکه های بزرگ استفاده از این روش پیچیده خواهد بود. زیرا روی تک تک روترهای موجود باید جداگانه اقدام به ایجاد آن Route ها نمائیم. انتخاب مسیرهای Static در شبکه های بزرگ انتخاب مناسبی نیست. در شبکه های بزرگ بهتر است از پروتکل های مسیریابی پویا استفاده شود که بطور خودکار مسیرهای بین مسیریاب ها را انجام دهد.

2-1-1 پیکربندی Static Route:

برای ایجاد یک Static Route یکی از دو دستور زیر را می توان مورد استفاده قرار داد:

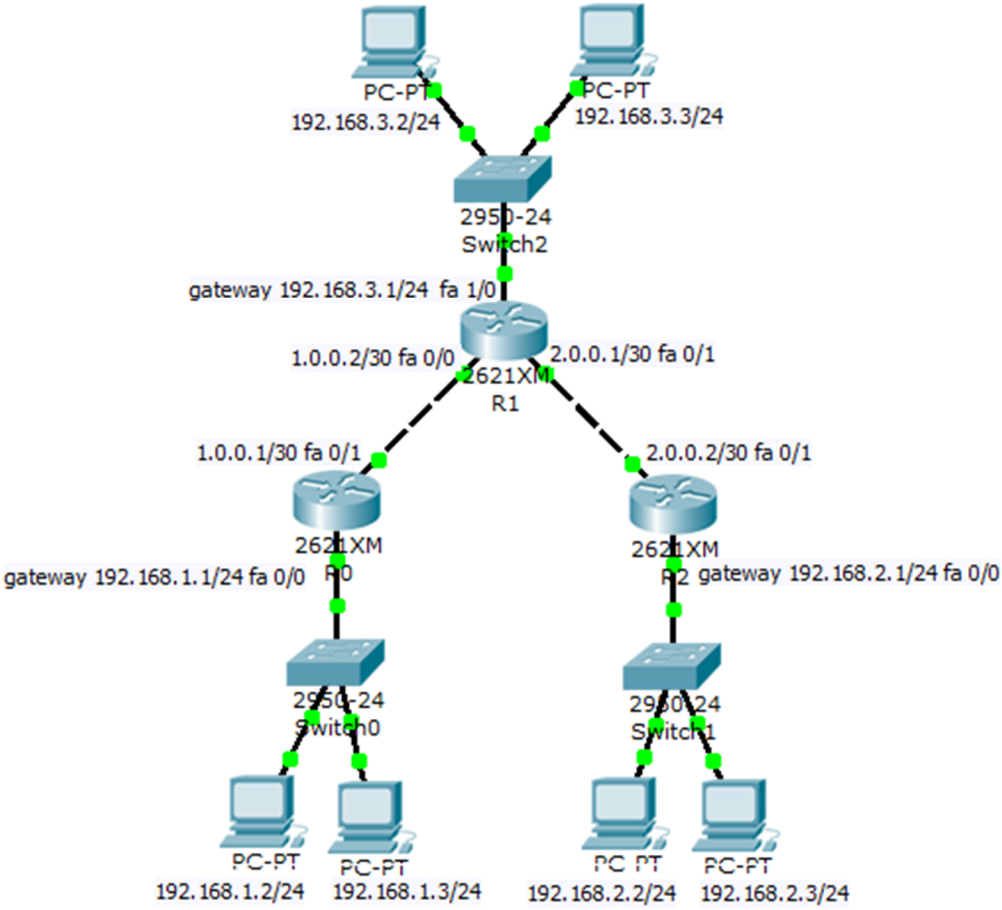
Router(config)# **ip route** *destination_network subnet_mask ip_address_next_hop*

Router(config)# **ip route** *destination_network subnet_mask interface_to_exit*

برای ایجاد جداول مسیریابی در روترهای یک شبکه، بهترین شیوه این است که به ازا هر مقصد که قرار است در شبکه دیده شود، مسیر آن در تمام روترهای شبکه ایجاد شود. برای مثال Static Route را در سناریو زیر پیکربندی می کنیم:

www.Prozhe.com

www.Prozhe.com



شکل 2-1: سناریو Static Route

برای پیکربندی Static Rout در این مثال مراحل زیر را انجام میدهیم:

1)در این مرحله به Interface های روتر IP می دهیم:

برای IPدادن به Interfaceهای روتر، به Interface مربوطه رفته و از دستور زیر استفاده میکنیم:

Router(config)#**ip address** *ip subnet_mask*

برای مثال روتر R1 را تنظیم میکنیم:

www.Prozhe.com

www.Prozhe.com

زمانی که روتر روشن میشود وارد user mode میشویم

Router>

برای وارد شدن به privilege mode دستور enable را وارد میکنیم

Router>enable

و برای وارد شدن به global mode دستور configuration terminal را وارد میکنیم

Router#configuration terminal

حال به Interface های روتر آدرس IP میدهیم

Router(config)#interface fastEhterner 0/0

Router(config-if)#ip address 1.0.0.2 255.255.255.252

سپس Interface را با دستور no shutdown فعال می کنیم

Router(config-if)#no shutdown

به همین ترتیب وارد تمام Interface های روترهای R0،R1 و R2 شده وبه آنها آدرس IP میدهیم سپس آنها را فعال میکنیم.

- ✓ نکته:هر روتر، مسیر مربوط به subnet های متصل به خود را(Connected) به صورت اتوماتیک در جدول مسیریابی ایجاد می نماید.برای دیدن جدول مسیریابی از دستور show ip route در محیط Enable استفاده میکنیم.

Router#show ip route

با زدن این دستور در روتر R1،جدول مسیر یابی به صورت زیر میباشد:

C 1.0.0.0 is directly connected, FastEthernet0/0

C 2.0.0.0 is directly connected, FastEthernet0/1

C 192.0.0.0/8 is directly connected, FastEthernet1/0

مسیرهای مربوط به subnet های متصل، با برچسب C نشان داده میشوند.

www.Prozhe.com

www.Prozhe.com

2)در این مرحله،در هر روتر به global mode وارد شده و دستورات لازم جهت مسیریابی به صورت Static را وارد می کنیم.

در روتر R0:

R0(config)# **ip route** 192.168.3.0 255.255.255.0 1.0.0.2

R0(config)# **ip route** 192.168.2.0 255.255.255.0 1.0.0.2

در روتر R1:

R1(config)# **ip route** 192.168.1.0 255.255.255.0 1.0.0.1

R1(config)# **ip route** 192.168.2.0 255.255.255.0 2.0.0.2

در روتر R2:

R2(config)# i**p route** 192.168.3.0 255.255.255.0 2.0.0.1

R2(config)# **ip route** 192.168.1.0 255.255.255.0 2.0.0.1

پیکربندی Static Route در این مثال به پایان رسید. مسیرهایی که به صورت Static ایجاد می شوند با برچسب S در جدول مسیریابی نشان داده می شوند.جدول مسیر یابی هر روتر به صورت زیر است:

جدول مسیریابی روتر R0:

is subnetted, 1 subnets 30/1.0.0.0

C 1.0.0.0 is directly connected, FastEthernet0/1

C 192.0.0.0/8 is directly connected, FastEthernet0/0

S 192.168.2.0/24 [1/0] via 1.0.0.2

S 192.168.3.0/24 [1/0] via 1.0.0.2

جدول مسیریابی در روتر R1:

is subnetted, 1 subnets 30/1.0.0.0

C 1.0.0.0 is directly connected, FastEthernet0/0

www.Prozhe.com

www.Prozhe.com

is subnetted, 1 subnets 30/2.0.0.0

C 2.0.0.0 is directly connected, FastEthernet0/1

C 192.0.0.0/8 is directly connected, FastEthernet1/0

S 192.168.1.0/24 [1/0] via 1.0.0.1

S 192.168.2.0/24 [1/0] via 2.0.0.2

جدول مسیریابی در روتر R2:

is subnetted, 1 subnets 30/2.0.0.0

C 2.0.0.0 is directly connected, FastEthernet0/1

C 192.0.0.0/8 is directly connected, FastEthernet0/0

S 192.168.1.0/24 [1/0] via 2.0.0.1

S 192.168.3.0/24 [1/0] via 2.0.0.1

2-2 پروتکل RIP(Routing Information Protocol):

RIP یک پروتکل distance-vector می باشد. پروتکل فوق در هر 30 ثانیه تمام اطلاعات موجود در جدول روتینگ را برای تمامی Interface های فعال ارسال می نماید. RIP صرفا از تعداد hop برای تعیین بهترین مسیر به شبکه راه دور استفاده می نماید .حداکثر تعداد hop می تواند عدد 15 را داشته باشد.

در این پروتکل Administrative Distance Number برابر با 120 می باشد ، زمان همگرایی بالایی دارد و دید به توپولوژی شبکه ندارد. به عبارت دیگر حوزه نفوذ Route Update تا روتر همسایه می باشد. RIP از سه نوع تایمر مختلف برای تنظیم کارآئی خود استفاده می نماید:

Router Update Timer:

فاصله زمانی ارسال یک نسخه کامل از اطلاعات بهنگام روتینگ را مشخص می نماید . در بازه زمانی فوق ، روتر یک نسخه کامل از اطلاعات موجود در جدول روتینگ خود را برای تمامی همسایگان ارسال می نماید . این زمان معمولا 30 ثانیه در نظر گرفته می شود.

www.Prozhe.com

www.Prozhe.com

:Router Invalid Timer

مدت زمانی را مشخص می نماید که پس از سپری شدن آن ، روتر به این نتیجه خواهید رسید که یک مسیر غیرمعتبر است . این زمان معمولا 180 ثانیه در نظر گرفته می شود و اگر یک روتر در بازه زمانی فوق هیچگونه اطلاعات جدیدی را در خصوص یک مسیر خاص دریافت ننماید ، آن مسیر را غیرمعتبر می نماید . در صورت تحقق چنین شرایطی ، روتر اقدام به ارسال اطلاعات بهنگام برای تمامی همسایگان خود می نماید تا به آنها بگوید که مسیر غیرمعتبر است.

:Router Flush Timer

مدت زمان بین غیرمعتبر اعلام شدن یک مسیر و حذف آن از جدول روتینگ را مشخص می نماید . این زمان معمولا 240 ثانیه در نظر گرفته می شود . قبل از این که یک مسیر از جدول روتینگ حذف گردد ، روتر این موضوع را به اطلاع همسایگان خود می رساند . مقدار Route invalid timer می بایست کمتر از route flush timerباشد تا روتر زمان کافی جهت اطلاع به همسایگان خود را قبل از بهنگام سازی جدول در اختیار داشته باشد.

RIPدر شبکه های کوچک به خوبی کار می کند ولی برای شبکه های بزرگ که دارای لینک های ارتباطی WAN و تعداد بسیار زیادی روتر هستند مناسب نمی باشد.

2-2-1 مقایسه RIPv1 با RIPv2 :

پروتکل RIP در دو نسخه می باشد که مهمترین تفاوت های RIPv1 با RIPv2 به صورت زیر است:

1) آدرس مقصد بسته های RIPv1،Broadcast(255.255.255.255)وآدرس مقصد بسته های RIPv2،Multicast(224.0.0.9)است.
2) در RIPv1،Subnet بدون Mask ارسال می شود بنابراین از روتینگ classful استفاده می گردد. اما در RIPv2 به همراه هر Subnet،Muskنیز ارسال می شود بنابراین روتینگ classless می باشد.
3) پروتکل RIPv2،امنیت از نوع Authentication را پشتیبانی می کند.بنابراین روتر، زمانی Route Updateهای دریافتی را می پذیرد که هویت ارسال کننده بسته های دریافتی تایید شود. جزئیات این بحث در فصل بعد مطرح می شود.

www.Prozhe.com

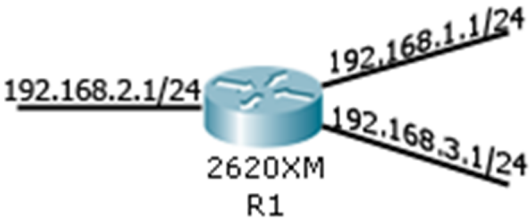
www.Prozhe.com

2-2-2 پیاده سازی پروتکل RIPv1:

برای پیاده سازی این پروتکل در یک شبکه باید دو مرحله زیر اجرا شود:

1) فعال کردن پروتکل RIP درهر روتر با دستور Router RIP
2) فعال کردن اینترفیس های متصل به روتر با دستور Network

در هنگام نوشتن آدرس های شبکه بعد از دستور Network، در هردوی پروتکل ها آدرس ها را باید به صورت کلاس استاندارد C،B،A نوشته شوند.



شکل 2-2: آدرس های شبکه

به عنوان مثال در شکل فوق اگر بخواهیم در روتر پروتکل RIP فعال کنیم از دستورات زیر استفاده میکنیم:

Router RIP

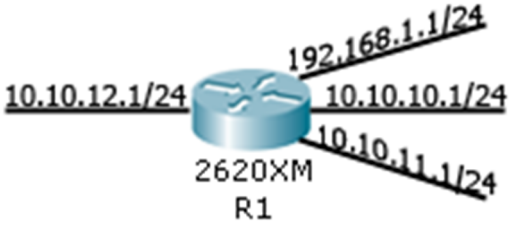
Network 192.168.1.0

Network 192.168.2.0

Network 192.168.3.0

www.Prozhe.com

www.Prozhe.com



شکل 2-3: آدرس های شبکه

و در شکل فوق برای فعال کردن Interface های روتر برای پیکربندی پروتکل RIP از دستور زیر استفاده میکنیم:

Router RIP

Network 192.168.1.0

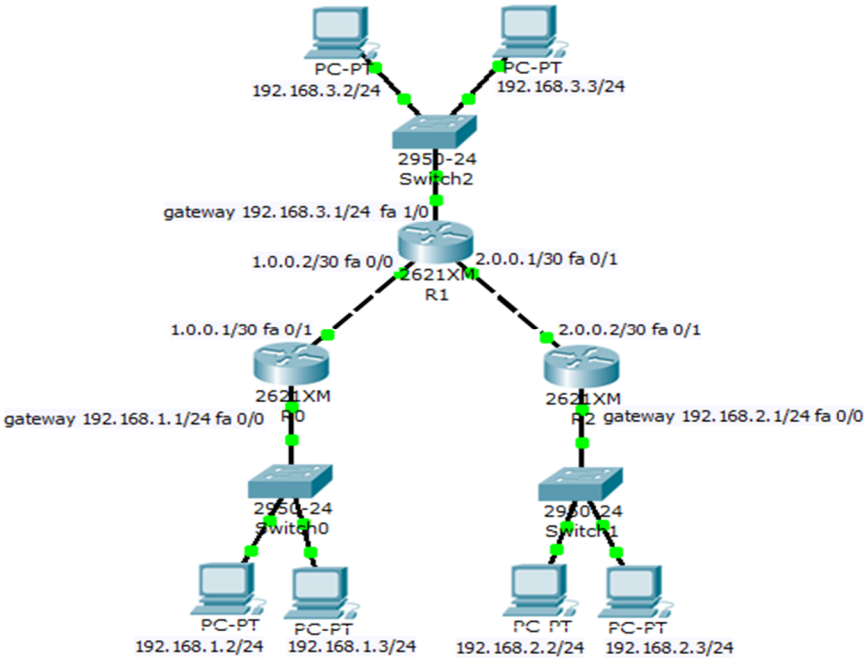
Network 10.0.0.0

دستور Network 10.0.0.0، هر Interface که آدرس IP آن در محدوده قرار دارد را فعال می کند.

برای مثال پروتکل RIP را در سناریوی زیر پیکربندی می کنیم:

www.Prozhe.com

www.Prozhe.com



شکل 4-2 : سناریو RIP

در روتر R0:

Router(config)# **router rip**

Router(config-router)# **network** 192.168.1.0

Router(config-router)# **network** 1.0.0.0

در روتر R1:

Router(config)# **router rip**

Router(config-router)# **network** 192.168.3.0

Router(config-router)# **network** 1.0.0.0

Router(config-router)# **network** 2.0.0.0

در روتر R2:

Router(config)# **router rip**

Router(config-router)# **network** 192.168.2.0

Router(config-router)# **network** 2.0.0.0

www.Prozhe.com

www.Prozhe.com

با فعال کردن این Interfaceها روی آن ها Route Update ارسال می گردد و پردازش می شوند.پروتکل RIP در جدول مسیریابی با برچسب R نمایش داده می شود.با دستور show ip route می توان جدول مسیر یابی را دید.

3-2-2 پیاده سازی پروتکل RIPv2:

برای پیاده سازی RIPv2 عینا همانند RIPv1 عمل می نمائیم با این تفاوت که نسخه آن را در روتر اعلام می کنیم و auto-summary را غیرفعال می کنیم.

- ✓ نکته: auto-summary در RIP فعال است. به این معنی که به طور پیش فرض classful روت می کند.

برای مثال در روتر R1 به صورت زیر است:

Router(config)# **router rip**

Router(config-router)# **version 2**

Router(config-router)# **no auto-summary**

Router(config-router)# **network** 192.168.3.0

Router(config-router)# **network** 1.0.0.0

Router(config-router)# **network** 2.0.0.0

- ✓ نکته:RIPv2 با RIPv1 سازگار نمی باشد. بدین معنی که اگر بعضی روترهای شبکه، RIPv2 را پشتیبانی نکنند، باید در روتر روی بعضی Interfaceها،RIPv1 و روی دیگر Interfaceها،RIPv2 اجرا نمود.

به طور کلی ما می توانیم روتر را برای انجام اعمال زیر تنظیم کنیم:

- استفاده از RIPv1 برای دریافت و ارسال پیام ها
- استفاده از RIPv2 برای دریافت و ارسال پیام ها

www.Prozhe.com

www.Prozhe.com

- ترکیب هردوی این پروتکل ها بسته به شرایط موجود در هنگام دریافت و ارسال پیام ها.بنابراین می توان مشخص نمود که هرکدام از Interfaceهای روتر از چه نسخه ای استفاده کنند:

Router(config)# **interface** *type [slot] port*

Router(config-router)# **ip rip send version 1 |version 2|**

Router(config)# **interface** *type [slot] port*

Router(config-router)# **ip rip receive version 1 |version 2|**

2-2-4 عیب یابی RIP:

بعد از تنظیم RIP از یکسری دستورات می توان برای عیب یابی استفاده کرد که در محیط Privilege EXEC اجرا می شوند:

- Show IP Route: هر روتر لیست بهترین مسیرها به مقاصد مختلف را در Routing Table خود نگه می دارد. با این دستور می توان جدول مسیریابی را مشاهده کرد.
- Show IP Protocol: این دستور تمامی پروتکل های فعال روی روتر را نشان می دهد.
- Debug IP RIP: این دستور تمامی Route های رسیده و ارسال شده از طریق یک Interface نمایش می دهد.

2-3 پروتکل OSPF(Open Shortest Path First):

OSPF به این دلیل که انحصاری محسوب نمی شود و هم اینکه بسیار سریع است یکی از پرکاربرد ترین پروتکل ها است. این پروتکل جزو پروتکل های مسیر یابی از نوع Link State محسوب می شود .مزایای این پروتکل به شرح زیر است:

این پروتکل بر اساس الگوریتم SPF باعث حذف چرخه های لایه سوم شده است ، با استفاده از پیام های LSA سرعت همگرایی شبکه را افزایش می دهد ، از نوع classless می باشد Incremental Update است ،در پیام های خود از Authentication پشتیبانی می کند و دید به توپولوژی شبکه دارد.نیاز به پردازش بیشتری

www.Prozhe.com

www.Prozhe.com

توسط پردازنده، اشغال منابع شبکه مانند حافظه RAM و پیکربندی و عیب یابی مشکل این پروتکل از معایب آن محسوب می شود.پروتکل OSPF از Cost به عنوان Metric بهره می برد.Cost عکس پرامتر Bandwidth یا پهنای باند در نظر گرفته می شود یعنی هر چقدر سرعت اتصال بیشتر باشد،میزان Cost کمتر خواهد بود و بلعکس.بهترین مسیر،مسیری است که کمترین میزان Costرا داشته باشد.

2-3-1 کنترل حوزه نفوذ Update در OSPF:

در OSPF برای کنترل Updateها از Area بندی استفاده می شود. درواقع به این دلیل از area ها استفاده میکنیم تا بتوانیم یک ASرا که ممکن است بسیار بزرگ باشد را به چند قسمت تقسیم کنیم و با این کار دیتابیس روتر های موجود در هر ناحیه کوچکتر شود -چون در پروتکل های از نوع Link State همه روتر ها باید یک جدول یکسان داشته باشند که در ان، جداول همه مسیر ها برای رسیدن هر روتری به هر روتر دیگر موجود هست- و با اینکار سرعت این پروتکل افزایش پیدا خواهد کرد، بار پردازشی روتر ها کمتر می شود و عیب یابی برای مدیر شبکه راحت تر خواهد شد.

- ✓ نکته: Area 0 حتما باید ساخته شود. اگر کلا یک Area داریم همه روتر ها باید در Area 0 باشند. به روتر هایی که در Area 0 قرار دارند، Backbone میگویند.

2-3-2 انواع روتر در پروتکل OSPF:

بر اساس طراحی انجام شده3 نوع روتر در این پروتکل وجود خواهند داشت.

1)روتر درون ناحیه ای Inter-Area Router:

این روتر ها همان روتر هایی هستند که همه Interface های آنها درون یک ناحیه قرار دارد و در واقع به طور کامل عضو یک ناحیه است.

2)روتر مرزی Area-Border Router:

این روتر ها روتر هایی هستند که وظیفه اتصال دو یا چند ناحیه به هم را بر عهده دارند و همانطور که قابل پیش بینی است تعدادی از اینترفیس های آنها در Area 0 و تعدادی دیگر در ناحیه های دیگر قرار دارند.

www.Prozhe.com

www.Prozhe.com

3)روتر بین ناحیه خود مختار Autonomous System Boundary Router:

این روتر ها همانند ABR ها هستند با این اختلاف که در واقع وظیفه ارتباز دو AS مختلف را بر عهده دارند. یعنی ممکن است همزمان دو پروتکل مسیر یابی مختلف را اجرا کنند.

2-3-3 پیدا کردن روترهای همسایه (Neighbors):

پیدا کردن همسایه به این صورت است که اگر در شبکه های نقطه به نقطه(یعنی شبکه هایی که 2 روتر مستقیم به هم اتصال دارند) و همچنین شبکه های پخش فراگیر(یعنی چند روتر که توسط یک سوئیچ به هم متصل هستند و تشکیل یک سگمنت را میدهند. در باره این شبکه، سگمنت و روتر های DR و BDR در ادامه صحبت خواهد شد)هر 10 ثانیه 1 بار بسته های Hello Packetارسال می گردد.اما در شبکه هایی که به لینک WAN اتصال دارند به عبارت دیگر به NBMA یا None Broadcast Multi Access معروف هستند این پیغام هر 30 ثانیه 1 بار ارسال می گردد. به این زمان ها Hello Interval می گویند.در این پروتکل Dead Interval،40 ثانیه است به این معنی که اگر تا 40 ثانیه Hello packetبهش نرسد آن لینک را حذف می کند.

با تبادل بسته های Hello Packet،هر روتر برای خود جدولی تشکیل می دهد به نام جدول همسایگی یا Neighborhood Table که این جدول اطلاعات مربوط به روتر هایی که مستقیم به روتر ما متصل هستند و همانند روتر ما پروتکل OSPF را اجرا کرده اند و آخرین زمان Hello را نگه داری میکند.بعد از مشخص شدن همسایه ها یک بستهLSA که حاوی همان Updateها می باشد به همسایه و غیر همسایه ارسال می شود وپس از دریافت LSA توسط هر روتر جدول توپولوژی شبکه یا Topology Table ساخته می شود.

Topology Table: در پروتکل Link State مثل OSPF در واقع کل Network و روتر ها و مسیر های ناحیه خودش را آنالیز می کند و از همه مسیر های ممکن برای رسیدن هر روتری به روتر دیگر یک جدول ایجاد می کند. و از انجایی که همه روتر های موجود در ناحیه همین کار را انجام می دهند پس همه آنها یک topology Table یکسان خواهند داشت. به عبارت دیگه هر روتری نقشه کامل Network در ناحیه خودش را دارد و می داند هر روتری چه اتصالاتی به روتر های دیگر دارد.

www.Prozhe.com

www.Prozhe.com

بعد از اینکه روتر به Topology Table دسترسی پیدا کرد،این جدول را در اختیار الگوریتمSPF قرار می دهد تا بهترین و بهینه ترین مسیر برای رسیدن روتر به Network های دیگر مشخص شود و این اطلاعات بدست امده در Routing Table ذخیره می شود.

روترهایی که از پروتکل OSPF استفاده می نمایند سه مرحله زیر را طی می کنند:

Down state: هیچ یک از روتر ها تا بحال عمل تبادل اطلاعات Routing را با دیگران انجام نداده است.

Init state:در این مرحله، روتر گیرنده پیام Hello مربوط به روتر فرستنده را دریافت کرده و آنها را در جدول Neighborخود وارد میکند.

Two-Way State:در این مرحله،روتر فرستنده جواب پیام ارسالی خود را از طرف روتر گیرنده دریافت کرده و آن را در جدول Neighbor خود ثبت می کند.

4-3-2 DR(Designated Router) و BDR(Backup Designated Router):

حالت خاصی از طراحی داخل ناحیه ای روتر ها حالتی است که روتر ها توسط یک سوئیچ به هم متصل باشند و تشکیل یک سگمنت را دهند. در این حالت در صورتی که ارتباط یکی از روتر ها با یکی از شبکه های خود قطع شود وظیفه دارد آنرا به همه اعلام کند. وقتی روتر های دیگر متصل به سوئیچ این پیام را دریافت کنند آنرا به همه روتر های دیگر دوباره ارسال خواهند کرد و این چرخه همچنان ادامه خواهد داشت و باعث به بن بست رسیدن شبکه خواهد شد.دلیل این امر این است که پس از دریافت هر آپدیت حاوی تغییر در شبکه، هر روتر باید الگوریتم SPF را اجرا کند تا مسیر های جایگزین را بیابد و این نیاز به پردازش بسیار و زمان دارد.
برای رفع این مشکل یک روتر به عنوام DR در بین این چند روتر با برگذاری یک انتخابات انتخاب خواهد شد و یک روتر هم به عنوان پشتیبان آن تا در صورت از کار افتادن آن وظیفه آن را به عهده بگیرد.BDR
این انتخابات بدین صورت است که هر روتر یک عدد به عنوان اولویت یا Priority دارد که هر روتری که اولویت بالاتری داشته باشد به عنوان DR و روتر با اولویت بعدی به عنوان BDR شناخته خواهد شد. اما به دلیل برابر بودن اولویت همه روتر ها به صورت پیش فرض، در صورت عدم تغییر آن به صورت دستی برای تعیید روتری خاص به عنوانDR ، روتری که Router-ID بالاتری داشته باشد به عنوان DR انتخاب خواهد شد.به این ترتیب در صورتی که تغییری در شبکه رخ دهد (یعنی اگر ارتباط جدیدی ایجاد شود یا روتری قطع شود) روتری که این تغییر را بیابد آنرا به جای پخش فراگیر به صورت پخش گروهی یا Multicast به

www.Prozhe.com

www.Prozhe.com

ادرس 224.0.0.6 (ادرس مربوط به DRو BDR) ارسال میکند. سپس DR پس از بررسی پیام رسیده، انرا به آدرس multicastمربوط به همه روتر ها یعنی 224.0.0.5 ارسال میکند و چون این پیغام MultiCast است دیگر هیچ روتری آنرا به روتر دیگر نخواهد فرستاد و بن بست بالا اتفاق نخواهد افتاد. پروتکل OSPF به منظور ارتباطات خود از MultiCastاستفاده می کند.

2-3-5 پیاده سازی پروتکل OSPF:

برای پیاده سازی باید مراحل زیر را انجام دهیم:

1) فعال کردن OSPF به همراه شماره Process ID.Process ID نیاز به یکسان بودن بین روترهای همسایه نیست.

Router(config)# **router ospf** *process_id*

2) مشخص کردن شناسه روتر در ناحیه. در حالت عادی و در صورت عدم وارد کردن این دستور، بر اساس قوانین زیر این شناشه تعیین می شود:

اگر اینترفیس loopback در روتر ست نشده باشد، بالاترین آدرس IP اینترفیس های فیزیکی موجود ،به عنوان شناسه تعیین خواهد شد.

اگر اینترفیس loopback در روتر ست شده باشد، بالاترین آدرس IP اینترفیس Loopbackایجاد شده در روتر بدون در نظر گرفتن IP اینترفیس های فیزیکی، به عنوان شناسه قرار خواهد گرفت.

Router(config-router)#**router-id** *IP_address*

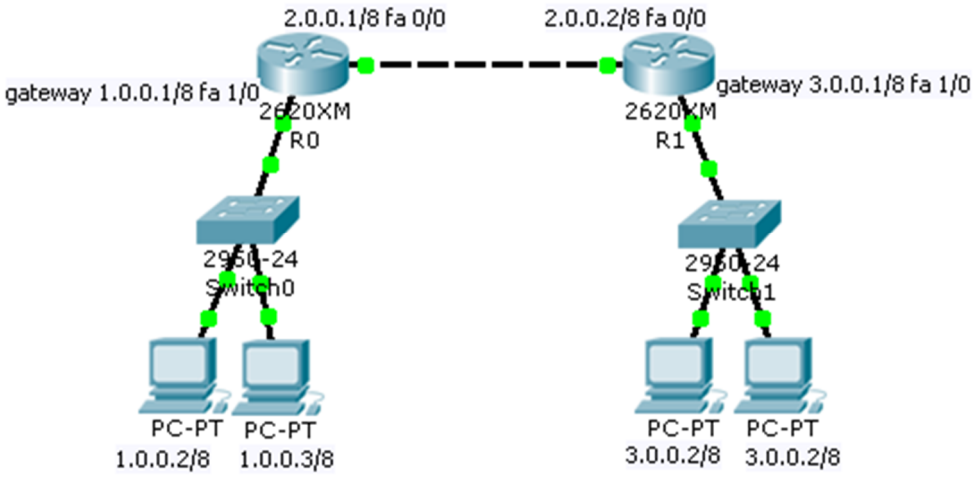
3) فعال کردن Interfaceهای متصل به روتر با دستور Network

Router (config-router) # **network** *IP_address wildcard_mask*

www.Prozhe.com

www.Prozhe.com

برای مثال در سناریوی زیر پروتکل OSPF را پیکربندی میکنیم:



شکل 2-5: سناریو OSPF

در روتر R0:

R0(config)# **router ospf** 10

R0(config-router)# **network** 1.0.0.1 0.0.0.255 area 0

R0(config-router)# **network** 2.0.0.1 0.0.0.255 area 0

در روتر R1:

R1(config)# **router ospf** 10

R1(config-router)# **network** 3.0.0.1 0.0.0.255 area 0

R1(config-router)# **network** 2.0.0.2 0.0.0.255 area 0

در جدول مسیریابی هر روتر،مسیر Subnetهایی که از طریق پروسه SPF یادگرفته می شود با برچسب O در جدول مسیریابی نشان داده می شود.به عبارت دیگر Subnetهای Area محلی، با برچسب O در جدول مسیریابی نشان داده می شود.مسیر Subnetهایی که به دیگرAreaها مربوط می شود با برچسب OIA و یا OSPF InterArea ،در جدول مسیریابی نشان داده می شود.مسیر Subnetهایی که به خارج از شبکه OSPf

www.Prozhe.com

www.Prozhe.com

مربوط می شود(مانند اینترنت و WAN)،با برچسب OE1 ویا OE2(OSPF External) در جدول مسیریابی نشان داده می شود.

در روتر های مرزی، مسیر Subnetهای مربوط به Area های متصل به روتر،با برچسب Oنشان داده می شود.زیرا جزئیات توپولوژی Areaهای متصل به روتر مرزی، در دیتابیس اصلی روتر مرزی قرار می گیرد.برای مثال جدول مسیر یابی در روتر R0 به صورت زیر است:

C 1.0.0.0/8 is directly connected, FastEthernet1/0

C 2.0.0.0/8 is directly connected, FastEthernet0/0

O 3.0.0.0/8 [110/2] via 2.0.0.2, 00:00:10, FastEthernet0/0

6-3-2 عیب یابی OSPF:

بعد از تنظیم OSPF از یکسری دستورات می توان برای عیب یابی استفاده کرد که در محیط Privilege EXEC اجرا می شوند:

- Show IP Route: هر روتر لیست بهترین مسیرها به مقاصد مختلف را در Routing Table خود نگه می دارد. با این دستور می توان جدول مسیریابی را مشاهده کرد.
- Show IP Protocol: این دستور تمامی پروتکل های فعال روی روتر را نشان می دهد.
- Show IP OSPF Interface: برای مشاهده این که کدام interface به کدام Area تعلق دارد و نیز کدام Interface به روترهای همسایه اتصال دارد.
- Show IP OSPF Neighbor: برای مشاهده تمامی روترهای همسایه.
- Debug IP OSPF adj: برای مشاهده تمامی مراحلی را که روتر برای انجام عمل مجاورت یا Adjacency طی می کند.
- Debug IP OSPF Events: با این دستور می توان از حوادث و یا Eventهایی که در Ospf اتفاق می افتد، آگاه شوید.
- Debug IP OSPF Packet: برای مشاهده محتویات پیام های LSA بکار می رود.

www.Prozhe.com

www.Prozhe.com

4-2 پروتکل EIGRP(Enhanced Interior Gateway Routing Protocol):

در پروتکل EIGRP،هردو روتر همسایه ابتدا تشکیل همسایگی می دهند.سپس هر روتر اطلاعات Subnetهایی را که دارند به همسایه هایش یاد می دهد.سپس هر روتر با استفاده از متریک بهترین مسیر را تشخیص داده وآن را در جدول مسیریابی قرار می دهد.اساس این پروتکل روش Distance Vector است اما بجای این که مسیر Subnetهایی که می داند به صورت دوره ای ارسال شود،تنها یکبار و به صورت مطمئن منتقل می شود.

این پروتکل همانند OSPF زمان همگرایی سریعی دارد و حتی سریع تر نیز می باشد و در عین حال پروتکل بسیار ساده ای است.برخلاف OSPF سنگین نمی باشد و در مقیاس های بزرگ مشکلی پیدا نمی کند. در واقع تنها نکته منفی در این پروتکل انحصاری بودنش هست و اینکه فقط تجهیزات سیسکو میتونن از این پروتکل استفاده کنند.

همه پروتکل ها برای اینکه بهترین مسیر رو انتخاب کنند،از نوعی الگوریتم استفاده میکنن که معمولاً زمان و هزینه پردازشی زیادی در بر دارند. مثلاً پروتکل OSPFبرای اینکه بهترین مسیر رو پیدا کنه د از الگوریتم SPFکه دایجکسترا اونو ارائه کرده استفاده میکند که یک الگوریتم بسیار سنگین و زمانبر هست. البته SPF همیشه اجرا نمیشه. بلکه فقط 1 بار اجرا میشه و بعد از پیدا شدن بهترین مسیر، اون مسیر در جدول Topology tableذخیره میشه و درصورت از کار افتادن اون مسیر باید دوباره OSPFبیاد برای پیدا کردن بهترین مسیر جایگرین از SPFاستفاده کنه.

اما پروتکل EIGRP از SPF استفاده نمی کند .در عوض از الگوریتم خود سیسکو به نام DUALیا Diffusing Update Algorithmاستفاده میکند که بسیار سریع و از نظر پردازشی کم هزینه هست. با این حال EIGRP از Backup routeهم پشتیبانی می کند. یعنی از DUALبرای پیدا کردن 2 تا از بهترین مسیرها استفاده میکنه و بهترین مسیر رو به عنوان مسیر پیش فرض و دومی رو به عنوان مسیر پشتیبان قرار میده تا بعد از از کار افتادن مسیر پیش فرض، بجای صرف زمان برای پیدا کردن دوباره بهترین مسیر، خیلی سریع از مسیر جایگرینی که توی جدول topology tableذخیره کرده استفاده کنه .EIGRP تنها پروتکلی هست که از Backup Route پشتیبانی میکند.

یکی از مزایای EIGRPنسبت به پروتکل های دیگه مثل OSPFداشتن Unequal Cost Load Balancing هست.بعضی از پروتکل های دیگه مثل OSPF از Equal Cost Load Balancing فقط پشتیبانی می کنند .

www.Prozhe.com

www.Prozhe.com

یعنی فقط وقتی میتوانند از 2 مسیر به عنوان یک مسیر واحد استفاده کنند که Metric آن 2 مسیر کاملاً یکسان باشد.

این به این معنیه که اگه ما برای رسیدن به یک مقصد 2 مسیر مختلف داشته باشیم، که Metricمتفاوت داشته باشند، میتونیم برای ارسال دیتا به مقصد همزمان از هر 2 مسیر استفاده کنیم.

در این پروتکل پیام های Updateبه صورت Multicast ، باآدرس 224.0.0.10 کار میکند و از پیام های Incremental update استفاده میکند.از دیگر مزایای این پروتکل این است که می توان شبکه ای بدون چرخه لایه سوم طراحی کرد.

این پروتکل از MTU،Load،Reliability، Delay،Bandwidth برای انتخاب بهترین مسیر بهره می برد.به طور پیش فرض Bandwidth و Delay مورد استفاده قرار می گیرند.

2-4-1 تشکیل همسایگی در پروتکل EIGRP:

EIGRP همانند OSPF با ارسال و دریافت Hello Packet تشکیل همسایگی می دهد.پیام های Hello در هر 5 ثانیه به صورت Multicast با آدرس 224.0.0.10 فرستاده می شوند.عدم دریافت Hello Packet از روتر همسایه در مدت زمان Dead Time،به معنای Down شدن پروسه EIGRP در روتر همسایه است.زمان Dead Time،15 ثانیه می باشد. پیام هایی که در EIGRP وجود دارد:

- Hello
- Update: شامل اطلاعات Routingمی باشد.
- Query: با استفاده از این پیام از روتر همسایه درخواست می شود تا اطلاعات Routing را قبول کند.
- Reply: در پاسخ پیام های Query ارسال می شود.
- Ack: پیامی که مبنی بر صحت پیام ارسالی است که به روتر فرستنده ارسال خواهد شد.

پارامتر هایی که بین روتر های همسایه در تشکیل همسایگی بررسی می شوند:

1) AS_NO (شمارهAS) ، بین روترهای همسایه باید یکسان باشد.
2) Authentication Key
3) Hello Time و Dead Timeبین دو روتر همسایه چک می شود و عدد کوچکتر معیار این دو پارامتر در هر روتر همسایه خواهد بود.

www.Prozhe.com

www.Prozhe.com

4) IP هر روتر همسایه، باید در یک Subnet مشترک باشند.

بعد از آنکه دو روتر تشکیل همسایگی می دهند،هر روتر اطلاعات Routing Update را یک بار و به صورت مطمئن انتقال می دهد.اطمینان از ارسال Routing Update بادریافت Ack حاصل می شود.

2-4-2 پیاده سازی EIGRP:

برای پیاده سازی باید مراحل زیر را انجام دهیم:

4) فعال کردن EIGRP به همراه شماره AS.شماره ASباید بین روترهای همسایه یکسان باشد.

Router(config)# **router eigrp** *autonomous_system#*

5) فعال کردن Interfaceهای متصل به روتر با دستور Network

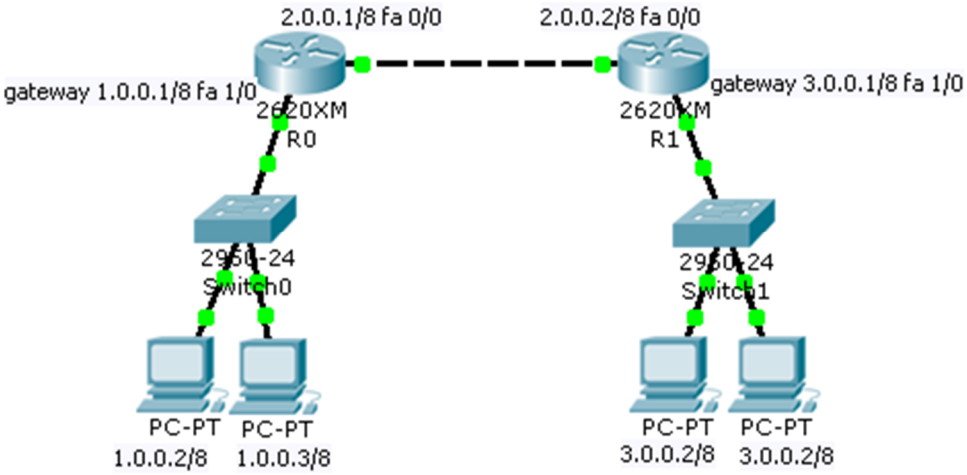
Router(config)# **network** *IP_address[network] wildcard_mask*

- ✓ نکته:در این پروتکل همانند RIPv2به صورت پیش فرض Auto-Summary فعال است. بنابراین بعد از فعال کردن EIGRP، Auto-Summary را نیز غیر فعال می نمائیم.

برای مثال در سناریوی زیر پروتکل EIGRP را پیکربندی می کنیم:

www.Prozhe.com

www.Prozhe.com



شکل 6-2 : سناریو EIGRP

در روتر R0:

R0(config)# **router eigrp** 2

R0(config-router)# **network** 1.0.0.1 0.0.0.255

R0(config-router)# **network** 2.0.0.1 0.0.0.255

در روتر R1:

R1(config) # **router eigrp** 2

R1(config-router)# **network** 3.0.0.1 0.0.0.255

R1(config-router)# **network** 2.0.0.2 0.0.0.255

در جدول مسیریابی هر روتر،مسیر Subnetهایی که از طریق این پروتکل یادگرفته می شود با برچسب D در جدول مسیریابی نشان داده می شود. برای مثال جدول مسیر یابی در روتر R0 به صورت زیر است:

C 1.0.0.0/8 is directly connected, FastEthernet1/0

is subnetted, 1 subnets 30/2.0.0.0

C 2.0.0.0 is directly connected, FastEthernet0/0

D 3.0.0.0/8 [90/30720] via 2.0.0.2, 00:00:14, FastEthernet0/0

www.Prozhe.com

www.Prozhe.com

2-4-3 عیب یابی EIGRP:

برای عیب یابی EIGRP از دستورات زیر استفاده می کنیم:

- Show IP Route: هر روتر لیست بهترین مسیرها به مقاصد مختلف را در Routing Table خود نگه می دارد.با این دستور میتوان جدول مسیریابی را مشاهده کرد.
- Show IP Protocol: این دستور تمامی پروتکل های فعال روی روتر را نشان می دهد.
- Show IP OSPF Neighbor: برای مشاهده جدول همسایگی
- Show IP EIGRP Topology: برای مشاهده جدول توپولوژی
- Debug IP EIGRP: با این دستور تمامی حوادث مربوط به EIGRP نمایش داده می شود.
- Show IP EIGRP Traffic: با این دستور می توان ترافیک انتقالی EIGRP را مشاهده نمود.

www.Prozhe.com

www.Prozhe.com

فصل سوم

امنیت در پروتکل های مسیریابی

3-1 امنیت:

امروزه امنیت یکی از نگرانی های اولیه طراحان شبکه می باشد.ایمن سازی شبکه شامل تأمین امنیت در تبادل اطلاعات مسیریابی بین روترها می باشد به نحوی که اطمینان حاصل کرد که اطلاعات وارد شده به جدول مسیر یابی معتبر باشد و شامل اطلاعات دستکاری شده توسط شخصی به منظور مختل کردن شبکه نباشد.

مهاجم ممکن است به منظور فریب روتر و ارسال داده ها به مسیر اشتباه و یا کاهش عملکرد شبکه،برای روتر های شبکه Routing Update نامعتبر بفرستد.علاوه براین به علت پیکربندی ضعیف،وجود Routing Update نامعتبر در جدول مسیریابی ممکن است روتر درست عمل نکند.در نتیجه برای جلوگیری از ارسال اطلاعات مسیریابی نامعتبر به روتر، اجرای Authentication در روتر برای فرآیند Routing Update بسار مفید و عاقلانه می باشد.در این فصل تائید هویت روتر همسایه (Neighbor Router Authentication) را بعنوان بخشی از یک طرح امنیتی توصیف می کنیم.این توصیف شامل،تائید هویت روتر همسایه چیست و چگونه کار می کند؟و این که چرا باید از آن برای افزایش امنیت شبکه استفاده کنیم؟

3-2 تائید هویت روتر همسایه (Neighbor Router Authentication):

شما می توانید با تنظیم Authentication در روتر خود از دریافت Routing Update جعلی از روتر همسایه جلوگیری کنید.زمانی که Authentication تنظیم شود،هر زمان که بین روترهای همسایه Routing Update ردوبدل می شود،تائید هویت همسایه اتفاق می افتد.بدون تائید هویت روتر همسایه،Routing Updateهای غیر مجاز و یا مخرب می تواند امنیت شبکه شمارا مختل کند.برای مثال یک روتر می تواند Routing Update ساختگی را برای متقاعد کردن روتر شما برای ارسال ترافیک به مقصد نادرست ارسال کند. اما تنظیم تائید هویت تضمین می کند که روتر اطلاعات مسیریابی قابل اطمینان را از منبع مورد اعتماد دریافت می کند.

www.Prozhe.com

www.Prozhe.com

3-3 پروتکل هایی که از Neighbor Authentication پشتیبانی می کنند:

Neighbor Authentication برای پروتکل های زیر می توان تنظیم کرد:

- Routing Information Protocol (RIP) version 2
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)
- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)

4-3 چه زمانی Neighbor Authentication باید تنظیم شود؟

در صورتی که روتر شرایط زیر را داشته باشد شما باید Neighbor Authentication را برای هر روتر تنظیم کنید:

- اگر روتر از هریک از پروتکل های مسیریابی که قبلا ذکر شده است استفاده کند.
- اگر ممکن است که روتر Routing Update نادرست دریافت کند.
- اگر با دریافت Routing Update نادرست ممکن است شبکه به خطر بیافتد.
- اگر در یک روتر Neighbor Authentication تنظیم کنید،باید در روتر همسایه نیز تنظیم کنید.

5-3 Neighbor Authentication چگونه کار می کند؟

زمانی که Neighbor Authentication روی یک روتر تنظیم می شود،روتر صحت منبع که بسته های Routing Update را دریافت می کند را اثبات می کند.در تبادل اطلاعات هم در ارسال هم در دریافت،تائید هویت توسط کلید (Authentication Key)انجام می شود.دو نوع Neighbor Authentication وجود دارد:

- plain text authentication
- Message Digest Algorithm Version 5 (MD5) authentication

هردو به یک روش کار می کنند با این تفاوت که MD5 یک خلاصه پیام بعنوان کلید(Authentication Key) ارسال می کند.این خلاصه پیام از یک کلید و پیام ایجاد می شود و در انتقال برای جلوگیری از خوانده شدن آن خود کلید ارسال نمی شود.اما plain text خود کلید را بر روی خط ارسال می کند.

توجه داشته باشید که plain text authentication بعنوان بخشی از استراتژی امنیت توصیه نمی شود، استفاده اصلی آن اجتناب از تغییرات تصادفی زیر ساخت های مسیریابی است. استفاده از MD5 authentication بعنوان یک عمل امنیتی توصیه می شود.

www.Prozhe.com

www.Prozhe.com

3-5-1 Plain Text Authentication:

بین روترهای همسایه باید یک کلید (Authentication Key) به اشتراک بگذارید.این کلید در زمان پیکربندی مشخص می شوند.در برخی از پروتکل ها می توان کلید های چندگانه مشخص نمود سپس هر کلید توسط یک شماره کلید باید شناسایی شود.

به طور کلی زمانی که Routing Update ارسال می شود، authentication به صورت زیر رخ می دهد:

1) یک روتر Routing Update را با یک کلید و شماره کلید مربوطه به روتر همسایه ارسال می کند. پروتکل هایی که تنها یک کلید می توانند داشته باشند، شماره کلید همیشه باید صفر باشد.
2) در دریافت روتر کلید دریافت شده را با کلید ذخیره شده در حافظه خود مقایسه میکند.
3) اگر دو کلید تطابق داشتند، روتر بسته Routing Update را می پذیرد. اگر دو کلید تطابق نداشتند، بسته Routing Update را رد می کند.

پروتکل هایی که از Plain Text Authentication استفاده می کنند:

- RIP version 2
- OSPF
- IS-IS

3-5-2 MD5 Authentication:

MD5 مانند Plain Text Authentication کار می کند با این تفاوت که کلید هرگز روی خط فرستاده نمی شود در عوض با استفاده از الگوریتم MD5 یک خلاصه پیام از کلید تولید می کند (Hash نیز نامیده می شود) ،سپس خلاصه پیام به جای خود کلید ارسال می شود.این روش تضمین می کند که در زمان انتقال کسی نمی تواند استراق سمع کند و کلید را یاد بگیرد.در نتیجه امنیت بالاتری دارد.

پروتکل هایی که از MD5 Authentication استفاده میکنند:

- RIP version 2
- OSPF
- EIGRP
- BGP

www.Prozhe.com

www.Prozhe.com

6-3 مدیریت زنجیره کلید(Key Chains):

شما می توانید زنجیره کلید را برای پروتکل های مسیریابی زیر پیاده سازی کنید:

- RIP version 2
- EIGRP

این پروتکل های مسیریابی با استفاده از مدیریت زنجیره کلید عملکرد های اضافی ارائه می کنند.زمانی که زنجیره کلید پیاده سازی می کنیم یکسری از کلید ها را با طول عمر مشخص میکنیم این کار احتمال این که کلید در معرض خطر باشد را کاهش می دهد.

در زمان تعریف هر کلید در زنجیره کلید باید یک بازه زمانی تعیین شود که مشخص باشد کلید تا چه زمانی فعال خواهد بود.سپس در طول عمر که به کلید داده شده است بسته ها Routing Update با کلید فعال ارسال می شوند.توجه داشته باشید که کلید در دوره های زمانی که فعال نیست استفاده نمی شوند.بنابراین توصیه می شود که در زمان تعریف زنجیره کلید از دوره ای از زمان که زمان فعال سازی کلید ها تداخل دارد جلوگیری شود به این دلیل که اگر در یک دوره زمان هیچ کلیدی فعال نباشد،تائید هویت همسایه انجام نمی شود و Routing Update با مشکل مواجه خواهد شد.

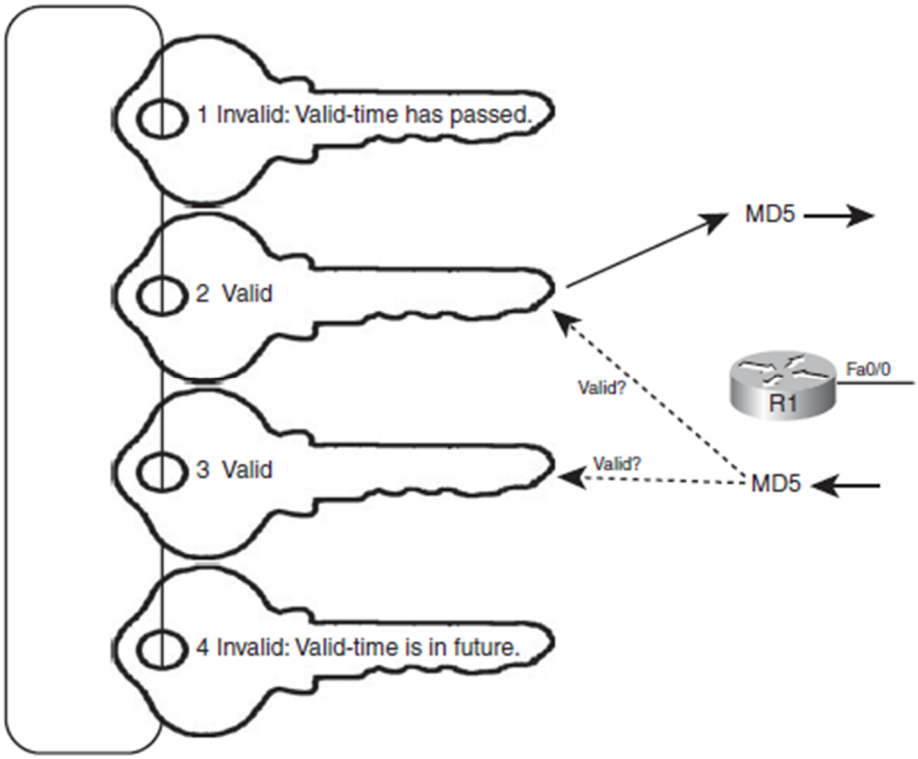
توجه داشته باشید که روتر های دیگر نیز باید زمان فعال بودن کلید را بدانند تا تمامی روترها از یک کلید همزمان استفاده کنند.وجود کلیدهای متعدد در زنجیره کلید و وجود عم معتبر برای هرکلید باعث سردرگمی می شود،قوانین در مورد زمانی که کلید استفاده می شود به شرح زیر است:

- ارسال پیامها: در میان کلیدهای در حال حاضر معتبر از کمترین شماره کلید استفاده کنید.
- دریافت پیام ها: بررسی خلاصه MD5 با استفاده از تمام کلیدهای در حال حاضر معتبر.

برای مثال شکل زیر نشان دهنده منطق روتر R1 هنگام ارسال و دریافت پیام می باشد که زنجیره ای با چهار کلید است.

www.Prozhe.com

www.Prozhe.com



شکل 3- 1: مدیریت کلید

طول عمر کلید1 گذشته و نا معتبر است.طول عمر کلید4 هنوز شروع نشده و نامعتبر می باشد(در آینده معتبر خواهد بود).با این حال کلیدهای 2و3 در حال حاضر معتبر هستند.

شکل نشان می دهد که پیام در روتر R1 توسط کلید2 ارسال شده،به این دلیل که کلیدهای 1و4 که در حال حاضر نامعتبر هستند و از میان دو کلید معتبر،کلید2 کمترین شماره کلید می باشد.روتر R1 در فرآیند دریافت پیام با هر دو کلید 2و3 بررسی می کند چرا که هردو در حال حاضر معتبر هستند.

3-7 Authentication در پروتکل RIPv2:

در پروتکل RIP، نسخه دوم این پروتکل از Authentication پشتیبانی می کند.اگر در حال ارسال و دریافت بسته با RIPv2 هستید شما می توانید Authentication را بر روی Interface فعال کنید.همانطور که قبلا گفته شد این پروتکل از دو حالت تائید هویت پشتیبانی می کند،زمانی که Authentication فعال است Plain Text در هر بسته به طور پیش فرض است.زمانی که مسئله امنیت در میان است Plain Text Authentication نباید مورد استفاده قرار بگیرد زیرا رمز عبور Authentication در هر بسته RIPv2 به صورت کدگذاری نشده فرستاده می شود.

www.Prozhe.com

www.Prozhe.com

3-7-1 فعال سازی Authentication در پروتکل RIPv2:

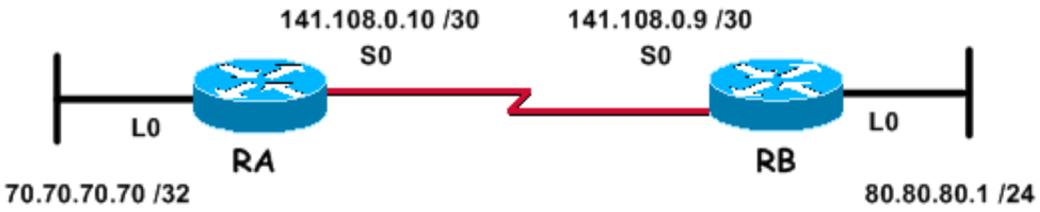
انجام مراحل تنظیم Authentication در پروتکل RIPv2:

1) تعریف زنجیره کلید

- ✓ نکته:زنجیره کلید مجموعه ای از کلید ها است که می توانند در Interface مورد استفاده قرار بگیرند.

2) تعریف کلید یا کلید های زنجیره کلید
3) مشخص کردن رمز عبور یا رشته کلید که در کلید مورد استفاده قرار می گیرد.این رشته تائید هویت است که در تصدیق مسیریابی ارسال و دریافت شود.
4) Authentication را بر روی یک Interface فعال کنید و زنجیره کلید که مورد استفاده قرار می گیرد را مشخص کنید.از آنجا کهAuthentication بر اساس هر Interface فعال است،یک روتر در حال اجرا RIPv2 می تواند روی یک Interface خاص فعال باشد و در Interfaceدیگر فعال نباشد.
5) مشخص کنید Interface از Plain Text Authentication یا MD5 Authentication استفاده می کند. Authenticationدر پروتکل RIPv2 به طور پیش فرض Plain Text است.درصورت استفاده از Plain Text این مرحله نیازی نیست.
6) مدیریت کلید را پیکربندی کنیم(این مرحله اختیاری است).

برای مثال Authentication را در سناریو زیر تنظیم میکنیم:



شکل 3-2 : سناریو RIP Authentication

www.Prozhe.com

www.Prozhe.com

شبکه فوق شامل دو روتر RA و RB است که هر دو در حال اجرای RIP هستند که به صورت دوره ای Routing Update ردو بدل می کنند.تبادل اطلاعات مسیریابی از لینک سریال تائید هویت می شود.

تنظیم Plain Text Authentication

ایجاد زنجیره کلید در روتر RA:

در زنجیره کلید حداقل یک کلید باید ساخته شود.

1) در حالت global

RA# configure terminal

2) ایجاد زنجیره کلید.در این مثال Kal مورد استفاده قرار می گیرد.این نام لزومی ندارد با روتر های همسایه مطابقت داشته باشد.

RA(config)#**key chain** Kal

3) ایجاد یک یا چند کلید.در این مثال شماره 1 مورد استفاده قرار می گیرد.توصیه می شود شماره کلید در همه روتر ها تنظیم شود.

RA(config−keychain)#**key** 1

4) تعیین رشته کلید برای کلید.در این مثال 234 استفاده می شود.رشته کلید باید در روتر های همسایه مطابقت داشته باشد.تعریف طول عمر اختیاری است.

RA(config−keychain−key)#**key−string** 234

5) پایان دادن به پیکربندی

RA(config−keychain−key)#end

RA#

www.Prozhe.com

www.Prozhe.com

تنظیم Authentication:

1) در حالت global

RA#configure terminal

2) تعیین Interface که شما می خواهید تائید هویت پیام RIP انجام شود.در این مثال Serial 0

RA(config)#interface serial 0

3) تائید هویت پیام RIP فعال کنید.

RA(config−subif)# **ip rip authentication key−chain** kal

RA(config−subif)#end

تنظیم در روتر RB:

RB#configure terminal

RB(config)#**key chain** Kal

RB(config−keychain)#**key** 1

RB(config−keychain−key)#**key−string** 234

RB(config−keychain−key)#end

RB#

RB #configure terminal

RB (config) #interface serial 0

RB (config−subif) # **ip rip authentication key−chain** kal

RB (config−subif) #end

www.Prozhe.com

www.Prozhe.com

تنظیم MD5 Authentication

ایجاد زنجیره کلید در روتر RA:

RA#configure terminal

RA(config)#**key chain** Kal

RA(config−keychain)#**key** 1

RA(config−keychain−key)#**key−string** 234

RA(config−keychain−key)#end

RA#

تنظیم Authentication:

RA#configure terminal

RA(config)#interface serial 0

RA(config−subif)# **ip rip authentication mode md5**

RA(config−subif)**# ip rip authentication key−chain** kal

RA(config−subif)#end

تنظیم در روتر RB:

RB# configure terminal

RB(config)#**key chain** Kal

RB(config−keychain)#**key** 1

RB(config−keychain−key)#**key−string** 234

RB(config−keychain−key)#end

www.Prozhe.com

www.Prozhe.com

RB#

RB#configure terminal

RB(config) #interface serial 0

RB(config−subif)**# ip rip authentication mode md5**

RB(config−subif)**# ip rip authentication key−chain** kal

RB(config−subif)#end

با این تنظیمات تمامی مبادلات Routing Update بین دو روتر قبل از دریافت تائید هویت می شوند. برای عیب یابی می توان از دستور debug ip rip استفاده نمود.

RB#**debug ip rip**
RIP protocol debugging is on
*Mar 3 20:48:37.046: RIP: received packet with **MD5 authentication**
*Mar 3 20:48:37.046: RIP: received v2 update from 141.108.0.10 on Serial0
*Mar 3 20:48:37.050: 70.0.0.0/8 via 0.0.0.0 in 1 hop

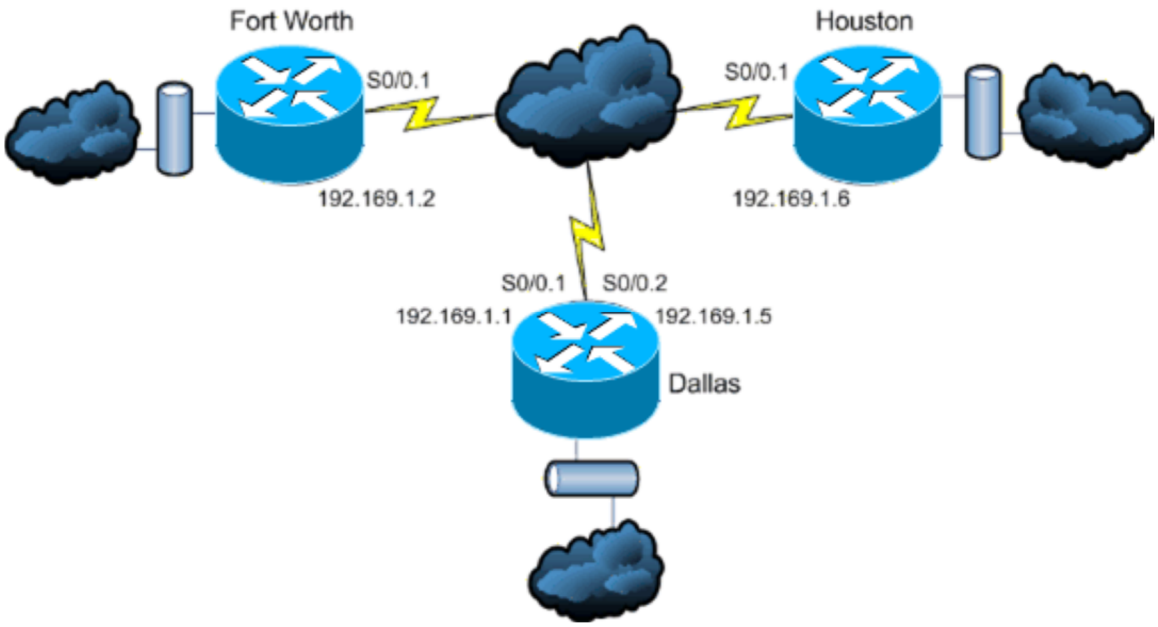
8-3 فعال سازی Authentication در پروتکل EIGRP:

تائید هویت EIGRP باعث می شود روتر به هر پیام EIGRP اعتبار بخشد.همانطور که قبلا گفته شد برای این کار روتر ها از یک کلید مشترک از قبل تعیین شده استفاده می کنند و در دیافت پیام کلید بررسی می شود در صورت متفاوت بودن روتر بسته را دور می ریزد.در نتیجه دو روتر به همسایه تبدیل نمی شوند به این دلیل که Hello Message را نادیده گرفتند.از دیدگاه طراحی EIGRP Authentication از حملات وتبلیغات نادرست اطلاعات مسیریابی همسایه ها جلوگیری می کنداما هیچگونه حریم خصوصی را فراهم نمی کند.

برای مثال Authentication را در سناریو زیر تنظیم میکنیم:

www.Prozhe.com

www.Prozhe.com



شکل 3-3: سناریو EIGRP Authentication

انجام مراحل تنظیم Authentication در پروتکل EIGRP:

1) ایجاد یک زنجیره کلید
2) تنظیم Authentication با استفاده از زنجیره کلید بر روی Interface

ایجاد زنجیره کلید در روتر Dallas:

در زنجیره کلید حداقل یک کلید باید ساخته شود.

6) در حالت global

Dallas#configure terminal

7) ایجاد زنجیره کلید.در این مثال MYCHAIN مورد استفاده قرار می گیرد.این نام لزومی ندارد با روتر های همسایه مطابقت داشته باشد.

Dallas(config)#**key chain** MYCHAIN

8) ایجاد یک یا چند کلید.در این مثال شماره 1 مورد استفاده قرار می گیرد.توصیه می شود شماره کلید در همه روتر ها تنظیم شود.

Dallas(config−keychain)#**key** 1

www.Prozhe.com

www.Prozhe.com

9) تعیین رشته کلید برای کلید.در این مثال securetraffic استفاده می شود.رشته کلید باید در روتر های همسایه مطابقت داشته باشد.تعریف طول عمر اختیاری است.

Dallas(config−keychain−key)#**key−string** securetraffic

10) پایان دادن به پیکربندی

Dallas(config−keychain−key)#end

Dallas#

تنظیم Authentication:

4) در حالت global

Dallas#configure terminal

5) تعیین Interface که شما می خواهید تائید هویت پیام EIGRP انجام شود.در این مثال Serial 0/0.1

Dallas(config)#interface serial 0/0.1

6) تائید هویت پیام EIGRP فعال کنید.شماره 10 به عنوان شماره AS در شبکه استفاده شده است.MD5 نیز نشان دهنده این است که از Authentication MD5 استفاده شده است.

Dallas(config−subif)#**ip authentication mode eigrp** 10 **md5**

7) تعیین زنجیره کلید برای تائید هویت.10 شماره AS می باشد.MYCHAIN زنجیره کلیدی است که قبلا ایجاد کردیم.

Dallas(config−subif)#**ip authentication key−chain eigrp** 10 MYCHAIN
Dallas(config−subif)#end

8) تنظیم مشابه در Serial 0/0.2

Dallas#configure terminal
Dallas(config)#interface serial 0/0.2
Dallas(config−subif)#**ip authentication mode eigrp** 10 **md5**
Dallas(config−subif)#**ip authentication key−chain eigrp** 10 MYCHAIN
Dallas(config−subif)#end
Dallas#

www.Prozhe.com

www.Prozhe.com

تنظیم در روتر Fort Worth:

```
FortWorth#configure terminal
FortWorth(config)#key chain MYCHAIN
FortWorth(config−keychain)#key 1
FortWort(config−keychain−key)#key−string  securetraffic
FortWort(config−keychain−key)#end
FortWorth#
```

```
Fort Worth#configure terminal
FortWorth (config) #interface serial 0/0.1
FortWorth (config−subif) #ip authentication mode eigrp 10 md5
FortWorth (config−subif) #ip authentication key−chain eigrp 10 MYCHAIN
FortWorth (config−subif) #end
FortWorth#
```

تنظیم در روتر Houston:

```
Houston#configure terminal
Houston(config)#key chain MYCHAIN
Houston(config−keychain)#key 1
Houston(config−keychain−key)#key−string securetraffic
Houston(config−keychain−key)#end
Houston#
```

```
Houston#configure terminal
Houston (config) #interface serial 0/0.1
Houston (config−subif) #ip authentication mode eigrp 10 md5
Houston (config−subif) #ip authentication key−chain eigrp 10 MYCHAIN
Houston (config−subif) #end
Houston#
```

برای عیب یابی دستورات زیر میتواند مفید باشد:

- Show Key Chain: این دستور فهرستی از پیکربندی زنجیره کلید و همچنین کلیه کلیدها که معتبر هستند را نشان می دهد.

- Debug EIGRP Packet: این دستور لیستی از پیام هایی را در مورد این که چرا روتر های همسایه شکست خورده اند را نشان می دهد.برای مثال خروجی این دستور را زمانی که Authentication فقط در روتر Dallas تنظیم شده است:

www.Prozhe.com

www.Prozhe.com

Dallas#**debug eigrp packets**
17:43:43: EIGRP: ignored packet from 192.169.1.2 (**invalid authentication**)
17:43:45: EIGRP: ignored packet from 192.169.1.6 (**invalid authentication**)

Authentication بسته ها از دو روتر دیگر نادیده گرفته می شوند زیرا

در روتر های دیگر هنوز تنظیم نشده است.

و خروجی دستور زمانی که Authentication در هر سه روتر تنظیم شده است:

debug eigrp packets FortWorth
00:47:04: EIGRP: **received packet with MD5 authentication, key id = 1**
00:47:04: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.1

بسته ها از روتر Dallas با MD5 authentication دریافت شد.

Houston#**debug eigrp packets**
00:12:50.751: EIGRP: **received packet with MD5 authentication, key id = 1**
00:12:50.751: EIGRP: Received HELLO on Serial0/0.1 nbr 192.169.1.5

بسته ها از روتر Dallas با MD5 authentication دریافت شد.

در زمان عیب یابی به خاطر داشته باشید:

- بررسی زمان جاری در روتر ها با دستور **Show Clock**
- نام زنجیره کلید و تعداد کلید های مورد استفاده در دو روتر نیاز نیست مطابقت داشته باشند.
- رشته کلید در هر یک از همسایه ها باید مطابقت داشته باشد.
- هر دو دستور **ip authentication mode eigrp** *asn* **md5** و **ip authentication key-chain eigrp** *asn* *name-of-chain* باید روی Interface پیکربندی شود.اگر هرکدام حذف شود با مشکل مواجه می شود.

9-3 فعال سازی Authentication در پروتکل OSPF:

تائید هویت OSPF باعث می شود روتر به هر پیام OSPF اعتبار بخشد.همانطور که قبلا گفته شد برای این کار روتر ها از یک کلید مشترک از قبل تعیین شده استفاده می کنند و در دیافت پیام کلید بررسی می شود در صورت متفاوت بودن روتر بسته را دور می ریزد.بنابراین میتوان به منظور مبادله اطلاعات مسیریابی به شیوه ای امن از Authentication استفاده کنید.

www.Prozhe.com

www.Prozhe.com

OSPF Authentication از دو نوع زیر استفاده می کند:

- Plain text authentication: رمز عبور به صورت Clear Text بر روی شبکه می رود.
- MD5 authentication : با این روش خلاصه رمز عبور روی شبکه می رود. MD5امن ترین حالت است.

برای هریک از این دو گزینه باید دو مرحله زیر را انجام دهید:

1) Authentication باید فعال شود و نوع Authentication را انتخاب کنید از طریق دو روش زیر:

فعال کردن در Interface با استفاده از زیر دستور

Plain text**: ip ospf authentication**

MD5**: ip ospf authentication [message-digest]**

فعال کردن روی تمامی Interfaceهای یک منطقه با استفاده از زیر دستور

Plain text**: area** *area-no* **authentication**

MD5**: area** *area-no* **authentication [message-digest]**

2) کلید تائید هویت باید در Interface پیکربندی شود

Plain text: **ip ospf authentication-key** key-value

MD5: **ip ospf message-digest-key** key-number **md5** key-value

توجه داشته باشید اگر Interface با زیر دستور **ip ospf authentication**

(نوع اول)تنظیم شده باشد و دستور **area authentication** به صورت MD5 تنظیم شود،این Interface به صورت Plain Text عمل می کند.

www.Prozhe.com

www.Prozhe.com

کد زیر نمونه ای از تنظیم MD5 در تمام Interface های ناحیه صفر:

```
R3#conf t
R3(config) #router ospf 3
R3(config-router)# area 0 authentication message-digest
R3(config-router)#interface fastethernet0/0
R3(config-if)# ip ospf message-digest-key 1 md5 secret
```

کد زیر نمونه ای از تنظیم Plain Text در یک Interface:

```
R3(config-if)#interface fastethernet0/1
R3(config-if)#ip ospf authentication
R3(config-if)#ip ospf authentication-key secret
```

برای مثال Authentication را در سناریو زیر تنظیم میکنیم:

شکل 3-4: سناریو OSPF Authentication

تنظیم Plain Text:

در روتر R2:

```
R2(config)# interface Serial0
R2(config-subif)# ip address 192.16.64.2 255.255.255.0
R2(config-subif)# ip ospf authentication−key kal
```

```
R2(config)# router ospf 10
R2(config)# network 70.0.0.0 0.255.255.255 area 0
R2(config)# network 192.16.64.0 0.0.0.255 area 0
R2(config)# area 0 authentication
```


www.Prozhe.com

www.Prozhe.com

در روتر R1:

R1(config)# interface Serial0
R1(config-subif)# ip address 192.16.64.1 255.255.255.0
R1(config-subif)**# ip ospf authentication−key** kal

R1 (config) # router ospf 10
R1 (config) # network 172.16.0.0 0.0.255.255area 0
R1 (config) # network 192.16.64.0 0.0.0.255 area 0
R1 (config) # **area** 0 **authentication**

تنظیم MD5:

در روتر R2:

R2(config)# interface Serial0
R2(config-subif)# ip address 192.16.64.2 255.255.255.0
R2(config-subif)**# ip ospf message−digest−key** 1 **md5** kal

R2(config)# router ospf 10
0.255.255.255 area 0 R2(config)# network 70.0.0.0
area 00.0.0.255R2(config)# network 192.16.64.0
R2(config)# **area** 0 **authentication message−digest**

در روتر R1:

R1(config)# interface Serial0
R1(config-subif)# ip address 192.16.64.1 255.255.255.0
R1(config-subif)# ip ospf message−digest−key 1 md5 kal

R1(config)# router ospf 10
R1(config)# network 172.16.0.0 0.0.255.255area 0
R1(config)# network 192.16.64.0 0.0.0.255 area 0
R1(config)# area 0 authentication message−digest

www.Prozhe.com

www.Prozhe.com

عیب یابی

برای بررسی اینکه تائید هویت فعال است و از چه نوعی می باشد از دستور show ip ospf interface استفاده ی شود.

برای مثال خروجی این دستور را در روتر R1 نشان می دهیم:

Plain Text:

```
R1# show ip ospf interface serial0
Serial0 is up, line protocol is up
Internet Address 192.16.64.1/24, Area 0
Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Simple password authentication enabled
```

MD5:

```
R1−2503# show ip ospf interface serial0
Serial0 is up, line protocol is up
Internet Address 192.16.64.1/24, Area 0
Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT, Cost: 64
Transmit Delay is 1 sec, State POINT_TO_POINT,
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 4 msec
Neighbor Count is 1, Adjacent neighbor count is 1
Adjacent with neighbor 70.70.70.70
Suppress hello for 0 neighbor(s)
Message digest authentication enabled
Youngest key id is 1
```


www.Prozhe.com

www.Prozhe.com

از دستور Debug ip ospf adj نیز می توان برای عیب یابی استفاده کرد:

زمانی که نوع Authentication در روترها تطابق نداشته باشد این پیغام ظاهر می شود.

R1# **debug ip ospf adj**
00:51:23: OSPF: Rcv pkt from 192.16.64.2, Serial0: **Mismatch**
Authentication type.

زمانی که نوع Authentication در روترها تطابق داشته باشد اما ارزش کلیدی متفاوت باشد این پیغام ظاهر می شود.

R1# **debug ip ospf adj**
00:51:33: OSPF: Rcv pkt from 192.16.64.2, Serial0: **Mismatch**
Authentication Key − Clear Text

زمانی که نوع MD5 Authenticationدر روترها تطابق داشته باشد اما شناسه کلیدی که استفاده می شود متفاوت باشد این پیغام ظاهر می شود.روتر R1 از کلید با ID 1استفاده می کند ولی روتر R2 از کلید با ID 2 در نتیجه پیغام زیر ظاهر می شود.

R1# **debug ip ospf adj**
00:59:33: OSPF: Send with youngest Key 1
00:59:43: OSPF: Rcv pkt from 192.16.64.2, Serial0: **Mismatch**
Authentication Key − No message digest key 2 on interface

www.Prozhe.com

www.Prozhe.com

نتیجه گیری:

همانطور که خواندید هرکدام از الگوریتم های مسیریابی نقاط قوت و نقاط ضعف خود را دارند و باید با توجه به مقیاس شبکه و هزینه ها باید بهترین الگوریتم مسیریابی را انتخاب کرد.بهترین الگوریتم مسیریابی، الگوریتمی است که دارای خصوصیات زیر باشد:

زمان همگرایی بالایی داشته باشد،دید به توپولوژی شبکه داشته باشد و هوشمندانه عمل کند و انحصاری شرکت خاصی نباشد.پیاده سازی Static Route در شبکه های کوچک استفاده می شود و در شبکه های بزرگ مدیریت آن پیچیده خواهد شد و انتخاب مناسبی نمی باشد.پروتکل RIP زمان همگرایی بالایی دارد و دید به توپولوژی شبکه ندارد و امکان رخ دادن چرخه لایه سوم نیز وجود دارد.بنابراین در شبکه های بزرگ و پیچیده بهتر است از پروتکل های دیگر استفاده شود. پروتکل EIGRP زمان همگرایی بسیار عالی، دید به توپولوژی شبکه ، سرعت فوق العاده ای دارد،از منابع شبکه استفاده زیادی نمی کند و در شبکه های بزرگ بسیار عالی عمل می کند اما این پروتکل انحصاری شرکت CISCO می باشد که برای استفاده از این پروتکل باید تمامی Device های شبکه از شرکت CISCO باشد که هزینه زیادی می برد.پروتکل OSPF یکی از پرکاربرد ترین پروتکل ها می باشد، زمان همگرایی مناسبی ،دید به توپولوژی شبکه ،سرعت سریعی دارد وانحصاری محسوب نمی شود و در شبکه های بزرگ انتخاب مناسبی است.این پروتکل منابع شبکه را زیاد استفاده می کند .

www.Prozhe.com

www.Prozhe.com

پیوست

دستورات پیکربندی اولیه روتر:

Router Modes:

Router> User mode

Router# Privileged mode (also known as EXEC-level mode)

Router (config) # Global configuration mode

Router (config-if) # Interface mode

interface mode–Router (config-subif) # Sub

Router (config-line) # Line mode

Router (config-router) # Router configuration mode

Entring Global Configuration Mode:

Router> Limited viewing of configuration.

You cannot make changes in this mode.

Router# you can see the configuration and move to make changes.

Router# configure terminal

Router (config) #

Configuring a Router Name:

Router (config) # hostname Cisco The name can be any word you choose

Configuring Password:

Router (config) # enable password cisco Sets enable password

Router (config) # enable secret class Sets enable secret password

Router (config) # line console 0 Enters console line mode

www.Prozhe.com

www.Prozhe.com

password to console Router (config-line) # password console Sets console line mode

Router (config-line) # login Enables password checking at login

Router (config) # line vty 0 4 Enters vty line mode for all five vty

Lines

Router (config-line) # password telnet Sets vty password to telnet

Router (config-line) # login Enables password checking at login

Router (config) # line aux 0 Enters auxiliary line mode

Router (config-line) # password backdoor sets auxiliary line mode password to backdoor

Router (config-line) # login Enables password checking at login

Password Encryption:

Router (config) # service passwordencryption applies a weak encryption to passwords

Router (config) # enable password cisco Sets enable password to cisco

Router (config) # line console 0 Moves to console line mode

Router (config-line) # password Cisco Continue setting passwords as above

Router (config) # no service password encryption turns off password encryption

Configring a Serial Interface:

Router (config) # interface s0/0/0 Moves to serial interface 0/0/0 configuration mode

Router (config-if) # description Link to ISP Optional descriptor of the link is locally significant

Router (config-if) # ip address 192.168.10.1 255.255.255.0

Assigns address and subnet mask to interface

Router (config-if) # clock rate 56000 Assigns a clock rate for the interface

Router (config-if) # no shutdown Turns interface on

Configuring a Fast Ethernet Interface:

www.Prozhe.com

www.Prozhe.com

Router (config) # interface fastethernet 0/0 Moves to Fast Ethernet 0/0 interface configuration mode

Router (config-if) # description Accounting LAN Optional descriptor of the Link is locally significant

Router (config-if) # ip address 192.168.20.1 255.255.255.0 Assigns address and subnet mask to interface

Router (config-if) # no shutdown Turns interface on

Saving Configuration:

Router# copy running-config startup-config saves the running configuration to local NVRAM

Router# copy running-config tftp saves the running configuration remotely to a TFTP server

Erasing Configuration:

Router# erase startup-config deletes the startup configuration file from NVRAM

Show Commands:

Router# show? Lists all show commands available.

Router# show interfaces Displays statistics for all interfaces.

Router# show interface serial 0/0/0 Displays statistics for a specific Interface (in this case, serial 0/0/0).

Router# show ip interface brief displays a summary of all Interfaces, including status and IP address assigned.

Router# show controllers serial 0/0/0 Displays statistics for interface Hardware. Statistics display if the clock rate is set and if the cable is DCE, DTE, or not attached.

Router# show clock Displays time set on device.

Router# show hosts Displays local host-to-IP address cache. These are the names and Addresses of hosts on the network to which you can connect.

Router# show users Displays all users connected to device.

www.Prozhe.com

www.Prozhe.com

Router# show history displays the history of commands Used at this edit level.

Router# show flash Displays info about flash memory.

Router# shows version Displays info about loaded software version.

Router# show arp Displays the Address Resolution Protocol (ARP) table.

Router# show protocols Displays status of configured Layer 3 protocols.

Router# show startup-config displays the configuration saved in NVRAM.

Router# show running-config displays the configuration currently running in RAM.

www.Prozhe.com

www.Prozhe.com

فهرست منابع

- **کتاب ها**

[1] براین استوارت،راهنمای جامع CCNA BSCI ،ترجمه دکتر حسین محسن زاده،چاپ اول،آریا پژوه و موسسه فرهنگی و اطلاع رسانی آموزگارمهر (انتشارات زوفا) ،1387

[2] بیل پارکورست،مسیریابی گام اول،ترجمه علی مختار پور و نگار حمید سمیعی،چاپ اول ،انتشارات پندار پارس و با همکاری آریا پژوه،بهار 1387

- **پایان نامه ها**

محسن زوله، مسیریابی، کارشناسی، مرکز آموزش عالی جهاد دانشگاهی شعبه صنعتی اصفهان،تیر ماه 89

- **وب سایت ها**

[1] وب سایت شرکت سیسکو ، www.cisco.com

[2] منبع برای فن آوری سیسکو ، www.ciscopress.com

www.Prozhe.com