CCNP : Route

Cisco Certified Network Professional

Study Guide

Engineer SHOWAN KOLIJI

Routing Protocols

آشنایی با انواع Routing Protocolها

Routing پروسه ارسال Packetهای اطلاعاتی از یک مبدا (Source) به یک مقصد (Destination)در محیط Internetwork یا محیط Multi Network می باشد . در صورتی که زیربنای Routing به درستی در یک محیط Internetwork پیاده سازی نشود شبکه های مختلف قادر به برقراری ارتباط با یکدیگر نخواهند بود .

Routerها برای اینکه بتوانند به صورت صحیح در شبکه وظایف مسیریابی و برقراری ارتباط بین شبکه ها را انجام دهند قبل از استفاده باید پیکربندی شوند و جدول مسیریابی Routing Table بر روی Router ایجاد شود وجود این جدول برای مسیریابی مورد نیاز می باشد . Routerها تصمیمات مسیریابی خود را بر اساس این جدول اتخاذ می کنند هر Router در جدول مسیریابی خود باید از وجود کلیه شبکه هایی که قصد مسیریابی و ارتباط با آنها را دارد اطلاع داشته باشد .

جدول مسیریابی یا Routing Table در Router به دو صورت می تواند پیکربندی شود :

1. به صورت Static Routing
2. به صورت Dynamic Routing

Static Routing

برای پیکربندی جدول مسیریابی Router به صورت Static مدیر شبکه باید از اطلاعات مربوط به شبکه های موجود و مسیرهای آنها مطلع باشد و به صورت دستی مسیرها و شبکه ها را درون این جدول اضافه نماید .

این روش دارای مزایا و معایب زیر می باشد :

مزایای استفاده از Static Routing :

- این روش بار اضافی یا overhead برای CPU روتر نخواهد داشت .
- این روش پهنای باند لینک های ارتباطی بین Routerها توسط پیام های Update اشغال و مورد استفاده قرار نمی دهد .
- امنیت این روش بالاتر می باشد .

معایب استفاده از Static Routing :

- برای پیکربندی Static Routing نیاز به آشنایی با کلیه مسیرهای داخل Internetwork می باشد .
- اگر یک مسیر جدید به داخل Internetwork اضافه شود باید به صورت دستی روی کلیه Routerها تعریف شود .
- در صورتی که مسیری دچار مشکل شود امکان استفاده از مسیرهای دیگر به صورت Dynamic وجود نخواهد داشت .
- به علت اینکه نگهداری و مدیریت و پیکربندی Static Routing برای شبکه های بزرگ پروسه زمانی زیادی را نیاز دارد و همچنین امکان بروز خطا بسیار زیاد است از Static Routing بیشتر در شبکه های کوچک و مسیرهای محدود استفاده می شود .

Dynamic Routing

در این روش Dynamic Routing Protocol بر روی Routerها پیکربندی خواهد شد که بعد از پیکربندی این پروتکل های مسیریابی , Routerها به صورت Dynamic جدول مسیریابی خود را بین یکدیگر مبادله می کنند و مسیرهای جدید را اضافه و جدول خود را با ارسال Updateها برای یکدیگر به روز رسانی خواهند کرد .

این روش دارای مزایا و معایب زیر است :

مزایای استفاده از Dynamic Routing :

- کاهش بار مدیریتی برای مدیریت مسیرها
- در صورت اضافه شدن مسیر جدید به داخل Internetwork به صورت Dynamic کلیه روترهای داخل شبکه مسیر جدید را در جدول مسیریابی خود اضافه می کنند .
- در صورت که مسیری دچار مشکل شود امکان استفاده از مسیرهای دیگر به صورت Dynamic وجود خواهد داشت .
- قابل استفاده برای مسیردهی شبکه های بزرگ خواهد بود .

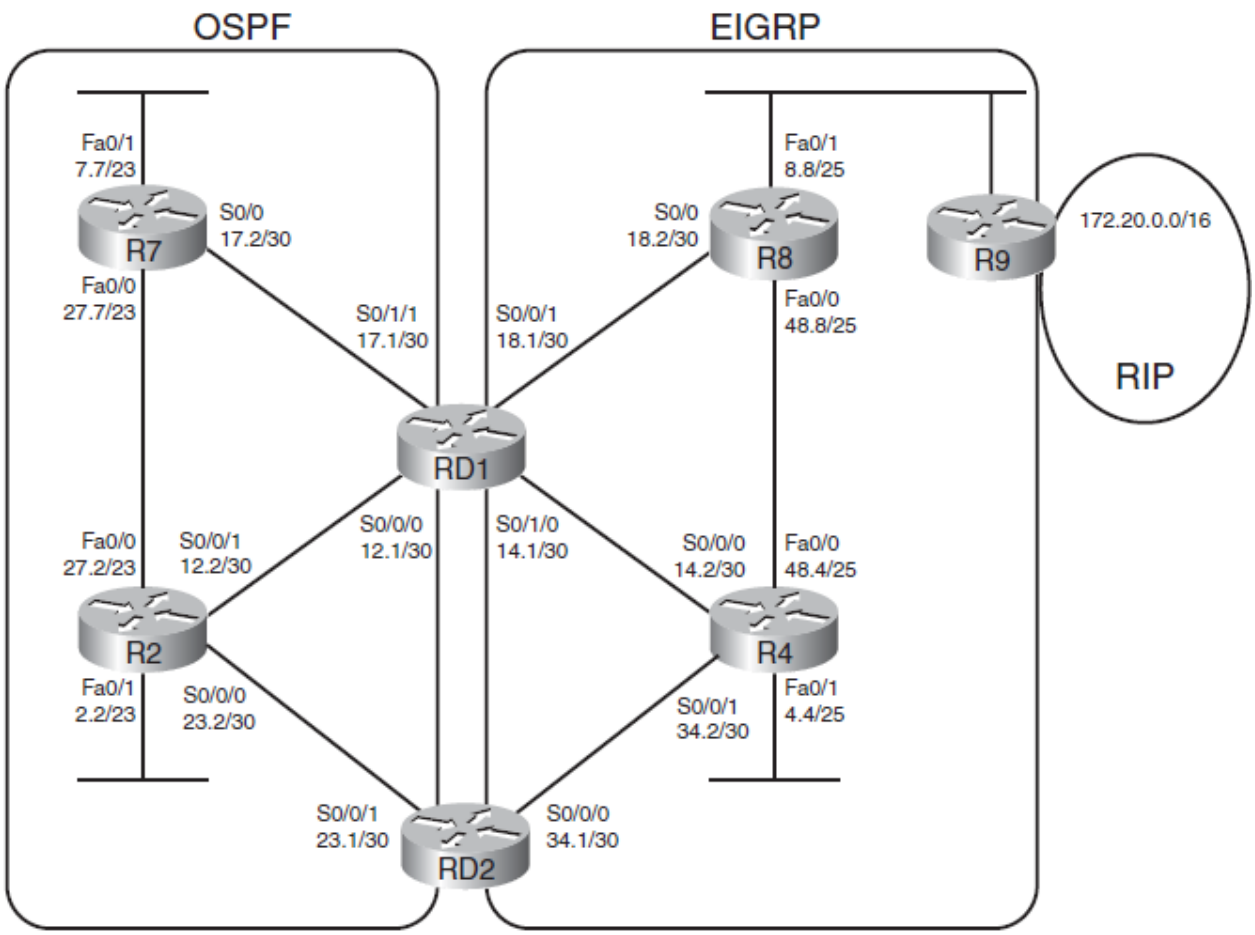
معایب استفاده از Dynamic Routing :

- پیکربندی مشکل و پیچیده تر
- استفاده از پهنای باند لینک های ارتباطی برای ارسال پیام های Update
- مبادله جدول مسیریابی با سایر Routerهای موجود در Internetwork
- دریافت پیام های Update از سایر Routerها و پردازش آنها
- به روز رسانی اتوماتیک جدول مسیریابی بین Routerها
- انتخاب بهترین مسیر برای هر مقصد و قرار دادن آن در جدول مسیریابی

انواع Routing Protocolها :

- RIP
- EIGRP
- OSPF
- BGP

حال که جدول مسیریابی Router با استفاده از Routing Protocolها یا همان پروتکل های مسیریابی Update می شود هر ترافیکی که به سمت Router برای مسیریابی ارسال شود Router تصمیمات مسیر را بر اساس اطلاعات داخل جدول Routing Table خود اتخاذ می کند. Routing Protocolها هدف یکسانی دارند که انتخاب بهترین مسیر می باشد ولی در مکانیسم عمل آنها و شرایط انتخاب بهترین مسیر در هر یک از پروتکل ها با یکدیگر متفاوت می باشد .



Metric

ممکن است در شبکه Internetwork برای رسیدن به یک مقصد دو مسیر وجود داشته باشد در این حالت Routerها برای شناسایی بهترین مسیر از واحدی به نام Metric استفاده میکنند . در واقع چون Routing Protocolهای مختلفی وجود دارد هر Routing Protocol به یک شکل فرم مخصوص به خود Metric را محاسبه می کند .

برای مثال پروتکل RIP از Hop Count برای محاسبه Metric استفاده می کند . منظور از Hop تعداد روترهایی که در مسیر وجود دارند . در RIP هر مسیری که دارای تعداد Hop یا تعداد Router کمتری باشد دارای Metric کوچکتر و مسیر بهتری می باشد .

جدول Metric در Routing Protocolهای مختلف :

Routing Protocol Metrics

Routing Protocol	Metric
RIPv1	Hop count.
RIPv2	Hop count
IGRP	Bandwidth, delay, load, reliability, MTU.
EIGRP	Bandwidth, delay, load, reliability, MTU.
OSPF	Cost. (The Cisco default states that the cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost.)
IS-IS	Cost.

Administrative distance

Routerهای شرکت سیسکو از واحد دیگری برای انتخاب بهترین مسیر به مقصد بین چندین Routing Protocol به نام Administrative distance استفاده میکنند . در این حالت برای رسیدن به یک مقصد مسیرهای مختلفی در داخل جدول مسیریابی روترها وجود دارد که توسط پروتکلهای مسیریابی مختلف به دست آمده است که در این شرایط روترهای شرکت سیسکو برای انتخاب بهترین مسیر بین چندین Routing Protocol از واحد Administrative distance استفاده خواهد کرد و از مسیری که دارای Administrative distance کمتری میباشد استفاده خواهد کرد . Administrative distance یک روش اختصاصی شرکت سیسکو برای رتبه بندی پروتکل ها و منابع Routing میباشد و عددی بین 0 تا 255 است که در جدول زیر مقادیر آن را برای هر پروتکل مشاهده می کنید :

Administrative Distance

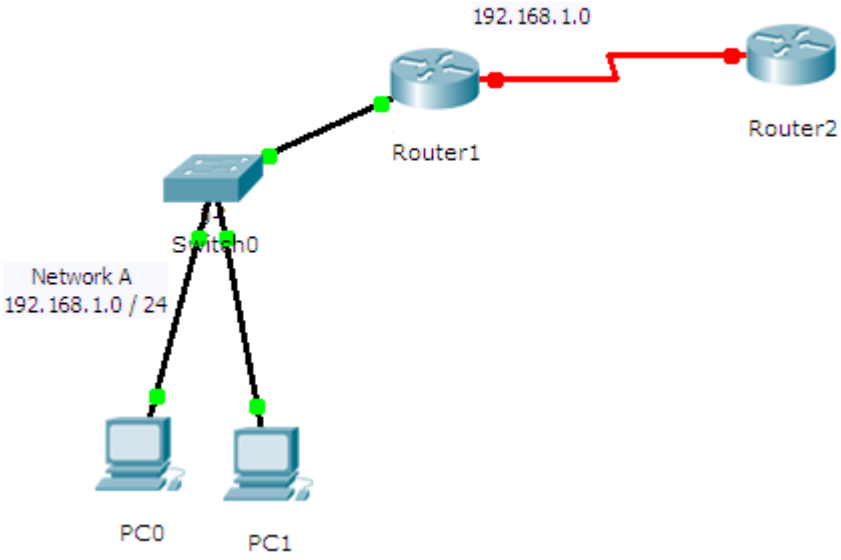
Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1, RIPv2	120
External EIGRP	170
Internal BGP	200
Unknown	255

تفاوت پروتکل های مسیریابی Classful با Classless

کلیه Routing protocolها به دو دسته زیر تقسیم می شوند :

1. Classful Routing protocol

پروتکل های Classful در زمان تبلیغ شبکه ها به سایر روترها همراه آدرس شبکه بخش Subnet Mask مربوط به شبکه ارسال نمی شود . به شکل زیر توجه کنید Router 1 در زمان تبلیغ شبکه 192.168.1.0/24 برای Router 2 فقط آدرس شبکه آن را که 192.168.1.0 است ارسال میکند و قسمت Subnet mask مربوط به شبکه که 24/ است را ارسال نمی کند :



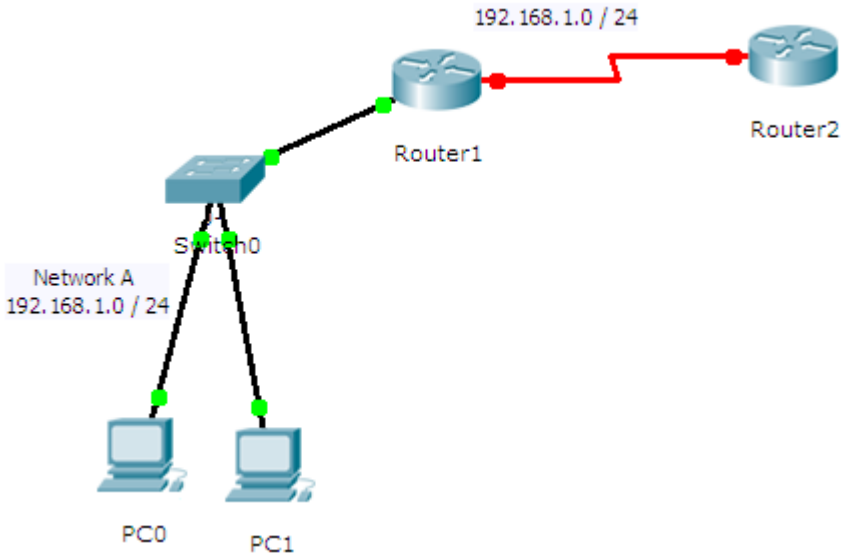
نکته :

پروتکل های مسیریابی Classful توانایی پشتیبانی از VLSM که استفاده از Maskهای با طول متغیر می باشد را نخواهد داشت .

پروتکل های مسیریابی RIP Ver 1 و IGRP از جمله پروتکل های Classful هستند.

2. Classless Routing protocol

پروتکل های Classless در زمان تبلیغ شبکه ها به سایر روترها همراه آدرس شبکه بخش Subnet Mask مربوط به شبکه ارسال می شود . به شکل زیر توجه کنید Router 1 در زمان تبلیغ شبکه 192.168.1.0/24 برای Router 2 همراه با آدرس شبکه که 192.168.1.0 است قسمت Subnet mask مربوط به شبکه که /24 است را نیز ارسال می کند :



نکته :

پروتکل های مسیریابی Classless توانایی پشتیبانی از VLSM که استفاده از Maskهای با طول متغیر می باشد را خواهد داشت .

پروتکل های مسیریابی RIP Ver 2 و EIGRP و OSPF و BGP از جمله پروتکل های Classless هستند.

EIGRP

Enhanced Interior Gateway Routing Protocol

پروتکل مسیریابی EIGRP پروتکل اختصاصی شرکت سیسکو می باشد . شرکت سیسکو کلیه توانمندی های محبوب پروتکل های Link State و Distance Vector را در این پروتکل قرار داده و آن را صورت یک پروتکل اختصاصی ارائه نموده است .

پروتکل EIGRP از الگوریتم DUAL که برگرفته از عبارت Diffusing Update Algorithm می باشد برای انتخاب بهترین مسیر استفاده خواهد کرد . یکی از نقاط مثبت این پروتکل ارسال تغییرات (Parttial Update) به روترهای همسایه یا Neighbor Router به جای ارسال کل جدول مسیریابی می باشد.

روترهایی که پروتکل EIGRP بر روی آنها فعال است قادر به برقراری رابطه مجاورت با روترهای همسایه می باشد که این رابطه مجاورت یا همسایگی به Neighbor Relationship معروف می باشد .

خصوصیات پروتکل EIGRP :

- پیکربندی راحت و بسیار ساده
- پشتیبانی و قابل استفاده در شبکه LAN و WAN و توپولوژی های مختلف
- پروتکل EIGRP یک پروتکل Classless می باشد . به عبارتی این پروتکل همراه پیام های Update ارسالی اطلاعات Subnet Mask را نیز ارسال خواهد کرد و به همین علت این پروتکل از VLSM پشتیبانی می کند .
- پروتکل EIGRP قادر به مسیریابی در شبکه های IP و IPX و Apple talk می باشد .

- پروتکل EIGRP روترهای همسایه را توسط پیام های Hello شناسایی میکند که این توانمندی به نام Neighbor Discovery معروف است .
- پروتکل EIGRP دارای سرعت همگرایی (Convergence Time) بالا می باشد.
- پروتکل EIGRP به صورت اتوماتیک Route Summarization را انجام خواهد داد .
- هر روتر EIGRP دارای سه عدد جدول به نام های Neighbor Table و Topology Table و Routing Table می باشد.
- پروتکل EIGRP از پیام های Multicast و Unicast برای Update جدول مسیریابی استفاده میکنند .
- پروتکل EIGRP از Metric پیشرفته برای انتخاب بهترین مسیر استفاده خواهد کرد . برای محاسبه Metric و انتخاب بهترین مسیر از پارامترهای Bandwidth و Delay به صورت پیش فرض استفاده میکند .
- EIGRP امکان load Balancing بر روی 6 مسیر با ارزش مساوی (Equal Cost Path) و 6 مسیر با ارزش نامساوی (Unequal Cost Path) را دارا می باشد .
- پروتکل EIGRP قادر به فعالیت در شبکه های بزرگ و گسترده می باشد .
- پروتکل EIGRP با پروتکل قدیمی IGRP سازگار می باشد .

Configuring EIGRP :

Router (config) # Router EIGRP As – number

این دستور باعث فعال شدن EIGRP بر روی Router خواهد شد و منظور از As که برگرفته از عبارت Autonomous System است شماره ای بین 0 تا 65535 می باشد که انتخاب این عدد اختیاری می باشد و برای تعیین مجموعه روترهایی که اطلاعات پروتکل مسیریابی EIGRP را با یکدیگر به اشتراک می گذارند استفاده می شود و این عدد برای تمام Routerهایی که در یک As می باشند یکسان می باشد .

Router (config – router) # Network IP – Address [WildCard – Mask]

این دستور باعث می شود شبکه (IP – Address) که به صورت مستقیم به Router متصل میباشد همراه با Subnet Mask مربوط به آن توسط پروتکل EIGRP به روترهای همسایه اعلام یا تبلیغ شود . می توانیم به جای استفاده از WildCard – Mask از Subnet Mask استفاده کنیم که بعد از وارد نمودن Subnet Mask خود روتر آنها را به WildCard – Mask تبدیل خواهد کرد . استفاده از WildCard – Mask اختیاری است در صورتی که از WildCard – Mask استفاده نشود پروتکل EIGRP از آدرس هایی با کلاس استاندارد یعنی Classful استفاده خواهد نمود .

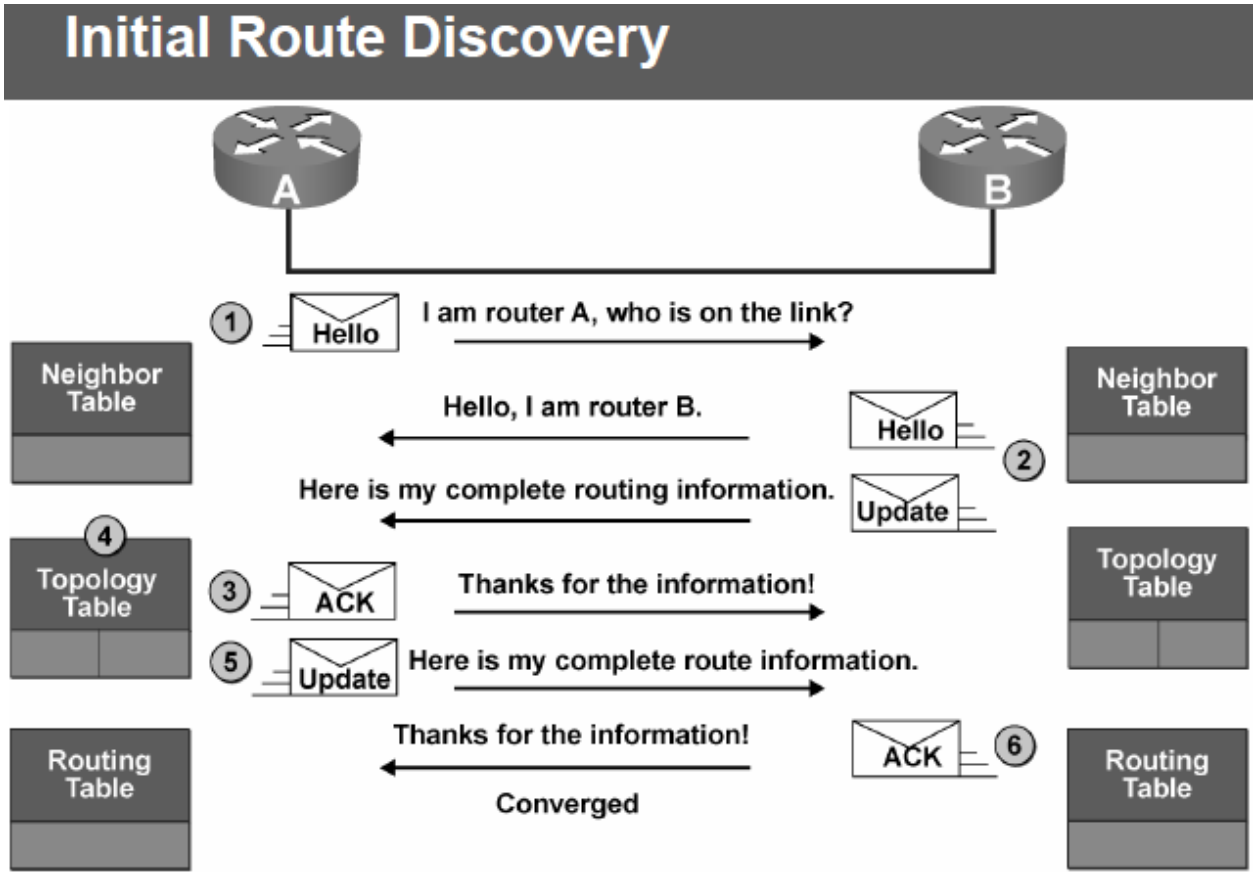
نکته : در صورتی که از WildCard – Mask در EIGRP برای تعیین شبکه ها استفاده نشود پروتکل EIGRP از کلاس استاندارد استفاده خواهد نمود . مثال در صورت تعیین نشدن WildCard – Mask بین دو شبکه زیر تفاوتی وجود نخواهد داشت :

192.168.1.0 / 24

192.168.0.0 / 16

Neighbor Relationship

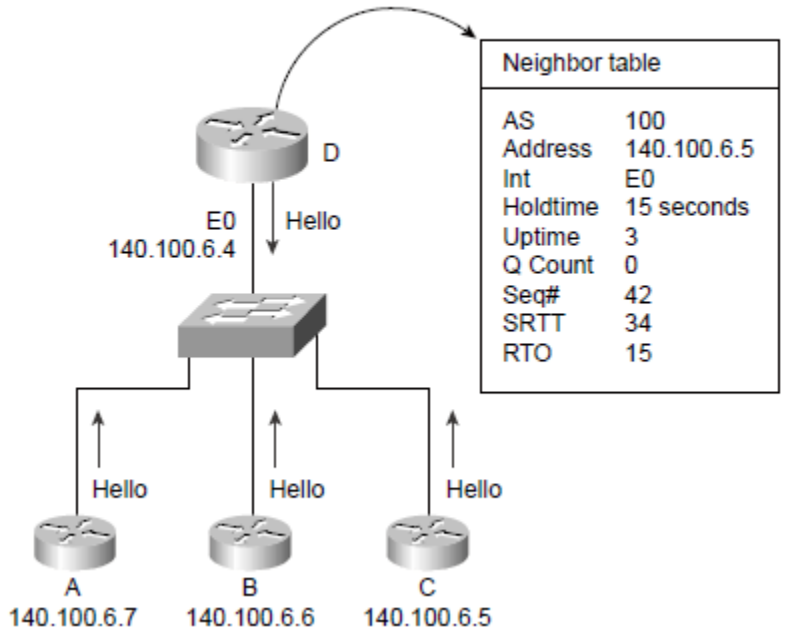
مراحل برقراری رابطه مجاورت یا همسایگی و ایجاد جداول :



مرحله اول :

همانطور که در شکل بالا مشاهده می کنید Router A اقدام به ارسال یک پیام Hello برای Router B می کند و Router B نیز اقدام به ارسال پیام Hello به Router A می کند . بعد از بیان این مرحله رابطه مجاورت Adjacency بین Router A و Router B برقرار خواهد شد و جدول Neighbor Table در پایان این مرحله ساخته خواهد شد.

Building the Neighbor Table



در شکل بالا جدول Neighbor table در Router D تشکیل شده است .

مرحله دوم :

در این مرحله Router B اقدام به ارسال پیام Update شامل اطلاعات شبکه هایی که از آنها اطلاع دارد به سمت Router A می نماید .

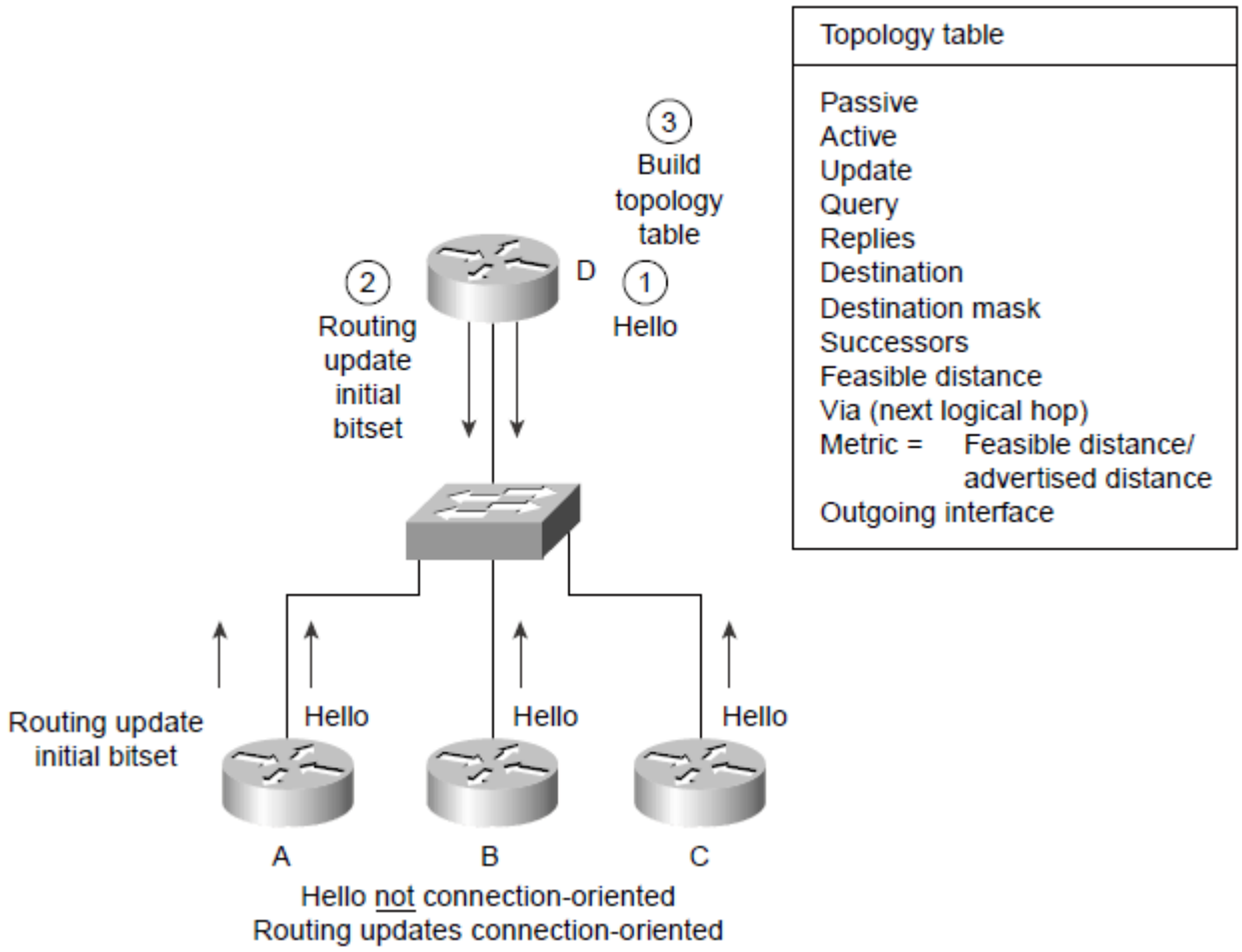
مرحله سوم :

در این مرحله Router A بعد از دریافت پیام Update یک پیام ACK به سمت Router B ارسال می کند و دریافت صحیح پیام Update را تصدیق می کند .

مرحله چهارم :

در این مرحله با استفاده از اطلاعات دریافت شده از Router B جدول Topology Table در Router A ایجاد خواهد شد که شامل کلیه مسیرها می باشد .

EIGRP—Updating the Topology Table with a New Router



در شکل بالا جدول Topology table در Router D تشکیل شده است .

مرحله پنجم :

در این مرحله Router A اقدام به ارسال پیام Update شامل اطلاعات شبکه هایی که از آنها اطلاع دارد به سمت Router B می نماید .

مرحله ششم :

در این مرحله Router B بعد از دریافت پیام Update یک پیام ACK به سمت Router A ارسال میکند و دریافت صحیح پیام Update را تصدیق می کند و با استفاده از پیام های دریافت شده از Router A جدول Topology Table در Router B ایجاد خواهد شد .

در مرحله آخر بر روی Topology Table هر دو روتر بعد از محاسباتی که با الگوریتم DUAL انجام خواهد شد بهترین مسیرهای موجود برای هر مقصد مشخص میشود و در جدول Routing Table هر دو روتر قرار خواهد گرفت .

از این به بعد فقط بسته های Helloبرای اطمینان از زنده بودن همسایه ها به هم ارسال میکنند .

پارامترهایی که در Neighborship چک می شود:

- As – Number
- Subnet Mask
- K – Values
- Authettication

انواع پیام ها در EIGRP :

- Hello : روترهای EIGRP برای شناسایی همسایگان خود از پیام Hello استفاده میکنند که این پیام ها به صورت Multicast به آدرس 224.0.0.10 برای کلیه روترها ارسال خواهد شد و پیام Hello نیازی به تصدیق یا Acknowledgment نخواهد داشت .

بسته های Hello هر 5 ثانیه یک بار ارسال می شوند. هر روتری بعد از مدت 3 عدد Hello – time یعنی 15 ثانیه از روتر همسایه بسته Hello دریافت نکند فرض را بر آن می دارد که ارتباط با همسایه قطع است و اطلاعات مربوط به آن را پاک می کند . در این پروتکل مهم نیست که مدت زمان Hello – time و Hold – time بین دو روتر همسایه با هم برابر باشد.

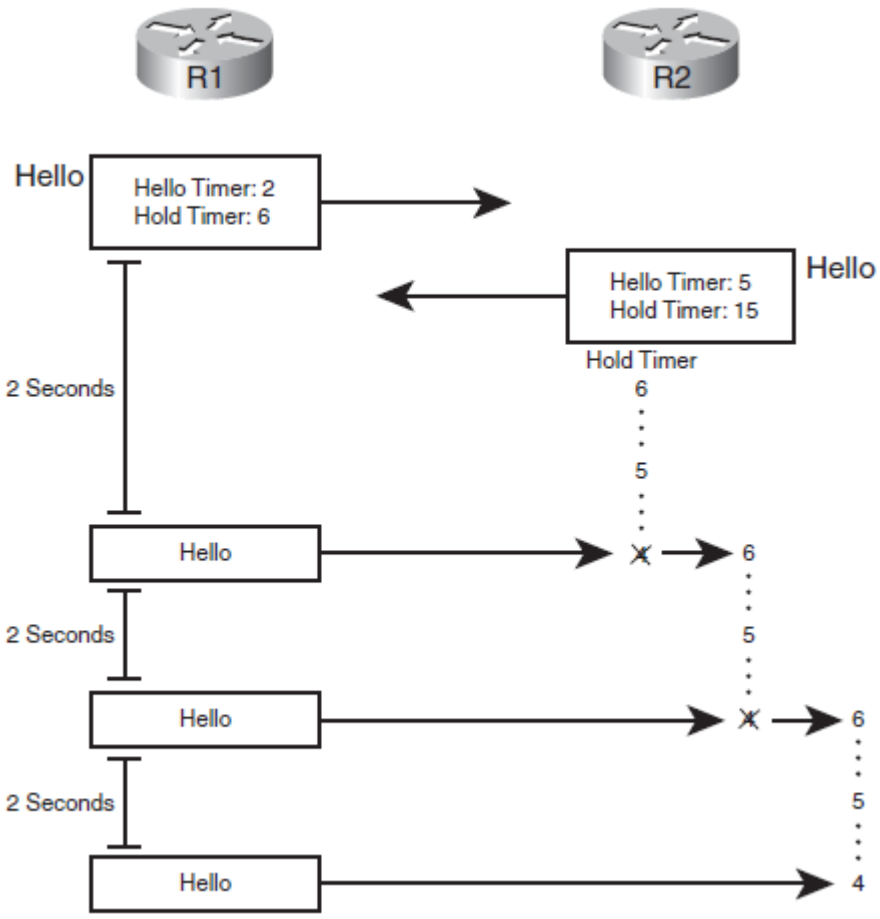
نکته :

یک روتر بر روی اینترفیس های مختلف می تواند Hello – timeهای متفاوتی داشته باشد.

در لینک های شبکه WAN که B.W < T1 = 1.544 Mbps می باشد مدت Hello – time = 60 s و مدت Hold – time = 180 s است .

دستور نمایش Hello – time و Hold – time :

Router # Show IP EIGRP Interface Detail type mod/num



در شکل بالا مشاهده می کنید که در Router 1 مدت زمان Hello و Hold را به 2 و 6 ثانیه تغییر داده ایم .

معمولا بهتر است که مقدار Hello و Hold به نسبت 1 به 3 تعیین کنیم . باید در تعیین مقدار آنها مواظب و

دقیق باشیم چون اگر زمان ها را اشتباهی محاسبه کنیم و تغییر دهیم ممکن است همسایگی از بین برود و دوباره برقرار شود و این Loop ادامه پیدا کند و باعث از کار افتادگی شبکه می شود.

نکته مهم :

در Hello روتر خودش را موظف می کند که به همان اندازه زمان تعیین شده در Hello – time بسته های Hello را برای روتر همسایه بفرستد .ولی در Hold – time روتر همسایه را موظف میکند که در مدت زمان تعیین شده در Hold – time اگر از من بسته Hello دریافت نکردی من را Down کن .

Hello و Hold مقادیری هستند که روی اینترفیس ها باید تعریف و یا تغییر داده شوند.

دستور تغییر Hello و Hold :

Router (config) # Interface type mod/num

Router (config – if) # IP Hello – interval eigrp As – num seconds

Router (config – if) # IP Hold – time eigrp As – num seconds

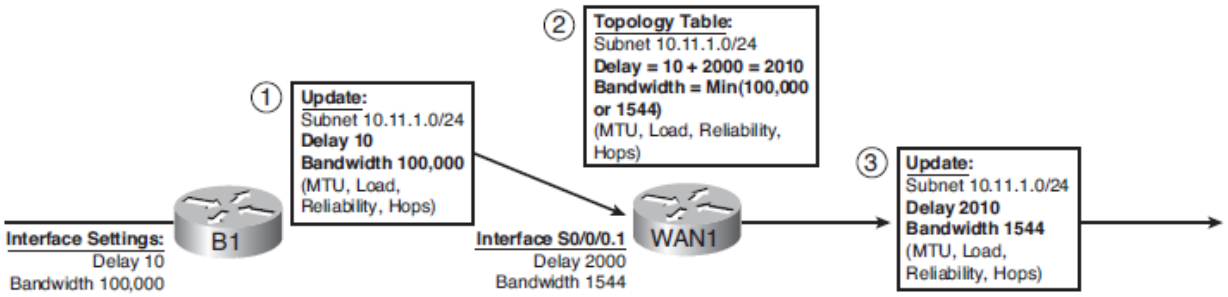
مثال :

Router (config) # Interface serial 0/0

Router (config – if) # IP Hello – interval eigrp 1 2

Router (config – if) # IP Hold – time eigrp 1 6

Update : این پیام شامل اطلاعات مربوط به شبکه می باشد که به روترها به شکل Unicast ارسال خواهد شد . پیام Update نیاز به تصدیق یا ACK دارد .



Contents of EIGRP Update Messages

در شکل بالا مشاهده میکنید که روتر B1 پیام Update خود را به روتر WAN 1 می فرستد و روتر WAN 1 نیز بعد از قرار دادن اطلاعات جدید در جدول Topology Table خود پیام Update جدید را به دیگر روترها ارسال می کند .

در بسته های Update هر روتر به روتر همسایه اطلاعات زیر ارسال می شود:

Prefix = Subnet Number

Prefix Length = Subnet Mask

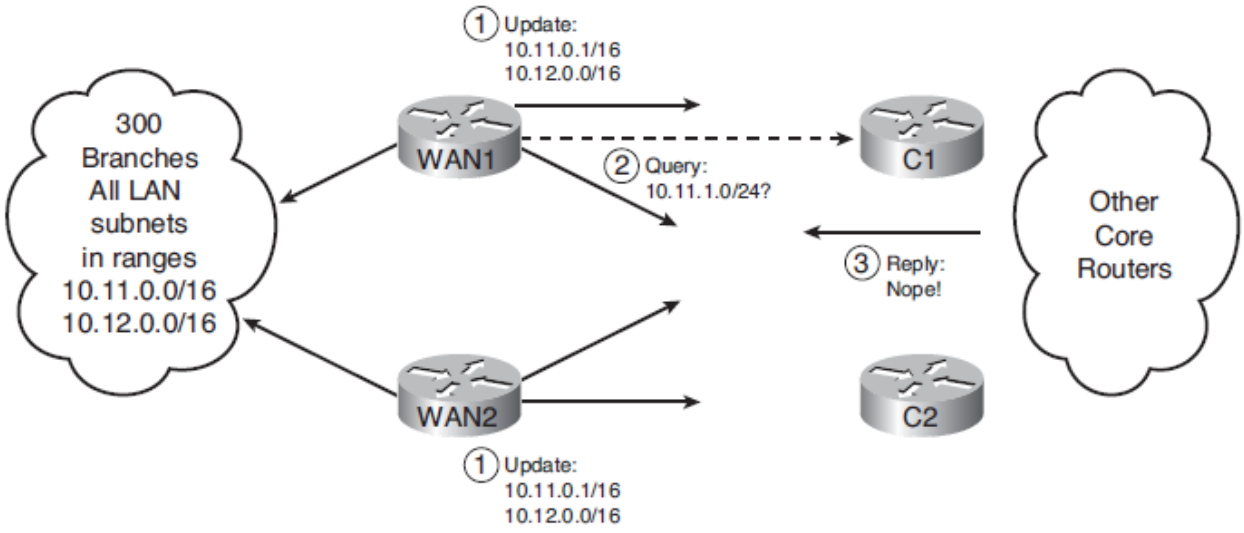
Metric Components = Min B.W , Delay , Load , Reliability

Non – Metric Components = Hop Count , MTU

- Query : این پیام در صورتی که مسیر اصلی یا Successor مربوط به یک مقصد دچار مشکل شود و مسیر جایگزین یا Feasible Successor در جدول Topology table روتر وجود نداشته باشد . روتر از طریق پیام Query روترهای همسایه را برای یافتن یک مسیر جایگزین پرسش یا Query می کنند . پیام های Query اکثرا به صورت Multicast میباشد ولی در برخی مواقع می تواند به صورت Unicast نیز باشد .

- Reply : این پیام در پاسخ به یک پیام Query به روتر ارسال کننده پیام Query ارسال خواهد شد و این پاسخ به صورت Unicast می باشد .

- ACK : که برگرفته از Acknowledgment میباشد در پاسخ به دریافت پیامهای Update و Query و Reply به روتر ارسال کننده این پیام ها ارسال می شود .



در شکل بالا روتر WAN1 پیام Query می فرستد که چه کسی به شبکه 10.11.1.0/24 مسیر دارد و روتر C1 با پیام Reply جواب می دهد .

EIGRP Table

هر روتری که پروتکل EIGRP بر روی آن پیکربندی شده باشد دارای سه جدول به شرح زیر است :

- Neighbor Table
- Topology Table
- Routing Table

Example: EIGRP Tables

Router C Tables:

IP EIGRP Neighbor Table

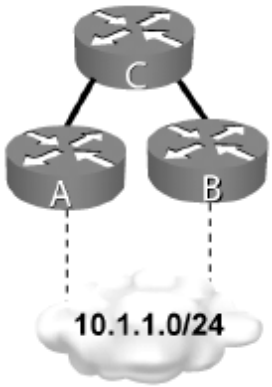
Next-Hop Router	Interface
Router A	Ethernet 0
Router B	Ethernet 1

IP EIGRP Topology Table

Network	Feasible Distance (EIGRP Metric)	Advertised Distance	EIGRP Neighbor
10.1.1.0 /24	2000	1000	Router A (E0)
10.1.1.0 /24	2500	1500	Router B (E1)

IP Routing Table

Network	Metric (Feasible Distance)	Outbound Interface	Next Hop (EIGRP Neighbor)
10.1.1.0 /24	2000	Ethernet 0	Router A



در این شکل جدول های EIGRP روتر C نمایش داده شده است.

Neighbor Table

هر روتری که پروتکل EIGRP بر روی آن پیکربندی شده است یک جدول به نام Neighbor Table ایجاد خواهد شد که شامل لیستی از روترهای همسایه می باشد که با این روتر رابطه مجاورت برقرار نموده اند .

برای مشاهده جدول Neighbor Table از دستور زیر استفاده می کنیم :

Verifying EIGRP: show ip eigrp neighbors

```
R1#show ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address         Interface   Hold  Uptime    SRTT   RTO  Q  Seq
                                (sec)           (ms)       Cnt Num
0   192.168.1.102   Se0/0/1     10    00:07:22   10   2280  0  5
R1#
```

خروجی دستور Show IP eigrp neighbors را در بالا مشاهده می کنید .

در خروجی دستور میبینیم که روتر با روتری که IP Address آن 192.168.1.102 است رابطه مجاورت و همسایگی دارد که از طریق لینک Se 0/0/1 به آن متصل است .

Topology Table

روترهای EIGRP بعد از تشکیل همسایگی مسیرهایی را که شناسایی کرده اند و از آنها اطلاع دارند را با پیام های Update به روترهای همسایه ارسال می کنند که روترها با دریافت این اطلاعات جدولی را به نام Topology Table ایجاد خواهند نمود که این جدول شامل کلیه مسیرها برای رسیدن به مقصدهای مختلف می باشد.

برای مشاهده جدول Topology Table از دستور زیر استفاده می کنیم :

Verifying EIGRP: show ip eigrp topology

```
R1#show ip eigrp topology
IP-EIGRP Topology Table for AS(100)/ID(192.168.1.101)
Codes: P - Passive, A - Active, U - Update, Q - Query, R -
Reply,
       r - reply Status, s - sia Status
P 192.168.1.96/27, 1 successors, FD is 40512000
        via Connected, Serial0/0/1
P 192.168.1.0/24, 1 successors, FD is 40512000
        via Summary (40512000/0), Null0
P 172.16.0.0/16, 1 successors, FD is 28160
        via Summary (28160/0), Null0
P 172.16.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0
P 172.17.0.0/16, 1 successors, FD is 40514560
        via 192.168.1.102 (40514560/28160), Serial0/0/1
```

در خروجی دستور Show IP eigrp topology همانطور که مشاهده میکنید یکسری Codes وجود دارد . P یعنی Passive یعنی روتر برای رسیدن به آن شبکه یک مسیر فعال دارد . A یعنی Active یعنی برای یک شبکه خاص مسیر وجود ندارد و یا دچار مشکل شده است .

Routing Table

روترهای EIGRP دارای جدول دیگری به نام Routing Table می باشد که شامل بهترین مسیرها را برای دسترسی به مقصدهای مختلف می باشد که این مسیرها بعد از محاسبه الگوریتم DUAL بر روی جدول Topology Table بهترین مسیر(Successor) برای هر مقصد در داخل جدول Routing Table قرار می گیرد .

برای مشاهده جدول Routing Table از دستور زیر استفاده می کنیم :

Verifying EIGRP: show ip route eigrp

```
R1#show ip route eigrp
D    172.17.0.0/16 [90/40514560] via 192.168.1.102, 00:07:01, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:05:13, Null0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.1.0/24 is a summary, 00:05:13, Null0

R1#show ip route
<output omitted>
Gateway of last resort is not set
D    172.17.0.0/16 [90/40514560] via 192.168.1.102, 00:06:55, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 00:05:07, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.96/27 is directly connected, Serial0/0/1
D       192.168.1.0/24 is a summary, 00:05:07, Null0
```

اگر فقط دستور Show IP Route را بنویسیم تمام بهترین مسیرها را نمایش میدهد اما اگر Show IP Route eigrp را بنویسیم فقط بهترین مسیرهایی که از طریق پروتکل EIGRP به دست آمده را نمایش می دهد .

دستورات مانیتورینگ :

با دستور Show IP Protocols کلیه پروتکل هایی که بر روی Router فعال می باشد را نمایش می دهد :

Verifying EIGRP: show ip protocols

```
R1#show ip protocols
Routing Protocol is "eigrp 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 100
  EIGRP NSF-aware route hold timer is 240s
<output omitted>

Maximum path: 4
  Routing for Networks:
    172.16.1.0/24
    192.168.1.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    (this router)         90      00:09:38
    Gateway         Distance      Last Update
    192.168.1.102         90      00:09:40
  Distance: internal 90 external 170
```

با این دستور تمام اطلاعات مربوط به پروتکل های فعال بر روی روتر را می توانیم مشاهده کنیم .

با دستور Show IP eigrp interface [type mod/num] می توانیم اینترفیس های فعال و اطلاعات مربوط به آنها را که در EIGRP هستند مشاهده کنیم :

Verifying EIGRP: show ip eigrp interfaces

```
R1#show ip eigrp interfaces
IP-EIGRP interfaces for process 100
                        Xmit Queue   Mean   Pacing Time   Multicast    Pending
Interface        Peers  Un/Reliable  SRTT   Un/Reliable  Flow Timer   Routes
Fa0/0              0        0/0         0       0/10          0           0
Se0/0/1            1        0/0        10      10/380        424          0
```

این دستور آمار ترافیک مربوط به EIGRP را نمایش می دهد :

Verifying EIGRP: show ip eigrp traffic

```
R1#show ip eigrp traffic
IP-EIGRP Traffic Statistics for AS 100
  Hellos sent/received: 429/192
  Updates sent/received: 4/4
  Queries sent/received: 1/0
  Replies sent/received: 0/1
  Acks sent/received: 4/3
  Input queue high water mark 1, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 113
  PDM Process ID: 73
```

Metric

پروتکل EIGRP از الگوریتم DUAL یا Diffusing Update Algorithm استفاده می کند که بهترین مسیر که کمترین Metric را داشته باشدبه عنوان Successor انتخاب و مسیرهای دیگر را که Metric کمتری دارند را به عنوان Fesible Successor یا مسیر جایگزین انتخاب می کند .

EIGRP برای محاسبه Metric از روش ترکیبی استفاده می کند که شامل 5 پارامتر است که به صورت پیش فرض از 2 پارامتر Bandwidth و Delay برای محاسبه Metric استفاده می کند . پارامترهای دیگر شامل Load و Reliability و MTU (که برگرفته از عبارت Maximum Transmission Unit می باشد) هستند که توصیه می شود از این پارامترها به علت احتمال کاهش کارایی مسیریابی استفاده نشود .

EIGRP Metric Values

Metric Symbol	Metric Value	Description
K1	Bandwidth	Selects the smallest bandwidth media between the source and destination hosts. The equation used is [10000000 ÷ bandwidth kbps] × 256.
K2	Loading	Is based on the statistics held at the outgoing interface and is recorded in bits per second.
K3	Delay	Is the delay calculated on the outgoing interface. The value used is the cumulative total of the delay on all the interfaces between the hosts. The delay is measured in units of 10 ms to 168 seconds. A delay of all ones in the 32 bit field means the network is unreachable.
K4	Reliability	Is based on the statistics held on the outgoing interface gained from keepalives, and is exponentially averaged over 5 minutes.
K5	MTU	Is the smallest MTU found configured on an interface along the route. This value is included although it has not been used as part of the metric calculation.

همانطور که در جدول بالا مشاهده می کنید پارامترها به صورت K Valueها مشخص شده اند که تنظیم پیش فرض برای محاسبه Metric در پروتکل EIGRP به صورت زیر است :

By Default : K1 = 1 , K2 = 0 , K 3 = 1 , K4 = 0 , K5 = 0

همانطور که مشاهده می کنید چون مقدار K Valueهای پارامترهای Bandwidth و Delay برابر با 1 است برای محاسبه Metric در پروتکل EIGRP استفاده می شود . مقادیر مربوط به K Valueها در بسته های Hello قرار دارد که روترها به یکدیگر می فرستند و باید حتما K Valueها در بین دو روتر همسایه برابر باشند چون اگر برابر نباشد همسایگی تشکیل نمی دهند .

فرمول محاسبه Metric در EIGRP :

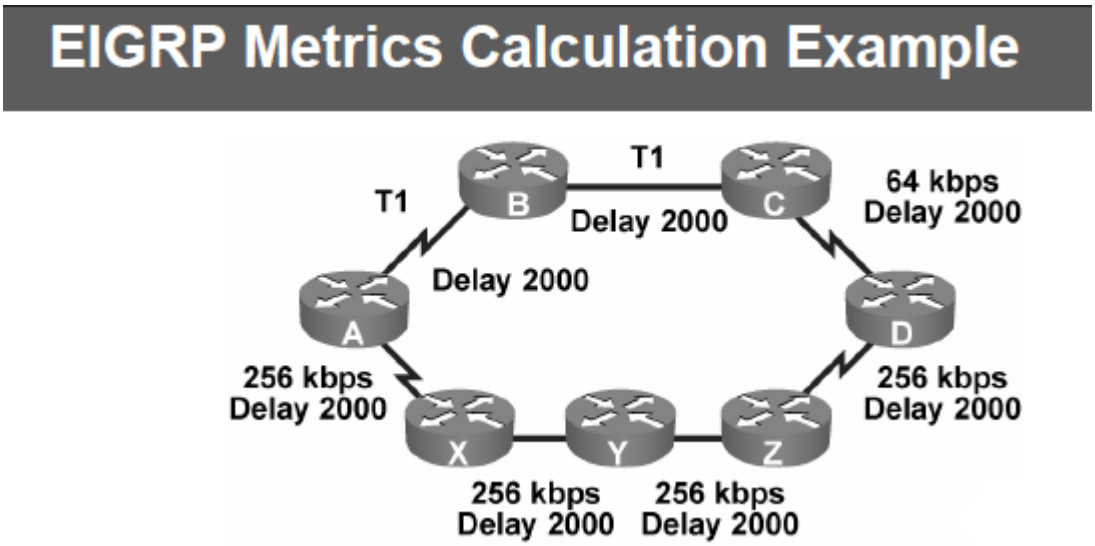
$$\text{Metric} = \left(\left(\frac{10^7}{\text{least-bandwidth}}\right) + \text{cumulative-delay}\right) * 256$$

10^7 = 10000000

Bandwidth = کمترین پهنای باند لینک های موجود در مسیر

Cumulative – Delay = مجموع کل Delay های مسیر

به مثال زیر توجه کنید :



در تصویر بالا همانطور که مشاهده میکنید دو مسیر به صورت زیر است :

1. A ⟶ B ⟶ C ⟶ D

کمترین پهنای باند مسیر معادل : 64 kbps

جمع کل Delayهای مسیر معادل : 6000

در فرمول بالا قرار می دهیم :

Bandwidth : (10000000 / 64) * 256 = 40000000

Delay : (2000 + 2000 + 2000) * 256 = 1536000

Metric = Bandwidth + Delay

Metric = 40000000 + 1536000 = 41536000

2. A → X → Y → Z → D

کمترین پهنای باند مسیر معادل : 256 kbps

جمع کل Delayهای مسیر معادل : 8000

در فرمول بالا قرار می دهیم :

Bandwidth : (10000000 / 256) * 256 = 10000000

Delay : (2000 + 2000 + 2000 + 2000) * 256 = 2048000

Metric = Bandwidth + Delay

Metric = 10000000 + 2048000 = 12048000

دستور تغییر K Valueها :

Router (Config-Router) # Metric Weights tos K1 K2 K3 K4 K5

مقدار tos همیشه برابر با صفر است .

مثال :

Router (Config-Router) # Metric Weights 0 1 1 2 1 1

تغییر Bandwidth و Delay اینترفیس ها :

در صورتی که پهنای باند اتصالات Serial برای پروتکل EIGRP مشخص نشود پروتکل EIGRP پهنای باند Serial را سرعت 1544 Kbps محاسبه خواهد کرد که با این سرعت ممکن است محاسبه Metric به درستی انجام نشود .

با استفاده از دستور زیر پهنای باند و Delay لینک ها را تعیین می کنیم :

Router (config) # Interface type mod / num

Router (config – if) # Bandwidth number

Router (config – if) # Delay Number

(Number) مقدار Bandwidth بر حسب Kbps باید نوشته شود.

(Number) مقدار Delay بر حسب 10 ms باید نوشته شود.

مثال :

Router (config) # Interface serial 2/0

Router (config – if) # Bandwidth 1024

Router (config – if) # Delay 2000

به صورت پیش فرض EIGRP از 50% پهنای باند یا Bandwidth برای ارسال پیامهای Update استفاده می کند . با دستور زیر می توانیم مقدار آن را تغییر دهیم:

Router (config) # Interface type mod / num

Router (config – if) #IP Bandwidth – Percent EIGRP As-num Percent

مثال :

Router (config) # Interface Serial 2/0

Router (config – if) #IP Bandwidth – Percent EIGRP 1 70

با این دستور 70% پهنای باند یا Bandwidth را در اختیار EIGRP قرار داده ایم برای ارسال پیام های Update بین دو روتر همسایه .

جدول مقادیر پیش فرض Bandwidth و Delay انواع اینترفیس ها :

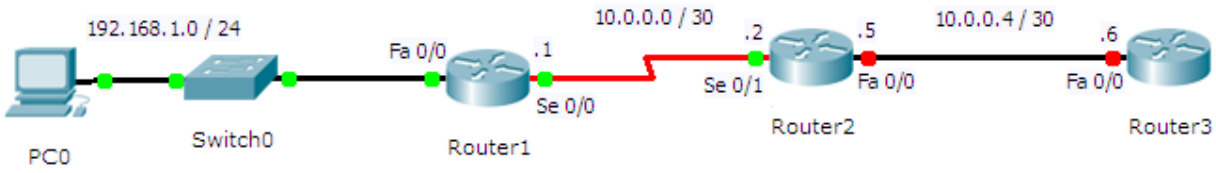
Common Defaults for Bandwidth and Delay

Interface Type	Bandwidth (Kbps)	Delay (Microseconds)
Serial	1544	20000
GigE	1,000,000	10
FastE	100,000	100
Ethernet	10,000	1000

نکته :

مقدار Delay اینترفیس های Loopback تقریبابرابر با 500 Ms است .

مثال :



در شکل بالا شبکه 192.168.1.0 / 24 از طریق اینترفیس Fastethernet 0/0 به Router 1 متصل است و Router 1 از طریق پیام Update این شبکه را به اطلاع Router 2 می رساند و Router 2 نیز از طریق پیام Update این شبکه را به اطلاع Router 3 می رساند و Router 3 این اطلاعات جدید را در جداول خود قرار می دهد پیام های Update ارسالی به صورتی که در صفحه بعد نمایش داده شده است فرستاده می شود :

بسته Update که Router 1 به Router 2 ارسال می کند :

192.186.1.0

255.255.255.0

Min B.W = 100000 kbps , Delay = 10 $_{10Ms}$, Load = 1 , Reliability = 255

Hop Count = 0 , MTU = 1500

بسته Update که Router 2 به Router 3 ارسال می کند :

192.186.1.0

255.255.255.0

Min B.W = 1544 kbps , Delay =2010 $_{10Ms}$, Load = 1 , Reliability = 255

Hop Count = 1 , MTU = 1500

بسته Update که Router 3 در جدول خود ذخیره می کند :

192.186.1.0

255.255.255.0

Min B.W = 1544 kbps , Delay =2020 $_{10Ms}$, Load = 1 , Reliability = 255

Hop Count = 2 , MTU = 1500

همانطور که مشاهده می کنید هر روتر حداقل Bandwidth را در نظر می گیرد و مقدار Delay در طول مسیر با هم جمع می شود .

Reliability : در یک مقطع زمانی که چند بار یک اینترفیس روشن و خاموش شده است را Reliability می گویند . هرچه بشتر باشد بهتر است : 255/255

Delay : مدت زمانی که طول می کشد یک بسته از اینترفیس بیرون بیاید را Delay می گویند .

نکته :

مقدار Load هرچه کمتر باشد بهتر است : 1/255

با استفاده از دستور زیر می توانیم ببینیم که با چه متریک هایی به یک IPمشخص رسیده ایم :

Router # Show IP EIGRP Topology IP – Address

حالا Metric هر روتر را نسبت به شبکه 192.168.1.0 / 24 حساب می کنیم :

Metric Router 1 = [10^7 / 100000 + 10] * 256 = 28160

Metric Router 2 = [10^7 / 1544 + 2010] * 256 = 2172416

Metric Router 3 = [10^7 / 1544 + 2020] * 256 = 2174976

Feasible Distance (FD) : فاصله خود روتر تا مقصد است .

Reported Distance یا Advertised Distance : فاصله روتر قبلی تا مقصد می باشد.

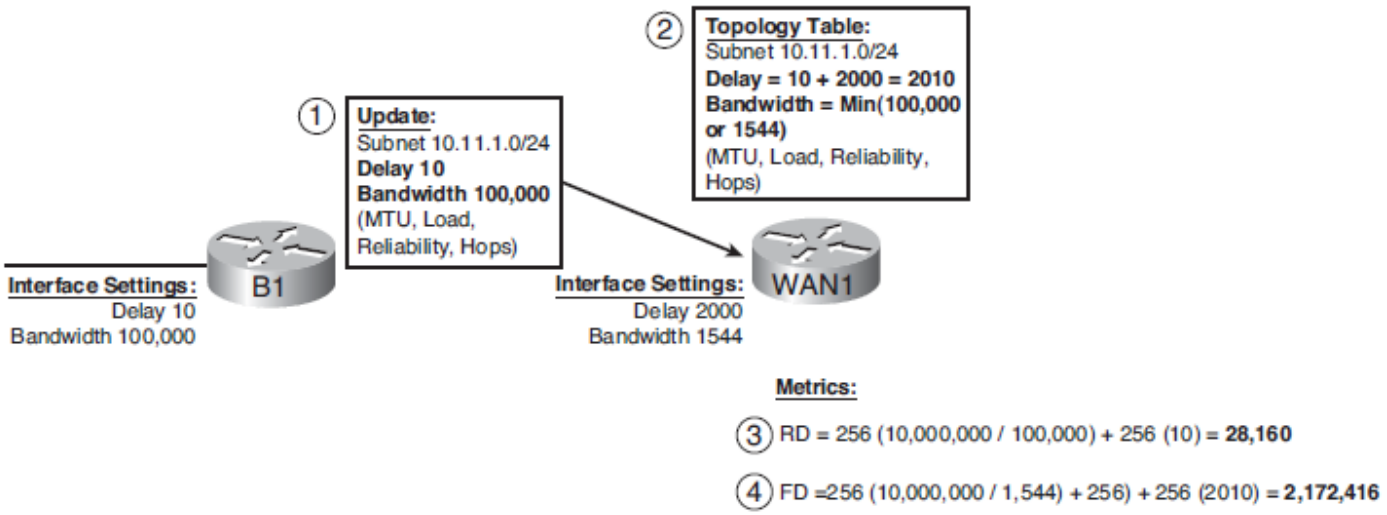
Router X ⟵ (FD / RD)

Router 1 ⟵ (28160 / 0)

Router 2 ⟵ (2172416 / 28160)

Router 3 ⟵ (2174976 / 2172416)

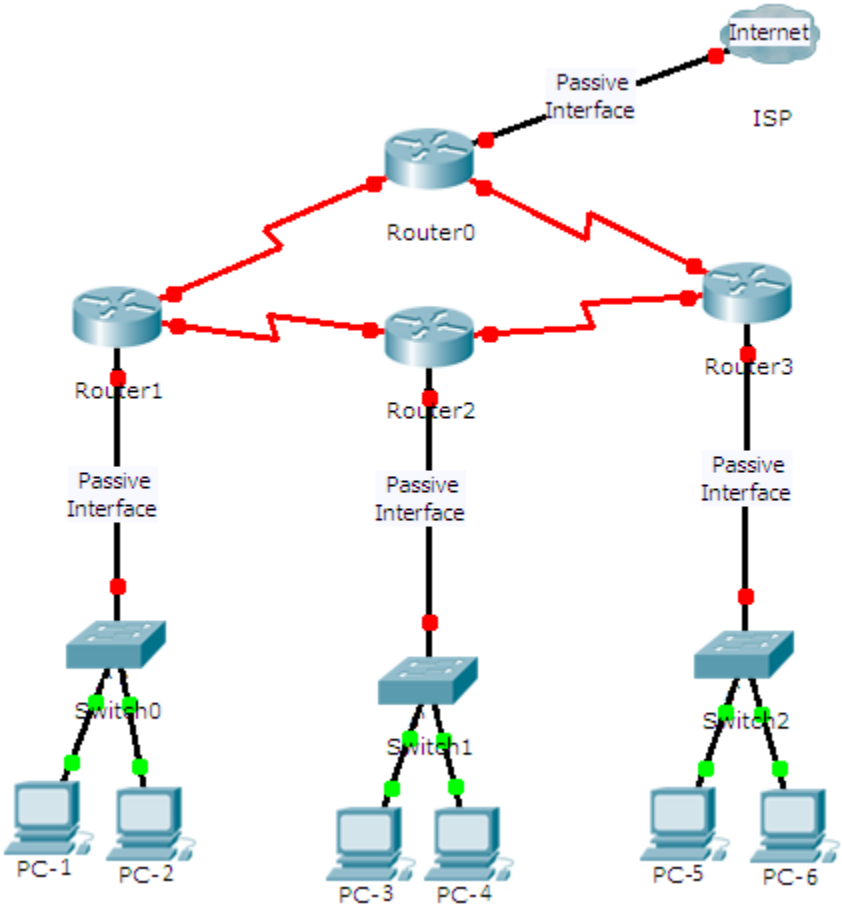
به شکل زیر توجه کنید :



Example Calculation of RD and FD on Router WAN1

در شکل بالا مشاهده می کنید که در مرحله اول Router B1 به وسیله یک پیام Update اطلاعات راجع به شبکه 10.11.1.0/24 را از طریق اینترفیس سریال به Router WAN1 می رساند . در مرحله دوم Router WAN1 اطلاعات را در جدول Topology Table خود ذخیره می کند . در مرحله سوم Router WAN 1 با استفاده از فرمول Metric می فهمد فاصله Router B1 نسبت به شبکه 10.11.1.0/24 برابر است با 28160 که به آن RD یا Reported Distance می گویند . در مرحله چهارم Router WAN 1 با استفاده از فرمول Metric خود را نسبت به شبکه 10.11.1.0/24 حساب می کند که به آن FD یا Feasible Distance می گویند که برابر 2172416 است .

Passive – Interface



به تصویر بالا نگاه کنید در این تصویر نیازی به ارسال پیام های Hello و برقراری ارتباط مجاورت از طریق برخی از اینترفیس ها نمی باشد . به علت اینکه برخی از اینترفیس ها به روترهای دیگر اتصال نخواهند داشت . ارسال مرتب اطلاعات و تلاش برای برقراری رابطه مجاورت از طریق این اینترفیس ها باعث اشغال پهنای باند لینک و همچنین افزایش بار پردازشی CPU روتر خواهد داشت .با غیر فعال کردن ارسال پیام های EIGRP بر روی برخی از اینترفیس ها علاوه بر افزایش کارایی , امنیت را نیز افزایش می دهیم .

وقتی که بر روی یک اینترفیس توانمندی Passive Interface را فعال می کنیم از ارسال و دریافت پیام های EIGRP یعنی Hello و Update جلوگیری می کند و در نتیجه رابطه مجاورت از طریق این اینترفیس تشکیل نمی شود ولی شبکه های متصل شده به این اینترفیس توسط پروتکل EIGRP تبلیغ می شود .

دو روش زیر برای فعال کردن Passive Interface بر روی اینترفیس ها وجود دارد :

روش اول :

Router (config – Router) # Passive - Interface type mod/num

در این روش یک اینترفیس خاص را Passive می کنیم .

روش دوم :

Router (config – Router) # Passive - Interface Default

Router (config – Router) # No Passive - Interface type mod/num

در این روش به صورت پیش فرض (Default) همه اینترفیس ها را Passive میکنیم بعد اینترفیس هایی را که نمیخواهیم Passive باشند را با دستور دوم غیر Passive می کنیم .

با دستور های زیر متوجه می شویم کدام اینترفیس ها Passive هستند :

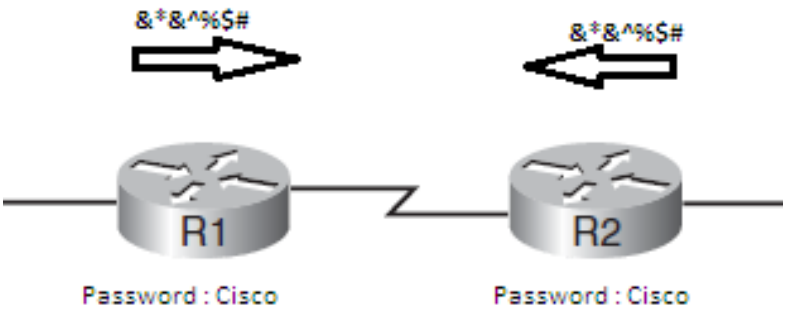
Router # Show IP Protocols

Router # Show IP Route EIGRP

Router # Show Runing – Config

EIGRP Authentication

Authentication یکی از توانمندی های پروتکل مسیریابی EIGRP برای احراز یا تصدیق هویت می باشد که با استفاده از آن روترها می توانند قبل از تبادل اطلاعات مسیریابی باید یکدیگر را تصدیق هویت کنند . در این روش پروتکل EIGRP برای Authentication از مکانیزم MD5 که برگرفته از عبارت Message Digest 5 استفاده می کند .



EIGRP Authentication

همانطور که در شکل بالا مشاهده می کنید مکانیزم MD5 کلمه رمز که در اینجا Cisco است را به صورت Hash شده و غیرقابل خواندن تبدیل می کند که امنیت بالاتری دارد . MD5 با همه بسته های EIGRP این کار را می کند .

مراحل Authentication :

1. Define Key – Chain (دسته کلید را تعریف کن)
2. Set Authentication Mode (Authentication را فعال کن چون پیش فرض غیرفعال است)
3. Set Authentication Key – Chein (تعیین کن از کدام دسته کلید استفاده کند)

دستورات اعمال Authentication در EIGRP :

بهتر است که یک دسته کلید یعنی چند عدد کلید را تعریف کنیم بجای تعریف یک کلید.

1. تعریف دسته کلید : از این دسته کلید در همه جا برای Authentication میتوانیم استفاده کنیم نه فقط در EIGRP

```
Router ( config) # Key Chain Name
Router ( config – keychain ) # Key Number
Router ( config – keychain – key ) # Key – String  String
```

مثال :

```
Router ( config) # Key Chain  Cisco
Router ( config – keychain ) # Key   1
Router ( config – keychain – key ) # Key – String  a123A@
Router ( config – keychain – key ) # Exit
Router ( config – keychain ) # Key   2
Router ( config – keychain – key ) # Key – String  b123B@
Router ( config – keychain – key ) # Exit
```

نکته : اینترفیس ها Authentication می کنند پس باید بر روی اینترفیس ها فعال شود :

2. فعال کردن Authentication :

Router (Config) # Interface Type mod/num

Router (Config – if) # IP Authentication Mode eigrp As-num MD5

3. تعیین کن از کدام دسته کلید استفاده کند :

Router (Config – if) # IP Authentication Key – Chain eigrp As-num name

مثال :

Router (Config) # Interface Serial 1/0

Router (Config – if) # IP Authentication Mode eigrp 1 MD5

Router (Config – if) # IP Authentication Key – Chain eigrp 1 Cisco

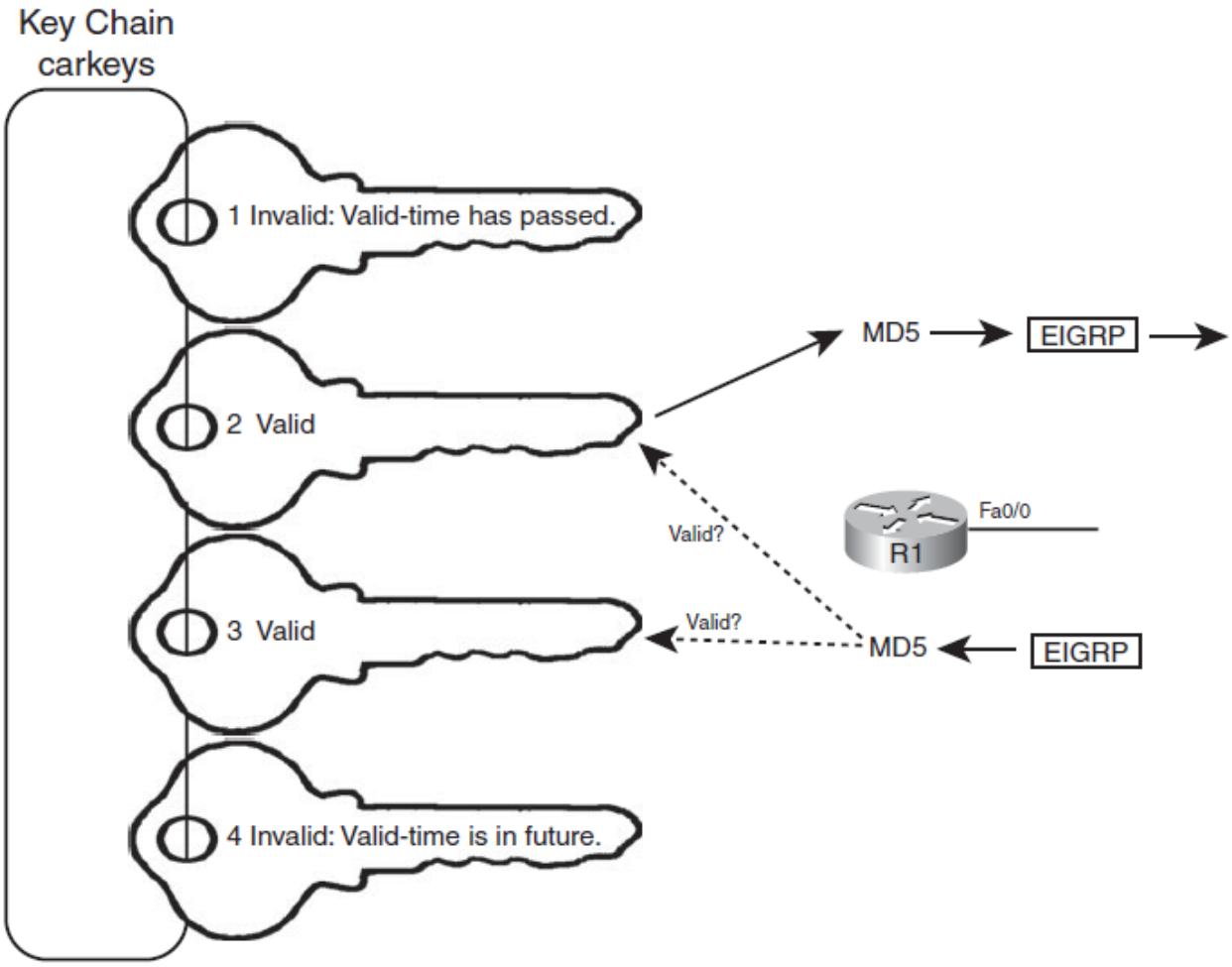
نکته :

بر روی هر دو روتر باید دستورات بالا را وارد کنیم . نام دسته کلید در دو روتر مهم نیست که یکسان باشد ولی حتما باید شماره کلید و رمز کلید یکسان باشد .

دستور نمایش دسته کلید :

Router # Show Key – Chain

به شکل زیر توجه کنید :



EIGRP's Usage of Authentication Keys

نکته :

هر روتر برای ارسال یا Send از کلید با شماره کمتر و Valid استفاده می کند ولی برای دریافت یا Accept از همه کلیدهای Valid دسته کلید برای چک کردن استفاده می کند .

دستور استفاده از کلیدها در مقاطع زمانی مختلف :

```
Router(config-keychain-key)#
accept-lifetime start-time {infinite | end-time | duration seconds}
```

- **Optional: Specifies when key will be accepted for received packets**

```
Router(config-keychain-key)#
send-lifetime start-time {infinite | end-time | duration seconds}
```

- **Optional: Specifies when key can be used for sending packets**

این دستورات اختیاری می باشد و دستور اول زمان فعال بودن پسورد را در زمان دریافت یا Accept پیام های Update بر روی روتر تعیین می کند . دستور دوم زمان فعال بودن پسورد را در زمان ارسال یا Send پیام های Update بر روی روتر تعیین می کند .

مثال :

Router (config – keychain – key) #Accept – Lifetime 04:55:00 june 22 2010 04:55:00 june 22 2011

Router (config – keychain – key) # Send – Lifetime 04:55:00 june 22 2010 04:55:00 june 22 2011

Router – ID in EIGRP

Router – ID : هر کدام از روترهای دخیل در پروسه EIGRP دارای یک شناسه یا ID برای خود می باشند که یک عدد 32 بیتی است و در فرمت Dotted – Decimal , شبیه به آدرس IP بیان می گردد .هر روتر در ابتدا شروع پروسه EIGRP اقدام به تعیین این شناسه خواهد کرد .

از سه طریق Router – ID تعریف می شود :

1. Static : با دستور زیر می توانیم Router – ID را تعریف یا تغییر دهیم و با نوشته شدن این دستور , همین شناسه مورد استفاده قرار می گیرد:

Router (config – Router) # EIGRP Router – ID A.B.C.D

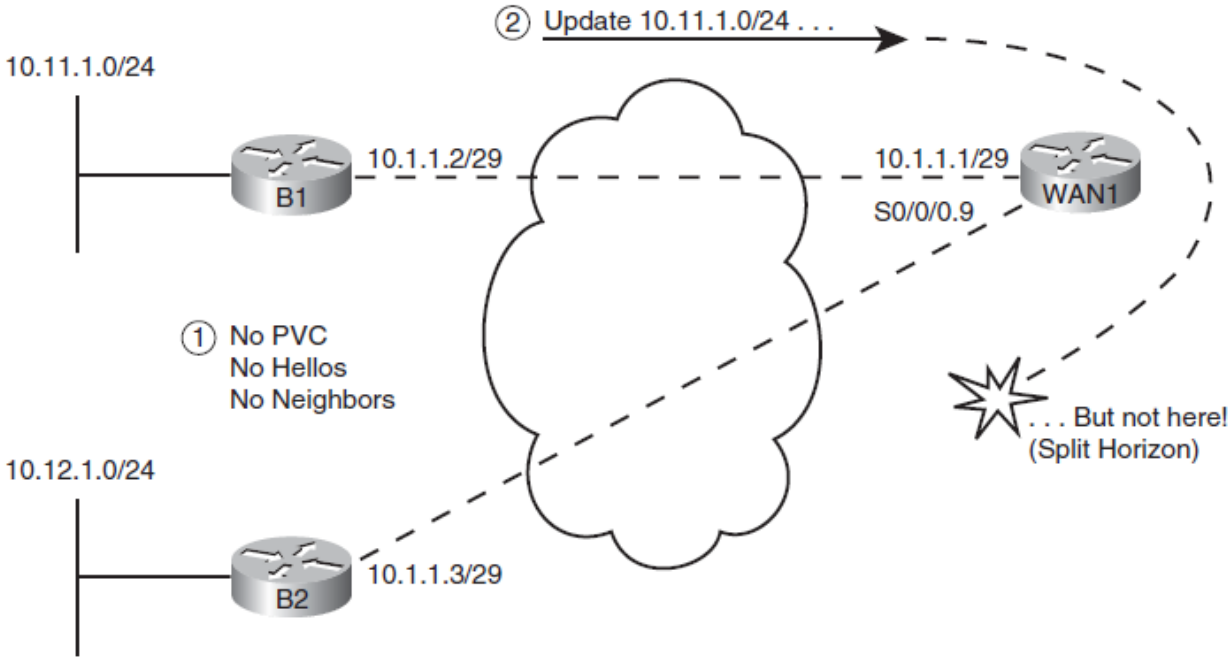
2. Highest Loopback IP – Address UP/UP : در صورت موجود بودن پورت های Loopback , بزرگترین آدرسIP مربوط به آنها به عنوان شناسه روتر تعیین می گردد .

3. Highest Non – Loopback IP – Address UP/UP : در صورت نبودن هیچ پورت Loopback , بالاترین IP مربوط به Interface های فعال (UP/UP) به عنوان شناسه روتر برگزیده خواهند شد .

Router – ID را می توانیم با دستور زیر مشاهده کنیم :

Router # Show IP EIGRP Topology

Split Horizon



: Split Horizon

یعنی اینکه اگر مسیری را از کسی (روتری) یاد گرفتی دوباره به خودش (یعنی همان روتر) یاد نده .

دستور غیرفعال کردن Split Horizon :

Router (config) # Interface type mod/num

Router (config – if) # IP Split – Horizon EIGRP As – num

NBMA : Non – Broadcast Multi Access

پروتکل EIGRP را می توان برای برقراری رابطه مجاورت با روترهای خاصی که به روش استاتیک تعیین شده اند مجبور ساخت .با استفاده از این ویژگی می توان از انتشار پیام های Multicast زیادی جلوگیری کرده و بار کمتری بر روی اتصال تحمیل نمود . یکی از مواردی که بهره گیری از این ویژگی می تواند مفید باشد اتصالات Frame Relay است .روترها در هنگام برقراری ارتباطات Frame Relay با یکدیگر باید یک کپی از پیام های Broadcast و Multicast را ایجاد کرده و به سمت هر کدام از روترهای همسایه ارسال نمایند که این کار به دلیل کم بودن پهنای باند اتصالات WAN و همچنین هزینه نسبتا زیاد این اتصالات می تواند در برخی از مواقع مشکل ساز باشد. برای نمونه در صورتی که در روی یک Subinterface اقدام به تعریف 10 عدد PVC کرده باشید ولی تنها دو عدد از این PVCها متصل به روترهای EIGRP در آنسوی ارتباط باشند این روتر به سوی هر 10 روتر مزبور اقدام به ارسال پیام های Hello که از نوع Multicast هستند خواهد کرد .

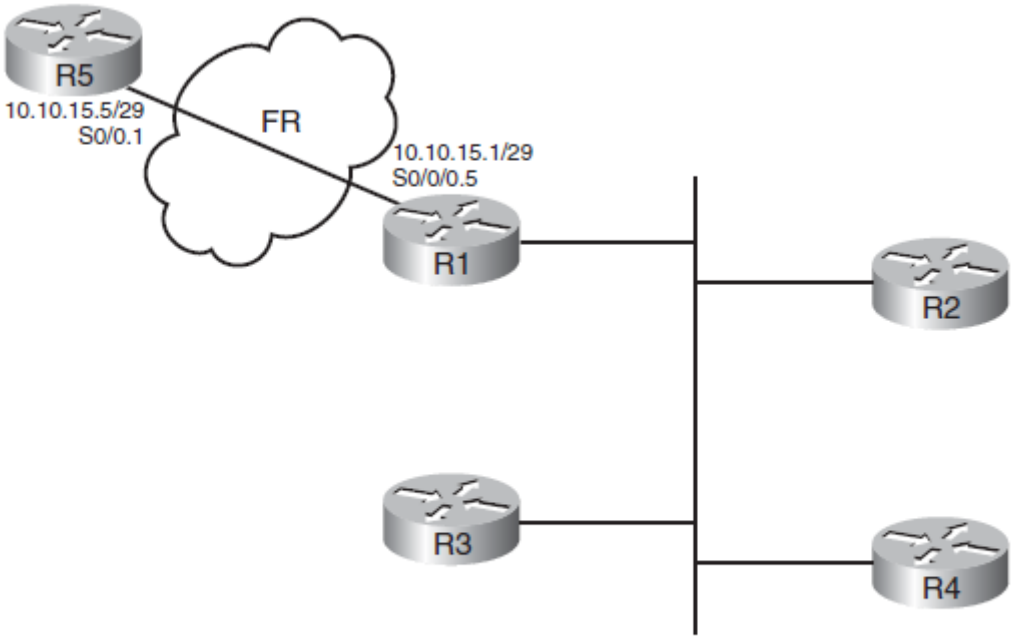
اما اگر دو روتر Remote را به روش دستی به عنوان همسایه این روتر انتخاب کنیم پیام های Hello به صورت Unicast به دو روتر یاد شده ارسال شده و از سویی دیگر هیچ پیام دیگری به سمت 8 روتر دیگر فرستاده نمی شود .

این دستور را در هر دو روتر وارد میکنیم :

Router (config – Router) # Neighbor IP – Address Outgoing – Interface

متغیر IP – Address اشاره به آدرس IP مربوط به روتر همسایه دارد .

متغیر Outgoing – Interface اشاره به پورت متصل به خود روتر دارد که از طریق آن به روتر همسایه متصل است .



Adding a Branch, with a Static EIGRP Neighbor

برای مثال در شکل بالا همسایگی بین دو روتر R1 و R5 را به صورت زیر تعریف می کنیم :

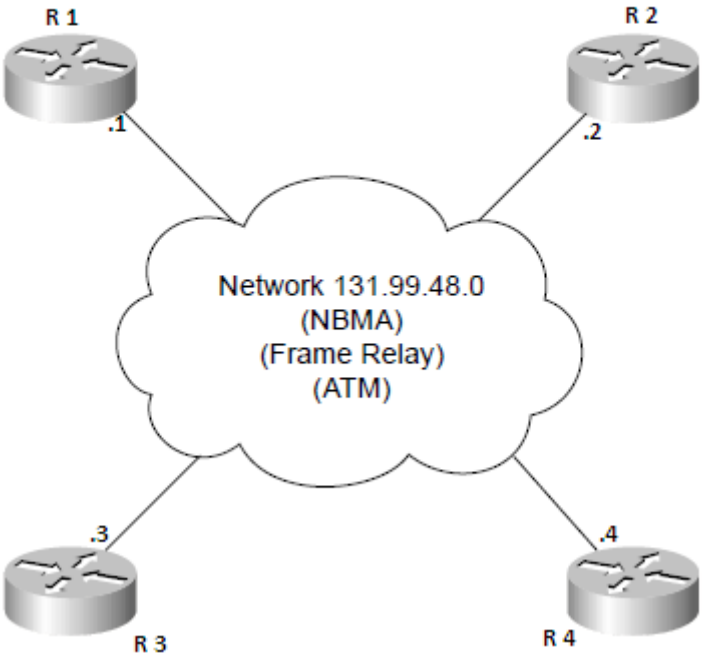
Router 1 (config – Router) # Neighbor 10.10.15.5/29 Se 0/0/0.5

Router 2 (config – Router) # Neighbor 10.10.15.1/29 Se 0/0.1

دستور مشاهده کردن همسایگی هایی که به صورت Static به وجود آمده اند :

Router # Show IP EIGRP Neighbor Detail

A Nonbroadcast Multiaccess (NBMA) Network



به شکل بالا توجه کنید در شبکه های Multi Access باید حتما برای همه روترها به صورت Static همسایگی تشکیل دهیم .

مثلا اگر برای R1 و R4 همسایگی را به صورت Static تشکیل بدهیم این دو روتر با روترهای R 2 و R3 تشکیل همسایگی نمی دهند چون روی اینترفیس های خود بسته های Hello را به آدرس Unicast هم می فرستند . پس باید برای روترهای دیگر نیز همسایگی را به صورت Static تشکیل بدهیم .

نکته :

حتما در EIGRP باید با دستور Network شبکه را Add کنیم تا تشکیل همسایگی بدهند فقط دستور Neighbor کافی نیست .

مانند مثال زیر :

R1 , R4 :

Router 1 (config) # Router eigrp 1

Router 1 (config – Router) # Neighbor 131.99.48.4 Fastethernet 0/0

Router 1 (config – Router) # Network 131.99.48.0

Router 4 (config) # Router eigrp 1

Router 4 (config – Router) # Neighbor 131.99.48.1 Fastethernet 0/0

Router 4 (config – Router) # Network 131.99.48.0

R2 , R3 :

Router 2 (config) # Router eigrp 1

Router 2 (config – Router) # Neighbor 131.99.48.3 Fastethernet 0/0

Router 2 (config – Router) # Network 131.99.48.0

Router 3 (config) # Router eigrp 1

Router 3 (config – Router) # Neighbor 131.99.48.2 Fastethernet 0/0

Router 3 (config – Router) # Network 131.99.48.0

Offset – List

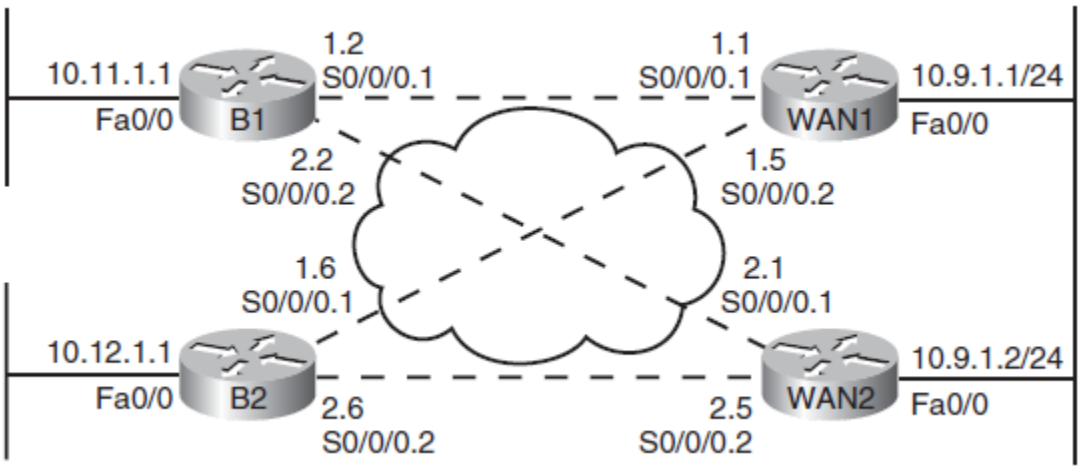
این ویژگی برای اعمال تغییر در مقدار Metric است . با استفاده از این ویژگی می توان عدد مشخصی را بر روی مقدار Metric مربوط به یک مسیر اضافه کرد . برای انجام این کار یک مدیر شبکه در ابتدا باید اقدام به تعیین لیستی شامل Prefixهای مجاز نماید و سپس عددی که بر روی Metric آنها اضافه می شود را نیز تعیین کند .

Offset – List امکان انجام موارد زیر را در اختیار ما می گذارد :

- تعیین لیستی از Prefixهای مجاز : برای انجام این کار باید اقدام به ایجاد یک IP ACL نمود که در آن لیستی از Routeهای مجاز با استفاده از دستور Permit مشخص شده باشد. به عبارتی تنها در صورتی عدد Offset بر روی مقدار Metric مربوط به یک Route اضافه خواهد شد که Route مزبور با قوانین نوشته شده در ACL مطابقت داشته باشد.
- تعیین جهت انتقال پیام های Update (ورودی و خروجی)
- مشخص کردن نام Interface مورد نظر
- تعیین مقدار عدد Offset که قرار است بر روی FD و RD افزوده گردد.

دستور Offset – List که در محیط پیکربندی EIGRP نوشته می شود :

Router (config – Router) #Offset – List {Acl num | Acl name} {in | out} offset interface



به شکل بالا نگاه کنید مقدار متریک مربوط به مسیر مابین روتر WAN 1 , روتر B1 و شبکه 10.11.1.0/24 بر روی روتر WAN 1 برابر با 2172416 محاسبه شده است . همچنین مشاهده می فرمایید که مقدار RD در مورد این Route بر روی روتر WAN 1 نیز برابر با 28160 می باشد .

```
WAN1#show ip eigrp topo 10.11.1.0/24
IP-EIGRP (AS 1): Topology entry for 10.11.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2172416
  Routing Descriptor Blocks:
  10.1.1.2 (Serial0/0/0.1), from 10.1.1.2, Send flag is 0x0
      Composite metric is (2172416/28160), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

دستورات زیر نشان دهنده استفاده از Offset-list در روی روتر WAN 1 و در مورد پیام های دریافت شده از روتر B1 می باشد :

```
WAN1(config)#access-list 11 permit 10.11.1.0
WAN1(config)#router eigrp 1
WAN1(config-router)#offset-list 11 in 3 Serial0/0/0.1
WAN1(config-router)#end
```

مثال فوق دارای 2 قسمت مهم است که شامل ACL 11 و دستور offset-list است . که در ACL 11 تنها اقدام به مشخص کردن شبکه 10.11.1.0 نموده ایم .

در نتیجه اجرای دستور offset-list 11 in 3 s0/0/0.1 در روی روتر WAN 1 , روتر مزبور تمام پیام های Update دریافتی از پورت s0/0/0.1 خود را بررسی کرده ودر صورت یافتن Route یا همان شبکه 10.11.1.0 , مقدار 3 را بر روی FD و RD مربوط به همان Route اضافه می کند .

در خروجی زیر مشاهده کنید :

```
WAN1#show ip eigrp topo 10.11.1.0/24
IP-EIGRP (AS 1): Topology entry for 10.11.1.0/24
  State is Passive, Query origin flag is 1, 1 Successor(s), FD is 2172416
  Routing Descriptor Blocks:
  10.1.1.2 (Serial0/0/0.1), from 10.1.1.2, Send flag is 0x0
      Composite metric is ( 2172419/28163 ), Route is Internal
      Vector metric:
        Minimum bandwidth is 1544 Kbit
        Total delay is 20100 microseconds
        Reliability is 255/255
        Load is 1/255
        Minimum MTU is 1500
        Hop count is 1
```

Successor

Successor به بهترین مسیر با بهترین متریک گفته می شود .

Feasible Successor به تمام مسیرهای جایگزین معتبر (با متریک کمتر از مسیر Successor) که مستقل از مسیر Successor است گفته می شود .

هر روتر با بررسی موارد موجود در جدول Topology خود اقدام به محاسبه متریک به ازای تمام مسیرهای منتهی به مقاصد مختلف می کند که این متریک به نام Feasible Distance یا FD نامیده می شود . همچنین هر روتر در هنگام ارسال پیام Update شامل یک Route به روترهای همسایه مقدار FD محاسبه شده توسط خود را نیز به اطلاع آن روترهای همسایه می رساند که این مقدار از دید روترهای همسایه Reported Distance یا RD خوانده می شود .

در صورتی که به ازای هر کدام از آدرس های شناخته شده بیش از یک مسیر در داخل جدول topology وجود داشته باشد روتر اقدام به بررسی این مسیرها خواهد کرد تا مسیرهای معتبری که عاری از چرخه لایه 3 می باشد را شناسایی نماید . برای انجام این کار الگوریتمی ساده انجام خواهد گرفت و روتر بعد از شناسایی مسیرهای جایگزین معتبر (عاری از چرخه لایه 3) آنها را در داخل جدول توپولوژی به ثبت می رساند .

نتیجه بدین صورت خواهد بود که اگر مسیر اصلی یا successor به سمت یکی از مقاصد معیوب گردد روتر بلافاصله از مسیر جایگزین معتبری که قبلا آن را شناسایی کرده و در داخل جدول توپولوژی به ثبت رسانده بود بهره خواهد گرفت .

از نظر پروتکل EIGRP به این مسیرهای جایگزین که عاری از چرخه های لایه 3 هستند Feasible Successor اطلاق می شود .

در صورتی یک مسیر به عنوان مسیر جایگزین معتبر یا Feasible Successor شناسایی خواهد شد که از شرایط خاصی برخوردار باشد به این شرایط در اصطلاح Feasibility Condition گفته می شود . به این ترتیب اگر مقدار RD مربوط به مسیر غیر اصلی کمتر از مقدار FD مربوط به مسیر اصلی که هم اکنون برای ارسال اطلاعات به سمت آن مقصد مورد استفاده قرار می گیرد باشد , مسیر مزبور را می توان به عنوان Feasible Successor عنوان کرد .

: Feasibility Condition

IF RD < FD ⟶ Feasible Successor

RD > FD ⟶ Check it

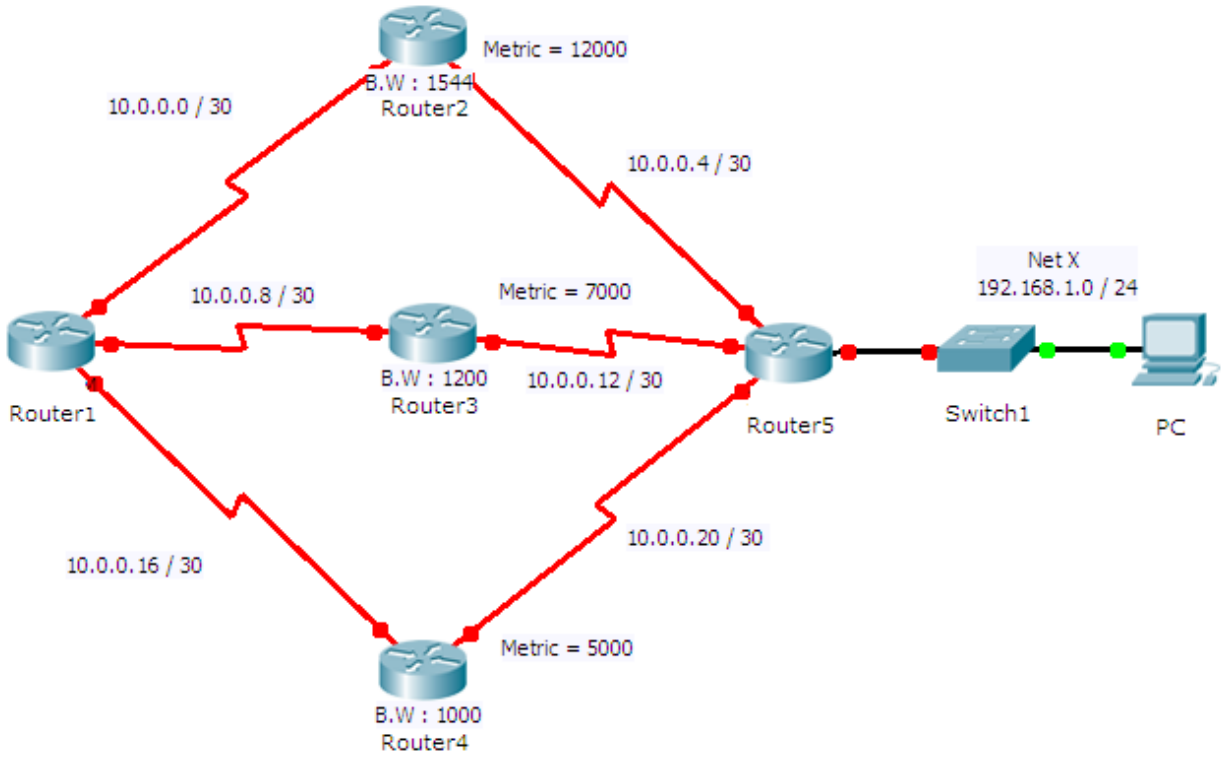
برای دیدن مسیرهای Successor و Feasible Successor از دستور زیر استفاده می کنیم :

Router # Show IP EIGRP Topology

برای دیدن کل مسیرها از این دستور استفاده می کنیم :

Router # Show IP EIGRP Topology All – Links

به شکل زیر توجه کنید :



در جدول توپولوژی Router 1 تمام مسیرهای موجود برای رسیدن به Net X یا شبکه 192.168.1.0/24 به شکل زیر نمایش داده می شود :

Router 1 : Topology Table (FD / RD)

Net X Router 2 (16000 / 12000)

Router 3 (11000 / 7000)

Router 4 (9000 / 5000)

Router 1 در جدول Routing خود این مسیر را قرار می دهد :

Router 1 : Routing table

Next Router 4 9000

7000 / 9000 √ : FS

12000 / 9000 ×

حالا مقدار متریک RD و FD روترها را حساب می کنیم تا نتیجه بالا به دست بیاید :

RD : Router 2 = [10^7 / 1544 + 2010] * 256 = 2172416

RD : Router 3 = [10^7 / 1200 + 2010] * 256 = 2647808

RD : Router 4 = [10^7 / 1000 + 2020] * 256 = 307566

FD : Router 2 = [10^7 / 1544 + 4010] * 256 = 26844116

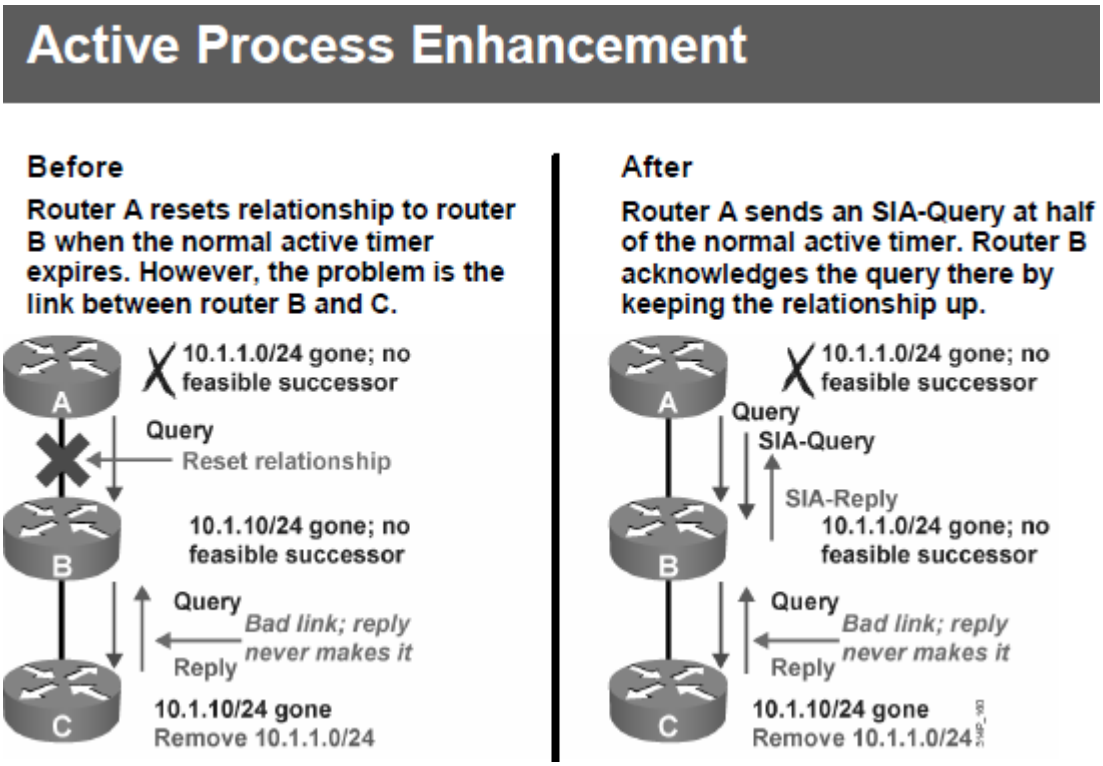
FD : Router 3 = [10^7 / 1200 + 4010] * 256 = 3159808

FD : Router 4 = [10^7 / 1000 + 4020] * 256 = 3586560

برای Reset کردن اطلاعات EIGRP از دستور زیر استفاده می کنیم :

Router # Clear EIGRP Neighbor ship

Query & Reply



زمانی که مسیر اصلی منتهی به یک مقصد خاص قطع یا معیوب شود و روتر بعد از بررسی جدول توپولوژی خود هیچ مسیر Feasible Successor را به سمت آن مقصد شناسایی نکند مرحله ای در رابطه با Route مزبور آغاز خواهد شد که به نام Active State نامیده می شود .مسیرهایی که یک روتر به عنوان مسیر اولیه از آنها برای دسترسی به یک مقصد بهره می گیرد و یا مسیرهایی که دارای Feasible Successor می باشند در وضعیت Passive قرار خواهد داشت . در حالت کلی مراحل ورود به وضعیت Active به شکل زیر است:

- وضعیت مسیر مزبور از Passive به Active تغییر پیدا خواهد کرد .
- ارسال پیام های Query به تمامی روترهای همسایه به منظور پرسش از وجود مسیرهای معتبر و جایگزین به سمت مسیر ذکر شده در روی آن روترها میباشد .

- چنانچه روتر همسایه ای که این پیام Query را دریافت کرده است دارای یک مسیر معتبر Passive در روی خود باشد دو عمل را انجام خواهد داد : الف) پیام Reply را به سمت روتر اول فرستاده و وجود مسیر جایگزین را به اطلاع آن می رساند . ب) از انتشار دوباره پیام Query به دیگر روترهای همسایه جلوگیری به عمل می آورد .
- در صورتی که روتر همسایه دارای مسیر معتبر Passive نبوده و خود نیز در مورد آن مسیر در وضعیت Active قرار داشته باشد دو عمل را در پیش خواهد گرفت : الف) پیام Query دریافت شده از روتر اول را به روترهای همسایه خود نیز ارسال می کند . ب) پیام Replyرا به روتر اولی نفرستاده و در عوض منتظر دریافت پیام Reply از روترهای همسایه خود می ماند .
- در صورتی که یک روتر در قبال ارسال پیام های Query به روترهای همسایه خود اقدام به دریافت پیام های Reply از همه روترها نماید در صورت نیاز پیام Reply را به دیگر روترهای همسایه نیز ارسال می کند .
- یک روتر بعد از دریافت پیام های Reply از روترهای همسایه اقدام به انتخاب بهترین مسیر ممکن به سمت آن مقصد کرده و در صورت شناسایی آن مسیر یاد شده را در جدول Routing خود قرار می دهد .

یکی از ویژگی های EIGRP بهره گیری از روترهای Stub است . یک روتر Stub نباید قادر به هدایت ترافیک مابین سایت Remote باشد یعنی روترهای Stub نمی توانند مسیرهای دریافتی از یک روتر همسایه را به روتر همسایه دیگری ارسال کنند . از سویی دیگر نیز روترهای دیگر از وجود روترهای Stub مطلع شده اند و در نتیجه از فرستادن پیام های Query به سمت آنها خودداری می کنند .

این پروسه باعث می شود تا محدوده گسترش پیام های Query کاهش پیدا کند و همچنین مقدار زمان مورد نیاز برای همگرایی یا Convergence شبکه نیز کمتر شود .

وقتی روتر پیام Query را برای همه روترهای دیگر می فرستد روتر منتظر می ماند تا جواب همه Queryها بیاید و از همه Reply بگیرد . بنابراین روتر تا از همه روترهای همسایه جواب یا همان Reply بگیرد در حالت فعال گیر کرده است که اصطلاحا به آن Stuck in Active (SIA) می گویند .

دو نوع پیام SIA وجود دارد :

1: SIA – Query پیامی است که روتری که پیام Query فرستاده و منتظر گرفتن پیام Reply از روتر همسایه است این پیام را می فرستد تا ببیند روتر همسایه هنوز در دسترس قرار دارد یا نه .

2: SIA – Reply پیامی است که در جواب پیام SIA – Query از روتر همسایه به روتر اصلی فرستاده می شود که هنوز در دسترس است .

به منظور محدود کردن مقدار زمانی که یک روتر در انتظار دریافت پیام های Reply باقی خواهد ماند سیستم عامل IOS زمان Active timer را معرفی کرده است که به صورت پیش فرض 3 دقیقه میباشد .برای تغییر مدت زمان Active timer از دستور زیر استفاده می کنیم :

Router(config-router)# Timers Active – time minutes

دستور برای Stub کردن روتر :

Router(config-router)#EIGRP Stub [Connected | Summery | Receive-only | Static | Redistributed]

پارامترهای پیش فرض connected و summery مورد استفاده قرار خواهند گرفت .

Connected :با تایپ این پارامتر روتر Stub تنها اقدام به ارسال شبکه های متصل به خود به سمت دیگر روترها می نماید . البته این کار در صورتی انجام خواهد شد که آدرس این شبکه های متصل بعد از دستور network مشخص شده باشد .

Summery :تایپ این پارامتر باعث میشود روتر Stub تنها اقدام به ارسال شبکه های Summarized به سمت دیگر روترها می نماید .

Static : در صورتی که در روی یک روتر Stub اقدام به نوشتن Route استاتیک کرده و سپس آنها را با استفاده از دستور Redistribute static به داخل پروسه EIGRP منتشر کرده باشیم تایپ این پارامتر روتر مذبور را مجبور می کند تا این اطلاعات را به سمت دیگر روترها نیز ارسال کند .

Redistributed : تایپ این پارامتر باعث میشود تا روتر Stub اطلاعات منتشر شده به داخل پروسه EIGRP طی عمل Redistribution را به سمت دیگر روترها ارسال نماید .

Receive-only : تایپ این پارامتر باعث میشود تا روتر Stub هیچ گونه اطلاعاتی را به سمت دیگر روترها ارسال نکند .

برای دیدن روتر Stub از دستور زیر استفاده می کنیم :

Router # Show IP EIGRP Neighbor Details

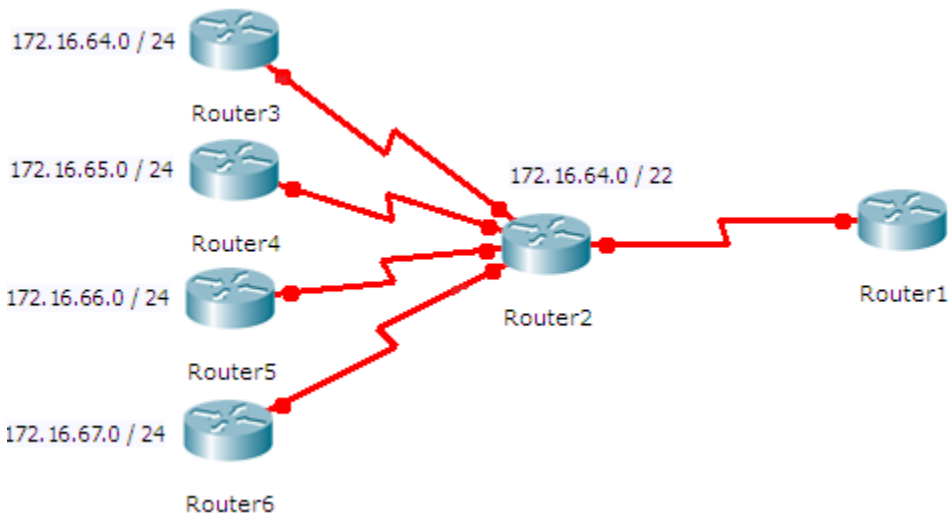
Route Summarization

در Internetworkهای متوسط و بزرگ صدها و هزاران شبکه وجود دارد که این تعداد شبکه باعث افزایش حجم جدول مسیریابی روترها میشود که با استفاده از توانمندی Route Summarization می توانید تعداد شبکه های موجود در جدول مسیریابی روترها را کاهش دهید . در حقیقت Route Summarization توانمندی می باشد که به ما اجازه خواهد داد تعدادی شبکه را فقط از طریق یک آدرس خلاصه یا Summarize کنیم.برخی مواقع به جای عبارت Route Summarization از عبارات Route Aggregation و Suppernetting نیز استفاده می شود .

نکته :

کاهش حجم جدول مسیریابی باعث افزایش کارایی پروسه Routing و کاهش میزان مصرف منابع سخت افزاری توسط روتر خواهد شد .

به شکل زیر توجه کنید مشاهده می کنید که کلیه شبکه های متصل شده به Router 2 خلاصه شده و از طریق یک شبکه 172.16.64.0 / 22 به سمت Router1 ارسال خواهد شد :



محاسبه Route Summarization

در انجام Route Summarization برای Summarize کردن شبکه ها از bitهای مشترک استفاده خواهد شد .

در تصویر زیر چهار آدرس شبکه را مشاهده میکنید که به صورت Binary نیز نمایش داده شده اند . به حالت binary توجه کنید و تعداد bitهای مشترک در چهار شبکه را مشخص می کنیم :

172.16.64.0 = 10101100.00010000.01000000.00000000

172.16.65.0 = 10101100.00010000.01000001.00000000

172.16.66.0 = 10101100.00010000.01000010.00000000

172.16.67.0 = 10101100.00010000.01000011.00000000

به تصویر زیر توجه کنید که در این تصویر تعداد bitهای مشترک چهار آدرس مشخص شده است :

172.16.64.0 = 10101100.00010000.010000**00**.00000000

172.16.65.0 = 10101100.00010000.010000**01**.00000000

172.16.66.0 = 10101100.00010000.010000**10**.00000000

172.16.67.0 = 10101100.00010000.010000**11**.00000000

همان طور که مشاهده می کنید این آدرس ها دارای 22 bits مشترک می باشند.

در این حالت می توانید کل چهار شبکه را با آدرس و Subnet Mask زیر خلاصه نمایید:

Network Address : 172.16.64.0 / 22

Subnet Mask : 255.255.252.0

ویژگی Route Summarization بدون تأثیرگذاری در نحوه دسترسی یک روتر به شبکه های مقصد باعث کاهش سایز جداول Routing می شود . در این حالت یک روتر به جای در اختیار داشتن تک تک Routeهای کوچکتر تنها یک Route که بیانگر تمامی آن شبکه های کوچکتر است را در داخل جدول Routing خود ثبت می کند.در نتیجه این کار روتر علاوه بر آنکه میتواند به همان شبکه های قبلی دسترسی داشته باشد از جدول Routing کوچکتری برخوردار خواهد بود .

دستور پیکربندی Route Summarization :

Router(config)# Interface type mod/num

Router(config – if)#IP Summary – Address EIGRP As-num Prefix Mask

مثال :

Router(config)# Interface serial 0/1

Router(config - if)#IP Summary – Address EIGRP 1 192.168.0.0 255.255.248.0

بعد از اجرای دستور Summarization در روی Interface اتفاقات زیر در روی روتر روی خواهد داد :

- روتر اقدام به قطع رابطه مجاورت با تمامی روترهای همسایه قابل دسترس از طریق آن Interface خواهد کرد و سپس این رابطه دوباره برقرار خواهد شد . این عمل باعث خواهد شد تا روترهای همسایه اطلاعات مربوط به توپولوژی قبلی را از داخل جدول خود پاک کنند و اطلاعات جدید را از این روتر دریافت کنند .
- بعد از برقراری دوباره رابطه مجاورت مابین این روتر و روترهای همسایه با فرض بر اینکه حداقل یکی از شبکه های زیر مجموعه summary route در داخل جدول Routing در روی این روتر وجود داشته باشد دستگاه اقدام به ارسال summary route به سمت روترهای دیگر می کند .
- از این به بعد روتر مزبور از انتشار Routeهای زیر مجموعه summary route به دیگر روترهای همسایه خودداری خواهد کرد .
- روتر اقدام به ایجاد یک route به سمت Null 0 کرده و آن را در داخل جدول Routing خود به ثبت می رساند در صورتی که یک پیام در مقایسه با دیگر routeهای موجود در جدول Routing با summary route که به Null 0 اشاره دارد مطابقت بیشتری داشته باشد در این صورت پیام به سمت Null 0 هدایت خواهد شد و مقدار AD آن را برابر 5 قرار خواهد داد و Drop می شود یعنی پیام از بین خواهد رفت .

Auto – Summary

روترها به صورت پیش فرض مسیرهایی را که به صورت Classful باشند Summary می کنند .

دستور فعال و غیرفعال کردن Auto – Summary :

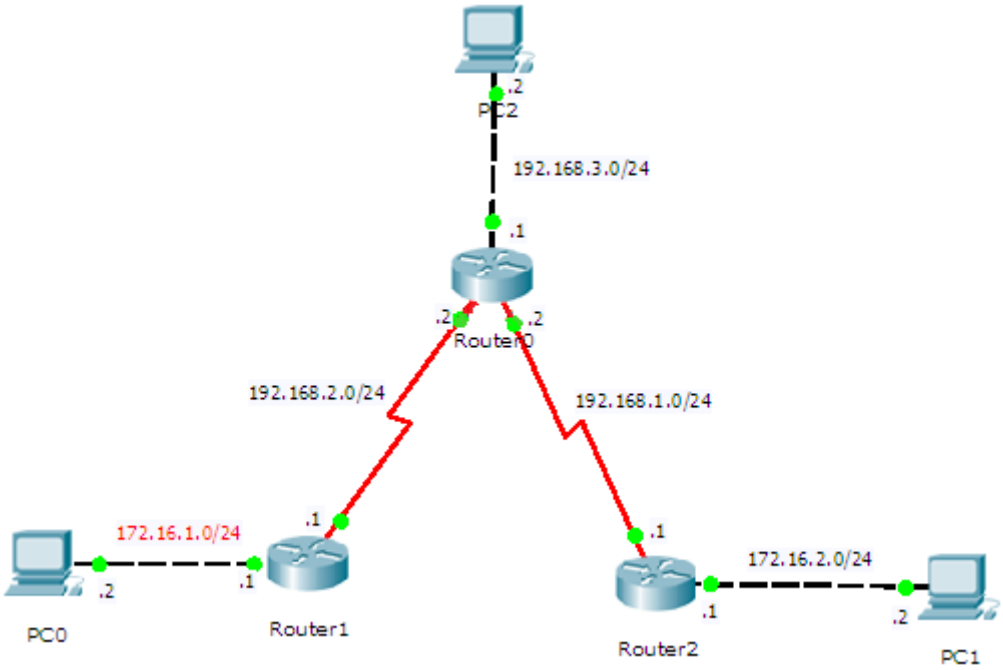
Router(config-router)# Auto – Summary فعال میشود

Router(config-router)# No Auto – Summary غیرفعال میشود

Contiguous network : به یک توپولوژی که همه پاکت ها برای رسیدن به شبکه های دیگر تنها از داخل سگمنت هایی که زیر مجموعه همان آدرس در کلاس استاندارد می باشد یعنی همه آدرس های شبکه های موجود از یک Range باشند عبور کند در اصطلاح شبکه های Contiguous می گویند و در این نوع شبکه ها از دستور Auto – Summary استفاده می کنیم .

Discontiguous Network : به یک توپولوژی که هر پاکتی برای رسیدن به شبکه های دیگر از داخل سگمنت هایی که زیر مجموعه همان آدرس در کلاس استاندارد نمی باشد (یعنی همه آدرس های شبکه های موجود از یک Range نباشند) عبور کند , شبکه های Discontiguous می گویند و در این نوع شبکه ها از دستور No Auto – Summary استفاده می کنیم .

مثال :



به شکل بالا توجه کنید . چون در EIGRP به صورت پیش فرض Auto – Summary صورت می گیرد Router1 و Router 2 شبکه های متصل به خود را به صورت Summary به Router 0 اعلام می کنند :

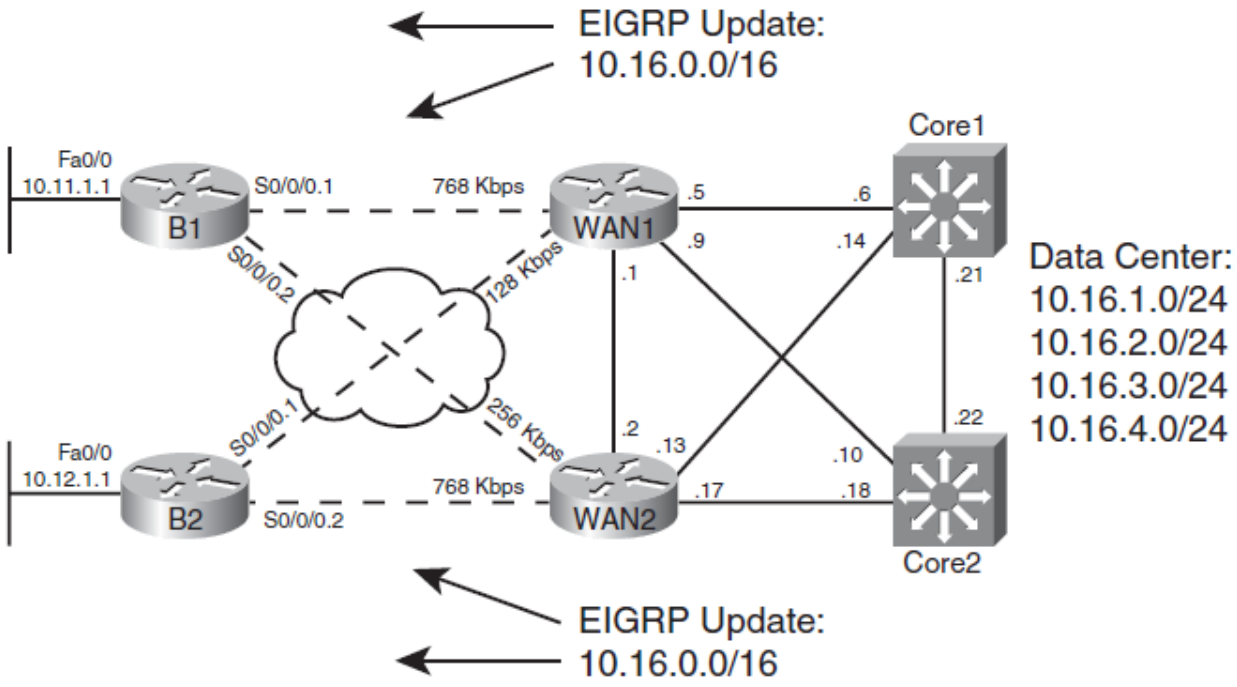
Router 1 → 172.16.1.0 / 24 summary → 172.16.0.0 /16

Router 2 → 172.16.2.0 / 24 summary → 172.16.0.0 /16

مشاهده می کنید که هر دو روتر شبکه خود را به یک Range آدرس Summary کرده اند و برای Router 0 فرستاده اند و Router 0 دو مسیر برای رفتن به شبکه 172.16.0.0 را دارد .

مثلا حال اگر از PC 2 بخواهیم PC 1 را Ping بزنیم Router 0 چون دو مسیر برای آدرس 172.16.0.0 دارد که یکی را از Router 1 و دیگری را از Router 2 یاد گرفته پس یک بسته را به Router 1 می فرستد و یک بسته

را به Router 2 می فرستد و این ایراد بزرگی در شبکه است که یک بسته به مقصد برسد و بسته دیگر به مقصد نرسد پس برای رفع این مشکل دستور No Auto – Summary را روی روترها اعمال می کنیم . با این کار Router 0 برای هر شبکه فقط یک مسیر دارد و همه بسته ها به شبکه مورد نظر می رسد .



Summary for 10.16.0.0/16 on WAN1, WAN2

در شکل بالا می بینیم که روترهای WAN1 و WAN2 شبکه های Data Center را به آدرس 10.16.0.0/16 خلاصه یا Summary کرده و به روترهای B1 و B2 اعلام می کنند . در اینجا باید از Auto – Summary استفاده کنیم .

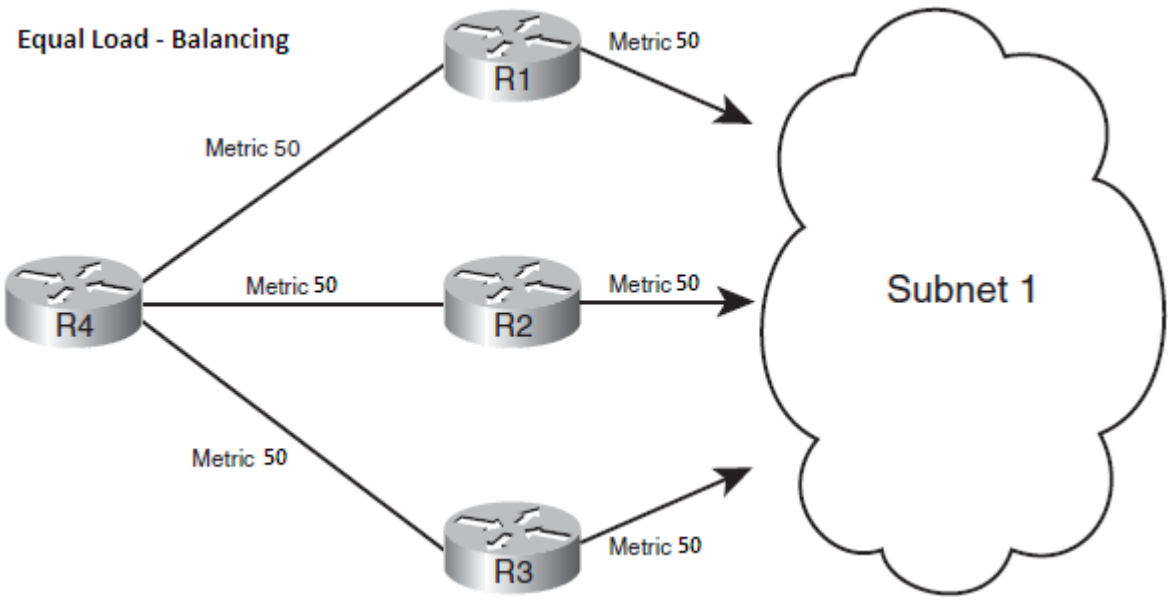
Load – Balancing

ویژگی Load – Balancing یا Load Sharing علاوه بر آنکه می تواند از یک مسیر به عنوان جایگزین برای مسیر اصلی بهره گرفت بلکه می توان از مسیرهای متعدد برای پخش ترافیک به سمت یک مقصد خاص نیز استفاده کرد . Load – Balancing به دو صورت زیر است :

: Equal Load – Balancing

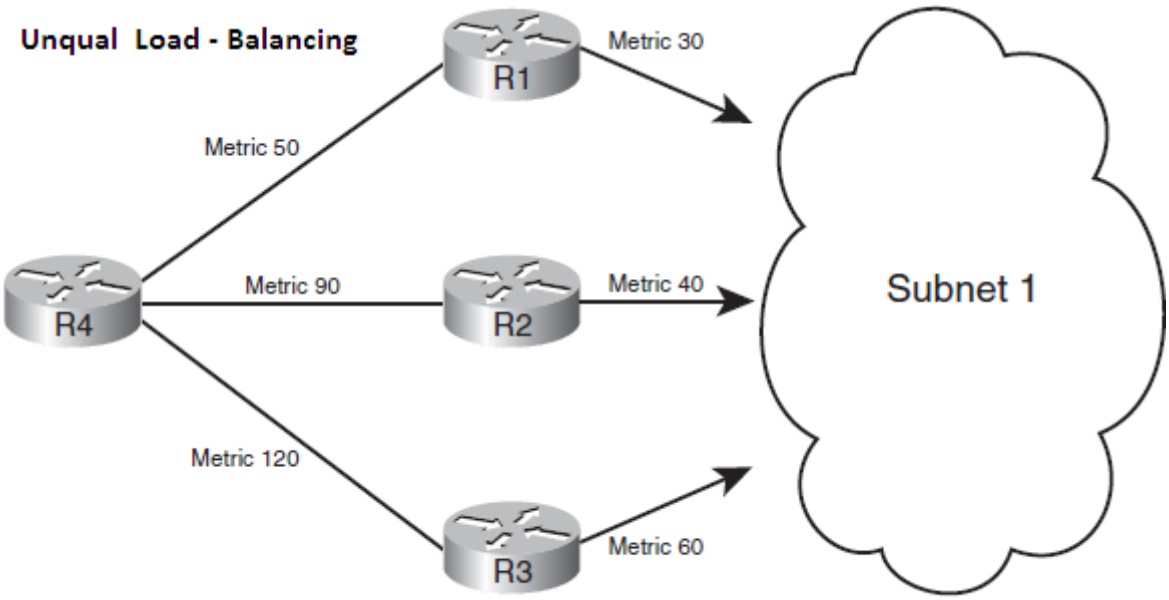
پروتکل EIGRP به صورت پیش فرض Load – Balancing (تعادل بار در انتقال ترافیک بر روی چندین لینک به صورت همزمان) را بر روی مسیرهایی با Metric یکسان انجام خواهد داد . پیش فرض 4 لینک در Load – Balancing می توانند شرکت کنند . با دستور زیر می توانیم تعداد مسیرها را تا 32 عدد تغییر بدهیم :

Router (config – Router) # Maximum – Paths Number



: Unqual Load – Balancing

به ویژگی Load – Balancing بر روی مسیرهایی با Metric نامساوی Unqual Load – Balancing گفته می شود که به صورت پیش فرض غیر فعال می باشد و در صورت نیاز به صورت دستی باید فعال شود و با استفاده از دستور Variance تعادل بار بر روی مسیرهایی با Metric نامساوی را فعال می کنیم .



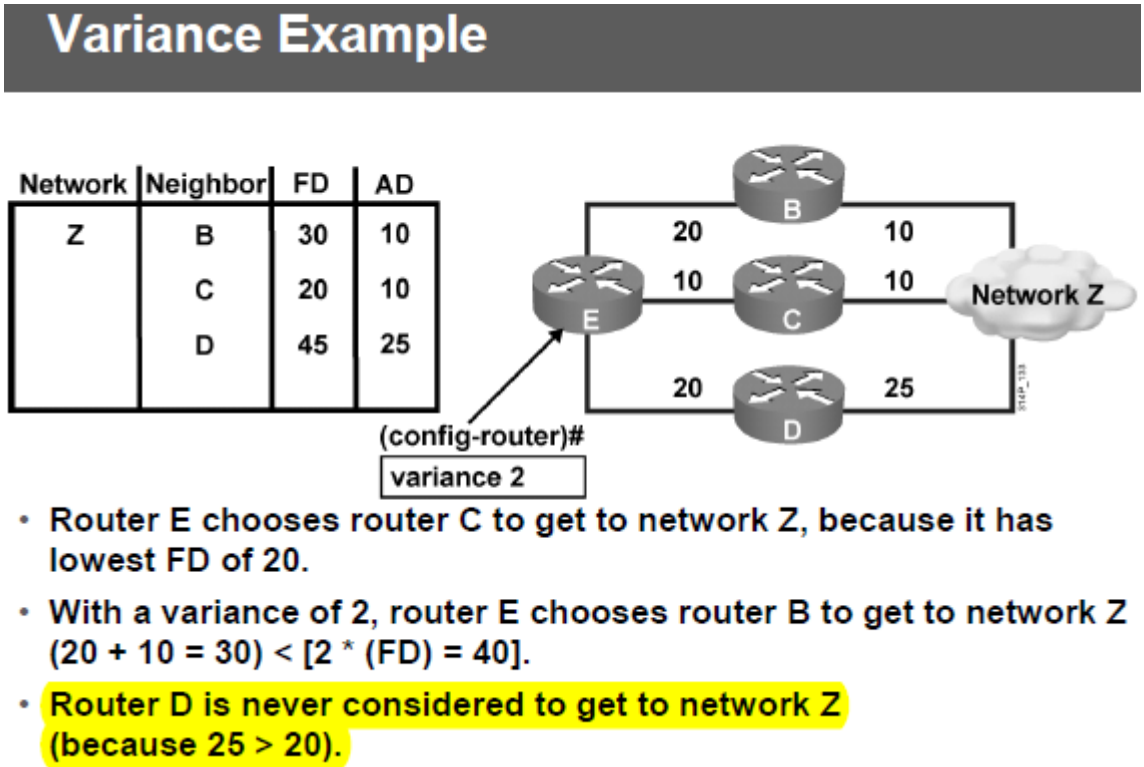
Variance : از طریق Variance می توان روتر را مجبور کرد تا مسیرهایی که Metric آنها نزدیک به Metric مربوط به مسیر اصلی است را نیز در داخل جدول Routing قرار دهد و Load – Balancing روی آنها صورت گیرد .

: دستور Variance

Router (config – Router) # Variance multiplier

متغیر multiplier اشاره به عددی دارد در Range = 1 تا 128

به شکل زیر دقت کنید :



از Router E برای رسیدن به Network Z سه مسیر با Metricهای متفاوت قرار دارد. Router E از طریق Router C که مقدار متریک آن برای رسیدن به Network Z برابر است با 20 استفاده می کند چون متریک دو مسیر دیگر بیشتر است .

حال اگر دستور زیر را وارد کنیم :

Router (config – Router) # Variance 2

با این دستور مقدار Variance را برابر با 2 قرار داده ایم که در این حالت عدد 2 در کوچکترین Metric ضرب خواهد شد و کلیه مسیرهایی که از عدد به دست آمده کوچکتر و یا مساوی آن باشند بین آنها – Load

Balancing انجام خواهد گرفت و تعادل بار فعال خواهد شد که در این مثال اگر عدد 2 را در کوچکترین Metric یعنی 20 ضرب کنیم مقدار 40 به دست خواهد آمد و همانطور که مشاهده می کنید Metric مسیری که از Router B عبور می کند و به Network Z می رسد برابر است با عدد 30 که از مقدار به دست آمده کمتر است که در این حالت Load – Balancing بر روی این مسیر فعال خواهد شد . ولی چون مسیر سوم یعنی مسیری که از Router D عبور می کند و به Network Z می رسد مقدار Metric آن برابر است با 45 که از مقدار به دست آمده بیشتر است در نتیجه Load – Balancing بر روی این مسیر فعال نمی شود :

E ⟶ B ⟶ Network Z : 40 > 30 √ = Load – Balancing

E ⟶ D ⟶ Network Z : 40 < 45 × = No Load – Balancing

به صورت پیش فرض پروتکل EIGRP بین مسیرهایی که در جدول Routing دارد Load sharing انجام می دهد :

Router (config – Router) # Traffic – Share Balanced

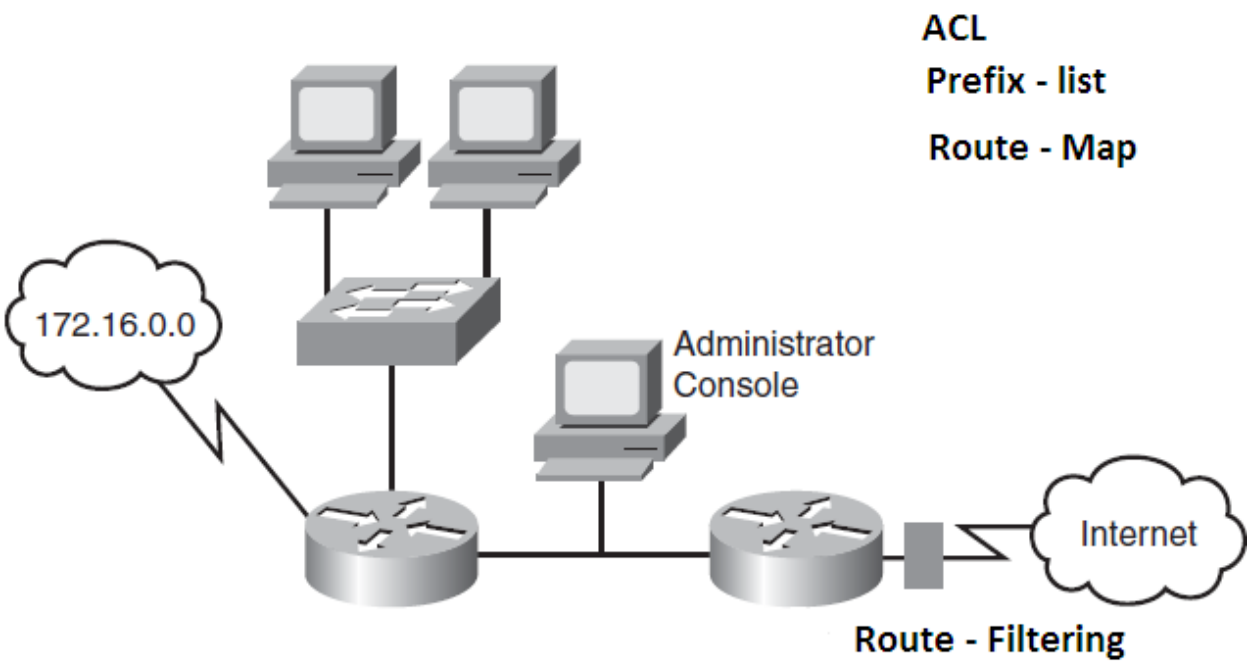
ولی می توان در سناریویی که هدف بالا بردن سرعت همگرای است مسیرهایی را در جدول مسیریابی آورد ولی روی آن Load sharing صورت نگیرد :

Router (config – Router) # Traffic – Share min across – Interface

Filtering

ویژگی Route Filtering امکان کنترل اطلاعات انتقالی توسط پیام های Update را فراهم میسازد . به عبارتی اگر نمی خواهید یکی از روترهای شبکه اقدام به کسب اطلاعات مربوط به شبکه ای خاص نماید در این صورت می توانید روترها را برای انجام Route Filtering پیکربندی کنید . این کار می تواند علاوه بر کاهش حجم جدول Routing و افزایش کارایی شبکه باعث بهبود امنیت شبکه نیز می گردد .

پروتکل EIGRP امکان استفاده از دستور Distribute – List را برای انجام Route Filtering مهیا کرده است . دستور فوق از سه ابزار Route – Map , Prefix – List , ACL برای انتخاب یک آدرس یا مجموعه ای از آدرس های مورد استفاده بهره می گیرد تا عملیات Route Filtering بر روی آنها صورت گیرد .



دستور Distribute – List :

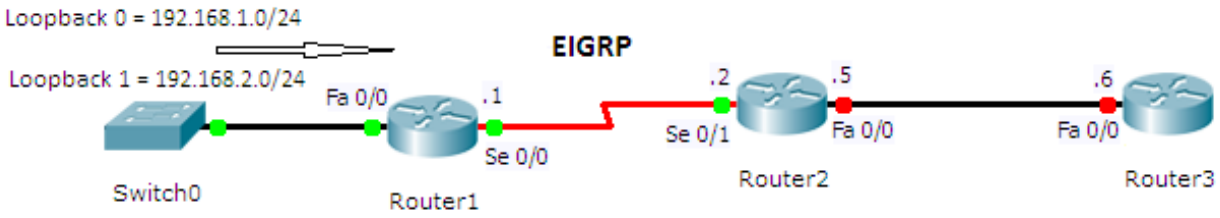
Router (config – Router) # Distribute – List { ACL-num | ACL-name }

{ in | out } { interface type mod/num }

1. Access – List

در صورتی که از Access – Listها برای انجام فیلترینگ استفاده می کنید باید بدانید که استفاده از پارامتر Permit باعث صدور اجازه و پارامتر Deny موجب بلوک شدن آدرس مورد نظر خواهد شد. ویژگی Distribute – List در پروتکل EIGRP تنها استفاده از ACLهای استاندارد را پشتیبانی میکند. به این ترتیب می توان از هر دو نوع ACL استاندارد یعنی Named و Numbered استفاده کرد و اقدام به مشخص کردن یک آدرس به همراه Wildcard Mask مربوطه به آن نمود.بعد از نوشتن ACL روتر اقدام به بررسی Net ID مربوط به آدرس فرستنده پیام ها و مقایسه آنها با ACL خواهد کرد .

به شکل زیر توجه کنید :



برای مثال می خواهیم که Router 1 در هنگام خروج Loopback0=192.168.1.0 را Filter کند ولی Loopback1=192.168.2.0 مجاز باشد که از Router 1 خارج شود :

اول ACL را تعریف می کنیم :

Router 1 (config) # Access – List 1 Deny 192.168.1.0

Router 1 (config) # Access – List 1 Permit any

حالا ACL را در Distribute – List اعمال می کنیم :

Router 1 (config – Router) # Distribute – List 1 out

حالا می خواهیم که Router 2 در هنگام ورود Loopback0=192.168.1.0 را Filter کند ولی Loopback1=192.168.2.0 مجاز باشد که به Router 2 وارد شود :

اول ACL را تعریف می کنیم :

Router 2 (config) # IP Access – List standard Cisco

Router 2 (config – std – nacl) # Deny 192.168.1.0

Router 2 (config – std – nacl) # Permit any

حالا ACL بالا را در Distribute – List اعمال می کنیم :

Router 2 (config – Router) # Distribute – List Cisco in

2. Prefix – List

Prefix – List امکان انتخاب آدرس ها با استفاده از Prefix و Prefix Length و یا Range از این دو را فراهم می کند. با بهره گیری از Prefix – List می توان روتر را مجبور کرد تا با در نظر گرفتن طول Prefix یا همان Prefix Length اقدام به بررسی Routeها نماید . با بکارگیری Prefix – Listها می توان یک Route را بر اساس دو پارامتر زیر ارزیابی کرد :

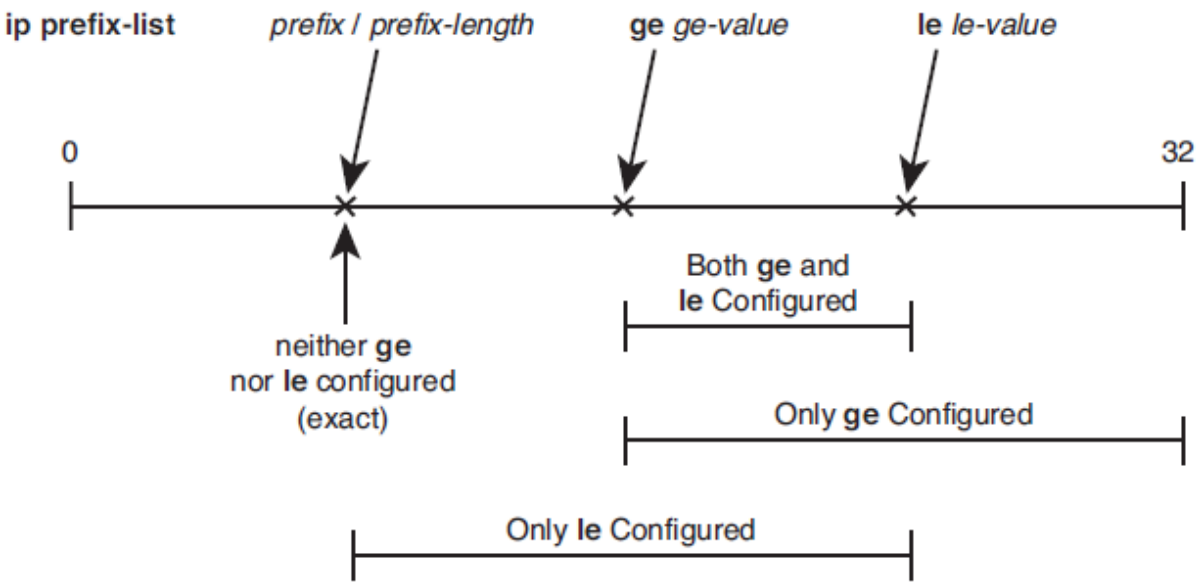
- IP Prefix (Subnet Number)
- Prefix Length (Subnet Mask)

دستور Prefix – List :

Router (config) # IP Prefix – List name [seq-num] { Permit | Deny } Prefix / Prefix length [ge value] [le value]

: seq-num

هر کدام از دستورات Prefix – List دارای یک شماره ترتیب یا sequence number برای خود هستند که امکان حذف و اضافه کردن دستورات دیگر را فراهم می سازد .



Representation of Prefix Length Ranges for ip prefix-list Command

ge ⟶ Greater Than or Equal to ⟶ ≥

Le ⟶ Less Than or Equal to ⟶ ≤

اگر هیچ کدام را ننویسیم فقط Prefix Length را بنویسیم باید طول ماسک یا Prefix Length یک Route دقیقا برابر دستور باشد .

اگر هر دو را بنویسیم باید به صورت زیر باشد :

ge ≤ Prefix Length ≤ Le

اگر فقط ge را بنویسیم باید به صورت زیر باشد :

ge ≤ Prefix Length ≤ 32

اگر فقط Le را بنویسیم باید به صورت زیر باشد :

Configured Prefix Length ≤ Prefix Length ≤ Le

دستور زیر شامل همه آدرس ها (IPها) می شود :

0.0.0.0 / 0 Le 32

قانون :همیشه باید ge ≤ Configured باشد .

دستور اعمال Prefix – List بر روی Distribute – List :

Router (config – Router) # Distribute – List Prefix name { in | out } { interface type mod/num }

3. Route – Map

Route – Mapها کاربردهای بسیاری دارند که تنها یکی از آنها را می توان فیلتر کردن اطلاعات انتقالی توسط پیام های Update عنوان کرد .

پردازش Route – Map ها بر اساس شماره Sequence آنها انجام می گیرد . مکانیسم کلی کار بدین ترتیب است که اقدام به نوشتن یک Route – Map خواهیم کرد و سپس نام آن را همراه جهت انتقال (in / out) و نام Interface در دستور Distribute – List مشخص خواهیم کرد .

دستور کلی Route – Map :

Router (config) # Route – Map name { Permit | Deny } [seq-num]

Router (config – route – map)# Match IP Address { ACL-num | ACL-name | Prefix-num | Prefix-name }

دستور اعمال Route – Map بر روی Distribute – List :

Router (config – Router) # Distribute – List Route - Map name { in | out } { interface type mod/num }

دستور نمایش Route – Map :

Router # Show Route – Map

مثال :

ACL را تعریف می کنیم :

Router (config) # Access – List 1 Permit 192.168.1.0

Router (config) # Route – Map Cisco Deny 10

Router (config – route – map)#Match IP Address 1

Router (config – route – map)# Exit

Router (config) # Route – Map Cisco Permit 20

Router (config – route – map)# Exit

Router (config) # Router EIGRP 1

Router (config – Router) # Distribute – List Route – Map Cisco out

مثال :

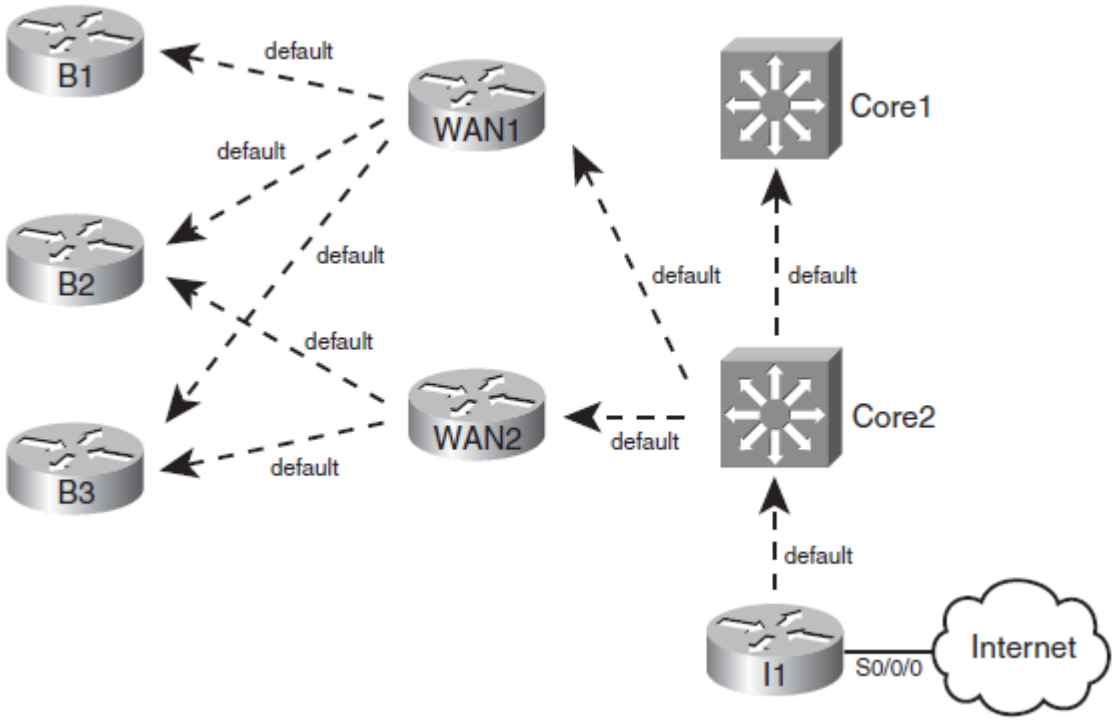
Prefix - List را تعریف می کنیم :

```
Router ( config ) #IP  Prefix – List   1  seq  5  Permit  192.168.1.0/24

Router ( config ) #IP  Prefix – List   2  seq  5  Permit   0.0.0.0/0  Le  32

Router ( config ) # Route – Map  Cisco   Deny  10

Router ( config – route – map )#Match   IP Address   Prefix – List  1

Router ( config – route – map )# Exit

Router  ( config ) # Route – Map  Cisco   Permit  20

Router ( config – route – map )#Match   IP Address   Prefix – List  2

Router ( config – route – map )# Exit

Router ( config) # Router  EIGRP   1

Router ( config – Router  ) # Distribute – List  Route – Map   Cisco   out
```

Default Route

در صورتی که روتر پیامی را دریافت کند که با هیچ کدام از routeهای واقع در داخل جدول Routing مطابقت نداشته باشد این پیام به سمت Default Route ارسال خواهد شد . در واقع Default Route را می توان به عنوان یک Summary Route دانست که نشان دهنده تمامی آدرس های IP بوده و به صورت 0.0.0.0/0 در داخل جدول Routing به ثبت می رسد .

به شکل زیر دقت کنید که در آن سازمان اقدام به برقراری یک رابطه با محیط اینترنت کرده است . روتر I1 باعث برقراری رابطه مابین سازمان و اینترنت شده است .



تمامی نودهای داخل شرکت می توانند از یک Default Route برای ارسال ترافیک به سمت اینترنت بهره بگیرند . برای رسیدن به این هدف روتری که باعث برقراری ارتباط با اینترنت شده است را باید برای انتشار Default Route به محیط داخلی پیکربندی کنیم . در این صورت تمامی روترهای دریافت کننده Default Route آن را به دیگر روترها نیز ارسال می کنند که در نتیجه این کار همه روترها از نحوه دسترسی به محیط

بیرون از شرکت آگاهی پیدا می کنند .در صورتی که پیامی به مقصد یکی از آدرس های بیرون از شرکت ارسال شده باشد در این شرایط به دلیل آنکه روترها از وجود چنین مقصدی بی اطلاع می باشند بنابراین از Default Route برای هدایت کردن آن پاکت استفاده خواهند کرد . در نهایت پاکت مزبور به دست روتر l1 خواهد رسید که آن روتر نیز با توجه به Default Route پیام را به مقصد روانه خواهد کرد .

پیکربندی Default Route در EIGRP :

Default Route به دو روش زیر پیکربندی می شود :

- Static :

این روش دارای دو مرحله زیر است :

1) ایجاد Default Route استاتیک
2) وارد کردن این Route به داخل پروسه EIGRP

مرحله اول :

```
Router ( config ) # IP Route  0.0.0.0  0.0.0.0  { [ outgoing-interface ] [ Next- hop ] }
```

مرحله دوم :

```
Router( config – Router )# Network  0.0.0.0
```

مثال :

```
Router( config )#IP  Route  0.0.0.0  0.0.0.0  Se1/0
Router( config – Router )# Network  0.0.0.0
```

Dynamic :

در این روش می توان یکی از Routeها را به عنوان Default Route تعیین کرد و روتر را مجبور کرد تا آن را برای دیگر روترها نیز ارسال کند .

دستور :

Router(config)#IP Default – Network network-numbar

network-numbar : حتما باید به صورت Classful تعریف شود .

مثال :

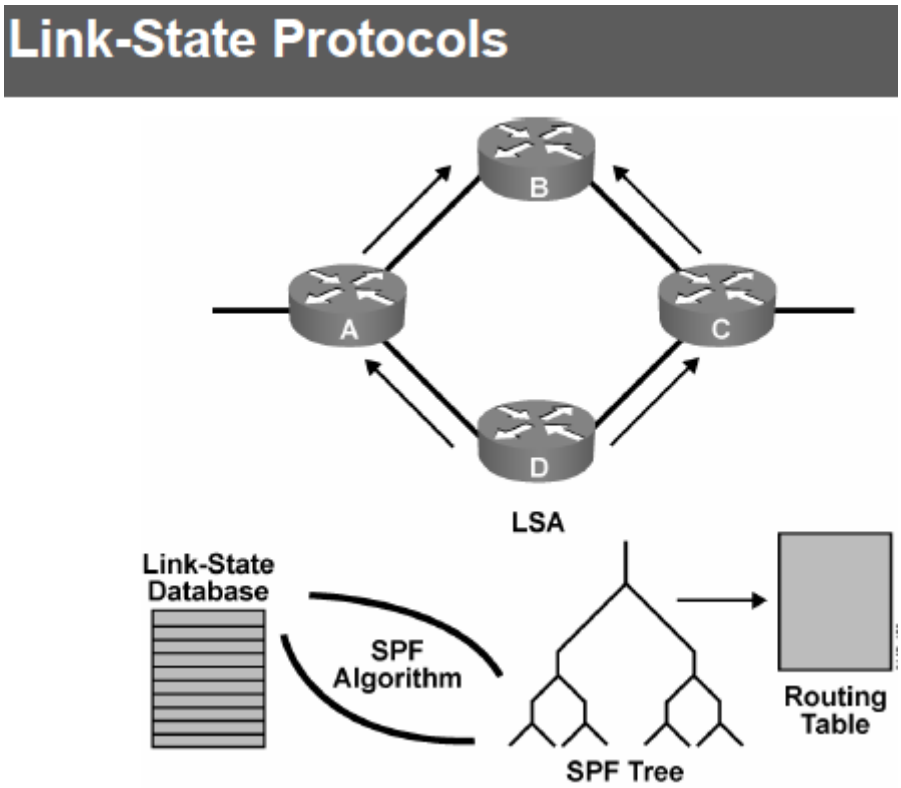
Router(config)#IP Default – Network 192.168.1.0

نکته :

Default Route در آخرین خط در جدول Routing روترها قرار می گیرد و با علامت D^* نمایش داده می شود .

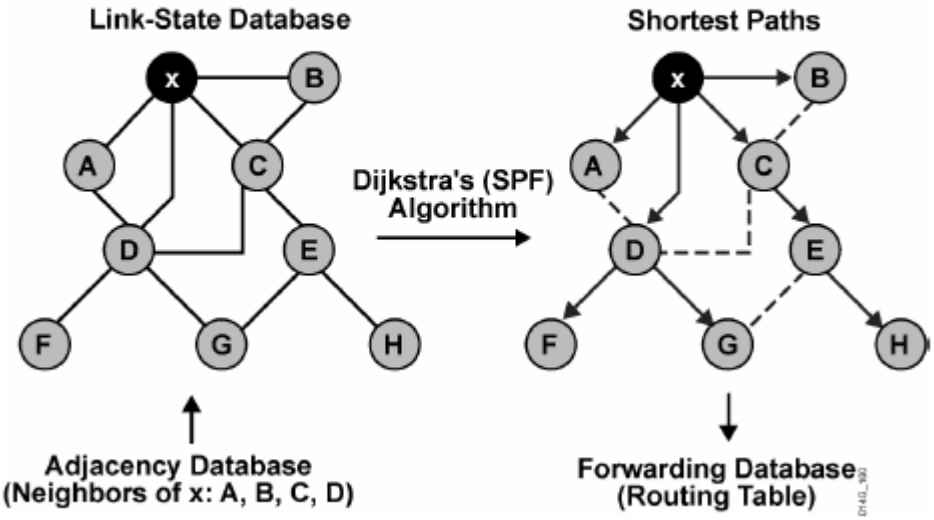
OSPF

Open Shortest Path First



پروتکل مسیریابی OSPF یک پروتکل با استاندارد باز می باشد که توسط بسیاری از شرکت های تولید کننده تجهیزات سخت افزاری و نرم افزاری شبکه مورد استفاده قرار میگیرد . OSPF یک پروتکل Link State می باشد که از الگوریتمی به نام SPF یا Shortest Path First (Dijkstra's)استفاده میکند تا بهترین مسیر را شناسایی و انتخاب کند . پروتکل OSPF همچنین دارای قابلیت مسیریابی با استفاده از طراحی به صورت سلسله مراتبی یا Hierarchical را دارا می باشد .

SPF Calculation



Assume all links are Ethernet, with an OSPF cost of 10.

پروتکل OSPF از Cost به عنوان Metric استفاده می کند و هر مسیری که Cost کمتری داشته باشد به عنوان بهترین مسیر انتخاب خواهد شد .OSPF نیاز به یک شماره پردازش یا Process ID خواهد داشت که این شماره عددی بین 1 تا 65535 است .

پروتکل OSPF از VLSM پشتیبانی میکند چون یک پروتکل Classless است. این پروتکل اطلاعات مسیریابی را از طریق آدرس Multicast منتشر می کند .

در پروتکل OSPF که دارای طراحی به صورت چندین Area یا ناحیه می باشد در صورت ایجاد تغییر دامنه تغییرات محدود به یک Area خواهد بود .

در OSPF یک Area به نام Area 0 یا Backbone Area وجود دارد که تمامی Areaهای دیگر باید به Area 0 متصل شوند .

پروتکل OSPF به دو روش زیر بر روی روترها فعال می شود :

Configuring Basic OSPF

```
Router(config)#
router ospf process-id
```

- Enables one or more OSPF routing processes

```
Router(config-router)#
network ip-address wildcard-mask area area-id
```

- Defines the interfaces that OSPF will run on

```
Router(config-if)#
ip ospf process-id area area-id
```

- Optional method to enable OSPF explicitly on an interface

مثال روش اول :

Router (config) # Router OSPF 1

Router (config - router) # Network 172.16.10.0 0.0.0.255 area 0

مثال روش دوم :

Router (config) # Interface FastEthernet 0/1

Router (config – if) # IP OSPF 1 area 0

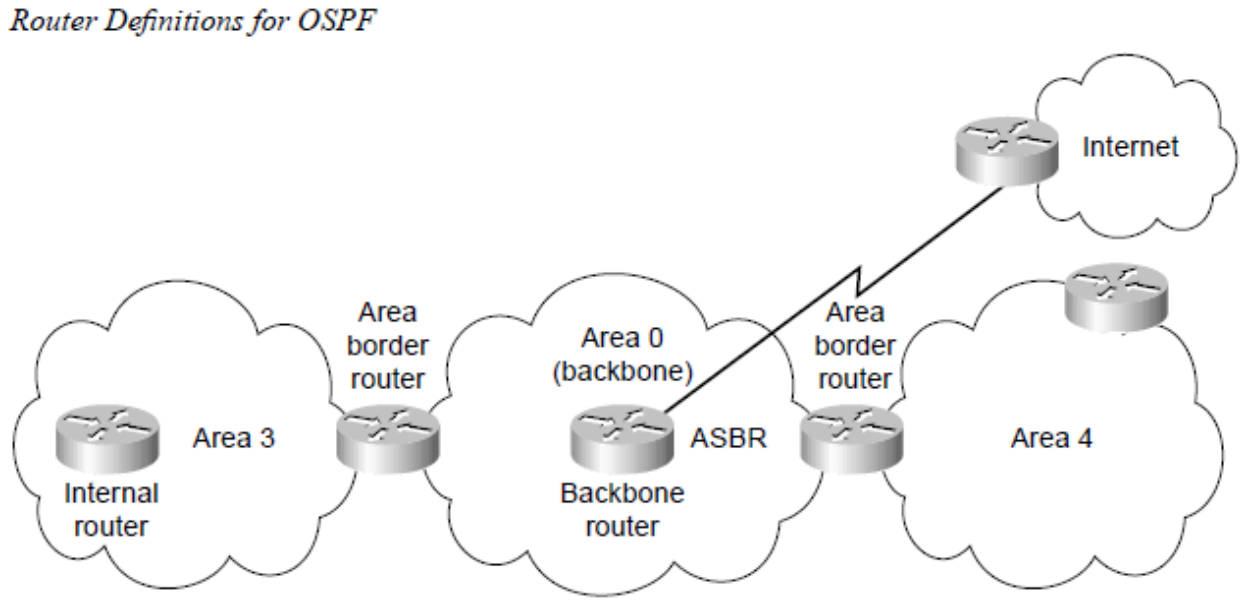
انواع روتر در OSPF :

Area Border Router (ABR) : روتر ABR حداقل به دو Area مختلف متصل شده است که بر اساس قانون یکی از این Areaها باید Area 0 باشد .

Backbone Router : به روترهایی گفته می شوند که حداقل دارای یک Interface متصل به Area 0 باشند .

Internal Router : روترهایی هستند که تنها به یک Area متصل شده اند یعنی تمام اینترفیس های آن روترها در داخل یک Area قرار داشته باشند .

ASBR Router : به روترهای مرزی که با بیرون از پروتکل OSPF ارتباط دارند گفته می شود .



Verifying OSPF Operation

```
Router#
show ip protocols
```

- Verifies the configured IP routing protocol processes, parameters, and statistics

```
Router#
show ip route ospf [process-id]
```

- Displays all OSPF routes learned by the router

```
Router#
show ip ospf interface [type number]
```

- Displays the OSPF router ID, area ID, and adjacency information

```
Router#
show ip ospf
```

- Displays the OSPF router ID, timers, and statistics

```
Router#
show ip ospf neighbor [type number] [neighbor-id]
[detail]
```

- Displays information about the OSPF neighbors, including DR and BDR information on broadcast networks

```
Router#
show ip ospf Database
```

مثال هایی از دستورات نمایش عملکرد پروتکل OSPF :

```
RouterB#sh ip ospf
 Routing Process "ospf 50" with ID 10.64.0.2
<output omitted>

 Number of areas in this router is 2. 2 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0)
    Area BACKBONE(0)
        Area has no authentication
        SPF algorithm last executed 00:01:25.028 ago
        SPF algorithm executed 7 times
<output omitted>

  Area 1
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 00:00:54.636 ago
        SPF algorithm executed 3 times
<output omitted>
```

Example: The show ip route ospf Command

```
RouterA#show ip route ospf
     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O IA    10.2.1.0/24 [110/782] via 10.64.0.2, 00:03:05, FastEthernet0/0
RouterA#
```

Example: The show ip ospf interface Command

```
RouterA#show ip ospf interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet Address 10.64.0.1/24, Area 0
  Process ID 1, Router ID 10.64.0.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 0
  Designated Router (ID) 10.64.0.2, Interface address 10.64.0.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 4
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.64.0.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Example: The show ip ospf neighbor Command

```
RouterB# show ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address     Interface
10.64.0.1       0     FULL/DROTHER    00:00:30    10.64.0.1   FastEthernet0/0
10.2.1.1        0     FULL/  -        00:00:34    10.2.1.1    Serial0/0/1
```

```
RouterB# show ip ospf neighbor detail
 Neighbor 10.64.0.1, interface address 10.64.0.1
    In the area 0 via interface FastEthernet0/0
    Neighbor priority is 0, State is FULL, 16 state changes
    DR is 10.64.0.2 BDR is 0.0.0.0
<output omitted>

Neighbor 10.2.1.1, interface address 10.2.1.1
    In the area 1 via interface Serial0/0/1
    Neighbor priority is 0, State is FULL, 6 state changes
    DR is 0.0.0.0 BDR is 0.0.0.0
<output omitted>
```

Interpreting the OSPF Database

```
RouterA#show ip ospf database
     OSPF Router with ID (10.0.0.11) (Process ID 1)
                Router Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum Link count
10.0.0.11       10.0.0.11       548         0x80000002 0x00401A 1
10.0.0.12       10.0.0.12       549         0x80000004 0x003A1B 1
100.100.100.100 100.100.100.100 548         0x800002D7 0x00EEA9 2
                Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
172.31.1.3      100.100.100.100 549         0x80000001 0x004EC9
                Summary Net Link States (Area 0)
Link ID         ADV Router      Age         Seq#       Checksum
10.1.0.0        10.0.0.11       654         0x80000001 0x00FB11
10.1.0.0        10.0.0.12       601         0x80000001 0x00F516
<output omitted>
```

The show ip route Command

```
RouterB>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.31.0.0/24 is subnetted, 2 subnets
O IA    172.31.2.0 [110/1563] via 10.1.1.1, 00:12:35, FastEthernet0/0
O IA    172.31.1.0 [110/782] via 10.1.1.1, 00:12:35, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.200.200.13/32 is directly connected, Loopback0
C       10.1.3.0/24 is directly connected, Serial0/0/0
O       10.1.2.0/24 [110/782] via 10.1.3.4, 00:12:35, Serial0/0/0
C       10.1.1.0/24 is directly connected, FastEthernet0/0
O       10.1.0.0/24 [110/782] via 10.1.1.1, 00:12:37, FastEthernet0/0
O E2    10.254.0.0/24 [110/50] via 10.1.1.1, 00:12:37, FastEthernet0/0
```

در جدول Routing در جلوی مسیرهایی که با پروتکل OSPF در جدول قرار گرفته اند با حرف O بزرگ نمایش داده می شوند .

Router – ID in OSPF

Router – ID : هر کدام از روترهای دخیل در پروسه OSPF دارای یک شناسه یا ID برای خود می باشند که یک عدد 32 بیتی است و در فرمت Dotted – Decimal , شبیه به آدرس IP بیان می گردد .هر روتر در ابتدا شروع پروسه OSPF اقدام به تعیین این شناسه خواهد کرد .بسیاری از عملکردهای پروتکل OSPF وابسته به Router – ID می باشد. Router – ID نباید در دو روتر همسایه برابر باشد .

از سه طریق Router – ID تعریف می شود :

1. Static : با دستور زیر می توانیم Router – ID را تعریف یا تغییر دهیم و با نوشته شدن این دستور , همین شناسه مورد استفاده قرار می گیرد:

Router (config – Router) # EIGRP Router – ID A.B.C.D

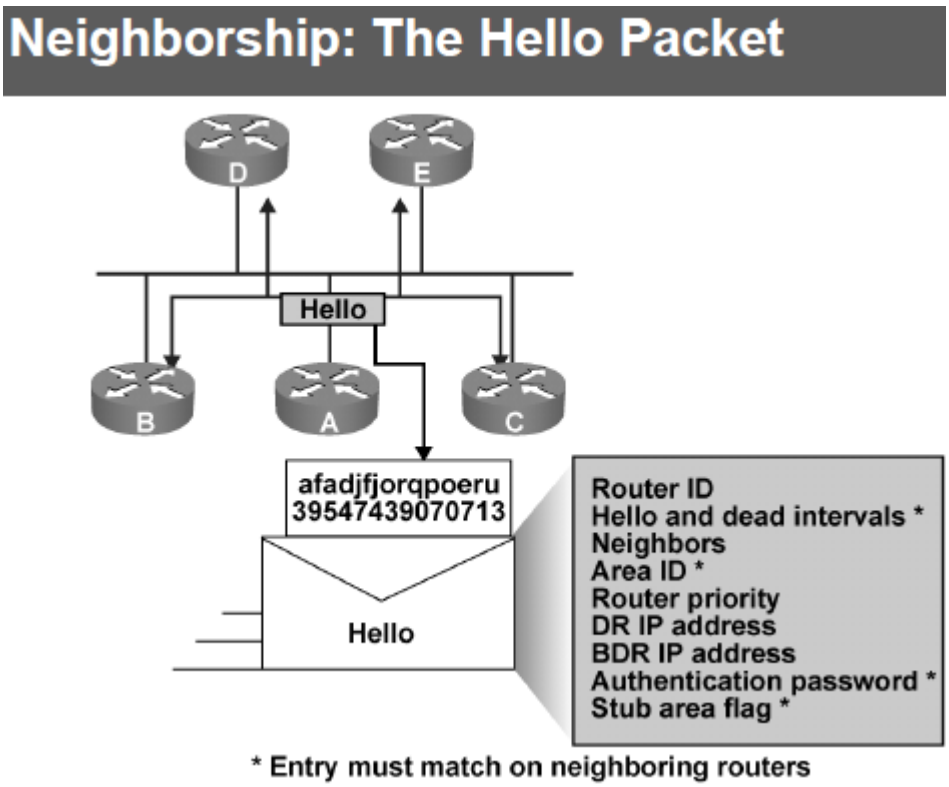
2. Highest Loopback IP – Address UP/UP : در صورت موجود بودن پورت های Loopback , بزرگترین آدرسIP مربوط به آنها به عنوان شناسه روتر تعیین می گردد .

3. Highest Non – Loopback IP – Address UP/UP : در صورت نبودن هیچ پورت Loopback , بالاترین IP مربوط به Interface های فعال (UP/UP) به عنوان شناسه روتر برگزیده خواهند شد .

دستور Reset کردن پروسه OSPF :

Router # Clear IP OSPF Process

Hello Packet



زمانی که پروتکل OSPF روی یک مسیر فعال می شود Router هر 10 ثانیه یک بار بسته های Hello را به روترهای همسایه ارسال می کند و در صورتی که در زمان حداکثر 40 ثانیه هیچ Hello Packet از روتر همسایه دریافت نشود آن Router به عنوان یک روتری که دچار مشکل شده است تشخیص داده می شود .

وقتی یک روتر یک Hello Packet از روتر همسایه دریافت می کند برخی پارامترها داخل آن توسط روتر بررسی خواهد شد و در صورتی که این پارامترها با پارامترهای خود مطابقت داشته باشد روتر اقدام به برقراری رابطه مجاورت با آن روتر خواهد نمود .

در شکل بالا پارامترهایی که در پیام Hello جهت برقراری رابطه مجاورت بررسی خواهد شد با ستاره (*) علامتگذاری شده است .

اطلاعات موجود در یک Hello Packet :

- OSPF Router ID
- Stub area flag
- Plus the following interface-specific settings:
  - Hello interval
  - Dead Interval
  - Subnet mask
  - List of neighbors reachable on the interface
  - Area ID
  - Router priority
  - Designated Router (DR) IP address
  - Backup DR (BDR) IP address
  - Authentication digest

Hello interval :

مدت زمان Hello در VAN مساوی 10 ثانیه است .

مدت زمان Hello در WAN مساوی 30 ثانیه است .

دستور تغییر زمان Hello interval :

Router (config – if) # IP OSPF Hello – interval seconds

مقدار زمان Hello را با دستور زیر می توانیم ببینیم :

Router # Show IP OSPF Interface type mod/num

Dead interval :

مدت زمان Dead در VAN مساوی با 4 تا Hello time یعنی 40 ثانیه است .

مدت زمان Dead در WAN مساوی با 4 تا 30 ثانیه یعنی 120 ثانیه است .

دستور تغییر زمان Dead interval :

Router (config – if) # IP OSPF Dead – interval seconds

: Subnet Mask

باید در هر دو روتر با هم برابر باشد یعنی باید در یک شبکه باشند (هم Subnet mask و هم Subnet number هر دو روتر باید برابر باشند)

: Area ID

هر دو Interface باید در یک Area باشند تا همسایگی تشکیل شود .

: Authentication Digest

چک کردن هویت یکدیگر و در صورت برابر بودن در دو روتر با هم همسایگی تشکیل می دهند .

: Maximum Transmission Unit (MTU)

MTU یکی از پارامترهایی است که در Hello Packetها قرار دارد و اندازه آن برابر است با 1500 بیت . که نشان دهنده مقدار Dataایی است که از لایه 3 فرستاده می شود .باید مقدار MTU در بین دو روتر همسایه برابر باشد اگر برابر نباشد در مرحله Exchange Topology به مشکل بر می خورد .

دستور تغییر MTU :

Router (config – if) # IP MTU number برای پروتکل IP

Router (config – if) # MTU number برای همه پروتکل ها

Authentication in OSPF

عبارت Authentication اشاره به پروسه بررسی هویت دارد . روترهای OSPF با استفاده از این ویژگی می توانند در هنگام دریافت پیامی از سوی دیگر روترها اقدام به بررسی هویت دستگاه ارسال کننده پیام نمایند .

پروتکل OSPF از سه روش مختلف برای انجام Authentication بهره می گیرد :

- Type 0 (No Authentication)
- Type 1 (Clear Text)
- Type 2 (MD5)

در صورتی که می خواهید از Type 0 استفاده کنید نیازی به انجام هیچ کاری نیست زیرا به صورت پیش فرض روترهای OSPF از ویژگی Authentication استفاده نمی کنند . اگر زمانی Authentication فعال باشد با دستور زیر می توان به حالت پیش فرض یعنی به حالت Type 0 برگردیم :

```
Router ( config – if ) # IP OSPF Authentication Null
```

اما اگر بخواهیم از دو نوع دیگر استفاده کنیم پیکربندی های زیر باید انجام گیرد :

Type 1 :

```
Router ( config – if ) # IP OSPF Authentication
Router ( config – if ) # IP OSPF Authentication – key String
```

Type 2 :

```
Router ( config – if ) # IP OSPF Authentication Message – Digest
Router ( config – if ) # IP OSPF Authentication – Digest – key # MD5
String
```

دستور فعال سازی Authentication بر روی یک Area :

Router (config) # Area # Authentication [Message – Digest]

وقتی دستور بالا را اعمال کردیم باید بر روی اینترفیس ها تک تک کلید را درست کنیم .

مثال 1 :

Router (config) # Interface FastEthernet 0/1

Router (config – if) # IP OSPF Authentication

Router (config – if) # IP OSPF Authentication – key Cisco

مثال 2 :

Router (config) # Area 0 Authentication Message – Digest

Router (config) # Interface FastEthernet 0/2

Router (config – if) # IP OSPF Authentication – Digest – key 1 MD5 Cisco

Router (config – if) # IP OSPF Authentication – Digest – key 2 MD5 Router

نکته :

همیشه از جوانترین کلید یعنی آخرین کلید ساخته شده برای Authentication در پروسه OSPF استفاده می شود.

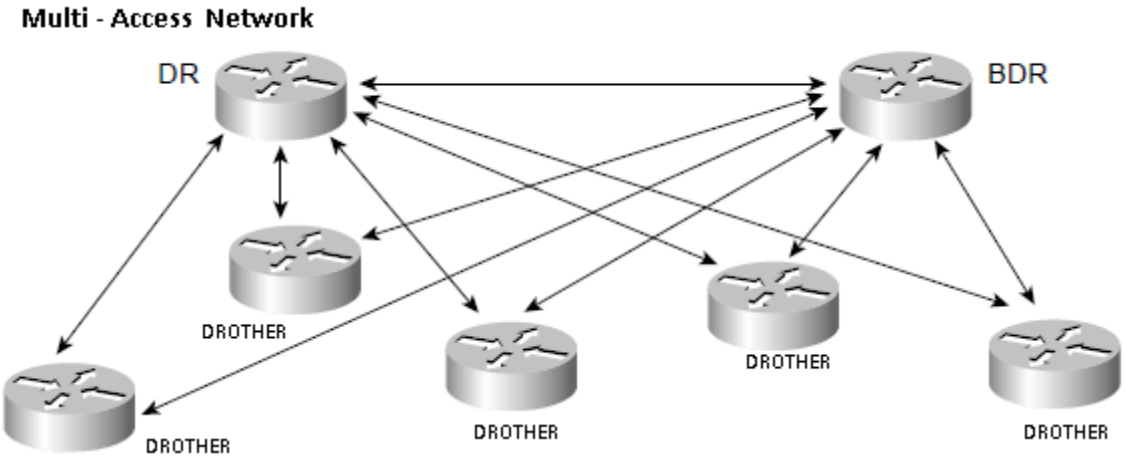
دستور نمایش نوع متد استفاده شده :

Router # Show IP OSPF Interface type mod/num

دستور زیر وجود مشکلات مربوط به برقراری رابطه مجاورت بین روترهای OSPF را نشان خواهد داد :

Router # Debug IP OSPF adj

روترهای DR و BDR و DROTHER :



Designated Router (DR) :

در صورتی که OSPF را در روی شبکه های Multi – Access مانند LAN اجرا کنیم روترها اقدام به انتخاب یک روتر به نام Designated Router (DR) می کنند که نقش اصلی را در تبادل اطلاعات مابین روترهای همان شبکه ایفا می کند .

Backup Designated Router (BDR) :

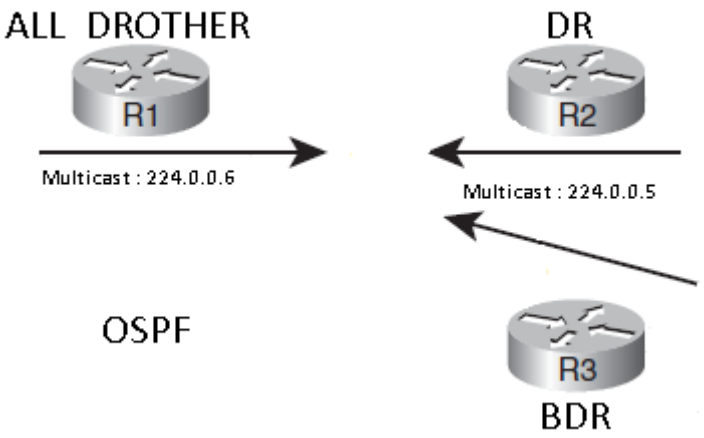
این روتر به عنوان جایگزینی برای روتر DR بوده و به صورت مستمر عملکرد DR را زیر نظر دارد . در صورتی که مشکلی در کار روتر DR ایجاد گردد وظایف آن بر روی BDR منتقل خواهد شد .

DROTHER :

به روترهای دیگر داخل شبکه که نه DR و نه BDR هستند DROTHER می گویند .

نکته :

تغییرات در شبکه از روترهای DROTHER از طریق آدرس Multicast = 224.0.0.6 به روترهای DR و BDR خبر داده می شود و روترهای DR و BDR با آدرس Multicast = 224.0.0.5 به همه روترها خبر می دهند .



تعیین روترهای DR و BDR به دو صورت زیر است :

روش اول :

به صورت پیش فرض هر روتری که بالاترین Router – ID را در بین همه روترهای شبکه داشته باشد به عنوان روتر DR و روتری که Router – ID آن بعد از روتر DR بالاترین در بین بقیه روترها باشد به عنوان روتر BDR انتخاب می شوند .

روش دوم :

اگر بخواهیم روتر DR یا BDR را تعیین یا تغییر بدهیم به صورت دستی باید دستور زیر را بر روی روتر مورد نظر اعمال کنیم :

Router (config – if) # IP OSPF Priority #

: عددی بین 1 تا 255 را می توانیم استفاده کنیم که پیش فرض عدد 1 است .

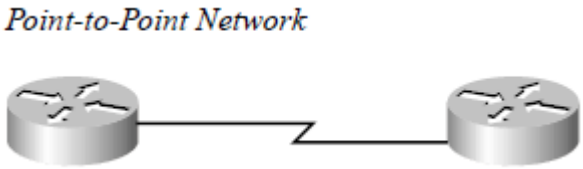
نکته :

در شبکه های Point – to – Point روترهای DR و BDR تعیین نمی شود .

Network Type

انواع Network Type :

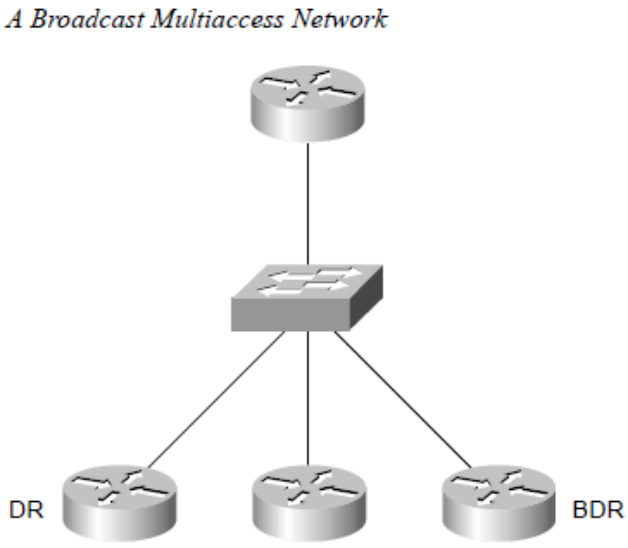
Point – to – Point Network



خصوصیات شبکه :

- Dynamic Neighbor ship
- No DR & BDR
- IOS
- Only 2 Nodes

Broadcast Network

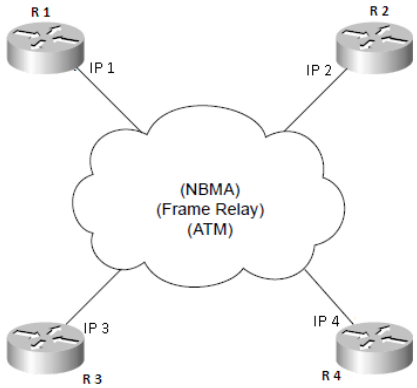


خصوصیات شبکه :

- Dynamic Neighbor ship
- DR & BDR
- IOS
- Mach Than 2 Nodes

NBMA (Non – Broadcast Multi Access)

A Nonbroadcast Multiaccess (NBMA) Network

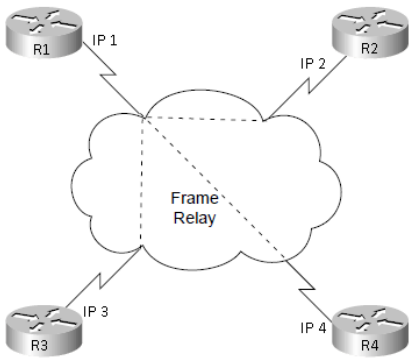


خصوصیات شبکه :

- Manual Neighbor ship
- DR & BDR
- Hello time : 30 s
- Mach Than 2 Nodes
- IP Unequal Range

Point – to – Multipoint Network

Point-to-Multipoint Network



خصوصیات شبکه :

- Manual Neighbor ship
- DR & BDR
- Hello time : 30 s
- Mach Than 2 Nodes
- IP Equal Range

دستور تعیین Network Type :

Selecting the OSPF Network Type for NBMA Networks

```
Router(config-if)#
ip ospf network [{broadcast | non-broadcast | point-to-
multipoint [non-broadcast] | point-to-point}]
```

- Defines OSPF network type

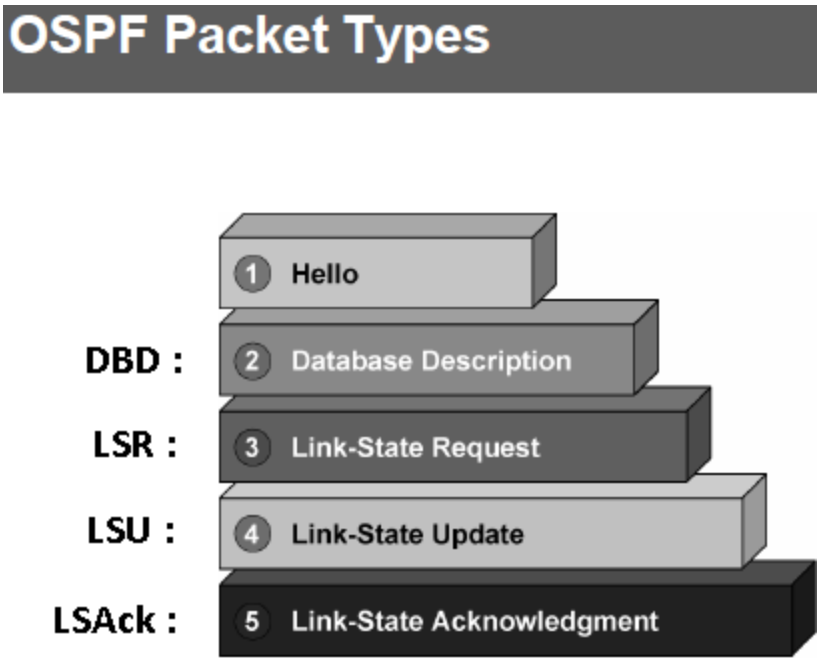
جدول زیر انواع Network typeها را نشان داده و با هم مقایسه کرده است :

OSPF over NBMA Topology Summary

OSPF Mode	NBMA Preferred Topology	Subnet Address	Hello Timer	Adjacency	RFC or Cisco
Broadcast	Full or partial mesh	Same	10 sec	Automatic, DR/BDR elected	Cisco
Nonbroadcast (NBMA)	Full or partial mesh	Same	30 sec	Manual configuration, DR/BDR elected	RFC
Point-to-multipoint	Partial-mesh or star	Same	30 Sec	Automatic, no DR/BDR	RFC
Point-to-multipoint nonbroadcast	partial-mesh or star	Same	30 sec	Manual configuration, no/DR/BDR	Cisco
Point-to-point	Partial-mesh or star, using subinterface	Different for Each Subinterface	10 sec	Automatic, no DR/BDR	Cisco

OSPF Packets

پروتکل OSPF برای بروزرسانی و Update جدول مسیریابی استفاده خواهد کرد :



Hello : با استفاده از این پیام یک روتر قادر به شناسایی روترهای همسایه خواهد شد و بعد از شناسایی بین آنها رابطه مجاورت برقرار می شود .

DBD : با استفاده از این پیام به روز بودن یا Update بودن اطلاعات جدول LSDB یک روتر مورد بررسی قرار خواهد گرفت .

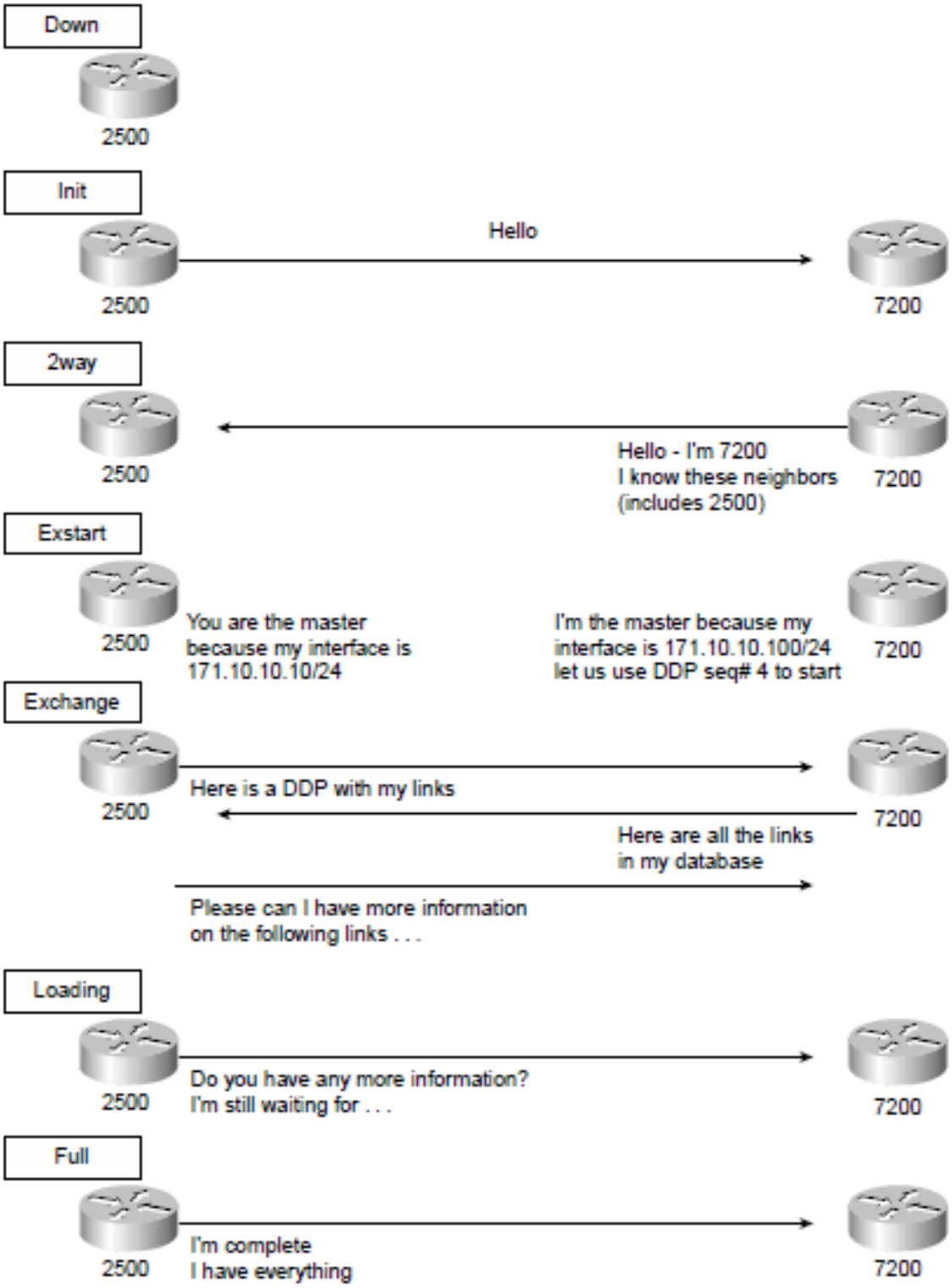
LSR : یک روتر با ارسال این پیام از سایر روترها درخواست دریافت اطلاعات مسیریابی می کند .

LSU : پاسخی خواهد بود که روتر به درخواست پیام LSR ارسال می کند و با استفاده از پیام LSU اطلاعات درخواستی را برای روترهای دیگر ارسال می کند .

LSAck : روتر بعد از دریافت پیام های LSU , LSR , DBD روتر دریافت کننده پیام با ارسال پیام LSAck برای روتر ارسال کننده پیام دریافت صحیح پیام را تأیید خواهد کرد .

مراحل پروسه OSPF :

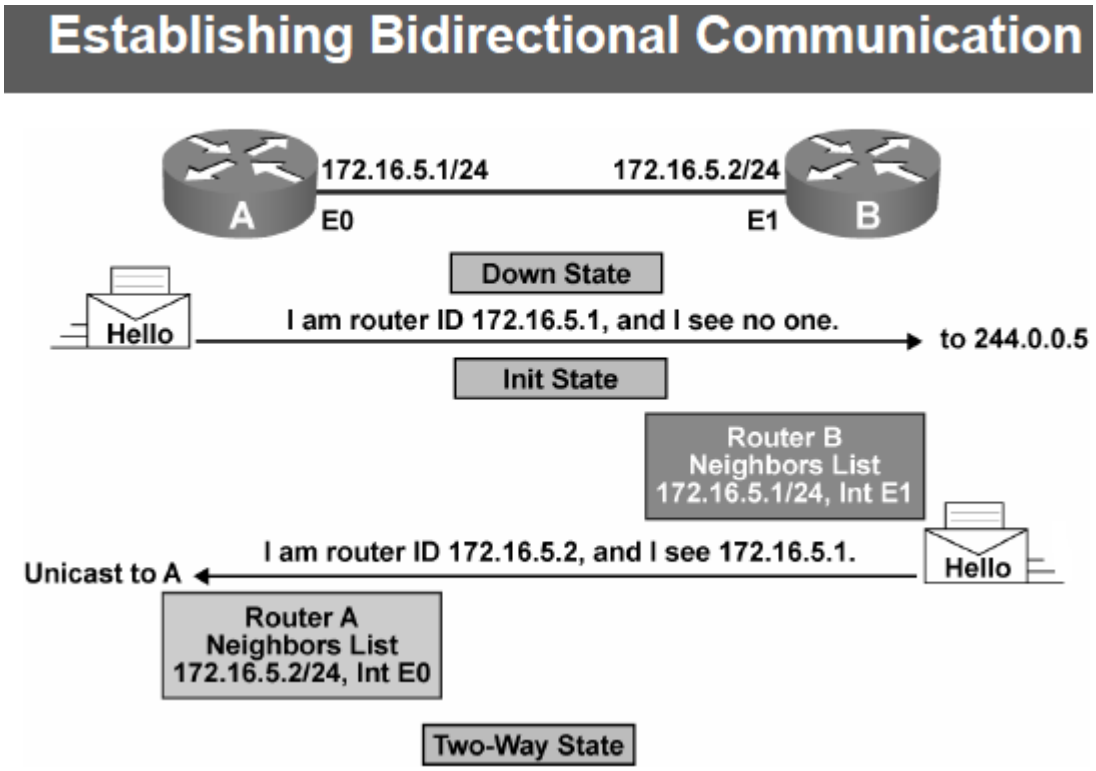
The Stages of Updating the Routers About the Network



Down → Init → Two – Way → Exstart → Exchange → Loading → Full

مرحله اول :

در این مرحله Router A بعد از فعال شدن در مد Down قرار خواهد گرفت و در صورتی که پیکربندی پروتکل OSPF بر روی این روتر از طریق اینترفیس های که در پیکربندی OSPF مشخص شده اند شروع به ارسال پیام های Hello به صورت Multicast خواهد کرد . به تصویر زیر توجه کنید مشاهده می کنید که Router A در حال ارسال پیام Hello به صورت Multicast برای Router B می باشد .



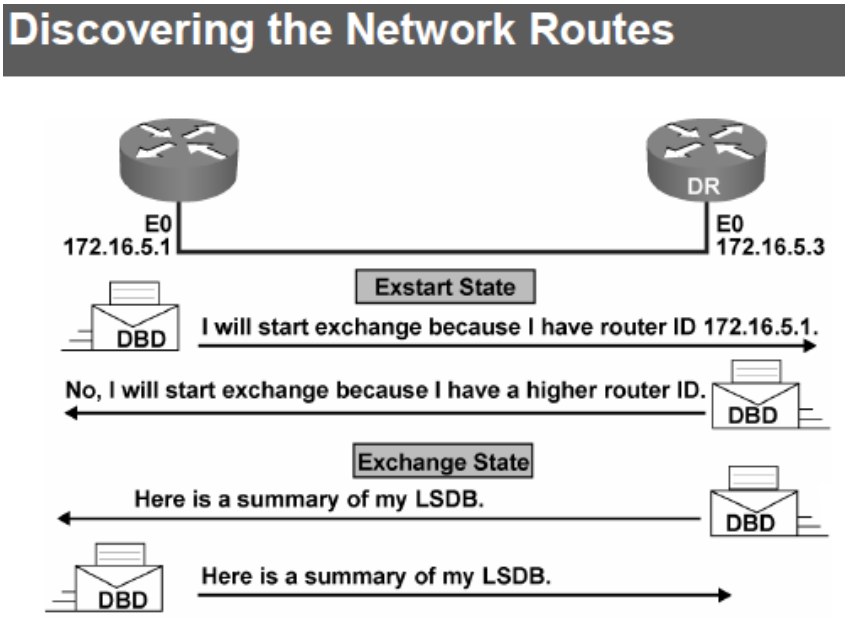
مرحله دوم :

در این مرحله پیام Hello مربوط به Router A توسط Router B دریافت می شود و Router B یکسری از فیلدها را از جمله Area ID و شماره As در پیام Hello چک خواهد کرد و در صورت یکسان بودن و مطابقت داشتن این فیلدها Router B مشخصات Router A را به عنوان همسایه در جدول Neighbor خود اضافه خواهد کرد و به Router A پیام Hello می فرستد .

نکته :

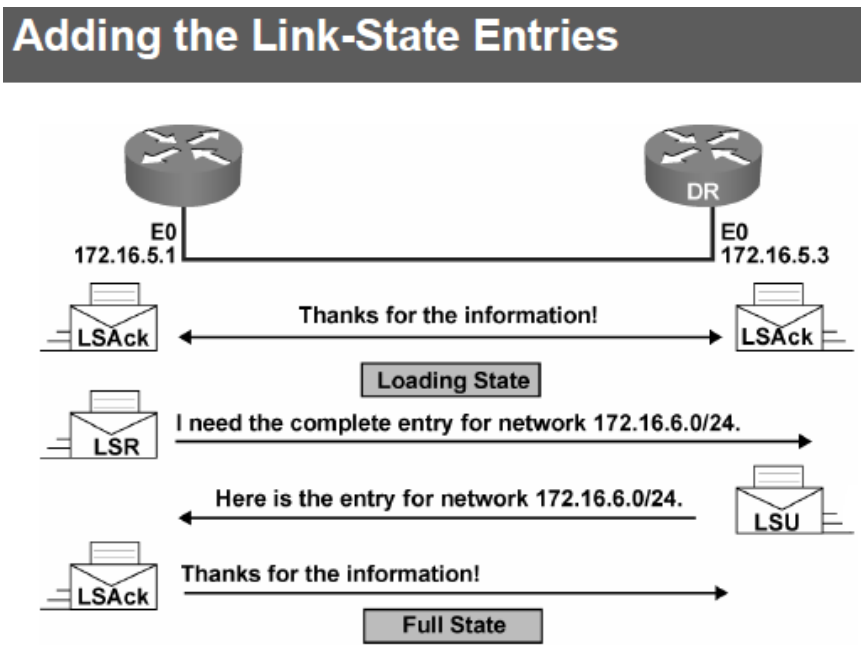
تا زمانی که دو روتر به مرحله two – way نرسند و همسایگی تشکیل نشود حق ندارند Topology Change انجام دهند .

در صورتی که ارتباط بین روترها و لینک بین آنها از نوع Broadcast باشد مانند اتصالات Ethernet نیاز به انتخاب DR و BDR می باشد و کلیه روترهای شبکه باید رابطه مجاورت با DR و BDR برقرار نمایند . روتری که دارای کمترین Router ID باشد به عنوان Master Router و روتر دیگر به عنوان Slave Router انتخاب می شود .



مرحله سوم :

بعد از پایان برقراری رابطه مجاورت پیام های DBD یا Database Description بین روترها ردوبدل خواهد شد.پیام های DBD جهت بررسی به روز بودن جدول LSDB استفاده خواهد شد و شامل خلاصه ای از جدول LSDB میباشد و در صورتی که یک روتر پیام DBD را دریافت نماید که دارای شماره Sequence Number بالاتری باشد یعنی شامل اطلاعات جدیدتری باشد حال با ارسال یک پیام LSR برای روتر ارسال کننده پیام DBD تقاضای ارسال اطلاعات جدید مسیریابی را خواهد کرد این مرحله Loading State نامیده می شود .



وقتی یک روتر پیام LSR دریافت نماید با استفاده از پیام LSU اطلاعات درخواست شده را برای ارسال کننده پیام LSR ارسال خواهد کرد و روتر دریافت کننده LSU جدول LSDB خود را با استفاده از اطلاعات جدید به روز رسانی میکند و یک پیام LSAck مبنی بر اینکه پیام به درستی دریافت شد را ارسال می کنند .

نکته :
هر 30 دقیقه یکبار پروتکل OSPF اقدام به انتشار خلاصه ای از اطلاعات LSDB در کل شبکه یا Area خواهد کرد .

در شبکه های Multipoint وضعیت روترهای شبکه با یکدیگر به حالت زیر است :

روترهای DROTHER با یکدیگر فقط در حالت tow – way قرار می گیرند ولی روترهای DROTHER با روترهای DR و BDR در حالت Full قرار می گیرند .

نکته :
پیام های LSUها از تعدادی LSA تشکیل شده است .

LSDB : Link State Database

تمامی روترهایی که در داخل یک Area قرار دارند دارای اطلاعات کاملا یکسانی در داخل جدول توپولوژی خود می باشند . جدول توپولوژی یا همان LSDB از مجموعه ای از LSAها تشکیل شده است .
به منظور محاسبه بهترین مسیرهای منتهی به مقاصد مختلف هر روتر اقدام به اعمال الگوریتم SPF بر روی محتویات جدول LSDB کرده و مسیرهای شناسایی شده را در داخل جدول Routing قرار می دهد .

جدول زیر نشان دهنده انواع LSAهای مورد استفاده در OSPF می باشد :

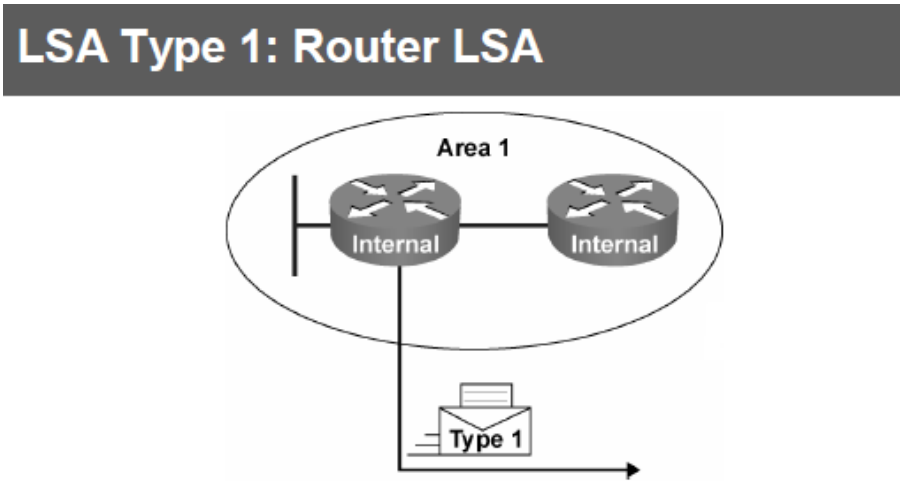
LSA Types

LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous system external LSAs
6	Multicast OSPF LSA
7	Defined for not-so-stubby areas
8	External attributes LSA for Border Gateway Protocol (BGP)
9, 10, 11	Opaque LSAs

توضیحات مختصری از انواع LSAها :

LSA type 1	این LSA در داخل یک Area توسط هر یک از روترهای داخل آن Area ایجاد خواهد شد و وضعیت اتصالات روتر یا اینترفیس های روتر را به اطلاع سایر روترها می رساند . هر یک از روترهای OSPF داخل یک Area قادر خواهند بود یک پیام LSA type 1 را ایجاد و داخل Area منتشر نمایند .
LSA type 2	این LSA از طریق یک DR در شبکه های Broadcast و NBMA به وجود خواهد آمد و روترهای متصل به این شبکه را تبلیغ خواهند کرد . LSA type 2 از طریق DR ایجاد و در داخل یک Area منتشرخواهد شد .
LSA type 3	این LSA توسط روتر ABRایجاد خواهد شد و شامل خلاصه ای از مسیرها و روترهای Areaهای متصل به روتر ABR می باشد .
LSA type 4	روترهای واقع در OSPF Domain با استفاده از این پیام از محل قرارگیری روتر ASBR مطلع می شوند .
LSA type 5	LSA نوع 5 از طریق یک ASBR ایجاد و مسیرهای بیرون OSPF Domain یا خارج از As را تبلیغ خواهد کرد .
LSA type 6	این LSA جهت عملکرد Multicasting مورد استفاده قرار خواهد گرفت .
LSA type 7	در صورتی که یک Area به عنوان NSSA تعیین گردد ASBR به جای ارسال LSA type 5 از این نوع پیام بهره خواهد گرفت .
LSA type 8	این نوع از LSAها در حقیقت Attributeهای خارجی مربوط به محیط های OSPF و BGP را تشریح خواهد کرد که فعلا در روترهای سیسکو مورد استفاده قرار نمی گیرد .
LSA type 9 , 10 , 11	این LSAها برای ارتقا و کاربردهای آینده OSPF رزرو شده اند . مثلا سیسکو از این LSAها برای شبکه های MPLS استفاده خواهد کرد .

LSA Type 1 : Router LSA



این نوع از LSA به نام Router LSA نیز نامیده می شود و به منظور شناساندن روترها از روی RID مربوط به آنها مورد استفاده قرار می گیرد . هر روتر اقدام به ایجاد یک LSA type 1 برای خود کرده و سپس آن را برای دیگر روترهای واقع در آن Area ارسال میکند . بدین ترتیب که یک روتر LSA type 1 خود را به روترهای همسایه خود ارسال کرده و آنها نیز این پیام را به دیگر روترهای همسایه واقع در همان Area می فرستد . این کار تا جایی ادامه پیدا می کند که همه روترهای واقع در داخل آن Area اقدام به دریافت LSA مزبور نماید .

هر LSA type 1 علاوه بر شناسه یا ID روتر فرستنده حاوی اطلاعات زیر است :

- Interfaceهایی که در روی آنها پروسه انتخاب روتر DR اتفاق نیفتاده است .این پیام شامل IP و ماسک آن اینترفیس به همراه Cost مربوط به همان پورت خواهد بود .این اینترفیس ها در خروجی دستورات به عنوان شبکه های Stub نشان داده خواهد شد .

Interfaceهایی که در روی آنها پروسه انتخاب روتر DR اتفاق افتاده است . این پیام شامل IP مربوط به روتر DR بوده که بیانگر آن است که اتصال یاد شده به عنوان یک Transit Network می باشد .

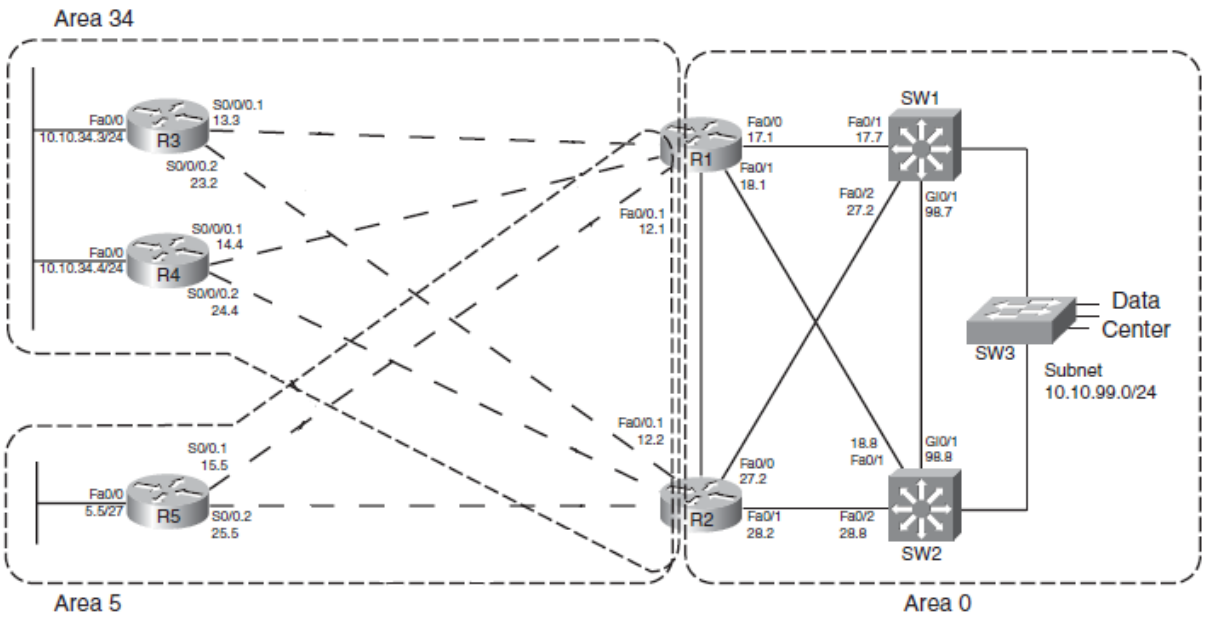
Interfaceهایی که در روی آنها پروسه انتخاب روتر DR اتفاق نیفتاده است اما روتری در طرف دیگر اتصال قرار دارد . این پیام حاوی RID مربوط به روتر مزبور است .

نکته :

شبیه به دیگر انواع LSAها پروتکل OSPF یک پیام LSA type 1 را با استفاده از یک عدد 32 بیتی به نام Link State Identifier (LSID) نامگذاری میکند . همه روترها در هنگام ایجاد LSA type 1 برای خود RID مربوط به خود را به عنوان LSID در نظر می گیرد .

نکته :

روترهای داخلی یک Area تنها یک LSA type 1 را ایجاد کرده اما روترهای ABR به ازای هر کدام از Area های متصل یک LSA type 1 برای خود ایجاد می نمایند.هر کدام از این LSA type 1ها تنها به اعضای همان Area ارسال می شود . همچنین به دلیل آنکه روترها تنها دارای یک RID برای خود می باشند تمامی LSA type 1های ایجاد شده حامل همان RID خواهند بود .



با توجه به شکل بالا تمامی روترهای داخل یک Area اقدام به ایجاد یک LSA type 1 برای خود کرده و آن را به دیگر اعضای همان Area ارسال می کنند . برای مثال در شکل فوق در Area 5 تنها دارای یک روتر

داخلی با RID : 5.5.5.5 و دو روتر ABR (روتر R1 با RID : 1.1.1.1 و روتر R2 با RID : 2.2.2.2) است . هر کدام از این روترها اقدام به ایجاد یک LSA type 1 برای Area 5 کرده و آن را به دو روتر دیگر ارسال می کنند . در نتیجه هر سه روتر دارای سه عدد LSA type 1 یکسان خواهند بود . روتر R5 دارای پورت های Fa 0/0 , s0/0/0.1 , s0/0/0.2 می باشد که پروتکل OSPF بر روی همه این پورت ها فعال می باشد . روتر R5 با اینترفیس های Point – to – Point به روترهای R1 و R2 متصل شده است .

در حالت کلی با مراجعه به خروجی دستورات می توان اطلاعات زیر را بدست آورد :

- LSID مربوط به LSA type 1 در روی روتر R5 که برابر با 5.5.5.5 می باشد .
- وجود سه عدد اتصال با شبکه Stub که نشان دهنده آدرس و ماسک است .
- وجود دو عدد اتصال با روترهای همسایه : (اتصال اول با روتر R1 با ID برابر با 1.1.1.1 و اتصال دوم با روتر R2 با ID برابر با 2.2.2.2)

اگر فقط دستور Show IP OSPF Database را بزنیم خروجی زیر نمایش داده می شود :

```
OSPF Router with ID (5.5.5.5) (Process ID 5)

                Router Link States (Area 5)

Link ID         ADV Router      Age         Seq#       Checksum Link count
1.1.1.1         1.1.1.1         835         0x80000002 0x006BDA 2
2.2.2.2         2.2.2.2         788         0x80000002 0x0082A6 2
5.5.5.5         5.5.5.5         787         0x80000004 0x0063C3 5

                Summary Net Link States (Area 5)

Link ID         ADV Router      Age         Seq#       Checksum
10.10.12.0      1.1.1.1         835         0x80000001 0x00F522
10.10.12.0      2.2.2.2         787         0x80000001 0x00D73C
```

دستور فوق نشان دهنده خلاصه ای از LSAهای شناسایی شده توسط R5 می باشد . در خروجی دستور فوق هر LSA در یک سطر جداگانه نشان داده شده است و بیانگر LSID مربوط به آن LSA خواهد بود . سه سطری که در خروجی این دستور پررنگ تر نمایش داده شده است بیانگر RIDهای موجود در داخل پیام های LSA type 1 می باشد .

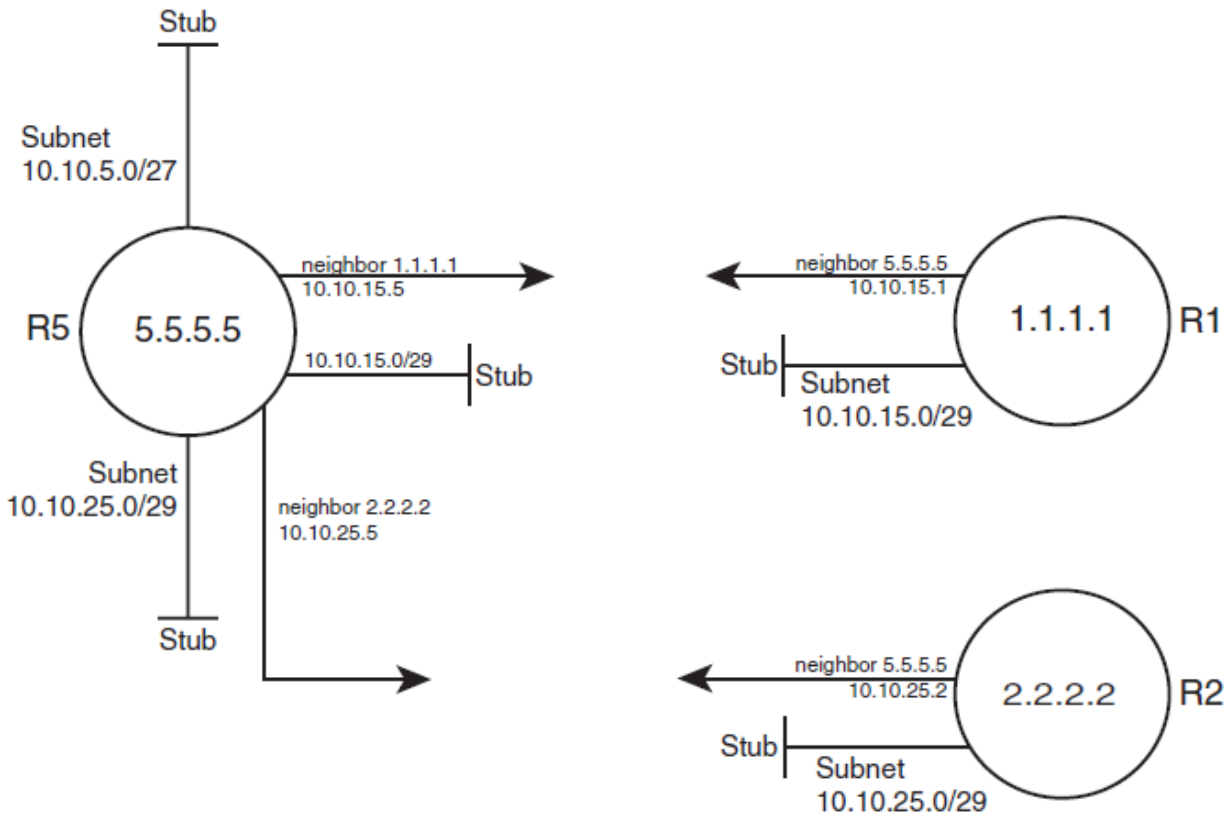
اگر دستور [Router LSID] Show IP OSPF Database را بزنیم خروجی زیر نمایش داده می شود :

```
R5#show ip ospf database router 5.5.5.5

            OSPF Router with ID (5.5.5.5) (Process ID 5)

                Router Link States (Area 5)

  LS age: 796
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 5.5.5.5
  Advertising Router: 5.5.5.5
  LS Seq Number: 80000004
  Checksum: 0x63C3
  Length: 84
  Number of Links: 5

    Link connected to: another Router (point-to-point)
     (Link ID) Neighboring Router ID: 2.2.2.2
     (Link Data) Router Interface address: 10.10.25.5
      Number of TOS metrics: 0
       TOS 0 Metrics: 64

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 10.10.25.0
     (Link Data) Network Mask: 255.255.255.248
      Number of TOS metrics: 0
       TOS 0 Metrics: 64


      Link connected to: a Stub Network
       (Link ID) Network/subnet number: 10.10.5.0
       (Link Data) Network Mask: 255.255.255.224
        Number of TOS metrics: 0
        TOS 0 Metrics: 1
```

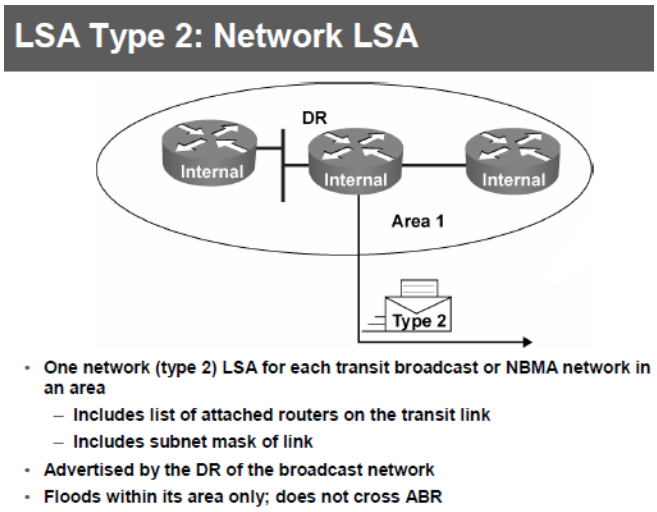
```
Link connected to: another Router (point-to-point)
 (Link ID) Neighboring Router ID: 1.1.1.1
 (Link Data) Router Interface address: 10.10.15.5
  Number of TOS metrics: 0
   TOS 0 Metrics: 64

Link connected to: a Stub Network
 (Link ID) Network/subnet number: 10.10.15.0
 (Link Data) Network Mask: 255.255.255.248
  Number of TOS metrics: 0
   TOS 0 Metrics: 64
```

اجرای دستور فوق باعث نمایش داده شدن تمامی جزئیات مربوط به LSAهای شناسایی شده توسط روتر 5.5.5.5 خواهد شد . با استفاده از تمامی اطلاعات موجود در داخل پیام های LSA type 1 ارسالی از روترهای R1 و R2 و R5 , روترها می توانند شمایی از توپولوژی شبکه و نوع اتصال با دستگاه های دیگر را از دید خود رسم نمایند .

شکل زیر نشان دهنده درک روترهای واقع در Area 5 از توپولوژی شبکه مربوط به همان Area است :



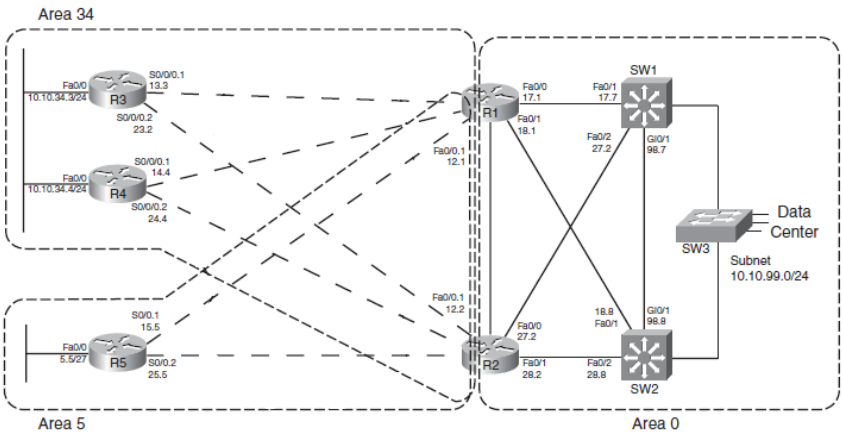
LSA Type 2 : Network LSA



الگوریتم SPF نیاز به در اختیار داشتن اطلاعات مربوط به نودها و اتصالات مابین آنها دارد مخصوصا در مورد شبکه های Multi – Access مانند LAN . به همین منظور است که OSPF از پیام های خاصی به نام Network LSA یا LSA Type 2 بهره می گیرد. LSA Type 2 را فقط روتر DR ایجاد و ارسال میکند و در یک Area منتشر می شود.روترهای دیگر با LSA Type 2 میتوانند Mask شبکه های Multi – Access را بفهمند و تعداد روترهای آن شبکه را تشخیص دهند .

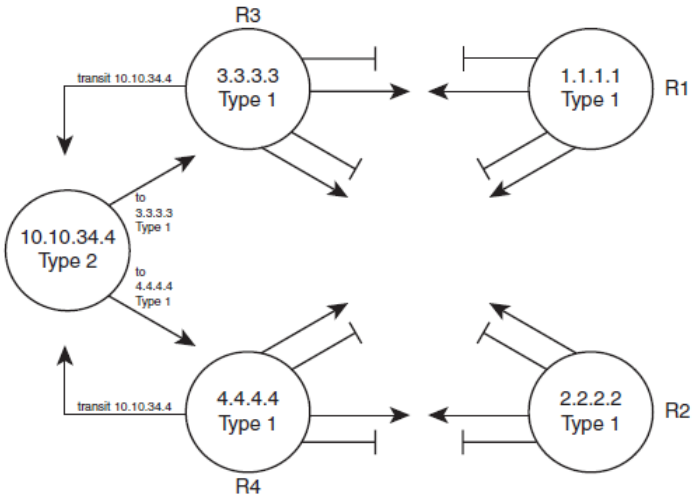
برای مشاهده LSA Type 2 بر روی روتر DR باید دستور زیر را وارد کنیم :

Router # Show IP OSPF Database Network DR – IP – Address



شکل فوق نشان می دهد روترهای R3 و R4 از طریق یک پورت LAN با یکدیگر در تماس می باشند که این باعث خواهد شد تا دو روتر مزبور اقدام به انتخاب روترهای DR و BDR در روی پورت LAN خود نمایند .

پروتکل OSPF پروسه انتخاب روترهای DR و BDR را آغاز می کند . در صورتی که پارامتر Priority برابر با مقدار پیش فرض آن یعنی عدد 1 باشد روتر R4 به دلیل دارا بودن RID بزرگتر به عنوان DR برگزیده خواهد شد . در مرحله بعد روتر R4 اقدام به ایجاد و انتشار LSA Type 2 از روی اینترفیس Fa0/0 خواهد کرد .شکل زیر شمایی از توپولوژی مربوط به Area 34 است :



خروجی دستور Show IP OSPF Database Network 10.10.34.4 به صورت زیر نمایش داده می شود :

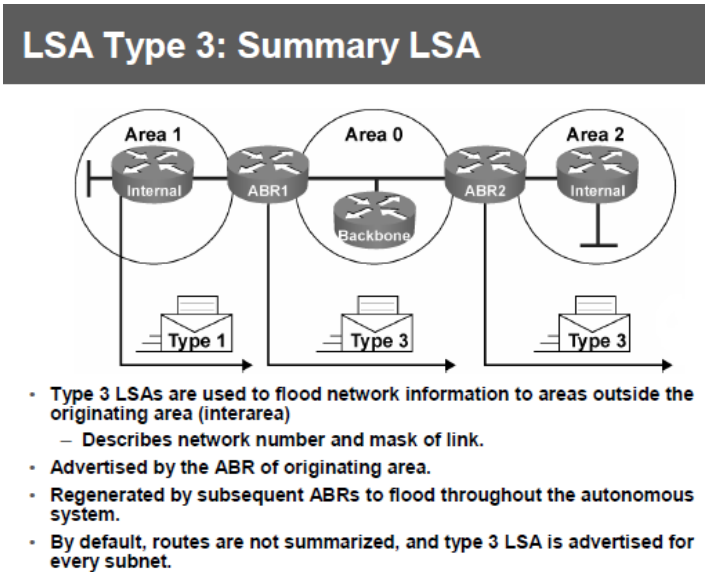
```
R3#show ip ospf database network 10.10.34.4

            OSPF Router with ID (3.3.3.3) (Process ID 3)

                Net Link States (Area 34)

  Routing Bit Set on this LSA
  LS age: 1161
  Options: (No TOS-capability, DC)
  LS Type: Network Links
  Link State ID: 10.10.34.4 (address of Designated Router)
  Advertising Router: 4.4.4.4
  LS Seq Number: 80000001
  Checksum: 0xAB28
  Length: 32
  Network Mask: /24
        Attached Router: 4.4.4.4
        Attached Router: 3.3.3.3
```

دستور بالا محتویات پیام LSA Type 2 را در رابطه با LSID برابر با 10.10.34.4 نمایش می دهد . همچنین RID مربوط به روترهای متصل را می توانید در قسمت انتهای دستور مشاهده کنید .

نکته :

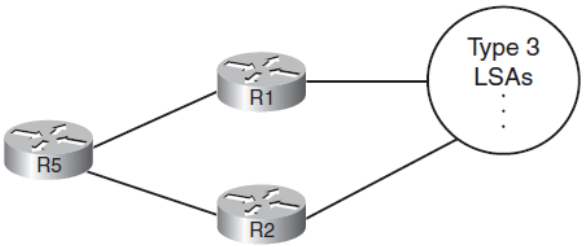
در نتیجه مباحث فوق می توان گفت که توپولوژی مربوط به یک Area توسط پیام های LSA Type 1 و LSA Type 2 ترسیم می گردد .

LSA Type 3 : Summary LSA



با وجود اینکه روترهای ABR نباید اقدام به هدایت پیام های LSA Type 1 و LSA Type 2 از یک Area به Areaهای دیگر نماید , روترهای داخلی یک Area می بایست از شبکه های موجود در Areaهای دیگر نیز اطلاع داشته باشند . انجام چنین کاری در پروتکل OSPF با بکارگیری پیام های LSA Type 3 امکان پذیر است .بدین ترتیب که روترهای ABR به ازای هر کدام از شبکه های واقع در داخل یک Area اقدام به ایجاد یک پیام LSA Type 3 کرده و آن را به سمت دیگر Areaها ارسال می کند . همانگونه که از نام Summary LSA نیز برمی آید این پیام ها تمامی جزئیات مربوط به یک Area را به Area های دیگر ارسال نخواهد کرد .

با توجه به شکل بالا , شکل زیر نشان دهنده آن است که روترهای R1 و R2 که به عنوان ABR می باشند شبکه های متصل به این دو روتر در Area 5 را در قالب پیام های LSA Type 3 برای دیگر Areaها ارسال می کنند :



برای مشاهده LSA Type 3 بر روی روتر باید دستور زیر را وارد کنیم :

Router # Show IP OSPF Database Summary IP – Address

نکته :

روترهای ABR در هنگام ایجاد کردن یک پیام LSA اقدام به جایگذاری RID خود به عنوان روتر فرستنده یا Advertising Router و LSID مربوط به شبکه داخلی (Link ID) در داخل این پیام می کنند . همچنین ماسک مربوط به شبکه داخلی نیز در داخل LSA Type 3 گنجانده می شود . اطلاعات موجود در داخل پیام های LSA Type 3 این امکان را برای پروسه SPF فراهم می سازد تا توپولوژی مربوط به Areaهای دیگر را نیز ترسیم کنند .

به خروجی دستور زیر دقت کنید :

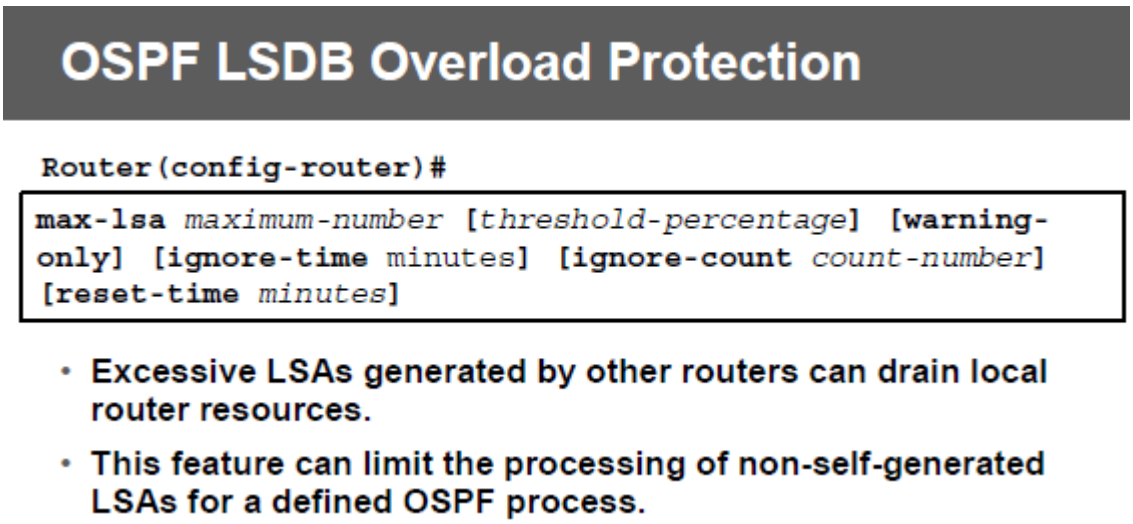
```
R3#show ip ospf database summary 10.10.99.0

            OSPF Router with ID (3.3.3.3) (Process ID 3)

                Summary Net Link States (Area 34)

  Routing Bit Set on this LSA
  LS age: 1062
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(Network)
  Link State ID: 10.10.99.0 (summary Network Number)
  Advertising Router: 1.1.1.1
  LS Seq Number: 80000002
  Checksum: 0x3D81
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 2

  Routing Bit Set on this LSA
  LS age: 1109
  Options: (No TOS-capability, DC, Upward)
  LS Type: Summary Links(Network)
  Link State ID: 10.10.99.0 (summary Network Number)
  Advertising Router: 2.2.2.2
  LS Seq Number: 80000002
  Checksum: 0x1F9B
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 2
```

دستور صفحه قبل را بر روی روتر R3 واقع در Area 34 وارد کرده ایم و LSA Type 3 را نشان می دهد که روتر R2 که یک روتر ABR است به Area 34 ارسال کرده و شبکه 10.10.99.0با ماسک 24/ که در Area 0 قرار دارد را تبلیغ کرده است .

محدود کردن تعداد LSA ها :

به صورت پیش فرض روترهای سیسکو اقدام به محدود کردن تعداد LSAها دریافتی خود نمی کنند . اما با این وجود می توان به منظور جلوگیری از اشغال بیش از حد حافظه روتر اقدام به انجام این کار نمود . در صورتی که اطلاعات نگهداری شده در داخل جدول LSDB زیادتر از حد نرمال باشد احتمالا روترهای ضعیف تر توانایی پردازش این حجم بزرگ اطلاعات را نداشته و سرعت همگرایی شبکه کاهش خواهد یافت .

با استفاده از دستور زیر که در محیط پیکربندی OSPF نوشته می شود میتوان حداکثر تعداد LSAهایی که یک روتر می تواند دریافت کند را مشخص کرد :



نکته :

OSPF اینترفیس های Loopback را به عنوان یک Host در نظر می گیرد و مقدار ماسک آنها را برابر با 32/ در نظر می گیرد . باید Network type اینترفیس های Loopback را به حالت Point – to – Point تغییر دهیم تا ماسک آنها را برابر با 24/ تغییر دهد و مقدار Cost آنها 1 است .

Metric

محاسبه Metric برای تعیین بهترین مسیر برای هر مقصد در پروتکل OSPF بر اساس پهنای باند لینک محاسبه می شود که از طریق فرمول زیر محاسبه خواهد شد :

Cost = 1000 / (Interface Bandwidth) ⟶ Cost = 10^8/B.W

Default Costs in OSPF :

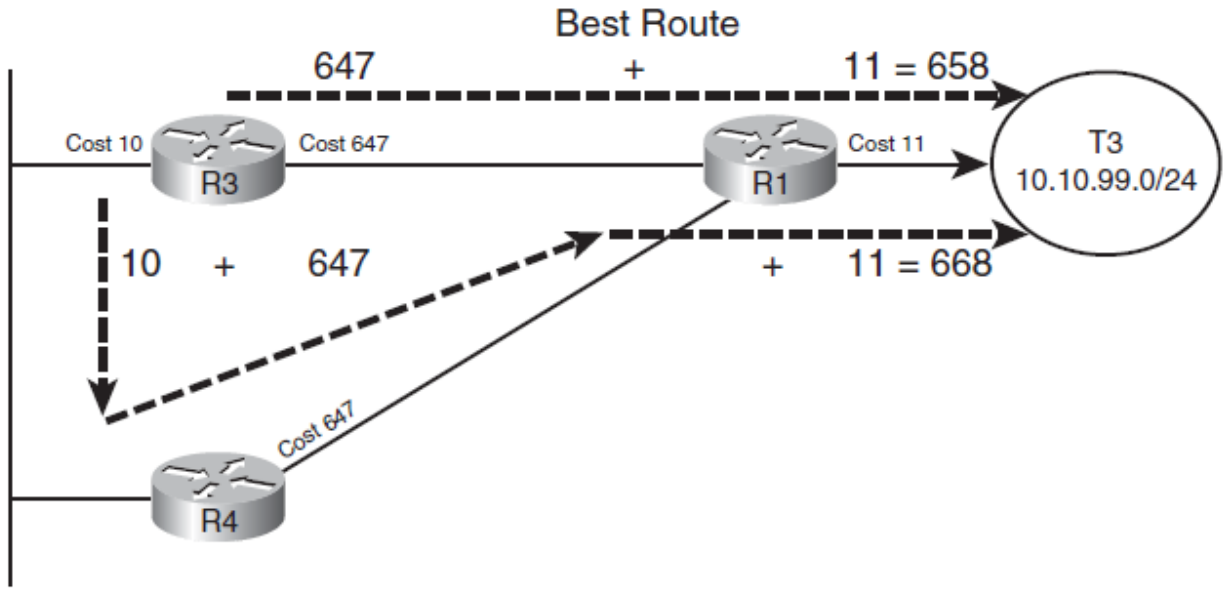
نوع اینترفیس	پهنای باند اینترفیس	OSPF Metric
10 Ethernet	10 Mbps	10
100 Fast Ethernet	100 Mbps	1
1 Gigabit Ethernet	1000 Mbps	1
T1	1.544 Mbps	64
E1	2.048 Mbps	48

نکته : اگر توجه داشته باشید ارزش لینک یا همان Link Cost به صورت پیش فرض در لینک یا اتصال Fast Ethernet و Gigabit Ethernet برابر می باشد . پروتکل OSPF ارزش این دو اتصال را یکسان فرض خواهد کرد که شما می توانید رفتار OSPF را برای محاسبه Metric لینک ها تغییر دهید . برای این منظور از دستور زیر استفاده می کنید :

Router (config – router) # Auto – cost Reference – Bandwidth 1000

با وارد کردن دستور صفحه قبل OSPF متریک اتصالات Fast Ethernet و Gigabit Ethernet را یکسان فرض نخواهد کرد و حال اتصالات Gigabit Ethernet دارای ارزش 1 و اتصالات Fast Ethernet دارای ارزش 10 و اتصالات Ethernet دارای ارزش 100 خواهند بود .

به شکل زیر توجه کنید :



R3's Calculation of Cost for 10.10.99.0/24

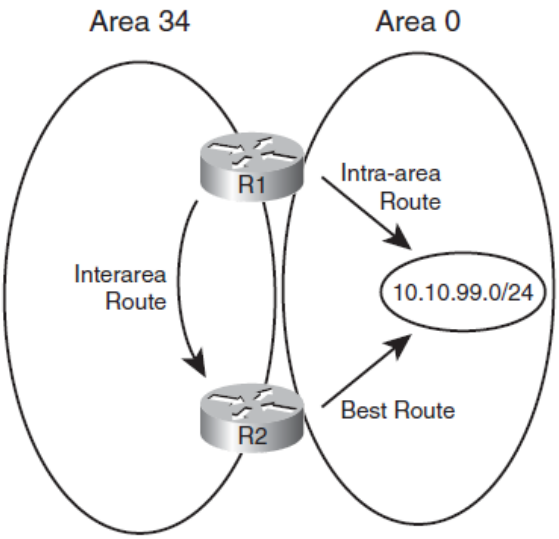
همانطور که مشاهده میکنید روتر R3 برای رسیدن به شبکه 10.10.99.0/24 دو مسیر با مقدار Cost متفاوت را در جدول توپولوژی خود دارد با محاسبه Cost هر دو مسیر روتر R3 مسیر R3 : R1 : T3 که Cost کمتری نسبت به مسیر R3 : R4 : T3 دارد را به عنوان بهترین مسیر انتخاب می کند و در جدول مسیریابی خود قرار می دهد.

با دستور زیر می توانیم مقدار Cost اینترفیس های فعال در پروسه OSPF را تغییر دهیم :

Router (config – if) # IP OSPF Cost value

در این دستور می بایست به جای متغیر value مقدار دقیق cost را تایپ کرد .

به شکل زیر توجه کنید :



R1's Choice: Intra-Area or Interarea Route to 10.10.99.0/24

با نگاه کردن به شکل بالا میبینید که دو مسیر مختلف از روتر R1 برای رسیدن به شبکه 10.10.99.0/24 وجود دارد.برای نمونه روتر R1 میتواند برای دسترسی به 10.10.99.0/24 در ابتدا از طریق مسیرهای موجود در داخل Area 34 به روتر ABR دیگر (یعنی R2) متصل شده و سپس با گذشتن از Area 0 به شبکه 10.10.99.0/24 برسد. اما قوانین OSPF از انتخاب چنین مسیرهایی جلوگیری می کند .

این قوانین عبارتنداز :

- با صرفنظر از Metric مربوط به هر مسیر , مسیرهای Intra – area دارای اولویت بیشتری نسبت به مسیرهای Interarea می باشد .
- زمانی که روتر ABR یک پیام LSA type 3 را در داخل LSDB مربوط به یک nonbackbone Area مشاهده نماید در بررسی مسیرها از آن چشم پوشی می کند .

بر اساس قانون اول روترهای ABR در هنگام حضور مسیرهای intra – area از به کارگیری مسیرهای interarea خودداری میکنند .همچنین قانون دوم نیز بیانگر آن است که روتر R1 هیچگاه برای دسترسی به 10.10.99.0/24 از مسیرهای interarea بهره نخواهد گرفت . این کار بدین دلیل انجام می گیرد که روتر R1 باید با استفاده از اطلاعات مربوط به خود قادر به شناسایی مسیرهای مناسب باشد و نه با بهره گیری از اطلاعات رسیده از Areaهای دیگر .

Route Filtering

در پروتکل OSPF فقط بر روی روترهای مرزی یعنی ABR و ASBR عمل Filtering انجام می گیرد . Filtering در OSPF به دو روش صورت می گیرد .

روش اول :

فیلتر کردن پیام های LSA type 3

روترهای ABR به عنوان یکی از وظایف خود اقدام به ایجاد و انتشار پیام های LSA type 3 به داخل یک Area کرده و شبکه های موجود در داخل یک Area دیگر را به اطلاع این Area می رسانند . در عملیات فیلترکردن از انتشار LSA type 3های مورد نظر توسط روتر ABR جلوگیری خواهیم کرد .

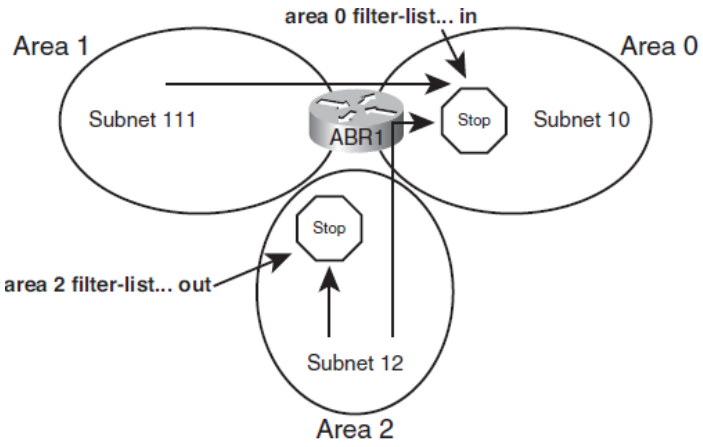
دستور فیلتر کردن بر روی روتر ABR :

Router (config – router)# Area number Filter – list Prefix name { in | out }

دستور فوق به یک Prefix – list احتیاج دارد که در صورت دارا بودن پارامتر deny پیام فیلتر شده و در صورت استفاده از پارامتر Permit نیز پیام اجازه انتشار خواهد یافت .

یکی از مهمترین پارامترها ، تعیین in یا out در انتهای دستور فوق است . این پارامترها جهت انتقال پیام را در مورد آن Area که در دستور مشخص شده است بیان می کنند . بدین صورت که :

- زمانی که پارامتر in مورد استفاده قرار می گیرد روتر اقدام به بررسی و فیلتر کردن پیام های ورودی به Area مشخص شده در دستور خواهد کرد .
- در صورتی که پارامتر out مورد استفاده قرار گیرد روتر اقدام به بررسی و فیلتر کردن پیام های خروجی از Area مشخص شده در دستور خواهد کرد .



Generic View of Type 3 LSA Filtering

با توجه به شکل بالا دستور Area 0 Filter – list ... in باعث خواهد شد تا روتر ABR1 تمامی پیام های LSA type 3 حاوی شبکه های موجود در Area 1 و Area 2 را در هنگام ورود به Area 0 بررسی و برای انجام فیلتر کردن مد نظر قرار دهد. همچنین دستور Area 0 Filter – list ... out در این شکل بر روی شبکه های موجود در داخل Area 2 تمرکز دارد . بدین ترتیب که روتر ABR1 اقدام به بررسی پیام های LSA type 3 که از Area 2 خارج می شود می کند و اقدام به فیلتر کردن آنها می کند .

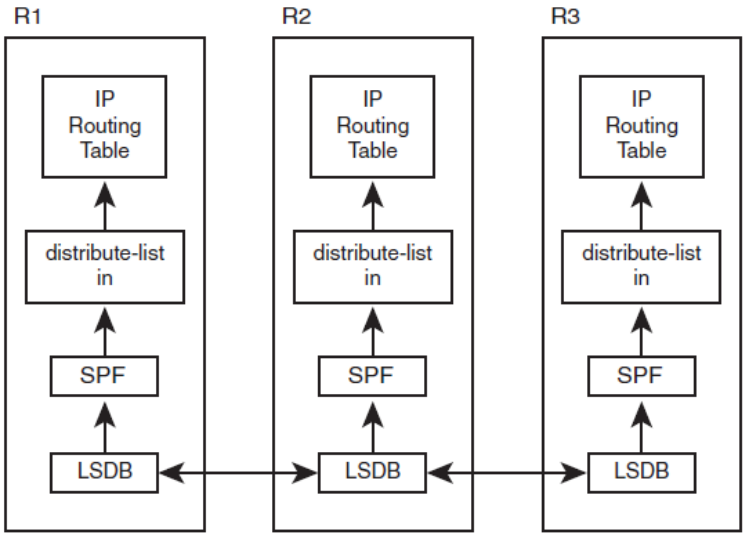
روش دوم : جلوگیری از قرارگیری برخی از Routeها در داخل جدول Routing با استفاده از Distribute – list

با استفاده از این روش می توان هر کدام از روترها را مجبور کرد تا از قرار دادن OSPF Routeهای خاص در داخل جدول Routing خودداری کنند . ویژگی های بهره گیری از این روش عبارتنداز :

- این روش تاثیری بر پروسه انتشار اطلاعات LSDB ندارد .
- این روش باعث بروز هیچ تغییری در LSAهای ارسالی از روترهای ABR و ASBR نمی گردد .
- پروسه انتخاب بهترین مسیرهای منتهی به مقاصد مختلف توسط الگوریتم SPF نیز تحت تاثیر قرار نخواهد گرفت .

زمانی که یک روتر OSPF قصد افزودن یک مسیر به داخل جدول Routing را داشته باشد و ما نیز اقدام به اجرای دستور Distribute – list in در داخل محیط پیکربندی OSPF نموده باشیم این روتر از قرار دادن شبکه مورد نظر در داخل جدول Routing خودداری خواهد کرد .

شکل زیر بیانگر این ایده است :



OSPF Filtering with Distribute Lists

نکته : با اجرای دستور Distribute – list مسیرها از جدول Routing فیلتر می شوند ولی در جدول Topology قرار دارند .

دستور فیلتر کردن با Distribute – list :

با Access – List :

Router (config – router)# Distribute – list { ACL – Name | ACL – Num } in

با Prefix – List :

Router (config – router)# Distribute – list Prefix Prefix – name in

با Route – Map :

Router (config – router)# Distribute – list Route – Map name in

نکته : در دستور فوق تنها امکان استفاده از پارامتر in وجود دارد .

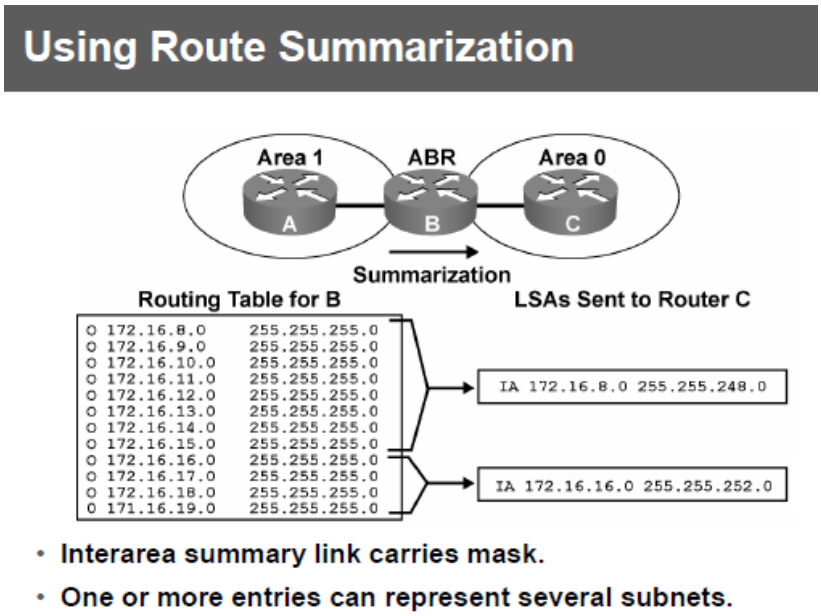
شبکه های منطبق با دستور Permit قادر به قرارگیری در داخل جدول Routing بوده ولی شبکه های منطبق با دستور Deny در جدول Routing ثبت نمی شوند .

در انتهای دستور می توان اقدام به مشخص نمودن یک اینترفیس کرد که در این شرایط این پارامترها در مورد اینترفیس مشخص شده بررسی و اعمال خواهد شد .

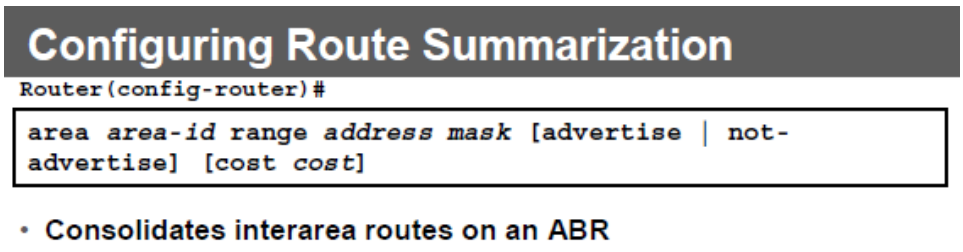
Summarization in OSPF

پروتکل OSPF امکان انجام Summarization را تنها بر روی روترهای ABR و ASBR فراهم می سازد . زیرا تمامی روترهای داخل یک Area باید از محتویات LSDB یکسانی برخوردار باشند .

انجام Summarization بر روی روتر ABR :



دستور Summarization بر روی روتر ASBR :



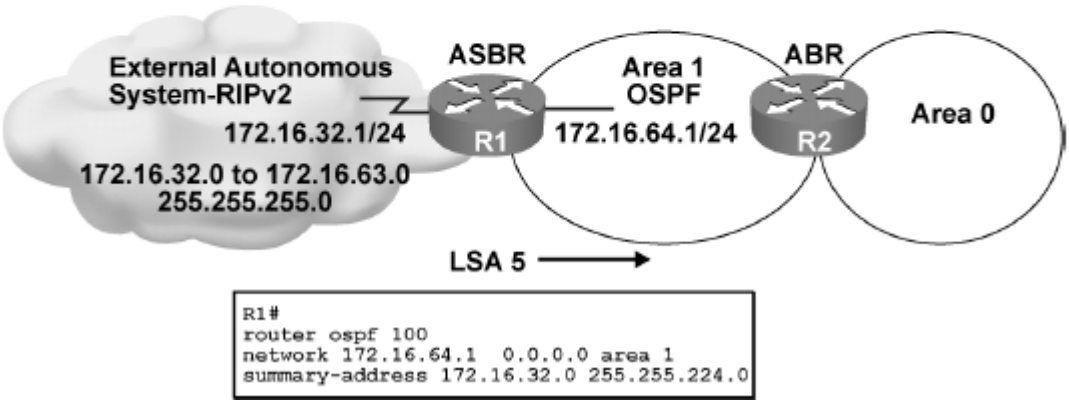
Area-id : اشاره به شماره آن Area دارد که IPهایی را که می خواهیم Summary کنیم در آن Area قرار دارند.

Cost : با مقداردهی به cost می توانیم مقدار cost همه IPهایی را که Summary می کنیم را تعیین کنیم .

[Advertise | Not – Advertise] :پیش فرض در حالت Advertise قرار دارد. اگر حالت Not – Advertise را وارد کنیم یعنی این Range آدرس IP یا شبکه را نفرست تقریبا حالت فیلترکردن دارد .

انجام Summarization بر روی روتر ASBR :

Route Summarization Configuration Example at ASBR




```
R1#
router ospf 100
network 172.16.64.1  0.0.0.0 area 1
summary-address 172.16.32.0 255.255.224.0
```

دستور Summarization بر روی روتر ASBR :

Configuring Route Summarization

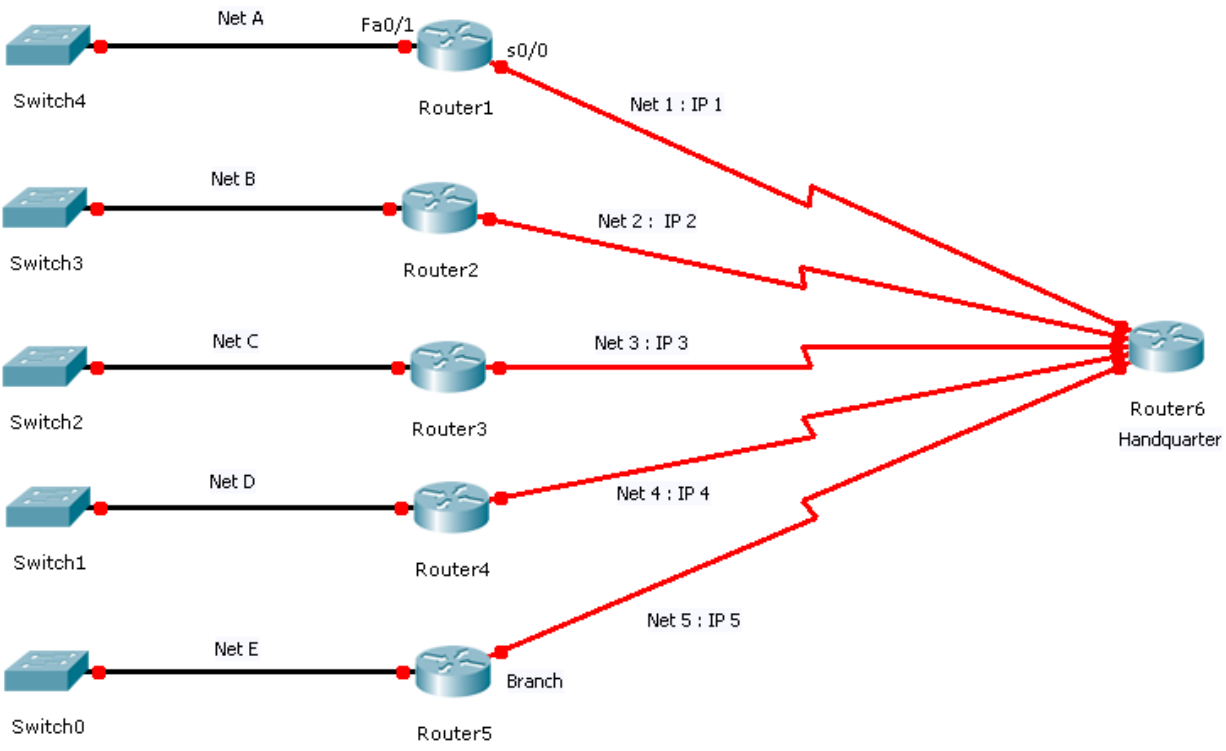
```
Router(config-router)#
summary-address ip-address mask  [not-advertise]
```

- Consolidates external routes, usually on an ASBR

Default – Route

سازمان ها در دو موقعیت زیر از Default – Route استفاده می کنند :

کاربرد اول Default – Route :



با توجه به شکل بالا اگر به جدول Routing روتر R1 نگاه کنیم به صورت زیر می باشد :

R1	outgoing interface	Next – Hop
C Net A	Fa0/1	Connected
C Net 1	s0/0	Connected
C Net 2	s0/0	IP 1
C Net 3	s0/0	IP 1
C Net 4	s0/0	IP 1
C Net 5	s0/0	IP 1
C Net B	s0/0	IP 1
C Net C	s0/0	IP 1
C Net D	s0/0	IP 1
C Net E	s0/0	IP 1

همانطور که مشاهده می کنید اگر بخواهیم از Net A به هر کدام از شبکه های دیگر دسترسی پیدا کنیم باید از اینترفیس s0/0 روتر R1 خارج شود و به شبکه مورد نظر برسد .

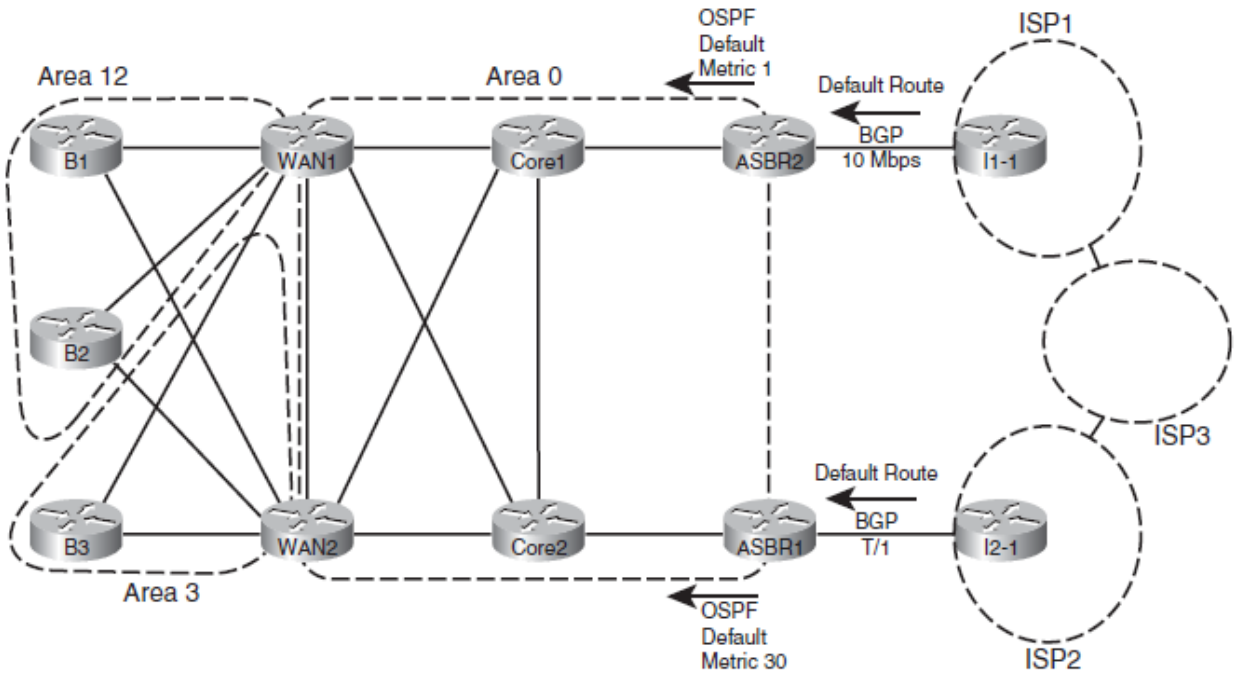
پس با تعیین یک مسیر یا همان Default – Route بر روی روتر R1 به جای آن همه مسیر که مشخص کرده ایم با یک مسیر Default – Route خلاصه می کنیم .

با دستور زیر این کار را انجام می دهیم :

```
Router ( config – router ) # Default – Route   0.0.0.0   0.0.0.0   s0/0
```

این دستور را بر روی تمام روترهای دیگر شبکه وارد می کنیم تا حجم جدول Routing همه روترها کاهش یابد .

کاربرد دوم Default – Route :



Dual-Homed Internet Design Using Default Routes

برای اینکه اگر در شبکه روترها برای رسیدن به شبکه ای مسیری را پیدا نکنند به روترهای ASBR تحویل دهند تا از طریق آنها به اینترنت دسترسی پیدا کنند .

دستور تزریق Default – Route به داخل Area :

Configuring OSPF Default Routes

```
Router(config-router)#
default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]
```

- Normally, this command advertises a 0.0.0.0 default into the OSPF network only if the default route already exists in the routing table.
- The always keyword allows the 0.0.0.0 default to be advertised even when the default route does not exist in the routing table.

نکته :

اگر پارامتر always را در دستور فوق استفاده کنیم حتی اگر روتر ASBR دارای یک Default – Route در داخل جدول Routing خود نباشد نیز اقدام به انتشار Default – Route در بین روترهای داخلی خواهد کرد .

مقدار پیش فرض Metric در دستور بالا برابر با 1 است .

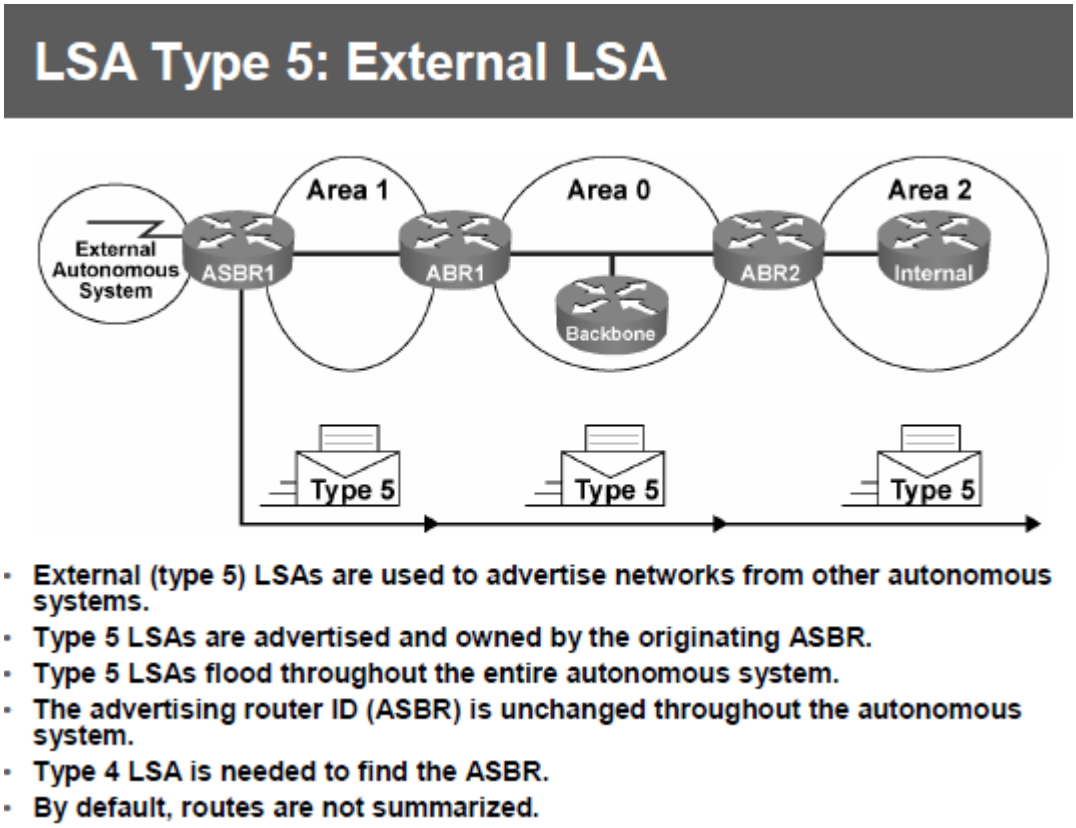
مقدار پیش فرض Metric – type در دستور بالا برابر با external type 2 است .

E2 : اگر مقدار Metric – type برابر با external type 2 باشد در کل شبکه Metric مسیر وارد شده ثابت باقی می ماند و تغییر نمی کند .

E1 : اگر مقدار Metric – type برابر با external type 1 باشد در شبکه Metric مسیر وارد شده تغییر می کند و از روتری به روتر دیگر افزایش می یابد .

اگر قسمت Route – map را در دستور بالا بنویسیم یعنی تا زمانی که اینترفیسی که به اینترنت وصل است و قطع نیست Default – Route را بفرست اگر قطع شد دیگر Default – Route را نفرست .

LSA Type 5 : External LSA



این پیام را فقط روترهای ASBR ارسال می کنند و روترهای ABR زمانی که در شبکه روترهای ASBR نیز موجود باشند این پیام ها را ارسال می کنند .

اطلاعاتی که در پیام های type 5 LSA وجود دارد و ارسال می شود :

ASBR
- ASBR (ABR)
- Subnet number / Subnet mask
- Metric – type
- Metric

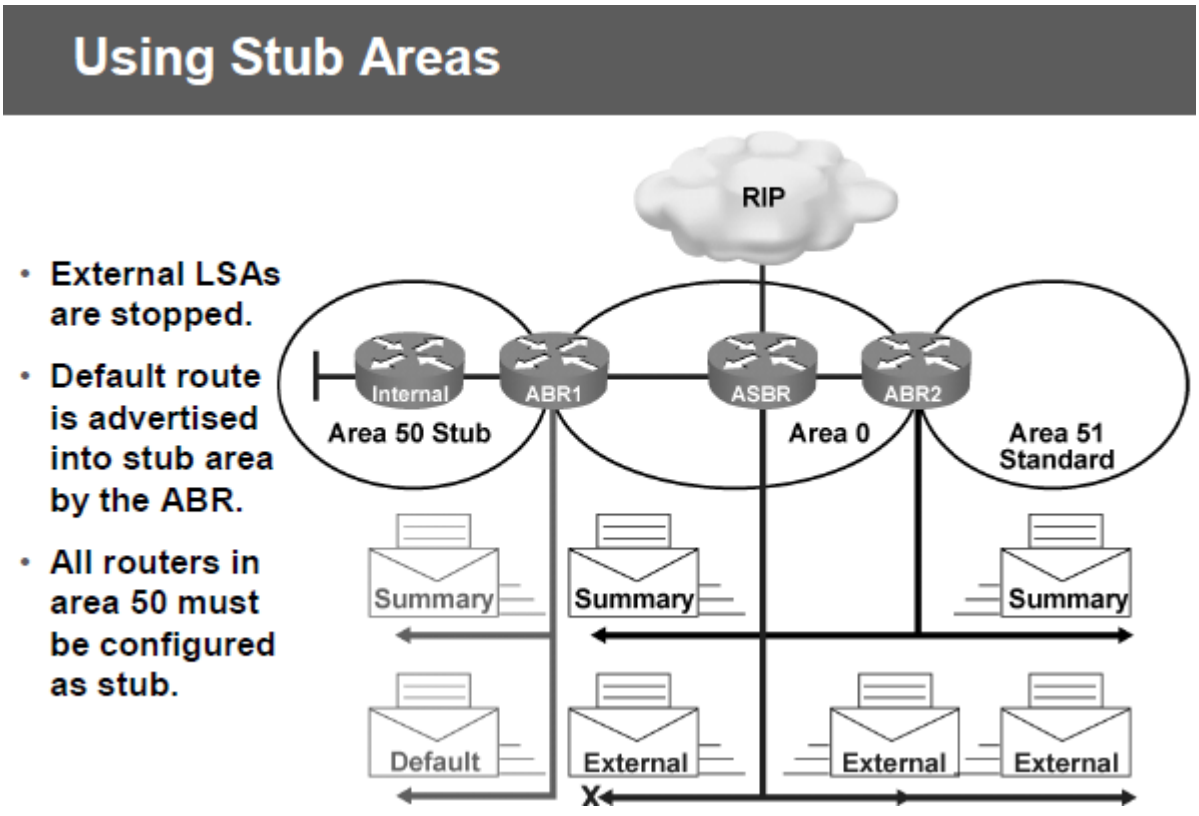
برای مشاهده پیام های type 5 LSA از دستور زیر استفاده می کنیم :

Router # Show IP OSPF Database External subnet – number

Stub Area

به صورت کلی می توان خصوصیات اصلی Stub Area را به صورت زیر بیان کرد :

- در صورت قرار دادن یک Area به عنوان Stub روتر ABR اقدام به ایجاد یک پیام LSA type 3 حاوی شبکه 0.0.0.0 و ماسک 0.0.0.0 کرده و این پیام را برای اعضای Area ارسال می کند.
- روترهای ABR از هدایت LSA type 5 به داخل Stub Area خودداری می کنند.
- به غیر از یک پیام LSA type 3 که آن هم حاوی Default route است هیچ کدام از پیام های LSA type 3 دیگر توسط روتر ABR به داخل Stub Area ارسال نخواهد شد.
- تمامی روترهای واقع در یک Area را باید به عنوان یک روتر Stub تعیین کرد . در غیر این صورت برقراری رابطه مجاورت مابین روترهای داخل همان Area با اختلال مواجه می شود .



دستور Stub Area :

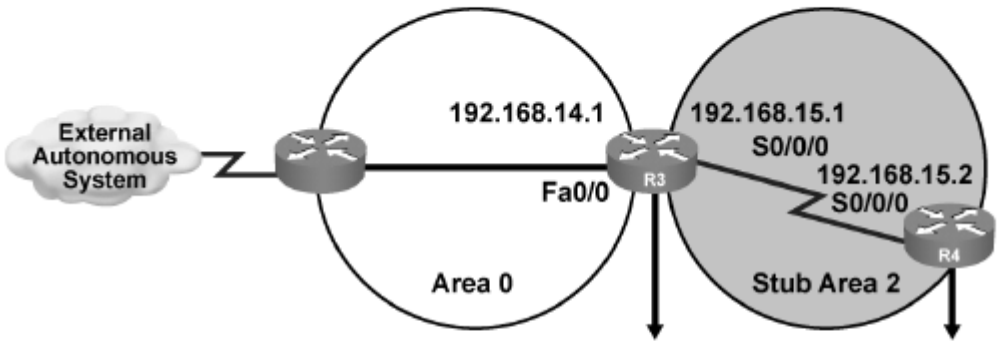
Stub Area Configuration

```
RouterA(config-router)#
area area-id stub
```

- This command turns on stub area networking.
- All routers in a stub area must use the stub command.

مثال Stub Area :

OSPF Stub Area Configuration Example




```
R3#

interface FastEthernet 0/0
ip address 192.168.14.1 255.255.255.0
interface Serial 0/0/0
ip address 192.168.15.1 255.255.255.252

router ospf 100
network 192.168.14.0 0.0.0.255 area 0
network 192.168.15.0 0.0.0.255 area 2
area 2 stub
```

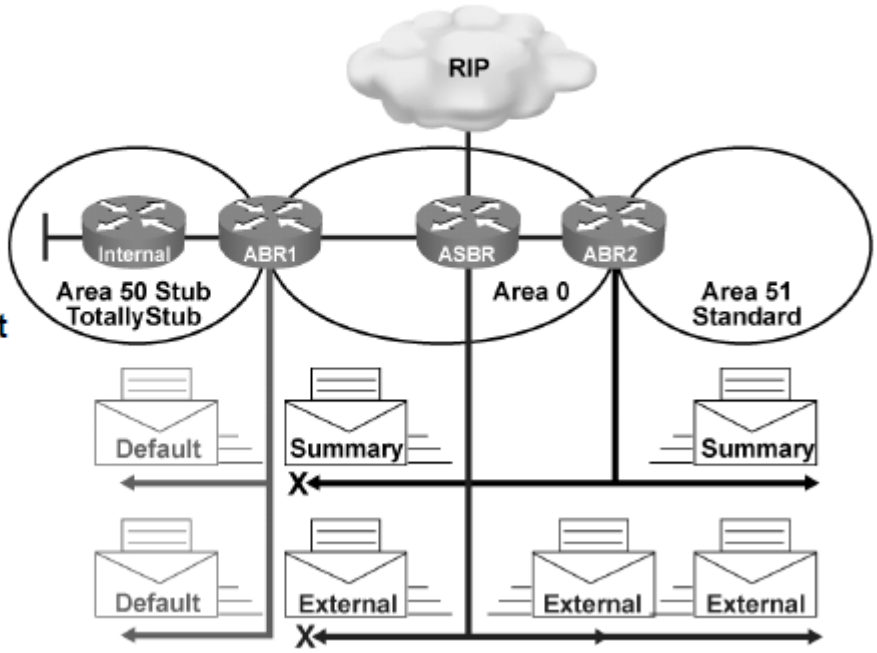
```
R4#

interface Serial 0/0/0
ip address 192.168.15.2 255.255.255.252

router ospf 15
network 192.168.15.0 0.0.0.255 area 2
area 2 stub
```

: Totally Stubby Area

به نوعی از Areaها که روتر ABR از ایجاد و ارسال پیام های LSA type 3 و LSA type 5 به داخل Area خودداری می نماید Totally Stubby Area می گویند .

Using Totally Stubby Areas

- External LSAs are stopped.
- Summary LSAs are stopped.
- Routing table is reduced to a minimum.
- All routers must be configured as stub.
- ABR must be configured as totally stubby.
- This is a Cisco proprietary feature.



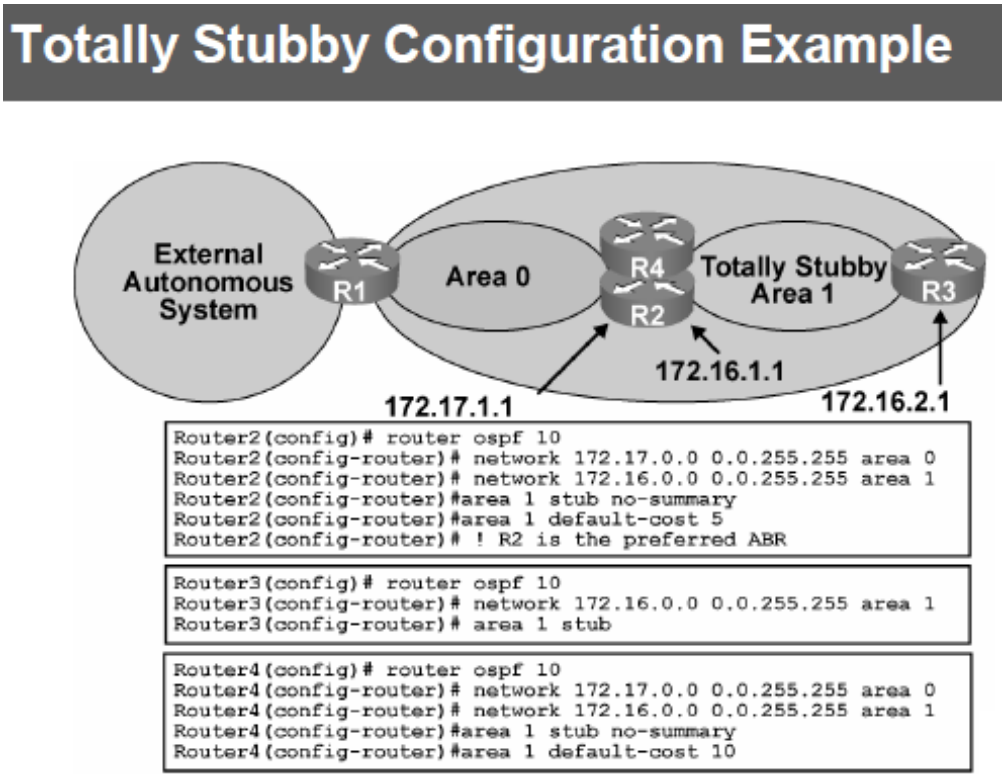
دستور Totally Stubby Area :

Totally Stubby Configuration

```
RouterA(config-router)#
area area-id stub no-summary
```

- The addition of no-summary on the ABR creates a totally stubby area and prevents all summary LSAs from entering the stub area.

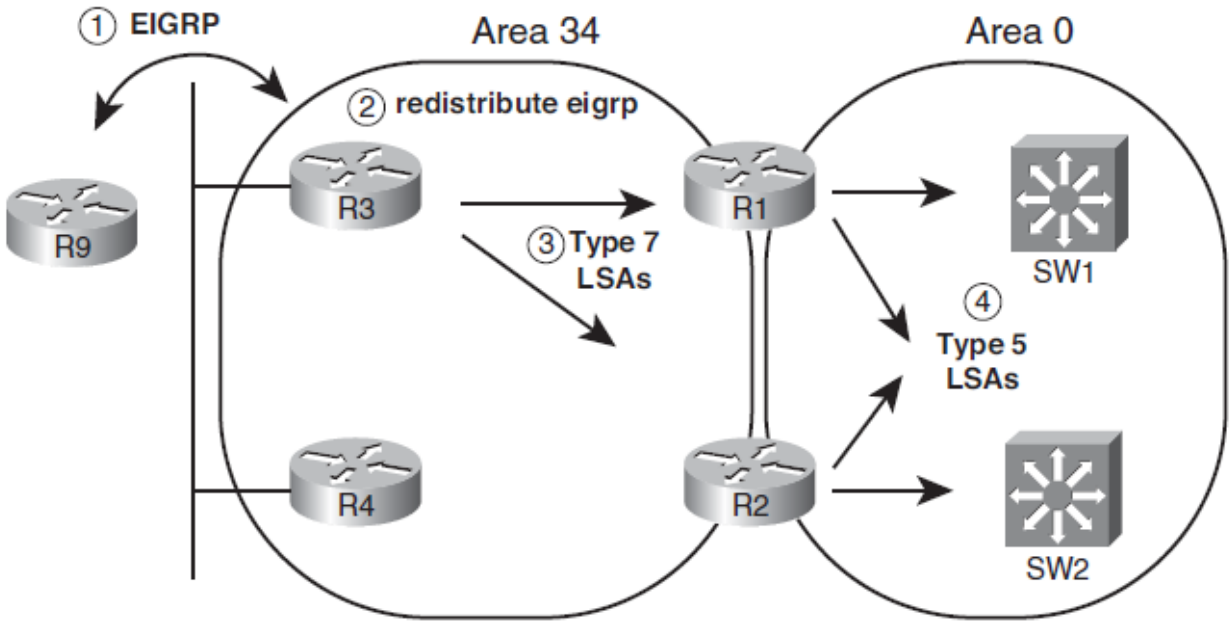
مثال Totally Stubby Area :



: Not – So – Stubby – Area

در صورت پیکربندی یک Area به عنوان Stub یا Totally Stub پیام های External یا همان LSA type 5 قادر به ورود به داخل این Area نخواهد بود که این کار در برخی شرایط باعث بروز مشکلاتی می گردد. به عبارت دیگر یک stub area یا totally stub area نمی توانند شامل یک روتر ASBR که آنها را به دنیای خارج از OSPF Domain متصل می سازد باشد .در این جا از NSSA استفاده می کنیم . بنا به قانون به دلیل آنکه external routeها را نمی توان از طریق پیام های LSA type 5 به داخل Stub area یا totally stub area منتشر کرد بنابراین به جای آن می توان از پیام های LSA type 7 برای ارسال به داخل این Areaها استفاده کرد . کاربرد پیام های LSA type 7 دقیقا شبیه به LSA type 5 بوده اما روترهای ASBR این پیام ها را تنها به سمت اعضای یک NSSA area ارسال می کنند .

برای درک بیشتر به شکل زیر دقت کنید در این مثال Area 34 به عنوان NSSA قرار داده شده است :



External Routes in an NSSA Area (34)

مراحل نشان داده شده در شکل به صورت زیر است :

1. روتر R3 به عنوان ASBR بوده و از طرفی دیگر به EIGRP Domain و روتر R9 متصل است . بنابراین این روتر هم از محتویات OSPF Domain و هم EIGRP Domain آگاه است .
2. مدیر شبکه با استفاده از دستور Redistribute اقدام به انتشار EIGRP routeها به داخل OSPF می نماید .
3. روتر R3 به عنوان ASBR می باشد پیام های LSA type 7 حاوی شبکه های EIGRP را به تمامی اعضای Area 34 ارسال می کند .
4. روترهای ABR (شامل R1 , R2) این پیام را دریافت کرده و سپس اقدام به ایجاد یک پیام LSA type 5 به ازای هر یک از شبکه های موجود در داخل LSA type 7 می کنند . در نهایت این پیام به سمت Areaهای دیگر (Area 0) فرستاده می شود .

بر روی تمام روترهای داخل Area دستور NSSA را وارد می کنیم :

NSSA Configuration

```
RouterA(config-router)#
area area-id nssa [no-redistribution] [default-
information-originate [metric metric-value] [metric-
type type-value]] [no-summary]
```

- **Use this command instead of the** area stub **command to define the area as NSSA.**
- **The** no-summary **keyword creates an NSSA totally stubby area; this is a Cisco proprietary feature.**

بر روی روتر مرزی ABR این دستور را وارد می کنیم :

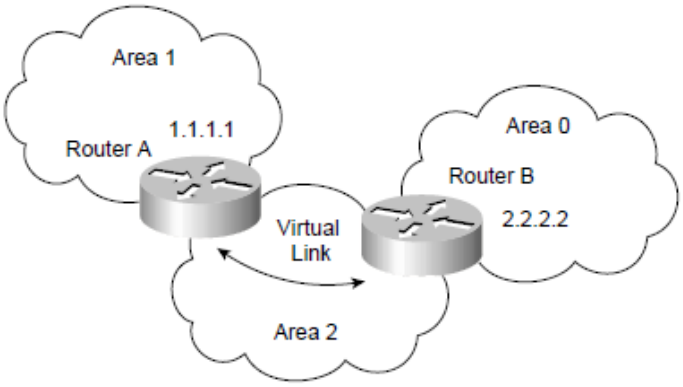
Router (config – router) # nssa no summary

با این دستور پیام های LSA type 3 نیز در جدول Routing حذف می شوند .

نکته :

این مسیرها در جدول Routing با علامت N2 نمایش داده می شوند .

Virtual Links



با این روش یک لینک مجازی در بین دو روتر مرزی ABR ایجاد می کنیم تا در بین این دو روتر رابطه مجاورت تشکیل شود و بتوانند از طریق این لینک مجازی پیام های Hello و LSAها را به یکدیگر ارسال کنند .

دستور Virtual Link را بر روی هر دو روتر وارد می کنیم :

Configuring Virtual Links

```
Router(config-router)#
area area-id virtual-link router-id [authentication
[message-digest | null]] [hello-interval seconds]
[retransmit-interval seconds] [transmit-delay
seconds] [dead-interval seconds] [[authentication-
key key] | [message-digest-key key-id md5 key]]
```

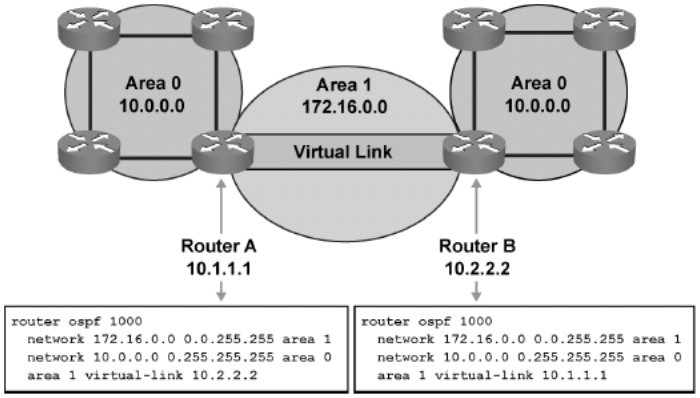
نکته :

شماره Area اشاره به شماره Area حامل دارد که Virtual Link در روی آن ایجاد خواهد شد .

در جدول Database در جلوی مسیرهایی که از Virtual Link گرفته شده اند DNA نوشته شده است .

مثال : می خواهیم در بین دو روتر Router A و Router B یک لینک مجازی یا Virtual Link راه اندازی کنیم طبق شکل صفحه بعد دستورات را بر روی هر دو روتر اعمال می کنیم :

OSPF Virtual Link Configuration Example



همانطور که مشاهده می کنید بر روی روتر های ABR این دستورات اعمال شده است و شماره Area در دستور Virtual Link همان شماره Areaایی است که Transit روی آن صورت می گیرد که در این مثال Area 1 می باشد .

بررسی صحت پیکربندی Virtual Link در مثال صفحه قبل :

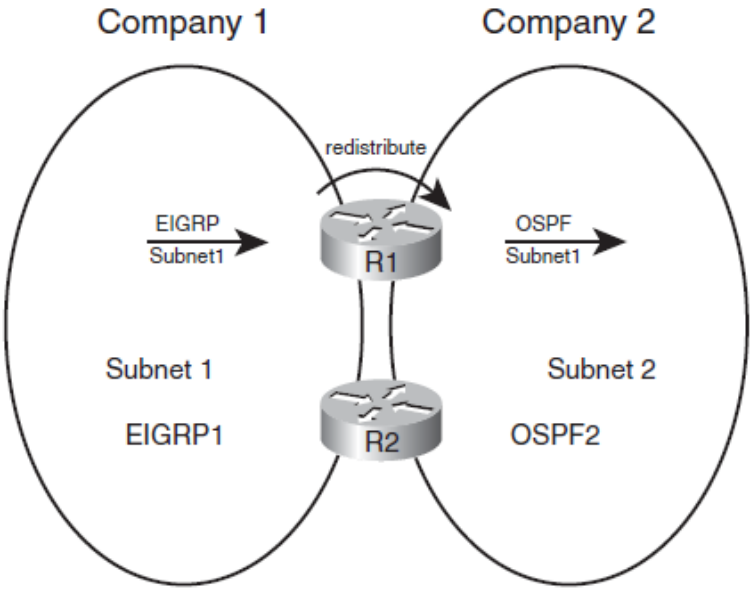
The show ip ospf virtual-links Command

```
RouterA#sh ip ospf virtual-links
Virtual Link OSPF_VL0 to router 10.2.2.2 is up
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 1, via interface Serial0/0/1, Cost of using 781
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
    Adjacency State FULL (Hello suppressed)
    Index 1/2, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
RouterA#
```

این دستور را بر روی روتر A وارد می کنیم و می بینیم که با روتری که RID آن برابر با 10.2.2.2 است Virtual Link را تشکیل داده است . Area 1 به عنوان transit انتخاب شده است . شبکه در حالت Point – to – Point قرار دارد .مقدار Hello برابر با 10 ثانیه و مقدار Dead برابر با 40 ثانیه است .

Adgacency در بین دو روتر همسایه در حالت Full قرار دارد .

Redistribution



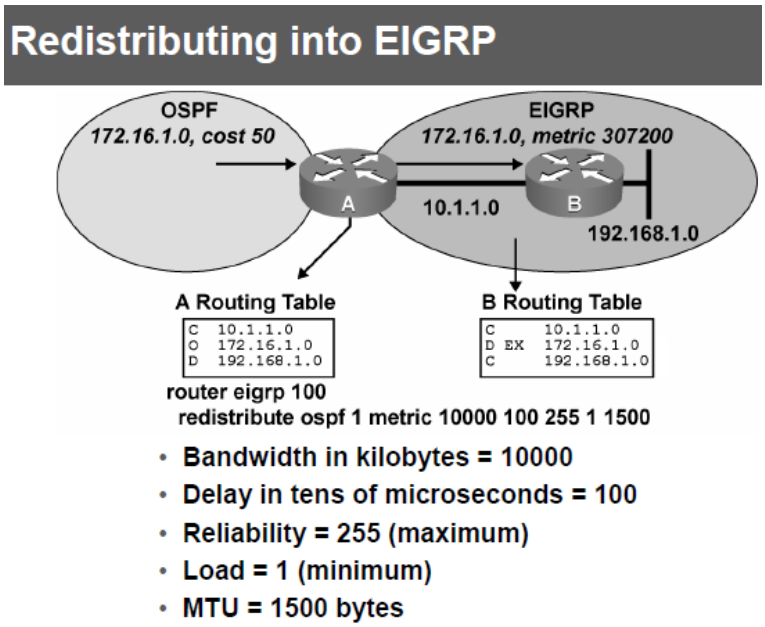
Typical Use of Redistribution

در برخی محیط ها از چندین پروتکل مسیریابی استفاده خواهد شد . فرض کنید که در یک قسمت از شبکه از یک پروتکل و در قسمت های دیگر از یک پروتکل دیگری استفاده خواهد شد که در این حالت شما نیاز به استفاده از توانمندی به نام Route Redistribution خواهید داشت .

Route Redistribution توانمندی می باشد که امکان انتشار اطلاعات مسیریابی یک پروتکل در داخل پروتکل دیگر را در اختیار شما قرار خواهد داد .

شکل بالا نشان می دهد که در آن روترهای R1 و R2 در مرز بین دو Domain قرار دارند . در این مثال روتر R1 اطلاعات مربوط به Subnet 1 را که در داخل EIGRP Domain قرار دارد به داخل شبکه OSPF انتقال می دهد . البته این کار می تواند در جهت عکس نیز انجام گیرد . بدین ترتیب که اطلاعات مربوط به Subnet 2 که در داخل شبکه OSPF قرار دارد به داخل شبکه EIGRP ارسال خواهد شد .

اعمال توانمندی Route Redistribution از پروتکل OSPF به داخل پروتکل EIGRP :



دستور Route Redistribution از پروتکل های مختلف به داخل پروتکل EIGRP :

Router(config–router) #Redistribute Protocol [As–num | Process–id] [Metric B.W Delay Reliability Load MTU] [Match { Internal | External 1 | External 2 | NSSA – External }] [Route – Map Map – name] [Tag Tag – Value]

Protocol : در این قسمت باید پروتکل مسیریابی که قصد انتشار اطلاعات مربوط به آن را در پروتکل EIGRP خواهید داشت را تعیین نمایید در این قسمت می توان از پروتکل های BGP , Connected , RIP , OSPF , Static , ISIS استفاده نمایید .

Process – id : از این مقدار در پروتکلی مانند OSPF که دارای Process – id میباشد استفاده میشود.

Metric : با استفاده از این پارامتر در داخل دستور Redistribute می توانید متریک پیش فرض مربوط به مسیرها بعد از انتشار به داخل EIGRP را تعیین نمایید .

Match : با استفاده از این پارامتر می توان نوع پیام هایی که باید انتخاب شده و به داخل EIGRP منتشر شوند را مشخص کرد .

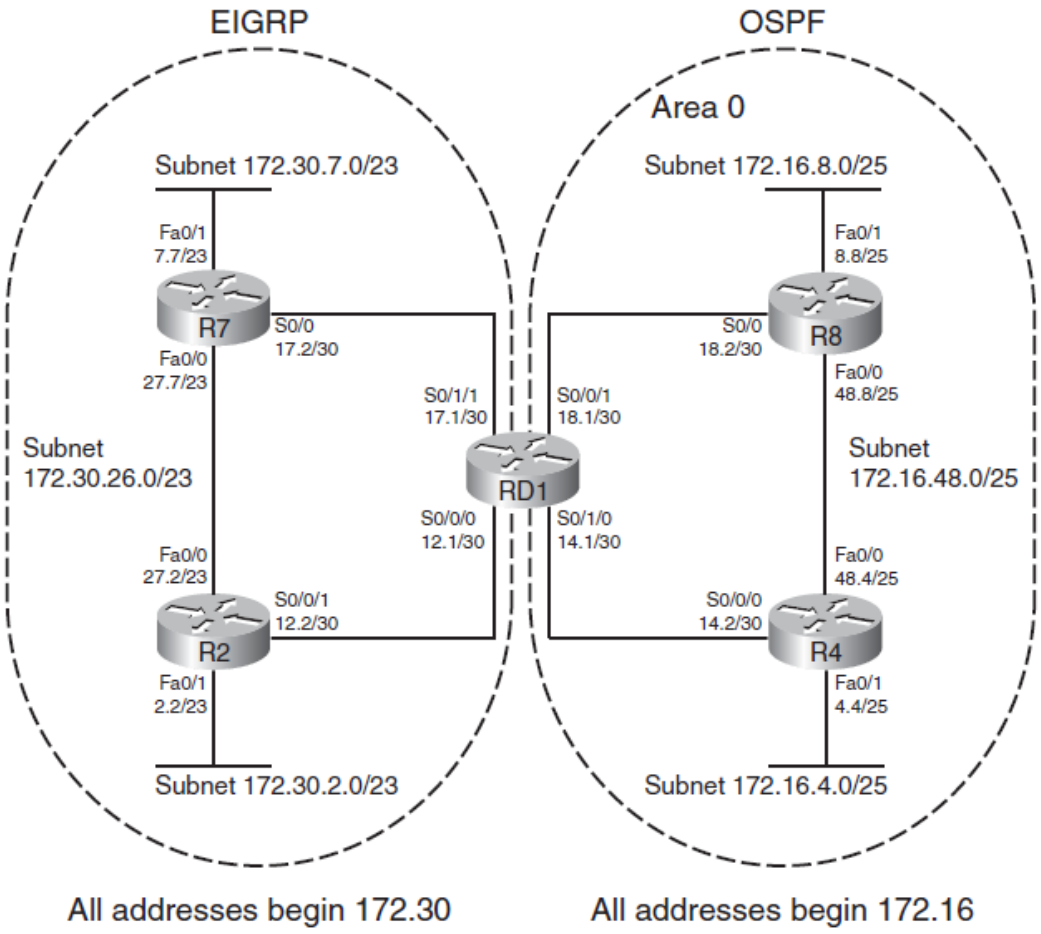
برای نمونه در صورت نوشتن دستور Match internal تمامی OSPF internal routeهایی که در داخل جدول Routing این روتر قرار دارد به داخل EIGRP منتشر می شوند . لازم به یادآوری است که OSPF internal routeها با علامت O یا O IA در جدول Routing نشان داده می شوند .

Tag : با استفاده از این دستور می توان یک Tag مخصوص بر روی Routeهای منتشر شده اختصاص داد. از این Tag می توان در Route – Mapها استفاده کرد .

Route – Map : از این دستور می توان برای اعمال فیلتر و تعیین مقدار متریک و موارد دیگر استفاده کرد .

نکته : تعیین Default Metric در انتشار اطلاعات مسیریابی پروتکل های دیگر به داخل EIGRP اجباری می باشد . در صورتی که تعیین نشود اطلاعات مسیریابی به داخل حوزه EIGRP منتشر نمی شود .

مثال :



با توجه به شکل صفحه قبل می خواهیم شبکه هایی که در داخل OSPF Domain قرار دارند را به داخل EIGRP Domain با استفاده از توانمندی Redistribute منتشر کنیم .

روش اول :

```
RD 1 (config) #Router EIGRP  1
RD 1 (config–router) #Redistribute  OSPF  1
RD 1 (config–router) #Default – Metric  1000  10  255  1  1500
```

روش دوم :

```
RD 1 (config) #Router EIGRP  1
RD 1 (config–router) #Redistribute  OSPF  1  Metric  1200  100  255  1  1500
```

روش سوم :

```
RD 1 (config) # IP  Prefix – List  1  seq  5  Permit  172.16.8.0/25
RD 1 (config) # IP  Prefix – List  2  seq  5  Permit  172.16.48.0/25
RD 1 (config) # IP  Prefix – List  3  seq  5  Permit  172.16.4.0/25
RD 1 (config) # IP  Prefix – List  4  seq  5  Permit  172.16.14.0/30
RD 1 (config) # IP  Prefix – List  5  seq  5  Permit  172.16.18.0/30

RD 1 (config) # Route – Map  Cisco  Permit  10
RD 1 (config – route – map) # Match  IP  Address  Prefix – list  1
RD 1 (config – route – map) # Set  Metric  1000  10  255  1  1500
RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map  Cisco  Permit  20
RD 1 (config – route – map) # Match  IP  Address  Prefix – list  2
RD 1 (config – route – map) # Set  Metric  1200  100  255  1  1500
RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map  Cisco  Permit  30
RD 1 (config – route – map) # Match  IP  Address  Prefix – list  3
RD 1 (config – route – map) # Set  Metric  1544  15  255  1  1500
RD 1 (config – route – map) # Exit
```

```
RD 1 (config) # Route – Map  Cisco  Permit  40
RD 1 (config – route – map) # Match  IP  Address  Prefix – list  4
RD 1 (config – route – map) # Set  Metric  2000  30  255  1  1500
RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map  Cisco  Permit  50
RD 1 (config – route – map) # Match  IP  Address  Prefix – list  5
RD 1 (config – route – map) # Set  Metric  1500  45  255  1  1500
RD 1 (config – route – map) # Exit

RD 1 (config) #Router EIGRP  1
RD 1 (config–router) #Redistribute  OSPF  1  Route – Map  Cisco
```

همانطور که در دستورات بالا مشاهده می کنید با سه روش متفاوت می توانیم Metric شبکه هایی را که Redistribute کرده ایم را تعیین کنیم .

روش اول با استفاده از یک Default – Metric مقدار شبکه های Redistribute شده را تعیین می کنیم . در روش دوم از پارامتر خود دستور Redistribute استفاده می کنیم که این روش اولویت دارد بر روش اول . در روش آخر با استفاده از Route – Map این کار را انجام داده ایم با این تفاوت که در این روش برای شبکه های مختلف Metricهای مختلف را با استفاده از Prefix – list و Route – Map تعیین کرده ایم و به داخل پروتکل EIGRP ارسال کرده ایم .

نکته :

مسیرهایی که EIGRP از پروتکل های دیگر با استفاده از Redistribute در جدول Routing خود ذخیره می کند را با علامت EX نمایش می دهد .

باید بر روی روتر مرزی این دستورات اعمال شود . باید این روتر در هر دو شبکه ای که EIGRP و OSPF برقرار است دارای اینترفیس باشد .

در Redistribute مسیرهایی که در جدول Routing دو پروتکل قرار دارند به یکدیگر فرستاده می شوند نه مسیرهایی که در جدول توپولوژی خود دارند .

دستور Route Redistribution از پروتکل های مختلف به داخل پروتکل OSPF :

Router (config – router) # Redistribute Protocol [As–num | Process–id] [Metric metric–value] [Metric – Type 1 | 2] [Subnet] [Route – Map Map – name] [Tag Tag – Value] [Match { Internal | External 1 | External 2 | NSSA – External }]

Protocol : در این قسمت باید پروتکل مسیریابی که قصد انتشار اطلاعات مربوط به آن را در پروتکل OSPF خواهید داشت را تعیین نمایید در این قسمت می توان از پروتکل های , EIGRP , RIP , Connected , BGP Static , ISIS استفاده نمایید .

Process – id : در صورتی که پروتکل Source دارای شماره پروسس یا AS باشد به منظور اشاره دقیق تر باید شماره مربوطه را نیز در خلال دستور مشخص کنیم .

Metric : این دستور برای تعیین Metric مربوط به شبکه های منتشر شده مورد استفاده قرار می گیرد می دانید که OSPF از پارامتر Cost برای نشان دادن متریک استفاده می کند .

Metric – type : در هنگام انتشار اطلاعات به داخل OSPF باید نوع متریک مربوط به پیام های منتشر شده نیز مشخص گردد. مقدار این پارامتر را می توان برابر با 1 (E1 route) و 2 (E2 route) قرار داد.

Match : این پارامتر می توان نوع پیام هایی که باید انتخاب شده و به داخل EIGRP منتشر شوند را مشخص کرد . برای نمونه در صورت نوشتن دستور Match internal تمامی OSPF internal routeهایی که در داخل جدول Routing این روتر قرار دارد به داخل EIGRP منتشر می شوند.

Tag : با استفاده از این دستور می توان یک Tag مخصوص بر روی Routeهای منتشر شده اختصاص داد. از این Tag می توان در Route – Mapها استفاده کرد .

Subnet :این دستور باعث می شود که شبکه های زیر مجموعه یک شبکه مادر نیز به داخل OSPF منتشر شوند. اگر این دستور را ننویسیم تنها شبکه های مادر وارد OSPF خواهند شد.

Route – Map :این دستور می توان برای اعمال فیلتر و تعیین مقدار متریک و موارد دیگر استفاده کرد .

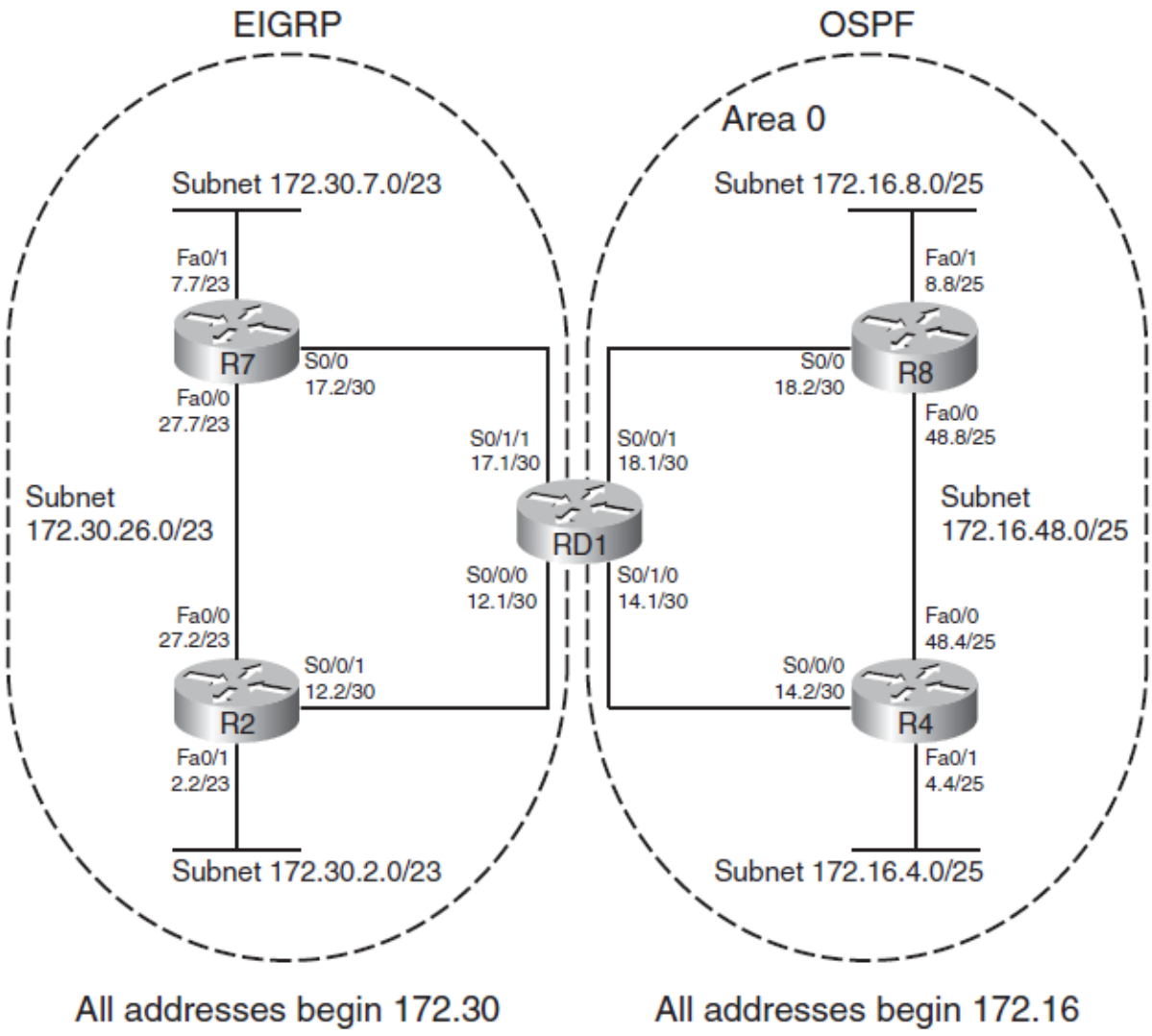
رفتار پیش فرض دستور Redistribute در مورد OSPF به صورت زیر است :

- در صورتی که اطلاعات BGP به داخل OSPF منتشر گردد مقدار متریک به صورت پیش فرض برابر با 1 قرار داده خواهد شد .
- در صورتی که اطلاعات مربوط به یک OSPF به داخل OSPF دیگری منتشر گردد مقدار متریک به صورت پیش فرض برابر با متریک اولیه هر Route خواهد بود .
- در صورتی که اطلاعات مربوط به دیگر پروتکل ها به داخل OSPF منتشر گردد مقدار متریک به صورت پیش فرض برابر با 20 تعیین می گردد .
- در نتیجه Redistribute به ازای هر کدام از شبکه هایی که به داخل OSPF منتشر خواهد شد یک پیام LSA type 5 توسط روتر ASBR ایجاد شده و برای دیگر روترهای OSPF domain ارسال میشود.در صورتی که روتر ASBR در داخل یک NSSA Area قرار داشته باشد به جای پیام های LSA type 5 از پیام های LSA type 7 بهره می گیرد .
- مقدار پارامتر Metric – type برابر با 2 قرار داده خواهد شد . یعنی پیام های منتشر شده به صورت E2 external نمایش داده می شود .
- تنها شبکه مادر در کلاس های A , B , C به داخل OSPF منتشر خواهند شد و نه تمامی شبکه های زیر مجموعه آن .

نکته :

اگر دو مسیر با متریک مساوی که از طریق Redistribute وارد پروتکل OSPF شوند روتر مبدأ این دو مسیر را در جدول توپولوژی خود ذخیره می کند ولی فاصله خود را با روتر ASBR حساب می کند و مسیری که نزدیکتر باشد را انتخاب می کند و در جدول Routing خود قرار می دهد و اگر مقدار Cost هر دو مسیر تا روتر ASBR نیز مساوی باشند هر دو مسیر را در جدول Routing خود قرار می دهد .

مثال :



با توجه به شکل بالا می خواهیم شبکه هایی که در داخل EIGRP Domain قرار دارند را به داخل OSPF Domain با استفاده از توانمندی Redistribute منتشر کنیم .

روش اول :

RD 1 (config) #Router OSPF 1

RD 1 (config–router) #Redistribute EIGRP 1 Subnet

RD 1 (config–router) #Default – Metric 50

روش دوم :

RD 1 (config) #Router OSPF 1

RD 1 (config–router) #Redistribute EIGRP 1 Metric 50 Subnet

روش سوم :

RD 1 (config) # IP Prefix – List A seq 5 Permit 172.30.7.0/23

RD 1 (config) # IP Prefix – List B seq 5 Permit 172.30.2.0/23

RD 1 (config) # IP Prefix – List C seq 5 Permit 172.30.26.0/23

RD 1 (config) # IP Prefix – List D seq 5 Permit 172.30.12.0/30

RD 1 (config) # IP Prefix – List E seq 5 Permit 172.30.17.0/30

RD 1 (config) # Route – Map Cisco Permit 10

RD 1 (config – route – map) # Match IP Address Prefix – list A

RD 1 (config – route – map) # Set Metric – type type 1

RD 1 (config – route – map) # Set Metric 30

RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map Cisco Permit 20

RD 1 (config – route – map) # Match IP Address Prefix – list B

RD 1 (config – route – map) # Set Metric – type type 1

RD 1 (config – route – map) # Set Metric 55

RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map Cisco Permit 30

RD 1 (config – route – map) # Match IP Address Prefix – list C

RD 1 (config – route – map) # Set Metric – type type 2

RD 1 (config – route – map) # Set Metric 40

RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map Cisco Permit 40

RD 1 (config – route – map) # Match IP Address Prefix – list D

RD 1 (config – route – map) # Set Metric – type type 1

RD 1 (config – route – map) # Set Metric 35

RD 1 (config – route – map) # Exit

RD 1 (config) # Route – Map Cisco Permit 50

RD 1 (config – route – map) # Match IP Address Prefix – list E

RD 1 (config – route – map) # Set Metric – type type 2

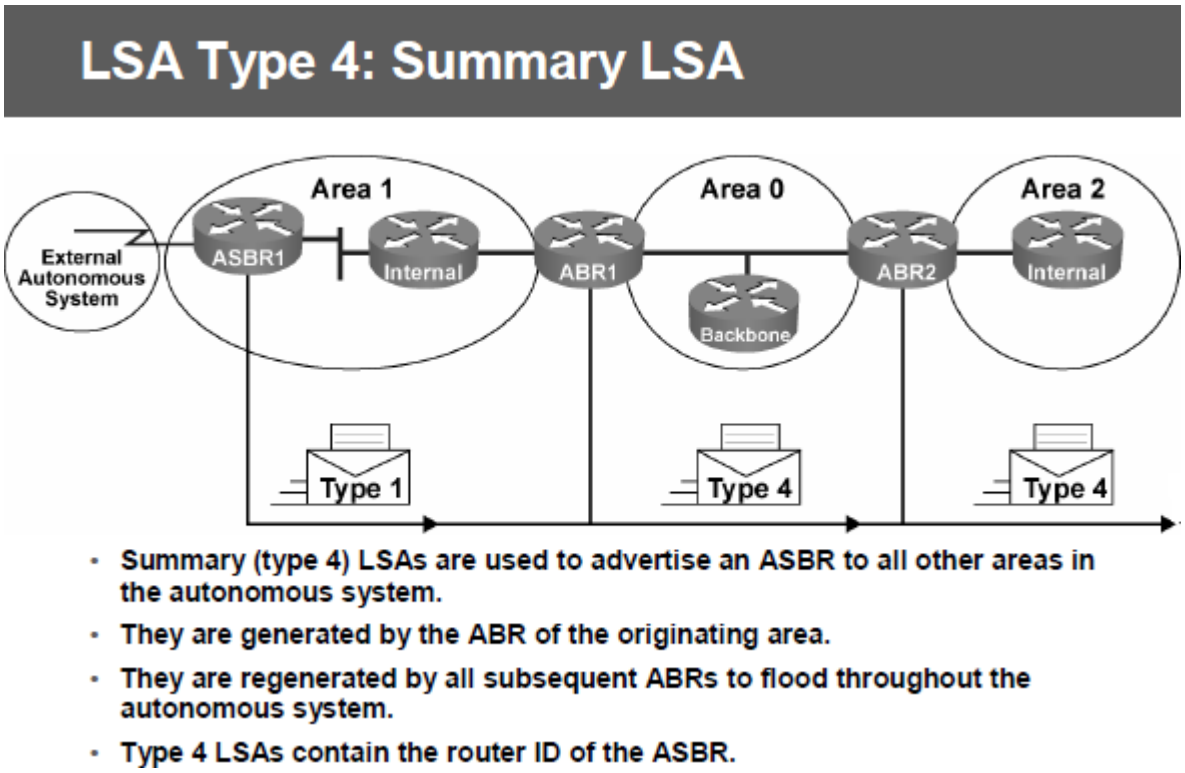
RD 1 (config – route – map) # Set Metric 60

RD 1 (config – route – map) # Exit

RD 1 (config) #Router OSPF 1

RD 1 (config–router) #Redistribute EIGRP 1 Route – Map Cisco Subnet

LSA Type 4 : ASBR – Summary LSA



LSA type 4 توسط روتر ABR ایجاد و ارسال می شود. پیام های LSA type 4 تعیین می کنند که شبکه مورد نظر تا روتر ASBR چقدر فاصله دارد .

با دستور زیر پیام های LSA type 4 را می توانیم مشاهده کنیم :

Router # Show IP OSPF Database ASBR – Summary LSID

LSID ⟶ Router ID ASBR

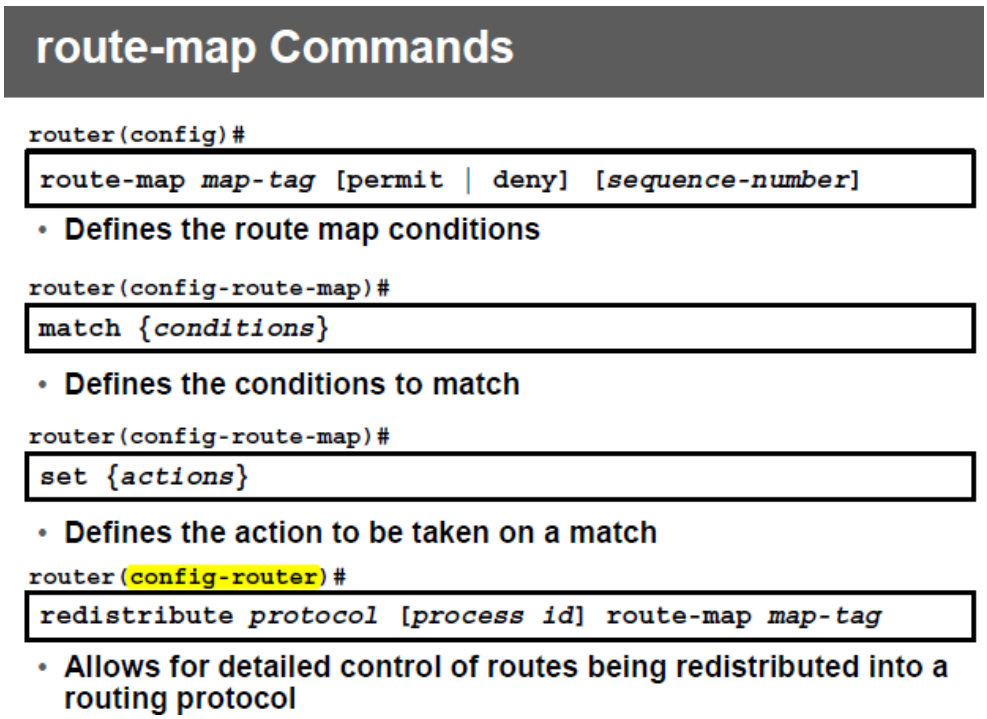
نکته : تمام Areaها پیام های LSA type 4 را به صورت یکسان دریافت می کنند و در کل مسیر تغییری نمی کنند.

دستور نمایش تمام روترهای ABR و ASBR :

Router # Show IP OSPF Border – Router

Filtering in Redistribute

انواع پارامترهای دستور Match در هنگام استفاده از Route – Map در پروسه Redistribution :



فیلتر کردن از طریق IP Address :

Router (config) # IP Prefix – List 1 seq 5 Permit 192.168.0.0/22 ge 24 le 24

Router (config) # Route – Map Cisco Deny 10

Router (config – route – map) # Match IP Address Prefix – list 1

Router (config – route – map) # Exit

Router (config) # Route – Map Cisco Permit 20

Router (config – route – map) # Exit

Router (config) #Router EIGRP 1

Router (config–router) #Redistribute OSPF 1 Route – Map Cisco

Router (config–router) #Default – Metric 1000 10 255 1 1500

فیلتر کردن از طریق Interface :

```
Router (config) # Route – Map   Cisco  Deny   10
Router (config – route – map) # Match  Interface   Serial  1/0
Router (config – route – map) # Exit
Router (config) # Route – Map   Cisco  Permit  20
Router (config – route – map) # Exit

Router (config) #Router EIGRP   1
Router (config–router) #Redistribute   OSPF  1   Route – Map  Cisco
Router (config–router) #Default – Metric    1000   10   255   1   1500
```

فیلتر کردن از طریق Next – Hop :

```
Router (config) # Access  – List   1      Permit    10.0.0.9
Router (config) # Route – Map   Cisco  Deny   10
Router (config – route – map) # Match  IP  Next – Hop   1
Router (config – route – map) # Exit
Router (config) # Route – Map   Cisco  Permit  20
Router (config – route – map) # Exit
Router (config) #Router EIGRP   1
Router (config–router) #Redistribute   OSPF  1   Route – Map  Cisco
Router (config–router) #Default – Metric    1000   10   255   1   1500
```

فیلتر کردن از طریق Metric :

Router (config) # Route – Map Cisco Deny 10

Router (config – route – map) # Match Metric 128 + - 5

Router (config – route – map) # Exit

Router (config) # Route – Map Cisco Permit 20

Router (config – route – map) # Exit

Router (config) #Router EIGRP 1

Router (config–router) #Redistribute OSPF 1 Route – Map Cisco

Router (config–router) #Default – Metric 1000 10 255 1 1500

Configuring distribute-list

For outbound updates:

```
Router(config-router)#
distribute-list {access-list-number | name} out
[interface-name | routing-process [routing-process
parameter]]
```

For inbound updates:

```
Router(config-router)#
distribute-list [access-list-number | name] | [route-map
map-tag] in [interface-type interface-number]]
```

- Use an access list (or route map) to permit or deny routes.
- Can be applied to transmitted, received, or redistributed routing updates.

فیلتر کردن از طریق Distribute – List :

Router (config) # IP Prefix – List 1 seq 5 Deny 192.168.0.0/22 ge 24 le 24

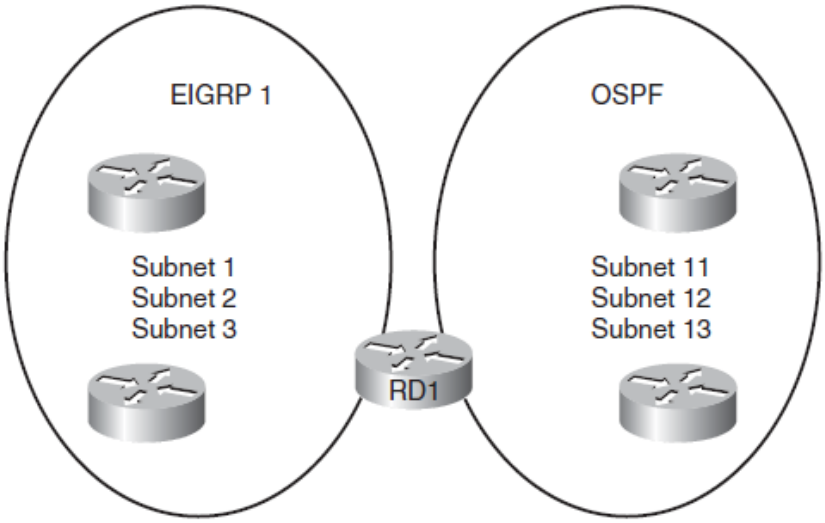
Router (config) # IP Prefix – List 1 seq 10 Permit 0.0.0.0/0 le 32

Router (config) #Router EIGRP 1

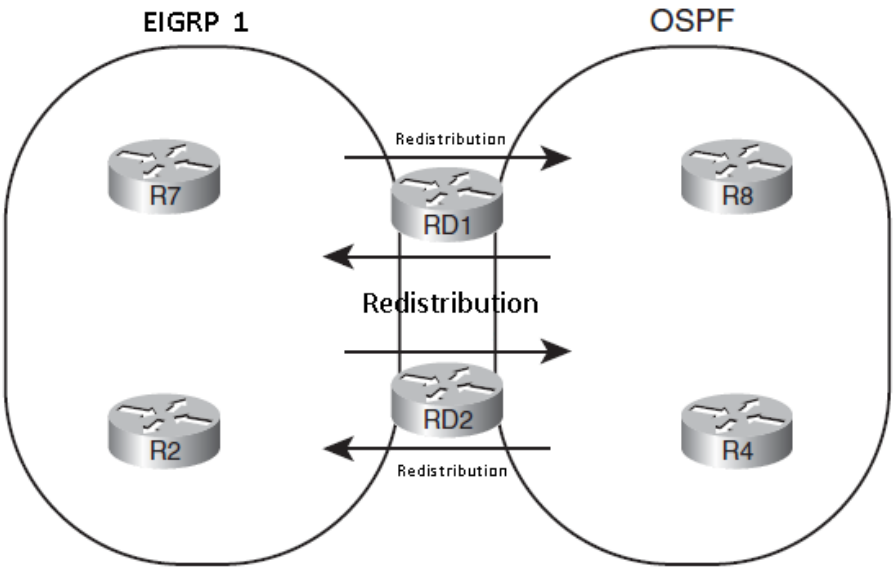
Router (config–router) #Redistribute OSPF 1

Router (config–router) #Default – Metric 1000 10 255 1 1500

Router (config–router) # Distribute – List Prefix 1 out OSPF 1



Single Point of Failure : نقطه گلوگاه شبکه می گویند که اگر قطع شود خطر دارد و باعث قطع دو شبکه می شود . مانند شکل بالا که اگر روتر RD1 به هر دلیلی قطع شود ارتباط بین دو شبکه OSPF و EIGRP 1 از بین می رود .در پروسه Redistribute بهتر است از دو روتر مرزی استفاده کنیم تا اگر یکی از روترها قطع شد روتر دیگر ارتباط بین دو شبکه را حفظ کند .



جدول مربوط به انواع مختلف پروتکل ها و AD مربوط به آنها :

Administrative Distance

Route Source	Default Distance
Connected interface	0
Static route	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1, RIPv2	120
External EIGRP	170
Internal BGP	200
Unknown	255

دستور تغییر AD در انواع پروتکل ها :

: RIP

Router (config) #Router RIP

Router (config–router) # Distance Ad – value

: EIGRP

Router (config) #Router EIGRP AS-number

Router (config–router) # Distance EIGRP Internal – Ad External – AD

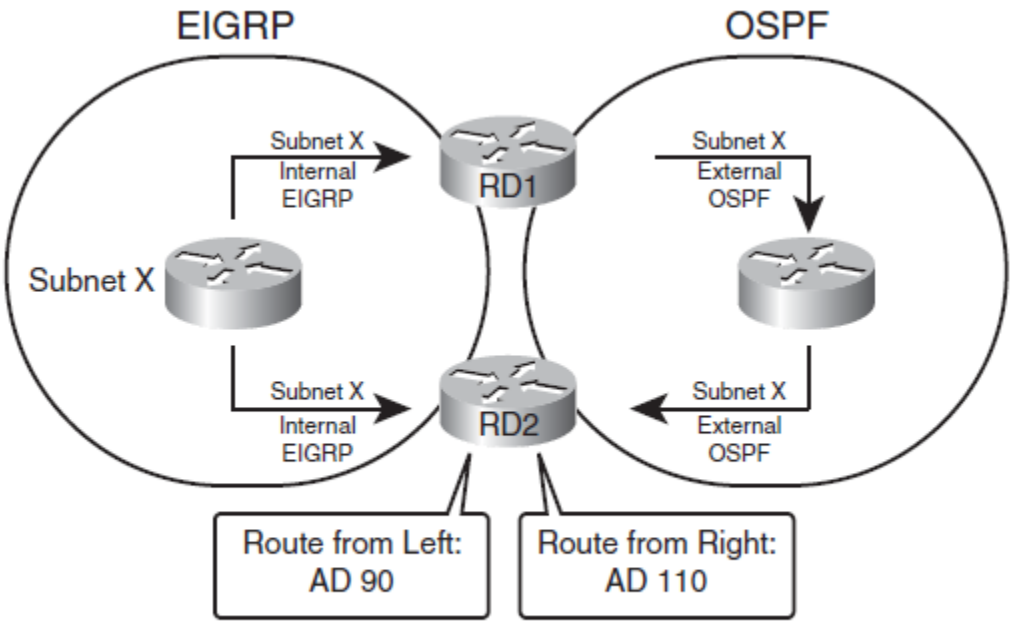
: OSPF

Router (config) #Router OSPF Process-id

Router (config–router) # Distance OSPF { Inter-area Ad – value | Intra – area Ad – value | External AD – value }

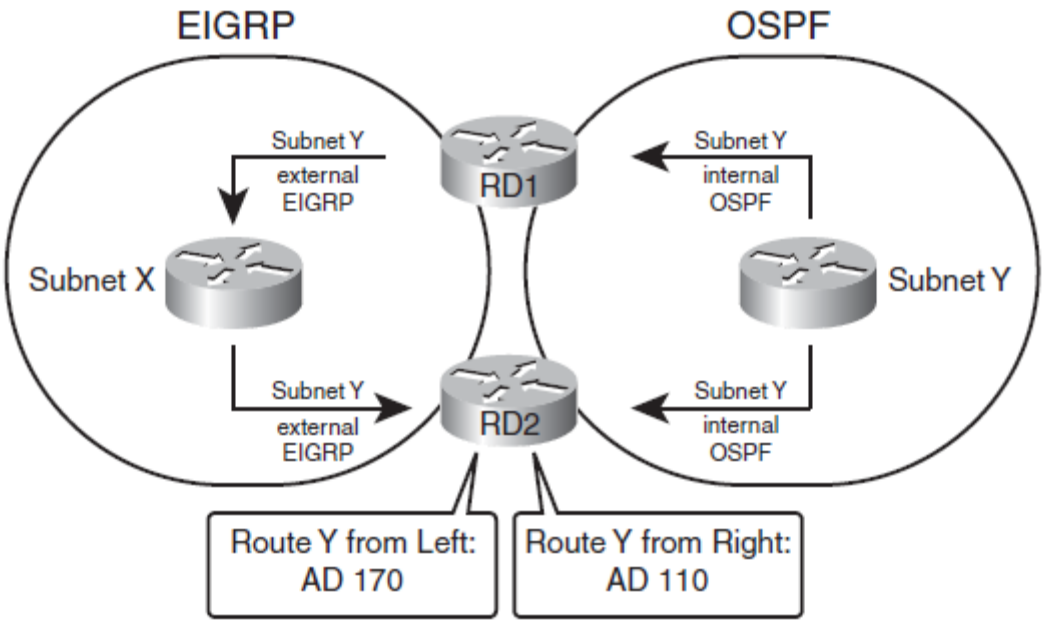
نکته : در بین دو پروتکل که پروسه Redistribute بین آنها برقرار می شود همیشه باید مقدار AD مربوط به Internal routeها کمتر از مقدار AD مربوط به External routeها باشد .

مقدار AD پیش فرض EIGRP باعث جلوگیری از بروز چرخه های Routing می شود. به شکل های زیر دقت کنید :



Subnet X: Internal EIGRP, External OSPF, on Router RD2

روتر RD2 با استفاده از پروتکل EIGRP اقدام به شناسایی Subnet X کرده و بر طبق قانون مقدار AD آن را برابر 90 قرار می دهد . زیرا این شبکه در داخل شبکه EIGRP واقع شده و Route مربوط (یعنی یک Internal EIGRP route) نیز توسط EIGRP شناسایی شده است . همچنین RD2 اطلاعات مربوط به Subnet X را از طریق یک Route دیگر (یعنی یک External OSPF route) نیز دریافت میکند که مقدار AD آن برابر با 110 است.روتر RD2 هم اکنون دارای 2 مسیر مختلف برای Subnet X می باشد .اما به دلیل آنکه مقدار AD مربوط به EIGRP route برابر با 90 بوده و کمتر از مقدار AD مربوط به OSPF route است و روتر RD2 برای دسترسی به Subnet X از EIGRP route به عنوان مسیر اصلی استفاده خواهد کرد و در نتیجه این مسیر را در داخل جدول Routing خود قرار می دهد .



Avoiding Domain Loops from OSPF to EIGRP to OSPF

در شکل بالا روتر RD2 اطلاعات مربوط به Subnet Y را از دو منبع می گیرد : یکی توسط پروتکلOSPF (Internal OSPF با AD برابر با 110) و دیگری توسط External EIGRP با AD برابر با 170 . بنابراین روتر RD2 مسیر شناسایی شده توسط OSPF را به عنوان مسیر اصلی انتخاب می کند و آن را در جدول Routing خود قرار می دهد و برای دسترسی به Subnet Y از آن مسیر استفاده می کند .

When comparing EIGRP's and OSPF's defaults, both of the generic criteria are met:

- EIGRP internal AD 90 < OSPF external AD 110
- OSPF internal AD 110 < EIGRP external AD 170

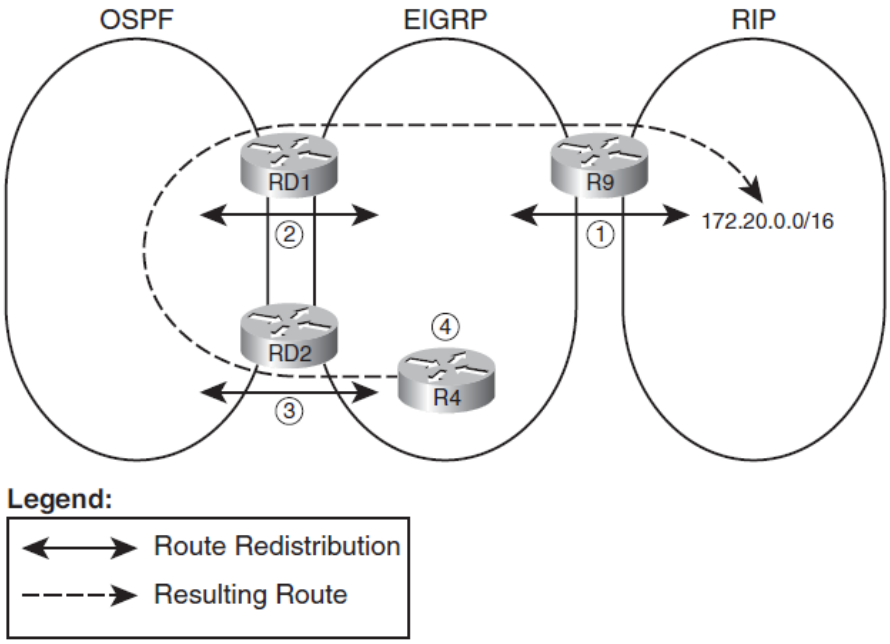
Likewise, when redistributing between EIGRP and RIP:

- EIGRP internal AD 90 < RIP external AD 120
- RIP internal AD 120 < EIGRP external AD 170

اما در مورد دو پروتکل OSPF و RIP به مشکل بر میخوریم :

- RIP Internal AD 120 < OSPF External AD 110 ×
- OSPF Internal AD 110 < RIP External AD 110 √

با توجه به شکل زیر :



Inefficient Routing with Looped Routing Advertisements

در مرحله اول :

روتر R9 اطلاعات مربوط به شبکه 172.20.0.0/16 را که در داخل RIP Domain قرار دارد به داخل شبکه EIGRP منتشر می کند که در این حالت مقدار AD مربوط به این EIGRP External route برابر با 170 قرار خواهد داد .

در مرحله دوم :

روتر RD1 اقدام به انتشار این EIGRP External route به داخل شبکه OSPF خواهد کرد که در این شرایط این route منتشر شده به داخل OSPF به عنوان یک E2 route بوده و مقدار AD آن برابر با 110 می باشد .

مرحله سوم :

در این بین روتر RD2 نیز پیام ارسالی از RD1 را دریافت می کند . از این رو روتر RD2 دارای دو عدد route به سمت شبکه 172.20.0.0/16 خواهد بود. که یکی به صورت External EIGRP با AD برابر با 170 بوده و دیگری از نوع E2 OSPF با مقدار ADبرابر با 110 می باشد . به دلیل کمتر بودن مقدار AD مربوط به E2 OSPF route روتر RD2 برای دسترسی به شبکه 172.20.0.0/16 از همین مسیر استفاده می کند که مسیر طولانی تری نسبت به دیگری است . به دلیل آنکه روتر RD2 نیز برای انجام Redistribute تمام

محتویات جدول Routingخود را به داخل جدول توپولوژی EIGRP منتشر می کند . این پیام منتشر شده و به دست روتر R4 خواهد رسید .

مرحله چهارم :

روتر R4 نیز که در داخل شبکه EIGRP قرار دارد هم اکنون دارای دو عدد route مختلف برای دسترسی به شبکه 172.20.0.0/16 می باشد : یکی به صورت External EIGRP با AD برابر با 170 بوده و در ابتدای کار از طریق R9 بدست آمده و دیگری نیز به صورت External EIGRP با AD برابر با 170 بوده و از طریق RD2 کسب شده است . در نتیجه مقدار AD مربوط به این دو مسیر به مقصد 172.20.0.0/16 با هم یکسان خواهد بود . در چنین شرایطی که روتر R4 به مقدار متریک مربوط به دو مسیر مراجعه خواهد کرد تا مسیر مناسب را از دیگری تشخیص دهد . در این وضعیت احتمال آنکه مقدار متریک مربوط به مسیر کسب شده از روتر RD2 کمتر باشد نیز وجود داشته که در نتیجه آن R4 برای دسترسی به شبکه 172.20.0.0/16 از روتر RD2 یعنی مسیر طولانی تر بهره خواهد گرفت .

سه روش برای حل این مشکل وجود دارد :

روش اول : از طریق تغییر مقدار AD به ازای هر کدام از مسیرها

با استفاده از دستور زیر می توانیم مقدار AD مربوط به پروتکل های مختلف را تغییر دهیم .

Router (config – router) # Distance distance – value IP – Advertise – value Waildcard Mask [ACL – number | ACL – name]

در صورت نوشتن این دستور در روی یک روتر مقدار AD مربوط به تمامی پیام های ارسالی از یک روتر که آدرس IP آن به جای متغیر IP – Advertise – value و Waildcard Mask آن نیز به جای متغیر Waildcard Mask نوشته شده است برابر با مقدار تعیین شده قرار خواهد گرفت .دستور Distance می تواند حاوی یک ACL نیز در انتهای خود باشد.در این صورت تمامی پیام های ارسالی از روتری که در دستور فوق مشخص شده است با ACL نوشته شده مقایسه خواهند شد.در صورت وجود تطابق مابین این پیام ها و قوانین ACL مقدار AD مربوط به آنها برابر با مقدار تعیین شده در دستور قرار خواهد گرفت .

مثال :

Router (config) #Router OSPF 1

Router (config–router) # Distance 171 1.1.1.1 0.0.0.0 1

Router (config) # Access – list 1 Permit Host 172.16.21.0

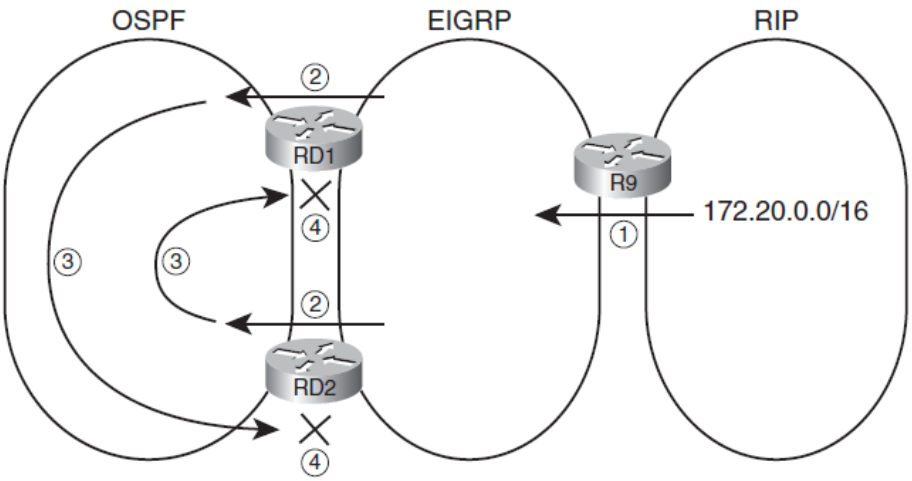
نکته :

فقط باید ACL استاندارد بنویسیم .

با این دستور انتخاب می کنیم که کدام یک از مسیرها را می خواهیم و در هنگام Advertise مقدار AD آن مسیر را به 171 تغییر دهد .

روش دوم : از طریق فیلتر کردن مسیرهای مورد نظر

در این روش با فیلتر کردن پیام ها بر اساس Prefix و ماسک مربوط به آنها اقدام به ممانعت از بروز چرخه های Routing خواهیم نمود . به شکل زیر دقت کنید :



Preventing Domain Loops with Route Filtering

مراحل موجود در شکل عبارتنداز :

- مرحله اول : روتر R9 اطلاعات مربوط به شبکه 172.20.0.0/16 را که در داخل RIP Domain قرار دارد به داخل شبکه EIGRP منتشر می سازد .

مرحله دوم : هر دوی روترهای RD1 و RD2 این external EIGRP routeها را به داخل شبکه OSPF منتشر می نمایند .

مرحله سوم : هر دوی روترهای RD1 و RD2 در حین انجام Redistribution پیام LSA type 5 حاوی این شبکه را به صورت E2 route به تمامی روترهای واقع در داخل شبکه OSPF ارسال می کنند .

مرحله چهارم : هر دوی روترهای RD1 و RD2 در حین انجام Redistribution از OSPF به EIGRP یک Route – Map را بر روی پیام ها اعمال کرده و بدین ترتیب از انتشار شبکه 172.20.0.0/16 جلوگیری به عمل می آورد .

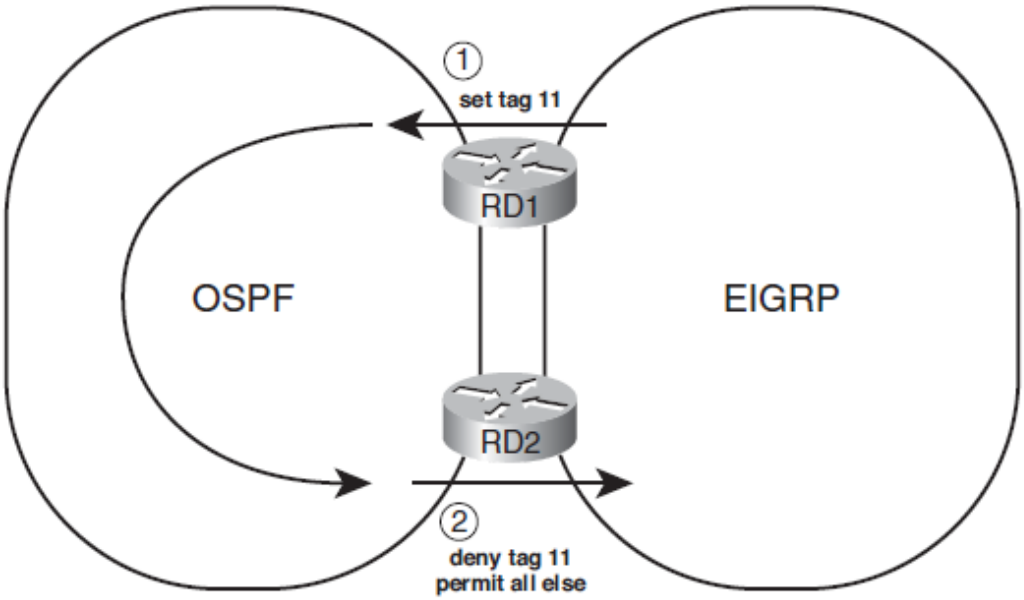
مثال :

```
Router (config) # IP  Prefix – List  1  seq  5  Permit  172.16.0.0/16  ge  17  le  24
Router (config) # Route – Map  A  Deny  10
Router (config – route – map) # Match  IP  Address  Prefix – list  1
Router (config – route – map) # Exit
Router (config) # Route – Map  A  Permit  20
Router (config – route – map) # Exit

Router (config) #Router EIGRP  1
Router (config–router) #Redistribute  OSPF  1  Route – Map  A
```

با این روش مشکل برای روترهای داخل شبکه EIGRP حل می شود ولی روترهای مرزی یعنی RD1 و RD2 برای رسیدن به شبکه 172.20.0.0/16 از داخل OSPF می رود تا به این شبکه برسد و این خود مشکل است .

روش سوم : استفاده از Tag

یک Tag در واقع عدد 32 بیتی است که هر کدام از پروتکل های Routing می توانند بر روی هر کدام از routeها تخصیص دهند . به شکل زیر توجه کنید :



Using Route Tags to Prevent Domain Loop Problems

در مرحله اول بر روی روتر RD1 اقدام به پیکربندی پروسه Redistribution از شبکه EIGRP به OSPF نموده ایم و با استفاده از دستور Route – Map بر روی Routeهای منتشر شده به داخل OSPF یک Tag به نام 11 اختصاص داده ایم . روتر RD2 نیز این پیام منتشر شده توسط RD1 را از طریق OSPF دریافت می کند . در مرحله دوم روتر RD2 اقدام به انتشار اطلاعات OSPF به داخل EIGRP کرده اما در این بین تمام پیام هایی را که دارای یک Tag 11 هستند را بلوکه خواهد نمود . در نتیجه EIGRP routeها دوباره به داخل شبکه EIGRP منتشر نخواهد شد .

مثال :

این دستورات را بر روی روتر RD1 وارد می کنیم تا بر روی مسیرهای مورد نظر Tag 11 را بزنند :

RD 1 (config) # Route – Map B Permit 10

```
RD 1 (config – route – map) # Set   Tag   11
RD 1 (config – route – map) # Exit

RD 1 (config) #Router   OSPF    1
RD 1 (config–router) #Redistribute   EIGRP  1     Route – Map  B    Subnet
```

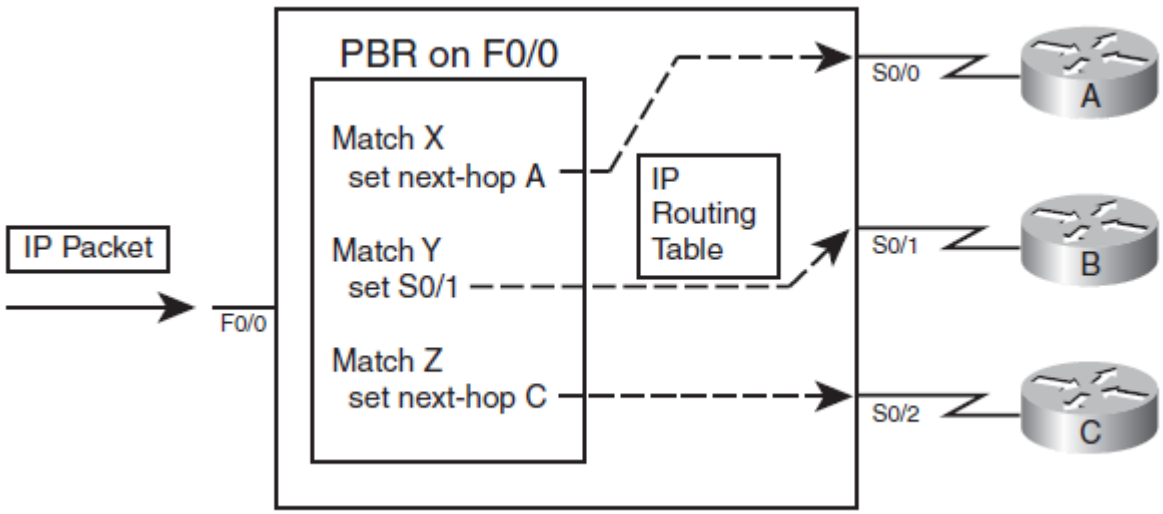
این دستورات را بر روی روتر RD2 وارد می کنیم تا مسیرهایی که دارای Tag 11 هستند را فیلتر کند :

```
RD2 (config) # Route – Map   C  Deny   10
RD2 (config – route – map) # Match  Tag   11
RD2 (config – route – map) # Exit
RD2 (config) # Route – Map   C  Permit  20
RD2 (config – route – map) # Exit

RD2 (config) #Router EIGRP   1
RD2 (config–router) #Redistribute   OSPF  1   Route – Map  C
```

Path Control

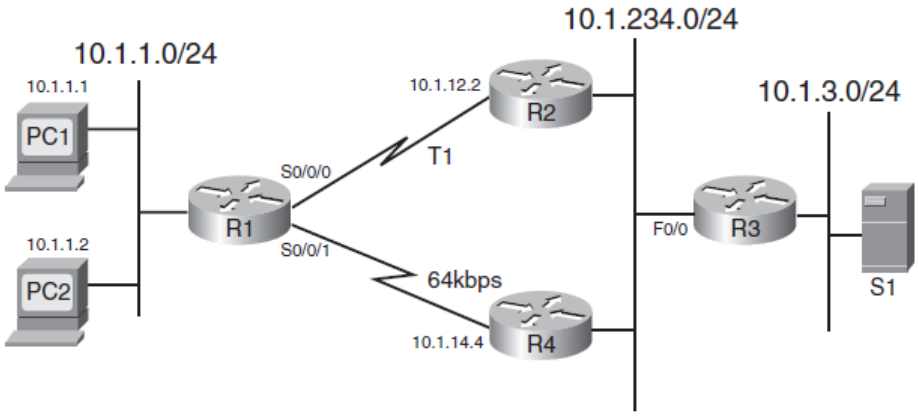
: Policy – Based Routing (PBR)

ویژگی PBR باعث تغییر در پروسه طبیعی ارسال اطلاعات توسط روتر می شود . بدین ترتیب که PBR بعد از پردازش فریم در سطح لایه 2 و قبل از ارسال به لایه 3 فعال شده و پاکت را بر اساس قوانین خاصی به سمت مقاصد یاد شده هدایت می کند . البته انتخاب مقصد ارسال پیام بر اساس آدرس مشخص شده در فیلد Destination IP آن صورت نمی گیرد . مقصد ارسال پیام در PBR معمولا توسط یک Route – Map مشخص می گردد که آن نیز معمولا اشاره به یک ACL دارد . از طریق این Route – Map است می توان اینترفیس خروجی پیام های منطبق بر قوانین ذکر شده و یا آدرس Next – Hop آن را مشخص نمود .در شکل زیر PBR در روی Fa0/0 فعال شده و پروسه هدایت پیام ها توسط این روتر را تحت تأثیر قرار داده است :



برای این کار باید اول یک Route – Map را به منظور مشخص نمودن مسیرها ایجاد نمود بعد فعال کردن PBR بر روی یک اینترفیس ورودی و متناظر قرار دادن آن با Route – Map ایجاد شده .

مثالی از پیکربندی PBR :



Network Used in PBR Example

با توجه به شکل بالا در این توپولوژی پروتکل EIGRP بر روی روتر R1 به دلیل بالا بودن مقدار پهنای باند مربوط به اتصال بالایی (با سرعت T1) از همین مسیر برای دسترسی به شبکه های واقع در سمت راست یا سرور استفاده می کند . مثلا PC2 اگر بخواهد به سرور S1 دسترسی پیدا کند از طریق اینترفیس S0/0/0 روتر R1 این ارتباط برقرار می شود چون پهنای باند بیشتری نسبت به اینترفیس S0/0/1 دارد . اما ما می خواهیم از طریق اینترفیس S0/0/1 این ارتباط برقرار شود که برای این کار از PBR استفاده می کنیم .

دو روش دارد هم با استفاده از Next – Hop و هم از طریق Interface می توانیم این کار را انجام دهیم :

اول Access – List را می نویسیم :

R 1 (config) # Access – list 101 Permit IP Host 10.1.1.2 10.1.3.0 0.0.0.255

بعد از این دو روش پایین یکی را انتخاب می کنیم برای نوشتن Route – Map :

روش اول از طریق Next – Hop :

R 1 (config) # Route – Map Cisco Permit 10

R 1 (config – route – map) # Match IP Address 101

R 1 (config – route – map) # Set IP Next – Hop 10.1.14.4

R 1 (config – route – map) # Exit

روش دوم از طریق Interface :

R 1 (config) # Route – Map Cisco Permit 10

R 1 (config – route – map) # Match IP Address 101

R 1 (config – route – map) # Set Interface Serial 0/0/1

R 1 (config – route – map) # Exit

در آخر این دستور را روی اینترفیسی که ترافیک را می گیرد اعمال می کنیم :

R 1 (config) #Interface Fastethernet 0/0

R 1 (config–if) #IP Policy Route – Map Cisco

دستورات مانیتورینگ Policy :

Router # Show IP Policy

Router # Debug IP Policy

دستور کلی :

Router (config) # Route – Map Name { Permit | Deny } { Seq }

Router (config – route – map) # Match IP Address { ACL – number | ACL – name }

Router (config – route – map) # Match Length min max

Router (config – route – map) # Set Next – Hop [IP – Address , …]

Router (config – route – map) # Set Interface [out – going type mod/num , …]

اگر در دستور Route – Map دستورات قسمت Set آن را مثل دو دستور بالا بنویسیم و اعمال کنیم اول PBR بررسی می شود بعد جدول Routing ولی در دو دستور Set پایین اول جدول Routing بررسی می شود بعد PBR :

Router (config – route – map) # Set IP Default Next – Hop [IP – Address , …]

Router (config – route – map) # Set Default Interface [out – going type mod/num , …]

اگر ترافیکی بیاید اول با جدول Routing بررسی می شود و اگر با هیچ مسیری Set نشود بعد با PBR بررسی می شود و اگر با آن هم Set نشد در آخر به وسیله Default Root هدایت می شود .

دستور وارد کردن Policy به اینترفیس :

Router (config) #Interface type mod/num

Router (config–if) #IP Policy Route – Map name

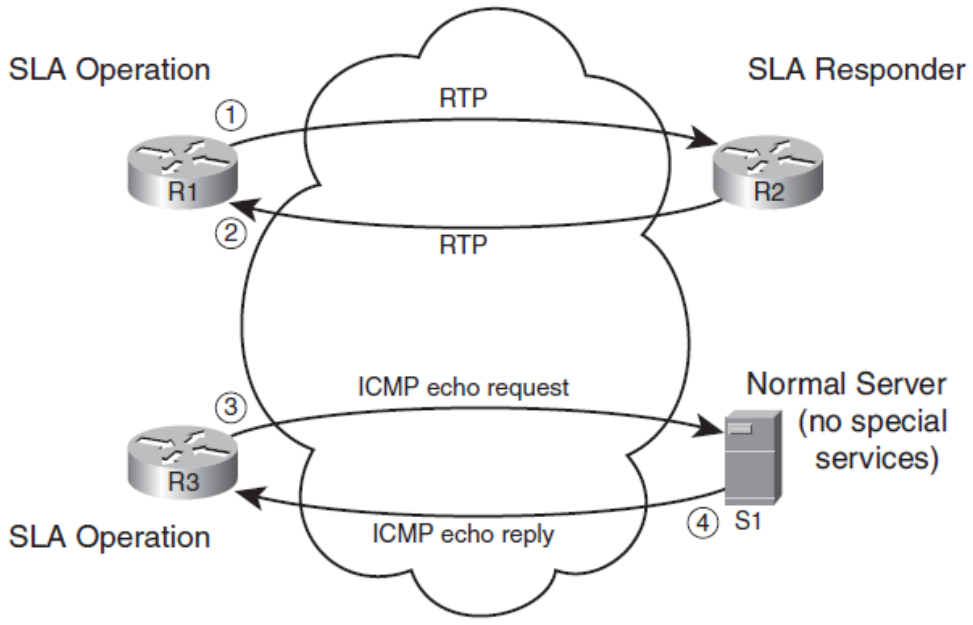
نوع دیگر اعمال Policy :

Router (config) # IP Local Policy Route – Map name

Service – Level Agreement (SLA) :

SLA ابزاری است که با استفاده از دستور Ping و یا traceroute به منظور کنترل دسترسی به شبکه های مختلف و مقدار تأخیر و Jitter در مورد هر کدام از مسیرهاست . پروسه SLA روترها را مجبور به ارسال و دریافت پاسخ هایی خواهد نمود و در نتیجه این ارسال و دریافت روترها میتوانند آمار مربوط به شبکه و مقدار Delay و jitter در هر مسیر را اندازه گیری نموده و عکس العمل مناسبی را در مواقع ضروری نشان دهند .

شکل زیر بیانگر ایده اصلی SLA است :



Sending and Receiving Packets with IP SLA

یک IP SLA Operation می تواند روتر را مجبور نماید تا اقدام به ارسال پاکت ها به سمت یک آدرس IP نماید . در صورتی که گیرنده این پیام ها یک دستگاه یا Host باشد در چنین شرایطی Operation typeهایی باید مورد استفاده قرار گیرند که پیام های قابل درک توسط دستگاه یا Host را برای او ارسال نمایند . مثلا روتر می تواند پیام های ICMP echo درخواست برای برقراری ارتباط TCP به سمت Host ارسال نماید .

شکل کلی دستور به صورت زیر است :

مرحله اول : اقدام به ایجاد یک IP SLA :

Router (config) # IP SLA sla – ops – number

مرحله دوم : تعیین نوع مربوط به operation :

Router (config – IP – SLA) #ICMP – Echo Dst – Network [Source – IP Ip – Address]

مرحله سوم : تعیین زمانی را که می خواهید روتر بعد از سپری شدن آن اقدام به ارسال پیام های تعیین شده نماید . مثلا هر چند ثانیه یک بار Ping بزند .

Router (config – IP – SLA) # Frequency Second

مرحله چهارم : تعیین زمانبندی مربوط به آغاز IP SLA :

Router (config) #IP SLA Schedule sla – ops – number Start – time { hh.mm.ss | now }

در قسمت operation دستور SLA می توانیم از نمونه های زیر استفاده کنیم :

- ICMP (echo, jitter)
- RTP (VoIP)
- TCP connection (establishes TCP connections)
- UDP (echo, jitter)
- DNS
- DHCP
- HTTP
- FTP

دستورات مانیتورینگ :

Router # Show IP SLA Statics

Router # Show IP SLA Configuration

: Tracking

چیزی که به عنوان Tracking تعیین می شود به مقدار return code مربوط به SLA operation مراجعه کرده و نتیجه عملیات Tracking را به صورت up یا down گزارش می دهد . یکی از دلایل اصلی نیاز به Tracking مسئله route flapping است . زمانی که روتری یک مسیر را به داخل جدول Routing خود اضافه کرده و بعد از مدتی به هر دلیل اقدام به حذف آن و بلافاصله افزودن دوباره آن به داخل جدول Routing نماید می توان گفت route flapping رخ داده است .

در ادامه به نحوه پیکربندی Tracking برای استفاده از PBR و route static خواهیم پرداخت :

مرحله اول : ایجاد یک نوع Track :

Router (config) # Track Track – number IP SLA sla – ops – number

مرحله دوم : تعیین زمان مابین Up و Down شدن پروسه Tracking :

Router (config – Track) # Delay Up seconds Down seconds

مرحله سوم : تعریف route static با استفاده از Track تعریف شده :

Router (config) # IP route IP – Address Subnet – Mask Interface type mod/num Track Track – number

اعمال Track به PBR :

Router(config–Route–Map)#Set IP Next – Hop Verify – Availability Next – Hop – ip # Track Track – number

دستور نمایش Track :

Router # Show Track

BGP

Border Gateway Protocol

پروتکل های مسیریابی به دو گروه تقسیم می شوند :

- پروتکل مسیریابی داخلی IGP
- پروتکل مسیریابی خارجی BGP

پروتکل مسیریابی داخلی IGP : IGP برگرفته از Interior Gateway Protocol می باشد که این گروه از پروتکل ها توانایی مسیریابی درون یک AS را خواهد داشت . پروتکل های OSPF , RIP EIGRP جزوه IGP می باشند .

پروتکل مسیریابی داخلی EGP : EGP برگرفته از Exterior Gateway Protocol می باشد که این گروه از پروتکل ها توانایی مسیریابی بین ASها را خواهد داشت . پروتکل BGP جزوه گروه EGPمی باشند .

خصوصیات پروتکل BGP :

- پروتکل مسیریابی BGP قادر به مسیریابی بین ASها و در حقیقت مسیریابی اینترنت می باشد .
- نسخه پروتکل BGP که در حال حاضراستفاده می شود نسخه 4 است .
- روترهای همسایه در پروتکل BGP به عنوان یک BGP Peer نامیده می شوند . روترهای همسایه به صورت دستی در پیکربندی BGP باید تعریف شوند .
- پروتکل BGP برای انتقال اطلاعات از پروتکل TCP با شماره پورت 179 استفاده می کنند .
- پروتکل BGP برای Update جدول مسیریابی از دو توانمندی Incremental و Triggered update پشتیبانی خواهد کرد .
- Metric در پروتکل BGP بر اساس یکسری Attribute (خصوصیات) محاسبه می شود.
- پروتکل BGP یک پروتکل Advance Distance Vector می باشد .
- پروتکل BGP از ایجاد Loop جلوگیری خواهد کرد .

- پروتکل BGP از VLSM پشتیبانی می کند .
- هر روتر فقط قادر به اجرای یک BGP Process خواهد بود .
- پروتکل BGP یک پروتکل مورد استفاده در مسیریابی اینترنت می باشد که این پروتکل بین سرویس دهنده های اینترنت ISP و شرکت های بزرگ استفاده می شود.
- روترهایی که پروتکل BGP بر روی آنها اجرا شده است BGP Spakers نامیده می شود .
- پروتکل BGP برای مسیریابی بین ASها استفاده می شود که ASها با شماره های بین 0 تا 65535 شناسایی می شوند که توسط سازمان جهانی IANA کنترل خواهد شد که ASهای معتبر اینترنتی دارای شماره بین 1 تا 64495 می باشد که به آنها Public می گویند و ASهای غیر معتبر که دارای شماره ای بین 64512 تا 65534 می باشند که به Private معروف میباشند و شماره های بین 64496 تا 65511 جهت تست و تمرین مورد استفاده قرار میگیرند و شماره 0 و شماره 65535 رزرو شده اند . ASها در جدول زیر مشخص شده اند :

16-Bit ASN Assignment Categories from IANA

Value or Range	Purpose
0	Reserved
1 through 64,495	Assignable by IANA for public use
64,496 through 65,511	Reserved for use in documentation
64,512 through 65,534	Private use
65,535	Reserved

مراحل تخصیص IP در دنیا :

ICANN : Internet Corporation For Assigned Network Numbers نام سازمان مدیریت اینترنت که مسئول تخصیص آدرس های IP می باشد .

IANA : Internet Assigned Numbers Authority که زیر مجموعه سازمان ICANN می باشد و نحوه تخصیص IP به مناطق جغرافیایی مختلف را تعیین می کند و همچنین مدیریت مربوط به سرویس Domain Name System (DNS) و Top Level Domain (TLD) مانند (.com) نیز بر عهده این سازمان می باشد.

سازمان هایی نیز در زیر مجموعه ICANN وجود دارند که وظایف آنها به شرح زیر است :

- مرحله اول : سازمان های IANA و ICANN آدرس هایی را که مخصوص هر منطقه جغرافیایی هستند مشخص می کنند .
- مرحله دوم :سازمان IANA آدرس های مخصوص هر منطقه جغرافیایی را به شرکت های مسئول در آن ناحیه که به نام (RIR) Regional Internet Registries نامیده می شود تحویل می دهد .
- مرحله سوم : هر کدام از شرکت های RIR آدرس های مربوط به هر کشور یا مناطق کوچکتر را به سازمان های مسئول که به نام (NIR) National Internet Registries یا (LIR) Local Internet Registries نامیده می شوند تحویل می دهند .
- مرحله چهارم : هر کدام از شرکت های (IR) Internet Registry آدرس های تحویل گرفته را شکسته و Subnetهای ایجادی خود را به کاربران انتهایی و یا سازمان های درخواست کننده تخصیص می دهند .

آدرس دهی و Routing در اینترنت :

برخی از آدرسهای IP را نمیتوان به مشتریانی که درخواست دریافت آدرس IP را دارند اختصاص داد. جداول زیر بیانگر آدرس های Private و آدرس هایی هستند که در استاندارد RFC 3330 تعریف شده و رزرو شده اند و در محیط اینترنت نمی توان از این آدرس ها بهره گرفت :

Private IP Address Reference

Number of Classful Networks	Range of Classful Networks	Prefix for Entire Range
(1) Class A:	10.0.0.0	10.0.0.0/8
(16) Class B:	172.16.0.0 through 172.31.0.0	172.16.0.0/12
(256) Class C:	192.168.0.0 through 192.168.255.0	192.168.0.0/16

Reserved Values in IPv4 Address Range (RFC 3330)

Value or Range	Reason
0.0.0.0/8	Used for self-identification on a local subnet.
127.0.0.0/8	Loopback testing.
169.254.0.0/16	This "link local" block is used for default IPv4 address assignment when DHCP process fails.
192.0.2.0/24	Reserved for use in documentation and example code.
192.88.99.0/24	Used for IPv6 to IPv4 relay (6to4 relay) (RFC 3068).
198.18.0.0/15	Benchmark testing for Internet devices (RFC 2544).

BGP Tables :

هر یک از روترهای BGP از سه جدول برای نگهداری از اطلاعات پروتکل BGP استفاده می کنند که این جدول ها به شرح زیر است :

- Routing Table
- Neighbor Table
- BGP Table or Topology Table

انواع پیام ها در BGP :

- Open
- Keepalive
- Update
- Notification

پیام **Open** : بعد از برقراری ارتباط TCP هر یک از روترها اقدام به ارسال پیام Open به سمت روترهایی که در پیکربندی BGP به عنوان همسایه تعیین شده اند خواهند کرد و در صورتی که پیام Open توسط یک روتر

دریافت گردد یک پیام Keepalive برای ارسال کننده پیام Open ارسال خواهد کرد و بعد از تکمیل این مرحله روترها توانایی ارسال پیام دیگر از جمله Update و Notification و Keepalive را خواهند داشت .

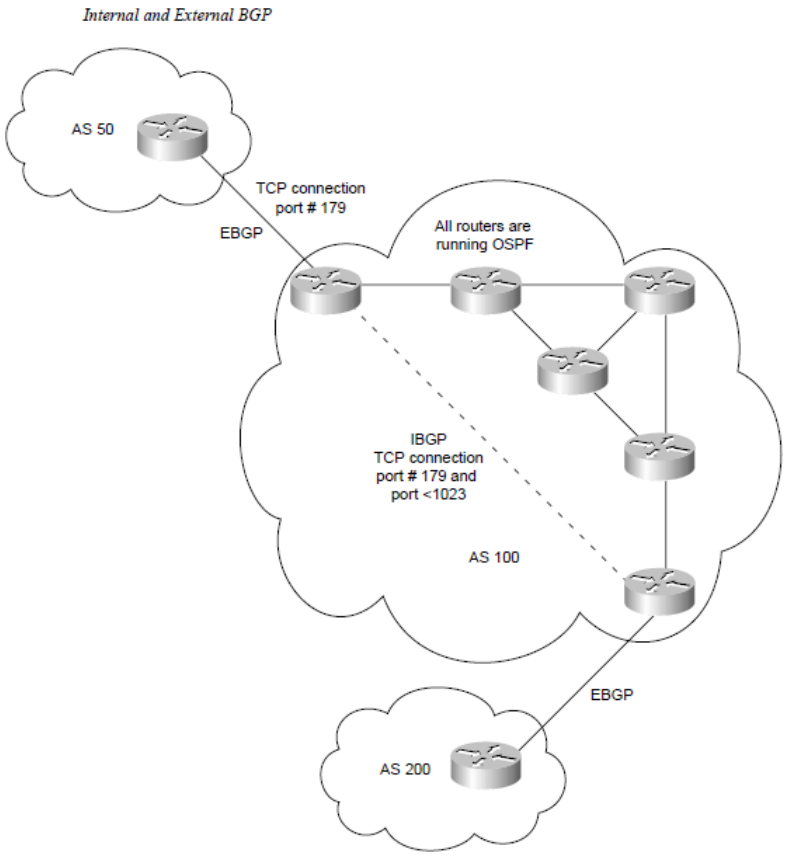
پیام **Keepalive** : به صورت پیش فرض هر 60 ثانیه یک بار به صورت مکرر به همسایگان BGP ارسال خواهد شد که این ارسال مکرر پیام ها مانع از انقضای زمان Hold time خواهد شد .

پیام **Update** : شامل اطلاعات مربوط به مسیرها میباشد که این پیام ها همچنین شامل Attributeهای که پروتکل BGP بر اساس آنها اقدام به شناسایی بهترین مسیر خواهد نمود هستند .

پیام **Notification** : در صورتی که error در اتصال BGP رخ دهد یک پیام Notification ارسال خواهد شد و ارتباط قطع خواهد شد .

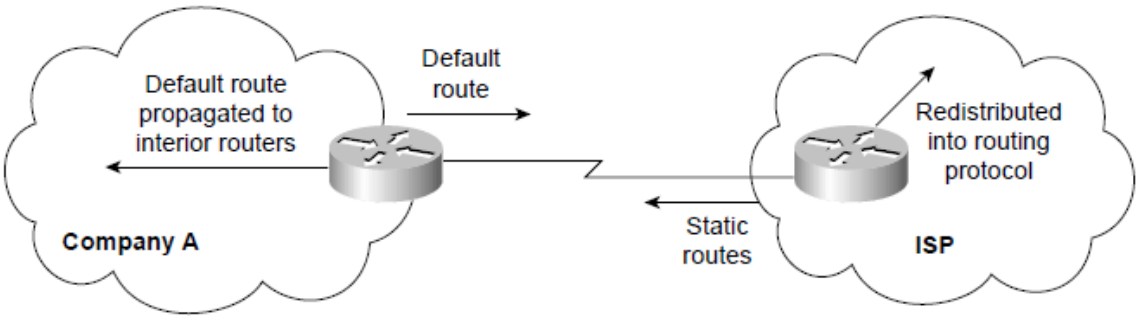
در پروتکل BGP دو نوع رابطه مجاورت داریم :

- IBGP : وقتی که Neighbor Routerها در یک AS باشند این نوع رابطه مجاورت از نوع IBGP می باشد .
- EBGP : وقتی که Neighbor Routerها در ASهای متفاوت باشند این نوع رابطه مجاورت از نوع EBGP می باشد .



: Default Route

Default and Static Route Configuration into the Internet



The command syntax to configure a static route is as follows:

```
ip route prefix mask {interface | ip-address} [distance]
```

در صورتی که روتر پیامی را دریافت کند که با هیچ کدام از routeهای واقع در داخل جدول routing مطابقت نداشته باشد این پیام به سمت Default Route ارسال خواهد شد . در واقع Default Route را می توان به عنوان یک Summary Route دانست که نشان دهنده تمامی آدرس های IP بوده و در داخل جدول Routing به ثبت می رسد .

دستور کلی همانطور که در شکل بالا مشاهده می کنید به صورت زیر است :

Router (config) # IP Route prefix mask { interface | ip – address }

انواع روش های اتصال به ISP :

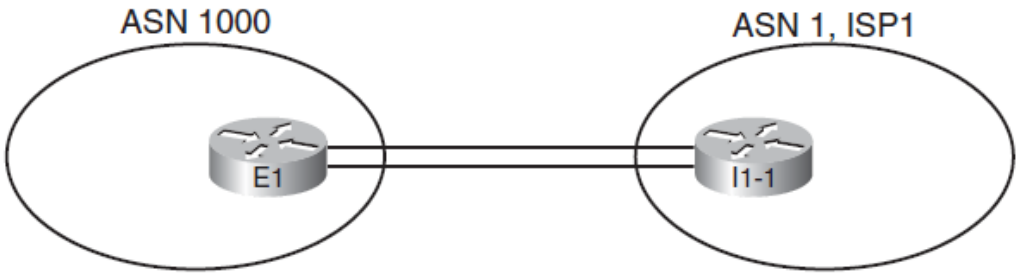
To aid in the discussion, this section examines four separate cases:

- Single homed (1 link per ISP, 1 ISP)
- Dual homed (2+ links per ISP, 1 ISP)
- Single multihomed (1 link per ISP, 2+ ISPs)
- Dual multihomed (2+ links per ISP, 2+ ISPs)

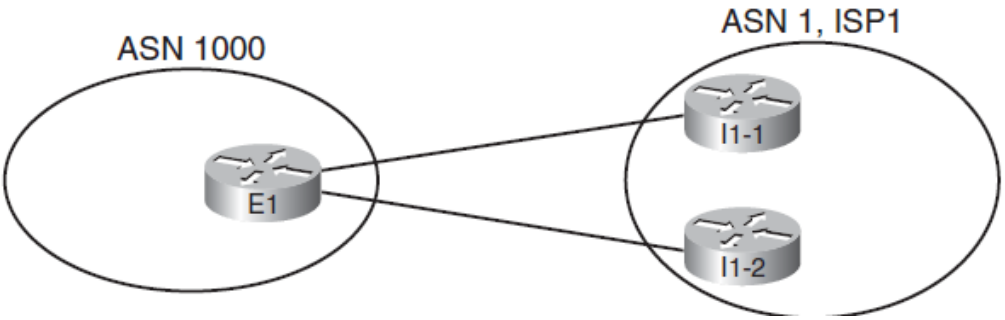
Single Homed : در این روش برای اتصال به اینترنت بین شرکت و سرویس دهنده اینترنت ISP تنها یک مسیر برای عبور کلیه بسته ها به سمت اینترنت وجود خواهد داشت و در این حالت ضرورتی نیست که از BGP استفاده کنیم بهتر است از Default Route استفاده کنیم .

Dual Homed : در این روش برای اتصال به اینترنت از دو یا بیشتر از دو اتصال استفاده خواهد شد که کلیه اتصالات از طریق یک ISP برقرار خواهد شد . این روش حالت های مختلفی دارد :

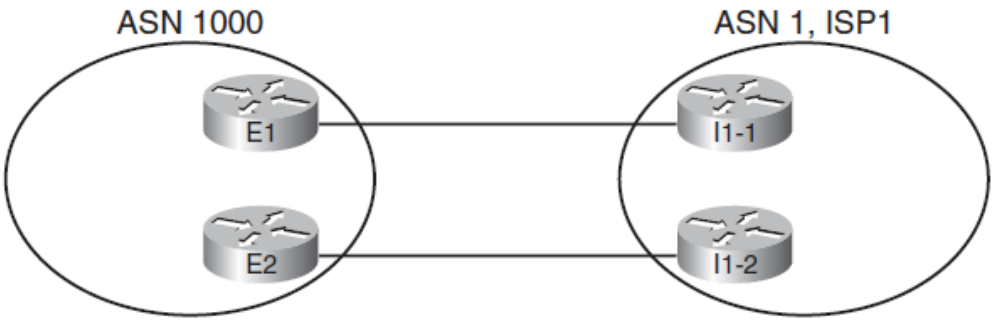
حالت اول :



حالت دوم :



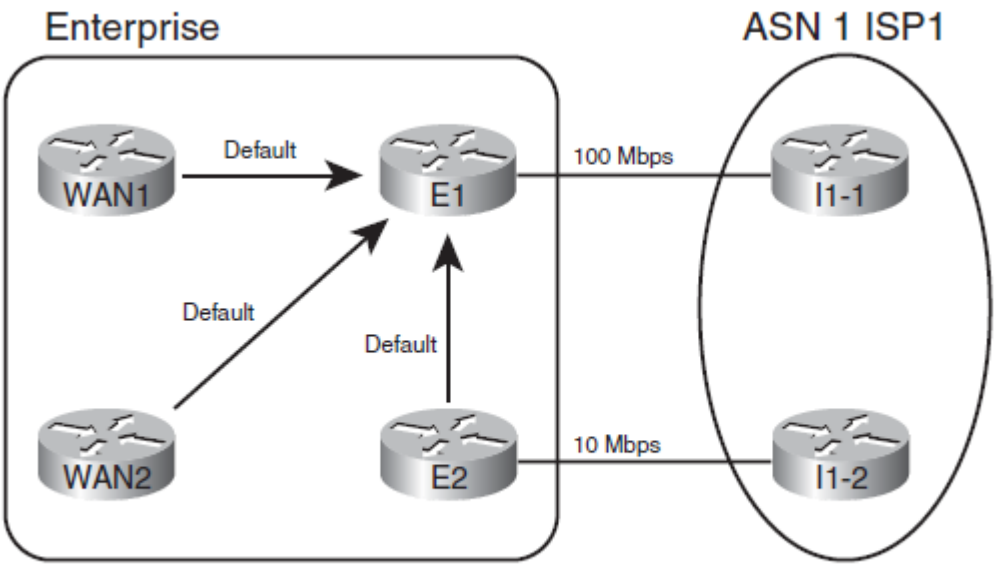
حالت سوم :



در این روش هم می توانیم از BGP استفاده کنیم هم از Default Route .

مثال :

در شکل زیر برای دسترسی به اینترنت مسیر اتصالی به روتر E1 به مسیر اتصالی روتر E2 ترجیح داده خواهد شد . مسیر اتصالی به روتر E2 را به عنوان مسیر Backup قرار می دهیم تا اگر مسیر اتصالی به روتر E1 قطع شود این مسیر استفاده شود . برای هر دو روتر Default Route تعریف می کنیم و مسیر اتصالی به روتر E1 را با متریک بهتر Redistribution می کنیم :



Dual-Homed Design, Using Defaults to Favor One Link

E1 (config) # IP Route 0.0.0.0 0.0.0.0 Serial 0

E1 (config) # Router EIGRP 10

E1 (config – router) # Redistribute Static Metric 100 1 255 1 1500

E1 (config – router) # Exit

E2 (config) # IP Route 0.0.0.0 0.0.0.0 Serial 0

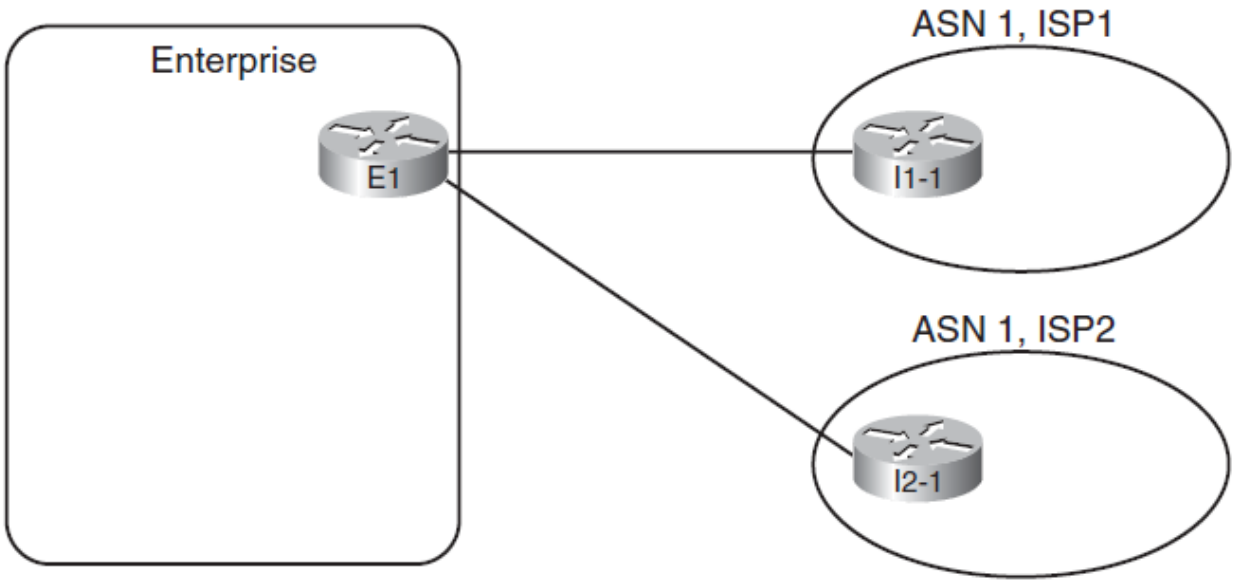
E2 (config) # Router EIGRP 10

E2 (config – router) # Redistribute Static Metric 10 1 255 1 1500

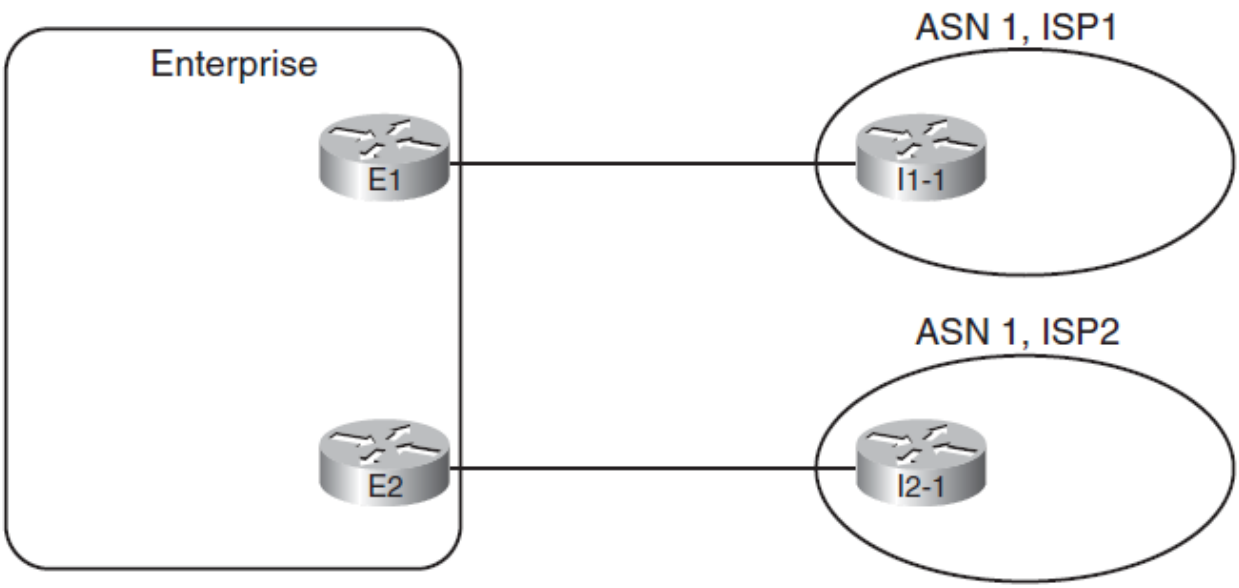
E2 (config – router) # Exit

Single Multihomed :در این روش برای دسترسی به اینترنت شرکت ها به بیش از یک ISP متصل خواهند شد که برای اتصال به هر ISP از یک اتصال جداگانه استفاده خواهند کرد . این روش نیز چندین حالت دارد :

حالت اول :

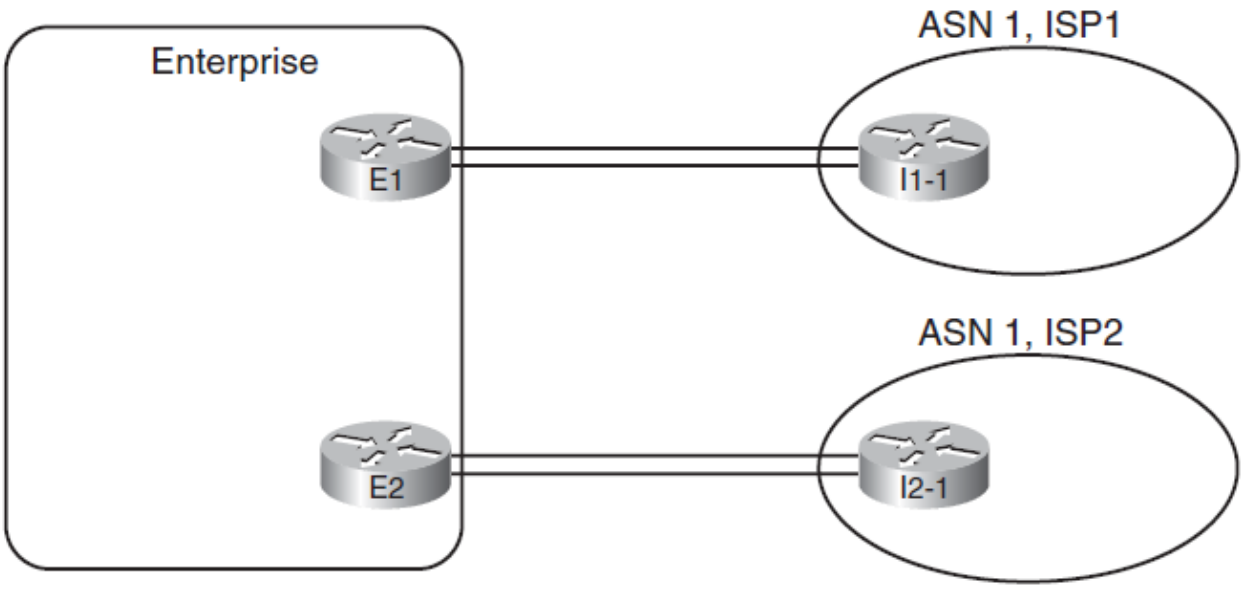


حالت دوم :

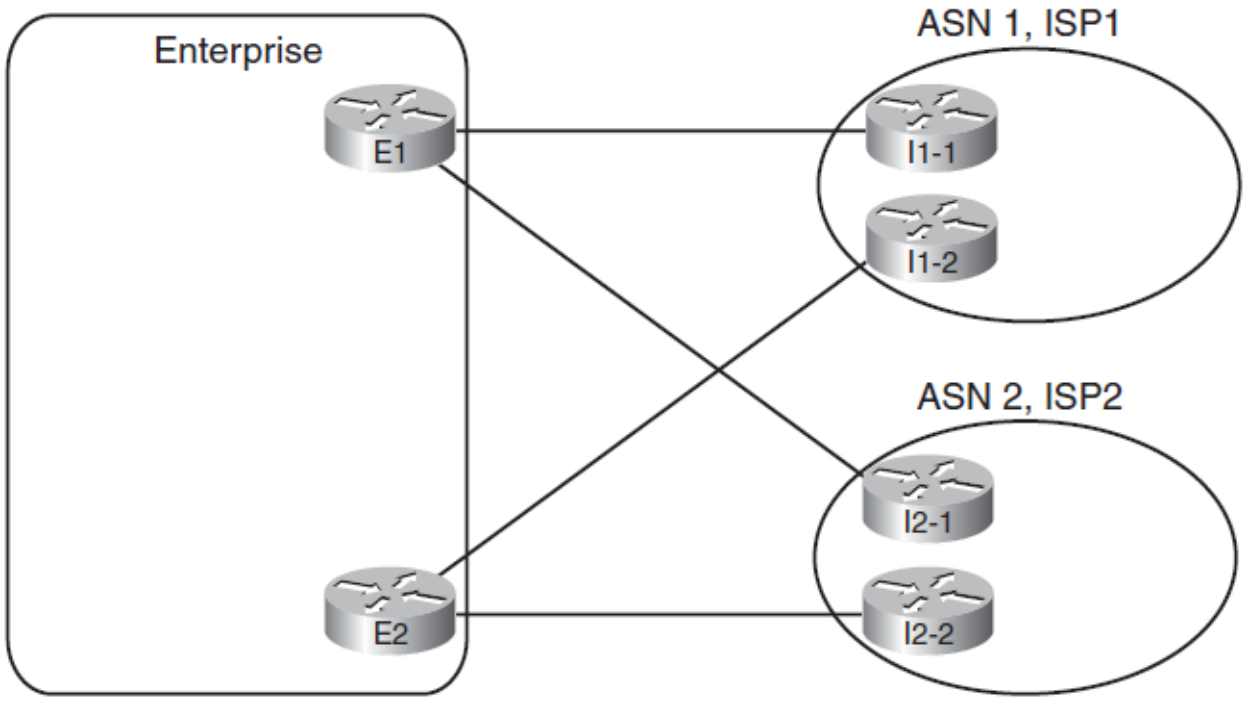


Dual Multihomed : در این روش شرکت به بیش از یک ISP متصل خواهد شد و هر روتر مرزی با بیش از یک اتصال به ISP متصل می شوند . این روش نیز حالت های زیر را دارد :

حالت اول :



حالت دوم :



تشکیل همسایگی در روترهای EBGP :

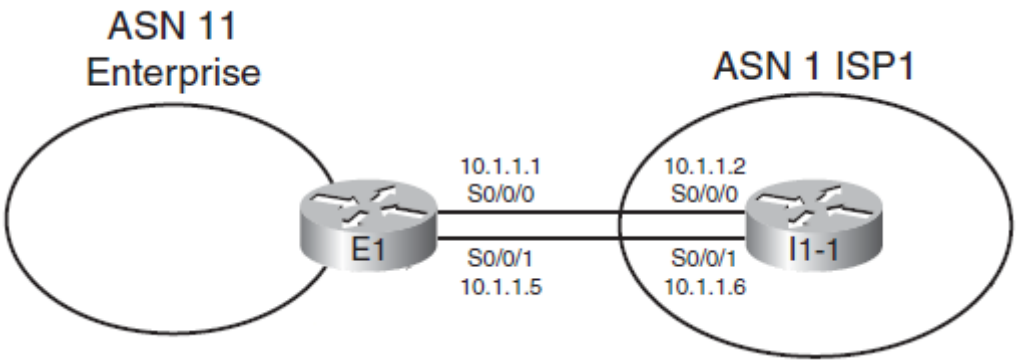
دستور کلی :

Router (config) # Router BGP As – number

Router (config – router) # Neighbor IP–Address Remote – As

Remute – As – Number

مثال :به شکل زیر دقت کنید .



دستورات زیر را وارد می کنیم تا همسایگی EBGP تشکیل شود در بین دو روتر :

BGP Configuration on E1: Neighborships Configured

```
! Configuration on router E1
router bgp 11
 neighbor 10.1.1.2 remote-as 1
```

```
! Next commands are on I1-1
router bgp 1
 neighbor 10.1.1.1 remote-as 11
```

دستورات مانیتورینگ :

Router # Show IP BGP Summary

Router # Show IP BGP Neighbor

نحوه تعریف Router – ID در پروتکل BGP :

Router (config – router) # BGP Router – ID A.B.C.D

Highset up/up Loopback IP – Address

Highset up/up non – Loopback IP – Address

نکته :

در BGP روتر همسایه با IP – Address آن روتر نمایش داده می شود نه با Router – ID

پارامترهای تشکیل همسایگی :

- AS – Number که به روتر اول اختصاص داده ایم باید با Remute – AS – number در روتر دوم برابر باشند و برعکس .
- Router – ID در دو روتر همسایه نباید برابر باشند .
- باید حتما امکان برقراری یک اتصال TCP Port در بین دو روتر همسایه وجود داشته باشد تا روی این بستر همسایگی تشکیل شود و همه کارها و پیام ها در BGP بر روی این بستر صورت می گیرد .
- اگر Authentication داشته باشیم باید در بین دو روتر برابر باشد و فقط از متد MD5 می توانیم استفاده کنیم .

دستور Authentication در پروتکل BGP :

Router (config – router)# Neighbor IP – Address Password password

استفاده از چندین اتصال مجزا بین دو روتر همسایه :

بهتر است در بین دو روتر همسایه در EBGP از دو اتصال مجزا استفاده کنیم تا اگر یکی از اتصال ها دچار مشکل شد از اتصال دوم استفاده کنند و همسایگی از بین نرود . در این حالت اگر همسایگی را به صورت قبل که توضیح داده ایم تشکیل دهیم دو همسایگی در بین دو روتر به وجود می آید برای رفع این مشکل از دستورات زیر استفاده می کنیم :

مرحله اول :

BGP neighbor remote-as Command

```
Router(config-router)#
neighbor {ip-address | peer-group-name}
remote-as autonomous-system
```

مرحله دوم :

BGP neighbor update-source Command

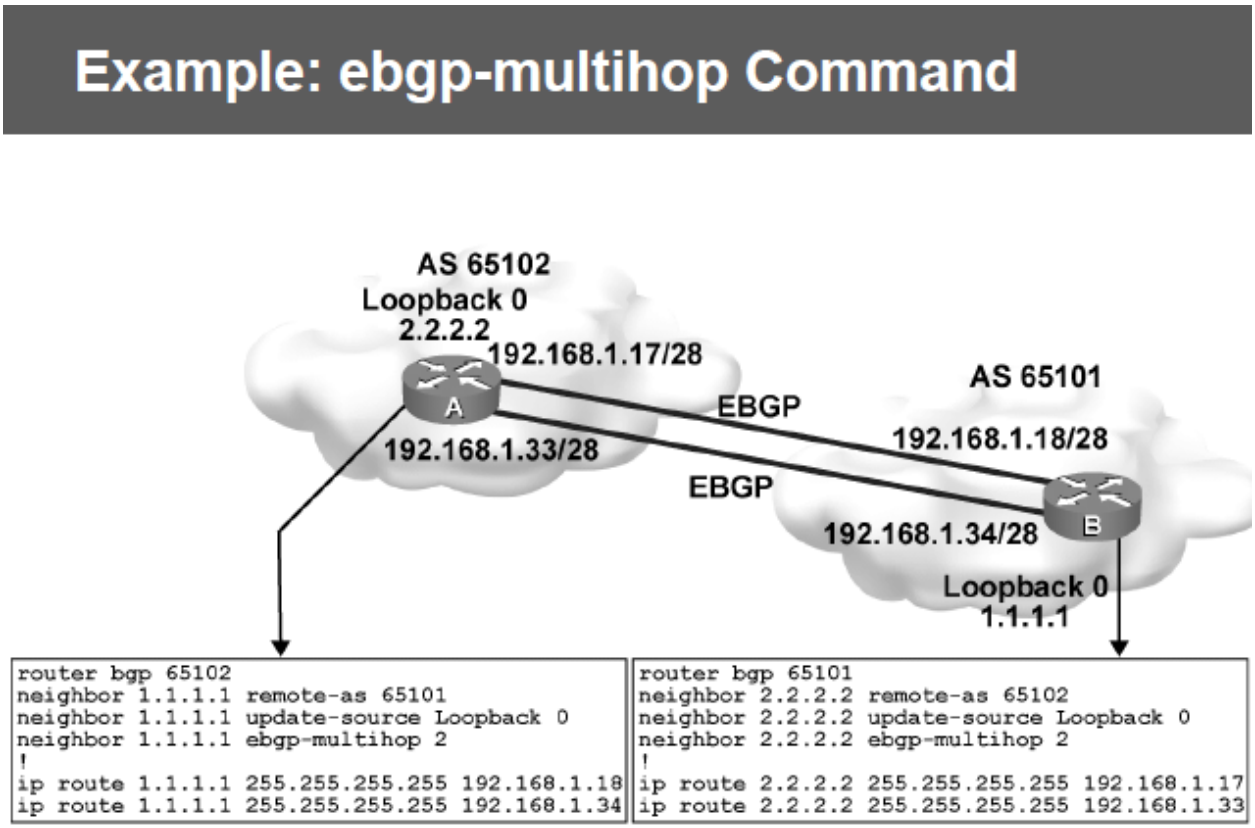
```
Router(config-router)#
neighbor {ip-address | peer-group-name} update-source
interface-type interface-number
```

مرحله سوم :

BGP neighbor ebgp-multihop Command

```
Router(config-router)#
neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]
```

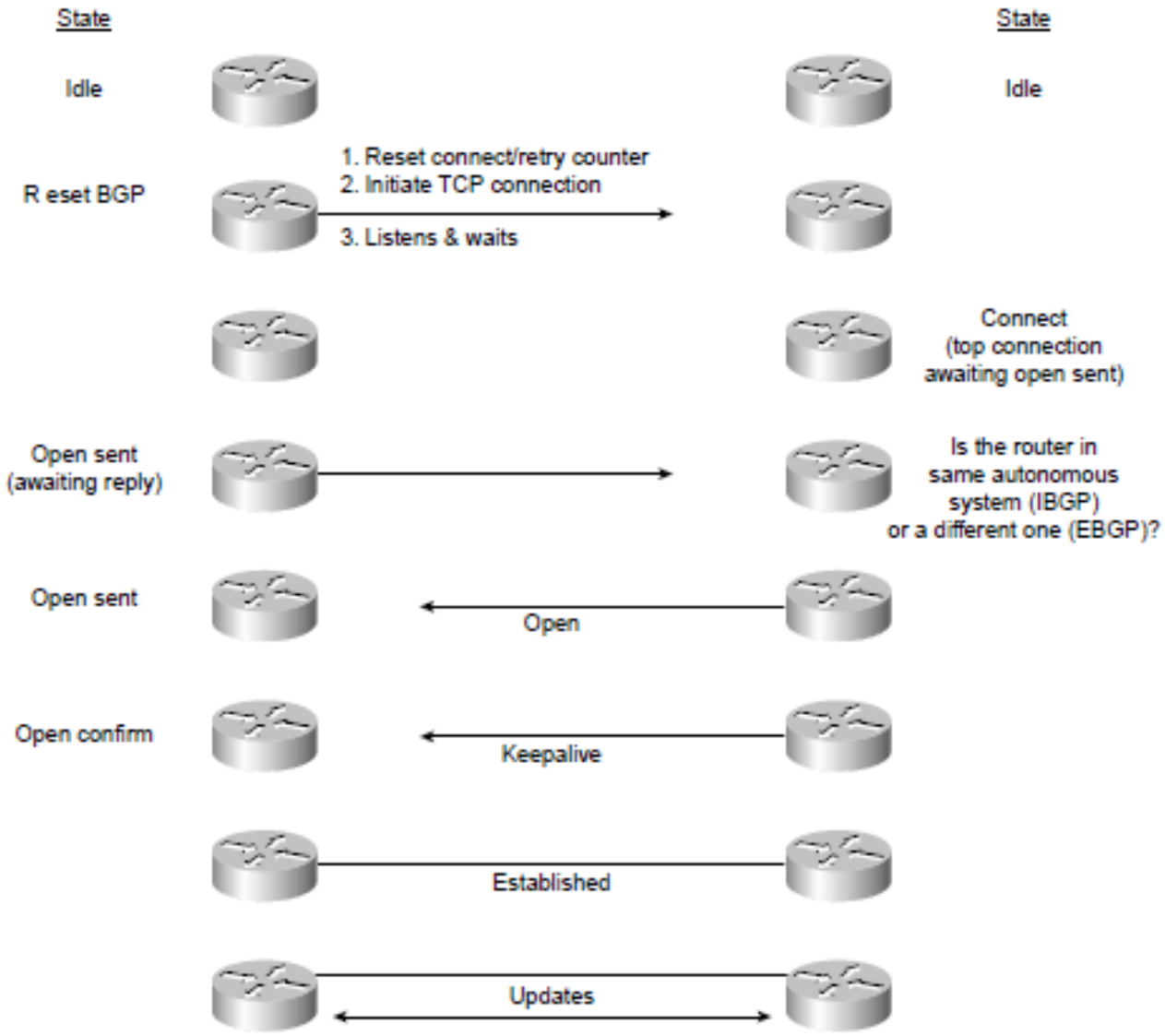
مثال :



اگر به شکل بالا دقت کنید دستور **Neighbor IP – Address ebgp – multihop [ttl]** اشاره به ویژگی EBGP Multihop دارد . به صورت پیش فرض زمانی که روتر قصد ارسال یک پیام به سمت روتر همسایه EBGP داشته باشد مقدار فیلد (Time – To – Live (TTL را برابر با 1 قرار میدهد. با این تنظیمات پیش فرض برقراری رابطه مجاورت EBGP مابین دو روتر با استفاده از Interface Loopbackها با شکست مواجه خواهد شد . زیرا در صورتی که پاکتی با مقدار TTL برابر با 1 به دست روتر همسایه برسد مقدار آن به صفر کاهش پیدا میکند و پیام قبل از پردازش از بین خواهد رفت .

اجرای دستور **Neighbor ... ebgp – multihop 2** باعث برطرف شدن این مشکل می گردد . این دستور روترها را مجبور می کند مقدار TTL مربوط به پیام های ارسالی را به جای 1 برابر با 2 قرار دهند . بدین ترتیب روتر دریافت کننده بعد از کاهش دادن یک واحدی TTL می تواند پیام را به سمت Interface Loopback خود ارسال کند .

مراحل همسایگی :



Idle : این حالت بیانگر آن است که هنوز پروسه مربوط به برقراری رابطه مجاورت BGP آغاز نشده و یا روترها سعی در آغاز دوباره آن خواهند داشت .

Connect : بروز این وضعیت بیانگر آن است که برقراری اتصال TCP آغاز شده اما هنوز به اتمام نرسیده است.

Active : این حالت بیانگر آن است که پروسه برقراری اتصال TCP به اتمام رسیده اما هیچ پیام BGP بین روترها مبادله نشده است .

Opensent : در این حالت پیام Open به روتر همسایه ارسال شده است اما روتر همسایه هنوز پیام Open خود را به این روتر نفرستاده است .

Openconfirm : در این مرحله هر دو روتر همسایه اقدام به ارسال پیام های Keepalive به یکدیگر می کنند و در صورت برابر بودن پارامترهای همسایگی رابطه مجاورت تشکیل می شود . اما اگر این پارامترها در روی دو روتر با هم متفاوت باشند به جای پیام Keepalive پیام Notification فرستاده خواهد شد .

Established : وضعیت نهایی یک ارتباط BGP را نمایش می دهد . بدین ترتیب روترها اقدام به برقراری رابطه مجاورت با یکدیگر کرده و پیام های BGP Update را برای هم ارسال می کنند .

کنترل وضعیت روتر همسایه :

میتوانیم یک روتر همسایه BGP را غیر فعال نماییم . برای انجام این کار باید دستور زیر را اجرا کنیم . اجرای این دستور باعث می شود روتر در حالت Idle قرار بگیرد . برای دوباره فعال سازی روتر کافی است همان دستور را با No اجرا کنیم :

BGP neighbor shutdown Command

```
Router(config-router)#
neighbor {ip-address | peer-group-name} shutdown
```

- Administratively brings down a BGP neighbor
- Used for maintenance and policy changes to prevent route flapping

```
Router(config-router)#
no neighbor {ip-address | peer-group-name} shutdown
```

- Re-enables a BGP neighbor that has been administratively shut down

دستورات مانیتورینگ :

Router # Debug IP BGP

Router # Show TCP Brife

نکته :

در پروتکل BGP برای تشکیل همسایگی بین دو روتر لازم نیست با هم در حالت Connect باشند. چون از بستر TCP استفاده می کنند فقط کافی است دو روتر یکدیگر را ببینند یعنی مسیری به یکدیگر داشته باشند همسایگی تشکیل می دهند .

BGP Table :

هر مسیری که وارد BGP Table روتر شود , روتر به همسایه ها خبر می دهد .

با دستور زیر می توانیم BGP Table را ببینیم :

```
Router # Show  IP  BGP
```

ارسال آدرس های داخل یک سازمان به محیط اینترنت با استفاده از BGP :

از دو روش زیر استفاده می کنیم :

- روش اول : استفاده از دستور Network

اجرای دستور Network باعث خواهد شد مقایسه ای مابین پارامترهای نوشته شده در دستور Network و محتویات جدول Routing صورت گیرد . در صورتی که تطابق کاملی مابین آدرس و ماسک نوشته شده در آن دستور با routeهای واقع در جدول Routing وجود داشته باشد همان route در داخل جدول BGP Table در روی همان روتر قرار خواهد گرفت. این مطلب زمانی صحت دارد که از Auto – Summary No استفاده کرده باشیم .

در حالت پیش فرض Auto – Summary No است .

```
Router ( config – Router )# Network  IP – Address  Mask  subnet-mask

Router ( config – Router )# No  Auto – Summary
```

اما اگر دستور Auto – Summary را وارد کنیم و از نوشتن پارامتر Mask در دستور Network خودداری کنیم در صورتی که subnetهای زیرمجموعه همان آدرس با کلاس استاندارد در داخل جدول Routing وجود داشته باشد روتر اقدام به قرار دادن شبکه با کلاس استاندارد در داخل جدول BGP خواهد کرد .

Router (config – Router)# Network IP – Address

Router (config – Router)# Auto – Summary

- روش دوم : انجام پروسه Redistribution از IGP به داخل BGP

میتوانیم از Redistribution برای انتشار routeهای مربوط به یک سازمان به محیط اینترنت استفاده کرد .
هدف از این روش :

1. انتشار آدرس های Public مربوط به سازمان و جلوگیری از انتشار آدرس های Private
2. انتشار یک route مادر به جای تمامی Subnetهای زیر مجموعه آن

مثال :

Router (config) # Router BGP 1

Router (config – Router)# Redistribute OSPF 1 Route – Map Cisco

باید یک Route – Map بنویسیم تا همه مسیرها را نیاورد :

Router (config) # IP Prefix – List 1 Permit 182.168.0.0/22 ge 24 le 24

Router (config) # Route – Map Cisco permit 10

Router (config – Route – Map)# Match IP Address Prefix – List 1

به سه روش می توانیم مسیرهایی را که به BGP می فرستیم Summary کنیم :

روش اول : به صورت Summary آدرس ها را بگیرد و بفرستد

OSPF → آدرس ها → 182.168.0.0./22 → Network 182.168.0.0 Mask 255.255.255.0

روش دوم : به صورت چند مسیر بگیرد و به صورت یک Default Route بفرستد

OSPF → آدرس ها
- IP – Route 182.168.0.0 255.255.255.0 Null 0
- Network 182.168.0.0 Mask 255.255.255.0

روش سوم : به صورت چند مسیر می گیرد و خود BGP به حالت Summary در می آورد .

OSPF → Router (config – router) # Aggregate – Address IP-Address subnet-mask Summary – Only

مقدار AD در پروتکل eBGP برابر با عدد 20 است. به جدول زیر دقت کنید :

Default Administrative Distances

Route Type	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
eBGP	20
EIGRP (internal)	90

تشکیل همسایگی در روترهای iBGP :

دستور کلی :

Router (config) # Router BGP As – number

Router(config – router)# Neighbor IP–Address Remote – As Remute – As – Number

خصوصیات iBGP :

- مقدار As – number هر دو دستور بالا با هم برابر است زیرا در یک As می خواهیم همسایگی تشکیل دهیم .
- پروتکل BGP مسیرهایی را که از طریق iBGP می گیرد در جدول BGP در ابتدا آنها یک حرف i می گذارد ولی جلوی مسیرهای eBGP هیچ علامتی نمی گذارد .
- مقدار AD مسیرهای iBGP برابر با 200 است .
- در iBGP مقدار TTL همان برابر با 1 است و تغییر نمی دهیم .
- Next – Hop مسیرهایی که از طریق iBGP می گیرد از روتری که گرفته تا خود روتر تغییری نمی کند و ثابت است . باید Next – Hop روتری که مسیر iBGP را فرستاده تغییر دهیم و Next – Hop خودش را بنویسیم .

با دستور زیر این کار را انجام می دهیم :

Router(config – router)#Neighbor IP-Address Next – Hop – Self

IP-Address: آدرس IP اینترفیس روتری که همسایگی iBGP را تشکیل داده است را مینویسیم

نکته :

می توانیم همسایگی را مثل eBGP با اینترفیس های Loopback نیز تشکیل دهیم . حتما باید روی روترهای مرزی Next – Hop – Self را تعریف کنیم تا روترهای داخلی از طریق Next – Hop روتر مرزی به بیرون دسترسی داشته باشند .

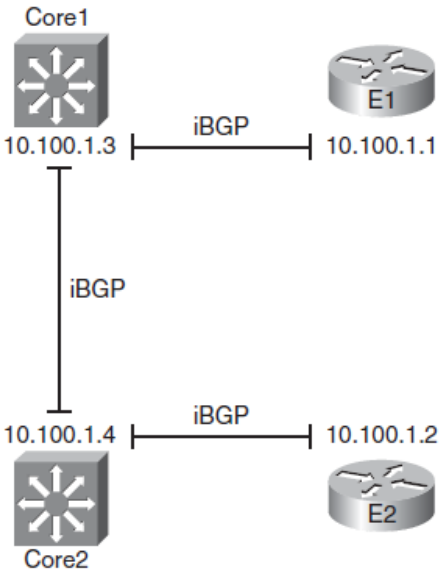
نکته :

همانطور که در جدول زیر مشاهده می کنید مقدار AD مسیرهای iBGP برابر با عدد 200 در جدول Default Administrative Distances است .

Default Administrative Distances

Route Type	Administrative Distance
IGRP	100
OSPF	110
IS-IS	115
RIP	120
On-Demand Routing (ODR)	160
EIGRP (external)	170
iBGP	200
Unreachable	255

مثال : به شکل زیر دقت کنید با برقراری رابطه مجاورت iBGP مابین تک تک روترهای داخلی واقع در As 11 تمامی آنها به صورت مستقیم قادر به دریافت اطلاعات از همدیگر بوده چون بر اساس قانون زمانی که یک روتر اقدام به دریافت پیامی از روتر iBGP می کند همان پیام را به سمت روترهای iBGP دیگر نخواهد فرستاد تا از بروز چرخه لایه 3 جلوگیری شود .



Partial Mesh of iBGP Peers

در شکل صفحه قبل هر چهار روتر در As 11 قرار دارند و روترهای E1 و E2 روترهای مرزی هستند . روتر E1 در بیرون از منطقه As 11 به شبکه 181.0.0.0/8 نزدیکتر است و ارتباط مستقیم دارد و روتر E2 در بیرون از منطقه As 11 به شبکه 192.135.250.0/28 نزدیکتر است و ارتباط مستقیم دارد. اگر بخواهیم که روترهای داخلی از اطلاعات یکسانی در داخل جدول BGP خود برخوردار باشند باید اقدام به اجرای یک توپولوژی Full Mesh مابین آنها نماییم . در نتیجه این کار شش رابطه مجاورت iBGP مابین 4 دستگاه موجود ایجاد خواهد شد .

مثال زیر بیان کننده پیکربندی روترهای E1 و Core1 می باشد :

Core2–E1 and Core1 Only

```
! First, E1's configuration
router bgp 11
 neighbor 10.100.1.2 remote-as 11
 neighbor 10.100.1.2 update-source loopback0
```

```
 neighbor 10.100.1.2 next-hop-self
!
 neighbor 10.100.1.3 remote-as 11
 neighbor 10.100.1.3 update-source loopback0
 neighbor 10.100.1.3 next-hop-self
!
 neighbor 10.100.1.4 remote-as 11
 neighbor 10.100.1.4 update-source loopback0
 neighbor 10.100.1.4 next-hop-self
```

```
! Next, Core1's configuration
interface loopback0
 ip address 10.100.1.3 255.255.255.255
!
router bgp 11
 neighbor 10.100.1.1 remote-as 11
 neighbor 10.100.1.1 update-source loopback0
!
 neighbor 10.100.1.2 remote-as 11
 neighbor 10.100.1.2 update-source loopback0
!
 neighbor 10.100.1.4 remote-as 11
 neighbor 10.100.1.4 update-source loopback0
```

همین دستورها را بر روی روترهای E2 و Core2 نیز وارد می کنیم . اگر دقت کنید میبینید که دستور Next – Hop – Self را فقط بر روی روتر E1 وارد کرده ایم یعنی فقط باید این دستور را بر روی روترهای مرزی (E1 و E2) وارد کنیم .

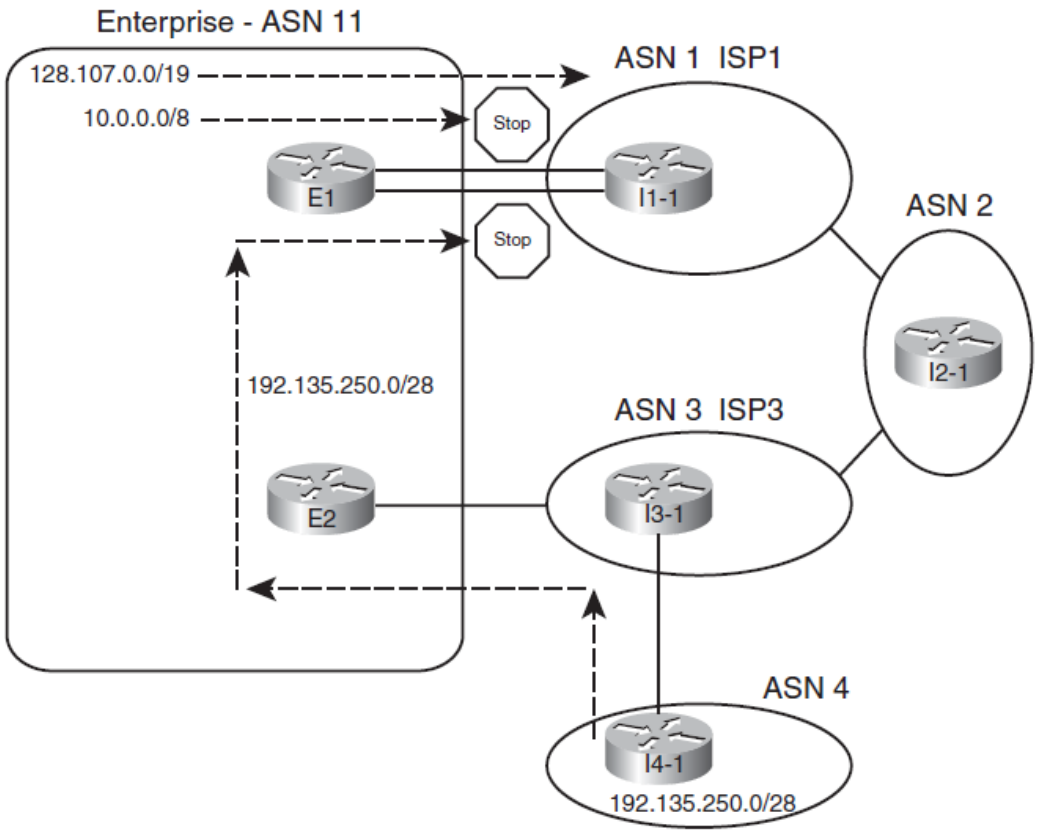
مثال زیر نشان دهنده محتویات جدول BGP در روی روتر Core1 بعد از اعمال پیکربندی های نشان داده شده در سناریوی قبل می باشد :

BGP Table on Router Core1

```
Core-1# show ip bgp
BGP table version is 10, local router ID is 10.100.1.3
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
r i0.0.0.0          10.100.1.2               0    100      0 3 i
r>i                 10.100.1.1               0    100      0 1 i
* i128.107.0.0/19   10.100.1.2               0    100      0 i
*>i                 10.100.1.1               0    100      0 i
*>i181.0.0.0/8      10.100.1.1               0    100      0 1 2 111 112 i
*>i182.0.0.0/8      10.100.1.1               0    100      0 1 2 222 i
*>i183.0.0.0/8      10.100.1.1               0    100      0 1 2 i
*>i184.0.0.0/8      10.100.1.1               0    100      0 1 2 i
*>i185.0.0.0/8      10.100.1.1               0    100      0 1 2 i
*>i192.135.250.0/28 10.100.1.2               0    100      0 3 4 i
```

اطلاعات بالا نشان می دهد که روتر E1 بهترین مسیر برای دسترسی به شبکه 181.0.0.0/8 و روتر E2 نیز به عنوان بهترین نقطه دسترسی به شبکه 192.135.250.0/28 انتخاب شده اند . در نتیجه روتر Core1 تنها از وجود یک مسیر نهایی به سمت هر کدام از این شبکه ها مطلع خواهد شد . همچنین با بررسی آدرس های Next – Hop در می یابیم که آدرس Next – Hop در مورد شبکه 192.135.250.0/28 برابر با 10.100.1.2 (یعنی روتر E2) و آدرس Next – Hop در مورد شبکه 181.0.0.0/8 برابر با 10.100.1.1 (یعنی روتر E1) قرار داده شده است .

BGP Filtering



The Need for Enterprise BGP Filtering

پروتکل BGP امکان اعمال فیلتر بر روی پیام های Update را در روی تمامی روترها فراهم ساخته است . یعنی یک روتر BGP می تواند به ازای هر کدام از روترهای همسایه خود اقدام به فیلتر بر روی ترافیک ورودی (Inbound) و یا خروجی (Outbound) نماید . در صورت پیکربندی یک فیلتر BGP در روی روتر تمامی ارتباطات مجاورت BGP را در روی همان روتر یک بار Reload می کنیم فیلتر مزبور بر روی پیام ها اعمال گردد .

با سه روش می توانیم Filtering را اجرا کنیم :

- روش اول Prefix – List :

دستور کلی فیلتر کردن با Prefix – List :

Router (config – router) # Neighbor IP-Neighbor Prefix – List name { in | out }

مثال : با توجه به شکل صفحه قبل این دستورات را می نویسیم :

Router E1 (config) # IP Prefix – List Cisco seq 5 Permit 128.107.0.0/19

Router E1 (config) # IP Prefix – List Cisco seq 10 Deny 10.0.0.0/8

Router E1 (config) # IP Prefix – List Cisco seq 15 Deny 192.135.250.0/28

Router E1 (config) # Router BGP 11

Router E1 (config – router) # Neighbor 1.1.1.1 Prefix – List Cisco Out

با اعمال دستورات بالا بر روی روتر E1 اطلاعات ارسالی به روتر 1-1 فیلتر می شود . یعنی فقط اطلاعات شبکه 128.107.0.0/19 اجازه خروج از روتر E1 را دارد و شبکه های دیگر از جمله شبکه های 10.0.0.0/8 و 192.135.250.0/28 فیلتر شده و اجازه خروج از روتر E1 را ندارند . بنابراین روتر 1-1 نمی تواند از As 11 برای رسیدن به این شبکه ها استفاده کند و در نتیجه پهنای باند این سازمان (As 11) در اختیار ترافیک دیگران قرار نمی گیرد . بعد از اعمال دستورات بالا باید حتما یک بار روتر E1 را Reload کنیم . با استفاده از دستور زیر این کار را انجام می دهیم :

Router # Clear IP BGP *

روش دوم Access – List :

دستور کلی فیلتر کردن با Access – List :

Router (config – router) # Neighbor IP-Neighbor Distribute – List { ACL-name | ACL-number } { in | out }

مثال : با توجه به شکل صفحه قبل این دستورات را می نویسیم :

Router E1 (config) # Access – List 1 Deny 10.0.0.0 0.255.255.255

Router E1 (config) # Access – List 1 Deny 192.135.250.0 0.0.0.255

Router E1 (config) # Access – List 1 Permit any

Router E1 (config) # Router BGP 11

Router E1 (config – router) # Neighbor 1.1.1.1 Distribute – List 1 Out

روش سوم Route – Map :

مثال : با توجه به شکل صفحه قبل این دستورات را می نویسیم :

```
Router E1 ( config ) # IP  Prefix – List   2      Permit  10.0.0.0/8
Router E1 ( config ) # IP  Prefix – List   2      Permit  192.135.250.0/28
Router E1 ( config ) # Route – Map    Cisco      Deny  10
Router E1 ( config- Route – Map ) #Match  IP  Address  Prefix – List   2
Router E1 ( config- Route – Map ) # Exit
Router E1 ( config ) # Route – Map    Cisco      Permit    20
Router E1 ( config- Route – Map ) # Exit
Router E1 ( config ) # Router  BGP   11
Router E1 ( config – router ) # Neighbor   1.1.1.1   Route – Map    Cisco     Out
```

Clearing BGP Neighbors

دستوری که برای ریست کردن رابطه مجاورت مابین روترهای BGP مورد استفاده قرار می گیرد Clear IP BGP است . البته این دستور دارای پارامترهای دیگری نیز می باشد که نحوه انجام این ریست را تعیین می کنند .زمانی که دستور فوق باعث قطع رابطه TCP مابین دو روتر BGP شده و روترهای دخیل اقدام به حذف BGP routeهای دریافت شده از یکدیگر از داخل جدول BGP خود نمایند این روش به عنوان Hard Reset نامیده می شود . اما روشی دیگر وجود دارد به نام Soft Reset که باعث قطع ارتباط TCP و یا حذف رابطه مجاورت مابین روترها نمی شود .بدین ترتیب یک دستگاه اقدام به ارسال دوباره محتویات جدول BGP خود به روتر همسایه مزبور کرده ولی این بار قبل از هر عمل دیگر فیلتر تعیین شده را بر روی آنها اعمال میکند. در صورت تعیین شدن یک فیلتر ورودی نیز روتر مجبور خواهد بود تا تمامی پیام های دریافتی را یکبار دیگر از فیلتر تعیین شده عبور داده و سپس جدول BGP خود را به روز نماید .

جدول زیر نسخه های مختلفی از دستور Clear IP BGP و نحوه تأثیرگذاری آنها را نشان میدهد :

BGP clear *Command Options*

Command	Hard or Soft	One or All Neighbors	Direction (in or out)
clear ip bgp *	Hard	all	both
clear ip bgp *neighbor-id*	Hard	one	both
clear ip bgp *neighbor-id* out	Soft	one	out
clear ip bgp *neighbor-id* soft out	Soft	one	out
clear ip bgp *neighbor-id* in	Soft	one	in
clear ip bgp *neighbor-id* soft in	Soft	one	in
clear ip bgp * soft	Soft	all	both
clear ip bgp *neighbor-id* soft	Soft	one	both

Router # Clear IP BGP *

به این حالت Hard Reset می گویند.روتر در این حالت همه مسیرهای خود را پاک می کند بعد Update می کند و در آخر ارسال می کند.در این حالت همسایگی از بین می رود و دوباره تشکیل می گردد .

Router # Clear IP BGP neighbor - id

در این حالت فقط با یک روتر همسایه که مشخص کرده ایم جدول خود را پاک می کند و دوباره ارسال می کند . در این حالت همسایگی از بین می رود و دوباره تشکیل می گردد .

Router # Clear IP BGP neighbor – id out

به این حالت Soft Reset می گویند .در این حالت همسایگی برقرار است فقط مسیرهایی که به روتر همسایه ارسال می کند را پاک کرده و دوباره ارسال می کند .

Router # Clear IP BGP neighbor – id in

به این حالت Soft Reset می گویند .در این حالت همسایگی برقرار است فقط مسیرهای ورودی را پاک می کند و درخواست دوباره ارسال مسیرها را از روتر همسایه می کند و به این مکانیزم Route – Refresh می گویند .

Router # Clear IP BGP neighbor – id Soft in

این دستور همام دستور بالا است که در گذشته از آن استفاده می شد . در این حالت نمی تواند روتر از روتر همسایه درخواست دوباره ارسال مسیر بکند . قبلا یک حافظه داشتند که ورژن قبل و بعد دستور Clear را در خود ذخیره می کرد و باید دستور زیر را وارد می کردیم تا یک ورژن قدیمی قبل از دستور Clear را ذخیره می کرد :

Router (config – router) # Neighbor neighbor – id Soft – Reconfiguration inbaund

از این روش دیگر استفاده نمی شود .

Router # Clear IP BGP Soft

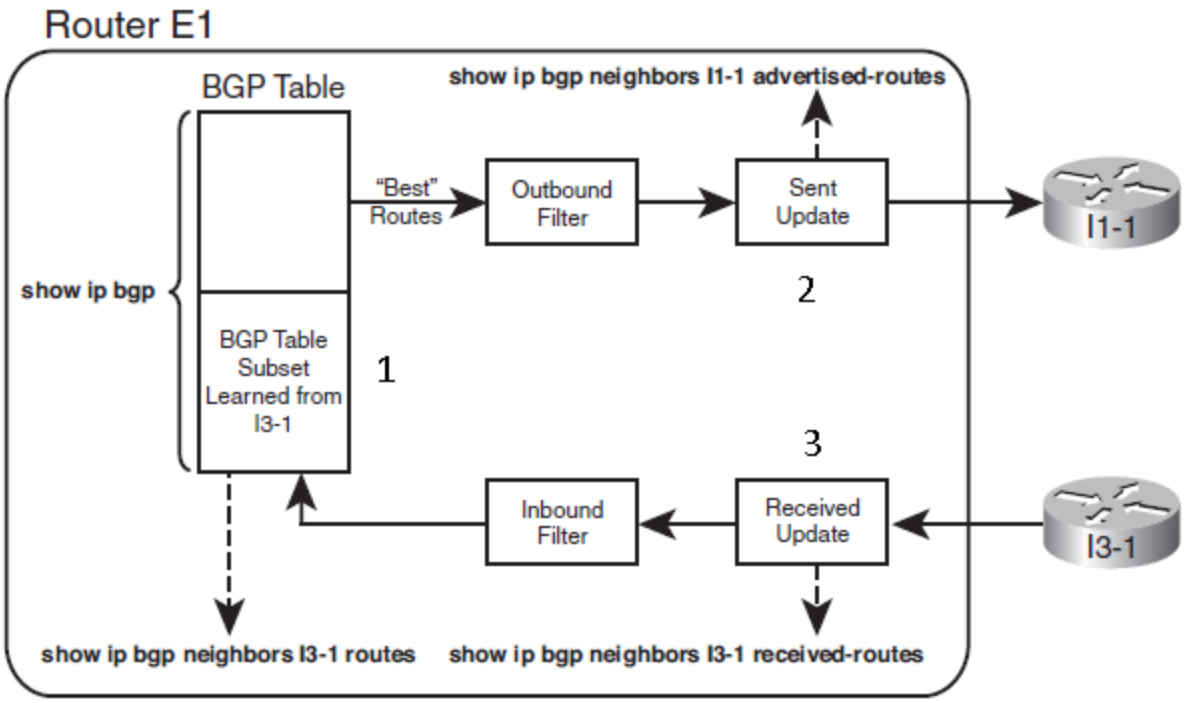
در این حالت با همه روترها همسایگی را قطع می کند و دوباره تشکیل می دهد و اطلاعات را ارسال می کند .

Router # Clear IP BGP neighbor – id Soft

مثل حالت بالا است فقط با یک روتر این کار را انجام می دهد .

بهتر است بیشتر از Soft Reset استفاده کنیم تا از Hard Reset استفاده کنیم .

استفاده از دستور Show در BGP برای مشاهده انواع مسیرها :



show *Commands Related to BGP Filtering*

برای مشاهده ناحیه 1 از دستور زیر استفاده می کنیم :

Router # Show IP BGP Neighbor neighbor-id Routes

برای مشاهده ناحیه 2 از دستور زیر استفاده می کنیم :

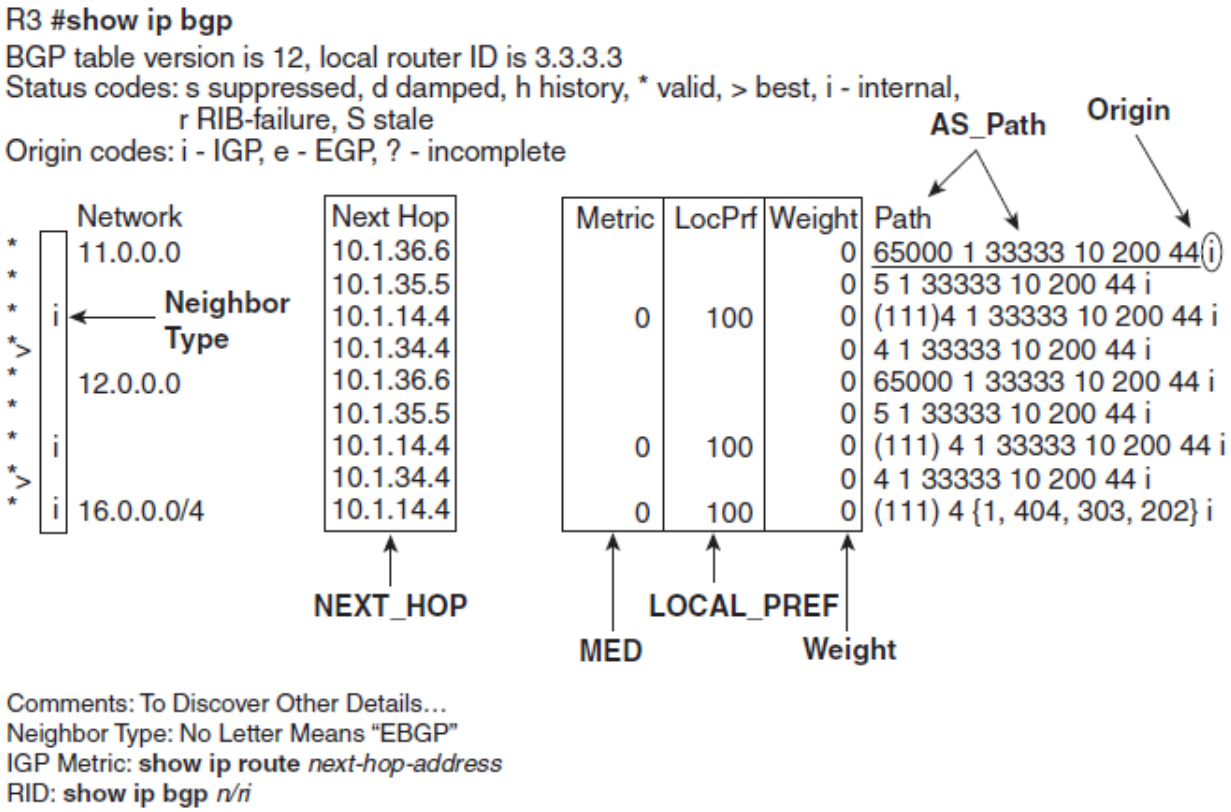
Router # Show IP BGP Neighbor neighbor-id Advertised – Routes

برای مشاهده ناحیه 3 از دستور زیر استفاده می کنیم :

Router # Show IP BGP Neighbor neighbor-id Recived – Routes

BGP Path Attributes

پروتکل مسیریابی BGP بر اساس یکسری Attribute (خصوصیات) قادر به تعیین بهترین مسیر برای هر مقصد می باشد .



BGP Attributes شامل موارد زیر می باشد :

- AS – Path
- Next – Hop
- ORIGIN
- Local – Preference
- MED
- Others

اصول الگوریتم انتخاب بهترین مسیر در BGP :

مراحلی که یک روتر BGP برای انتخاب بهترین مسیر ممکن برای دسترسی به شبکه ها طی می کند در جدول زیر نمایش داده شده است :

Route Selection Decision Process

Consider only (synchronized) routes with no AS loops and a valid next hop, and then:

1. Prefer highest weight (local to router).
2. Prefer highest local preference (global within AS).
3. Prefer route originated by the local router (next hop = 0.0.0.0).
4. Prefer shortest AS path.
5. Prefer lowest origin code (IGP < EGP < incomplete).
6. Prefer lowest MED (exchanged between autonomous systems).
7. Prefer EBGP path over IBGP path.
8. Prefer the path through the closest IGP neighbor.
9. Prefer oldest route for EBGP paths.
10. Prefer the path with the lowest neighbor BGP router ID.
11. Prefer the path with the lowest neighbor IP address.

1. Prefer highest Weight

Weight یک عدد از 0 تا 65535 می باشد که پیش فرض مقدار آن 0 است . Weight مسیرهایی که به یک روتر وصل هستند برابر است با 32768 در همان روتر ولی در روترهای همسایه Weight آنها برابر با 0 است . اگر بخواهیم مسیری را به عنوان بهترین مسیر انتخاب کنیم از طریق بالا بردن مقدار Weight به وسیله نوشتن route – map این کار را انجام می دهیم .

مثال :

Router (config) # IP Prefix – List 1 Permit 192.168.1.0/24

Router (config) # Route – Map Cisco Permit 10

Router (config- Route – Map) # Match IP Address Prefix – List 1

```
Router ( config- Route – Map ) # Set   Weight   200
Router ( config- Route – Map ) # Exit
Router ( config ) # Route – Map    Cisco      Permit    20
Router ( config- Route – Map ) # Exit
Router ( config ) # Router  BGP   1
Router ( config – router ) # Neighbor   1.1.1.1   Route – Map    Cisco     in
```

دستور صادر کردن یک حکم کلی برای یک همسایه که هر مسیری را از آن یاد گرفته Weight آن مسیرها را بالا می برد و اولویت می دهد :

```
Router ( config ) # Router  BGP   1
Router ( config – router ) # Neighbor   neighbor-id   Weight   number
```

2. Prefer highest Local Preference

در صورت یکسان بودن مقدار Weight و یا set نشدن این مقدار از Local Preference استفاده خواهد شد و مسیری که Local Preference بالاتری داشته باشد به عنوان بهترین مسیر انتخاب می شود و به تمام روترهای دیگر نیز خبر می دهد تا بدانند این مسیر بهترین مسیر است . مقدار عددی آن در iBGP برابر با 100 است و در eBGP مقدار عددی ندارد .

از عدد 0 تا 2^{32} -1 را می توانیم برای Local Preference انتخاب کنیم .

با دستور زیر Local Preference را تعیین می کنیم :

```
Router ( config- Route – Map ) # Set   Local – Preference   number
```

مثال :

```
Router ( config ) # IP  Prefix – List  1      Permit  14.0.0.0/30

Router ( config ) # Route – Map    Cisco      Permit  10

Router ( config- Route – Map ) # Match  IP  Address  Prefix – List  1

Router ( config- Route – Map ) # Set  Local – Preference    200

Router ( config- Route – Map ) # Exit

Router ( config ) # Route – Map    Cisco      Permit    20

Router ( config- Route – Map ) # Exit

Router ( config ) # Router  BGP  1

Router ( config – router ) # Neighbor  11.0.0.9  Route – Map    Cisco     out
```

نکته :

Local – Preference فقط برای روترهای داخلی شبکه iBGP کار می کند . برای روترهای خارجی شبکه eBGP کار نمی کند و مقدار آن 0 است .

3. Prefer Route Originated By The Local Router

در صورتی که مسیرها دارای Weight و Local – Preference یکسانی باشند مسیرهایی که خود روتر آنها را ایجاد کرده (یعنی Connected یا خودش به دیگر روترها یاد داده) دارای اولویت نسبت به دیگر مسیرها می باشند .

4. Prefer Shortest AS – Path

یعنی تعداد AS هایی را که از آن رد شده را به عنوان معیار در نظر می گیرد . هرگاه برای رسیدن به یک مسیر از ASهای کمتری عبور کند آن مسیر به عنوان بهترین مسیر به وسیله BGP انتخاب می شود . می توانیم یک مسیر دیگری که با AS – Path بیشتری در جدول قرار دارد را به عنوان بهترین مسیر انتخاب کنیم . با این روش که مقدار AS – Path مسیری که BGP به عنوان بهترین مسیر انتخاب کرده را از مقدار AS – Path مسیری که ما می خواهیم به عنوان بهترین مسیر انتخاب شود را بیشتر کنیم . نمی توانیم از عددهایی غیر از خود عدد AS برای بالا بردن مقدار آن استفاده کنیم باید همان شماره AS را با تعداد بیشتر

وارد کنیم مثلا برای AS 2 می توانیم با وارد کردن عدد 22222 مقدار AS – Path آن مسیر را افزایش دهیم .

دستور کلی :

Router (config- Route – Map) # Set AS – Path #####...

مثال :

Router (config) # IP Prefix – List 1 Permit 181.0.0.0/8

Router (config) # Route – Map Cisco Permit 10

Router (config - Route – Map) # Match IP Address Prefix – List 1

Router (config - Route – Map) # Set AS – Path 22222

Router (config - Route – Map) # Exit

Router (config) # Route – Map Cisco Permit 20

Router (config - Route – Map) # Exit

Router (config) # Router BGP 1

Router (config – router) # Neighbor 12.0.0.2 Route – Map Cisco in

5. Prefer Lowest Origin Code

در صورت یکسان بودن تعداد ASها از Origin Code استفاده می شود . در این حالت ابتدا مسیر i معادل IGP و سپس مسیر e معادل eBGP و سپس ? معادل Incomptete اولویت خواهد داشت .

6. Prefer Lowest MED (Multi – Exit Discriminatore)

در صورت یکسان بودن کلیه موارد فوق از MED استفاده می شود .هر مسیری که دارای مقدار MED کمتری باشد به عنوان بهترین مسیر انتخاب می شود . در این روش به روترهای دیگر پیشنهاد می دهید که این مسیرهایی که به شبکه من وصل هستند MED آنها این مقدار است و سپس روترهای دیگر اگر در 5 مورد قبلی با هم یکسان باشند به پیشنهاد روتر گوش می کنند و از مسیری که MED کمتری داشته باشد وارد شبکه آن روتر می شوند . مقدار پیش فرض MED برابر با 0 است .MED مانند متریک است هرچه کمتر باشد آن مسیر بهتر است .

دستور تغییر MED مسیر :

Router (config- Route – Map) # Set MED number

مثال :

```
Router ( config ) # IP Prefix – List 1 Permit 180.0.0.0/8
Router ( config ) # Route – Map A Permit 10
Router ( config- Route – Map ) # Match IP Address Prefix – List 1
Router ( config- Route – Map ) # Set Metric 100
Router ( config- Route – Map ) # Exit
Router ( config ) # Route – Map A Permit 20
Router ( config- Route – Map ) # Exit
Router ( config ) # Route – Map B Permit 10
Router ( config- Route – Map ) # Match IP Address Prefix – List 1
Router ( config- Route – Map ) # Set Metric 200
Router ( config- Route – Map ) # Exit
Router ( config ) # Route – Map B Permit 20
Router ( config- Route – Map ) # Exit
Router ( config ) # Router BGP 1
Router ( config – router ) # Neighbor 11.0.0.2 Route – Map A out
Router ( config – router ) # Neighbor 11.0.0.6 Route – Map B out
```

7. Prefer EBGP Path Over IBGP Path

در صورت یکسان بودن کلیه موارد فوق مسیرهای EBGP نسبت به مسیرهای IBGP اولویت بیشتری خواهند داشت و به عنوان بهترین مسیر انتخاب می شوند .

8. Prefer The Path Through The Closest IGP Neighbor

در این حالت اگر روتری بیشتر یک مسیر داخلی داشته باشد هر کدام که نزدیکتر باشد را به عنوان بهترین مسیر انتخاب می کند .

9. Prefer Oldest Route For EBGP Paths

در صورت یکسان بودن کلیه موارد فوق مسیرهایی که قدیمیترند انتخاب خواهند شد .

10. Prefer The Path With The Lowest Neighbor BGP Router-id

در این حالت مسیری را که از روتری که کمترین Router-id را دارد گرفته به عنوان بهترین مسیر انتخاب می کند .

11. Prefer The Path With The Lowest Neighbor IP-Address

در این حالت مسیری را که کمترین IP-Address را دارد به عنوان بهترین مسیر انتخاب می کند .

دستورات مانیتورینگ BGP :

Example: show ip bgp neighbors Command

```
RouterA#sh ip bgp neighbors
BGP neighbor is 172.31.1.3,  remote AS 64998, external link
  BGP version 4, remote router ID 172.31.2.3
  BGP state = Established, up for 00:19:10
  Last read 00:00:10, last write 00:00:10, hold time is 180, keepalive
interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  7          7
    Notifications:          0          0
    Updates:               13         38
<output omitted>
```

Example: show ip bgp rib-failure Command

```
RouterA# show ip bgp rib-failure
Network            Next Hop                  RIB-failure   RIB-NH Matches
172.31.1.0/24      172.31.1.3          Higher admin distance          n/a
172.31.11.0/24     172.31.11.4         Higher admin distance          n/a
```

- Displays networks that are not installed in the RIB and the reason that they were not installed

Example: BGP Peering

```
RouterA# show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65001
BGP table version is 124, main routing table version 124
9 network entries using 1053 bytes of memory
22 path entries using 1144 bytes of memory
12/5 BGP path/bestpath attribute entries using 1488 bytes of memory
6 BGP AS-PATH entries using 144 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3829 total bytes of memory
BGP activity 58/49 prefixes, 72/50 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd

10.1.0.2        4 65001      11      11      124    0    0 00:02:28        8
172.31.1.3      4 64998      21      18      124    0    0 00:01:13        6
172.31.11.4     4 64999      11      10      124    0    0 00:01:11        6
```

Example: show ip bgp Command

```
RouterA# show ip bgp
BGP table version is 14, local router ID is 172.31.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal, r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.0.0/24      0.0.0.0                  0         32768 i
* i                 10.1.0.2                 0    100      0 i
*> 10.1.1.0/24      0.0.0.0                  0         32768 i
*>i10.1.2.0/24      10.1.0.2                 0    100      0 i
*> 10.97.97.0/24    172.31.1.3                             0 64998 64997 i
*                   172.31.11.4                            0 64999 64997 i
* i                 172.31.11.4              0    100      0 64999 64997 i
*> 10.254.0.0/24    172.31.1.3               0             0 64998 i
*                   172.31.11.4                            0 64999 64998 i
* i                 172.31.1.3               0    100      0 64998 i
r> 172.31.1.0/24    172.31.1.3               0             0 64998 i
r                   172.31.11.4                            0 64999 64998 i
r i                 172.31.1.3               0    100      0 64998 i
*> 172.31.2.0/24    172.31.1.3               0             0 64998 i
<output omitted>
```

Displays networks from lowest to highest

IPv6

یک آدرس IPv6 به طول 128 بیت و در مبنای Hexadecimal یا 16 بوده و به صورت 8 اکتت 16 بیتی که به وسیله یک علامت کولن (:) از هم جدا می شوند نوشته می شود . به مثال زیر توجه کنید :

2340:1111:AAAA:0001:1234:5678:9ABC

برای ساده کردن تایپ یک آدرس IPv6 قوانینی وجود دارد که در برخی مواقع باعث کوتاهتر شدن آن خواهد شد :

- اعداد صفر ابتدای هر اکتت را می توانیم حذف کنیم .

مثال :

2001:0009:104b:0000:0008:0004:3212:809c

به آدرس خلاصه شده زیر توجه کنید :

2001:9:104b:0:8:4:3212:809c

همانطور که مشاهده می کنید صفرهای اول هر اکتت حذف شده و آدرس ساده تر شده است .

- در صورتی که مقدار یک یا چند اکتت برابر با 0000 باشد می توانیم به جای تمامی آنها از (::) بهره گرفت . البته تنها یک بار مجاز به انجام این کار هستیم .

به مثال زیر توجه کنید :

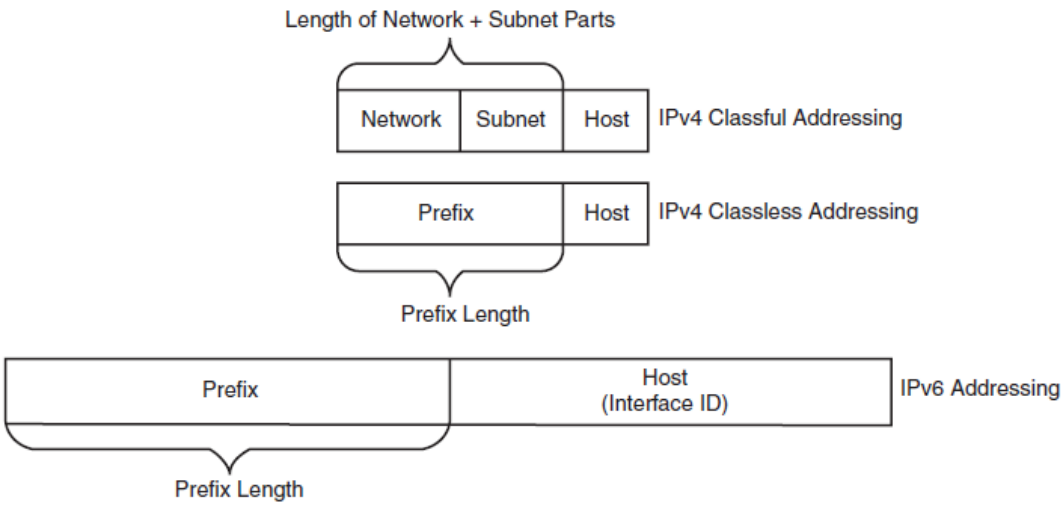
FE00:0000:0000:0001:0000:0000:0000:0056

با استفاده از دو قانون بالا به دو صورت زیر می توانیم آدرس را خلاصه کنیم :

FE00::1:0:0:0:56

FE00:0:0:1::56

قسمت های مختلف یک آدرس IPv6 :



IPv4 Classless and Classful Addressing, IPv6 Addressing

پروتکل IPv6 آدرس ها را تنها به صورت Classless بیان کرده و اصلا ایده ای به نام آدرس های Classful در پروتکل IPv6 وجود ندارد . IPv6 شامل یک Prefix و یک علامت (/) و یک عدد که نشان دهنده طول Prefix خواهد بود می باشد . در IPv6 کلاس بندی نداریم .

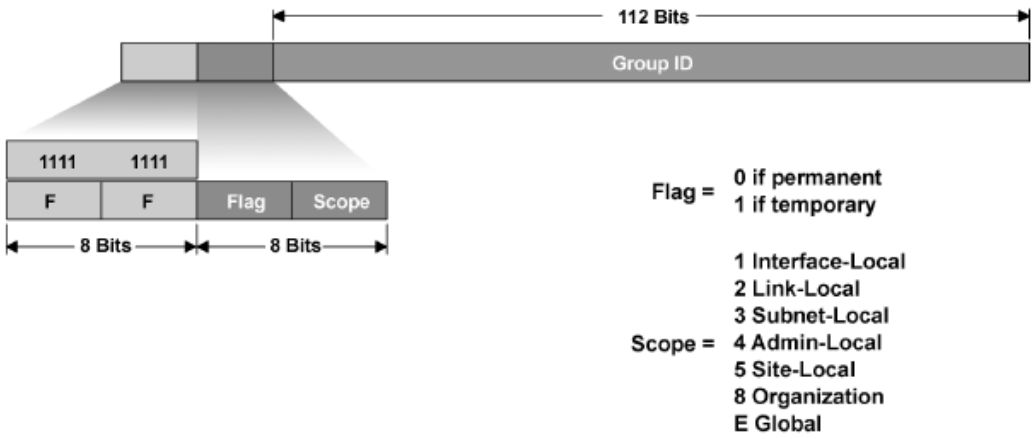
انواع آدرس ها در IPv6 :

- Unicast
- Multicast
- Anycast

Multicast :

یک آدرس Multicast بیان کننده گروهی از دستگاه های مشخص است که یک پیام ارسال شده به سمت این آدرس به تمامی دستگاه های استفاده کننده از آن آدرس تحویل داده خواهد شد . هر آدرسی که با FF شروع شود یک آدرس Multicast است .شکل کلی آدرس Multicast به صورت FF00::/8 می باشد.

Multicasting



همانطور که در شکل بالا مشاهده می کنید یک آدرس Multicast با FF شروع می شود . اگر بعد از FF یعنی در قسمت Flag که در شکل بالا نشان داده شده است عدد 0 باشد به این نوع آدرس Permanent Multicast (دائمی) می گویند . اگر بعد از FF یعنی در قسمت Flag عدد 1 باشد به این نوع آدرس Temporary Multicast (موقتی) می گویند .

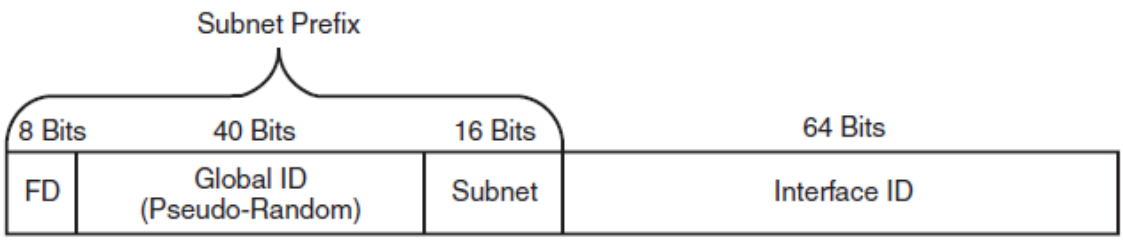
FF00::/12 ⟶ Permanent Multicast

FF10::/12 ⟶ Temporary Multicast

اگر 4 بیت آخر یعنی در قسمت Scope برابر اعداد نمایش داده شده در شکل باشند هر کدام از اعداد نمایانگر یک سری از مشخصات می باشد . مثلا اگر عدد 1 باشد به یک نقطه یا اینترفیس اشاره دارد یا اگر عدد 5 باشد به یک سایت اشاره دارد .

: Unicast

آدرس های Unicast آدرس هایی هستند که فقط برای یک اینترفیس یا یک کارت شبکه ارسال خواهد شد که در این حالت یک بسته اطلاعاتی به آدرس Unicast یک کامپیوتر یا یک Host ارسال خواهد شد .



Unique Local Address Format

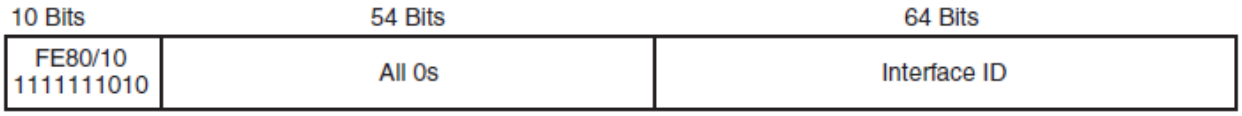
پروتکل IPv6 چندین نوع آدرس Unicast را معرفی کرده که عبارتنداز :

Unique Local Unicast :

آدرس هایی هستند که شکل کلی آنها به صورت FD00::/8 می باشد.

Link Local Unicast :

آدرس هایی هستند که شکل کلی آنها به صورت FE80::/10 می باشد.



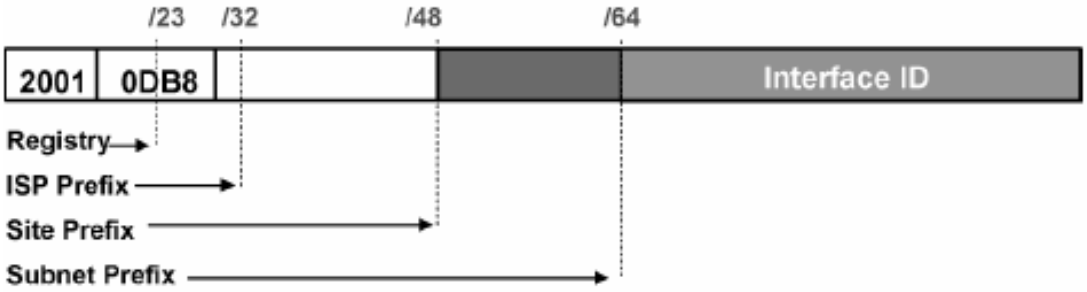
Link Local Address Format

Global Unicast : این آدرس شبیه به Public IP Addressهای IPv4 می باشد و این آدرس ها برای Host ها یا دستگاه هایی که می خواهند به اینترنت متصل شوند استفاده خواهد شد و این آدرس ها توسط سازمان جهانی IANA از طریق نمایندگی های خود در هر قاره به ISPها اختصاص خواهد داد .

ساختار Global Unicast Address از سه بخش به شرح زیر تشکیل شده است :

- Prefix
- Subnet
- Interface Identifie

برای درک بهتر این بخش به تصویر زیر توجه کنید :

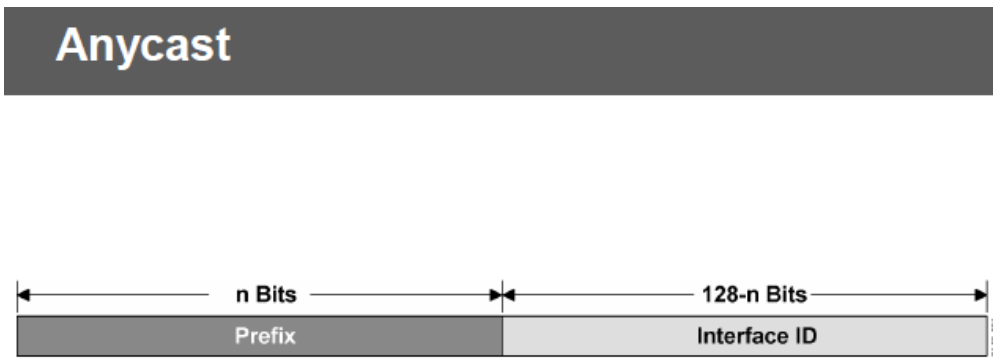


همانطور که مشاهده می کنید قسمت Prefix به چهار بخش به شرح زیر تقسیم شده است :

- Registry که توسط IANA ایجاد خواهد شد .
- ISP Prefix که این بخش توسط نمایندگان IANA ایجاد خواهد شد .
- Site Prefix که این بخش توسط ISPها ایجاد خواهد شد .
- Subnet Prefix که این بخش توسط شرکت ها برای ایجاد زیرشبکه ها استفاده خواهد شد .

Anycast :

این حالت یک آدرس Global Unicast Address به مجموعه ای از اینترفیس ها یا کارت شبکه ها اختصاص داده می شود و پیامی که به آدرس Anycast ارسال شود توسط اولین و نزدیکترین اینترفیس داخل مجموعه Anycast دریافت خواهد شد که در این حالت نزدیکترین اینترفیس به وسیله Routing Protocol بر اساس متریک و Distance شناسایی خواهد شد .



- **An IPv6 anycast address is a global unicast address that is assigned to more than one interface.**

Special Address : شامل آدرس های خاص در IPv6 به شرح زیر می باشد :

آدرس Loopback : این آدرس در IPv6 معادل 1:: می باشد. در IPv4 این آدرس معادل 127.0.0.1 می باشد.

2001:0DB8::/32 : این آدرس برای بیان مثال های آموزشی در Documentها رزرو شده است .

2002::/16 : از این آدرس برای ترجمه آدرس های IPv6 به آدرس های IPv4 استفاده می شود .

IPv6 Assignment :

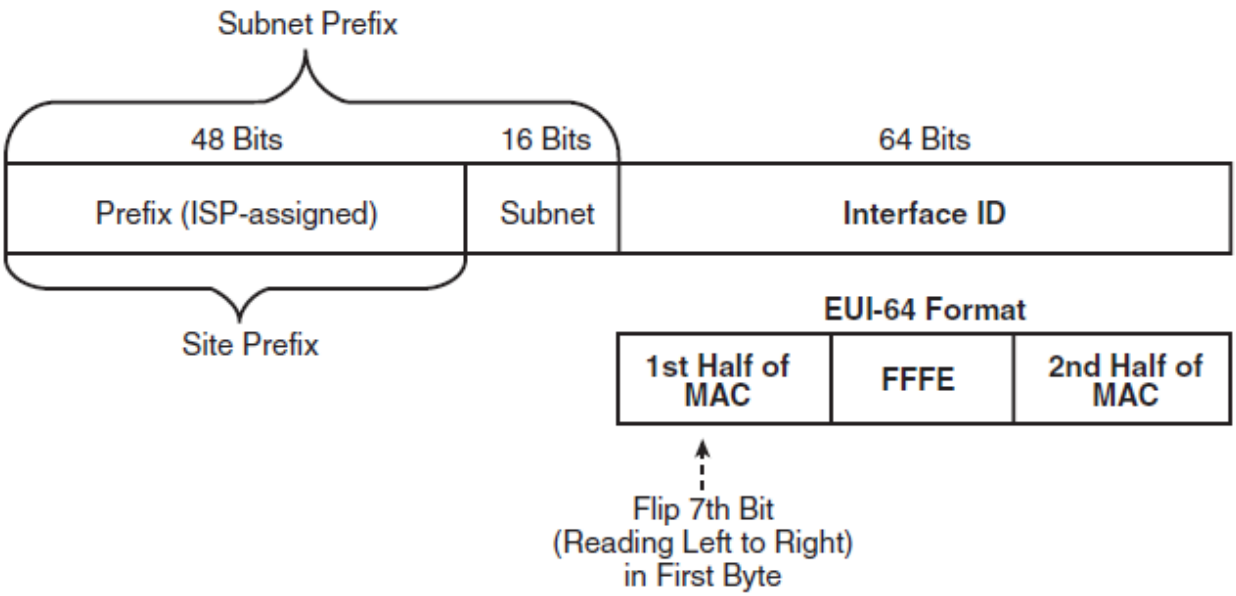
دستور اختصاص IPv6 به یک اینترفیس به صورت Static :

Router (config – if) # IPv6 Address Prefix/Length

مثال :

Router (config – if) # IPv6 Address 2000:0:0:0::1/64

EUI – 64 Metod :



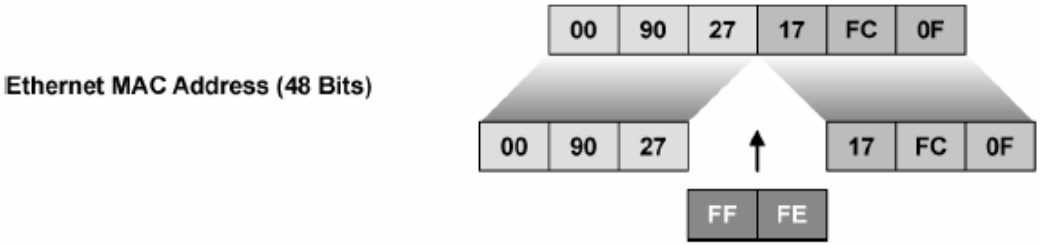
IPv6 Address Format with Interface ID and EUI-64

در این متد از MAC – Address خود دستگاه استفاده می شود برای آدرس دهی . همانطور که اطلاع دارید MAC – Address از دو قسمت OUI و VAA درست شده است . این متد با قرار دادن FFFE در بین دو قسمت MAC – Address مرحله اول را انجام می دهد .

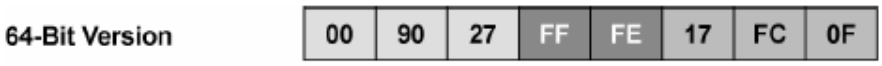
روش ساخت :

MAC – Address ⟶ OUI + VAA

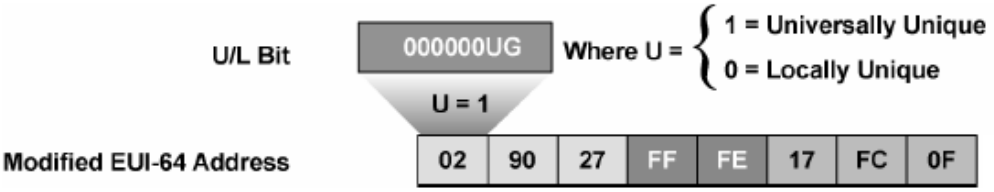
EUI – 64 Metod ⟶ OUI + FFFE + VAA



باتوجه به شکل بالا مشاهده می کنید با قرار گرفتن FFFE در وسط MAC – Address مرحله اول این متد به صورت شکل زیر تمام می شود :



در مرحله دوم یک قانون وجود دارد به این شرح که اگر مقدار بیت هفتم آدرس صفر باشد آن را به عدد یک تغییر می دهیم و اگر یک باشد آن عدد را به صفر تغییر می دهیم . اگر به شکل بالا دقت کنید دو بیت اول آدرس 00 است یعنی برابر است با 00000000 و چون بیت هفتم برابر با 0 است طبق قانون آن را به 1 تغییر می دهیم و به این عدد 00000010 تغییر می دهیم و آدرس به 02 تغییر می کند مانند شکل پایین :



در نهایت آدرس به صورت زیر درست می شود :

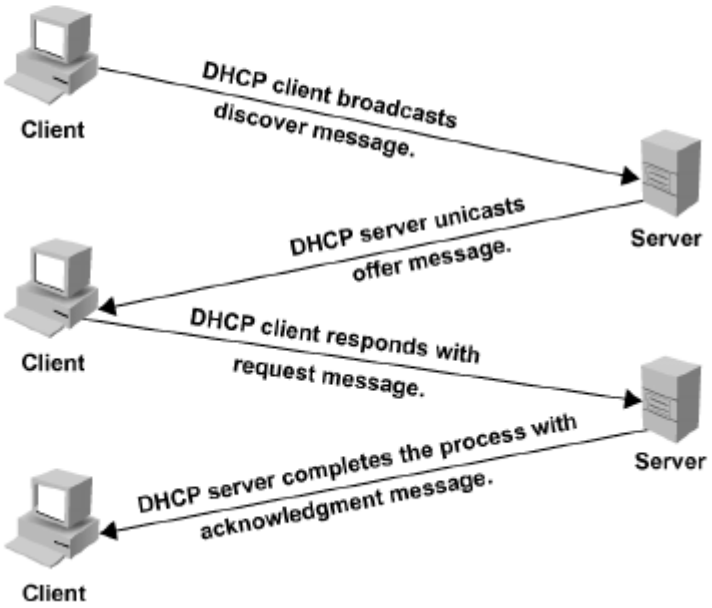
0290:27FF:FE17:FC0F

دستور استفاده از EUI – 64 Metod برای آدرس دهی :

Router (config – if) # IPv6 Address Prefix/Length EUI – 64

DHCP

Dynamic Host Configuration Protocol

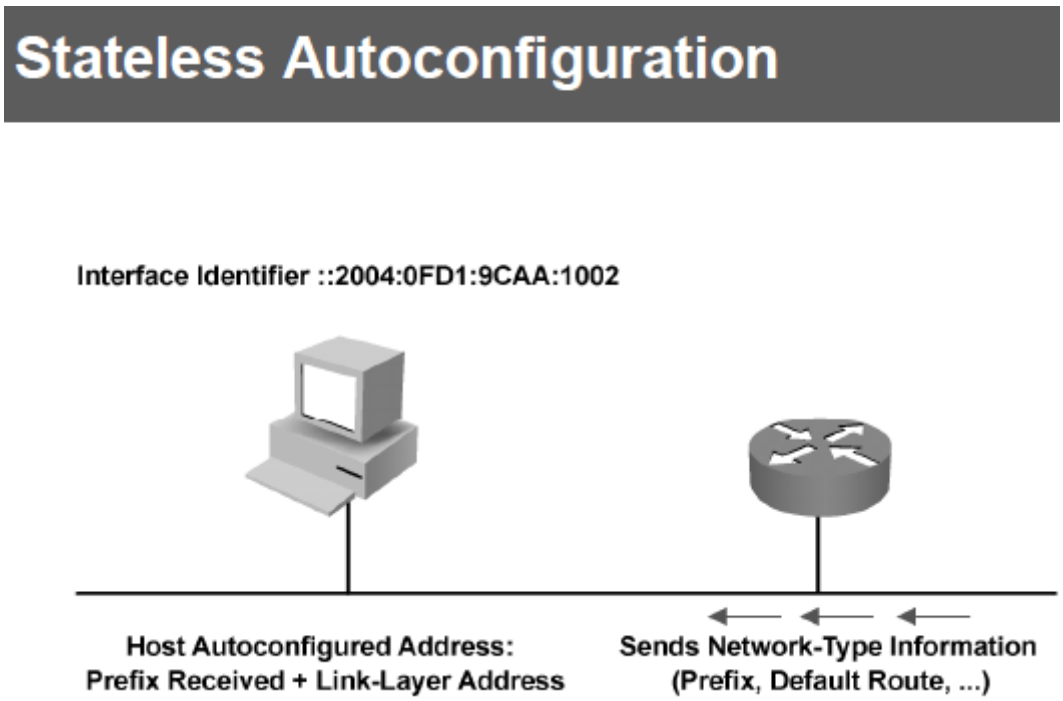


همانطور که در شکل بالا مشاهده می کنید در مرحله اول Client به صورت Broadcast یک پیام DHCP Discover ارسال میکند که از DHCP Server درخواست می کند که یک IP به او اختصاص دهد. DHCP Server پیام را دریافت می کند و آدرس MAC کامپیوتر (Client) را می گیرد و تمام مشخصات Client را در حافظه خود ذخیره می کند و یک IP به آن اختصاص می دهد و با یک پیام Offer Message به Client پیشنهاد می دهد بعد Client که پیشنهاد را دریافت کرد از طریق یک پیام Request message به DHCP Server اعلام میکند که پیشنهاد را میپذیرد و DHCP Server در آخر یک پیام Acknowledgment برای تأیید پایان پروسه به Client می فرستد.

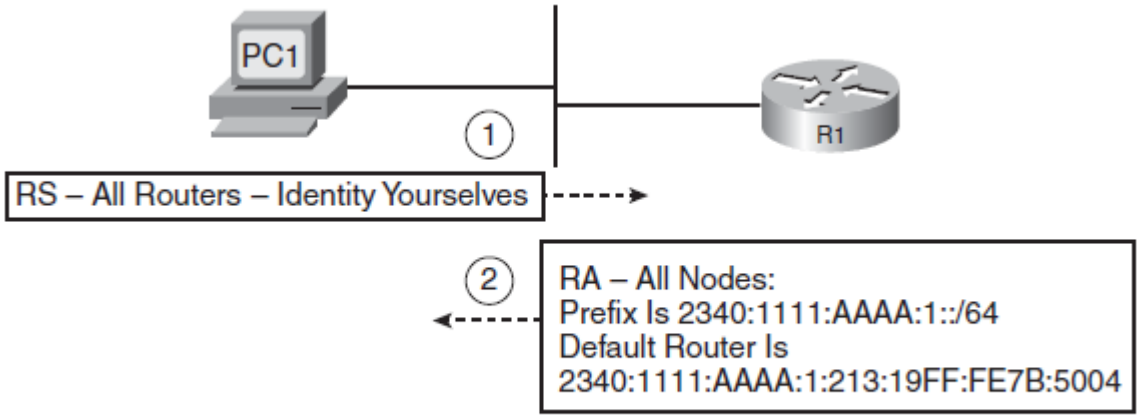
DHCP در IPv6 به دو روش کار می کند :

- روش اول : مثل IPv4 عمل می کند و به نام DHCP Statful کار می کند و با یک آدرس مشخص شده Multicast کامپیوترها به DHCP Server پیام می فرستند و DHCP Server با توجه به MAC آنها یک آدرس IP به آنها اختصاص می دهد . به صورت اتوماتیک آدرس DHCP که برابر است با FF02::1:2 بر روی اینترفیس ها فعال می شود .

- روش دوم : به نام DHCP Stateless کار می کند. IPv6 روی هر روتری در شبکه فعال شود به صورت اتوماتیک یک آدرس Multicast برابر با FF02::2 روی اینترفیس هایش فعال می شود .



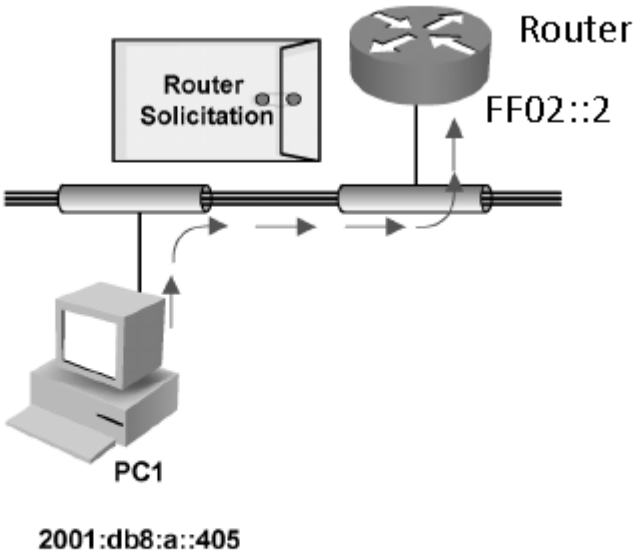
پروتکل NDP :



Example NDP RS/RA Process to Find the Default Routers

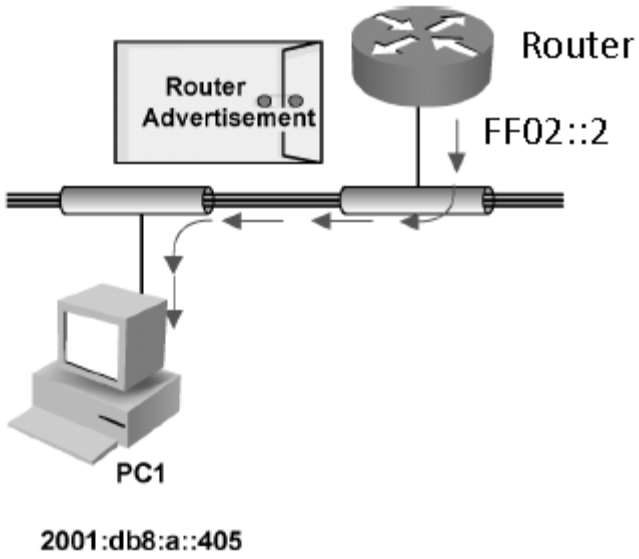
در این پروتکل قسمت Prefix شبکه را برای دستگاه هایی که لازم دارد می فرستد تا آنها بتوانند با استفاده از Prefix شبکه و MAC خود یک آدرس IPv6 بسازند.

در مرحله اول PC با یک پیام (RS) Router Solicitation به مقصد روتر با آدرس Multicast برابر با FF02::2 از روتر می خواهد که قسمت Network شبکه را برایش ارسال کند :



- **Stage 1: The PC sends a router solicitation to request a prefix for stateless autoconfiguration.**

در مرحله دوم روتر قسمت Network شبکه را برای PC به آدرس MAC آن با استفاده از پیام Router Advertisement ارسال می کند :



- **Stage 2: The router replies with a router advertisement.**

آدرس مقصد در داخل پیام های RS بوده و به نام Solicited Node Multicast نامیده می شود . تمام دستگاه های IPv6 به ازای هر Subnet متصل دارای یک آدرس Solicited Node Multicast برای خود می باشند . این آدرس با FF02::1:FF0/104 آغاز گشته و 24 بیت باقیمانده از 24 بیت آخر آدرس IPv6 مربوط به دستگاه برداشته می شود .

مثلا آدرس IPv6 مربوط به روتر R1 برابر است با : 2340:1111:aaaa:1:213:19ff:fe7b:5004

آدرس Solicited Node Multicast مربوط به روتر R1 برابر است با : ff02::1:ff:7b:5004

برای استخراج آدرس Multicast MAC مربوط به یک دستگاه نیز می توان همان 24 بیت آخر آدرس IPv6 را در ادامه 0100.5E نوشت . برای مثال آدرس Multicast MAC مربوط به روتر R1 برابر خواهد بود با 0100.5E7b.5004 .

Duplicate Address Detection

زمانی که به یک اینترفیس یک آدرس IPv6 را از طریق متد EUI-64 اختصاص دهیم اقدام به انجام پروسه DAD خواهد کرد . هدف از انجام این پروسه اطمینان از منحصربه فرد بودن آن آدرس IPv6 است . مکانیزم پروسه DAD به این صورت است که از IP که می خواهد به یک کامپیوتر اختصاص بدهد یک Solicited Node می سازد و آن را Ping می کند اگر جواب Ping را دریافت کرد پس متوجه می شود از آن آدرس IPv6 در شبکه وجود دارد و IPv6 به کامپیوتر اختصاص نمی دهد.

نکته :

در اینترفیس ها IPv6 به صورت Enable نیست باید با دستور زیر Enable شود :

Router (config – if) # IPv6 Enable

اگر این دستور را وارد کنیم IPv6 را درست میکند و در اول IPv6 مقدار زیر را قرار می دهد :

FE80::

بعد از متد EUI-64 استفاده می کند و بقیه آن را قرار می دهد .

نکته :

اینترفیس های Serial چون آدرس MAC ندارند کوچکترین آدرس MAC اینترفیس Fastethernet برای متد EUI-64 استفاده می شود تا به وسیله آن IPv6 اختصاص داده شود .

دستوری که به روترها می فهماند که روتر است و با Host فرق دارد و باید روی همه روترهای شبکه که از IPv6 استفاده می کنند اعمال شود :

Router (config) # IPv6 Unicast – Routing

دستورات مانیتورینگ :

Router # Show IPv6 Interface Brife

Router # Show IPv6 Route

IPv6 Routing

: RIP ng (new generation)

همان RIPv2 است . پورت UDP آن برابر با 521 است از IPv6 استفاده می کند از VLSM پشتیبانی می کند پروتکل Distance Vector است و مقدار AD آن برابر با 120 است . آدرس Multicast که پیام ها بدان مقصد ارسال می گردد برابر با FF02::9 است . متریک در این پروتکل نیز همان Hop Count است .

در RIP مقدار متریک را با خودش جمع می کند و نمایش می دهد یعنی اگر از مسیری یک روتر فاصله داشته باشد با خودش جمع می کند و مقدار 2 را به عنوان متریک نمایش می دهد.

دو روتر RIP با IP Link – Local همدیگر را می شناسند .

دستورات :

Router (config) # IPv6 Router RIP name

Router (config - rtr) # Exit

Router (config) # Interface type mod/num

Router (config – if) # IPv6 RIP name Enable

EIGRP For IPv6 :

پروتکل مسیریابی EIGRP از IPv6 پشتیبانی می کند . یک پروتکل Advanced Distance Vectorاست که برای محاسبه متریک از روش ترکیبی استفاده می کند . این پروتکل در محیط IPv6 به صورت پیش فرض توانمندی Auto Summarization بر روی کلاس های استاندارد غیر فعال می باشد. این پروتکل در محیط IPv6 بسیار سریعتر از پروتکل EIGRP در محیط IPv4 اطلاعات مربوط به Prefix و Prefix Length را به روترهای همسایه ارسال خواهد کرد .

- پروتکل EIGRP در IPv6 از آدرس Multicast برابر با FF02::A استفاده می کند .
- پیش فرض EIGRP خاموش است باید EIGRP را روشن یا فعال کنیم .
- باید یک Router – ID را نیز تعریف کنیم .
- در آخر باید بر روی اینترفیس ها EIGRP را فعال کنیم .

دستورات :

Router (config) # IPv6 Router EIGRP AS – number

Router (config - rtr) # No Shutdown

Router (config - rtr) # EIGRP Router – ID A.B.C.D

Router (config - rtr) # Exit

Router (config) # Interface type mod/num

Router (config – if) # IPv6 EIGRP AS – number

OSPF ver3 For IPv6 :

OSPF ver3 توانایی کار در محیط IPv6 را دارد و بسیار شبیه به پروتکل مسیریابی OSPF ver2 میباشد . این پروتکل از VLSM پشتیبانی می کند . روترها در این پروتکل با آدرس های Multicast برابر با FF02::5 و FF02::6 با یکدیگر تبادل اطلاعات می کنند .

دستورات :

Router (config) # IPv6 Router OSPF Process – ID

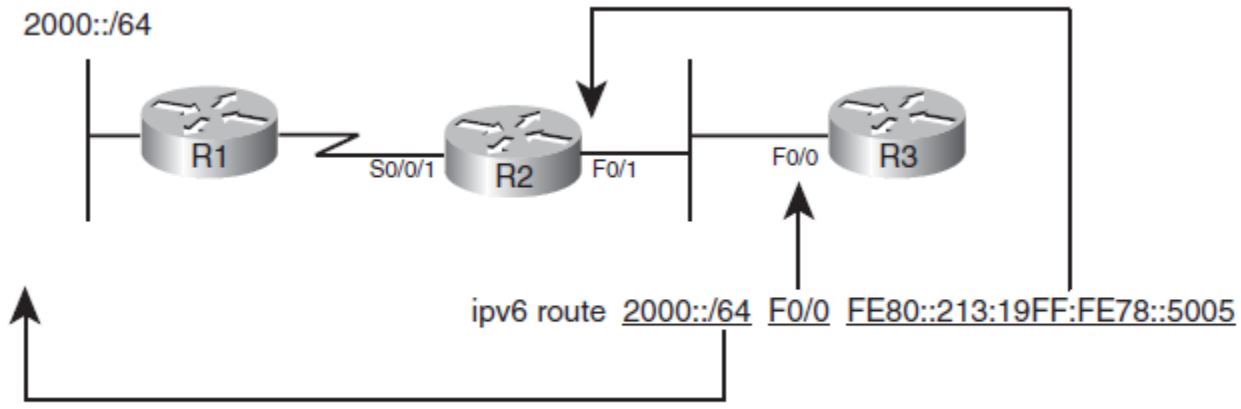
Router (config - Router) # Router – ID A.B.C.D

Router (config - rtr) # Exit

Router (config) # Interface type mod/num

Router (config – if) # IPv6 OSPF Process – ID Area area – number

Static Route in IPv6 :

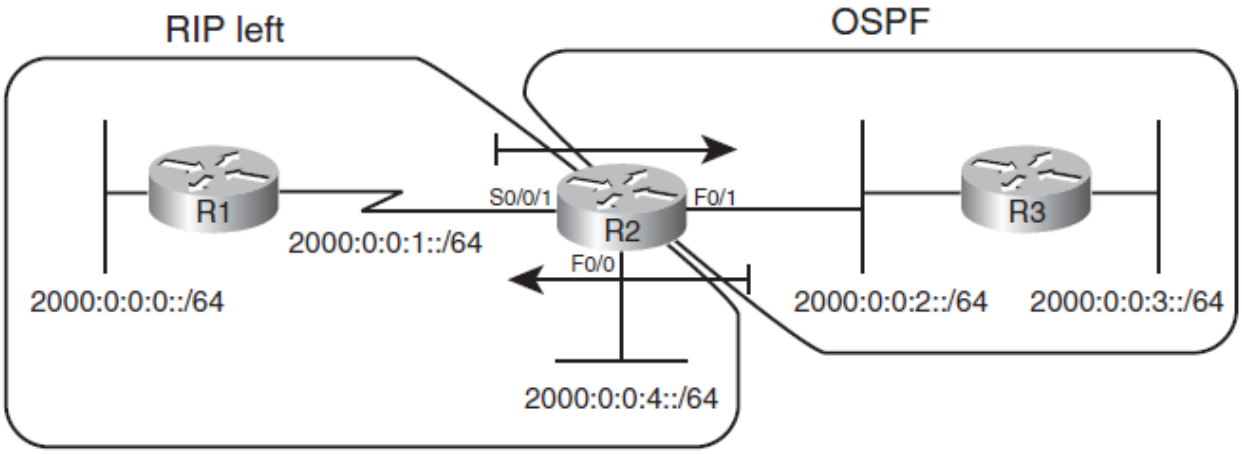


Static IPv6 Route on Router R3

همان دستوری است که قبلا استفاده می کردیم با این تفاوت که به جای اینکه IP را بنویسیم از IPv6 استفاده می کنیم :

Router (Config) # IPv6 route Dst – IP – Address outgoing – Interface Next – Hop

: Redistribution in IPv6



Redistribution Plan

در پروسه Redistribution در پروتکل IPv6 به صورت پیش فرض Connected routeهای مربوط به اینترفیس هایی که پروتکل IGP بر روی آن فعال است منتشر نخواهد شد.برای اینکه این routeها نیز طی پروسه Redistribution منتشر گردد باید از پارامتر Include – Connected در دستور Redistribute استفاده کرد .

دستور کلی :

Router (config - Router) # Redistribute Router – Protocol [Include – Connected]

با توجه به شکل بالا اگر بخواهیم که routeهای پروتکل OSPF را در RIP منتشر کنیم باید دستورات زیر را بر روی روتر R2 وارد کنیم :

```
R2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# ipv6 router rip left
R2(config-rtr)# redistribute ospf 5 include-connected
R2(config-rtr)# ^Z
R2#
```

نتیجه عمل Redistribution بر روی روتر R1 به صورت زیر است :

```
! The next command is executed on router R1
R1# show ipv6 route rip
IPv6 Routing Table - Default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, M - MIPv6, R - RIP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
R   2000:0:0:2::/64 [120/2]
     via FE80::213:19FF:FE7B:5004, Serial0/0/0
R   2000:0:0:3::/64 [120/3]
     via FE80::213:19FF:FE7B:5004, Serial0/0/0
R   2000:0:0:4::/64 [120/2]
     via FE80::213:19FF:FE7B:5004, Serial0/0/0
```

همانطور که در بالا مشاهده می کنید هر دو شبکه موجود در OSPF در روتر R1 با متریک 2 و 3 نمایش داده شده است.

Network Engineer
IRAN : +989127687757
ERBIL : +964 750 530 8221
Kolijis@Yahoo.com
Showan.Koliji

Showan koliji