سیسکو به پارسی

آشنایی با Multicast

نوشته:
شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian
انجمن سیسکو به پارسی http://forum.shafagh.com

آشنایی با Multicast

هدف از Multicast ارسال پیام تنها به گروهی از گیرندگان است که علاقه مشترکی در دریافت یک Data بخصوص دارند. پس جهت دریافت ترافیک مورد نظر عضو آن گروه میشوند. Multicast کاربردهایی نظیر IPTV، CCTV، Online Training - ELearning، Software Distribution، Conferencing و غیره دارد و در لایه دو و لایه سه قابل پیاده سازی است.

در شبکه سه نوع ترافیک IP منتقل میشود:

- **Unicast**
  بسته ای که از یک فرستنده به یک گیرنده ارسال میشوند.

- **Broadcast**
  بسته ای که از یک فرستنده به همه ارسال (منتشر) میشود. این نوع بسته ها، توسط روتر به بخشهای دیگر شبکه منتقل نمیگردد مگر آنکه بدلیل خاصی آنرا برای این کار تنظیم کنیم.

- **Multicast**
  بسته ای که از یک فرستنده به سمت گروهی از گیرنده ها ارسال میشود.

Cisco in Persian

Ethernet و FDDI ارسال Unicast، Multicast و Broadcast را پشتیبانی کردند و Token Ring نیز توسط Functional Address این کار را پیاده سازی کرد. اگر کاربرد برای یک LAN باشد، استفاده از L2 Multicast (لایه دو) در شبکه LAN کافی بنظر میرسد، اما در جاییکه پراکندگی بین گیرنده ها در سطح چندین شبکه یا VLAN باشد، باید از Multicast Routing استفاده کنیم.

رفتار روتر با Multicast مشابه Broadcast است. روتر Multicast را در ورودی Interface و بین شبکه ها فیلتر میکند (بصورت پیش فرض).

گیرندگان Multicast میتوانند در سطح شبکه (و شبکه ها) پراکنده باشند. اگر نیاز به ارتباط با بیرون باشد، باید Multicast Routing تنظیم گردد.

برای Route کردن ترافیک Multicast باید از Multicast Routing Protocol استفاده کنیم. پروتکل هایی نظیر DVMRP، MOSPF، PIM-SM و یا PIM-DM.

Multicast و لایه دو

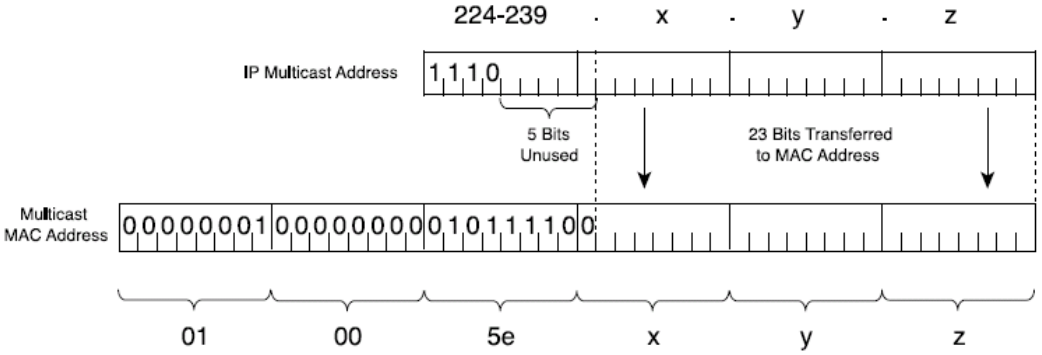
آدرس های Multicast بصورت Class D و همیشه با 1110 شروع می شوند. صرف نظر از 4 بیت اولیه که همیشه یکسان است، 28 بیت باقیمانده آدرس گروه را تشکیل میدهند (از 224.0.0.0 تا 239.255.255.255). هر گروه نیازمند یک آدرس است.

برای Map کردن این آدرس لایه سه (IP) به لایه دو (Data-Link)، از ARP نمیتوان استفاده کرد. اما روش آدرس دهی وجود دارد که براساس آدرس لایه 3 میتوان آدرس لایه 2 را محاسبه کرد.

آدرسهای MAC که با 0100.5E شروع میشوند (سه بایت اولیه آدرس بعنوان Organizationally Unique Identifier (OUI)) برای این کار رزرو شدند که از 28 بیت IP گروه، 23 بیت را می توان به باقی OUI اضافه کرد (چون MAC، 48 بیتی است).

با توجه به اینکه آدرس MAC، 48 بیتی است و 25 بیت اول آن جهت 01-00-5E رزرو شده است. تنها 23 بیت برای آدرس گروه باقی میماند. به ناچار 5 بیت از Group Address به آدرس MAC تبدیل نخواهد شد. به ازای 5 بیت باقی مانده 32 گروه هم آدرس خواهیم داشت. برای حل مشکل 32 گروه هم آدرس، گیرنده می تواند پس از دریافت فریم از IP آن در L3 Header مطلع شود.

Cisco in Persian



ترافیک Multicast

گیرنده یک Multicast گروهی از Host ها هستند که در گروه Join شده و شروع به دریافت اطلاعات میکنند. به این گروه Multicast Group میگوییم. اعضا برای پاسخ یا درخواست از فرستنده، از Unicast استفاده میکنند. Multicast بصورت Connectionless و Best-Effort ارسال شده و از UDP استفاده میکند.

آدرس Multicast

کلاس D برای آدرس دهی Multicast در نظر گرفته شده است:

غیرقابل Route	224.0.0.255	224.0.0.0	Link-Local address
قابل Route	238.255.255.255	224.0.1.0	Globally Scoped address
خصوصی درون شبکه	239.255.255.255	239.0.0.0	Administratively Scope address
CLASS D	**239.255.255.255**	**224.0.0.0**	**Complete Multicast address**

ردیف اول جدول بالا، به آدرس های Multicast که توسط Routing Protocol ها و تنها درون Broadcast Domain ارسال میشود، اشاره میکند. مثل آدرس All-Hosts که 224.0.0.1 است یا آدرس All-Routers که 224.0.0.2 است. این رنج (224.0.0.0/24) تحت عنوان Fixed-group addresses تعریف شده اند.

ردیف دوم جدول بنام آدرس های جهانی Multicast بین شبکه ها استفاده میشود. نه Local است نه Private.

ردیف سوم به آدرس های Private اشاره میکند که بصورت درون شبکه ای، قابل استفاده بوده و نباید به بیرون Route شوند.

ردیف آخر جدول، به کل آدرس های Multicast که در برگیرنده ردیف های بالاتر میباشد، بعنوان Class D اشاره میکند.

Cisco in Persian

IGMP (Internet Group Management Protocol)

IGMP – RFC 1112
IGMPv2 – RFC 2236
IGMPv3 – RFC 3376

برای Multicasting در شبکه، گیرنده باید عضو Multicast Group شود که این کار توسط پروتکل IGMP صورت می گیرد.

هر 60 ثانیه یک روتر بعنوان IGMP Querier از Host ها دعوت می کند که در صورت تمایل به عضویت گروه مورد نظرشان، درخواست خود را ارسال کنند. این دعوت به نشانی 224.0.0.1 (All-Hosts) فرستاده می شود.

وقتی یک Host مایل به عضویت در گروه باشد، درخواست خود را بوسیله IGMP به Local Router ارسال میکند. اعضایی که تمایل به ادامه عضویت دارند نیز بهمین صورت کار خود را ادامه میدهند.

Router نیازی ندارد که لیست کامل اعضا را داشته باشد، بلکه باید بداند چه گروهی را به کدام Interface، ارسال کند.

در IGMPv1 روشی برای خروج از گروه وجود نداشت. راه حل این بود که در صورت عدم تمایل، Host عضویت خود را تمدید نکند. پس به پیام عضویت Router جواب نمیداد تا پس از 3 دقیقه Timeout شده و از گروه حذف شود.

در IGMPv2 (نسخه دو این پروتکل) Host بوسیله ارسال Leave Group Message به آدرس 224.0.0.2 یا All-Routers Address در هر زمانی می تواند خروج خود را اعلام کند.

از دیگر تفاوت های IGMP نسخه اولیه با IGMPv2 در نوع Query هاست. در IGMPv2 به یک گروه خاص هم میتوان Query فرستاد (Group-Specific Message).

اگر روی یک سگمنت روتری IGMPv1 صحبت کند، بقیه روترها مجبور هستند روی آن سگمنت IGMPv1 عمل کنند زیرا IGMPv1 پیامهای نسخه دوم را درک نمیکند.

IGMPv3 نسخه جدیدتر IGMP است که بدلیل کفایت عملکرد IGMPv2 و عدم نیاز به خصوصیات پیچیده تر رشد و استفاده از نسخه سوم در شبکه ها کند پیش میرود. یکی از ویژگی های IGMPv3 پشتیبانی از SSM یا Source Specific Multicast است.

IGMP برای مدیریت گروه های Multicast در IPv4 ارائه شده و MLD یا Multicast Listener Discovery در IPv6 برای اینکار ساخته شده است.

Cisco in Persian

نکته: وقتی PIM (جهت Multicast Routing) روی یک Interface فعال شود، همراه آن IGMPv2 نیز بصورت قراردادی فعال میشود.

Multicast Switching

بطور کل یک سوییچ لایه دو از Multicast چیزی نمی داند پس فریم های Multicast را همانند Broadcast به همه پورت ها ارسال می کند. روش هایی برای Forward کردن فریم ها فقط به پورتهای عضو Multicast وجود دارد که موجب کم کردن ترافیک زائد شبکه می شوند اعم از: IGMP Snooping و CGMP.

IGMP Snooping

همانطور که اشاره شد، برای اینکه یک Host عضو گروه شود باید بوسیله IGMP به روتر پیام دهد. IGMP Snooping روی سوییچ از طریق گوش دادن به این پیام ها، متوجه وجود متقاضی شده و در زمان دریافت Multicast بخوبی میداند که آنرا تنها به کدام پورت ها ارسال کند.

برای یک L2 Switch گوش کردن به تمام Multicast Frame ها دشوار و منجر به اشغال منابع خواهد شد، در حالیکه برای Multilayer Switch ها این کار به سادگی انجام پذیر است.

IGMP Snooping بصورت Default روی اکثر سوییچ های سیسکو فعال است. برای غیرفعال کردن آن میتوان از دستور زیر استفاده کرد:

```
Switch(config)# no igmp snooping
```

Cisco in Persian

Cisco Group Membership Protocol – CGMP

این روش قدمی توسط سیسکو در نبود IGMP Snooping ارائه شد تا سوییچهایی که توانایی لازم برای Snooping را ندارد با کمک روتر نزدیک خود بتواند ترافیک Multicast را تفکیک و به پورتهای عضو شده بفرستد. CGMP باید علاوه بر سوییچ، روی روتر نیز فعال شود تا پیام های CGMP به آدرس 0100.0CDD.DDDD بین سوییچ و روتر رد و بدل شوند. در عین حال سوییچ هایی که CGMP نمیفهمند این ترافیک را از خود عبور میدهند.

درون یک پیام CGMP، آدرس MAC و آدرس Multicast یک Host در موقع عضو شدن و یا خارج شدن، درج میشود تا سوییچ CAM Table خود را Update کند. در واقع روتر نقش سمعک را برای سوئیچ ایفا می کند!

برای فعال کردن CGMP از دستور زیر استفاده میکنیم:

```
Router(config-if)# ip cgmp
```

در سوییچ هایی که قابلیت IGMP Snooping را پشتیبانی نمیکنند، CGMP بصورت Default فعال است.

اگر در شبکه سوییچ از CGMP یا IGMP Snooping پشتیبانی نکند، در صورت استفاده از Multicast، ترافیک زائد در سطح شبکه منتشر خواهد شد.

در صورتیکه روتر LAN، قابلیت IGMP را پشتیبانی نکند، ارتباط Multicast تنها درون LAN برقرار میگردد. Host ها درخواست Join خود را بصورت IGMP ارسال میکنند و منتظر دریافت ترافیک میماند. اگر فرستنده در همان LAN باشد، ارتباط برقرار میشود. اما باید توجه داشت: از آنجا که IGMP Snooping بصورت Default فعال است در صورتیکه IGMP روتری وجود نداشته باشد، پورت ها برای Multicast بلوکه شده و حتی ترافیک درون VLAN نیز قابل دسترس نخواهد بود. در این صورت راه حل فعال کردن IGMP Querier روی سوییچ است تا کار IGMP Router را ایفا کند و Host هایی که تمایل عضویت دارند را شناسایی کند.

```
Switch(config)# ip igmp snooping querier
```

Cisco in Persian

چک کردن Multicast

یکی از ابزارهای کلیدی در تست ارتباطات شبکه، PING و پروتکل محبوب ICMP است. در ارتباط Multicast نیز میتوان یک گروه را Ping کرد. بدین صورت فرستنده، Source و گیرنده Group است.

میتوانیم گروه Multicast را Ping کنیم تا از وضعیت ارتباط مطلع شویم. بوسیله دستورات زیر وضعیت IGMP را میتوان بررسی کرد. دستورات زیر روی یک L3 Switch و روتر قابل استفاده هستند:

```
Switch# show ip igmp groups
Switch# show ip igmp snooping
Switch# show ip igmp interface Interface
```

برای آزمودن عضویت در یک گروه از دستور زیر میتوانیم استفاده کنیم:

```
Switch(config-if)# ip igmp join-group multicast-address
```

Cisco in Persian

پروتکل های Multicast Routing

برای Route کردن ترافیک Multicast از یک Multicast Routing Protocol استفاده می کنیم. پروتکل هایی نظیر:

- CBT یا Core Based Trees
- DVMRP - مشابه پروتکل RIP در Unicast Routing است.
- MOSPF - براساس OSPF
- PIM-SM - فرض میکند اعضای گروه پراکنده اند.
- PIM-DM - فرض میکند اعضای گروه متراکم اند.

Distance Vector Multicast Routing Protocol - DVMRP

پروتکلی است که در RFC 1075 تشریح شده و از تکنیکی بنام Reverse Path Forwarding استفاده میکند. این پروتکل از پروتکلی Distance Vector که مشابه RIP و براساس Hop Count است، بهره میبرد. بدلیل استفاده از Routing Protocol خاص خود، ممکن است مسیر Multicast با مسیر Unicast متفاوت باشد. یکی از مشکلات بزرگ DVMRP در رشد پذیری آن (Scalability) است.

از DVMRP در ساخت MBONE استفاده شد. MBONE با هدف اینکه Multicast Backbone اینترنت باشد بصورت آزمایشی اجرا شد.

Cisco in Persian

Multicast OSPF - MOSPF

RFC 1584 به تشریح Multicast Extension to OSPF پرداخت، که به اضافه شدن قابلیت Multicast Routing به OSPF اشاره میکند.

OSPF اطلاعات مربوط به Multicast را داخل Link State Advertisement خود ارسال میکند و هر روتر از وجود گروه های Multicast در هر قسمت از شبکه مطلع میشود. OSPF به ازای هر فرستنده و گروه یک درخت توزیع ایجاد و محاسبه میکند. هرگاه وضعیت لینک تغییر کرد محاسبات دوباره انجام میشود.

MOSPF تنها میتواند در شبکه هایی که بر پایه OSPF کار میکنند، بکار گرفته شود. این پروتکل در شرایطی که تعداد کمی فرستنده/گروه فعال وجود داشته باشد، بهتر عمل میکند و برای شبکه هایی که همیشه در حال تغییر هستند و فرستنده زیادی دارند مناسب نیست.

Protocol-Independent Multicast – PIM

این پروتکل میتواند فارغ از نیاز به پروتکل خاصی عمل کند و طرح شبکه خود را از روی Unicast Routing Table میسازد. PIM انواع گوناگونی دارد نظیر Dense Mode (PIM-DM) و Sparse Mode (PIM-SM):

مدل Dense Mode برای زمانی مناسب است که فرستنده و گیرندگان در نقاطی به صورت مجتمع و متمرکز قرار گرفته باشند. حجم زیاد ترافیک، تاخیر کم و تعدد گیرنده در مقابل فرستنده، شرایطی هستند که ما Dense Mode را بر Sparse Mode ترجیح میدهیم. این مدل مثل DVMRP، از RPF بهره میبرد اما تفاوت در اینجاست که PIM محدود به یک Unicast Routing Protocol نیست.

مدل Sparse مزایای خاصی نسبت به Dense دارد و در زمانی استفاده میشود که فرستنده و گیرنده ها از هم متفرق و در سطح شبکه پخش باشند. این مدل زمانی که تعداد بیشتری فرستنده داشته باشیم بکار گرفته میشود و برعکس Dense Mode از مفهومی بنام Rendezvous Point بهره میبرد.

Rendezvous Point (بخوانید راند وو) مرکزی ایست که فرستنده، اطلاعات را به آن ارسال و گیرنده از آن دریافت میکند. البته باید ابتدا خود را با آن نقطه Register کند. Sparse Mode بر خلاف Dense Mode، بسته Multicast را در سطح شبکه ارسال نمیکند مگر آنکه از بخشی از شبکه درخواست ترافیک را دریافت کند.

در دنیای Linux و Unix، Multicast Routing ابتدا باید در کرنل فعال گردد. علاوه بر آن به برنامه هایی نظیر Zebra، mrouted و pimd نیاز داریم تا برای ما Multicast Routing را پیاده سازی کنند. بعد از تنظیم کردن Kernel، IGMP در هنگام بوت شدن دستگاه، Load میشود که همانطور که اشاره شد، رکن اساسی Multicast Management یا مدیریت گروه های Multicast است.

Cisco in Persian

Multicast Routing

یکی از تفاوت های Multicast Routing نسبت به Unicast Routing در تعدد مسیرهای مقصد یک آدرس است. زیرا گیرنده یک نقطه نیست و یک گروه است! پس بر خلاف Unicast Routing که از بین چندین مسیر یک Interface برای رسیدن به مقصد انتخاب میشود، در Multicast Routing یک بسته دریافتی به چندین Interface ارسال میگردد.

برای فعال کردن Multicast Routing در سیسکو از دستور زیر استفاده می کنیم:

```
Router(config)# ip multicast-routing
```

برای Forward کردن Packet های Multicast، مسیر توسط الگوریتمی مشابه Spanning Tree، محاسبه می شود. این درخت، فرستنده را بعنوان ریشه درخت و گیرندگان را بصورت شاخه در نظر میگیرد تا ارتباط Loop-Free باشد. (بدون Loop)

RPF یا Reverse Path Forwarding برای اطمینان از Loop Free بودن مسیر و اینکه Packet به سمت فرستنده مجددا ارسال نگردد، استفاده میشود. در واقع ایده اصلی RPF این است که باید Packet از Interface ی دریافت گردد که فرستنده آن، بر اساس Routing table در همان Interface قرار دارد. یعنی اگر بخواهیم به فرستنده پیامی بفرستیم، براساس Routing-Table همان Interface جهت ارسال انتخاب شود. پس پیام های Multicast آن فرستنده را تنها از آن Interface قبول میکند و به بقیه Interface ها ارسال میکند (در صورت نیاز)

در صورتیکه Multicast Packet از Interface ی غیر از آنچه که روتر انتظار دارد وارد شود، روتر آنرا دور می اندازد. به این رخداد RPF Failure میگوییم.

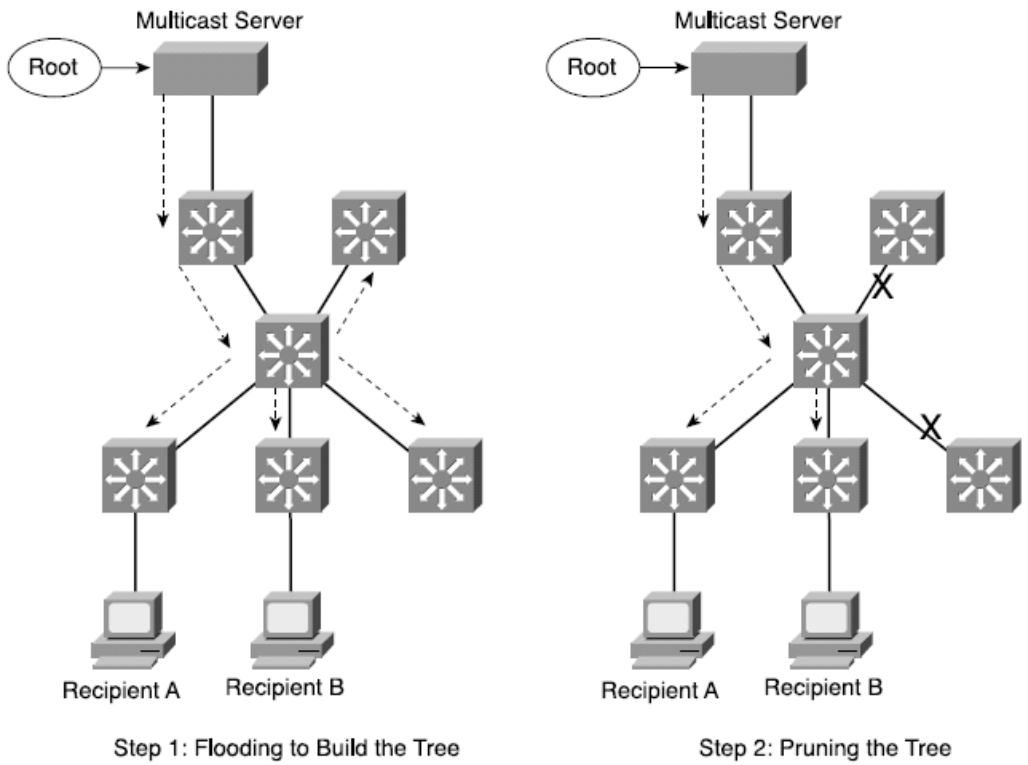
برای Multicast Routing از پروتکل های مختلفی استفاده می شود، پروتکلی که در ادامه به تشریح آن میپردازیم PIM یا Protocol Independent Multicast است.

Cisco in Persian

PIM

همانطور که اشاره شد، PIM از Routing Table منحصر به خود استفاده نکرده و از IP Routing Table بهره میبرد. از آنجا که محدود به هیچ Routing Protocol خاصی نیست به آن Protocol-Independent Multicast میگوییم (پروتکلی مستقل از پروتکلهای دیگر). PIM در دو نسخه و در دو Mode کار میکند:

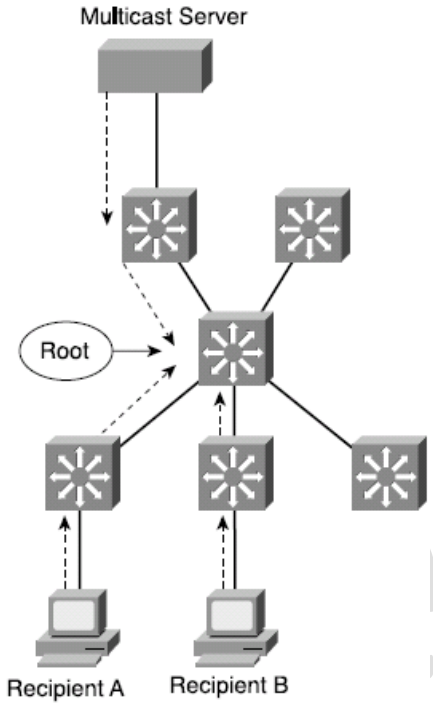
Dense-mode: فرض میکند که اعضای گروه در همه شبکه وجود دارند. فرستنده Multicast بعنوان Root درنظر گرفته شده و درخت از فرستنده به گروه (S,G) شکل میگیرد. در صورتیکه در بخشی از شبکه هیچ گیرنده ای عضو گروه نشده باشد یک پیام Prune از روتر آن بخش به همسایه خود در جهت Root ارسال میشود تا آن مسیر درگیر ترافیک زاید نگردد. در واقع به این عملیات Flood-then-Prune می گوییم یعنی اول ارسال سپس Prune. (Prune بمعنی هرس کردن)



روتر های PIM-DM بوسیله Hello-message از همسایگان خود مطلع می شوند و درخت شکل میگیرد. در صورتیکه عضو جدیدی وارد شود، آن بخش از شبکه به درخت متصل یا Grafted میشود (قلمه زدن). برای تنظیم یک Interface برای Multicast:

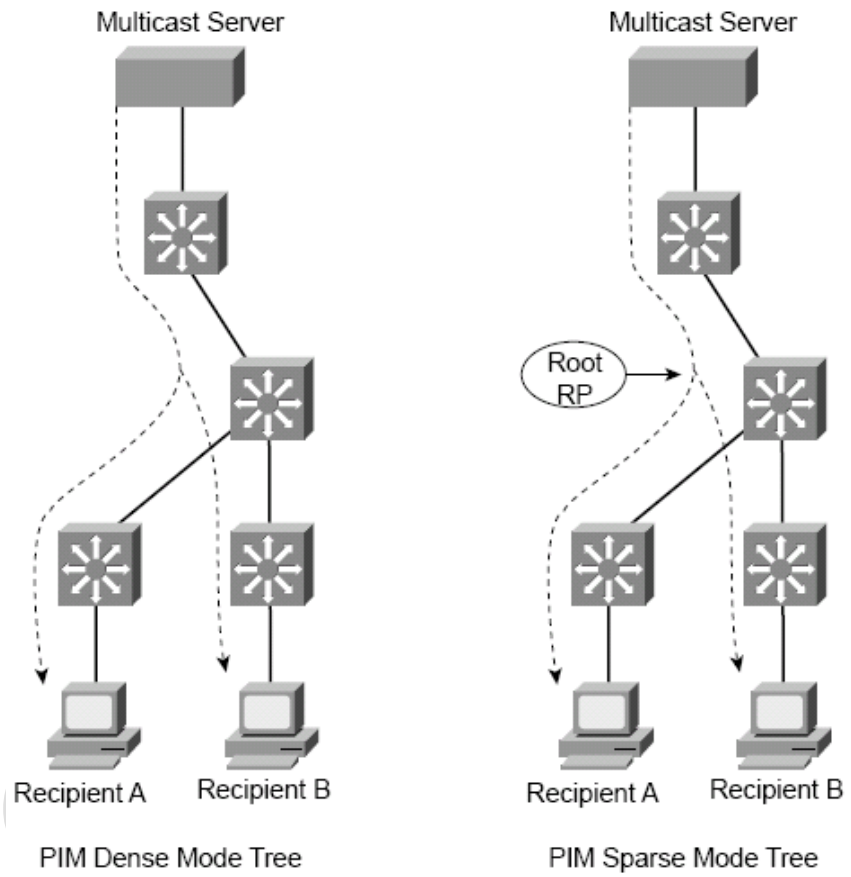
```
Router(config-if)# ip pim dense-mode
```

Sparse-mode: درخت خود را از انتها می سازد و به آن Shared-tree میگوییم. Root در این شبکه RP (Rendezvous Point) نامیده می شود که در مرکز شبکه قرار دارد. بهمین دلیل به آن Shared Tree می گوییم (*,G). فرستنده باید خود را با RP، Register کند. برخلاف PIM-DM، از ابتدا روتر هایی که عضوی ندارند در درخت قرار نمیگیرند که بعدا Prune شوند.




```
Router(config-if)# ip pim sparse-mode
```

شکل زیر به مقایسه Dense-mode و Sparse-mode میپردازد:



سیسکو مدل سومی نیز بعنوان PIM Sparse-Dense Mode (به ازای هر گروه) ارائه کرده است. در واقع اگر در گروهی RP وجود داشته باشد از Sparse و در غیر این صورت از Dense استفاده میکند.

```
Router(config-if)# ip pim sparse-dense-mode
```

PIM Version 1

در نسخه اول PIM باید به صورت Manual یک RP تعریف کرد.

برای تنظیم کردن یک RP از این دستور استفاده میکنیم:

```
Switch(config)# ip pim rp-address ip-address [ACL] [override]
```

اگر override را در انتهای این دستور وارد کنیم، آنچه Manual تنظیم شده به Dynamic اولویت خواهد داشت. از access-list برای محدود کردن یک RP به Multicast Group استفاده میشود.

پس از چندی، سیسکو راه حلی برای Dynamic کردن این عملیات ارائه کرده است. (تحت عنوان Auto-RP که به آن PIM Version 1.5 میگویند!)

در مدل Cisco Auto-RP از یک یا چند Mapping Agent جهت انتخاب RP هر گروه استفاده میشود. در واقع روترهایی که بعنوان Candidate RP (C-RP) تنظیم شده باشند، پیام RP-Announce را هر 60 ثانیه به آدرس 224.0.1.39 (Cisco-RP-Announce) ارسال می کنند. Mapping Agent ها این پیام را گرفته، به ازای گروه، RP را از میان کاندیدها انتخاب کرده و به اطلاع روترهای PIM می رسانند. این انتخاب بر اساس بالاترین IP از میان C-RP های گروه صورت میگیرد و هر 60 ثانیه به آدرس 224.0.1.40 – Cisco-RP-Discovery ارسال میشود.

Cisco in Persian

برای تنظیم یک Mapping agent

```
Switch(config)# ip pim send-rp-discovery scope ttl
```

برای تنظیم یک Candidate RP

```
Switch(config)# ip pim send-rp-announce interface scope ttl group-list ACL
```

PIM Version 2

نسخه دوم PIM عملکرد Auto-RP را بعنوان یک استاندارد تحت نام Bootstrap Router Method ارائه کرد. BSR، RP را بصورت داینامیک و پویا به همه PIM Router ها معرفی میکند. در واقع تنها کافیست BSR و C-RP ها را مشخص کنیم.

برای تنظیم BSR

```
Switch(config)# ip pim bsr-candidate interface hash-mask-length
[priority]
```

سپس باید Candidate RP را مشخص کنیم

```
Switch(config)# ip pim rp-candidate interface ttl group-list ACL
```

برای محدود کردن یک Multicast Domain (دامنه ارسال Multicast) و جهت جلوگیری از خروج PIMv2 Advertisement از PIM Border استفاده میکنیم.

PIM Border از Forward کردن اطلاعات Bootstrap جلوگیری میکند:

```
Switch(config)# ip pim border
```

برای دیدن وضعیت PIM میتوانیم از دستورات زیر استفاده کنیم:

```
Switch# show ip rpf ip-address
Switch# show ip pim neighbor
Switch# show ip pim rp
Switch# show ip pim autorp
Switch# show ip pim bsr-router
```

Cisco in Persian