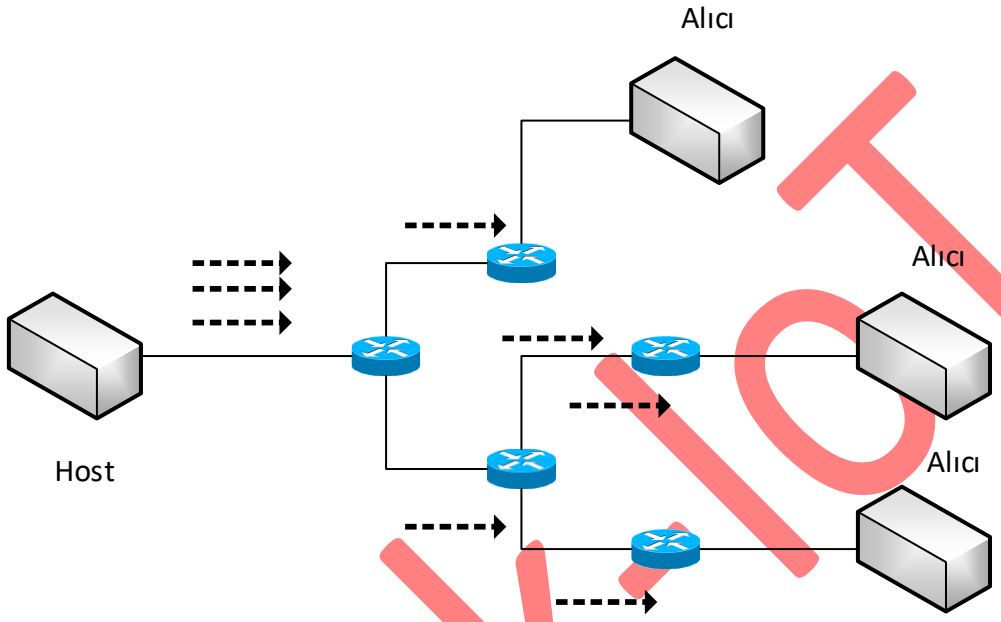
Multicast nedir ve multicast'in faydaları nelerdir bunları inceleyeceğiz.

BÖLÜM 1 / IP Multicasting – Giriş :

Multicast nedir ?

Bir mesajı bir kaynaktan seçili birden çok hedefe göndermedir.

Aşağıdaki topolojide tüm alıcılar, hosttan yayın istiyor ve tek bir yayın 3 ayrı alıcı ayrı ayrı üretiliyor ve iletiliyor. Unicast trafik, one to one trafik olarak da bilinmektedir.



Multicast :

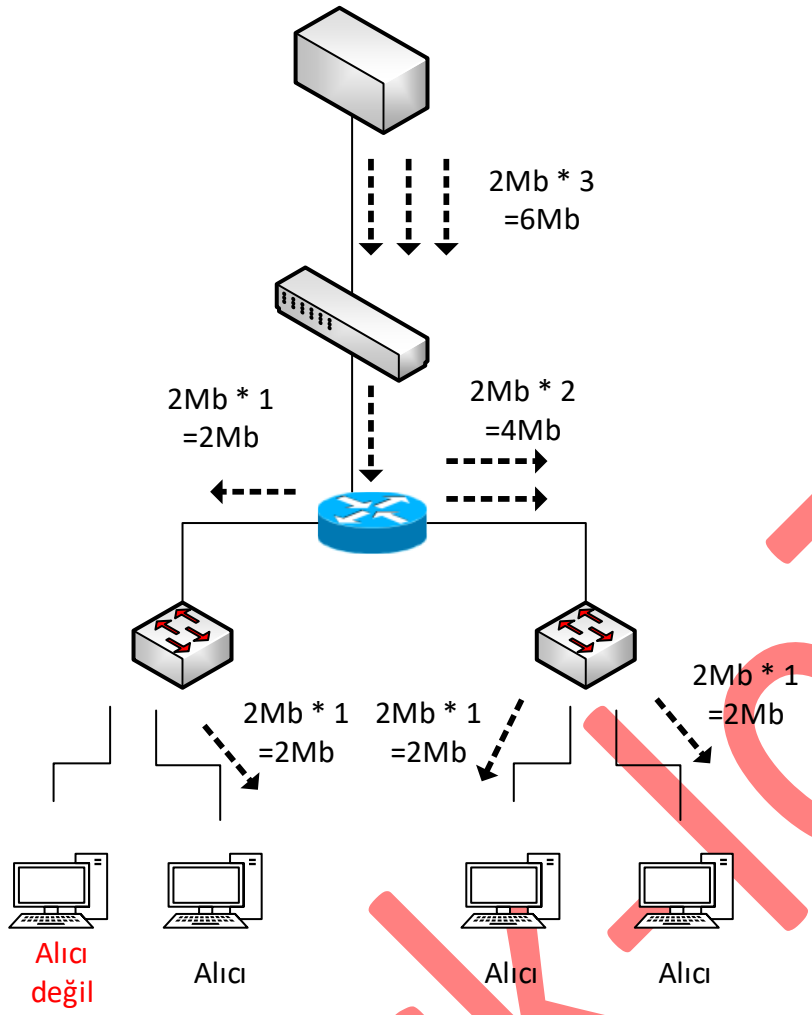
Multicast trafik, tüm alıcılara değil ya da tek bir alıcıya değil. Bir grup alıcıya iletilir.

Teknik olarak source mesajın bir kopyasını gönderir ve birden çok alıcı tarafından mesaj alınır. Source, mesajı herkese iletmez, bunun yerine sadece talep eden alıcılara iletir.

Multicast trafik teknolojisi günümüzde oldukça yaygın hale gelmeye başlamıştır. IPTV, uzaktan eğitim sistemleri, video konferans, vb..

Niçin multicast trafik tipini kullanıyoruz ?

Multimedia Trafikte Unicast aktarım Tipi :



Her birisi için ayrı ayrı video stream gönderilecektir.

Örneğin 2Mbps'lık bir video stream'i 100 alıcıya gönderdiğimizde, toplamda 200Mbps'lık trafik anlamına gelir. Alıcı sayısı arttıkça, gereksinim duyulan bant genişliği miktarı da artar. Bu durum video source üzerinde de ekstra kaynak kullanımına sebep olur.

Büyük video stream yapılarında, unicast hiç akıllıca bir yöntem değildir.

Video server'dan bir paketin bir kopyası, paketi almak isteyen her alıcıya iletilir.

Az sayıda alıcının , video server'dan yayın aldığı durumlarda kullanılabilir

Mesaj eğer büyük bir gruba iletiliyorsa, aynı mesaj aynı link üzerinde çok defa gereksiz bir şekilde taşınır.

Bant genişliği kullanımı, kullanıcı sayısı ile doğru orantılıdır.

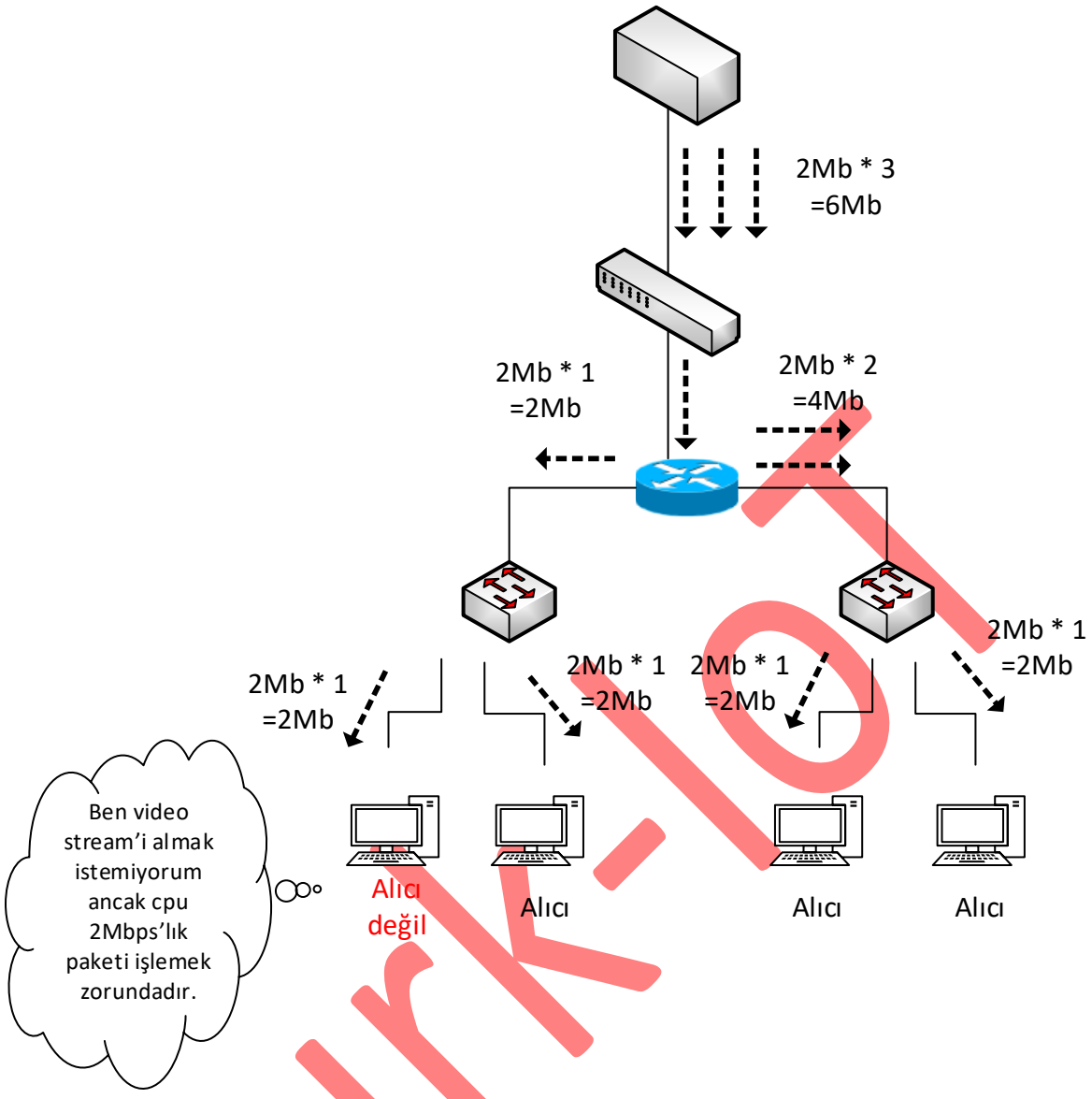
Yönlendirici, her bir kaynak ve alıcı çiftine göre, bireysel yönlendirme kararı verir.

Multimedia Trafikte Broadcast aktarım Tipi :

Video server, bir paketin yalnızca bir kopyasını broadcast kullanarak alıcılara gönderir.

Tüm alıcılar paketi almasa bile, gelen paketi işlemek zorundadır.

Ses, videonun birden çok alıcıya iletiminde, tavsiye edilen bir yöntem değildir.



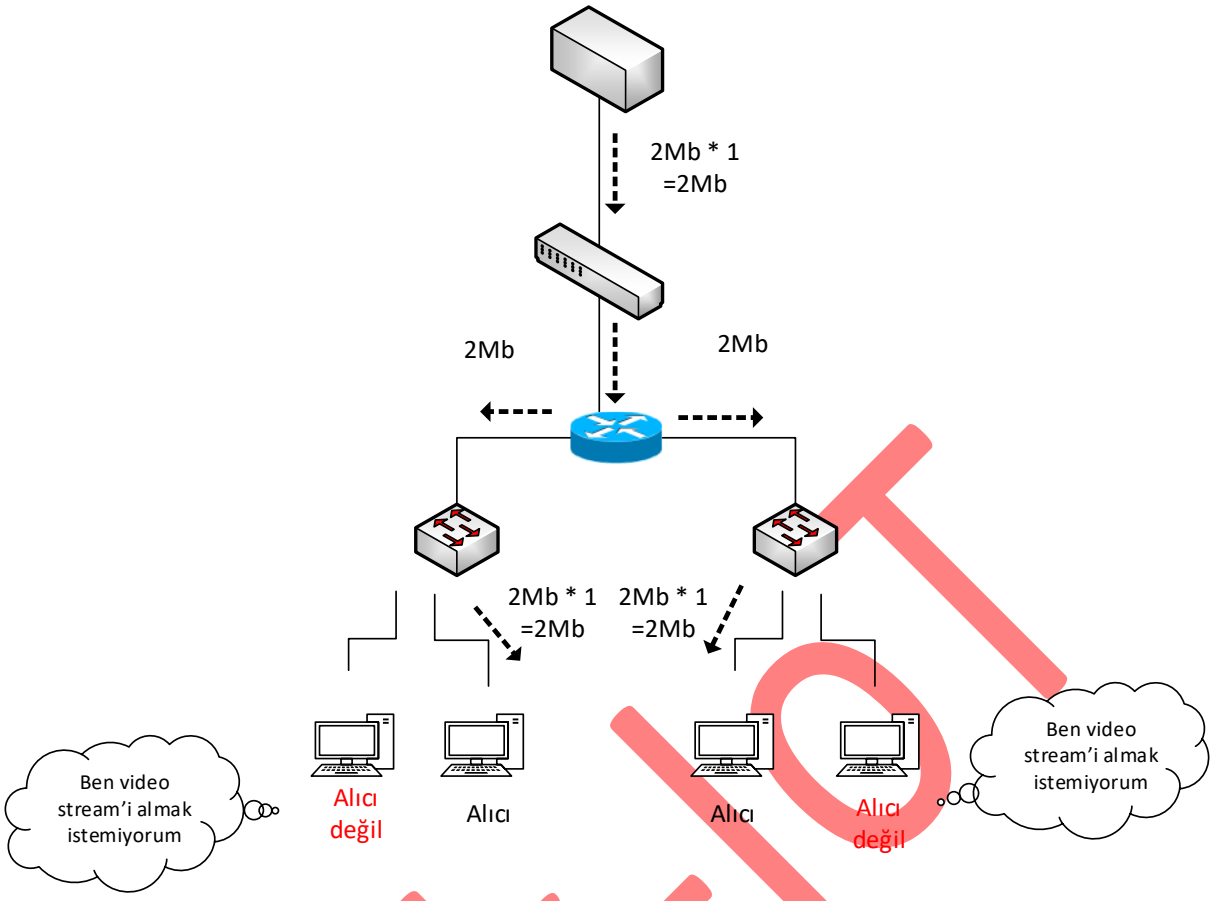
Eğer LAN'da yüzlerce, binlerce alıcı olması durumunda, ağda gereksiz çok miktarda trafik geziyor olurdu.

Multimedia Trafikte Multicast aktarım Tipi :

Broadcast ve unicast arasındaki en efektif ve verimli çözümdür.

Server, her paketin bir kopyasını özel bir adrese gönderir. Bu adres birçok istemciyi tanımlayan bir adrestir. Bu class D bir IP adresidir.

Video server bir stream'i birden çok alıcıya gönderir.



Eğer alıcı sayısı artsa bile, bir mesajın yalnızca bir kopyası gönderildiği için video server üzerinde ekstra bir yük oluşmaz. Bu mesaj replike edilmektedir. Replike işlemi, alıcı sayısı bazındadır.

Multicast aktarım tipinde azalanlar :

1- Server işlem kabiliyeti,
2- Bant genişliği kullanımı,
3- Daha az host / router işlemi

Sonuç olarak, eğer multimedya bir trafik aktarımı yapacaksak örneğin video stream, en iyi çözüm multicast aktarım tipinin kullanılmasıdır.

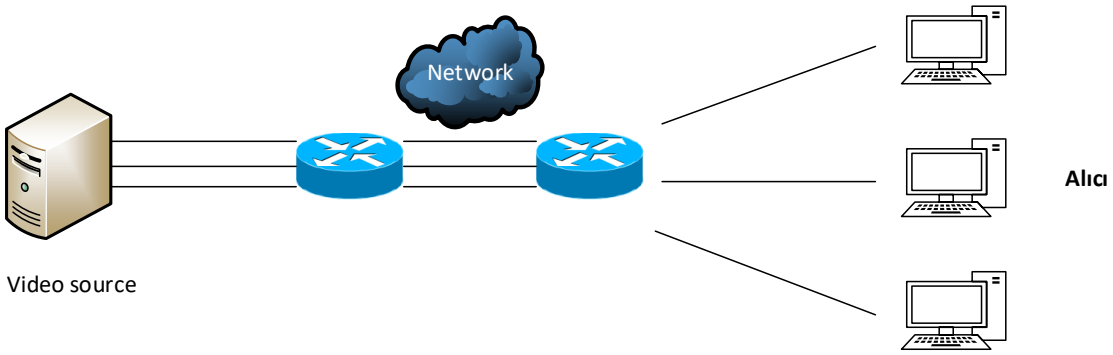
Kaynakların korunmasında Multicast nasıl yardımcı olur ?

Video kaynağı, video stream'i almak isteyen alıcılar için tek bir data beslemesi yapar.

Gönderici ya da multicast trafiğin kaynağı, alıcının/alıcıların unicast adreslerini bilmek zorunda değildir. (multicast grup adresine gönderir)

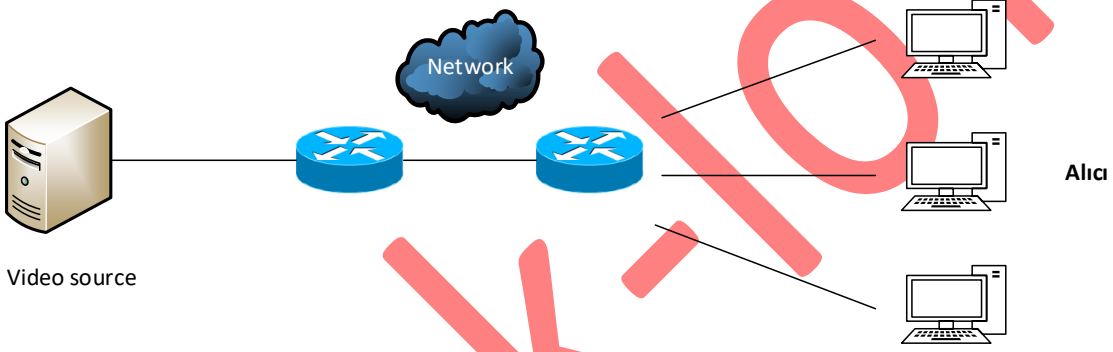
Paketi almak istemeyen alıcılar, paketi almazlar.

Unicast trafik tipi :

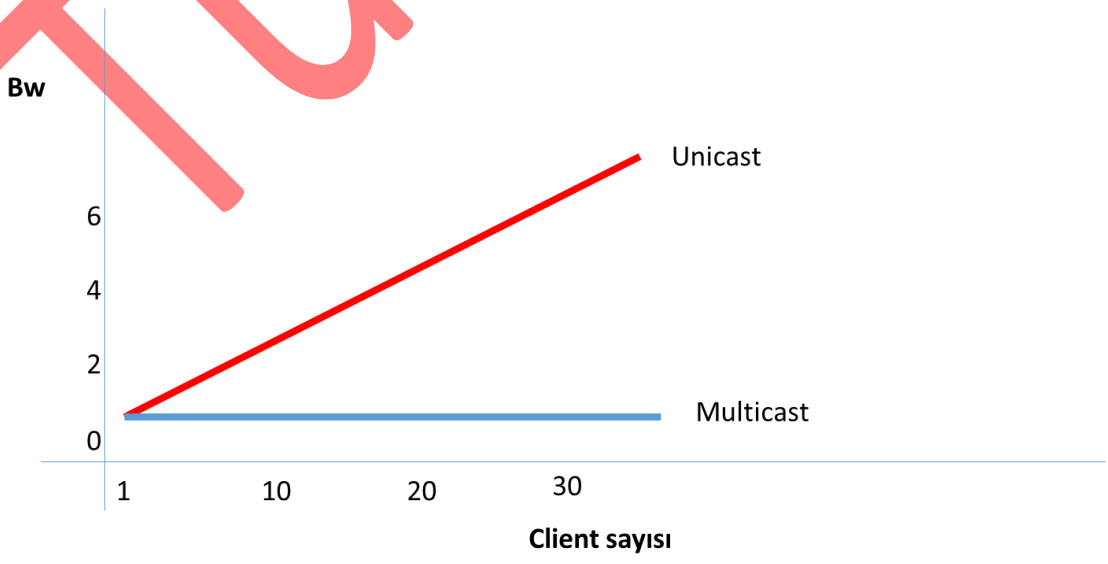


Video kaynağı çok sayıda aynı stream'i talep eden alıcılara, aynı stream'i üretir ve gönderir. Video kaynağı, hedefleri ya da alıcıların adreslerini bilmek zorundadır.

Multicast trafik tipi :



Video kaynağı ,özel bir grup adresine class D adrese iletir. Video kaynağı, video stream'i yalnızca bir kopyasını gönderir, router üzerinde çoklanır. Çoklama işlemi alıcı sayısına bağlı olarak yapılır. Yukarıdaki örnekte 3 alıcı bulunuyor ve 3'üne de çoklama yapılıyor. Video stream'i almak istemeyenler için çoklama yapılmaz.



Multicast trafik olduğu durumda;

Ağdaki bant genişliği kontrol edilir, göndericinin kaynaklarının tüketimini azaltır.

Multicast Dezavantajları :

UDP tabanlıdır.

Acknowledgement yok, en iyi eforla iletim,

Congestion avoidance mekanizması yoktur

Sırasız paket teslimi,

Multicast Nasıl Çalışır ?

Multicast uygulamalarda uçtan uca multicast olarak tasarlanmış olması gerekmektedir.

Video kaynağı, layer 3 adres (Class D) ile yapılandırılmış olmalıdır. Örneğin 224.5.5.5 gibi.

Multicast uygulama tüm istemcilerde yüklenmiş olmalıdır. Örneğin VLC ile IP güvenlik kamerasından live video talebi, bu talebi yaparken multicast grup adresine yapılmasına.

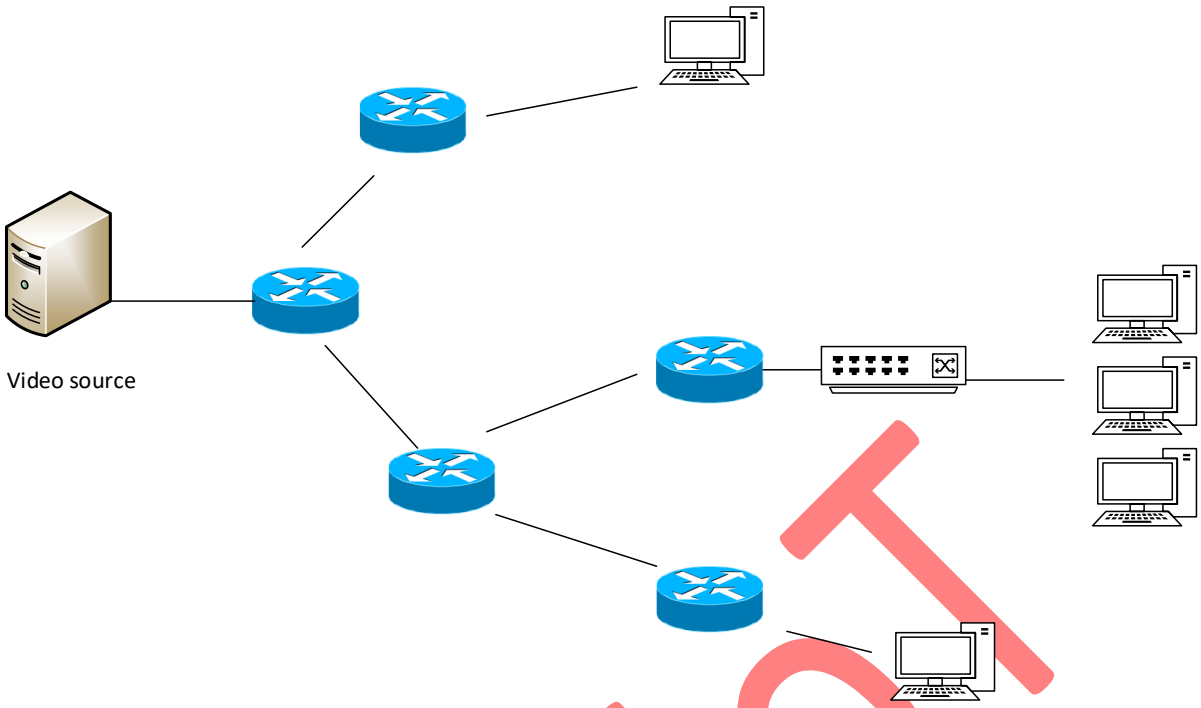
Multicast trafiği almak istediğini en yakındaki Router'a bildir. (IGMP)

Client, ya da multicast uygulamanın yüklü olduğu client, video source'un nerede olduğunu araştırmaya başlayacak. Bu bazı routing protokolleri ile gerçekleştirilmektedir. Bunlar MULTICAST ROUTING PROTOKOL olarak bilinir. PIM-Protocol Independent Multicast örnek verebiliriz.

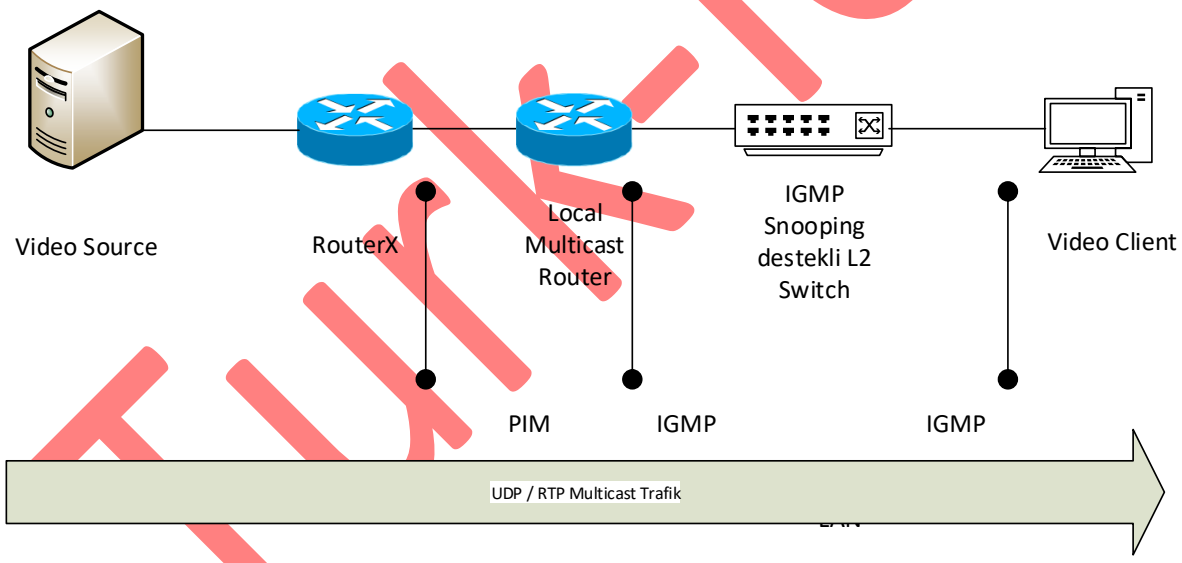
IGMP, client'tan router'a bir istek göndermekten sorumlu olan protokoldür.

Layer 2 multicast MAC Adresini hesapla. (IGMP Snooping/CGMP) Switch'ler IP'yi anlamaz. Bu yüzden multicast IP adresi eşleniği olan MAC adresine dönüştürülmelidir. Sonrasında switch hangi porttan multicast trafiğin gideceğini anlayabilir.

Multicast Grup IP adresi nedir ?
Bir multicast grup IP adresi, hem source ve alıcılar tarafından multicast paket göndermek ve almak amacıyla kullanılmaktadır. source data paketlerinde, grup adresini destination adresi olarak kullanır. Alıcılar, bu gruba gönderilen paketleri almak için ağı bilgilendirmek amacıyla bu grup adresini kullanır.



2 farklı protokol tüm multicast trafiğinden sorumludur.



Client, IGMP protokolünü kullanarak Router'a istek gönderir.

IGMP, Router – Client arasındaki protokoldür.

Router – Router arasında PIM protokolü bulunur. PIM protokolü aracılığı ile video source'un nerede olduğu bilinir.

Layer 2 multicast MAC Adresini hesapla. (IGMP Snooping/CGMP) Switch'ler IP'yi anlamaz. Bu yüzden multicast IP adresi eşleniği olan MAC adresine dönüştürülmelidir. Sonrasında switch hangi porttan multicast trafiğin gideceğini anlayabilir.

Multicast IP Yapısı :

IANA (Internet Assigned Numbers Authority) Class D IP adreslerini multicast uygulamalar için rezerve etmiştir.

224.0.0.0 – 239.255.255.255

1	1	1	0	Multicast Grup ID 28 bit

Destination IP adres : Multicast

Source IP adres : Unicast

Class D adres aralığı, yalnızca grup adresi ya da IP multicast trafiğin hedef adresi olarak kullanılır.

Multicast datagramlar için kaynak adres daima unicast kaynak adresidir.

Video server, alıcı client'ların unicast adreslerine yayın yapmaz. Bunun yerine grup adresine gönderim yapar. Eğer alıcılar yayını almak istiyorlarsa, multicast grup adresine join olurlar.

Multicast IP adresleri :

1- Permanent multicast groups :
   a. 224.0.0.0 – 224.0.1.255 aralığındaki adresler
   b. Yönlendirme amacı olmayan multicast adresler : (rezerve edilmiş multicast adres)
      i. 224.0.0.0 – 224.0.0.255 **(aynı local segmentteki ağ protokolleri için rezerve edilmiştir. TTL değeri 1'dir. Router'lar bu adres aralığındaki paketleri yönlendirmez)**
   c. Yönlendirme amacı olan multicast adres aralığı :
      i. 224.0.1.0 – 224.0.1.255 (**224.0.1.39 ve 224.0.1.40 IP adresleri PIM RP mesajları için rezerve edilmiştir.**)
2- Source Spesifik Multicast (SSM)
   a. 232.0.0.0 – 232.255.255.255 aralığındaki adresler
3- Private multicast adresler :
   a. 239.0.0.0 – 239.255.255.255 (kurum organizasyon içinde kullanılan private IP adreslerine benzetebiliriz. Amaç hemen hemen aynıdır.)

Örneğin ağımızda multicast çalışan PC'ler olsun, bağlantıyı kontrol etmek ve multicast çalıştıran tüm host'lardan yanıt almak için kullanılır. 224.0.0.1

Tüm multicast çalıştıran host'lar bu gruba join olmak zorundadır.

Eğer 224.0.0.1 adresine ICMP echo request gönderilirse, aynı ağdaki tüm multicast destekli hostlar ICMP reply ile yanıt verir.

Network protokolleri otomatik router keşfi için bu adresleri kullanır ve önemli routing datalarını iletirler.

Örneğin OSPF 224.0.0.5 ve 224.0.0.6 IP adreslerini link-state bilgisinin değişimi için kullanır.

224.0.0.9, tüm RIPv2 destekli router'lar.

224.0.0.13 Tüm PIM router'lar için.

BÖLÜM 2 / IGMP – PIM Protokolleri :

IGMP Protokol ve versiyonları :

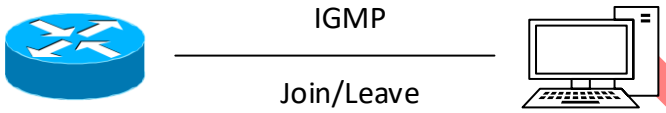
Multicast için kullanılan protokoller :

IGMP ve PIM

IGMP – Internet Group Management Protocol : End host ile router iletişimi,

PIM - Protocol Independent Multicast : Router – Router iletişimi,

IGMP :



Router ile bağlı olan hostlar arasında iletişimi sağlar.

IGMP'nin temelde 2 temel görevi vardır.

1- Bir hostun spesifik bir gruptan multicast trafik almak istediğini, local multicast router'a bildirir.
2- Bir hostun multicast bir uygulamayı kapattığında, bir multicast gruptan ayrılmak istediğini bir local multicast router'a bildirir.

IGMP Versiyonları :

IGMPv1

IGMPv2 (varsayılan)

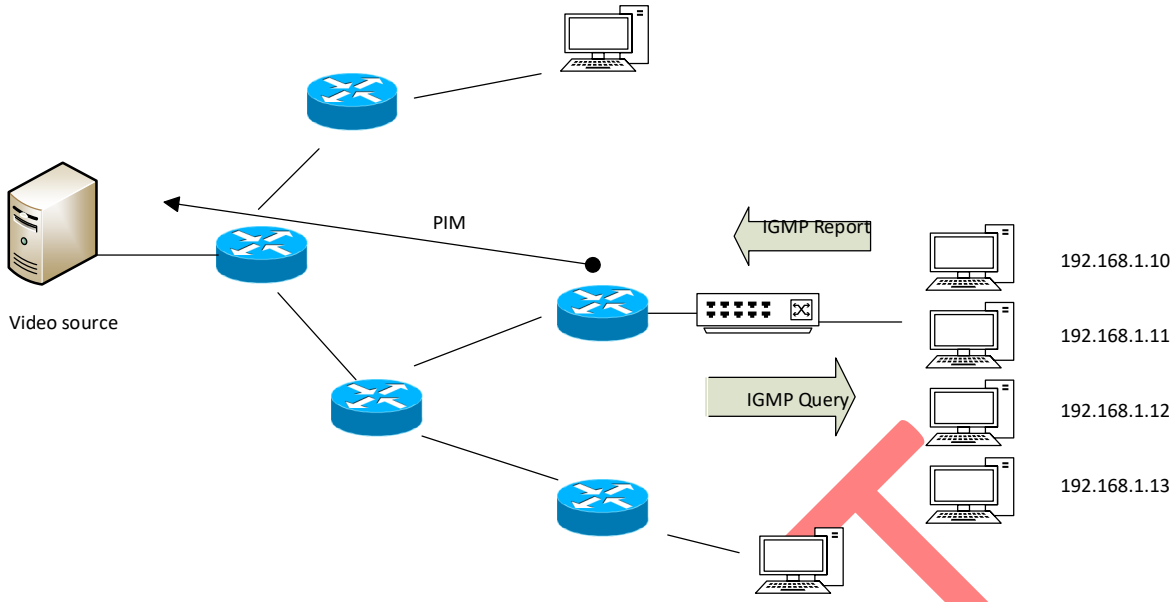
IGMPv3

IGMP v1 :

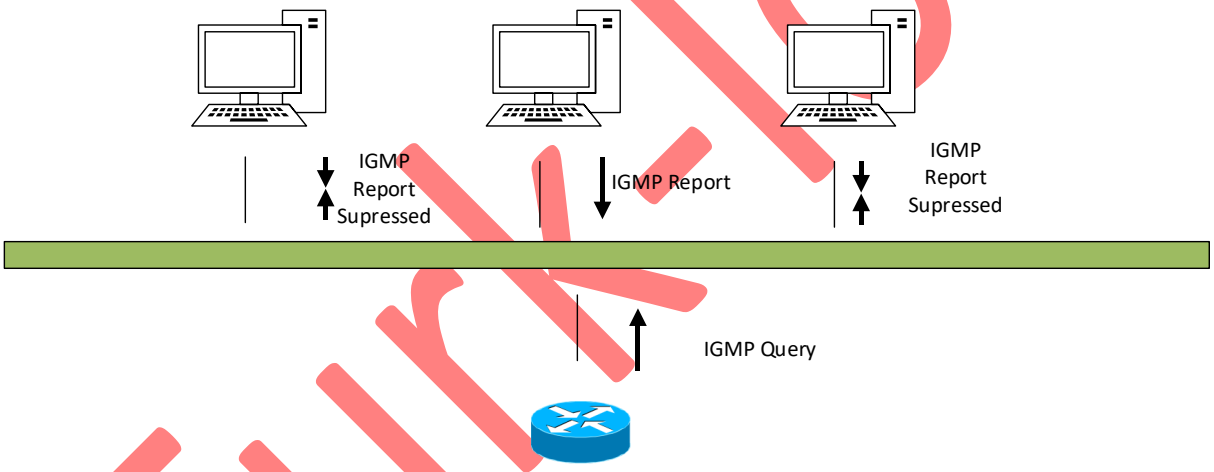
IGMP, 2 spesifik mesaj yapısını kullanır. REPORT MESSAGE, QUERY MESSAGE

Report message : **client** tarafından gruba join olmak için kullanılır.

Query message : grubun üyeleri halen mevcut mu değil mi bunu tespit etmek için **router** tarafından kullanılır. Multicast router tarafından devamlı 224.0.0.1'e gönderilir. Router, alıcılara halen multicast trafiği almak istiyor musun istemiyor musunu sorar.



IGMPv1 devamı :



Router periyodik olarak 224.0.0.1 adresine IGMP query'leri gönderir.

Örneğin en sağdaki host, multicast trafiği almayı durdurmak istediğinde, router bunu bilmez.

Host'lar sessiz bir şekilde gruptan ayrılır.

IGMP query aralığı 60 saniyedir ve 180 saniye içinde hostun multicast grup adresine join isteğini görmezse, bu süre sonuna kadar halen multicast trafiği göndermeye devam eder ve keser.

Ancak host'ların gruptan ayrıldığı bilgisi gelmez.

IGMPv2 :

IGMPv2 , birkaç yeni iyileştirmeye sahiptir. V1 ile v2 arasındaki en önemli gelişme, Leave group message'dır.

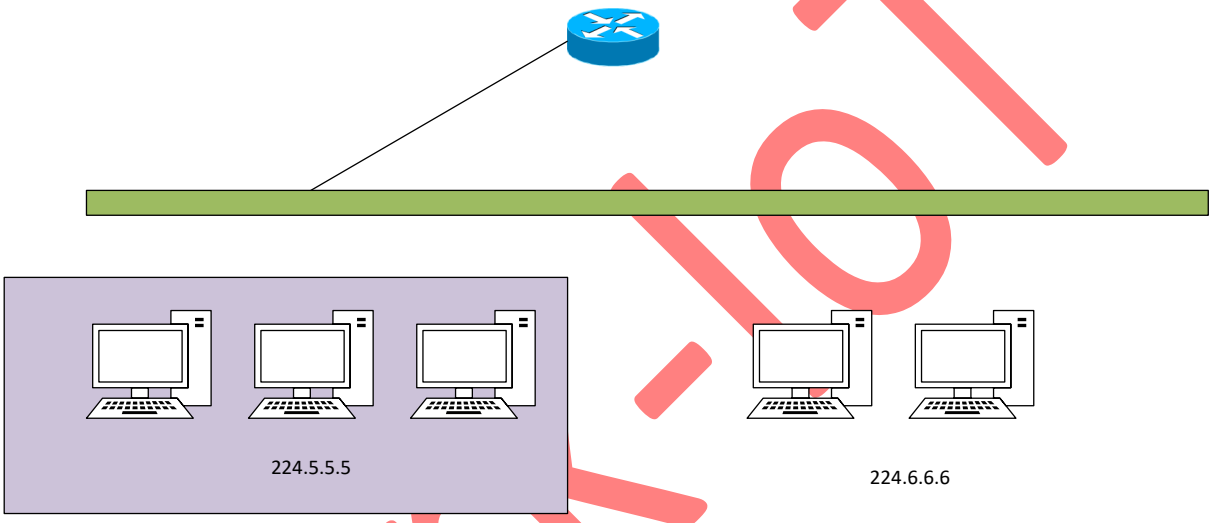
1- Report ve query mesajından bağımsız olarak, hosttan router'a **Leave Grup** mesajı,
2- Tunable timers
3- Querier election

4- Group spesific queries

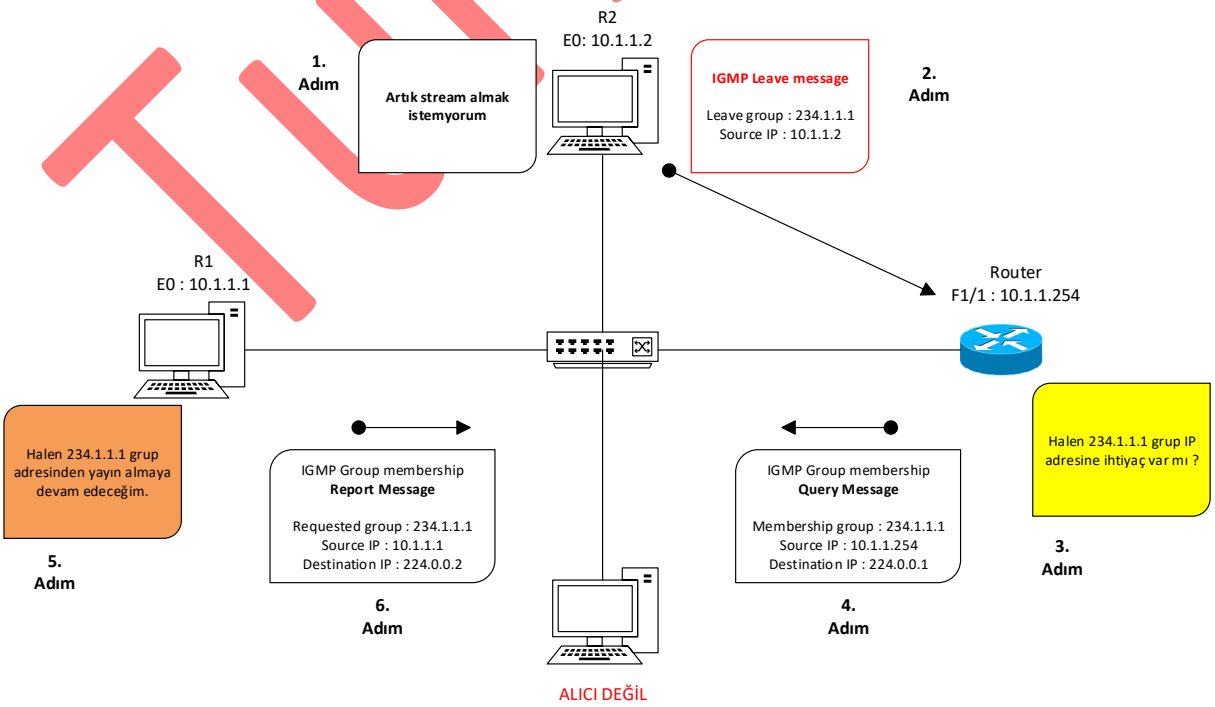
Multicast olarak video,ses trafiğini alan host, leave mesajı gönderirse, Router bu sefer kalan hostlara query mesajı gönderir. Halen trafiği almak istiyor musunuz diye sorar. Hangi host/lar yanıt dönerse, multicast streaming yalnızca bu hostlara devam eder ve cevap vermeyen hostlar için multicast streaming durur.

Eğer birden fazla router'a sahipsek, querier election yapabiliriz.

Query mesajlarını spesifik bir gruba gönderebiliriz.



Leave Group message mantığı : (224.0.0.2 – aynı ağ segmentindeki tüm router'ların multicast grup adresi)



IGMP Leave Group :

Bir client gruptan ayrılmak istediğinde, IGMP Leave Message'ını 224.0.0.2 adresine gönderir.

Sonrasında Router 224.0.0.1 adresine IGMP Query Message gönderir.

Grupta 1 client varsa bile, switch IGMP report message'ını ilk hop'taki router'a iletecektir.

IGMPv1'de 224.0.0.1 adresi aracılığı ile tüm hostlara IGMP query mesajı gönderilir. IGMPv2'de spesifik bir gruptaki cihazlara yapılabilir.

IGMPv3 :

Source spesific multicast yapmaya izin verir.

V1, v2 yalnızca grup spesifik multicast saplar. (*,G) -> herhangi bir kaynağa bağlan / spesifik grup

Yani spesifik bir gruptaki herhangi bir kaynağa bağlan demektir.

V3 source spesifik multicast destekler. (S,G)

R1 normalde source 192.168.1.2, 234.1.1.2 grup adresi aracılığı ile yayını alırken, R1 yani Receiver1, IGMP Change State yapar.

INCLUDE grp 234.1.1.3 src 192.168.1.3

EXCLUDE grp 234.1.1.2 src 192.168.1.2

IGMPv1 v2'de (*,G) herhangi bir kaynaktan gelirken, v3'te source tanımı yapılabilir.

Protocol Independent Multicast (PIM) :

Multicast routing farklı protokoller ile yapılabilmektedir.

- Distance vector Multicast Routing Protocol (DVMRP) (legacy)
- Multicast OSPF (MOSPF) (legacy)
- Protocol Independent Multicast (PIM)

Günümüzde yaygın olarak kullanılan PIM protokolüdür.

Multicast routing protokolü, router tarafından multicast yayın yapan kaynağa nasıl ulaşabileceğini bulmaya çalışır.

PIM :

Protocol Independent Multicast

Router – Router iletişimini döngü olmaksızın sağlar

Ağda, yolları (route'ları) anons etmez. (IGP gibi)

PIM Modları :

Göndericiden alıcıya multicast ağaç yapısının nasıl olduğunu söyler.

PIM Dense mod

PIM Sparse mod

PIM modu, ağaç yapısının nasıl tasarlanacağını belirler, ve trafiği kim alacak..

Dense mod:

PIM Dense mod küçük ölçekli multicast uygulamaları için.

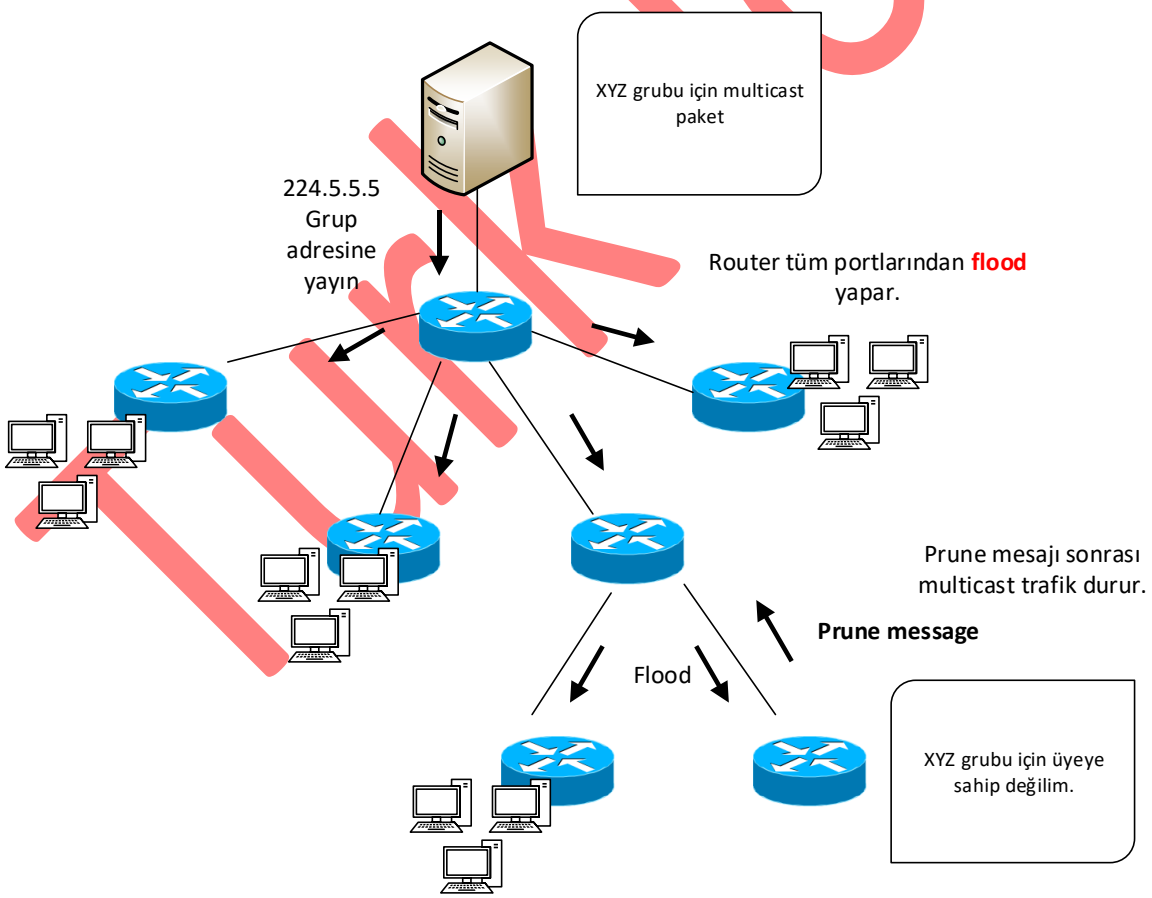
Prune mesajı 3 dk içinde expire olur ve yeniden flood başlar.

Bu durum periyodik olarak flooding ve pruning davranışıdır.

S,G

Flood ve prune davranışı kullanılır.

İmplicit join olarak adlandırılabilir



Eğer multicast yayını alacak bir alıcı yoksa, otomatik olarak prune.

Büyük ağlarda efektif bir PIM modu değildir. Çünkü trafik heryere iletilmektedir.

Sparse Mod :

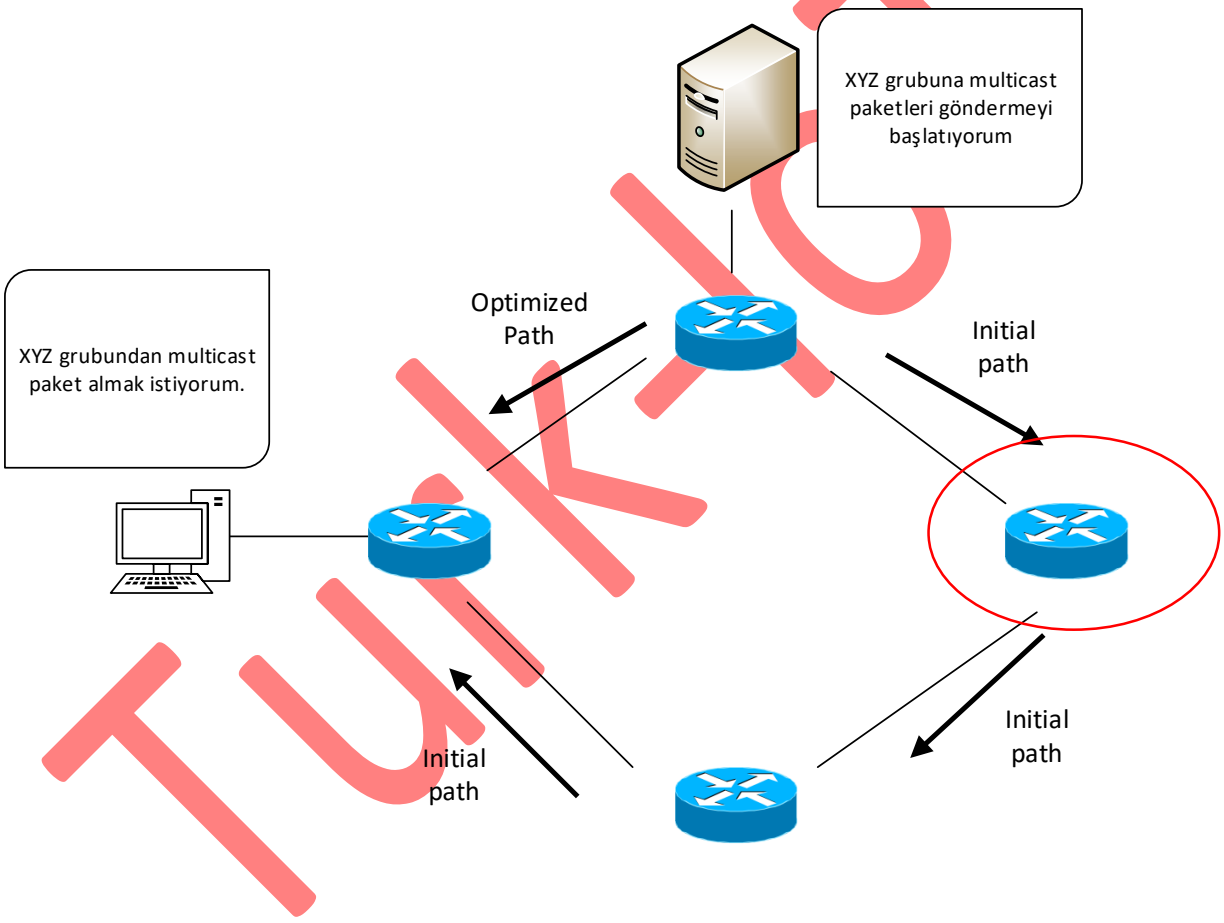
Explicit join olarak bilinir.

Join isteklerini işlemek için RP kullanır.

Topolojide multicast trafik gönderen bir gönderici ve alıcı bulunmaktadır. Göndericinin bağlı olduğu Router,multicast trafiği flood yapmaz. Bunun yerine hem gönderici hem de alıcı Rendezvous Point'e join olurlar.

RP (Rendezvous Point) trafiğin göndericiden alıcıya nasıl gideceğinin kararı verir. Eğer multicast trafiği almak isteyen bir alıcı varsa,

Bu alıcı RP'ye join mesajı gönderir. Sender'da RP'ye join olur.



Source Tree vs Shared Tree :

Multicast tree, göndericiden alıcıya trafiğin nasıl yönlendirileceğinin kararını verir.

Source Tree :

Göndericiden alıcıya en kısa IGP yolu (path) kullanır

Dense mod / Sparse mod

Shared Tree :

- Göndericiden RP'ye en kısa yolu kullanır.
- RP'den alıcıya en kısa yol,
- Sparse mod yalnızca, (RP yalnızca sparse modda)
- Flooding ve pruning kaldırır ve routing'i daha ölçeklenebilir yapar.

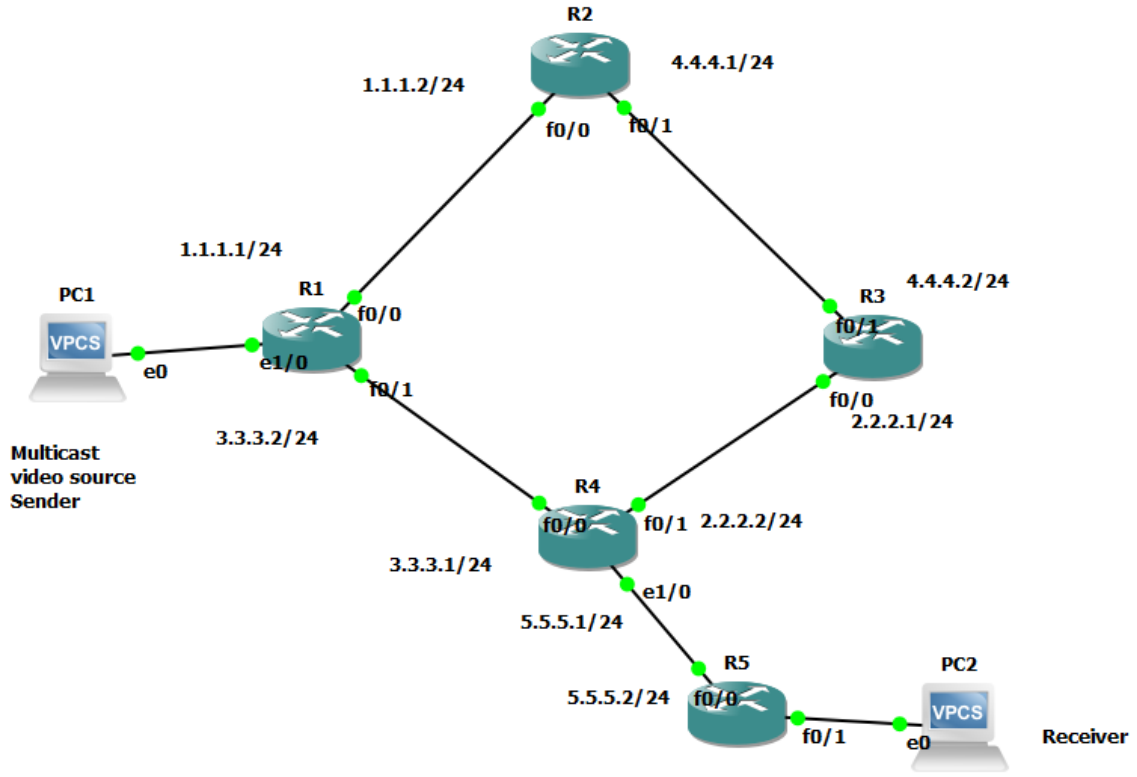
PIM Sparse modda öncelikle shared tree ile ağaç yapısı kurulur. Sonrasında source tree ile en kısa optimize yol yapılandırılır.

Shared tree'nin **dezavantajı**; gönderici ve alıcı arasındaki yol en optimal yol olmayabilir.

Bazı linkleri çok defa kullanabilir ve bazı linkler kullanılmayabilir.

RP'nin konumlandırması çok dikkatli bir şekilde yapılmalıdır.

PIM DENSE MOD UYGULAMASI :



Tüm router'lar arasında statik route ya da dynamic route protokollerinden birisini kullanarak, route tanımları yapılmalıdır.

```
conf t
router ospf 1
network 1.1.1.0 0.0.0.255 area 0
network 3.3.3.0 0.0.0.255 area 0
network 10.1.1.0 0.0.0.255 area 0
```

```
R1 (config)# ip multicast-routing
R1 (config)# int e1/0
R1 (config-if)# ip pim dense-mode
R1 (config-if)# int f0/0
R1 (config-if)# ip pim dense-mode
R1 (config-if)# int f0/1
R1 (config-if)# ip pim dense-mode

sh ip pim interface
sh ip pim neighbour
```

PIM Neighbours:

Tüm PIM aktif router'lara 224.0.0.13 adresinden "hello mesajı" kullanılır

Default hello = 30 saniye, dead = 90 saniye

sh ip pim neighbours

join-group komutu bir router'ın belirli grubun bir üyesi gibi davranmasını sağlar.

int f0/1

ip igmp join-group 224.5.5.5

show ip mroute 224.5.5.5

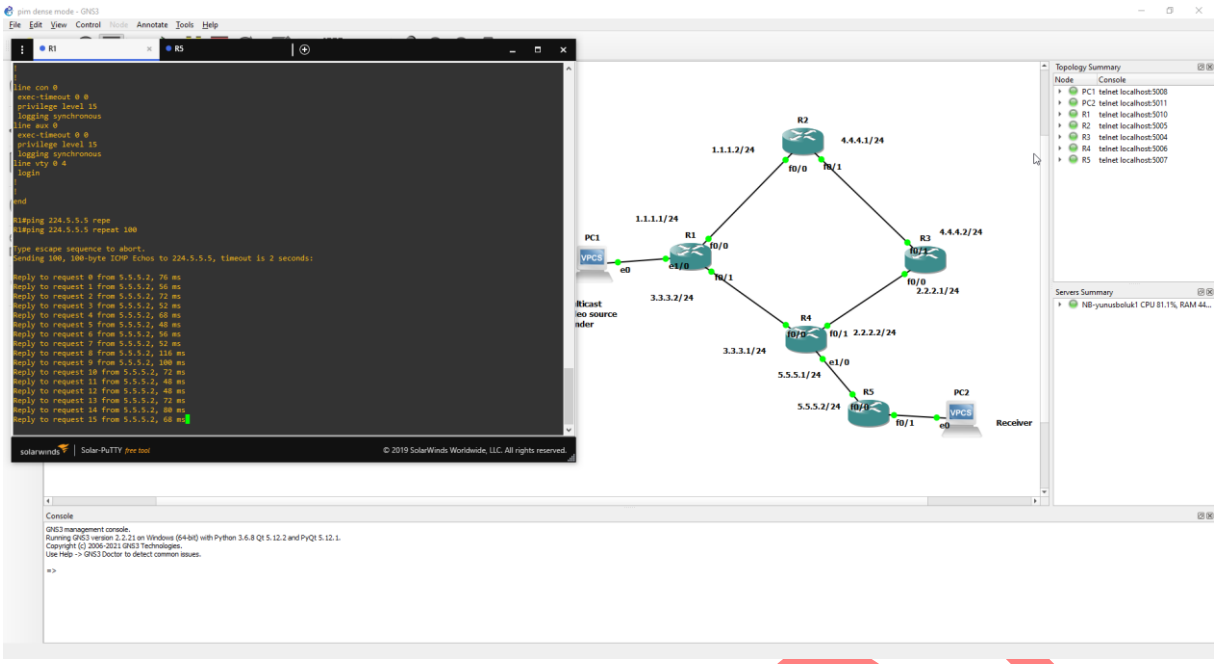
kontrol etmek için bu komutu kullanacağız. Bu komutu her router'da yazarak inceleme yaparız. R1,R2,R3,R4,R5.

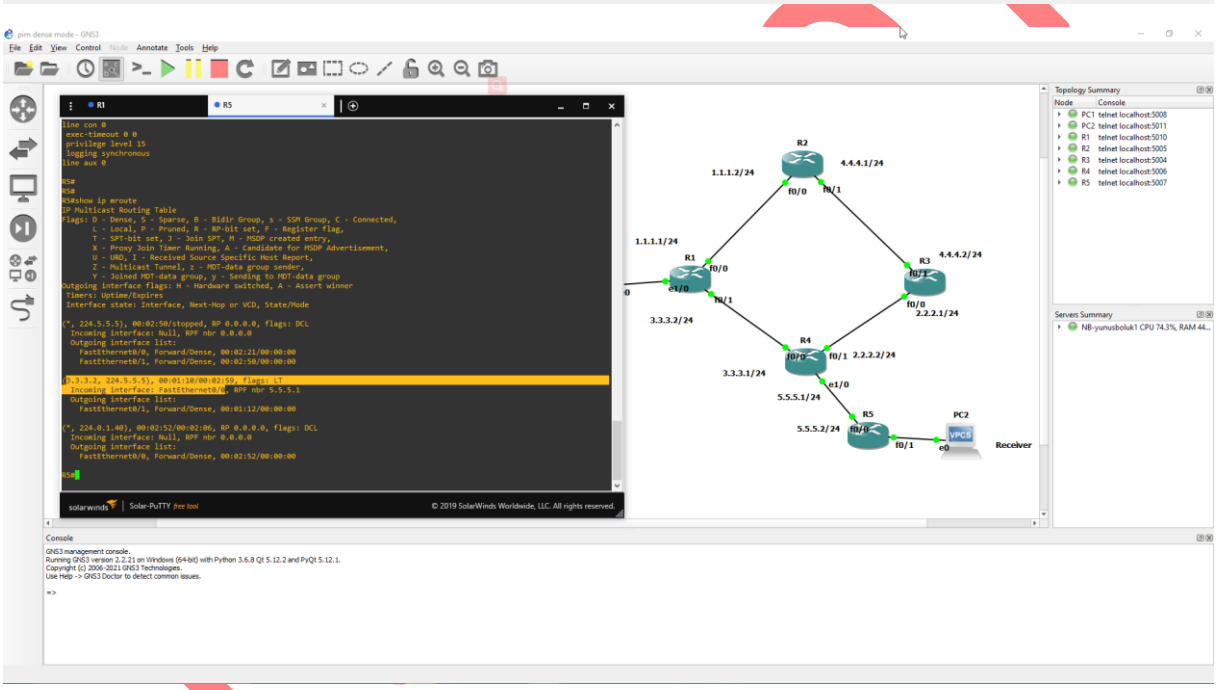
IP PIM Dense mod, flood / prune yapısındadır.

show ip mroute 224.5.5.5 yazdıktan sonra, Incoming interface null mu gözüküyor diye kontrol edilmeli.

Şimdi video source'tan 224.5.5.5 grup adresi için ping request oluşturacağız.

ping 224.5.5.5 repeat 100





(S,G) yapısı içinde düşünürsek, 224.5.5.5 grup IP adresinden, 3.3.3.2 source IP adresinden yayın alıyoruz.

3.3.3.2 IP adresi R1'in f0/1 ara yüzüdür.

Aslında bakacak olursak birden Source'a giden birden fazla yol olmasına rağmen, shortest path tercih edilmiştir.

show ip mroute 224.5.5.5

R4 ya da diğer Router'larda yazıp kontrol ettiğimizde, bildiğimiz gibi PIM DENSE MOD, flood/prune yapısındadır.

```
R3#sh ip mroute 224.5.5.5
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.5.5.5), 00:06:00/stopped, RP 0.0.0.0, flags: D
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Dense, 00:06:00/00:00:00
    FastEthernet0/0, Forward/Dense, 00:06:00/00:00:00

(1.1.1.1, 224.5.5.5), 00:06:00/00:00:17, flags: T
  Incoming interface: FastEthernet0/1, RPF nbr 4.4.4.1
  Outgoing interface list:
    FastEthernet0/0, Forward/Dense, 00:06:02/00:00:00

(3.3.3.2, 224.5.5.5), 00:06:02/00:00:15, flags: T
  Incoming interface: FastEthernet0/0, RPF nbr 2.2.2.2
  Outgoing interface list:
    FastEthernet0/1, Forward/Dense, 00:06:02/00:00:00

R3#
```

S,G yapısını incelediğimizde, R3'te (1.1.1.1,224.5.5.5) ve (3.3.3.2,224.5.5.5) olmak üzere 224.5.5.5 grup IP adresine 2 farklı source olduğunu görüyoruz. Trafiği R1'den generate etmiştik. R1 tüm interface'lerinden flood yaptı.

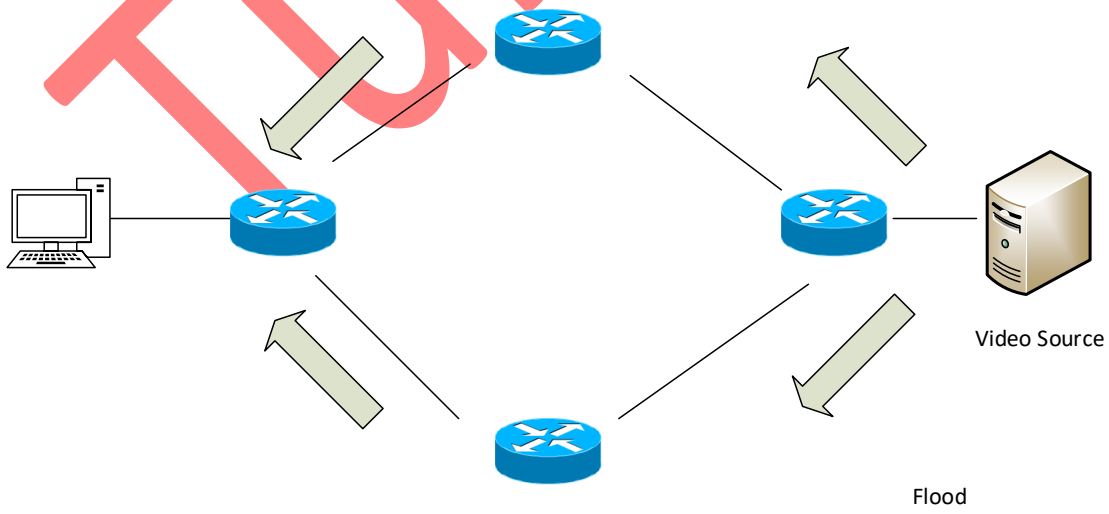
Topoloji içinde R5 router'ı dışında alıcı olmadığı için diğer router'lardan prune mesajı üretilir.

RPF Check Mekanizması :

Duplike paketleri alma konusu ile başa çıkabilmek için, Cisco router'lar Reverse Path Forwarding (RPF) yapar.

Multicast paket doğru interface'den girip girmediğinin kontrolünü yapar.

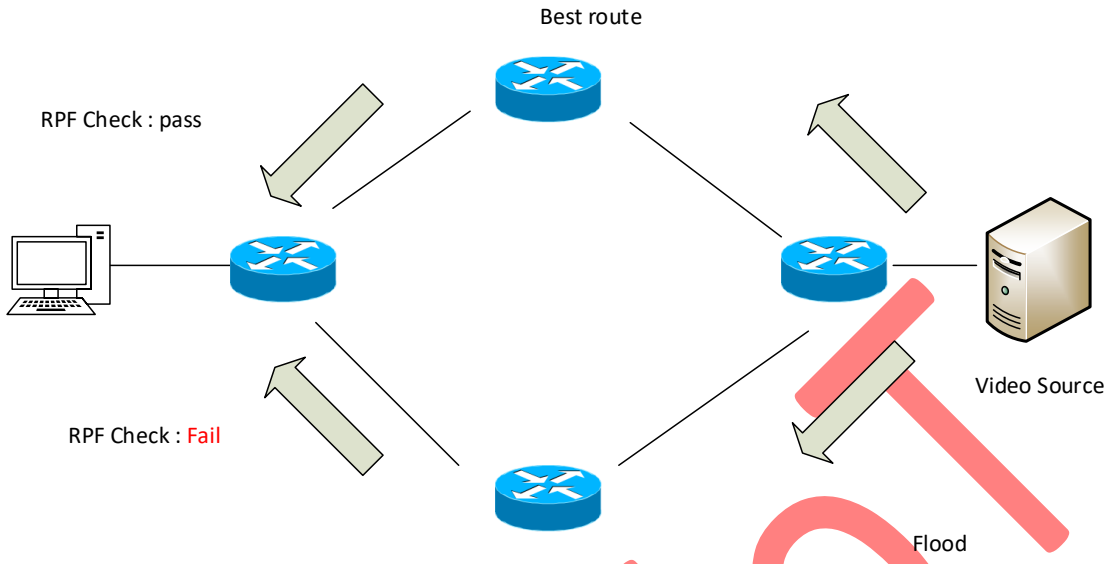
RPF, loop'ları önlemek içindir.



RPF mekanizması yoksa, multicast trafiği birden çok noktadan alıyor olacaktık. Alıcının olduğu noktadaki router multicast trafiğin nereden geldiğini nasıl bilecek ? Bilemez çünkü multicast trafik.

Bir router multicast paket aldığında, paketin source IP adresine bakacaktır.

Paketi en kısa hangi yol üzerinden alacağına bakar.



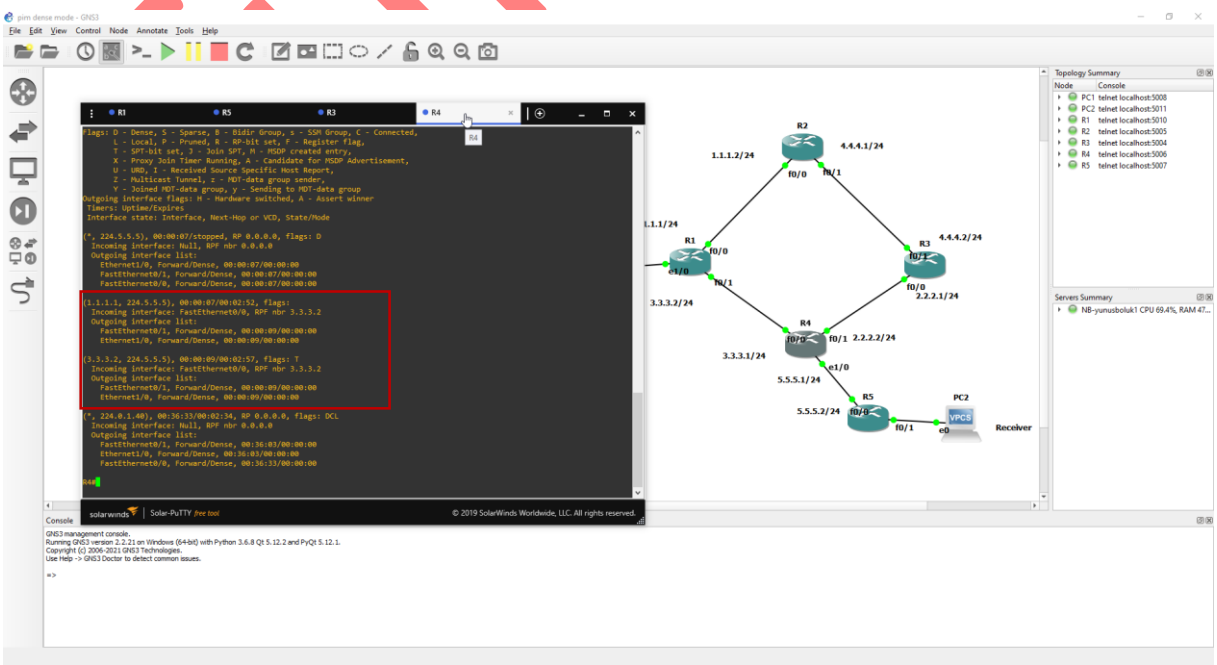
RPF check : fail olan interface multicast paketleri discard edecektir.

Yani RPF check: **pass** olan interface aracılığıyla multicast paketler alınmaktadır.

LAB yapalım.

1- IGP – OSPF konfigüre edilmiş olmalıdır
2- Dense mode yapılandırılmış olmalıdır.
3- Receiver olan R5'te join-group yapılandırılmalıdır.

R4'e bakacak olursak en az 2 interface'ten multicast trafik alabilir durumdadır.



RPF check pass olan interface 3.3.3.2 olan interface'tir. Nedeni en kısa ya da en iyi yol olmasıdır.

show ip mroute

"show ip route connected" ile bakarsanız aslında 3.3.3.2 bacağının directly connected ya da doğrudan bağlantı olduğunu görürüz. Directly connected yollar en kısa yollardır.

```
Reply to request 42 from 5.5.5.2, 56 ms
Reply to request 43 from 5.5.5.2, 48 ms
Reply to request 44 from 5.5.5.2, 60 ms
Reply to request 45 from 5.5.5.2, 48 ms
Reply to request 46 from 5.5.5.2, 60 ms
Reply to request 47 from 5.5.5.2, 44 ms
Reply to request 48 from 5.5.5.2, 64 ms
Reply to request 49 from 5.5.5.2, 64 ms
R1#ping 224.5.5.5 repeat 50

Type escape sequence to abort.
Sending 50, 100-byte ICMP Echos to 224.5.5.5, timeout is 2 seconds:

Reply to request 0 from 5.5.5.2, 60 ms
Reply to request 1 from 5.5.5.2, 72 ms
```

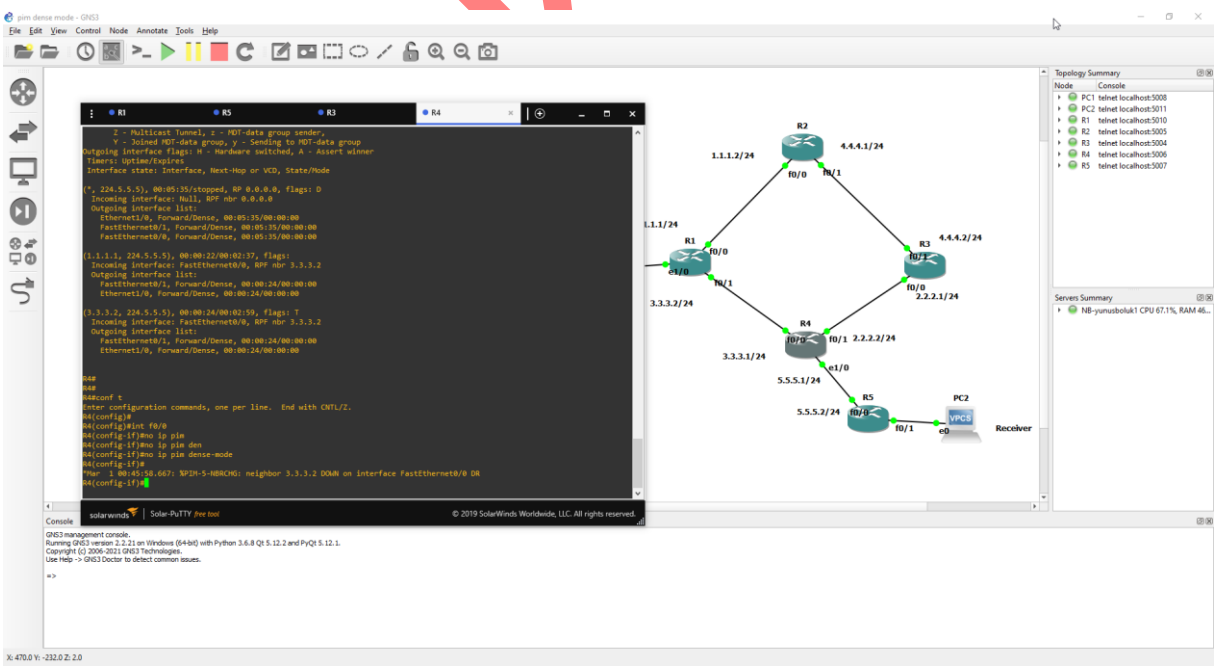
R4 router'ının incoming interface'i : f0/0

Outgoing interface'i : f0/1 ve e1/0'dır.

Eğer R4'ün f0/0 ara yüzünde pim dense modu devre dışı bırakırsak;

int f0/0

no ip pim dense-mode



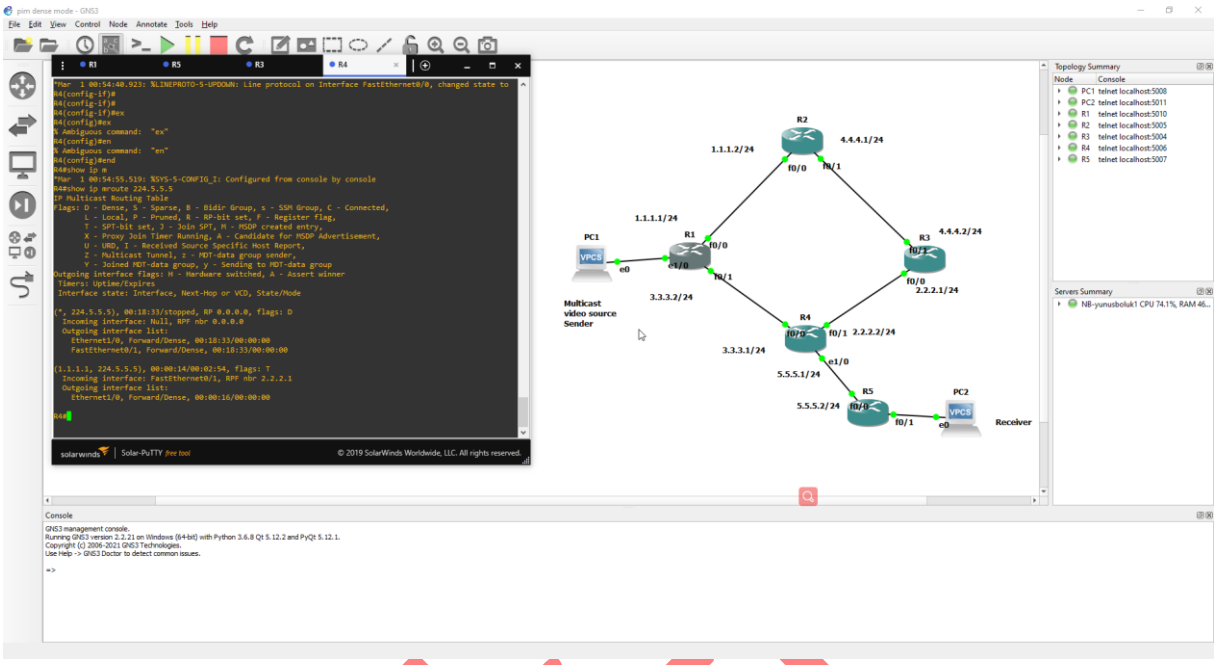
Önemli husus, router'lar tarafından kullanılan IGP yolunun best path olması gerekmektedir ve bu best path üzerinde multicast aktifleştirilmiş olmalıdır. Dolayısıyla directly connected interface varsa bu yolda pim dense mod aktif olmalıdır.

Eğer link kapalıysa – (shutdown) böyle bir durumda yol değişecektir.

R4 içine girip :

int f0/0 ara yüzünü kapatalım.

Shutdown

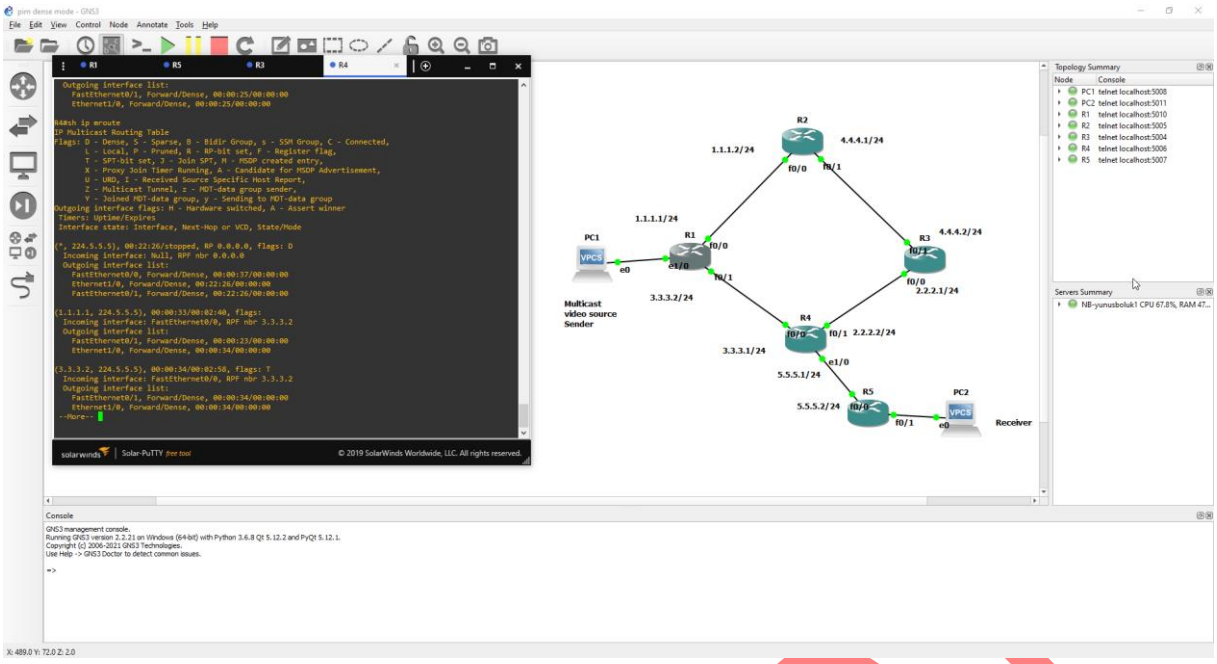


RPF check pass olan yol 2.2.2.1'dir.

S : 1.1.1.1

G : 224.5.5.5

R4 f0/0 interface'ini no shutdown ile aktif yaptıktan sonra :



RPF check işlemi otomatik olarak gerçekleştirilmektedir.

Ya da son olarak bazen router'ın bazı interface'lerinin multicast trafik ile ilgili bir işlem yapmasını istemediğinizde static route yazılabilir.

R4 : ip mroute 0.0.0.0 0.0.0.0 2.2.2.1

Static route, dynamic route'a göre AD değeri daha düşük olduğu için önceliklidir ve bu yol aracılığı ile gider.

***Troubleshooting Notu** :*

Eğer R1'den R5'e ping 224.5.5.5 grup IP adresine gidilemiyorsa, RPF check kontrol edilmelidir.

sh ip mroute yazdığımızda, Incoming interface null olarak gelir.

BÖLÜM -3 : PIM SPARSE MOD :

Explicit join metodu, yani sen talep etmedikçe multicast trafik almazsın, dense modda flood/prune davranışı vardı hatırlayın ☺ Explicit join'de multicast trafiği almak istiyorum dersin.

Hem shared tree hem de source tree yapısını kullanır

Daha ölçeklenebilirdir.

PIM Sparse modda flooding yoktur. Multicast trafiği yalnızca trafiği almak isteyen alıcıya gönderir.

PIM Sparse mod 6 adımda çalışır.

1- PIM komşularını keşfeder (Discover PIM Neighbours)
2- RP'yi keşfeder (Discover RP)

3- RP göndericiyi ya da video,ses kaynağını dinler. (PIM register)
4- RP, alıcıları dinler (PIM join)
5- Göndericiden alıcıya doğru RP aracılığı ile shared tree yapılandırır.
6- En kısa yol ile join olur

Router'lar arasında int fx/y , ip pim sparse-mode konfigürasyonu bulunur.

```
int fx/y
ip pim sparse-mode
```

Bu komutları topoloji içindeki Router'ların interface'lerinde aktifleştirdikten sonra, komşuları keşfedecektir. Her 30 sn'de bir komşular arasında "Hello" mesajı yayınlanır. Dead time 90 sn'dir.

İkinci aşamada Router'lar, RP'ye karar vermeleri gerekiyor ve her router'ın RP'yi öğrenmesi gerekiyor. RP, ağaç yapısının köküdür ya ni root of the tree ya da merkez nokta.

Video,ses göndericisi kaynak, RP'yi bilmelidir. Aynı şekilde kimler bu multicast trafiği almak istiyorsa RP'yi bilmelidir. RP'ye register olurlar.

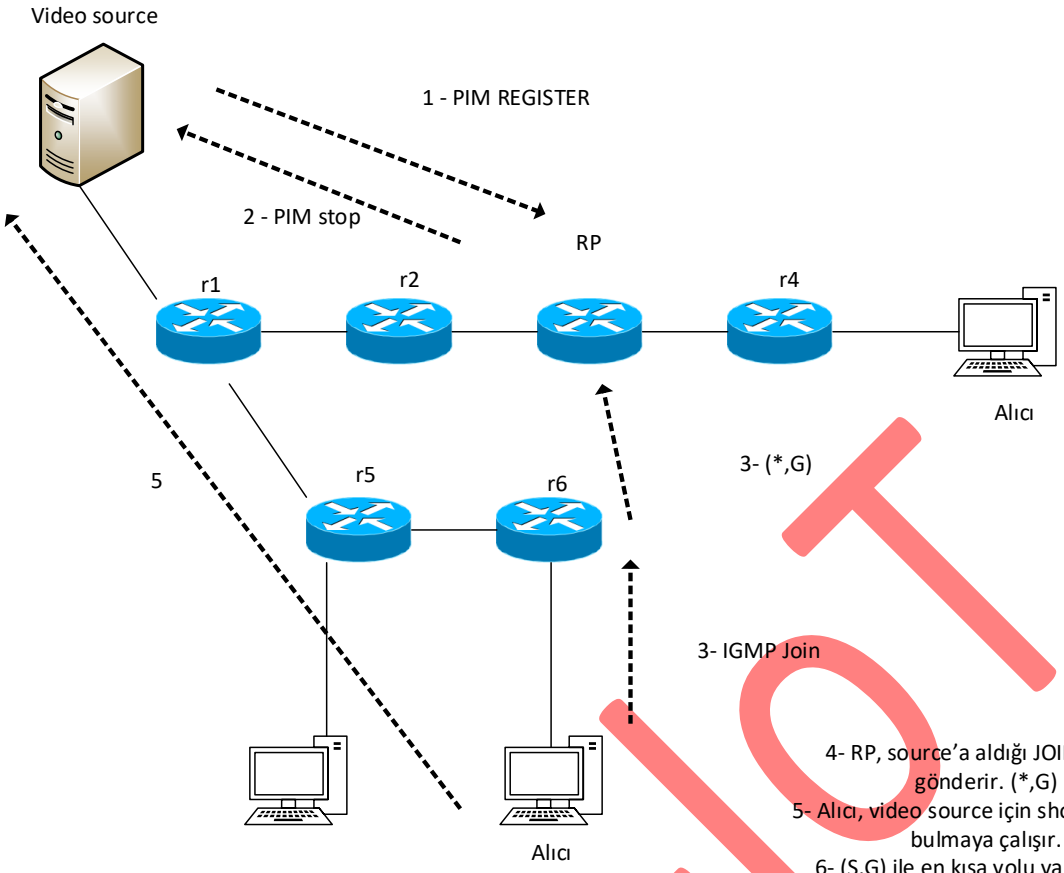
RP'yi manuel olarak seçip yapılandırabilirizde.

Kaynak, RP'ye register olurken, unicast olarak PIM Register mesajı gönderir. RP mesajı aldıktan sonra, onay döner. Bu mesaj Register Stop'tur. Artık RP, video source'u bilir. (Source,Group) bilgisine sahiptir.

Bu noktada RP, video kaynağını bilir. Diğer router'lar henüz bunu bilmiyor.

Bu arada Source, RP'ye PIM Register mesajı gönderdiğinde, RP; RPF'i kontrol eder ve hangi interface'den multicast trafiğin geleceğini bilir.

Şimdi, ağda multicast trafiği almak isteyen alıcı ya da alıcılar varsa, IGMP join mesajı en yakın local Router'a request yapar. Bu local router / first hop router, RP'ye döner ve der ki , Merhaba RP, ben multicast trafik almak isteyen bir alıcıya sahibim. (*,G)

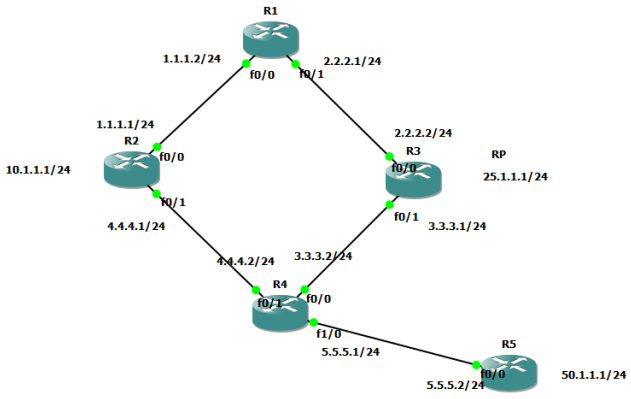


Artık alıcının olduğu local router ya da first hop router (S,G) bilgisi ile en kısa yolu yapılandırdığından, bu router, RP'ye PRUNE mesajı gönderir.

SPARSE MOD KONFİGÜRASYONU :

Tanımlar :

RP : Rendezvous Point

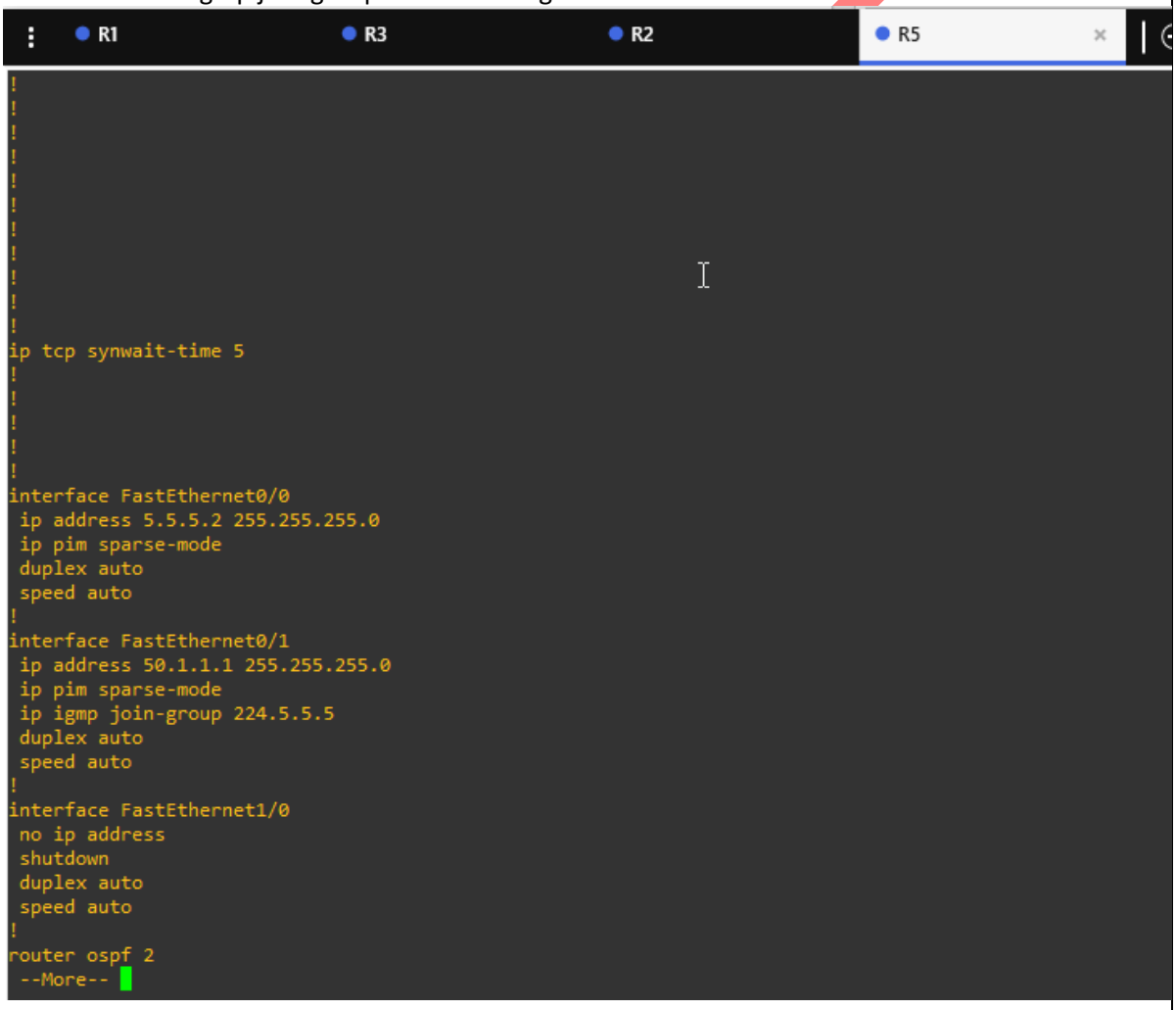


Temelde tüm router'larda yapılandırma :
1 - Router'lar arasında IGP (OSPF area) tanımı
2- ip pim sparse-mode

ip multicast-routing
int fx/y
ip pim sparse-mode

3- **ip pim sparse mod aktif interface'leri görüntüleme:**
sh ip pim int

4- R5 router'da igmp join-group simüle edeceğiz.



İgmp join-group konfigürasyonu sonrası, igmp join mesajı gönderilecek ancak nereye gönderecek ? Çünkü PIM Sparse modda igmp join mesajı, RP'ye gönderilmelidir ancak henüz RP yok.

224.5.5.5 grup adresine, R1'den ICMP echo request yapalım. Reply göremeyeceğiz.
Eğer RP – Rendezvous Point yoksa, Source kaydolamaz. Join istekleri işlenemez.

RP tanımı için aşağıdaki komutu tüm router'larda yapılandırmak gerekiyor.

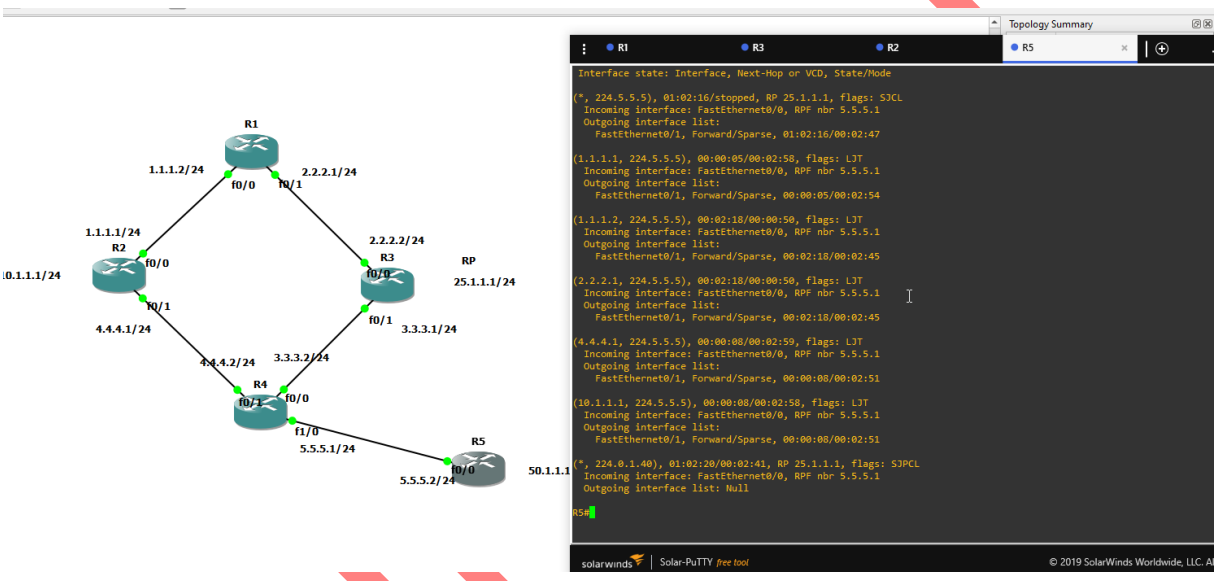
R1(config)# ip pim rp-address **ipaddress**
Örnek : ip pim rp-address 25.1.1.1

Yapılandırılan RP'yi görmek için :
show ip pim rp mapping

```
R1#show ip pim rp mapping
PIM Group-to-RP Mappings

Group(s): 224.0.0.0/4, Static
    RP: 25.1.1.1 (?)
R1#
```

Tüm grup için RP adresi 25.1.1.1 adresidir.

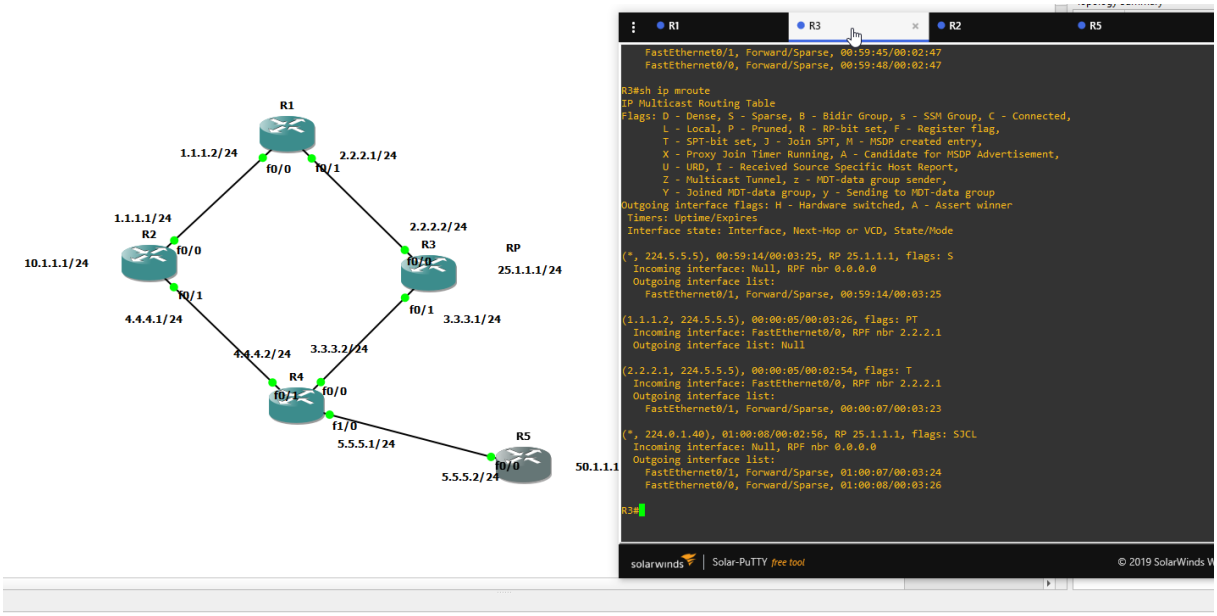


R2 router'ından, **ping 224.5.5.5 repeat 10** yazdıktan sonra;

R5 router'ında **show ip mroute** ile kontrol yapıyoruz.

İlk satırda (*,G) -> (*,224.5.5.5) olduğunu ve sonradan stopped olduğunu görüyoruz. RP bilgisi 25.1.1.1 olarak düşmüş. En son satırda (S,G) bilgisini görüyoruz. (10.1.1.1,224.5.5.5)

R3'te baktığımızda, trafiğin 2.2.2.1 ara yüzünden geldiğini görüyoruz. Best path olması sebebiyle.



RP (Rendezvous Point) YAPILANDIRMASI :

1- STATİK
2- DİNAMİK
   a. Auto-RP (Cisco proprietary metot)
   b. BSR (standart metot)

Statik RP :

- Manuel RP (Rendezvous Point) adresi her router üzerinde yapılandırılmış olmalıdır.
- Tüm router'lar aynı RP adresine sahip olmalıdır.
- RP fail-over mümkün değildir.

Büyük ölçekli yapılarda kullanımı zordur. Örneğin RP'nin değişimi gerektiğinde tüm router'larda RP değişiminin manuel olarak yapılması gerekmektedir.

```
Rx(config)# ip pim rp-address 25.1.1.1
```

Örnek PIM Sparse Mod Konfigürasyonu :

```
R4(config)# ip multicast-routing
R4(config)#int f0/0
R4(config-if)# ip pim sparse-mode
R4(config-if)#int s1/0
R4(config-if)#ip pim sparse-mode
R4(config-if)#int s1/1
R4(config-if)#ip pim sparse-mode

Rx(config)# ip pim rp-address 25.1.1.1
```

Auto-RP :

RP bilgisini öğrenirken kullanılır ve Legacy Cisco proprietary metodudur.

Tüm router'lar RP adresini otomatik olarak öğrenir.

Candidate RP yapılandırması dışında fazla bir konfigürasyon gerektirmez.

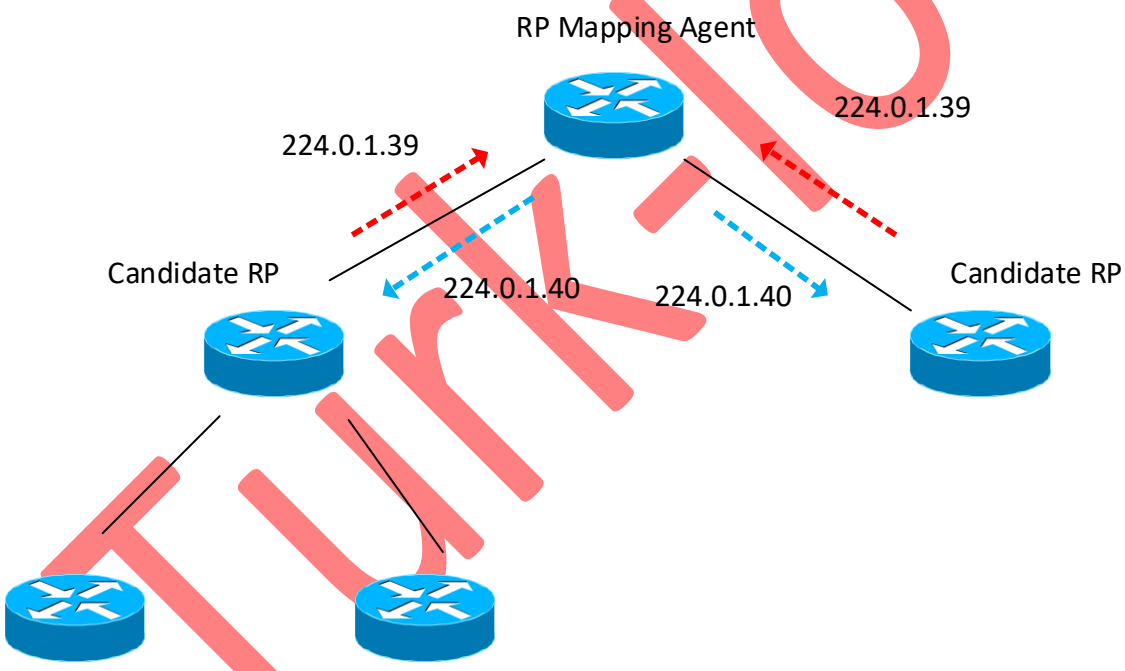
Candidate RP : RP olmak isteyen cihazdır.

Mapping-Agents : RP'yi dinler ve PIM domain'i içindeki diğer router'lara bu bilgiyi aktarır.

Back-up RP konfigürasyonu yapılmasını destekler.

Auto-RP Nasıl Çalışır ?

- Aday RP'ler / Candidate RP (S,224.0.1.39) kullanarak RP Mapping Agent'a yayın oluştururlar.
- Mapping Agent, RP mapping hakkında öğrenmek için (*,224.0.1.39) dinler.
- Mapping Agent anons yapar (S,224.0.1.40) ile, RP mapping bilgisini yayar.



Tüm router'lar 224.0.1.40 IP adresini dinler.

Auto RP Konfigürasyonu :	
R3(config)# ip pim send-rp-announce f1/0 scope 10	#candidate RP
R3(config)# ip pim send-rp-discovery f1/0 scope 10	#Mapping agent

Scope nedir : scope değeri TTL değeri ile aynı düşünülebilir. Bu bilginin propagate edileceği Hop sayısını tanımlar.

Auto-RP Konfigürasyonu :

Şimdi Candidate RP ve RP mapping agent konfigürasyonlarını yaptıktan sonra, diğer router'lar Mapping agent ve RP'yi nasıl bilecek ?

224.0.1.40 grup adresinden yapılan yayını dinleyebilmeleri gerekiyor.

İnterface'ler içinde **ip pim sparse-mode** konfigürasyonunu yazdık. Ancak router'lar 224.0.1.40'a join olamaz.

Bu problemi çözmek için 2 farklı yöntem kullanılabilir.

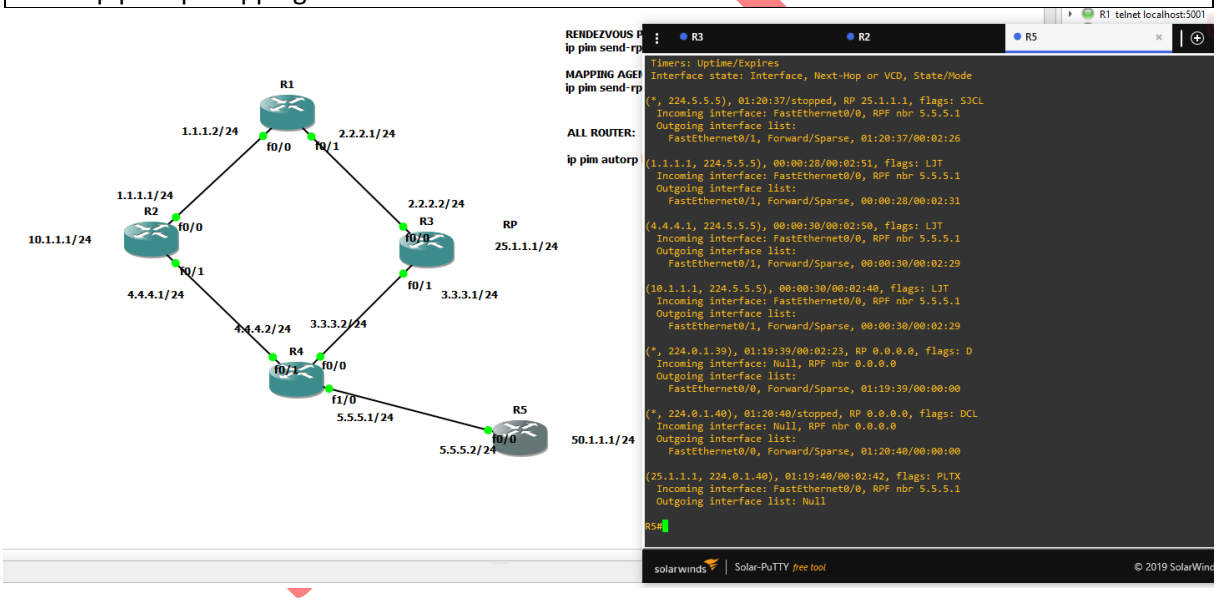
1- Pim sparse-dense mode
2- Auto-RP listener

Rx(config)# ip pim autorp listener

```
R5#sh ip pim rp map
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 25.1.1.1 (?), v2v1
    Info source: 25.1.1.1 (?), elected via Auto-RP
         Uptime: 01:21:59, expires: 00:02:18
R5#
```

show ip pim rp mappings



(25.1.1.1,224.0.1.40) , mapping agent ve RP aynı router. Mapping agent router anons yapıyor. 224.0.1.40 aracılığı ile.. RP'nin kaynağını öğreniyoruz. S,G bilgisi alınmış oluyor.

Auto-RP Yedeklilik Yapısı :

Auto-RP yedeklilik (redundancy) ve yük paylaşımı (load sharing) destekler.

ACL (access control list) hangi grup için hangi RP'nin olacağı kontrolü yapılabilir.

Birden fazla RP yapılandırıldıysa, mapping agent IP adresinin büyüklüğüne göre seçim yapar.

Aynı grup için aynı anda iki RP kullanılamaz.

Not : Birden fazla RP olduğunda, RP Mapping Agent IP adresi büyük olan router'ı RP olarak anons eder.

```
R5#
R5#sh ip pim rp map
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 25.1.1.1 (?), v2v1
    Info source: 35.1.1.1 (?), elected via Auto-RP
         Uptime: 01:23:07, expires: 00:02:13
R5#sh ip pim rp map
PIM Group-to-RP Mappings

Group(s) 224.0.0.0/4
  RP 15.1.1.1 (?), v2v1
    Info source: 35.1.1.1 (?), elected via Auto-RP
         Uptime: 00:00:49, expires: 00:02:11
R5#
```

25.1.1.1 RP'yi shutdown konumuna getirdikten sonra, tekrardan aşağıdaki komutu çalıştırılaım. RP değişip değişmediğini inceleyelim.

show ip pim rp mapping

Auto-RP Yük Dengeleme :

Aynı grup için aynı anda iki RP kullanılamaz diye söylemiştik. Farklı grupları farklı RP'ler ile yapılandırabiliriz.

Örneğin 224.4.4.4 grup adresi RP1,

224.3.3.3 grup adresi join istekleri RP2 aracılığı ile ....

Auto-RP'yi birden çok RP olduğunda Load sharing nasıl yaparız konfigürasyonunu görelim.

```
R1(config)# access-list 11 permit host 224.5.5.5
R1(config)#ip pim send-rp-announce f1/0 scope 20 group-list 11
```

```
R3(config)# access-list 10 permit host 224.4.4.4
R3(config)#ip pim send-rp-announce f0/1 scope 20 group-list 10
```

```
R5#sh ip pim rp map
PIM Group-to-RP Mappings

Group(s) 224.4.4.4/32
  RP 25.1.1.1 (?), v2v1
    Info source: 35.1.1.1 (?), elected via Auto-RP
         Uptime: 00:12:34, expires: 00:02:14
Group(s) 224.5.5.5/32
  RP 15.1.1.1 (?), v2v1
    Info source: 35.1.1.1 (?), elected via Auto-RP
         Uptime: 00:12:34, expires: 00:02:16
R5#
```

show ip pim rp mapping

Görüleceği üzere 224.4.4.4 grup adresi için RP : 25.1.1.1

224.5.5.5 için : 15.1.1.1

İlave olarak D class içinde diğer IP adresleri içinde permit access list yazalım.

R1(config)# access-list 2 permit 224.0.0.0 15.255.255.255

```
R1(config)#access-list 2 permit 224.0.0.0 15.255.255.255
R1(config)#do sh acc-l
R1(config)#do sh acc-l
sh acc-l
     ^
% Invalid input detected at '^' marker.

R1(config)#do sh acces
R1(config)#do sh access-list
Standard IP access list 2
    10 permit 224.0.0.0, wildcard bits 15.255.255.255
Standard IP access list 11
    10 permit 224.5.5.5
R1(config)#
```

R3(config)# access-list 3 permit 224.0.0.0 15.255.255.255

```
R3(config)#access-list 3 permit 224.0.0.0 15.255.255.255
R3(config)#do sh access-l
R3(config)#do sh access-l
Standard IP access list 3
    10 permit 224.0.0.0, wildcard bits 15.255.255.255
Standard IP access list 10
    10 permit 224.4.4.4
R3(config)#
```

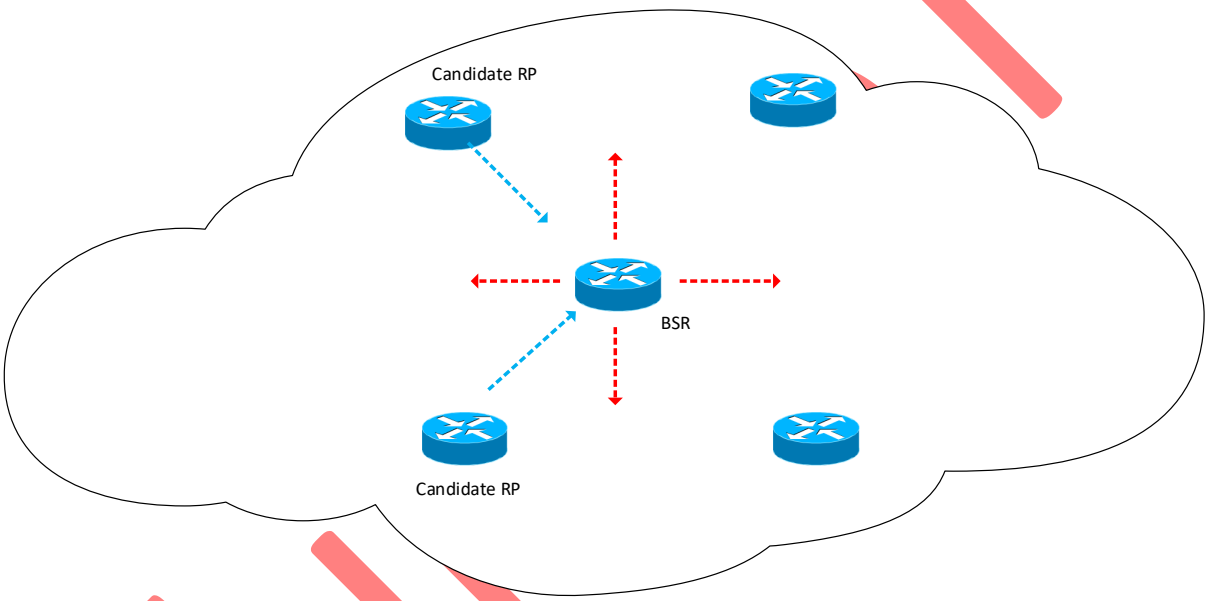
PIM – BOOTSTRAP ROUTER :

- Fonksiyonellik olarak Auto-RP ile benzerdir.
- Standart protokoldür. Auto-RP ,cisco proprietary'dir.

- IPv6 multicast destekler.
- Bootstrap router, PIMv2 standardının parçasıdır.

BSR domain'de 2 rol vardır.

- **RP Candidate :** Auto-RP'deki candidate RP gibi. Unicast PIM kullanır ve kendisini BSR'a advertise eder.
- **Bootstrap Router** : Auto-RP'deki Mapping Agent gibi.



Kırmızı ok : BSR Mesajı

Mavi ok : Candidate RP Advertisement (Unicast)

BSR Konfigürasyonu :

```
R3(config)# ip pim rp-candidate fx/y
R3(config)# ip pim bsr-candidate fx/y

Hem bsr hem de rp aynı router atanmıştır.
```

show ip pim rp mapping ile kontrol edelim.

```
R3(config)#ip pim rp-candidate f1/0
R3(config)#ip pim rp-candidate f1/0
R3(config)#ip pim bsr
R3(config)#ip pim bsr-candidate f1/0
R3(config)#do wr
Building configuration...
[OK]
R3(config)#do sh ip pim rp map
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)

R3(config)#
```

BÖLÜM -4 : LAYER 2 MULTICAST :

Bu bölümde LAN segmentinde multicast'ın nasıl çalıştığını inceleyeceğiz.

Layer 2 Multicast

Layer 2 MAC Adres

IGMP Snooping

Switch'ler nasıl multicast trafiği tanımlıyor, unicast normal trafik olup olmadığını nasıl anlıyor ?

Multicast MAC Adres :

Multicast Ethernet MAC Adresi 01:00:5E hexadecimal ile başlar.

L3 IP multicast ve L2 MAC multicast adres arasında çevrim sağlanır.

Hatırlayacak olduğunuz üzere, Alıcı ya da Receiver local router'a bir grup adresinden multicast trafik almak istediğini IGMP report mesajı ile bildiriyordu. Router'da PIM protokolü ile source'u buluyordu. Şimdi L2 switch bu multicast trafiği nasıl iletiyor?

Source Address :	Router Adresi
Destination Address :	224.5.5.5

Switch 224.5.5.5 adresinin MAC eşleniğini görecek.

Multicast adresi tanımlayabilmek için 01:00:5E'ye bakar.

Multicast MAC Adres Dönüşümü :

Multicast IP Adres : 228.10.24.5

Binary format : **1110**0**1**00.0001010.00011000.00000101

01-00-5E-0A-18-05

IGMP layer 3 katmanında çaoışır, ve switch'ler IGMP mesajlarını anlamaz.

IGMP; router'lara, multicast trafiği nasıl dağıtacağı konusunda yardımcı olur.

Switch'ler CAM tablolarında Multicast MAC adres hiç bulamayacaklar, çünkü Multicast MAC adresi bir SOURCE ADRES olarak kullanılmaz.

Switch'ler multicast trafiği bir broadcast domain'deki tüm hostlara FLOOD yapar. Bu da gereksiz bant genişliği tüketimidir.

ÇÖZÜM ?

IGMP Snooping

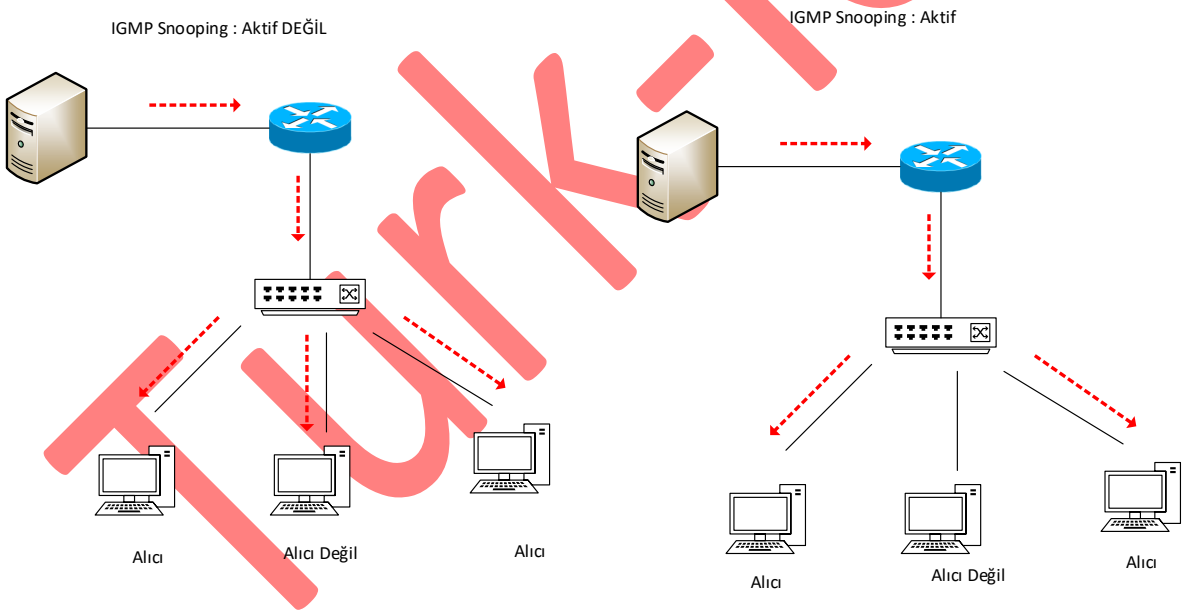
CGMP

IGMP Snooping :

Standart

Belirli bir VLAN'e bağlı olan ve multicast trafiği almak isteyen hostları dinamik olarak tespit eder

Switch IGMP mesajını analiz eder ve multicast routerların konumunu ve grup üyelerini öğrenir.



Eğer herhangi bir alıcı, multicast trafiği almak istemezse, leave mesajı gönderilir. Switch ilgili alıcıyı MAC adresinden düşürür.

IGMP Snooping cisco catalyst multi layer switch'lerinde aktif olarak gelmektedir.

Snooping global olarak aktiftir.

IGMP Snooping konfigürasyonu :

```
Router(config)# ip igmp snooping
Router(config)# ip igmp snooping vlan 10
```

İster global olarak istersekte bir vlan bazında aktif edebiliriz.

```
SW1# show ip igmp snooping vlan 105
```