
TOMORROW
starts here.
Cisco live!

IP Multicast – Concepts, Design and Troubleshooting

BRKMPL-1261

Therdtoon Theerasasana
Consulting Systems Engineer

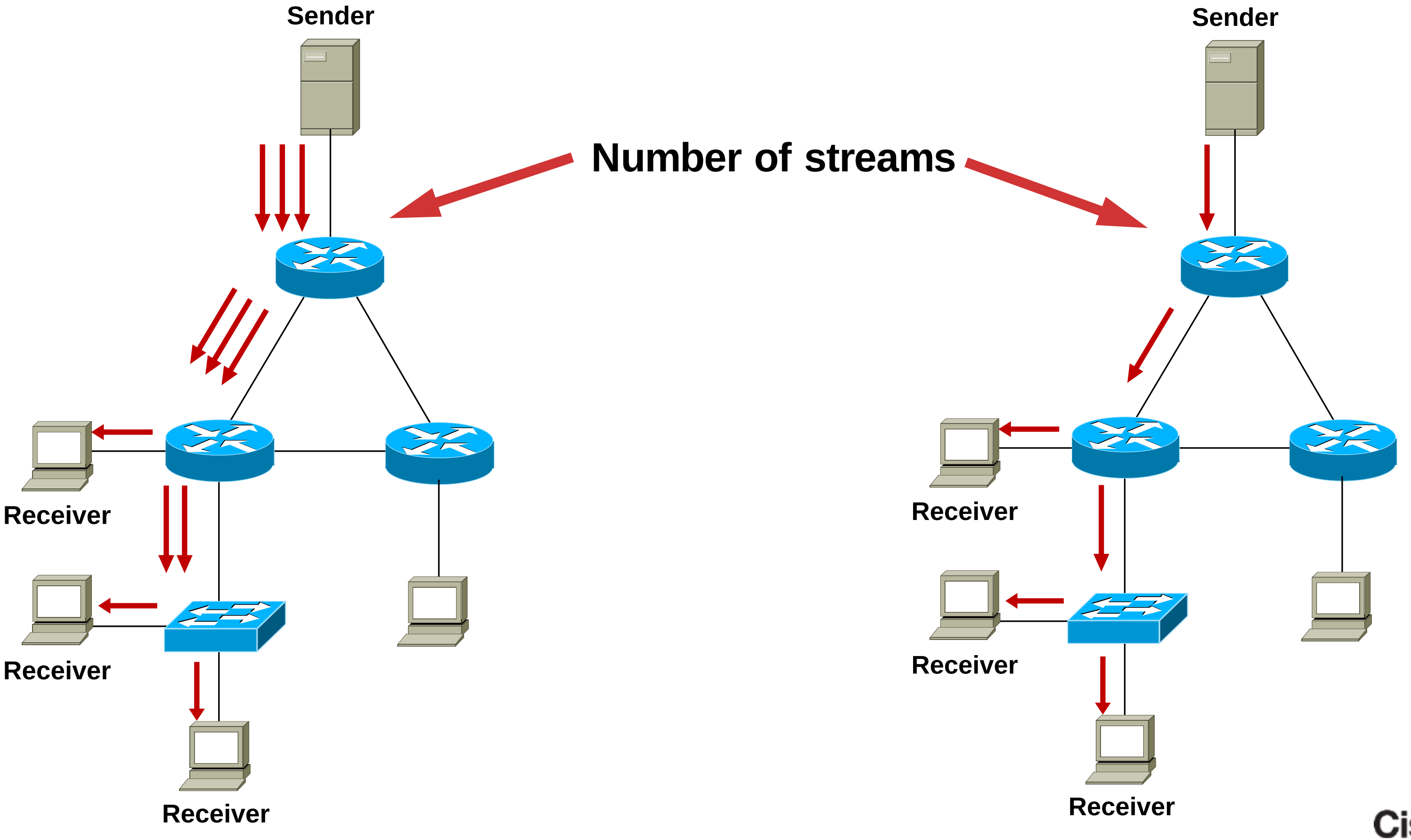
#clmel

Agenda

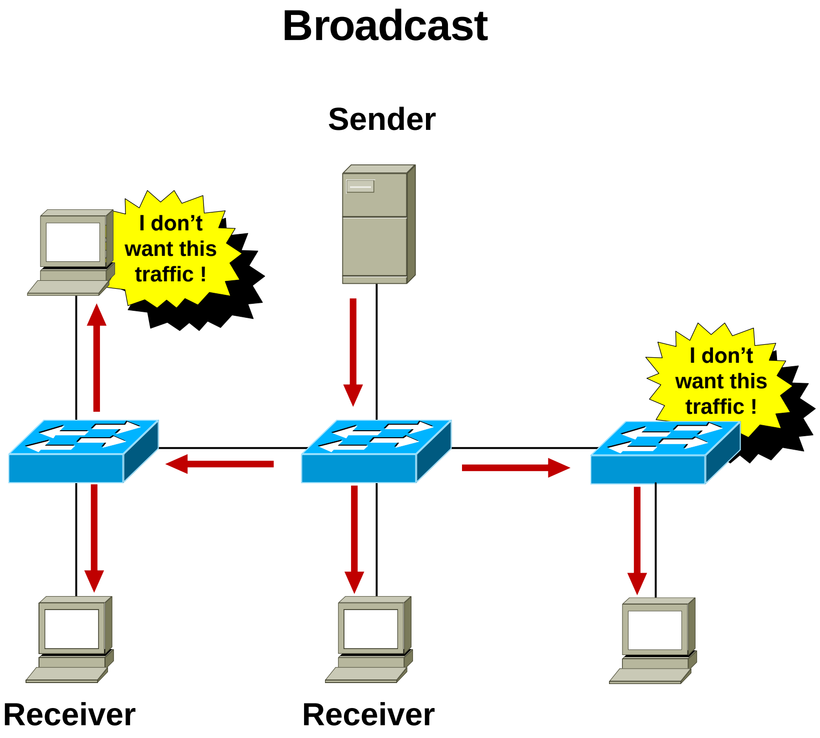
- Multicast overview
  – What is it and when would we use it ?
- Multicast fundamentals
  – Technical concepts and protocols
- Multicast Design and Configuration
  – 1 case study, 3 solutions
- Troubleshooting common multicast issues

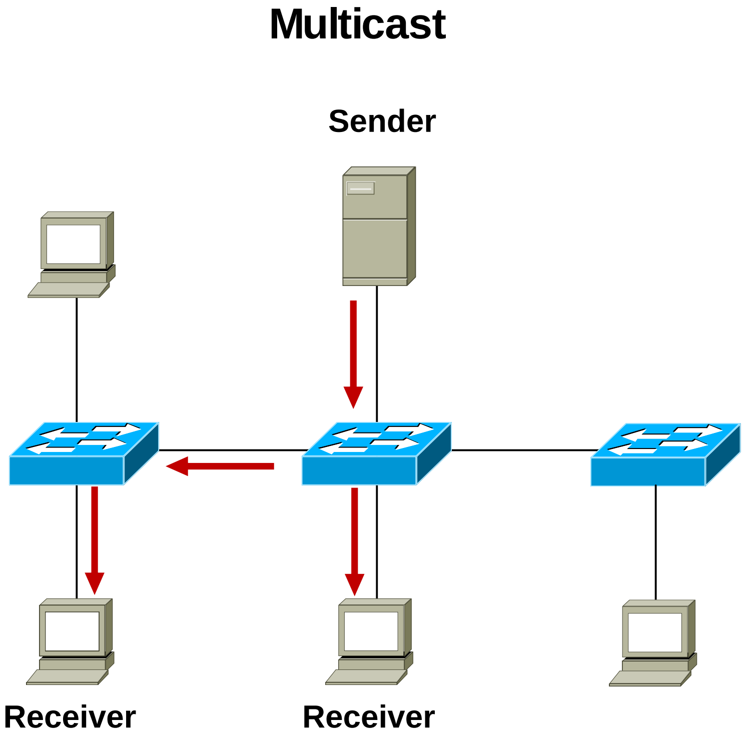
Multicast Overview

Unicast Vs Multicast



Broadcast Vs Multicast





Multicast Uses

- Any situation where multiple endpoints need to receive identical information at the same time
  - Streaming video, IPTV
  - Music on hold
  - Data replication
  - Periodic data delivery - stock quotes, sports scores, news reports
- Most commonly used for one-to-many or some-to-many data flows

Multicast Advantages

- **Enhanced scalability:** Network utilisation is independent of the number of receivers
- **Reduced resource utilisation:** Controls network bandwidth and reduces server and router loads
- **Deterministic performance:** subscriber number 1 and subscriber number 10000 have identical experience

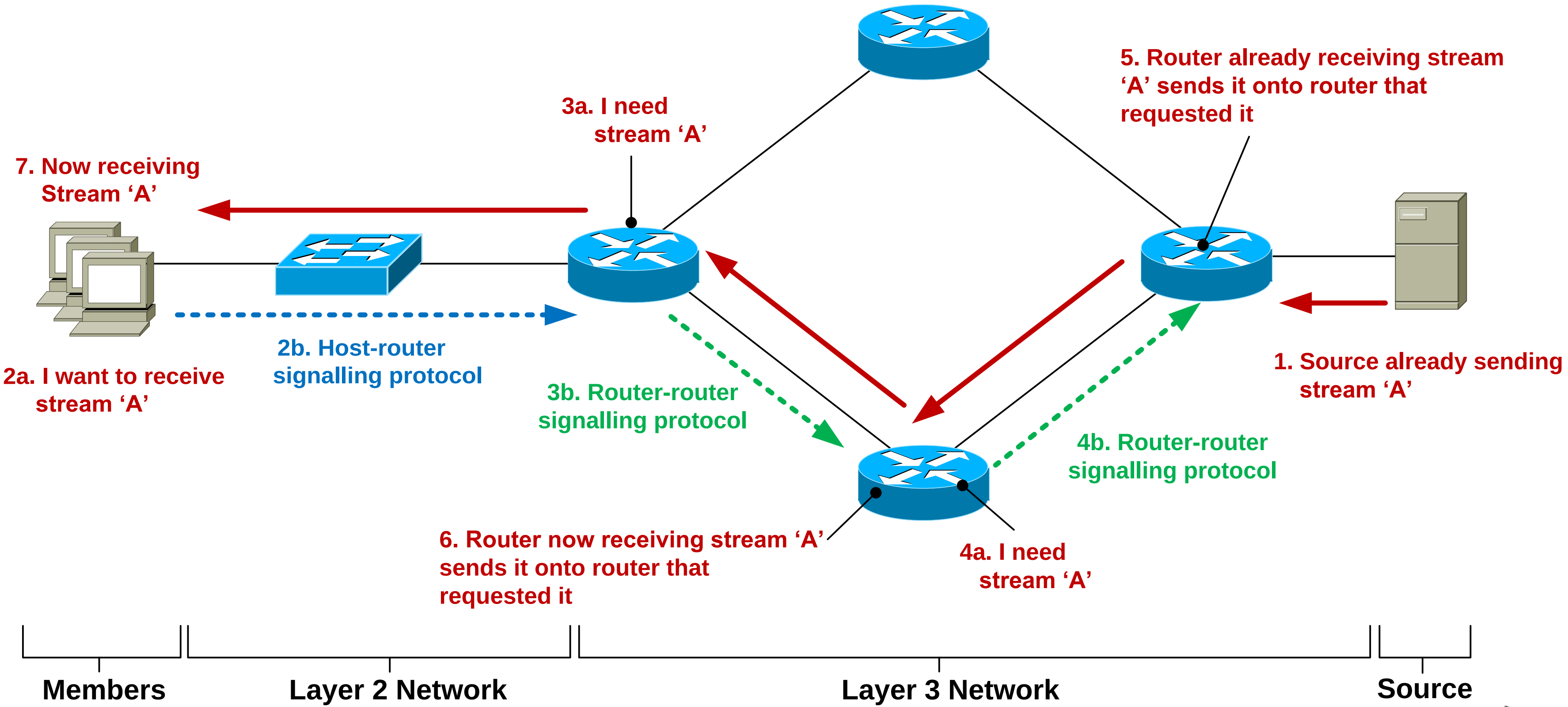
LOWER TCO

Multicast Considerations

- Multicast is UDP-based: No flow control, sequencing, error-correction, retransmissions.
- "Best effort" delivery: Sender has no idea if all subscribers have received the data. Subscribers don't know if they have missed a packet. Applications should be handling missed packets.
- No congestion avoidance: Lack of TCP windowing and "slow-start" mechanisms may result in network congestions.
- Added Complexity: If you have the bandwidth available then unicast delivery model may be a simpler option.

Multicast Fundamentals

Multicast Service Model Overview



IP Multicast Source

- Any device that sends an IP packet with a destination address between 224.0.0.0 – 239.255.255.255
- A device can be a multicast sender and a multicast receiver at the same time
- There is no multicast control traffic between the sender and the network, or between the sender and receiver.

Q: So how does the source know when to send traffic ?

A: An application tells the source to start transmitting

Multicast Addressing—224/4

- IANA Reserved addresses (never use these !)

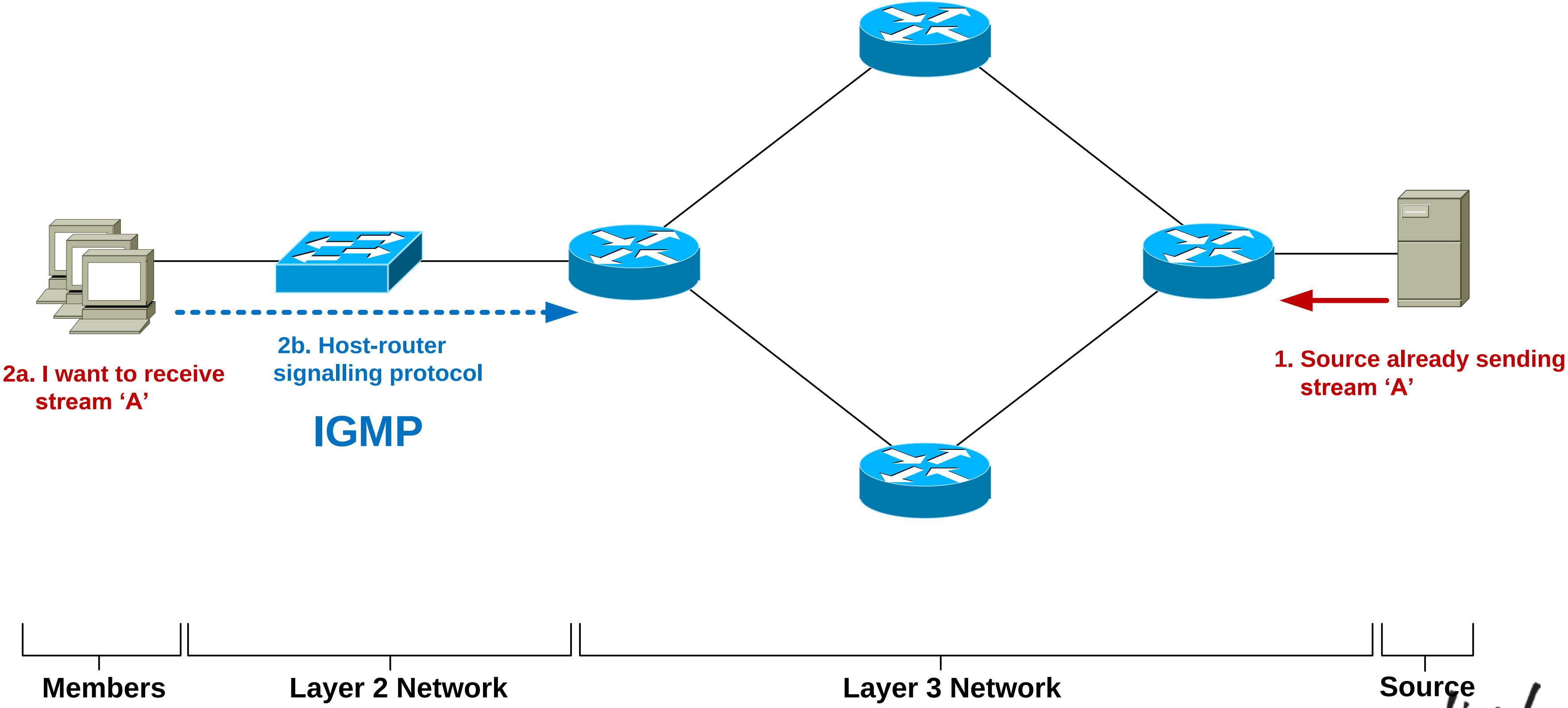
224.0.0.0 – 224.0.0.255	Local network control block
224.0.1.0 – 224.0.1.255	Internetwork control block

- Other IANA allocated address ranges

232.0.0.0 – 232.255.255.255	Source Specific Multicast
233.0.0.0 – 234.255.255.255	GLOP/UBM Addressing
239.0.0.0 – 239.255.255.255	'Private' multicast range

- Check http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml

Multicast Service Model Overview – Layer 2



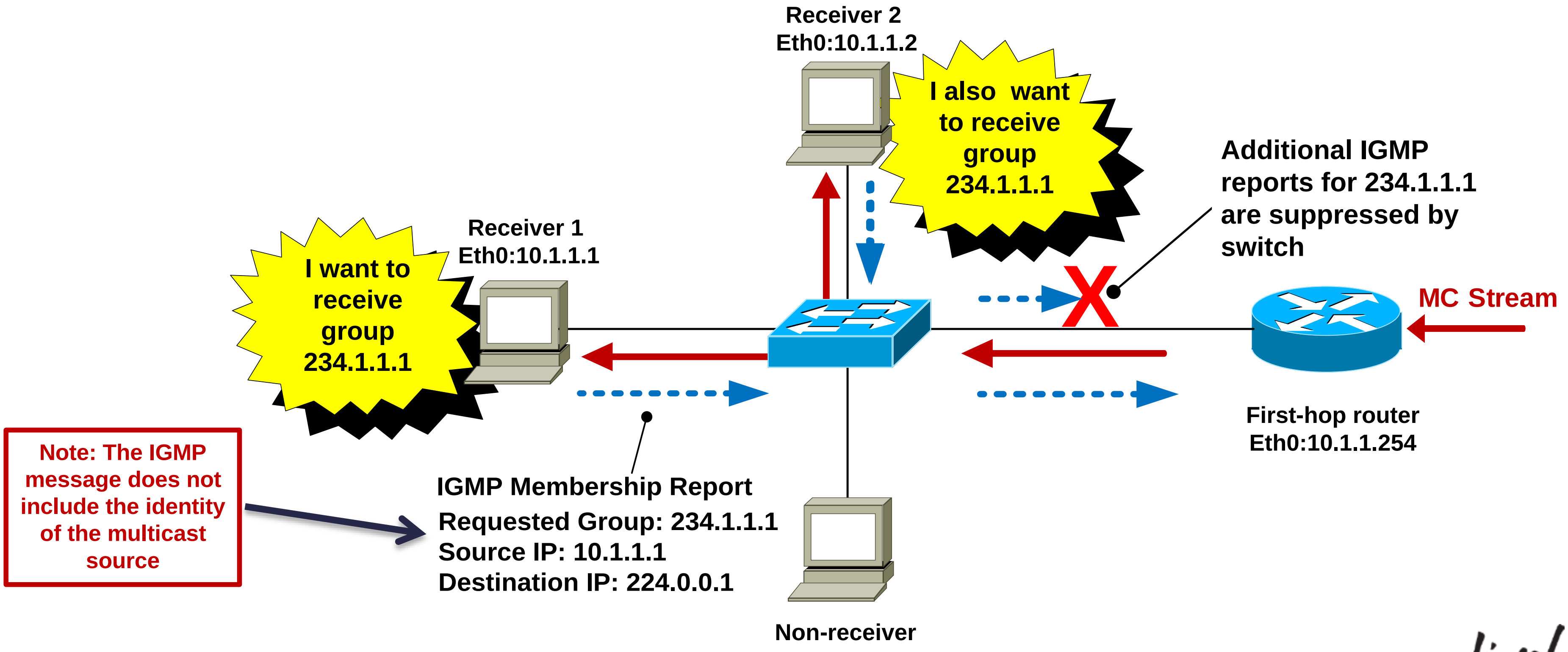
Host-Router Signalling: IGMP

- **I**nternet **G**roup **M**anagement **P**rotocol
- Used by a **host** to notify the local **router** that it wishes to receive (or stop receiving) multicast traffic for a given destination address or “group”.
- RFC 2236 specifies version 2 of IGMP

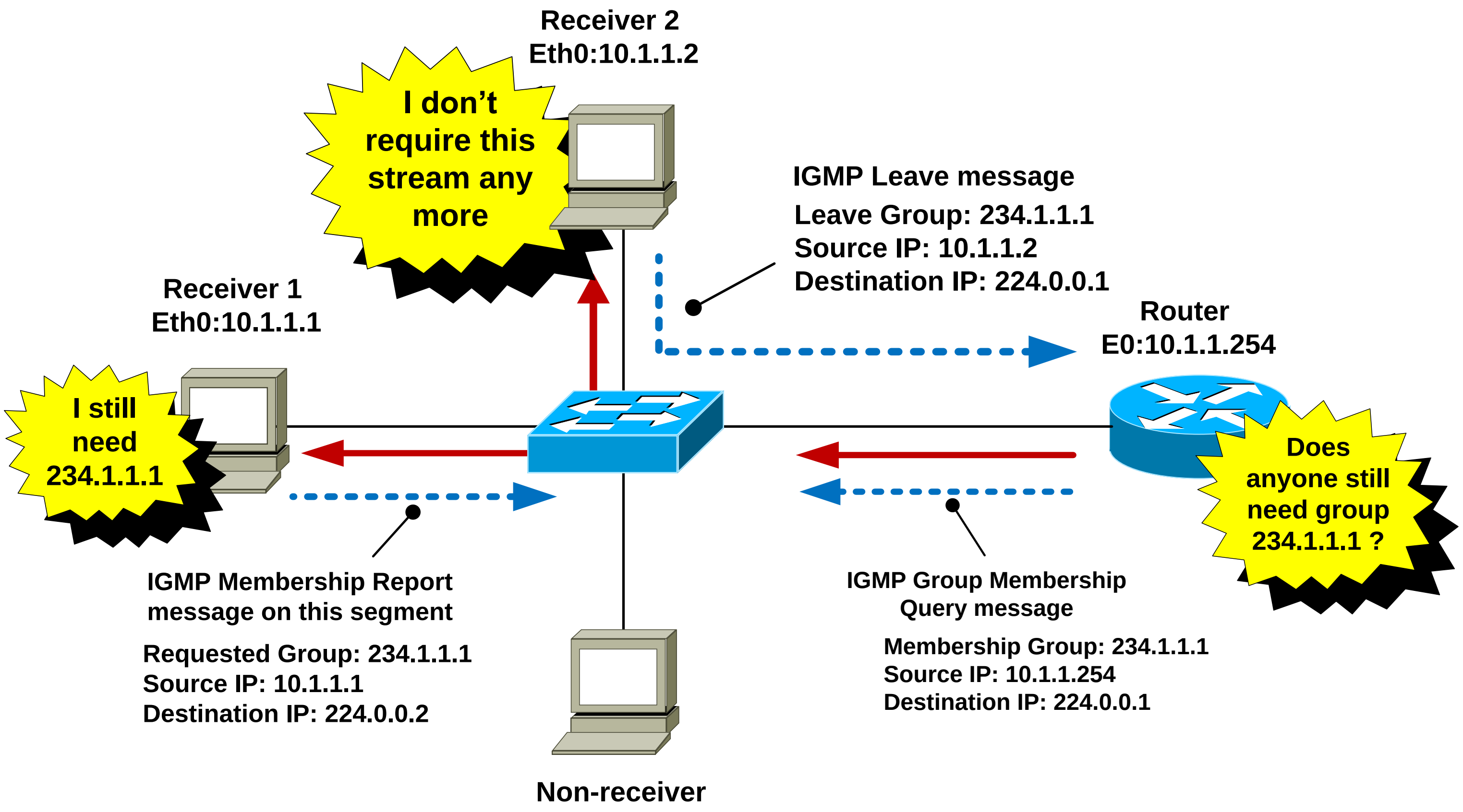
  Most widely deployed and supported
- RFC 3376 specifies version 3 of IGMP

  Good network support but host implementations still patchy

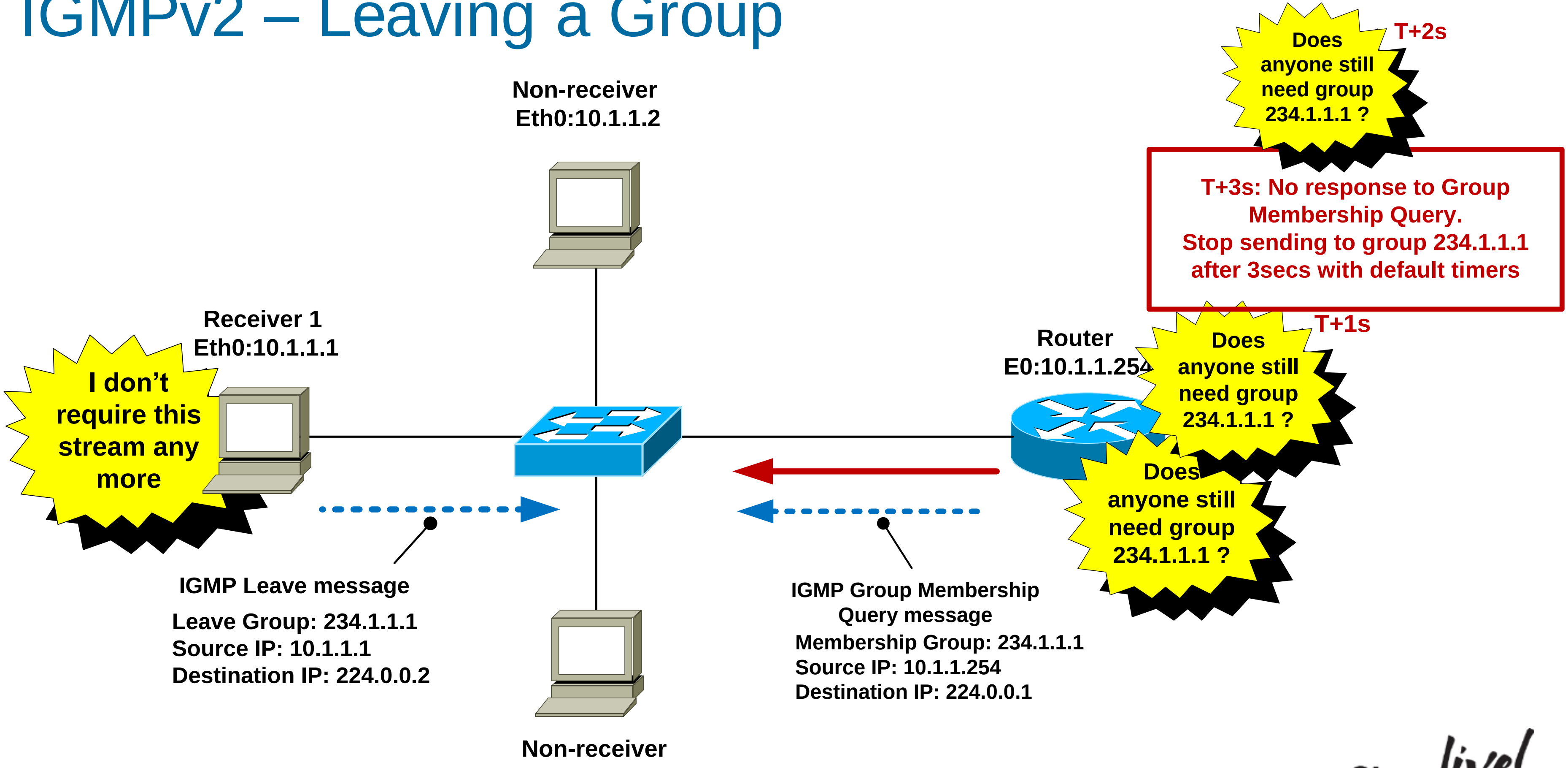
IGMPv2 – Joining a Group



IGMPv2 – Maintaining a Group



IGMPv2 – Leaving a Group



IGMP Snooping

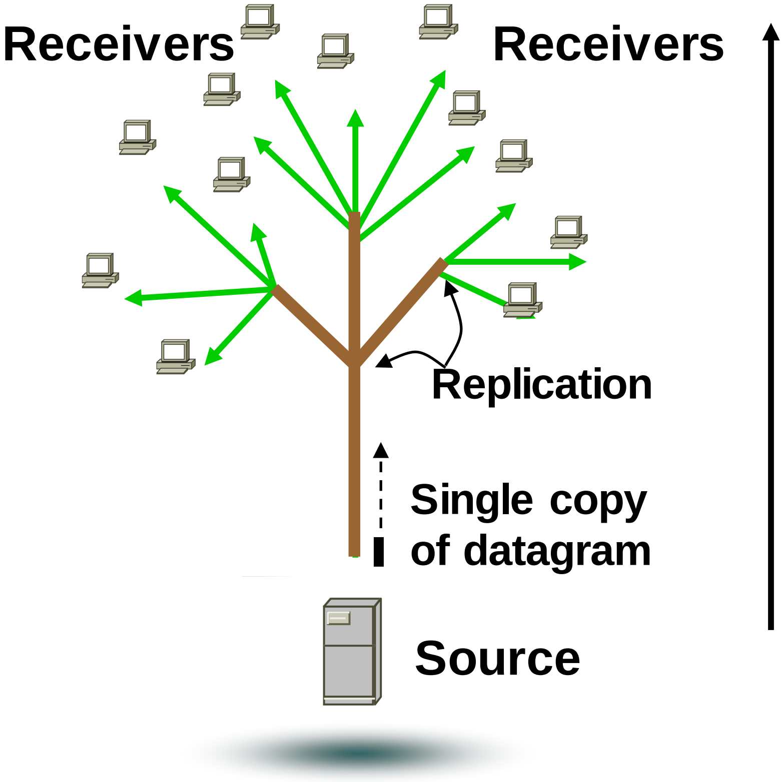
- By default, switches forward all layer 2 multicast frames to all ports (except the originating port)
- IGMP snooping eavesdrops on IGMP messaging
- Switch constrains MC to *only* ports that want it (key point)
- IGMP snooping is on by default in IOS-based switches
- Replaced Cisco Group Management Protocol (CGMP).

Advantages of IGMP Snooping

- Hosts only receive MC traffic that they request
- Report suppression – switch acts as a IGMP middleman, prevents first-hop router from being flooded with IGMP reports for the same group
- “Fast-leave” functionality – stop sending MC group as soon as switch hears a “leave” on an interface

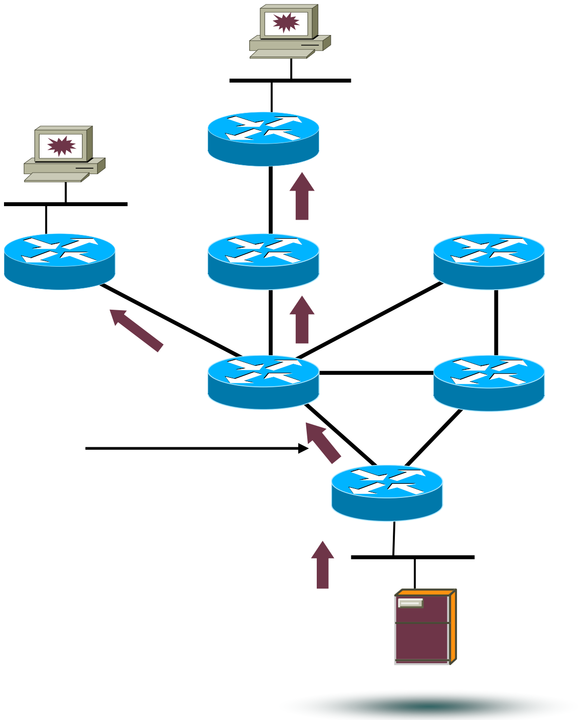
Q. When would IGMP snooping fast-leave be a bad idea ?
A. When there is more than 1 receiver attached to an interface

Its all about Trees!



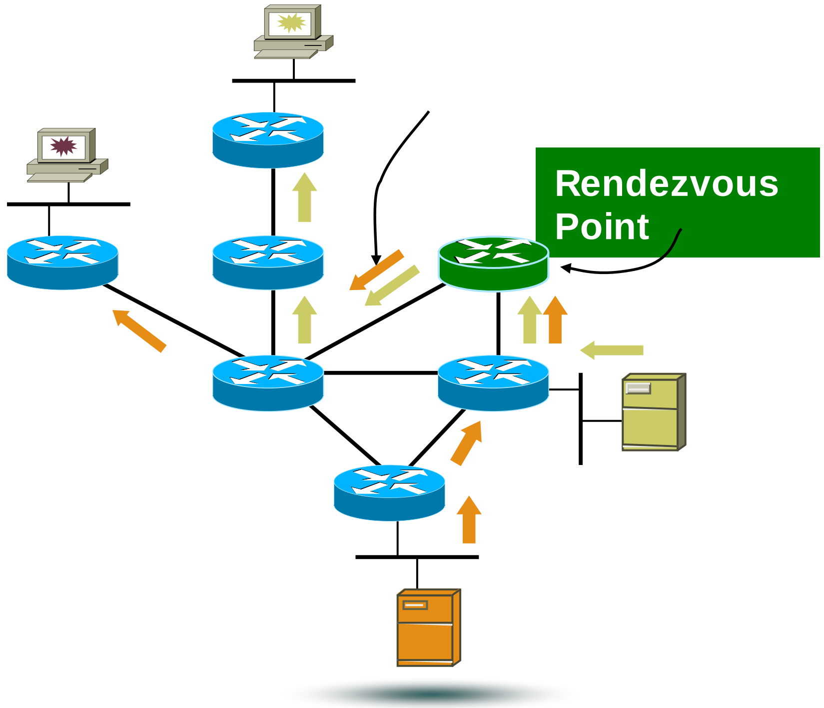
- Mechanism for transmitting information from a single source (root) to many receivers (leaves)
- Single copy of a datagram is sent from the source and replicated through the tree to receivers
- Two Tree Types: Source and Shared

Source Tree



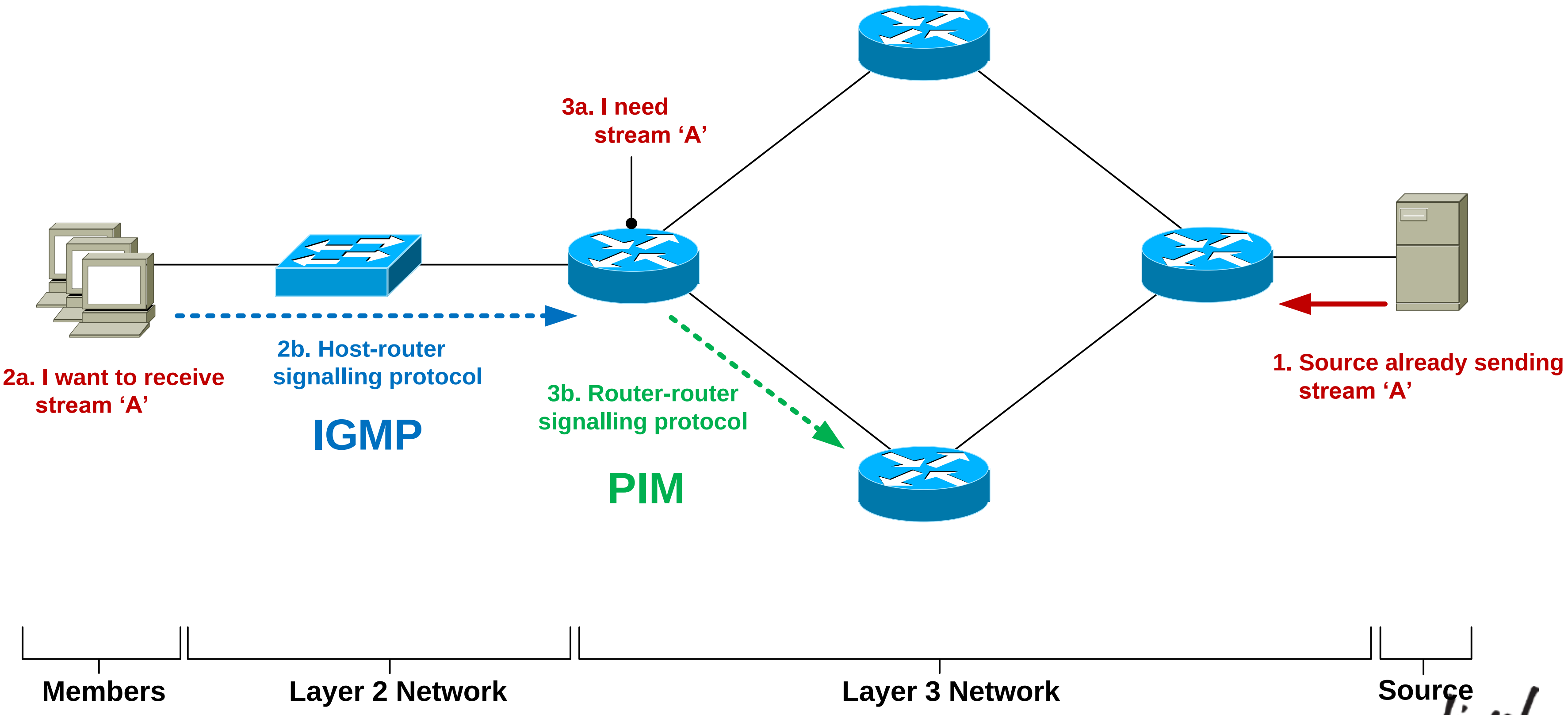
- Simplest form of tree
  - Receiver requires knowledge of source
- Traffic travels from source (root) to receivers (leaves), shortest path taken
- Packets replicated at branch point
- Fwding entry states represented as (S, G) in mroute table
- Provides Optimal routing
  - At the expense of more state (S, G)

Shared Tree



- Root is a common point
  - Rendezvous Point
  - Many multicast groups at RP
- Receivers join RP
  - To learn of sources
- Sources only transmit to RP
  RP forward to receivers
- Forwarding represented as (*, G) in mroute table
- Less state required
  - At expense of optimal routing

Multicast Service Model Overview – Layer 3



Router-Router Signalling: PIM

- **P**rotocol **I**ndependent **M**ulticast
- Used by a **router** to notify an upstream **router** that it wishes to receive (or stop receiving) multicast traffic for a given group (G).
- 3 main classifications of PIM

  Any Source Multicast (asm-pim) – 3 "submodes"

  Legacy – – ~~Dense~~, sparse, ~~sparse-dense~~ – – – **Cisco Specific**

  Source-Specific Multicast (pim-ssm)

  ~~Bidirectional (pim-bidir)~~ – – – – – **Only for specific-use cases (many senders)**

Router-Router Signalling: PIM-SM

- Each PIM router forms neighbour relationship with adjacent PIM routers using PIM "hello" messages every 30 seconds.

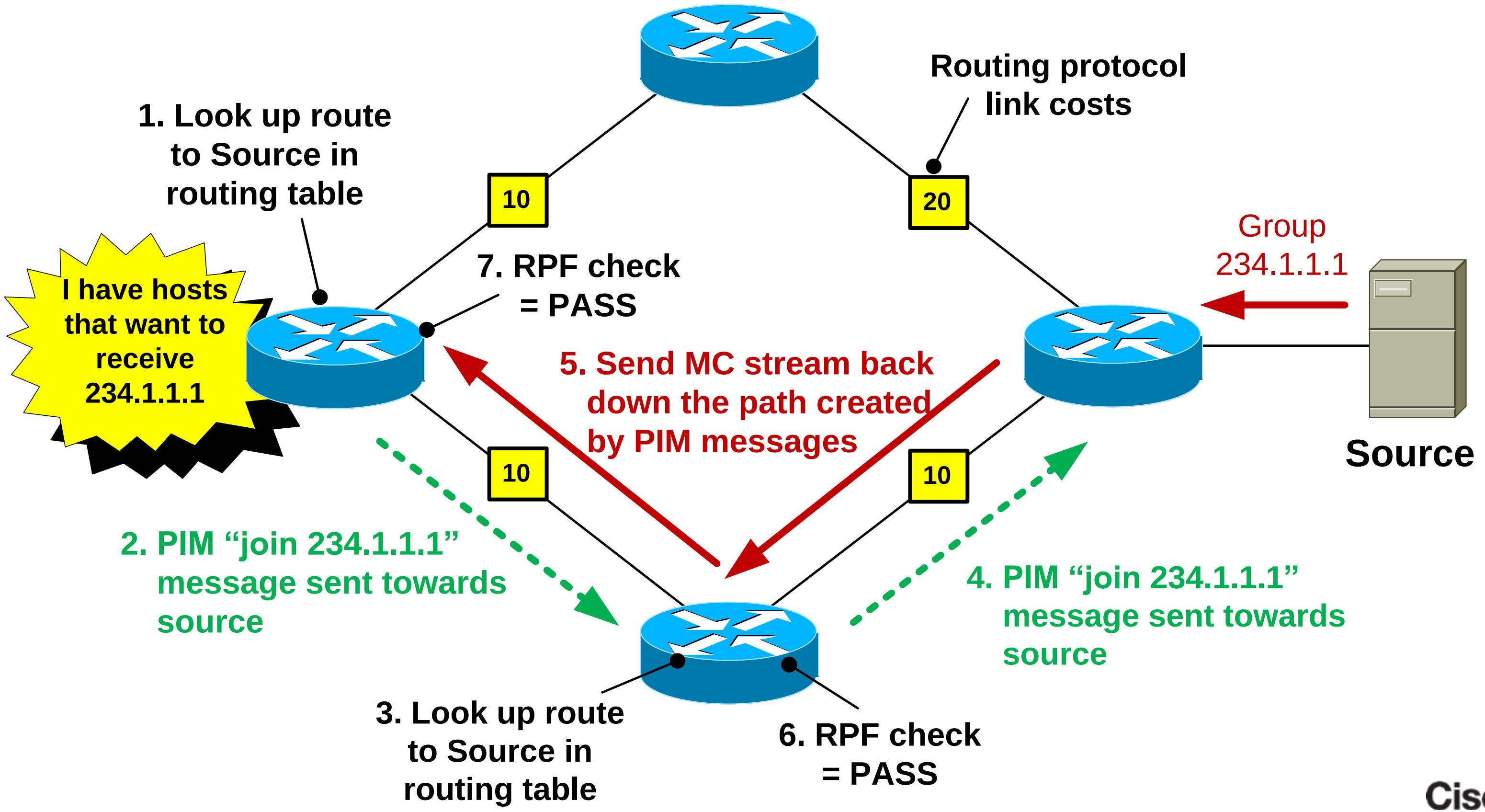
- When a PIM router wants to receive a multicast stream, it sends a PIM "join" message towards the IP address of the multicast source.

- When a PIM router wants to stop receiving a multicast stream, it sends a PIM "prune" message towards the IP address of the multicast source.

RPF Mechanism

- Multicast traffic flows are checked from the sender back down the path created by the PIM messages. This is known as Reverse Path Forwarding (**RPF**).
- All received multicast traffic is subject to an **RPF check**
  - Is the incoming MC traffic being received via the interface on which I have a route to the source?
  - RPF check **PASS** = accept MC traffic and send it on
  - RPF check **FAIL** = drop traffic on floor
- Prevents loops and duplicate packets

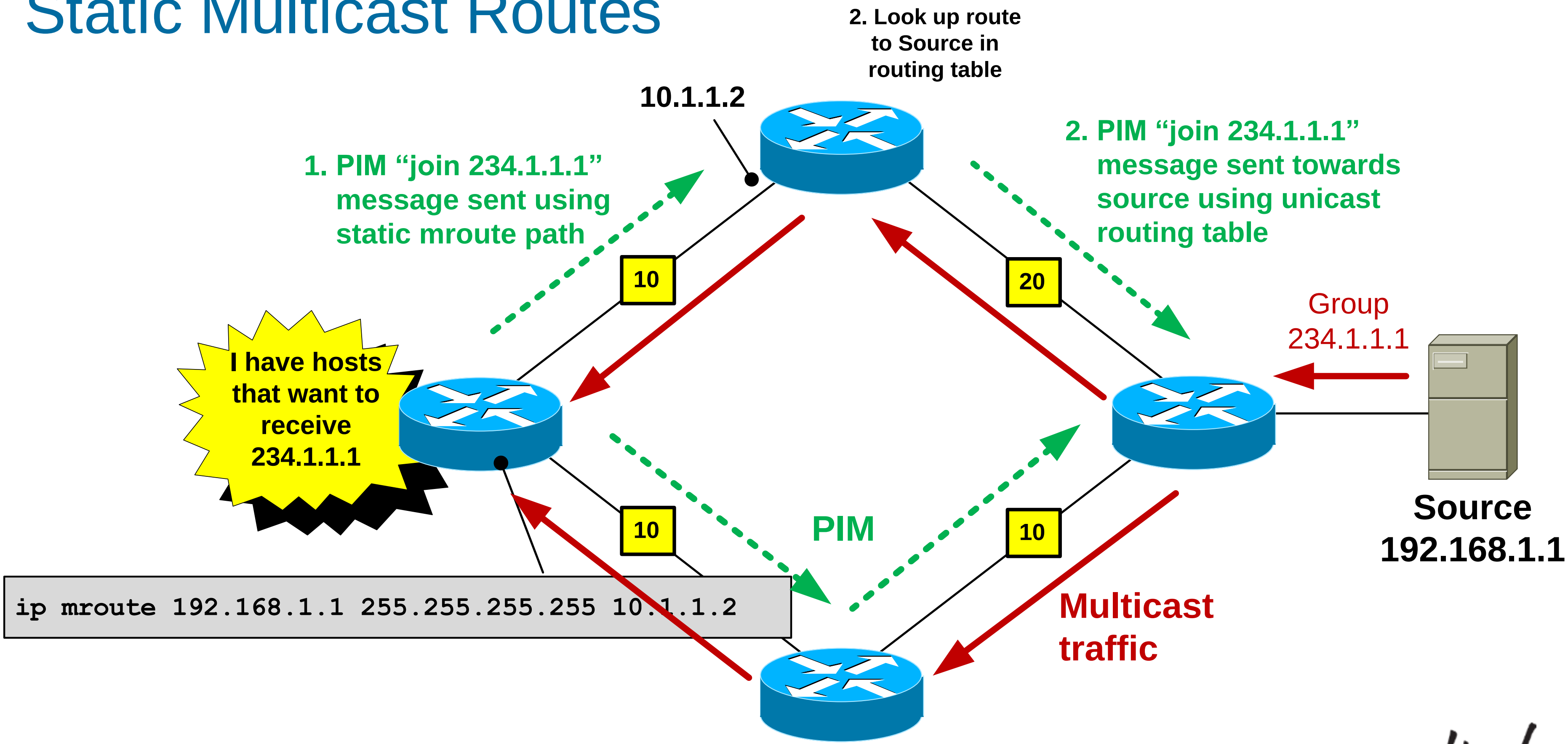
RPF Mechanism



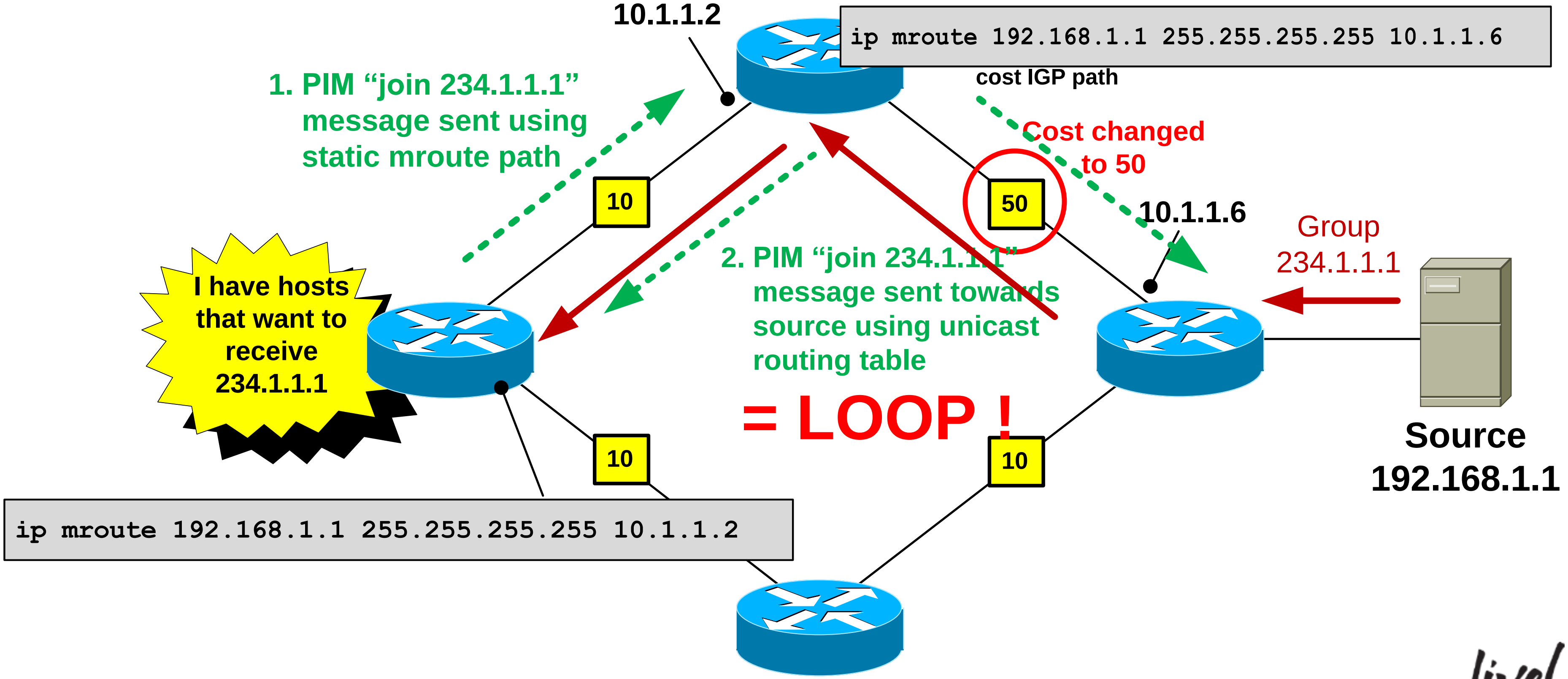
Static Multicast Routes

- Static multicast routes can be used to send PIM messages down a different path than would be selected from the unicast routing table.
- Useful if you want MC traffic to travel over different links to unicast traffic
- Best suited for small networks due to scalability issues managing many static routes.
- Be careful of creating PIM routing loops !

Static Multicast Routes

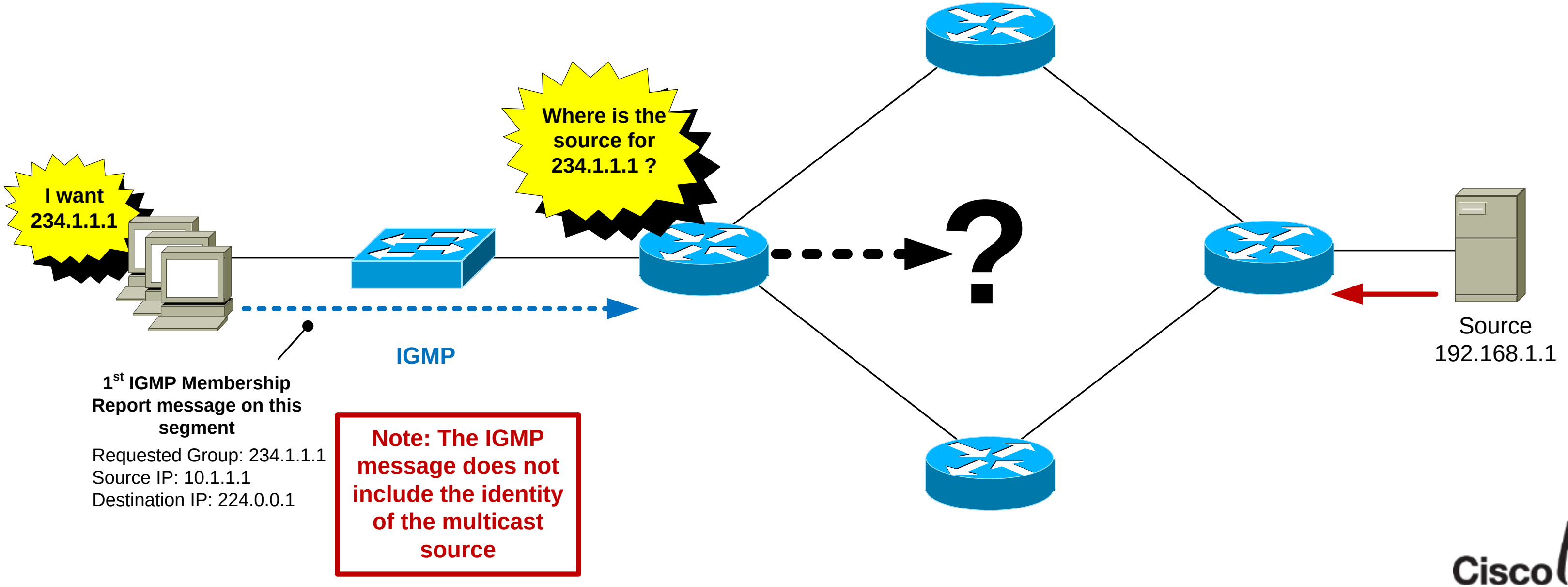


Static Multicast Routing Loop



Router-Router Signalling: PIM-SM

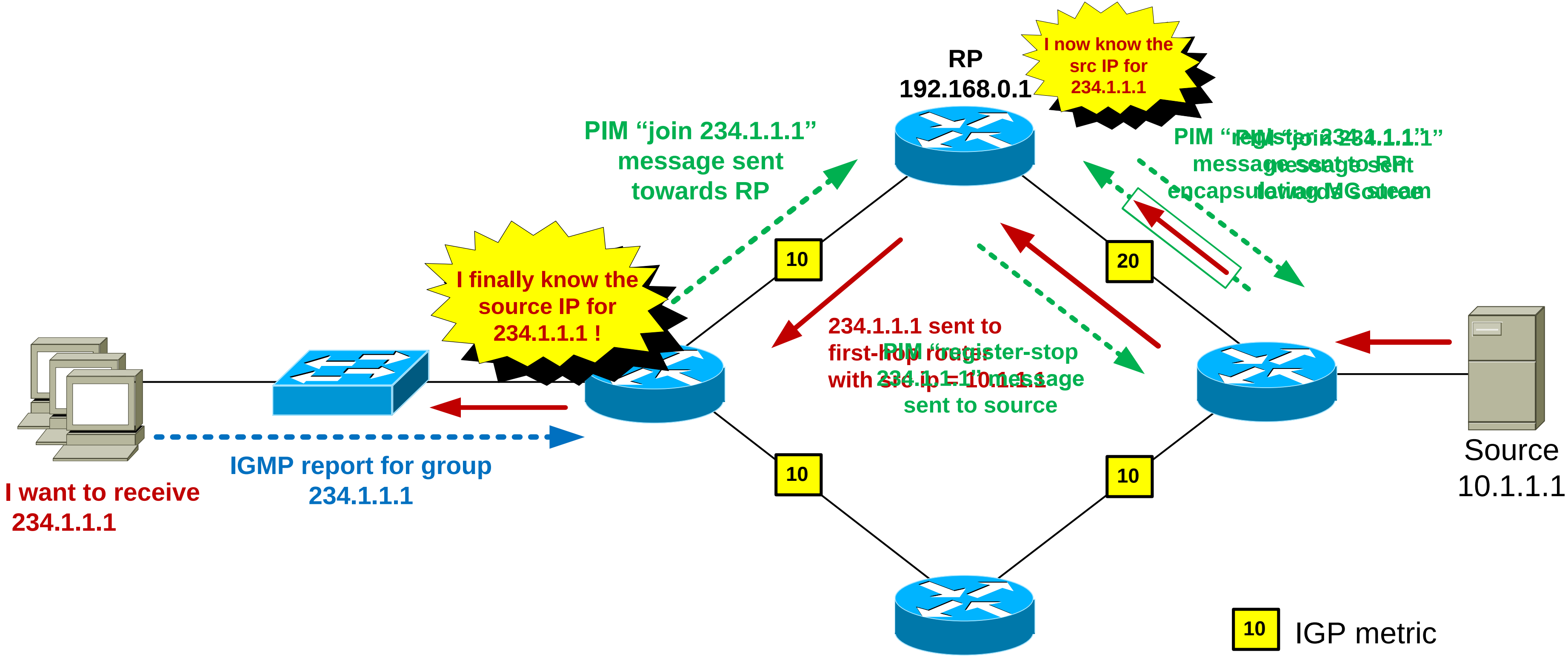
- But.....we have a problem. The receiver just told me the group it wants to join but didn't identify the source! So in which direction is the "upstream" router ?



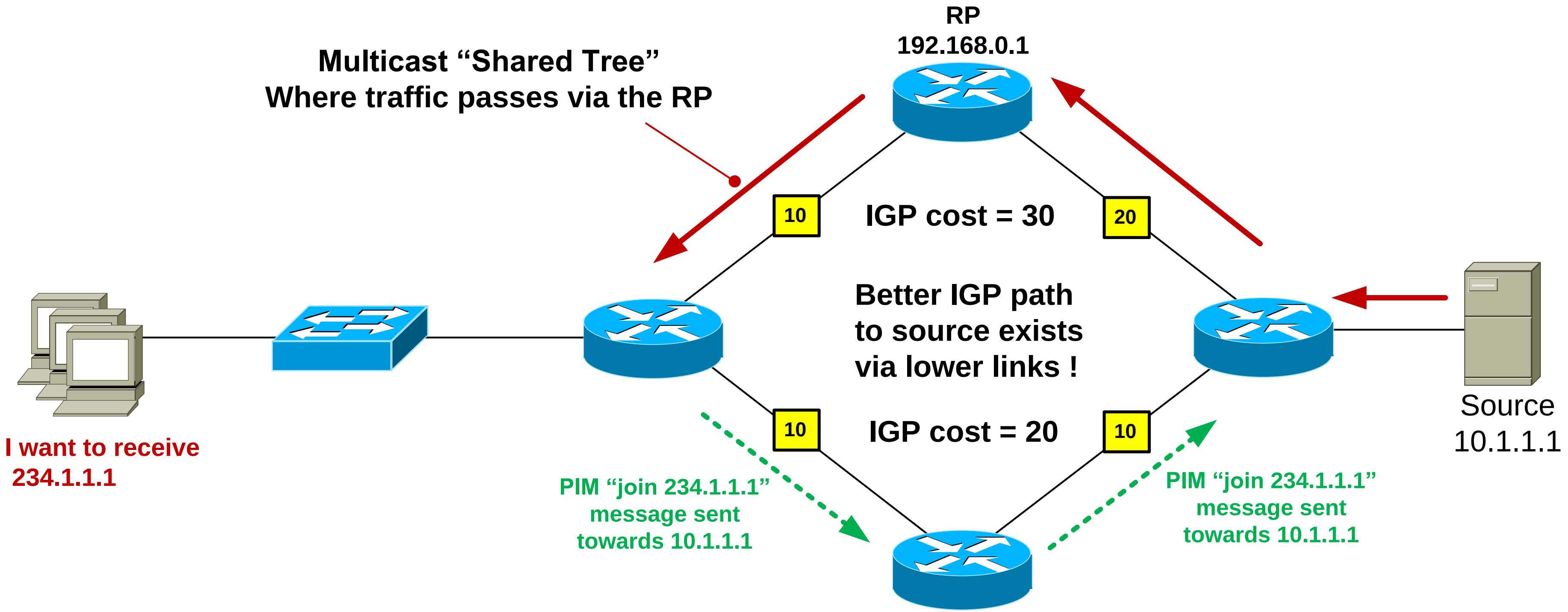
PIM-SM: Rendezvous Point (RP)

- PIM-SM uses a router called a Rendezvous Point (RP).
- The sole purpose of the RP is to allow the first-hop router to find out the IP address of the source for a particular group.
- The receivers don't know the source address and don't care - hence the term "Any Source Multicast".
- An RP is **mandatory** for PIM sparse-mode networks.

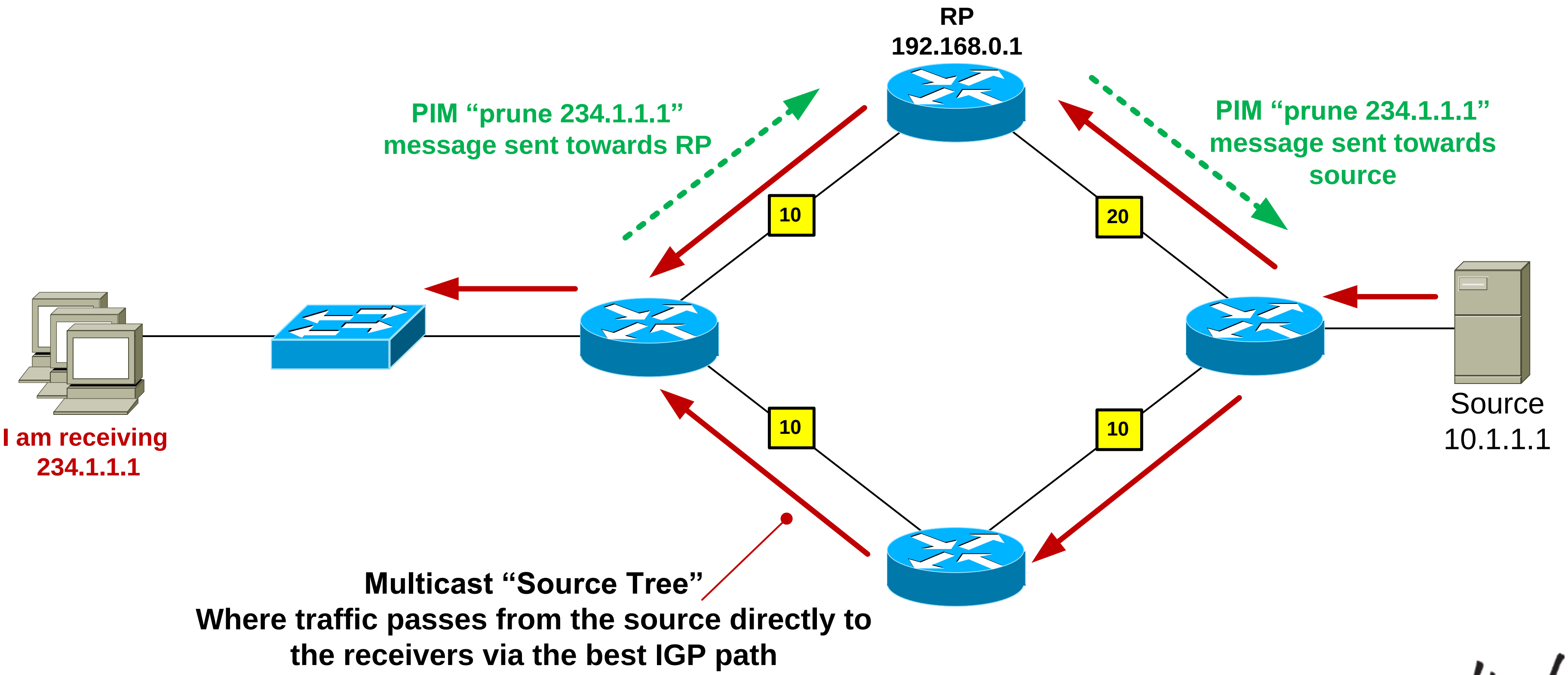
PIM-SM: Rendezvous Point (RP)



PIM-SM: Shortest Path Tree Switchover



PIM-SM: Shortest Path Tree Switchover



PIM-SM: Rendezvous Point Discovery

So how does the network know where the RP is ?

- **Option 1:** Static RP configuration

  Configure **all** routers in the network with the IP address of the RP

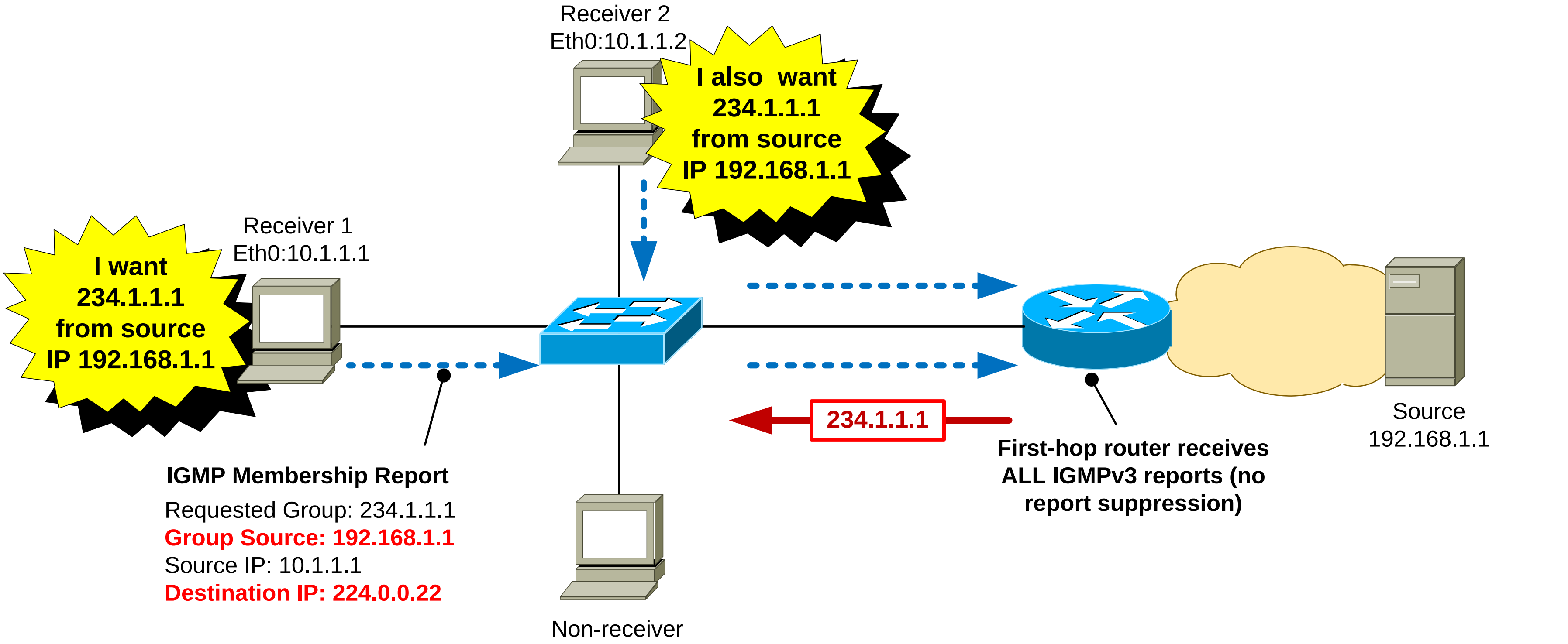
```
ip pim rp-address 192.168.0.1
```

- **Option 2:** Dynamic RP configuration

  Configure the RP to tell all other routers that it is the RP
  - Cisco proprietary mechanism is called "Auto-RP"
  - IETF standard is known as Bootstrap Router (BSR) – RFC 5059

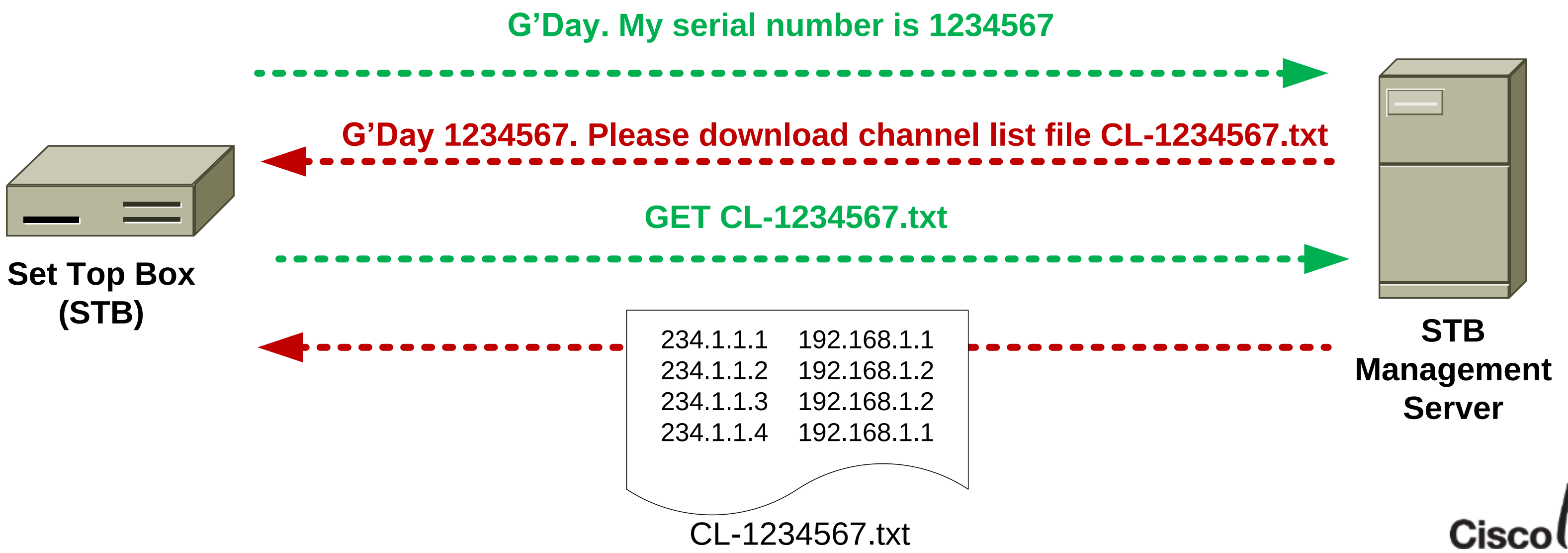
Q: What if receivers router knew the source from the start?....

IGMPv3 – Joining a Group

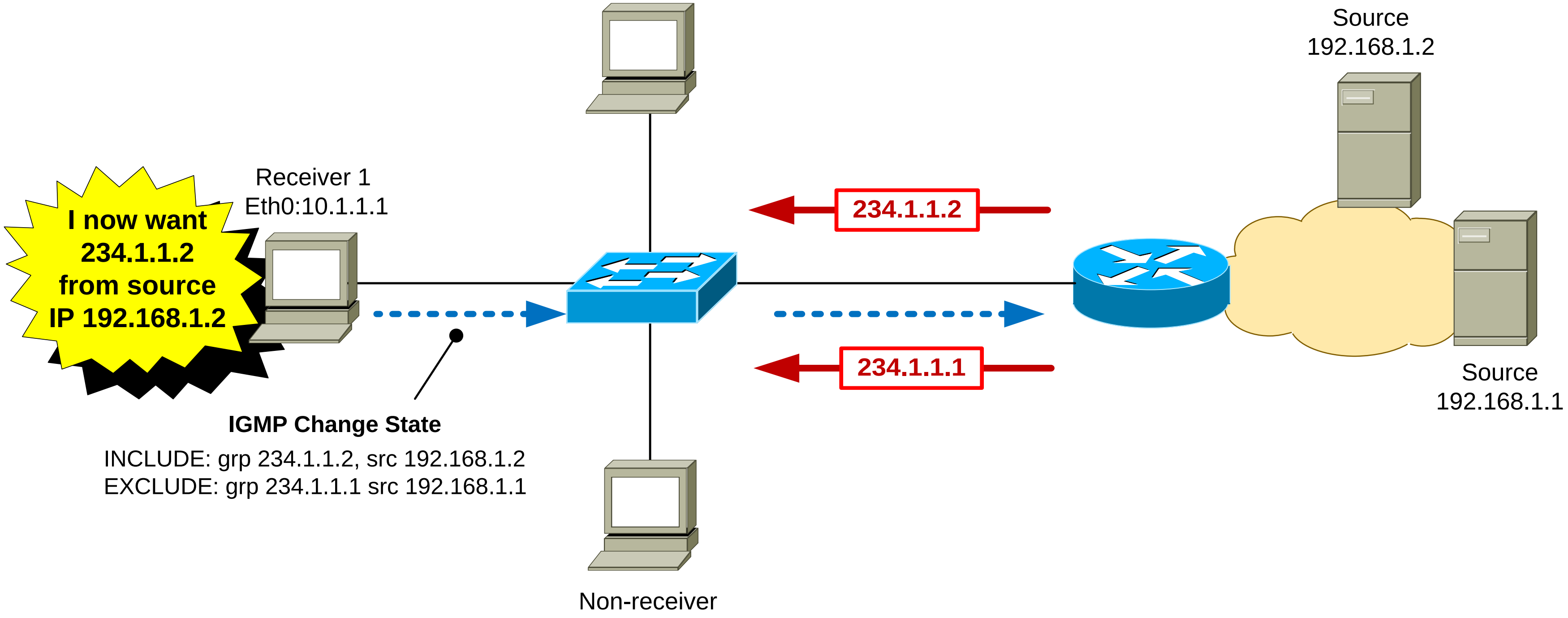


IGMPv3 Source Discovery

- Q: How does the receiver know the source address for each group ?
- A: The receiver app is pre-populated with this information.



IGMPv3 – Changing a Group



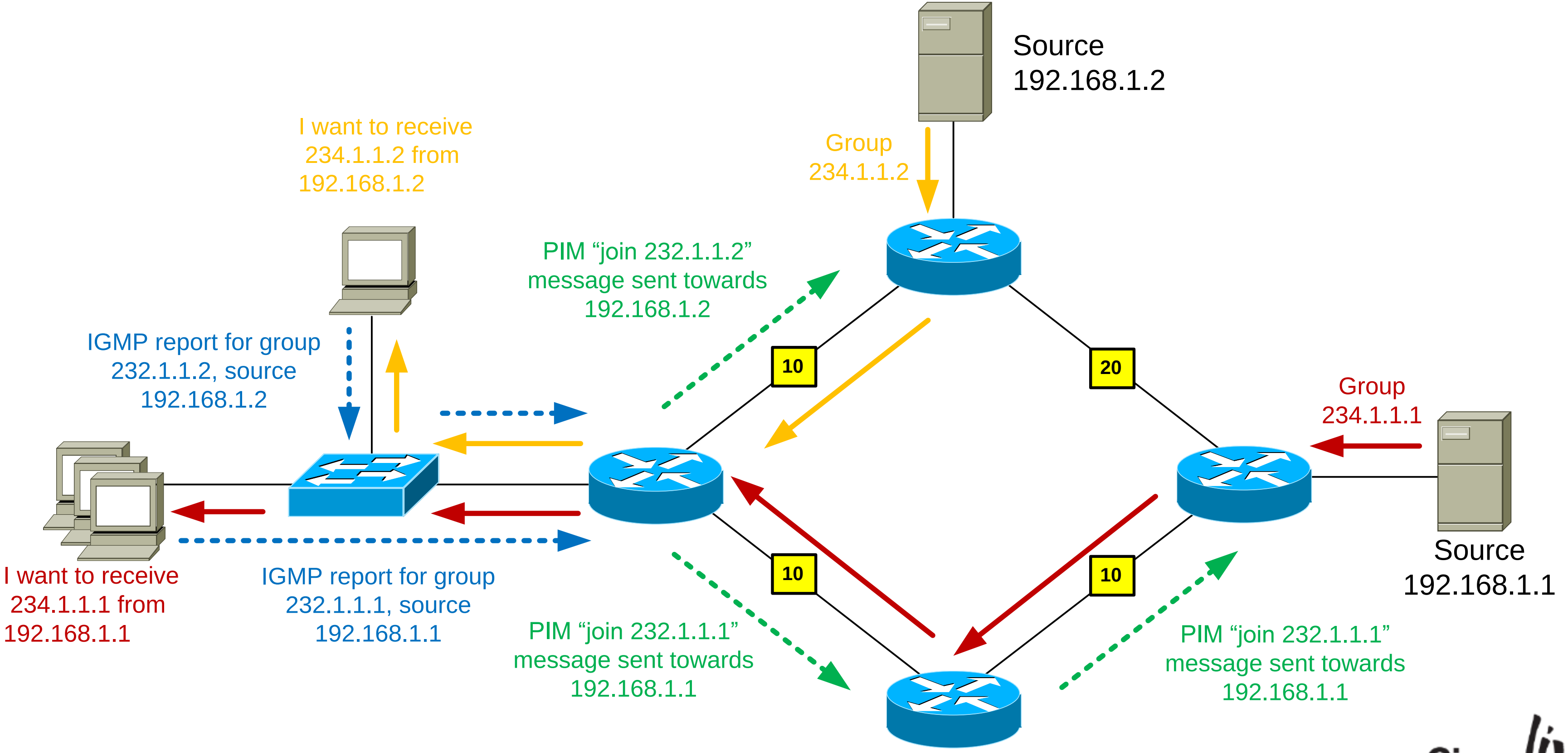
Advantages of IGMPv3

- Hosts can join one group and leave another in the same transaction. IGMPv2 requires separate report/leave messages.
- Reduces the likelyhood of multicast group being spoofed by a rogue source.
- Eliminates overlapping multicast addresses.
- First-hop router immediately knows the source address, so no need for Rendezvous Point – can use PIM-SSM.

Router-Router Signalling: PIM-SSM

- **SSM = Source Specific Multicast**
- PIM-SSM requires the first-hop router to know the address of the MC source for each group
- PIM-SSM is usually deployed in conjunction with IGMPv3, where the receiver indicates the source address in the IGMPv3 report packet
- The first-hop router sends a PIM join **directly** towards the sender using the unicast routing table. There is no “Shared Tree” via an RP as in PIM-SM.

PIM-SSM: Operation



PIM-SSM Advantages

- Easy to configure and maintain
  - No RPs
  - No Multicast Source Discovery Protocol (MSDP) between redundant RPs
- Efficient network usage
  - Traffic is not routed temporarily via the RP
  - Most direct path from source to receiver is always used
- Enhanced security
  - Spoofing of MC stream is more difficult

PIM-SSM Mapping

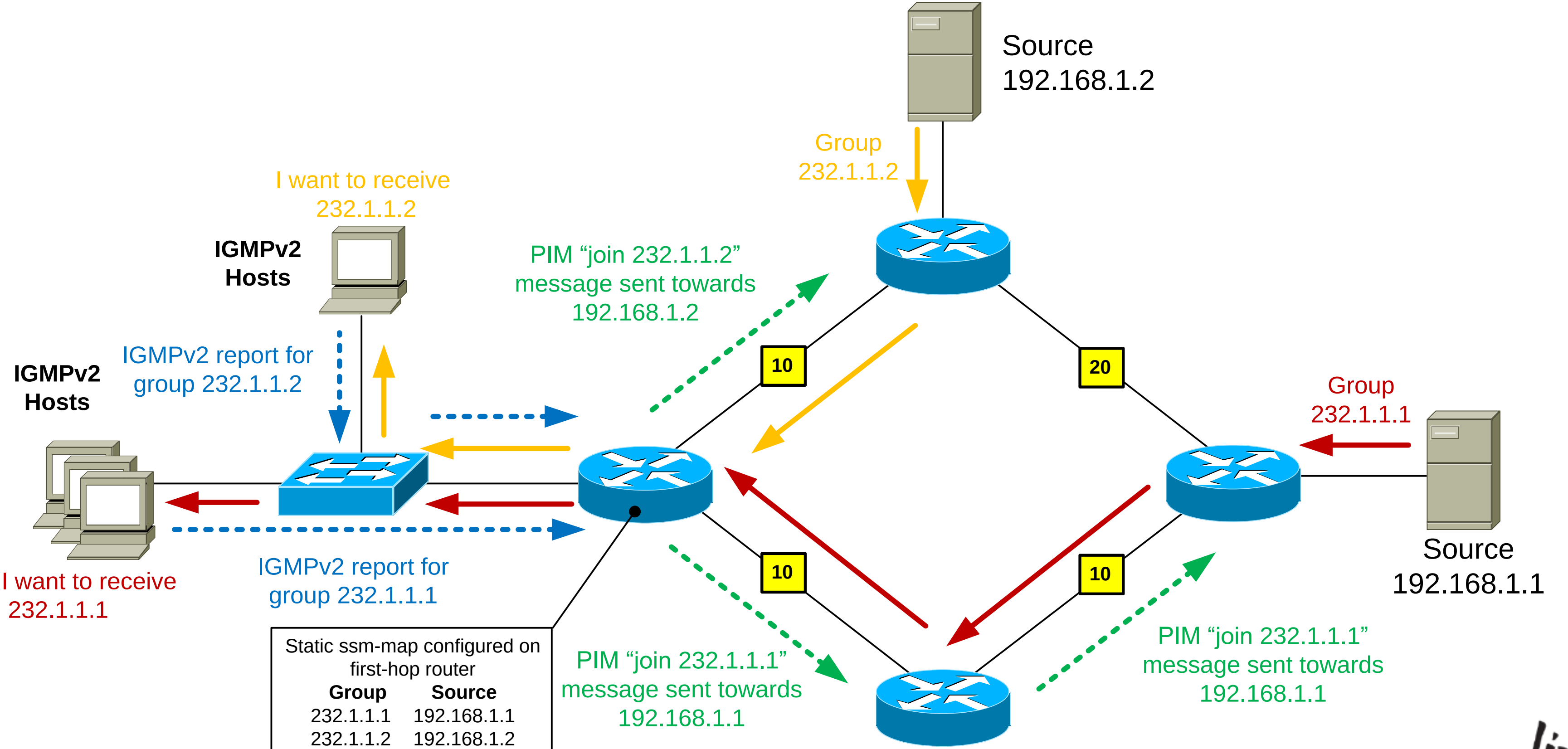
- The ideal SSM architecture uses IGMPv3 for host-router signalling and PIM-SSM for router-router signalling
- But...IGMPv3 host support is patchy, whereas IGMPv2 is ubiquitous

  Q: Is there a way to use PIM-SSM in the network when I have hosts that only support IGMPv2 ?

  A: Yes – its called PIM-SSM mapping

- PIM-SSM mapping can be used as an interim measure until IGMPv3 is supported on all hosts

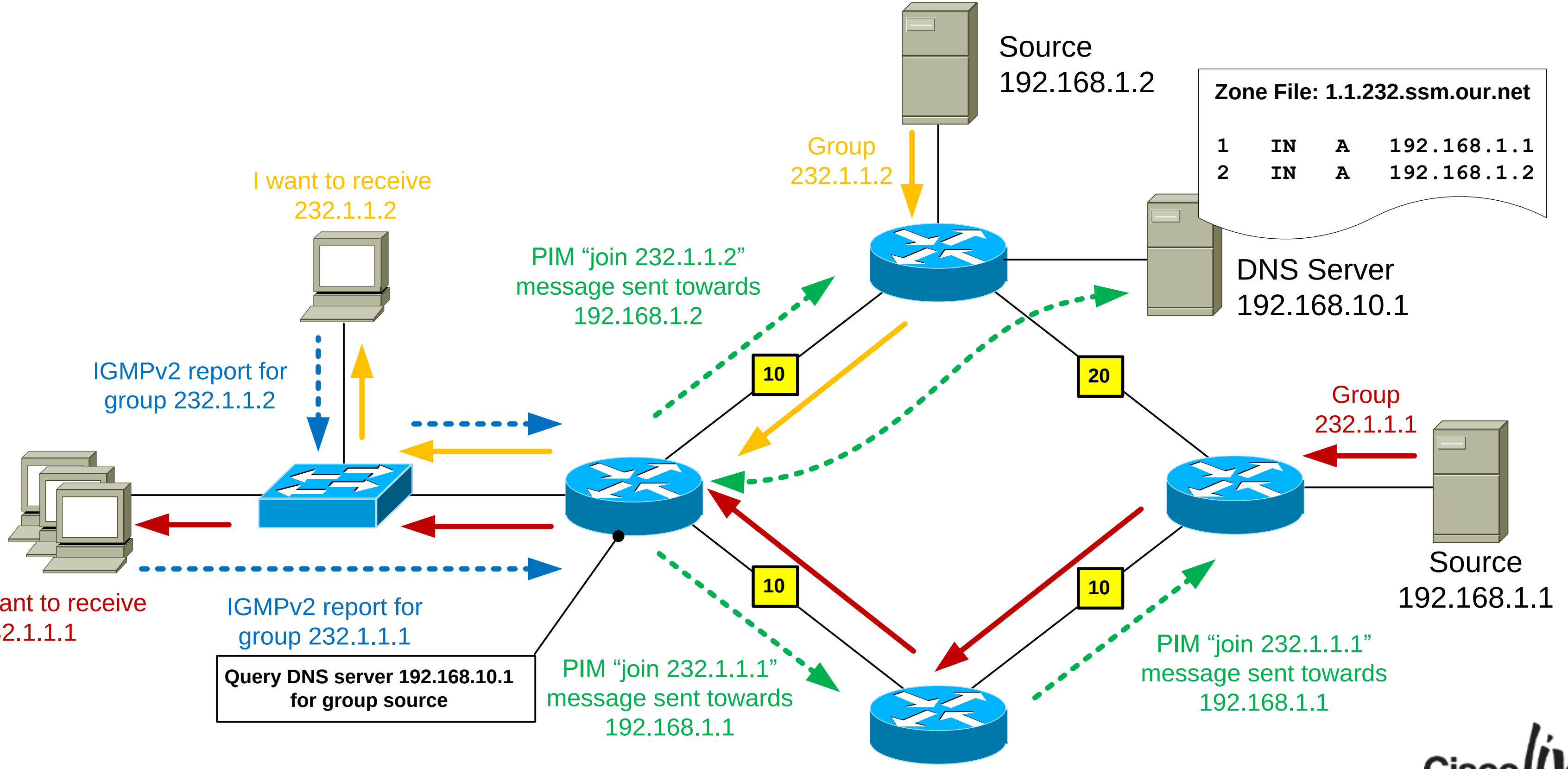
PIM-SSM Static Mapping



Static ssm-map configured on first-hop router

Group	Source
232.1.1.1	192.168.1.1
232.1.1.2	192.168.1.2

PIM-SSM Dynamic (DNS) Mapping



IPv4 vs. IPv6 Multicast

A quick glimpse

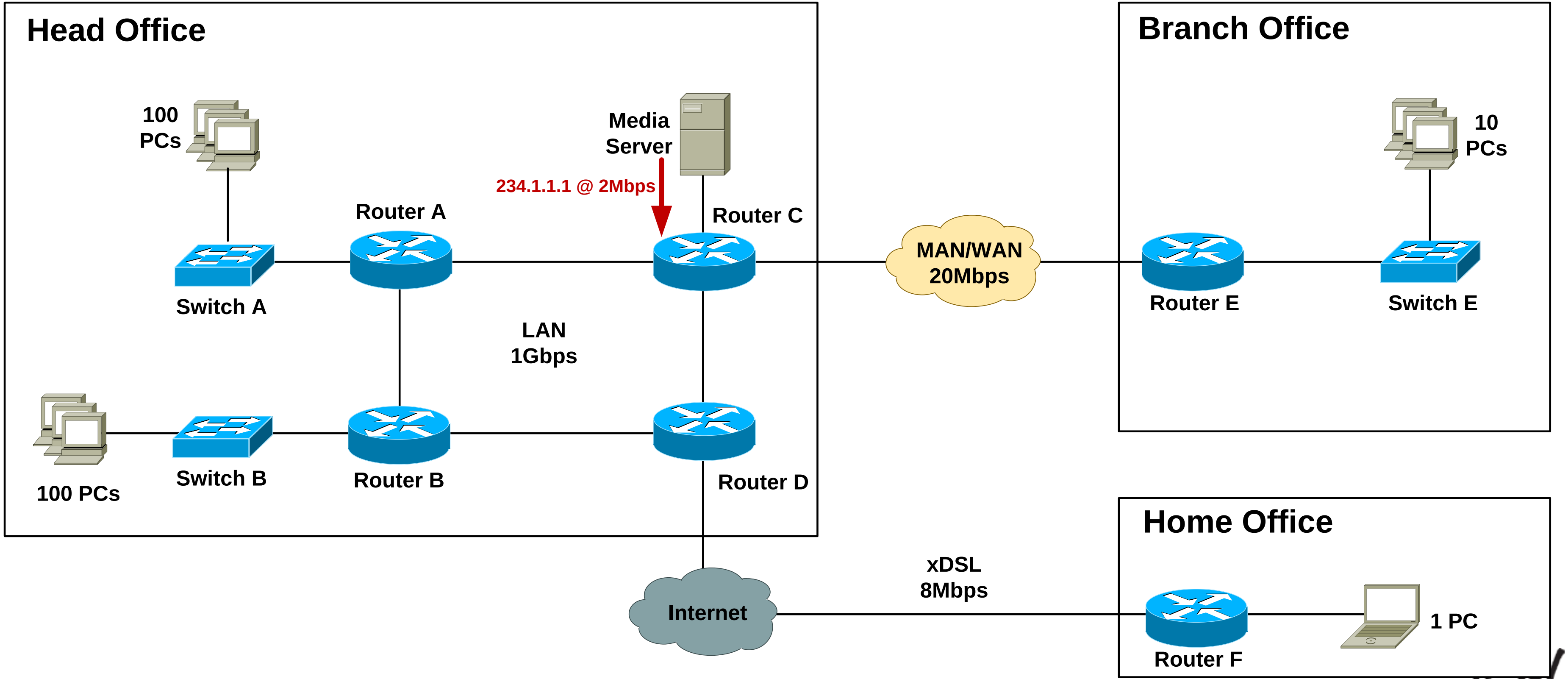
IP Service	IPv4 Solution	IPv6 Solution
Address Range	32-Bit, Class D	128-Bit (112-Bit Group)
Routing	Protocol-Independent All IGPs and BGPv4+	Protocol-Independent All IGPs and BGPv4+ with IPv6 Mcast SAFI
Forwarding	PIM-DM, PIM-SM: ASM, SSM, BiDir	PIM-SM: ASM, SSM, BiDir
Group Management	IGMPv1, v2, v3	Multicast Listener Discovery MLDv1, v2
Domain Control	Boundary/Border	Scope Identifier
Interdomain Source Discovery	MSDP Across Independent PIM Domains	Single RP Within Globally Shared Domains

Multicast Design

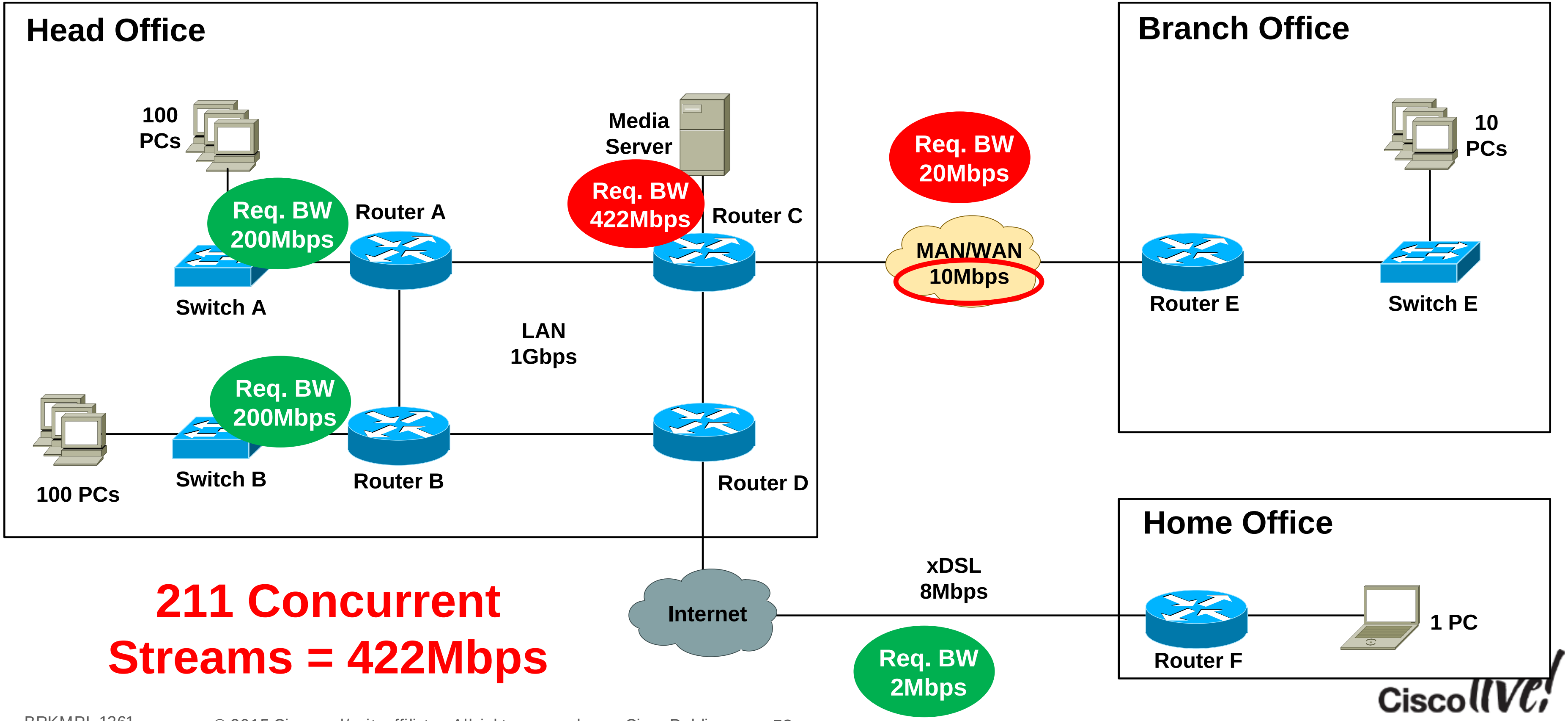
Case Study - Background

- Company has 1 head office with 200 staff, 1 branch office with 10 staff and occasional home users
- Management wants to deploy an in-house, always-on video channel that staff may watch at any time for the latest product releases and Company news
- Important events will require all users to watch the channel at the same time
- The video bitrate is 2 Mbps

Case Study – Network Topology

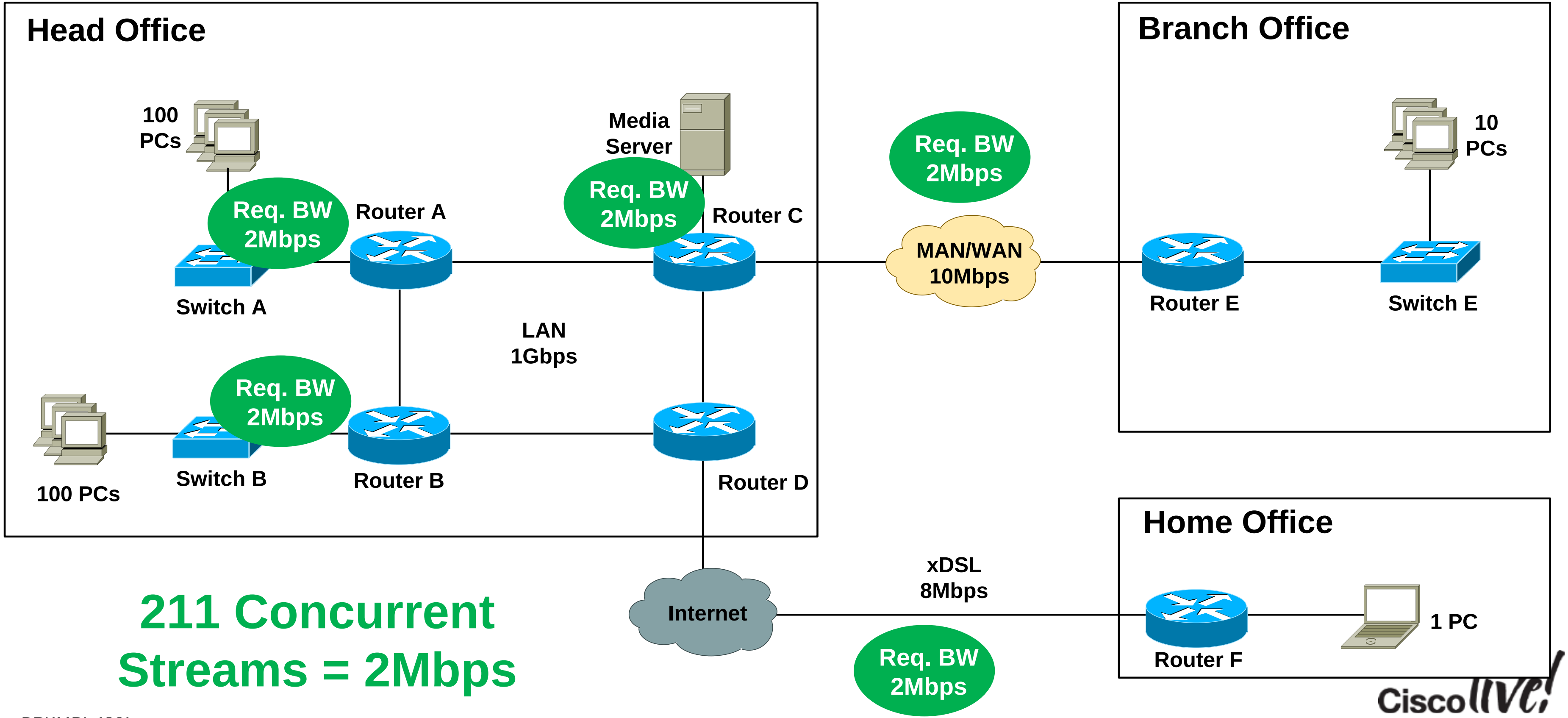


Case Study – Unicast Bandwidth Scenario



211 Concurrent Streams = 422Mbps

Case Study – Multicast Bandwidth Scenario



211 Concurrent Streams = 2Mbps

Case Study – Network Support for MC

- Cisco IOS provides broad platform support for PIM (all variants) and IGMPv1/2/3
- Check with WAN provider for MC support
  - Dark fibre, EoSDH, EoMPLS, Frame relay, ATM, SDH/SONET, leased-line services – usually no issues
  - Managed Ethernet, L3VPN, VPLS – check with provider.
  - SP network generally needs to be configured for MC support
- No native support for multicast across the Internet
- No native IPSec support for multicast

Case Study – Design Options

- **Option 1:** Any Source Multicast **(ASM)** design
  Hosts run IGMPv2
  Network runs PIM-SM with RP
- Option 2: Source Specific Multicast (SSM) design
  Hosts run IGMPv3
  Network runs PIM-SSM
- Option 3: SSM design with IGMP mapping
  Hosts run IGMPv2
  Network runs PIM-SSM with source address mapping

Case Study – ASM

▪ Step 1: Configure IGMP snooping on access switches

- IGMP snooping enabled by default on Cisco devices
- Configure "`ip igmp snooping vlan <x> immediate-leave`" for vlans with directly attached hosts only.

```
Switch_A#sh ip igmp snooping vlan 10
Vlan 10:
--------
IGMP snooping                              : Enabled
IGMPv2 immediate leave                     : Enabled
Multicast router learning mode             : pim-dvmrp
CGMP interoperability mode                 : IGMP_ONLY
Robustness variable                        : 2
Last member query count                    : 2
Last member query interval                 : 1000

Switch_A#
```

Case Study – ASM

- Step 2: Configure all routers for multicast

  - Globally enable multicast routing:

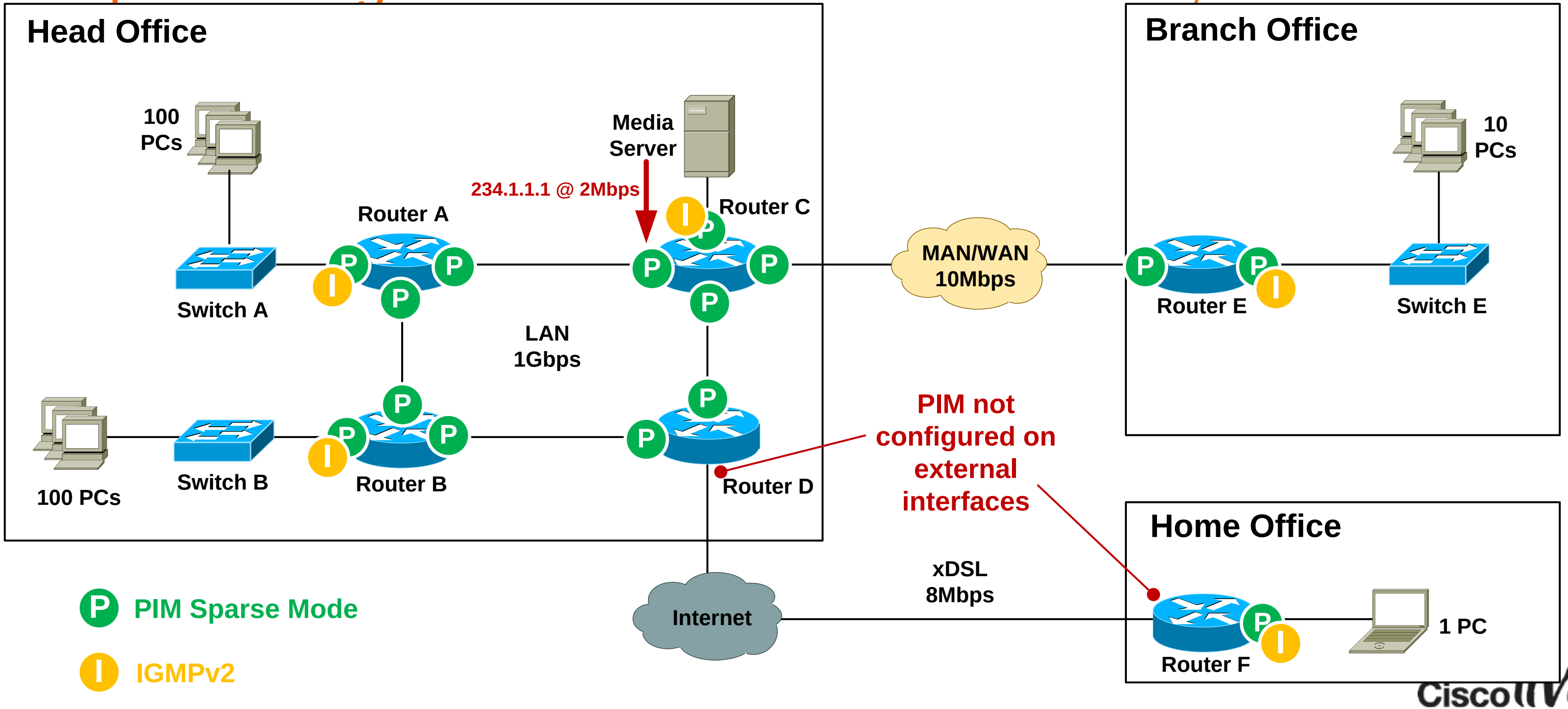
```
Router_A(config)#ip multicast-routing
Router_A(config)#do show ip multicast global
        Multicast Routing: enabled
        Multicast Multipath: disabled
        Multicast Route limit: No limit
        Multicast Triggered RPF check: enabled
        Multicast Fallback group mode: Sparse
Router_A(config)#
```

  - Configure PIM on all internal router interfaces:

```
Router_A(config-if)#int fast 0/3
Router_A(config-if)#ip pim sparse-mode
Router_A(config-if)#
```

Case Study – ASM

- Step 3: Configure all internal links for PIM-SM, IGMPv2



Case Study – ASM

▪ Step 4: Verify PIM neighbours

```
Router_A#sh ip pim neighbor
PIM Neighbor Table
Neighbor          Interface              Uptime/Expires    Ver   DR
Address                                                          Prio/Mode
10.0.0.5          FastEthernet0/3      1d02h/00:01:17    v2    1 / DR S
10.0.0.3          FastEthernet0/2      1d01h/00:01:31    v2    1 / DR
Router_A#
```

- Note: when PIM is enabled on an interface, IGMPv2 is also automatically enabled on that interface.

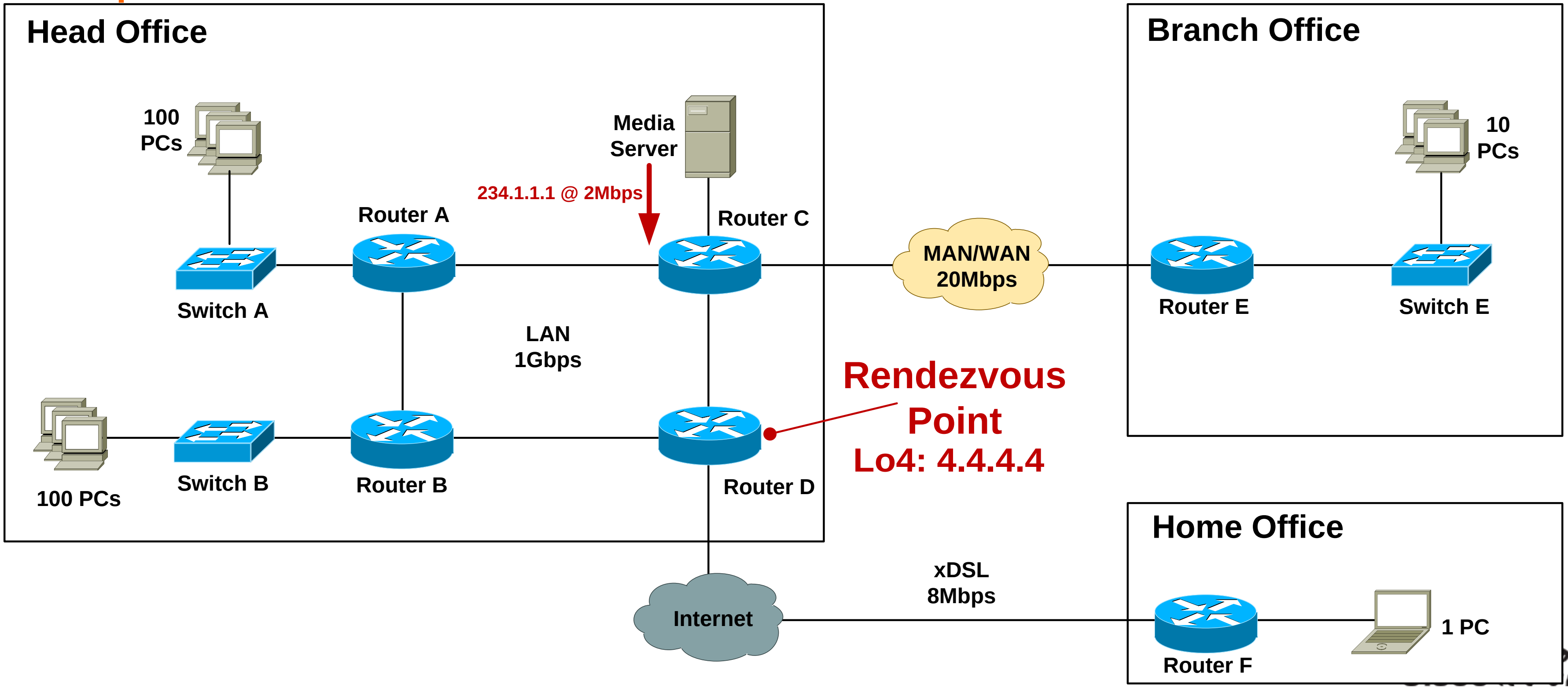
Case Study – ASM

▪ Step 5: Select RP router

- RP should be in a central location between sender and receivers.
- CPU grunt not critical as RP processing overhead is low.
- Select a router that has high network availability.
- Ensure the RP has a /32 loopback address as the source.
- Recommended to assign loopback address dedicated for RP use only (not used for router ID etc).

Case Study - ASM

- Step 5: Select RP router



Case Study – ASM

- Step 6: Configure static RP on all routers (including the RP)

```
ip access-list standard MC_Group_1
  permit 234.1.1.0 0.0.0.255

Router_C#conf t
Enter configuration commands, one per line.  End with CNTL/Z.

Router_C(config)#ip pim rp-address 4.4.4.4 MC_Group_1
```

- Step 7: Verify RP to Group mappings

```
Router_C#sh ip pim rp mapping

PIM Group-to-RP Mappings
Acl: MC_Group_1, Static
    RP: 4.4.4.4 (Router_D)
Router_C#
```

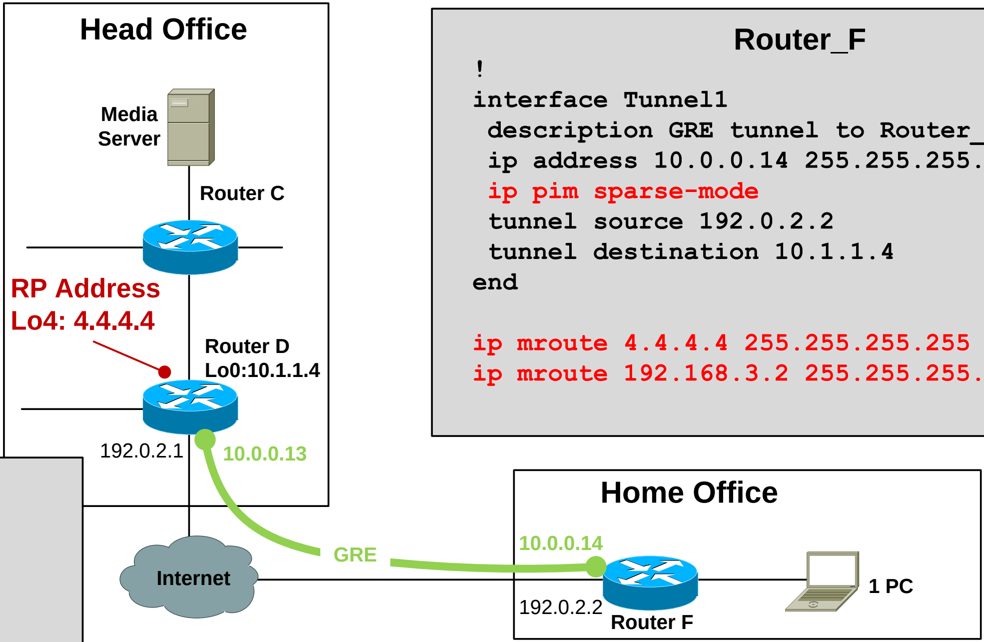
Case Study – ASM

▪ Step 8: Enable multicast over non-multicast networks

- Use GRE, L2TPv3 to tunnel MC over non-MC networks
- Need a static mroute for **both** the RP address and the MC source address for RPF check to pass.
- http://www.cisco.com/c/en/us/support/docs/ip/ip-multicast/43584-mcast-over-gre.html

Case Study – ASM

- Step 8: Enable multicast over non-multicast networks



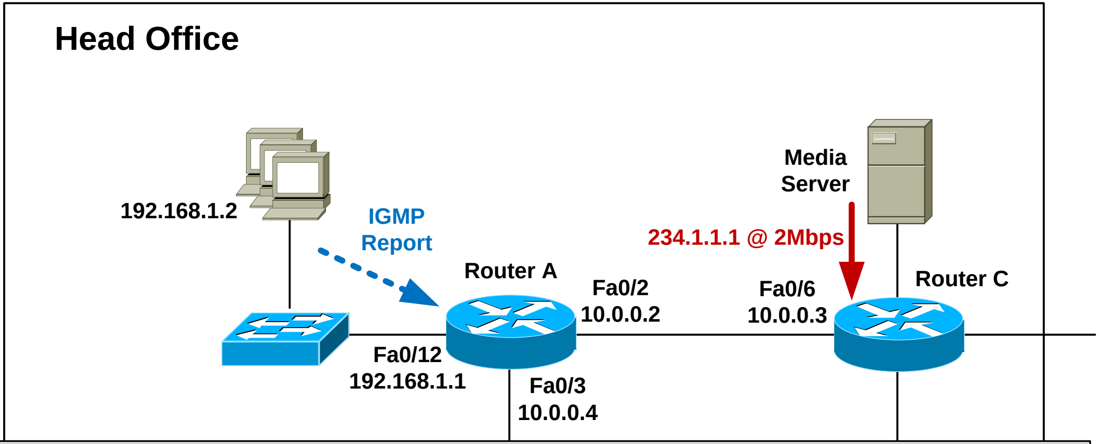
Router_F

```
!
interface Tunnel1
 description GRE tunnel to Router_D
 ip address 10.0.0.14 255.255.255.252
 ip pim sparse-mode
 tunnel source 192.0.2.2
 tunnel destination 10.1.1.4
end

ip mroute 4.4.4.4 255.255.255.255 Tunnel1
ip mroute 192.168.3.2 255.255.255.255 Tunnel1
```

Router_D

```
!
interface Tunnel1
 description GRE tunnel to Router_F
 ip address 10.0.0.13 255.255.255.252
 ip pim sparse-mode
 tunnel source 10.1.1.4
 tunnel destination 192.0.2.2
end
```

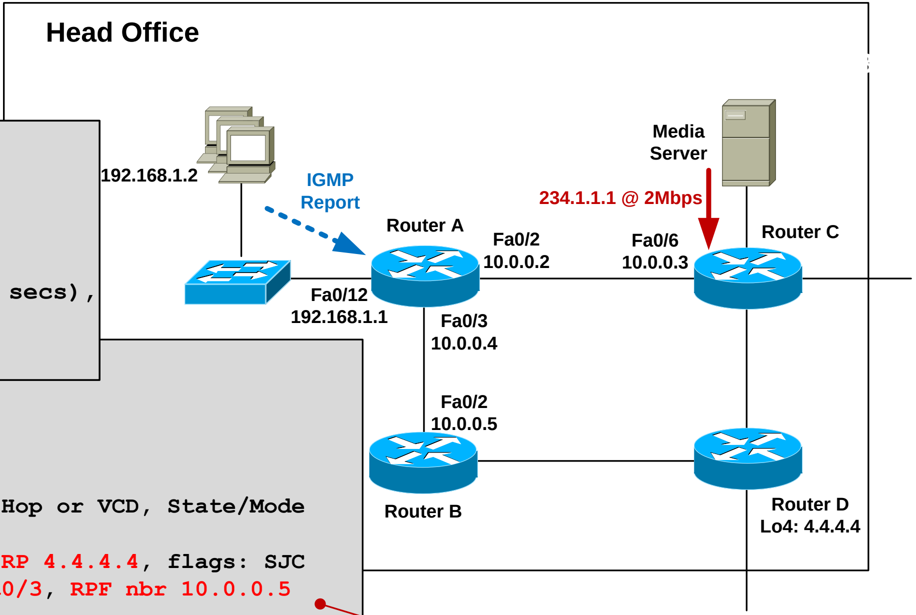
Case Study – ASM – IGMP Verification




```
Router_A#sh ip igmp membership
Flags: A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, U - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP the group is in
 <snip>
 Channel/Group                  Reporter        Uptime   Exp.  Flags  Interface
 *,234.1.1.1                    192.168.1.2     00:00:12 02:47 2A     Fa0/12
 Router_A#
```

Case Study – ASM – Mroute Verification

```
Router_A#show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 234.1.1.1, (Stream_1)
   Source: 192.168.3.2 (Media_Server)
     Rate: 245 pps/1967 kbps(1sec), 1968 kbps(last 20 secs),
       1966 kbps(life avg)
Router_A#
```




```
Router_A#show ip mroute
IP Multicast Routing Table
<snip>
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 234.1.1.1), 00:08:40/stopped, RP 4.4.4.4, flags: SJC
  Incoming interface: FastEthernet0/3, RPF nbr 10.0.0.5
  Outgoing interface list:
    FastEthernet0/12, Forward/Sparse, 00:08:40/00:02:11

(192.168.3.2, 234.1.1.1), 00:08:40/00:02:56, flags: JT
  Incoming interface: FastEthernet0/2, RPF nbr 10.0.0.3
  Outgoing interface list:
    FastEthernet0/12, Forward/Sparse, 00:08:40/00:02:11
```

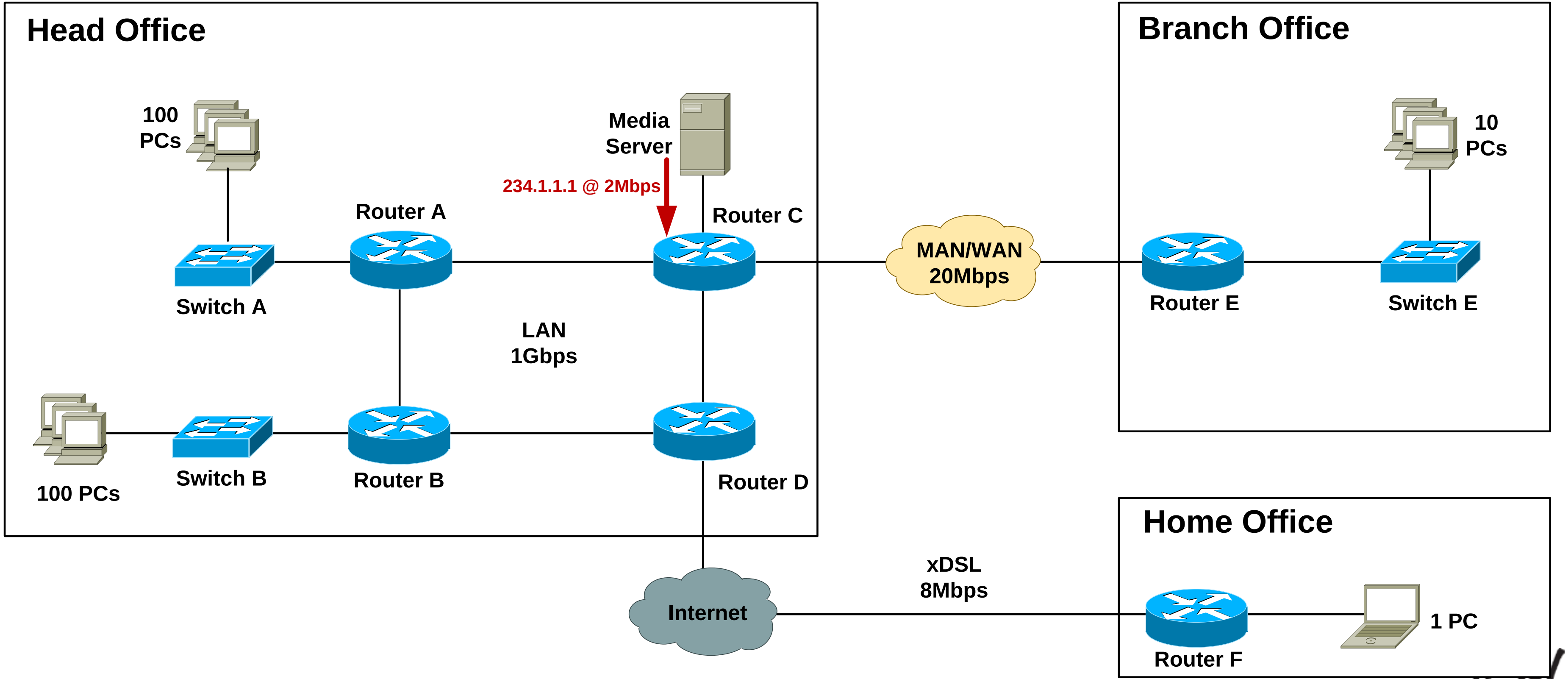
How Router_A receives MC traffic via the RP (src IP unknown)

How Router_A receives MC traffic directly from the source (src IP known)

Case Study – Design Options

- Option 1: Any Source Multicast (ASM) design
  Hosts run IGMPv2
  Network runs PIM-SM
- **Option 2:** Source Specific Multicast (**SSM**) design
  Hosts run IGMPv3
  Network runs PIM-SSM
- Option 3: SSM design with IGMP mapping
  Hosts run IGMPv2
  Network runs PIM-SSM with source address mapping

Case Study – SSM



Case Study – SSM

Step 1: Configure all routers for SSM

- Globally enable multicast routing:

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

- Configure PIM-SSM ranges:

```
! Define ACL for SSM ranges (default is 232.0.0.0/8)

Router_A(config)#ip access-list standard SSM-Groups
Router_A(config-std-nacl)#permit 234.0.0.0 0.255.255.255

! Configure SSM range

Router_A(config-std-nacl)#ip pim ssm range SSM-Groups
Router_A(config)#
```

Case Study – SSM

Step 2: Configure IGMP

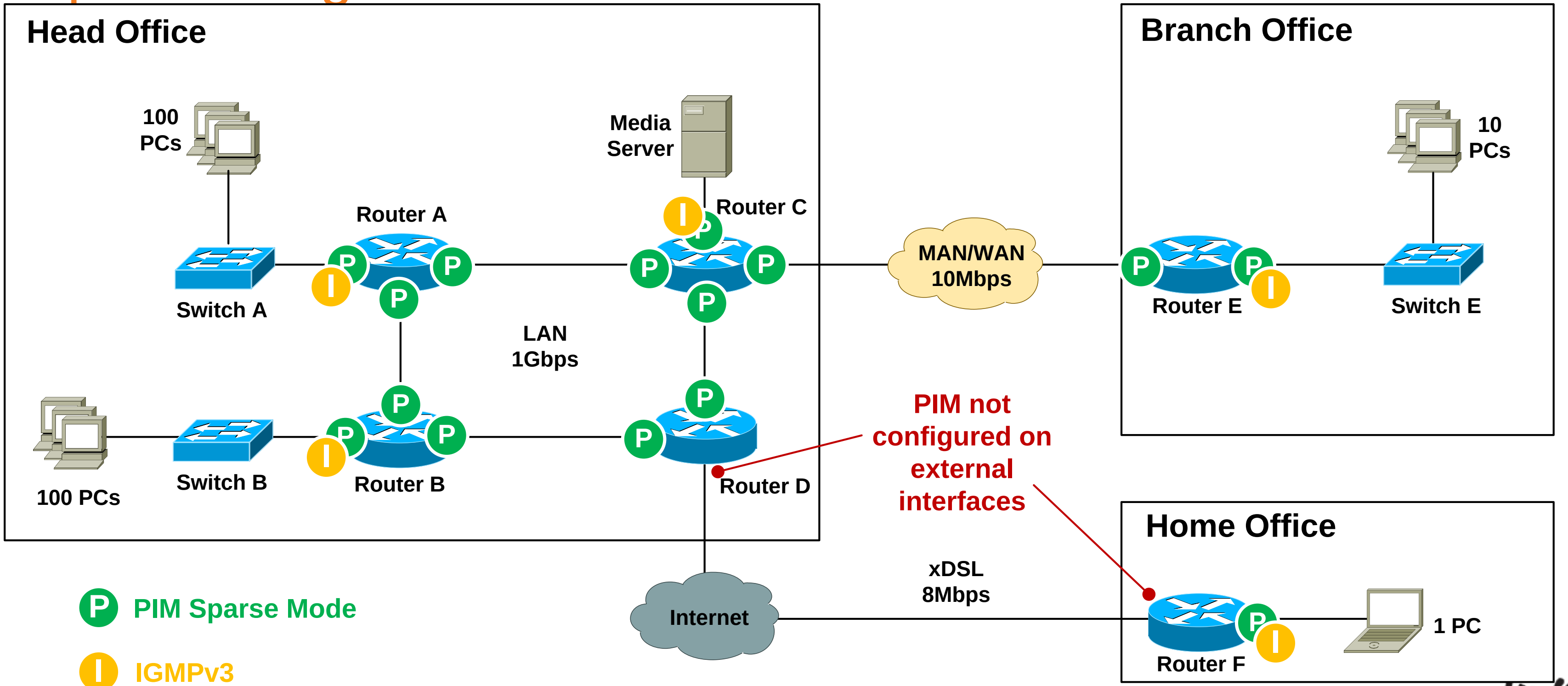
- IGMPv3 snooping enabled by default on Cisco devices
- Need to explicitly configure IGMPv3 on router interface that connects to LAN

```
Router_A(config)#int fast 0/12
Router_A(config-if)#ip igmp version 3
Router_A(config-if)#
```

```
Router_A#sh ip igmp interface fast 0/12
FastEthernet0/12 is up, line protocol is up
  Internet address is 192.168.1.1/24
  IGMP is enabled on interface
  Current IGMP host version is 3
  Current IGMP router version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  <snip>
  Router_A#
```

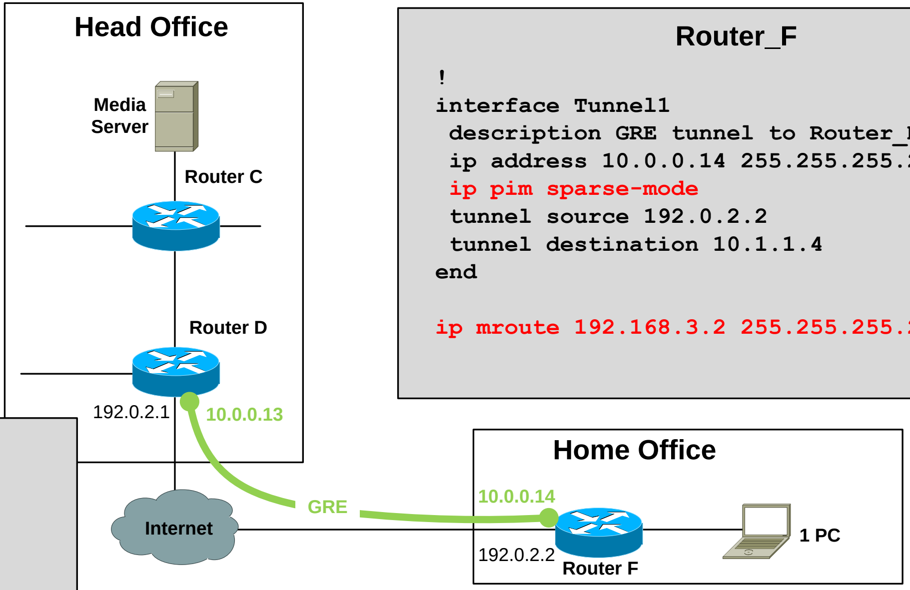
Case Study – SSM

- Step 3: Configure all internal links for PIM-SM



Case Study – SSM

- Step 4: Enable multicast over non-multicast networks
  - Need a static mroute for MC source only



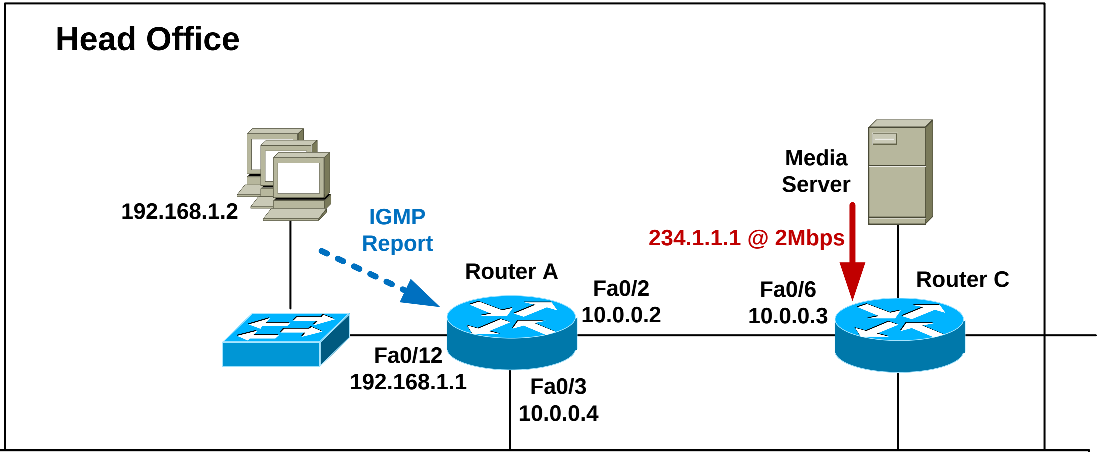
Router_F

```
!
interface Tunnel1
 description GRE tunnel to Router_D
 ip address 10.0.0.14 255.255.255.252
 ip pim sparse-mode
 tunnel source 192.0.2.2
 tunnel destination 10.1.1.4
end

ip mroute 192.168.3.2 255.255.255.255 Tunnel1
```

Router_D

```
!
interface Tunnel1
 description GRE tunnel to Router_F
 ip address 10.0.0.13 255.255.255.252
 ip pim sparse-mode
 tunnel source 10.1.1.4
 tunnel destination 192.0.2.2
end
```

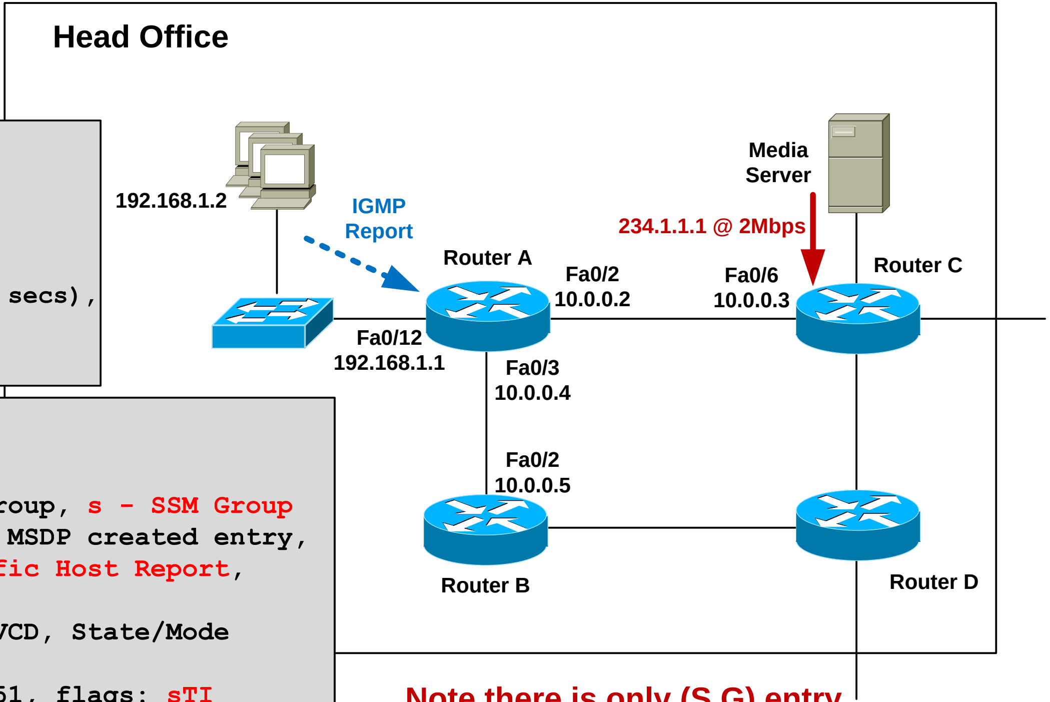
Case Study – SSM – IGMP Verification




```
Router_A#show ip igmp membership

Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))

 Channel/Group                   Reporter        Uptime   Exp.  Flags  Interface
/*,234.1.1.1                     192.168.1.2     00:43:29 stop  3MA    Fa0/12
 192.168.3.2,234.1.1.1                           00:43:29 02:03 RA     Fa0/12

Router_A#
```

Case Study – SSM – Mroute Verification

```
Router_A#show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 234.1.1.1, (Stream_1)
   Source: 192.168.3.2 (Media_Server)
     Rate: 245 pps/1967 kbps(1sec), 1968 kbps(last 20 secs),
       1966 kbps(life avg)
Router_A#
```




```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       U - URD, I - Received Source Specific Host Report,
       Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(192.168.3.2, 234.1.1.1), 00:59:25/00:02:51, flags: sTI
  Incoming interface: FastEthernet0/2, RPF nbr 10.0.0.3
  Outgoing interface list:
    FastEthernet0/12, Forward/Sparse, 00:59:01/00:02:05
```

Note there is only (S,G) entry and no (*,G) as no RP is present

Case Study – Design Options

- Option 1: Any Source Multicast (ASM) design
  Hosts run IGMPv2
  Network runs PIM-SM
- Option 2: Source Specific Multicast (SSM) design
  Hosts run IGMPv3
  Network runs PIM-SSM
- **Option 3:** SSM design with IGMP mapping
  Hosts run IGMPv2
  Network runs PIM-SSM with source address mapping

Case Study – IGMPv2 + PIM-SSM

- **Step 1:** Configure IGMPv2 snooping on access switches
- **Step 2:** Configure all routers for multicast-routing
- **Step 3:** Enable PIM-SM (even though we are using SSM) on all internal interfaces)

Case Study – IGMPv2 + PIM-SSM

Step 4: Configure all routers for SSM

- Configure PIM-SSM ranges:

```
! Define ACL for SSM ranges (default is 232.0.0.0/8)

Router_A(config)#ip access-list standard SSM-Groups
Router_A(config-std-nacl)#permit 234.0.0.0 0.255.255.255

! Configure SSM range

Router_A(config-std-nacl)#ip pim ssm range SSM-Groups
Router_A(config)#
```

Case Study – IGMPv2 + PIM-SSM

▪ Step 5a: Configure static IGMP SSM mapping

- Globally enable IGMP mapping

```
Router_A(config)#ip igmp ssm-map enable
```

- Configure static group-to-source mapping using ACL:

```
Router_A(config)#no ip igmp ssm-map query dns
Router_A(config)#access-list 10 permit host 234.1.1.1
Router_A(config)#ip igmp ssm-map static 10 192.168.3.2
```

"When I see an IGMPv2 report for groups defined in ACL 10, assign the source address 192.168.3.2"

Case Study – IGMPv2 + PIM-SSM

▪ Step 5b: Configure dynamic IGMP SSM mapping

- Globally enable IGMP mapping

```
Router_A(config)#ip igmp ssm-map enable
```

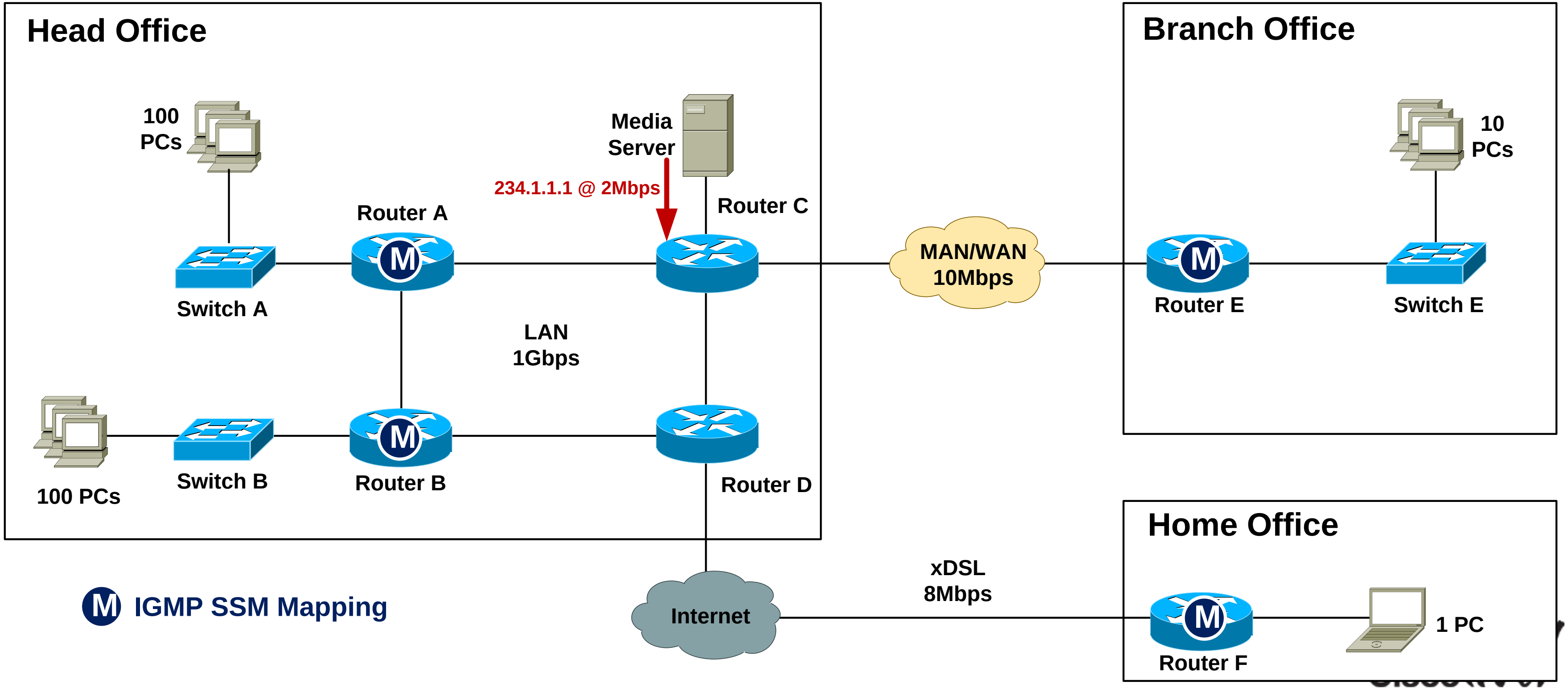
- Configure dynamic group-to-source mapping using DNS:

```
Router_A(config)#ip igmp ssm-map query dns
Router_A(config)#ip name-server 192.168.3.10
```

"When I see an IGMPv2 report for any group, perform a reverse DNS lookup to obtain the source address"

Case Study – IGMPv2 + PIM-SSM

- IGMP SSM mapping configuration locations



Case Study – SSM Mapping Verification

Step 5: Verify IGMP mapping

- Static mapping

```
Router_A#sh ip igmp ssm-mapping 234.1.1.1
Group address: 234.1.1.1
Database      : Static
Source list   : 192.168.3.2
Router_A#
```

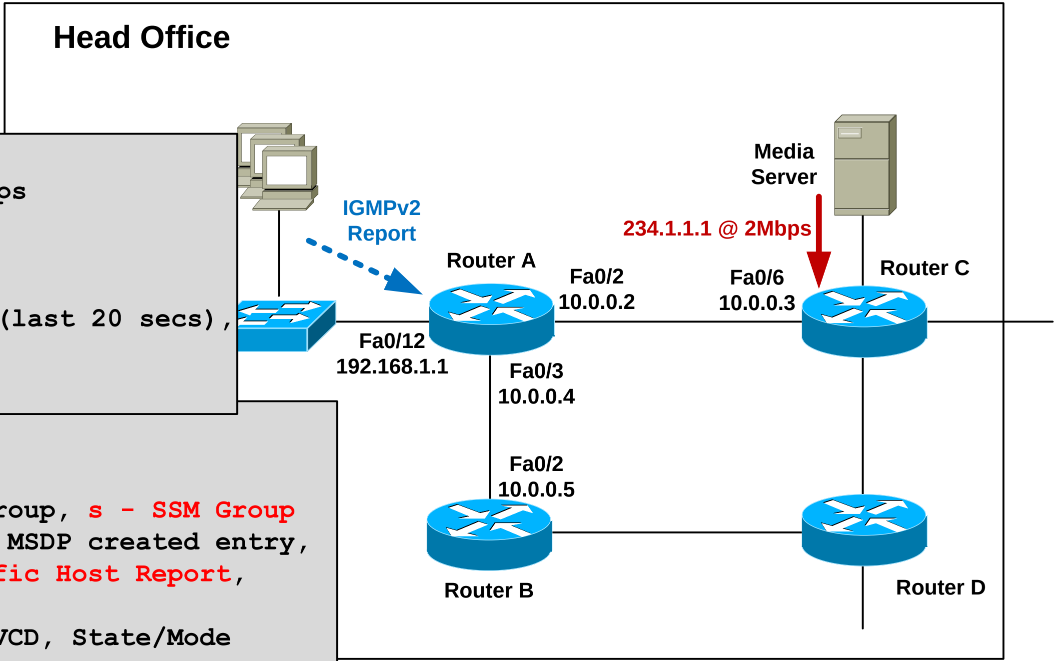
- Dynamic mapping

```
Router_A#sh ip igmp ssm-mapping 234.1.1.1
Group address: 234.1.1.1
Database      : DNS
DNS name      : 1.1.1.234.in-addr.arpa
Expire time   : 860000
Source list   : 192.168.3.2
Router_A#
```

Case Study – SSM Mapping – Verification

```
Router_A#show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 234.1.1.1, (Stream_1)
   Source: 192.168.3.2 (Media_Server)
     Rate: 245 pps/1968 kbps(1sec), 1968 kbps(last 20 secs),
       1967 kbps(life avg)
Router_A#
```

```
Router_A#show ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       U - URD, I - Received Source Specific Host Report,
       Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(192.168.3.2, 234.1.1.1), 01:23:13/00:02:29, flags: sTI
  Incoming interface: FastEthernet0/2, RPF nbr 10.0.0.3
  Outgoing interface list:
    FastEthernet0/12, Forward/Sparse, 00:09:01/00:02:12
```



IGMP ssm-mapping not evident in output

Troubleshooting

Mimicking a Multicast Source

- Use video streaming software on a PC such as VLC:

```
vlc --repeat filename.avi --sout '#standard{access=udp,mux=ts,dst=234.1.1.1:1234}
```

- Use a ping flood or traffic generator to fake it....

```
MC_Source#ping
Protocol [ip]:
Target IP address: 234.1.1.1
Repeat count [1]: 100000000000
Datagram size [100]: 1300
Timeout in seconds [2]: 0
Extended commands [n]: y
Interface [All]: FastEthernet1/0/24
Source address: 192.168.3.2
Type escape sequence to abort.
Sending 1215752192, 1300-byte ICMP Echos to 234.1.1.1,
 timeout is 0 seconds:
Packet sent with a source address of 192.168.3.2
...................................................
```

Mimicking a Multicast Receiver

- PC running VLC to join MC group

```
vlc udp:@234.1.1.1 (IGMPv2 report)
or
vlc udp:192.168.3.2@234.1.1.1 (IGMPv3 report)
```

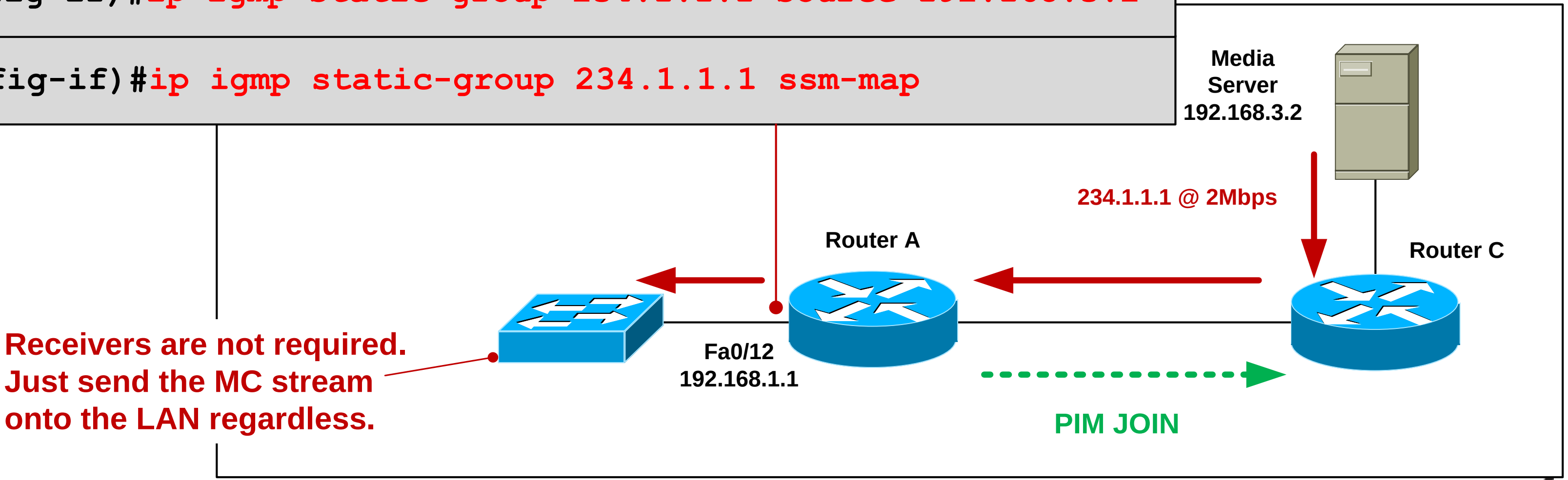
- Router joins MC group as if it were a receiver

```
! Send IGMPv2 report for 234.1.1.1
Router(config-if)#ip igmp version 2
Router(config-if)#ip igmp join-group 234.1.1.1

or

! Send IGMPv3 report for 234.1.1.1, source 192.168.3.2
Router(config-if)#ip igmp version 3
Router(config-if)#ip igmp join-group 234.1.1.1 source 192.168.3.2
```

Mimicking a Multicast Receiver

- Statically join a router interface to a group

```
Router(config-if)#ip igmp static-group 234.1.1.1
Router(config-if)#ip igmp static-group 234.1.1.1 source 192.168.3.2
Router(config-if)#ip igmp static-group 234.1.1.1 ssm-map
```



Common Causes of Multicast Problems

- Source problem
  Is the source sending the MC stream properly ?
- Receiver issue
  Is the client asking to receive the stream ?
- Underlying network issue
  Is the underlying network OK ?
- MC network misconfiguration
  Is the network configured correctly ?

Source Not Sending Stream Correctly

- Verify source is actually sending MC stream
  - tcpdump, Wireshark, SNMP
- Check first-hop router is receiving MC at correct bit-rate
  - compare current rate to baseline and historical rate

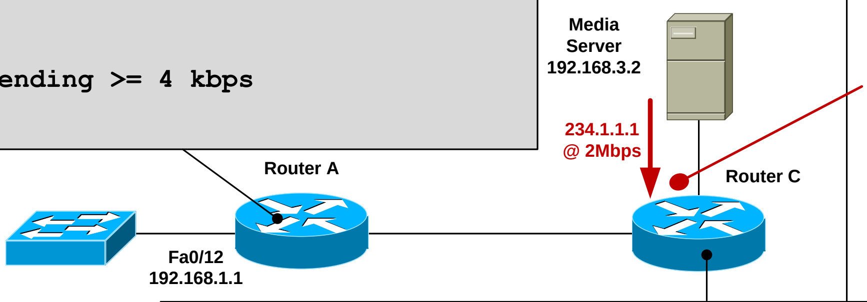
```
Router_C#sh ip mroute active
Active IP Multicast Sources - sending >= 4 kbps

Group: 234.1.1.1, (Stream_1)
   Source: 192.168.3.2 (Media_Server)
     Rate: 165 pps/1324 kbps(1sec), 1964 kbps(last 30 secs), 1963 kbps(life avg)
Router_C#
```

Source – Low TTL value

- Incorrect source TTL can cause MC stream to be dropped

```
Router_A#show ip mroute
IP Multicast Routing Table
<snip>
 (192.168.3.2, 234.1.1.1), 1d18h/00:02:35, flags: sTI
  Incoming interface: FastEthernet0/2, RPF nbr 10.0.0.3
  Outgoing interface list:
    FastEthernet0/12, Forward/Sparse, 1d18h/00:02:35

Router_A#show ip mroute active
Active IP Multicast Sources - sending >= 4 kbps
Router_A#
```

mroute is accurate but no active streams



Stream stops at first-hop router (TTL=1) or part-way into the network (TTL >1)

```
Router_C#sh ip traffic | i bad hop count
          0 format errors, 0 checksum errors, 193949 bad hop count
Router_C#sh ip traffic | i bad hop count
          0 format errors, 0 checksum errors, 194069 bad hop count
Router_C#
```

Receiver Issue

- Use "**debug ip igmp**" to verify IGMP reports are being received.

```
IGMP(0): Received v2 Report on FastEthernet0/12 from 192.168.1.2 for 234.1.1.1
IGMP(0): Received Group record for group 234.1.1.2, mode 2 from 192.168.1.2 for 0 sources
IGMP(0): WAVL Insert group: 234.1.1.1 interface: FastEthernet0/12 Successful
IGMP(0): MRT Add/Update FastEthernet0/12 for (*,234.1.1.1)
```

- If not seeing reports come in, then use packet sniffer on receiver.

Underlying Network Issue

- The cause of most multicast problems is not multicast (!)

Q: Why might users report a general network issue as a multicast problem ?

A: Small amounts of packet loss, excessive latency or jitter, routing reconvergence are immediately evident to streaming audio/video users.

- Check for interface errors, link congestion, duplex mis-match, routing reachability – Networking 101 stuff !

Multicast Network Misconfiguration

- **Verify**
  - All internal links have PIM sparse mode configured
  - RP is configured on all routers (including the RP itself)

```
Router_F#sh ip mroute
IP Multicast Routing Table
<snip>
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 234.1.1.1), 00:06:17/stopped, RP 0.0.0.0, flags: SJC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:06:17/00:02:44
```

Missing RP configuration

Multicast Network Misconfiguration

- **Verify**
  - Network and hosts are running same IGMP version
  - Verify RPF check passes. ‘**sh ip mroute count | inc RPF failed|Other**

```
Router_F#sh ip mroute
IP Multicast Routing Table
<snip>
(*, 234.1.1.1), 00:15:01/stopped, RP 4.4.4.4, flags: SJC
  Incoming interface: Tunnel1, RPF nbr 10.0.0.13, Mroute
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:15:01/00:01:19

(192.168.3.2, 234.1.1.1), 00:04:40/00:02:33, flags: J
  Incoming interface: Null, RPF nbr 0.0.0.0, Mroute
  Outgoing interface list:
    FastEthernet0/1, Forward/Sparse, 00:04:40/00:01:19
Router_F#
```

RPF Check OK

RPF Check Failure (should never be 0.0.0.0)

Summary – What have we learnt?

- IPv4 Multicast & Addressing
- Internet Group Management Protocol (IGMP) version 2 and 3
- IGMP Snooping
- Multicast Distribution Tree (Source & Shared)
- Protocol Independent Multicast (PIM)
  - Any-Source Multicast (ASM) - PIM Sparse Mode (PIM-SM), Rendezvous Point (RP)
  - Source-Specific Multicast (SSM)
- Case Study
- Troubleshooting

Where to go from here.....

- Rendezvous Point Auto-discovery
- High availability
  - Source Redundancy
  - RP Redundancy
  - Fast convergence
- Multicast Security
- Inter-Domain Multicast
- IPv6 Multicast

Additional Resources

- Cisco Live Virtual Breakout Sessions
  https://www.ciscoliveaustralia.com/portal/login.ww

- Cisco Live “Meet the Expert” sessions

- CCO documentation: http://www.cisco.com/go/multicast

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

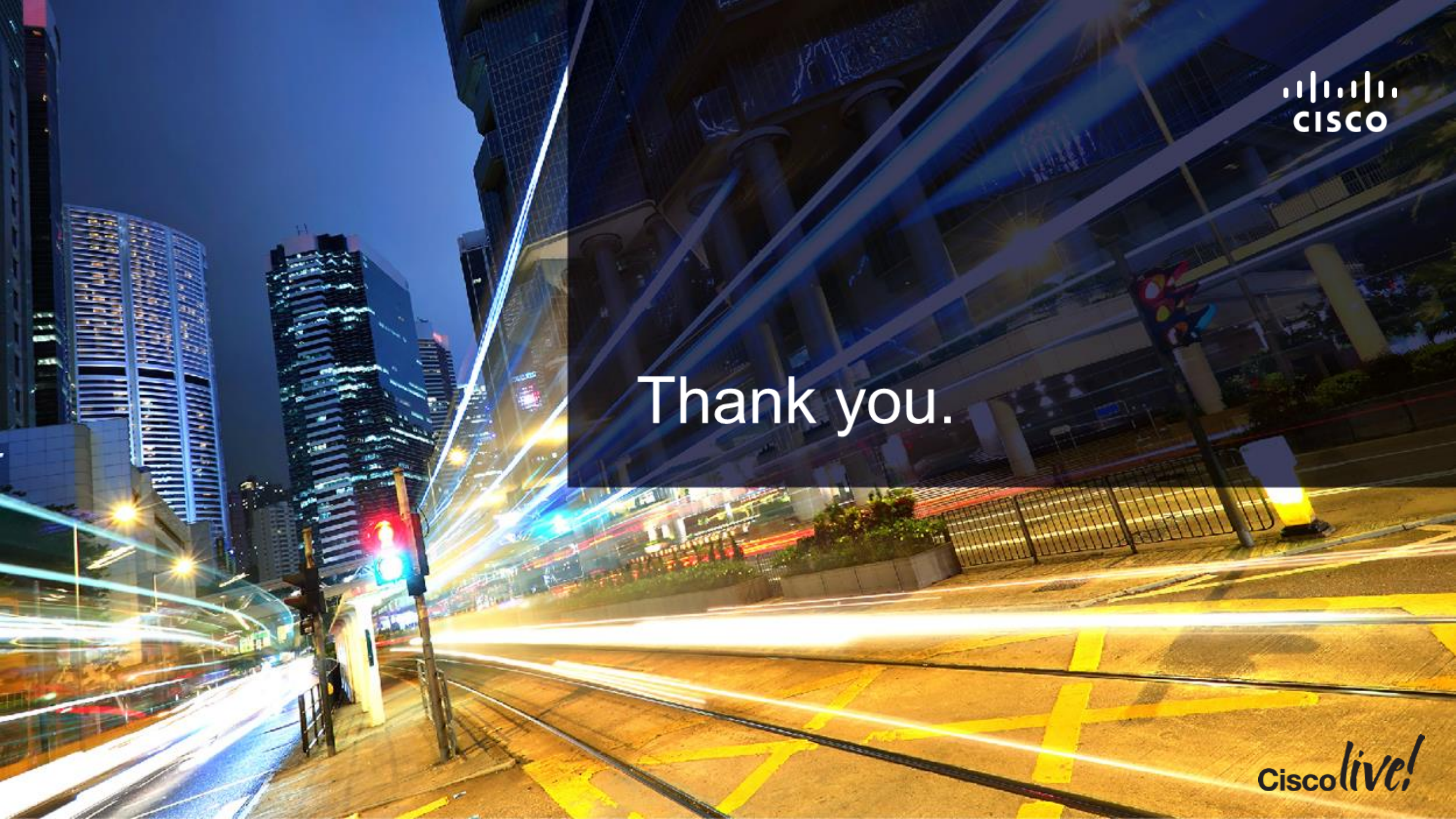
Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Cisco live!


Thank you.