

DDOS Attacks against PIM-SM Control Plane

Jean-Jacques PANSIOT
LSIIT Lab
Louis Pasteur University
Strasbourg – France

Benoît HILT
MIPS/GRTC Lab
Haute Alsace University
Colmar - France

Multicast today

Actual multicast model was defined by Deering in 1989

Entirely open and hosts driven model

Most deployed protocol is PIM in its Sparse Mode (SM)

It permits two communication models :

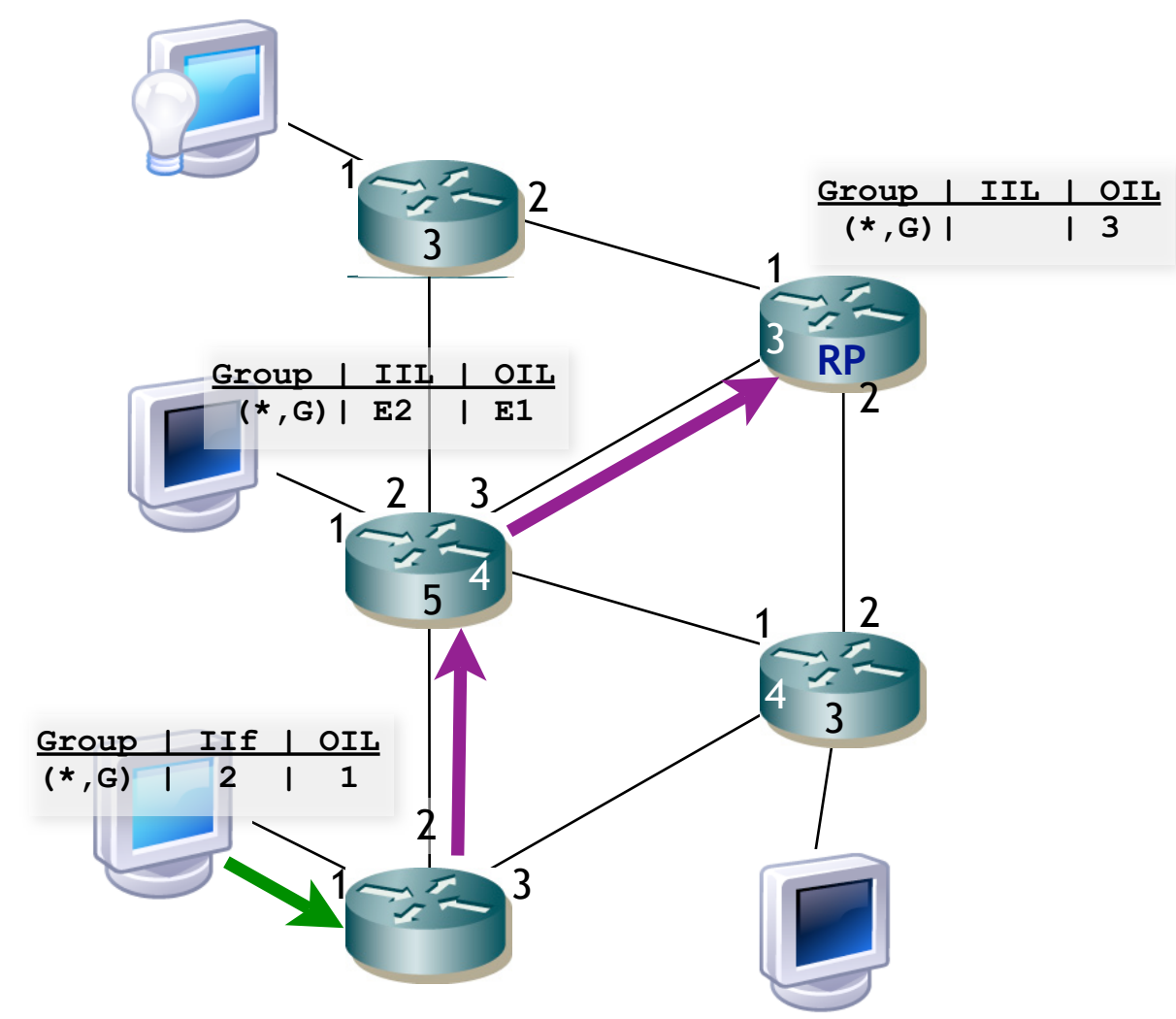
- ASM mode. Several trees are rooted at a unique point called Rendezvous Point (RP),
- SSM mode. Each tree is rooted at its data source.

Around PIM, additional protocols are needed

- IGMP for managing receivers in IPv4 LANs
- MLD for managing receivers in IPv6 LANs
- MBGP for interdomain multicast routing
- MSDP for interdomain source announcements (ASM model)
- RP-Embedded interdomain multicast (IPv6 ASM model)

Multicast more in details - ASM mode

Receiver side

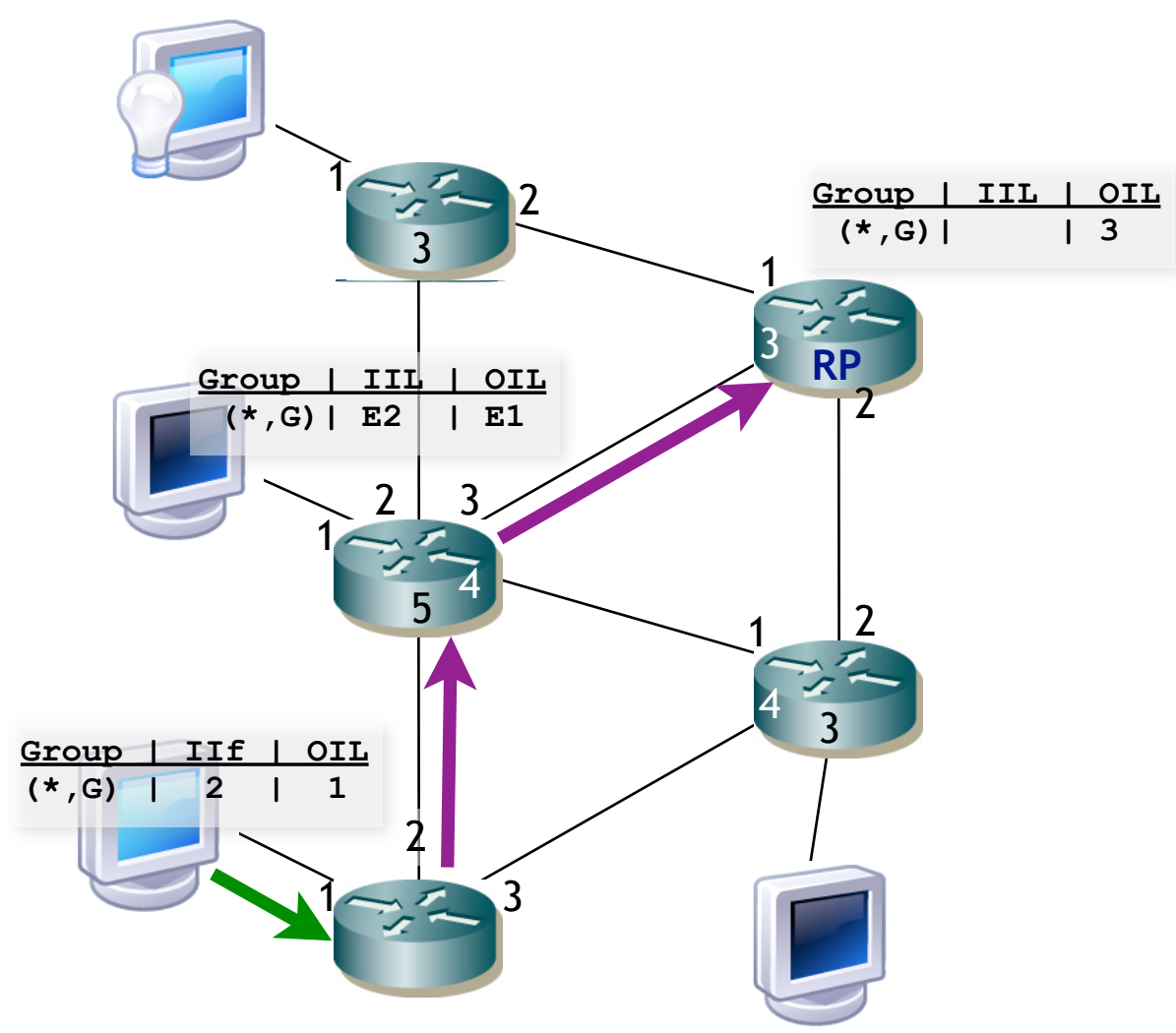


- Green arrow: IGMP Report
- Purple arrow: PIM Join
- Blue dashed arrow: Multicast data

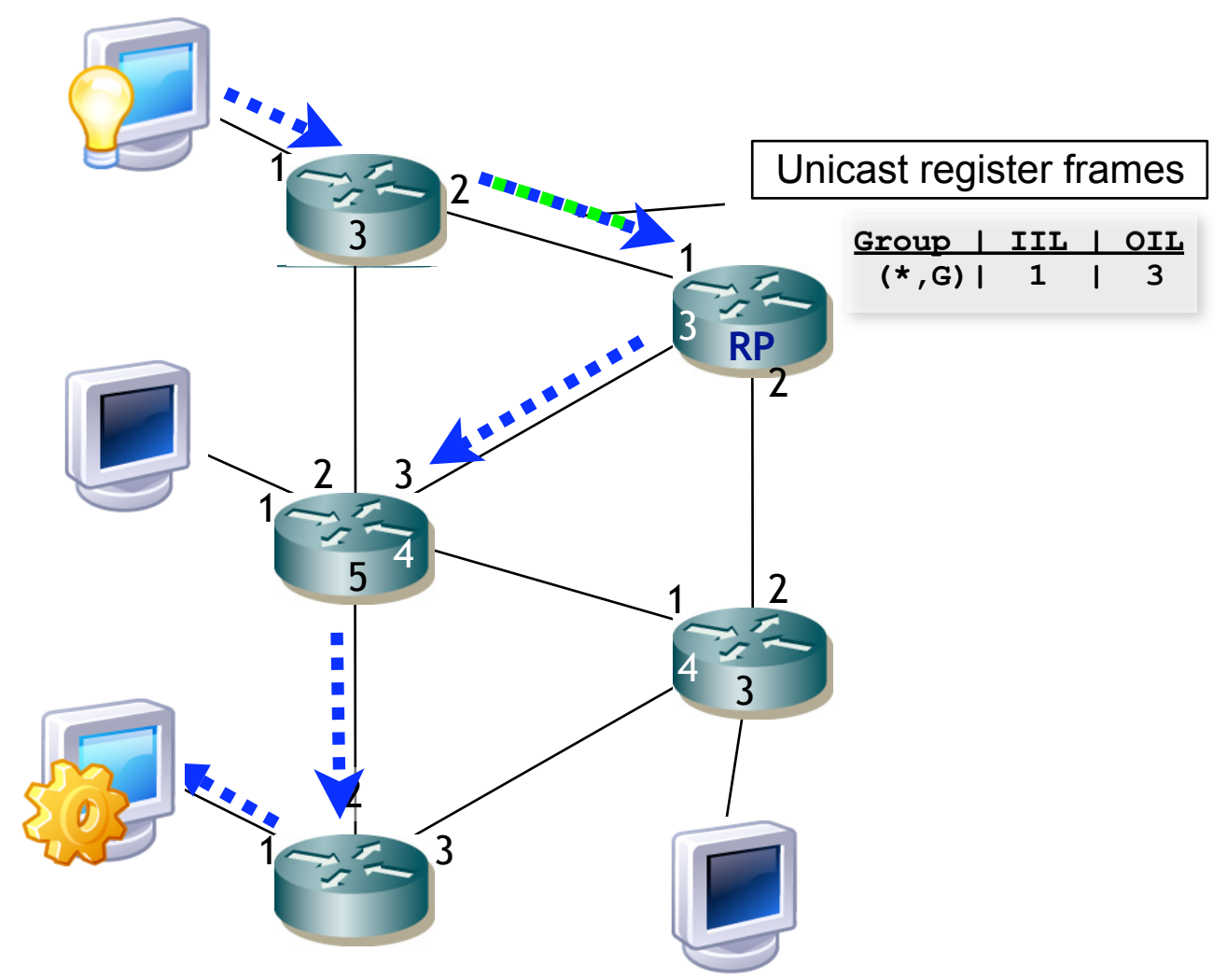
Router with numbered interfaces

Multicast more in details - ASM mode

Receiver side



Source side

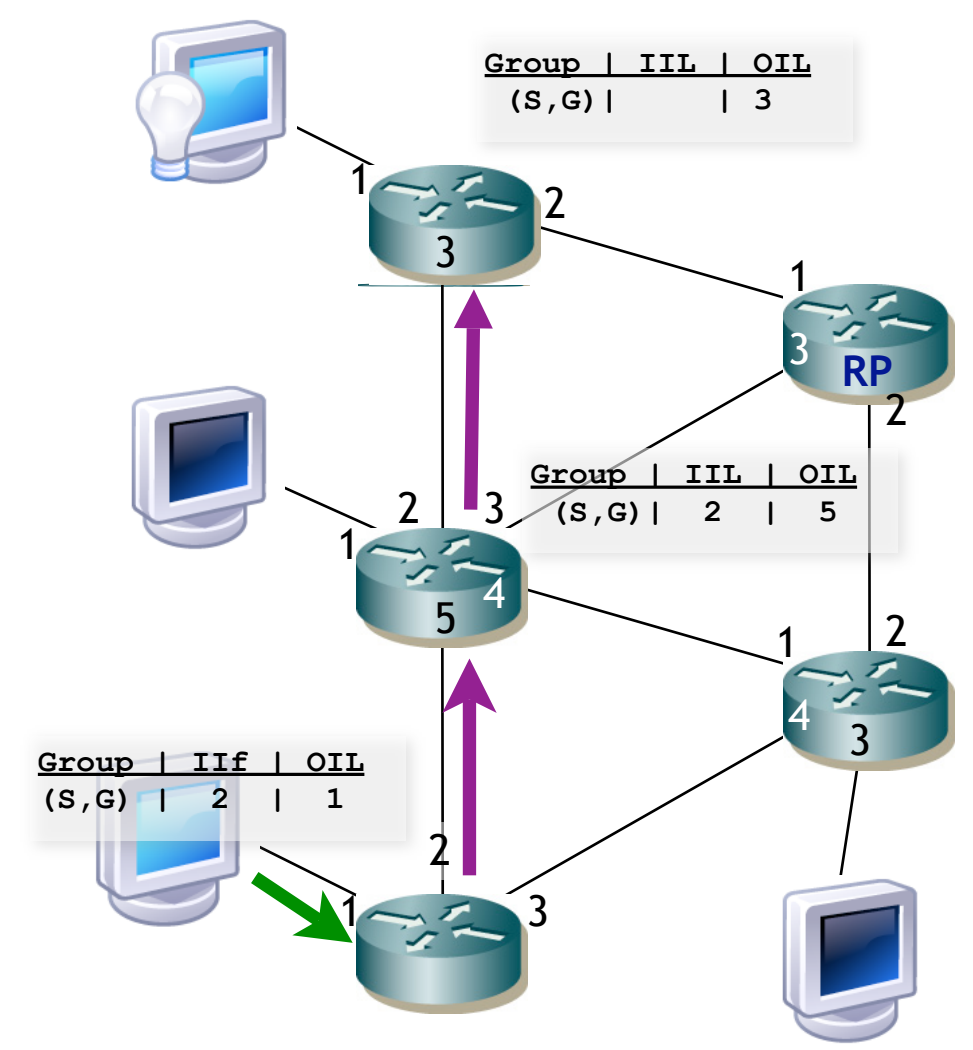


- IGMP Report
- PIM Join
- Multicast data

Router with numbered interfaces

Multicast more in details - SSM mode

Receiver side

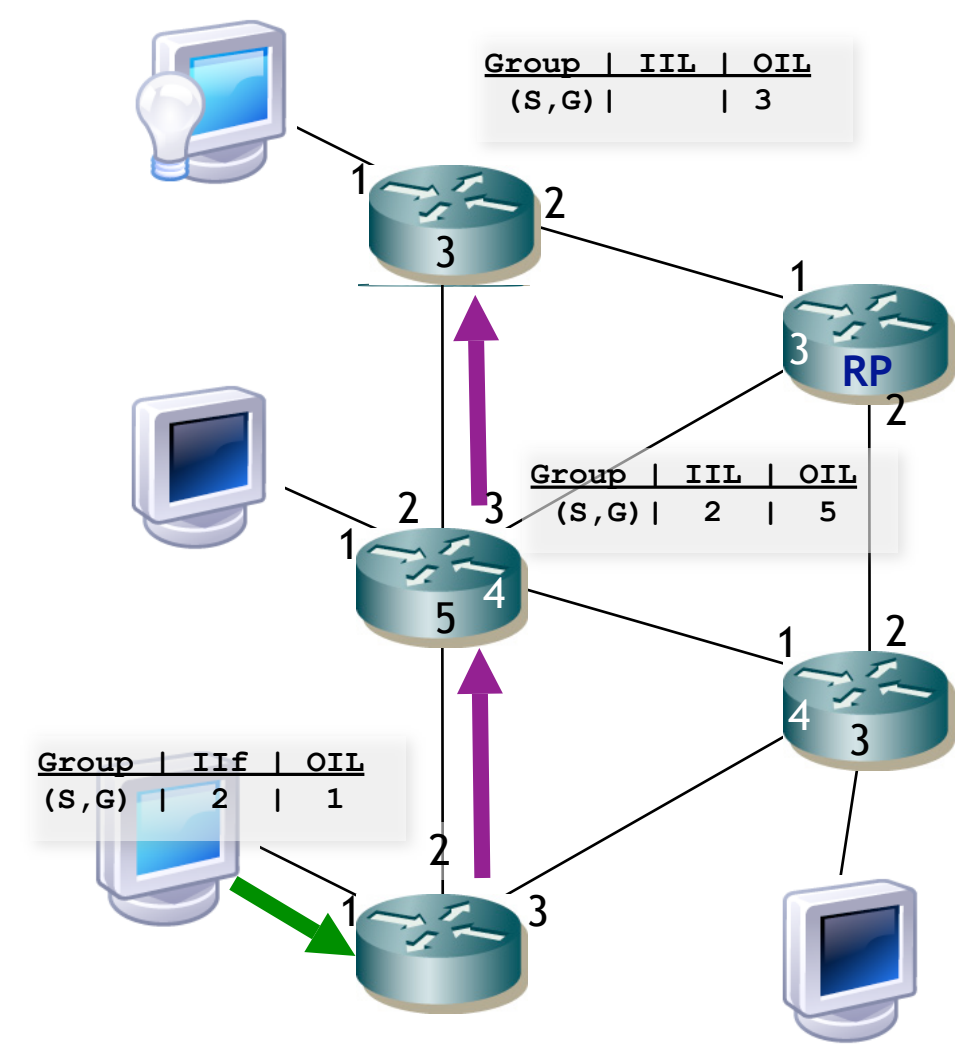


- IGMP Report
- PIM Join
- Multicast data

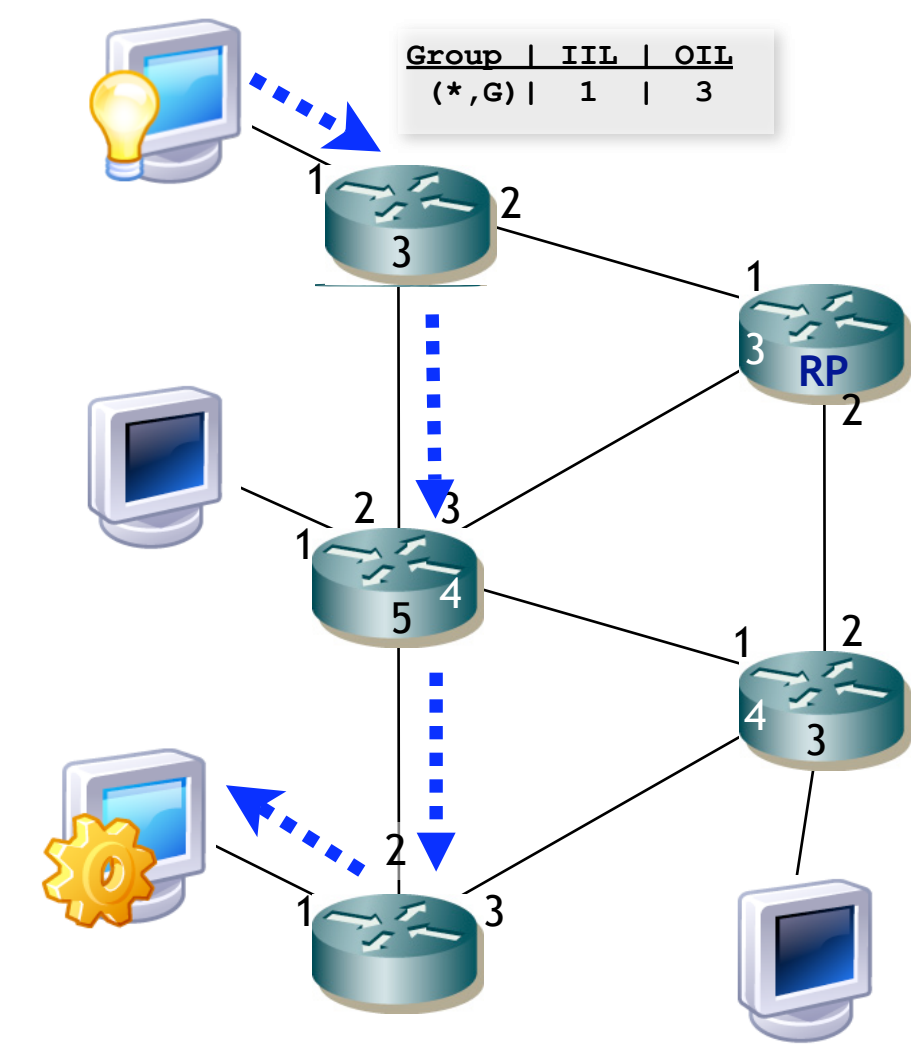
Router with numbered interfaces

Multicast more in details - SSM mode

Receiver side



Source side

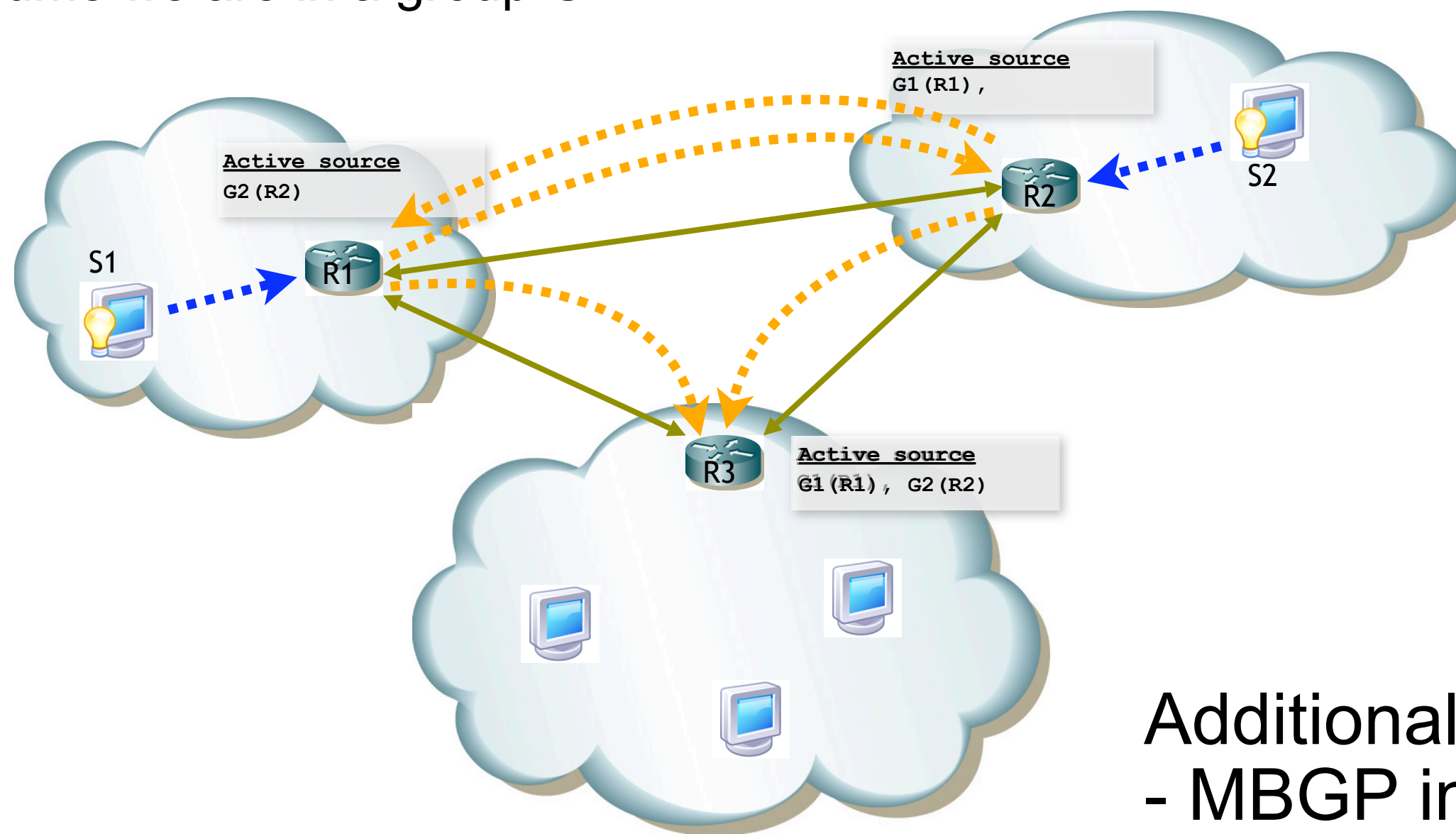


- IGMP Report
- PIM Join
- Multicast data

Router with numbered interfaces

Multicast more in details - ASM interdomain IPv4

Assume we are in a group G



Additional needed protocols
- MBGP informs of routes to join RP (if different from unicast ones)
- MSDP allows to know locally existence of external active sources

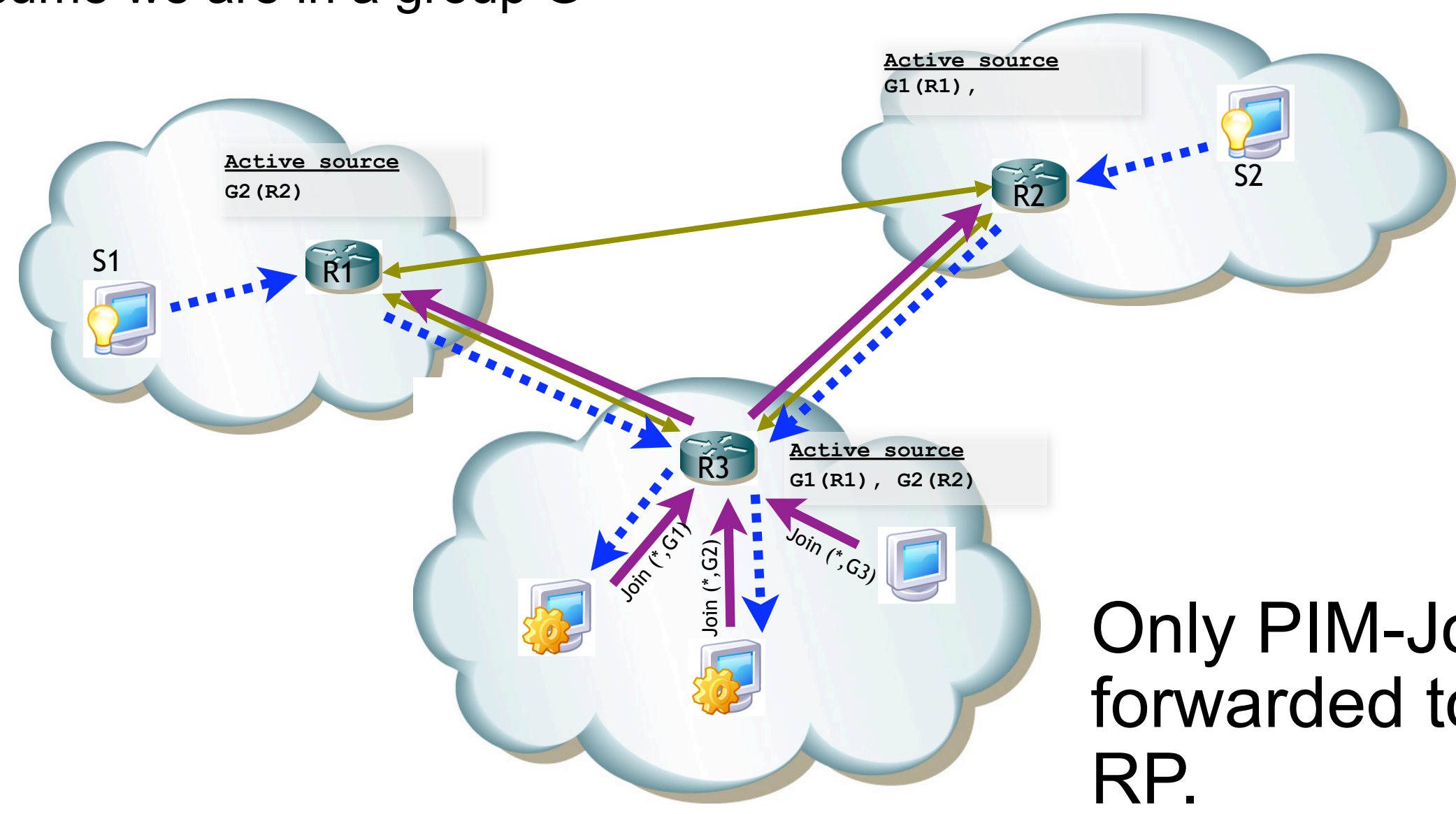
MSDP peering

- Active source announcement
- PIM Join
- Multicast data

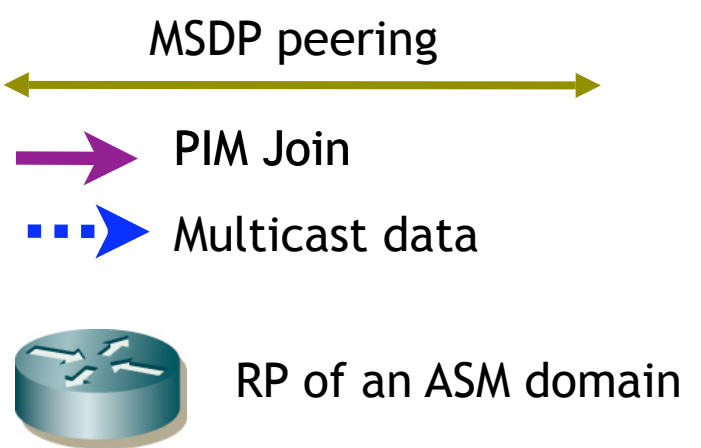
RP of an ASM domain

Multicast more in details - ASM interdomain IPv4

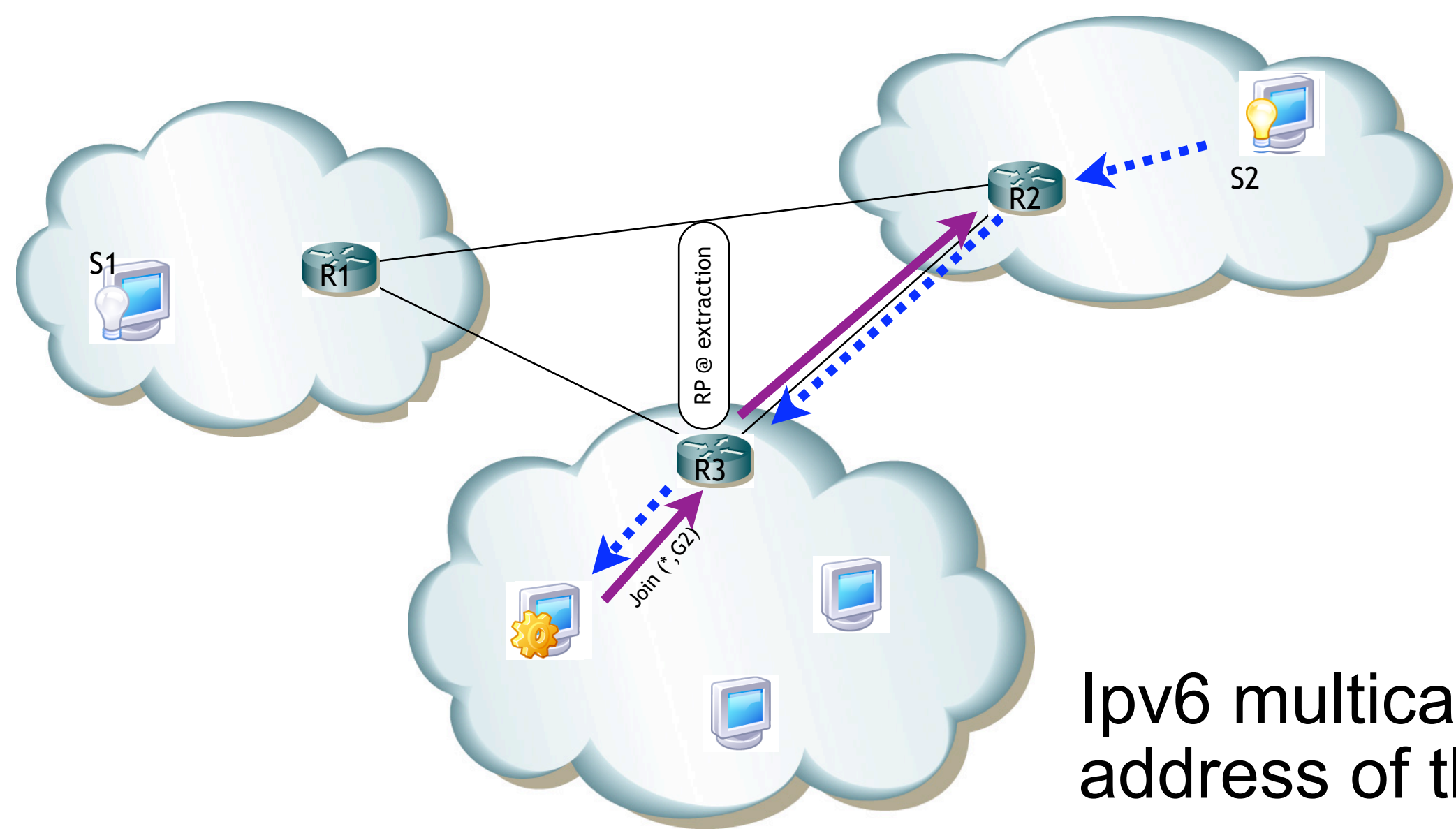
Assume we are in a group G



Only PIM-Join for active source are forwarded toward neighbor domain RP.



Multicast more in details - ASM interdomain Ipv6 or SSM



Ipv6 multicast address embeds the address of the RP for the group

No more additional mechanism is needed

Types of attacks against multicast - Data plane

How : by taking the control of hosts

Goal : create points of congestion by increasing traffic.

Launched from Senders

SSM : only S can send to a group,
distributed attack not powerful.

ASM : anybody can send to a group,
⇒ increases source traffic in the LAN,
⇒ generates a "register mechanism"
unicast attack which is limited to the
multicast domain,
⇒ generates signaling MSDP attack
which is easy to launch (randomly
groups addresses multicast packets
generation).

Launched from Receivers

ASM or SSM :

How ? Join a many as possible groups/
channels.

⇒ if groups are the same no efficiency
because goal of multicast !
⇒ could be efficient as a global attack
against, but difficult to launch because
of localization and flows availability.

- Most effective with IPv4 ASM in
interdomain (with MSDP).

+ Uses SSM or IPv6 ASM with Embedded
RP.

Types of attacks against multicast - Control plane

Goal : increases routers resources usage.

Launched from Senders

SSM : sender don't generate signalization.

ASM : ⇒ triggers MSDP announcement messages

⇒ may trigger PIM-Join(S,G) from RP or DR while switching from shared to source tree (data rate triggered).

- MSDP is very vulnerable (should no more be used).

+ RP must associate filtering policy.
At the internet level RP should be seen as a session level service.

Launched from Receivers

Receiver signalization (i.e. IGMP) stays local to LAN

⇒ this is a problem in attacks trace back.

⇒ can play as a fake PIM router sending PIM/Join

⇒ triggers PIM/Join/Prune messages (main issue related to DDoS attacks)

- PIM most vulnerability is at its control plane and with respect to PIM/Join signalization.

Generalities

Goal : increases routers resources usage.

General comments :

⇒ distributed PIM/Join to *different groups* is more efficient that to a *unique group*.

⇒ to act on the data plane knowledge on *many active groups* is needed.

How to build efficient attack ?

⇒ PIM/Join(S,G) with S in a targeted network,

⇒ PIM/Join(*,G) with the Embedded RP in the targeted network,

⇒ PIM/Join(*,G) toward local RP,

if no active source in the targeted group

useless branches to local RP,

else

interdomain branches.

Hosts reporting IGMP for several groups and thus generating PIM/Join messages is the best way to clutter up router resource usage.

Example

Assume that 120.000 channels (max. router multicast entries capacity) have been created, need of PIM/Join max size message can embed 73 channels (in 1494 bytes),

Signaling these channels every 60s needs 28 max sized messages/s and generates a 335Kb/s continuous traffic.

Action on routers

- ⇒ Can downgrade router global activity because PIM messages enter through the slow path to router CPU. Can result in a possible connectivity loss.
- ⇒ Can generate a multicast denial of service. If multicast allowed memory is used up new messages will be discarded.
- ⇒ Increasing memory consumption for multicast, specially if shared with unicast, can produce unicast capacities downgrading.

2000 compromised hosts each joining 60 channels (S_i, G_i) can create up to 120K multicast routing entries in a target network access router (if S_i are in the targeted network prefix).

Detection criterions

Legitimate PIM/Join is not distinguishable from malicious

Detection can only be based on *PIM/Join series*.

Implies observed values can only be *rates*.

RNJ - New entries (N) created by PIM/Join during period T

N/T can detect high rate attacks. If possible RNJ per interface RNJ_i

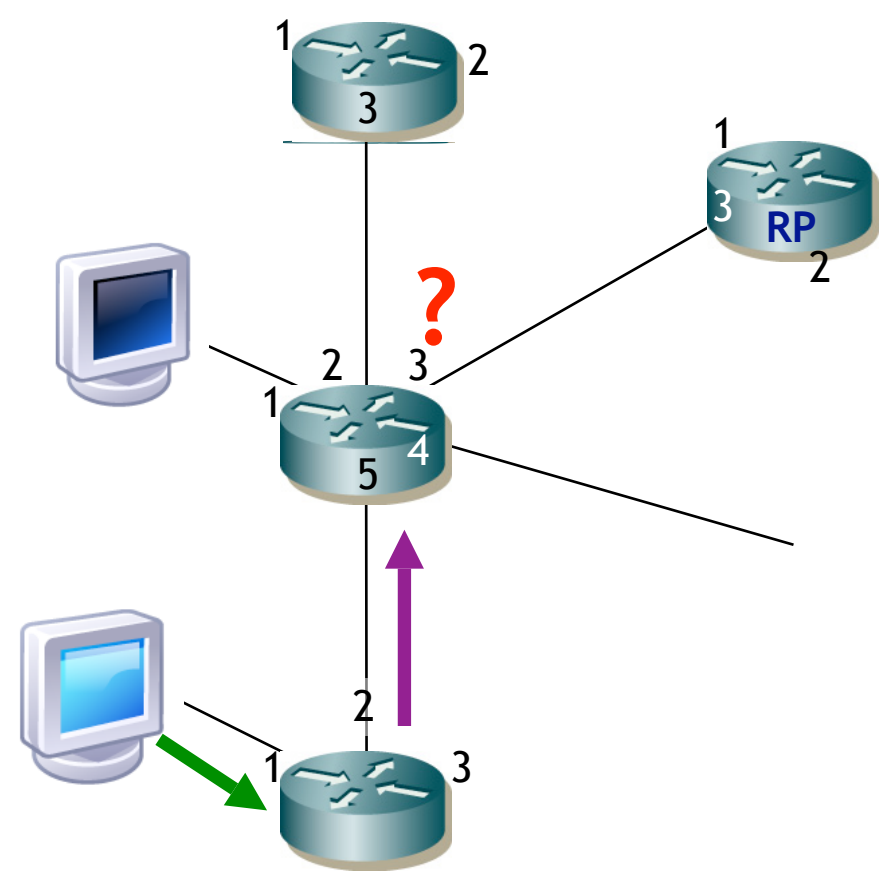
NME - Number of multicast entries

can preserve router from resource wasting

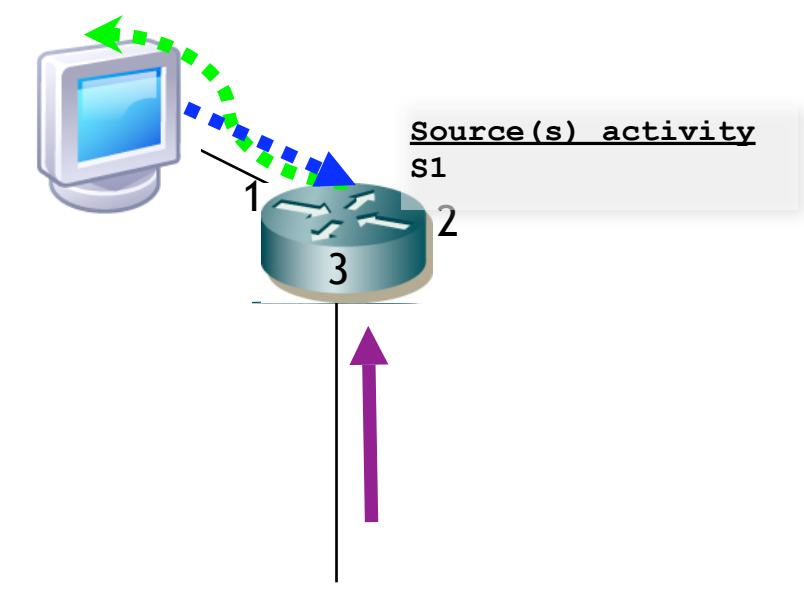
While using randomly generated PIM/Join(S,G) or PIM/Join(*,G) for attacks, many will be useless in terms of multicast data forwarding and could be malicious.

What is a useless tree branch

No route to S
(or RP for G).

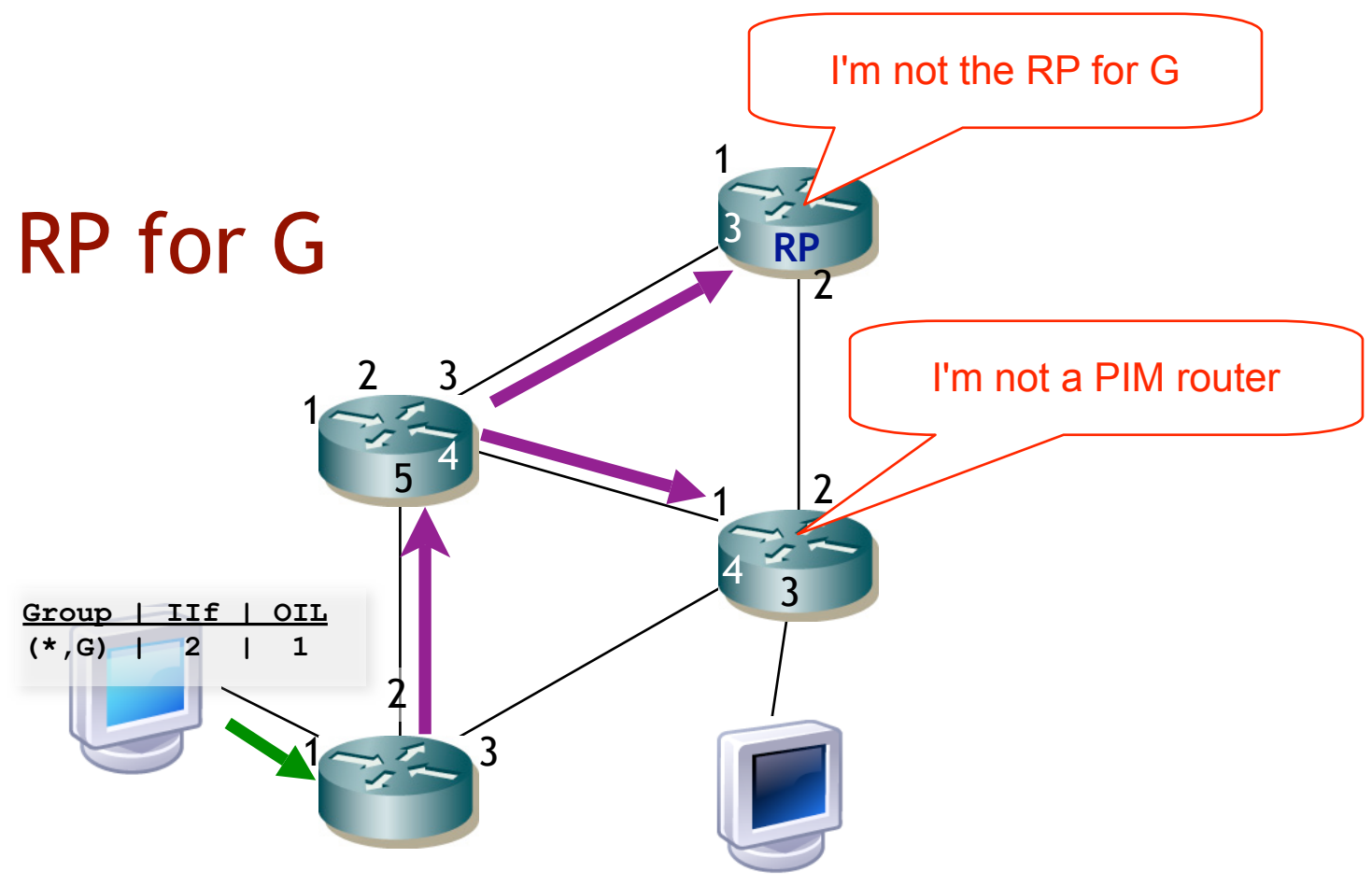


Source does not exist.
info could be available
by source **pinging**/
snooping in FHR.



Channel (S,G) does not exist while
S exist. S never sent to G.

No RP for G



S exist but is a silent source. Can
be a suspicious case.

Detection criterions

Legitimate PIM/Join is not distinguishable from malicious
Detection can only be based on PIM/Join *series*.
Implies observed values can only be *rates*.

RNJ - *New entries (N) created by PIM/Join during period T*
N/T can detect high rate attacks. If possible RNJ per interface RNJ_i

NME - *Number of multicast entries*
can preserve router from resource wasting

RUJ - Useless entries

Rate of entries that are marked as useless

NUJ - Number of useless entries

Helpful to detect slow growing of useless branches with a same target

Similar indicators are needed on LHR per host and per interface

RIR-H - Rate of IGMP reports per host or per Interface - **RIR-I**

NIR-H - Number of IGMP reports per host or per Intreface - **NIR-I**

Cost of the detection

Counters and associated thresholds.

Flags in the TIB (Tree Information Base) to mark trees as malicious

How to mitigate DDoS attack with these indicators

Better place to *detect* is FHR or RP (closer to target and because of concentration).

Better place to *counter* is LHR (closer to attackers).

Need to *trace back* toward attackers.

Source address of PIM/Join message is PIM neighbor router address.

We suggest to incorporate a *feedback mechanism* to PIM.

A feedback mechanism - The message

When a problem occurs, for example PIM/Join forwarding failure, a new PIM message, ***PIM/Tree-Unreachability*** (PIM/TU), is sent ***hop by hop*** in the builded tree part to inform about unavailability.

PIM/TU message contains information about;

- group address,
- source address (in SSM case),
- RP address (ASM case),
- error code,
- address of the detecting router.

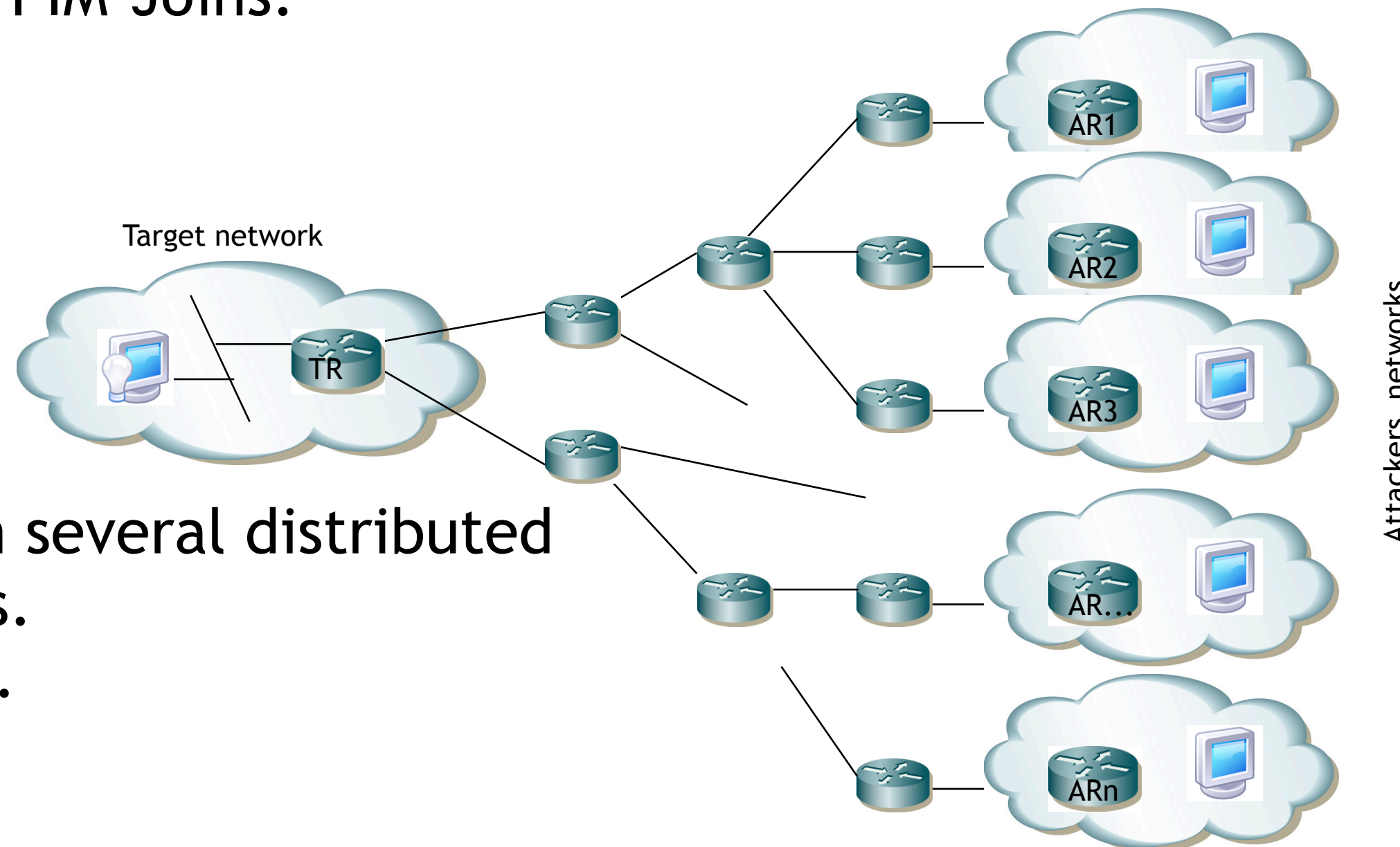
Unavailability information aggregation limit bandwidth consumption.

A feedback mechanism - How to use it

By caching unavailability information in LHR, PIM/TU message can avoid maintaining useless branches.

By generating specifically marked DDoS PIM/TU messages and cache this information in attackers LHR, it become possible to mitigate DDoS attacks by stopping attackers PIM-Joins.

Example



SSM mode.

Attack occurs from several distributed attackers networks.

Source stays silent.

DDoS attacks mitigation

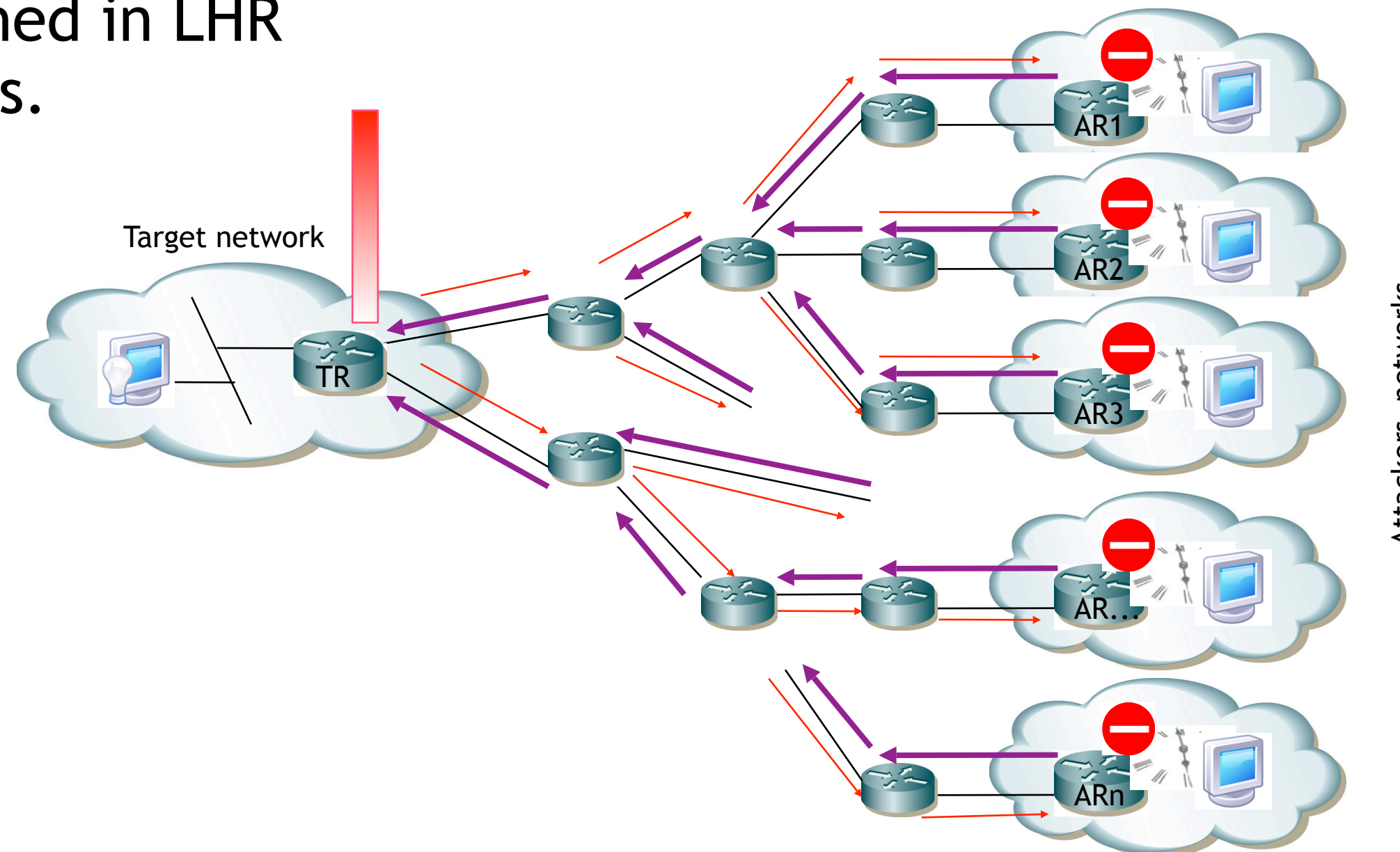
Detection - On TR router, PIM states increasing speeds up (RUJ) or their number rises up the set threshold (NUJ).

Note that PIM-Join are targeted to several TN sources and groups.

Downstream information - TR sends in builded tree parts PIM-TU message with DDoS flag set (*PIM-DDoS*).

Information is cached in LHR and block PIM-Joins.

Attack mitigated
Network resources are released and attackers blocked.



→ PIM Joins
→ PIM-DDoS

Conclusion and perspectives

Summary - DDoS attacks can mainly occur on multicast control plane, with PIM-Join and.

We present a framework which allows to detect DDoS attacks by counting multicast states and/or messages in routers.

To mitigate/block DDoS attack we propose to use a new PIM message, PIM-Tree Unreachability (PIM-TU) with addition of a specific DDoS flag.

Open issues

This framework is fine for a multicast domain, but some points are not solved at its borders :

- information about source activity,
- trusting DDoS information from neighbor domain

Technical information is then needed

- how long it is necessary to cache DDoS,
- how are the best values to or relationship between values of counts and rates to detect DDoS attack,
- what is the cost of this architecture.

Thank you for your attention

Do you have any questions