


# Redundant Router Issues with IP Multicast in Stub Networks



IP Multicast uses one router to be forward data onto a LAN in redundant topologies. If multiple routers have interfaces onto a LAN only one router will forward the data—there is no load balancing for multicast traffic on LANs. Depending on the topology there may not even be multicast routing state in the redundant routers.

Multicast traffic is always visible by every router on a LAN. This is also the case even if CGMP or IGMP Snooping are configured. The routers need to see the multicast traffic so that they can make a forwarding decision.

The redundant router (router not forwarding the multicast traffic stream) sees this data on the outbound interface for the LAN. The redundant router must drop this traffic because it has arrived on the wrong interface and therefore will fail the Reverse Path Forwarding (RPF) check. We call this traffic “non-RPF traffic” because it is being reflected backwards against the flow from the source.

The 6500 and 8500 multilayer switches with the right hardware can be configured to act as full-fledged routers. RPF traffic (multicast traffic flowing in the right direction) is forwarded in hardware by special ASICs in the switch. The ASICs are given information from the multicast routing state—(\*,G) and (S,G)—so that a hardware shortcut can be programmed. These hardware shortcuts allow the 6500/8500 routers to forward multicast traffic in the millions of packets per second instead of thousands of packets per seconds.

## The Problem

All Cisco routers may not handle non-RPF traffic for Sparse Mode groups efficiently in certain topologies. For non-RPF traffic, there is usually no (\*,G) or (S,G) state in the redundant router and therefore no hardware or software shortcuts can be created to drop the packet. Each multicast packet must be examined by the processor individually. This can cause the CPU on these routers to run very high.

## The Solution

On the 6500/8500 routers there is an access list engine that enables filtering to take place at wire rate. This feature can be used to handle non-RPF traffic for Sparse Mode groups efficiently.

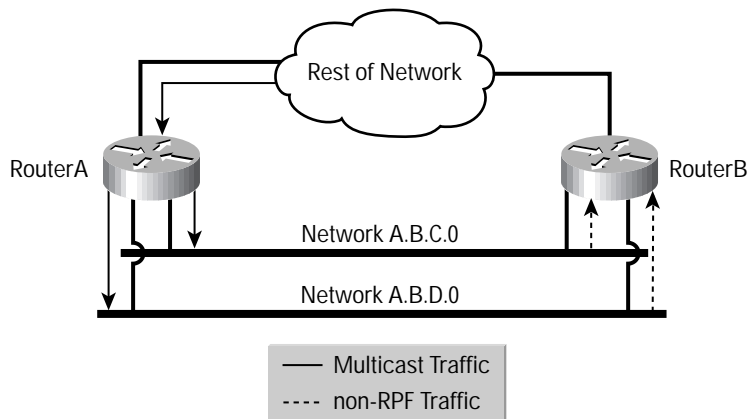
To implement this solution, we place an access list on the incoming interface of the 'stub network' to filter multicast traffic that did not originate from the 'stub network'. The access list is pushed down to the hardware in the switch. This access list prevents the CPU from ever seeing the packet and allows the hardware to drop the non-RPF traffic.

**Note:** Do not place this access list on a transit interface. It is only intended for stub networks (networks with hosts only).

Example

Assume that you have two routers with two VLANs in common. (expand this to as many VLANs as necessary)

Figure 1 Typical Redundant Network Topology



RouterA is HSRP primary for VLAN1, secondary for VLAN2. RouterB is secondary for VLAN1, and primary for VLAN2. It is recommended that you make either RouterA the Designated Router (give it a higher IP address), or pick RouterB, but make just one router the DR for all segments.

RouterA	VLAN1 Physical IP Address	A.B.C.3
RouterB	VLAN1 Physical IP Address	A.B.C.2
	VLAN1 HSRP Address	A.B.C.1
RouterA	VLAN2 Physical IP Address	A.B.D.3
RouterB	VLAN2 Physical IP Address	A.B.D.2
	VLAN2 HSRP Address	A.B.D.1

Place this access list on the non-DR router:

```
access-list 100 permit ip A.B.C.0 0.0.0.255 any
access-list 100 permit ip A.B.D.0 0.0.0.255 any
access-list 100 permit ip any 224.0.0.0 0.0.0.255
access-list 100 permit ip any 224.0.1.0 0.0.0.255
access-list 100 deny ip any 224.0.0.0 15.255.255.255
access-list 100 permit ip any any
```

Have one permit for each subnet the two routers share in common. Other permits are to allow Auto-RP and reserved groups to operate correctly.

Apply the ACLs to each VLAN interface on the non-DR with these additional commands:

```
ip access-group 100 in
no ip redirects
no ip unreachable
```

**Note:** You must be running at least Catalyst Software 5.4(2.5) for the ACLs to work in Hybrid configuration.

**Note:** The redundant router designs discussed in this document are Externally Redundant— there are two physical 6500 routers. Internal Redundancy, two Route Processors in one box, is not recommended with multicast.



Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

European Headquarters  
Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy Les Moulineaux  
Cedex 9  
France  
www.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco.com Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE  
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia  
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore  
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela