

# IP Multicast

## DOS Attack

11/10/00

[Click here to start](#)

### Table of Contents

Author: jan

[Title](#)

[Set-up](#)

[Users leave groups](#)

[Attack comes](#)

[Consequences](#)

[...and traffic-wise](#)

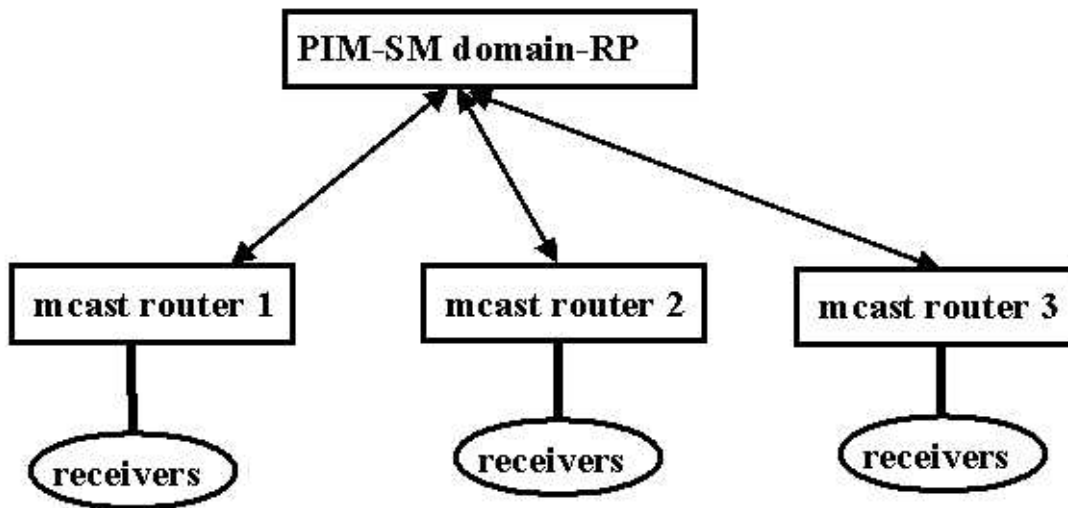
# An IP Multicast DOS attack

jan.novak@dante.org.uk

First Previous [Next](#) [Last](#) [Index](#) [Text](#)

Slide 1 of 6

**The beginning :**



[First](#) [Previous](#) [Next](#) [Last](#) [Index](#) [Text](#)

**Then:**

**Receivers leave the group**

**Cisco keeps the states with Oif=NULL**

```
(* , 224.2.246.13), 07:33:23/00:02:59, RP A.B.C.D, flags: SP
```

```
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.:
```

```
Int Limit 768 kbps
```

```
Outgoing interface list: Null
```

```
(128.223.83.26/32, 224.2.246.13), 00:00:36/00:02:23, flags: PT
```

```
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.:
```

```
Int Limit 768 kbps
```

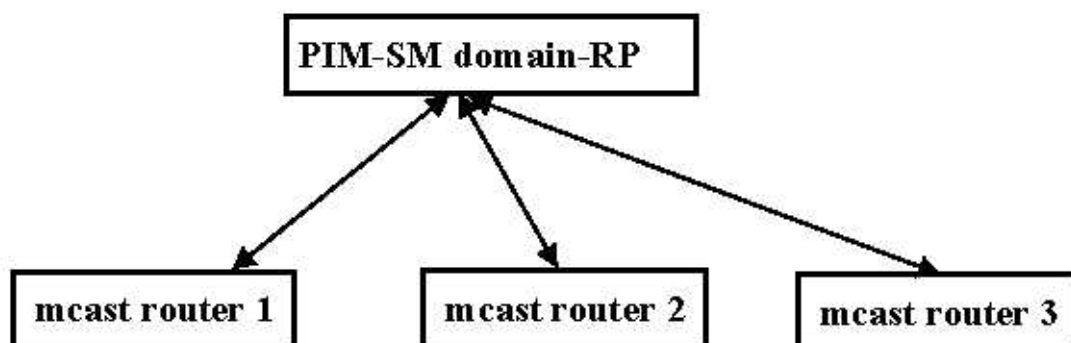
```
Outgoing interface list: Null
```

```
(130.243.65.35/32, 224.2.246.13), 00:02:46/00:00:13, flags: PT
```

```
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.:
```

```
Int Limit 768 kbps
```

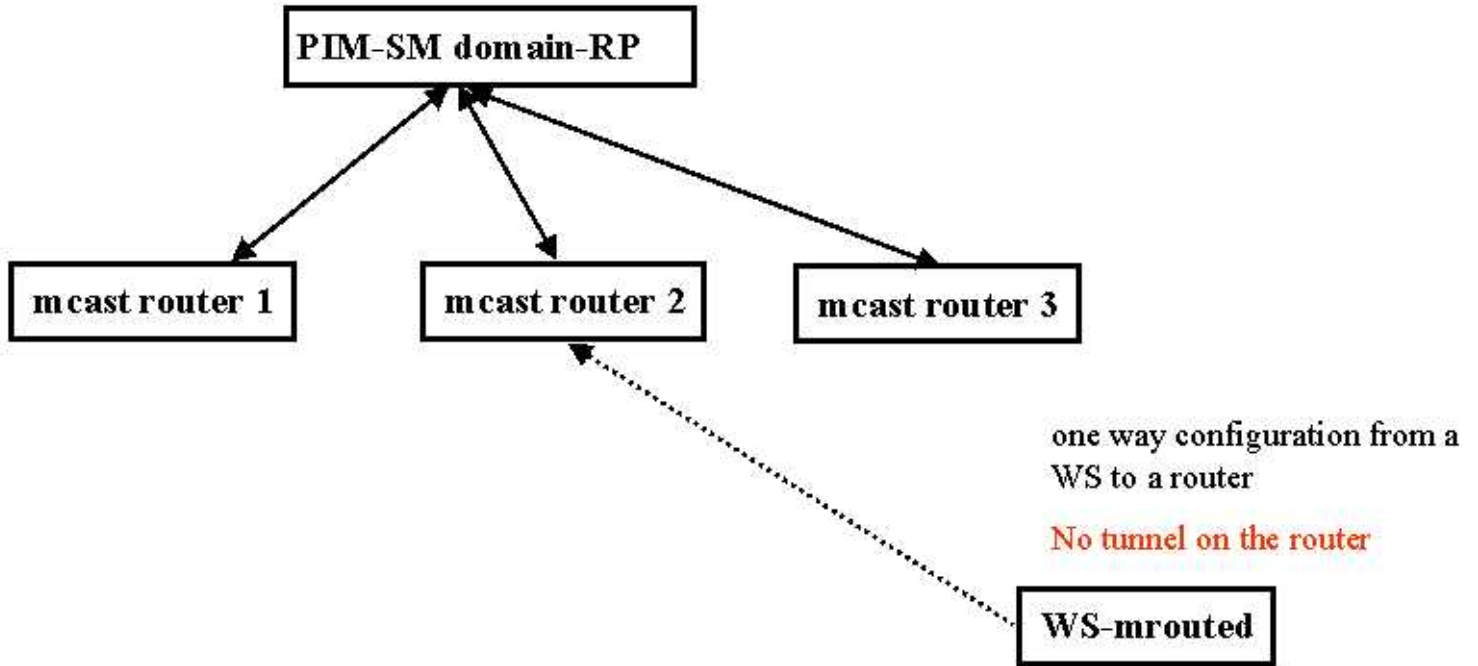
```
Outgoing interface list: Null
```



[First](#) [Previous](#) [Next](#) [Last](#) [Index](#) [Text](#)

**Then:**

**“Nasty” attack comes - some “left over” from old DVMRP tunnels ....**



**Then:**

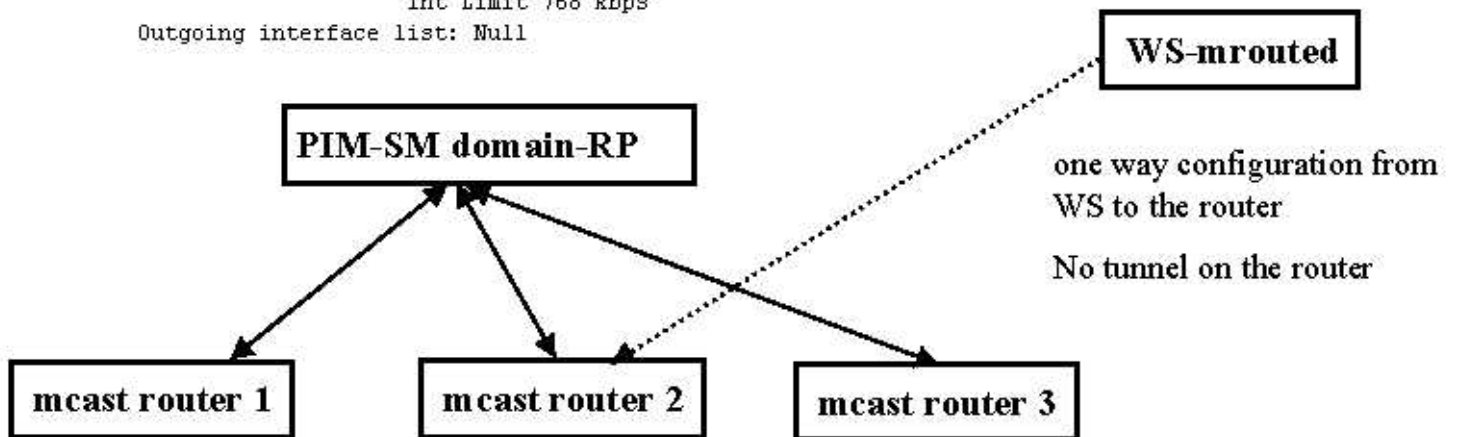
**Cisco sees DVMRP probes, sets C flag for interoperability and ..... starts to send**

**(\*G) joins because of locally connected receivers**

```
(*, 224.2.246.13), 07:29:03/00:02:59, RP A.B.C.D, flags: SJPC  
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.Z  
Int Limit 768 kbps  
Outgoing interface list: Null
```

```
(128.223.83.26/32, 224.2.246.13), 00:02:18/00:00:41, flags: PCT  
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.Z  
Int Limit 768 kbps  
Outgoing interface list: Null
```

```
(130.243.65.35/32, 224.2.246.13), 00:01:34/00:01:25, flags: PCT  
Incoming interface: ATM0/0.1, RPF nbr X.Y.W.Z  
Int Limit 768 kbps  
Outgoing interface list: Null
```



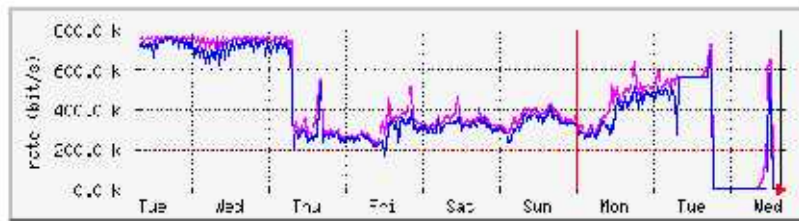
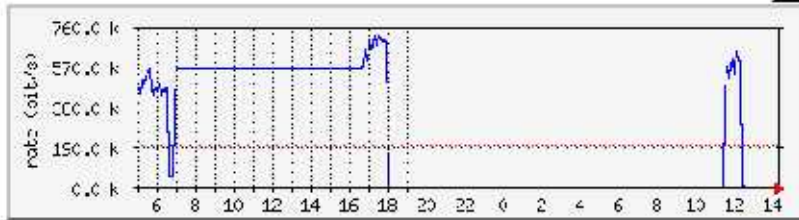
[First](#) [Previous](#) [Next](#) [Last](#) [Index](#) [Text](#)

**The result:**

**Traffic on the outgoing interface of RP towards a downstream router**

A DVMRP tunnel configured on a WS

about 2500 km from the router



**How to detect: “debug ip dvmrp detail”**

**How to prevent: “deny igmp from the host IP address”**