



# IPv4 Multicast on JANET

**Dave Price, Sandy Spence,  
Fred Long and Edel Sherratt**  
*University of Wales Aberystwyth*

**Technical Guide**



## UKERNA Technical Guides

UKERNA Technical Guides are a series of user guides available to JANET customers. Technical Guides contain detailed technical information and are intended for technical support staff at JANET sites, network specialists, or those with a particular interest in the specialist area.

If you have any queries or comments about the Guides or would like to obtain copies, please contact:

### JANET Customer Service

UKERNA	Tel: 0870 850 2212
Atlas Centre, Chilton, Didcot	Fax: 0870 850 2213
Oxfordshire, OX11 0QS	E-mail: <a href="mailto:service@janet.ac.uk">service@janet.ac.uk</a>

Further details of the documents in this series are available at:

**<http://www.ja.net/services/publications/technical-guides/>**



## Authors and Contributors

This first version of this document was authored by Dave Price and Sandy Spence of the Department of Computer Science, University of Wales, Aberystwyth. This updated version has been authored by Dave Price, Fred Long, Edel Sherratt and Sandy Spence, all of the Department of Computer Science, University of Wales, Aberystwyth.

The authors of the first version expressed their gratitude to Ashok Shawney, Henry Hughes and David Salmon of UKERNA and Jonathan Couzens, Tony Hacche and Duncan Rogerson of the JANET NOSC (Network Operations and Service Centre), for their various contributions, and their time spent reading and commenting on early drafts.

The authors of the present version record their thanks to Gorry Fairhurst (University of Aberdeen), Stig Venaas (Uninett, Norway and University of Southampton), Tim Chown (University of Southampton), Steve Williams (University of Swansea and UKERNA), Rob Evans (JANET NOSC), John Linn (University of Aberdeen), Jean-Marc Uze (Juniper Networks) and Rina Samani (UKERNA) for feedback on the first version, extensive comments on early drafts of the present version, and other valuable comments which together have inspired the changes now present in this document.

The authors also wish to thank various people, too numerous to mention by name, from several JANET sites and connected Regional Networks who have contributed facts and participated in e-mail and personal discussions on topics covered by this document.



# Contents

<b>1</b>	<b>Introduction to Multicast Connectivity on JANET .....</b>	<b>9</b>
1.1	Intended Audience .....	9
1.2	This Updated Technical Guide .....	9
1.3	Overview .....	9
1.4	The History of IP Multicast and its Transmission on JANET .....	10
1.5	Non-IP Multicast .....	10
1.6	References .....	11
<b>2</b>	<b>An Introduction to IP Multicast .....</b>	<b>12</b>
2.1	<b>Multicast – What Is it? .....</b>	<b>12</b>
2.1.1	Network Costs .....	12
2.2	<b>Multicast Service Models – ASM v SSM.....</b>	<b>13</b>
2.3	<b>Multicast Address Space.....</b>	<b>14</b>
2.3.1	Multicast Address Allocation .....	14
2.3.2	IPv4 Local Network Control Address Block: 224.0.0.0–224.0.0.255.....	14
2.3.3	Internetwork Control Block: 224.0.1.0–224.0.1.255 .....	15
2.3.4	ADHOC Block: 224.0.2.0–224.0.255.0.....	15
2.3.5	RFC1190: 224.1.0.0–224.1.255.255 .....	15
2.3.6	SDP/SAP Block: 224.2.0.0–224.2.255.255 .....	15
2.3.7	Various/Reserved: 224.3.0.0–231.255.255.255 .....	16
2.3.8	Source Specific Multicast: 232.0.0.0–232.255.255.255 .....	16
2.3.9	GLOP Block: 233.0.0.0–233.251.255.255.....	16
2.3.10	EGLOP Block: 233.252.0.0–233.255.255.255 .....	16
2.3.11	Reserved: 234.0.0.0–238.255.255.255 .....	17
2.3.12	Administratively Scoped Addresses: 239.0.0.0–239.255.255.255.....	17
2.4	<b>Multicast Packet Forwarding .....</b>	<b>18</b>
2.4.1	Multicast Routing Protocols .....	18
2.4.2	Reverse Path Forwarding (RPF) .....	18
2.5	<b>Multicast Traffic Reception – the Single LAN View.....</b>	<b>19</b>
2.5.1	Receiving Multicast Traffic.....	19
2.5.2	IGMP – the Host View .....	20
2.5.3	IGMP – the Router View .....	21
2.6	<b>Multicast Traffic Transmission.....</b>	<b>21</b>
2.6.1	Multicast Sources .....	21
2.6.2	Generation of Multicast Traffic.....	21
2.7	<b>Single Domain Multicast Routing and PIM-SM.....</b>	<b>22</b>
2.7.1	Distribution Trees and Rendezvous Points.....	22
2.7.2	Stage 1: Building the RPT – from Receiver to RP.....	23
2.7.3	Stage 2: Building the Distribution Tree – from Source to RP... ..	23
2.7.4	Stage 3: Building the Shortest Path Tree – from Source to Host .....	24
2.7.5	Other Scenarios.....	25
2.8	<b>Intra-Domain Multicast Routing.....</b>	<b>26</b>
2.8.1	Multicast Source Discovery Protocol (MSDP) .....	26

---

2.8.2	Multiprotocol Extensions for BGP-4 (MBGP) and the RPF Routing MRIB .....	27
<b>2.9</b>	<b>Source Specific Multicast (SSM) .....</b>	<b>27</b>
2.9.1	SSM Specifications and Documentation .....	27
2.9.2	SSM Terminology .....	28
2.9.3	SSM-Related Host and Application Requirements .....	28
2.9.4	SSM-Related Router Requirements .....	28
2.9.5	SSM and Rendezvous Point Behaviour .....	28
2.9.6	Selecting Addresses Within 232.0.0.0/8 .....	29
2.9.7	Delivery of SSM Between Multiple Domains .....	29
<b>2.10</b>	<b>Multicast in an MPLS Environment .....</b>	<b>29</b>
<b>3</b>	<b>Multicast Security, Vulnerabilities and Related Issues .....</b>	<b>30</b>
<b>3.1</b>	<b>Firewalls, Network Address Translation and IP Multicast.....</b>	<b>30</b>
3.1.1	Firewall Support.....	30
3.1.2	Security Risks from IP Multicast Traffic .....	30
3.1.3	NAT and Private IP Addresses .....	30
3.1.4	IP Packet Filtering at Firewalls .....	30
<b>4</b>	<b>The JANET Multicast Architecture .....</b>	<b>32</b>
<b>4.1</b>	<b>Connecting a Regional Network to the Backbone .....</b>	<b>32</b>
4.1.1	Single RP Within the Regional Network Adjacent to the BAR .	32
4.1.2	Single RP Within the Regional Network Distant from the BAR	32
4.1.3	RP on a Stick.....	32
4.1.4	Resilient RPs within the Regional Network .....	33
<b>4.2</b>	<b>Multicast Connectivity from JANET to External Networks .....</b>	<b>33</b>
<b>4.3</b>	<b>Use of Multicast Addresses within JANET .....</b>	<b>33</b>
4.3.1	Use of Administratively Scoped Addresses within JANET.....	33
4.3.2	Use of GLOP Addresses within JANET .....	34
<b>4.4</b>	<b>Use of SSM within JANET .....</b>	<b>34</b>
<b>4.5</b>	<b>Connection of Regional Networks that Cannot Meet the Above Specifications .....</b>	<b>34</b>
<b>5</b>	<b>Suggestions for How Regional Networks Might Carry Multicast IP Packets.....</b>	<b>35</b>
<b>5.1</b>	<b>Use of PIM-SM .....</b>	<b>35</b>
<b>5.2</b>	<b>Other Approaches .....</b>	<b>35</b>
<b>5.3</b>	<b>Serving the Site Networks.....</b>	<b>35</b>
<b>6</b>	<b>Issues for Site Networks .....</b>	<b>36</b>
<b>6.1</b>	<b>Routed versus Switched versus Repeated LANS .....</b>	<b>36</b>
6.1.1	Co-axial Cable-based Ethernets.....	36
6.1.2	Twisted Pair Cable Ethernets .....	36
6.1.3	Translating IPv4 Multicast Addresses to Ethernet Group Addresses.....	36
<b>6.2</b>	<b>Multicast on Repeated Ethernets .....</b>	<b>37</b>
<b>6.3</b>	<b>Multicast on Bridged or Switched Ethernets.....</b>	<b>37</b>
6.3.1	Control via Filter Tables .....	37
6.3.2	Control via IGMP Snooping .....	38
6.3.3	Switches Act as IGMP Queriers (IGMP Proxies).....	38



6.3.4	Control via CGMP.....	38
6.3.5	Other Approaches to Control.....	39
<b>6.4</b>	<b>Multicast on Wireless LANs .....</b>	<b>39</b>
<b>6.5</b>	<b>IP Level Issues .....</b>	<b>39</b>
6.5.1	Rendezvous Point Selection.....	39
6.5.2	Site Non-RP IP Router Configuration.....	40
<b>6.6</b>	<b>LAN Deployment Considerations .....</b>	<b>40</b>
<b>6.7</b>	<b>Miscellaneous Issues .....</b>	<b>40</b>
<b>7</b>	<b>Management and Monitoring of IP Multicast.....</b>	<b>41</b>
<b>7.1</b>	<b>Multicast Beacons.....</b>	<b>41</b>
7.1.1	The NLANR Beacon Software.....	41
7.1.2	The JANET Beacon Service.....	41
<b>7.2</b>	<b>SSMPING / ASPING .....</b>	<b>41</b>
<b>7.3</b>	<b>Multicast Detective.....</b>	<b>41</b>
<b>7.4</b>	<b>Other Approaches to Monitoring.....</b>	<b>42</b>
7.4.1	Simple Network Management Protocol (SNMP).....	42
7.4.2	Mtrace.....	42
<b>7.5</b>	<b>Multicast IP Interaction with Unicast IP .....</b>	<b>42</b>
<b>7.6</b>	<b>The JANET Looking Glass .....</b>	<b>42</b>
<b>8</b>	<b>Multicast Applications .....</b>	<b>43</b>
<b>8.1</b>	<b>Multicast Videoconferencing .....</b>	<b>43</b>
<b>8.2</b>	<b>Access Grid .....</b>	<b>43</b>
<b>8.3</b>	<b>Multicast Newsfeeds and other Live Streaming Servers .....</b>	<b>43</b>
<b>8.4</b>	<b>Multicast Access to On-demand Servers .....</b>	<b>44</b>
<b>8.5</b>	<b>Non-media Applications .....</b>	<b>44</b>
<b>8.6</b>	<b>Information Dissemination.....</b>	<b>44</b>
<b>8.7</b>	<b>Infrastructure Applications .....</b>	<b>45</b>
<b>8.8</b>	<b>Multicast File Transfer .....</b>	<b>45</b>
<b>8.9</b>	<b>Service Location Protocol.....</b>	<b>45</b>
<b>8.10</b>	<b>Summary.....</b>	<b>45</b>
<b>9</b>	<b>Further Information/Getting Help .....</b>	<b>46</b>
<b>9.1</b>	<b>Regional Network Connection Procedure and Support.....</b>	<b>46</b>
<b>9.2</b>	<b>Operational Queries and Fault Reporting.....</b>	<b>46</b>
<b>9.3</b>	<b>Customer Site Network Connection Procedure and Support.....</b>	<b>46</b>
<b>9.4</b>	<b>Queries Related to the Use of Video over Multicast.....</b>	<b>46</b>
<b>Appendix A: Configuration Examples.....</b>		<b>47</b>
<b>A.1</b>	<b>Example Configurations.....</b>	<b>47</b>
<b>A.2</b>	<b>Some Cisco® Based Examples .....</b>	<b>47</b>
A.2.1	Simple Non-RP Router Configuration.....	47
A.2.2	Simple Non-RP Router Configuration with Local Multicast Groups.....	48
A.2.3	Adding Support for SSM.....	48
A.2.4	Simple RP Router Configuration .....	49
A.2.5	Making Sure Multicast RPF Checks Work Correctly .....	50
A.2.6	Establishing Scoped Boundaries.....	51

A.2.7	Configuring Boundary Routers .....	51
A.2.8	Cisco® Performance Enhancements .....	52
<b>A.3</b>	<b>Multicast on Juniper Networks J-, M- and T-Series Routers.....</b>	<b>52</b>
A.3.1	Multicast Support on J-, M- and T-Series Routers.....	52
A.3.2	Configuring PIM Sparse Mode .....	53
A.3.3	Configuring Source-Specific Multicast.....	54
A.3.4	Configuring PIM Join Filters .....	55
A.3.5	Multicast Boundaries .....	56
A.3.6	Configuring MSDP.....	57
A.3.7	References .....	58
<b>A.4</b>	<b>The XORP Public Domain Multicast Router .....</b>	<b>58</b>
<b>Appendix B: Translating IP Multicast Addresses to Ethernet Group Addresses.....</b>		<b>64</b>
<b>Appendix C: Multicast Security .....</b>		<b>65</b>
<b>C.1</b>	<b>Multicast Security as Reported in the Literature .....</b>	<b>65</b>
<b>C.2</b>	<b>Multicast Security Searches .....</b>	<b>65</b>
C.2.1	<a href="http://www.kb.cert.org/vuls">http://www.kb.cert.org/vuls</a> .....	65
C.2.2	<a href="http://www.cert.org/nav/index_red.html">http://www.cert.org/nav/index_red.html</a> .....	66
C.2.3	Google search for 'multicast vulnerabilities'.....	68
<b>Appendix D: Bibliography .....</b>		<b>69</b>
<b>D.1</b>	<b>Books and Journals.....</b>	<b>69</b>
<b>D.2</b>	<b>Internet RFCs.....</b>	<b>69</b>
D.2.1	Internet RFCs of interest and relevance to readers.....	69
D.2.2	Internet RFCs of less interest and relevance to readers .....	71
<b>D.3</b>	<b>Internet Drafts – Work in Progress.....</b>	<b>72</b>
D.3.1	The IETF MBONED Working Group.....	72
D.3.2	The IETF PIM Working Group .....	72
D.3.3	The IETF SSM Working Group.....	73
D.3.4	The IETF MAGMA Working Group .....	73
D.3.5	The IETF MPLS Working Group.....	73
D.3.6	The IETF L3vpn Working Group.....	73
D.3.7	Other Internet Drafts .....	74
<b>D.4</b>	<b>Conference Papers .....</b>	<b>74</b>
<b>D.5</b>	<b>Web Sites and Miscellaneous .....</b>	<b>74</b>
<b>Appendix E: Glossary.....</b>		<b>76</b>
<b>Index</b>	.....	<b>80</b>

# 1 Introduction to Multicast Connectivity on JANET

## 1.1 Intended Audience

This guide assumes a good knowledge of the unicast Internet Protocol (IP) normally referred to as IPv4. The guide also assumes some knowledge of network planning and configuration issues. This is a highly technical subject and the guide is inevitably very acronym heavy. Readers are recommended to use the Glossary provided in Appendix E.

The guide provides technical guidance to the administrators within Regional Networks and end sites whose responsibility it is to manage multicast and make it available as a service within their domain. The current method of connection to the JANET IPv4 multicast service has been used since 2002. Administrators of Regional Networks need to connect their networks using the information provided in this document and referenced websites in order to gain access to external multicast services.

Site administrators will find this document useful, but they will also need to consult their Regional Network Operator for further information.

Another new document, currently being produced, will address the use and role of IPv6 Multicast on JANET.

## 1.2 This Updated Technical Guide

This updated version of the IP Multicast on JANET Technical Guide has been produced at the start of 2006 to reflect progress and changes with regard to the specifications of protocols used to support the IPv4 multicast service. It also reflects changes to the JANET infrastructure where these have some impact on users of multicast traffic.

## 1.3 Overview

JANET has a long established history of close collaboration between designers of network equipment and developers of network applications. This collaborative work is especially supportive in the development of tools that enable geographically dispersed groups, particularly in the areas of research and in more recent years the area of distance (remote) teaching, to communicate and share data. The development of networks and applications supporting remote collaboration, such as the Access Grid and H.323 Videoconferencing, has gathered pace in recent years. The increase in pace has been further encouraged by the availability of relatively low cost hardware. It is now not uncommon to purchase an off-the-shelf desktop PC that comes with support for multimedia communication as a standard. In the early days the use of such tools, expensive in themselves, would have required dedicated and often prohibitively expensive WAN (Wide Area Network) links.

The advances in communications technology, in particular over IP networks, have provided a reliable and effective method for delivering data with high multimedia content. The rate at which users are participating in multimedia communication indicates that demands made by bandwidth intensive products are catching up with the progressive improvements in bandwidth supply. It is no longer practical, nor financially viable, just to throw resources into improving bandwidth technology; new and more effective ways of delivering multimedia data must be sought in order to meet future demands. One of the biggest moves is in IP Multicast.

In addition, IP Multicast has a very important role in other areas, such as the distribution of standard time information, multicast software distribution and the distribution of real time financial data.

This document is not intended to be a fully self-contained technical description of all aspects of IP Multicast, but it does provide a substantial introduction to the topic. References are included to technical books and specifications where appropriate. In addition, recommendations of very comprehensive introductory texts are given in section 1.6. A full bibliography, including all references made in this guide, is given in Appendix D.

## 1.4 The History of IP Multicast and its Transmission on JANET

IP Multicast is not new. The term ‘multicast’ has been used for well over 20 years. Steve Deering and his then professor, Dave Cheriton of Stanford University, produced the first major Internet Engineering Task Force (IETF) Request for Comment (RFC) document relating to multicast [RFC966]. Dave Price, one of the co-authors of this Technical Guide, was actively involved in various early UK projects deploying and evaluating IP Multicast, including the Multi-media Integrated Conferences for Europe (MICE) National Support Centre (MICE-NSC), Video over IP (VIP) and Networked Expertise, Advice and Tuition (NEAT) Projects.

JANET has, as previously stated, always played an active part in promoting the use of multicast applications. In 1992 the experimental MBONE (Multicast Backbone) was established, running until late 1993 when the JANET IP Service MBONE Pilot superseded it.

This was later replaced with the JANET MBONE Service in February 1996 which has been running ever since. As with most things technological, the JANET Multicast Service has evolved to match technical progress and become more efficient. A more up-to-date connection method for Regional Networks was introduced in 2002 to take full advantage of the advances made to multicast, its associated protocols and their implementation in routers.

The aim of this document is to give assistance to those responsible for enabling their networks for the flow of multicast traffic. The contents of this document are presented in a structured manner to provide a best practice approach to the control and routing of multicast traffic to and within a network. The current required protocols and management thereof are described.

The original system employed on a UK wide basis for the movement of multicast packets between Regional Networks connected to JANET was via the JANET MBONE. Distance Vector Multicast Routing Protocol (DVMRP) [RFC1075] tunnelling was needed to link together multicast enabled networks that communicated multicast traffic via the then non-multicast JANET backbone. This approach is now deprecated.

Multicast is supported natively in today’s Internet backbones and JANET now carries multicast in this native manner. Sites that use DVMRP are no longer permitted to connect to the JANET backbone.

## 1.5 Non-IP Multicast

Finally, it should also be noted that protocols other than IP include the concept of multicast; this document only covers issues related to IP Multicast. Indeed, this entire document is focused on IPv4 Multicast.

## 1.6 References

This document supersedes the earlier document [BROWN1998] that provided much useful information to the authors.

The authors would also like to strongly recommend readers to [EDWARDS].


Readers using products from Cisco® should also be aware of [WILLIAMSON], which provides good technical background. A second useful source of information from Cisco Press is [ADAMS]. This second Cisco® book presents a range of typical complex network scenarios and appropriate configurations of devices and protocols to achieve both interdomain and intradomain multicast routing. Both of these books will prove useful for readers using products from other manufacturers.

## 2 An Introduction to IP Multicast

### 2.1 Multicast – What Is It?

The term ‘multicast’ refers to the sending of data from one to many or many to many registered recipients. This contrasts with broadcast, which floods a network with data that all hosts receive whether they want it or not, and is likely to have a very high proportion of redundant data. These methods can be summarised as follows:

- Unicast – provides for a single source to a single recipient one to one. (Figure 1)
- Broadcast – delivers to all, much like the unsolicited mail shots that pile up on your doormat, one to all. (Figure 2)
- Multicast – delivers only to those that have expressed an interest, one to many. (Figure 3)

Note: In the figures in this guide, the symbol  refers to the network routers.

#### 2.1.1 Network Costs

These three methods each have an impact on the networks carrying the multicast traffic:

- Unicast: each duplicate request results in the source producing duplicate packets. The network also has the added overhead of transferring multiple copies to the requesting clients.
- Broadcast: the source only has to produce one copy; the network has to provide the resources to duplicate the data at each branch.
- Multicast: the source only produces one copy, only interested parties receive the data and the network is still responsible for replicating the data, but replication is restricted to hosts connected to links that have explicitly requested the data. Links that do not have interested parties do not carry the data.

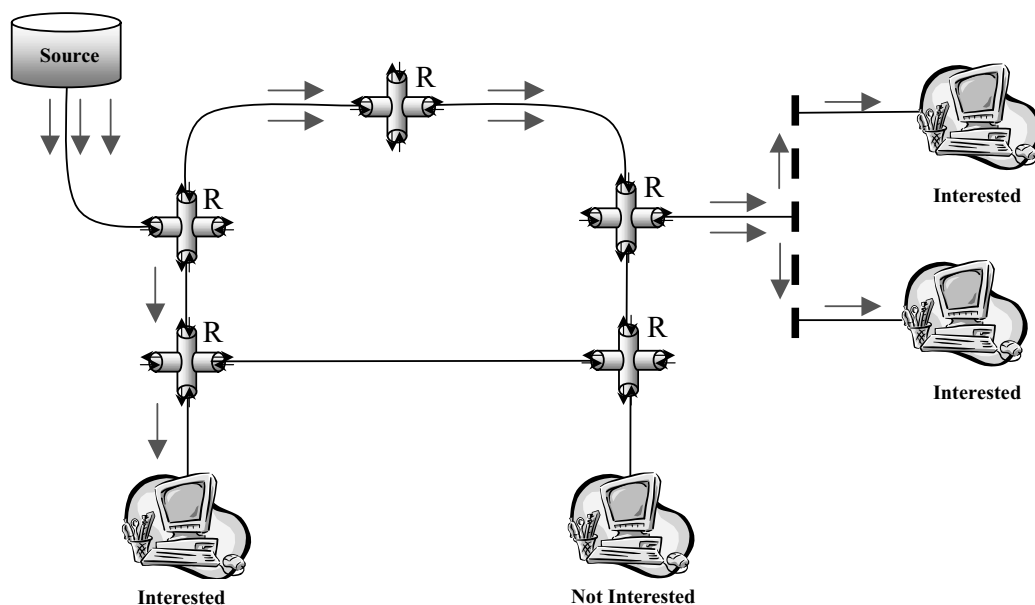
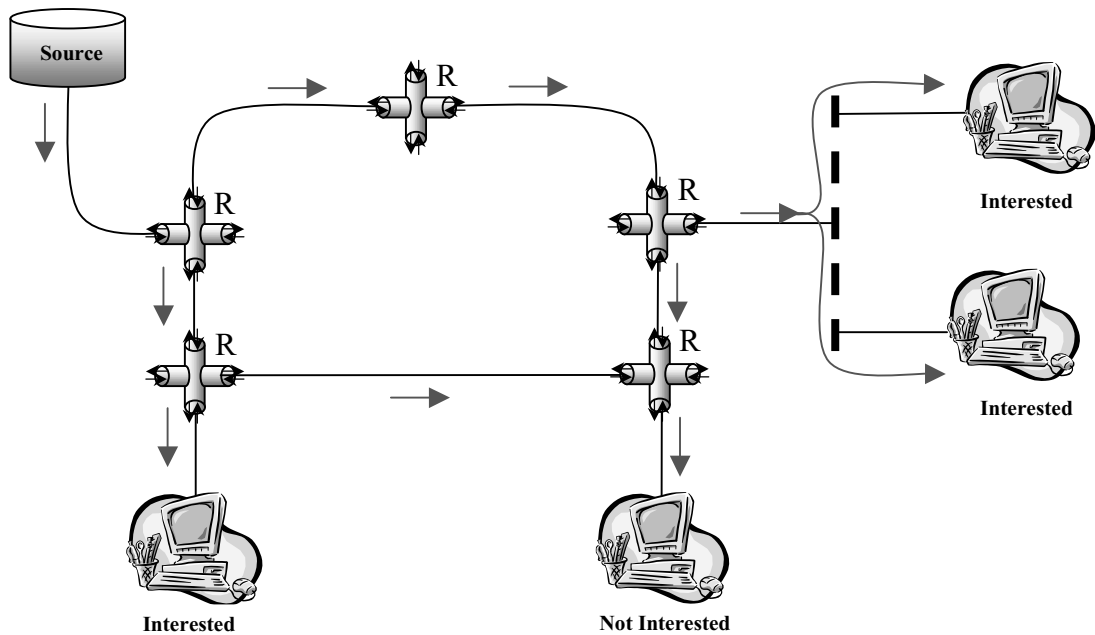
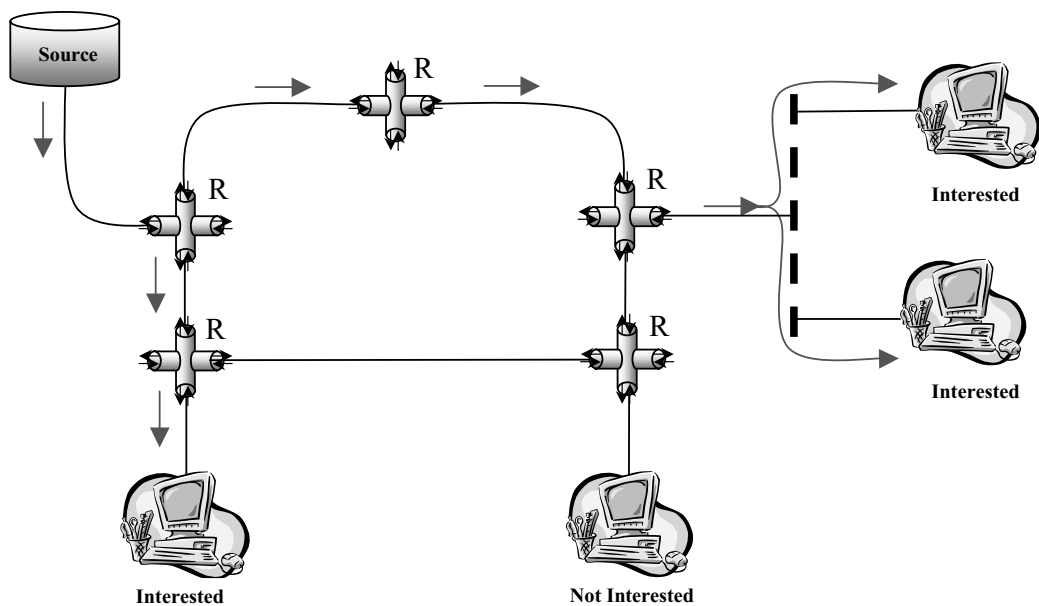


Figure 1. Unicast Delivery.



**Figure 2. Broadcast Delivery.** Note that although the above demonstrates the broadcast concept, in the case of the IP protocol, broadcasts do not in general get propagated by routers.



**Figure 3. Multicast delivery.**

## 2.2 Multicast Service Models – ASM v SSM

As described above, the reception of multicast IP traffic occurs as a result of an end point (computer) expressing an interest in certain multicast traffic to the IP router that serves its network.

In the traditional service model, an end point indicates that it wishes to receive all multicast traffic sent to a certain multicast address, no matter where that traffic originated. This approach is often referred to as Any Source Multicast (ASM), though some authors use the term Internet Standard Multicast (ISM) to describe this service model.

In a more recent service model, an endpoint indicates that it wishes to receive multicast traffic sent to a certain multicast address, but only if it originates from a specific identified source address. This approach is normally referred to as Source Specific Multicast (SSM), though some authors use the term Single-Source Multicast. While SSM is not yet supported by every router vendor, it is now approaching that position. While SSM is not supported in older end point operating systems, it is supported in MS Windows XP, various recent versions of Linux and in recent versions of the UNIX operating system from several vendors. Support of SSM by software applications is beginning to emerge. SSM and related protocols are described further in Section 2.9.

## 2.3 Multicast Address Space

The range of IPv4 addresses reserved for multicast is taken from the Class D group of addresses. The range is from 224.0.0.0–239.255.255.255. These are referred to as multicast group addresses. With the exception of some reserved addresses (mainly SSM and some administration addresses) the allocation of a multicast group address is in general dynamic. When a source continues transmission after stopping (or restarting), it may use a different group address. Well-known multicast sources are usually allocated a fixed (advertised) multicast address. Work is progressing within various IETF working groups on mechanisms that may improve support for multicast address request and allocation.

### 2.3.1 Multicast Address Allocation

Some multicast addresses have been statically allocated to certain roles. The current state of multicast address allocation can be found in [IANA].

[RFC3171] provides general guidance on the use of the multicast address space and procedures for number allocation in certain blocks of the addresses.

This general area is still considered ‘work in progress’ by various IETF working groups. At the time of writing, two Internet Drafts [draft-ietf-mboned-addrarch] and [draft-ietf-mboned-addrdisc-problems] are being considered by the MBONED working group.

### 2.3.2 IPv4 Local Network Control Address Block: 224.0.0.0–224.0.0.255

The number block from 224.0.0.0–224.0.0.255, i.e. 224.0.0.0/24 in prefix notation, has been allocated for local network control. IP packets carrying addresses in this range should never be forwarded by any multicast router no matter what value is set for the Time To Live (TTL) field. In general, addresses within this range are used by items of system infrastructure, e.g. routers when intercommunicating. The list of allocated numbers is quite large, but some examples are:

- 224.0.0.1 – all systems on this subnet
- 224.0.0.2 – all routers on this subnet
- 224.0.0.4 – DVMRP routers
- 224.0.0.9 – Routing Information Protocol version 2 (RIPv2) routers
- 224.0.0.13 – all Protocol Independent Multicast (PIM) routers
- 224.0.0.22 – all IGMP queriers

Note: IGMP Membership Reports are not required for the above block of addresses and all LANs (Local Area Networks) should carry all packets belonging to these groups.



### 2.3.3 Internetwork Control Block: 224.0.1.0–224.0.1.255

The number block 224.0.1.0–224.0.1.255, i.e. 224.0.1.0/24 in prefix notation, has been allocated for internetwork control. IP packets carrying these addresses are forwarded by multicast routers providing the TTL so allows. These have been allocated for a wide range of purposes – some for serious internetwork control and others for what might be regarded as more trivial purposes.

Again the list of allocated numbers is very extensive, but some examples are:

- 224.0.1.2 SGI-Dogfight (a game)
- 224.0.1.12 IETF-1-VIDEO (traditionally used to carry multicast video coverage of IETF events)
- 224.0.1.39 cisco-rp-announce
- 224.0.1.40 cisco-rp-discovery

### 2.3.4 ADHOC Block: 224.0.2.0–224.0.255.0

This block is identified in the Internet Assigned Numbers Authority (IANA) document, but the actual document covers the whole of the range from 224.0.2.0–224.0.255.255. Some allocations in the range suggest multicast media services, whereas some allocations are clearly for device control. Some examples are:

- 224.0.2.192–224.0.2.255 – SIAC MDD Market Service
- 224.0.18.0–224.0.18.255 – Dow Jones
- 224.0.19.0–224.0.19.63 – Walt Disney Company
- 224.0.23.1 and 224.0.23.2 – Ricoh-device-ctrl

This early allocation of specific group addresses to individual services is no longer recommended and the IANA no longer allocates such addresses. The current policy is to recommend that developers and network operators applications/services use multicast addresses from the standard range, rather than static configuration of specific addresses.

### 2.3.5 RFC1190: 224.1.0.0–224.1.255.255

This range is allocated to Internet Stream Protocol (ST) Multicast Groups as specified in [RFC1819]. It was not widely implemented and is not in use in current networks.

### 2.3.6 SDP/SAP Block: 224.2.0.0–224.2.255.255

This range of addresses is in very common use. It is allocated for use by the protocols Session Announcement Protocol (SAP) [RFC2974] and Session Description Protocol (SDP) [RFC2327]. The majority of early use of multicast on the Internet was for the transmission of audio/video coverage of events and desktop videoconferencing. The application programs Session Directory (SD) and Session Directory Tool (SDR) (*sic*) [MICE] provide a directory service of current and planned audio/video sessions, and a mechanism to announce and join such sessions. The allocations in this block are:

- 224.2.0.0–224.2.127.253 – Multimedia Conference Calls
- 224.2.127.254 – SAPv1 Announcements
- 224.2.127.255 – SAPv0 Announcements (deprecated)
- 224.2.128.0–224.2.255.255 – SAP Dynamic Assignments

### 2.3.7 Various/Reserved: 224.3.0.0–231.255.255.255

A substantial part of the range has been reserved by IANA with usage currently not defined.

- 224.3.0.0–224.3.0.63 – Nasdaqmdfeeds
- 224.3.0.64–224.251.255.255 – Reserved
- 224.252.0.0–224.255.255.255 – Distributed Interactive Simulation (DIS) Transient Groups
- 225.0.0.0–231.255.255.255 – Reserved

The DIS Transient Groups allocation reflects a request for the allocation of multicast addresses to support an initiative from the US Department of Defense (DoD) and others to build and operate DIS applications. It is not known whether addresses in this range are currently in active use.

Documentation on the use of the Nasdaqmdfeeds allocation is not currently available.

### 2.3.8 Source Specific Multicast: 232.0.0.0–232.255.255.255

The topic of SSM is covered in a later section of this document. All addresses in the range 232.0.0.0–232.255.255.255 are now explicitly reserved for SSM and any other use of this number range is now inappropriate.

The IETF MBONED working group has completed another document, *Source-Specific Protocol Independent Multicast in 232/8* [draft-ietf-mboned-ssm232], which at the time of writing was in the RFC Editor queue waiting to be formally approved as an RFC/BCP document.

### 2.3.9 GLOP Block: 233.0.0.0–233.251.255.255

The usage of this address block is defined in RFC 3180, *GLOP Addressing in 233/8* [RFC3180].

As far as can be located, the term ‘GLOP’ is not an abbreviation or acronym but a neologism. The general concept of the GLOP address space is that it is an area of multicast addresses that are allocated in a methodical manner to the holders of the registered Autonomous Systems (ASs). Each AS has been allocated 256 addresses from this range, namely the addresses where the middle two address bytes correspond to their AS number. The AS is then free to specify how all the 256 alternative values of the last byte are used. The use of GLOP within JANET is defined in section 4.3.2.

### 2.3.10 EGLOP Block: 233.252.0.0–233.255.255.255

A small selection of the possible full range of AS numbers, the range from 64512 to 65535, has been allocated for ‘private use’. The private block can be used to create internal administrative domains within what is perceived by the rest of the Internet to be a single domain. Having recognised this, there is therefore a subset of the 233/8 number space, 233.252.0.0–233.255.255.255, which does not uniquely belong to any one unicast routing area (autonomous system). Therefore, rather than just leaving these trapped and unused in the GLOP address space, they are titled as the extended GLOP or EGLOP address space and used as described in *Extended Assignments in 233/8* [RFC3138].

The basic idea is that these numbers will be allocated by regional routing registries.

### 2.3.11 Reserved: 234.0.0.0–238.255.255.255

This large block of addresses is currently defined as reserved by IANA and marked as ‘must not be used’.

### 2.3.12 Administratively Scoped Addresses: 239.0.0.0–239.255.255.255

The administratively scoped address block [RFC2365] is allocated with the intention that packets carrying such addresses will in some sense be restrained and their propagation restricted, to the effect that they are not forwarded by certain routers at the edges of some administrative domains. Thus the addresses can be used within a particular part of the multicast network with the source having confidence that they will not flow to the entire global Internet, and indeed will not leave their administration. [RFC2365] is a little unclear as to what exactly should be considered ‘an administration’. The result of the uncertainty is that practical deployments of multicast are interpreting the scope boundaries and behaviour at the boundaries in different ways.

The roles currently allocated to the numbers in this range as of 18 January 2006 are as follows:

- 239.0.0.0–239.063.255.255 – Reserved
- 239.064.0.0–239.127.255.255 – Reserved
- 239.128.0.0–239.191.255.255 – Reserved
- 239.192.0.0–239.251.255.255 – Organization-Local Scope
- 239.252.0.0–239.252.255.255 – Site-Local Scope (reserved)
- 239.253.0.0–239.253.255.255 – Site-Local Scope (reserved)
- 239.254.0.0–239.254.255.255 – Site-Local Scope (reserved)
- 239.255.0.0–239.255.255.255 – Site-Local Scope
- 239.255.2.2 – rasadv

As will be seen from the above, one specific address within the Site-Local scope area, namely 239.255.2.2, has apparently been pre-allocated for a specific purpose. Documentation concerning this use is not readily available, but it would appear that this address is used in association with the Microsoft® Remote Access Server. Packets using this address are reported as carrying User Datagram Protocol (UDP) traffic going to or from port number 9753.

It should also be noted that the IANA document [IANA] from which the above allocation has been extracted is at odds with the contents of [RFC2365], *Administratively Scoped IP Multicast*. The MBONED IETF working group is of the opinion that the RFC should be considered to be authoritative. The RFC only allocates 239.192.0.0 to 239.195.255.255 to Organization-Local Scope (i.e. 239.192.0.0/14) and the addresses from 239.196.0.0 to 239.251.255.255 remain unallocated.

As mentioned above, the definition of the terms ‘Organization-Local Scope’ and ‘Site-Local Scope’ is subject to interpretation. Clearly, there needs to be some consistent interpretation within the JANET backbone, the Regional Networks and the site networks, or at worst, the interpretation and usage within the various parts of the JANET domain should not conflict. This issue will be considered again in section 4, JANET Multicast Architecture.

## 2.4 Multicast Packet Forwarding

### 2.4.1 Multicast Routing Protocols

There are two main classes of multicast protocol used for multicast forwarding. These are typically referred to as Dense Mode (DM) and Sparse Mode (SM).

DM protocols assume that a large number of recipients exist in a network domain. These protocols therefore initially flood multicast packets to all links. They use a flood and prune mechanism whereby flooding only stops when downstream routers make a direct request for this to happen.

SM protocols on the other hand do not send multicast packets anywhere unless the packets are explicitly requested. A network running an SM protocol requires the existence of a central point, typically called a Rendezvous Point (RP), with which interested receivers register their desire to receive information destined to certain multicast groups.

Three common protocols are:

- DVMRP
- Protocol Independent Multicast – Dense Mode (PIM-DM)
- Protocol Independent Multicast – Sparse Mode (PIM-SM).

The terms ‘SSM’, referring basically to a one-to-many multicast, and ‘ASM’, referring to the inclusion of both one-to-many and many-to-many multicast, are both service models, not separate protocols.

As explained in section 2.7, Regional Networks that wish to receive multicast via the JANET network need to adopt the PIM-SM protocol. Even though JANET will support no other protocol, it is felt that a very brief explanation of the other protocols is required for clarity.

Recent work has improved the readability of the PIM specification [RFC2362] and clarified several issues. The new version, *Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)*, is contained in [draft-ietf-pim-sm-v2-new], which is expected to be published as an RFC in 2006.

The dense mode protocol DVMRP was the first true multicast routing protocol to be used on the MBONE. As mentioned earlier, it formed the main support for the JANET MBONE and was previously also used to peer with other ASs, GEANT etc. In many respects PIM-DM is very much like DVMRP. The main difference is that PIM is protocol independent, in the sense that it can use the ordinary unicast routing tables when making its checks and forwarding decisions no matter which protocols were used to populate the tables. By contrast DVMRP is protocol dependent. PIM-SM, like PIM-DM, can use either the unicast routing tables or separate routing tables specifically populated for multicast. It is now commonly believed that SM protocols are the preferred choice in all situations, even if receiver density is high.

### 2.4.2 Reverse Path Forwarding (RPF)

This appears countless times in documents describing IP Multicast and associated issues. It is crucial that anyone reading such documents has a clear understanding of how the term is being used in a variety of contexts. The mechanism used for routing multicast traffic is in some respects the complete reverse of that used to forward unicast traffic. Unicast routing decisions are based on the recipient’s destination address. In effect, the routers push the unicast packet onto the network in the direction of the receiver.

By contrast, the routers will potentially replicate all multicast packets and forward a copy out of all interfaces. Of course, a router will not send a duplicate of a multicast packet

directly back towards its original source out of the interface by which it arrived. In a complex network it is also important to prevent routing loops involving multiple routers. To address this issue the key questions that need to be asked are: has this packet arrived by the expected route from the source, or is this packet an unexpected duplicate caused by some anomaly in packet forwarding by other routers or a router loop? Such a check is thus not considering paths to potential destinations, normally termed Forward Paths, but rather the path by which a packet has arrived from its original source, thus a Reverse Path.

Only packets that pass the RPF check are candidates for forwarding out of interfaces to potential multicast receivers. The central concept of routing multicast traffic, regardless of any other protocols being used, is RPF.

The RPF mechanism is also used in many other multicast contexts. When a router is attempting to forward packets towards the Rendezvous Point (RP) of a sparse mode network, the interface that passes an RPF check with respect to the address of the RP is selected. The protocol Multicast Source Discovery Protocol (MSDP) [RFC3618], discussed below, uses RPF checks when attempting to decide whether or not to accept Source Active (SA) messages received from MSDP peers.

At this stage the routing table to be used as the basis of making the RPF decisions has not been specified. With some protocols, such as DVMRP, the protocol builds its own routing table. Other protocols – PIM for instance, as described above – are inherently defined independently of any specific routing table. Recent IETF documents describing multicast IP and related protocols have introduced the term Multicast Routing Information Base (MRIB) [draft-ietf-pim-mib-v2] as the name of the (possibly virtual) routing table used for such RPF checking. In some manufacturer implementations, the MRIB may indeed be identifiable as a single routing table. In other implementations, the MRIB is effectively provided by a set of rules that specify how a set of routing tables, often also used for other purposes, will be used when considered to be the MRIB. In either case, the MRIB used for the RPF checks only holds unicast routing information; it most definitely does not hold any multicast addresses. RPF checks are performed on the unicast addresses and not on multicast group addresses.

This current document will use the term MRIB to mean the data used for RPF checking no matter how it is implemented. Section 2.8.2 discusses how the protocol Multiprotocol Extensions for BGP-4 (MBGP) [RFC2858, RFC4271] might be used to contribute to the populating of the MRIB.

## **2.5 Multicast Traffic Reception – the Single LAN View**

### **2.5.1 Receiving Multicast Traffic**

To receive traffic from a multicast group a host must inform the routers on its LAN of its interest in joining that multicast group. Hosts and routers on a LAN use the Internet Group Management Protocol (IGMP) [RFC1112, RFC2236, RFC3376] to communicate multicast group membership information. There are currently three versions of IGMP, described in the following RFCs:

- Version 1: RFC 1112 – Host Extensions for IP Multicasting
- Version 2: RFC 2236 – Internet Group Management Protocol, Version 2
- Version 3: RFC 3376 – Internet Group Management Protocol, Version 3

The main difference between versions 1 and 2 is the way in which hosts leave a multicast group. Version 3 of IGMP has support for SSM and source filter records [RFC3678]; more on this later.

Here IGMP is described in its broader sense; a more in-depth discussion will follow concentrating on how IGMP works in the context of hosts and routers.

In the text that follows, the notations (\*,G) and (S,G) will be encountered several times. The notation (\*,G) refers to all traffic being sent to group G, no matter from which source it originates. The notation (S,G), refers to all traffic being sent to group G, but only if it originates from source S.

When joining a multicast group that is not currently being forwarded on to its LAN, a host must send an IGMP Membership Report. In IGMPv1 and IGMPv2, this is sent to the group concerned. In IGMPv3, the report is sent to a separate well-known multicast group. All of the routers (and some layer 2 switches) on a LAN that are IGMP enabled continually listen to these IGMP Membership Reports. On hearing the host's IGMP Membership Report, a router on the LAN sends a (\*,G) Join message via a multicast routing protocol.

A PIM-SM router receiving an IGMP Membership Report for a group in the ASM range sends a (\*,G) Join message towards the router that has been configured as the RP for the particular group, G, for that network. In IGMPv1 and IGMPv2 a host can only specify the group address that it is interested in, hence the (\*,G) Join.

In IGMPv3 the host can specify that it only wants to receive multicast from selected sources (or from all but specified sources) [draft-ietf-magma-igmpv3-and-routing-05.txt]. The ability to request from specific sources is a key component of SSM. A PIM-SM router receiving an IGMPv3 Membership Report for a group in the SSM range [draft-holbrook-idmr-igmpv3-ssm-08.txt] triggers an (S,G) Join report by the intercepting router; however this is not sent to an RP, as these are not used in SSM, but rather to the next router on the path to the source S. It should be noted that while SSM may not at present be supported in all Regional Networks and site networks, the backbone routers of JANET do support SSM. SSM requires host support for IGMPv3, the Source-Specific API [RFC3678] and appropriate applications on the host that support SSM. SSM will be discussed further in section 2.9. IGMPv3 also supports a host requesting all traffic sent to a group with the exception of certain sources; this feature is not used in SSM.

Some router vendors provide an interim solution that allows SSM to be used without the need to use IGMPv3. Some vendors currently only support SSM when enabling IGMPv3. It is recommended that the current level of support for SSM and IGMPv3 need is confirmed by specific manufacturers.

## 2.5.2 IGMP – the Host View

A host must be capable of running IGMP in order for it to receive multicast packets. The host's version of IGMP is a direct function of the operating system installed on the host. The original version of Microsoft® Windows® 95 only supported IGMPv1, whereas later versions of 95, 98, ME and 2000 support IGMPv2 and Windows® XP supports IGMPv3. Mac OS® 9, Mac OS®/X and Linux® all support IGMPv2. Support for IGMPv3 does exist in some versions of the Linux® kernel and for some other UNIX®-like operating systems.

To express an interest in joining a multicast group, hosts must use IGMP. To join a multicast group a host must perform two actions:

1. Arrange for its network interface to receive packets sent to the multicast group of interest. This will necessitate asking the interface to listen on some layer 2 address that corresponds to the IP multicast group address of interest. The mapping is not actually 1-1 and is discussed further in section 6, Issues for Site Networks.
2. Make sure that traffic for that multicast group is indeed being delivered by appropriate routers to the network to which it is attached. The host does this by sending an IGMP Membership Report. The report has the effect of triggering one of the routers on the LAN into joining the group using one of the multicast routing protocols, once again PIM-SM.

Periodically a router on the LAN will send IGMP Membership Query messages. A LAN may have multiple hosts that are all interested in the same multicast groups but the router only requires acknowledgement from one host to continue forwarding traffic onto the

subnet for that group. If IGMPv1 or IGMPv2 is being used, then as a measure to limit the number of IGMP Membership Report messages on the network, any host interested in a group first waits for a random period to see if another host replies, rather than replying immediately to queries. If not, it generates an IGMP Membership Report. If IGMPv3 is being used, the report suppression does not take place and hosts always generate IGMP Membership Reports.

The main difference between IGMPv1 and IGMPv2 is in the way hosts leave a group. In IGMPv1, hosts simply stop responding to Membership Queries for the group. The router will continue forwarding multicast data traffic until a time period has elapsed since the last Membership Reports arrived. With IGMPv2 there is an explicit leave report that hosts send. On receiving this report the router sends out a membership query and, if there is no response, stops forwarding to the group. This markedly reduces leave latency.

IGMPv3 added support for two additional modes, exclude and include. In exclude mode a host can request packets from a group and only the packets from sources that are not on the exclude list will be let through. The include mode allows hosts to request packets from only those sources that are on the include list. Include mode allows hosts to participate in SSM.

IGMPv3 also permits routers (and IGMP-enabled switches) to perform explicit membership tracking. In this mode, a list of all hosts receiving a group can be maintained, and when the last host leaves the group, the multicast flow can immediately be terminated, reducing unwanted traffic in the LAN.

### **2.5.3 IGMP – the Router View**

IGMP Queriers (e.g. PIM-SM routers), with an IP TTL set to 1, send their IGMP Membership Query messages to the ALL-SYSTEMS (224.0.0.1) multicast group on their subnet. If more than one potential querier exists on the subnet then the potential querier with the lowest source IP address becomes the active querier. The other non-queriers monitor the messages from the querier and if these are not observed for an extended period, typically 250 seconds, then the other potential queriers restart the election process. All non-queriers still listen to traffic contained in IGMP messages.

Routers maintain an IGMP group cache on each of their IGMP enabled interfaces. The cache is a simple table that contains a list of all groups for which there are active members, the last member that responded to a Membership Query Message for each group (or all responders with explicit tracking in IGMPv3), and when each entry in the tables will time out.

The IGMP querier regularly issues Membership Query messages, default normally once every 125 seconds, to check that interested members exist for each group. If no responses are received for a group then eventually the corresponding entries are removed from the tables maintained by the router.

## **2.6 Multicast Traffic Transmission**

### **2.6.1 Multicast Sources**

A multicast address is referred to as a group address. A multicast source is a host that sends data to a group. A peculiarity of multicast is that a source does not itself have to be a member of a group to which it sends data.

### **2.6.2 Generation of Multicast Traffic**

The ability to be a source for multicast is completely unrelated to membership of any multicast group. Any Internet-connected computer can transmit multicast using no extra software or protocols other than those included in a typical TCP/IP implementation;

in particular, IGMP is neither used nor required. Multicast sources may commence transmission of packets to a multicast address even though there are no interested receivers anywhere in the whole Internet. Clearly, such a process makes a very inefficient use of the immediate LAN to which it is attached.

Sources of significant multicast traffic (such as video servers, conferencing tools, multicast file transfer servers etc.) should optimally be connected to a different router interface to that serving client machines. This permits the multicast enabled router to control forwarding of multicast packets and prevents the source from unnecessarily flooding the local LAN with unwanted multicast traffic.

## 2.7 Single Domain Multicast Routing and PIM-SM

### 2.7.1 Distribution Trees and Rendezvous Points

Getting multicast up and running is best done in two stages. Stage 1 concentrates on implementing multicast locally. As previously mentioned, the protocol acceptable to JANET is PIM-SM. Stage 2 concentrates on the connection to the JANET multicast service. PIM-SM does not itself have a facility for inter-domain multicast routing for which the MSDP protocol is required. MSDP [RFC3618] will be discussed in a little more detail in section 2.8.1.

A PIM-SM domain supporting the ASM service model requires the existence of a common meeting place for both multicast group broadcasters (senders) and listeners (receivers). This meeting place requires that a router adopts a specialised role and is known as the RP. The decisions on location, accessibility and choice of RP are important for PIM-SM to function properly. All the routers within a PIM-SM domain must have common agreement on the RP for a given group. It is worth noting that different groups can have different RPs.

By far the most common and arguably the simplest way to configure the location of the RP(s) is to specify this statically on all routers within the PIM-SM domain. This leads to a very deterministic configuration and it is then far easier to debug problems than would be the case with other approaches.

Mechanisms for redundancy and reliability are provided for within the PIM-SM protocol. These are discussed in more detail in section 4.1.4. Discussion here is focused on a single PIM-SM domain and on there being a single RP for all groups.

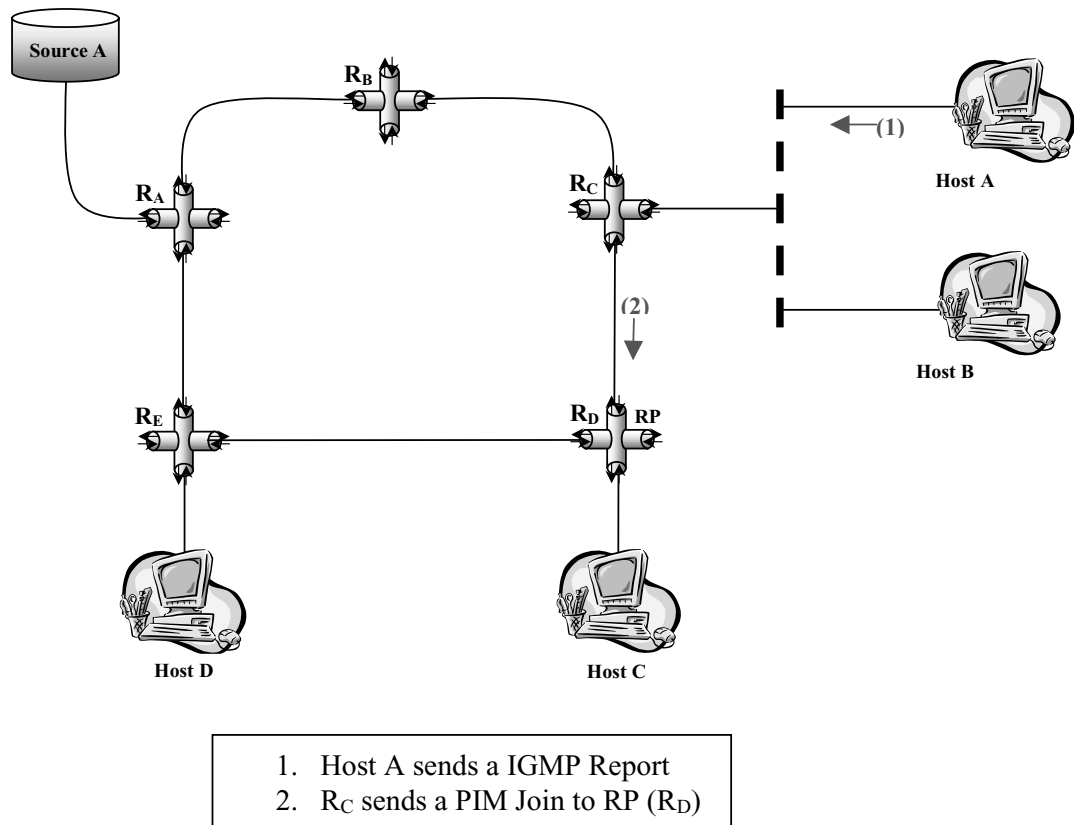
PIM-SM has three stages for delivering multicast from a source to a receiver for some given multicast group. These are:

- the building of a shared tree, often known as the Rendezvous Point Tree (RPT), that will deliver the packets between the RP and interested listeners for the group
- the building of a Shortest Path Tree (SPT) that will deliver packets between the source and the RP
- the building of a set of SPTs that will, for reasons of efficiency, deliver packets directly between the source and each interested listener.

The order in which these stages take place is not fixed – for instance, multicast sources can transmit before interested listeners exist and a SPT may already have been built between a source and its listeners when a new request to join a group is made.

A simple example describing the three stages between a single receiver and single source will aid in understanding the mechanism of PIM-SM. The example network that is used in earlier examples will be used throughout this section to aid in the readers' understanding; it is assumed to be an Autonomous System 64998 (AS-64998) (Figure 4).





**Figure 4. Host contacts RP.**

### 2.7.2 Stage 1: Building the RPT – from Receiver to RP

Once the shared RPT is built, multicast traffic will flow from the RP in the direction of the interested receivers. The RPT is however built starting at the receivers and towards the RP on a hop-by-hop basis.

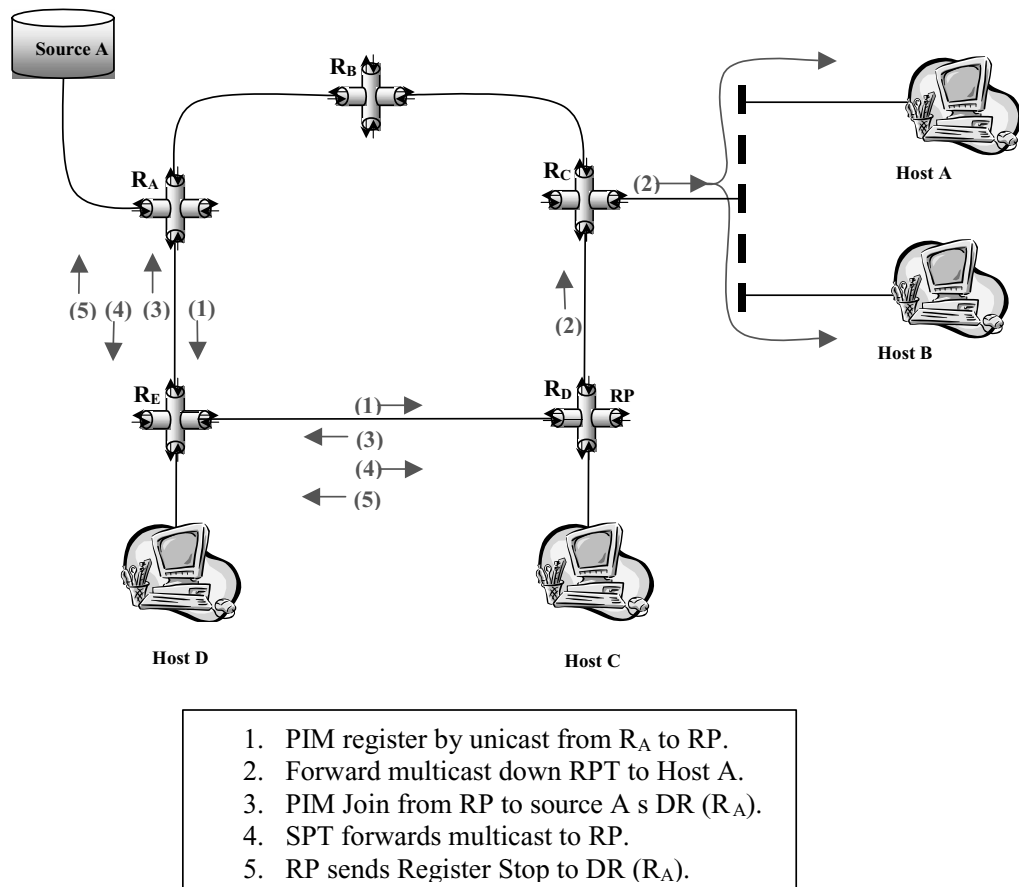
In this network, router D has been allocated the job of RP for all groups.

Host A is interested in receiving a certain multicast group and so transmits an appropriate IGMP Membership Report on to its connected subnet. This IGMP Membership Report will be received by the subnet's Designated Router (DR), in this case router C.

Router C will then send a (\*,G) PIM Join/Prune message to its neighbour in its RPF table (MRIB) for the IP address of the RP, namely router D. This process is repeated by each router until the RP is reached. The PIM-SM Join/Prune messages are sent to group address 224.0.0.13 (all PIM routers). Each router adds the interface over which the PIM Join was received to its list of interfaces via which interested receivers can be reached for the group mentioned in the join. In this example there is no active source, and so no actual multicast data will flow down the RPT at this stage (Figure 4).

### 2.7.3 Stage 2: Building the Distribution Tree – from Source to RP

When source A becomes active, it will start to send information to its directly connected network. Router A in this network is the DR with respect to source A. Router A will note that source A has become a multicast source and it will then send a PIM Register message by unicast to the RP, namely router D. The multicast packet from source A will be encapsulated in the Register message (Figure 5).



**Figure 5. Source becomes active and DR contacts RP.**

When router D, the RP, receives the Register message it will do two things. It will forward the encapsulated multicast data down the RPT for the specified (\*,G), should one exist, and will send a PIM Join message back towards the source so as to create an SPT.

Once the SPT from the source to the RP is built, the RP router will begin to receive two copies of each multicast packets. One copy arrives via the newly created SPT and the other arrives via the encapsulated Register messages, coming from router A. As soon as this occurs, the RP will send a Register Stop message to router A. When router A receives the Register Stop message for the source-group pair it stops sending Register messages.

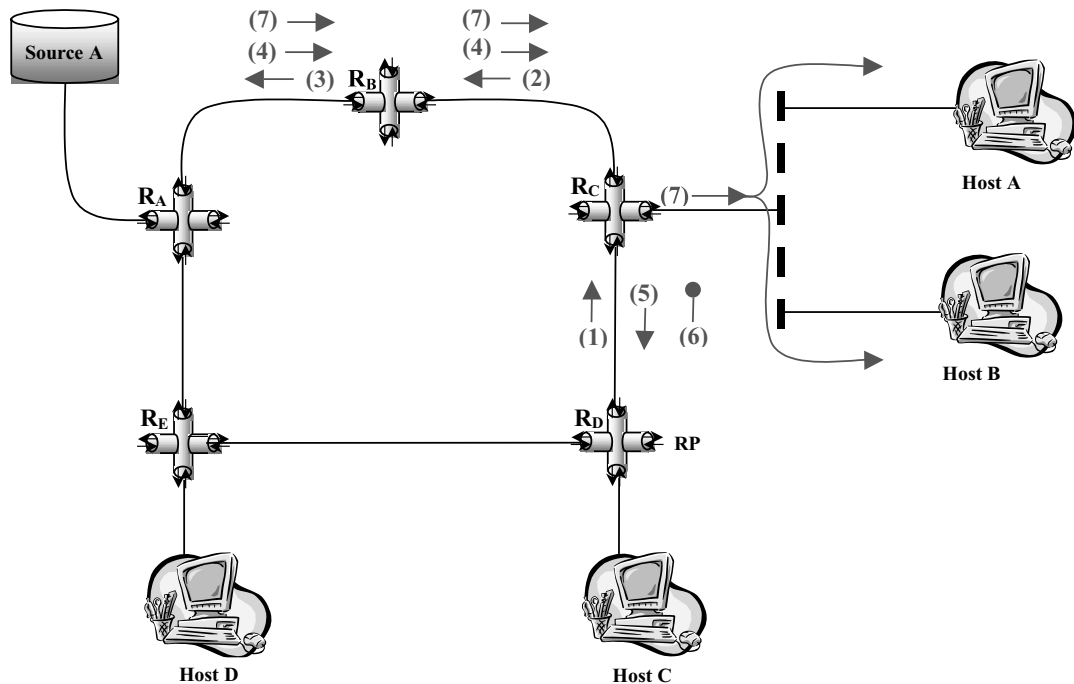
PIM Register messages continue to be repeated periodically while the source continues to remain active.

Once source A has become active and the first PIM Register packet has arrived at the RP from router A, multicast data from source A will start flowing down the RPT to all interested receivers. This data will arrive at the designated router for host A, namely router C.

### 2.7.4 Stage 3: Building the Shortest Path Tree – from Source to Host

When router C receives the first packet with a specific source address it will (usually) attempt to build a Shortest Path Tree directly from source A to itself. The shortest path to source A is actually via router B. Router C will thus send a (S,G) PIM Join to router B.

Router B will receive this Join message. Note that it has an interested receiver on the appropriate interface and itself then sends an (S,G) Join message to router A. The SPT is



1. Multicast data arrives at R<sub>C</sub> down the RPT.
2. Host A's DR (R<sub>C</sub>) sends a PIM Join via shortest route towards Source A (R<sub>B</sub>).
3. R<sub>B</sub> sends a join to R<sub>A</sub>.
4. Multicast flows down SPT to R<sub>C</sub> via R<sub>B</sub>.
5. R<sub>C</sub> sends (A, G, RPT) PIM Leave to R<sub>D</sub>.
6. RPT flow stops.
7. Multicast now from SPT flows on to Host A.

**Figure 6. Host A's DR builds an SPT and leaves RPT.**

now built and router A will start to forward multicast packets from source A in the direction of router B, which will in turn forward them to router C.

When the packets start to arrive at router C, it will now be receiving two copies of each packet – one via the new SPT via router B and one down the RPT from router D.

Router C will now send an (S,G,RPT) PIM prune towards the RP, router D which will respond by pruning the source from the RPT (Figure 6).

Router C is now receiving just a single copy of each packet from source A via the SPT and forwarding these onto the LAN where host A is located.

### 2.7.5 Other Scenarios

There are many variations on the above scenarios. Sources may become active when there are no receivers, network configurations may be more complex, SPTs may follow the same route as RPTs, RPs may be on isolated network links and so on. This present document only intends to provide an introduction to IP Multicast and it is thus describing such complex scenarios in detail is beyond its scope. Readers interested in more complex situations are referred to the texts, RFCs and Internet Drafts identified elsewhere in this document.

## 2.8 Intra-Domain Multicast Routing

So far our discussion on transmission of multicast traffic has centred on a single PIM-SM domain. The PIM-SM protocol is not sufficient to route multicast traffic between different multicast domains. The designated routers serving their subnets send **Register** and **Join** messages to the appropriate RP in their own domain on behalf of multicast sources and hosts. Two other protocols are required for RPs to be made aware of multicast sources in other domains and for sources to advertise. These are MSDP [RFC3618] and MBGP [RFC2858].

A domain's RP can be configured to implement MSDP and possibly MBGP, and use them to communicate with RPs in other domains. In order for multicast traffic to be transferred across multiple domains, two conditions must be met:

- an RP with receivers must have knowledge of the IP addresses of all active sources
- all routers directly connected along the path from sources to receivers must have entries matching the IP address of the source in their RPF table (MRIB).

### 2.8.1 Multicast Source Discovery Protocol (MSDP)

MSDP [RFC3618] fulfils the role of making available knowledge of all active sources. It allows multiple PIM-SM domains to connect together. MSDP speaking RPs exchange information on local active sources by sending out an **MSDP Source-Active (SA)** message to other MSDP speaking RPs situated in other domains via a reliable TCP connection. The **SA** message may optionally contain an encapsulated copy of the multicast packet. The use of MSDP means that sources and hosts in different domains do not have to share an RP.

On receiving an **SA** message the RP delivers the encapsulated information down any existing RPT for the (\*,G) to all interested receivers. When a destination DR receives the multicast packets it normally joins the SPT directly from the source, i.e. once the source's multicast traffic in one domain reaches the RP in another domain, the same chain of events takes place as occurs in the single domain scenario.

Acceptance of **SA** messages received by an RP involves a complex set of RPF checks and pre-configured SA filter policies. If an RP has only one peer then the checking is simplified. In addition, if a group of RPs are set as a so-called Mesh Group then the SA checking is also simplified. It is appropriate to declare a set of RPs as a Mesh Group if essentially a single administration team runs them and the members can be quite convinced that the configuration of them and the network between them is correct and that routing loops cannot occur.

MSDP had been the subject of a long sequence of Internet Drafts. An effect of this is that many products are currently deployed in UK academic networks whose implementation of MSDP conforms to earlier MSDP Internet Drafts rather than RFC3618. One of the most important differences between RFC3618 and the various earlier drafts concerns the manner in which RPF checks are performed when an MSDP speaker receives an **SA** message. This document is not the place to discuss those differences in detail, but it is perhaps worth saying that the RPF check rules in the RFC make more allowance for the use of information learnt from interior routing protocols and will probably prove easier to configure for most users in most circumstances. Our firm recommendation is that equipment compliant with RFC3618 should be used wherever possible. The authors are aware of current reports of interoperability issues between implementations of the earlier drafts.

The IETF MBONED working group have defined a set of MSDP deployment scenarios [draft-ietf-mboned-msdp-deploy].

Sources using certain addresses, e.g. the private IPv4 address space, should never be announced outside of the private zone in which they exist. There are a set of well-known groups that should be filtered and not allowed to pass outside an administrative domain. The block of group addresses allocated to SSM should also not be announced in SA messages.

Cisco® Systems has developed a list of recommended addresses that should be filtered in SA announcements [CISCOd].

Note, however, that these filter the whole of the administratively scoped address range, whereas it is recommended that some of the range is allowed to flow to all of JANET and indeed, for some addresses, all of GÉANT.

Recommendations on MSDP SA filtering, as implemented in GÉANT, are also available at [GEANTMSDP]. The reference includes configuration information for both Cisco and Juniper routers.

Many authors have questioned the scalability of MSDP. Indeed, there is fairly well agreed consensus that MSDP is not really a very long term solution to the problems of interdomain multicast. However, MSDP is what we have to day and will have for at least the medium term.

## 2.8.2 Multiprotocol Extensions for BGP-4 (MBGP) and the RPF Routing MRIB

As mentioned in an earlier section, the information used by RPF checks is now often referred to as the MRIB. There can be significant advantages to having the information in the MRIB separate from the unicast routing tables.

For instance, traffic management considerations may require that multicast traffic is carried over different links between adjacent sub-networks to those used by unicast traffic. One suitable and commonly used way to populate the MRIB is via a protocol that has the capability to indicate that certain routing information is associated with multicast. Multiprotocol Extensions for BGP-4 [RFC 2858] provides suitable features. MBGP introduces two new BGP path attributes that can be used to carry reachability information for network layers other than simple unicast IPv4. The two extra attributes are called Multiprotocol Reachable NLRI (MP\_REACH\_NLRI) and Multiprotocol Unreachable NLRI (MP\_UNREACH\_NLRI). While these attributes can be used for several things, the most common current use is for carrying multicast IP routing information.

If a network is running as an AS, it is highly likely to be using BGP-4 to pass reachability information to and from the neighbour routers in adjacent networks. In such a circumstance, it is very sensible to change to using MBGP instead. It may be that initially the same reachability information is supplied marked for both unicast and multicast use, but at least the basis has been laid should the network connections ever become non-congruent (i.e. where the multicast RPF path from the source does not match the unicast path used to send towards the source). Specific router commands to enable the use of MBGP vary from manufacturer to manufacturer and so readers will need to consult their router manuals. Some useful information, for some readers, may be found in a later appendix.

## 2.9 Source Specific Multicast (SSM)

This was briefly mentioned earlier in section 2.2. In essence, SSM provides a mechanism whereby receivers do not just join a multicast group and receive all traffic sent to that group from any source, but instead only receive traffic sent to the group if it originates from identified sources.

### 2.9.1 SSM Specifications and Documentation

SSM is currently described in [RFC3569], *An Overview of Source-Specific Multicast (SSM)*.

The SSM working group is actively preparing an Internet Draft, *Source-Specific Multicast for IP* [draft-ietf-ssm-arch] with the intention that it eventually becomes accepted as a standards track RFC.

The MBONED working group has also prepared an Internet Draft related to SSM entitled *Source-Specific Protocol Independent Multicast in 232/8* [draft-ietf-mboned-ssm232].

SSM is also briefly mentioned in many other RFCs and Internet Drafts, notably those discussing PIM.

## 2.9.2 SSM Terminology

With SSM, the network service identified by (S,G), for SSM address G and source host address S, is referred to as a 'channel.' Rather than referring to hosts 'joining a multicast group', as one might with ASM, one refers to hosts subscribing to, or unsubscribing from, a channel.

## 2.9.3 SSM-related Host and Application Requirements

The key requirement for host computers running applications that wish to receive SSM is that they support IGMPv3. The IP protocol stack installed as part of the host's operating system must contain an IGMPv3 implementation and the applications in use must be knowledgeable in terms of SSM.

Few applications currently support SSM. In terms of selecting appropriate sources, some applications may have a mechanism to know automatically what sources to connect to, while others may require user interaction to specify required sources.

Host operating system support for IGMPv3 was briefly discussed in section 2.5.2 above.

If a host wishes to send SSM then there are no special requirements; an application can just start sending packets using an address in the SSM range.

## 2.9.4 SSM-related Router Requirements

The protocol PIM-SM already has most features required for support of SSM. The main behaviour changes relate to the use of rendezvous points. In simple terms they are not used for SSM. All routers on any LAN with directly connected hosts need to support IGMPv3.

The designated routers serving networks with SSM receivers need to act differently for SSM groups than for non-SSM groups. The IP number range 232.0.0.0–232.255.255.255 has now been reserved for SSM use only. When such a designated router sees an IGMPv3 message from a receiver for a group in the SSM range, the designated router immediately starts to build an SPT towards the source. The designated router will never contact an RP and will never take traffic from an RPT for groups within the SSM range.

Designated routers attached to networks with SSM sources should never report the existence of such sources to any RP.

Some manufacturer's routers handle SSM traffic correctly by default, while in other cases appropriate configuration commands may need to be issued.

## 2.9.5 SSM and Rendezvous Point Behaviour

RPs should never be contacted by correctly behaving designated routers with respect to SSM. Should an RP erroneously receive a (\*,G) PIM Join with respect to an SSM group G, it should be rejected. Similarly, should any RP erroneously receive any PIM register messages mentioning SSM groups, they too should be ignored.

MSDP SA messages originated by RPs should never include sources for addresses within the range allocated to SSM. Any erroneously received SA messages mentioning SSM sources should be ignored.

### 2.9.6 Selecting Addresses Within 232.0.0.0/8

The problem of address selection is much less difficult for SSM than is the case for ASM. Because receivers subscribe to a (S,G) channel, and because routers forward traffic based on (S,G) state, two sources transmitting to the same group do not interfere with each other. The problem of address selection thus becomes a local issue and cooperation is only required between multiple applications within single end points.

### 2.9.7 Delivery of SSM Between Multiple Domains

RPs have no role in a multicast network that carries only SSM traffic. Because of this, we have no requirement for a protocol for RPs to communicate their knowledge of active sources and therefore no need for a protocol such as MSDP.

SSM therefore does not suffer the scalability constraints associated with the use of MSDP in ASM. Many of the important uses of multicast are precisely those that will fit into an SSM service model. For instance, on-demand servers of live news material are naturally one to many (rather than many to many) and are therefore perfect candidates for use of SSM.

Although applications which support SSM are in short supply, this situation is expected to rapidly change. SSM will probably emerge as the most important inter-domain multicast service.

## 2.10 Multicast in an MPLS Environment

The authors are aware that MPLS (Multiprotocol Label Switching) [RFC 3031] is a technology in use at various locations within UK academic networks.

MPLS adds an extra layer below the IP layer. Packets sent over MPLS networks (or virtual MPLS tunnels) need to be mapped to this layer, and the way this is done depends on the reasons for using MPLS. There are a number of ways the PIM routing protocols and MPLS-switched networks could manage multicast packet forwarding.

An overview of the use of multicast within an MPLS environment is given in [RFC3353].

Some enhancements are under consideration within both the MPLS and IP routing communities which could optimise the multicast forwarding across MPLS clouds, but currently this is work in progress. At the time of writing, three Internet Drafts exist that reference both MPLS and IPv4 multicast [draft-raggarwa-l3vpn-2547bis-mcast-bgp], [draft-ietf-mpls-multicast-encaps], [draft-ietf-l3vpn-2547bis-mcast].

At the present time the authors do not have any specific recommendations with regard to how multicast is best run in an MPLS environment, and readers with such requirements are recommended to raise any issues that may arise with JANET Customer Service.

## **3 Multicast Security, Vulnerabilities and Related Issues**

### **3.1 Firewalls, Network Address Translation and IP Multicast**

See [RFC2588], *IP Multicast and Firewalls*, which has a good discussion of this general area.

#### **3.1.1 Firewall Support**

At the time of writing very few, if any, firewalls have any significant support for the handling of IP Multicast. Cisco® systems recommend that tunnelling is used to pass across firewalls. The present document does not discuss the use of IP tunnelling. Simple packet filtering capabilities of routers normally have the ability to identify IP Multicast traffic and either permit or deny its passage.

#### **3.1.2 Security Risks from IP Multicast Traffic**

The community has mixed opinions as to the risks posed to a network by the arrival of external IP Multicast traffic. Multicast IP cannot be used proactively by malicious parties to attack any chosen machine in a network in the same way as unicast. Multicast IP traffic will only be handed to machines that have expressed multicast group membership, and only then for groups to which they have subscribed.

If receivers were to use an SSM model then multicast traffic will only be delivered to them if it appears to arrive from the sources they have nominated. The RPF checks used in multicast forwarding make it hard for a malicious attacker to spoof multicast source addresses successfully.

Overall, it is felt that the current risk from the arrival of multicast IP traffic is very low when compared to the risks posed by unicast IP. Note however that there have been some significant negative incidents. The so-called Ramen Worm used multicast as part of its behaviour. Its use of multicast was really more accidental than deliberate. The Computer Emergency Response Team (CERT) web site [CERT] discusses this and also has reports of other incidents that involved the use of multicast IP in some way.

#### **3.1.3 NAT and Private IP Addresses**

For traffic completely within an isolated network the use of the private addresses may work in a satisfactory manner. However, a host using a private IP address cannot directly be the source of a globally distributed multicast group.

Rendezvous points should never report the existence of sources using the private IP address space in any MSDP SA messages. This document's authors currently have no information with respect to whether or not a host using the private IP space can be the receiver of a globally distributed multicast group. Cisco® reports [CISCOc] that its Multicast NAT facility supports source address translation.

#### **3.1.4 IP Packet Filtering at Firewalls**

At boundary routers between one organisation's network and another's it is essential that certain multicast traffic is filtered. Such filtering is normally also appropriate at firewalls.



The addresses given below are used by applications which it is normally appropriate to run within the confines of a single LAN – in some cases because they are used for device or protocol control, in others because they generate high volumes of data.

In addition, any packets with private IP source addresses should be filtered, as should packets sent to the site-local administratively scoped addresses.

Any IP packets with the following multicast destination addresses should be filtered. This list shows the typical use of such addresses.

**224.0.1.2 ! SGI- Dogfight**  
**224.0.1.3 ! Rwhod**  
**224.0.1.8 ! SUN NIS +**  
**224.0.1.20 ! Any private experiment**  
**224.0.1.22 ! SVRLOC**  
**224.0.1.24 ! Microsoft-ds**  
**224.0.1.25 ! nbc-pro**  
**224.0.1.35 ! SVRLOC-DA**  
**224.0.1.39 ! cisco-rp-announce**  
**224.0.1.40 ! cisco-rp-discovery**  
**224.0.1.60 ! hp-device-disc**  
**224.0.1.76 ! IAPP – wireless base-station comms**  
**224.0.2.1 ! RWHO**  
**224.0.2.2 ! SUN RPC**  
**224.0.2.3 ! EPSON-disc-set**  
**224.0.23.1 ! Ricoh-device-ctrl**  
**224.0.23.2 ! Ricoh-device-ctrl**  
**225.1.2.3 ! Altiris**  
**224.77.0.0/16 ! Norton Ghost**  
**226.77.0.0/16 ! Norton Ghost**  
**229.55.150.208 ! Norton Ghost**  
**234.42.42.40/30 ! Imagecast disk duplication**  
**234.142.142.142 ! Imagecast disk duplication**  
**239.255.0.0 0.0.255.255 ! Site-local scope**

Any IP packets shown as coming from the following sets of source IP addresses should be filtered no matter what multicast IP address is given as the destination.

**10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/20 and 192.168.0.0/16.**

## 4 The JANET Multicast Architecture

The JANET backbone now transfers multicast IP natively using PIM-SM and provides full support for the use of both ASM and SSM.

All Backbone Access Routers (BARs) are configured to act as RPs for all multicast groups. The BARs all run MSDP and MBGP and are enabled ready to peer with routers within Regional Networks.

The overall concept is that Regional Networks will exchange multicast with the backbone via PIM-SM, using MSDP to exchange multicast source availability and MBGP to exchange network reachability. A paper on this issue, *Multicast: Wide-Area Perspective*, [COUZENS] was presented at Networkshop 31 2003 in York.

Further details on the configuration requirements and status of each Regional Network can be found in [RNS].

### 4.1 Connecting a Regional Network to the Backbone

At present (March 2006) on JANET, Regional Networks may either

- use the JANET BAR as an RP, or
- run their own RP.

With the forthcoming JANET backbone upgrade, Regional Networks will be required to run their own RP. The option of using the BAR as the RP in the present network was really only intended as a last resort option.

There are several possible approaches for connecting a Regional Network to the backbone using PIM-SM.

#### 4.1.1 Single RP Within the Regional Network Adjacent to the BAR

One approach is that the router that directly connects to the BAR is selected as the RP. This router needs to be configured to run MSDP and MBGP peering with the BAR.

#### 4.1.2 Single RP Within the Regional Network Distant from the BAR

A second approach is that a router which is distant from the BAR can be used as the RP. The chosen router would need to use MSDP to peer with the BAR and would need sufficient information in its MRIB routing tables so as to be able to perform RPF checks for all possible sources. If the Regional Network has a uni-homed connection to the JANET backbone then all should work correctly using the unicast routing tables as the MRIB. The Regional Networks edge router, i.e. the router which is adjacent to the BAR, must also be configured to use MBGP to advertise multicast reachability to JANET of all networks within or connected to the Regional Network and its customer sites.

#### 4.1.3 RP on a Stick

There will be real instances where the router infrastructure within a Regional Network does not fully support MSDP or MBGP. One possible solution to this problem is by the acquisition of a single router that does support MSDP and possibly MBGP to perform this task. This router would be attached at a strategic point within the backbone of the Regional Network and then configured as in the single RP scenario described above. The RP router may indeed perhaps only have a single interface and thus be described by the term 'RP on a Stick' as defined in [WILLIAMSON]

#### 4.1.4 Resilient RPs Within the Regional Network

The PIM-SM specifications permit more than one RP to be set up for the same set of multicast addresses [RFC3446]. This can provide improved resilience to failure, and can offer load-balancing. The technique is normally known as Anycast-RP.

The selection of routers chosen to act as RPs each need to have a loopback interface (a pseudo internal interface not corresponding to real hardware) configured with a common IP address. This address is referred to as the Anycast-RP address.

All other routers specify that the RP address is the Anycast-RP address. When a router sends a packet towards the Anycast-RP address, the first router configured with that address on a loopback interface will intercept and process the packet.

The Anycast-RP routers must be configured as an MSDP Mesh Group. One or more of the Anycast-RP routers should be configured to MSDP peer with the BAR. If only one router peers with the BAR then it is strongly recommended that the selected router is the one directly connected to the BAR.

It should also be noted that the activity of being an RP is not particularly onerous for a router. The benefits to be gained by having multiple RPs are probably outweighed by the complexity involved and, in the short term, Regional Networks are strongly recommended to adopt the single RP scenarios given earlier.

### 4.2 Multicast Connectivity from JANET to External Networks

The JANET backbone currently has a native IP Multicast peering with GÉANT. In addition the JANET backbone is fully IP Multicast peered with both Sprint and Level-3. JANET is also multicast peered with:

- BBC (British Broadcasting Corporation) [BBC]
- GlobalMix (Global Multicast Internet Exchange) [GLOBALMIX]

### 4.3 Use of Multicast Addresses within JANET

#### 4.3.1 Use of Administratively Scoped Addresses within JANET

The existence, role and general usage of administratively scoped addresses was described in section 2.3.12 together with the need to define appropriate administrative scoping rules. It is clearly important that such uncertainties are removed in terms of how they are to be used with JANET and connected Regional Networks and site networks. How such addresses are handled at the boundaries between the JANET backbone and other external networks also needs to be defined.

The range of addresses noted as Site-Local Scope in RFC2365 *Administratively Scoped IP Multicast* (239.255/16) will be blocked at all external boundaries between the JANET backbone and Regional Networks. It is recommended that Regional Networks block these addresses at the JANET backbone boundary and, in addition, at all boundaries between the Regional Networks and site networks. Assuming Regional Networks adopt our recommendation, all sites can use this number range with no risk of duplicate conflicting use with others external to themselves. Clearly, each site will need mechanisms to avoid duplicate use within the site.

At the boundaries between the JANET backbone and all external networks, with one exception, all the administratively scoped addresses (239/8) will be completely blocked. The one exception is at the boundary with GÉANT, where the range 239.194.0.0–

239.194.255.255 will not be blocked. This range has been specified by GÉANT as a pan-GÉANT number range that is intended to reach all hosts on all networks within GÉANT but not be propagated beyond. It is recommended that the whole of the number range 239.0.0.0–239.255.255.255 (239/8), except for the number range 239.255/16, is not blocked by Regional Networks at either the Regional Network to JANET boundary or at site boundaries. Assuming Regional Networks and sites adopt this recommendation then there will be a pan-JANET number range that cannot leak or conflict with others outside of JANET (or GÉANT with 239.194/16).

However, with the large number of NRENs, and the fact that many have external multicast peerings with other networks, it must be accepted that the pan-GÉANT number range may leak to other networks.

#### **4.3.2 Use of GLOP Addresses within JANET**

JANET, like all other ASs, has been allocated one block of addresses from the GLOP range. The JANET addresses are the range 233.3.18.0–233.3.18.255, i.e., 233.3.18.0/24. The range of numbers available in this GLOP range is 256. It is therefore inappropriate to sub-allocate these in any way to JANET-connected Regional Networks or sites, and thus these numbers will be used for JANET-wide infrastructural purposes, in at least the first instance.

#### **4.4 Use of SSM within JANET**

As mentioned in section 2.5.1, the routers within the JANET backbone already have the capability to support SSM. If Regional Networks, site networks and connected computers all have appropriate support for SSM then end-to-end transmission may be provided across the network. SSM support in JANET has been tested. Examples of use include successful connections from JANET sites to `ssmping.uninett.no` and SSM access to coverage of the Olympics provided by the BBC's multicast trials.

#### **4.5 Connection of Regional Networks that Cannot Meet the Above Specifications**

There may be a small number of networks that technically cannot currently adopt the recommendations given above. For instance, in an earlier section we noted some interworking problems associated with MSDP. Any Regional Networks facing such difficulties should contact JANET Customer Service who will arrange for consultations with the JANET NOSC (Network Operations and Service Centre) with a view to locating a temporary solution to the problems. Each problem will be dealt with on a case-by-case basis.

## 5 Suggestions for How Regional Networks Might Carry Multicast IP Packets

### 5.1 Use of PIM-SM

When PIM-SM is used and RPs are appropriately placed, all should be relatively trouble free. In addition to PIM-SM, the RP will also need to support MSDP and in some cases MBGP.

### 5.2 Other Approaches

Some Regional Networks, for good reason, are using technologies or product ranges where the adoption of PIM-SM, MSDP and MBGP as described above is not easily possible. MSDP was specified in a long sequence of Internet Drafts before finally being defined in RFC3618. It may be that MSDP is supported by a Regional Network's infrastructure, but the implementation conforms to an early Internet Draft and not RFC 3618. If MSDP is not supported by the current infrastructure, or the version supported is an old one, then the acquisition of a single new router may be able to enable connectivity as described in RP on a Stick, section 4.1.3.

Any Regional Networks that are not able to adopt the recommended approaches should contact UKERNA. It will arrange for the NOSC to liaise with the Regional Network staff with a view to locating some alternative acceptable arrangement to achieve multicast connectivity.

### 5.3 Serving the Site Networks

If site networks are running equipment capable of supporting PIM-SM then connection should be straightforward.

The workload of a router being an RP is widely considered in the literature to be fairly light; we do not believe there is an argument, based on sharing workload, that would require sites to deploy their own RPs. One might argue that a good reason to deploy site RPs might be for resilience should the Regional Network's RP become unavailable.

If sites are willing to be part of a common domain in terms of shared groups etc. then there is no need for them to deploy their own RPs and they can simply use the Regional Network's RP.

If it is felt necessary for them to have some multicast groups that only travel within their domain and do not travel to the Regional Network or beyond, then the sites will need to establish their own RP for those groups, while for other groups they will choose to use the RP of the Regional Network.

## 6 Issues for Site Networks

Sites will in general have to address two sets of issues. To use the terminology of protocol models, these can be viewed as 'level 2' or link level issues and 'level 3' or network level issues. The earlier sections of this chapter will address the data link issues and later sections will address network level issues.

### 6.1 Routed versus Switched versus Repeatered LANS

The networks used to serve the sites of JANET users are by no means all of the same nature. Many small sites consist essentially of a site access router connecting a simple LAN to the Regional Network supplying connectivity to the site. Other large sites have networks that are much more complex and include many routers within the site in addition to the site access router.

Most LANs deployed within JANET user sites are implemented using varieties of Ethernet. There are other technologies in use, but they will not be addressed in the current version of this document.

Wireless LANs have been deployed within many sites and some brief guidance on the use of multicast with such networks is given in section 6.4 below.

This section concentrates on issues associated with multicast within a single LAN. It is a relatively brief coverage of the issues. Readers interested in more extensive coverage are referred to [FAIRHURST2002a] and accompanying slides [FAIRHURST2002b].

#### 6.1.1 Co-axial Cable-Based Ethernets

Ethernet LANs were originally constructed consisting only of co-axial cables segments coupled together using devices known as repeaters. These are simply devices that clean all signals at the bit level and forward them onwards to all connected segments. A traditional repeatered LAN is often described as consisting of a single 'broadcast domain'. Repeatered Ethernets forward all frames to all cable segments no matter what destination address is included within the frame. Relatively early in the lifetime of Ethernet technology, the device known as a bridge was introduced. The bridge forwards traffic in a more selective manner. Unicast addressed traffic is in general only forwarded onto segments that lead towards the destination. Broadcast addressed traffic is flooded forwards onto all segments as also is unicast traffic if the location of the destination is unknown. Multicast traffic was little used in the early days of Ethernet and was generally handled by bridges in the same way as broadcast traffic.

#### 6.1.2 Twisted Pair Cable Ethernets

Ethernet technology has evolved over recent years, one of the major changes being the introduction of twisted pair cabling and corresponding changes to connectivity devices. In a twisted pair Ethernet, a device known as a hub replaces the repeater. A simple hub acts identically to a repeater, forwarding all traffic to all cable segments. The traditional bridge is replaced by the switch in a twisted pair network. In essence, the forwarding behaviour of a straightforward switch is identical to that of a bridge.

#### 6.1.3 Translating IPv4 Multicast Addresses to Ethernet Group Addresses

IP Multicast traffic is carried within group addressed Ethernet frames. The group addressing space within Ethernet that is available for IP Multicast use is unfortunately only 1/32 of the addressing space used by IP Multicast. A direct consequence of this limitation is that groups

of 32 different IP Multicast addresses all share the same Ethernet group address. Thus, the Ethernet group address alone is not sufficient to identify all packets belonging to the same group.

Further text on this issue, kindly supplied by Gorry Fairhurst, is provided in Appendix B.

## 6.2 Multicast on Repeated Ethernet

A repeated Ethernet, whether built using repeaters or hubs, will treat all multicast as though it were broadcast traffic. Thus, all the multicast traffic will reach the hardware NICs (Network Interface Cards) of all connected computers.

Many early NICs had essentially no hardware support for multicast. An immediate consequence was that for a computer to receive multicast, it had to request the card to go into 'promiscuous' mode, thus causing all arriving network traffic to be taken into the computer for subsequent software processing by the IP protocol software. More recent NICs do possess hardware/firmware multicast support, but another potential problem still remains. As mentioned above, sets of 32 IP Multicast groups share a single Ethernet level group address. Thus, even with modern NIC cards, computers can unintentionally receive traffic for 31 unwanted IP Multicast groups for each group required. Fortunately, the large range of available IP Multicast group addresses currently means that the occurrence of this situation is not highly likely.

If multicast traffic within the LAN is at a low level then the arrival of unwanted traffic at all connected computers may not be an issue, especially if modern, high-speed computers are in use. However, many current and emerging applications of IP Multicast, e.g. Access Grid, tend to generate relatively high levels of multicast traffic. An Access Grid meeting involving six sites could generate of the order of 5 Mbit/s of multicast traffic continuously.

In summary, it is generally not recommended that repeated LANs are used if there are intentions to use IP Multicast. This is especially the case with 10Mbit/s segments where even a small number of multicast flows can consume a significant proportion of the total available link capacity.

## 6.3 Multicast on Bridged or Switched Ethernet

In this section, the term 'switched Ethernet' will be used to refer to an Ethernet constructed using either bridges or switches, unless the text specifically states otherwise. Similarly, the term 'switch' will include 'bridge'.

As briefly mentioned above, most bridges and all early switches treated multicast traffic as though it was broadcast traffic and thus flooded it forwards to all connected segments (see previous section). In such circumstances, IP Multicast is not recommended.

A few managed bridges and most recent managed switches have some mechanism to handle multicast in a more sophisticated manner.

### 6.3.1 Control via Filter Tables

If the requirement for IP Multicast in a LAN is well understood and relatively static, then one possible approach is to create appropriate filters within the switches's frame filtering configuration. Such filters would completely block multicast to some segments while allowing all, or perhaps some multicast Ethernet group addressed frames into other segments. There is however a significant administrative overhead to this approach and it can only be recommended in a very limited set of circumstances.

### 6.3.2 Control via IGMP Snooping

Many recent switches include a facility typically described as ‘IGMP snooping’. This basically involves the switch, a level 2 device, examining level 3 information, and using this to establish tables to direct its frame forwarding. Some switches perform this snooping purely within software; others use hardware support. For switches performing the snooping in software, the overhead can become very high and lead to degradation in switch performance that is clearly undesirable. Switches that perform the snooping in hardware have much better performance but are often very costly due to the expense of the specialised hardware components used. High cost is clearly also very undesirable for many sites.

IGMP snooping is able to control the flooding of multicast with switched Ethernets but it is not all trouble free. [FAIRHURST2003] discusses what is termed the ‘ten thorny issues’, of which a few points are mentioned here. First, some multicast groups (e.g. 224.0.0.0/24) should be forwarded to all connected networks; some switches are reported as not implementing this correctly. Secondly, the network may be carrying non-IP multicast and IGMP snooping will not help to control this traffic. Finally, various anomalous situations may arise, and of course more recent versions of IGMP may be deployed and used by some equipment and devices which can lead to unexpected behaviour elsewhere.

Many currently deployed switches do not support IGMPv3 and lack of support for these protocols can result in operational problems and/or prevent clients using the new protocols in IGMP snooping networks. IGMPv3 is in some ways easier to snoop than earlier versions because the IGMP Membership Report messages are sent to the well known multicast address 224.0.0.22 rather than to the group addresses to which they refer. It is therefore not hard to implement such snooping in switches and manufacturers are expected to provide support in new products.

There are some anecdotal reports of switches which perform IGMPv2 snooping, sometimes causing unexpected/unwanted interactions if hosts and routers start to use IGMPv3.

It is important to realise that not all equipment vendors differentiate clearly between the two methods of IGMP Proxy and IGMP Snooping, and many vendors implement IGMP Snooping with some IGMP proxy functions.

### 6.3.3 Switches Act as IGMP Queriers (IGMP Proxies)

A further possibility is that a switch contains a full implementation of IGMP as though it were a router. Using such a scenario, often called the IGMP proxy approach [draft-ietf-magma-igmp-proxy], the switch may become the IGMP querier for downstream computers and will behave as a proxy for those machines when an upstream router queries the switch itself.

### 6.3.4 Control via CGMP

Cisco Group Management Protocol (CGMP) is a Cisco® proprietary protocol to enable switches and routers to exchange information relating to multicast group membership. Being a proprietary protocol, this largely only has value within an environment that is implemented using equipment from Cisco®. In essence, CGMP involves the routers within the network communicating with the switches and informing them of which Ethernet level addresses are associated with computers that wish to receive multicast. Essentially, the routers are automatically configuring the filter tables within the switches.



### 6.3.5 Other Approaches to Control

Some other approaches to handling multicast at switches do exist, for instance the use of IEEE 802.p Generic Multicast Registration Protocol (GMRP). This is not covered further in the current document, but is explored a little more in [FAIRHURST2003].

## 6.4 Multicast on Wireless LANs

Wireless LANs (WLANs) effectively provide a shared media network. In a somewhat similar situation to 10Mbit/s shared Ethernets mentioned above, even a small number of multicast flows can consume a significant proportion of the total available link capacity.

In the short term, it may be prudent to connect wireless access points to their own ports on routers and then completely disable the flow of multicast to those access points. Hopefully, it may be possible to publish more positive advice related to IP Multicast and WLANs as experience is gained around the JANET community.

## 6.5 IP Level Issues

Once a site has established an appropriate infrastructure of switches etc., it then has to consider the issues of handling the multicast traffic at the IP level. In essence, this involves many of the same issues as addressed in previous chapters. Any IP routers within the site environment need to be configured to support the use of multicast IP traffic and, again, the use of PIM-SM is in almost all cases the appropriate approach.

### 6.5.1 Rendezvous Point Selection

In some cases it will be appropriate for the site to use only the serving Regional Network's rendezvous points. However, in many cases a site will establish its own RP infrastructure, even if only to serve a small set of addresses for private internal traffic.

As mentioned in earlier chapters, the role of being an RP is not in itself very onerous for a router. For many sites the establishment of a single RP will be all that is required. Almost all JANET connected sites have a single connection to a single Regional Network. In such cases, the most appropriate location for the RP will either be the site's router that connects to the Regional Network or a router immediately adjacent to that. Such a router would be a single point of failure in any case and so does not further compromise external multicast connectivity.

If the RP is serving all group addresses, rather than just a small subset for internal use, then the router chosen will need to MSDP peer with the RP infrastructure operated by the serving Regional Network with respect to the global group addresses. Regional Network staff should be consulted as to their procedures and arrangements for establishing such MSDP peering. If BGP is currently used to pass reachability information between the Regional Network and the site networks then it is likely that this will need to change over to MBGP.

If the RP is only serving a small subset for internal use, probably the site-local administratively scoped addresses 239.255.0.0–239.255.255.255, then it should not be set up as an MSDP peer with the Regional Network's RP.

Some sites may have a complex structure of networks being operated by separate departments and groups rather than having a single, corporately run network. In such cases it may be appropriate for the departmental networks to run their own RPs. Such decisions will be based on considerations of whether or not the departments wish to run multicast applications whose traffic does not leave the department's own network infrastructure.

## 6.5.2 Site Non-RP IP Router Configuration

All the non-RP IP routers on the site will need to be configured with the correct addresses for the RPs to use. If a local RP is not deployed then the Regional Network's RP should be specified as the RP address. However, if a site-based RP has been established then the routers should be configured with that as the RP for the group addresses that it serves and the Regional Network's RP for the remaining group addresses (if any).

## 6.6 LAN Deployment Considerations

It is well worth considering deployment within the LAN environment using a staged approach rather than enabling everything everywhere at once. It is sensible to test multicast capability as deployment progresses. A relatively simple approach to testing is to download a selection of the Multicast Tools such as sdr, rat, vic and wb and use these to test multicast connectivity. These tools can be downloaded from [MICE].

Sites are also recommended to monitor for unexpected changes in traffic profiles as discussed in the next subsection and the next chapter.

## 6.7 Miscellaneous Issues

Various peculiarities have troubled successful multicast deployment over the years. Some early implementations of TCP/IP protocol stacks had bugs within the multicast area. In particular, TCP/IP implementations are never supposed to issue ICMP (Internet Control Message Protocol) packets in response to multicast. One particular network attached print server had a specific bug which indeed caused it to issue ICMP error messages in response to multicast. On one occasion this caused, most embarrassingly for one of the authors, a large amount of the multicast video coverage of a NASA event to be trashed. A lesson learnt from this experience is that it is well worth monitoring to detect unexpectedly high levels of ICMP traffic immediately after multicast IP traffic is allowed to enter a network section for the first time.

## 7 Management and Monitoring of IP Multicast

The management and monitoring of IP Multicast has been a problematic area and has in some ways delayed the successful deployment of multicast IP through its early years. Approaches for the management and monitoring of IP Multicast are now emerging and this section briefly discusses some of them.

Multicast traffic does not flow through a sparse mode network until receivers have notified their interest in certain groups. The purely passive monitoring of a network's ability to deliver multicast successfully with appropriate measures of latency, jitter and loss is therefore impossible. Several approaches have been developed over the years that transmit and monitor typically low levels of IP Multicast traffic purely to support monitoring.

### 7.1 Multicast Beacons

#### 7.1.1 The NLANR Beacon Software

The Beacon Architecture [NLANR] has emerged relatively recently and is rapidly gaining ground as the most commonly used method of IP Multicast monitoring. Developed by the American National Laboratory for Applied Network Research (NLANR), beacons are both sources and receivers of multicast traffic. The beacons record statistics of multicast traffic reception and then unicast these statistics to a server. The server collates the reports and makes them available for inspection.

#### 7.1.2 The JANET Beacon Service

JANET now operates a central beacon service [BEACON]. At the time of writing (March 2006) the JANET beacon service is based on version 1.3 of the beacon software. The JANET beacon service provides a public beacon, a beacon for the Access Grid community and a beacon for use by Regional Network Operators. All JANET-connected sites, all Access Grid locations and all Regional Network Operators are very strongly encouraged to install a beacon client on a suitable machine and arrange for them to interact with the appropriate JANET beacon server.

### 7.2 SSMPING / ASMPING

These two pieces of software provide a facility whereby checks are made to see whether SSM or ASM traffic being sent by a test server running on a distant machine can be received by the client application. The software applications were created by Stig Venaas [VENAAS].

### 7.3 Multicast Detective

This piece of software [DETECTIVE] attempts to probe the network to which the client computer is attached, attempting to explore the nature of the multicast service that is available. It attempts to test which versions of IGMP are supported by both the client computer and the routers attached to the network, and whether or not ASM and SSM multicast connectivity is supported.

### 7.4 Other Approaches to Monitoring

Other approaches to monitoring have been used over the years, but many are either dependent on out of date multicast routing protocols or are manufacturer-dependent. Many

of the approaches are quite crude and the information available is only of any real use to expert multicast managers.

#### **7.4.1 Simple Network Management Protocol (SNMP)**

Work is in progress to define SNMP Management Information Bases (MIBs) for various aspects of an IP Multicast infrastructure. Indeed, some relevant MIBs are already defined in RFCs and Internet drafts. Some manufacturers have defined their own proprietary MIBs. The information provided typically requires a very in-depth understanding of multicast behaviour for it to be useful. The current document does not pursue this avenue further.

#### **7.4.2 Mtrace**

The application program mtrace has been in existence for a considerable period and has often proved very useful to the current authors in tracking down multicast related problems. It provides a traceroute type facility for multicast connectivity. Mtrace is normally used by asking it to check the multicast path from an identified source to the current destination. It depends on successful RPF checks being possible with respect to the source. Thus, typically, the local host needs to have joined an ASM group. Initial implementations of mtrace were for UNIX<sup>®</sup> environments only, but in recent years implementations for other operating systems have emerged.

### **7.5 Multicast IP Interaction with Unicast IP**

Adverse interactions between multicast IP traffic and unicast IP have been observed. Section 6.7 noted problems with ICMP traffic being erroneously generated in response to arrival of multicast IP packets in some incorrectly coded IP protocol stacks.

Based on personal experience, it is strongly recommended that routine traffic monitoring of network segments is conducted before and after enabling of IP Multicast. Such monitoring can help to rapidly locate unexpected problems.

### **7.6 The JANET Looking Glass**

The JANET network runs a service known as the JANET Looking Glass [LOOKINGGLASS].

This service enables the user to gain visibility of a number of aspects of the current state of the JANET core routers. Several of the items which can be observed have a direct relationship to the state of multicast forwarding, routing and so on.

## 8 Multicast Applications

Multicast provides efficient support for a wide variety of applications. For example, videoconferencing, information dissemination, shared whiteboards, multi-player games and multicast file transfer are all achieved far more efficiently using multicast than by way of multiple unicast transmissions.

### 8.1 Multicast Videoconferencing

An important use of IP Multicast, certainly within the academic Research and Development community, is to support applications providing enhanced videoconferencing capabilities. These tools can be downloaded from the Multimedia Conferencing Applications Archive [MMCA].

An alternative location where many of these applications can be located is on the UCL Network and Multimedia Research Group's web pages [MICE].

In addition to the tools mentioned above, some manufacturers have commercially available products that include multicast support. For instance, Emblaze-Vcon [VCON] and Polycom [POLYCOM] list multicast support in the specifications of some of their products.

### 8.2 Access Grid

The Access Grid [ACCESSGRIDa] provides access to grid middleware in order to support distributed meetings, collaborative work and seminars. It enables shared visualisation, communal data access and remote control of instruments. It also enables observation and study of collaborative work in a virtual environment. It differs from other approaches to videoconferencing in its scalability and also in its emphasis on group-to-group rather than person-to-person interaction.

The Access Grid project is driven by a global community of developers and users covering business, cultural, not-for-profit and academic sectors.

The Access Grid is used by way of an Access Grid node which brings together a variety of familiar pieces of equipment, including projectors, cameras, microphones and large-format displays, to create an integrated studio-like videoconferencing facility. Access grid nodes vary from the simplest, personal node, which runs on a laptop that can be brought into a room that has been set up for an Access Grid, through the room-based node that provides a shared display for multiple users, multiple video streams and an audio stream, to the advanced node with a tiled display, multiple video streams and localized audio.

Access grid nodes are available at several centres in the UK and overseas.

The UKERNA Access Grid Support Centre [AGSC], run by the University of Manchester with JISC funding, provides comprehensive services, training, support and advice to academic users in the UK.

A status report of the progress of Access Grid deployment in the UK can be located at [ACCESSGRIDb].

### 8.3 Multicast Newsfeeds and other Live Streaming Servers

Multicast access to live feeds from news services, conferences, Internet-based TV and radio, web cameras and so on has great potential. The live streaming server merely has to issue one copy of each packet with the multicast enabled routers in the network taking care of all packet duplication when required, no matter how many viewers attach.

Several reports have noted that after the attacks on 11 September 2001 the news servers at CNN and ABC were completely overwhelmed by the demand from vast numbers of unicast

accesses. Many such servers resorted to using simple text only web pages in an attempt to keep operating. The University of Illinois, in co-operation with CNN and Cable-Satellite Public Affairs Network (CSPAN), transmitted MPEG video coverage of the tragic event via multicast to concerned viewers.

Products exist from many manufacturers including VBrick [VBRICK], Cisco® (IP/TV) [IPTV] and Apple (Quicktime Streaming Server) [APPLE], amongst others.

The BBC has been running a technical test of IP Multicast for a couple of years. This was referred to in sections 4.2 and 4.4 above. In February 2006, the BBC together with ITV moved this activity a step towards it becoming a service [BBC].

At the time of writing, their technical trial has provided access to BBC1, BBC2, BBC3, BBC4, ITV1, ITV2, ITV3, ITV4 and BBC News 24. In addition, access was available to nine radio stations.

## 8.4 Multicast Access to On-demand Servers

Multimedia streaming applications include video on demand and pre-recorded coverage of conferences, concerts and so on provided by servers that are accessed by potentially millions of end-users. Many suppliers of on-demand media servers provide multicast access to their products. In order to benefit from multicast access, clever techniques are used by on-demand providers. For example, streaming is delayed until the same media can be delivered to multiple users at essentially the same time. Such use only provides major benefits if it is likely that many viewers will wish to watch a certain item at the same time. Many media on-demand servers can also support transmission of live events. Such use has been described above.

## 8.5 Non-media Applications

There are several other applications that can benefit from the use of multicast IP. Network time synchronisation can be achieved using multicast, as can the distribution of network news. Some financial applications have been deployed to distribute real time financial data, such as stock prices, simultaneously to multiple dealer desks.

The distribution of software updates to multiple sites and the replication of database information could all gain leverage from the use of IP Multicast.

## 8.6 Information Dissemination

Multicast news feeds, instantaneous information on share data and advertising can all benefit from IP Multicast. Although all these applications fall under the broad general heading of information dissemination, different applications pose different challenges. When using IP Multicast some of the questions the designer needs to ask are as follows.

- How large is the target audience? For example, the challenge of enabling millions of viewers to access a news feed [NEUMANN] is very different from that of providing bulk data or high-quality multimedia to small numbers of recipients.
- How large is the quantity of data being transmitted? For example, the European Space Agency regularly carries out multi-gigabyte bulk data transfers to small numbers (between 10 and 20) of sites [JEACLE].
- Are the intended recipients of the information human users or software agents? Where information is being transmitted to human users (for example, in the case of information about share prices), issues of visual or aural presentation are very important. If the same information is transmitted to software agents then processing tractability becomes much

more important. Agent recipients of multicast data are becoming more common and their importance is likely to grow [BUSETTA].

## 8.7 Infrastructure Applications

Multicast provides an efficient way to distribute software updates, to replicate database information and to synchronise network time. These applications are not directly used by end-users or by user agents, but rather serve to maintain the network infrastructure and to preserve data integrity across the network. They do not normally entail transmission of video or audio data and require minimal presentational facilities; usually these are limited to an indication of success or failure of the update.

One important infrastructure application that can benefit from multicast is PC cloning. This is used for backup/recovery and for deployment of new software across large numbers of machines. Updates are sent using IP Multicast to a well-defined set of target machines. Software to support this includes Symantec's Norton Ghost [GHOST], Phoenix ImageCast MFG [IMAGECAST] and Codework's Altiris RapiDeploy [CODEWORK].

A problem that can arise when using multicast for software updates is that the network becomes flooded with updates and all other applications run extremely slowly. This is solved by 'throttling', which effectively limits the amount of traffic generated by the multicast update.

## 8.8 Multicast File Transfer

File transfer using multicast protocols can be very network efficient. The protocol FLUTE [RFC3926] was implemented by the MAD project [MAD] to support the unidirectional delivery of files over the Internet and makes use of multicast. The application Mad-Flute is an implementation of FLUTE.

## 8.9 Service Location Protocol

The service location protocol (SLP) enables discovery and selection of network services [RFC2614]. In IPv4, SLP underlies discovery mechanisms in AppleTalk, Novell Netware and Sun Microsystems' Jini. OpenSLP [OPENSLP] is an open source implementation of SLP.

SLP introduces three kinds of agent: the Service Agent (SA), the User Agent (UA) and the Directory Agent (DA). The UA queries the network to discover the location of a service. The SA listens for UA requests, which can be either multicast or unicast, and provides unicast responses to the UA. The DA is optional. If present, it periodically makes multicast announcements. In a very large network, SAs are required to register with DAs, and UAs interact with DAs instead of SAs. SLP specifies protocols for service request and reply messages, as well as messages defining service types, and security enhancements using digital signatures to verify message content.

## 8.10 Summary

Applications that benefit from multicast include videoconferencing, on-demand multimedia, support for collaborative work and for multi-user games, and information dissemination, including bulk data transfers to small numbers of recipients as well as smaller transfers to thousands or millions of recipients. Multicast also provides an effective mechanism for automatic software updating and for network and database synchronisation.

An important recent development is the Access Grid, a community based project that uses multicast to enable videoconferencing on a global scale, as well as data sharing, an element of mobility (using personal Access Grid nodes) and the study of issues related to remote collaboration.

## **9 Further Information/Getting Help**

General information on the use of IP Multicast with networks belonging to the UK JANET community can be located on the JANET web site [JANET].

Specific information concerning multicast of JANET is located at [MULTICAST].

### **9.1 Regional Network Connection Procedure and Support**

Requests for new multicast connections and general queries should be sent to JANET Customer Service (JCS) at [service@janet.ac.uk](mailto:service@janet.ac.uk). Please note that only Regional Network operations staff may make requests for new multicast connections.

### **9.2 Operational Queries and Fault Reporting**

Operational queries and fault reporting on existing multicast connections must be sent to the JANET Operations Desk (JOD) [JOD].

### **9.3 Customer Site Network Connection Procedure and Support**

Requests for new multicast connections to customer sites should be directed via the appropriate Regional Network.

### **9.4 Queries Related to the Use of Video over Multicast**

Queries related to the use of video over multicast should be directed to the staff of the JANET Video Technology Advisory Service (VTAS). This should be contacted via JCS at [service@janet.ac.uk](mailto:service@janet.ac.uk). JANET sites may contact VTAS via this route.



---

# Appendix A: Configuration Examples

## A.1 Introduction

In this appendix we present some simple configuration examples to assist readers in establishing basic multicast IP connectivity. This appendix is not intended in any way to replace manufacturer documentation, and in all but the simple cases we illustrate, readers must be prepared to consult detailed information from product manuals etc. We focus our attention mainly on Cisco® examples but we also draw some attention to issues we are aware of with other products. We assume that readers are familiar with general configuration of Cisco® routers. The Cisco® document *Multicast Quick-Start Configuration Guide* will be sufficient for readers in many straightforward circumstances. It can be located at:

<http://www.cisco.com/warp/public/105/48.html>

## A.2 Some Cisco®-Based Examples

In these examples, we assume that the recommendations given elsewhere in this guide have been adopted. In particular, we explain the extra commands that sites will need to use to configure SSM as well as ASM multicast, as both are likely to be needed at some time in the near future even if not immediately.

### A.2.1 Simple Non-RP Router Configuration

In this first scenario, we assume that a single RP is being used to serve all multicast IP addresses. The RP might be one operated by the site, or might be one operated by a Regional Network. In the examples, we assume this RP has 1.1.1.1 as its IP address.

We assume that this router is not at a boundary between its operator's network and that of another organisation.

The configuration of most of the routers in a network is fairly straightforward with respect to multicast. They merely require their PIM-SM multicast capabilities to be enabled and they need to be informed of the location of the network's RP.

*NOTE: we do not recommend readers use the Cisco® sparse-dense-mode as this can cause the network to drop all groups back to dense mode – a very bad idea – if an RP cannot be located. If readers do choose to use sparse-dense-mode then they should take appropriate precautions as recommended in the fine print of the Cisco® documentation.*

We firmly recommend the use of static specification of the RP address. The address given can either be the real IP address of the RP if only one exists, or the logical Anycast-RP address that has been chosen if Anycast-RP is in use. From a pragmatic viewpoint, static RP configuration is much easier to understand and troubleshoot or debug than alternatives such as auto-RP or Boot Strap Router (BSR).

To enable overall multicast capabilities it is only necessary to issue the global Cisco® IOS commands:

```
ip multicast-routing  
ip pim rp-address 1.1.1.1
```

Having issued that command, each interface present on the router over which the use of multicast IP is to be supported needs to be configured. This can be done by entering interface configuration mode for the appropriate interface and then issuing the command:

```
ip pim sparse-mode
```

The above really is all that is necessary to get ASM multicast IP working!

## A.2.2 Simple Non-RP Router Configuration with Local Multicast Groups

As mentioned in the body of this document, some sites are likely to decide that they would like to have local multicast groups so that they can run applications whose multicast traffic does not leave their site. To do this a site must establish its own RP for the local groups. We will assume that the site follows our recommendations and chooses to use the site-local administratively scoped addresses 239.255.0.0–239.255.255.255. We will assume that the site's RP serves just these addresses and that the Regional Network's RP is used for global group addresses.

The main difference between this example and the one in the previous subsection is that we now have to indicate which addresses are served by the site's RP and which are served by the Regional Network's RP. We will assume the Regional Network's RP has the IP address 1.1.1.1 and that the site's RP has the IP address 2.2.2.2.

On a Cisco® router, we are required to create two access lists to represent the internal and external addresses. In addition, while we may desire hosts with private unicast IP addresses to join into sessions using the internal groups, it would be quite inappropriate for them to join groups served by the Regional Network's RP. As we are now creating access lists, we might as well also set them so that they exclude the addresses allocated to SSM as that address range does not use RPs.

First, we define the access list 10 for the internal groups.

```
access-list 10 deny 232.0.0.0 0.255.255.255
access-list 10 permit 239.255.0.0 0.0.255.255
```

Now we create the access list 12 for the groups served by the external RP

```
access-list 12 deny 232.0.0.0 0.255.255.255
access-list 12 deny 239.255.0.0 0.0.255.255
access-list 12 permit 224.0.0.0 15.255.255.255
```

We now simply replace the single command **ip pim rp-address 1.1.1.1** as used in the example in the previous sub-section with two commands

```
ip pim rp-address 2.2.2.2 10
ip pim rp-address 1.1.1.1 12
```

## A.2.3 Adding Support for SSM

As mentioned above, we recommend that all sites consider configuring routers to support SSM multicast from the outset. Enabling SSM on a Cisco® router is easy if the standard multicast IP addresses for SSM, namely 232.0.0.0–232.255.255.255 are used. The commands needed are as follows.

```
ip pim ssm default
```

In addition to the above, IGMPv3 needs to be enabled on all the interfaces which have hosts connected. This can be done by entering interface configuration mode for the appropriate interface and then issuing the command:

```
ip igmp version 3
```

If the hosts attached to the router's interfaces do not themselves have full support for IGMPv3 in their operating systems, Cisco® does have some other solutions. Readers are advised to consult the following document:

```
http://www.cisco.com/en/US/tech/tk828/technologies\_design\_guide09186a00800c995a.shtml
```

## A.2.4 Simple RP Router Configuration

Cisco® routers are exceedingly simple from the viewpoint of them becoming the RP for a network. In many versions of the Cisco® IOS they report that you actually have to do nothing at all to configure them! If a router receives a (\*,G) PIM Join that indicates one of the router's own interface IP addresses as the RP address, then it just starts to behave as an RP.

However, if there is any chance that the RP may have directly connected hosts, then the commands as given in the above non-RP routers need to be issued and nothing is lost by having them anyway.

### A.2.4.1 An Isolated RP Serving Only Local Scoped Addresses

In this example we construct access lists so as to tell the RP to accept only attempts to use it as an RP for any addresses in the local scope, namely 239.255.0.0–239.255.255.255.

```
ip multicast-routing
access-list 10 deny 232.0.0.0 0.255.255.255
access-list 10 permit 239.255.0.0 0.0.255.255
ip pim rp-address 2.2.2.2 10
ip pim accept-rp 2.2.2.2 10
```

Having issued that command, each interface present on the router over which the use of multicast IP is to be supported needs to be configured. This can be done by entering interface configuration mode for the appropriate interface and then issuing the command:

```
ip pim sparse-mode
```

### A.2.4.2 An RP Serving All Groups Except Local Scoped Addresses and Also MSDP Peered with Another RP Higher Up the Hierarchy

In this example we construct access lists so as to tell the RP to refuse attempts to use it as an RP for any addresses in the local scope, namely 239.255.0.0–239.255.255.255.

```
ip multicast-routing
access-list 12 deny 232.0.0.0 0.255.255.255
access-list 12 deny 239.255.0.0 0.0.255.255
access-list 12 permit 224.0.0.0 15.255.255.255
ip pim rp-address 1.1.1.1 12
ip pim accept-rp 1.1.1.1 12
```

Having issued that command, each interface present on the router over which the use of multicast IP is to be supported needs to be configured. This can be done by entering interface configuration mode for the appropriate interface and then issuing the command:

```
ip pim sparse-mode
```

Now, we also wish to tell this RP to use another RP as an MSDP peer. We will assume that the other RP has IP address 3.3.3.3.

As discussed earlier in section 2.8.1, there are a large number of multicast group addresses which it is not appropriate to pass on via MSDP. In addition, if any local hosts are using the private addresses (as defined in RFC 1918) then their existence as sources should not be announced via MSDP. Thus, a fairly long access list needs to be constructed to control MSDP exchanges.

```
access-list 114 deny ip any host 224.0.1.2 ! SGI- Dogfight
access-list 114 deny ip any host 224.0.1.3 ! Rwhod
access-list 114 deny ip any host 224.0.1.8 ! SUN NIS +
access-list 114 deny ip any host 224.0.1.20 ! Any private experiment
access-list 114 deny ip any host 224.0.1.22 ! SVRLOC
```

```
access-list 114 deny ip any host 224.0.1.24 ! Microsoft-ds
access-list 114 deny ip any host 224.0.1.25 ! nbc-pro
access-list 114 deny ip any host 224.0.1.35 ! SVRLOC-DA
access-list 114 deny ip any host 224.0.1.39 ! cisco-rp-announce
access-list 114 deny ip any host 224.0.1.40 ! cisco-rp-discovery
access-list 114 deny ip any host 224.0.1.60 ! hp-device-disc
access-list 114 deny ip any host 224.0.1.76 ! IAPP – wireless base-station comms
access-list 114 deny ip any host 224.0.2.1 ! RWHO
access-list 114 deny ip any host 224.0.2.2 ! SUN RPC
access-list 114 deny ip any host 224.0.2.3 ! EPSON-disc-set
access-list 114 deny ip any host 224.0.23.1 ! Ricoh-device-ctrl
access-list 114 deny ip any host 224.0.23.2 ! Ricoh-device-ctrl
access-list 114 deny ip any 224.77.0.0 0.0.255.255 ! Norton Ghost
access-list 114 deny ip any host 225.1.2.3 ! Altiris
access-list 114 deny ip any 226.77.0.0 0.0.255.255 ! Norton Ghost
access-list 114 deny ip any host 229.55.150.208 ! Norton Ghost
access-list 114 deny ip any 234.42.42.40 0.0.0.252 ! Imagecast disk duplication
access-list 114 deny ip any host 234.142.142.142 ! Imagecast disk duplication
access-list 114 deny ip any 239.255.0.0 0.0.255.255 ! Site-local scope
access-list 114 deny ip any 232.0.0.0 0.255.255.255 ! SSM addresses
access-list 114 deny ip 10.0.0.0 0.255.255.255 any ! private address space
access-list 114 deny ip 127.0.0.0 0.255.255.255 any ! loopback network
access-list 114 deny ip 172.16.0.0 0.15.255.255 any ! private address space
access-list 114 deny ip 192.168.0.0 0.0.255.255 any ! private address space
access-list 114 permit ip any any
```

Having now constructed access list 114, we can use it to control MSDP behaviour. We now have the MSDP peering commands etc. We assume that the IP address corresponding to interface FastEthernet0/0 is the local address for MSDP traffic.

```
ip msdp peer 3.3.3.3 connect-source FastEthernet0/0
ip msdp sa-request 3.3.3.3
ip msdp sa-filter in 3.3.3.3 list 114
ip msdp sa-filter out 3.3.3.3 list 114
ip msdp redistribute list 114
ip msdp cache-sa-state
ip msdp default-peer 3.3.3.3
```

The RPF rules for MSDP are non-trivial. However, as this RP has only one MSDP peer, it must be the right RP for any external sources. Thus, the final command above makes sure that RPF checks will work as intended.

## A.2.5 Making Sure Multicast RPF Checks Work Correctly

Many sites use static, rather than dynamic, routing between themselves and the serving Regional Network. In such environments, to make sure that all RPF checks work correctly, it is sensible to also add manual multicast routes. If we assume two local networks 4.4.0.0/16 and 5.5.5.0/24 are reachable via interfaces FastEthernet1/0 and FastEthernet2/0 and that the rest of the Internet is reached via an external router with IP address 6.6.6.6, then the following commands would be appropriate.

```
ip mroute 4.4.0.0 255.255.0.0 FastEthernet1/0
ip mroute 5.5.5.0 255.255.255.0 FastEthernet2/0
ip mroute 0.0.0.0 0.0.0.0 6.6.6.6
```

## A.2.6 Establishing Scoped Boundaries

Earlier sections have talked about administratively scoped addresses. Clearly, if addresses are to be used in this way then the specifications of the boundaries need to be defined.

Multicast boundaries on specified interfaces on Cisco® routers can be set by defining ACLs and informing the router that these should be used. As mentioned earlier, the site-local addresses (239.255/16) ought to be blocked at the boundary between a Regional Network and the JANET backbone. Assuming the interface that leads from the Regional Network router to the BAR were Ethernet interface 0 then this can be achieved as follows:

```
access-list 1 deny 239.255.0.0 0.0.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
interface ethernet 0
ip multicast boundary 1
```

Similar boundaries should be established on routers that connect sites to Regional Networks.

## A.2.7 Configuring Boundary Routers

At routers which are boundary routers between one organisation's network and another's it is essential that certain multicast traffic, typically associated with applications that only have local significance, is filtered.

In addition, any packets with private IP source addresses should be filtered as should packets sent to the site-local administratively scoped addresses.

Finally, we should configure a block for any packets concerned with the selection of RPs by bootstrap router protocol, even if this is not consciously being used on the site.

Assuming the interface that leads from the current router to the adjacent network were Ethernet interface 1 then this can be achieved as follows:

```
access-list 116 deny ip any host 224.0.1.2 ! SGI- Dogfight
access-list 116 deny ip any host 224.0.1.3 ! Rwhod
access-list 116 deny ip any host 224.0.1.8 ! SUN NIS +
access-list 116 deny ip any host 224.0.1.20 ! Any private experiment
access-list 116 deny ip any host 224.0.1.22 ! SVRLOC
access-list 116 deny ip any host 224.0.1.24 ! Microsoft-ds
access-list 116 deny ip any host 224.0.1.25 ! nbc-pro
access-list 116 deny ip any host 224.0.1.35 ! SVRLOC-DA
access-list 116 deny ip any host 224.0.1.39 ! cisco-rp-announce
access-list 116 deny ip any host 224.0.1.40 ! cisco-rp-discovery
access-list 116 deny ip any host 224.0.1.60 ! hp-device-disc
access-list 116 deny ip any host 224.0.1.76 ! IAPP – wireless base-station comms
access-list 116 deny ip any host 224.0.2.1 ! RWHO
access-list 116 deny ip any host 224.0.2.2 ! SUN RPC
access-list 116 deny ip any host 224.0.2.3 ! EPSON-disc-set
access-list 116 deny ip any host 224.0.23.1 ! Ricoh-device-ctrl
access-list 116 deny ip any host 224.0.23.2 ! Ricoh-device-ctrl
access-list 116 deny ip any 224.77.0.0 0.0.255.255 ! Norton Ghost
access-list 116 deny ip any host 225.1.2.3 ! Altiris
access-list 116 deny ip any 226.77.0.0 0.0.255.255 ! Norton Ghost
access-list 116 deny ip any host 229.55.150.208 ! Norton Ghost
access-list 116 deny ip any 234.42.42.40 0.0.0.252 ! Imagecast disk duplication
access-list 116 deny ip any host 234.142.142.142 ! Imagecast disk duplication
access-list 116 deny ip any 239.255.0.0 0.0.255.255 ! Site-local scope
access-list 116 deny ip 10.0.0.0 0.255.255.255 any ! private address space
access-list 116 deny ip 127.0.0.0 0.255.255.255 any ! loopback network
access-list 116 deny ip 172.16.0.0 0.15.255.255 any ! private address space
access-list 116 deny ip 192.168.0.0 0.0.255.255 any ! private address space
```

```
access-list 116 permit ip any any
interface ethernet 1
ip multicast boundary 116
ip pim bsr-border
```

## A.2.8 Cisco® Performance Enhancements

Some versions of Cisco® IOS on some models of router can support multicast fast switching with hardware support. Various commands including the following are associated with this feature. Readers should check for compatibility with their router IOS versions and router model number before enabling these features.

```
ip multicast-routing distributed
ip route-cache distributed
ip mroute-cache distributed
```

## A.3 Multicast on Juniper Networks J-, M- and T-Series Routers

This section is a small 'How to' on getting Multicast running on Juniper routers. It currently only covers IPv4 networks, though it has some mentions of IPv6.

This appendix is not intended in any way to replace manufacturer documentation; readers must be prepared to consult detailed information from product manuals.<sup>1</sup>

### A.3.1 Multicast Support on J-, M- and T-Series Routers

All J, M and T-Series routers of Juniper Networks run the JUNOS modular operating system. For the full, official list for JUNOS Multicast features, see the list of supported multicast specifications in JUNOS documentation.

As a summary, JUNOS supports the following:

PIM-SM (IPv4 and IPv6), PIM-DM, PIM-Sparse-Dense, PIM-SSM (IPv4 and IPv6), DVMRP, IGMPv1/2/3, MLDv1/2, MSDP, SAP, MBGP, MISIS (IPv4-mcast and IPv6-mcast), Embedded RP, AutoRP, BSR, Mtrace.

Unicast and multicast forwarding is performed on M and T-Series by dedicated ASICs. On J-Series, the packet forwarding is assisted by standard-hardware network processors.

A services Physical Interface Card (Tunnel, LS or AS PIC) is needed in JUNOS to encapsulate and decapsulate PIM register messages, which are sent by the source's Designated Router (DR) to the Rendezvous Point (RP). Any router that is a source DR or RP will need a service PIC, which provides hardware encapsulation/decapsulation, protecting the system from potential attack based on a high rate of PIM registers from a misbehaving/misconfigured/malicious DR.

If, however, the source DR is the RP, then no register messages need to be created or sent anywhere. So one workaround for the service PIC-impaired is to make all the DRs into RPs (typically anycast) and run a full mesh of MSDP to all of these. M7i's have a tunnel PIC built in and J-series handles this in software, so no service PICs are needed on M7i or J-series. For all other M/T-Series boxes, a PIC is needed.

In the case of IPv6, an IPv6 source DR will send PIM Null-Register Messages instead of Register Messages in JUNOS. Therefore, an IPv6 DR doesn't need a tunnel PIC; however an IPv6 RP still does need a tunnel PIC.

---

1. <http://www.juniper.net/techpubs/software/junos/junos76/swconfig76-multicast/frameset.htm>

Administrative scoping, as defined in RFC 2365, can be achieved using scoping. Access control can be provided by PIM policy, BSR Policy and MSDP policy. For a full description of the JUNOS filtering and security features, see the JUNOS best practices guide to securing a multicast infrastructure.<sup>2</sup>

The default SPT shortest path tree threshold is 0. This means the receiver's DR will switch to the shortest path tree upon receiving the first packet down the shared tree.

JUNOS supports three ways to inform routers of the RP's address:

1. static
2. AutoRP
3. BSR.

## A.3.2 Configuring PIM Sparse Mode

By default, PIM uses inet.0 as its reverse-path-forwarding (RPF) routing table group. PIM uses an RPF routing table group to resolve its RPF neighbour for a particular multicast source address and to resolve the RPF neighbour for the RP address. PIM can optionally use inet.2 as its RPF routing table group. To do this, add the rib-group statement to the [routing-options] hierarchy level, and then name the routing table group in the pim statement (see section A3.6 for an example with inet.2 usage).

The following example shows a configuration for the RP router and for non-RP routers.

### A.3.2.1 Configuring the RP Router

This example shows a static RP configuration. Add the address statement at the [edit protocols pim rp local] hierarchy level.

For all interfaces, use the mode statement to set the mode to sparse, and use the version statement to set the PIM version to 2 at the [edit protocols PIM rp interface all] hierarchy level. When configuring all interfaces, exclude the fxp0.0 management interface by adding the disable statement for that interface.

```
[edit]
protocols {
  pim {
    rp {
      local {
        address 198.58.3.253;
      }
      interface all {
        mode sparse;
        version 2;
      }
      interface fxp0.0 {
        disable;
      }
    }
  }
}
```

NOTE: You do not need to configure IGMP version 2 for a sparse mode configuration. When PIM is enabled, IGMP version 2 is also enabled by default.

2. [http://www.juniper.net/solutions/literature/app\\_note/350051.pdf](http://www.juniper.net/solutions/literature/app_note/350051.pdf)

### A.3.2.2 Configuring All Non-RP Routers

In this example, we configure a non-RP router for PIM sparse mode. To specify a static RP address, add the address statement at the [edit protocols pim rp static] hierarchy level. Use the version statement at the [edit protocols pim rp static address] hierarchy level to specify PIM version 2.

Add the mode statement at the [edit protocols pim interface all] hierarchy level to configure the interfaces for sparse mode operation. Then add the version statement at the [edit protocols pim interface all mode] to specify PIM version 2 for all interfaces. When configuring all interfaces, exclude the fxp0.0 management interface by adding the disable statement for that interface.

```
[edit]
protocols {
  pim {
    rp {
      static {
        address 198.58.3.253 {
          version 2;
        }
      }
    }
    interface all {
      mode sparse;
      version 2;
    }
    interface fxp0.0 {
      disable;
    }
  }
}
```

### A.3.3 Configuring Source-Specific Multicast

SSM is typically supported with a subset of IGMPv3 and PIM sparse mode known as PIM SSM. Using SSM, a client can receive multicast traffic directly from the source.

PIM SSM uses the PIM sparse mode functionality to create an SPT between the client and the source, but builds the SPT without the help of an RP.

By default, the SSM group multicast address is limited to the IP address range 232.0.0.0 to 232.255.255.255. However, you can extend SSM operations into another Class D range by including the address statement at the [edit routing-options multicast ssm-groups] hierarchy level.

To enable IGMPv3 on all host-facing interfaces, include the version 3 statement under the interface all statement at the [edit protocols igmp] hierarchy level:

```
[edit protocols igmp]
interface all {
  version 3;
}
interface fxp0.0 {
  disable;
}
```



If the hosts attached to the router's interfaces do not themselves have full support for IGMPv3, SSM mapping feature translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report. This allows hosts running IGMPv1/IGMPv2 to participate in SSM until the hosts transition to IGMPv3.

### A.3.4 Configuring PIM Join Filters

Multicast scopes prevent multicast data packets from flowing into or out of an interface. PIM join filters prevent the creation of PIM-SM state so multicast traffic is not transmitted across your network and dropped at a scope at the edge. Also, PIM join filters reduce the potential for denial-of-service attacks and PIM state explosion. PIM join filters only apply to PIM-SM state. If you use them, apply them to all routers in your network. The following configuration will reject PIM joins sent by neighbours for groups that do not belong on the Internet. This same configuration permits PIM joins to flow over backbone links, which is necessary on networks that allow 239/8 traffic for internal purposes.

```

protocols {
  pim {
    import pim-join-filter;
  }
}
policy-options {
  policy-statement pim-join-filter {
    term permit-239-on-backbone {
      from {
        interface [ so-0/0/0.0 so-1/0/0.0 ];
        route-filter 239.0.0.0/8 orlonger;
      }
      then accept;
    }
    term bad-groups {
      from {
        route-filter 224.0.1.2/32 exact;
        route-filter 224.0.1.3/32 exact;
        route-filter 224.0.1.8/32 exact;
        route-filter 224.0.1.20/32 exact;
        route-filter 224.0.1.22/32 exact;
        route-filter 224.0.1.24/32 exact;
        route-filter 224.0.1.25/32 exact;
        route-filter 224.0.1.35/32 exact;
        route-filter 224.0.1.39/32 exact;
        route-filter 224.0.1.40/32 exact;
        route-filter 224.0.1.60/32 exact;
        route-filter 224.0.1.76/32 exact;
        route-filter 224.0.2.1/32 exact;
        route-filter 224.0.2.2/32 exact;
        route-filter 224.0.2.3/32 exact;
        route-filter 224.0.23.1/32 exact;
        route-filter 224.0.23.2/32 exact;
        route-filter 224.77.0.0/16 orlonger;
        route-filter 225.1.2.3/32 exact;
        route-filter 226.77.0.0/16 orlonger;
        route-filter 229.55.150.208/32 exact;
        route-filter 234.42.42.40/30 orlonger;
        route-filter 239.255.0.0/16 orlonger;
      }
      then reject;
    }
  }
}

```

```
    }
    term bad-sources {
      from {
        source-address-filter 10.0.0.0/8 orlonger;
        source-address-filter 127.0.0.0/8 orlonger;
        source-address-filter 172.16.0.0/12 orlonger;
        source-address-filter 192.168.0.0/16 orlonger;
      }
      then reject;
    }
    term accept-everything-else {
      then accept;
    }
  }
}
```

### A.3.5 Multicast Boundaries

Apply multicast boundary filters on all customer-facing interfaces by using multicast scoping. Multicast scoping prevents multicast packets from flowing into or out of an interface. Apply these scopes on all interfaces and on all routers in your network, since there is usually no good reason for these groups to flow on backbone links. The following configuration prevents multicast data packets from flowing into or out of all interfaces on the router for groups that do not belong on the Internet. This configuration also permits data packets in 239/8 to flow over backbone links, which is necessary on networks that allow 239/8- traffic for internal purposes.

```
routing-options {
  multicast {
    scope-policy boundary-filter;
  }
}
policy-options {
  policy-statement boundary-filter {
    term permit-239-on-backbone {
      from {
        interface [ so-0/0/0.0 so-1/0/0.0 ];
        route-filter 239.0.0.0/8 orlonger;
      }
      then accept;
    }
  }
  term bad-groups {
    from {
      route-filter 224.0.1.2/32 exact;
      route-filter 224.0.1.3/32 exact;
      route-filter 224.0.1.8/32 exact;
      route-filter 224.0.1.20/32 exact;
      route-filter 224.0.1.22/32 exact;
      route-filter 224.0.1.24/32 exact;
      route-filter 224.0.1.25/32 exact;
      route-filter 224.0.1.35/32 exact;
      route-filter 224.0.1.39/32 exact;
      route-filter 224.0.1.40/32 exact;
      route-filter 224.0.1.60/32 exact;
      route-filter 224.0.1.76/32 exact;
      route-filter 224.0.2.1/32 exact;
```

```

route-filter 224.0.2.2/32 exact;
route-filter 224.0.2.3/32 exact;
route-filter 224.0.23.1/32 exact;
route-filter 224.0.23.2/32 exact;
route-filter 224.77.0.0/16 orlonger;
route-filter 225.1.2.3/32 exact;
route-filter 226.77.0.0/16 orlonger;
route-filter 229.55.150.208/32 exact;
route-filter 234.42.42.40/30 orlonger;
route-filter 239.255.0.0/16 orlonger;
}
then reject;
}
term accept-everything-else {
then accept;
}
}
}
}

```

### A.3.6 Configuring MSDP

Configure a router to act as a PIM sparse-mode rendezvous point and an MSDP peer:

```

[edit]
routing-options {
interface-routes {
rib-group ifrg;
}
rib-groups {
ifrg {
import-rib [inet.0 inet.2];
}
mcrp {
export-rib inet.2;
import-rib inet.2;
}
}
}
}
protocols
bgp {
group lab {
type internal;
family any;
neighbor 192.168.6.18 {
local-address 192.168.6.17;
}
}
}
}
pim {
dense-groups {
224.0.1.39/32;
224.0.1.40/32;
}
rib-group mcrp;
rp {
local {

```

```
        address 192.168.1.1;
    }
}
interface all {
    mode sparse-dense;
    version 1;
}
}
msdp {
    rib-group mcrg;
    group lab {
        peer 192.168.6.18 {
            local-address 192.168.6.17;
        }
    }
}
}
```

### A.3.7 References

JUNOSTM Internet Software for J-seriesTM, M-seriesTM, and T-seriesTM Routing Platforms: Multicast Protocols Configuration Guide  
<http://www.juniper.net/techpubs/software/junos/junos76/swconfig76-multicast/frameset.htm>

Understanding and Implementing Multicast Services  
[http://www.juniper.net/solutions/literature/app\\_note/350034.pdf](http://www.juniper.net/solutions/literature/app_note/350034.pdf)

Calm During the Storm: Best Practices in Multicast Security  
[http://www.juniper.net/solutions/literature/app\\_note/350051.pdf](http://www.juniper.net/solutions/literature/app_note/350051.pdf)

*Interdomain Multicast Routing, Practical Juniper Networks and Cisco Systems Solutions* (Addison Wesley 2002), Brian Edwards, Leonard A. Giuliano, and Brian Wright  
<http://www.juniper.net/training/jnbooks/0-201-74612-3.html>

## A.4 The XORP Public Domain Multicast Router

Xorp, eXtensible Open Router Platform, is intended to be ‘an open router software platform’. Xorp currently lacks an implementation of MSDP. At the time of writing, the Xorp project has just released version 1.2.

Further information about it can be located at:

<http://www.xorp.org>

While not promoting either of these products as being appropriate for use within a service infrastructure, some readers may find knowledge of their existence useful.

### Example XORP Configuration file

The following is a real XORP configuration file, making use of PIM-SM for a router with four interfaces. The router is internal to a campus, feeding several departmental subnets and connects upstream to the central router, which itself then connects onwards to a regional network. The first two octets of the IP addresses used have been replaced by XX or YY in this example to preserve anonymity. Interface eth4 leads to the upstream central router which has IP address YY.YY.35.253, our address on that interface being YY.YY.34.30. The network YY.YY is a class B network but has been sub-netted with 22 bits in the prefix. The other networks are class C. The file is based on the sample configuration file provided with the release candidate for version 1.2 of XORP.

```
/* $XORP: xorp/rtrmgr/config.boot.sample,v 1.33 2005/10/28 18:55:34 pavlin Exp $
*/

interfaces {
  restore-original-config-on-shutdown: false
  interface eth1 {
    description: "AI Interface"
    disable: false
    /* default-system-config */
    vif eth1 {
      disable: false
      address XX.XX.10.90 {
        prefix-length: 24
        broadcast: XX.XX.10.255
        disable: false
      }
    }
  }
  interface eth2 {
    description: "SEG Interface"
    disable: false
    /* default-system-config */
    vif eth2 {
      disable: false
      address XX.XX.11.33 {
        prefix-length: 24
        broadcast: XX.XX.11.255
        disable: false
      }
    }
  }
  interface eth3 {
    description: "Teaching Interface"
    disable: false
    /* default-system-config */
    vif eth3 {
      disable: false
      address XX.XX.15.40 {
        prefix-length: 24
        broadcast: XX.XX.15.255
      }
      disable: false
    }
  }
  interface eth4 {
    description: "Upstream Interface"
    disable: false
    /* default-system-config */
    vif eth4 {
      disable: false
      address YY.YY.34.30 {
        prefix-length: 22
        broadcast: YY.YY.35.255
        disable: false
      }
    }
  }
}
```

```
interface discard0 {
  description: "discard interface"
  disable: false
  discard: true
  vif discard0 {
    disable: false
    address 192.0.2.1 {
      prefix-length: 32
      disable: false
    }
  }
}
```

```
fea {
  unicast-forwarding4 {
    disable: true
  }
}
```

```
protocols {
  static {
    route4 0.0.0.0/0 {
      metric: 1
      next-hop: YY.YY.35.253
    }
    mrib-route4 0.0.0.0/0 {
      metric: 1
      next-hop: YY.YY.35.253
    }
  }
}
```

```
plumbing {
  mfea4 {
    disable: false
    interface eth1 {
      vif eth1 {
        disable: false
      }
    }
    interface eth2 {
      vif eth2 {
        disable: false
      }
    }
    interface eth3 {
      vif eth3 {
        disable: false
      }
    }
    interface eth4 {
      vif eth4 {
        disable: false
      }
    }
  }
}
```

```
interface register_vif {
  vif register_vif {

      /* Note: this vif should be always enabled */
      disable: false
  }
}
traceoptions {
  flag all {
    disable: true
  }
}
}
protocols {
  igmp {
    disable: false
    interface eth1 {
      vif eth1 {
        disable: false
        /* version: 2 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */
        /* query-response-interval: 10 */
        /* robust-count: 2 */
      }
    }
    interface eth2 {
      vif eth2 {
        disable: false
        /* version: 2 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */
        /* query-response-interval: 10 */
        /* robust-count: 2 */
      }
    }
    interface eth3 {
      vif eth3 {

        disable: false
        /* version: 2 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */
        /* query-response-interval: 10 */
        /* robust-count: 2 */
      }
    }
    interface eth4 {
      vif eth4 {
        disable: false
        /* version: 2 */
        /* enable-ip-router-alert-option-check: false */
        /* query-interval: 125 */
        /* query-last-member-interval: 1 */

```

```
        /* query-response-interval: 10 */
        /* robust-count: 2 */
    }
}
traceoptions {
    flag all {
        disable: true
    }
}
}
}

protocols {
    pimsm4 {
        disable: false
        interface eth1 {
            vif eth1 {
                disable: false
                /* enable-ip-router-alert-option-check: false */
                /* dr-priority: 1 */
                /* hello-period: 30 */
                /* hello-triggered-delay: 5 */

                /* alternative-subnet 10.40.0.0/16 */
            }
        }
        interface eth2 {
            vif eth2 {
                disable: false
                /* enable-ip-router-alert-option-check: false */
                /* dr-priority: 1 */
                /* hello-period: 30 */
                /* hello-triggered-delay: 5 */
                /* alternative-subnet 10.40.0.0/16 */
            }
        }
        interface eth3 {
            vif eth3 {
                disable: false
                /* enable-ip-router-alert-option-check: false */
                /* dr-priority: 1 */
                /* hello-period: 30 */
                /* hello-triggered-delay: 5 */
                /* alternative-subnet 10.40.0.0/16 */
            }
        }
        interface eth4 {
            vif eth4 {
                disable: false
                /* enable-ip-router-alert-option-check: false */
                /* dr-priority: 1 */
                /* hello-period: 30 */
                /* hello-triggered-delay: 5 */
                /* alternative-subnet 10.40.0.0/16 */
            }
        }
        interface register_vif {
            vif register_vif {
                /* Note: this vif should be always enabled */
            }
        }
    }
}
```



```

        disable: false
    }
}

static-rps {
    rp 193.61.213.3 {
        group-prefix 224.0.0.0/4 {
            /* rp-priority: 192 */
            /* hash-mask-len: 30 */
        }
    }
}

switch-to-spt-threshold {
    /* approx. 1K bytes/s (10Kbps) threshold */
    disable: false
    interval-sec: 100
    bytes: 102400
}

traceoptions {
    flag all {
        disable: true
    }
}
}

/*
 * Note: fib2mrib is needed for multicast only if the unicast protocols
 * don't populate the MRIB with multicast-specific routes.
 */
protocols {
    fib2mrib {
        disable: false
    }
}

/*
 * See xorp/mibs/snmpdscripts/README on how to configure Net-SNMP in your
 * host
 * before uncommenting the snmp section below.
 * Also check that the "bgp4_mib_1657.so" exists in the correct location.
 */

/*
protocols {
    snmp {
        mib-module bgp4_mib_1657 {
            abs-path: "/usr/local/xorp/mibs/bgp4_mib_1657.so"
        }
    }
}
*/

```

## Appendix B: Translating IP Multicast Addresses to Ethernet Group Addresses

The text in this appendix is based on words kindly provided by Gorry Fairhurst.

For IPv4 multicast, the Ethernet MAC group destination address is formed by using the lowest 23 bits of the IP Multicast address and a prefix of (01:00:5E). The mapping of the 28-bit IP Multicast group to the 23-bit LAN address space results in a 5-bit overlap. This overlap means 32 IP Multicast addresses map to the same MAC group address. This may cause a NIC to forward received IP packets to the end host operating system with an IP Multicast address that was not wanted. In this case, the operating system filters (discards) the unwanted IP packets. IPv6 packets are mapped in a similar way, by copying the lower 32 bits of the IPv6 group destination address and using a prefix of 33:33, instead of 01:00:5E. The appearance of a multicast address on the cable is shown below (bits transmitted from left to right). Note that, confusingly, the bit-order of transmission in Ethernet means that first bit sent on a wire/fibre is actually the least significant bit of the first byte.

```

0           23 IP Multicast Address Group 47
|           | <----->|
1000 0000 0000 0000 0111 1010 xxxx xxx0 xxxx xxxx xxxx xxxx
|           |
Multicast Bit      0 = Internet Multicast
                   1 = Assigned for other uses
    
```

### Mapping an IPv4 multicast network address to an Ethernet LAN group address

Apart from using a MAC destination address mapped from the IP group address, an IP multicast packet is a standard Ethernet frame. (N.B. The use of a group address in the source address is illegal for both Ethernet and IP.)

## Appendix C: Multicast Security

### C.1 Multicast Security as Reported in the Literature

In order to get a feel for the actual security of multicast, the CERT vulnerability database and other CERT web pages were searched for multicast vulnerabilities. The results are summarised here and the details can be found below. (The searches were carried out on 10 February 2006.)

The US-CERT vulnerability database at

**<http://www.kb.cert.org/vuls>**

was searched with the search string 'multicast'. There were just five hits: one from 1998, one from 2003 and three from 2004. These describe vulnerabilities in software that in most cases is peripheral to multicast technology.

The CERT/CC 'red page' at

**[http://www.cert.org/nav/index\\_red.html](http://www.cert.org/nav/index_red.html)**

was searched, again with the search string 'multicast', under various categories.

In the category of Vulnerability Notes there were six hits; the same five as found in the US-CERT vulnerability database plus information about a bug in which implicit multicast IPv4 network addresses were not fully handled.

In the category of Advisories there were two hits; one from 1998 on Smurf IP denial-of-service attacks and one from 2001 on a buffer overflow in the UPnP service on Microsoft Windows.

In the categories of Research and of Security Improvement Modules there were three hits each, and in the category of Other CERT Docs there were seven hits. There were no hits in Tech Tips nor in Training and Education.

Furthermore, a Google search for 'multicast vulnerabilities' produced only three genuine hits (although searching for 'multicast' + 'vulnerabilities' produced about 155,000 hits).

The very limited number of finds as a result of these searches suggests that there are very few exploits of multicast vulnerabilities to date.

### C.2 Multicast Security Searches

The remainder of this appendix contains the result of searches carried out on 10 February 2006.

#### C.2.1 <http://www.kb.cert.org/vuls>

Search string 'multicast' produced five hits.

**Sun Solaris SSH Daemon fails to properly log client IP addresses**  
VU#737548 2004-04-07

The text 'MULTICAST' occurs in some ifconfig examples.

**Ethereal integer underflow when parsing malformed PGM packets with NAK lists**  
VU#433596 2004-03-22

Overview: 'Ethereal fails to properly parse Pragmatic General Multicast (PGM) packets containing a crafted negative acknowledgement (NAK) list'.

**Microsoft Windows Media Services fails to properly validate TCP requests**

VU#982630 2004-03-09

Workarounds: 'Block ports 7007 and 7778 at your firewall. If you block port 7007, you will prevent multicast streams and the enabling of playlists from functioning across the firewall. ...'

**Microsoft Windows Media Services contains buffer overflow in 'nsiislog.dll'**

VU#113716 2003-06-25

Overview: 'Microsoft Windows Media Services provides streaming audio and video capabilities. A vulnerability in a component of this software could allow a remote attacker to compromise the server running it'.

**Hot Standby Router Protocol (HSRP) uses weak authentication**

VU#228186 1998-03-01

Overview: 'A denial-of-service vulnerability exists in the Hot Standby Router Protocol (HSRP). HSRP-enabled routers operate by exchanging multicast messages amongst themselves that advertise their priority levels. ...'

## C.2.2 [http://www.cert.org/nav/index\\_red.html](http://www.cert.org/nav/index_red.html)

Search string 'multicast'

### (i) Search area: Vulnerability Notes

Six hits: the five above, plus:

**Internet Software Consortium Information for VU#734644**

2004-01-04 '... 1580. [bug] inet\_net\_pton() didn't fully handle implicit multicast IPv4 network addresses. ...' <http://www.kb.cert.org/vuls/id/JPLA-5SJT44>

### (ii) Search area: Advisories

Two hits:

**CERT Advisory CA-2001-37 Buffer Overflow in UPnP Service On Microsoft Windows**

2001-12-20

'... Note that Microsoft Internet Connection Firewall, which runs by default on Windows XP, does not provide complete protection against this attack. Specifically, an intruder can still use a broadcast or multicast address to reach the UPnP service on Microsoft Windows. On systems that don't require UPnP, it can be disabled. ...' <http://www.cert.org/advisories/CA-2001-37.html>

**CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks**

1998-01-05

'... In FreeBSD 2.2.5 and up, the tcp/ip stack does not respond to icmp echo requests destined to broadcast and multicast addresses by default. This behaviour can be changed via the sysctl command via mib net.inet.icmp.bmcastecho. ...' <http://www.cert.org/advisories/CA-1998-01.html>

### (iii) Search area: Research

Three hits (all showed the same date of 2006-01-19, which is clearly wrong):

**On Survivable Multi-Networks for Information Systems Survivability, ISW'98 no.39**

2006-01-19

'... layout of survivable multipoint (aka multicast) group communications in

connection oriented (i.e. ... Self-Healing Virtual Ring (SHVR) multicast and consists of two counter-rotating ...'

[http://www.cert.org/research/isw/isw98/all\\_the\\_papers/no39.html](http://www.cert.org/research/isw/isw98/all_the_papers/no39.html)

**Survivability Issues for Evolvable Real-time Command and Control Systems:  
A Position Paper**

2006-01-19 'Fault-Tolerance: The RTIS should support fault-tolerance by providing group communication services (reliable multicast, atomic multicast, causal multicast, and group membership services)'

[http://www.cert.org/research/isw/isw97/all\\_the\\_papers/no17.html](http://www.cert.org/research/isw/isw97/all_the_papers/no17.html)

**Internet Characteristics**

2006-01-19

This thesis chapter contains a table of IP addressing schemes.

<http://www.cert.org/research/JHThesis/Chapter2.html>

**(iv) Search area: Security Improvement Modules**

Three hits:

**Installing and securing Solaris 2.6 servers**

2005-10-05

<http://www.cert.org/security-improvement/implementations/i027.02.html>

**Protect your Web server against common attacks**

2001-05-02

<http://www.cert.org/security-improvement/practices/p082.html>

**Installing and operating tcpdump 3.5.x on systems running Solaris 2.x**

2000-11-21

<http://www.cert.org/security-improvement/implementations/i042.13.html>

**(v) Search area: Tech Tips**

No hits

**(vi) Search area: Training and Education**

No hits

**(vii) Search area: Other CERT Docs**

Seven hits:

**Infosec Outlook**

2006-01-25

[http://www.cert.org/infosec-outlook/infosec\\_1-1.html](http://www.cert.org/infosec-outlook/infosec_1-1.html)

**CERT Coordination Center Reports**

2006-01-25

[http://www.cert.org/congressional\\_testimony/Fithen\\_testimony\\_Feb29.html](http://www.cert.org/congressional_testimony/Fithen_testimony_Feb29.html)

**Microsoft PowerPoint – FlowCon2005Qosient.ppt**

2005-10-10

<http://www.cert.org/flocon/2005/presentations/FlowCon2005Qosient.pdf>

**Microsoft PowerPoint – IP Flow Information eXport.ppt**

2005-10-10

[http://www.cert.org/flocon/2005/presentations/ipflow\\_infexport.pdf](http://www.cert.org/flocon/2005/presentations/ipflow_infexport.pdf)

**Microsoft Word – FRGCF\_v1.3.doc**

2005-10-10

[http://www.cert.org/archive/pdf/FRGCF\\_v1.3.pdf](http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf)

**Systems Quality Requirements Engineering (SQUARE) Methodology:  
Case Study**

2005-01-27

[http://www.cert.org/archive/pdf/SQUARE\\_Asset.pdf](http://www.cert.org/archive/pdf/SQUARE_Asset.pdf)

**infosec 1-1**

2000-04-07

[http://www.cert.org/infosec-outlook/infosec\\_1-1.pdf](http://www.cert.org/infosec-outlook/infosec_1-1.pdf)

### C.2.3 Google search for ‘multicast vulnerabilities’

Three genuine hits (plus two which appeared to be random collections of words, not investigated):

**18th APAN Meetings/QUESTnet 2004 in Cairns**

2004.7.2-7, Cairns, Australia

<http://apan.net/meetings/cairns2004/ws/application.htm>

Access Grid & HDTV session (1 slot )

3. Jinyong Jo and Okhwan Byeon, KISTI

Topic : Multicast monitoring system for Access Grid

‘... The aim is to provide a user-oriented monitoring system diagnosing multicast vulnerabilities. ...’

**Iolus: A Framework for Scalable Secure Multicasting**

(no date)

<http://discovery.csc.ncsu.edu/~pning/Courses/csc774-S03/Presentations/01-Iolus.pdf>

(slide presentation)

**DShield – Distributed Intrusion Detection System**

(no date)

[http://www.dshield.org/port\\_report.php?port=1674](http://www.dshield.org/port_report.php?port=1674)

(Example results from an IDS tool – the juxtaposition of ‘multicast’ and ‘vulnerabilities’ appears to be an accident.)

A Google search for ‘multicast’ + ‘vulnerabilities’ produced about 155,000 hits (including the above three, of course) which were not investigated further.

## Appendix D: Bibliography

The bibliography contains a wide range of items of several types. In an attempt to add some consistency to presentation and to structure the material so it is easy to locate by the reader it is presented in several subsections.

In addition to items mentioned in the main body of the text of this document, the bibliography also includes other items, e.g. many RFCs that are not directly discussed elsewhere.

### D.1 Books and Journals

[ADAMS] Adams B. et al. *Interdomain Multicast Solutions Guide*, ISBN 1-58705-083-8, Cisco Press, 2002.

[BROWN1998] Brown S, JANET MBONE Service Technical Guide version 3.4, UKERNA, March 1998.

[BROWN2002] Brown I. et al. Internet Multicast Tomorrow, *The Internet Protocol Journal*, Volume 5, Issue 4, Dec. 2002.

[http://www.cisco.com/warp/public/759/ipj\\_5-4/ipj\\_5-4\\_internet\\_multicast.html](http://www.cisco.com/warp/public/759/ipj_5-4/ipj_5-4_internet_multicast.html)

[BUSETTA] Busetta P, Donà A, Nori M, *Channeled Multicast for Group Communications*, AAMAS 02, ACM, July 2002.

[EDWARDS] Edwards B.M. et al. *Interdomain Multicast Routing*, ISBN 0-201-74612-3, Addison-Wesley, 2002.

[HANDLEY] Handley M. and Crowcroft J. Internet Multicast Today, *The Internet Protocol Journal*, Volume 2, Number 4, Dec. 1999.

[http://www.cisco.com/warp/public/759/ipj\\_2-4/ipj\\_2-4\\_multicast.html](http://www.cisco.com/warp/public/759/ipj_2-4/ipj_2-4_multicast.html)

[JEACLE] Jeacle K, Crowcroft J, Barcellos MP, Pettini S, Hybrid Reliable Multicast with TCP-XM, CoNext 05, ACM 2005.

[NEUMANN] Neumann C, Roca V, Walsh R, Large Scale Content Distribution Protocols, *ACM SIGCOMM Computer Communication Review*, 35(5), October 2005.

[SAVETZ] Savetz K. et al. *MBONE: Multicasting Tomorrow's Internet*, ISBN 1-56884-723-8, IDG Books, 1996.

[WILLIAMSON] Williamson B. *Developing IP Multicast Networks*, Volume 1, ISBN 1-57870-077-9, Cisco Press, 2000.

### D.2 Internet RFCs

In this section we try to list all current RFCs that have some relevance to multicast IP. All RFCs can be found from:

<http://www.ietf.org/rfc.html>

We have split this section into a first group, which we believe will be of interest and have relevance to many users, and a second group which are retained for the sake of completeness.

These will be referenced elsewhere in this guide by entries of the form [RFC9999].

#### D.2.1 Internet RFCs of interest and relevance to readers

RFC 1075 Distance Vector Multicast Routing Protocol, November 1988.

RFC 1112 Host Extensions for IP Multicasting, August 1989.

- RFC 2236 Internet Group Management Protocol, Version 2, November 1997 (now obsolete).
- RFC 2327 SDP: Session Description Protocol, April 1998.
- RFC 2362 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, June 1998 (Obsoletes 2117).
- RFC 2365 Administratively Scoped IP Multicast, July 1998.
- RFC 2432 Terminology for IP Multicast Benchmarking, October 1998.
- RFC 2588 IP Multicast and Firewalls, May 1999.
- RFC 2614 An API for Service Location, June 1999.
- RFC 2627 Key Management for Multicast: Issues and Architectures, June 1999.
- RFC 2674 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions, August 1999.
- RFC 2715 Interoperability Rules for Multicast Routing Protocols, October 1999.
- RFC 2729 Taxonomy of Communication Requirements for Large-scale Multicast Applications, December 1999.
- RFC 2858 Multiprotocol Extensions for BGP-4, June 2000.
- RFC 2887 The Reliable Multicast Design Space for Bulk Data Transfer, August 2000.
- RFC 2932 IPv4 Multicast Routing MIB, October 2000.
- RFC 2934 Protocol Independent Multicast MIB for IPv4, October 2000.
- RFC 2974 Session Announcement Protocol, October 2000
- RFC 3031 Multiprotocol Label Switching Architecture, January 2001.
- RFC 3048 Reliable Multicast Transport Building Blocks for One-to-Many Bulk-Data Transfer, January 2001.
- RFC 3138 Extended Assignments in 233/8, June 2001
- RFC 3170 IP Multicast Applications: Challenges and Solutions, September 2001.
- RFC 3171 IANA Guidelines for IPv4 Multicast Address Assignments, August 2001.
- RFC 3180 GLOP Addressing in 233/8, September 2001.
- RFC 3208 PGM Reliable Transport Protocol Specification, December 2001.
- RFC 3228 IANA Considerations for IPv4 Internet Group Management Protocol (IGMP)
- RFC 3259 A Message Bus for Local Coordination, April 2002.
- RFC 3261 SIP: Session Initiation Protocol, June 2002.
- RFC 3353 Overview of IP Multicast in a Multi-Protocol Label Switching (MPLS) Environment, August 2002.
- RFC 3376 Internet Group Management Protocol, Version 3, October 2002.
- RFC 3446 Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP), January 2003.
- RFC 3488 Router-port Group Management Protocol (RGMP), February 2003.
- RFC 3559 Multicast Address Allocation MIB, June 2003.
- RFC 3569 An Overview of Source-Specific Multicast (SSM), July 2003.
- RFC 3618 Multicast Source Discovery Protocol (MSDP), October 2003.
- RFC 3678 Socket Interface Extensions for Multicast Source Filters, January 2004.



- RFC 3740 The Multicast Group Security Architecture, March 2004.
- RFC 3754 IP Multicast in Differentiated Services (DS) Networks, April 2004.
- RFC 3913 Border Gateway Multicast Protocol (BGMP): Protocol Specification September 2004
- RFC 3918 Methodology for IP Multicast Benchmarking, October 2004.
- RFC 3926 FLUTE - File Delivery over Unidirectional Transport, October 2004.
- RFC 3956 Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address, November 2004. (Updates RFC3306)
- RFC 3973 Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised), January 2005.
- RFC 4045 Extensions to Support Efficient Carrying of Multicast Traffic in Layer-2 Tunneling Protocol (L2TP), April-20-2005.
- RFC 4046 Multicast Security (MSEC) Group Key Management Architecture, April-29-2005.
- RFC 4082 Timed Efficient Stream Loss-Tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction, June 2005.
- RFC 4271 A Border Gateway Protocol 4 (BGP-4), January 2006 (Obsoletes 1771).
- RFC 4286 Multicast Router Discovery, December 2005.
- RFC 4363 Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions, January 2006 (Obsoletes RFC2674).

## D.2.2 Internet RFCs of less interest and relevance to readers

*This set of RFCs is included for completeness. They are in this section as they are either of less direct relevance to the operation of a multicast IP service or common applications, or are in some cases obsolete or of historic interest only.*

- RFC 966 Host Groups: A Multicast Extension to the Internet Protocol, December 1985 (now obsolete).
- RFC 988 Host Extensions for IP Multicasting, July 1986 (now obsolete).
- RFC 1054 Host Extensions for IP Multicasting, May 1988 (now obsolete).
- RFC 1458 Requirements for Multicast Protocols, May 1993.
- RFC 1584 Multicast Extensions to OSPF, March 1994.
- RFC 1585 MOSPF: Analysis and Experience, March 1994.
- RFC 1819 Internet Stream Protocol Version 2 (ST2) Protocol Specification-Version ST2+, August 1995.
- RFC 2117 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification, June 1997 (Obsoleted by 2362).
- RFC 2201 Core Based Trees (CBT) Multicast Routing Architecture, September 1997.
- RFC 2429 RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+), October 1998.
- RFC 2431 RTP Payload Format for BT.656 Video Encoding, October 1998.
- RFC 2730 Multicast Address Dynamic Client Allocation Protocol (MADCAP), December 1999.
- RFC 2770 GLOP Addressing in 233/8, February 2000 (obsoleted by RFC 3180).
- RFC 2771 An Abstract API for Multicast Address Allocation, February 2000.

- RFC 2776 Multicast-Scope Zone Announcement Protocol (MZAP), February 2000.
- RFC 2907 MADCAP Multicast Scope Nesting State Option, September 2000.
- RFC 2908 The Internet Multicast Address Allocation Architecture, September 2000.
- RFC 2909 The Multicast Address-Set Claim (MASC) Protocol, September 2000.

## D.3 Internet Drafts – Work in Progress

The IETF formal position on Internet Drafts is that they should always be regarded as Work-in-Progress. Internet Drafts are only considered to be current for a six-month period from their date of publication. In an attempt to be helpful to readers, a list is provided below of relevant Internet Drafts as of the time of editing of the current document. Readers are firmly advised to check whether or not the documents have been updated. Unfortunately in some respects, some aspects of the transmission and processing of multicast IP are still active research areas. In those areas RFCs either do not exist or perhaps are already out of date and thus the Internet Drafts are essential. Readers are advised to check carefully with their equipment suppliers in terms of which RFCs or Internet Drafts are currently supported by their products.

These will be referenced elsewhere in this guide by entries of the form [draft-origin-title].

### D.3.1 The IETF MBONED Working Group

The documents produced as part of the MBONED working group's activities include:

[draft-ietf-mboned-msdp-deploy] Multicast Source Discovery Protocol (MSDP) Deployment Scenarios

[draft-ietf-mboned-msdp-mib] Multicast Source Discovery protocol MIB

[draft-ietf-mboned-addrarch] Overview of the Internet Multicast Addressing Architecture

[draft-ietf-mboned-routingarch] Overview of the Internet Multicast Routing Architecture

[draft-ietf-mboned-addrdisc-problems] Lightweight Multicast Address Discovery Problem Space

[draft-ietf-mboned-ssm232] Source-Specific Protocol Independent Multicast in 232/8

The status of these documents can be checked at the following URL:

<http://tools.ietf.org/wg/mboned/>

### D.3.2 The IETF PIM Working Group

The documents produced as part of the PIM working group's activities include:

[draft-ietf-pim-sm-v2-new] Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification (Revised)

[draft-ietf-pim-mib-v2] Protocol Independent Multicast MIB

[draft-ietf-pim-bidir] Bi-directional Protocol Independent Multicast (BIDIR-PIM)

[draft-ietf-pim-sm-bsr] Bootstrap Router (BSR) Mechanism for PIM

[draft-ietf-pim-anycast-rp] Anycast-RP using PIM

The status of these documents can be checked at the following URL:

<http://tools.ietf.org/wg/pim/>

### **D.3.3 The IETF SSM Working Group**

The documents produced as part of the SSM working group's activities include:

[draft-ietf-ssm-arch] Source-Specific Multicast for IP

The status of this document can be checked at the following URL:

<http://tools.ietf.org/wg/ssm/>

### **D.3.4 The IETF MAGMA Working Group**

The documents produced as part of the MAGMA working group's activities include:

[draft-ietf-magma-igmpv3-and-routing] IGMPv3/MLDv2 and Multicast Routing Protocol Interaction

[draft-ietf-magma-snoop] Considerations for IGMP and MLD Snooping Switches

[draft-ietf-magma-igmp-proxy] IGMP/MLD-based Multicast Forwarding ('IGMP/MLD Proxying')

The status of these documents can be checked at the following URL:

<http://tools.ietf.org/wg/magma/>

### **D.3.5 The IETF MPLS Working Group**

The documents produced as part of the MPLS working group's activities include:

[draft-ietf-mpls-multicast-encaps] MPLS Multicast Encapsulations

The status of this document can be checked at the following URL:

<http://tools.ietf.org/wg/mpls/>

### **D.3.6 The IETF L3vpn Working Group**

The documents produced as part of the L3vpn working group's activities include:

[draft-ietf-l3vpn-2547bis-mcast] Multicast in MPLS/BGP IP VPNs

The status of this document can be checked at the following URL:

<http://tools.ietf.org/wg/l3vpn/>

### **D.3.7 Other Internet Drafts**

These documents have been promoted by individual authors rather than an IETF Working Group.

[draft-holbrook-idmr-igmpv3-ssm] Using IGMPv3 and MLDv2 for Source-Specific Multicast

The status of this document can be checked at the following URL:

<http://tools.ietf.org/wg/idmr/>

[draft-raggarwa-l3vpn-2547bis-mcast-bgp] BGP Encodings for Multicast in MPLS/BGP IP VPNs

The status of this document can be checked at the following URL:

<http://tools.ietf.org/wg/l3vpn/>

## D.4 Conference Papers

[COUZENS] Couzens J. Multicast: Wide-Area Perspective, proceedings of Networkshop 2003.

**<http://www.ja.net/services/events/archive/2003/networkshop-31/16-352emulticast.pdf>**

[FAIRHURST2002a] Fairhurst G. Multicast & LANs, University of Aberdeen, proceedings of Networkshop 2002.

**<http://www.ja.net/services/events/archive/2002/networkshop-30/g.fairhurst-paper.pdf>**

[FAIRHURST2002b] Fairhurst G. IP Multicast in LANs, University of Aberdeen, proceedings of Networkshop 2002.

**<http://www.ja.net/services/events/archive/2002/networkshop-30/g.fairhurst.pdf>**

[FAIRHURST2003] Fairhurst G. Multicast & LANs, University of Aberdeen, proceedings of Networkshop 2003.

**<http://www.ja.net/services/events/archive/2003/networkshop-31/prog.html>**

## D.5 Web Sites and Miscellaneous

[ACCESSGRIDa] Access Grid.

**<http://www-fp.mcs.anl.gov/fl/accessgrid/>**

[ACCESSGRIDb] Status of UK Access Grid deployment.

**[http://www.ja.net/development/multicast/grid\\_status.html](http://www.ja.net/development/multicast/grid_status.html)**

[AGSC] The Access Grid Support Centre's web site.

**<http://www.agsc.ja.net/>**

[APPLE] Apple's Quicktime Streaming Server.

**<http://www.apple.com/quicktime/streamingserver/>**

[BBC] BBC Multicast Trials.

**<http://support.bbc.co.uk/multicast/>**

[BEACON] The JANET beacon service.

**<http://chilton.beacon.ja.net/>**

[CERT] The Computer Emergency Response Team (CERT).

**<http://www.cert.org/>**

[CISCOa] Cisco IOS Multicast Technical Documents.

**<http://www.cisco.com/warp/public/732/Tech/multicast/>**

[CISCOb] Cisco IP Multicast Groups external Homepage.

**<ftp://ftpeng.cisco.com/ipmulticast/>**

[CISCOc] How Does Multicast NAT Work on Cisco Routers?

**[http://www.cisco.com/warp/public/105/multicast\\_nat.html](http://www.cisco.com/warp/public/105/multicast_nat.html)**

[CISCOd] Multicast Source Discovery Protocol SA Filter Recommendations.

**<http://www.cisco.com/warp/public/105/49.html>**

[CODEWORK] Codework's RapiDeploy web site.

**<http://www.codework.com/rapideploy/product.html>**

[DETECTIVE] The web site for the Multicast Detective.

**[http://www.nmsl.cs.ucsb.edu/mcast\\_detective/](http://www.nmsl.cs.ucsb.edu/mcast_detective/)**

[EXTREME] Case study of the use of Extreme Networks equipment at Network+Interop 2001, Key3Media Events, Inc.

**[http://www.interop.com/interopnet/pdf/case\\_study.pdf](http://www.interop.com/interopnet/pdf/case_study.pdf)**

[GEANTMSDP] GÉANT MSDP deployment.

**<http://archive.dante.net/nep/GEANT-MULTICAST/deployment-msdp.html>**

[GHOST] Symantec's web site for Ghost.

**<http://www.symantec.com/Products/enterprise?c=prodinfo&refId=865>**

[GLOBALMIX] Global Multicast Internet Exchange's home page

**<http://www.global-mix.org/>**

[IANA] IANA, Internet Multicast Addresses.

**<http://www.iana.org/assignments/multicast-addresses>**

[IMAGECAST] Imagecast's web site.

**<http://www.imagecast.com.au/>**

[IPTV] Cisco's IP/TV product.

**[http://www.cisco.com/en/US/netsol/ns340/ns394/ns158/ns88/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns158/ns88/networking_solutions_package.html)**

[JANET] The JANET web site.

**<http://www.ja.net/>**

[JOD] The JANET Operations Desk web site.

**<http://www.ja.net/services/network-services/jod/index.html/>**

[LOOKINGGLASS] The JANET Looking Glass service web site.

**<http://lg.ja.net/>**

[MAD] MAD Project's Home Page.

**<http://www.atm.tut.fi/mad/>**

[RNS] Configuration requirements and status of Regional Networks connected to JANET.

**<http://www.ja.net/development/multicast/rns.html>**

[MICE] The Multimedia Conferencing Applications Archive.

**<http://www-mice.cs.ucl.ac.uk/multimedia/software/>**

[MMCA] An archive of multimedia conferencing applications.

**<http://www.zcu.cz/mice/archive/>**

[MULTICAST] JANET Multicast development.

**<http://www.ja.net/development/multicast/>**

[NLANR] NLANR's Multicast Beacon web site.

**<http://dast.nlanr.net/projects/beacon>**

[OPENSIP] OpenSLP's web site.

**<http://www.openslp.org>**

[POLYCOM] Polycom's web site.

**<http://www.polycom.com/>**

[VBRICK] VBRICK's web site.

**<http://www.vbrick.com/>**

[VCON] VCon's web site.

**<http://www.vcon.com/>**

[VENAAS] The web site for asmping and ssm ping.

**<http://www.venaas.no/multicast/ssmping/>**

## Appendix E: Glossary

(* ,G)	a notation indicating all sources sending to a group G.
(S,G)	a notation indicating all data sent from source S to group G.
(S,G,RPT)	a notation indicating all data sent from source S to group G, but only if arriving via an RPT.
ABC	American Broadcasting Company.
ACL	Access Control List.
Anycast-RP	a mechanism to provide redundant RPs by getting all the set to use a given address on an internal loopback interface.
AS	Autonomous System – a group of systems managed by a single administration.
ASM	Any Source Multicast – the traditional form of multicast where receivers express their interest in all traffic sent to a certain multicast address, no matter where it originated.
auto-RP	a Cisco® designed mechanism to elect RPs automatically – this mechanism is not recommended by the current document.
BAR	Backbone Access Router – one of the routers making up the boundary of the JANET backbone.
Beacon	A device to assist in monitoring multicast transmissions.
BGP, BGP-4	Border Gateway Protocol – a protocol used to exchange routing information between ASs. The current version is version 4.
Bridge	A level-2 device that selectively forwards network traffic based upon MAC addresses.
BSR	Boot Strap Router – used as part of one way to discover RPs.
CERT	Computer Emergency Response Team.
CGMP	Cisco® Group Management Protocol – a proprietary protocol used by routers to control packets forwarding by bridges and switches.
CNN	Cable News Network.
CSPAN	Cable-Satellite Public Affairs Network.
DIS	Distributed Interactive Simulation.
DM	Dense Mode – a style of multicast whereby traffic is flooded everywhere unless explicitly pruned.
DoD	US Department of Defense.
DR	Designated Router – a router elected to perform various activities on behalf of all hosts connected to a given LAN.
DVMRP	Distance Vector Multicast Routing Protocol – an important early dense mode protocol for forwarding.
EGLOP	Extended GLOP – a mechanism to allow routing registries to allocate multicast addresses.
GÉANT	The pan-European academic and research network.
GlobalMix	Global Multicast Internet Exchange – <a href="http://www.global-mix.org/">http://www.global-mix.org/</a> .
GLOP	A mechanism that allocates multicast addresses to ASs.
GMRP	Generic Multicast Registration Protocol.
H.323	The ITU recommendation for real time packet-based multimedia communication services.
IANA	Internet Assigned Numbers Authority.

---

ICMP	Internet Control Message Protocol – a protocol used in conjunction with IP to transfer control information between routers and hosts.
IEEE	Institute of Electrical and Electronic Engineers.
IETF	Internet Engineering Task Force.
IGMP	Internet Group Management Protocol – the protocol whereby hosts and routers exchange multicast group membership information.
IOS	Internetwork Operating System – Cisco® name for the operating system of their networking devices.
IP	Internet Protocol.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 6.
ISM	Internet Standard Multicast – an alternative term, used by some authors, for ASM.
ITU	International Telecommunications Union.
JANET	The UK education and research network.
JCS	JANET Customer Services.
JOD	JANET Operations Desk.
Join	A PIM message to request connection to a flow of multicast information.
LAN	Local Area Network.
Leave	A PIM message to request disconnection from a flow of multicast information.
MBGP	A specification for extensions to the BGP-4 protocol to enable it to carry reachability information for protocols other than unicast IP. This is often used to transmit multicast reachability information.
MBONE	An early approach to the transmission of multicast information over unicast based networks using tunnels, now largely obsolete.
MIB	Management Information Bases.
MICE-NSC	Multimedia Integrated Conferences for Europe-National Support Centre. A UKERNA funded project that ran until 31 March 1997.
MLD	Multicast Listener Discovery
MP_REACH_NLRI	Multiprotocol Reachable Network Layer Reachability Information.
MP_UNREACH_NLRI	Multiprotocol Unreachable Network Layer Reachability Information.
MPEG	Moving Pictures Expert Group.
MPLS	multiprotocol label switching
MRIB	Multicast Routing Information Base – a generic name for the table, or set of tables, or other information used as the basis of multicast packet forwarding and RPF checks.
MSDP	Multicast Source Discovery Protocol.
Multicast	A mechanism that enables a single transmitted IP packet to be delivered to multiple destinations. Differs from broadcast in so much as packets are only delivered to hosts that have expressed an interest in receiving the packets.
NAT	Network Address Translation.
NEAT	Networked Expertise, Advice and Tuition. A JISC Technologies Application (JTAP) Programme project that ran from 1 September 1996 to 31 March 1999.

NIC	Network Interface Card – a generic term used to refer to the interface card that connects a host to its serving network.
NLANR	National Laboratory for Applied Network Research.
NLRI	Network Layer Reachability Information.
NOSC	JANET Network Operations and Service Centre.
PIC	Peripheral Interface Card.
PIM	Protocol Independent Multicast – a specification for forwarding multicast that can make its forwarding or RPF decisions on the basis of any available routing information.
PIMD	A public domain multicast routing software.
PIM-DM	The dense mode variant of PIM.
PIM-SM	The sparse mode variant of PIM.
PIM-SMM	subset of PIM sparse mode.
Ramen	A worm-like virus that used multicast as part of its attack methodology.
RFC	Request for Comments – the documents that in practice are the specifications for the behaviour of the Internet and its protocols.
RIPv2	Routing Information Protocol version 2.
RP	Rendezvous Point – a router taking on the special role of providing a meeting point for sources and hosts within a sparse mode multicast environment.
RPF	Reverse Path Forwarding – a mechanism that looks at where a packet came from when making decisions on whether or not it should be forwarded.
RPT	Rendezvous Point Trees – shared trees used for forwarding multicast information that are rooted at the RP of a sparse mode network.
SA	Source Active.
SAP	Session Announcement Protocol.
SD	Session Directory – a software tool developed by Van Jacobson at Lawrence Berkeley National Laboratory.
SDR	Session Directory Tool – a software tool developed by staff in Computer Science, University College London.
SDP	Session Description Protocol.
Shared Trees	A branching path through a network used to deliver information to multiple recipients.
SM	Sparse Mode – a form of multicast where information is only sent to hosts if it is specifically requested.
SNMP	Simple Network Management Protocol.
SPT	Shortest Path Tree – a path through a network that is the most direct from a source to a recipient.
SSM	Source Specific Multicast – a form of multicast where only information from a nominated source is delivered to interested receivers as opposed to information from all sources. Some authors use the term Single-Source Multicast. Contrast this with ASM/ISM defined above.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TTL	Time To Live.
UDP	User Datagram Protocol.
UKERNA	United Kingdom Education & Research Networking Association.
WAN	Wide Area Network.



VIP	Video over IP. A UKERNA-funded project that investigated the feasibility of operating H.323 videoconferencing over JANET.
VTAS	Video Technology Advisory Service. A UKERNA funded initiative to offer advice and support to JANET customers in the use of video technologies.
Xorp	eXtensible Open Router Platform. A project whose goal is to develop an open source software router platform that is stable and fully featured enough for production use, and flexible and extensible enough to enable network research.

# Index

## Symbols

(\* ,G) PIM Join 28, 49  
(S,G) Join 24  
(S,G) PIM Join 24  
(S,G,RPT) PIM prune 25

## A

Aberdeen 3  
Access Grid Support Centre 43  
ACL 50  
administratively scoped address 17  
Administratively Scoped IP Multicast 17, 33  
administrative overhead 37  
AG 43  
agents 44  
AGSC 43  
Altiris RapiDeploy 45  
Anycast 33, 47  
Anycast-RP 33, 47  
Apple 44  
AppleTalk 45  
AS 16, 18, 22, 27, 34  
ASM 13, 18, 20, 22, 28, 29, 32, 41, 42, 47, 48  
audio stream 43  
auto-RP 47  
autonomous systems 16, 24

## B

Backbone Access Routers 32  
bandwidth 9  
BAR 32, 33, 51  
BBC 44  
Beacon 41  
Beacon Architecture 41  
BGP 19, 27, 39  
BGP-4 19  
blocks 14, 15, 16  
Boot Strap Router 47  
boundaries 17  
boundary 50, 51  
branch 12  
broadcast 12, 36  
broadcasters 22  
BSR 47  
bug 59  
bugs 40

## C

cable 36, 58  
Cable-Satellite Public Affairs Network 44  
cable segments 36  
cabling 36  
candidates 19

CERT 30, 59, 60, 61  
CERT/CC 59  
CGMP 38  
Cisco 44, 47, 48, 49, 50  
Cisco Group Management Protocol 38  
CNN 44  
co-axial cables 36  
Codework 45  
command 48  
commands 27, 28, 50  
configuration 47  
configure 22, 26  
configured 26  
congruent 27  
connected 3, 10, 12, 36, 37  
connectivity 9  
CSPAN 44

## D

DA 45  
debug 22, 47  
Deering 10  
degradation 38  
Denial-of-Service 60  
dense mode 18, 47  
deprecated 15  
Designated Router 23  
destination 18, 26, 58  
Directory Agent 45  
DIS 16  
Disney 15  
Distributed Interactive Simulation 16  
DM 18  
DoD 16  
Dow Jones 15  
DR 23, 26  
DVMRP 10, 14, 18, 19  
dynamic 15

## E

EGLOP 16  
Emblaze-Vcon 43  
encapsulated 24, 26  
end-to-end 34  
equipment 26  
erroneously 28  
Ethernet 36, 37, 38, 39, 51, 58  
European Space Agency 44  
exception 14, 20

## F

Fairhurst 3, 37, 58  
FastEthernet1/0 50  
FastEthernet2/0 50

- filter 19, 26, 27, 38
  - filtering 30, 37
  - filters 37, 58
  - firewall 60
  - flood 18
  - flooding 18, 22
  - floods 12
  - forward paths 19
  - frame 36, 37, 38, 58
  - frames 36, 37
  - frame filtering configuration 37
- G**
- GÉANT 27, 33, 34
  - Generic Multicast Registration Protocol 39
  - GLOP 16, 34
  - GMRP 39
  - Grid 9, 37, 41, 43, 45, 62
  - group 19, 26, 33, 38
- H**
- Hot Standby Router Protocol 60
  - HSRP 60
  - hubs 37
- I**
- IANA 15, 16, 17
  - ICMP 40, 42
  - icmp echo requests 60
  - IEEE 802.p 39
  - IETF 10, 14, 16, 17, 19, 26
  - IGMP 14, 19, 20, 21, 22, 23, 38, 41
  - IGMPv1 20, 21
  - IGMPv2 20, 21, 38
  - IGMPv3 20, 21, 28, 38, 48
  - IGMP Membership Query 20
  - IGMP Membership Report 20, 23, 38
  - IGMP Proxy 38
  - IGMP Query 21
  - IGMP snooping 38
  - inter-domain 22, 29
  - inter-domain multicast service 29
  - interface 19, 20, 22, 23, 33, 50, 51
  - interfaces 18, 23
  - Internetwork 15
  - Internet Control Message Protocol 40
  - Internet Group Management Protocol 19
  - Internet Group Management Protocol, Version 2 19
  - Internet Group Management Protocol, Version 3 19
  - Internet Stream Protocol 15
  - interoperability 26
  - IOS 47, 49, 51
  - IP 9, 12, 33, 48, 61
  - IP/TV 44
  - IPv4 9, 10, 14, 26, 27, 45, 58, 59, 60
  - IPv6 10, 58
  - IP Multicast 10, 18, 20, 25, 30, 33, 36, 37, 39, 41, 42, 43, 44, 45, 46, 58
  - IP Multicast and Firewalls 30
  - isolated RP 49
- J**
- JANET 3, 9, 27, 34
  - JANET Beacon Service 41
  - JANET Customer Service 34, 46
  - JANET Looking Glass 42
  - JANET Operations Desk 46
  - JCS 46
  - Jini 45
  - JISC 43
  - JOD 46
  - Join 20, 23, 24, 26, 28, 49
  - Join/Prune 23
  - joining 19, 20
  - Juniper 52
- K**
- kernel 20
- L**
- LAN 19, 20, 21, 22, 25, 28, 36, 37, 58
  - LANS 36
  - latency 21
  - layer 20
  - layers 27
  - layer 2 20
  - Linux 14, 20
  - listen 20, 21
  - listeners 22
  - loopback 33
- M**
- MAC destination 58
  - MAC group 58
  - malicious parties 30
  - Management Information Bases 42
  - many-to-many 18
  - mapping 20, 58
  - MBGP 19, 26, 27, 32, 35, 39
  - MBONE 10, 18
  - MDD 15
  - members 26
  - membership 14, 20, 38
  - membership report 20, 21
  - Mesh 26, 33
  - message 20
  - MIBs 42
  - MICE-NSC 10
  - Microsoft 17, 20, 59, 60, 61, 62
  - MMCA 43
  - MP\_REACH\_NLRI 27

MP\_UNREACH\_NLRI 27  
MPEG 44  
MRIB 19, 23, 26, 27, 32  
MSDP 26, 27, 28, 29, 32, 33, 35, 39, 49, 50, 52  
MSDP Mesh Group 33  
mtrace 42  
multicast capability 40  
multicast groups 15  
Multicast Quick-Start Configuration Guide 47  
Multicast Routing Information Base 19  
Multicast Source Discovery Protocol 19  
Multimedia Conferencing Applications Archive 43  
multiple video streams 43  
Multiprotocol Reachable NLRI 27  
Multiprotocol Unreachable NLRI 27

## N

NASA 40  
Nasdaqmdfeeds 16  
National Laboratory for Applied Network Research 41  
neighbour 23  
networks 3, 9  
Networkshop 32  
Network Interface Cards 37  
network time 45  
Network time synchronisation 44  
new multicast connections 46  
NIC 37, 58  
NLANR 41  
NLRI 27  
Non-IP 10  
non-IP multicast 38  
non-multicast 10  
non-querier 21  
non-RP 40  
non-RP routers 49  
non-RP Router Configuration 47, 48  
non-SSM 28  
Norton Ghost 45  
NOSC 3, 34, 35  
Novell Netware 45

## O

on-demand 29  
on-demand media servers 44  
on-demand multimedia 45  
on-demand servers 29  
one-to-many 18  
OpenSLP 45  
operating 20  
operating system 28  
Organization-Local Scope 17  
overhead 12, 37, 38

## P

packets 17  
pan-JANET 34  
peer 18, 26, 32, 33, 39, 49, 50  
peering 32, 39, 50  
peers 19  
performance 38  
performed 19, 26  
Phoenix ImageCast MFG 45  
PIM 14, 18, 19, 20, 23, 24, 25, 26, 28, 49  
PIM-DM 18  
PIM-SM 18, 20, 21, 22, 26, 28, 32, 35, 39, 47, 52  
PIM-SM Join/Prune 23  
PIM Join 24  
PIM Register 23  
Point 52  
Polycom 43  
port 17, 60  
PowerPoint 61  
pre-allocated 17  
problems 14, 22, 27  
procedures 14  
process 21  
processing 37, 52  
promiscuous mode 37  
propagation 17  
Protocol 9  
Protocol Independent Multicast – Dense Mode 18  
Protocol Independent Multicast – Sparse Mode 18  
proxy 38

## Q

querier 21, 38  
queriers 14, 21  
query 21  
query message 21  
Quicktime Streaming Server 44

## R

Ramen 30  
range 11, 14, 15, 16, 17, 20, 27, 28, 33, 34, 37, 48  
ranges 35  
rasadv 17  
rat 40  
reachability 27  
receive 12, 13, 14, 18, 19, 20, 26, 28  
receivers 18, 19, 22, 23, 24, 25, 26, 27, 28, 29, 30, 41  
recipients 12, 18  
recommendation 10, 26  
recommended 20, 27, 33, 42  
record 3, 52

- 
- redundancy 22
  - redundant 12
  - Regional Networks 3, 9, 10, 17, 18, 20, 32, 33, 34, 35, 36, 39, 40, 46, 47, 48, 50
  - Regional Network Operators 9, 41
  - register 23, 24, 26
  - registered 12
  - Register Stop 24
  - registries 16
  - rejected 28
  - reliability 22
  - reliable 26
  - Rendezvous Point 18, 19, 22, 52
  - Rendezvous Point Tree 22
  - repeater 36
  - repeated LAN 36
  - replicate 18
  - replicating 12
  - replication 12
  - replies 21
  - report 20, 21, 38
  - reporting 46
  - reports 26
  - requested 12
  - requesting 12
  - required 10, 37
  - resilience 33, 35
  - resources 12
  - responded 21
  - responses 21
  - responsibility 9
  - responsible 10, 12
  - restricted 12, 17
  - Reverse Path 19
  - RFC1190 15
  - RFC3180 16
  - RFC3446 33
  - RFC3618 35
  - RFC1112 19
  - RFC223 19
  - RFC3376 19
  - RFC2365 17, 33
  - RFCs 10, 16, 18, 19, 25, 26, 27, 28, 42, 49
  - RIPv2 14
  - risk 30
  - routers 21, 23
  - routing 26
  - RPF 18, 19, 23, 26, 27, 30, 32, 42, 50
  - RPs 18, 19, 20, 22, 23, 24, 25, 26, 28, 29, 32, 33, 35, 39, 40, 47, 48, 49, 50
  - RPT 22, 23, 24, 25, 26, 28
  - rules 19, 26
- S**
- SA 19, 26, 28, 45
  - SAP 15
  - SAPv0 15
  - SAPv1 15
  - scenario 26
  - scope 17
  - SDP 15
  - SDP/SAP 15
  - sdr 40
  - security 59
  - Self-Healing Virtual Ring 61
  - send 18, 20, 23
  - senders 22
  - sending 12, 26
  - sends 21
  - sequence 26, 35
  - servers 29
  - services 9, 13, 15
  - Service Agent 45
  - Service Location Protocol 45
  - sessions 15
  - Session Announcement Protocol 15
  - Session Description Protocol 15
  - Shortest Path Tree 22, 24
  - SHVR 61
  - Simple Network Management Protocol 42
  - Site-Local Scope 17, 33
  - site administrators 9
  - SLP 45
  - SM 18, 26
  - Smurf 59, 60
  - SNMP 42
  - snooping 38
  - software 9, 14, 21, 37, 38, 41, 44, 45, 52, 59, 60
  - software agents 44
  - Solaris 2.6 servers 61
  - Solaris 2.x 61
  - solution 27
  - source 24, 26
  - Source-Active 19, 26
  - Source-Specific API 20
  - Source-Specific Multicast for IP 27
  - Source-Specific Protocol 16
  - Source-Specific Protocol Independent Multicast in 232/8 28
  - sparse-dense-mode 47
  - sparse mode 18
  - specifications 9, 10, 18
  - specified 24
  - Sprint 33
  - SPT 22, 24, 25, 26, 28
  - SPTs 22, 25
  - SSM 13, 14, 16, 18, 20, 21, 26, 27, 28, 29, 30, 32, 34, 41, 47, 48
  - ST 15
  - static 15
  - statically 14, 22
  - static specification 47
  - streams 43
  - subnet 14, 21, 23, 26, 52
  - Sun Microsystems 45

switched Ethernet 37  
Switches 38  
switch performance 38  
Symantec 45

**X**  
XORP 52  
XP 14, 20, 60

**T**

TCP 21, 26, 40, 60  
TCP/IP 21, 40  
tcpdump 3.5.x 61  
time 3, 9, 16  
traceroute 42  
tracking 21  
traffic profiles 40  
Transient Groups 16  
transmit 22  
tunnel 52  
tunnelling 10, 30  
twisted pair cabling 36

**U**

UA 45  
UCL Network and Multimedia Research Group  
43  
UDP 17  
UKERNA 3, 35, 43  
uncertainty 17  
unicast 12, 18, 36  
unicast IP 42, 48  
University of Illinois 44  
University of Manchester 43  
UNIX 14, 42  
unsolicited 12  
UPnP 59, 60  
US-CERT 59  
User Agent 45  
User Datagram Protocol 17

**V**

VBrick 44  
vic 40  
video 46  
video servers 22  
video streams 43  
Video Technology Advisory Service 46  
videoconferencing 9, 45  
VIP 10  
VTAS 46

**W**

websites 9  
Windows 14, 20, 59, 60  
wireless 36, 39  
wireless LAN 36, 39  
WLAN 39  
worm 30

## Tell us what you think

Technical Guides are produced and published by UKERNA for use within the JANET Community.

We welcome your comments on all aspects of this document and on any other UKERNA publication.

Please direct feedback to JANET Customer Service, at the address below, or e-mail us directly at:

documentation@janet.ac.uk

UKERNA manages the networking programme on behalf of the higher and further education and research community in the United Kingdom. JANET, the United Kingdom's academic and research network, is funded by the Joint Information Systems Committee (JISC).

For further information please contact:

JANET Customer Service  
UKERNA  
Atlas Centre, Chilton, Didcot  
Oxfordshire, OX11 0QS

Tel: 0870 850 2212  
Fax: 0870 850 2213  
E-mail: service@janet.ac.uk

### Copyright:

This document is copyright The JNT Association trading as UKERNA. Parts of it, as appropriate, may be freely copied and incorporated unaltered into another document unless produced for commercial gain, subject to the source being appropriately acknowledged and the copyright preserved. The reproduction of logos without permission is expressly forbidden. Permission should be sought from JANET Customer Service.

### Trademarks:

JANET®, SuperJANET® and UKERNA® are registered trademarks of the Higher Education Funding Councils for England, Scotland and Wales. The JNT Association is the registered user of these trademarks.

Microsoft® and Windows® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

The term 'Linux'® is a registered trademark of Linus Torvalds, the original author of the Linux kernel.

UNIX® is a registered trademark licensed to X/OPEN.

Mac OS® is a registered trademark of Apple Computer, Inc., registered in the U.S. and other countries.

### Disclaimer:

The information contained herein is believed to be correct at the time of issue, but no liability can be accepted for any inaccuracies.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and e-mail addresses should be used with caution.

The JNT Association cannot accept any responsibility for any loss or damage resulting from the use of the material contained herein.

### Availability:

Further copies of this document may be obtained from JANET Customer Service at the above address.

This document is also available electronically from: <http://www.ja.net/services/publications/technical-guides>



© The JNT Association 2006

The logo for JISC, consisting of the letters 'JISC' in a large, bold, orange, sans-serif font.

