

**DRAFT Proposal for RUNet Administratively Scoped Multicast**  
 OIT Telecommunications Division  
 P. Palanchi and M. Scarpellino  
 March 25, 2008

**Abstract**

This document outlines techniques to bound multicast traffic within the Rutgers University enterprise. TD will define RUNet zones for Administratively Scoped Multicast Addresses per RFC 2365, and apply Multicast Boundary Filters to constrain the unintentional flooding of IP multicast throughout RUNet. This change may adversely impact applications that employ IP Multicast to distribute content beyond the local network segment. This change may require application administrators to take action to avoid potential disruption in their multicast application where large-scale distribution is intended.

**Background**

IP Multicast is increasingly being used as a distribution mechanism for large-volume and real-time information. RUNet is designed to transparently pass IP multicast traffic, but relies on distribution mechanisms that were designed to handle much lower traffic rates than are typical of modern applications. Furthermore, RUNet's IP multicast mechanisms operate in a single, flat policy space, which allows pervasive advertisement and transmission of high-rate streams. With increasing usage, IP multicast becomes more taxing on RUNet resources, and requires the application of modern standards and practices. These changes may have an adverse impact on the way some applications currently operate, though it is expected that these changes will work to the overall benefit RUNet and its customers.

There a number of applications in use that take advantage of IP Multicast to perform one-to-many distribution of content. Many of these applications are assumed to operate in LAN environments, or make other assumptions that are incompatible with a broad, flat multicast policy as implemented on RUNet. It is increasingly the case that using multicast for high-rate data transfer causes operational problems. These IP Multicast groups are prevalent and permitted run unbounded throughout RUNet. In some cases, the developers of IP multicast enabled applications have selected multicast group addresses that may also lead to the application leaking to external networks such as Internet2.

Table 1 below lists some applications and their default IP multicast groups that would most likely benefit from the use of administratively scoped multicast addressing and multicast boundary filters. This list is not exhaustive, but is representative of the applications observed by TD to be operating on RUNet.

Address	Imaging Applications
224.2.0.2/32	Altiris Rapideploy
224.2.0.3/32	Altiris Rapideploy
224.77.0.0/16	Norton Ghostcast
229.55.150.208/32	Norton Ghostcast
225.1.2.3/32	Altiris Development Server & Deployment Agent
234.42.42.42/30	Phoenix/Storagesoft& Imagecast
239.254.5.6	ECopy ShareScan

**Table 1 – Default IP Multicast addresses of common desktop imaging applications**

Table 2, below, lists a number of network service discovery protocols that use group addresses found in the Local Scope- Scope Relative multicast group address range of 239.255.255.0/24. In particular, WindowsXP - Simple Services Discovery Protocol (SSDP) uses 239.255.255.250. Windows documentation indicates that SSDP works with Universal Plug and Play (UPnP) for home user LANs for device discovery. The implication is that the Local Scope-Scope Relative range is for local discovery mechanisms and probably should not leave the LAN. If service discovery is desired across a larger domain, the administrator should reconfigure the application to use a

different service address.

<b>Address</b>	<b>Services Discovery Protocols</b>
239.255.255.255	SAP Session Announcement Protocol (SDR)
239.255.255.254	Multicast Address Dynamic Client Allocation Protocol (MADCAP) RFC2730
239.255.255.253	Service Location Protocol (SLP) v2
239.255.255.252	Multicast-Scope Zone Announcement Protocol (MZAP) RFC2776
239.255.255.251	Multicast Discovery of DNS Services
239.255.255.250	WinXP SSDP for UPnP
239.255.255.249	DHCPv4
239.255.255.248	AAP
239.255.255.247	Message Bus (MBUS) RFC2359

**Table 2 – Default IP Multicast addresses of common service announcement protocols**

SSDP and SLPv2 sources are the most pervasive groups observed on the RUNet. Again, it is likely not the intent of most administrators to advertise SSDP and SLPv2 services to foreign networks. It should be noted that SAP announcements on group 239.255.255.255 should not be confused with global SAP group address 224.2.127.254.

Administratively Scoped Multicast Addresses, detailed in Table 3 and fully defined in RFC 2365, are available for enterprise network managers to define and configure scoped network zones. The addresses are drawn from the IP multicast 239.0.0.0/8 address space, known as the "ORG-LOCAL" space. The address range is similar in its use to the RFC 1918 address ranges, and is not used on the public Internet or Research and Education Networks. In order to accommodate the ad-hoc use of IP multicast addresses, many organizations follow the recommendations set forth in RFC 2365 to limit the natural scope of IP multicasts.

*Multicast boundary filters* are rules established by the network administrator and installed on router interfaces at proscribed regional or logical network boundaries. They are applied to the router interface specifically to either prevent or allow multicast traffic in and out of the interface. This mechanism would be used to implement the administrative scoping policy at key aggregation points throughout the network.

<b>Administratively Scoped Zones</b> RFC2365	
<b>Organization-Local Scope Expansion</b>	239.0.0.0/8
Do Not Use	239.0.0.0/24
IANA Reserved	239.0.0.0/10
IANA Reserved	239.64.0.0/10
Do Not Use	239.128.0.0/24
IANA Reserved	239.128.0.0/10
<b>Organization-Local Scope /14</b>	239.192.0.0/14
<b>CAMPUS 239.192/14</b>	239.192.0.1
Org-Local Scope - Last Address	239.195.254.255
Org-Local Scope Relative-Do Not Use	239.195.255.0/24
<b>Local Scope Expansion</b>	239.196.0.0
<b>REGION 239.196/14</b>	239.196.0.1
<b>ENTERPRISE 239.200/14</b>	239.200.0.1
Private Source-Specific Multicast (SSM) Range	239.232.0.0 /16
IANA Reserved	239.252.0.0/16
IANA Reserved	239.253.0.0/16
IANA Reserved	239.254.0.0/1
<b>Local Scope /16</b>	239.255.0.0/16
IANA RAS/RRAS	239.255.2.2
Local Scope-Scope Relative-Do Not Use	239.255.255.0/24

**Table 3 – Extended definition of Organizational-Local scope IP Multicast group addresses**

**Proposal**

TD proposes to implement a hierarchical addressing scheme that will define several logical, geographical boundaries, or *scopes*. The proposal is based on RFC 2365, Administratively Scoped Multicast Addresses. Once implemented, most IP Multicast enabled applications currently in use will be bounded from unintentional flooding of the RUNet backbone and external Internet resources.

Multicast boundary filters will be deployed to constrain default application addresses, shown in Table 1, and Local Scope-Scope Relative addresses shown in Table 2 from the RUNet backbone. Similarly, the filters would give treatment to the new ranges of organizational-local scope (CAMPUS, REGION or ENTERPRISE), as shown in Table 4, in addition to the multicast groups presently allowed on Internet2. It should be noted that there are a number of addresses that are reserved and should not be used. These are also listed in the Table 3. Multicast group numbers are normally used as /32's - host specific assignments.

Range:	Base:	IP Addresses:
CAMPUS	239.192.0.0/14	239.192.0.1 - 239.195.254.255 (last usable address)
REGION	239.196.0.0/14	239.196.0.1 - 239.199.255.254
ENTERPRISE	239.200.0.0/14	239.200.0.1 - 239.203.255.254

**Table 4 – Rutgers Organizational-Local scope IP Multicast group ranges**

TD will apply multicast boundary filters to significant traffic aggregation points such as building router uplinks, campus unlinks and Internet handoffs in order to define the different administrative scopes.

The addresses in Table 4 are defined hierarchically. The ENTERPRISE scope encompasses all of RUNet, and is visible across RUNet for each of the three metropolitan campuses. The REGIONAL scope is distinct for each of the three metropolitan campuses. Addresses in the REGIONAL scope are visible only within that metropolitan region, so that a group address of 239.196.127.1 used in New Brunswick/Piscataway is distinct from a group address of 239.196.127.1 when used in Newark or Camden. The CAMPUS scope is distinct for each of the four New Brunswick/Piscataway “minor” campuses Busch, Livingston, College Avenue, and Cook/Douglass. The CAMPUS scope is also configured for the Newark and Camden campuses, and is handed the same as the REGIONAL scope.

Network managers should consider where the intended recipients are when selecting a multicast group address for their application. If the application is intended for use throughout RUNet, then a group address from the ENTERPRISE scope is an appropriate selection, whereas if the application is intended for use by the local campus community, then the REGIONAL or CAMPUS scope is appropriate. At the time of this proposal, it is intended that groups are established *ad hoc*, without need for formal assignment or central administration.

### Conclusion

By implementing administratively scoped IP multicast addressing, TD will enable network managers to selectively limit the logical distribution of their multicast traffic by selecting a group address from the appropriate address range. The plan brings further benefits by reducing the scope and impact of unintentional, high-rate data transfers on the campus backbone.

TD is hoping to obtain feedback from the Rutgers technical community on the changes proposed in this document. After the discussion period, TD will move ahead and implement this change.