Network Working Group
Internet-Draft
Expire in six months

Ross Finlayson
Live Networks
1997.03.25

Using TTLs with Administratively Scoped IP Multicast Addresses

<draft-finlayson-ttl-admin-scope-00.txt>

1. Status of this Memo

2. Abstract

The use of "administratively scoped" multicast address ranges (as described in [1]) leads to a multicast traffic scoping mechanism that is superior to the original "TTL scoping" mechanism.

Contrary to popular opinion, however, administrative (often abbreviated as "admin") scoping does not truly *replace* TTL scoping. In particular, multicast-based applications must still be aware of which TTL value(s) they use.

In this document, we note that each definition of a range of admin scoped multicast addresses should be accompanied by a corresponding "maximum effective TTL" that should be used with these addresses. We describe how these TTL values are used by applications, and how they may influence the configuration of multicast border routers.

3. The need for a "maximum effective TTL" for each admin scoped range

A multicast-based application needs to be aware of the TTL value(s) that is uses in the packets that it sends. If it uses a TTL that's too low, it may not reach all of the other nodes that it wants to. On the other hand, if it uses a TTL that's too high, it may waste network resources.

If the entire MBone were to use admin scoping, then it would, in principle, be OK for applications to always use a TTL of 255 (the maximum possible value). In reality, however, this would be disastrous, because there will inevitably be some sections of the MBone that (i) do not implement admin scoping, and (ii) use "flood-and-prune" multicast routing protocols (such as DVMRP). If many applications were to use a TTL of 255, then these sections of the MBone would likely become overwhelmed. Instead, well-behaved multicast-based applications should use a TTL that's large enough to reach all of the nodes that they're interested in, but not much larger.

To address this problem, we propose that whenever a range of admin scoped multicast addresses is defined (e.g., by IANA), then this definition be accompanied by the explicit definition of a "maximum effective TTL" for this range. This TTL is chosen to be large enough to guarantee reaching all nodes within the corresponding scope, but not too much larger. Thus, the "maximum effective TTL" for an admin scoped range describes the topological 'size' of the scope. (As with pure TTL scoping, each such range will typically also be given a descriptive label, such as "continent", that describes the size in human terms.)

4. Use by applications

Many multicast-based applications will not have to concern themselves with this, because they will already know both the multicast address(es) that they use, and the corresponding TTL(s). In particular, applications that are launched from "session descriptions" (e.g., in SDP [2]) will get both the multicast address and the TTL from the session description itself.

However, applications that choose multicast addresses dynamically should be aware of the corresponding "maximum effective TTL" for each multicast address that they choose. For example, an application that *creates* a new session description might prompt the user for the size of the scope required (perhaps using descriptive human-understandable labels such as "continent"). It would then use the user's response to select an appropriate-sized admin scope, with a corresponding address range and TTL.

An application that varies its TTL - e.g., to perform "expanding ring"-type searches - need not (and should not) increase the TTL beyond the "maximum effective TTL" for the multicast address that it's using.

5. Implementation & configuration of multicast border routers

A multicast router that implements admin scoped boundaries (as described in [1]) need have no knowledge of "maximum effective TTLs". Such routers may be configured by defining only the multicast addresses that define the boundaries.

However, because a "maximum effective TTL" is defined for each admin scoped range, a (reimplemented) multicast router could, in principle, be configured using TTL thresholds only. That is, a specification of a TTL threshold "t" would denote a boundary for addresses in all admin scoped ranges whose "maximum effective TTL" is less than or equal to "t".

An advantage of this approach is that TTL-threshold-based configuration is (arguably) more intuitive and easier to understand (and thus less susceptible to errors) than address-range-based configuration. Also, existing configuration files (that define only TTL threshold boundaries) could remain unchanged, and admin scoping would get implemented automatically via a router software upgrade.

Finally, it should be noted that - regardless of how admin scope boundaries may be configured - all border routers in the MBone should eventually implement such boundaries. It has been noted [3] that optimal pruning (with flood-and-prune routing protocols) in the MBone does not occur if admin scoped boundaries are not used.

6. Security considerations

While the use of "maximum effective TTLs", as described here, helps limit the distribution of multicast traffic, neither this mechanism, nor administrative scoping itself, should be viewed as a mechanism for ensuring confidentiality.

7. References

[1] David Meyer. "Administratively Scoped IP Multicast".
Work in progress,
Internet Draft: draft-ietf-mboned-admin-ip-space-01.txt
[2] M Handley, V. Jacobson. "SDP: Session Description Protocol"
Work in progress, Internet Draft: draft-ietf-mmusic-sdp-02.txt
[3] Stephen Casner. "Discovery of Pruning Problem"
Email to the MBONED working group, 30 January 1997.

8. Author's address

Ross Finlayson
finlayson@lvn.com