

IPNGWG Working Group
Internet Draft
[draft-ietf-ipngwg-scoped-routing-03.txt](#)
February 2000
Expires August 2000

B. Haberman
Nortel Networks

Routing of Scoped Addresses
in the Internet Protocol Version 6 (IPv6)

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>.

Abstract

This document outlines a mechanism for generating forwarding tables that include scoped IPv6 addresses. It defines a set of rules for routers to implement in order to forward packets addressed to scoped unicast or multicast addresses regardless of the routing protocol. These rules apply to all scoped addresses.

1. Introduction

This document defines a set of rules for the generation of forwarding table entries for scoped addresses. These rules will describe the handling of scoped addresses for both single site and site boundary routers. These rules apply to all routing protocols that support IPv6 addresses.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

In a single site router, a routing protocol can advertise and route all addresses and prefixes, except the link-local prefixes, on all interfaces. This configuration does not require any special handling for site local addresses. The reception and transmission of site local addresses is handled in the same manner as globally scoped addresses. This applies to both unicast and multicast routing protocols.

[4.](#) Site Boundary Unicast Routing

With respect to site boundaries, routers must consider which interfaces a packet can be transmitted on as well as control the propagation of routing information specific to the site. This includes controlling which prefixes can be advertised on an interface.

4.1 Routing Protocols

When a routing protocol determines that it is a site boundary router, it must perform additional work in order to protect inter site integrity and still maintain intra site connectivity.

In order to maintain connectivity, the routing protocol must be able to create forwarding information for the global prefixes as well as for all of the site prefixes for each of its attached sites. The most straightforward way of doing this is to create up to $(n+1)$ forwarding tables; one for the global prefixes, if any, and one for each of the (n) sites.

To protect inter site integrity; routers must be selective in the forwarding information that is shared with neighboring routers. Routing protocols routinely transmit their routing information to its neighboring routers. When a router is transmitting this routing information, it must not include any information about sites other than the site defined on the interface used to reach a neighbor.

As an example, the router in Figure 1 must advertise routing information on four interfaces. The information advertised is as follows:

- Interface 1
 - All global prefixes

- All site prefixes learned from Interfaces 1 and 2
- Interface 2
 - All global prefixes
 - All site prefixes learned from Interfaces 1 and 2
- Interface 3
 - All global prefixes
 - All site prefixes learned from Interface 3
- Interface 4
 - All global prefixes
 - No site prefixes

By imposing advertisement rules, site integrity is maintained by keeping all site routing information contained within the site.

4.2 Packet Forwarding

In addition to the extra cost of generating additional forwarding information for each site, site boundary routers must also do some additional checking when forwarding packets that contain site local addresses.

If a packet being forwarded contains a site local destination address, regardless of the scope of the source address, the router must perform the following:

- Lookup incoming interface's site identifier
- Perform route lookup for destination address in arrival interface's site scoped routing table

If a packet being forwarded contains a site local source address and a global scoped destination address, the following must be performed:

- Lookup outgoing interface's site identifier
- Compare inbound and outbound interfaces' site identifiers

If the site identifiers match, the packet can be forwarded. If they do not match, an ICMPv6 destination unreachable message must be sent to

the sender with a code value, code = 2 (beyond scope of source address).

[5. Scoped Multicast Routing](#)

With IPv6 multicast, there are multiple scopes supported. Multicast routers must be able to control the propagation of scoped packets based on administratively configured boundaries.

5.1 Routing Protocols

Multicast routing protocols must follow the same rules as the unicast protocols. They will be required to maintain information about global prefixes as well as information about all scope boundaries that exist on the router.

Multicast protocols that rely on underlying unicast protocols for route exchange (i.e. PIM, MOSPF) will not suffer as much of a performance impact since the unicast protocol will handle the forwarding table generation. They must be able to handle the additional scope boundaries used in multicast addresses.

Multicast protocols that generate and maintain their own routing tables will have to perform the additional route calculations for scope boundaries. All multicast protocols will be forced to handle fourteen additional scooping identifiers above the site identifiers supported in IPv6 unicast addresses.

5.2 Packet Forwarding

The following combinations describe the forwarding rules for multicast:

- Global multicast destination / Global unicast source
- Global multicast destination / Site local unicast source
- Scoped multicast destination / Global unicast source
- Scoped multicast destination / Site local unicast source

The first combination requires no special processing over what is currently in place for global IPv6 multicast. The remaining combinations should result in the router performing the same identifiers check as outlined for the site local unicast addresses. Since IPv6 multicast supports fifteen unique multicast scopes, it is assumed that scopes 0x1 through 0x4 are strictly less than the unicast site scope, scope 0x5 (site) is equal to the unicast site scope, scopes 0x6 through 0xd are strictly greater than the unicast site scope and strictly less than the unicast global scope, and scope 0xe is equal to the unicast global scope.

[6. Protocol Impact](#)

The performance impact on routing protocols is obvious. Routers

implementing scoped address support will be forced to perform an additional check in the main forwarding path to determine if the source address is a site-local address. This will add overhead to the processing of every packet flowing through the router. This overhead

Haberman

4

Internet Draft

Routing of Scoped IPv6 Addresses

November 1999

is no different than the overhead occurred in checking for invalid source addresses such as multicast addresses, the loopback address, and the unspecified address, which is a required function in IPv6. In addition, there will be storage overhead for the scope identifiers and the forwarding tables that must be maintained for each site.

[7.](#) Security Considerations

This document specifies a set of guidelines that allow routers to prevent site-specific information from leaking out of each site. If site boundary routers allow site routing information to be forwarded outside of the site, the integrity of the site could be compromised.

[8.](#) References

[RFC 2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), [BCP14](#), March 1999.

Acknowledgements

The author would like to thank Thomas Narten, Steve Deering, Erik Nordmark, Matt Crawford, and Jim Bound for their comments and reviews of this document.

Haberman

5

Author's Address

Brian Haberman
Nortel Networks
4309 Emperor Blvd.
Suite 200
Durham, NC 27703
1-919-992-4439
Email : haberman@nortelnetworks.com

