Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 12, 2008

A. Lindem
Redback Networks
A. Roy
Cisco Systems
S. Mirtorabi
Force10 Networks
September 9, 2007

OSPF Multi-Instance Extensions
draft-acee-ospf-multi-instance-00.txt

Status of this Memo

Copyright Notice

Abstract

OSPFv3 includes a mechanism for supporting multiple instances on the same link. OSPFv2 could benefit from such a mechanism in order to support multiple routing domains on the same subnet. The OSPFv2 instance ID is reserved for support of separate OSPFv2 protocol instances. This is different from OSPFv3 where it could be used for other purposes such as putting the same link in multiple areas. OSPFv2 supports this capability using a separate subnet or the OSPF multi-area adjacency capability.

Table of Contents

1. Introduction

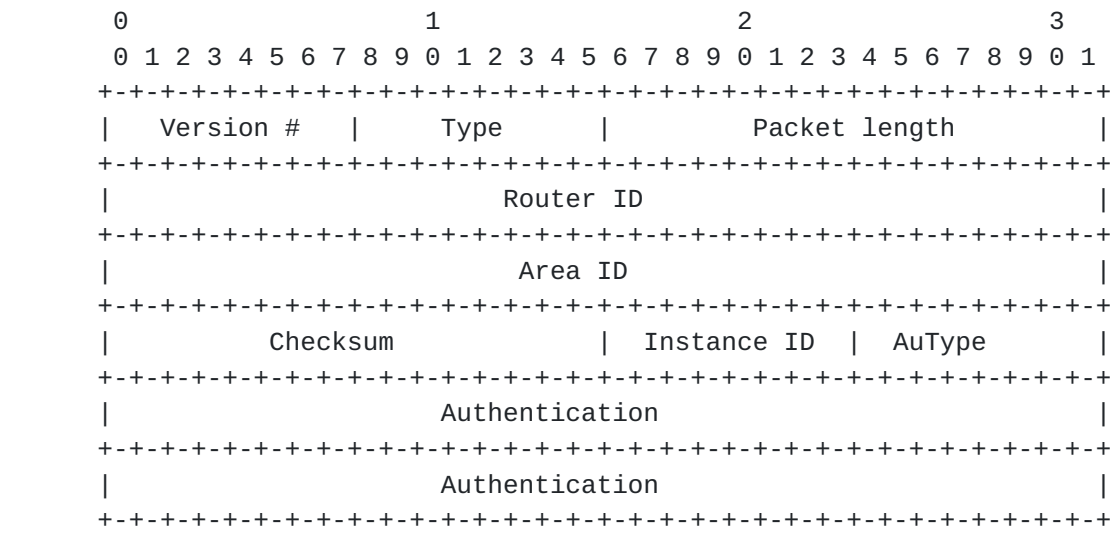
OSPFv3 [OSPFV3] includes a mechanism for supporting multiple instances on the same link. OSPFv2 [OSPFV2] could benefit from such a mechanism in order to support multiple routing domains on the same subnet. The OSPFv2 instance ID is reserved for support of separate OSPFv2 protocol instances. This is different from OSPFv3 where it could be used for other purposes such as putting the same link in multiple areas. OSPFv2 supports this capability using a separate subnet or the OSPF multi-area adjacency capability [MULTI-AREA].

1.1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC-KEYWORDS].

2. OSPFv2 Instance Packet Encoding

OSPFv2 currently doesn't offer a mechanism to differentiate packets for different instances sent and received on the same interface. In support of this capability, this document introduces a modified packet header format when the Authentication Type field is split into an instance ID and type.



The OSPFv2 Packet Header

Version #
The OSPFv2 version number - 2

Type
The OSPFv2 packet type as specified [OSPFV2].

Packet length
The length of the OSPF protocol packet in bytes. This length includes the standard OSPF header.

Router ID
The Router ID of the packet's source.

Area ID
A 32-bit number identifying the area corresponding the packet as specified in [OSPFV2].

Checksum
: OSPFv2 standard checksum calculation as specified in specified in [OSPFV2].

Instance ID
: Enables multiple instances of OSPF to be run over a single link. Each protocol instance would be assigned a separate Instance ID; the Instance ID has local subnet significance only. Received packets whose Instance ID is not equal to the receiving interface's Instance ID are discarded.

AuType
: OSPFv2 authentication type as specified in specified in [OSPFV2].

Authentication
: A 64-bit field for Authentication type dependent authentication data.

3. OSPF Interface Instance ID

OSPF [OSPFV2] describes the conceptual interface data structure in section 9. The OSPF Interface ID will be added to this structure. The Interface Instance ID will default to 0. Its setting to a non-zero value may be accomplished through configuration or implied by some usage beyond the scope of this document.

3.1. Sending and Receiving OSPF packets

When sending OSPF packets, if the interface instance ID has a non-zero value, it will be set in the OSPF packet header. When receiving OSPF packets, the OSPFv2 Header Instance ID will be used to aid in demultiplexing the packet and routing it to the correct OSPFv2 instance.

4. Backward Compatibility and Deployment Considerations

When there are OSPF routers that support this capability on the same broadcast capable link as those that do not, packets with non-zero Instance IDs will be received by those legacy routers. Since the authentication type will be unknown to them they will not process the packet. This is what is desired. However, the impact varies by implementation and some implementations may log every single authentication type mismatch.

4.1. Separate Multicast Addresses for Backward Compatibility

Another way to avoid the backward compatibility problem would be to use new IPv4 multicast addresses for OSPF multicast packets with non-zero instance IDs. We would need to reserve two, one for AllSPFRouters and another for ALLDRouters. This would have the added benefit that the OSPF routers not supporting this specification would not receive the packet or at least drop it silently at an earlier junction. However, it isn't clear whether this is justified simply for migration.

4.2. Separate Protocol ID for Backward Compatibility

Another way to avoid the backward compatibility problem would be to use a different IPv4 header protocol ID for OSPF packets with non-zero instance IDs. This approach would have the added benefit of allowing all packets associated with a non-zero Instance ID to be identified at the IP layer. This may be desirable for some applications utilizing multiple instances.

5. Security Considerations

The enhancement described herein doesn't add any additional security considerations to OSPFv2. Security considerations for OSPFv2 are described in [OSPFV2].

Given that only three OSPFv2 authentication types have been standardized, it seems reasonable to reduce the OSPF packet header field to 8 bits.

6. IANA Considerations

A new registry will be added for OSPF Instance IDs. The allocation is TBD.

Dependent on the approach, two new multicast addresses from the IPv4 Multicast Addresses registry would need to be allocated.

Dependent on the approach, a new protocol ID may need to be allocated from the Protocol Numbers registry.

7. Normative References

[MULTI-AREA]
Mirtorabi, S., Psenak, P., Lindem, A., and A. Oswal, "OSPF Multi-Area Adjacency", draft-ietf-ospf-multi-area-adj-08.txt (work in progress).

[OSPFV2] Moy, J., "OSPF Version 2", RFC 2328, April 1998.

[OSPFV3] Coltun, R., Ferguson, D., and J. Moy, "OSPF for IPv6", RFC 2740, April 2007.

[RFC-KEYWORDS]
Bradner, S., "Key words for use in RFC's to Indicate Requirement Levels", RFC 2119, March 1997.

Appendix A. Acknowledgments

The RFC text was produced using Marshall Rose's xml2rfc tool.

Authors' Addresses

Acee Lindem
Redback Networks
102 Carric Bend Court
Cary, NC 27519
USA

Email: acee@redback.com

Abhay Roy
Cisco Systems
225 West Tasman Drive
San Jose, CA 95134
USA

Email: akr@cisco.com

Sina Mirtorabi
Force10 Networks
350 Holger Way
San Jose, CA 95134
USA

Email: sina@force10networks.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).