                     OSPFv2 Multi-Instance Extensions

Abstract

   OSPFv3 includes a mechanism to support multiple instances of the
   protocol running on the same interface. OSPFv2 can utilize such a
   mechanism in order to support multiple routing domains on the same
   subnet.

   This document defines the OSPFv2 Instance ID to enable separate
   OSPFv2 protocol instances on the same interface. Unlike OSPFv3 where
   the Instance ID can be used for multiple purposes, such as putting
   the same interface in multiple areas, the OSPFv2 Instance ID is
   reserved for identifying protocol instances.

   This document updates RFC 2328.

Status of This Memo

Table of Contents

1. Introduction

   OSPFv3 [OSPFV3] includes a mechanism to support multiple instances of
   a protocol running on the same interface. OSPFv2 [OSPFV2] can
   utilize such a mechanism in order to support multiple routing domains
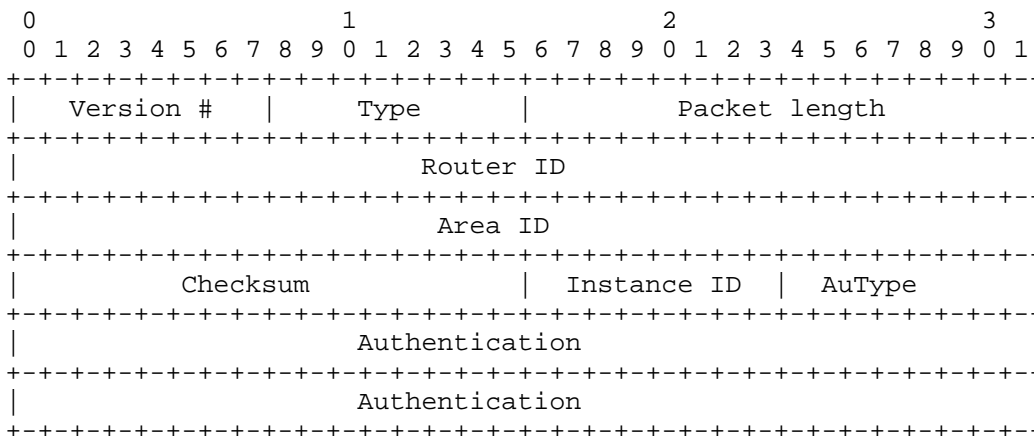   on the same subnet.

   This document defines the OSPFv2 Instance ID to enable separate
   OSPFv2 protocol instances on the same interface. Unlike OSPFv3 where
   the Instance ID can be used for multiple purposes, such as putting
   the same interface in multiple areas, the OSPFv2 Instance ID is
   reserved for identifying protocol instances.

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

   This document extends OSPFv2 with a mechanism to differentiate
   packets for different instances sent and received on the same
   interface. In support of this capability, a modified packet header
   format with the Authentication Type field split into an Instance ID
   and AuType.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Version #   |     Type      |         Packet length         |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                          Router ID                            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                           Area ID                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |           Checksum            |  Instance ID  |    AuType     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Authentication                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                       Authentication                          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

                       The OSPFv2 Packet Header

   All fields are as defined in [OSPFV2] except that the Instance ID
   field is new, and the AuType field is reduced to 8 bits from 16 bits
   without any change in meaning. The Instance ID field is defined as
   follows:

   Instance ID
      Enables multiple instances of OSPFv2 to be used on a single
      interface. Each protocol instance would be assigned a separate
      Instance ID; the Instance ID has local subnet significance only.
      Received packets with an Instance ID not equal to one of the
      Instance IDs corresponding to one of the configured OSPFv2
      Instances for the receiving interface MUST be discarded.

3. OSPFv2 Interface Instance ID

   Section 9 of [OSPFV2] describes the conceptual interface data
   structure. The OSPFv2 Interface Instance ID is added to this
   structure. The OSPFv2 Interface Instance ID has a default value of
   0. Setting it to a non-zero value may be accomplished through
   configuration.

3.1. Sending and Receiving OSPFv2 Packets

   When sending OSPFv2 packets, the OSPFv2 Interface Instance ID is set
   in the OSPFv2 packet header. When receiving OSPFv2 packets, the
   OSPFv2 Header Instance ID is used to aid in demultiplexing the packet
   and associating it with the correct OSPFv2 instance. Received
   packets with an Instance ID not equal to one of the configured OSPFv2
   Instance IDs on the receiving interface MUST be discarded.

3.2. Interface Instance ID Values

   The following OSPFv2 Instance IDs have been defined:

   0   Base IPv4 Instance - This is the default IPv4 routing instance
           corresponding to default IPv4 unicast routing and the
           attendant IPv4 routing table. Use of this Instance ID
           provides backward compatibility with the base OSPF
           specification [OSPFV2].

   1   Base IPv4 Multicast Instance - This IPv4 instance corresponds
           to the separate IPv4 routing table used for the Reverse Path
           Forwarding (RPF) checking performed on IPv4 multicast traffic.

   2   Base IPv4 In-band Management Instance - This IPv4 instance
           corresponds to a separate IPv4 routing table used for network
           management applications.

   3-127   Private Use - These Instance IDs are reserved for definition
           and semantics defined by the local network administrator. For
           example, separate Interface Instance IDs and their
           corresponding OSPFv2 instances could be used to support
           independent non-congruent topologies for different classes of
           IPv4 unicast traffic. The details of such deployments are
           beyond the scope of this document.

   The first three Interface Instance IDs are analogous to the topology
   IDs defined in [RFC4915].

4. State-Sharing Optimizations between OSPFv2 Instances

   This is beyond the scope of this document and is an area for further
   study.

5. OSPFv2 Authentication Impacts

   Now that the AuType OSPFv2 header field has been reduced from 2
   octets to 1 octet, OSPFv2 routers not supporting this specification
   will fail packet authentication for any instance other than the
   default (i.e., the Base IPv4 Unicast Instance). This is solely due
   to the difference in field definition as opposed to any explicit
   change to OSPFv2 authentication, as described in Appendix D of RFC
   2328 [OSPFV2] and RFC 5709 [RFC5709]. However, this is exactly what
   is desired since OSPFv2 routers not supporting this specification
   should only support the default instance (refer to Section 6).

6. Backward Compatibility and Deployment Considerations

   When there are OSPFv2 routers that support OSPFv2 Multi-Instance
   extensions on the same broadcast-capable interface as OSPFv2 routers
   that do not, packets with non-zero OSPFv2 header Instance IDs are
   received by those legacy OSPFv2 routers. Since the non-zero Instance
   ID is included in the AuType by these legacy OSPFv2 routers, it is
   misinterpreted as a mismatched authentication type and the packet is
   dropped. This is exactly what is expected and desired.

   Previously, there was concern that certain implementations would log
   every single authentication type mismatch. However, discussions with
   implementers have led us to the conclusion that this is not as severe
   a problem as we'd first thought, and it will be even less of a
   problem by the time the mechanism described herein is standardized,
   implemented, and deployed. Most implementations will dampen the
   logging of errors. Hence, the more drastic mechanisms to avoid
   legacy OSPFv2 routers from receiving multicast OSPFv2 packets with
   non-zero Instance IDs have been removed.

   If the OSPF MIB as specified in [OSPF-MIB] is implemented, even the
   damped generation of the ospfIfAuthFailure or ospfVirtIfAuthFailure
   Simple Network Management Protocol (SNMP) notifications would be
   undesirable in situations where legacy OSPFv2 routers are deployed on
   the same subnet as OSPFv2 routers supporting this specification.
   Consequently, it is recommended that implementations that implement
   this specification and the OSPF MIB also implement SNMP Notification
   filtering as specified in Section 6 of [RFC3413].

7. Security Considerations

   The enhancement described herein doesn't include 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 OSPFv2 packet header
   field to 8 bits.

8. IANA Considerations

   The size of the AuType field is reduced from 16 octets to 8 octets.
   This changes the OSPF Authentication Codes registry in that the
   values 256-65535 are no longer defined and are therefore deprecated.
   There is no backward compatibility issue since this range of values
   was previously defined as "Reserved and should not be assigned".

   A new registry has been created for OSPFv2 Instance IDs. The initial
   allocation of OSPFv2 Instance IDs is described below. Refer to
   Section 3.2 for more information.

   +-------------+---------------------+-------------------+
   | Value/Range | Designation | Assignment Policy |
   +-------------+---------------------+-------------------+
0	Base IPv4 Unicast	Assigned
	Instance	
1	Base IPv4 Multicast	Assigned
	Instance	
2	Base IPv4 In-band	Assigned
	Management Instance	
3-127	Private Use	Reserved for local
		policy assignment
128-255	Unassigned	Standards Action
   +-------------+---------------------+-------------------+

                        OSPFv2 Instance ID

9. References

9.1. Normative References

   [OSPFV2]   Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

   [OSPFV3]   Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF
               for IPv6", RFC 5340, July 2008.

   [RFC-KEYWORDS]
               Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

9.2. Informative References

   [OSPF-MIB] Joyal, D., Ed., Galecki, P., Ed., Giacalone, S., Ed.,
               Coltun, R., and F. Baker, "OSPF Version 2 Management
               Information Base", RFC 4750, December 2006.

   [RFC3413]   Levi, D., Meyer, P., and B. Stewart, "Simple Network
               Management Protocol (SNMP) Applications", STD 62, RFC
               3413, December 2002.

   [RFC4915]   Psenak, P., Mirtorabi, S., Roy, A., Nguyen, L., and P.
               Pillay-Esnault, "Multi-Topology (MT) Routing in OSPF", RFC
               4915, June 2007.

   [RFC5709]   Bhatia, M., Manral, V., Fanto, M., White, R., Barnes, M.,
               Li, T., and R. Atkinson, "OSPFv2 HMAC-SHA Cryptographic
               Authentication", RFC 5709, October 2009.

Appendix A. Acknowledgments

   Thanks to Adrian Farrel for reviewing and providing some suggested
   improvements during the IESG review.

   Thanks to Paul Wells for commenting on the backward compatibility
   issues.

   Thanks to Paul Wells and Vladica Stanisic for commenting during the
   OSPF WG last call.

   Thanks to Manav Bhatia for comments and for being the document
   shepherd.

   Thanks to Magnus Nystrom for comments under the auspices of the
   Security Directorate review.

   Thanks to Dan Romascanu for comments during the IESG review.

   Thanks to Pete McCann for comments under the auspices of the Gen-ART
   review.

Authors' Addresses

   Acee Lindem
   Ericsson
   102 Carric Bend Court
   Cary, NC 27519
   USA

   EMail: acee.lindem@ericsson.com

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

   EMail: akr@cisco.com

   Sina Mirtorabi
   Cisco Systems
   3 West Plumeria Drive
   San Jose, CA 95134
   USA

   EMail: sina@cisco.com