

Network Working Group  
Internet Draft  
Document: [draft-ietf-ospf-ospfv3-auth-01.txt](#)  
Expires: October 2003

M. Gupta  
Nokia  
N. Melam  
Nokia  
April 2003

## Authentication/Confidentiality for OSPFv3

### Status of this Memo

This document is an Internet-Draft and is subject to 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/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at

<http://www.ietf.org/shadow.html>.

### Abstract

This document describes means/mechanisms to provide authentication/confidentiality to OSPFv3 using IPv6 AH/ESP Extension Header.

### Conventions used in this document

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-2119](#) [5].

### Table of Contents

|  |                   |
|--|-------------------|
| <a href="#">1. Introduction.....</a>                             | <a href="#">2</a> |
| <a href="#">2. OSPFv2 to OSPFv3.....</a>                         | <a href="#">2</a> |
| <a href="#">3. Authentication.....</a>                           | <a href="#">2</a> |
| <a href="#">4. Confidentiality.....</a>                          | <a href="#">3</a> |
| <a href="#">5. Authentication and Encryption Algorithms.....</a> | <a href="#">3</a> |
| <a href="#">6. Key Management.....</a>                           | <a href="#">3</a> |



|  |                   |
|--|-------------------|
| <a href="#">7. SA Granularity and Selectors.....</a> | <a href="#">4</a> |
| <a href="#">8. Virtual Links.....</a>                | <a href="#">5</a> |
| <a href="#">9. IPsec rules.....</a>                  | <a href="#">5</a> |
| <a href="#">10. Replay Protection.....</a>           | <a href="#">6</a> |
| <a href="#">Security Considerations.....</a>         | <a href="#">6</a> |
| <a href="#">References.....</a>                      | <a href="#">7</a> |
| <a href="#">Acknowledgments.....</a>                 | <a href="#">7</a> |
| <a href="#">Authors' Addresses.....</a>              | <a href="#">7</a> |

## [1. Introduction](#)

In OSPFv3 for IPv6, authentication fields have been removed from OSPF headers. When running over IPv6, OSPF relies on the IPv6 Authentication Header (AH) and IPv6 Encapsulating Security Payload (ESP) to ensure integrity, authentication and/or confidentiality of routing exchanges.

This document describes how IPv6 AH/ESP extension headers can be used to provide authentication/confidentiality to OSPFv3.

It is assumed that the reader is familiar with OSPFv3 [1], AH [4], ESP [3], the concept of security associations, tunnel and transport mode of IPsec and the key management options available for AH and ESP (manual keying and IKE) [2].

## [2. OSPFv2 to OSPFv3](#)

Security concerns MUST be taken away from OSPFv3 protocol and IPv6 stack MUST provide inherent security to OSPFv3 by using AH/ESP extension headers. It means OSPFv3 protocol MUST not receive any unauthenticated packets. As OSPFv2 has its own security mechanisms, no inherent security needs to be provided by the IPv4 stack. As OSPFv2 is only for IPv4 and OSPFv3 is only for IPv6, the distinction between the packets can be easily made by IP version.

Authentication and confidentiality, if provided, MUST be provided to the entire OSPFv3 header and data. Authentication to the selected portions of IPv6 header, selected portions of extension headers and selected options may also be provided optionally.

## [3. Authentication](#)

Transport mode SA is the security association between two hosts or security gateways that are acting as hosts. SA must be tunnel mode if either end of the security association is a security gateway. OSPFv3 packets are exchanged between the routers but as the packets are destined to the routers, the routers act like host in this case. So



transport mode SA MUST be used in order to provide required security to OSPFv3.

In order to support OSPFv3 authentication, "ESP with NULL encryption" MUST be supported in transport mode. "AH" in transport mode SHOULD also be provided. AH in transport mode provides authentication to higher layer protocols, selected portions of IPv6 header, selected portions of extension headers and selected options. ESP with NULL encryption in transport mode will provide authentication to only higher layer protocol data and not to the IPv6 header, extension headers and options.

OSPF packets received in clear text and OSPF received with incorrect AH ICV MUST be dropped when authentication is enabled.

#### **4. Confidentiality**

Providing confidentiality to OSPFv3 in addition to authentication is optional. Confidentiality must be implemented using ESP extension header of IPv6 if it is being provided. ESP with non-null encryption in transport mode MUST be used for the providing confidentiality to OSPFv3.

#### **5. Authentication and Encryption Algorithms**

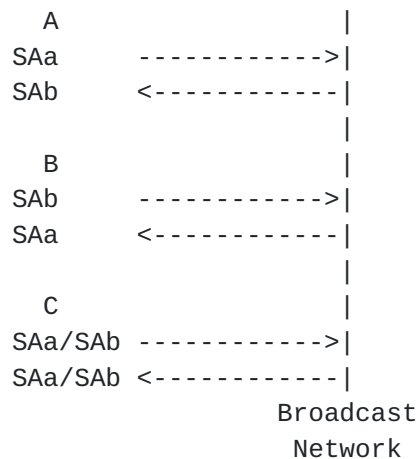
The implementations MUST be conformant to the RFCs that describe mandatory-to-implement algorithms for use with ESP and AH.

#### **6. Key Management**

OSPFv3 exchanges both multicast and unicast packets. While running OSPFv3 over a broadcast interface, the authentication/confidentiality required is "one to many". Since IKE is based on the Diffie-Hellman key agreement protocol and works only for two communicating parties, it is not possible to use IKE for providing the required "one to many" authentication/confidentiality. Manual keying MUST be used for this purpose. In manual keying SAs are statically installed on the routers and these static SAs are used to encrypt/authenticate the data.

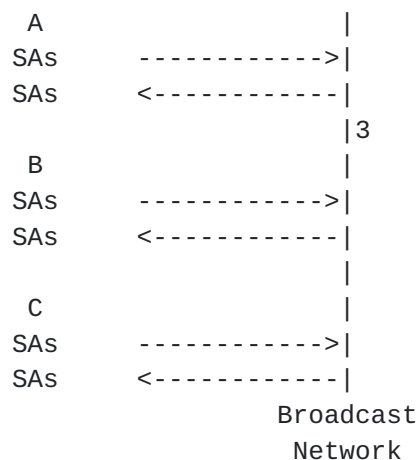
Since security associations (SAs) are directional, generally different security associations are used for inbound and outbound processing for providing higher security. The following figure explains that it is not possible to use different security associations for inbound and outbound processing in order to provide the required "one to many" security.





If we consider communication between A and B in the above diagram, everything seems to be fine. A uses security association SAa for outgoing packets and B uses the same for incoming packets and vice versa. Now if we include C in the group and C sends a packet out using SAa then only A will be able to understand it or if C sends the packets out using SAb then only B will be able to understand it. Since the packets are multicast packets and they are going to be processed by both A and B, there is no SA for C to use so that A and B both can understand it.

The problem can be solved with the following figure where all of them use the same SA for incoming and outgoing direction.



So, all the adjacent routers on a broadcast medium MUST use the same SA and the same SA MUST be used for inbound and outbound processing.

## 7. SA Granularity and Selectors

The user SHOULD be given a choice to share the same SA among multiple interfaces or using unique SA per interface.





## 8. Virtual Links

Different SA than the SA of underlying interface MUST be provided for virtual links. Packets sent out on virtual links use unicast site local or global IPv6 addresses as the IPv6 source address and all the other packets use multicast and unicast link local addresses. This difference in the IPv6 source address should be used in order to differentiate the packets sent on interfaces and virtual links.

As the end point IP addresses of the virtual links are not known at the time of configuration, the secure channel for these packets need to be setup dynamically. The end point IP addresses of virtual links are learnt during the routing table build up process. The packet exchange over the virtual links starts only after the discovery of end point IP addresses. In order to provide security to these exchanges, the routing module should setup a secure IPsec channel dynamically once it acquires the required information.

According to the OSPFv3 RFC, the virtual neighbor's IP address is set to the first prefix with the "LA-bit" set from the list of prefixes in intra-area-prefix-LSAs originated by the virtual neighbor. But when it comes to choosing the source address for the packets that are sent over the virtual link, the RFC simply suggests using one of the router's own site-local or global IPv6 addresses. In order to install the required rules for virtual links, the source address also needs to be predictable. So the router MUST use the first prefix with the "LA-bit" set from the list of its own intra-area-prefix-LSAs as the source address of the packet. This makes both the source and destination address of the packets exchanged over the virtual link, predictable on both the routers.

## 9. IPsec rules

The following set of rules can be installed in a typical IPsec implementation to provide the authentication/confidentiality to OSPFv3 packets.

Outbound Rules for interface running OSPFv3 security:

| No. | interface | source    | destination | protocol | action |
|-----|-----------|-----------|-------------|----------|--------|
| 1   | iface     | fe80::/10 | any         | OSPF     | apply  |
| 2   | any       | src/128   | dst/128     | OSPF     | apply  |

Inbound Rules for interface running OSPFv3 security:

| No. | interface | source    | destination | protocol  | action |
|-----|-----------|-----------|-------------|-----------|--------|
| 3   | iface     | fe80::/10 | any         | ESP or AH | apply  |
| 4   | iface     | fe80::/10 | any         | OSPF      | drop   |
| 5   | any       | src/128   | dst/128     | ESP or AH | apply  |



|   |     |         |         |      |      |
|---|-----|---------|---------|------|------|
| 6 | any | src/128 | dst/128 | OSPF | drop |
|---|-----|---------|---------|------|------|

For outbound rules, action "apply" means encrypting/calculating ICV and adding ESP or AH header. For inbound rules, action "apply" means decrypting/authenticating the packets and stripping ESP or AH header.

Rules 4 and 6 are to drop the in-secure OSPFv3 packets without ESP/AH headers.

Rules 2, 5 and 6 are meant to secure the packets being exchanged over virtual links. These rules are dynamically installed after learning the end point IP addresses of a virtual link. These rules **MUST** be installed on at least the interfaces that are connected to the transit area for the virtual link. These rules **MAY** alternatively be installed on all the interfaces. If these rules are not installed on all the interfaces, clear text or malicious OSPFv3 packets with same source and destination addresses as virtual link end point addresses will be delivered to OSPFv3. Though OSPFv3 drops these packets because they were not received on the right interface, OSPFv3 receives some clear text or malicious packets even when the security is on. Installing these rules on all the interfaces insures that OSPFv3 does not receive these clear text or malicious packets when security is turned on. On the other hand installing these rules on all the interfaces increases the processing overhead on the interfaces where there is no IPsec processing otherwise. The decision of installing these rules on all the interfaces or on just the interfaces that are connected to the transit area is a private decision and doesn't affect the interoperability in any way. So this decision is left to the implementers.

Rules 1, 3 and 4 are meant to secure the unicast and multicast packets that are not being exchanged over the virtual links. These rules are interface specific.

## **10. Replay Protection**

As it is not possible as per the current standards to provide complete replay protection while using manual keying, the proposed solution will not provide protection against replay attacks.

Fields LS age, LS Sequence Number and LS checksum in LSA header are kept intact in OSPFv3. Though these fields do not provide the complete protection, they certainly help against replay attacks.

## **Security Considerations**

This memo discusses the use of IPsec AH and ESP headers in order to provide security to OSPFv3 for IPv6.



The use of manual keying does not provide very high level of security as compared to IKE but the security provided should be adequate for a routing protocol.

## References

1. Coltun, R., Ferguson, D. and Moy, J., "OSPF for IPv6", [RFC 2740](#), December 1999
2. Kent, S. and Atkinson, R., "Security Architecture for the Internet Protocol", [RFC 2401](#), November 1998
3. Kent, S. and Atkinson, R., "IP Encapsulating Security Payload (ESP)", [RFC 2406](#), November 1998
4. Kent, S. and Atkinson, R., "IP Authentication Header (AH)", [RFC 2402](#), November 1998
5. Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", [BCP 14](#), [RFC 2119](#), March 1997.

## Acknowledgments

Authors would like to extend sincere thanks to Marc Solsona, Janne Peltonen, John Cruz, Dhaval Shah and Abhay Roy for providing useful information and critiques in order to write this memo.

We would also like to thank IPsec and OSPF WG people to provide valuable review comments.

## Authors' Addresses

Mukesh Gupta  
Nokia  
313 Fairchild Drive  
Mountain View, CA 94043  
Phone: 650-625-2264  
Email: Mukesh.Gupta@nokia.com

Nagavenkata Suresh Melam  
Nokia  
313 Fairchild Drive  
Mountain View, CA 94043  
Phone: 650-625-2949  
Email: Nagavenkata.Melam@nokia.com

