

Network Working Group  
Request for Comments: 3101  
Obsoletes: 1587  
Category: Standards Track

P. Murphy  
US Geological Survey  
January 2003

## The OSPF Not-So-Stubby Area (NSSA) Option

### Status of this Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

### Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

### Abstract

This memo documents an optional type of Open Shortest Path First (OSPF) area that is somewhat humorously referred to as a "not-so-stubby" area (or NSSA). NSSAs are similar to the existing OSPF stub area configuration option but have the additional capability of importing AS external routes in a limited fashion.

The OSPF NSSA Option was originally defined in RFC 1587. The functional differences between this memo and RFC 1587 are explained in Appendix F. All differences, while expanding capability, are backward-compatible in nature. Implementations of this memo and of RFC 1587 will interoperate.

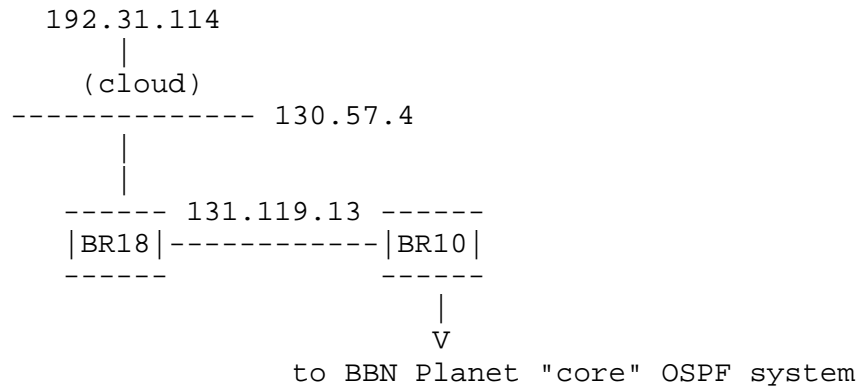
## Table Of Contents

|  |    |
|--|----|
| 1.0 Overview .....                                 | 2  |
| 1.1 Motivation - Transit Networks .....            | 2  |
| 1.2 Motivation - Corporate Networks .....          | 4  |
| 1.3 Proposed Solution .....                        | 5  |
| 2.0 NSSA Intra-Area Implementation Details .....   | 7  |
| 2.1 The N-bit .....                                | 7  |
| 2.2 Type-7 Address Ranges .....                    | 7  |
| 2.3 Type-7 LSAs .....                              | 8  |
| 2.4 Originating Type-7 LSAs .....                  | 9  |
| 2.5 Calculating Type-7 AS External Routes .....    | 10 |
| 2.6 Incremental Updates .....                      | 14 |
| 2.7 Optionally Importing Summary Routes .....      | 14 |
| 3.0 Intra-AS Implementation Details .....          | 15 |
| 3.1 Type-7 Translator Election .....               | 15 |
| 3.2 Translating Type-7 LSAs into Type-5 LSAs ..... | 16 |
| 3.3 Flushing Translated Type-7 LSAs .....          | 19 |
| 4.0 Security Considerations .....                  | 20 |
| 5.0 Acknowledgements .....                         | 21 |
| 6.0 Contributors .....                             | 22 |
| 7.0 References .....                               | 22 |
| Appendix A: The Options Field .....                | 23 |
| Appendix B: Router-LSAs .....                      | 24 |
| Appendix C: Type-7 LSA Packet Format .....         | 26 |
| Appendix D: Configuration Parameters .....         | 27 |
| Appendix E: The P-bit Policy Paradox .....         | 28 |
| Appendix F: Differences from RFC 1587 .....        | 30 |
| Author's Addresses .....                           | 32 |
| Full Copyright Statement .....                     | 33 |

## 1.0 Overview

## 1.1 Motivation - Transit Networks

Wide-area transit networks often have connections to moderately complex "leaf" sites. A leaf site may have multiple IP network numbers assigned to it. Typically, one of the leaf site's networks is directly connected to a router provided and administered by the transit network while the others are distributed throughout and administered by the site. From the transit network's perspective, all of the network numbers associated with the site make up a single "stub" entity. For example, BBN Planet has one site composed of a class-B network, 130.57.0.0, and a class-C network, 192.31.114.0. From BBN Planet's perspective, this configuration looks something like the diagram on the next page, where the "cloud" consists of the subnets of 130.57 and network 192.31.114, all of which are learned by RIP on router BR18.



Topologically, this cloud looks very much like an OSPF stub area. The advantages of running the cloud as an OSPF stub area are:

1. External routes learned from OSPF's Type-5 AS-external-LSAs are not advertised beyond the router labeled "BR10". This is advantageous because the link between BR10 and BR18 may be a low-speed link or the router BR18 may have limited resources.
2. The transit network is abstracted to the "leaf" router BR18 by advertising only a default route across the link between BR10 and BR18.
3. The cloud becomes a single, manageable "leaf" with respect to the transit network.
4. The cloud can become, logically, a part of the transit network's OSPF routing system.

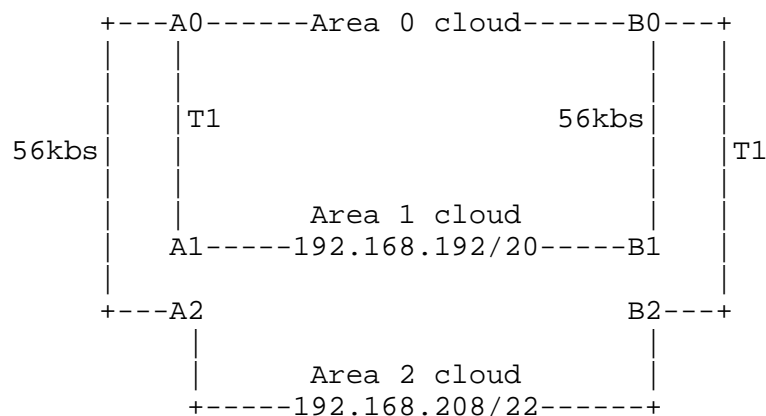
However, the original definition of the OSPF protocol (See [OSPF]) imposes topological limitations that restrict simple cloud topologies from becoming OSPF stub areas. In particular, it is illegal for a stub area to import routes external to OSPF; thus it is not possible for routers BR18 and BR10 to both be members of the stub area and to import into OSPF as Type-5 AS-external-LSAs routes learned from RIP or other IP routing protocols. In order to run OSPF out to BR18, BR18 must be a member of a non-stub area or the OSPF backbone before it can import routes other than its directly connected network(s). Since it is not acceptable for BR18 to maintain all of BBN Planet's Type-5 AS external routes, BBN Planet is forced by OSPF's topological limitations to only run OSPF out to BR10 and to run RIP between BR18 and BR10.

## 1.2 Motivation - Corporate Networks

In a corporate network that supports a large corporate infrastructure it is not uncommon for its OSPF domain to have a complex non-zero area infrastructure that injects large routing tables into its Area 0 backbone. Organizations within the corporate infrastructure may routinely multi-home their non-zero OSPF areas to strategically located Area 0 backbone routers, either to provide backbone redundancy or to increase backbone connectivity or both. Because of these large routing tables, OSPF aggregation via summarization is routinely used and recommended. Stub areas are also recommended to keep the size of the routing tables of non-backbone routers small. Organizations within the corporation are administratively autonomous and compete for corporate backbone resources. They also want isolation from each other in order to protect their own network resources within the organization.

Consider the typical example configuration shown below where routers A1, B1 and A2, B2 are connected to Area 1 and Area 2 respectively, and where routers A0 and B0 are Area 0 border routers that connect to both Area 1 and Area 2. Assume the 192.168.192/20 and 192.168.208/22 clouds are subnetted with a protocol different from the corporate OSPF instance. These other protocols could be RIP, IGRP, or second and third OSPF instances separate from the corporate OSPF backbone instance.

Area 1 and Area 2 would like to be stub areas to minimize the size of their link state databases. It is also desirable to originate two aggregated external advertisements for the subnets of 192.168.192/20 and 192.168.208/22 in such a way that the preferred path to 192.168.192/20 is through A0 and the preferred path to 192.168.208/22 is through B0.



The current standard OSPF stub area has no mechanism to support the redistribution of routes for the subnets of 192.168.192/20 and 192.168.208/22 within a stub area or the ability to aggregate a range of external routes in any OSPF area. Any solution to this dilemma must also honor Area 1's path of choice to 192.168.192/20 through A0 with redundancy through B0 while at the same time honoring Area 2's path of choice to 192.168.208/20 through B0 with redundancy through A0.

### 1.3 Proposed Solution

This document describes a new optional type of OSPF area, somewhat humorously referred to as a "not-so-stubby" area (or NSSA), which has the capability of importing external routes in a limited fashion.

The OSPF specification defines two general classes of area configuration. The first allows Type-5 LSAs to be flooded throughout the area. In this configuration, Type-5 LSAs may be originated by routers internal to the area or flooded into the area by area border routers. These areas, referred to herein as Type-5 capable areas (or just plain areas in the OSPF specification), are distinguished by the fact that they can carry transit traffic. The backbone is always a Type-5 capable area. The second type of area configuration, called stub, does not allow Type-5 LSAs to be propagated into/throughout the area and instead depends on default routing to external destinations.

NSSAs are defined in much the same manner as existing stub areas. To support NSSAs, a new option bit (the "N" bit) and a new type of LSA (Type-7) are defined. The "N" bit ensures that routers belonging to an NSSA agree on its configuration. Similar to the stub area's use of the "E" bit, both NSSA neighbors must agree on the setting of the "N" bit or the OSPF neighbor adjacency will not form.

Type-7 LSAs provide for carrying external route information within an NSSA. Type-7 LSAs have virtually the same syntax as Type-5 LSAs with the obvious exception of the link-state type. (See section 2.3 for more details.) Both LSAs are considered a type of OSPF AS-external-LSA. There are two major semantic differences between Type-5 LSAs and Type-7 LSAs.

- o Type-7 LSAs may be originated by and advertised throughout an NSSA; as with stub areas, Type-5 LSAs are not flooded into NSSAs and do not originate there.
- o Type-7 LSAs are advertised only within a single NSSA; they are not flooded into the backbone area or any other area by border routers, though the information that they contain may be propagated into the backbone area. (See Section 3.2.)

In order to allow limited exchange of external information across an NSSA border, NSSA border routers will translate selected Type-7 LSAs received from the NSSA into Type-5 LSAs. These Type-5 LSAs will be flooded to all Type-5 capable areas. NSSA border routers may be configured with address ranges so that multiple Type-7 LSAs may be aggregated into a single Type-5 LSA. The NSSA border routers that perform translation are configurable. In the absence of a configured translator one is elected.

In addition, an NSSA border router should originate a default LSA (IP network is 0.0.0.0/0) into the NSSA. Default routes are necessary because NSSAs do not receive full routing information and must have a default route in order to route to AS-external destinations. Like stub areas, NSSAs may be connected to the Area 0 backbone at more than one NSSA border router, but may not be used as a transit area. Note that a Type-7 default LSA originated by an NSSA border router is never translated into a Type-5 LSA, however, a Type-7 default LSA originated by an NSSA internal AS boundary router (one that is not an NSSA border router) may be translated into a Type-5 LSA.

Like stub areas, NSSA border routers optionally import summary routes into their NSSAs as Type-3 summary-LSAs. If the import is disabled, particular care should be taken to ensure that summary routing is not obscured by an NSSA's Type-7 AS-external-LSAs. This may happen when the AS's other IGPs, like RIP and ISIS, leak routing information into the NSSA. In these cases all summary routes should be imported into the NSSA. The recommended default behavior is to import summary routes into NSSAs. Since Type-5 AS-external-LSAs are not flooded into NSSAs, NSSA border routers should not originate Type-4 summary-LSAs into their NSSAs. Also an NSSA's border routers never originate Type-4 summary-LSAs for the NSSA's AS boundary routers, since Type-7 AS-external-LSAs are never flooded beyond the NSSA's border.

When summary routes are not imported into an NSSA, the default LSA originated into it by its border routers must be a Type-3 summary-LSA. This default summary-LSA insures intra-AS connectivity to the rest of the OSPF domain, as its default summary route is preferred over the default route of a Type-7 default LSA. Without a default summary route the OSPF domain's inter-area traffic, which is normally forwarded by summary routes, might exit the AS via the default route of a Type-7 default LSA originated by an NSSA internal router. The Type-7 default LSAs originated by NSSA internal routers and the no-summary option are mutually exclusive features. When summary routes are imported into the NSSA, the default LSA originated by a NSSA border router into the NSSA should be a Type-7 LSA.

In our transit topology example the subnets of 130.57 and network 192.31.114 will still be learned by RIP on router BR18, but now both

BR10 and BR18 can be in an NSSA and all of BBN Planet's external routes are hidden from BR18; BR10 becomes an NSSA border router and BR18 becomes an AS boundary router internal to the NSSA. BR18 will import the subnets of 130.57 and network 192.31.114 as Type-7 LSAs into the NSSA. BR10 then translates these routes into Type-5 LSAs and floods them into BBN Planet's backbone.

In our corporate topology example if Area 1 and Area 2 are NSSAs the external paths to the subnets of the address ranges 192.168.192/20 and 192.168.208/22 can be redistributed as Type-7 LSAs throughout Area 1 and Area 2 respectively, and then aggregated during the translation process into separate Type-5 LSAs that are flooded into Area 0. A0 may be configured as Area 1's translator even though B0 is the translator of Area 2.

## 2.0 NSSA Intra-Area Implementation Details

### 2.1 The N-bit

The N-bit ensures that all members of an NSSA agree on the area's configuration. Together, the N-bit and E-bit reflect an interface's (and consequently the interface's associated area) external LSA flooding capability. As explained in [OSPF] Section 10.5, if Type-5 LSAs are not flooded into/throughout the area, the E-bit must be clear in the option field of the received Hello packets. Interfaces associated with an NSSA will not send or receive Type-5 LSAs on that interface but may send and receive Type-7 LSAs. Therefore, if the N-bit is set in the options field, the E-bit must be clear.

To support the NSSA option an additional check must be made in the function that handles the receiving of the Hello packet to verify that both the N-bit and the E-bit found in the Hello packet's option field match the area type and ExternalRoutingCapability of the area of the receiving interface. A mismatch in the options causes processing of the received Hello packet to stop and the packet to be dropped.

### 2.2 Type-7 Address Ranges

NSSA border routers may be configured with Type-7 address ranges. Each Type-7 address range is defined as an [address,mask] pair. Many separate Type-7 networks may fall into a single Type-7 address range, just as a subnetted network is composed of many separate subnets. NSSA border routers may aggregate Type-7 routes by advertising a single Type-5 LSA for each Type-7 address range. The Type-5 LSA resulting from a Type-7 address range match will be distributed to all Type-5 capable areas. Section 3.2 details how Type-5 LSAs are generated from Type-7 address ranges.

A Type-7 address range includes the following configurable items.

- o An [address,mask] pair.
- o A status indication of either Advertise or DoNotAdvertise.
- o An external route tag.

### 2.3 Type-7 LSAs

External routes are imported into NSSAs as Type-7 LSAs by NSSA AS boundary routers. An NSSA AS boundary router (ASBR) is a router that has an interface associated with the NSSA and is exchanging routing information with routers belonging to another AS. Like OSPF ASBRs, an NSSA router indicates it is an NSSA ASBR by setting the E-bit in its router-LSA. As with Type-5 LSAs a separate Type-7 LSA is originated for each destination network. To support NSSAs the link-state database must therefore be expanded to contain Type-7 LSAs.

Type-7 LSAs are identical to Type-5 LSAs except for the following (see [OSPF] Section 12.4.4, "AS external links").

1. The Type field in the LSA header is 7.
2. Type-7 LSAs are only flooded within the originating NSSA. The flooding of Type-7 LSAs follows the same rules as the flooding of Type-1 and Type-2 LSAs.
3. Type-7 LSAs are only listed within the OSPF area data structures of their respective NSSAs, making them area specific. Type-5 LSAs, which are flooded to all Type-5 capable areas, have global scope and are listed in the OSPF protocol data structure.
4. NSSA border routers select which Type-7 LSAs are translated into Type-5 LSAs and flooded into the OSPF domain's transit topology.
5. Type-7 LSAs have a propagate (P) bit that, when set, tells an NSSA border router to translate a Type-7 LSA into a Type-5 LSA.
6. Those Type-7 LSAs that are to be translated into Type-5 LSAs must have their forwarding address set.



Type-5 LSAs that are translations of Type-7 LSAs copy the Type-7 LSAs' non-zero forwarding addresses. Only those Type-5 LSAs that are aggregations of Type-7 LSAs may have 0.0.0.0 as a forwarding address. (See Section 3.2 for details.) Non-zero forwarding addresses produce efficient inter-area routing to an NSSA's AS external destinations when it has multiple border routers. Also the non-zero forwarding addresses of Type-7 LSAs ease the process of their translation into Type-5 LSAs, as NSSA border routers are not required to compute them.

Normally the next hop address of an installed AS external route learned by an NSSA ASBR from an adjacent AS points at one of the adjacent AS's gateway routers. If this address belongs to a network connected to the NSSA ASBR via one of its NSSAs' active interfaces, then the NSSA ASBR copies this next hop address into the forwarding address field of the route's Type-7 LSA that is originated into this NSSA, as is currently done with Type-5 LSAs. (See [OSPF] Section 12.4.4.1.) For an NSSA with no such network the forwarding address field may only be filled with an address from one of the its active interfaces or 0.0.0.0. If the P-bit is set, the forwarding address must be non-zero; otherwise it may be 0.0.0.0. If an NSSA requires the P-bit be set and a non-zero forwarding address is unavailable, then the route's Type-7 LSA is not originated into this NSSA.

When a router is forced to pick a forwarding address for a Type-7 LSA, preference should be given first to the router's internal addresses (provided internal addressing is supported). If internal addresses are not available, preference should be given to the router's active OSPF stub network addresses. These choices avoid the possible extra hop that may happen when a transit network's address is used. When the interface whose IP address is the LSA's forwarding address transitions to a Down state (see [OSPF] Section 9.3), the router must select a new forwarding address for the LSA and then re-originate it. If one is not available the LSA should be flushed.

The metrics and path types of Type-5 LSAs are directly comparable with the metrics and path types of Type-7 LSAs.

## 2.4 Originating Type-7 LSAs

NSSA AS boundary routers may only originate Type-7 LSAs into NSSAs. An NSSA internal AS boundary router must set the P-bit in the LSA header's option field of any Type-7 LSA whose network it wants advertised into the OSPF domain's full transit topology. The LSAs of these networks must have a valid non-zero forwarding address. If the P-bit is clear the LSA is not translated into a Type-5 LSA by NSSA border routers.

When an NSSA border router originates both a Type-5 LSA and a Type-7 LSA for the same network, then the P-bit must be clear in the Type-7 LSA so that it isn't translated into a Type-5 LSA by another NSSA border router. If the border router only originates a Type-7 LSA, it may set the P-bit so that the network may be aggregated/propagated during Type-7 translation. If an NSSA's border router originates a Type-5 LSA with a forwarding address from the NSSA, it should also originate a Type-7 LSA into the NSSA. If two NSSA routers, both reachable from one another over the NSSA, originate functionally equivalent Type-7 LSAs (i.e., same destination, cost and non-zero forwarding address), then the router having the least preferred LSA should flush its LSA. (See [OSPF] Section 12.4.4.1.) Preference between two Type-7 LSAs is determined by the following tie breaker rules:

1. An LSA with the P-bit set is preferred over one with the P-bit clear.
2. If the P-bit settings are the same, the LSA with the higher router ID is preferred.

A Type-7 default LSA for the network 0.0.0.0/0 may be originated into the NSSA by any NSSA router. The Type-7 default LSA originated by an NSSA border router must have the P-bit clear. An NSSA ASBR that is not an NSSA border router may originate a Type-7 default LSA with the P-bit set. A Type-7 default LSA may be installed by NSSA border routers if and only if its P-bit is set. (See Appendix E.)

NSSA border routers must originate an LSA for the default destination into all their directly attached NSSAs in order to support intra-AS routing and inter-AS routing. This default destination is advertised in either a Type-3 LSA or a Type-7 LSA, as described in Section 2.7. The default LSA's metric should be configurable. For Type-7 default LSAs, the metric type (1 or 2) should also be configurable.

## 2.5 Calculating Type-7 AS External Routes

This calculation must be run when Type-7 LSAs are processed during the AS external route calculation. This calculation may process Type-5 LSAs, but it is written that way only for comparison sake.

Non-default Type-7 LSAs with the P-bit clear may be installed in the OSPF routing table of NSSA border routers. Since these LSAs are not propagated throughout the OSPF domain, traffic that originates external to an NSSA and that passes through one of the NSSA's border routers may be unexpectedly diverted into the NSSA. (See Appendix E.)

An NSSA border router should examine both Type-5 LSAs and Type-7 LSAs if either Type-5 or Type-7 routes need to be updated or recalculated. This is done as part of the AS external route calculation. An NSSA internal router should examine Type-7 LSAs when Type-7 routes need to be recalculated.

What follows is only a modest modification of [OSPF] Section 16.4. Original paragraphs are tagged with [OSPF]. Paragraphs with minor changes are tagged with ~[OSPF]. Paragraphs specific to NSSA are tagged with [NSSA].

AS external routes are calculated by examining AS-external-LSAs, be they Type-5 or Type-7. Each of the AS-external-LSAs is considered in turn. Most AS-external-LSAs describe routes to specific IP destinations. An AS-external-LSA can also describe a default route for the Autonomous System (Destination ID = DefaultDestination, network/subnet mask = 0x00000000). For each AS-external-LSA:  
~[OSPF]

- (1) If the metric specified by the LSA is LSInfinity, or if the age of the LSA equals MaxAge, then examine the next LSA.  
[OSPF]
- (2) If the LSA was originated by the calculating router itself, examine the next LSA.  
[OSPF]
- (3) Call the destination described by the LSA N. N's address is obtained by masking the LSA's Link State ID with the network/subnet mask contained in the body of the LSA. Look up the routing table entries that match the LSA's type for the AS boundary router (ASBR) that originated the LSA. For a Type-5 LSA, routing table entries may only be selected from each attached Type-5 capable area. Since the flooding scope of a Type-7 LSA is restricted to the originating NSSA, the routing table entry of its ASBR must be found in the originating NSSA. If no entries exist for the ASBR (i.e. the ASBR is unreachable over the transit topology for a Type-5 LSA, or, for a Type-7 LSA, it is unreachable over the LSA's originating NSSA), do nothing with this LSA and consider the next in the list.  
[NSSA]

Else if the destination is a Type-7 default route (destination ID = DefaultDestination) and one of the following is true, then do nothing with this LSA and consider the next in the list:

- o The calculating router is a border router and the LSA has its P-bit clear. Appendix E describes a technique whereby an NSSA border router installs a Type-7 default LSA without propagating it.
  - o The calculating router is a border router and is suppressing the import of summary routes as Type-3 summary-LSAs.
- [NSSA]

Else, this LSA describes an AS external path to destination N. Examine the forwarding address specified in the AS-external-LSA. This indicates the IP address to which packets for the destination should be forwarded.

[OSPF]

If the forwarding address is set to 0.0.0.0 then packets should be sent to the ASBR itself. If the LSA is Type-5, from among the multiple non-NSSA routing table entries for the ASBR (both NSSA and non-NSSA ASBR entries might exist on an NSSA border router), select the preferred entry as follows:

~[OSPF]

If RFC1583Compatibility is set to "disabled", prune the set of routing table entries for the ASBR as described in OSPF Section 16.4.1. In any case, among the remaining routing table entries, select the routing table entry with the least cost; when there are multiple least cost routing table entries the entry whose associated area has the largest OSPF Area ID (when considered as an unsigned 32-bit integer) is chosen.

[OSPF]

Since a Type-7 LSA only has area-wide flooding scope, when its forwarding address is set to 0.0.0.0, its ASBR's routing table entry must be chosen from the originating NSSA. Here no pruning is necessary since this entry always contains non-backbone intra-area paths.

[NSSA]

If the forwarding address is non-zero look up the forwarding address in the routing table. For a Type-5 LSA the matching routing table entry must specify an intra-area or inter-area path through a Type-5 capable area. For a Type-7 LSA the matching routing table entry must specify an intra-area path through the LSA's originating NSSA. If no such path exists

then do nothing with this LSA and consider the next in the list.

[NSSA]

- (4) Let X be the cost specified by the preferred routing table entry for the ASBR/forwarding address, and Y the cost specified in the LSA. X is in terms of the link state metric, and Y is a type 1 or 2 external metric.  
[OSPF]
- (5) Now, look up the routing table entry for the destination N. If no entry exists for N, install the AS external path to N, with the next hop equal to the list of next hops to the ASBR/forwarding address, and advertising router equal to the ASBR. If the external metric type is 1, then the path-type is set to Type-1 external and the cost is equal to  $X + Y$ . If the external metric type is 2, the path-type is set to Type-2 external, the link-state component of the route's cost is X, and the type 2 cost is Y.  
[OSPF]
- (6) Otherwise compare the AS external path described by the LSA with the existing paths in N's routing table entry. If the new path is preferred, it replaces the present paths in N's routing table entry. If the new path is of equal preference, it is added to the present paths in N's routing table entry.  
[OSPF]

Preference is defined as follows:

- (a) Intra-area and inter-area paths are always preferred over AS external paths.  
[OSPF]
- (b) Type 1 external paths are always preferred over type 2 external paths. When all paths are type 2 external paths, the paths with the smallest advertised type 2 metric are always preferred.  
[OSPF]
- (c) If the new AS external path is still indistinguishable from the current paths in N's routing table entry, and RFC1583Compatibility is set to "disabled", select the preferred paths based on the intra-AS paths to the ASBR/forwarding addresses, as specified in Section 16.4.1. Here intra-NSSA paths are equivalent to the intra-area paths of non-backbone regular OSPF areas.  
[NSSA]

(d) If the new AS external path is still indistinguishable from the current paths in N's routing table entry, select the preferred path based on a least cost comparison. Type 1 external paths are compared by looking at the sum of the distance to the ASBR/forwarding addresses and the advertised type 1 metric (X+Y). Type 2 external paths advertising equal type 2 metrics are compared by looking at the distance to the ASBR/forwarding addresses.

~[OSPF]

(e) If the current LSA is functionally the same as an installed LSA (i.e., same destination, cost and non-zero forwarding address) then apply the following priorities in deciding which LSA is preferred:

1. A Type-7 LSA with the P-bit set.
2. A Type-5 LSA.
3. The LSA with the higher router ID.

[NSSA]

## 2.6 Incremental Updates

Incremental updates for Type-7 LSAs should be treated the same as incremental updates for Type-5 LSAs (see [OSPF] Section 16.6). When a new instance of a Type-7 LSA is received it is not necessary to recalculate the entire routing table. Call the destination described by the Type-7 LSA N. N's address is obtained by masking the LSA's Link State ID with the network/subnet mask contained in the body of the LSA. If there is already an intra-area or inter-area route to the destination, no recalculation is necessary (internal routes take precedence).

Otherwise, the procedure in the preceding section will have to be performed but only for the external routes (Type-5 and Type-7) whose destination is N. Before this procedure is performed, the present routing table entry for N should be invalidated.

## 2.7 Optionally Importing Summary Routes

In order for OSPF's summary routing to not be obscured by an NSSA's Type-7 AS-external-LSAs, all NSSA border router implementations must support the optional import of summary routes into NSSAs as Type-3 summary-LSAs. The default behavior is to import summary routes. A new area configuration parameter, ImportSummaries, is defined in Appendix D. When ImportSummaries is set to enabled, summary routes

are imported. When it is set to disabled, summary routes are not imported. The default setting is enabled.

When OSPF's summary routes are not imported, the default LSA originated by an NSSA border router into the NSSA should be a Type-3 summary-LSA. This protects the NSSA from routing intra-AS traffic out the AS via the default route of a Type-7 default LSA originating from one of the NSSA's internal routers. When summary routes are imported into the NSSA, the default LSA originated by an NSSA border router must not be a Type-3 summary-LSA; otherwise its default route would be chosen over the potentially more preferred default routes of Type-7 default LSAs.

### 3.0 Intra-AS Implementation Details

#### 3.1 Type-7 Translator Election

It is not recommended that multiple NSSA border routers perform Type-7 to Type-5 translation unless it is required to route packets efficiently through Area 0 to an NSSA partitioned by Type-7 address ranges. It is normally sufficient to have only one NSSA border router perform the translation. Excessive numbers of Type-7 translators unnecessarily increase the size of the OSPF link state data base.

A new area configuration parameter, `NSSATranslatorRole`, is defined in Appendix D. It specifies whether or not an NSSA router will unconditionally translate Type-7 LSAs to Type-5 LSAs when acting as an NSSA border router. Configuring the identity of the translator can be used to bias the routing to aggregated destinations. When `NSSATranslatorRole` is set to Always, Type-7 LSAs are always translated regardless of the translator state of other NSSA border routers. When `NSSATranslatorRole` is set to Candidate an NSSA border router will participate in the translator election process described below.

A new area parameter, `NSSATranslatorState`, is maintained in an NSSA's OSPF area data structure. By default all NSSA routers initialize `NSSATranslatorState` to disabled. When an NSSA border router's `NSSATranslatorState` changes from disabled to either enabled or elected, it begins translating the NSSA's Type-7 LSAs into Type-5 LSAs. When its `NSSATranslatorState` changes from either enabled or elected to disabled, it ceases translating the NSSA's Type-7 LSAs into Type-5 LSAs. (See paragraphs below.)

A new bit, `Nt`, is defined for the router-LSAs of NSSAs. (See Appendix B.) By default routers clear bit `Nt` when originating router-LSAs. However, when an NSSA border router has its

NSSATranslatorState enabled, it sets bit Nt in the router-LSA it originates into the NSSA. An NSSA router whose NSSATranslatorRole is set to Always should re-originate a router-LSA into the NSSA whenever its NSSATranslatorState changes.

When an NSSA router with the NSSA's NSSATranslatorRole set to Always attains border router status, it should change NSSATranslatorState from disabled to enabled. When it loses border router status, it should change NSSATranslatorState from enabled to disabled.

All NSSA border routers must set the E-bit in the Type-1 router-LSAs of their directly attached non-stub areas, even when they are not translating. This allows other NSSA border routers to see their ASBR status across the AS's transit topology. Failure to do so may cause the election algorithm to elect unnecessary translators. Every NSSA border router is a potential translator.

An NSSA border router whose NSSA's NSSATranslatorRole is set to Candidate must maintain a list of the NSSA's border routers that are reachable both over the NSSA and as ASBRs over the AS's transit topology. Any change in this list, or to the Nt bit settings of members of this list, causes the NSSA border router to reevaluate its NSSATranslatorState. If there exists another border router in this list whose router-LSA has bit Nt set or who has a higher router ID, then its NSSATranslatorState is disabled. Otherwise its NSSATranslatorState is elected.

An elected translator will continue to perform translation duties until supplanted by a reachable NSSA border router whose Nt bit is set or whose router ID is greater. Such an event may happen when an NSSA router with NSSATranslatorRole set to Always regains border router status, or when a partitioned NSSA becomes whole. If an elected translator determines its services are no longer required, it continues to perform its translation duties for the additional time interval defined by a new area configuration parameter, TranslatorStabilityInterval. This minimizes excessive flushing of translated Type-7 LSAs and provides for a more stable translator transition. The default value for the TranslatorStabilityInterval parameter has been defined as 40 seconds. (See Appendix D.)

### 3.2 Translating Type-7 LSAs into Type-5 LSAs

This step is performed as part of the NSSA's Dijkstra calculation after Type-5 and Type-7 routes have been calculated. If the calculating router is currently not an NSSA border router translator, then this translation algorithm should be skipped. Only installed



Type-7 LSAs and those non-default Type-7 LSAs originated by the router itself should be examined. Locally sourced Type-7 LSAs should be processed first.

Note that it is possible for a Type-5 LSA generated by translation to supplant a Type-5 LSA originating from a local OSPF external source. Future reoriginations of the locally sourced Type-5 LSA should be suppressed until the Type-5 LSA generated by translation is flushed.

A Type-7 LSA and a Type-7 address range best match one another if there does not exist a more specific Type-7 address range that contains the LSA's network. For each eligible Type-7 LSA perform the following:

- (1) If the Type-7 LSA has the P-bit clear, or its forwarding address is set to 0.0.0.0, or the most specific Type-7 address range that subsumes the LSA's network has DoNotAdvertise status, then do nothing with this Type-7 LSA and consider the next one in the list. Otherwise term the LSA as translatable and proceed with step (2).
- (2) If the Type-7 LSA is not contained in any explicitly configured Type-7 address range and the calculating router has the highest router ID amongst NSSA translators that have originated a functionally equivalent Type-5 LSA (i.e. same destination, cost and non-zero forwarding address) and that are reachable over area 0 and the NSSA, then a Type-5 LSA should be generated if there is currently no Type-5 LSA originating from this router corresponding to the Type-7 LSA's network, or there is an existing Type-5 LSA and either it corresponds to a local OSPF external source whose path type and metric is less preferred (see Section 2.5 step (6), parts (b) and (d)), or it doesn't and the Type-5 LSA's path type or cost(s) have changed (See Section 2.5 step (5)) or the forwarding address no longer maps to a translatable Type-7 LSA.

The newly originated Type-5 LSA will describe the same network and have the same network mask, path type, metric, forwarding address and external route tag as the Type-7 LSA. The advertising router field will be the router ID of this NSSA border router. The link-state ID is equal to the LSA's network address (in the case of multiple originations of Type-5 LSAs with the same network address but different mask, the link-state ID can also have one or more of the network's "host" bits set).

- (3) Else the Type-7 LSA must be aggregated by the most specific Type-7 address range that subsumes it. If this Type-7 address range has the same [address,mask] pair as the LSA's network and no other translatable Type-7 LSA with a different network best matches this range, then flag the LSA as not contained in any explicitly configured Type-7 address range and process the LSA as described in step (2). Otherwise compute the path type and metric for this Type-7 address range as described below.

The path type and metric of the Type-7 address range is determined from the path types and metrics of those translatable Type-7 LSAs that best match the range plus any locally sourced Type-5 LSAs whose network has the same [address,mask] pair. If any of these LSAs have a path type of 2, the range's path type is 2, otherwise it is 1. If the range's path type is 1 its metric is the highest cost amongst these LSAs; if the range's path type is 2 its metric is the highest Type-2 cost + 1 amongst these LSAs. (See Section 2.5 step (5).) 1 is added to the Type-2 cost to ensure that the translated Type-5 LSA does not appear closer on the NSSA border than a translatable Type-7 LSA whose network has the same [address,mask] pair and Type-2 cost.

A Type-5 LSA is generated from the Type-7 address range when there is currently no Type-5 LSA originated by this router whose network has the same [address,mask] pair as the range or there is but either its path type or metric has changed or its forwarding address is non-zero.

The newly generated Type-5 LSA will have a link-state ID equal to the Type-7 address range's address (in the case of multiple originations of Type-5 LSAs with the same network address but different mask, the link-state ID can also have one or more of the range's "host" bits set). The advertising router field will be the router ID of this area border router. The network mask and the external route tag are set to the range's configured values. The forwarding address is set to 0.0.0.0. The path type and metric are set to the range's path type and metric as defined and computed above.

The pending processing of other translation eligible Type-7 LSAs that best match this Type-7 address range is suppressed. Thus at most a single Type-5 LSA is originated for each Type-7 address range.

For example, given a Type-7 address range of [10.0.0.0, 255.0.0.0] that subsumes the following Type-7 routes:

```
10.1.0.0/24 path type 1, cost 10
10.2.0.0/24 path type 1, cost 11
10.3.0.0/24 path type 2, type 2 cost 5
```

a Type-5 LSA would be generated with a path type of 2 and a metric 6.

Given a Type-7 address range of [10.0.0.0, 255.0.0.0] that subsumes the following Type-7 routes:

```
10.1.0.0/24 path type 1, cost 10
10.2.0.0/24 path type 1, cost 11
10.3.0.0/24 path type 1, cost 5
```

a Type-5 LSA will be generated with a path type of 1 and a metric 11.

These Type-7 address range metric and path type rules will avoid routing loops in the event that path types 1 and 2 are both used within the area.

As with all newly originated Type-5 LSAs, a Type-5 LSA that is the result of a Type-7 LSA translation or aggregation is flooded to all attached Type-5 capable areas.

Like Type-3 address ranges, a Type-7 address range performs the dual function of setting propagation policy via its Advertise/DoNotAdvertise parameter and aggregation via its network address and mask pair. Unlike the origination of Type-3 summary-LSAs, the translation of a Type-7 LSA into a Type-5 LSA may result in more efficient routing when the forwarding address is set, as is done during step (2) of the translation procedure.

Another important feature of this translation process is that it allows a Type-7 address range to apply different properties (aggregation, forwarding address, and Advertise/DoNotAdvertise status) for the Type-7 routes it subsumes, versus those Type-7 routes subsumed by other more specific Type-7 address ranges contained in the Type-7 address range.

### 3.3 Flushing Translated Type-7 LSAs

If an NSSA border router has either translated or aggregated an installed Type-7 LSA into a Type-5 LSA that should no longer be translated or aggregated, then the Type-5 LSA should either be flushed or reoriginated as a translation or aggregation of other Type-7 LSAs.

If an NSSA border router is translating Type-7 LSAs into Type-5 LSAs with NSSATranslatorState set to elected and the NSSA border router has determined that its translator election status has been deposed by another NSSA border router (see Section 3.1), then, as soon as the TranslatorStabilityInterval has expired without the router reelecting itself as a translator, Type-5 LSAs that are generated by aggregating Type-7 LSAs into their best matched Type-7 address ranges (see Section 3.2, Step (3)) are flushed. Conversely Type-5 LSAs generated by translating Type-7 LSAs are not immediately flushed, but are allowed to remain in the OSPF routing domain as if the originator is still an elected translator. This minimizes the flushing and flooding impact on the transit topology of an NSSA that changes its translators frequently.

#### 4.0 Security Considerations

There are two types of issues that need be addressed when looking at protecting routing protocols from misconfigurations and malicious attacks. The first is authentication and certification of routing protocol information. The second is denial of service attacks resulting from repetitive origination of the same router advertisement or origination of a large number of distinct advertisements resulting in database overflow. Note that both of these concerns exist independently of a router's support for the NSSA option.

The OSPF protocol addresses authentication concerns by authenticating OSPF protocol exchanges. OSPF supports multiple types of authentication; the type of authentication in use can be configured on a per network segment basis. One of OSPF's authentication types, namely the Cryptographic authentication option, is believed to be secure against passive attacks and provides significant protection against active attacks. When using the Cryptographic authentication option, each router appends a "message digest" to its transmitted OSPF packets. Receivers then use the shared secret key and the received digest to verify that each received OSPF packet is authentic.

The quality of the security provided by the Cryptographic authentication option depends completely on the strength of the message digest algorithm (MD5 is currently the only message digest algorithm specified), the strength of the key being used, and the correct implementation of the security mechanism in all communicating OSPF implementations. It also requires that all parties maintain the secrecy of the shared secret key. None of the standard OSPF authentication types provide confidentiality, nor do they protect against traffic analysis. For more information on the standard OSPF security mechanisms, see Sections 8.1, 8.2, and Appendix D of [OSPF].

[DIGI] describes the extensions to OSPF required to add digital signature authentication to Link State data and to provide a certification mechanism for router data. [DIGI] also describes the added LSA processing and key management as well as a method for migration from or co-existence with standard OSPF V2.

OSPF addresses repetitive origination of advertisements by mandating a limit on how frequent new instances of any particular LSA can be originated and accepted during the flooding procedure. The frequency at which new LSA instances may be originated is set to once every MinLSInterval seconds, whose value is 5 seconds. (See [OSPF] Section 12.4.) The frequency at which new LSA instances are accepted during flooding is once every MinLSArrival seconds, whose value is set to 1 second. (See [OSPF] Section 13, Appendix B, and G.1.)

Proper operation of the OSPF protocol requires that all OSPF routers maintain an identical copy of the OSPF link state database. However, when the size of the link state database becomes very large, some routers may be unable to keep the entire database due to resource shortages; this is termed "database overflow". When database overflow is anticipated, the routers with limited resources can be accommodated by configuring OSPF stub areas and NSSAs. [OVERFLOW] details a way of gracefully handling unanticipated database overflows.

## 5.0 Acknowledgements

This document was produced by the OSPF Working Group, chaired by John Moy.

In addition, the comments of the following individuals are also acknowledged:

|                   |                       |
|-------------------|-----------------------|
| Antoni Przygienda | Redback Networks, Inc |
| Alex Zinin        | cisco                 |

It is also noted that comments from

|                   |                    |
|-------------------|--------------------|
| Phani Jajjarvarpu | cisco              |
| Dino Farinacci    | cisco              |
| Jeff Honig        | Cornell University |
| Doug Williams     | IBM                |

were acknowledged in the predecessor of this document, RFC 1587.

## 6.0 Contributors

This document, RFC 3101, adds new sections, features, edits, and revisions to its predecessor, RFC 1587, "The OSPF NSSA Option", authored by Rob Coltun, Movaz Networks, and Vince Fuller. Content from RFC 1587 is used throughout RFC 3101. In addition to adding new features, this document makes the NSSA specification consistent with the OSPFv2 specification, RFC 2328, authored by John Moy, Sycamore Networks, Inc. Section 2.5, Calculating Type-7 AS External Routes, and Section 2.6, Incremental Updates, rely heavily on text in RFC 2328's Section 16.4 and Section 16.6 respectively. Section 4.0, Security Considerations, is an edit of similar content in Rob Coltun's RFC 2370, "The OSPF Opaque LSA option", Section 6.0.

Acee Lindem, Redback Networks, Inc, is also recognized for the first full known implementation of this specification. Acee's implementation resulted in substantive content change.

## 7.0 References

- [DIGI] Murphy, S., Badger, M. and B. Wellington, "OSPF with Digital Signatures", RFC 2154, June 1997.
- [MUEX] Moy, J., "Multicast Extensions to OSPF", RFC 1584, March 1994.
- [OSPF] Moy, J., "OSPF Version 2", RFC 2328, April 1998.
- [OPAQUE] Coltun, R., "The OSPF Opaque LSA Option", RFC 2370, July 1998.
- [OVERFLOW] Moy, J., "OSPF Database Overflow", RFC 1765, March 1995.

## Appendix A: The Options Field

The OSPF options field is present in OSPF Hello packets, Database Description packets and all link state advertisements. See [OSPF] Appendix A.2 and [OPAQUE] Appendix A.1 for a description of the options field. Six bits are assigned but only two (the E-bit and the N/P bit) are described completely in this section.

```

-----
| * | O | DC | EA | N/P | MC | E | * |
-----

```

## The Type-7 LSA options field

- E-bit:** Type-5 AS-external-LSAs are not flooded into/through OSPF stub areas and NSSAs. The E-bit ensures that all members of a stub area or NSSA agree on that area configuration. The E-bit is meaningful only in OSPF Hello and Database Description packets. When the E-bit is clear in the Hello packet sent out a particular interface, it means that the router will neither send nor receive Type-5 AS-external-LSAs on that interface (in other words, the interface connects to a stub area or NSSA). Two routers will not become neighbors unless they agree on the state of the E-bit.
- N-bit:** The N-bit describes the router's NSSA capability. The N-bit is used only in Hello packets and ensures that all members of an NSSA agree on that area's configuration. When the N-bit is set in the Hello packet that is sent out a particular interface, it means that the router will send and receive Type-7 LSAs on that interface. Two routers will not form an adjacency unless they agree on the state of the N-bit. If the N-bit is set in the options field, the E-bit must be clear.
- P-bit:** The P-bit is used only in the Type-7 LSA header. It flags the NSSA border router to translate the Type-7 LSA into a Type-5 LSA. The default setting for the P-bit is clear.

## Appendix B: Router-LSAs

Router-LSAs are the Type-1 LSAs. Each router in an area originates a router-LSA. The LSA describes the state and cost of the router's links (i.e., interfaces) to the area. All of the router's links to the area must be described in a single router-LSA. For details concerning the construction of router-LSAs, see [OSPF] Section 12.4.1.

| 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 |  |  |  |  |  |  |  |  |
| LS age             |   |   |   |   |   |   |   |   |   | Options |   |   |   |   |   |   |   |   |   | 1            |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Link State ID      |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Advertising Router |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| LS sequence number |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| LS checksum        |   |   |   |   |   |   |   |   |   | length  |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| 0 Nt W V E B       |   |   |   |   |   |   |   |   |   | 0       |   |   |   |   |   |   |   |   |   | # links      |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Link ID            |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Link Data          |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Type               |   |   |   |   |   |   |   |   |   | # TOS   |   |   |   |   |   |   |   |   |   | TOS 0 metric |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| TOS                |   |   |   |   |   |   |   |   |   | 0       |   |   |   |   |   |   |   |   |   | metric       |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| ...                |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| TOS                |   |   |   |   |   |   |   |   |   | 0       |   |   |   |   |   |   |   |   |   | metric       |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Link ID            |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| Link Data          |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |
| ...                |   |   |   |   |   |   |   |   |   |         |   |   |   |   |   |   |   |   |   |              |   |   |   |   |   |   |   |   |   |   |   |  |  |  |  |  |  |  |  |

In router-LSAs, the Link State ID field is set to the router's OSPF Router ID. Router-LSAs are flooded throughout a single area only.



## bit V

When set, the router is an endpoint of one or more fully adjacent virtual links having the described area as their transit area (V is for virtual link endpoint).

## bit E

When set, the router is an AS boundary router (E is for external). ALL NSSA border routers set bit E in those router-LSAs originated into directly attached Type-5 capable areas. An NSSA's AS boundary routers also set bit E in their router-LSAs originated into the NSSA. (See Section 3.1 for details.)

## bit B

When set, the router is an area border router (B is for border).

## bit W

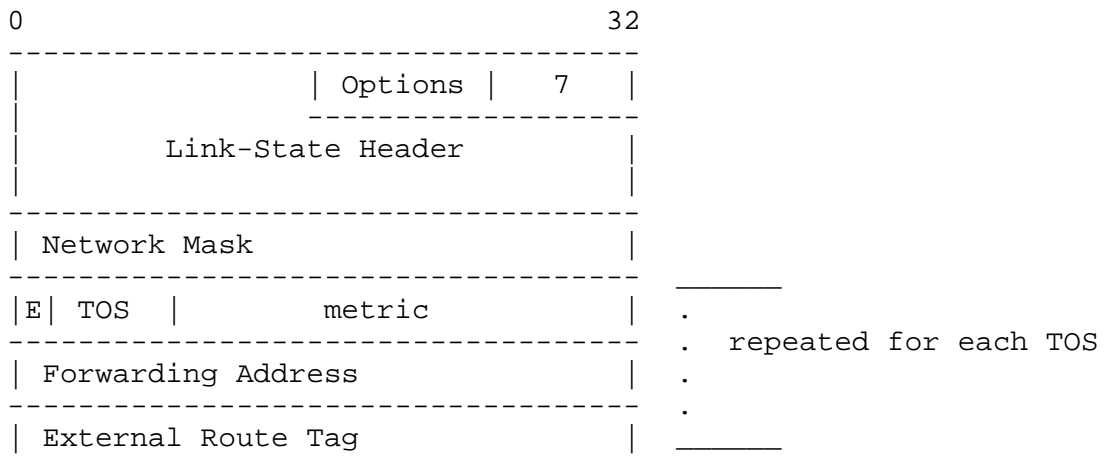
When set, the router is a wild-card multicast receiver (W is for wild).

## bit Nt

When set, the router is an NSSA border router that is unconditionally translating Type-7 LSAs into Type-5 LSAs (Nt stands for NSSA translation). Note that such routers have their NSSATranslatorRole area configuration parameter set to Always. (See Appendix D and Section 3.1.)

The remainder of the router-LSAs specification is defined in [OSPF] Section A.4.2.

## Appendix C: Type-7 LSA Packet Format



The definitions of the link-state ID, network mask, metrics and external route tag are the same as the definitions for Type-5 LSAs (See [OSPF] Appendix A.4.5), except for the forwarding address and the N/P-bit. The Options field must have the N/P bit set as described in Appendix A when the originating router desires that the external route be propagated throughout the OSPF domain.

## Forwarding address

Data traffic for the advertised destination will be forwarded to this address. If the forwarding address is set to 0.0.0.0, data traffic will be forwarded to the LSA's originator (i.e., the responsible NSSA AS boundary router). Normally the next hop address of an installed AS external route learned by an NSSA ASBR from an adjacent AS points at one of the adjacent AS's gateway routers. If this address belongs to a network connected to the NSSA ASBR via one of its NSSAs' active interfaces, then it is the forwarding address for the route's Type-7 LSA originated into this NSSA. For an NSSA with no such network the forwarding address is either an address from one of its active interfaces or 0.0.0.0. If the P-bit is set, the forwarding address must be non-zero, otherwise it may be 0.0.0.0. (See Section 2.3 for details.)

## Appendix D: Configuration Parameters

[OSPF] Appendix C.2 lists the area configuration parameters. The area ID and the list of address ranges for Type-3 summary routes remain unchanged. Section 2.2 of this document lists the configuration parameters for Type-7 address ranges. The following area configuration parameters have been added:

### NSSATranslatorRole

Specifies whether or not an NSSA border router will unconditionally translate Type-7 LSAs into Type-5 LSAs. When it is set to Always, an NSSA border router always translates Type-7 LSAs into Type-5 LSAs regardless of the translator state of other NSSA border routers. When it is set to Candidate, an NSSA border router participates in the translator election process described in Section 3.1. The default setting is Candidate.

### TranslatorStabilityInterval

Defines the length of time an elected Type-7 translator will continue to perform its translator duties once it has determined that its translator status has been deposed by another NSSA border router translator as described in Section 3.1 and 3.3. The default setting is 40 seconds.

### ImportSummaries

When set to enabled, OSPF's summary routes are imported into the NSSA as Type-3 summary-LSAs. When set to disabled, summary routes are not imported into the NSSA. The default setting is enabled.

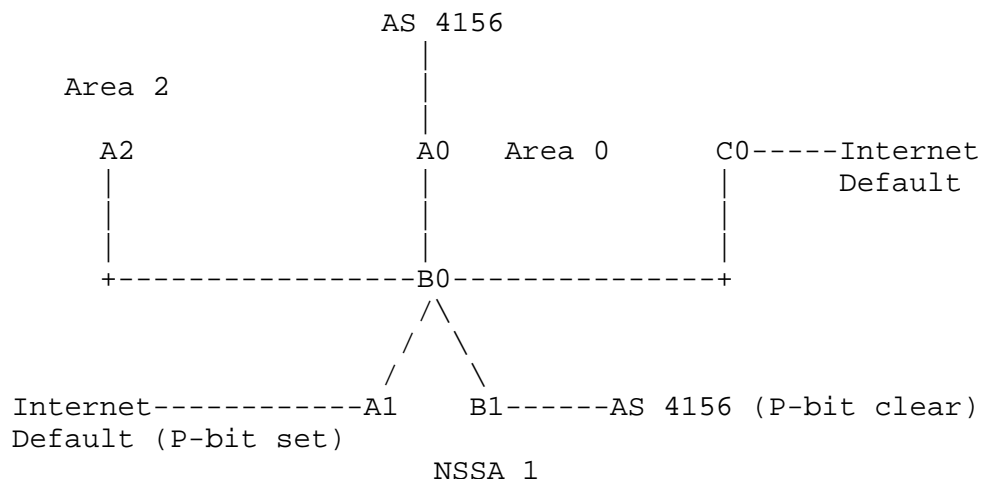
Implementations must provide a vehicle for setting the P-bit when external routes are imported into the NSSA as Type-7 LSAs. Without configuration, the default setting of the P-bit is clear. (See Section 2.3 and Appendix B.)

For NSSAs the ExternalRoutingCapability area configuration parameter must be set to accept Type-7 external routes. Additionally there must be a way of configuring the metric of the default LSA that a border router advertises into its directly attached NSSAs. If a Type-7 default LSA is advertised, its metric type (1 or 2) should also be configurable.

## Appendix E: The P-bit Policy Paradox.

Non-default Type-7 LSAs with the P-bit clear may be installed in the OSPF routing table of NSSA border routers. (See Section 2.5.) These LSAs are not propagated throughout the OSPF domain as translated Type-5 LSAs. (See Section 3.2.) Thus, traffic that is external to an NSSA and that passes through one of the NSSA's border routers may be hijacked into the NSSA by a route installed from a Type-7 LSA with the P-bit clear. This may be contrary to the expected path at the source of the traffic. It may also violate the routing policy intended by the Type-7 LSA's clear P-bit. A Type-7 address range that is configured with DoNotAdvertise exhibits the same paradox for any installed Type-7 LSAs it subsumes, regardless of the P-bit setting.

This paradox is best illustrated by the following example. Consider an OSPF domain (AS 1842) with connections for default Internet routing and to external AS 4156. NSSA 1 and OSPF Area 2 are partially defined in the following diagram:



Here A0, B0, and C0 are Area 0 routers, A1 and B1 are NSSA 1 routers, and A2 is an Area 2 router. B0 is a border router for both NSSA 1 and Area 2.

If the Type-7 external routes imported by B1 for AS 4156 are installed on B0 so that the NSSA 1 tree below A1 can take advantage of them, then A2's traffic to AS 4156 is hijacked through B0 by B1, rather than its computed path through A0.

An NSSA border router's installed Type-7 default LSAs will exhibit this paradox when it possesses a Type-7 address range [0,0] configured with DoNotAdvertise, as these LSAs are not propagated even

though their P-bit is set. In the example above, if A1's default is installed on B0, which has a configured Type-7 address range [0,0] with DoNotAdvertise set, then A2's Internet traffic is hijacked through B0 by A1 rather than the computed path through C0.

## Appendix F: Differences from RFC 1587

This section documents the differences between this memo and RFC 1587. All differences are backward-compatible. Implementations of this memo and of RFC 1587 will interoperate.

### F.1 Enhancements to the import of OSPF's summary routes.

The import of OSPF's summary routes into an NSSA as Type-3 summary-LSAs is now optional. In RFC 1587 the import of summary routes was mandated in order to guarantee that inter-area summary routing was not obscured by an NSSA's Type-7 AS-external-LSAs. The current recommended default behavior is to import summary routes. When summary routes are not imported into an NSSA, the default LSA originated by its border routers must be a Type-3 summary-LSA.

See Sections 1.3 and 2.7 for details.

### F.2 Changes to Type-7 LSAs.

The setting of the forwarding address in Type-7 LSAs has been further refined.

See Section 2.3 for details.

### F.3 Changes to the Type-7 AS external routing calculation.

The Type-7 external route calculation has been revised. Most notably:

- o The path preference defined in [OSPF] Section 16.4.1 has been included.
- o A Type-7 default route with the P-bit clear will not be installed on an NSSA border router. This protects the default routing of other OSPF Areas. (See Appendix E.)
- o The LSA type of two AS-external-LSAs plays no role in determining path preference except when the LSAs are functionally the same (i.e., same destination, cost and non-zero forwarding address).

See Section 2.5 for details.

#### F.4 Changes to translating Type-7 LSAs into Type-5 LSAs

The translator election algorithm of RFC 1587 has been updated to close a bug that results when the translator with the highest router ID loses connectivity to the AS's transit topology. The default translator election process occurs only in the absence of an existing translator.

The identity of the translator is optionally configurable, with more than one allowed. This allows the network designer to choose the most cost effective intra-AS route for NSSA originated Type-5 LSA aggregations of Type-7 LSAs.

Self-originated non-default Type-7 LSAs are now included in the translation process.

The translation process has been strengthened to close some of the weak points of RFC 1587.

See Sections 3.1 and 3.2 for details.

#### F.5 Changes to flushing translated Type-7 LSAs

An NSSA border router, which was elected by the augmented RFC 1587 translator selection process defined in Section 3.1 and which has been deposed from its translation duties by another NSSA border router, flushes its self-originated Type-5 LSAs that resulted from the aggregation of Type-7 LSAs. This prevents these obsolete aggregations from short circuiting the preferred path through the new translator(s). A deposed translator continues to maintain its self-originated Type-5 LSAs resulting from translation until they age out normally.

See Section 3.3 for details.

#### F.6 P-bit additions

The P-bit default has been defined as clear. RFC 1587 had no default setting. (See Appendix C.)

A discussion on the packet forwarding impact of installing Type-7 LSAs with the P-bit clear on NSSA border routers has been added as Appendix E.

## Author's Addresses

Pat Murphy  
US Geological Survey  
345 Middlefield Road  
Menlo Park, California 94560

Phone: (650) 329-4044  
EMail: pmurphy@noc.usgs.net



## Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

## Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

