Security Considerations

All OSPF protocol exchanges are authenticated. This is accomplished through authentication fields contained in the OSPF packet header. For more information, see Sections 8.1, 8.2, and Appendix E.

Author's Address

John Moy
Proteon, Inc.
2 Technology Drive
Westborough, MA 01581

Phone: (508) 898-2800
EMail: jmoy@proteon.com

F.3.2 Packet simplification

To simplify the format of Database Description packets and Link State Acknowledgment packets, their description of link state advertisements has been modified. Each advertisement is now be described by its 20-byte link state header (see Section A.4). This does not consume any additional space in the packets. The one additional piece of information that will be present is the LS length. However, this field need not be used when processing the Database Description and Link State Acknowledgment packets.

F.3.3 Adding forwarding addresses to AS external advertisements

As discussed in Section F.1.3, a forwarding address field has been added to the AS external advertisement.

F.3.4 Labelling of virtual links

Virtual links will be labelled as such in router links advertisements. This separates virtual links from unnumbered point-to-point links, allowing all backbone routers to discover whether any virtual links are in use. See Section 12.4.1 for more details.

F.3.5 TOS costs ordered

When a link state advertisement specifies a separate cost depending on TOS, these costs must be ordered by increasing TOS value. In other words, the cost for TOS 16 must always follow the cost for TOS 8.

F.3.6 OSPF's TOS encoding redefined

The way that OSPF encodes TOS in its link state advertisements has been redefined in version 2. OSPF's encoding of the Delay (D), Throughput (T), and Reliability (R) TOS flags defined by [RFC 791] is described in Section 12.3.

F.4 Backward-compatibility provisions

Additional functionality will probably be added to OSPF in the future. One example of this is a multicast routing capability, which is currently under development. In order to be able to add such features in a backward-compatible manner, the following provisions have been made in the OSPF specification.

New capabilities will probably involve the introduction of new link state advertisements. If a router receives a link state advertisement of unknown type during the flooding procedure, the advertisement is simply ignored (Section 13. The router should not attempt to further flood the advertisement, nor acknowledge it. The advertisement should not be installed into the link state database. If the router receives an advertisement of unknown type during the Database Description process, this is an error (see Sections 10.6 and 10.3). The Database Description process is then restarted.

There is also an **Options** field in both the Hello packets, Database Description packets and the link state advertisement headers. Unrecognized capabilities found in these places should be ignored, and should not affect the normal processing of protocol packets/link state advertisements (see Sections 10.5 and 10.6). Routers will originate their Hello packets, Database Description packets and link state advertisements with unrecognized capabilities set to 0 (see Sections 9.5, 10.8 and 12.1.2).

appears on any neighbor **Link State Retransmission lists** and b) none of the router's neighbors are in states **Exchange** or **Loading**. See Sections 13 (step 4c) and 14.1 for more details.

In addition, a new step has been added to the flooding procedure (Section 13) in order to make the Database Description process more robust. This step detects when a neighbor lists one instance of an advertisement in its Database Description packets, but responds to Link State Request packets by sending another (earlier) instance. This behavior now causes the event **BadLSReq** to be generated, which restarts the Database Description process with the neighbor. In OSPF version 1, the neighbor event **BadLSReq** erroneously did not restart the Database Description process.

F.2.7 Receiving OSPF Hello packets

The section detailing the receive processing of OSPF Hello packets (Section 10.5) has been modified to include the generation of the neighbor **Backup Seen** event. In addition, the section detailing the Designated Router election algorithm (Section 9.4) has been modified to include the algorithm's initial state.

F.2.8 Network mask defined for default route

The network mask for the default route, when it appears as the destination in either an AS external link advertisement or in a summary link advertisement, has been set to `0.0.0.0`. See Sections A.4.4 and A.4.5 for more details.

F.2.9 Rate limit imposed on flooding

When an advertisement is installed in the link state database, it is timestamped. The flooding procedure is then not allowed to install a new instance of the advertisement until MinLSInterval seconds have elapsed. This enforces a rate limit on the flooding procedure; a new instance can be flooded only once every MinLSInterval seconds. This guards against routers that disregard the limit on self-originated advertisements (already present in OSPF version 1) of one origination every MinLSInterval seconds. For more information, see Section 13.

F.3 Packet format changes

The following changes have been made to the format of OSPF packets and link state advertisements. Some of these changes were required to support the added functionality listed above. Other changes were made to further simplify the parsing of OSPF packets.

F.3.1 Adding a Capability bitfield

To support the new "stub area" and "optional TOS" features, a bitfield listing protocol capabilities has been added to the Hello packet, Database Description packet and all link state advertisements. When used in Hello packets, this allows a router to reject a neighbor because of a capability mismatch. Alternatively, when capabilities are exchanged in Database Description packets a router can choose not to forward certain link state advertisements to a neighbor because of its reduced functionality. Lastly, listing capabilities in link state advertisements allows routers to route traffic around reduced functionality router, by excluding them from parts of the routing table calculation. See Section A.2 for more details.

of the advertisement must be originated (due either to topological change of the expiration of the LS refresh timer) the current instance must first be "prematurely aged".

There will be a new section discussing premature aging (Section 14.1). This is a method for flushing a link state advertisement from the routing domain: the advertisement's age is set to MaxAge and advertisement is reflooded just as if it were a newly received advertisement. As soon as the new flooding is acknowledged by all of the router's adjacent neighbors, the advertisement is flushed from the database.

Premature aging can also be used when, for example, a previously advertised external route is no longer reachable. In this circumstance, premature aging is preferable to the alternative, which is to originate a new advertisement for the destination specifying a metric of LSInfinity.

A router may only prematurely age its own (self-originated) link state advertisements. These are the link state advertisements having the router's own OSPF router ID in the **Advertising Router** field.

F.2.2 Flooding of unexpected MaxAge advertisements

Version 1 of the OSPF omitted the handling of a special case in the flooding procedure: the reception of a MaxAge advertisement that has no database instance. A paragraph has been added to Section 13 to deal with this occurrence. Without this paragraph, retransmissions of MaxAge advertisements could possibly delay their being flushed from the routing domain.

F.2.3 Virtual links and address ranges

When summarizing information into a virtual link's transit area, version 2 of the OSPF specification prohibits the collapsing of multiple backbone IP networks/subnets into a single summary link. This restriction has been added to deal with certain anomalous OSPF area configurations. See Sections 15 and 12.4.3 for more information.

F.2.4 Routing table lookup explained

When forwarding an IP data packet, a router looks up the packet's IP destination in the routing table. This determines the packet's next hop. A new section (Section 11.1) has been added describing the routing table lookup (instead of just specifying a "best match"). This section clarifies OSPF's four level routing hierarchy (i.e., intra-area, inter-area, external type 1 and external type 2 routes). It also specifies the effect of TOS on routing.

F.2.5 Sending Link State Request packets

OSPF Version 2 eases the restrictions on the sending of Link State Request packets. Link State Request packets can now be sent to a neighboring router before a complete set of Database Description packets have been exchanged. This enables a more efficient use of a router's memory resources; an OSPF version 2 implementation may limit the size of the neighbor **Link state request lists**. See Sections 10.9, 10.7 and 10.3 for more details.

F.2.6 Changes to the Database description process

The specification has been modified to ensure that, when two routers are synchronizing their databases during the Database Description process, none of the component link state advertisements can have their sequence numbers decrease. A link state advertisement's sequence number decreases when it is flushed from the routing domain via premature-aging, and then reoriginated with the smallest sequence number `0x80000001` (see Section 14.1). So the specification now dictates that an advertisement cannot be flushed from a router's database until both a) it no longer

X from the calculation. In effect, an attempt will be made to bypass router X when forwarding non-zero TOS traffic. Summary link and AS external link advertisements can also indicate their non-availability for non-zero TOS traffic (Sections 12.4.3 and 12.4.4).

The result may be that no route can be found for some non-zero value of TOS. When this happens, the packet is routed along the TOS 0 route instead (Section 11.1).

It is still mandatory for all OSPF implementations to be able to construct separate routing tables for each TOS value, if desired by the system administrator.

F.1.3 Preventing external extra-hops

In some cases, version 1 of the OSPF specification will introduce extra-hops when calculating routes to external destinations. This is because it is implicit in the format of AS external advertisements that packets should be forwarded through the advertising router. However, consider the situation where multiple OSPF routers share a LAN with an external router (call it router Y) , and only one OSPF router (call it router X) exchanges routing information with Y. The OSPF routers on the LAN other than X will forward packets destined for Y and beyond through X, generating an extra hop (see Section 2.2).

To fix this, a new field has been added to AS external advertisements. This field (called the **forwarding address**) will indicate the router address to which packets should be forwarded (Section 12.4.4). In the above example, router X will put Y's IP address into this field. If the field is 0, packets are (as before) forwarded to the originator of the advertisement. A different **forwarding address** can be specified for each TOS value.

Whenever possible, this new field should be set to 0. This is because setting it to an actual router address incurs additional cost during the routing table build process (Section 16.4).

Besides preventing extra-hops, there are two other applications for this field. The first is for use by "route servers". Using the **forwarding address**, a router in the middle of the Autonomous System can gather external routing information and originate AS external advertisements that specify the correct exit route to use for each external destination (Section 2.2).

The other application possibly enables the reduction of the number of AS external advertisements that need be imported. Suppose in the example at the beginning of this section that there are two routers (X and Z) exchanging EGP information with the non-OSPF router Y. It is then likely that both X and Z will originate the same set of external routes. Two AS external advertisements that specify the same (non-zero) forwarding address, destination and cost are obviously functionally equivalent, regardless of their originators (advertising routers). The OSPF specification dictates that the advertisement originated by the router with the largest Router ID will always be used. This allows the other router to flush its equivalent advertisement (Section 12.4.4).

F.2 Corrected problems

The following problems in OSPF version 1 have been corrected in version 2.

F.2.1 LS sequence number space changes

The LS sequence number space has been changed from version 1's lollipop shape to a linear sequence space (Section 12.1.6). Sequence numbers will now be compared as signed 32-bit integers. Link state advertisements having larger sequence numbers will be considered more recent. The sequence number space will still begin at (-N+1) (where N = 2**31). The value of -N remains reserved. The LS sequence number of successive instances of an advertisement will continue to be incremented until it reaches the maximum possible value: N-1. At this point, when a new instance

F Version 1 differences

This section documents the changes between OSPF version 1 and OSPF version 2. The impetus for these changes derives from comments received on RFC 1131 and recent field experience with the OSPF protocol. Unfortunately, the changes are not backward-compatible. For that reason, OSPF version 1 will not interoperate with OSPF version 2. However, the changes are small in scope and should not greatly affect any existing implementations. In addition, some of the proposed changes should enable future protocol additions to be made in a backward-compatible manner (see Section F.4).

F.1 Protocol Enhancements

The following enhancements were made to the OSPF protocol.

F.1.1 Stub area support

In many Autonomous Systems, the majority of the OSPF link state database consists of AS external advertisements. In these Autonomous Systems, some OSPF areas may be organized in such a way that external advertisements can be safely ignored, enabling a reduction of the area's database size. This applies to OSPF areas where there is only a single exit/entry that is used by all externally addressed packets, or to cases where some sub-optimality of external routing is acceptable.

Therefore, an OSPF area configuration option has been added (see Sections 3.6 and C.2) allowing the import of external advertisements to be disabled for an area. When this option is enabled, no AS external advertisements will be flooded into the area (Sections 13, 13.3 and 10.3). Instead, within the area all data traffic to external destinations will follow a (per-area) default route. These areas are called "stub" areas.

To implement this, all area border routers attached to stub areas will originate a default summary link advertisement for the area (Section 12.4.3). This will direct all internal routers to an area border router when forwarding externally addressed packets. In addition, to ensure that stub areas are configured consistently, an **Options** field has been added to OSPF Hello packets (Sections A.2 and A.3.2). A bit is reset in the Options field indicating that the attached area is a stub area (Section 9.5). A router will not accept a neighbor's hellos unless they both agree on the area's ability to process AS external advertisements (Section 10.5). In this way, a system administrator will be able to discover incorrectly configured routers, and data traffic will be routed around them (in order to avoid potential looping situations) until their configuration can be repaired.

F.1.2 Optional TOS support

In OSPF there is conceptually a separate routing table for each TOS; the calculations detailed in steps 1-5 of Section 16 must be done separately for each TOS. (Note however that link and summary costs need not be specified separately for each TOS; costs for unspecified TOS values default to the cost of TOS 0).

In version 1 of the OSPF specification, all OSPF routers were required to route based on TOS. However, producing a separate routing table for each TOS may prove costly, both in terms of memory and processor resources. For this reason, version 2 allows the system administrator to configure routers to calculate/use only a single routing table (the TOS 0 table). When this is done, some traffic may take non-optimal routes. But all packets will still be delivered, and routing will remain loop free (see Section 2.4).

In order to avoid routing loops, a router (router X) using a single table must communicate this information to its peers. This is done by resetting the new TOS-capable bit in the router X's router links advertisement (Section 12.4.1). Then, when its peers perform the Dijkstra calculation (Section 16.1) for non-zero TOS values, they will omit router

E Authentication

All OSPF protocol exchanges are authenticated. The OSPF packet header (see Section A.3.1) includes an authentication type field, and 64-bits of data for use by the appropriate authentication scheme (determined by the type field).

The authentication type is configurable on a per-area basis. Additional authentication data is configurable on a per-interface basis. For example, if an area uses a simple password scheme for authentication, a separate password may be configured for each network contained in the area.

Authentication types 0 and 1 are defined by this specification. All other authentication types are reserved for definition by the IANA (iana@ISI.EDU). The current list of authentication types is described below in Table 24.

AuType	*Description*
0	No authentication
1	Simple password
All others	Reserved for assignment by the IANA (iana@ISI.EDU)

Table 24: OSPF authentication types.

E.1 Autype 0 – No authentication

Use of this authentication type means that routing exchanges in the area are not authenticated. The 64-bit field in the OSPF header can contain anything; it is not examined on packet reception.

E.2 Autype 1 – Simple password

Using this authentication type, a 64-bit field is configured on a per-network basis. All packets sent on a particular network must have this configured value in their OSPF header 64-bit authentication field. This essentially serves as a "clear" 64-bit password.

This guards against routers inadvertently coming up in the area. They must first be configured with their attached networks' passwords before they can join the routing domain.

LS type	*Link State ID*	*Advertising Router*	*LS seq no*	*LS age*	*LS checksum*
1	192.1.1.1	192.1.1.1	*	*	*
1	192.1.1.2	192.1.1.2	*	*	*
1	192.1.1.3	192.1.1.3	*	*	*
1	192.1.1.4	192.1.1.4	*	*	*
2	192.1.1.4	192.1.1.4	*	*	*
3	Ia,Ib	192.1.1.3	*	*	*
3	N6	192.1.1.3	*	*	*
3	N7	192.1.1.3	*	*	*
3	N8	192.1.1.3	*	*	*
3	N9-N11,H1	192.1.1.3	*	*	*
3	Ia,Ib	192.1.1.4	*	*	*
3	N6	192.1.1.4	*	*	*
3	N7	192.1.1.4	*	*	*
3	N8	192.1.1.4	*	*	*
3	N9-N11,H1	192.1.1.4	*	*	*
4	RT5	192.1.1.3	*	*	*
4	RT7	192.1.1.3	*	*	*
4	RT5	192.1.1.4	*	*	*
4	RT7	192.1.1.4	*	*	*
4	N12	RT5's ID	*	*	*
4	N13	RT5's ID	*	*	*
4	N14	RT5's ID	*	*	*
4	N12	RT7's ID	*	*	*
4	N15	RT7's ID	*	*	*

Table 23: Sample OSPF link state database display.

6. A listing of the entire routing table. Several examples are shown in Section 11. The routing table is calculated from the combined databases of each attached area (see Section 16). It may be desirable to sort the routing table by Type of Service, or by destination, or a combination of the two.

Again consider router RT3 in Figure 15. Table 21 below indicates that RT4 has been selected as Designated Router for network N3, and router RT1 has been selected as Backup. Adjacencies have been established to both of these routers. There are no routers besides RT3 attached to network N4, so it becomes DR, yet still advertises the network as a stub in its router links advertisements.

Interface IP address	*state*	*cost*	*DR*	*Backup*	*# nbrs*	*# adjs*
192.1.1.3	DR other	1	192.1.1.4	192.1.1.1	3	2
192.1.4.3	DR	2	192.1.4.3	none	0	0

Table 21: Sample OSPF interface display.

3. The list of neighbors associated with a particular interface. Each neighbor's IP address, router ID, state, and the length of the three link state advertisement queues (see Section 10) to the neighbor is displayed.

   Suppose router RT4 is the Designated Router for network N3, and router RT1 is the Backup Designated router. Suppose also that the adjacency between router RT3 and RT1 has not yet fully formed. The display of router RT3's neighbors (associated with its interface to network N3) may then look like Table 22. The display indicates that RT3 and RT1 are still in the database exchange procedure, Router RT3 has more Database Description packets to send to RT1, and RT1 has at least one link state advertisement that RT3 doesn't. Also, there is a single link state advertisement that has been flooded, but not acknowledged, to each neighbor that participates in the flooding procedure (state >= **Exchng**). (In the following examples we assume that a router's Router ID is assigned to be its smallest IP interface address).

Neighbor IP address	*Router ID*	*state*	*LS rxmt len*	*DB summ len*	*LS req len*
192.1.1.1	192.1.1.1	Exchng	1	10	1
192.1.1.2	192.1.1.2	2-Way	0	0	0
192.1.1.4	192.1.1.4	Full	1	0	0

Table 22: Sample OSPF neighbor display.

4. A list of the area's link state database. This is the same in all of the routers attached to the area. It is composed of that area's router links, network links, and summary links advertisements. Also, the AS external link advertisements are a part of all the areas' databases.

   The link state database for Area 1 in Figure 15 might look like Table 23 (compare this with Figure 7). Assume the the Designated Router for network N3 is router RT4, as above. Both routers RT3 and RT4 are originating summary link advertisements into Area 1, since they are area border routers. Routers RT5 and RT7 are AS external routers. Their location must be described in summary links advertisements. Also, their AS external link advertisements are flooded throughout the entire AS.

   Router RT3 can locate its self-originated advertisements by looking for its own router ID (192.1.1.3) in advertisements' Advertising Router fields.

   The LS sequence number, LS age, and LS checksum fields indicate the advertisement's instance. Their values are stored in the advertisement's link state header; we have not bothered to make up values for the example.

5. The contents of any particular link state advertisement. For example, a listing of the router links advertisement for Area 1, with LS type = 1 and Link State ID = 192.1.1.3 is shown in Section 12.4.1.

R5 An advertisement has been received through the flooding procedure that is LESS recent the the router's current database copy (see Section 13). The logging message should include the received advertisement's LS type, Link State ID, Advertising Router, LS sequence number, LS age and LS checksum. Also, the message should display the neighbor from whom the advertisement was received.

The following messages are indication of normal, yet infrequent protocol events. These messages will help in the interpretation of some of the above messages:

N1 The Link state refresh timer has fired for one of the router's self-originated advertisements (see Section 12.4). A new instance of the advertisement must be originated. The message should include the advertisement's LS type, Link State ID and Advertising Router.

N2 One of the advertisements in the router's link state database has aged to MaxAge (see Section 14). At this point, the advertisement is no longer included in the routing table calculation, and is reflooded. The message should list the advertisement's LS type, Link State ID and Advertising Router.

N3 An advertisement of age MaxAge has been flushed from the router's database. This occurs after the advertisement has been acknowledged by all adjacent neighbors. The message should list the advertisement's LS type, Link State ID and Advertising Router.

D.2 Cumulative statistics

These statistics display collections of the routing data structures. They should be able to be obtained interactively, through some kind of network management facility.

All the following statistics displays, with the exception of the area list, routing table and the AS external links, are specific to a single area. As noted in Section 4, most OSPF protocol mechanisms work on each area separately.

The following statistics displays should be available:

1. A list of all the areas attached to the router, along with the authentication type to use for the area, the number of router interfaces attaching to the area, and the total number of nets and routers belonging to the area.

   For example, consider the router RT3 pictured in Figure 15. It has interfaces to two separate areas, Area 1 and the backbone (Area 0). Table 20 then indicates that the backbone is using a simple password for authentication, and that Area 1 is not using any authentication. The number of nets includes IP networks, subnets, and hosts (this is the reason for 2 backbone nets – they are the host routes corresponding to the serial line between backbone routers RT6 and RT10).

Area ID	*# ifcs*	*AuType*	*# nets*	*# routers*
0	1	1	2	7
1	2	0	4	4

Table 20: Sample OSPF area display.

2. A list of all the router's interfaces to an area, along with their addresses, output cost, current state, the (Backup) Designated Router for the attached network, and the number of neighbors currently associated with the interface. Some number of these neighbors will have become adjacent, the number of these is noted in the display also.

C1 A received OSPF packet is rejected due to errors in its IP/OSPF header. The reasons for rejection are documented in Section 8.2. They include OSPF checksum failure, authentication failure, and inability to match the source with an active OSPF neighbor. The logging message produced should include the IP source and destination addresses, the router ID in the OSPF header, and the reason for the rejection.

C2 An incoming Hello packet is rejected due to mismatches between the Hello's parameters and those configured for the receiving interface (see Section 10.5). This indicates a configuration problem on the attached network. The logging message should include the Hello's source, the receiving interface, and the non-matching parameters.

C3 An incoming Database Description packet, Link State Request Packet, Link State Acknowledgment Packet or Link State Update packet is rejected due to the source neighbor being in the wrong state (see Sections 10.6, 10.7, 13.7 , and 13 respectively). This can be normal when the identity of the network's Designated Router changes, causing momentary disagreements over the validity of adjacencies. The logging message should include the source neighbor, its state, and the packet's type.

C4 A Database Description packet has been retransmitted. This may mean that the value of RxmtInterval that has been configured for the associated interface is too small. The logging message should include the neighbor to whom the packet is being sent.

The following messages can be caused by packet transmission errors, or software errors in an OSPF implementation:

E1 The checksum in a received link state advertisement is incorrect. The advertisement is discarded (see Section 13). The logging message should include the advertisement's LS type, Link State ID and Advertising Router (which may be incorrect). The message should also include the neighbor from whom the advertisement was received.

E2 During the aging process, it is discovered that one of the link state advertisements in the database has an incorrect checksum. This indicates memory corruption or a software error in the router itself. The router should be dumped and restarted.

The following messages are an indication that a router has restarted, losing track of its previous LS sequence number. Should these messages continue, it may indicate the presence of duplicate Router IDs:

R1 Two link state advertisements have been seen, whose LS type, Link State ID, Advertising Router and LS sequence number are the same, yet with differing LS checksums. These are considered to be different instances of the same advertisement. The instance with the larger checksum is accepted as more recent (see Section 12.1.7, 13.1). The logging message should include the LS type, Link State ID, Advertising Router, LS sequence number and the two differing checksums.

R2 Two link state advertisements have been seen, whose LS type, Link State ID, Advertising Router, LS sequence number and LS checksum are the same, yet can be distinguished by their LS age fields. This means that one of the advertisement's LS age is MaxAge, or the two LS age fields differ by more than MaxAgeDiff. The logging message should include the LS type, Link State ID, Advertising Router, LS sequence number and the two differing ages.

R3 The router has received an instance of one of its self-originated advertisements, that is considered to be more recent. This forces the router to originate a new advertisement (see Section 13.4). The logging message should include the advertisement's LS type, Link State ID, and Advertising Router along with the neighbor from whom the advertisement was received.

R4 An acknowledgment has been received for an instance of an advertisement that is not currently contained in the router's database (see Section 13.7). The logging message should detail the instance being acknowledged and the database copy (if any), along with the neighbor from whom the acknowledgment was received.

D Required Statistics

An OSPF implementation must provide a minimum set of statistics indicating the operational state of the protocol. These statistics must be accessible to the user; this will probably be accomplished through some sort of network management interface.

It is hoped that these statistics will aid in the debugging of the implementation, and in the analysis of the protocol's performance.

The statistics can be broken into two broad categories. The first consists of what we will call logging messages. These are messages produced in real time, with generally a single message produced as the result of a single protocol event. Such messages are also commonly referred to as traps.

The second category will be referred to as cumulative statistics. These are counters whose value have collected over time, such as the count of link state retransmissions over the last hour. Also falling into this category are dumps of the various routing data structures.

D.1 Logging messages

A logging message should be produced on every significant protocol event. The major events are listed below. Most of these events indicate a topological change in the routing domain. However, some number of logging messages can be expected even when the routing domain remains intact for long periods of time. For example, link state originations will still happen due to the link state refresh timer firing.

Any of the messages that refer to link state advertisements should print the area associated with the advertisement. There is no area associated with AS external link advertisements.

The following list of logging messages indicate topological changes in the routing domain:

T1 The state of a router interface changes. Interface state changes are documented in Section 9.3. In general, they will cause new link state advertisements to be originated. The logging message produced should include the interface's IP address (or other name), interface type (virtual link, etc.) and old and new state values (as documented in Section 9.1).

T2 The state of a neighbor changes. Neighbor state changes are documented in Section 10.3. The logging message produced should include the neighbor IP address, and old and new state values.

T3 The (Backup) Designated Router has changed on one of the attached networks. See Section 9.4. The logging message produced should include the network IP address, and the old and new (Backup) Designated Routers.

T4 The router is originating a new instance of a link state advertisement. The logging message produced should indicate the LS type, Link State ID and Advertising Router associated with the advertisement (see Section 12.4).

T5 The router has received a new instance of a link state advertisement. The router receives these in Link State Update packets. This will cause recalculation of the routing table. The logging message produced should indicate the advertisement's LS type, Link State ID and Advertising Router. The message should also include the neighbor from whom the advertisement was received.

T6 An entry in the routing table has changed (see Section 11). The logging message produced should indicate the Destination type, Destination ID, and the old and new paths to the destination.

The following logging messages may indicate that there is a network configuration error:

C.4 Virtual link parameters

Virtual links are used to restore/increase connectivity of the backbone. Virtual links may be configured between any pair of area border routers having interfaces to a common (non-backbone) area. The virtual link appears as an unnumbered point-to-point link in the graph for the backbone. The virtual link must be configured in both of the area border routers.

A virtual link appears in router links advertisements (for the backbone) as if it were a separate router interface to the backbone. As such, it has all of the parameters associated with a router interface (see Section C.3). Although a virtual link acts like an unnumbered point-to-point link, it does have an associated **IP interface address**. This address is used as the IP source in protocol packets it sends along the virtual link, and is set dynamically during the routing table build process. **Interface output cost** is also set dynamically on virtual links to be the cost of the intra-area path between the two routers. The parameter **RxmtInterval** must be configured, and should be well over the expected round-trip delay between the two routers. This may be hard to estimate for a virtual link. It is better to err on the side of making it too large. **Router Priority** is not used on virtual links.

A virtual link is defined by the following two configurable parameters: the Router ID of the virtual link's other endpoint, and the (non-backbone) area through which the virtual link runs (referred to as the virtual link's **transit area**). Virtual links cannot be configured through stub areas.

C.5 Non-broadcast, multi-access network parameters

OSPF treats a non-broadcast, multi-access network much like it treats a broadcast network. Since there many be many routers attached to the network, a Designated Router is selected for