ISIS Working Group
Internet-draft

Chris Gunner
Digital Equipment Corp.

Doug Montgomery
National Institute of Standards
and Technology (NIST)

July 1994

Experience with the Integrated ISIS Protocol
(draft-ietf-isis-opexp-01.txt)

Table of Contents

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months. Internet-Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet-Drafts as reference material or to cite them other than as a "working draft" or "work in progress."

To learn the current status of any Internet-Draft, please check the 1id-abstracts.txt listing contained in the Internet-Drafts Shadow Directories on ds.internic.net, nic.nordu.net, ftp.nisc.sri.com, or munnari.oz.au.

2. Abstract

This document is one of two reports on the Integrated ISIS protocol. The other report documents an analysis of the protocol. These two reports are required by the IAB/IESG in order for an Internet routing protocol to advance to Draft Standard Status. Integrated ISIS is an Interior Gateway Protocol and is designed to carry both IP and ISO CLNP routing information.

Integrated ISIS is currently designated as a Proposed Standard. The protocol was first published in RFC 1195. Internet Draft [2] was published subsequently to RFC 1195 and documents the current version of the protocol.

This report documents experience with Integrated ISIS. This includes reports on interoperability testing, field experience and the current state of Integrated ISIS implementations. It also presents a summary of the Integrated ISIS Management Information Base (MIB), and a summary of the Integrated ISIS authentication mechanism.

Please send comments to isis@merit.edu.

3. Introduction

This document addresses, for Integrated ISIS, the requirements set forth by the IAB/IESG for an Internet routing protocol to advance to Draft Standard state. These requirements are summarized below. The remaining sections of this report document how Integrated ISIS satisfies these requirements.

3.1. General Requirements

1. **Documents specifying the Protocol and its Usage. This may be one or more documents. The specifications for the** routing protocol must be well written such that independent, interoperable implementations can be developed solely based on the specification. For example, it should be possible to develop an interoperable implementation without consulting the original developers of the routing protocol.

2. **A Management Information Base (MIB) must be written for the protocol. Routing protocols, like all other Internet** protocols, need a MIB defined so they can be remotely managed.

3. **A security architecture of the protocol must be defined. The security architecture must include mechanisms for** authenticating routing messages and may include other forms of protection.

4. **Generally, a number of interoperable implementations must exist. At least two must be written independently.**

5. **There must be evidence that all features of the protocol have been tested, running between at least two** implementations. This must include that all of the security features have been demonstrated to operate, and that the mechanisms defined in the protocol actually provide the intended protection.

6. **There must be operational experience with the routing protocol. The level of operational experience required is** dependent on which level of standardization is requested. All significant features of the protocol must be exercised. In the case of an Interior Gateway Protocol (IGP), both interior and exterior routes must be carried (unless another mechanism is provided for the exterior routes). In the case of a Exterior Gateway Protocol (EGP), it must carry the full complement of exterior routes.

7. **Two reports must be submitted to the IESG via the Routing Area Director. The first report must document how** requirements 1) through 6) of this document have been satisfied. It must include:

a. Implementation experience.

b. Reference to the MIB for the protocol.

c. Description of the authentication mechanisms in the protocol.

d. List of implementations including origin of code.

e. Test scenarios and test results showing that all features of the protocols have been tested.

f. Description of operational experience. This must include topology, environment, time and duration, implementations involved, and overall results and conclusions gained from the operational experience.

The second report must summarize the key features of the protocol and analyze how the protocol will perform and scale in the Internet. The intent of this requirement is to understand the boundary conditions of the routing protocol. The new routing protocol must be compared with the existing routing protocols (e.g., RIP, EGP, etc.) as appropriate. The report should answer several questions:

g. What are the key features and algorithms of the protocol?

h. How much link bandwidth, router memory and router CPU cycles does the protocol consume under normal conditions?

i. For these metrics, how does the usage scale as the routing environment grows? This should include topologies at least an order of magnitude larger than the current environment.

j. What are the limits of the protocol for these metrics? (I.e., when will the routing protocol break?)

k. For what environments is the protocol well suited, and for what is it not suitable?

The IESG will forward to the IAB its recommendation for advancement of the new routing protocol based on its evaluation of protocol specifications and these reports.

3.2. Specific Requirements for Draft Standard

1. Revisions to the Protocol and Usage documents showing

changes and clarifications made based on experience gained
in the time between when the protocol was made a Proposed

Standard and it being submitted for Draft Standard. The revised documents should include a section summarizing the changes made.

2. **The Management Information Base (MIB) must be at the Proposed Standard level of standardization.**

3. **There must be significant operational experience. This must include running in a moderate number of routers configured** in a moderately complex topology, and must be part of the operational Internet. All significant features of the protocol must be exercised. In the case of an Interior Gateway Protocol (IGP), both interior and exterior routes must be carried (unless another mechanism is provided for the exterior routes). In the case of a Exterior Gateway Protocol (EGP), it must carry the full complement of exterior routes.

4. Documentation

The Integrated ISIS protocol is an extension of the ISIS protocol defined by ISO 10589. The first definition of Integrated ISIS which was documented in RFC 1195 was based on the DP version of the ISO standard. In developing Integrated ISIS some revisions to the ISO standard were suggested and defined in RFC 1195. These were incorporated into ISO 10589 with the result that the definitions in RFC 1195 were no longer necessary. Hence an Internet Draft exists for Integrated ISIS which defines the protocol as derived from the ISO 10589 version of ISIS.

The details of what changed between RFC 1195 and the Internet Draft are described in [4]. The implementations and testing described in this document were all based on the RFC 1195 definition of the Integrated additions to the base protocol. They were initially based on the DIS 10589 definition of the base ISIS protocol. Subsequent implementations and testing were based on the standard ISO 10589 definition of the base protocol (see section 9.1 for details).

The Integrated ISIS protocol was developed by the ISIS Working Group of the Internet Engineering Task Force (IETF). This Working Group has a mailing list, isis@merit.edu, where discussions of protocol features and operation are held. The ISIS Working Group also meets during the quarterly Internet Engineering Task Force conferences. Reports of these meetings are published in the IETF's Proceedings.

A Management Information Base (MIB) for the protocol has been developed and published as an Internet Draft [3]. There have been 4 revisions of this MIB. For more information see section 5 of this document.

There is a public-domain implementation of Integrated ISIS available from the University of Wisconsin. This implementation has been incorporated into the public-domain gated program.

5. MIB

A Management Information Base for Integrated ISIS has been published as an Internet Draft [3]. The latest draft is the fourth version of the MIB.

The MIB is based on the managed object definitions defined in ISO's GDMO and contained in ISO 10589 and parts of ISO 10733. A design goal of the MIB was that it provide equivalent functionality as that in the ISO standards. This results in a large MIB since the ISO standards provide richer functionality than that traditionally found in MIBs, for example, the ability to dynamically create and delete table rows and generally provide full configuration control. The MIB provides complete management for both the base ISIS protocol and the Integrated ISIS protocol

A partial implementation of the MIB has been developed by Novell (level 1 and OSI only). A second implementation has been developed by Interactive Systems Corp.

The MIB provides full configuration and monitoring control for the protocol. It supports multiple instances of the protocol running on the same system.

The MIB consists of 17 groups and 214 objects of which:

- 4 groups (106 objects) are mandatory

- 13 are optional depending on the functions supported by the instance of the protocol:

  5 groups (29 objects) must be supported if the instance supports IP

  2 groups (14 objects) must be supported if the instance supports OSI at level 1

  1 group (8 objects) must be supported if the instance

```
        supports OSI at level 2
```

2 groups (10 objects) must be supported if the instance supports the authentication functions

1 group (10 objects) must be supported if the instance supports the partition repair function

2 groups (37 objects) may be supported if the instance wishes to support static route configuration

6. Security architecture

Integrated ISIS provides the option of carrying authentication information in all the protocol's packets. The encoding is extensible to multiple authentication mechanisms. However, currently the only defined mechanism is a simple password, transmitted without encryption. This use of a simple password does not provide useful protection against intentional misbehaviour. Rather, this should be thought of as a weak protection against accidental errors such as misconfiguration.

The protocol and MIB permit separate passwords for each circuit, each area and the domain. Also, although only a single password can be configured for inclusion in transmitted packets, a set of passwords can be configured for reception. This makes migration from one password to another simple. The process is to add the new password to the reception set on each router in turn, then change the transmission password on each router in turn and finally to remove the old password from the reception set on each router. During this process no change in the routing topology need occur.

Since the encoding of the authentication option is extensible to other mechanisms, the protocol can be enhanced in a backwards compatible fashion to support stronger authentication should that be required.

7. Implementations

There are multiple interoperable implementations of Integrated ISIS currently available. This section gives a brief overview of the six implementations that are known to have taken part in interoperability testing. Other implementations also exist or are in development.

The six implementations that are known to have undergone interoperability testing are (listed in alphabetical order):

-   3com. This implementation was wholly developed by 3com. It has participated in the Interop fall '92 demonstration and NIST interoperability testing.

- Cisco. This implementation was wholly developed by Cisco. It has participated in the Interop fall '92 demonstration and NIST interoperability testing.

- Digital. This implementation was wholly developed by Digital. It has participated in the Interop fall '92 demonstration and NIST interoperability testing.

- Phase 2 Networks. This implementation was wholly developed by Phase 2 Networks. It has participated in the Interop Fall '92 demonstration and NIST interoperability testing.

- Proteon. This implementation was wholly developed by Proteon. It has participated in the Interop Fall '92 demonstration and NIST interoperability testing.

- University of Wisconsin. This implementation was developed wholly by the University of Wisconsin. It has participated in the early ISIS testing conducted by NIST. This version is in the public domain and has been incorporated into gated.

In addition to these there are implementations of the base ISIS protocol which have participated in interoperability testing at NIST. These are:

- Wellfleet

- Fibercom

- Retix

- Novell

Note that, as required by the IAB/IESG for Draft standard status, there are multiple interoperable independent implementations of Integrated ISIS, namely those from 3com, Cisco, Digital, Phase 2 Networks, Proteon and the University of Wisconsin.

8. Operational Experience

This section describes some examples of significant operational experience with the protocol. Since Integrated ISIS is a derivation of the ISIS protocol, most of the core algorithms and protocol are common to both ISIS and Integrated ISIS. However, the operational experience reported here is restricted to deployments using Integrated ISIS (those using ISIS are not considered). The interoperability testing includes both ISIS and Integrated ISIS testing since most aspects of the ISIS testing are relevant to showing that Integrated ISIS is interoperable.

As can be seen from the sections below, the protocol has been in use in some reasonable size networks for a significant time. In no case has there been a significant problem with the protocol.

8.1. Case A

This deployment in a large research network has been following a migration plan from DECnet Phase IV and IP to DECnet Phase V and IP over the last few years. Currently I ISIS is in use only on Digital routers of which there are approximately 38 split into **12 level 2 routers and 26 level 1 routers. These are in two** different areas with 6 level 2 and 5 level 1 routers in one area and 6 level 2 and 21 level 1 routers in the other area. Note that all level 2 routers are also level 1 routers.

A small number of the level 1 routers are currently running ISIS (i.e. not Integrated ISIS) even though they are in the same area as the I ISIS routers. This is technically in violation of the topology restriction defined in RFC 1195 which state that all routers in an area of all the level 2 routers must be either ISIS only or be I ISIS only. The reason for this restriction is that an ISIS only router that was on the path between two I ISIS routers would not be able to forward IP packets sent to it consistently with the I ISIS routers (if at all). In this network the ISIS only routers are only at stubs of the area where there is no IP traffic to be routed and this has proved to work correctly.

There are approximately 600 endnodes in each of the two areas. Most of these run DECnet Phase IV and IP and some run DECnet Phase V and IP.

The network migration is currently in the stage of migrating a larger number of Cisco routers to also run I ISIS so that at the end of this stage there will be approximately 130 routers running I ISIS.

The current network topology for the Digital I ISIS routers is a partial mesh of Ethernet and point to point links (at various speeds: 19.2kbps, 64kbps, 128kbps, 256kbps, 512 kbps).

In some cases the routers running I ISIS are configured to not announce reachability to any IP Addresses. This was done to avoid the subnets to which the router attached being announced into the I ISIS domain. These subnets were being announced by other routers using other IP routing protocols already. In these cases these routers forwarded IP traffic as expected.

The network also currently has a larger number (70 or so) routers (mostly Ciscos) which are doing IP routing using Cisco's IGRP. Exchange of IP routes between the IGRP and I ISIS routers is done either using RIP, since that is a protocol common to both, or using static routes. In the RIP case the I ISIS domain propagates all its routes into RIP while the IGRP domain propagates just a default route into the I ISIS domain. The IGRP domain is connected to the Internet.

One problem that this network had was in managing the default route within an area. A restriction of the Digital routers meant that a default route originated on a level 2 router was always at level 2, while on a level 1 router it was always at level 1. Because of the precedence of routes in I ISIS this meant that for that area, the default route at level 1 was always preferred, regardless of metric, over the default route at level 2**. This is the opposite of what would normally be required. This** is not really a problem with the I ISIS protocol but indicates the flexibility that is required in the configuration controls for the routers. In this case implementations should make sure they permit the configuration of which level routes are announced into on a level 2 router.

The use of I ISIS in this network has been operational for approximately 6 months.

8.2. Case B

This commercial deployment has 21 Digital routers all running Integrated ISIS. All routers are configured as level 2. Note that all level 2 routers are also level 1 routers. A main Ethernet LAN has eight I ISIS routers attached together with 10 other IP-only routers (from various vendors: Cisco, 3Com, Sun) which exchange RIP with most of the Digital I ISIS routers. The other routers are connected through a mix of 56kbps and 384kbps point to point links in a partial mesh such that no single link failure will partition the network. At each of the 13 branch sites there is an Ethernet LAN. All the point-to-point links use the DDCMP data link protocol over which I ISIS uses the same point-to-point subnetwork convergence functions as over an HDLC link. Throughout the network there are approximately 900

endnodes of various types: 15 OSI, 200 DECnet Phase IV, 500 IP,
200 IPX (whose traffic is tunnelled through IP).

The network has 14 sites, each of which has a separate OSI Area Address and a separate IP subnet address (using a single subnetted class B network address with a single network-wide subnet mask).

The I ISIS routers that exchange RIP with the IP-only routers operate RIP in send and receive mode and propagate routes from I ISIS to RIP and from RIP to I ISIS. They are configured to accept the default route from RIP but not to announce it in RIP.

The network has a single connection to the Internet via an endnode. Therefore there is no route propagation to or from the Internet.

The average traffic load over the network (including all network protocols) is approximately 300Mbytes per day.

The overall network uptime has been over 99%. Link failures have averaged one per month. These failures have not caused any problems with the applications.

There have been a few designated router changeovers (caused by manual intervention rather than failure). During a changeover there has been no problem with the applications. The changeover process completes within a few seconds.

This network has now been operational for two years.

8.3. Case C

This commercial deployment includes Digital routers running Integrated ISIS and routers from Cisco, Wellfleet and NSC running IP only. The network is a partial mesh of Ethernet, FDDI and point to point links (at 256kbps and 512kbps). There are over 2000 endnodes in the network mostly running IP and/or DECnet Phase IV with 5 OSI endsystems.

All the I ISIS routers are configured as level 2. Note that all level 2 routers are also level 1 routers. Static IP routes are used between some I ISIS routers and some IP-only routers. In some cases the circuit metrics were changed from their default values to create the desired traffic patterns. Convergence of the protocol after link failures has not been a problem.

There are approximately 28 IP subnets with varying subnet masks in use.

This network is not connected to the Internet.

This network has now been operational for over 1 year

8.4. Case D

This commercial deployment has 15 Digital routers. These are interconnected via a mix of 64kbps and 2Mbps WAN links. All routers are running Integrated ISIS. The network has been operational for over 8 months.

9. Interoperability Testing

There have been four testing sessions of the protocol hosted by NIST. These are described in detail in the sections below. For the first three sessions, only the base ISIS protocol was tested. The fourth session was conducted prior to the Fall '92 Interop demonstration and included testing I ISIS.

The information in this section is derived from reference [9].

The following provides a broad summary of the scope of the interoperability testing activities:

- NIST testing has involved 21 distinct ISs, representing 16 distinct models/products from 11 distinct vendors/implementors (3Com, Cisco, Digital, Fibercom, IBM, Novell, Phase2 Networks, Retix, Proteon, University of Wisconsin, Wellfleet). The range of products tested has spanned the spectrum from PC-based LAN routers to FDDI capable backbone routers.

- IS-IS routers have been connected using LANs (802.3, 802.5, and FDDI), point-to-point links (PPP, LAPB, and proprietary) and X.25. To date, only the various LAN technologies have been thoroughly tested with significant multi-vendor interconnections.

- The testing environment has employed ESs from 7 vendors (3Com, Apple, Digital, Hewlett-Packard, NCR, Novell, Sun Microsystems). These ESs have been used to test the interaction between host protocols (ES-IS, CLNP, IP, ICMP) and the IS-IS routing protocol.

9.1. Interoperability Testing Methodology

NIST ISIS interoperability testing has been conducted on an informal basis. The primary objectives of the testing has been to foster mature commercial implementations of OSI-based routing technology. No notions of official NIST certification or endorsement are associated with this activity.

While the primary focus of the testing has been IS-IS functionality, the testing also addresses aspects of the operation of the corresponding data (i.e., CLNP and IP) and supporting protocols (i.e., ES-IS, ICMP, ARP).

The interoperability testing sessions consist of several test scenarios that focus on subsets of the protocol functionality. Within each scenario, individual tests are executed by manually altering: the physical configuration of the testbed, the logical configuration of ISs, and/or the flow of data traffic across the testbed.

9.1.1. Protocol Functions Tested

Individual interoperability tests are selected to exercise specific protocol functions. The functions addressed by NIST testing include:

- IS Adjacencies - L1/L2 IS adjacency acquisition. Primarily tested on LANs, issues tested include: area boundaries, area address computation, protocols supported, authentication. Configurations of 10, or more, ISs adjacencies on a single lan have been tested at L1 and L2.

- Designated IS (DIS) Election - L1/L2 LAN DIS functions. Issues tested include: DIS priority election, resignation, crash, pseudo node generation and sequence number processing.

- Link State Data Base Maintenance - L1/L2 update process functions. Issues tested included: event driven and periodic LSP generation, sequence number LSP processing, LSP propagation, LSP lifetime control.

- ES Adjacencies - L1/ES-IS functions. Issues tested include: dynamic ES adjacencies, area boundaries, manual ES adjacencies, ES poll. Configurations with approximately 30 multi-vendor ES neighbors have been tested at L1.

- L1 Route Computation - L1 decision process functions. Issues addressed include: minimum cost paths, routing to dynamic and manual ES neighbors, computation of nearest L2 IS, equal cost multipaths, path pruning, overloaded ISs, multiple metrics. Configurations with 10, or more, equal cost paths have been tested.

- Reachable Address Prefix (RAP)s - L2 RAP configuration and processing. Issues addressed include: internal and external metrics, RAP reporting in LSPs, default routes.

- L2 Route Computation - L2 decision process functions. Issues addressed include: area routes, prefix routes, path preference, attached flag, partition detection. Configurations with 10, or more, areas within a domain have been tested.

- CLNP/IP Forwarding and other protocol Interactions - Issues addressed include: route switching, error notifications, ES redirection.

9.1.2. Evaluation of Interoperability

Evaluations of the results of interoperability tests are made using various techniques. First order observation of the protocols under test are usually made using the console/management capabilities of individual ISs and protocol analyzers attached to appropriate subnets. Second order observations are made using data streams between ESs positioned throughout the testbed. Observations of the following attributes are typically made during testing:

- Reachability - Examination of individual IS forwarding tables using console/management interface. Observations of duplex data streams between ESs (e.g. ECHO/PING, remote login, file transfer).

- Convergence Time - Maintenance of Transport level connections during routing convergence. Observations of rate controlled ECHO/PING sessions.

- Protocol Stability - Observations of protocol analyzers during reconfigurations and stable periods.

- Protocol Efficiency - No serious attempt has been made to assess protocol efficiency. Casual observations are made using statistics maintained by individual ISs and utilization measurements on protocol analyzers.

9.2. Testing Sessions

Participation in NIST interoperability testing has varied over time. Likewise, the maturity of the implementations tested has varied as new participants joined later sessions. In the sections that follow the results and observations of various sessions are documented. These results document the implementations and specification errors/issues that were found during the session. In many instances, implementation errors were corrected and retested during a single session. In instances in which an issue was raised in multiple sessions, it is typically only documented once.

9.2.1. August 1991 DIS-level Implementation Testing

The first open lab was conducted August 12-16 1991 for the purpose of testing early implementations of the Draft International Standard (DIS) for IS-IS. The participants in this session were: 3Com, Digital, Proteon, Wellfleet, and University of Wisconsin (WISIS in GATED, running on a BSD 4.4 microvax). For most of the participants the implementations under test were relatively immature.

Testing primarily focused upon 802.3 LAN tests. Hardware interface problems prevented successful testing on the FDDI LAN. The testing covered the basic LAN capabilities, level 1 and level 2 routing test scenarios.

The following implementation issues/errors were found during testing:

- Multiple LSPs - Some implementations did not process multiple LSPs from the same system correctly. Once systems began generating non-zero numbered LSPs these systems displayed various problems in LSDB synchronization.

- Unexpected PDU Encodings - Several simple PDU parsing errors were found. Implementations that made novel use of the PDU encoding rules (e.g., that place IS neighbors one per TLV option, use non contiguous LSP numbers) revealed some less than general parsing assumptions in implementations.

- DIS/Pseudo Node Operation - Several implementation issues were discovered with DIS/pseudo Node procedures, including:

  Non DIS systems generating CSNs and responding to PSNs.

  Systems not generating Pseudo Node PDUs correctly.

  Systems not adjusting IIH Hello timers when DIS.

  Few systems implement the ES poll function.

- Area Address Computation - Errors were found in the computation of area addresses. Some implementations only reported the set of manual area addresses.

- LSDB Synchronization - Several implementations had errors in synchronizing LSP sequence numbers after a restart (e.g., either ignored previous sequence number in old LSPs, or counted by 1 up to the correct number).

- L1 Routing L2 IS - Several implementation errors were noted related to the use of L2 attached bit and computation of the nearest L2 IS. Some implementations did not correctly set the attached bit, some set the attached bit when configured L1-only, others did not recognize changes in attached status of remote ISs during L1 SPF. Some systems did not perform background SPF computations.

- L2 Routing - Some errors were found in implementation of path precedence rules and Reachable Address Prefix (RAP) processing of interesting prefixes (e.g., use of odd RAP lengths, use of RAPs with IDI padding rules).

- ES-IS Redirection - Some errors were found in the ES-IS redirect function (e.g., redirecting ISs, improper RD PDU encodings).

The following specification issues/errors were found during testing:

- Precedence of Routing Protocols - Questions arose relating to the relative precedence of IS-IS and ES-IS derived routing information. Some implementations assign routes derived from ES-IS a higher precedence than those computed by IS-IS. That is, CLNP PDUs are delivered to ESs over the subnets to which they are directly attached while other IS-IS paths with lesser cost exist.

  The intention of the ISIS protocol specification is that only routes computed by the protocol are used for forwarding to end systems. Adjacencies to end systems derived from ESIS are reported in the router's LSPs. Since a router includes its own LSPs in its forwarding database computation, routes to its adjacent end systems will be computed. The shortest path from a router to an end system will depend only on the metrics assigned to the circuits. The relative preference of circuits can be controlled by adjusting their metric through management parameters. This has been clarified in the Integrated ISIS specification [2]. This clarification is intended for submission as a defect report to the base ISIS standard [5].

- Redirection Based Upon RAPs - It was noted that issuing a redirect as the result of forwarding based upon a RAP may require the Network Entity Title (NET) of the next hop. This information is not specified as part of the RAP configuration information. It was also noted that if an NET was specified, the SNPA and the "liveness" of the RAP next hop could be determined using the ES-IS protocol.

  The next hop's NET must be included in a Redirect if the next hop is a router. This requires that the base ISIS standard have an additional attribute in the Reachable Address managed object which is set to the NET of the next hop. A new attribute (nextHopNET) for the Reachable Address managed object which can be set to the next hop NET is defined in the Integrated ISIS specification [2]. An equivalent object (isisRANextHopNET) has been added to the Integrated ISIS MIB [3]. The default value of both of these is an octetstring of length 1 with octet value zero. This default means that Redirect PDUs will be encoded with a NET field even though the NET value is not that of any system. Some End systems use the presence or absence of the NET field in the Redirect PDU to determine how to originate packets for that destination, for example, the maximum PDU size to use. This addition is intended for submission as a defect report to the base ISIS standard [5].

- ES Poll - Some implementors that did not implement the ES poll function did so intentionally noting that few ESs support the ESCT option upon which the function is based. It was noted that for the ES poll function to be effective ESCT processing must be supported by ESs.

  The problem with ESs not supporting the option is that during a poll the router will adjust the timer for ES adjacencies on the assumption that ESs will respond to the poll. If they do not process the ESCT option then their adjacencies will be timed out by the router and then reformed later when the ESs send out their normal frequency ES Hellos. Before being reformed those end systems will be unreachable. The polling process is triggered when there has been a routing topology change, since this may have occurred when an extended LAN becomes partitioned on failure of a bridge. In this case the router wants to determine as quickly as possible the circuits through which the end systems are reachable. To avoid the problem of end systems that do not implement the option, a management attribute has been added to each circuit which controls whether existing end system adjacencies are timed out more quickly (as defined by the poll function) or left to time out with their current holding time. The new attribute is useESConfigurationPolling in the base ISIS standard [5] and is isisCircESPolling in the MIB [3]. The default value for these is to not do polling. This addition is intended for submission as a defect report to the base ISIS standard [5].

9.2.2. February 1992 IS-level Implementation Testing

The second open lab was conducted February 24-28 1992 for the purpose of testing implementations of the recently finalized International Standard (IS) version IS-IS. The participants in this session were: 3Com, Digital, Fibercom, Proteon, Wellfleet, Cisco, Retix, Novell.

Testing primarily focused upon 802.3, and FDDI LAN tests. The testing covered the basic LAN capabilities, level 1 and level 2 routing test scenarios. The maturity level of the implementations, including those participating for the first time, was significantly higher than in the previous open lab. This allowed more time for testing additional, secondary features of the protocol, including:

- Authentication features.

- Overloaded ISs.

- Partition Repair.

During this open-lab session, the NIST IS-IS Multiparty Conformance Test Systems was demonstrated operating upon vendor implementations. Experimental conformance test suites for the subnetwork and update processes were executed.

The following implementation issues/errors were found during testing:

- Circuit State Changes - Some implementations were unable to determine the status of circuits in some situations (e.g., serial circuits marked external).   Some implementations failed to reflect changes in circuit states in their LSPs (e.g., failure of event driven LSP to drop IS neighbors or RAPs lost due to circuit state changes).

- Multi-pathing - Configurations with up to 10 equal cost multipaths revealed some SPF implementation/scaling errors.

- Overloaded ISs - Some implementations completely ignore LSDB overload state in ISs. In those that recognized the state, there were differences in implementation of this feature (see specification issues below).

The following specification issues/errors were found during testing:

- IIH Padding - Discrepancies in configured data link block sizes on FDDI initially prevented IS adjacency acquisition. The IS with the smaller configured data link block size was capable of receiving larger IIHs, but the other IS would reject IIHs that were padded to a smaller block size than its own. Questions arose regarding whether PAD length checks are required upon receipt of IIHs.

  The Integrated ISIS specification [2] has been clarified to state that no check is made on the padded length of received IIHs. The purpose of the padding is to ensure that ISIS protocol packets of maximum size can traverse the transmission path between the neighbors (which may be an extended LAN made up of different media). It is not necessary that neighbors have the same data link block size. This clarification is intended for submission as a defect report to the base ISIS standard [5].

  In addition a new management attribute has been defined in the Integrated ISIS specification [2] and the GDMO in ISO 10589 and to the I ISIS MIB which controls whether ISIS Hellos transmitted on a broadcast circuit are padded. The use of padding can cause significant overhead, for example, over remote bridging using low bandwidth WAN links.

- Area Addresses - Questions arose as to the use of computed area addresses in uses other than IS-IS PDUs. In particular questions arose as to:

  If dynamic ES adjacencies should be rejected if they match a manual area address that has been dropped.

  If a manual area address is dropped from the area this indicates a configuration error since the result will be that reachability to some systems may be lost, since that area address will not be announced at level 2. The Integrated ISIS specification [2] has been clarified to describe what is the effect of dropping a manual area address on the parameter manualAreaAddresses (there is no effect).

  For the purposes of forwarding and lowest NET computation some interpretations varied, with different implementations using: the manual area addresses, the computed area addresses, the union of both.

The Integrated ISIS specification [2] has been clarified to make it clearer in the forwarding description which area addresses are used (the set defined by the areaAddresses parameter).

- Routing Through an Overloaded IS - There were some questions regarding the description of SPF computation in the presence of an overloaded IS.   While the text implies that one should consider ES adjacencies on the other side of an overloaded IS, some implementations will not compute the SPF through the overloaded IS to the pseudo node (which contains the LSP for the dynamic ES adjacencies). Such implementations will only compute routes to the the manual ES adjacencies of an overloaded IS.

  The purpose of including ES adjacencies of an overloaded router in the SPF computation is really just to maintain a path to the overloaded router itself, since a router announces its own ID as reachable in its level 1 LSP ES neighbor options. This path is needed so that management traffic can reach the overloaded router. During overload, reachability to other systems in the area or domain is affected and it doesn't seem worthwhile adding extra complexity to the SPF computation to try and keep reachability to end systems through an overloaded router. The SPF algorithm in the base standard is not very clear about this and so some clarifying text has been added to explain the behaviour. What happens is that the LAN end systems will be reachable through non-overloaded routers on the LAN, but will not be reachable through any overloaded routers including the designated router itself (if it is overloaded). If the designated router is overloaded it sets the "infinite hippity cost" bit in its pseudonode LSPs and its own LSPs. Therefore a path through the designated router is not computed because its reachability to the pseudonode is blocked.

- Partition Repair - In attempting to test the partition repair function it became obvious that the description of partition repair forwarding had the real potential for routing loops. In the two sets of modifications to the standard to add descriptions of precedence of routes and make partition repair optional the standard created a potential looping condition in areas in which only some ISs implement partition repair.

  This problem has been clarified in the base ISIS standard through the submission of defect reports which have been agreed as part of Technical Corrigenda 1 and 2 [6 and 7].

- Attached Bit in Single Area Domains - In testing inter-area routing and computation of the nearest L2 IS discussion arose as to the inability to support single area domains with external RAPs. In particular, an L2 IS with RAPs (e.g., default prefix) but no area routes will not identify itself as attached. It was felt that this was a deficiency in the protocol.

This has been clarified in the base ISIS standard through the submission of a Defect Report which has been agreed as part of Technical Corrigendum 1 [6]. The presence of any Reachable Address Prefix causes the level 2 router to consider itself as "attached".

9.2.3. Spring 1992 Interop Demonstration

The participants in NIST interoperability testing activities demonstrated multi-vendor IS-IS interoperability at the spring 1992 **Interop conference. The demonstration was conducted within** the NIST booth, with periodic (i.e., after hours) interoperability testing with the shownet routers. The participants in this demonstration were: 3Com, Digital, Cisco, Proteon, and Phase 2 Networks.

The demonstration consisted primarily of L1/L2 route switching demonstrations across 802.3, and FDDI LAN tests.

During the course of this demonstration one specification issue was raised:

- DIS TOS Support - Questions arose as to whether the DIS should report support for all metrics in its pseudo node LSPs. Failure to do so causes some SPF implementations to abandon TOS paths that actually are contiguous.

  The problem here is that the designated router announces reachability to systems on the LAN on behalf of other routers on the same LAN, but the TOS supported by the routers may be different. Since all routers must support the default TOS, there will always be a default TOS path. However, if there were a path at a non-default TOS that were contiguous except for the pseudonode hop then that non-default TOS path could not be used - the default TOS path would be used.

  The solution is to have the designated router announce reachability at all TOS to LAN systems in its pseudonode LSPs even if that router is not configured to support one or more of those TOS. Since the announced cost in these LSPs is always zero, there is no problem of choosing the cost to use when doing this. This permits fully contiguous TOS paths to be computed through the pseudonode. This change has been added to the Integrated ISIS specification [2].

9.2.4. Fall 1992 Interop Demonstration Hot Stage

An open lab was conducted in October 1992 for the purpose of hot staging the fall 1992 Interop integrated IS-IS multi-vendor demonstration. The direct participants in this session were: 3Com, Digital, Cisco, Proteon, and Phase 2 Networks. Most of the participants in this session had recently added Integrated support to their existing IS-IS implementations.

Testing primarily focused upon 802.3, and FDDI LAN tests.

The testing scenarios covered the basic LAN capabilities, level 1 **level 2 routing test scenarios.** Given maturity level of the OSI capabilities of the implementations under test, most effort was directed at testing those IP capabilities required for the upcoming Interop demonstration.

The following implementation issues/errors were found during testing:

- L2 Reachability Summarization - Some implementations reported configured address summaries when there was no corresponding internal reachability.

- Nearest L2 IS and L1 Default Routes - Some implementations did not correctly establish a default route to the nearest L2 IS. Also, some implementations did not replace the route to the nearest L2 IS with announced L1 default routes.

The following specification issues/errors were found during testing:

- Precedence of Routes - There were some questions regarding the relative precedence of I-IS-IS derived routes and directly attached interfaces. In particular, some implementations chose to treat local direct interfaces at a higher priority than I-IS-IS derived routes. Thus, longer-match or lesser cost I-IS-IS derived routes are ignored when the destination appears to be on the locally attached subnet.

  As with end system adjacencies, routes derived from the router's local interfaces are reported in the router's LSPs and will be included in the shortest paths computation.

There is no need to have preference controls for local routes versus Integrated ISIS derived routes. Text has been added to the Integrated ISIS specification [2] to make this clear.

- Reporting Interfaces on Which I-IS-IS is disabled - Questions arose as to whether an interface over which I-IS-IS is not operating should be reported as reachable?

  There are two ways that the IP reachability information attached to an interface get announced in LSPs. First, some or all of the addresses of the router on its interfaces are announced in the "IP Interface Address" options in LSPs so that other routers learn one or more addresses for the router. Second, the subnet addresses (IP address and mask) associated with each interface are announced in the router's "IP internal Reachability Information" options. In both cases, IP reachability information can be included even if the interface it is attached to does not have I ISIS enabled. A router may provide configuration controls to determine which information is announced in LSPs. For interface addresses, this must default to announcing at least one address from any of the router's interface regardless of the state of I ISIS on that interface. For subnet addresses this must default to announcing all subnet addresses from all the router's interfaces regardless of the state of I ISIS on that interface. Clarifying text has been added to the Integrated ISIS specification [2].

10. References

[1]Callon, R.W., "Use of OSI IS-IS for Routing in TCP/IP and dual environments", RFC 1195, December 1990.

[2]Callon, R.W., "Use of OSI IS-IS for Routing in TCP/IP and dual environments", Internet-draft draft-ietf-isis-tcpip-01.txt, July, 1994 (obsoletes RFC 1195)

[3]Gunner, C.W., "Integrated IS-IS Management Information Base", Internet-draft draft-ietf-isis-mib-04.txt, July, 1994.

[4]Gunner, C.W., "Integrated IS-IS Protocol Analysis", Internet-draft draft-ietf-isis-prot-anal-00.txt, March, 1994.

[5]"Information Technology - Telecommunications and information

exchange between systems - Intermediate system to Intermediate system Intra-Domain routeing exchange protocol

for use in Conjunction with the Protocol for providing the Connectionless-mode Network Service (ISO 8473)", International Standard 10589 (ISO submission copy), October 1991.

[6]International Standard 10589 - Technical Corrigendum 1

[7]International Standard 10589 - Technical Corrigendum 2

[8]"Information Technology - Telocommunications and information exchange between systems - Elements of Management Information Related to OSI Network Layer Standards", International Standard 10733 (ISO submission copy), September 1992.

[9]Montgomery, D. "IS-IS Interoperability Testing at NIST", Draft, October 1993.

11. Acknowledgements

Thanks are due to members of the ISIS working group of the Internet Engineering Task Force (IETF) for their input to this document. Thanks are due especially to Ross Callon and Mike Shand for technical review. Doug Montgomery acknowledges support for the NIST interoperability testing work from the National Science Foundation (Contract No. NCR-9120054).

12. Working Group Information

The current co-chairs of the ISIS working group are:

Ross Callon
Wellfleet Communications Inc.
2 Federal Street
Billerica
MA 01821
USA

Phone: (508) 436 3936
Email: rcallon@wellfleet.com

Chris Gunner
Digital Equipment Corp.
550 King Street
Littleton
MA 01460-1289

USA

Phone: (508) 486 7792
Fax: (508) 486 5279
Email: gunner@dsmail.enet.dec.com

The working group mailing list is:

isis@merit.edu

Subscription requests should be sent to:

isis-request@merit.edu

13. Author's Addresses

Chris Gunner
(see co-chair information above for mail, etc.)

Doug Montgomery
National Institute of Standards and Technology (NIST)

Phone: (301) 975 3630
Fax: (301) 590 0932
Email: dougm@osi.ncsl.nist.gov