Attacks on the IS-IS routing protocol
Project in Computer Security (236349)

Roee Hay ◆ Jonathan Kalechstain
<roeehay,kalechstain@gmail.com>

Under the supervision of Dr. Gabi Nakibly <gabin@rafael.co.il>

July 8, 2012

We start by describing the IS-IS routing protocol. We then depict some documented IS-IS attacks, and state whether some known OSPF attacks are also feasible on IS-IS. Afterwards we dive into IS-IS attack which are either new or have a greater implication in comparison to their OSPF counterpart. The document ends with our PoC results.

1 The IS-IS routing protocol

1.1 Basics
IS-IS is a link-state routing protocol that is very different than other network protocols such as RIP, OSPF because it runs on layer 2 of the OSI Reference Model.

1.1.1 Areas
Area is a part of a large network.

If the entire network was consisted of a single set of routers, all with a common database, then calculating the SPF would cost exponential time.

The main idea is that a router would have to know only its area topological horizon, thus calculating the SPF on a smaller graph which keeps the CPU less busy. Inter-area routing is done by choosing the path to the closest interconnecting router, without considering the graph outside the area. Thus it trades CPU resources for sub-optimal routing.

1.1.2 Levels
In IS-IS each router carries one of three tags: L1,L2 or L1L2. In IS-IS there are no “border area” routers and each router is assigned to only one area.

In OSPF the Area-Id of two routers has to match or no adjacency will occur.

If that was true in IS-IS no routing information would pass between areas that has no intersection, the levels help taking care of this problem:
Two graphs are formed. one with L1 ,L1L2 routers and one with L2,L1L2 routers. In Level 1 topology all routers must have the same Area-Id or no adjacencies will form.

For L2 an adjacency will form whether the Area-Id matches or not.

1.1.3 IS-IS Addressing
IS-IS inherited its addressing structure from the OSI suite of networking protocols.

There is just one OSI address assigned per router. The OSI address, also referred as NET consists the area-ID, the System-ID and The NET Selector.

The NET Selector-the last byte of the NET. In IS-IS it always has to be zero, or else no adjacencies are formed.

The System-ID consists of 6 bytes before the Net Selector which uniquely identifies the router.

Area-ID is the variable part of the NET, ranging from 1 to 13 bytes.

1.2 Neighbor Discovery and Handshaking
IS-IS, like most routing protocols, provides a mechanism that allows routers to identify if adjacent routers speak IS-IS. This is done by Network Discovery. The second mechanism, Handshaking, allows a router to classify whether a given link is bi-directional.

1.2.1 Neighbor Discovery: The Hello message
The Hello message provides the above. There are three types of Hello messages: Level 1 LAN Hello, Level 2 LAN Hello and P2P Hello. All messages begin with an IS-IS common header, followed by an Hello type-specific header.

LAN Hello (PDU types 15,16) The message states the following attributes:

- Link levels (L1, L2, L12).
- System-ID (’Source-ID’) of the sender
- Holding Time: Maximum session life time. A received Hello resets the associated timer (corresponding to the PDU type). A router contains a constant \( ISISHoldingMultiplier \), which directs the router to send an Hello message every \( HoldingTime/ISISHoldingMultiplier = ISISHelloTimer \) seconds. Each router can set its Holding Time independently from other routers, in contrast to OSPF.
- Priority and DIS LAN-ID: Relate to the DIS election and are discussed in the next section.

P2P Hello (PDU type 17) This message is similar to the LAN Hello one, with two small differences. First, it does not contain information needed for the DIS election, since there is no DIS in P2P links. Second, it contains another attribute called ‘Local Circuit-ID’, which specifies the link’s circuit number. The latter is only used for informational purposes. Notice that in contrast to the LAN Hello message, the P2P Hello can reset both timers. This is specified by the Circuit-Type field, which is placed in the common header.
1.2.2 Handshaking: Verifying two-way connectivity

Routers verify whether a link is two-way capable, before advertising an adjacency. There are two types of handshakes: 2-way and 3-way. The former, is done as follows: Router A sends an Hello message to Router B. When A has received an Hello from B, it will set up an adjacency. This protocol is stateless in the sense that the Hello from B does not contain any indication that it is a response to A's hello. The 3-way handshake is very similar to TCP's handshake. Router A sends an Hello to B. The latter responds with an Hello to A, with indication in the form of a TLV that specifies A's MAC address. When A has received this message, it sets up an adjacency, and responds with an Hello with a similar TLV. B sets up an adjacency to A when it has received that message. The 3-way handshake is stateful. On LANs, only 3-way handshaking is supported, and the IS-Neighbor TLV (#6) is used for the MAC specification. The original protocol only support 2-way handshakes for P2P, which causes problems such as black holes or blind-spots. Later, [2] added support for 3-way handshaking over Point-to-Point links, in order to overcome these problems.

1.2.3 Sub-net verification

As explained above, IS-IS should be network layer agnostic, as it is implemented on top of Layer-2. There are various TLVs for different Layer-3 protocols, such as the IP Interface TLV (#132), which are bundled with the Hello message. The TLV (#132) for example, is used to check if the potential adjacency can be used as a next-hop.

1.2.4 Liveness detection

As mentioned above, the router should be consider dead if an Hello hasn’t been received for HoldingTime seconds. In addition to that, a link can be detected to be down, either physically or by using a Layer-2 Local Management Interface. Moreover, an external protocol, BFD, can be used, and is supported by JunOS and IOS [6].

1.3 Generating, Discovering and Aging LSPs

Link state protocols like OSPF and IS-IS distribute their IP reachability and topological view throughout an area.

In order to flood the information and keep it updated, the information is encoded into a link state protocol data unit, or LSP.

1.3.1 Distributed Databases

In distributed Databases all routers share information about the topology of a network. If each router contributed its information to its neighbors who would pass it along in a connective graph, then eventually all routers would hold that information and understand the entire network.

IS-IS stores two databases for such maps of the network.

1) The first is the map which typically represents the closer routers, called POP and is stored in the Level 1 database.

2) The second map typically represents the backbone of the network, and is stored in the Level 2 database.
1.3.2 LSP’s And Revision Control

After distributing the local information each router computes the SPF using Dijkstra’s algorithm.

LSP can be considered as an envelope that is used to pass information throughout the network. that information can be IP-routes, check-sums etc.

LSP needs to be genuine always; if a connection between two routers broke they must inform the rest of the network (by LSP’s) and subsequently local databases are updated and the SPF trees are recomputed.

A few important LSP attributes:
1) Sequence number: the sequence number is an integer (32 bit) that helps deciding which LSP is newer. When a router gets an LSP that is new to him, it just installs it in its database.

If the LSP is already installed then it checks whether the LSP that arrived has a newer sequence number and if so it updates that database. If its older he disregards it.

2) Lifetime: a 16 bit entity that indicates the number of second the LSP is valid in the system (usually 20 minutes)

3) LSP Refresh Interval: the number of seconds before a new LSP is issued by a router (with seq_num++). It is important that the interval time is lower than the Lifetime so LSPs won’t expire. (it is usually set to 300 seconds less than the Lifetime).

1.3.3 Link State PDU

The LSP header in the PDU has 4 very important elements: Lifetime, Sequence Number, LSP-ID and Checksum.

The first two were discussed, while the last will be mentioned in the security section. The LSP-ID field is an eight byte field which determines the LSP type. The last byte in the LSP header is the attribute block. The block has a few bits that tells us whether the router is attached to another router.

A more significant bit is the overload bit. If this bit is turned on it means the router is running short of memory, and from now on all other routers will calculate Dijkstra disregarding the router for delivery of transit traffic.

1.3.4 Flooding

Flooding is an algorithm that is meant to pass information throughout the network, and is carried after a router acquired its neighbors and built up adjacencies.

We differentiate between a router $A$ that is the origin of the LSP and an intermediate router $B$ that just passes the message.

$A$ simply sends the LSP to all his adjacencies. $B$ is very similar, despite that it does not send the message back to to the originating interface.

If a circle exists in the graph, an endless loop can occur. This is another important use of the sequence number: if it is newer, install it. If it is older or the same (for our case a second visit occurs in the circle) discard it.

1.4 Pseudonodes and Designated Routers

1.4.1 Scaling periodic events

In order to avoid a self-synchronization scenario, at which a router received a large amount of a messages at a very short time, a 25% jitter is applied to various timers, such as $ISISHelloTimer$. 

4
1.4.2 Pseudonodes

**Problem** If a LAN were simply treated as a set of adjacencies, a couple of issues would arise. First, the number of adjacencies would be $O(n^2)$ where $n$ is the number of routers. This would create very large databases. Second, in case of a state change, according to the flooding algorithm, all routers would need to notify the network of that update.

**Solution** Within a LAN, a special node is elected, called the DIS. This node represents the LAN, and adjacencies are only made with that node.

**Pseudonode addressing** The LSP-ID is composed of a System-ID, Pseudonode-ID and Fragment-ID.

- Real systems (including the DIS) have their Pseudonode-ID set to zero.
- The Pseudonode carries the System-ID of the DIS, and a Pseudonode-ID different than zero.

**Pseudonode cost** In order to preserve the original cost topology of the LAN, the cost from the Pseudonode to the real routers is always zero, and the cost from the real routers to the Pseudonode is the original link cost.

**The election process** The LAN Hello message (LAN-IIH) is used for electing the DIS. Recall that there are two fields in the LAN-IIH, Priority and Source SNPA (MAC). A priority of zero means that the system does not wish to become a DIS. In case of a collision, the system with the higher SNPA address is elected. If a new DIS is elected (e.g. a router with a priority higher than the current DIS becomes online), the older DIS purges the Pseudonode.

1.5 SPF and Route Calculation

1.5.1 The SPF Algorithm

The SPF algorithm was invented by Edsger Dijkstra in 1956. Given a directed graph $G = (V, E)$ with weights on the edges $W : E \rightarrow R^+$ the algorithm runs from a given vertex $s$ and calculates the shortest paths from $s$ to all other vertices in the graph.

During the run of the SPF algorithm, 3 lists are held : UNKNOWN, Tentative and Paths.

- At first, all nodes are held in the UNKNOWN list. The next node being examined is moved to the Tentative list, along with the router running SPF, $s$.
- In that list are held in triplets the neighbors names, the edges cost and the cost to $s$.
- When the best path is determined, the node is moved to the Paths list, which means that the best route has been found.

1.5.2 Full SPF Run

The full SPF re-computes the topological grid in an area as well as recomputes the reachable IP prefixes.

Events like local configuration change, receipt of a new unknown LSP, link metric change and more, all trigger the run of the algorithm.

When one of these events happen, the SPF calculation doesn’t immediately begin, but has a delay time. The idea behind this is to wait a little if another relevant LSP shows up (what usually happens).

During the calculation itself, the database is locked, because else the SPF calculation may result with bogus routes.
The main idea behind the SPF hold down is to allow the router work less. When calculating the full SPF the CPU utilization is 100%, and once finished it drops to 0%.

In an unstable system many appearances of LSP’s can keep the CPU extremely busy. Therefore we may lose responsiveness, but earn stability of the router control plane.

1.5.3 Partial SPF Run

This run only calculates the leaf related information. This run is usually triggered by Metric of prefixes change, new prefix and deletion of prefix.

This partial run is basically a search operation, which finds the lowest metric for a given prefix.

Because the burden this sort of run adds to the CPU is much lower, the need for self protection here is much smaller than in Full SPF Run.

1.5.4 Incremental SPF Run

This is a basically faster method of the full SPF Run. It has additional data structures which hold data from previous SPF calculation and help making better decisions.

For example, if a link between two routers fell, and that link wasn’t in the latest SPF tree, then there is no need to recalculate the Full SPF Run because that route wasn’t taken into consideration anyway. It was studied that the incremental SPF Run performances are by a factor of 80% better than the Full SPF Run.

1.6 Synchronizing Databases

IS-IS has two PDU types for synchronizing databases: CSNP (Complete Sequence Number Packet) and PSNP (Partial Sequence Number Packet). The mechanisms and the use of CSNPs and PSNPs are different depending on the media-type (broadcast LAN or P2P).

1.6.1 Synchronization on Broadcast LANs

In the LAN IIH message, a router specifies what it believes the LAN’s DIS is. The DIS should periodically send the link-state database using a CSNP, to the address AllL1ISs or to AllL2ISs.

LSP entry TLV (#9) is inserted to these PDUs. This TLV describes the LSP by containing the following attributes:

- LSP-ID
- Sequence Number
- Remaining lifetime
- Checksum

When a LAN router receives a CSNP from the DIS, it compares each LSP entry with its own local database. If the sequence number matches, then it everything fine. Otherwise, there are three scenarios:

1. If the received sequence number is older, then the DIS is not synched, and the router floods the the new version of the LSP. The DIS does not ack the update, as the local router can notice the change in the next CSNP.
2. If the received sequence number is newer, than the local router sets the SRM flag for the LSP, which causes a PSNP PDU to be sent to the DIS, and the latter re-floods the more recent LSPs into the LAN.

3. If a new LSP-ID is reported, then the local router requests the missing LSP using a PSNP PDU, which causes the DIS to re-flood the LSP into the LAN.

1.6.2 Synchronization on P2P links

When a router comes up, it will jitter a 5-second timer by 25%, before sending a CSNP PDU. The other end realizes the missing LSPs, and re-floods them.

On P2P links, updates must be acknowledged, hence the SRM flag is set on the flooded LSP, and cleared (and removed from the retransmissions list) when an ack (a PSNP PDU with a corresponding LSP Entry TLV) is received.

1.7 TLVs and Sub-TLVs

IS-IS is an extensible protocol. It uses TLVs (Type-Length-Value) encoding in various information exchanges.

The length field is used for backward comparability. The length field is one byte long. TLVs can be present in all three IS-IS packets types (IIHs, SNPs, LSPs).

Sub-TLVs are similar to TLVs, but are used inside TLVs, in order to extend them.

See Appendix 1 for a list of various TLVs.

1.8 Security in IS-IS

1.8.1 Authentication

Authentication is supported through the Authentication TLV, that specifies the Authentication Type attribute. To date, authentication is supported on all PDU types (IIHs, SNPs, LSPs). Originally, IS-IS only supported simple password authentication, but HMAC-MD5 signing was declared in [5], and later support for generic authentication was proposed by [1]. Simple Text authentication supports passwords up to 254 bytes. It is sent in clear-text in IIHL message. HMAC-MD5 supports a 16 bytes key. Generic authentication is carried over the Authentication TLV (#10), and defines a new Authentication type (CRYPTO_ATUH).

The generic authentication schemes supports various authentication algorithms (at present HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 are supported).

2 Documented IS-IS attacks

2.1 Fight-back of death ([7])

This attack takes leverage of the Fight-back mechanism. The attacker sends an LSP with Sequence Number set to SequenceModulus to the attacked router, and set the latter as its source. This shall trigger a Fight-back mechanism, but according to section 7.3.16.1 of [3], it would generate the event “Attempt to Exceed Maximum Sequence Number”, that subsequently disables the Routing Module for a period of at least MaxAge + ZeroAgeLifetime. This attack is similar to the MaxSeq# one of [12]. In addition, a similar attack to the one depicted under [11] can be achieved, by putting false routing information on the SequenceModulus injected LSP.
2.2 DoS by using the authentication mechanism ([7])
It is possible to flood a given system with integrity protected PDUs which would trigger the HMAC validation routines. These routines are CPU intensive, so attackers can cause significant CPU usage.

2.3 Replay attacks ([7])
IIH and SNP PDUs have no sequence numbers, thus they are vulnerable to replay attack, in order to cause churn in the network or bring down the adjacencies. Link State PDUs contain 32-bit sequence number. When the latter wraps around or when the system is reset, and if the key has not changed, the attacker can replay these packets, which would potentially contain different information than the current one. In addition, The CSNP or PSNP packets can be replayed in order to cause LSP flood in the network.

3 Porting OSPF attacks to IS-IS

3.1 Periodic Injection ([10])
Ported from . According to the [3], there is an LSP generation hold-time timer, MinLSPGenerationInterval, which most likely also constraints the generation of 'Fight-back' LSPS. An attacker can inject malicious LSPs into the network at a higher frequency, in order to reduce the effectiveness of the fight-back mechanism. In contrast to OSPF, the attacked router would not participate in the flooding process.

3.2 Partitioned Networks ([10])
If the subverted router is a cut vertex, it can be arranged that the forged LSP would never reach the legitimate router, hence fight back would not be triggered.

3.3 Phantom Routers ([10])
Attack is performed on behalf of non-existing routers, thus there are no legitimate router which would fight-back.

3.4 Attacker Leveraging Fight Back ([10])
Fight back can be used for DoS. Traffic produced by a single forged LSP packet is amplified by the correcting LSPs traffic.

3.5 Dealing with External Routes ([10])
A subverted $L_2$ router can announce IP External Reachability Information, with internal metrics. According to [4] if the external reachability is defined with internal metrics, it would be preferred over paths with external metrics, regardless of their weight.

3.6 Packet Header with Cryptographic Authentication Enabled ([10])
The MAC does not sign the Layer-2 header. This means that any operation which relies on the Layer-2 header, can be subverted by an attacker.
3.7 Tampering with the Hello Message ([10])

According to [3], upon the receipt of LAN IIH PDU, if there is no intersection between the announced area addresses and the set of area addresses in the manualAreaAddresses characteristic, then the adjacency is bounced. In addition, a malicious system may inject a spoofed LAN IIH PDU, which has a low holding timer, in order to tear down the adjacency. Moreover, if a LAN IIH is received on \( R \), and \( R \) is not included in the PDU, then the adjacency downgrades to the initializing state. An attacker may also cause a router to resign as a designated IS, by spoofing sending an IIH PDU with a highest priority, from a ghost router.

3.8 Tampering with Level 1/2 Link-State Updates PDUs ([10])

A malicious router can maliciously modify an incoming LSP, or inject a new LSP, which claims to originate from some router (and increase its sequence number by one (analogous to the Seq++ attack of [12]). This injection or modification should trigger a fight back from the attacked router. The malicious router can do the following:

1. Enable the hippity bit (in case it is disabled) so the router would not be considered as a transit path.
2. Disable the hippity bit (in case it is enabled), in order to overwhelm an exhausted router.
3. Tamper the Intermediate System Neighbours TLV
   a. Remove neighbours in order to affect the SPF algorithm or moreover affect the connectivity of the graph
   b. Changing metrics in order to affect the SPF algorithm.
   c. Modify the topology of the network, by introducing phantom routers.
4. Tamper with the Area addresses TLV in order to affect the SPF algorithm (by disconnecting routers from the area)
5. Tamper with the IS TYPE bits in order to affect the SPF algorithm.

3.9 Compromised Router becomes a DIS ([9])

A router can cause itself to become a DIS by choosing the highest priority in the IIH PDU. For a tie-break the compromised router can change its MAC to one above the LAN’s maximum.

3.10 Min Lifetime (MaxAge [12])

In this internal attack, the compromised router receives an LSP, and changes its lifetime to 0, and re-floods it into the system, so other routers will purge it. This attack triggers the fight-back mechanism.

3.11 Various Resource consumption attacks ([10])

3.11.1 DIS Election

An attack can force a DIS election process which consumes various resources, by sending a IIH PDU from a phantom router, which highest priority. The re-election process has an area-wide effect since the resigning router would send a purge LSP.
3.11.2 LSP Databases Inflation

Attackers can inflate LSP databases across the network by sending bogus LSPs from phantom routers, which would then be part of the SPF algorithm.

3.11.3 Abusing Partial Sequence Numbers PDUs (PSNPs)

A malicious system may flood the LAN with PSNP PDUs which specify missing LSPs, in order to cause the DIS to respond with the missing info. Similarly, a malicious system may flood the LAN with spoofed CSNP PDUs, in order to cause the relevant system to respond with the missing information.


This attack allows to inject a malicious LSP into the domain, with no fight-back. The attacker uses a sequence number of SequenceModules (the highest sequence number). As explained by

3.13 Disguised LSPs (Disguised LSAs [8])

According to [3], section 7.3.16.1, if a router receives a Link State Update PDU, with an LSP that it is its source, with a sequence number greater than the one it is aware of, it would generate a new LSP, with a greater sequence number. This is similar to OSPF “Fight-back” mechanism.

A Link State PDU carries a 16-bit Fletcher checksum, which is computed over all fields of the LSP, after the Remaining Lifetime field. Since the checksum size is small, given a message \( A \) with checksum \( C(A) \) we can find another message \( B \) s.t. \( C(B) = C(A) \).

The attacker works as follows:

1. Let \( L_1 \) be some LSP, originated by the attacked router, and Sequence Number \( S_1 \)

2. The attacker sends to the attacked router, an LSP, \( L_1^* \), with Sequence Number \( S_1^* > S_1 \). According to the Fight-back mechanism, the attacked router will issue a new LSP, \( L_2 \), with Sequence Number \( S_2 > S_1^* \).

3. Since everything is predictable, the attacker knows the checksum value of \( L_2 \) and can race this LSP, with \( L_2^* \), having the same checksum, but different (malicious) data.

4. A system that receives \( L_2^* \) before \( L_2 \) will not react to the latter, according to section 7.3.16.2 of [3]

3.14 Remote False Adjacency ([8])

This attack assumes [4.2] is possible as otherwise the attacker cannot reach remote networks. The LAN IH PDU may contain a large holding time value, and must contain the target’s MAC address (LAN address) in its Intermediate System Neighbours TLV. Sending this PDU twice will cause the adjacency to be in the ‘Up’ state. Notice that there will be two adjacencies with the same LAN address, however, [3] section 8.4.1.4 defines the adjacency as the triplet (LANAddress, neighborSystemID, adjacencyType).

After the adjacency has been set to the ‘Up’ state, the attacker can introduce Link-State updates into the domain, by sending them to the attacked router, using [4.2].
4 New attacks on IS-IS

4.1 Avoiding Fight-back by Sending Unicast Link-State Updates

We assume the attacker controls a malicious router. Recall that IS-IS runs on top of Layer 2. The attacker can issue unicast Link-State updates to specific LAN nodes to prevent it from reaching the victim. According to [3], section 7.3.15.3, A receiving router will not set the SRM flag on the arriving circuit, hence by sending unicast PDUs the attacker has some control over the flooding process.

For example, consider the following topology:

![Topology Diagram]

*Attacker* sends the PDU on behalf of *Victim*, by issuing two unicast updates to $R_1$ and $R_2$. It will never reach *Victim*, since both $R_1$ and $R_2$ would not flood back into $LAN_1$.

4.2 Attacking Remote Routers via Virtual Links

It is a common belief that since IS-IS runs on top of Layer-2, a remote attacker cannot reach routers on external networks. We show that this is not the case in CLNP domains.

In the CLNP world, IS-IS overcomes partitioned areas by exploiting the fact that the $L_2$ domain is contiguous. When a partitioned area is detected, two $L_2$ routers of the same area of different parts are used in order to tunnel information. This is done by encapsulating IS-IS inside the NPDU.

According to Section 7.4.4 of [3], if an NPDU is received and addressed to the underlying system, with the “Intra-Domain routeing” SELECTOR, it is first decapsulated and then passed to the Update process as in the normal behavior. It is unsafe since each IS-IS supports this behavior by default and there is construction stage for such tunnels (they are stateless). Hence an unauthenticated system may send encapsulated IS-IS PDUs in order to reach remote networks. This may aid in conducting further attacks from remote.

4.3 DIS Disconnection: One LAN, No DIS

This attack exploits the DIS election mechanism. The attacker sends a unicast Hello to the DIS system, with a higher priority. This will cause the DIS to resign, issuing a purge LSP. However, other routers would still think it has the highest priority (since they haven’t seen the unicast IIHL), thus a new DIS would not be elected. This breaks the connectivity of the LAN. In contrast to OSPF, IS-IS supports asymmetric holding times, which makes the attack near persistent.
4.4 Downgrading DIS LANs to become Fully Meshed Networks: One LAN, Multiple DISs

We show a mechanism for elevating all routers within a LAN to concurrently become a DIS. We assume the LAN has a local attacker. The local attacker sends spoofed unicast Hello messages, originating from the DIS to the other systems, with a minimal priority. In the perspective of the attacked router, it still indeed has the highest priority, thus it would not resign as a DIS (by purging its pseudonode). However, in the perspective of other LAN routers, it has the lowest priority, thus the router with the next maximal priority is elected to become the new DIS.

We can repeat this process for each router, until every router in the LAN assumes it is the DIS itself.

5 Proof of concept

We implemented a PoC for attacks [5.2], [5.3], [5.4], and tested the results under the GNS3 environment.

5.1 Attacking remote routers via Virtual links

5.1.1 Topology

Available systems

<table>
<thead>
<tr>
<th>Name</th>
<th>IP addresses</th>
<th>NSAP</th>
<th>Area</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_1$</td>
<td>10.0.1.1</td>
<td>00.0001.0000.0000.0001.00</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$R_2$</td>
<td>10.0.1.2/10.1.0.2</td>
<td>00.0001.0000.0000.0002.00</td>
<td>1</td>
<td>1-2</td>
</tr>
<tr>
<td>$R_3$</td>
<td>10.0.2.3/10.1.0.3</td>
<td>00.0002.0000.0000.0003.00</td>
<td>2</td>
<td>1-2</td>
</tr>
<tr>
<td>$R_4$</td>
<td>10.0.2.4</td>
<td>00.0002.0000.0000.0004.00</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

**IOS versions** 15.1 and 12.4, with CLNP support.

Links
5.1.2 Attack scenario

The attacker is $R_1$, and the victim is $R_4$. First we create the following payload $LSP_{ID}$, which is a Link-State Update with LSP-ID $ID$, with SequenceNumber of value $SequenceModulus$

We encapsulate $LSP_{R_3}$ on a CLNS PDU with target $R_4$. When it arrives on $R_4$, its LSPDB should be updated for $ID = R_3$

5.1.3 Results

Cisco IOS has no virtual links support. We hoped that it decapsulates CLNP NPDUs either way but unfortunately that is not the case.

5.2 DIS Disconnection: One LAN, No DIS

5.2.1 Topology

Available systems

<table>
<thead>
<tr>
<th>Name</th>
<th>IP addresses</th>
<th>NSAP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_1$</td>
<td>10.0.1.1</td>
<td>00.0001.0000.0000.0001.00</td>
<td>10</td>
</tr>
<tr>
<td>$R_2$</td>
<td>10.0.1.2DISs</td>
<td>00.0001.0000.0000.0002.00</td>
<td>20</td>
</tr>
<tr>
<td>$R_3$</td>
<td>10.0.1.3</td>
<td>00.0001.0000.0000.0003.00</td>
<td>30</td>
</tr>
<tr>
<td>$R_4$</td>
<td>10.0.1.4</td>
<td>00.0001.0000.0000.0004.00</td>
<td>40</td>
</tr>
</tbody>
</table>

IOS versions 15.1

Links

![Diagram showing network topology]
5.2.2 Attack scenario

As of the topology, the DIS would be $R_4$. We assume the attacker can inject packets to the network, as a phantom system named 'Attacker'.

1. We inject a unicast Hello packet with maximal holding-time (65535) to $R_4$ from Attacker with priority 50. This puts Attacker in the INIT state in $R_4$.

2. We inject a unicast Hello packet with maximal holding-time (65535) to $R_4$ from Attacker with priority 50. This puts Attacker in the UP state in $R_4$, causing $R_4$ to resign as DIS and generate a purge LSP.

5.2.3 Results

The attack works. Interestingly, when $R_4$ resigns, it issues an Hello, claiming Attacker is the DIS. Every router on the LAN honors this DIS, even though there is no adjacency.

Sample output after a successful attack:

```
R1#show isis database verbose
IS-IS Level-1 Link State Database:
LSPID   LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
R1.00-00  * 0x00000004 0x9344 873 0/0/0
Area Address: 00.0001
NLPID: 0xCC
Hostname: R1
IP Address: 10.0.1.1
Metric: 10 IP 10.0.1.0 255.255.255.0
R4.00-00 0x000004 0x1227 871 0/0/0
Area Address: 00.0001
NLPID: 0xCC
Hostname: R2
IP Address: 10.0.1.2
Metric: 10 IP 10.0.1.0 255.255.255.0
R3.00-00 0x00000003 0x9009 871 0/0/0
Area Address: 00.0001
NLPID: 0xCC
Hostname: R3
IP Address: 10.0.1.3
Metric: 10 IP 10.0.1.0 255.255.255.0
R4.00-00 0x00000003 0x2922 871 0/0/0
Area Address: 00.0001
NLPID: 0xCC
Hostname: R4
IP Address: 10.0.1.4
Metric: 10 IS 6666.6666.6666.01
R4.01-00 0x00000002 0x0122 0 (873) 0/0/0
R4
```

Another indication that the attack is successful is that every router claims Attacker to be the DIS, in their periodic Hello messages (Designated IS field).

5.3 Downgrading DIS LANs to become Fully Meshed Networks: One LAN, Multiple DISs

5.3.1 Topology

Available systems
<table>
<thead>
<tr>
<th>Name</th>
<th>IP addresses</th>
<th>NSAP</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_1$</td>
<td>10.0.1.1</td>
<td>00.0001.0000.0000.0001.00</td>
<td>10</td>
</tr>
<tr>
<td>$R_2$</td>
<td>10.0.1.2</td>
<td>00.0001.0000.0000.0002.00</td>
<td>20</td>
</tr>
<tr>
<td>$R_3$</td>
<td>10.0.1.3</td>
<td>00.0001.0000.0000.0003.00</td>
<td>30</td>
</tr>
<tr>
<td>$R_4$</td>
<td>10.0.1.4</td>
<td>00.0001.0000.0000.0004.00</td>
<td>40</td>
</tr>
</tbody>
</table>

**IOS versions** 15.1

**Links**

![Diagram](image)

### 5.3.2 Attack scenario

As of the topology, the DIS would be $R_4$.

1. We inject multiple unicast *Hello* packets to $R_1, R_2, R_3$ from $R_4$ with priority 1.
2. Sleep 5 seconds.
3. We inject multiple unicast *Hello* packets to $R_1, R_2$ from $R_3$ with priority 1.
4. Sleep 5 seconds.
5. We inject a unicast *Hello* packet to $R_1$ from $R_2$ with priority 1.

### 5.3.3 Results

The attack works. We should denote that if a DIS resigns by issuing an *Hello PDU* with a lower priority, only the next DIS elects itself as a DIS, and automatically issues an *Hello packet*, which causes other systems to also elect it as a DIS. In addition, Cisco has a very short default hold-time value, which makes the attack...
very limited. Interestingly, when a new DIS is elected, a purge LSP is issued by the new DIS, however, the original DIS (which hasn’t actually resigned), fights back, so this behavior has no effect.

Sample output after a successful attack:

R1#show isis database verbose
IS-IS Level-1 Link State Database:

<table>
<thead>
<tr>
<th>LSPID</th>
<th>LSP Seq Num</th>
<th>LSP Checksum</th>
<th>LSP Holdtime</th>
<th>ATT/P/OL</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1.00-00</td>
<td>* 0x00000035</td>
<td>0x0736</td>
<td>1192</td>
<td>0/0/0</td>
</tr>
</tbody>
</table>

   Area Address: 00.0001
   NLPID: 0xCC
   Hostname: R1
   IP Address: 10.0.1.1
   Metric: 10  IP 10.0.1.0 255.255.255.0
   Metric: 10  IS R1.01
   Metric: 0  IS R1.00
   Metric: 0  IS R2.00
   Metric: 0  IS R3.00
   Metric: 0  IS R4.00

R2.00-00 0x00000031 0x929A 1180 0/0/0

   Area Address: 00.0001
   NLPID: 0xCC
   Hostname: R2
   IP Address: 10.0.1.2
   Metric: 10  IP 10.0.1.0 255.255.255.0
   Metric: 10  IS R2.01
   Metric: 0  IS R2.00
   Metric: 0  IS R1.00
   Metric: 0  IS R3.00
   Metric: 0  IS R4.00

R3.00-00 0x0000008B 0x7E91 1170 0/0/0

   Area Address: 00.0001
   NLPID: 0xCC
   Hostname: R3
   IP Address: 10.0.1.3
   Metric: 10  IP 10.0.1.0 255.255.255.0
   Metric: 10  IS R3.01
   Metric: 0  IS R3.00
   Metric: 0  IS R1.00
   Metric: 0  IS R2.00
   Metric: 0  IS R4.00

R4.00-00 0x00000019 0x8EE2 852 0/0/0

   Area Address: 00.0001
   NLPID: 0xCC
   Hostname: R4
   IP Address: 10.0.1.4
   Metric: 10  IP 10.0.1.0 255.255.255.0
   Metric: 10  IS R4.01
   Metric: 0  IS R4.00
   Metric: 0  IS R1.00
   Metric: 0  IS R2.00
   Metric: 0  IS R3.00

Other indications that the attack is successful are:

1. Each system generates pseudonode LSP
2. Each system generates periodic CSNP PDUs
3. Each system specifies itself as the DIS in the Hello message.
References


