ISIS Tutorial

Philip Smith <pfs@cisco.com>

MENOG 4

5th-9th April 2009

Bahrain

Presentation Slides

- Will be available on

  ftp://ftp-eng.cisco.com

  /pfs/seminars/MENOG4-ISIS-Tutorial.pdf

  And on the MENOG website

- Feel free to ask questions any time

Agenda

- Comparing ISIS and OSPF
- Introduction to ISIS
- ISIS Best Practices

Comparing ISIS and OSPF

Both Link State Protocols use the Dijkstra SPF Algorithm

So what's the difference then??

What Is IS-IS ?

- Intermediate System to Intermediate System
- An “IS” is ISO terminology for a router
- IS-IS was originally designed for use as a dynamic routing protocol for ISO CLNP, defined in the ISO 10589 standard
- Later adapted to carry IP prefixes in addition to CLNP (known as Integrated or Dual IS-IS) as described in RFC 1195
- Predominantly used in ISP environment

IS-IS Timeline

- 1978ish “New” Arpanet Algorithm
  - Eric Rosen et al
- 1986 to 90 Decnet Phase V
  - Radia Perlman, Mike Shand
- 1987 ISO 10589 (IS-IS)
  - Dave Oran
- 1990 RFC 1195 (Integrated IS-IS)
  - Ross Callon, Chris Gunner
- 1990 to present: All sorts of enhancements
  - Everyone contributed!
- 2008 RFC5308 adds IPv6 support
  - And RFC5120 adds Multi-Topology Routing support

What Is OSPF ?

- Open Shortest Path First
- Link State Protocol using the Shortest Path First algorithm (Dijkstra) to calculate loop-free routes
- Used purely within the TCP/IP environment
- Designed to respond quickly to topology changes but using minimal protocol traffic
- Used in both Enterprise and ISP Environment

OSPF Timeline

- Development began in 1987 by IETF
- OSPFv1 published in 1989 with RFC 1131
- OSPFv2 published in 1991 with RFC 1247
- Further enhancements to OSPFv2 in 1994 with RFC 1583 and in 1997 with RFC 2178
- Last revision was in 1998 with RFC 2328 to fix minor problems
- All above OSPF RFCs authored by John Moy
- RFC2740 introduced OSPFv3 (for IPv6) in 1999, replaced by RFC5340 in 2008

IS-IS & OSPF: Similarities

- Both are Interior Gateway Protocols (IGP)

  They distribute routing information between routers belonging to a single Autonomous System (AS)

- With support for:

  Classless Inter-Domain Routing (CIDR)

  Variable Subnet Length Masking (VLSM)

  Authentication

  Multi-path

  IP unnumbered links

IS-IS and OSPF Terminology

OSPF	ISIS
Host	End System (ES)
Router	Intermediate System (IS)
Link	Circuit
Packet	Protocol Data Unit (PDU)
Designated router (DR)	Designated IS (DIS)
Backup DR (BDR)	N/A (no BDIS is used)
Link-State Advertisement (LSA)	Link-State PDU (LSP)
Hello packet	IIH PDU
Database Description (DBD)	Complete sequence number PDU (CSNP)

IS-IS and OSPF Terminology (Cont.)

OSPF

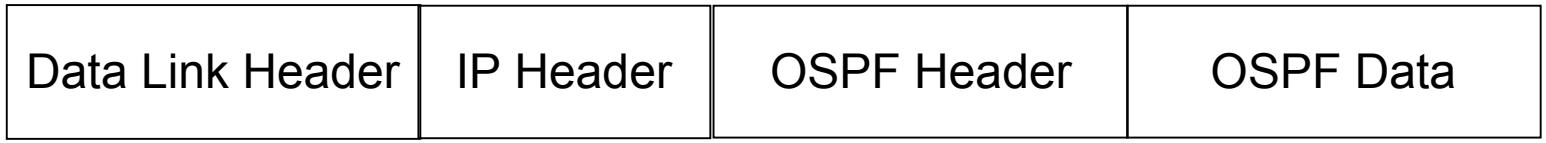
- Area
- Non-backbone area
- Backbone area
- Area Border Router (ABR)
- Autonomous System Boundary Router (ASBR)

ISIS

- Sub domain (area)
- Level-1 area
- Level-2 Sub domain (backbone)
- L1L2 router
- Any IS

Transport

- OSPF uses IP Protocol 89 as transport



- IS-IS is directly encapsulated in Layer 2

For Service Providers

- Which IGP should an ISP choose?
  - Both OSPF and ISIS use Dijkstra SPF algorithm
  - Exhibit same convergence properties
  - ISIS less widely implemented on router platforms
  - ISIS runs on data link layer, OSPF runs on IP layer
  - Biggest ISPs tend to use ISIS
  - Main ISIS implementations more tuneable than equivalent OSPF implementations

How to choose an IGP?

- OSPF

  Rigid area design - all networks must have area 0 core, with sub-areas distributed around

  Suits ISPs with central high speed core network linking regional PoPs

  Teaches good routing protocol design practices

- ISIS

  Relaxed two level design - L2 routers must be linked through the backbone

  Suits ISPs with “stringy” networks, diverse infrastructure, etc, not fitting central core model of OSPF

  More flexible than OSPF, but easier to make mistakes too

Other considerations

- ISIS runs on link layer
  - Not possible to “attack” the IGP using IP as with OSPF
- ISIS’s NSAP addressing scheme avoids dependencies on IP as with OSPF
- Because biggest ISPs use ISIS, it tends to get new optimisation features before OSPF does

Introduction to ISIS

IS-IS Standards History

- ISO 10589 specifies OSI IS-IS routing protocol for CLNS traffic
  - Tag/Length/Value (TLV) options to enhance the protocol
  - A Link State protocol with a 2 level hierarchical architecture.
- RFC 1195 added IP support
  - I/IS-IS runs on top of the Data Link Layer
  - Requires CLNP to be configured
- RFC5308 adds IPv6 address family support to IS-IS
- RFC5120 defines Multi-Topology concept for IS-IS
  - Permits IPv4 and IPv6 topologies which are not identical

ISIS Levels

- ISIS has a 2 layer hierarchy
  - Level-2 (the backbone)
  - Level-1 (the areas)
- A router can be
  - Level-1 (L1) router
  - Level-2 (L2) router
  - Level-1-2 (L1L2) router

ISIS Levels

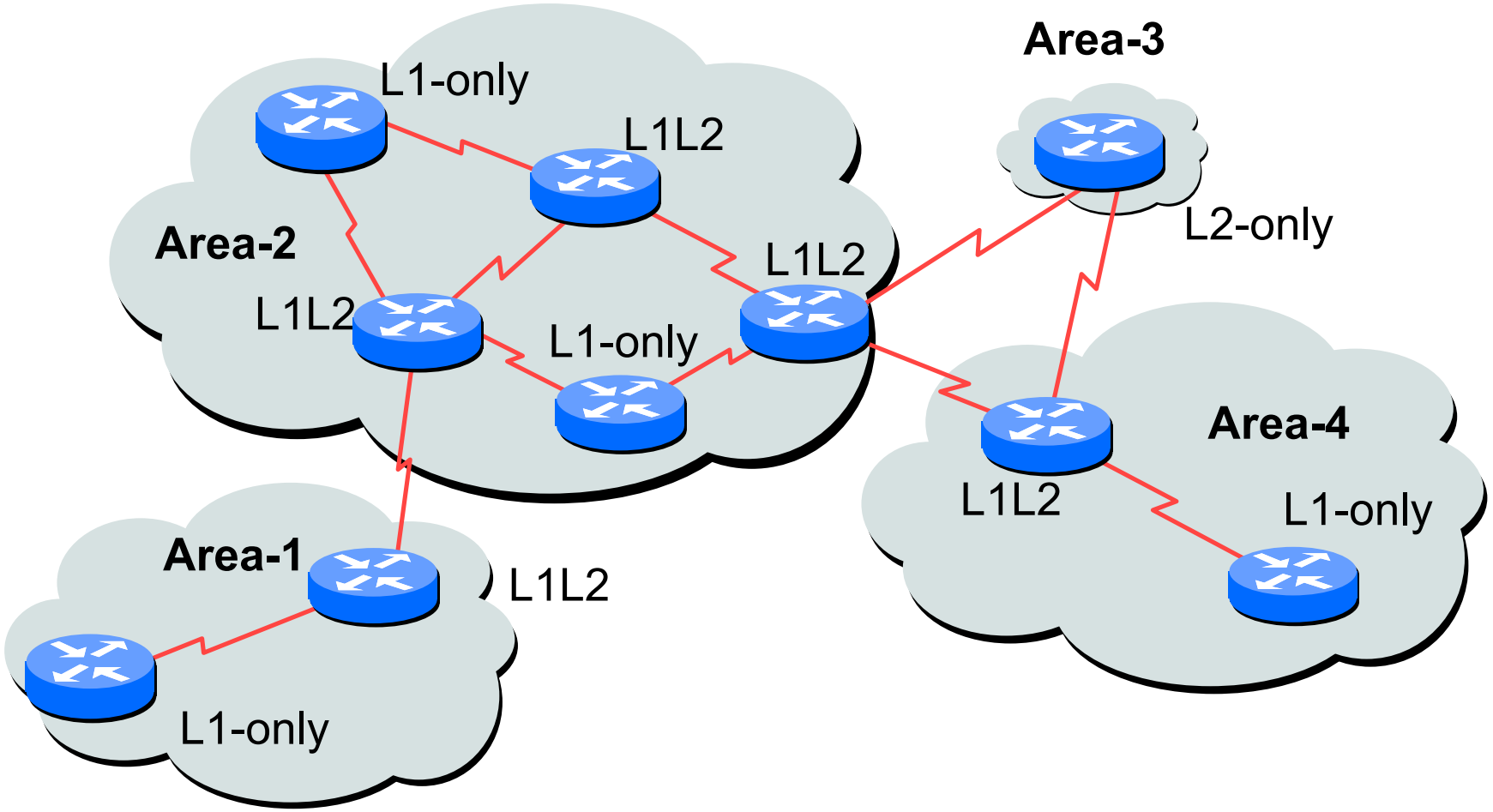
- Level-1 router
  - Has neighbours only on the same area
  - Has a level-1 LSDB with all routing information for the area
- Level-2 router
  - May have neighbours in the same or other areas
  - Has a Level-2 LSDB with all routing information about inter-area
- Level-1-2 router
  - May have neighbours on any area.
  - Has two separate LSDBs: level-1 LSDB & level-2 LSDB

Backbone & Areas

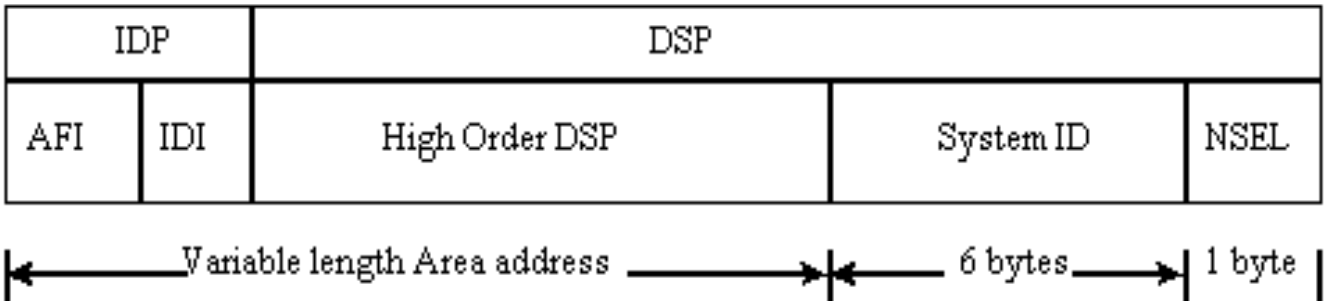
- ISIS does not have a backbone area as such (like OSPF)
- Instead the backbone is the contiguous collection of Level-2 capable routers
- ISIS area borders are on links, not routers
- Each router is identified with Network Entity Title (NET)

  NET is an NSAP where the n-selector is 0

L1, L2, and L1L2 Routers

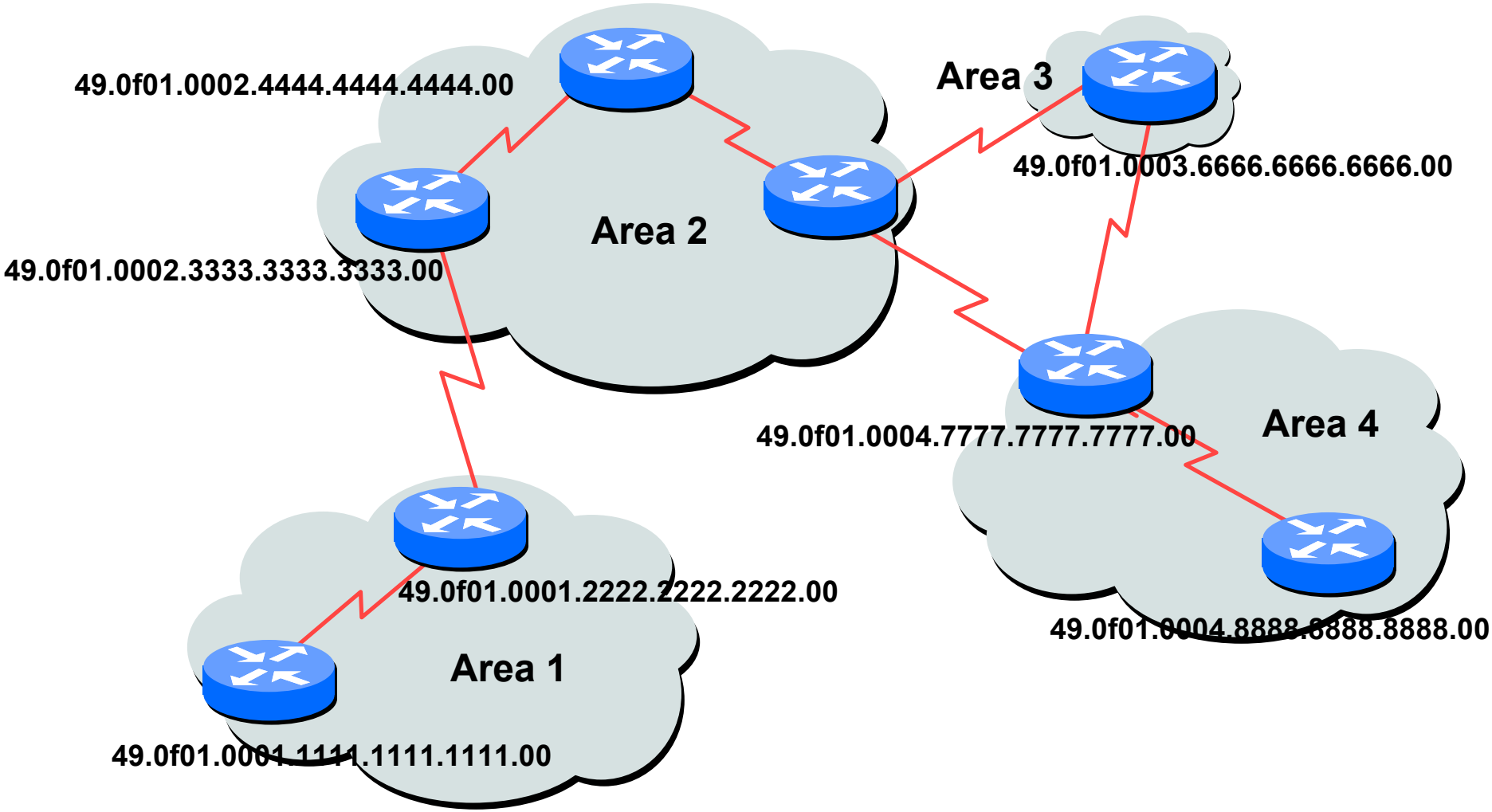


NSAP and Addressing



- NSAP: Network Service Access Point
  - Total length between 8 and 20 bytes
  - Area Address: variable length field (up to 13 bytes)
  - System ID: defines an ES or IS in an area.
  - NSEL: N-selector. identifies a network service user (transport entity or the IS network entity itself)
- NET: the address of the network entity itself

An Addressing Example

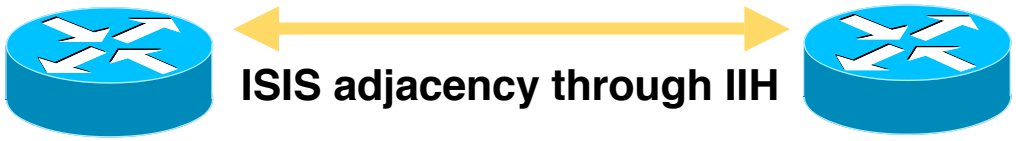


Addressing Common Practices

- ISPs typically choose NSAP addresses thus:
  - First 8 bits – pick a number (usually 49)
  - Next 16 bits – area
  - Next 48 bits – router loopback address
  - Final 8 bits – zero
- Example:
  - NSAP: 49.0001.1921.6800.1001.00
  - Router: 192.168.1.1 (loopback) in Area 1

Adjacencies

- Hello PDU IIHs are exchanged between routers to form adjacencies



- Area addresses are exchanged in IIH PDUs

Link State PDU (LSP)

- Each router creates an LSP and flood it to neighbours
- A level-1 router will create level-1 LSP(s)
- A level-2 router will create level-2 LSP(s)
- A level-1-2 router will create

  level-1 LSP(s) and

  level-2 LSP(s)

LSP Header

- LSPs have
  - Fixed header
  - TLV coded contents
- The LSP header contains
  - LSP-id
  - Sequence number
  - Remaining Lifetime
  - Checksum
  - Type of LSP (level-1, level-2)
  - Attached bit
  - Overload bit

LSP Contents

- The LSP contents are coded as TLV (Type, Length, Value)
  - Area addresses
  - IS neighbors
  - Authentication Info

LSDB content

- Each router maintains a separate LSDB for level-1 and level-2 LSPs
- LSP headers and contents
- SRM bits: set per interface when router has to flood this LSP
- SSN bits: set per interface when router has to send a PSNP for this LSP

Flooding of LSPs

- New LSPs are flooded to all neighbors
- It is necessary that all routers get all LSPs
- Each LSP has a sequence number
- 2 kinds of flooding
  - Flooding on a p2p link
  - Flooding on LAN

Flooding on a p2p link

- Once the adjacency is established both routers send CSNP packet
- Missing LSPs are sent by both routers if not present in the received CSNP
- Missing LSPs may be requested through PSNP

Flooding on a LAN

- There's a Designated Router (DIS)
- DIS election is based on priority
  - Best practice is to select two routers and give them higher priority – then in case of failure one provides deterministic backup to the other
- Tie break is by the highest MAC address
- DIS has two tasks
  - Conducting the flooding over the LAN
  - Creating and updating a special LSP describing the LAN topology (Pseudonode LSP)
- Pseudonode represents LAN (created by the DIS)

Flooding on a LAN

- DIS conducts the flooding over the LAN
- DIS multicasts CSNP every 10 seconds
- All routers in the LAN check the CSNP against their own LSDB (and may ask specific re-transmissions with PSNPs)

Complete Sequence Number PDU

- Describes all LSPs in your LSDB (in range)
- If LSDB is large, multiple CSNPs are sent
- Used at 2 occasions

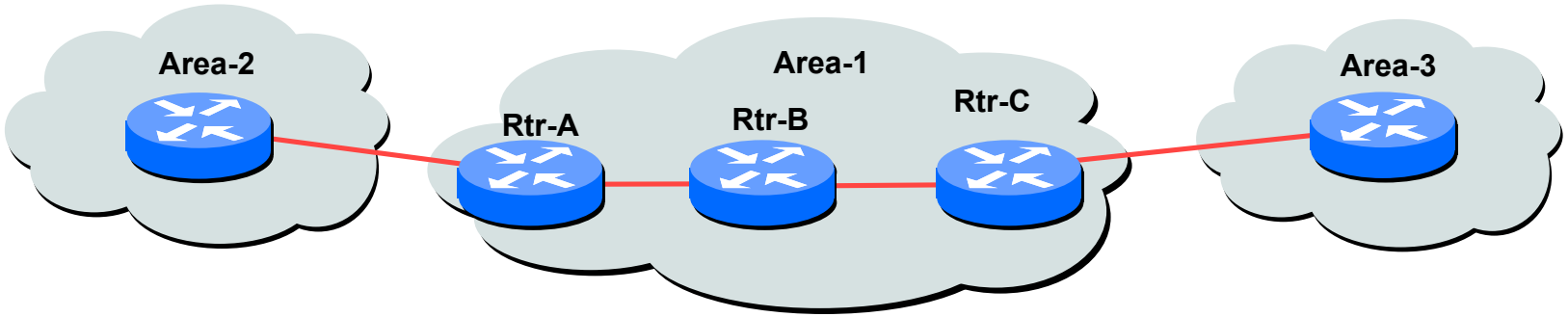
  Periodic multicast by DIS (every 10 seconds) to synchronise LSDB over LAN subnets

  On p2p links when link comes up

Partial Sequence Number PDUs

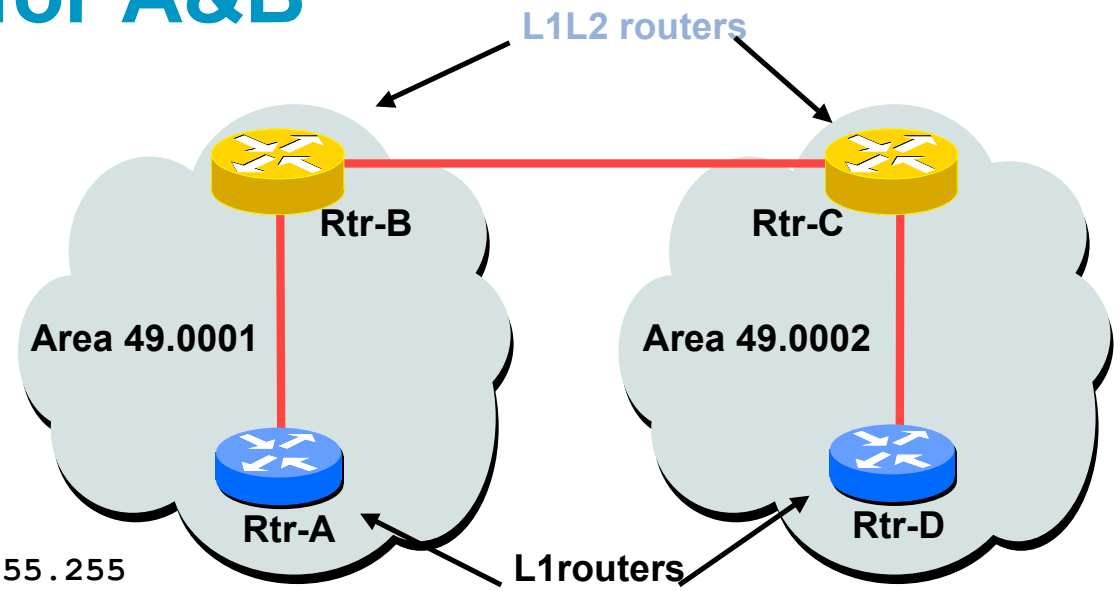
- PSNPs Exchanged on p2p links (ACKs)
- Two functions
  - Acknowledge receipt of an LSP
  - Request transmission of latest LSP
- PSNPs describe LSPs by its header
  - LSP identifier
  - Sequence number
  - Remaining lifetime
  - LSP checksum

Configuration



- L1, L2, L1-L2
  - **By default cisco routers will be L1L2 routers**
  - Routers can be manually configured to behave as
    - Level-1 only, Level-2 only, Level-1-2
    - This is what most ISPs do
  - Configuration can be done per interface or at the router level

Configuration for A&B



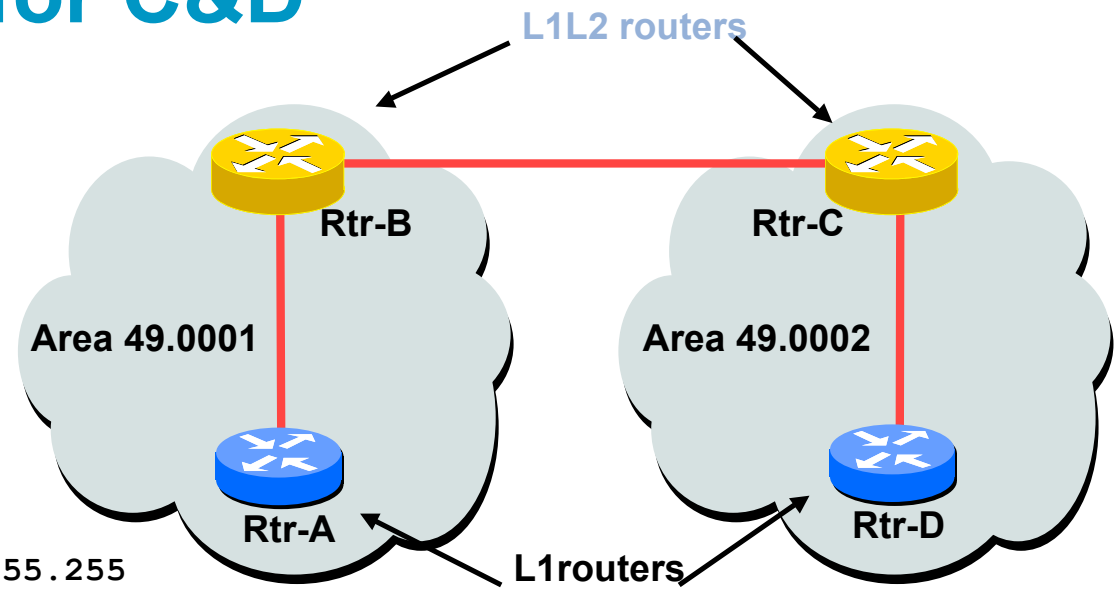
Router-B

```
interface Loopback0
 ip address 192.168.1.1 255.255.255.255
!
Interface Pos2/0/0
 ip address 192.168.222.1 255.255.255.0
 ip router isis
 isis circuit-type level-2
!
FastEthernet4/0/0
 ip address 192.168.120.10 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 passive-interface Loopback0
 net 49.0001.1921.6800.1001.00
```

Router-A

```
interface Loopback0
 ip address 192.168.1.5 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.120.5 255.255.255.0
 ip router isis
!
router isis
 is-type level-1
 passive-interface Loopback0
 net 49.0001.1921.6800.1005.00
```

Configuration for C&D



Router-C

```
interface Loopback0
 ip address 192.168.2.2 255.255.255.255
!
Interface Pos1/0/0
 ip address 192.168.222.2 255.255.255.0
 ip router isis
 isis circuit-type level-2
!
interface Fddi3/0
 ip address 192.168.111.2 255.255.255.0
 ip router isis
 isis circuit-type level-1
!
router isis
 passive-interface Loopback0
 net 49.0002.1921.6800.2002.00
```

Router-D

```
interface Loopback0
 ip address 192.168.2.4 255.255.255.255
!
interface Fddi6/0
 ip address 192.168.111.4 255.255.255.0
 ip router isis
!
router isis
 is-type level-1
 passive-interface Loopback0
 net 49.0002.1921.6800.2004.00
```

Adding interfaces to ISIS

- To activate ISIS on an interface:

```
interface HSSI 4/0
 ip route isis isp-bb
 isis circuit-type level-2
```

- To disable ISIS on an interface:

```
router isis isp-bb
 passive-interface GigabitEthernet 0/0
```

  Disables CLNS on that interface

  Puts the interface subnet address into the LSDB

- No ISIS configuration on an interface

  No CLNS run on interface, no interface subnet in the LSDB

Adding interfaces to ISIS

- Scaling ISIS: **`passive-interface default`**

  Disables ISIS processing on all interfaces apart from those marked as no-passive

  Places all IP addresses of all connected interfaces into ISIS

  Must be at least one non-passive interface:

```
router isis isp-bb
 passive-interface default
 no passive-interface GigabitEthernet 0/0
interface GigabitEthernet 0/0
 ip router isis isp-bb
 isis metric 1 level-2
```

Status Commands in ISIS

- Show clns

  Shows the global CLNS status as seen on the router, e.g.

```
Rtr-B>show clns
Global CLNS Information:
  2 Interfaces Enabled for CLNS
  NET: 49.0001.1921.6800.1001.00
  Configuration Timer: 60, Default Holding Timer: 300, Packet
  Lifetime 64
  ERPDU's requested on locally generated packets
  Intermediate system operation enabled (forwarding allowed)
  IS-IS level-1-2 Router:
    Routing for Area: 49.0001
```

Status Commands in ISIS

- Show clns neighbors

  Shows the neighbour adjacencies as seen by the router:

```
Rtr-B> show clns neighbors
System Id       SNPA          Interface State Holdtime Type Protocol
1921.6800.2002 *PPP*            PO2/0/0    Up        29   L2    IS-IS
1921.6800.1005 00e0.1492.2c00 Fa4/0/0    Up         9   L1    IS-IS
```

  More recent IOSes replace system ID with router hostname – ease of troubleshooting

Status Commands in ISIS

- Show clns interface

  Shows the CLNS status on a router interface:

```
Rtr-B>  show clns interface POS2/0/0
POS2/0/0 is up, line protocol is up
  Checksums enabled, MTU 4470, Encapsulation PPP
  ERPDUs enabled, min. interval 10 msec.
  RDPDUs enabled, min. interval 100 msec., Addr Mask enabled
 Congestion Experienced bit set at 4 packets
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 47 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x100
    Level-1 Metric: 10, Priority: 64, Circuit ID: 1921.6800.2002.00
    Number of active level-1 adjacencies: 0
    Level-2 Metric: 10, Priority: 64, Circuit ID: 1921.6800.1001.00
    Number of active level-2 adjacencies: 1
    Next IS-IS Hello in 2 seconds
```

Status Commands in ISIS

- Show CLNS protocol

  Displays the status of the CLNS protocol on the router:

```
Rtr-B> show clns protocol
IS-IS Router: <Null Tag>
  System Id: 1921.6800.1001.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        FastEthernet4/0/0 - IP
        POS2/0/0 - IP
  Redistributing:
    static
  Distance: 110
```

Other status commands

- “show clns traffic”

  Shows CLNS traffic statistics and activity for the network

- “show isis database”

  Shows the ISIS link state database

  i.e. the “routing table”

Network Design Issues

- As in all IP network designs, the key issue is the addressing lay-out
- ISIS supports a large number of routers in a single area
- When using areas, use summary-addresses
- >400 routers in the backbone is quite doable

Network Design Issues

- Possible link cost
  - Default on all interfaces is 10
  - (Compare with OSPF which sets cost according to link bandwidth)
  - Manually configured according to routing strategy
- Summary address cost
  - Equal to the best more specific cost
  - Plus cost to reach neighbor of best specific
- Backbone has to be contiguous
  - Ensure continuity by redundancy
- Area partitioning
  - Design so that backbone can NOT be partitioned

Scaling Issues

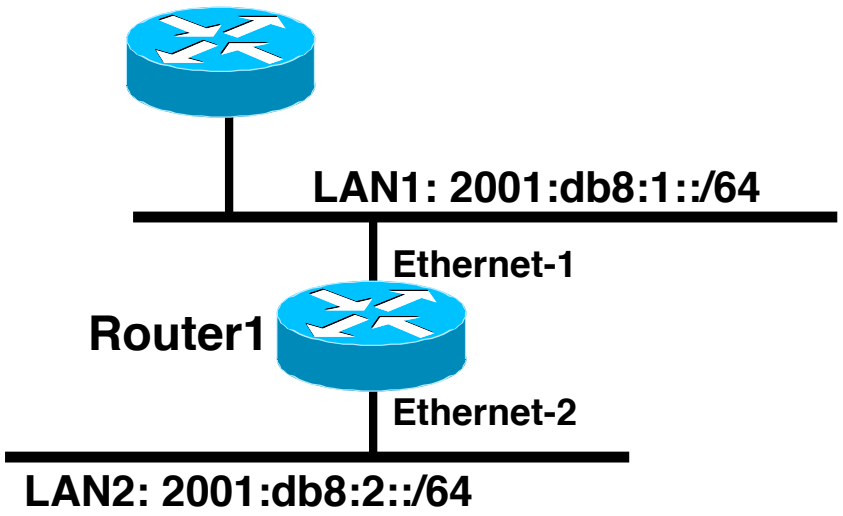
- Areas vs. single area
  - Use areas where
    - sub-optimal routing is not an issue
    - areas with one single exit point
  - Start with L2-only everywhere is a good choice
  - Future implementation of level-1 areas will be easier
  - Backbone continuity is ensured from start

ISIS for IPv6

IS-IS for IPv6

- 2 Tag/Length/Values added to introduce IPv6 routing
- IPv6 Reachability TLV (0xEC)
  - External bit
  - Equivalent to IP Internal/External Reachability TLV's
- IPv6 Interface Address TLV (0xE8)
  - For Hello PDUs, must contain the Link-Local address
  - For LSP, must only contain the non-Link Local address
- IPv6 NLPID (0x8E) is advertised by IPv6 enabled routers

IOS IS-IS dual IP configuration



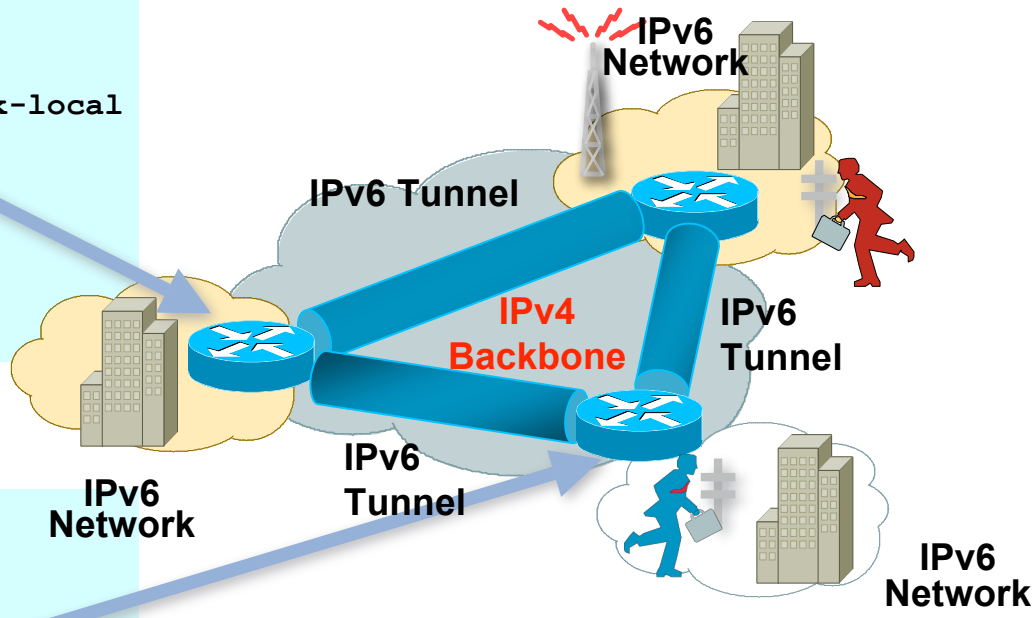
Dual IPv4/IPv6 configuration.
Redistributing both IPv6 static routes and IPv4 static routes.

```
Router1#
interface ethernet-1
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 2001:db8:1::1/64
 ip router isis
 ipv6 router isis

interface ethernet-2
 ip address 10.2.1.1 255.255.255.0
 ipv6 address 2001:db8:2::1/64
 ip router isis
 ipv6 router isis

router isis
 address-family ipv6
  redistribute static
  exit-address-family
 net 49.0001.0000.0000.072c.00
 redistribute static
```

IOS Configuration for IS-IS for IPv6 on IPv6 Tunnels over IPv4

```
On Router1:
interface Tunnel0
 no ip address
 ipv6 address 2001:db8:1::1/64
 ipv6 address FE80::10:7BC2:ACC9:10 link-local
 ipv6 router isis
 tunnel source 10.42.1.1
 tunnel destination 10.42.2.1
!
router isis
 net 49.0001.0000.0000.0001.00
```

```
On Router2:
interface Tunnel0
 no ip address
 ipv6 address 2001:db8:1::2/64
 ipv6 address FE80::10:7BC2:B280:11 link-local
 ipv6 router isis
 tunnel source 10.42.2.1
 tunnel destination 10.42.1.1
!
router isis
 net 49.0001.0000.0000.0002.00
```



IS-IS for IPv6 on an IPv6 Tunnel requires GRE Tunnel; it can't work with IPv6 configured tunnel as IS-IS runs directly over the data link layer

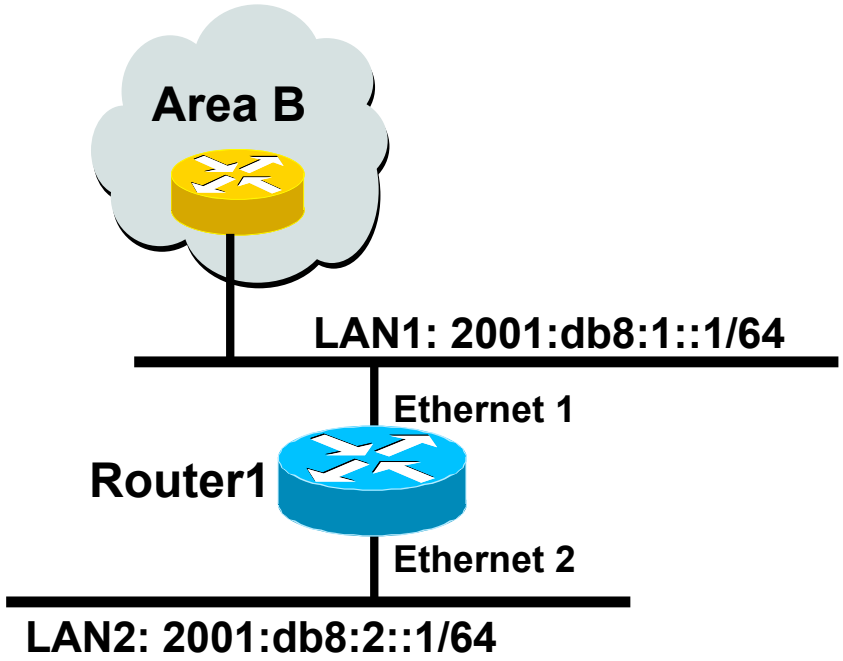
Multi-Topology IS-IS extensions

- IS-IS for IPv6 assumes that the IPv6 topology is the same as the IPv4 topology
  - Single SPF running, multiple address families
  - Some networks may be like this, but many others are not
- Multi-Topology IS-IS solves this problem
  - New TLV attributes introduced
  - New Multi-Topology ID #2 for IPv6 Routing Topology
  - Two topologies now maintained:
    - ISO/IPv4 Routing Topology (MT ID #0)
    - IPv6 Routing Topology (MT ID #2)

Multi-Topology IS-IS extensions

- New TLVs attributes for Multi-Topology extensions:
  - Multi-topology TLV: contains one or more multi-topology ID in which the router participates
  - MT Intermediate Systems TLV: this TLV appears as many times as the number of topologies a node supports
  - Multi-Topology Reachable IPv4 Prefixes TLV: this TLV appears as many times as the number of IPv4 announced by an IS for a given MT ID
  - Multi-Topology Reachable IPv6 Prefixes TLV: this TLV appears as many times as the number of IPv6 announced by an IS for a given MT ID

Multi-Topology ISIS configuration example (IOS)



- The optional keyword **`transition`** may be used for transitioning existing IS-IS IPv6 single SPF mode to MT IS-IS
- Wide metric is mandated for Multi-Topology to work

```
Router1#
interface Ethernet 1
 ip address 10.1.1.1 255.255.255.0
 ipv6 address 2001:db8:1::1/64
 ip router isis
 ipv6 router isis
 isis ipv6 metric 20

interface Ethernet 2
 ip address 10.2.1.1 255.255.255.0
 ipv6 address 2001:db8:2::1/64
 ip router isis
 ipv6 router isis
 isis ipv6 metric 20

router isis
 net 49.0001.0000.0000.072c.00
 metric-style wide
 !
 address-family ipv6
  multi-topology
 exit-address-family
```

Narrow to Wide Metrics Transition

- When migrating from narrow to wide metrics, care is required
  - Narrow and wide metrics are NOT compatible with each other
  - Migration is a two stage process, using the “transition” keyword
- Networks using narrow metrics should first configure across all routers:

```
router isis isp
 metric-style transition
```

- Once the whole network is changed to transition support, the metric style can be changed to wide:

```
router isis isp
 metric-style wide
```

ISP common practices

- NSAP address construction
  - Area and loopback address
- L2
  - L1-L2 and L1 used later for scaling
- Wide metrics
  - Narrow metrics are too limiting
- Deploying IPv6 in addition to IPv4
  - Multi-topology is recommended – gives increased flexibility should there be future differences in topology

ISP Best Practices

Extra detailed information

Purging the RIB on link failure

- For routing protocols that are capable of responding to link failures, IOS allows such routing protocols to quickly and more efficiently delete associated routes from the RIB when a link, and the interface is removed from the routing table
- Without this command, the "less efficient" RIB process is used to delete the associated next-hop routes of the failed interface, by default

  If this process has to work through a very large routing table, it can use up a number of CPU cycles and potentially increase convergence time.

```
ip routing protocol purge interface
```

ISIS neighbour authentication

- Create key chains to be used for HMAC-MD5 authentication for both Level-1 and Level-2

```
key chain isis-sec-l1
 key 1
   key-string xxxxx
key chain isis-sec-l2
 key 1
   key-string xxxxx
```

Setting up Loopback Interface

- Create the Loopback interface/Router-ID

  It will NOT have IS-IS running on it because it is not a transit interface

  Disabling IS-IS on it, while announcing the IP prefixes into IS-IS, allows the IS-IS domain to scale because LSP/Hello packets are not unnecessarily generated for the Loopback interface

  An IS-IS metric will NOT be set, which will default the Loopback interface's metric to zero (0).

```
interface loopback0
 ip address 192.168.0.1 255.255.255.255
 ipv6 address 2001:db8:192:168:0:1/128
```

Level-1 Interface Configuration

- Configure addresses and enable ISIS for IPv4 and IPv6

```
interface gigabitethernet0/1
 ip address 192.168.1.1 255.255.255.192
 ipv6 address 2001:db8:192:168:1:1/112
 !
 ip router isis 1
 ipv6 router isis 1
```

- Ensure this interfaces runs at Level-1

```
isis circuit-type level-1
```

Level-1 Interface: Metrics & Auth

- Set the costs for IPv4 and IPv6

```
interface gigabitethernet0/1
 isis metric 400 level-1
 isis ipv6 metric 400 level-1
```

- Enable HMAC-MD5 for level-1

```
isis authentication mode md5 level-1
```

- Associate the key-chain defined earlier

```
isis authentication key-chain isis-sec-l1 level-1
```

Level-1 Interface: DIS and BFD

- Set this IS to be the DIS in this Level-1 area

  A DIS of 126 (higher than the default of 64) configured on another IS in this area sets it up as the backup DIS

```
interface gigabitethernet0/1
 isis priority 127 level-1
```

- Enable BFD for fast failure detection

  BFD helps reduce the convergence times of IS-IS because link failures will be signalled much quicker

```
interface gigabitethernet0/1
 bfd interval 250 min_rx 250 multiplier 3
```

Level-2 interface

- This interface is used for a trunk link to another PoP forming part of your network-wide backbone

  As such it will be a Level-2 interface, making this router a Level-1/Level-2 IS.

  Metric and authentication are all configured for Level-2

```
interface gigabitethernet0/2
 ip address 192.168.2.1 255.255.255.252
 ipv6 address 2001:db8:192:168:2:1:/126
 ip router isis 1
 ipv6 router isis 1
 isis circuit-type level-2-only
 isis metric 400 level-2
 isis ipv6 metric 400 level-2
 isis authentication mode md5 level-2
 isis authentication key-chain isis-sec-l2 level-2
```

Level 2 interface: more details

- To make this IS-IS BCP more interesting, we will assume this trunk link is a broadcast multi-access link, i.e., Ethernet.
- As this is an Ethernet interface, IS-IS will attempt to elect a DIS when it forms an adjacency

  Because it is running as a point-to-point WAN link, with only 2 IS's on the wire, configuring IS-IS to operate in "point-to-point mode" scales the protocol by reducing the link failure detection times

  Point-to-point mode improves convergence times on Ethernet networks because it:

  - Prevents the election of a DIS on the wire,
  - Prevents the flooding process from using CSNP's for database synchronization
  - Simplifies the SPF computations and reduces the IS's memory footprint due to a smaller topology database.

```
int gi0/2
 isis network point-to-point
```

ISP Best Practices

- We now configure parameters specific to the IS-IS routing protocol

  This covers both IPv4 and IPv6, as IS-IS supports both IP protocols in the same implementation

  ```
  router isis 1
  ```

- Create an NET

  This is made up of a private AFI (49), an area part, a System ID (taken from the padded Loopback interface IP address) and an N-SEL of zero (0).

  ```
  net 49.0001.1921.6800.0001.00
  ```

- Enable HMAC-MD5 authentication

  ```
  authentication mode md5
  authentication key-chain isis-sec-l1 level-1
  authentication key-chain isis-sec-l2 level-2
  ```

ISP Best Practices

- Enable iSPF (incremental SPF).

  This, in the long run, reduces CPU demand because SPF calculations are run only on the affected changes in the SPT.

  As this is a Level-1/Level-2 router, enable iSPF at both levels 60 seconds after the command has been entered into the configuration.

  Note that IOS only supports iSPF for IPv4.

```
ispf level-1-2 60
```

- Enable wide/extended metric support for IS-IS.

  IOS, by default, supports narrow metrics, which means you can define cost values between 1-63. This is not scalable.

  To solve this problem, enable wide metrics, which allows you to define cost values between 1-16777214.

```
metric-style wide
```

ISP Best Practices

- Increase ISIS default metric
  - Default value is 10
  - All interfaces in both L1 and L2 have this value
  - Not useful if configured value is “accidentally” removed - a low priority interface could end up taking full load by mistake
  - Configure a “very large” value as default

```
metric 100000
```

- Disable IIH padding because on high speed links, it may strain huge buffers; and on low speed links, it may waste bandwidth and affect other time sensitive applications, e.g., voice.
  - Disabling IIH padding is safe because IOS will still pad the first 5 IIH's to the full MTU to aid in the discovery of MTU mismatches.

```
no hello padding
```

ISP Best Practices

- Allow the Loopback interface IP address to be carried within IS-IS, while preventing it from being considered in the flooding process.

```
passive-interface Loopback0
```

- Log changes in the state of the adjacencies.

```
log-adjacency-changes
```

- Tell the IS to ignore LSP's with an incorrect data-link checksum, rather than purge them

  Purging LSP's with a bad checksum causes the initiating IS to regenerate that LSP, which could overload the IS if perpetuated in a cycle

  So rather than purge them, ignore them.

```
ignore-lsp-errors
```

ISP Best Practices

- Reduce the amount of control traffic, conserving CPU usage for generation and refreshing of LSP's.

  Do this by increasing the LSP lifetime to its limits.

  ```
  max-lsp-lifetime 65535
  ```

- Reduce the frequency of periodic LSP flooding of the topology, which reduces link utilization

  This is safe because there other mechanisms to guard against persistence of corrupted LSP's in the LSDB.

  ```
  lsp-refresh-interval 65000
  ```

- Customize IS-IS throttling of SPF calculations.

  Good for when you also use BFD for IS-IS.

  These are recommended values for fast convergence.

  ```
  spf-interval 5 1 20
  ```

ISP Best Practices

- Customize IS-IS throttling of PRC calculations.

  PRC calculates routes without performing a full SFP calculation.

  This is done when a change is signaled by another IS, but without a corresponding change in the basic network topology, e.g., the need to reinstall a route in the IS-IS RIB.

  These are recommended values for fast convergence.

  ```
  prc-interval 5 1 20
  ```

- Customize IS-IS throttling of LSP generation.

  These are recommended values for fast convergence.

  ```
  lsp-gen-interval 5 1 20
  ```

ISP Best Practices

- Enable IS-IS fast-flooding of LSP's.

  This tells the IS to always flood the LSP that triggered an SPF before the router actually runs the SPF computation.

  This command used to be 'ip fast-convergence' and has since been replaced from IOS 12.3(7)T.

  Below, we shall tell the IS to flood the first 10 LSP's which invoke the SPF before the SPF computation is started

  ```
  fast-flood 10
  ```

- Enable IS-IS IETF Graceful Restart.

  This ensures an IS going through a control plane switchover continues to forward traffic as if nothing happened

  Software and platform support is limited, so check whether your particular platform/code supports this

  Also, deploy only if it's necessary.

  ```
  nsf ietf
  ```

ISP Best Practices

- Enable BFD support for IS-IS.

  With BFD running on the interface, a failure of the link would signal IS-IS immediately

  IS-IS will then converge accordingly.

  ```
  bfd all-interfaces
  ```

- Tell IS-IS to ignore the attached bit

  The Attached bit is set when an L1/L2 IS learns L1 routes from other L1 routers in the same area

  The Attached bit causes the installation of an IS-IS-learned default route in the IS-IS RIB on L1 routers in the same area, as well as in the forwarding table if IS-IS is the best routing protocol from which the default route was learned – this can lead to suboptimal routing.

  ```
  ignore-attached-bit
  ```

ISP Best Practices

- Wait until iBGP is running before providing transit path

  `set-overload-bit on-startup wait-for-bgp`

  Avoids blackholing traffic on router restart

  Causes ISIS to announce its prefixes with highest possible metric until iBGP is up and running

  When iBGP is running, ISIS metrics return to normal, make the path valid

- Enable the IPv6 address family for in IS-IS.

  `address-family ipv6`

- Enable multi-topology support for IPv6 in IS-IS.

  Multi-topology support allows the IPv4 topology to be independent of that of IPv6

  `multi-topology`

ISP Best Practices

- Things to consider on routers operating as Level-1-only IS's:

  IS-IS BCP techniques under the IS-IS routing process

  In addition to the interface, tell the IS-IS routing process to operate in a Level-1 area only

```
router isis 1
 is-type level-1
```

ISP Best Practices

- Things to consider on routers operating as Level-1 and Level-2 IS's:

  To prevent sub-optimal routing of traffic from L1 IS's in one area to L1 IS's in another area, configure and enable Route Leaking on L1/L2 routers that form the backbone connectivity between two or more different areas

  Route Leaking permits L1/L2 routers to install L1 routes learned from one area into L1 IS's routing/forwarding tables in another area

  This allows for reachability between L1 routers located behind L1/L2 routers in different areas

```
router isis 1
 redistribute isis ip level-2 into level-1 route-map FOO
!
ip prefix-list foo permit 0.0.0.0/0 le 32
!
route-map FOO permit 10
 match ip address prefix-list foo
```

ISP Best Practices

- Doing the same for IPv6:

```
router isis 1
 address-family ipv6
  redistribute isis level-2 into level-1 route-map FOO6
!
ip prefix-list foo6 permit 0.0.0.0/0 le 32
!
route-map FOO6 permit 10
 match ip address prefix-list foo6
!
```

ISP Best Practices

- Summary

  Best practice recommendations are commonly implemented on many ISP backbones

  Ensures efficient and scalable operation of ISIS

Introduction to ISIS

Philip Smith pfs@cisco.com

MENOG 4

5th-9th April 2009

Bahrain