

## HCRSE105-ISIS 双栈原理

IS-IS ( Intermediate System-to-Intermediate System , 中间系统到中间系统 )

### ISIS 知识点 :

ISIS 基础 , 报文类型 , 网络实体名 , padding 开启关闭 , 网络类型 , 路由器类型 , 邻居建立过程 2-way,3-way , 接口开销 , 默认路由 , 路由渗透 , ISIS 收敛 4 个步骤 , LSP 生成智能定时器 , SPF 计算智能定时器 , LSP 快速扩散 , 管理标记 , LSP 分片 , ISISv6 新增两个 TLV , 一个 NLPID,ISISv6 多拓扑

### IS-IS 报文 :

Hello PDU ( IIH PDU )

链路状态 PDU ( LSP )

完全序列号数据包 ( CSNP )

部分序列号数据包 ( PSNP )

CSNP 类似于 OSPF 的 DD 报文传递的是 LSDB 里所有链路信息摘要。

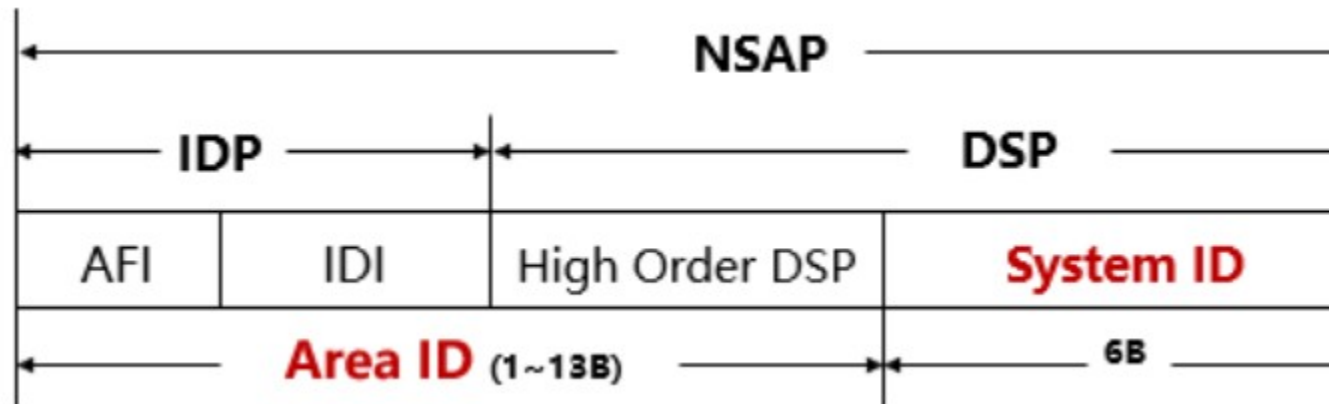
PSNP 类似于 OSPF 的 LSR 或 LSAck 报文用于请求和确认部分链路信息。

网络实体名称 NET ( Network Entity Title ) 指的是设备本身的网络层信息 , 可以看作是一类特殊的 NSAP ( SEL = 00 ) 。 NET 的长度与 NSAP 的相同 , 最多为 20 个字节 , 最少为 8 个字节。在路由器上配置 IS-IS 时 , 只需要考虑 NET 即可 , NSAP 可不必去关注。在配置 IS-IS 过程中 , NET 最多也只能配 3 个。在配置多个 NET 时 , 必须保证它们的 System ID 都相同。

isis

network-entity 10.0000.0000.0001.00

NSAP 网络服务接入点



```
[-] IEEE 802.3 Ethernet
  [+ Destination: ISIS-all-level-1-IS's (01:80:c2:00:00:14)
  [+ Source: HuaweiTe_45:31:dc (54:89:98:45:31:dc)
    Length: 1500
[-] Logical-Link Control
  DSAP: ISO Network Layer (0xfe)
  IG Bit: Individual
  SSAP: ISO Network Layer (0xfe)
  CR Bit: Command
  [+ Control field: U, func=UI (0x03)
[-] ISO 10589 ISIS InTRA Domain Routeing Information Exchange Protocol
  Intra Domain Routing Protocol Discriminator: ISIS (0x83)
  PDU Header Length: 27
  Version (==1): 1
  System ID Length: 6
  PDU Type : L1 HELLO (R:000)
  Version2 (==1): 1
  Reserved (==0): 0
  Max.AREAs: (0==3): 3
  [+ ISIS HELLO
```

3 字节

建立邻居，这两个值必须一致

用 IS-IS 协议 物理接口的 MTU 为 1497，有 3 个字节给 LLC 使用了

system ID length 默认为 6，是系统 ID 号长度

max area 默认为 3，代表最大支持 3 个 network-entity

每台设备最多可以配置三个 NET，系统 ID 必须是相同，区域

ID 可以不同。

TLV : type length value

- ▼ Area address(es) (t=1, l=4)
  - Type: 1
  - Length: 4
  - Area address (3): 49.0001
- IS Neighbor(s) (t=6, l=6)
- ▼ IP Interface address(es) (t=132, l=4)
  - Type: 132
  - Length: 4
  - IPv4 interface address: 192.168.56.6

在 IS-IS 网络中，所有的 level-2 和 level-1-2 路由器构成了一个连续的骨干区域。

为了减少在链路上发送 IS-IS hello 报文的频率，可以人为地增大报文的时间间隔。默认 hello 为 10s, DIS 为 3s(自动取相应值的三分之一，并取整)

```
int g0/0/0
```

```
isis timer hello 30 level-1
```

### padding 开启与关闭

hello 报文中的 padding 在 P2P 网络中，建立好之后，就没有了，节约带宽，在广播网络中一直有

```
int s0/0/0
```

```
isis padding-hello 一直有 padding
```

```
int s0/0/0
```

isis small-hello 没有 padding

**IS-IS 的网络类型**：broadcast , P2P

IS-IS 只支持两种类型的网络，根据物理链路不同可分为：

广播链路：如 Ethernet、Token-Ring 等。

点到点链路：如 PPP、HDLC 等

int g0/0/0

isis circuit-type p2p : 两端接口的网络类型不同建立不了邻居

### 路由器类型

Level-1 路由器 ( 只能创建 level-1 的 LSDB )

Level-2 路由器 ( 只能创建 level-2 的 LSDB )

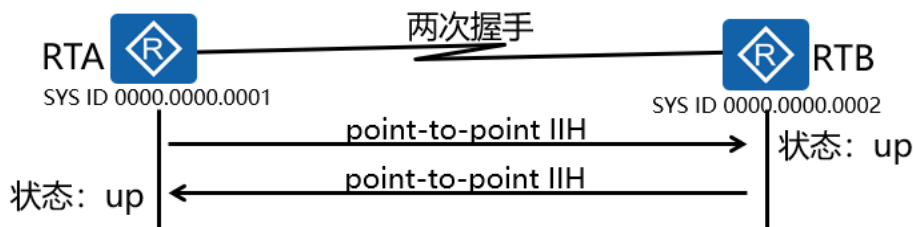
Level-1-2 路由器 ( 路由器默认的类型，能同时创建 level-1 和 level-2 的 LSDB )

### 邻居关系的建立:

在 P2P 链路上，邻居关系的建立不同于广播链路。分为两次握手机制和三次握手机制。

两次握手机制:只要路由器收到对端发来的 Hello 报文，就单方面宣布邻居为 Up 状态，建立邻居关系。

三次握手机制 :通过三次发送 P2P 的 IS-IS Hello PDU 最终建立起邻居关系，类似广播邻居关系的建立。

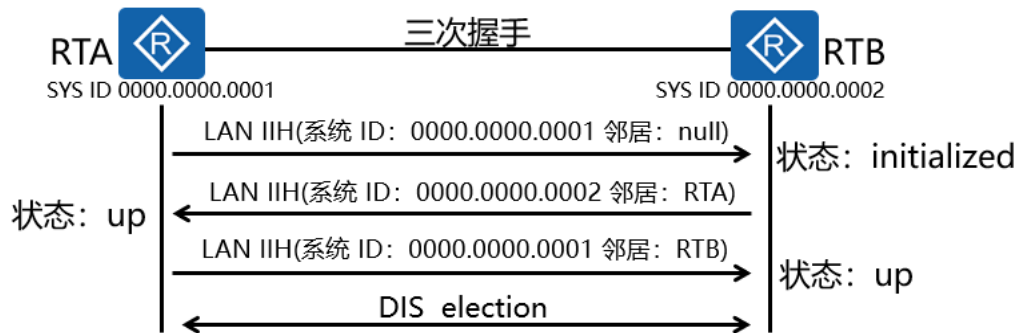


ISO10589使用两次握手，RFC3373定义了P2P三次握手机制。

P2P 链路用 3-way 来建立

int s0/0/0

isis ppp-negotiation 3-way only



MA网络类型的邻居关系建立必须是三次握手。

在广播链路上，使用 LAN IIH 报文执行三次握手建立邻居关系。当收到邻居发送的 Hello PDU 报文里面没有自己的 system ID 的时候，状态机进入 initialized。

只有收到邻居发过来的 Hello PDU 有自己的 system ID 才会 up，排除了链路单通的风险。

广播网络中邻居 up 后会选举 DIS(虚节点)，DIS 的功能类似 OSPF 的 DR(指定路由器)。

IS-IS 按如下原则建立邻居关系：

只有同一层次的相邻路由器才有可能成为邻居。

对于 Level-1 路由器来说，区域号必须一致。

链路两端 IS-IS 接口的网络类型必须一致。

链路两端 IS-IS 接口的地址必须处于同一网段。

- 1.同一层次
- 2.同一区域
- 3.同一网段
- 4.相同网络类型 P2P broadcast
- 5.相同的 mtu 值
- 6.认证相同
- 7.在 P2P 网络中，system-id 长度要一致，最大区域地址数要相同

## 接口开销

IS-IS 接口开销类型两端类型不一致，邻居可以建立，但路由不能学习

### isis

`cost-style wide`：两台设备的 cost 类型不同，邻居可以建立，但报文不能收发，所以没有路由

① narrow：指定 IS-IS 设备所有接口只能接收和发送开销类型为 narrow 的路由。

Narrow 模式下路由的开销值取值范围为 1~63 的整数。

② wide：指定 IS-IS 设备所有接口只能接收和发送开销类型为 wide 的路由。

wide 模式下路由的开销值取值范围为 1~16777215 的整数。

③ wide-compatible：指定 IS-IS 设备所有接口可以接收开销类型为 narrow 和 wide 的路由，

但却只发送开销类型为 wide 的路由。

④ narrow-compatible：指定 IS-IS 设备所有接口可以接收开销类型为 narrow 和 wide 的路由，

但却只发送开销类型为 narrow 的路由。

⑤ compatible：指定 IS-IS 设备所有接口可以接收和发送开销类型为 narrow 和 wide 的路由。

IS-IS 有三种方式来确定接口的开销，按照优先级由高到底分别如下：

① 接口开销：为单个接口设置开销，优先级最高。

int g0/0/0

isis cost 50

② 全局开销：为所有接口设置开销，优先级中等。

isis

circuit-cost 30

③ 自动计算开销：根据接口带宽自动计算开销，优先级最低。

isis

auto-cost enable

## 缺省路由

isis

default-route-advertise match default level-1-2

=====

## LSP 生成智能定时器 timer lsp-generation

在运行 IS-IS 的网络中，当本地路由信息发生变化时，设备需要产生新的 LSP 来通告这些变化。当本地路由信息的变化比较频繁时，立即生成新的 LSP 会占用大量的系统资源。

为了加快网络的收敛速度，同时又不影响系统性能，通过 timer lsp-generation 命令设置生成 LSP 使用的智能定时器，该定时器它可以根据路由信息的变化频率自动调整延迟时间。该命令可以通过参数的调整实现不同的功能：

在只使用 max-interval 的情况下，智能定时器退化为一般的一次性触发定时器。

在同时配置了 init-interval 及 incr-interval 参数时，初次产生 LSP 的延迟时间为 init-interval；第二次产生具有相同 LSP ID 的 LSP 的延迟时间为 incr-interval。随后，路由每变化一次，产生 LSP 的延迟时间都增大为前一次的两倍，直到 max-interval。稳定在 max-interval 三次或者 IS-IS 进程被重启，延迟时间又降回到 init-interval。

在配置 init-interval 但不配置 incr-interval 参数时，初次产生 LSP 使用 init-interval 作为延迟时间，随后都是使用 max-interval 作为延迟时间。同样，稳定在 max-interval 三次或者 IS-IS 进程被重启，延迟时间又降回到 init-interval。

isis

timer lsp-generation 20 50 2000

设置产生 LSP 的最大延迟为 20 秒，初始延迟为 50 毫秒，递增延迟时间为 2000 毫秒

timer lsp-generation 1 50 50 level-1

产生 LSP 的最大的延迟时间是 1S，初始延迟为 50ms，递增时间为 50ms

### SPF 计算智能定时器 timer spf

IS-IS 中，LSDB 发生变化时需要进行路由计算，但频繁的路由计算会占用大量的系统资源，导致系统性能下降。延迟 SPF 计算可以在一定程度上提高路由计算的效率。另一方面，如果路由计算的延迟时间过长，则会减慢路由的收敛速度。为了加快路由的收敛速度且不影响路由器的效率，在 SPF 计算中使用了智能定时器，它可以根据 LSDB 的变化频率自动调整延迟时间。

初次进行 SPF 计算的延迟时间为 init-interval；第二次进行 SPF 计算的延迟时间为 incr-interval。随后，每变化一次，SPF 计算的延迟时间增大为前一次的两倍，直到 max-interval。稳定在 max-interval 三次或者 IS-IS 进程被重启，延迟时间又降回到 init-interval。

max-interval 指定路由计算最大延迟时间。1 ~ 120，单位是秒。缺省值是 5 秒。



init-interval 指定初次路由计算的延迟时间。如果不指定 init-interval，智能定时器就退化为一般的一次性触发定时器。单位是毫秒。缺省值是 50 毫秒。缺省情况下不使用这个延迟时间。

incr-interval 指定两次路由计算之间的递增延迟时间。如果不指定 incr-interval，初次进行 SPF 计算用 init-interval 作为延迟时间，随后都是使用 max-interval 作为延迟时间。1 ~ 60000，单位是毫秒。缺省值是 200 毫秒。

isis

timer spf 15 10 5000

设置 SPF 计算最大延迟为 15 秒，初始延迟为 10 毫秒，递增时间为 5000 毫秒。

timer spf 1 100 100

SPF 计算最大延迟时间是 1S，初始延迟为 100ms，递增时间为 100ms

timer lsp-max-age 65000 命令用来配置当前 IS-IS 进程生成的 LSP 的最大有效时间。

缺省情况下，

LSP 的最大有效时间为 1200 秒，最大 65535

timer lsp-refresh 900 命令用来配置 LSP 的刷新周期。

缺省情况下，

LSP 的刷新周期是 900 秒，最大 65534

## LSP 快速扩散

由于 LSP 数量比较庞大，通常为了减轻大量 LSP 一起发送时

对网络设备带来的冲击，一般 IS-IS 都是采用周期性分批扩散 LSP 的方法（缺省情况下，接口上发送 LSP 报文的最小间隔时间是 50 毫秒，每次发送 LSP 报文的数目是 0）。使能 flash-flood 功能后，当 LSP 发生变化而导致 SPF 重新计算时，SPF 重新计算的 LSP 会立即扩散出去，从而有效缩短拓扑变化时全网设备上 LSDB 不一致的时间，提高全网的快速收敛性能。

```
isis
```

```
flash-flood level-1
```

## ISIS 管理标记

管理标记用来携带关于 IP 地址前缀的管理信息，其用途包括控制不同级别和不同区域间的路由引入，利用该标记可以允许在 IS-IS 域中通过 IP 地址前缀发布进行控制，简化管理。

通过 isis tag-value 命令，可以实现对指定接口上的路由进行标记，该标记可以作为路由过滤策略的过滤条件，从而对路由进行按需过滤。

```
int g0/0/0
```

```
isis enable 1
```

```
isis tag-value 77
```

## LSP 分片

当 IS-IS 要发布的链路状态协议数据报文 PDU ( Protocol Data Unit ) 中的信息量太大时，IS-IS 路由器将会生成多个 LSP 分片，用来携带更多的 IS-IS 信息。

在 IS-IS 中，每个系统 ID 都标识一个系统，每个系统都最多可生成 256 个 LSP 分片。通过增加附加系统 ID，可以最多配

置 50 个虚拟系统，从而使得 IS-IS 进程最多可生成 13056 个 LSP 分片。

Mode-1 用于网络中的部分路由器不支持 LSP 分片扩展特性的情况

Mode-2 用于网络中所有路由器都支持 LSP 分片扩展特性的情况。

Mode-1 工作原理：虚拟系统参与路由 SPF 计算，初始系统发布的 LSP 中携带了到每个虚拟系统的链路信息。类似地，虚拟系统发布的 LSP 也包含到初始系统的链路信息。这样，在网络中虚拟系统看起来与初始系统相连的真实路由器是一样的。这种方式是为了兼容不支持分片扩展的老版本所做的一个过渡模式。在老版本中，IS-IS 无法识别 IS Alias ID TLV，所以虚拟系统的 LSP 必须表现的像一个普通 IS-IS 发出的报文

Mode-2 工作原理：虚拟系统不参与路由 SPF 计算，网络中所有路由器都知道虚拟系统生成的 LSP 实际属于初始系统。在该模式下工作的 IS-IS，可以识别 IS Alias ID TLV 的内容，并作为计算树和路由的依据。

说明：无论在哪种方式下，初始系统和虚拟系统的 LSP 零分片中，都必须包含 IS Alias ID TLV 来表示初始系统是谁。

isis

lsp-fragments-extend mode-1 level-2

## 路由渗透

IS-IS 路由渗透指的是 Level 1-2 和 Level-2 路由将自己知道的其他 Level-1 区域以及 Level-2 区域的路由信息通报给指

定的 Level-1 区域的过程。

通常情况下，Level-1 区域内的路由通过 Level-1 路由器进行管理。所有的 Level-2 和 Level-1-2 路由器构成一个连续的骨干区域。Level-1 区域必须且只能与骨干区域相连，不同的 Level-1 区域之间并不相连。

Level-1-2 路由器将学习到的 Level-1 路由信息装进 Level-2 LSP，再泛洪 LSP 给其他 Level-2 和 Level-1-2 路由器。因此，Level-1-2 和 Level-2 路由器知道整个 IS-IS 路由域的路由信息。但是，为了有效减小路由表的规模，在缺省情况下，Level-1-2 路由器并不将自己知道的其他 Level-1 区域以及骨干区域的路由信息通报给它所在的 Level-1 区域。这样，Level-1 路由器将不了解本区域以外的路由信息，可能导致与本区域之外的目的地址通信时无法选择最佳的路由。

isis

import-route isis level-2 into level-1

=====

## ISISv6

为了支持 IPv6 路由的处理和计算，IS-IS 新增了两个 TLV ( Type-Length-Value ) 和一个新的 NLPID ( Network Layer Protocol Identifier )

IPv6 Reachability TLV [Type 236]

IPv6 Interface Address TLV [Type 232]

NLPID ( Network Layer Protocol Identifier ) 网络层协议 ID

**IPv6 Reachability** : 类型值为 236 ( 0xEC ) , 通过前缀、度量、标记等来描述可达的 IPv6 前缀信息。在 IPv4 中有 IPv4 内部可达性 TLV 和 IPv4 外部可达性 TLV , 在 IPv6 的扩展当中使用一个“X”bit 来区分“内部”和“外部”。

Type=236	Length	Metric..				
Metric..		U	X	S	Reserve	Prefix Length
Prefix..						
Sub-TLV Len(可选)	Sub-TLVs...					

U : up/down bit , 标识这个前缀是否是从高 level 通告下来的 ( 用来防环路 ) 。

X : external original bit , 标识这个前缀是否是从其他路由协议中引入过来的。

S : subtlv present bit , 子 TLV 标识位。 ( 可选 )

```

▼ IPv6 Reachability: 2222::/64
  Metric: 0
  0... .... = Distribution: Up
  .0.. .... = Distribution: Internal
  ..0. .... = Sub-TLV: No
  Prefix Length: 64
  IPv6 prefix: 2222::
  no sub-TLVs present
▼ IPv6 Reachability: 2024::/64
  ... ..

```

**IPv6 Interface Address** : 类型值为 232 ( 0xE8 ) , 它相当于 IPv4 中的“IP Interface Address” TLV , 只不过把原来的 32 比特的 IPv4 地址改为 128 比特的 IPv6 地址。

Type=232	Length	Interface Address 1..
..Interface Address 1..		
..Interface Address 1..		
..Interface Address 1..		
Interface Address 1..		Interface Address 2..

在 hello PDU 中，“接口地址 TLV”只包含发送 hello 包的接口的 Link-local 地址；对于 LSP，“接口地址 TLV”只包含 IS 的 non-link-local IPv6 地址。

- > Area address(es) (t=1, l=2)
- > IS Neighbor(s) (t=6, l=6)
- ▼ IP Interface address(es) (t=132, l=4)
  - Type: 132
  - Length: 4
  - IPv4 interface address: 192.168.12.2
- ▼ IPv6 Interface address(es) (t=232, l=16)
  - Type: 232
  - Length: 16
  - IPv6 interface address: fe80::2e0:fcff:fef6:f60
- > Protocols Supported (t=129, l=2)

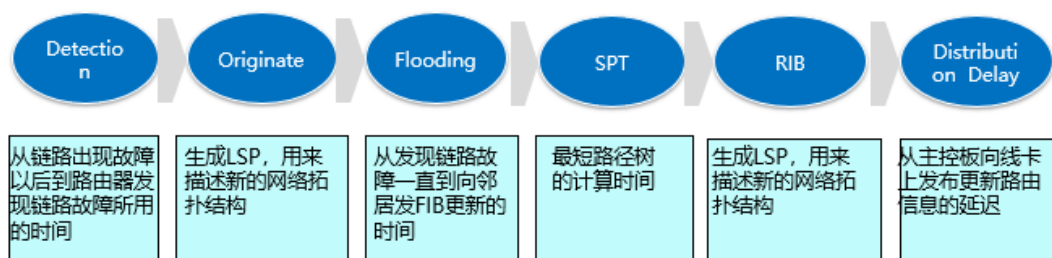
NLPID ( Network Layer Protocol Identifier ) 是标识网络层协议报文的一个 8 比特字段，IPv6 的 NLPID 值为 142 ( 0x8E )。如果 IS-IS 支持 IPv6，那么向外发布 IPv6 路由时必须携带 NLPID 值。



## 前言

- ISIS协议是IP网络中重要的内部网关协议，同时因为ISIS协议的TLV特性，使其具有很强的扩展性和生命力。ISIS作为一种高扩展性的IGP协议，其使用场景已不局限于传统IP网络，还包括数据中心，IPv6等各种IP场景。本章将围绕ISIS协议重点介绍其高级特性和IPv6下的ISIS特性与配置，并且围绕现网介绍双栈ISIS在现网的部署与实现。

## ISIS收敛步骤



- IS-IS的收敛可以总体描述为如下状态D+O+F+SPT+RIB+DD

- IGP 的收敛可以总体描述为如下状态 D+O+F+SPT+RIB+DD
- D 状态为从链路出现故障以后到路由器发现链路故障所用的时间。
- O 状态为生成 LSP，用来描述新的网络拓扑结构所需要的时间。
- F 状态为从发现链路故障一直到向邻居发布 FIB 更新的时间。
- SPT 状态为运行 SPF 算法，计算最短路径树的时间。
- RIB 状态为用主 CPU 更新 RIB 表项和 FIB 表项的时间
- DD 状态为从主控板向线卡上发布更新路由信息的延迟

- RIB 状态和 DD 状态一般与路由器的硬件有关，如主 CPU、线卡 CPU、内存、网络处理器有关，这两个状态人为无法对收敛时间做出很大的改变。所以本文基本上以讨论前四个状态为主。

## 链路故障检测



### 正常情况下IS-IS链路故障检测

- 正常情况下IS-IS的链路状态检测仅仅依赖于IS-IS协议本身，即IS-IS的IIH报文，IIH报文检测时间为秒级，不适合收敛要求高的网络
- 将IIH的发送间隔改小，可以缩短检测时间。

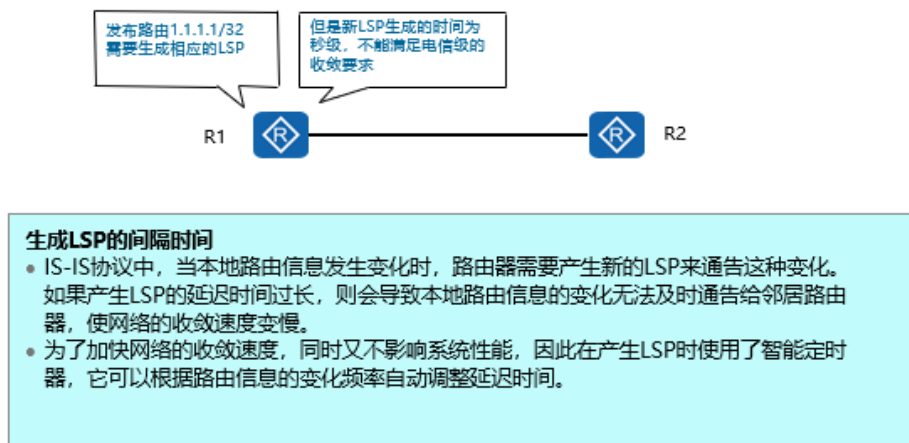
### 用其他协议辅助IS-IS链路故障检测

- 用SDH/SONET (POS)、光口以太做链路检测收敛速度比较快，为毫秒级，但是对接口类型有依赖性。
- BFD技术被通常应用于IP网络中做链路状态检测，BFD为毫秒级，对接口类型没有依赖性。

- 现有的故障检测方法主要包括：
- 硬件检测：例如通过 SDH ( Synchronous Digital Hierarchy，同步数字体系 ) 告警检测链路故障。硬件检测的优点是可以很快发现故障，但并不是所有介质都能提供硬件检测。
- 慢 Hello 机制：通常是指路由协议的 Hello 机制。这种机制检测到故障所需时间为秒级。对于高速数据传输，例如吉比特速率级，超过 1 秒的检测时间将导致大量数据丢失；对于时延敏感的业务，例如语音业务，超过 1 秒的延迟也是不能接受的。并且，这种机制依赖于路由协议。IS-IS 协议一般通过 IIH 报文，用来做邻居发现和失效性检测，这个检测的速度是秒级的。
- 其他检测机制：不同的协议或设备制造商有时会提供专用的检测机制，但在系统间互联互通时，这样的专用检测机制通常难以部署，如 BFD

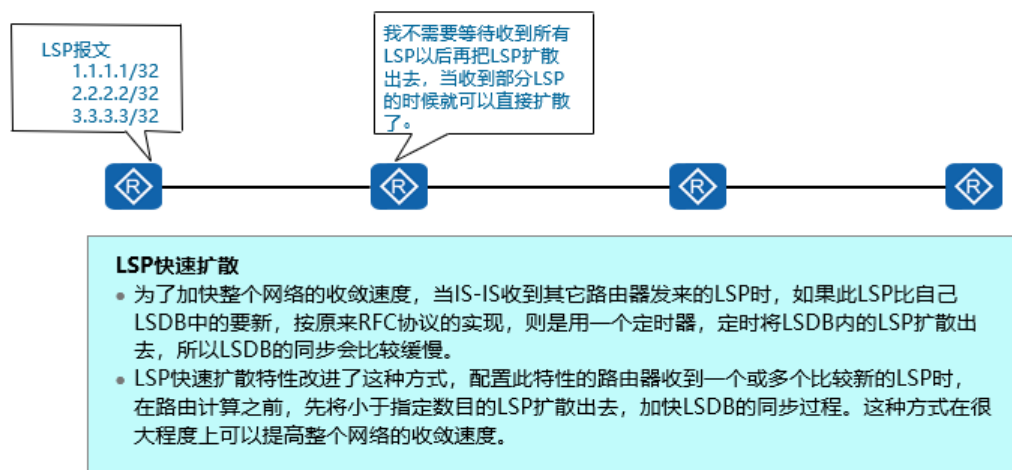


## 生成LSP的间隔时间



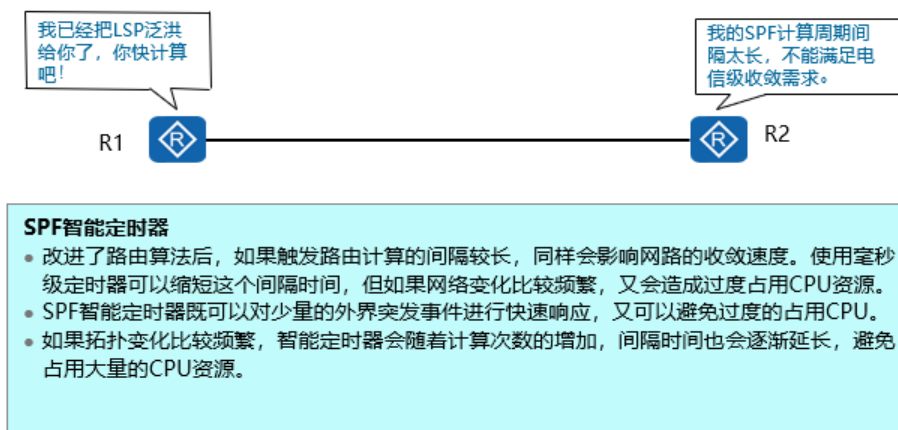
- 在 IS-IS 协议中，当 LSP 生成定时器到期时，系统会根据当前拓扑重新生成一个自己的 LSP。原有的实现机制是采用间隔时间定长的定时器，不能同时满足快速收敛和低 CPU 占用率的需要。
- 为了加快网络的收敛速度，同时又不影响系统性能，因此在产生 LSP 时使用了智能定时器，它可以根据路由信息的变化频率自动调整延迟时间。使其可以对于突发事件（如接口 Up/Down）快速响应，加快网络的收敛速度。同时，当网络变化频繁时，智能定时器的间隔时间会自动延长，避免过度占用 CPU 资源。

## 加快泛洪LSP的时间



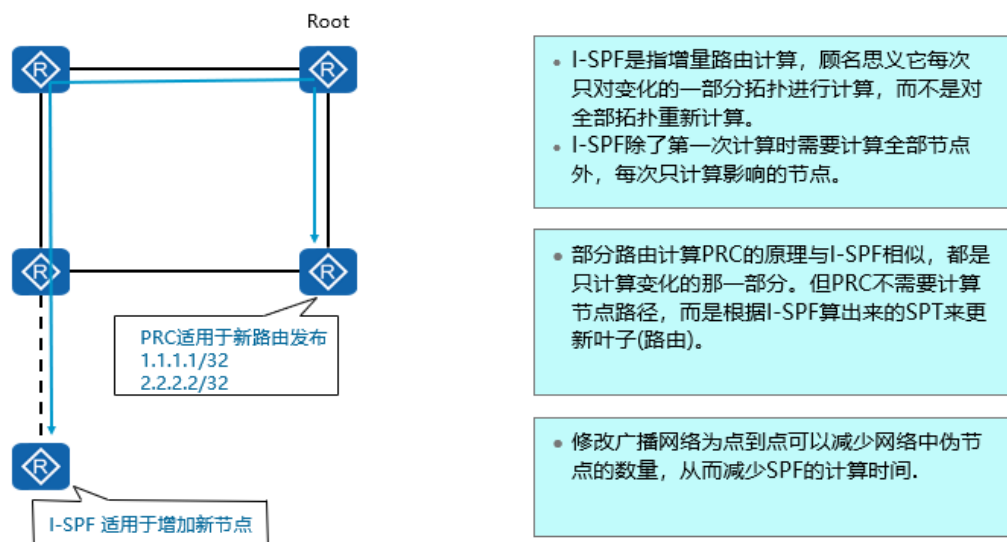
- 用户可以指定每次扩散的 LSP 数量, 这个数量是针对所有接口的。如果需要发送的 LSP 的数量大于这个数, 则就发送 *lsp-count* 个 LSP。如果配置了定时器, 在路由计算之前如果这个定时器未超时, 则立即扩散; 否则在该定时器超时发送。
- 如果命令中没有指定级别, 则缺省同时在 Level-1 和 Level-2 中使能此功能。

## 加快SPF的计算时间



- 通常情况下，一个正常运行的 IS-IS 网络是稳定的，发生大量的网络变动的几率很小，IS-IS 路由器不会频繁的进行路由计算，所以第一次触发的时间可以设置的非常短（毫秒级）。如果拓扑变化比较频繁，智能定时器会随着计算次数的增加，间隔时间也会逐渐延长，避免占用大量的 CPU 资源。

## 改进SPF的计算方法



- 在 ISO-10589 中定义使用 Dijkstra 算法进行路由计算。当网络拓扑中有一个节点发生变化时，这种算法需要重新计算网络中的所有节点，计算时间长，占用过多的 CPU 资源，影

响整个网络的收敛速度。

- I-SPF 改进了这个算法，除了第一次计算时需要计算全部节点外，每次只计算影响的节点，而最后生成的最短路径树 SPT 与原来的算法所计算的结果相同，大大降低了 CPU 的占用率，提高了网络收敛速度。

- 在路由计算中，路由代表叶子，路由器则代表节点。如果 I-SPF 计算后的 SPT 改变，PRC 会只处理那个变化的节点上的所有叶子；如果经过 I-SPF 计算后的 SPT 并没有变化，则 PRC 只处理变化的叶子信息。

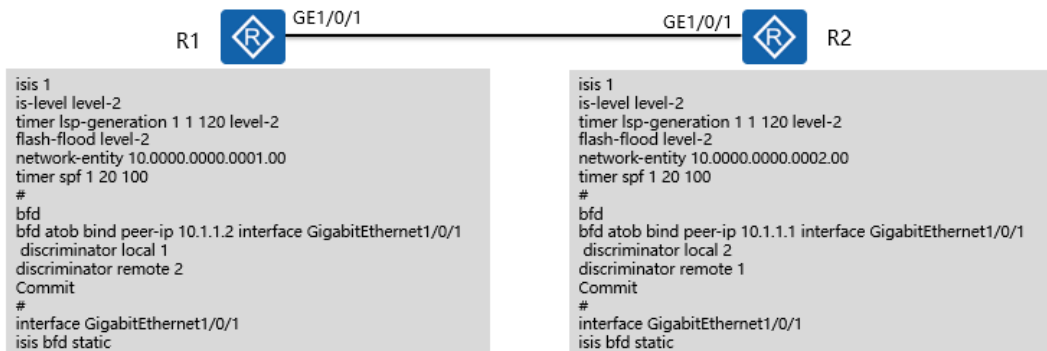
- 比如一个 IS 接口，则整个网络拓扑的 SPT 是不变的，这时 PRC 只更新这个节点的接口路由，从而节省 CPU 占用率。

- PRC 和 I-SPF 节点使能一个 IS-配合使用可以将网络的收敛性能进一步提高，它是原始 SPF 算法的改进，所以已经代替了原有的算法。

- 默认情况下华为路由器采用 I-SPF 和 PRC 进行计算，不需要命令配置。

## ISIS快收敛配置

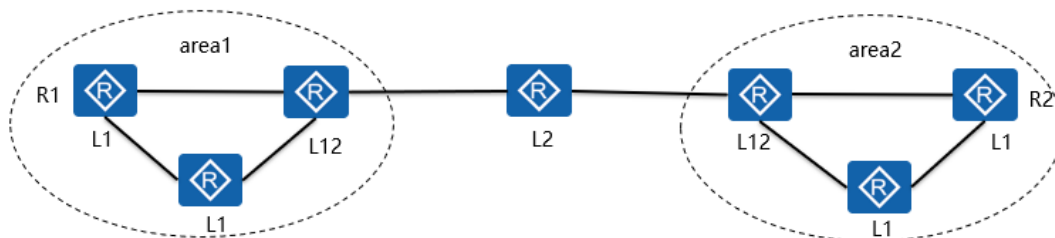
- R1和R2两台路由器互连，并且两个路由器之间通过IS-IS协议实现互通。现要求通过BFD提高两台路由器的收敛速度。



## 基本特性

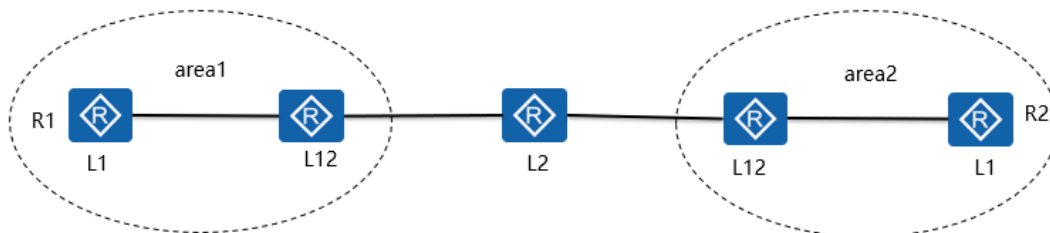
- 管理标记特性允许在IS-IS域中通过管理标记对IP地址前缀进行控制，可以达到简化管理。其用途包括控制不同级别和不同区域间的路由引入，以及在同一路由器上运行的IS-IS多实例。
- 管理标记值与某些属性相关联。当cost-style为wide、wide-compatible或compatible时，如果发布可达的IP地址前缀具有该属性，IS-IS会将管理标记加入到该前缀的IP可达信息TLV中。这样，管理标记就会随着前缀发布到整个路由域。

## 工作原理(1)



- R1需要与处于area2区域的R2相互通信，且为了保证信息安全，area2区域内的路由器不能收到R1发送的报文信息。首先，可以给R1、R2使能了IS-IS的接口配置相同的管理标记值tag。然后在area1的Level-1-2路由器做从Level-2到Level-1区域的路由渗透时，应用匹配指定的tag。这样就可以满足R1在与area2区域通信时，仅与R2进行通信。

## 工作原理(2)



- Tag管理标记应用以后，area1内的R1路由器的仅能看到area2内的R2路由器

## 基本概念

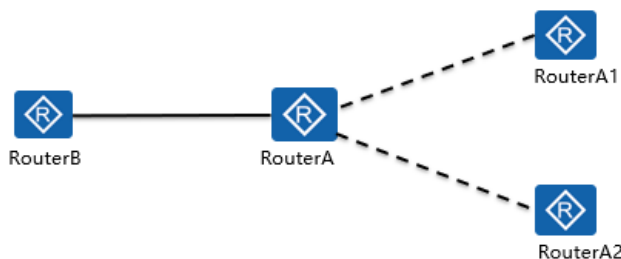
- 初始系统 (Originating System) : 初始系统是实际运行IS-IS协议的路由器。允许一个单独的IS-IS进程像多个虚拟路由器一样发布LSP, 而“Originating System”指的是那个“真正”的IS-IS进程。
- 系统ID (Normal System-ID) : 初始系统的系统ID。
- 虚拟系统 (Virtual System) : 由附加系统ID标识的系统, 用来生成扩展LSP分片。这些分片在其LSP ID中携带附加系统ID。
- 附加系统ID (Additional System-ID) : 虚拟系统的系统ID, 由网络管理器统一分配。每个附加系统ID都允许生成256个扩展的LSP分片。

## 工作原理

- 在IS-IS中, 每个系统ID都标识一个系统, 每个系统都最多可生成256个LSP分片。通过增加附加系统ID, 可以最多配置50个虚拟系统, 从而使得IS-IS进程最多可生成13056个LSP分片。
  - 使能分片扩展功能之后, 如果存在由于报文装满而丢失的信息, 系统会提醒重启IS-IS。重启之后, 初始系统会尽最大能力装载路由信息, 装不下的信息将放入虚拟系统的LSP中发送出去, 并通过24号TLV来告知其他路由器此虚拟系统和自己的关系。
- 
- 当 IS-IS 要发布的链路状态协议数据报文 PDU ( Protocol Data Unit ) 中的信息量太大时 , IS-IS 路由器将会生成多个 LSP 分片 , 用来携带更多的 IS-IS 信息。
  - IS-IS LSP 分片由 LSP ID 中的 LSP Number 字段进行标识 , 这个字段的长度是 1 字节。因此 , 一个 IS-IS 进程最多可产生 256 个 LSP 分片 , 携带的信息量有限。在 RFC3786 中规定 , IS-IS 可以配置虚拟的 System ID , 并生成虚拟 IS-IS 的 LSP 报文来携带路由等信息。

## 工作模式

- IS-IS路由器可以在两种模式下运行LSP分片扩展特性：



模式	应用场景
Mode-1	用于网络中的部分路由器不支持LSP分片扩展特性的情况。
Mode-2	用于网络中所有路由器都支持LSP分片扩展特性的情况。

- Mode-1 应用场景：用于网络中的部分路由器不支持 LSP 分片扩展特性的情况。
- Mode-1 工作原理：虚拟系统参与路由 SPF 计算，初始系统发布的 LSP 中携带了到每个虚拟系统的链路信息。类似地，虚拟系统发布的 LSP 也包含到初始系统的链路信息。这样，在网络中虚拟系统看起来与初始系统相连的真实路由器是一样的。这种方式是为了兼容不支持分片扩展的老版本所做的一个过渡模式。在老版本中，IS-IS 无法识别 IS Alias ID TLV，所以虚拟系统的 LSP 必须表现的像一个普通 IS-IS 发出的报文。
- Mode-2 应用场景：用于网络中所有路由器都支持 LSP 分片扩展特性的情况。
- Mode-2 工作原理：虚拟系统不参与路由 SPF 计算，网络中所有路由器都知道虚拟系统生成的 LSP 实际属于初始系统。在该模式下工作的 IS-IS，可以识别 IS Alias ID TLV 的内容，并作为计算树和路由的依据。
- 说明：无论在哪种方式下，初始系统和虚拟系统的 LSP 零分片中，都必须包含 IS Alias ID TLV 来表示初始系统是谁。

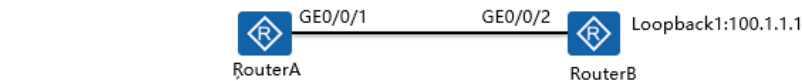
## IS-IS对LSDB计算为路由信息时进行过滤(1)

- 通过配置IS-IS LSDB中的信息是否加入IP路由表，来控制加入IP路由表的IS-IS路由数量，减少IP路由表的规模。
- 配置ACL规则：

```
acl { name basic-acl-name { basic | [ basic ] number basic-acl-number } | [ number ] basic-acl-number } [ match-order { config | auto } ]  
  
rule [ rule-id ] [ name rule-name ] { deny | permit } [ fragment-type { fragment | non-fragment | non-subseq | fragment-subseq | fragment-spe-first } | source { source-ip-address { source-wildcard | 0 | src-netmask } | any } | time-range time-name | vpn-instance vpn-instance-name ]
```
- 配置过滤器：
- ```
filter-policy { acl-number | acl-name acl-name } import
```

## IS-IS对LSDB计算为路由信息时进行过滤(2)

- RouterA与RouterB建立ISIS邻居，通过ISIS，RouterA可学习到RouterB的loopback1路由。



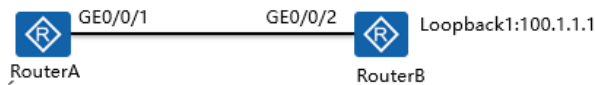
- 过滤前：

| Route Flags: R - relay, D - download to fib |         |     |      |       |           |                      |
|---------------------------------------------|---------|-----|------|-------|-----------|----------------------|
| -----                                       |         |     |      |       |           |                      |
| Routing Tables: Public                      |         |     |      |       |           |                      |
| Destinations : 9      Routes : 9            |         |     |      |       |           |                      |
| Destination/Mask                            | Proto   | Pre | Cost | Flags | NextHop   | Interface            |
| 1.1.1.1/32                                  | Direct  | 0   | 0    | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30                                 | Direct  | 0   | 0    | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32                                 | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32                                 | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 100.1.1.1/32                                | ISIS-L2 | 15  | 10   | D     | 10.1.1.2  | GigabitEthernet0/0/1 |



## IS-IS对LSDB计算为路由信息时进行过滤(3)

- RouterA与RouterB建立ISIS邻居，通过ISIS部署流策略使RouterA的路由表中没有RouterB的loopback1路由，而RouterB的loopback1信息会存在于RouterA的ISIS LSDB中。

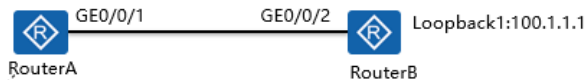


- 配置过滤:

```
#
acl name huawei 2000
rule 5 deny source 100.1.1.1 0
#
isis 1
is-level level-2
network-entity 01.0000.0000.0001.00
Filter-policy acl-name huawei import
#
```

## IS-IS对LSDB计算为路由信息时进行过滤(4)

- 配置过滤后，RouterA的路由表中没有RouterB的loopback1路由，而RouterB的loopback1信息会存在于RouterA的ISIS LSDB中。



- 查看路由表:

| Route Flags: R - relay, D - download to fib |        |     |      |       |           |                      |
|---------------------------------------------|--------|-----|------|-------|-----------|----------------------|
| -----                                       |        |     |      |       |           |                      |
| Routing Tables: Public                      |        |     |      |       |           |                      |
| Destinations : 9 Routes : 9                 |        |     |      |       |           |                      |
| Destination/Mask                            | Proto  | Pre | Cost | Flags | NextHop   | Interface            |
| 1.1.1.1/32                                  | Direct | 0   | 0    | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30                                 | Direct | 0   | 0    | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32                                 | Direct | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32                                 | Direct | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |

- 说明：
- ISIS LSDB LSP 里依然还有被过滤路由的前缀

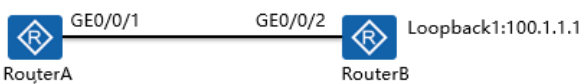
## IS-IS对引入的路由信息进行过滤(1)

- 通过配置IS-IS在引入外部路由时进行过滤，有效控制网络中IS-IS路由信息的数量。
- 配置地址前缀列表：  
**ip ip-prefix ip-prefix-name [ index index-number ] { permit | deny } ip-address mask-length [ greater-equal greater-equal-value ] [ less-equal less-equal-value ]**
- 配置路由策略：  
**route-policy route-policy-name { permit | deny } node node**  
**if-match acl { acl-number | acl-name }**  
**if-match ip-prefix ip-prefix-name**

## IS-IS对引入的路由信息进行过滤(2)

- RouterA与RouterB建立ISIS邻居，RouterB可以引入loopback1的直连路由到RouterB的ISIS LSDB，并通告给RouterA。

过滤前:



Route Flags: R - relay, D - download to fib

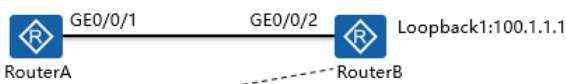
Routing Tables: Public  
Destinations : 9      Routes : 9

| Destination/Mask | Proto   | Pre | Cost | Flags | NextHop   | Interface            |
|------------------|---------|-----|------|-------|-----------|----------------------|
| 1.1.1.1/32       | Direct  | 0   | 0    | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30      | Direct  | 0   | 0    | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32      | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32      | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 100.1.1.1/32     | ISIS-L2 | 15  | 10   | D     | 10.1.1.2  | GigabitEthernet0/0/1 |

## IS-IS对引入的路由信息进行过滤(3)

- RouterA与RouterB建立ISIS邻居，RouterB在引入loopback1的直连路由到RouterB的ISIS LSDB时，配置引入的过滤。

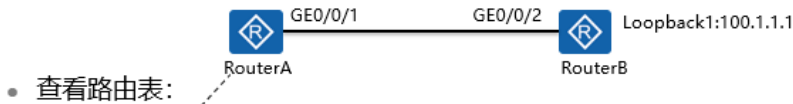
配置过滤:



```
#
ip ip-prefix huawei index 10 deny 100.1.1.1 32
#
route-policy huawei deny node 10
if-match ip-prefix huawei
#
isis 1
is-level level-2
network-entity 01.0000.0000.0002.00
import-route direct route-policy huawei
#
```

## IS-IS对引入的路由信息进行过滤(4)

- 配置过滤后，RouterB的loopback1的直连路由没有引入到RouterB的ISIS LSDB。从而RouterA不会学到RouterB的loopback1路由。



Route Flags: R - relay, D - download to fib

Routing Tables: Public  
Destinations : 9      Routes : 9

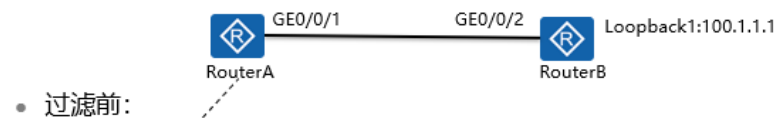
| Destination/Mask | Proto  | Pre | Cost | Flags | NextHop   | Interface            |
|------------------|--------|-----|------|-------|-----------|----------------------|
| 1.1.1.1/32       | Direct | 0   | 0    | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30      | Direct | 0   | 0    | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32      | Direct | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32      | Direct | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |

## IS-IS对外部路由信息在发布时进行过滤(1)

- IS-IS对已引入的外部路由在向外发布时进行过滤的策略。
- 配置外部路由的发布过滤策略:
- filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [ *protocol* [ *process-id* ] ]

## IS-IS对外部路由信息在发布时进行过滤(2)

- RouterA与RouterB建立ISIS邻居，RouterB可以引入loopback1的直连路由到RouterB的ISIS LSDB，并正常通告给RouterA。从而RouterA学习到RouterB的loopback1路由。



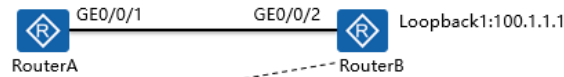
Route Flags: R - relay, D - download to fib

Routing Tables: Public  
Destinations : 9      Routes : 9

| Destination/Mask | Proto   | Pre | Cost | Flags | NextHop   | Interface            |
|------------------|---------|-----|------|-------|-----------|----------------------|
| 1.1.1.1/32       | Direct  | 0   | 0    | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30      | Direct  | 0   | 0    | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32      | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32      | Direct  | 0   | 0    | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 100.1.1.1/32     | ISIS-L2 | 15  | 10   | D     | 10.1.1.2  | GigabitEthernet0/0/1 |

## IS-IS对外部路由信息在发布时进行过滤(3)

- RouterA与RouterB建立ISIS邻居，RouterB的loopback1直连路由引入到RouterB的ISIS LSDB时，配置针对RouterB的loopback1的过滤。

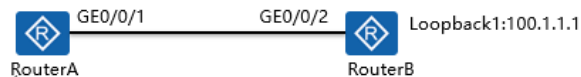


- 配置过滤:

```
#
ip ip-prefix huawei index 10 deny 100.1.1.1 32
#
isis 1
 is-level level-2
 network-entity 01.0000.0000.0002.00
 import-route direct
 filter-policy acl-name huawei export
#
```

## IS-IS对外部路由信息在发布时进行过滤(4)

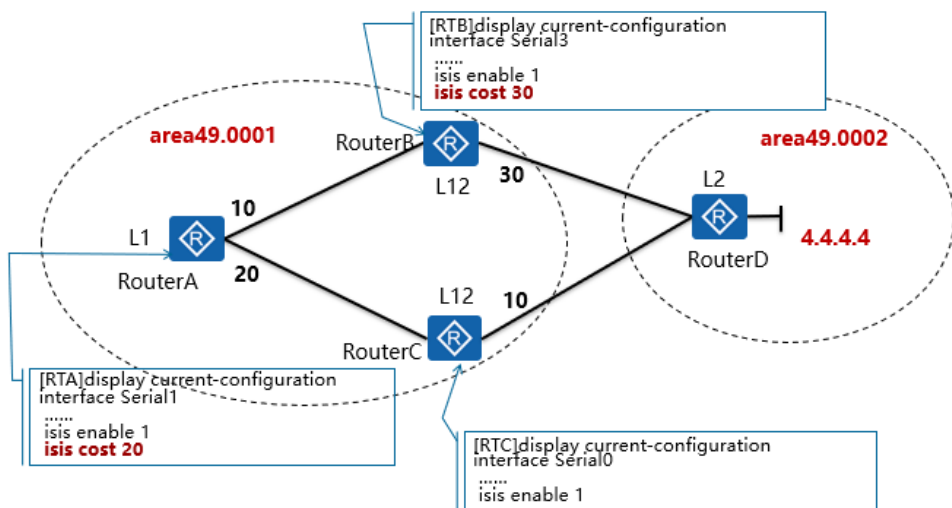
- 配置过滤后，RouterA的ISIS LSDB中没有RouterB的loopback1的信息，从而RouterA不会学到RouterB的loopback1路由。



- 查看路由表:

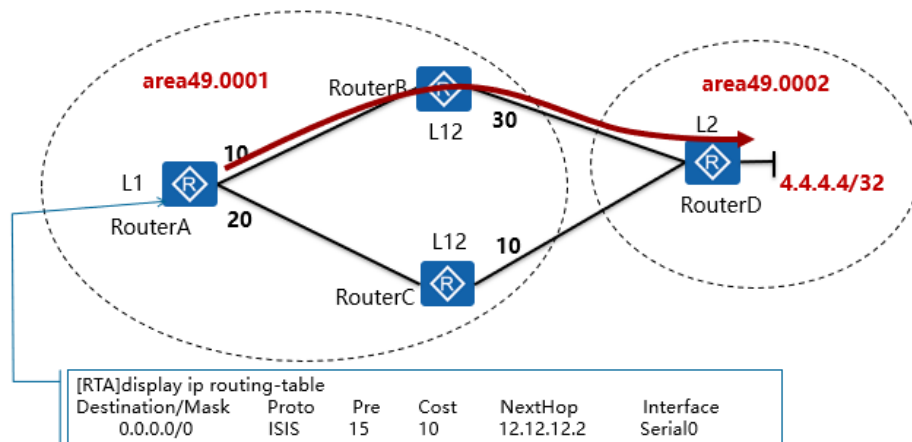
| Route Flags: R - relay, D - download to fib |        |     |            |       |           |                      |
|---------------------------------------------|--------|-----|------------|-------|-----------|----------------------|
| -----                                       |        |     |            |       |           |                      |
| Routing Tables: Public                      |        |     |            |       |           |                      |
| Destinations : 9                            |        |     | Routes : 9 |       |           |                      |
| Destination/Mask                            | Proto  | Pre | Cost       | Flags | NextHop   | Interface            |
| 1.1.1.1/32                                  | Direct | 0   | 0          | D     | 127.0.0.1 | LoopBack0            |
| 10.1.1.0/30                                 | Direct | 0   | 0          | D     | 10.1.1.1  | GigabitEthernet0/0/1 |
| 10.1.1.1/32                                 | Direct | 0   | 0          | D     | 127.0.0.1 | GigabitEthernet0/0/1 |
| 10.1.1.3/32                                 | Direct | 0   | 0          | D     | 127.0.0.1 | GigabitEthernet0/0/1 |

## IS-IS路由渗透(1)

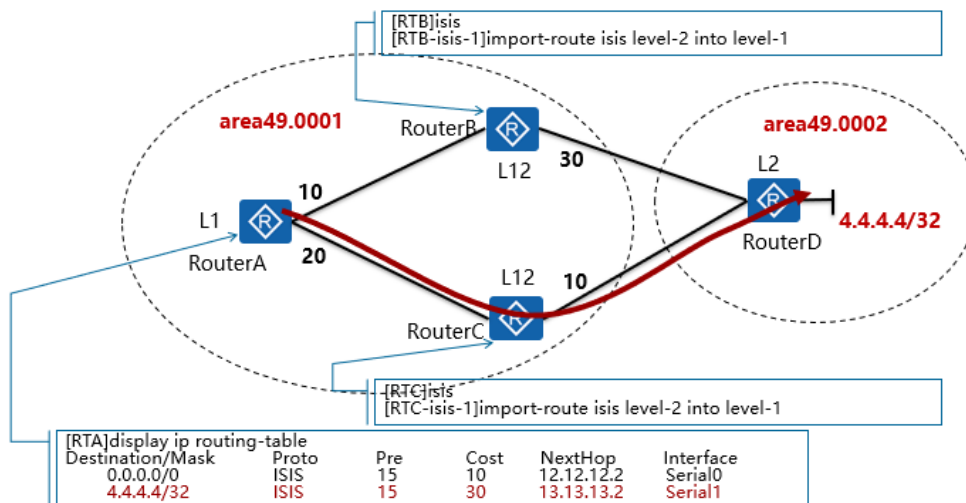


- 引入：
- Level-1 区域内的路由信息通过 Level-1-2 路由器通报给 Level-2 区域，因此，Level-1-2 和 Level-2 路由器知道整个 IS-IS 路由域的路由信息。但是，在缺省情况下，Level-2 路由器并不将自己知道的其他 Level-1 区域以及骨干区域的路由信息通报给 Level-1 区域。这样，Level-1 路由器将不了解本区域以外的路由信息，可能导致对本区域之外的目的地址无法选择最佳的路由。
- 为解决上述问题，IS-IS 提供了路由渗透功能。

## IS-IS路由渗透(2)



## IS-IS路由渗透(3)



- 注意 Level 1 路由器在收到两条相同的路由的时候，会优选本区域的路由，不会优选 L2 区域过来的路由，尽管 L2 的路由 cost 较小。

## ISIS协议概述

- ISIS是一种IGP协议。
- ISIS使用SPF算法计算路由。
- ISIS的报文采用TLV结构，因此扩展性很好。
  - 为支持新的协议和特性，只需要扩展新的TLV或子TLV。
  - 可以轻松扩展支持IPv6，TE，MT等协议和特性。
  - IS-IS对IPv6的支持不需要对协议做大的改动，因此协议的继承性很好；不像OSPF，为支持IPv6需要开发全新的协议OSPFv3。

## 扩展的TLV类型

- ISIS 为支持IPv6，扩展了以下两个TLV：
- IPv6 Reachability TLV [Type 236] [0xEC]
  - IPv6 Reachability：类型值为236（0xEC），通过前缀、度量、标记等来描述可达的IPv6前缀信息。在IPv4中有IPv4内部可达性TLV和IPv4外部可达性TLV，在IPv6的扩展当中使用一个“X” bit来区分“内部”和“外部”。
- IPv6 Interface Address TLV [Type 232] [0xE8]
  - IPv6 Interface Address：类型值为232（0xE8），它相当于IPv4中的“IP Interface Address” TLV，只不过把原来的32比特的IPv4地址改为128比特的IPv6地址。
- IETF 的 draft-ietf-isis-ipv6-05.txt 中规定了 IS-IS 为支持 IPv6 所新增的内容。主要是新添加的支持 IPv6 路由信息的两个 TLVs（Type-Length-Values）和一个新的 NLPID（Network Layer Protocol Identifier）。
- 新增的两个 TLV 分别是：
- IPv6 Reachability：类型值为 236（0xEC），通过前缀、度量、标记等来描述可达的 IPv6 前缀信息。在 IPv4 中有 IPv4 内部可达性 TLV 和 IPv4 外部可达性 TLV，在 IPv6 的扩展当中使用一个“X”bit 来区分“内部”和“外部”。
- IPv6 Interface Address：类型值为 232（0xE8），它相当于 IPv4 中的“IP Interface Address” TLV，只不过把原来的 32 比特的 IPv4 地址改为 128 比特的 IPv6 地址。

## IPv6 Reachability TLV

|                 |             |          |   |   |         |               |
|-----------------|-------------|----------|---|---|---------|---------------|
| Type=236        | Length      | Metric.. |   |   |         |               |
| Metric..        |             | U        | X | S | Reserve | Prefix Length |
| Prefix..        |             |          |   |   |         |               |
| Sub-TLV Len(可选) | Sub-TLVs... |          |   |   |         |               |

- U: up/down bit , 标识这个前缀是否是从高level通告下来的（用来防环路）。
  - X: external original bit , 标识这个前缀是否是从其他路由协议中引入过来的。
  - S: subtlv present bit, 子TLV标识位。(可选)
- 这个数据结构可能会重复多次（当有多个路由前缀的时候）。
  - Metric 字段已经被重新定义了，MAX\_PATH\_METRIC (1023) 变成了 MAX\_V6\_PATH\_METRIC (0xFE000000). 如果一个前缀的 METRIC 大于 MAX\_V6\_PATH\_METRIC , 那么它不是用来构建路由表的，而是用于一些特殊的目的。
  - TLV128：IP 内部可达性信息；TLV130：IP 外部可达性信息；在 TLV236 中，“外部”和“内部”用“X”比特表示。



## IPv6 Interface Address TLV(1)

- IPv6 Interface Address TLV [类型 232] [0xE8]
  - TLV 232 跟 TLV 132相似
  - 每个接口的地址长度变成128bits

| Type=232                | Length | Interface Address 1.. |
|-------------------------|--------|-----------------------|
| ..Interface Address 1.. |        |                       |
| ..Interface Address 1.. |        |                       |
| ..Interface Address 1.. |        |                       |
| Interface Address 1..   |        | Interface Address 2.. |

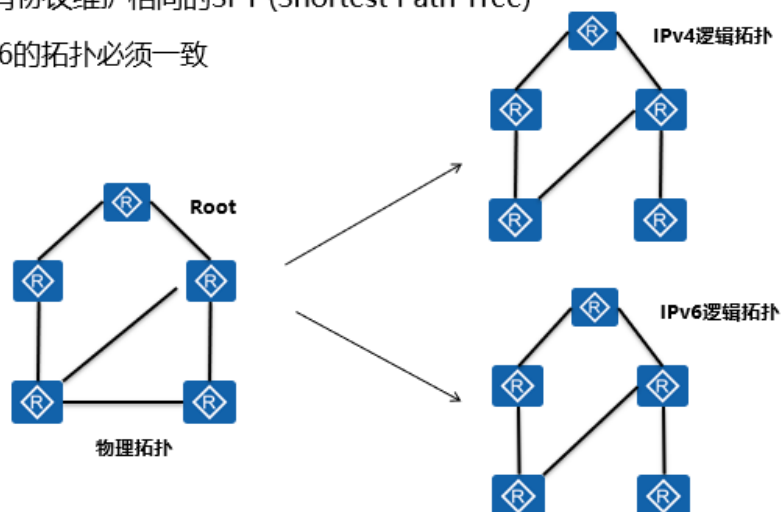
- 注意：在 hello PDU 中，“接口地址 TLV”只包含发送 hello 包的接口的 Link-local 地址；对于 LSP，“接口地址 TLV”只包含 IS 的 non-link-local IPV6 地址。

## IPv6 Interface Address TLV(2)

- 这个TLV结构是直接来自TLV132映射过来的，因此，原来TLV132最多可以64个IP地址(32位)，在TLV232中，最多只能有16个IPv6地址(128位)。
- 在不同的PDU中，这个字段的内容是不同的，在hello PDU中，“接口地址TLV”只能包含发送hello包的接口的Link-local地址；对于LSP，“接口地址TLV”只能包含IS的non-link-local IPv6

## IS-IS ST单拓扑

- IS-IS为所有协议维护相同的SPT (Shortest Path Tree)
- IPv4和IPv6的拓扑必须一致

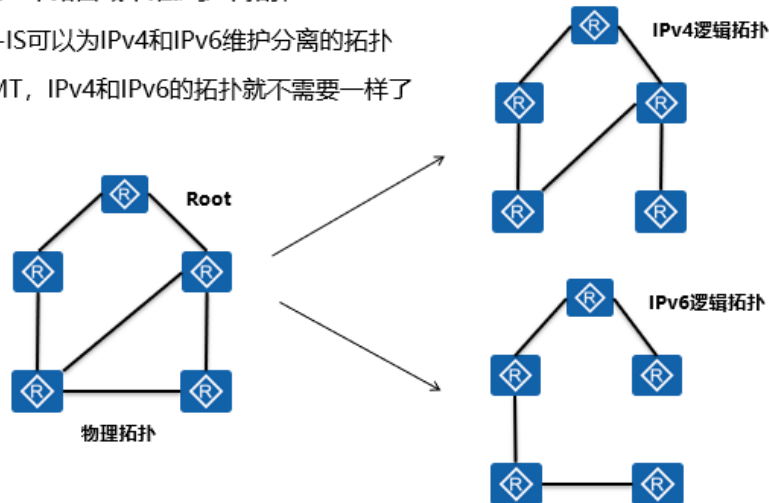


## ST单拓扑缺点

- 不足之处
  - 网络可维护性的需求在目前的运营商中越来越被重视，独立拓扑的维护网络，即带内维护网络的需求开始出现。
  - IS-IS为所有协议维护相同的SPT，这意味着IPv4和IPv6的拓扑必须一致
- 有什么问题？
  - 不适合分离拓扑的网络部署。
  - 为维护相同的拓扑，所有接口都必须同时运行IS-IS IPv4和IS-IS IPv6，部署不灵活。
  - 不能使用IPv4区域来链接不同的IPv6区域，否则IPv4区域会丢弃IPv6的流量

## IS-IS 对MT多拓扑的支持

- MT可以使IS-IS在一个路由域中维护多个拓扑
- 如果支持MT, IS-IS可以为IPv4和IPv6维护分离的拓扑
- 重要的是, 使用MT, IPv4和IPv6的拓扑就不需要一样了



## MT(多拓扑): 分离的拓扑

- IS-IS路由协议主要可以分为以下几个方面:
  - 邻居的建立,
  - 路由可达 (Prefix Reachable) 与路由器可达 (IS Reachable) 的发布,
  - SPF计算以及路由计算。
- 为了达到多拓扑的相互隔离, 以上几个方面均要求携带MT参数以满足这一要求 (SPF计算与路由计算在路由器内识别完成) 。
- 于是, draft-ietf-isis-wg-multi-topology-11中定义了四种新的TLV分别满足以上过程, 实现了通用环境下的ISIS MT的交互过程。
- 新增四个 TLV
  - TLV 229 – Multi-Topology Identifier
  - TLV 222 – Multi-Topologies Intermediate System
  - TLV 235 – Multi-Topologies Reachable IPv4 Prefixes
  - TLV 237 – Multi-Topologies Reachable IPv6 Prefixes
  - Reserved MT ID Values

## ISISv6配置

- 使能ISIS进程多拓扑:

```
[Huawei-isis-1]ipv6 enable topology ipv6
```

- 接口上使能ISIS:

```
[Huawei-GigabitEthernetX/Y/Z]isis ipv6 enable
```

- 查看ISIS邻居关系:

```
[Huawei]dis isis peer
```

- 查看ISIS路由:

```
[Huawei]dis isis route
```

## ISIS规划(1)

- **NET (Network Entity Title) 规划**
- NET格式: AA.BBBB.CCCC.DDDD.SSSS.SSSS.SSSS.00
  - Area ID = AA.BBBB.CCCC.DDDD
    - AA: 49, 地址格式标识符AFI (AFI=49的地址为OSI协议的私有地址)
    - BBBB: 可以是国家编码, 例如中国0086
    - CCCC: 可以是省编码, 自己定义, 例如辽宁省0003
    - DDDD: 可以是设备所在站点编码, 自己定义, 例如辽宁省大连站点3821
  - System ID = SSSS.SSSS.SSSS
    - 业界通行的做法是通过设备Loopback0地址演绎, 生成System ID
  - NSEL始终为00
- **分层分区域规划**
  - 所有ISIS路由器都工作在Backbone, Level-2模式; (首选)
  - 所有ISIS路由器都工作在同一个Area, Level-1模式;

## ISIS规划(2)

- **Cost规划**
- ISIS Cost设计比较灵活
  - 可以根据链路物理带宽设计
  - Cost的设计决定网络流量的走向
  - 所以除了考虑上述2个因素外，更重要的是考虑客户对网络流量走向的需求。这就要求在Cost设计前，要清楚不同端到端场景的流量走向。
- ISIS有三种设置链路Cost值的方法：
  - 在接口视图下设置接口的Cost值
  - 在系统视图下设置ISIS实例下所有接口Cost值
  - 在系统视图下根据带宽自动计算Cost值

## ISIS规划(3)

- **可靠性规划**
- ISIS快速收敛设计
  - BFD For ISIS：链路故障快速检测
  - ISPF(Incremental SPF)：加快路由收敛（缺省支持）
  - PRC(Partial Route Calculation)：加快路由收敛（缺省支持）
  - LSP Fast Flooding：加快LSDB同步
  - 智能定时器：加快路由收敛，增强网络稳定性

| 定时器参数                                           | 参考值      |
|-------------------------------------------------|----------|
| Hello interval                                  | 缺省值      |
| Dead interval                                   | 缺省值      |
| BFD For ISIS                                    | 缺省值      |
| Fast Flooding                                   | 缺省值      |
| Timer spf { max   init   increment }            | 1 50 100 |
| Timer lsp-generation { max   init   increment } | 2 50 100 |

## ISIS规划(4)

- **安全性规划**
  - ISIS支持三种认证方式：接口认证；区域认证；域认证；
  - 上述三种认证都支持简单密码和高密的MD5方式认证。高密的MD5认证方式具有更高的安全性，推荐高密的MD5。
- **ISIS 快速收敛特性建议全部部署**

## ISIS规划(5)

- 现网配置

```
isis 1
is-level level-2
cost-style wide
circuit-cost 100000 level-2
network-entity 86.4680.0551.0611.3313.7003.00
is-name 城市-机房-设备名-网络类型.设备类型
preference 155
log-peer-change
maximum load-balancing 16
timer lsp-max-age 65500
timer lsp-refresh 32768
#
ipv6 enable topology ipv6
ipv6 preference 155
ipv6 maximum load-balancing 16
ipv6 circuit-cost 100000
#
```

```
interface GigabitEthernet1/0/0
description uT:城市名-机房名-网元名-序列号.网络.
设备型号:端口号
undo shutdown
ipv6 enable
ip address X.X.X X.X.X.X
ipv6 address XXXX:X:XXXX:XXXX::X/127
ipv6 address auto link-local
isis enable 1
isis ipv6 enable 1
isis circuit-type p2p
isis circuit-level level-2
isis ipv6 cost 3000 level-2
isis cost 3000 level-2
isis small-hello
```

- ISIS 快速收敛特性建议全部部署



## 本章总结

- ISIS高级特性
- ISISv6基本原理与配置
- 双栈ISIS应用案例