

ICS 33.040.40

L 78

**YD**

# 中华人民共和国通信行业标准

YD/T 2901-2015

---

## 跨机框信息同步通信协议 (ICCP) 技术要求

Technical specification for Inter-  
Chassis communication protocol

2015-07-14 发布

2015-10-01 实施

---

中华人民共和国工业和信息化部 发布



## 目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	1
4 参考模型和需求	2
4.1 节点冗余保护参考模型	2
4.2 跨机框通信协议需求	3
5 LDP 协议扩展说明	3
5.1 层级说明	3
5.2 LDP ICCP 能力通告	3
5.3 RG 成员管理	4
5.4 冗余对象标识	5
5.5 应用连接管理	5
6 ICCP PE 节点故障检测机制	6
7 ICCP 消息格式	6
7.1 ICC 编码	6
7.2 RG 连接消息	7
7.3 RG 连接断开消息	8
7.4 RG 通告消息	9
7.5 RG 应用数据消息	10
8 应用扩展 TLVs	11
8.1 PW-RED 连接 TLV	11
8.2 多机框 LACP (Multi-chassis LACP、mLACP) 应用 TLVs	15
9 LDP ICCP 能力协商 TLV	22
10 客户应用	22
10.1 PW 冗余应用处理过程	22
10.2 接入链路冗余应用处理过程	23
附录 A(资料性附录) 多机框 MSP 的应用	28
参考文献	35

## 前 言

本标准按照 GB/T1.1-2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中兴通信股份有限公司、中国移动通信集团公司。

本标准主要起草人：马玉霞 魏月华 陈 然 黄 璐。



# 跨机框信息同步通信协议（ICCP）技术要求

## 1 范围

本标准规定了跨机架信息同步通信协议（ICCP）技术要求，包括参考模型、协议需求、协议实体、协议格式以及客户应用方式。

本标准适用于利用 ICCP 实现的双归场景。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

IETF RFC4447 使用 LDP 的伪线设置和维护（Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)）

IETF RFC5036 LDP 说明（LDP Specification）

IEEE802.1AX-2008 IEEE 局域网和城域网标准：链路聚合（IEEE Standard for Local and Metropolitan Area Networks - Link Aggregation）

## 3 术语、定义和缩略语

### 3.1 术语和定义

下面术语和定义适用于本文件。

#### 3.1.1

**冗余组 Redundancy Group**

同一管理域内的 2 个或多个 PE 节点组成一个冗余组（Redundancy Group, RG），针对特定业务实例，采用冗余机制进行保护。

#### 3.1.2

**冗余对象 Redundancy Object**

冗余组保护的對象，可以是链路，端口，转发结构等通用对象。

#### 3.1.3

**跨机框通信协议 Inter-Chassis Communication Protocol**

一种完成冗余组内 PE 之间的通信，同步配置和运行状态数据的协议。

### 3.2 缩略语

下列缩略语适用于本文件。

AC	Attachment Circuit	接入电路
APS	Associated Control Channel	随路控制信道
CE	Customer Edge	用户边缘设备
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线路接入复用器

LACP	Link Aggregation Control Protocol	链路汇聚控制协议
ICCP	Inter-Chassiscommunication protocol	跨机框通信协议
LDP	Label Distribution Protocol	标签分发协议
L2VPN	Layer 2 Virtual Private Networks	二层虚拟专用网
MPLS	Multi-Protocol Label Switching	多协议标签交换
MSP	multiplex section Protection	复用段保护
NAK	Negative Acknowlegment	否定应答
PE	Provider Edge	运营商边缘设备
PW	Pseudo-Wire	伪线
RG	Redundancy Group	冗余组
RO	Redundant Object	冗余对象
ROID	Redundant Object Identity	冗余对象标识
SDH	Synchronous Digital Hierarchy	同步数字体系
SONET	Synchronous Optical Network	同步光纤网
TLV	Type-Length-Value	类型-长度-值
VPN	Virtual Private Network	虚拟专用网

## 4 参考模型和需求

### 4.1 节点冗余保护参考模型

网络的高可用性对任何承载网以及应用 VPN 的网络来说都是关键指标。一般采用机框内或跨机框的冗余保护机制实现。本标准针对跨机框场景，即 PE 节点冗余。假设同一管理域内的 2 个或多个 PE 节点组成一个冗余组（Redundancy Group, RG），针对特定业务实例，面向接入（接入链路、接入伪线等）和/或核心（伪线等）采用冗余机制进行保护。冗余组内的 PE 提供多归连接到任意单个设备（比如 CE, DSLAM 等）或者整个网络（比如接入网络）。

图 1 为通用多归冗余模型。

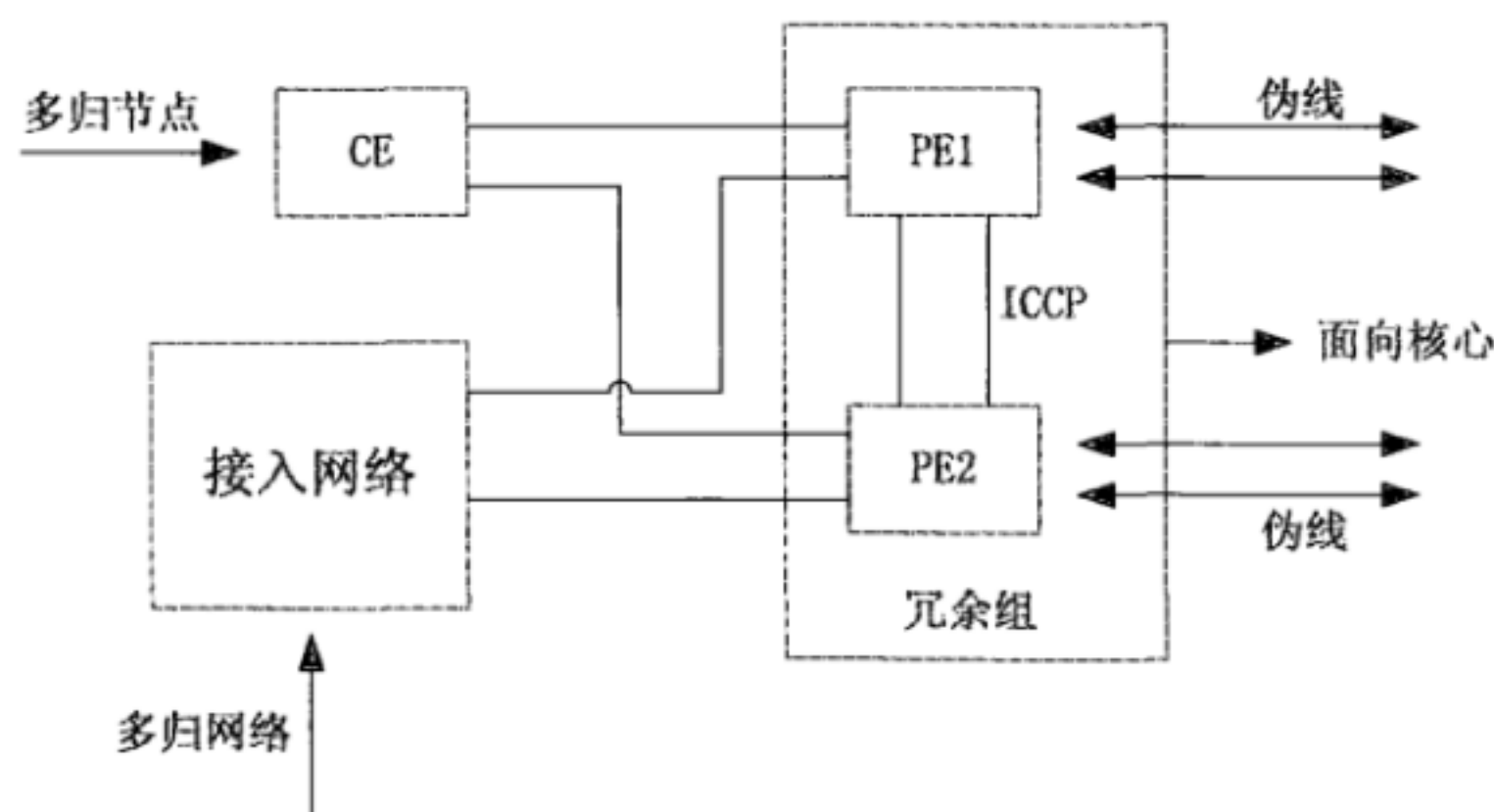


图 1 通用多归冗余模型

在图 1 的拓扑中，面向接入节点/网络采用的冗余机制可以是多种技术，比如伪线冗余组（采用 PW redundancy 控制协议），IEEE 802.1AX 链路聚合组（采用 LACP 控制协议）、SONET/SDH APS 等。为

了保证接入冗余机制运行正常，RG 内的 PE 之间需要通信，即它们之间需要运行跨机框通信协议来同步配置和运行状态数据。如果 PEs 面向核心侧采用伪线冗余保护机制，跨机框通信协议可以简化它的实现。需要说明的是，面向接入或核心所采用的具体技术不在本标准定义范围之内，而且本标准也不会影响其技术机制。

跨机框通信协议消息在冗余组内 PE 之间传送。同一冗余组内的 PE 可能处于相同地理位置或者分布于不同的地理位置，它们之间的连接可能是专用背靠背链路，也可能是穿过分组交换网络的共享连接。不管 PE 之间采用何种连接方式，只要提供通道供跨机框通信协议消息传递，那么跨机框通信协议对其实现方式没有要求。

## 4.2 跨机框通信协议需求

跨机框通信协议需要满足如下需求：

- ICCP 应为冗余组内的 PEs 通信提供控制通道；
- 应适用于多种客户应用（比如多机框 LACP、PW 冗余、多机框 MSP 等）。这意味着消息要支持扩展（比如基于 TLV）。
- 协议具有安全认证机制，应提供冗余组内的节点之间可靠的信息传送和有序传递。
- 应提供通用机制来监测冗余组内的 PE 的状态。该机制用于检测 PE 节点是否故障，并通知客户应用。客户应用根据 AC 与 PW 所采用的冗余协议来触发保护倒换。为了给客户应用提供足够的反应时间从而达到次秒级业务恢复时间，要求远端节点的故障检测时间是次秒级别的。
- 应提供异步的事件驱动状态更新，独立于周期消息，是基于客户应用状态变化的快速通知。换句话说，携带应用数据的消息应按需发送，而不是基于定时器发送，从而最小化机框之间的状态同步延时。
- 应适用于多链路多跳的节点互连。当冗余组内的设备安置在不同的地理位置时，它们之间的连接由网络构成而非直连链路。因此，ICCP 需适用于多跳的应用场景。另外，设备之间也可能存在多（冗余）路径或连接，ICCP 也需要适用于此情况。
- 应保证冗余组内设备间通信安全。当冗余组的节点处于不同地理位置，并由共享网络连接时，这一点尤其重要。
- 应允许运营商静态配置冗余组成员；
- 应允许灵活的冗余组成员关系。虽然每个冗余组包含 2 个节点，可以覆盖大部分冗余应用场景，但 ICCP 不应排除支持一个冗余组内多于 2 个节点。而且允许一个节点同时是多个 RG 的成员。

## 5 LDP 协议扩展说明

### 5.1 层级说明

为了满足上述需求，ICCP 模型包含以下三层。

- 应用层：为使用 ICCP 的不同冗余应用提供接口。ICCP 仅考虑定义通用连接管理过程和本层交换的消息格式。除此之外，它对客户的处理过程和状态机没有任何限制。
- 跨机框通信协议（Inter Chassis Communication protocol, ICCP）层：该层向客户应用提供 ICCP 的公共服务集。它处理协议版本管理、RG 成员、冗余对象标识、PE 节点标识和 ICCP 连接管理。
- 传输层：该层提供 ICCP 消息的传输。它负责寻址、路由解析、流控、可靠有序的消息传递、连接的弹性/冗余和 PE 节点的错误检测。互连链路的物理层不同，传输层可能不同。

### 5.2 LDP ICCP 能力通告



当一个 PE 设备配置了冗余组，如果它支持 ICCP 功能，则需要将这种能力通告给 RG 中其他 LDP 对等体（携带 ICCP LDP capability TLV 的 LDP 消息）。如果其他 LDP 对等体支持动态能力通告，需要发送一个新的能力通告消息。能力通告消息中携带了 ICCP capability TLV 中的 S 标志位置位，否则应在 LDP 的初始化消息中携带 ICCP LDP capability TLV，该过程与 IETF RFC5561 过程相同。

### 5.3 RG 成员管理

ICCP 提供一种 PE 节点管理 RG 成员的机制。当 PE 配置为 RG 成员时，它首先通告 ICCP 能力给对等体。接下来，PE 发送一个 RG 连接消息给已经通告有 ICCP 能力的对等体，然后 PE 等待对等体发送 RG 连接消息。对于一个 RG，只有当双方都发送和接收了 ICCP RG 连接消息后，两个设备之间的 ICCP 连接才被认为可以操作。

如果 PE 已经发送了 RG 连接消息却没有从对方接收到相应的 RG 连接（或者拒绝连接通知）消息，它将维持在等待回应 RG 连接消息（或通知消息）状态，直到接收到相应的 RG 连接消息后，RG 才可操作。如果 PE 接收到拒绝连接通知消息，它将立即停止建立 ICCP 连接。PE 从对等体接收到 RG 连接消息后，应重新建立连接，回应对方。

如果下列条件之一满足，那么设备应发送拒绝连接消息：

- PE 不是 RG 成员；
- 同时建立的 ICCP 连接数量已经超过 PE 能处理的最大值。

PE 发送 RG 连接断开消息结束 ICCP 连接。这是一个单方行为，不需要对方的任何回应。

ICCP 连接状态机有 6 个状态，ICCP 连接状态转换见表 1。

表 1 ICCP 连接状态转换

状态	触发事件	新状态
NON EXISTENT	LDP session 建立	INITIALIZED
INITIALIZED	发送LDP ICCP 能力	CAPSENT
	接收 LDP ICCP 能力 (动作: 发送LDP ICCP 能力)	CAPREC
	LDP session 断开	NON EXISTENT
CAPSENT	接收 LDP ICCP 能力	CAPREC
	LDP session 断开	NON EXISTENT
CAPREC	发送 RG 连接消息	CONNECTING
	接收可接受的RG 连接消息 (动作: 发送 RG 连接消息)	OPERATIONAL
	接收任何其他ICCP 消息 (动作: 发送NAK TLV 在RG通告消息)	CAPREC
	LDP session 断开	NON EXISTENT
CONNECTING	接收可接受的RG 连接消息	OPERATIONAL
	接收任何其他ICCP 消息 (动作: 发送NAK TLV在RG通告消息)	CAPREC
	LDP session 断开	NON EXISTENT
OPERATIONAL	接收可接受的RG 断开消息	CAPREC
	发送 RG 连接断开消息	CAPREC
	LDP session 断开	NON EXISTENT

## 5.4 冗余对象标识

ICCP 给客户应用提供了标识冗余保护对象，即链路、端口、转发结构和更多通用对象（比如接口、伪线、VLANs 等）的统一机制。这些统称为冗余对象（Redundant Objects、RO）。ICCP 引入一个 64 比特标识来唯一标识 RG 中的 ROs。这个标识称为冗余 ID（Redundant Object ID、ROID），RG 成员之间被保护对象应匹配。

## 5.5 应用连接管理

ICCP 发送应用相关的连接 TLV（承载在 RG 连接消息中）给 RG 内每个对端 PE。携带的信息用于在建立真正的应用连接之前的参数或属性协商。建立应用连接的过程和 ICCP 连接相似，只有当双方都发送和接收到携带适当的应用相关连接 TLVs 的 RG 连接消息，两个节点之间的应用连接才算建立。

如果下列情形之一发生，那么 PE 应发送拒绝连接通知消息，拒绝应用连接请求包括：

- 应用不存在或者在 RG 没有配置；
- 应用连接数量超过 PE 的处理能力。

当 PE 接收到拒绝连接通知，它应停止建立应用连接，直到从对端 PE 接收到新的应用连接请求。

当节点上某个应用停止或它不再与某个 RG 关联，那么该节点应发送携带应用相关的连接，断开 TLV 的 RG 连接，断开连接消息给对方 PE。这是一个单向通知，不需要对方回应。

在应用连接建立期间，PE 可以和对方 PE 协商应用版本，如果没有达成一致，那么应用连接建立失败。支持的版本不一致时，可以采用后向兼容或不兼容方式。

应用连接状态机有 6 个状态，应用连接状态转换见表 2。

表 2 应用连接状态转换

STATE	EVENT	NEW STATE
NON EXISTENT	ICCP 连接建立	RESET
RESET	ICCP 连接断开	NON EXISTENT
	发送应用连接TLV	CONNSSENT
	接收应用连接TLV	CONNREC
	接收任何其他应用TLV (动作: 发送NAK TLV)	RESET
CONNSSENT	接收 NAK TLV	RESET
	接收应用连接TLV, 且A-bit=1 (动作: 发送应用连接TLV, 且 A-bit=1)	OPERATIONAL
	接收任何其他应用TLV (动作: 发送 NAK TLV)	RESET
	ICCP 连接断开	NON EXISTENT
CONNREC	发送 NAK TLV	RESET
	发送应用连接TLV, 且A-bit=1	CONNECTING
	接收任何应用TLV, 除了连接TLV (动作: 发送NAK TLV)	RESET
	ICCP 连接断开	NON EXISTENT
CONNECTING	接收应用连接 TLV 且 A-bit=1	OPERATIONAL
	接收任何其他应用TLV (动作: 发送 NAK TLV)	RESET
	ICCP 连接断开	NON EXISTENT

表 2（续）

STATE	EVENT	NEW STATE
OPERATIONAL	接收应用断开TLV	RESET
	发送应用断开TLV	RESET
	ICCP 连接断开	NON EXISTENT

6 ICCP PE 节点故障检测机制

当 RG 成员的对端 PE 节点不可达时，客户应根据 AC 或 PW 的冗余协议触发保护倒换。ICCP 本身并不定义保活机制监测对端 PE 节点的状态，需重用现有的故障检测机制，如 BFD、IP 可达性监测以及其他 OAM 机制等。需要说明的是，LDP 会话丢失不能作为对端 PE 失效的可靠指示。比如：可能是对端 PE 遇到本地问题导致重新启动 LDP 会话，而 PE 节点仍然可以进行业务转发。

7 ICCP 消息格式

7.1 ICC 编码

7.1.1 概述

LDP 协议提供的可靠、有序、状态完整的消息传递，节点间的能力协商等属性，而这些也是 ICCP 所需的。因此，ICCP 利用现有的 LDP 协议架构。IETF RFC5036 定义了通用 LDP 消息结构，ICCP 定义了一系列新的 LDP 消息类型来传递 ICCP 信息。所使用的 LDP 消息类型范围是 0x700 到 0x07F。

7.1.2 ICC header

每个 ICCP 消息由 ICC LDP Header、后面跟着的消息 data 组成。ICC Header 的格式见表 3。

表 3 ICC Header 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
U	Message Type															Message Length																
Message ID																																
Type=0x0005 (ICC RG ID)																Length=4																
ICC RG ID																																
<div>.....</div> <div>Mandatory ICC Parameters</div> <div>.....</div>																																
<div>.....</div> <div>Optional ICC Parameters</div> <div>.....</div>																																

各个字段含义如下：

- U-bit，未知消息比特。接收到的未知消息，如果 U 置 0，那么需要回复通知消息给初始发送者；如果 U 置 1，那么忽略未知消息。
- Message Type，指示 ICCP 消息类型，应在 0x0700~0x070F 的范围内。
- Message Length，指示消息的字节长度，除了字段 U-bit、Message Type 和 Message Length 的消息字节长度。
- Message ID，消息 ID，对方 PE 发送 RG 通知消息回应这个消息时，应该在通知消息中的“NAK TLV”中包含这个消息 ID；



— ICC RG ID TLV、TLV type 为 0x0005，长度为 4，包含 4 字节 RG ID，用于标识发送者是这个 RG 的成员。

— Mandatory ICC Parameters，可变长度的必选消息参数。一些消息没有必选参数。

— Optional ICC Parameters，可变长度的可选消息参数。一些消息没有可选参数。

### 7.1.3 ICC 参数编码

ICC 参数的通用格式见表 4。

表 4 ICC 参数编码

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type														Length															
..... TLV(s) .....																															

各个字段含义如下：

— U-bit，未知 TLV 比特。接收到的未知 TLV，如果 U 置 0，那么需要回复通知消息给初始发送者，然后整个消息被忽略；如果 U 置 1，忽略未知 TLV，消息的其他部分正常处理就像未知 TLV 不存在一样。

— F-bit，转发未知 TLV 比特。只有当 U-bit 置 1 并且 LDP 消息包含未知 TLV 时，转发 LDP 消息。如果 F 置 0，未知 TLV 不被转发；如果 F 置 1，转发未知 TLV。

— Type，ICC 参数类型。

— Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 的 TLV 字节长度。

— TLV(s)，0 或多个 TLVs，根据消息类型变化。

### 7.1.4 ROID 编码

冗余对象标识 (ROID) 唯一标识一个冗余对象、一个 RG 保护对象（比如链路、聚合组、VLAN 等）。ROID 编码见表 5。

表 5 ROID 编码

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
ROID																															

ROID 是一个 8 字节无符号整数，在相关的 TLVs 中使用。

## 7.2 RG 连接消息

RG 连接消息用来建立 ICCP RG 连接以及同一个 RG 内 PEs 之间单独的应用连接。没有携带应用连接 TLV 的 RG 连接消息只建立 ICCP RG 连接。携带有效应用连接 TLV 的 RG 连接消息，不仅建立应用连接，而且如果 ICCP RG 连接没有建立的话，也同时建立。

PE 向同一个 RG 内的每个 PE 发送 RG 连接消息。哪些 PE 属于同一个 RG 可以由配置或某种自动发现机制来决定。如果一个设备是多个 RGs 的成员，那么 PE 针对每个 RG 都会发送不同的连接消息。

RG 连接消息的格式如下：

— ICC header，消息类型为 "RG 连接消息" (0x0700)；

— ICC Sender Name TLV，包含发送者的主机名字；

- 0 个或 1 个应用相关连接 TLV。
- 应用相关连接 TLVs 有：
- PW 冗余组连接 TLV；
  - mLACP 连接 TLV；
  - MSP 连接 TLV，其具体格式是可选的。

这些 TLVs 的细节见第 8 章，MSP 连接 TLV 相关内容参见附录 A。

7.2.1 ICC Sender Name TLV

带发送者主机名字的 TLV，名字是 UTF-8 编码。它主要用于 RG 管理，易于网络操作，其格式如表 6 所示。

表 6 带发送者主机名字的 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type = 0x0001														Length															
..... 发送者名字 .....																															

- 各个字段取值或含义如下：
- U 及 F 为 0；
  - Type 为 0x0001；
  - Length，除了 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
  - Sender Name，发送者的主机名字，UTF-8 编码，不超过 80 个字符。

7.3 RG 连接断开消息

RG 连接断开消息有两个目的：指示 RG 内某个应用连接关闭或者由于 PE 离开这个 RG，使得 ICCP RG 连接自身断开。RG 连接断开消息格式见表 7。

表 7 RG 连接断开消息格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
U	Message Type=0x0701															Message Length																
Message ID																																
Type=0x0005 (ICC RG ID)															Length=4																	
ICC RG ID																																
Disconnect Code TLV																																
..... Optional Application-specific Disconnect TLV .....																																
..... Optional Parameter TLVs .....																																

- 各个字段取值或含义如下：
- U 为 0；
  - Message Type 为 0x0701；



- Length, TLV 的字节长度, 除了字段 U-bit、Type 和 Length 字段外的 TLV 字节长度;
- Message ID, 见 7.1.1 “ICC header”;
- ICC RG ID, 见 7.1.1 “ICC header”;
- Disconnect Code TLV, 其格式见表 8。

表 8 Disconnect Code TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0004														Length															
ICCP Status Code																															

其中:

- U 及 F 为 0;
- Type 为 0x0004;
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- ICCP Status Code, 指示断开连接消息原因, 当前允许的值有 “ICCP RG Removed ” 和 “ICCP Application Removed from RG” 。

— Optional Application-specific Disconnect TLV, 0 或 1 个应用断开连接 TLV, 将在后面章节定义。如果 RG 断开连接消息的 ICCP Status Code 为 “ICCP RG Removed”, 那么它不能包含任何应用断开连接 TLV, 因为发送端 PE 表明它已经离开 RG, 因此已经断开 ICCP RG 连接和所有关联的应用连接。如果消息的 ICCP Status Code 为 “ICCP Application Removed from RG”, 那么它必须包含一个应用断开连接 TLV, 因为发送端 PE 只断开指定应用的连接。其他应用和 ICCP RG 连接不受影响。

Optional Parameter TLVs, 目前没有定义内容, 待后续扩展。

#### 7.4 RG 通告消息

PE 发送 RG 通告消息指示如下信息之一: 拒绝一个 ICCP 连接; 拒绝一个应用连接; 拒绝整个消息或者拒绝消息内 1 个或多个 TLVs。通告消息只能发送给加入 RG 的 PE。

RG 通告消息应仅用于拒绝一个 ICCP 应用中的消息或者 TLVs。

RG 通告消息限于最多只有一个 ICCP 应用。

RG 通告消息的格式: ”

— ICC header, 消息类型为 “RG 通告消息” (0x0702);

— 通告消息 TLVs。

定义的通告消息 TLVs:

— ICC Sender Name TLV, 见 7.2.1 定义;

— NAK TLV。其格式见表 9。

表 9 NAK TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0002														Length															
ICCP Status Code																															
Rejected Message ID																															
Optional TLV(s)																															
.....																															

其中：

- U 及 F 为 0；
- Type 为 “NAK TLV”（0x0002）；
- Length, TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- ICCP Status Code, ICCP 状态编码，表示 NAK TLV 原因，见表 10。

表 10 ICCP Status Code

状态编码	含义
未知RG (0x00010001)	拒绝一个新接收的RG ICCP连接，但RG并没有在PE配置。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG连接消息的消息ID
ICCP连接数溢出(0x00010002)	拒绝一个新接收的ICCP连接，这个连接将导致PE的ICCP连接数量超过它的处理能力。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG连接消息的消息ID
应用连接数溢出(0x00010003)	拒绝一个新接收的应用连接，这个连接将导致PE的应用连接数量超过它的处理能力。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG连接消息的消息ID以及对应应用连接TLV必须包含在“可选 TLV”字段
应用在RG中不存在(0x00010004)	拒绝一个新的应用连接，当PE不支持此应用或此应用在RG没有配置。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG连接消息的消息ID以及对应应用连接TLV必须包含在“可选 TLV”字段
不兼容的协议版本（0x00010005）	拒绝一个新的应用连接，当PE不兼容应用版本。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG连接消息的消息ID以及对应应用连接TLV必须包含在“可选 TLV”字段
被拒的消息（0x00010006）	拒绝一个RG应用数据消息，或者1个或多个消息内的TLVs。当使用这个编码时，“被拒消息ID”字段必须包含被拒绝的RG应用数据的消息ID
管理不使能ICCP（0x00010007）	拒绝从对方PE接收ICCP消息，由于本地管理策略，对方PE不允许交换ICCP消息

— Rejected Message ID, 被拒消息 ID。如果非 0，表示 NAK TLV 所针对的对方消息。

— Optional TLV(s), 可选 TLV(s)。1 个或多个可选 TLVs。如果状态码是“被拒的消息”，那么这个字段包含被拒的 TLVs。如果整个消息被拒，就应包含消息中所有的 TLV。如果状态码是“不兼容的协议版本”，那么这个字段包含对方发送的“应用连接 TLV”以及下面定义的“请求的协议版本 TLV”，其格式如表 11 所示。

表 11 请求的协议版本 TLV

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0003														Length															
Connection Reference																Requested Version															

其中：

- U 及 F 为 0；
- Type 为 0x0003，表示请求的协议版本 TLV；
- Length, TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Connection Reference, 设置为被拒的应用连接 TLV 的类型字段；
- Requested Version, 发送设备支持的应用版本。

7.5 RG 应用数据消息

RG 应用数据消息用来在同一个 RG 内的 PEs 之间传输应用数据。一个消息只能为一种应用携带数

据，可以携带同一应用的多个应用 TLV。应用数据消息的格式如下：

- ICC header，包含 Message type 为"RG 应用数据消息" (0x703)；
- 应用相关 TLVs。

这些 TLVs 的细节将在第 8 章讨论。一个 RG 应用数据消息内的所有应用 TLVs 应属于同一个应用，但可能涉及不同的冗余对象。

8 应用扩展 TLVs

8.1 PW-RED 连接 TLV

8.1.1 PW-RED 连接 TLV

这个 TLV 承载在 RG 连接消息中，指示 PW-RED 应用连接的建立。PW-RED 连接 TLV 格式如表 12 所示。

表 12 PW-RED 连接 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
U	F	Type=0x0010														Length																
Protocol Version																A	Reserved															
..... Optional Sub-TLVs .....																																

其中：

- U 及 F 为 0；
- Type 为 0x0010，表示 PW-RED 连接 TLV；
- Length，TLV 的字节长度，除了字段 U-bit, F-bit, Type 和 Length 字段外的 TLV 字节长度；
- Protocol Version，协议版本号；
- A-bit，如果发送端已经从接收端接收到 PW-RED 连接 TLV，那么设置为 1，否则设置为 0；
- Reserved，保留字段；
- Optional Sub-TLVs，可选子 TLVs，当前版本没有定义。

8.1.2 PW-RED 连接断开 TLV

这个 TLV 承载在 RG 连接断开消息中，表示要终止 PW-RED 应用的连接。PW-RED 连接断开 TLV 格式如表 13 所示。

表 13 PW-RED 连接断开 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0011														Length															
Optional Sub-TLVs																															

其中：

- U 及 F 为 0；
- Type 为 0x0011，表示 PW-RED 连接断开 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Optional Sub-TLVs，可选子 TLVs，目前版本定义的可选子 TLV 是“PW-RED 连接断开原因



TLV”，其格式如表 14 所示。

表 14 PW-RED 连接断开原因 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0019														Length															
..... Disconnect Cause String .....																															

其中：

- U 及 F 为 0；
- Type 为 0x0019，表示 PW-RED 连接断开原因 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Disconnect Cause String，可变长度的字符串，指明断开连接的原因。

8.1.3 PW-RED 配置 TLV

PW-RED 配置 TLV 承载在 RG 应用数据消息中，其格式见表 15。

表 15 PW-RED 配置 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0012														Length															
ROID																															
PW Priority																Flags															
Service Name TLV																															
PW ID TLV or Generalized PW ID TLV																															

其中：

- U 及 F 为 0；
- Type 为 0x0012，表示 PW-RED 配置 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- ROID，见“7.1.4 ROID 编码”；
- PW Priority，伪线优先级，用于比较哪个 PW 有更高优先级进入工作状态。数值越小，优先级越高；值相同，那么 ID（如 IP 地址）数值更小的 PE 有更高的优先级；
- Flags，有效值范围和说明，详见表 16。

表 16 有效值范围和说明

有效值	说明
同步 (0x01)	发生端已经结束一业务的PW配置传送
清除配置 (0x02)	PW不再参与PW冗余操作
独立模式 (0x04)	PW冗余机制采用独立操作模式
独立模式以及请求切换 (0x08)	PW冗余机制采用独立操作模式，同时“请求切换”
主用模式 (0x10)	PW冗余机制采用主用/备用模式，同时表明PE作为主用
备用模式 (0x20)	PW冗余机制采用主用/备用模式，同时表明PE作为备用

— Service Name TLV, 业务名字 TLV, 其格式见表 17。

表 17 业务名字 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0013														Length															
..... Service Name .....																															

其中:

- U 及 F 为 0;
- Type 为 0x0012, 表示业务名字 TLV;
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- Service Name, 业务名字, L2VPN 业务实例名字, UTF-8 格式编码, 不超过 80 字符。
- PW ID TLV, 其格式见表 18。

表 18 PW ID TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0014														Length															
Peer ID																															
Group ID																															
PW ID																															

其中:

- U 及 F 为 0;
- Type 为 0x0014, 表示 PW ID TLV;
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- Peer ID, PW 远端设备的 LDP Router ID。
- Group ID, 见 IETF RFC4447 定义。
- PW ID, 见 IETF RFC4447 定义。

#### 8.1.4 PW-RED 状态 TLV

PW-RED 状态 TLV 承载在 RG 应用数据消息中, 用来向同一个 RG 中的其他成员通告自己的 PW 状态。它的 TLV 格式见表 19。

表 19 PW-RED 状态 TL 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0016														Length															
ROID																															
Local PW State																															
Remote PW State																															

其中:

- U 及 F 为 0;
- Type 为 0x0016, 表示 PW-RED 状态 TLV;

- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- ROID, 见“7.1.4 ROID 编码”;
- Local PW State, 本地 PW 状态;
- Remote PW State, 远端 PW 状态。

8.1.5 PW-RED 同步请求 TLV

PW-RED 同步请求 TLV 承载在 RG 应用数据消息中, 用来请求对端 PE 重新发送配置或操作状态。请求信息包括下列内容:

- 一个或多个 PW 的配置和/或状态;
- 所有 PW 的配置和/或状态;
- 某个业务的所有 PW 的配置和/或状态。

PW-RED 同步请求 TLV 的格式见表 20。

表 20 PW-RED 同步请求 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0017														Length															
Request Number																C	S	Request Type													
Optional Sub-TLVs																															

其中:

- U 及 F 为 0。
- Type 为 0x0017, 表示 PW-RED 同步请求 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Request Number, 请求编号, 回复与请求匹配。
- C Bit, 设置为 1 表明请求配置数据, 否则设置为 0。
- S Bit, 设置为 1 表明请求运行状态数据, 否则设置为 0。
- Request Type, 取值如下:
  - 0x00: 请求某伪线的数据;
  - 0x01: 请求某业务的所有伪线数据;
  - 0x3FFF: 请求所有数据。
- Optional Sub-TLVs:

零或多个 TLV(s), 如果 Request Type 设置为 0x00, 那么这个字段包含一或多个 PW ID TLV(s), 或 GeneralizedPW ID TLV(s); 如果请求类型字段设置为 0x01, 那么这个字段包含一或多个 Service Name TLV(s); 如果 Request Type 设置为 0x3FFF, 那么这个字段应为空。

8.1.6 PW-RED 同步数据 TLV

PW-RED 同步数据 TLV 承载在 RG 应用数据消息。设备用一对 TLVs 给一系列回复 PW-RED 同步请求 TLV 的 TLVs 定界。定界 TLVs 表示同步数据的开始和结束, 并且通过请求编号字段将回复和请求对应。PW-RED 同步数据 TLV 也用于主动通告 PW-RED 配置和操作状态。这种情况下, 请求编号字段设置为 0。

PW-RED 同步数据 TLV 格式见表 21。

表 21 PW-RED 同步数据 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0018														Length															
Request Number																Flags															

其中：

- U 及 F 为 0；
- Type 为 0x0018，表示 PW-RED 同步数据 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Request Number，与“PW-RED 同步请求 TLV”匹配；
- Flags，取值范围：
  - 0x00：同步数据开始；
  - 0x01：同步数据结束。

8.2 多机框 LACP (Multi-chassis LACP, mLACP) 应用 TLVs

8.2.1 mLACP 连接 TLV

mLACP 连接 TLV 承载在 RG 连接消息中，表明 mLACP 应用连接的建立。mLACP 连接 TLV 格式见表 22。

表 22 mLACP 连接 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0030														Length															
Protocol Version																A	Reserved														
..... Optional Sub-TLVs .....																															

其中：

- U 及 F 为 0；
- Type 为 0x0030，表示 mLACP 连接 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Protocol Version，协议针对 ICCP 的版本；
- A-bit，如果发送端已经从接收端接收到 mLACP 连接 TLV，那么设置为 1，否则设置为 0；
- Reserved，保留字段；
- Optional Sub-TLVs，可选子 TLVs，当前版本没有定义。

8.2.2 mLACP 连接断开 TLV

这个 TLV 承载在 RG 连接断开消息中，表示要终止 mLACP 应用的连接。mLACP 连接断开 TLV 格式见表 23。

表 23 mLACP 连接断开 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0031														Length															
Optional Sub-TLVs																															



其中：

- U 及 F 为 0；
  - Type 为 0x0031，表示 mLACP 连接断开 TLV；
  - Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
  - Optional Sub-TLVs，可选子 TLVs，目前版本定义的可选子 TLV 是“mLACP 连接断开原因 TLV”。
- mLACP 连接断开原因 TLV 格式见表 24。

表 24 mLACP 连接断开原因 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x003A														Length															
..... Disconnect Cause String .....																															

- U 及 F 为 0。— Type 为 0x003A，表示 mLACP 连接断开原因 TLV。
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Disconnect Cause String，可变长度的字符串，指明断开连接的原因。

8.2.3 mLACP 系统配置 TLV

mLACP 系统配置 TLV 承载在 RG 应用数据消息中。这个 TLV 用于通告本地节点的 LACP 系统参数给 RG 对端。mLACP 系统配置 TLV 格式见表 25。

表 25 mLACP 系统配置 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x0032														Length															
System ID																System Priority															
Node ID																															

其中：

- U 及 F 为 0。
- Type=0x0032，表示 mLACP 系统配置 TLV。
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- System ID，LACP 使用的 System ID，见 IEEE802.1AX-2008 5.3.2 节定义。
- System Priority，LACP 系统优先级，见 IEEE802.1AX-2008 5.3.2 节 LACP System Priority 定义。
- Node ID，LACP 节点 ID，用来保证 RG 内所有设备的 LACP 接口号唯一。有效值范围 0~7。RG 成员的 LACP 端口号唯一性通过如下编码方式保证：最高位比特永远设置为 1，接下来的 3 位比特设置为 Node ID，剩下的 12bit 由系统设置。

8.2.4 mLACP 聚合器配置 TLV

mLACP 聚合器配置 TLV 承载在 RG 应用数据消息中。这个 TLV 用于通告聚合器的本地配置状态给 RG 对端。mLACP 聚合器配置 TLV 格式见表 26。



表 26 mLACP 聚合器配置 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0036														Length															
ROID																															
Aggregator ID																MAC Address															
Actor Key																Member Ports Priority															
Flags								Agg Name Len								Aggregator Name															

其中:

- U 及 F 为 0;
- Type 为 0x0036, 表示 mLACP 聚合器配置 TLV;
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- ROID, 见“7.1.4ROID 编码”;
- Aggregator ID, LACP 聚合器 ID, 见 IEEE802.1AX-2008 5.4.6 节定义;
- MAC Address, 聚合器 MAC 地址;
- Actor Key, 聚合器的 LACP Actor Key, 见 IEEE802.1AX-2008 5.3.5 节定义;
- Member Ports Priority, 聚合器的接口的 LACP 管理端口优先级。这个字段只在“Flags”字段设置为“Priority Set”时有效;
- Flags, 有效值范围, 详见表 27。

表 27 有效值范围

有效值	说明
0x01, 同步 (Synchronized)	发送方已经发送所有聚合器配置信息
0x02, 清除配置(Purge Configuration)	聚合器不再配置进行mLACP操作
0x04, 优先级设置 (Priority Set)	指示“Member Ports Priority”字段有效

- Agg Name Len, “Aggregator Name”字段的字节长度;
- Aggregator Name, 聚合器名字, UTF-8 格式, 最大 20 字符。

### 8.2.5 mLACP 端口配置 TLV

mLACP 端口配置 TLV 承载在 RG 应用数据消息中。这个 TLV 通告端口的本地配置状态给 RG 对端。mLACP 端口配置 TLV 格式见表 28。

表 28 mLACP 端口配置 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0033														Length															
Port Number																MAC Address															
Actor Key																Port Priority															
Port Speed																															
Flags								Port Name Len								Port Name															

其中：

- U 及 F 为 0。
- Type 为 0x0033，表示 mLACP 端口配置 TLV。
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Port Number，LACP 端口号，定义见 IEEE802.1AX-2008 5.3.4 节。端口号和节点 ID 一起编码，见 8.2.3 节说明。
- MAC Address，端口 MAC 地址。
- Actor Key，接口的 LACP Actor Key，定义见 IEEE802.1AX-2008 5.3.5 节。
- Port Priority，接口的 LACP 管理端口优先级，定义见 IEEE802.1AX-2008 5.3.4 节。这个字段只在“Flags”字段设置为“Priority Set”时有效。
- Port Speed，端口的当前带宽，单位是 1Mbit/s。
- Flags，有效值范围，详见表 29。

表 29 有效值范围

有效值	说明
0x01，同步（Synchronized）	发送方已经发送聚合器的所有成员链路的端口配置信息
0x02，清除配置(Purge Configuration)	端口不再配置进行mLACP操作
0x04，优先级设置（Priority Set）	指示“Port Priority”字段有效

- Port Name Len，“Port Name”字段的字节长度；
- Port Name，端口名字，UTF-8 格式，最大 20 个字符。

8.2.6 mLACP 端口优先级 TLV

mLACP 端口优先级 TLV 承载在 RG 应用数据消息中。设备用其发布可操作端口优先级给 RG 内其他成员；或者命令式地请求 RG 的某个成员改变它的端口优先级。mLACP 端口优先级 TLV 格式见表 30。

表 30 mLACP 端口优先级 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0034														Length															
OpCode																Port Number															
Aggregator ID																Last Port Priority															
Current Port Priority																															

其中：

- U 及 F 为 0。
- Type 为 0x0034，表示 mLACP 端口优先级 TLV。
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- OpCode，TLV 的操作码，取值如下：
  - 0x00 —— 本地优先级变化通知；
  - 0x01 —— 远端请求优先级变化。
- Port Number，LACP 端口号，定义见[IEEE-802.1AX] 5.3.4 节。这个字段设置为 0，表示与聚合器绑定的所有端口；当设置为非 0 时，端口号和节点 ID 一起编码，见 8.2.3 节说明。
- Aggregator ID，LACP 聚合器 ID，定义见 IEEE802.1AX-2008 5.4.6 节。

— Last Port Priority, 接口的 LACP 端口优先级, 定义见 IEEE802.1AX-2008 5.3.4 节。如果是本地端口, 那么这个字段是之前的端口优先级操作值; 如果是远端端口, 这个字段是通过从 RG 中的对端节点最后获知的 PE 的端口优先级操作值。

— Current Port Priority, 接口的 LACP 端口优先级, 定义见 IEEE802.1AX-2008 5.3.4 节。如果是本地接口, 这个字段是 PE 通告的最新的端口优先级操作值; 如果是远端端口, 这个字段是 PE 请求的最新的端口优先级。

8.2.7 mLACP 端口状态 TLV

mLACP 端口状态 TLV 承载在 RG 应用数据消息中。用来向 RG 中的成员报告自己的 LACP 端口状态。mLACP 端口状态 TLV 格式见表 31。

表 31 mLACP 端口状态 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0035														Length															
Partner System ID																															
Partner System Priority																															
Partner Port Number																															
Partner Port Priority																															
Partner Key																Partner State								Actor State							
Actor Port Number																Actor Key															
Selected								Port State								Aggregator ID															

其中:

- U 及 F 为 0。
- Type 为 0x0035, 表示 mLACP 端口状态 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- Partner System ID, 接口的 LACP Partner 系统 ID, 编码为 MAC 地址, 具体说明见 IEEE 802.1AX-2008 5.4.2.2 节。
- Partner System Priority, LACP Partner 系统优先级, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Partner Port Number, LACP Partner 端口号, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。端口号和节点 ID 一起编码, 见 8.2.3 节说明。
- Partner Port Priority, LACP Partner 端口优先级, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Partner Key, LACP Partner Key, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Partner State, LACP Partner State, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Actor State, 端口的 LACP Actor's State, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Actor Port Number, LACP Actor 端口号, 具体说明见 IEEE802.1AX-2008 5.3.4 节。端口号和节点 ID 一起编码, 见 8.2.3 节说明。
- Actor Key、LACP Actor Key, 具体说明见 IEEE802.1AX-2008 5.3.5 节。
- Selected, 具体说明见 IEEE802.1AX-2008 5.4.8 节, 取值范围如下:
  - 0x00: SELECTED;
  - 0x01: UNSELECTED;
  - 0x02: STANDBY。



- Port State, 端口的操作状态, 取值范围如下:
- 0x00: Up;
- 0x01: Down;
- 0x02: Administrative Down;
- 0x03: Test。
- Aggregator ID, 端口绑定的 LACP 聚合器 ID。

8.2.8 mLACP 聚合器状态 TLV

mLACP 聚合器状态 TLV 承载在 RG 应用数据消息中, 用来向 RG 中的成员通告自己的 LACP 聚合器状态。mLACP 聚合器状态 TLV 格式见表 32。

表 32 mLACP 聚合器状态 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0037														Length															
Partner System ID																Partner System Priority															
Partner Key																															
Actor Key																Agg State															

其中:

- U 及 F 为 0。
- Type 为 0x0037, 表示 mLACP 聚合器状态 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
- Partner System ID, 接口的 LACP Partner 系统 ID, 编码为 MAC 地址, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Partner System Priority, LACP Partner 系统优先级, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Partner Key, LACP Partner Key, 具体说明见 IEEE802.1AX-2008 5.4.2.2 节。
- Aggregator ID, LACP Aggregator ID, 具体说明见 IEEE802.1AX-2008 5.4.6 节。
- Actor Key, LACP Actor Key, 具体说明见 IEEE802.1AX-2008 5.3.5 节。
- Agg State, 聚合器的操作状态, 取值范围如下:
  - 0x00——Up;
  - 0x01——Down;
  - 0x02——Administrative Down;
  - 0x03——Test 。

8.2.9 mLACP 同步请求 TLV

mLACP 同步请求 TLV 承载在 RG 应用数据消息中, 用来请求对端重新发送配置或操作状态, 请求信息包括下列内容:

- 系统配置和/或状态;
- 某个端口的配置和/或状态;
- 具有某个 LACP key 的所有端口的配置和/或状态;
- 所有 mLACP 端口的配置和/或状态;

- 某个聚合器的配置和/或状态;
- 具有某个 LACP key 的所有聚合器的配置和/或状态;
- 所有 mLACP 聚合器的配置和/或状态。

mLACP 同步请求 TLV 的格式见表 33。

表 33 mLACP 同步请求 TLV 格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0038														Length															
Request Number																C	S	Request Type													
Port Number / Aggregator ID																Actor Key															

其中:

- U 及 F 为 0。
- Type 为 0x0038, 表示 mLACP 同步请求 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Request Number, 请求编号, 用来确认请求和回复是否一致。
- C Bit, 如果请求配置数据, 设置为 1, 否则设置为 0。
- S Bit, 如果请求运行状态数据, 设置为 1, 否则设置为 0。
- Request Type, 请求类型, 取值如下:
  - 0x00: 请求系统数据;
  - 0x01: 请求聚合器数据;
  - 0x02: 请求端口数据;
  - 0x3FFF: 请求所有数据。

— Port Number / Aggregator ID, 如果请求类型设置为请求端口数据, 那么这个字段设置为 LACP 端口号; 如果请求类型设置为请求聚合器数据, 那么这个字段设置为聚合器 ID; 如果此字段设置为 0, 表示所有端口或聚合器。

— Actor Key, 端口或聚合器的 LACP Actor key。如果设置为 0 (并且 Port Number / Aggregator ID 也设置为 0), 表示请求所有端口或聚合器的信息。

8.2.10 mLACP 同步数据 TLV

mLACP 同步数据 TLV 承载在 RG 应用数据消息中。设备用一对 TLVs 来定界一系列数据 TLVs, 它们是对 mLACP 同步请求 TLV 的回复。定界 TLVs 表示了同步数据的开始和结束, 并且通过 “Request Number” 字段把回复和请求对应起来。

mLACP 同步数据 TLV 同样用于主动通告完整的 mLACP 配置和操作状态数据, 这种情况下, “Request Number” 字段设置为 0。主动同步时, PE 应通告所有系统、聚合器和端口信息, 就像初始化时一样。

mLACP 同步数据 TLV 的格式见表 34。

表 34 mLACP 同步数据 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x0039														Length															
Request Number																Flags															

- 其中：
- U 及 F 为 0。
  - Type 为 0x0039，表示 mLACP 同步数据 TLV。
  - Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
  - Request Number，从“mLACP 同步请求 TLV”获得，确保回复和请求一致。
  - Flags，取值范围如下：
    - 0x00：同步数据开始；
    - 0x01：同步数据结束。

9 LDP ICCP 能力协商 TLV

定义 ICCP 能力协商 TLV 指示 ICCP 能力，其格式见表 35。

表 35 ICCP 能力协商 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	TLV Code Point=0x700														Length															
S	Reserved														VER/Maj								Ver/Min								

- 其中：
- U 为 1。
  - F 为 0。
  - TLV Code Point，指示 ICCP 能力。
  - Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
  - S-bit，状态指示位，指示发送方是发布还是收回 ICCP 能力。取值范围如下：
    - 1：发布 ICCP 能力；
    - 0：收回 ICCP 能力。
  - Ver/Maj，ICCP 协议的主要版本修订，当前是 1.0，这个字段设置为 1。
  - Ver/Min，ICCP 协议的次要版本修订，当前是 1.0，这个字段设置为 0。
- 如果本地 PE 至少使能了一个 RG，那么需要向 LDP 对端通告 ICCP 能力。

10 客户应用

10.1 PW 冗余应用处理过程

10.1.1 处理过程的原理

PW 冗余应用不能和接入链路冗余应用在一个业务实例中同时使能。这样可以简化多机框冗余方案的操作并消除接入链路和 PW 冗余机制之间死锁状态的可能性。

10.1.2 初始化设置

当一个系统配置了一个 RG，并且 RG 使能多机框 PW-RED 应用，那么 PW-RED 应用应发送一个携带“PW-RED 连接 TLV”的“RG 连接”消息给同一 RG 中的每个成员 PE。如果发送方 PE 已经从对端接收到“PW-RED 连接 TLV”，那么它设置 A 比特为 1，否则，设置 A 比特为 0。如果 PE 发送了 A 比特为 0 的 TLV 后，又从对端接收到“PW-RED 连接 TLV”，那么它应重新发送 A 比特为 1 的消息。当双方 PEs 都发送并接收了 A 比特设置为 1 的“PW-RED 连接 TLVs”后，PW-RED 应用连接才被看做是可用



的。一旦应用连接可用，那么两个设备开始交换“RG 应用数据”消息。

当设备不使能 PW-RED 应用或者 RG 没有配置这个应用，那么系统应发送携带有“PW-RED 连接断开 TLV”的“RG 连接断开”消息。

### 10.1.3 伪线配置同步

PE 应向同一 RG 中的其他成员 PE 通告自己的本地 PW 配置。当 PW-RED 应用连接建立好时，就开始通告。为了达到上述目的，系统发送携带有“PW-RED 配置 TLVs”的“RG 应用数据”消息作为主动同步的一部分。PE 应使用一对“PW-RED 同步数据 TLVs”定界这些 TLVs。

当配置变化时，PE 应重新通告被影响的 PW 的最新信息。

作为配置同步的一部分，PE 需要通告与 PW 关联的 ROID。它用来关联在不同 PEs 上保护彼此的伪线。PE 还需要通告配置的 PW 冗余模式，可以有如下 4 种选项：主用模式，备用模式，独立模式以及带有请求切换的独立模式。如果接收的冗余模式与本地配置不匹配，那么 PE 应回复“RG 通知消息”来拒绝“PW-RED 配置 TLV”。直到从对方接收到满意的“PW-RED 配置 TLV”，PE 才可以使能关联的本地伪线，这就保证设备误配置不会引起网络级问题（比如导致转发环路）。同样，PE 应该上报告警给管理者。如果 PE 接收到针对“PW-RED 配置 TLV”的否定应答，它应去使能关联的伪线并且应该上报告警给管理者。

此外，PE 在“PW-RED 配置 TLVs”中同时发布伪线的优先级值，业务名字和伪线标识。

### 10.1.4 伪线状态同步

为了确认哪条伪线处于 active 状态哪条伪线处于 standby 状态，RG 中的 PE 需要同步伪线状态。不论何时 PE 上的伪线的状态发生变化，都可以通过发送“PW-RED 状态 TLV”来同步伪线状态。

PE 可能请求对端 PE 重传之前发布的 PW-RED 状态，比如当 PE 从一个软故障恢复后。PE 应发送“PW-RED 同步请求 TLVs”来请求重传 PW-RED 状态。PE 应发送请求的数据来回复“PW-RED 同步请求 TLV”，这些数据封装在 PW-RED TLVs 中，由一对“PW-RED 同步数据 TLVs”定界。回复 TLVs 应有序，因此，具有“同步数据开始”标志的同步回复 TLV 优先于其他包含同步数据的 PW-RED TLVs，最后是具有“同步数据结束”标志的同步 TLV。

PE 可能主动重传它的 PW-RED 状态，即发送适当的配置和状态 TLVs，以一对“PW-RED 同步数据 TLVs”定界并设置“请求编号”为 0。

当 PE 对某条伪线或业务的同步请求未被回复之时，应忽略接收到的关于这条伪线或业务的所有非同步回复信息，即使它们携带了相同类型的请求信息。这减轻了系统更新状态的负担。

如果 PE 接收到不存在或不认识的伪线或业务的同步请求，那么应触发主动同步所有的伪线信息。（也就是说重复初始化过程）

### 10.1.5 PE 节点失效

当 PE 节点检测到同一 RG 中的对端 PE 不可达，对于受到影响的业务，本地 PE 会检测是否有冗余 PW。如果本地具有最高优先级（除了失效的 PE），它将成为业务的 active 节点，同时激活相关的 PW(s)。

## 10.2 接入链路冗余应用处理过程

### 10.2.1 接入链路通用处理过程

#### 10.2.1.1 处理过程的内容

本章介绍接入链路冗余应用的通用过程，不管接入链路的类型（ATM、FR、SDH 或 Ethernet），包

括多机框 LACP 应用及多机框 MSP 应用。

#### 10.2.1.2 接入链路失效

当 active PE 的接入链路冗余机制检测到接入链路失效，需首先判断与备用设备的通信链路是否异常。如果正常，它应该发送一个携带倒换决策的 ICCP 应用数据消息给备份 PEs，备份 PEs 根据所收到的消息进行切换，并将切换结果通知给 active PE，active PE 更新本地链路状态；如果异常，则将告警信息映射到远端发送方，由远端发送方触发倒换。检测到链路正常后，则将发送携带告警的发送 ICCP 应用数据消息给备份 PEs。接入链路失效存在如下几种场景：

- 连接 PE 的 CE 接口失效；
- 连接 PE 的 CE 上行链路失效；
- 连接 CE 的 PE 接口失效。

在多机框 MSP 应用中，备份 PEs 需要将切换结果转换为 K 值，通知给 active PE，active PE 根据 K 值更新本地链路状态。

#### 10.2.1.3 对端 PE 节点失效

当 PE 节点检测到同一 RG 中的对端 PE 不可达，对于受到影响的业务，本地 PE 会检测是否有冗余接入链路。如果本地 PE 具有最高优先级（除了失效的 PE），它将成为业务的 active 节点，同时激活相关的接入链路。

#### 10.2.1.4 本地 PE 隔离

当 PE 节点检测到它已经从核心网络孤立（比如，所有面向核心的接口/链路都已经不可用），那么应该保证它的接入链路冗余机制能将 active ACs 变为 standby。然后 active PE 的接入链路冗余应用应该发送 ICCP 应用数据消息来激活 standby PE。

#### 10.2.1.5 确定伪线状态

如果 RG 内的 PEs 运行 ICCP 接入链路冗余应用（如多机框 LACP，多机框 MSP），那么应使用 PW 冗余的独立模式。在某个 PE 上，PW 的优先转发状态（激活或备用）从相关联的接入链路状态继承获得。这样简化了多机框冗余方案的操作并消除了接入链路冗余机制与 PW 冗余机制之间的状态死锁可能性。PW 状态继承接入链路状态的规则如下：

- VPWS，每个业务实例只有一个接入链路。如果接入链路激活，那么 PW 状态也是激活；如果接入链路是备用，那么 PW 状态也应是备用；
- VPLS，每个业务实例（比如 VFI）有多个接入链路。如果至少一个接入链路激活，那么 PW 状态应该是激活的；如果所有接入链路都是备用的，那么 PW 状态应该是备用。

在这种情况下，PW-RED 应用在 PEs 之间不同步 PW 状态，而是接入链路冗余应用（如多机框 LACP，多机框 MSP）应在 PEs 间同步接入链路状态，从而针对某个业务确定哪个接入链路是激活或备用。PE 然后根据上述原则和接入链路状态信息确定 PW 状态。也就是说，当工作链路需要切换时，RG 内的 PE 将切换状态封装成报文发送至配置了 PW 冗余组保护的 PE，PW 冗余组的 PE 对收到的报文解析后取出切换状态，根据切换状态执行 PW 冗余组的切换。

### 10.2.2 多机框 LACP (mLACP) 应用处理过程

#### 10.2.2.1 初始化建立

当一个系统配置了一个 RG，并且 RG 使能多机框 LACP 冗余应用，那么 mLACP 应用应发送一个携



带“mLACP 连接 TLV”的“RG 连接”消息给同一 RG 中的每个成员 PE。如果发送方 PE 已经从对端接收到“mLACP 连接 TLV”，那么它设置 A 比特为 1，否则，设置 A 比特为 0。如果 PE 发送了 A 比特为 0 的 TLV 后，又从对端接收到“mLACP 连接 TLV”，那么它应重新发送 A 比特为 1 的消息。当双方 PEs 都发送并接收了 A 比特设置为 1 的“mLACP 连接 TLVs”后，mLACP 应用连接才被看做是可用的。一旦应用连接可用，那么两个设备开始交换“RG 应用数据”消息。这涉及每个 PE 主动发布它的 mLACP 配置和操作状态。当应用连接初始化建立时，PE 通告它的 mLACP 配置和状态应该遵从如下顺序：

- 通告系统配置；
- 通告聚合器配置；
- 通告端口配置；
- 通告聚合器状态；
- 通告端口状态。

PE 应使用一对“mLACP 同步数据 TLVs”来定界完整集合的 TLVs。

当 mLACP 应用连接建立之后，每个 PE 应使用“mLACP 系统配置 TLV”向对等体通告自己的系统级配置。从而每个 PE 发现对等体的 Node ID，本地配置的系统 ID 和系统优先级。

如果 PE 从对等体接收到一个“mLACP 系统配置 TLV”，通告了和本地系统相同的 Node ID，那么 PE 应回复“RG 通告消息”来拒绝“mLACP 系统配置 TLV”。PE 应停止 mLACP 应用直到从对等体接收到满意的“mLACP 系统配置 TLV”。同时，PE 需要上报告警给管理者。如果 PE 接收到“mLACP 系统配置 TLV”的否定应答，PE 应停止 mLACP 应用并上报告警，通知管理者存在潜在的错误配置。

如果 PE 从一个新的对等体接收到一个“mLACP 系统配置 TLV”，其通告的 Node ID 与另一个已存在的对等体（已经和本端建立 mLACP 应用连接）通告的 Node ID 相同，那么 PE 应回复“RG 通告消息”来拒绝这个“mLACP 系统配置 TLV”，同时忽略此 TLV。

如果某个 PE 的 Node ID 配置改变，那么 PE 应通知对方清除之前通告的所有端口和/或聚合器配置，同时应重新启动初始化过程，主动发送同步信息：系统配置、聚合器配置、端口配置、聚合器状态和端口状态。

当设备不使能 mLACP 应用或没有配置相应的 RG 时，系统应发送携带“mLACP 断开连接 TLV”的“RG 断开连接”消息。

#### 10.2.2.2 mLACP 聚合器和端口配置

系统应和 RG 中的成员同步聚合器和端口配置，分别通过使用“mLACP 聚合器配置 TLVs”和“mLACP 端口配置 TLVs”实现。实现时通告聚合器配置优先于端口的配置。

同一 RG 中的 PEs 应针对关联某个聚合器的 MAC 地址达成一致，可以通过对成员 PEs 统一配置实现。然而，为了避免可能的错误配置，应使用 RG 中的系统聚合优先级数值最小的 PE 的 MAC 地址。

系统接收到“mLACP 聚合器配置 TLV”，但 ROID 和 Key 值关联不同于本地关联的，应拒绝相关的 TLV 并去使能相同 ROID 的聚合器，同时上报告警。相似的，接收到否定应答 TLV，也应去使能相关聚合器并上报告警。

系统可能强制所有绑定到同一个 PE 的端口使用相同的端口优先级，这样的话，系统应在“mLACP 聚合器配置 TLV”中通告统一的优先级并设置“Priority Set”标志位，并且，不能在“mLACP 端口配置 TLVs”中通告独自の端口优先级，（例如，Priority Set”标志位置 0）。。

系统可以支持绑定到同一个 PE 的端口配置不同的端口优先级,这样的话,系统应在“mLACP 端口配置 TLVs”中通告各自的端口优先级,并且在对应的“mLACP 聚合器配置 TLV”中不设置“Priority Set”标志位。

如果与某个聚合器关联的所有链路端口的配置都已经通告完毕,那么它在最后端口的“mLACP 端口配置 TLV”中设置“Synchronized”标志位。如果聚合器不包含任何成员端口,那么设置“mLACP 聚合器配置 TLV”的“Synchronized”标志位。

对任一端口/聚合器,应通告配置信息优先于通告状态信息。如果 PE 接收到“mLACP 端口状态 TLV”或“mLACP 聚合器状态 TLV”,而之前没有接收到相关端口或聚合器的配置 TLV,那么 PE 应请求从对方重新同步所有 mLACP 端口和聚合器的配置和状态。

当端口/聚合器不再配置 mLACP, PE 应发送设置“清除配置”标志位的“端口/聚合器配置 TLV”。接收 PE 就可以清除保存的相关端口/聚合器状态。

#### 10.2.2.3 mLACP 聚合器和端口状态同步

同一 RG 中的 PE 需要同步它们的状态机。通过每个 PE 在“mLACP 聚合器状态 TLVs”和“mLACP 端口状态 TLVs”通告它们的聚合器和端口运行状态来实现。无论何时,不管是在对方(多归设备侧)或者是主动方(PE 侧),聚合器或端口的任何 LACP 参数发生变化,应通告更新状态后的 TLV。而且当聚合器或端口的管理或操作状态发生改变时,也应发送更新状态后的 TLV 给对方。

如果 PE 接收到的聚合器或端口状态 TLV 中的“Actor Key”与之前接收的聚合器或端口状态 TLV 中的不匹配,那么 PE 应请求受影响的聚合器和端口进行配置和状态同步。作为同步(主动或非主动)的一部分,如果上述不匹配在配置和状态 TLVs 之间发生,那么 PE 应针对状态 TLV 发送否定应答。如果 PE 接收的端口状态 TLV 中携带的聚合器 ID 与之前通过聚合器配置 TLV 中学习的的不同,PE 应请求同步所有聚合器和端口的配置和状态。

PE 可能请求对方重传之前通告的状态,比如当 PE 从软故障恢复后,需要重新学习状态。为了请求重传,PE 应发送一系列“mLACP 同步请求 TLVs”。

PE 应回复“mLACP 同步请求 TLV”,通过发送一系列包含请求数据的 mLACP TLVs 实现,这些 TLVs 用一对“mLACP 同步数据 TLVs”定界。

PE 设备可能主动重新发布它的 mLACP 状态,通过发送配置和状态 TLVs 实现,这些 TLVs 以一对“mLACP 同步数据 TLVs”定界,并设置“请求编号”为 0。

当 PE 对系统,聚合器或端口的同步请求未被回复之时,它应忽略接收到的关于系统、聚合器和端口的所有非同步回复信息,即使它们携带了相同类型的请求信息。这减轻了系统更新状态的负担。

如果 PE 接收到不存在或不认识的聚合器、端口或 Key 值同步请求,那么它应触发所有系统、聚合器和端口信息的主动同步(也就是说重复初始化过程)。

如果 PE 从对方学习到的节点 ID 与它之前发布的不同,那么 PE 应清除之前从对方学习的所有端口/聚合器数据。

#### 10.2.2.4 故障和恢复

当多机框链路聚合组的激活 PE 面向核心侧失效,它应尝试由相同 RO 的对方 PE 接替工作,恢复业务。

当从之前的故障恢复后,如果多机框链路聚合组配置为返回式模式,PE 可能重新成为激活角色。否



则的话，如果是非返回式模式，那么恢复的 PE 可能仍旧是备用角色。在返回式场景，PE 通过向当前的激活 PE 发送“mLACP 端口优先级 TLV”，要求它降低自己的 port priority。使得 PE 重新成为激活角色。

如果系统运行在这样的模式——绑定组的不同端口配置了不同的端口优先级，那么系统应不能通告或请求全部聚合端口的端口优先级的变化。

如果 PE 接收到的“mLACP 端口优先级 TLV”请求非本地的端口或聚合器的优先级改变，那么 PE 应重新通告本地配置，以及所有的 mLACP 端口和聚合器的配置和状态。

如果 PE 接收到“mLACP 端口优先级 TLV”，即远端系统发布的端口或聚合器的优先级改变，而本地 PE 通过之前的端口或聚合器配置 TLV 并没有学习到，那么 PE 应请求从对方同步所有 mLACP 端口以及所有 mLACP 聚合器的配置和状态。

附录 A  
(资料性附录)  
多机框 MSP 的应用

A.1 多机框 MSP (Multi-chassis Multiplex Section Protection, mMSP) 应用 TLVs

A.1.1 概述

本章定义采用 mMSP 应用的 SDH 接入链路冗余的 ICCP TLVs。

A.1.2 mMSP 连接 TLV

mMSP 连接 TLV 承载在 RG 连接消息中，表明 mMSP 应用连接的建立。mMSP 连接 TLV 格式，见表 A.1。

表 A.1 mMSP 连接 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
U	F	Type=0x3E00														Length																
Protocol Version																A	Reserved															
..... Optional Sub-TLVs .....																																

其中：

- U 及 F 为 0；
- Type 为 0x3E00，表示 mMSP 连接 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Protocol Version，协议针对 ICCP 的版本；
- A-bit，如果发送端已经从接收端接收到 mMSP 连接 TLV，那么设置为 1，否则设置为 0；
- Reserved，保留字段；
- Optional Sub-TLVs，可选子 TLVs，当前版本没有定义。

A.1.3 mMSP 连接断开 TLV

这个 TLV 承载在 RG 连接断开消息中，表示要终止 mMSP 应用的连接。mMSP 连接断开 TLV 格式见表 A.2。

表 A.2 mMSP 连接断开 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E01														Length															
Optional Sub-TLVs																															

其中：

- U 及 F 为 0；
- Type 为 0x3E01，表示 mMSP 连接断开 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Optional Sub-TLVs，可选子 TLVs，目前版本定义的可选子 TLV 是“mMSP 连接断开原因 TLV”。

mMSP 连接断开原因 TLV 格式见表 A.3。

表 A.3 mMSP 连接断开原因 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E09														Length															
..... Disconnect Cause String .....																															

其中：

- U 及 F 为 0；
- Type 为 0x3E09，表示 mMSP 连接断开原因 TLV；
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度；
- Disconnect Cause String，可变长度的字符串，指明断开连接的原因。

A.1.14 MSP 保护组配置 TLV

mMSP 保护组配置 TLV 在 RG 应用数据消息中发送。这个 TLV 通告本地 MSP 保护组配置给 RG 对端。mMSP 保护组配置 TLV 的格式见表 A.4。

表 A.4 mMSP 保护组配置 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type=0x3E02														Length															
ROID																															
Protect Type								Direction								Protect Mode								Flags							
WTR Time																															

其中：

- U 及 F 为 0。
- Type 为 0x3E02，表示 mMSP 保护组配置 TLV。
- Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- ROID，见“7.1.4 ROID 编码”。
- Protect Type，mMSP 保护组保护类型，取值范围如下：
  - 0x00：1+1 保护；
  - 0x01：1:1 保护；
  - 0x02-0xFF：保留。
- Direction，mMSP 保护组保护方向，取值范围如下：
  - 0x00：单向；
  - 0x01：双向。
- Reversion Mode，mMSP 保护组返回方式，取值范围如下：
  - 0x00：非返回方式；
  - 0x01：返回方式。
- Flags，操作类型，取值范围如下：

- 0x01: 同步, 表示发送方传送所有保护组配置信息;
- 0x02: 清除配置, 表示清除 mMSP 配置或操作。
- WTR Time, 等待恢复时间, 在返回方式下使用。

A.1.5 mMSP 端口配置 TLV

mMSP 端口配置 TLV 承载在 RG 应用数据消息中。这个 TLV 用于向 RG 中的对端 PE 通告本地 MSP 端口配置。mMSP 端口配置 TLV 的格式见表 A.5。

表 A.5 mMSP 端口配置 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E03														Length															
ROID																															
Role								Flags								Port Name Len															
Port Name																															

- 其中:
- U 及 F 为 0。
  - Type 为 0x3E03, 表示 mMSP 端口配置 TLV。
  - Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度;
  - ROID, 见“7.1.4 ROID 编码”。
  - Role, 复用段角色, 取值范围如下:
    - 0x00: 工作;
    - 0x01: 保护。
  - Flags, 操作类型, 取值范围如下:
    - 0x01: 同步, 表示发送方传送所有保护组端口配置信息;
    - 0x02: 清除配置, 表示清除 mMSP 端口配置或操作。
  - Port Name Len, “Port Name”字段的长度。
  - Port Name, 端口名字, UTF-8 格式, 最大 32 个字符。

A.1.6 mMSP 复用段状态 TLV

mMSP 复用段状态 TLV 承载在 RG 应用数据消息中。这个 TLV 用于向 RG 中的对端 PE 通告本地 MSP 复用段状态。mMSP 复用段状态 TLV 的格式见表 A.6。

表 A.6 mMSP 复用段状态 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E04														Length															
Section State																															

- 其中:
- U 及 F 为 0。
  - Type 为 0x3E04, 表示 mMSP 复用段状态 TLV。
  - Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。



- Section State, 取值范围如下:
- 0x00: 信号正常;
- 0x01: 高优先级信号失效;
- 0x02: 低优先级信号失效;
- 0x03: 高优先级信号劣化;
- 0x04: 低优先级信号劣化。

#### A.1.7 mMSP 倒换命令 TLV

mMSP 倒换命令 TLV 承载在 RG 应用数据消息中。这个 TLV 用于向 RG 中的对端 PE 通告本地 MSP 倒换命令。mMSP 倒换命令 TLV 的格式见表 A.7。

表 A.7 mMSP 倒换命令 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E05														Length															
Request Cmd																															

其中:

- U 及 F 为 0。
- Type 为 0x3E05, 表示 mMSP 倒换命令 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Request Cmd, mMSP 接收的倒换命令。取值范围如下, 二进制表示:
- 1111: Clear, 清除;
- 1101: Lockout of protection(LP), 闭锁;
- 1011 ; Forced Switch working-to-protection, 强制切换, 从工作到保护;
- 1001: Forced Switch protection-to-working, 强制切换, 从保护到工作;
- 0111: Manual switch working-to-protection, 人工切换, 从工作到保护;
- 0101: Manual switch protection-to-working, 人工切换, 从保护到工作;
- 0100: Exercise。

#### A.1.8 mMSP 保护组状态 TLV

mMSP 保护组状态 TLV 承载在 RG 应用数据消息中。这个 TLV 用于向 RG 中的对端 PE 通告本地 MSP 保护组状态。mMSP 保护组状态 TLV 的格式见表 A.8。

表 A.8 mMSP 保护组状态 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E06														Length															
Group State								Path																							

其中:

- U 及 F 为 0。
- Type 为 0x3E06, 表示 mMSP 保护组状态 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Group State, 保护组状态, 取值范围如下:
- 0x00: No request, 无请求;

- 0x01: Do not revert, 不返回;
  - 0x02: Reverse request, 返回请求;
  - 0x03: Unused, 暂不使用;
  - 0x04: Exercise;
  - 0x05: Unused, 暂不使用;
  - 0x06: Wait-to restore, 等待恢复;
  - 0x07: Unused, 暂不使用;
  - 0x08: Manual switch, 人工倒换;
  - 0x09: Unused, 暂不使用;
  - 0x0A: Signal degrade low priority, 信号劣化, 低优先级;
  - 0x0B: Signal degrade high priority, 信号劣化, 高优先级;
  - 0x0C: Signal fail low priority, 信号失效, 低优先级;
  - 0x0D: Signal fail high priority, 信号失效, 高优先级;
  - 0x0E: Forced switch, 强制倒换;
  - 0x0F: Lockout of protection, 闭锁。
- Path, 保护组的激活路径, 取值范围如下:
- 0x00: 激活路径为工作复用段;
  - 0x01: 激活路径为保护复用段。

#### A.1.9 mMSP 同步请求 TLV

mMSP 同步请求 TLV 承载在 RG 应用数据消息中, 用来向 RG 中的对端 PE 请求重传配置或操作状态。mMSP 同步请求 TLV 的格式见表 A.9。

表 A.9 mMSP 同步请求 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E07														Length															
Request Number																C	S	Request Type													

其中:

- U 及 F 为 0。
- Type 为 0x3E07, 表示 mMSP 请求 TLV。
- Length, TLV 的字节长度, 除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
- Request Number, 标识一个请求, 回复需要与请求对应。
- C bit, 如果请求配置数据, 设置为 1, 否则为 0。
- S bit, 如果请求状态数据, 设置为 1, 否则为 0。
- Request Type, 请求类型, 取值范围如下:
  - 0x00: 请求某个保护组的数据;
  - 0x01: 请求所有保护组的数据。

#### A.1.10 mMSP 同步数据 TLV

mMSP 同步数据 TLV 承载在 RG 应用数据消息中。设备用一对 TLVs 给一系列回复 mMSP 同步请求 TLV 的 TLVs 定界。定界 TLVs 表示同步数据的开始和结束, 并且通过请求编号字段将回复和请求对应。



mMSP 同步数据 TLV 也用于主动通告 mMSP 配置和操作状态。这种情况下，请求编号字段设置为 0。  
mMSP 同步数据 TLV 的格式见表 A.10。

表 A.10 mMSP 同步数据 TLV 的格式

0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
U	F	Type= 0x3E08														Length															
Request Number																Flags															

- 其中：
- U 及 F 为 0。
  - Type 为 0x3E08，表示 mMSP 同步数据 TLV。
  - Length，TLV 的字节长度，除了字段 U-bit、F-bit、Type 和 Length 字段外的 TLV 字节长度。
  - Request Number，与“mMSP 同步请求 TLV”匹配。
  - Flags，取值范围：
    - 0x00——同步数据开始；
    - 0x01——同步数据结束。

A.2 多机框 MSP (mMSP) 应用处理过程

A.2.1 初始化建立

当一个系统配置了一个 RG，并且 RG 使能多机框 MSP 应用，即工作链路所在的主 PE 设备和保护链路所在的备 PE 设备构成复用段保护组，那么 mMSP 应用应发送一个携带“mMSP 连接 TLV”的“RG 连接”消息给同一 RG 中的其他成员 PE。如果发送方 PE 已经从对端接收到“mMSP 连接 TLV”，那么它设置 A 比特为 1，否则，设置 A 比特为 0。如果 PE 已经发送 A 比特为 0 的 TLV 后，从对端接收到“mMSP 连接 TLV”，那么它应重新发送 A 比特为 1 的消息。当双方 PEs 都发送并接收了 A 比特设置为 1 的“mMSP 连接 TLVs”后，mMSP 应用连接才被看做是可用的。一旦应用连接可用，那么两个设备开始交换“RG 应用数据”消息。

当设备不使能 mMSP 应用或者 RG 没有配置这个应用，那么系统应发送携带有“mMSP 连接断开 TLV”的“RG 连接断开”消息。

A.2.2 mMSP 保护组和端口配置同步

系统应和 RG 成员同步保护组和端口配置，分别通过使用“mMSP 保护组配置 TLVs”和“mMSP 端口配置 TLVs”实现。实现时发布保护组配置优先于发布任何相关成员端口的配置。

当配置变化时，PE 应重新发布最新的信息。

作为配置同步的一部分，PE 也要发布与 MSP 保护组关联的 ROID。它用来关联在不同 PEs 上保护彼此的复用段。同样，PE 发布配置的保护组保护类型、保护方向、返回方式以及返回式下的 WTR。如果接收的保护组配置属性与本地配置不匹配，那么 PE 应回复“RG 通知消息”来否定应答“mMSP 保护组配置 TLV”，并应上报告警给用户，直到从对方接收到满意的“mMSP 保护组配置 TLV”。如果 PE 接收到针对“mMSP 保护组配置 TLV”的否定应答，它应去使能关联的复用段保护组并且应该上报告警给管理者。

通告保护组的配置优先于通告它的状态。如果 PE 接收到“mMSP 保护组状态 TLV”，而之前没有接收到保护组配置 TLV，那么 PE 应请求对方重新同步保护组配置和状态。

当不再配置 mMSP 保护组, PE 应发送设置“清除配置”标志位的“mMSP 保护组配置 TLV”和“mMSP 端口配置 TLV”。接收 PE 就可以清除保存的相关保护组和端口状态。

#### A.2.3 mMSP 倒换命令和复用段状态同步

当 PE 检测到工作链路出现故障时, 发送“mMSP 复用段状态 TLV”和“mMSP 倒换命令 TLV”报文给备用设备, 备用设备接收到报文后进行倒换。备用设备进行倒换后, 将结果通过“mMSP 保护组状态同步 TLV”发送给主设备。

#### A.2.4 mMSP 保护组状态同步

同一 RG 中的 PE 需要同步它们的状态。每个系统在“mMSP 保护组状态 TLVs”通告它们的保护组状态。无论何时, 备用 PE 设备接收到配置改变, 链路告警变化或接收到手动倒换命令后, 备用设备进行倒换决策后发送倒换结果, 即“mMSP 保护组状态同步 TLV”给主设备。主设备检查本地状态信息, 如果与接收的状态信息不同, 根据备用设备的状态信息进行更新。

PE 可能请求对方重传之前发布的状态, 比如当 PE 从软故障恢复后, 需要重新学习状态。为了请求重传, PE 应发送一系列“mMSP 同步请求 TLVs”。

PE 应回复“mMSP 同步请求 TLV”, 通过发送一系列包含请求数据的 mMSP TLVs 实现, 这些 TLVs 用一对“mMSP 同步数据 TLVs”定界。

PE 设备可能主动重新发布它的 mMSP 状态, 通过发送配置和状态 TLVs 实现, 这些 TLVs 以一对“mMSP 同步数据 TLVs”定界, 并设置“请求编号”为 0。

当 PE 对保护组或端口的同步请求未被回复之时, 它应忽略接收到的关于保护组或端口的所有非同步回复信息, 即使它们携带了相同类型的请求信息。这减轻了系统更新状态的负担。

#### A.2.5 故障和恢复

当多机框 MSP 保护组处于工作状态的 PE 面向核心侧失效或工作状态的复用段失效, 那么由保护状态的 PE (以及复用段) 接替工作, 恢复业务。

当故障恢复后, 如果多机框 MSP 保护组配置为返回式模式, 当前处于备用状态的 PE 可能重新处于激活状态; 如果是非返回式模式, 那么恢复的 PE 可能仍旧处于备用状态。在返回式场景下, PE 通过发送“mMSP 保护组状态 TLV”和“mMSP 复用段状态 TLV”来同步状态。

## 参 考 文 献

- [1] draft-hao-pwe3-iccp-extension-for-msp-04
-



中 华 人 民 共 和 国  
通 信 行 业 标 准  
跨机框信息同步通信协议（ICCP）技术要求  
YD/T 2901-2015

\*

人民邮电出版社出版发行  
北京市丰台区成寿寺路 11 号邮电出版大厦  
邮政编码：100164  
北京康利胶印厂印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16                      2015 年 12 月第 1 版  
印张：2.75                                  2015 年 12 月北京第 1 次印刷  
字数：69 千字

15115 • 819

定价：30 元

本书如有印装质量问题，请与本社联系 电话：(010)81055492