ICS 01.040.33
L 78

YD

中华人民共和国通信行业标准

YD/T 2447-2013

公众IP网络可靠性 双向转发检测（BFD）机制的技术要求

IP network reliability
—Technical requirements for bidirectional forwarding detection

2013-04-25 发布　　2013-06-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准为公众IP网络可靠性系列标准之一。该系列标准预计为：

1. YD/T 2373《公众IP网络可靠性 总体技术要求》；

2. YD/T 2175《公众IP网络可靠性 标记分发协议(LDP)平滑重启动技术要求及测试方法》；

3. YD/T 2176《公众IP网络可靠性 中间系统到中间系统路由交换协议（IS-IS）中平滑重启动技术要求及测试方法》；

4. YD/T 1702《公众IP网络可靠性 IP快速重路由技术框架》；

5.YD/T 2416-2012《公众IP网络可靠性 IP快速重路由技术要求》；

6.《公众IP网络可靠性 RSVP-TE平滑重启动技术要求》；

7.YD/T 2447-2013《公众IP网络可靠性 双向转发检测（BFD）机制的技术要求》；

8.YD/T 2448-2013《公众IP网络可靠性 虚拟路由器冗余协议（VRRP）技术要求》。

本标准技术内容和IETF RFC5880的技术内容保持一致。

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：工业和信息化部电信研究院。

本标准起草人：孙明俊、刘　述、赵　锋、马军锋、马　科、吴英桦。

公众IP网络可靠性
双向转发检测（BFD）机制的技术要求

1 范围

本标准规定了双向转发检测机制的技术要求，包括BFD控制报文格式，BFD Echo报文格式，BFD过程，操作问题，IANA，和安全等。

本标准适用于支持双向转发检测机制的网络设备。

2 术语、定义和缩略语

2.1 术语和定义

下列术语和定义适用于本文件。

2.1.1

异步模式 Asynchronous Mode

系统按一定周期向对端发送BFD报文，如果有一定数量的报文没有被接收到，会话即被认定中断。

2.1.2

命令模式 Demand Mode

在建立BFD会话后，系统会先请求对端不发送BFD控制报文，只有在系统认为需要确认连接性时，才会发送一个短的BFD序列。

2.2 缩略语

下列缩略语适用于本文件。

BFD	Bidirectional Forwarding Detection	双向转发检测
LSP	Label Switch Path	标签交换路径
MPLS	Multi-Protocol Label Switch	多协议标签交换

3 BFD 协议概述

BFD用来检测与转发平面的下一跳之间的通信故障。在转发和控制引擎分离的情况下，BFD一般在系统的转发引擎的某些部件上实现。这不仅将BFD更多的绑定到了转发平面，还降低了BFD与路由协议引擎耦合，使各种协议都能实现平滑重启。BFD也可以用在控制引擎，但这样可能会导致某些故障的检测困难。

BFD采用单向点对点的运行模式，可以运行在有路由转发的两个系统之间的任何数据协议上（网络层，链路层，tunnel等）。BFD数据报文可以封装在网络和物理媒介上的协议载荷中进行传送。任何特定BFD会话的操作的上下文都绑定在该封装中。

如果一对系统中的一个方向上存在多条通路，可以同时建立多条BFD会话。在另一个方向上的可用的通路数量较小也是可以的。如多并行不对称链路，或者MPLS LSP等。

BFD建立会话和拆除会话都是三次握手方式，以此来保证使用BFD的双方能及时感知状态的变化。

可以将BFD抽象的看作一个简单的业务，BFD的业务原语包括创建，撤销和修改BFD会话，可以根据目的地址和其他参数进行修改。当BFD会话建立或者结束时，BFD给客户端返回指示信号。

4 协议说明

4.1 说明

BFD是一个简单的“Hello”协议，在很多方面与大多数路由协议的邻居检测部分相似。一对系统在它们之间的所建立会话的通道上周期性的发送检测报文，如果某个系统在足够长的时间内没有收到对端的检测报文，则认为在这条到相邻系统的双向通道的某个部分发生了故障。在某些条件下，为了减少负荷，需要协商系统之间的发送和接收速率。

当系统之间建立起双向通信后，就认为是建立了一条可用的通路，不过有时候会有非双向链路的情况。两个系统之间的每条通路和数据协议都可以创建独立的BFD会话。

系统首先计算发送和接收BFD报文的速度，报文发送速度可以实时的修改以适应异常状况。然后与相邻系统进行协商，确定故障检测的时长。BFD允许快系统和慢系统一起使用，快系统之间可以快速的检测出故障，而慢系统则采用尽力而为的方式。

系统能够控制BFD报文双方向传送的速率，这可以提供一种拥塞控制机制，尤其是BFD穿越多跳网络的时候。在不影响互通的情况下，各个不同系统的算法可以有所不同，本标准不做规定。

4.2 寻址和会话建立

BFD会话根据具体应用的要求建立。BFD自身没有发现机制，根据应用的需求和应用的地址进行启动。

4.3 运行模式

BFD有两种运行模式可供选择，另外还有一个附加功能，可以和两种模式结合使用。

第一种是异步模式。在该模式下，系统按一定周期向对端发送BFD报文，如果有一定数量的报文没有被接收到，会话即被认定中断。

第二种是命令模式。该模式假定系统有其他方法验证与对端系统是否连接，在建立BFD会话后，系统会先请求对端不发送BFD控制报文，只有在系统认为需要确认连接性时，才会发送一个短的BFD序列，然后远端系统沉默。命令模式可以在任意方向上独立运行，也可以同时在两个方向上运行。

Echo是这两种模式的附加功能。启用Echo功能后，一个包含BFD Echo报文的流发送到对端后环回到发送端。如果有一部分Echo数据没有收到，该会话即被宣告中断。Echo功能可以用于异步或者命令模式，如果使用Echo来进行检测，在异步模式时，控制报文的发送周期可以降低；在命令模式时，可以取消BFD控制报文。

相比Echo功能,单独的异步模式只需使用一半的报文就可以实现特定的检测时间。在不能使用Echo功能的情况下，可使用单纯的异步模式。

Echo功能的优势在于，仅在远端系统的转发路径上进行真正的检测，可以减少环路抖动从而使检测时间更为迅速，这样某些情况下不易检测的故障也能够被检出。

Echo功能可以在每个方向上分别启用。如果系统允许Echo报文信号环回，可以在一个特定方向上启用Echo功能。

某些情况下，BFD报文的周期性发送会造成过多开销，如系统中存在很多的BFD会话时，可以选择使用命令模式。命令模式在对称使用Echo功能的情况非常有用。命令模式的优势在于检测时间是系统触发的，BFD协议不需要事先知道。命令模式不能用于通路的往返时间大于所需要的检测时间的情况，这种情况协议不能正常工作。

5 BFD 控制报文格式

5.1 通用控制报文格式

为适应不同的环境，BFD控制报文采用封装的形式。本标准不规定特定的封装格式。

BFD控制报文由必选字段和可选的授权字段组成。授权字段的格式由所采用的授权类型决定。BFD控制报文的必选字段的格式如图1所示。

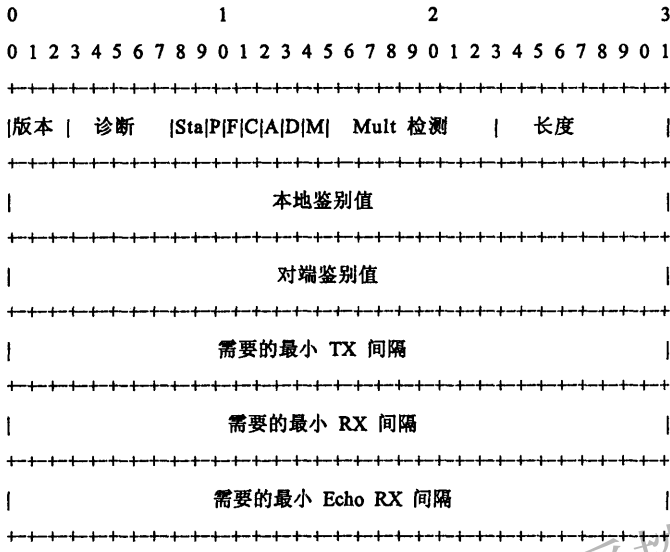

图1 BFD 报文必选字段格式

可选的授权字段可以采用的格式如图2所示。

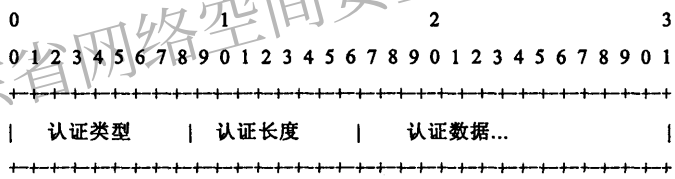

图2 BFD 报文可选字段格式

版本 (Vers)

协议的版本号。本标准采用第一版。

诊断 (Diag)

规定本地系统最近一次改变当前会话状态的原因：

0 – 不诊断；

1 – 控制检测时间超时；

2 – Echo 功能失败；

3 – 邻居宣布会话中断；

4 – 转发平面重置；

5 – 通路关闭；

6 – 级联通路关闭；

7 – 管理上的关闭；

8 – 反向级联路径关闭；

9~31 – 保留备用。

这个字段可以告知远端系统前一次会话失败的原因。

状态 (Sta)

传送系统中的BFD会话的当前状态，

有如下值：

0 – AdminDown；

1 – Down；

2 – Init；

3 – Up。

Poll (P)

如果设置，传送系统请求验证联通性，或者参数的改变；使用Final (F) 位进行回复。如果为空，传输系统不请求验证。

Final (F)

如果设置，是对接收到的BFD报文的P位的回复；如果为空，则不回复P位请求。

控制平面无关 (C)

如果设置，传输系统的BFD执行器不和控制平面共同使用（也就是说，BFD在转发平面执行，如果控制平面中断，功能仍可继续）。如果为空，传输系统的BFD执行器和控制平面共同使用。

C字节的使用是和具体应用相关的，不做规定。

Authentication Present (A)

如果设置，认证字段存在，BFD会话应该进行认证。

Demand (D)

如果设置，使用的是命令模式（系统希望运行在命令模式下，知道双方向都有BFD会话存在，指示远端系统释放周期性的BFD控制报文传输）。如果为空，系统没有使用命令模式。

多点 (M)

预留位。用于未来BFD扩展点到多点使用的情况。传送和接收都必须置为0.

检测Mult

检测时间的倍乘数。传输的时间间隔乘以这个值，得出异步检测系统的检测时间。

长度

BFD控制报文的长度，以字节为单位。

本地鉴别值（My Discriminator）

传输系统产生的唯一且非零的鉴别值，在同一对系统存在多个BFD会话时用来对会话进行鉴别。

远端鉴别值（Your Discriminator）

从相应的远程系统收到的鉴别值。该字段将收到的本地鉴别值的值返回对端，在本地鉴别值未知的情况下置0。

需要的最小TX 间隔 (Desired Min TX Interval)

本字段规定最小传送间隔，单位为微秒。本地系统传输BFD控制报文的时候使用，小于任何应用的抖动值(见7.9.2小节)。0值保留。

需要的最小RX间隔（Required Min RX Interval）

本字段规定系统能够支持的接收BFD控制报文的最小间隔，小于发送者应用的任何抖动值(见7.9.2小节)，单位为微秒。如果置为0，传送系统不希望远端系统发送周期性的BFD控制报文。

需要的最小Echo RX间隔（Required Min Echo RX Interval）

本字段规定系统能够支持的接收BFD Echo报文的最小间隔，小于发送者使用的抖动(见7.9.9小节)。单位为微秒。如果置为0，传送系统不支持BFD Echo报文。

认证类型（Auth Type）

如果设置该字段，启用认证类型。

0 – 保留；

1 – 简单密码；

2 – 密钥MD5；

3 – 严谨的密钥MD5；

4 – 密钥SHA1；

5 – 严谨的密钥SHA1；

6~255 – 保留。

认证长度（Auth Len）

认证字段的长度，单位为字节。包括Auth Type和Auth Len两个部分。

5.2 简单密码认证字段格式

如果包头中设置Authentication Present (A)字段，且Authentication Type包含1（简单密码），认证部分（section）采用的格式如图3所示。

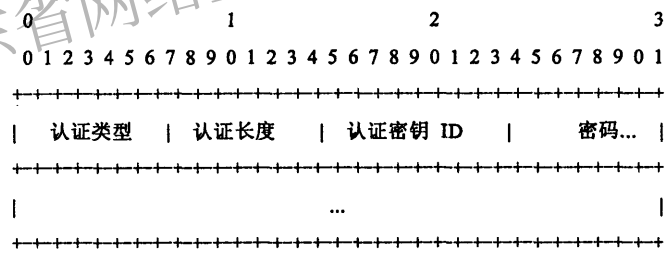

图3 BFD 报文简单密码认证字段格式

认证类型（Auth Type）

认证类型，本节为1（简单密码）。

认证长度（Auth Len）

认证Section的长度，以字节为单位。以简单密码验证为例，长度等于密码长度加3。

认证密钥ID（Auth Key ID）

本报文使用认证密钥ID，可以有多个密钥同时使用。

密码（Password）

会话中使用的简单密码，长度必须是1到16字节之间。

5.3 密钥 MD5 和严谨的密钥 MD5 认证格式

本标准不建议使用基于MD5的认证算法。本节的规定主要是为了和已经存在的MD5算法兼容。

如果包头中设置了Authentication Present (A)比特位，认证类型字段为2(密钥MD5)或者3(严谨的 密钥MD5)，认证Section的格式如图4所示。

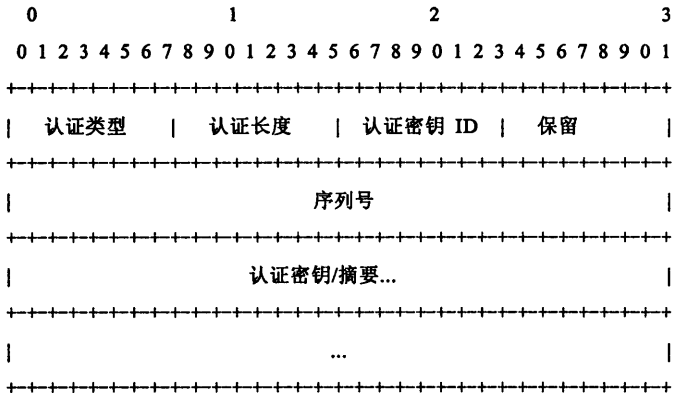

图4 BFD 报文密钥 MD5 和严谨的密钥 MD5 认证字段格式

认证类型（Auth Type）

此处为2 (密钥MD5)或者3(严谨的密钥MD5)。

认证长度（Auth Len）

认证section的长度，以字节为单位。采用密钥MD5和严谨的密钥MD5认证方法，长度为24。

认证密钥ID（Auth Key ID）

本报文使用的认证密钥ID。可以有多个密钥同时使用。

保留（Reserved）

本字节在传输时必须设为0，在收到后直接抛弃。

序列号（Sequence Number）

报文的序列号。对于密钥MD5认证，序列号值会间或递增。对于严谨的密钥MD5，序列号值会连续递增。序列号的递增机制可以防止重放攻击。

认证密钥/摘要（Auth Key/Digest）

本字段是报文的MD5摘要，长度为16字节。计算摘要时，共享的MD5密钥由该字段保存。共享的密钥长度必须是16字节。

5.4 密钥 SHA1 和严谨的密钥 SHA1 认证格式

如果包头中设置了Authentication Present (A)比特位，认证类型字段为4 (密钥SHA1)和5(严谨的密钥SHA1)，认证Section的格式如图5所示。

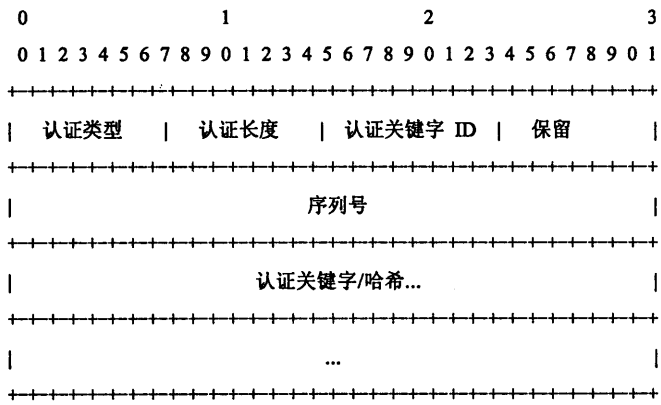

图5 密钥 SHA1 和严谨的密钥 SHA1 认证字段格式

认证类型（Auth Type）

此处为 4 (密钥SHA1) 或者5(严谨的密钥SHA1)。

认证长度（Auth Len）

认证section的长度，以字节为单位。对于eyed SHA1 和严谨的密钥SHA1算法，长度为28。

认证关键字ID（Auth Key ID）

报文使用的认证密钥ID。可以有多个密钥同时使用。

保留（Reserved）

本字节在传输时必须设为0，在收到后直接抛弃。

序列号（Sequence Number）

报文的序列号。对于密钥SHA1 认证，序列号值会间或递增。对于严谨的密钥SHA1，序列号值会连续递增。序列号的递增机制可以防止重放攻击。

认证密钥/摘要（Auth Key/Digest）

本字段是报文的SHA1 hash算法，长度为20字节。计算hash时，共享的SHA1 密钥由该字段保存。共享的密钥长度必须是20字节。

6 BFD Echo 报文格式

为适应不同的环境，BFD Echo报文以封装的方式发送。对于不同的环境，BFD Echo报文有不同的封装形式。

BFD Echo 报文的载荷是由本地系统发送并进行处理的，因此不需要远端的配合。本地只需提供鉴别信息，能够将BFD Echo 报文从多个BFD报文中鉴别出来，远端系统可以以此正确的进行环回。

7 BFD 过程

7.1 说明

本章规定协议的正文。本章中的"bfd.Xx"指的是内部状态变量，而"the Xxx field"指的是协议报文的字段。

7.2 概述

系统可以主动或者被动的发起一个会话。会话的主动发起方必须主动发送BFD控制报文；而会话的接收方只有在收到BFD报文、得到对端的鉴别值之后，才能发送BFD报文。一对系统必须至少有一个是会话的发起方，也可以两个都是。系统如何选择作为发送方还是作为接收方，取决于具体的应用，本标准不做规定。

首先使用周期性的，慢速传送的BFD控制报文开始一个会话。当双向通信建立之后，启动BFD会话。

如果系统需要使用Echo功能并且其他系统也支持，可以在BFD会话启动后启动Echo功能。在使用Echo功能时通常控制报文会保持比较低的传送速率。

如果不使用Echo功能，可以增加控制报文的传送速率以满足会话需要的检测时间。

会话建立之后，系统可能会发出进入命令模式的信号。收到此信号后，远端系统要停止BFD控制报文的传送。使用其他的连接方法来保持会话。系统可以通过发起一个短时的BFD控制报文的交换来确认双向连接的有效性。

如果没有使用命令模式，并且在可计算的检测时间内也没有收到控制报文，会话就会被宣布中断，通过中断包的状态（Sta）域来通知对端系统。

如果丢失的Echo报文达到一定的数量，采用上述方式来结束会话。见7.9.5小节。

如果命令模式启用，但没有收到与Poll序列相对应的控制报文，采用上述方式来结束会话。见7.7节。

如果会话中断，Echo报文的传送停止，控制报文的传输回到慢速率方式。

一旦会话已经宣布中断，在远端系统宣布会话中断之前（离开Up状态），会话不能被恢复。需要执行一次三方握手过程。

通过输入AdminDown状态并在诊断字段中填入解释性的诊断代码，会话可以保持为管理上的中断。

7.3 BFD 状态机

BFD的状态机共有三个状态，两个是会话初始化(Init)和建立（Up），一个是会话拆除（Down）。对应会话建立和会话拆除来说，都需要进行三方握手。另外还有一个状态是AdminDown，可以在管理层面将会话中断。

系统使用BFD控制报文的状态(Sta)字段来说明会话状态。将本地会话状态和收到的状态结合来驱动状态机。

Down状态意味着会话结束或者刚刚建立。在收到会话结束消息后，远端应回送状态字段设为非Up的BFD控制报文进行确认。在收到远端回送的包之前，会话需要一直保持Down状态。如果远端回送的控制报文的状态为Down，会话将准备进入Init状态；如果端回送的控制报文的状态为Init，会话将准备进入Up状态。Down状态说明转发路径不可用，应用应该采取的操作是监视BFD会话的状态。系统由于操作上的或者管理上的一些原因，也可能会将会话一直保持Down状态（对状态推进回复简单的拒绝）。

处于Init状态时，本地系统希望启动会话，正在与远端系统进行通信，但是远端系统还没有做出反应。Init状态将会保持到收到远端的BFD控制报文，如果BFD控制报文携带Init或者Up状态，会话将进入到Up状态；如果超出了检测时间还没有收到BFD报文，则认为和远端系统的通信中断，会话将进入Down状态。

处于Up状态时，BFD会话建立成功，两个系统之间有正常连接。会话一旦进入Up状态，将会一直保持。在遇到连接失败，或者管理上的会话拆除的情况时Up状态将无法保持。如果远端系统发送Down状态，或者是检测时间超时，系统将会进入到Down状态。

处于AdminDown状态时，会话在管理上被中断的，从而使远端系统也将会话变为Down状态，直至本地系统离开AdminDown状态为止。AdminDown状态对于转发通路没有影响。

图6所示是状态机的工作过程。为了说明的明确性，AdminDown状态没有作为单独的状态出现，在

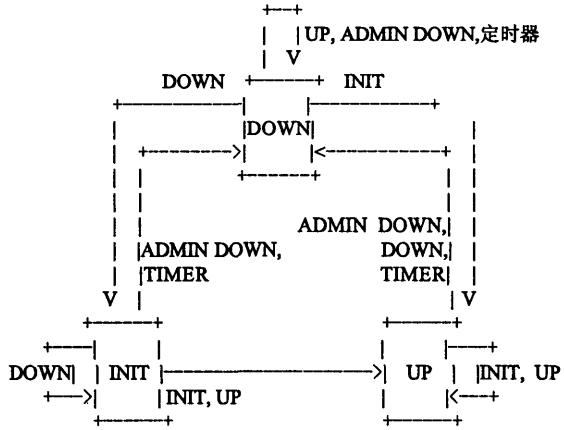

图6 BFD 状态机

7.9.6小节和7.9.16小节中有详细规定。每个方框上的注释表示的是远端系统的状态或者Detection Timer（检测定时器）的超时。

7.4 多路处理和鉴别值字段

由于在两个系统之间可能会存在多个BFD会话，需要多路处理机制用来将不同BFD报文分配给不同的会话。

系统的每个会话都要有一个特定的鉴别值，不同会话的鉴别值必须不同。本地鉴别值由My Discriminator字段进行传送，远端系统使用Your Discriminator 字段将鉴别值从远端返回。

远端返回了本地鉴别值后，对后续报文的多路处理是以Your Discriminator 值作为唯一标识，这样源地址改变或者接收包的端口改变时，BFD报文仍可以被分配到相应的会话。

初始包（Your Discriminator为0）的多路处理方法和具体的应用相关，本标准不做规定。

由于鉴别值仅用于多路分配，因此会话过程中，在不影响会话状态的前提下，鉴别值可以改变。本标准不规定如何改变鉴别值的具体过程。

7.5 Echo 功能和不对称

在一对系统中，Echo功能在每个方向上可以独立的运行。系统可以只接收（环回）报文但不发送。

系统使用Echo功能时，系统的存活检测可以由Echo报文实现，控制报文的速率就可以降到比较低的速率。可以通过手动改变Required Min RX Interval字段来实现。参见7.9.3小节。

如果只有单方向使用Echo功能，没有使用Echo功能的系统需要提高BFD控制报文速率以满足对检测时间的需求。

系统应该发布Required Min RX Interval和Required Min Echo RX Interval的最小值，这样其他系统可以在一定范围内选择传输速率。除了环境因素，由于系统的设计为可以同时接受BFD流和Echo流，发布两个值时也需要考虑到这一点。

7.6 Poll Sequence

Poll Sequence主要是在某些环境中用于确认远端系统是否已经感知到参数的改变。在命令模式中也用于确认通路的双向连通性。

系统周期性的发送设置了Poll（P）比特位的BFD控制报文。当其他系统收到Poll之后，会立即发出一个设置了Final(F)位的BFD控制报文，这个响应报文的发送不受正在进行的周期性发送的BFD控制报文的影响。发送Poll sequence的系统收到携带Final的报文之后，Poll sequence过程结束。后续的BFD控制报文的Poll（P）位设为空。BFD控制报文不能同时设置Poll(P)和Final (F)位。

如果系统正在发送周期性的BFD控制报文（远端系统没有处于命令模式），执行Poll Sequence必须是将设置正在周期性发送的报文的Poll (P)位，不允许发送额外的控制报文。

在Poll Sequence结束后，如果远端是命令模式，系统会请求Poll Sequence停止周期性的BFD控制报文传送；如果不是，系统就回到周期性的BFD控制报文发送过程，控制报文的Poll (P)位为空。

完整的Poll Sequence过程是在每个方向都有一个单独的报文。但是也可能有意外情况导致发送多个Poll报文，比如报文丢失，过长时间的延迟等。

7.7 命令模式（Demand Mode）

命令模式需要设置BFD控制报文的Demand (D)位，BFD控制报文的发送在每个方向上是独立的。系统收到设置Demand (D)位的报文后，停止周期性的BFD控制报文的发送。如果两个系统都进入了命令模式，后面将不再周期性发送BFD控制报文。

使用命令模式时，需要有另外的机制来监测两个系统之间的联通性。两个方向上可以使用不同的机制。可以根据接收到的远端系统的流量判断，也可以使用Echo功能。本标准不做规定

使用命令模式的系统可以通过Poll Sequence来验证双向联通性。Poll发送之后，如果没有收到Poll的响应，会一直重复发送，直到监测时间超时为止，这时可以认为会话结束。如果命令模式仅在本地运行，执行Poll Sequence只需将周期性发送的BFD控制报文的Poll (P)设置即可。

命令模式中的检测时间和异步模式不同，是基于本地系统的传输速率而不是远端系统的传输速率，这种算法可以保证Poll Sequence机制的正常工作。详见7.9.4小节。

需要注意的是Poll机制的启动需要两个系统协商得到的检测时间大于往返时间。该限制的实施方法本标准不做规定。

命令模式通过设置或者清除Demand (D)位来启动或者关闭，不影响BFD会话的状态。需要注意的是必须在会话的双方都已经确认会话处于Up状态之后，才能设置Demand位（本地系统认为会话已经Up，远端系统通过State (Sta)字段报告Up状态）。

如果在传输过程中Demand (D)位的值被改变，传输系统必须发起一次Poll Sequence，将比特位的改变通知会话双方系统。

在有一方或者两方系统启动了命令模式后，如果将要传递的BFD控制报文与前一个报文不同，需要发起一个Poll Sequence过程，不设置Poll (P)和Final (F) 比特位，以确保改变的参数可以传送到远端系统，远端系统能够对这些改变进行确认。

使用BFD检测的两个系统可能会采取不同的下层检测机制，因此每个系统都无法完全获得Detection Time的全部特征。一个特定系统的总Detection Time等于Poll Sequence初始化以前的时间加上计算出的Detection Time之和。

需要注意的是如果命令模式仅在一个方向启动，将会丢失对双方向连接性的验证（只有发起命令模式的系统到其他系统的方向上的连接能够被验证）。本标准不规定另一方向的验证方法。

7.8 认证

7.8.1 概述

在BFD控制包中可以存在可选的认证部分。认证部分用于承载所有使用中的认证类型所需的必要信息，使得接收系统来判断收到数据包的合法性。具体的机制与使用的认证类型相关，但总得来说，发送系统把一些信息放在认证部分用于标识数据包的合法性，接收系统可以对认证部分进行检查，然后接受数据包进行进一步处理，或丢弃。

显然两个系统应采用同一种认证类型，以外还有相关的密钥和必要的信息。协商认证类型、密钥交换等内容由本标准之外的方式实现。

在之后的章节内，“接受”一个数据包意味着，这个数据包已通过了认证；数据包可能因为7.9.6中规定的接收规则里描述的其他的原因，被丢弃。

支持认证必须支持SHA1认证算法，其他形式的认证为可选。

7.8.2 启用和禁用认证

会话过程中可能会需要启用或禁用认证，但不中断会话的过程。具体实现机制不在本标准规定之内。

在一个简单的应用中，当认证打开或关闭时，BFD会话会失败，因为数据包接收规则最基本的需求是本地与远端的主机或多或少进行同步操作（在检测时间内）——一个要认证的数据包只在认证“使用中”才会被接受。

一种可能的实现方法是建立一个会话，此会话中配置好认证，但没有“使用”，直到收到第一个有匹配的认证部分数据包（提供了需要的同步）。同样，认证可以配成“关闭”，但仍在使用，直到收到第一个没有认证部分的数据包。

为了避免安全的风险，这种方式的实现应只允许认证状态在不经干预的情况下最多变化一次（这样认证不会因为收到远端BFD控制包导致反复开关）。除非希望使能或关闭认证，一个会话应不允许认证状态因收到BFD控制包而变化。

7.8.3 简单密码认证

最直接的（也是最弱）的认证形式就是简单密码认证。这种认证方式里，在每一个系统里配置一个或多个密码（有相应的密钥ID），在每一个BFD控制包里，带有一个密码/ID对。系统收到数据包，如果密码和密钥ID与本端配置的密码/ID对相匹配，则接收这个数据包。

使用简单密码认证的传送

一个会话当前使用的密码和密钥ID必须保存在每一个BFD控制包的认证部分。认证类型字段必须设为1（简单密码）。认证长度字段必须设成正确的长度（4到19字节）。

使用简单密码认证的接收

如果收到BFD控制包不包含认证部分，或认证类型不为1（简单密码认证），这个收到的数据包必须丢弃。

如果认证密钥ID字段与配置的密码ID不匹配，接收的包必须丢弃。

如果认证长度字段不等于密钥ID选中的密码长度加3，该数据包必须丢弃。

如果密码字段与密钥ID选中的密码不匹配，该数据包必须丢弃。

否则接收该数据包。

7.8.4 密钥 MD5 与严谨的密钥 MD5

密钥MD5与严谨的密钥MD5认证机制使用与在其他协议里的使用十分相似，在这种认证方式里，在每个系统上配一个或多个密钥（及与之相应的密钥ID）。一个密钥经过MD5摘要计算，放入BFD控制包中，但密钥本身不会在数据包中传送。为了防止重放攻击，在数据包中有一个序列号。对于密钥MD5，这个序列号一段时间递增一次，对于严谨的密钥MD5，这个序列号在每次传送数据时都会递增一次。

接收系统收到数据包后，如果密钥ID与配置的密钥相匹配，且对应的密钥MD5摘要与数据包中的一致，以及序列号大于或等于上一个收到的序列号（对于密钥MD5），或严格地大于上一个接收的序列号（对于严谨的密钥MD5）。

发送使用密钥MD5和严谨的密钥MD5认证

认证类型字段必段为2（密钥MD5）或3（严谨的密钥MD5）。认证长度必须设为24.认证密钥ID字段必段设成当前密钥相应的ID。序列号字段必须设成bfd.XmitAuthSeq。

当前认证密钥值必须放在认证密钥/摘要字段。一个MD5摘要必须对整个BFD控制包进行计算。摘要的结果必须在传送之前存放在认证密钥/摘要字段。

对于密钥MD5，bfd.XmitAuthSeq可能以循环方式进行递增（该字段为32比特无符号类型）。bfd.XmitAuthSeq在会话状态改变，或当发送BFD控制包装载了与前一包不同内容时，应进行递增。何时bfd.XmitAuthSeq进行递增，不在本标准讨论范围内。

对于严谨的密钥MD5，bfd.XmitAuthSeq必须以循环方式进递增（该字段为32比特无符号类型）。

接收使用密钥MD5和严谨的密钥MD5认证

如果收到BFD控制包不包含认证部分或认证类型不正确（2为密钥MD5，3为严谨密钥MD5），收到的包必须丢弃。

如果认证密钥ID字段与配置的认证密钥ID不匹配，收到的包必须丢弃。

如果认证长度字段不等于24，该数据包必须丢弃。

如果bfd.AuthSeqKnown为1，检查序列号字段。对于密钥MD5，这个序列号在bfd.RcvAuthSeq到bfd.RcvAuthSeq+(3*Detect Mult)的取值之外（包括这两个值）（做为32位无符号类型），收到的包必须丢弃。对于严谨的密钥MD5，如果序列号在在bfd.RcvAuthSeq+1到bfd.RcvAuthSeq+(3*Detect Mult)的取值之外（包括这两个值）（做为32位无符号类型），收到的包必须丢弃。

否则(bfd.AuthSeqKnown为0)，bfd.AuthSeqKnown必须设为1，bfd.AuthSeqKnown必须设为收到的序列号字段的值。

把认证密码/摘要字段替换成由认证密钥ID字段指定的认证密钥。如果BFD控制包的全部字段的MD5摘要等于收到的认证密钥/摘要字段，收到的数据包必须接受。否则（摘要不等于认证密钥/摘要字段），收到的包必须丢弃。

7.8.5 密钥 SHA1 和严谨的密钥 SHA1 认证

密钥SHA1与严谨的密钥SHA1认证机制使用与在其他协议里的使用十分相似，在这种认证方式里，在每个系统上配一个或多个密钥（及与之相应的密钥ID）。一个密钥经过SHA1摘要计算，放入BFD控制包中，但密钥本身不会在数据包中传送。为了防止重放攻击，在数据包中有一个序列号。对于密钥SHA1，这个序列号一段时间递增一次，对于严谨的密钥SHA1，这个序列号在每次传送数据时都会递增一次。

接收系统收到数据包后，如果密钥ID与配置的密钥相匹配，且对应的密钥SHA1摘要与数据包中的一致，以及序列号大于或等于上一个收到的序列号（对于密钥SHA1），或严格地大于上一个接收的序列号（对于严谨的密钥SHA1）。

发送使用密钥SHA1和严谨的密钥SHA1认证

认证类型字段必段为4（密钥SHA1）或5（严谨的密钥SHA1）。认证长度必须设为28。认证密钥ID字段必段设成当前密钥相应的ID。序列号字段必须设成bfd.XmitAuthSeq。

当前认证密钥值必须放在认证密钥/摘要字段。一个SHA1摘要必须对整个BFD控制包进行计算。摘要的结果必须在传送之前存放在认证密钥/摘要字段。

对于密钥SHA1，bfd.XmitAuthSeq可能以循环方式进行递增（该字段为32比特无符号类型）。bfd.XmitAuthSeq在会话状态改变，或当发送BFD控制包装载了与前一包不同内容时，应进行递增。何时bfd.XmitAuthSeq进行递增，不在本标准讨论范围内。参见后文“安全考虑”。

对于严谨的密钥SHA1，bfd.XmitAuthSeq必须以循环方式进递增（该字段为32比特无符号类型）。

接收使用密钥SHA1和严谨的密钥SHA1认证

如果收到BFD控制包不包含认证部分或认证类型不正确（4为密钥SHA1，5为严谨密钥SHA1），收到的包必须丢弃。

如果认证密钥ID字段与配置的认证密钥ID不匹配，收到的包必须丢弃。

如果认证长度字段不等于28，该数据包必须丢弃。

如果bfd.AuthSeqKnown为1，检查序列号字段。对于密钥SHA1，这个序列号在bfd.RcvAuthSeq到bfd.RcvAuthSeq+(3*Detect Mult)的取值之外（包括这两个值）（该字段为32位无符号类型），收到的包必须丢弃。对于严谨的密钥SHA1，如果序列号在在bfd.RcvAuthSeq+1到bfd.RcvAuthSeq+(3*Detect Mult)的取值之外（包括这两个值）（该字段为32位无符号类型），收到的包必须丢弃。

否则(bfd.AuthSeqKnown为0)，bfd.AuthSeqKnown必须设为1，bfd.AuthSeqKnown必须设为收到的序列号字段的值。

把认证密码/摘要字段替换成由认证密钥ID字段指定的认证密钥。如果BFD控制包的全部字段的SHA1摘要等于收到的认证密钥/摘要字段，收到的数据包必须接受。否则（摘要不等于认证密钥/摘要字段），收到的包必须丢弃。

7.9 功能

7.9.1 说明

系统处于“Echo 功能激活”状态时，可以发送BFD Echo报文。在此之前，需要建立会话，并且其他系统做好了环回Echo报文的准备。

本地系统处于“命令模式激活”状态时，本地系统的bfd.DemandMode为1，会话为Up状态，远端系统也已经处于Up状态。

远端系统处于“命令模式激活”状态时，远端系统的bfd.RemoteDemandMode为1（远端系统在最近收到的BFD控制报文中设置Demand (D)位），会话为Up状态，远端系统正在发送的信令表明正处于Up状态。

7.9.2 状态变量

状态变量是会话过程中的少量信息，通过这些信息可以跟踪过程的进行情况。下面是描述BFD机制的一系列状态变量。如果协议遵守状态变量的描述，会话状态就能够通过一些方法进行跟踪。

状态变量只能在会话创建时进行初始化，随后由状态机进行操作；后续即便发生会话失败或者重建的情况，也不能再次进行初始化。

会话状态创建后，如果从远端收到最少一个BFD控制报文，从最后一个收到的BFD控制报文的时间算起，会话必须最少保留一个Detection Time周期（见7.9.4小节对Detection Time的规定）。在会话切换时，可以保留定时参数。放入会话状态可以被保留更长的时间。如果没有收到BFD控制报文，会话或者保留或者拆除，都由系统决定，本标准不做规定。

本标准中的所有状态变量都以"bfd.Xx"的形式表示，以与协议报文中携带的字段区别。第六章规定的参数字段都是拼写完整的。

bfd.SessionState

会话的常见状态（Init, Up, Down, 或AdminDown）。本标准不规定会话状态改变时系统的具体操作，但建议状态发生改变时通知系统的其他部分，尤其是进入和离开Up状态时。该变量初始化时必须设为Down。

bfd.RemoteSessionState

最近一次收到远端系统的BFD控制报文中，State (Sta)字段所表示的会话状态。该变量初始化时必须设为Down。

bfd.LocalDiscr

BFD会话的本地鉴别值，用来唯一的标识本会话。该值必须能将会话从所有BFD会话中唯一区别出来，不能为0。为提供安全性，可以选择随机的数值（必须唯一）。本标准不规定如何选择数值。

bfd.RemoteDiscr

BFD会话的远程鉴别值，由远端系统选定，对本地系统完全不透明。初始化时需要设为0。如果在一个Detection Time周期内没有收到远端系统发来的有效的，验证过的BFD报文，该值必须被设为0。

bfd.LocalDiag

诊断代码，说明最近一次本地会话状态改变的原因。初始化时必须设为0(无诊断)。

bfd.DesiredMinTxInterval

系统当前时间传输BFD控制报文的最小间隔，以微秒为单位， less any jitter applied。实际的传输使用的间隔由系统协商获得。根据7.9.3小节的规定，该值初始化时最小设为1秒（1,000微秒）。

bfd.RequiredMinRxInterval

系统接收BFD报文的最小间隔，以微秒为单位。本标准不规定变量如何设置。如果设为0值，系统不接受任何的周期性发送的BFD控制报文。

bfd.RemoteMinRxInterval

最近一个收到的远端系统的Required Min RX Interval。该值初始化时必须为1。

bfd.DemandMode

如果本地系统要使用命令模式，设为1；否则为0。

bfd.RemoteDemandMode

如果远端系统要使用命令模式，设为1；否则为0。该值取自于最近收到的BFD控制报文的Demand (D)比特位的值。该值初始化时必须为1。

bfd.DetectMult

BFD控制报文请求的Detection Time的乘数。本次会话的Detection Time等于协商的控制报文传输间隔乘以干变量。该变量必须是一个非0整数。7.9.4小节有详细规定。

bfd.AuthType

本次会话的认证类型，遵守5.1节的规定；如果不进行认证则设为0。

bfd.RcvAuthSeq

一个32位的无符号整数，是接下来希望收到的密钥MD5或者SHA1认证的序列号。初始值可以任意。

bfd.XmitAuthSeq

一个32位的无符号整数，是接下来要传输的密钥MD5或者SHA1认证的序列号。初始值必须是一个任意的32比特变量。

bfd.AuthSeqKnown

如果将要收到的密钥MD5或者SHA1认证的序列号已知，设为1；如果未知，则为0。初始值必须为0

如果两个Detection Time周期之后，当前会话没有收到任何报文，该变量必须设为0，以保证在远端系统重启之后序列号能够重新同步。

7.9.3 定时器协商

BFD报文的传输间隔和会话的检测时间都由定时器值决定，在会话过程持续不断的对该值进行协商，随时都可能改变。协商过程和定时器值和会话的方向无关。

系统在BFD控制报文中会报告接收和发送BFD报文的速率。作为本节的特例，如果bfd.DesiredMinTxInterval和bfd.RemoteMinRxInterval较大的一个值大于间隔值，系统不能传送BFD控制报文，也就是说，系统报告的较慢的速率决定传输速率。

BFD控制报文的周期性传输应该设置最高25%的抖动，也就是将传输间隔降低0到25%之间的随机值，从而避免自同步。这样，报文之间的平均间隔比协商值要减少12.5%。

如果bfd.DetectMult等于1，BFD控制报文的传输间隔必须不大于协商的传输间隔的90%，但不小于75%。这样远端计算出的DetectTime不会先于接收到下一个BFD控制报文的时刻。

7.9.4 计时器控制

BFD报文传输间隔的时间值和会话Detection Time都可以随时改变，但不能影响会话状态。本节的要求主要用于定时器参数改变的情况。

bfd.DesiredMinTxInterval或者bfd.RequiredMinRxInterval改变时，必须启动Poll Sequence。如果收到Poll Sequence的系统需要改变时间参数，新的参数值可以放在Final (F)字段，Poll Sequence可以在此之后。

如果bfd.DesiredMinTxInterval值增加且bfd.SessionState状态为Up，在上段的Poll Sequence结束之前，不允许改变实际的传输间隔，以保证远端系统可以在传输间隔增加之前及时更新Detection Time。

如果bfd.DesiredMinTxInterval值减少且bfd.SessionState状态为Up，在Poll Sequence结束以前，远端系统计算Detection Time时必须使用前一个bfd.RequiredMinRxInterval值。这样远端系统可以在Detection Time降低以前以较高的速率（和接收报文的速率相同）传输报文。

当bfd.SessionState为非Up状态，系统必须将bfd.DesiredMinTxInterval设为不小于1秒（1,000毫秒）的值。这样就可以使得处于非Up状态的BFD会话占用的带宽非常的小。

远端最小接收间隔bfd.RemoteMinRxInterval减小（减小Required Min RX Interval）时，本地系统需要相应减小传送间隔，如果远端系统没有处于命令模式（Demand mode），本地系统必须迅速使用新的间隔时间。如果由于新的间隔时间太短，导致系统不能及时按照新间隔发送控制报文，本地系统必须尽快发出下一个周期性的BFD控制报文。

如果Echo功能是激活的，系统应该将bfd.RequiredMinRxInterval设为不小于1秒（1,000毫秒）。这主要是因为实际的检测是由BFD Echo功能执行，BFD控制报文的流量可以尽量压缩。

除上述情况外，其他情况导致的时间参数的改变也必须迅速生效（改变传输速率或者检测时间，或者二者同时改变在）。

如果有来自多个报文的多个参数同时要求使用Poll Sequence机制（Final位没有清空），会导致Poll Sequence的混乱，有如下三种选择：

1）多个参数使用一个单独的BFD控制报文通信（Final位清空）

2）Poll Sequence结束以避免混乱后，在发起下一次Poll Sequence之前预留足够的时间（至少自上次Poll传输后，再进行一次报文往返传送的时间）。

3）在Poll Sequence结束，下一次Poll Sequence发起之前，必须收到一个Final (F)位清空的额外的BFD控制报文。

7.9.5 检测时长（Detection Time）的计算

Detection Time是指一个时间段，在该周期内如果没有收到任何BFD报文，会话即被认为失败，Detection Time不在协议中显式传送。接收系统根据协商的传输间隔和检测乘数计算Detection Time，不同方向的Detection Time的计算相互独立，可以是不同的数值。

命令模式和异步模式的检测时间的计算方法稍有不同。

在异步模式下，本地系统的Detection Time，等于收到的远端系统的Detect Mult值乘以与远端系统协商的传输间隔（bfd.RequiredMinRxInterval值和收到的上一个 Desired Min TX Interval值中较大的一个）。连续丢失报文导致会话宣布中断时，已经丢失的报文数是Detect Mult的值（粗略的计算，受抖动的影响）。

如果没有使用命令模式，经过了Detection Time值规定的时间之后，没有从远端系统收到任何BFD报文，并且bfd.SessionState状态为Init或者Up，会话已经中止—本地系统必须设置bfd.SessionState为Down，bfd.LocalDiag为1(Control Detection Time Expired)。

在命令模式下，本地系统计算Detection Time，是将bfd.DetectMult乘以本地系统协商的传输间隔(bfd.DesiredMinTxInterval和bfd.RemoteMinRxInterval较大的一个)。连续丢失报文导致会话宣布中断时，已经丢失的报文数就是bfd.DetectMult的值（粗略的计算，受抖动的影响）。

如果使用命令模式，在一个Poll Sequence初始化（第一个设置Poll 位的BFD报文发出）以后，经过Detection Time值规定的时间之后，会话中止，--本地系统必须设置bfd.SessionState为Down，bfd.LocalDiag为1(Control Detection Time Expired)。

7.9.6 Echo 检测失败

如果正在使用Echo功能，但已经有足够数量的Echo包没有收到，会话中断，本地系统必须设置bfd.SessionState为Down，bfd.LocalDiag为2（Echo Function Failed）。

检测Echo功能失败的方法本标准不做规定，任何能够检测出通信故障的方法都是可行的。

7.9.7 BFD 控制报文的接收

收到BFD控制报文后，必须遵守如下步骤按顺序进行处理。如果控制报文按照下述规则被丢弃，在丢弃时必须同时停止对BFD控制报文的处理。

如果版本号不正确（不是1），报文必须被丢弃。

如果Length字段的值小于报文长度的最小值（A比特为空时是24位，A比特设置时为26位），报文必须被丢弃。

如果Length字段大于封装协议的载荷，报文必须被丢弃。

如果Detect Mult字段为0，报文必须被丢弃。

如果Multipoint (M)非0，报文必须被丢弃。

如果My Discriminator字段非0，报文必须被丢弃。

如果Your Discriminator字段非0，必须将该字段分配到相应的会话。如果没有合适的会话相匹配，报文必须被丢弃。

如果Your Discriminator字段不为0，但State状态不是Down或者AdminDown，报文必须被丢弃。

如果Your Discriminator字段为0，需要结合其他的参数确认和控制报文相关的会话，比如源地址信息，My Discriminator字段，报文的接收端口等。本标准不规定参数的选择方法，如果没有匹配到合适的会话，可以创建一个新会话，或者丢弃。

如果A比特设置，但是没有认证方法被使用（bfd.AuthType为0），报文必须被丢弃。

如果A比特设置，控制报文必须遵守7.8节的规定，按照正在使用的认证类型(bfd.AuthType)进行认证，这可能会导致报文的丢弃。

设置 bfd.RemoteDiscr 为My Discriminator的值。

设置bfd.RemoteState 为State (Sta)字段的值。

设置bfd.RemoteDemandMode 为Demand (D) 的值。

设置bfd.RemoteMinRxInterval 为Required Min RX Interval的值。

Required Min Echo RX Interval字段为0时，如果有正在传输的Echo报文，必须停止传输。

本地系统正在传输Poll Sequence时，如果收到设置了Final (F)位的报文，Poll Sequence必须结束。

按照7.9.2小节要求更新传输间隔。

按照7.9.4小节要求更新Detection Time。

```
If bfd.SessionState is AdminDown
    Discard the packet

If received state is AdminDown
    If bfd.SessionState is not Down
        Set bfd.LocalDiag to 3 (Neighbor signaled
            session down)
        Set bfd.SessionState to Down

Else

    If bfd.SessionState is Down
        If received State is Down
            Set bfd.SessionState to Init
        Else if received State is Init
            Set bfd.SessionState to Up

    Else if bfd.SessionState is Init
        If received State is Init or Up
            Set bfd.SessionState to Up

    Else (bfd.SessionState is Up)
```

If received State is Down

Set bfd.LocalDiag to 3 (Neighbor signaled session down)

Set bfd.SessionState to Down

检查是否在使用Demand mode（见7.7节）

如果bfd.RemoteDemandMode等于1，bfd.SessionState状态为Up，并且 bfd.RemoteSessionState状态为Up，远端系统正在使用Demand mode，本地系统必须停止周期性发送的BFD控制报文（见7.8.7小节）。

如果bfd.RemoteDemandMode等于0，或者bfd.SessionState状态不是Up或者bfd.RemoteSessionState状态不是Up，远端系统没有使用Demand mode，本地系统必须发生周期性的BFD控制报文。

如果设置了Poll (P)位，向远端系统发送一个Poll (P)清空BFD控制报文。Final (F)设置（见7.9.7小节）。

如果报文没有被丢弃，接收后遵守7.9.4小节检测时间超时规则。

7.9.8 BFD 控制报文的传输

BFD控制报文的传输速率必须遵守7.9.2小节的协商结果，本节中有特殊规定的除外。传输间隔必须等于bfd.DesiredMinTxInterval和bfd.RemoteMinRxInterval的最大值，因此任何一个值改变后都需要重新计算传输间隔。

bfd.RemoteDiscr值为0时，系统不能主动传送BFD控制报文，转为被动接收角色（taking the Passive role）。

bfd.RemoteMinRxInterval值为0时，系统不能周期性的传输BFD控制报文。

远端系统激活命令模式（bfd.RemoteDemandMode等于1，bfd.SessionState设为Up，bfd.RemoteSessionState设为Up）后，本地系统不能发送周期性的BFD控制报文，不能传输Poll Sequence。

如果收到的BFD控制报文Poll (P)位为1，系统必须尽快发送Poll (P)位清空且Final (F)位设置的BFD控制报文，不受限于传输定时器及其他的传输限制，也不受限于会话状态，是否正在使用Demand mode等条件。系统可以限制此类报文的传输速率。如果限制生效，系统发布的Desired Min TX Interval值必须大于等于速率受限报文的传输间隔。

系统设置Demand (D)位需要满足如下条件：bfd.DemandMode为1，bfd.SessionState状态为Up，且bfd.RemoteSessionState状态为Up。

如果BFD控制报文的内容和前一控制报文相比有改变（不是Poll和Final位），应该在周期性传输的控制报文之间的间隔传送一个BFD控制报文，将状态的改变的信息最快告知对端。

BFD控制报文的内容必须按照如下格式配置：

Version

设为当前版本号 (1).

Diagnostic (Diag)

设为bfd.LocalDiag.

State (Sta)

设为bfd.SessionState表示的值。

Poll (P)

如果系统正在发送Poll Sequence，设为1，否则为0.

Final (F)

如果本地系统正在发送的控制报文是对Poll (P)位的响应，设为1；否则为0。

Control Plane Independent (C) （控制平面无关）

如果本地系统的BFD执行和控制平面无关（也就是说控制平面中断时可以继续执行BFD），设为1

Authentication Present (A)

如果会话使用了认证机制（bfd.AuthType非0），设为0；否则为0。

Demand (D)

如果bfd.SessionState是Up且bfd.RemoteSessionState也是Up，设为bfd.DemandMode；否则为0。

Multipoint (M)

设为0。

Detect Mult

设为 bfd.DetectMult。

Length

固定报文头长度加上认证部分的和。

My Discriminator

设为bfd.LocalDiscr。

Your Discriminator

设为bfd.RemoteDiscr。

Desired Min TX Interval

设为bfd.DesiredMinTxInterval。

Required Min RX Interval

设为bfd.RequiredMinRxInterval。

Required Min Echo RX Interval

本地能够接受的Echo报文的最小间隔。设为0时，本地系统不能对Echo报文进行环回，因此远端系统不能发送Echo报文。

Authentication Section

使用认证功能（bfd.AuthType非0）时，根据7.8节的规则进行设置。否则该字段不出现。

7.9.9 BFD Echo 控制报文的接收

系统接收到BFD Echo报文之后，需要进行多路分配处理，将Echo报文分配相应的会话。在对接收到的Echo报文处理的过程中，必须同时执行检测Echo报文丢失的机制。

7.9.10 BFD Echo 报文的传送

bfd.SessionState没有处于Up状态时，不能传送BFD Echo报文。只有收到来自于远端系统的BFD控制报文的Required Min Echo RX Interval值非0时，才能传送BFD Echo报文。

当bfd.SessionState是Up状态时，可以传送BFD Echo报文。传送BFD Echo报文的间隔不能小于远端系统的Required Min Echo RX Interval值，以下情况除外：

传输速率可以有25%的抖动，实际的传输间隔可以在75% 到100%之间选择。在正常传输的Echo报文之间可以有一个单独的BFD Echo报文被传送。

7.9.11 Min Rx Interval 的改变

当来自于远端系统的BFD控制报文的速率需要改变时，bfd.RequiredMinRxInterval的值可以随时改变成合适的值。新的值将会在下一个发出的控制报文中传送，远端系统将会自动做出调整。

7.9.12 Min Tx Interval 的改变

当传送到远端系统的BFD控制报文的速率需要改变时（受限于邻居系统的需求），bfd.RequiredMinRxInterval的值可以随时改变成合适的值。新的值将会在下一个发出的控制报文中传送，远端系统将会自动做出调整。

7.9.13 Detect Multiplier 的改变

如果需要改变检测乘数，bfd.DetectMult可以改变为任意非0值。更新的值可以使用下一个BFD控制报文传送，无需启用Poll Sequence。

7.9.14 Echo 功能的启用或者停用

BFD Echo报文的启动或者停止根据需要随时进行。

将要发送BFD控制报文的Required Min Echo RX Interval参数设为0或者非0，就可以启动或者停止对接收到的BFD Echo报文的环回。

7.9.15 Demand Mode 的启用或者停用

Demand Mode的启用或者停用由bfd.DemandMode的参数设置决定。

一旦远端系统的Demand mode停用，本地系统必须按照7.9.7小节的规定开始发送周期性的BFD控制报文。

7.9.16 转发平面复位

如果本地系统的转发平面复位，远端系统不能再和本地转发平面联系。本地系统必须将bfd.LocalDiag设为4(Forwarding Plane Reset)，将bfd.SessionState状态设为Down。

7.9.17 管理层面的控制

在对BFD会话做管理层面的启用或停用时，必须遵守如下步骤：

If enabling session
    Set bfd.SessionState to Down

Else
    Set bfd.SessionState to AdminDown
    Set bfd.LocalDiag to an appropriate value
    Cease the transmission of BFD Echo packets

如果有来自已经中断的底层通路的BFD报文，可能就需要执行管理层面的控制功能，将该会话状态设为诊断性的Path Down。

在系统将状态改为AdminDown 之后，BFD控制报文应该至少再传送一个Detection Time周期，以保证远端系统能够感知到状态的改变；为了保持系统间的会话，BFD控制报文也可以继续进行传输，详见7.9.18小节。

7.9.18 级联通路

如果BFD所监测的通路和其他通路之间有级联关系。在BFD会话的某一段通路出现问题时，可能会要求将故障发布出去（在活跃的BFD监测和其他监测技术之间建立活动链接）。

为此定义了两个诊断代码：Concatenated Path Down和Reverse Concatenated Path Down。第一个代码发布通路故障（通往互连系统方向的级联通路故障），第二个发布反向通路故障（可能是来自级联系统的通路故障，假定为双向通路故障）。

系统通过设置bfd.LocalDiag为合适的诊断代码来发布故障，但不会拆除BFD会话。如果远端系统没有活动的命令模式，诊断代码由周期性发送的BFD控制报文携带。如果远端系统有活动的命令模式（本地系统没有周期性的发送BFD控制报文），必须发起一个Poll Sequence来确保诊断代码能够被传送。如果BFD会话随后发生故障，那么要将故障的详细原因重写入诊断代码。一旦BFD会话为Up状态，若要重新发布级联通路失败的信息，是否再次执行上述过程取决于互联代理。

7.9.19 会话 Down 状态保持

在BFD会话建立时，系统可能会由于管理会话速率等原因，阻止会话的建立。阻止的方法可以是保持会话状态为Down 或者AdminDown。

会话Down状态保持有两种实现的机制，第一种是系统被要求保持会话状态（包括时间参数），在会话状态为down时状态也继续保持。在一个Detection Time周期之后没有收到任何BFD控制报文才能释放。这意味着系统可以拆除一个会话，然后发送一个非常大的Required Min RX Interval值来控制接收报文的速率。

另外，系统可以发送Required Min RX Interval为0的报文，通知远端系统停止发送报文。

如果本地系统继续发送BFD控制报文，远端系统需要遵守Required Min RX Interval规定的值。如果远端系统在一个Detection Time周期内不接收任何BFD控制报文，可以将bfd.RemoteMinRxIvl设为非常小的值，这样远端系统就可以按照自己的传输速率进行传输。

8 操作问题

BFD通常作为网络的基础设施的关键部分进行部署，因此，部署时需要对网络汇总的各种影响因素综合考虑以避免造成不必要的中断。

网络中使用的某些机制，如防火墙或者策略处理功能实体，都会阻塞BFD包从而造成BFD失败。

控制报文发送的调度机制，会受到管理策略，流量整形，优先级队列等因素的影响。BFD报文的发送有较强的时效性，如果Detection Time和报文发送或者接收的速率范围类似，会对BFD操作造成潜在影响。在安装部署时需要考虑到这些因素，尤其是使用非常短的Detection Time时。

9 IANA

本标准中有两个IANA管理的注册值，第一个是5.1节的"BFD 诊断代码"，注册的初始值如下：

值	BFD 诊断 名称
0	无诊断
1	控制检测时间超时
2	Echo 功能失败
3	邻居发送会话中断信号
4	转发平面复位
5	通路中断
6	级联通路中断
7	管理性中断
8	反向级联通路中断
9~31	保留

第二个是5.1节的"BFD认证类型"，注册的初始值如下：

值	BFD 认证类型名称
0	保留
1	简单密码
2	密钥 MD5
3	严谨的密钥 MD5
4	密钥 SHA1
5	严谨的密钥 SHA1
6~255	保留

10 安全

BFD和网络基础设施（比如路由协议）的稳定性紧密相关，在BFD会话上的攻击造成的影响可能会非常严重，最终会导致拒绝服务，链路中断（或者不能启动）

如果BFD运行在网络层协议上，会存在明显的拒绝服务的危险。

如果BFD建立在一个单独的链接上（物理的，或者一个安全的通道如IPsec），传输时必须将TTL 或者Hop Count设为最大值，接收时检查是否等于最大值；如果不是，BFD报文将被丢弃。

如果BFD允许在多跳或者不安全的tunnel上运行，应该使用认证字段。

不同的认证类型提供不同级别的安全能力。简单密码认证只能提供密码方式的认证，因此只能运行在BFD会话不会被侦听的网络设施之上。主要优点是可以使认真的计算工作量减到最小。

密钥MD5认证明显优于简单密码方式，密钥不会被侦听报文察觉。在序列号增时，非常容易实现重放攻击。因此按照要求，序列号应该尽量少（经常）增加，来平衡对抗重放攻击所需要计算工作量。

严谨的密钥MD5认证算法则更有优势，该算法要求序列号持续增加。由于每个包的序列号都增加，接收报文的窗口尺寸很小，并且初始序列号随机，重放攻击的可能大为降低。但是在会话开始，设定序列号的时候，仍然存在一个攻击窗口。该认证算法要求对每个发送和接收的报文进行MD5计算。

本章中所有关于MD5SHA1算法的评述同样适用于SHA1。

收发双方如果在会话开始时，都随机选择Local Discriminator值，无论采用何种认证算法，重放攻击的机会的可能性会大大降低。由于Local Discriminator会在会话过程中随时改变，也可以降低攻击的可能性。

中华人民共和国
通信行业标准
公众IP网络可靠性
双向转发检测（BFD）机制的技术要求
YD/T 2447-2013
*
人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷
*
开本：880×1230 1/16 2013年5月第1版
印张：2 2013年5月北京第1次印刷
字数：48千字
15115·95
定价：30元