



双向转发检测路由

本章介绍如何配置 ASA 以使用双向转发检测 (BFD) 路由协议。

- [关于 BFD 路由，第 1 页](#)
- [BFD 路由准则，第 4 页](#)
- [配置 BFD，第 5 页](#)
- [BFD 监控，第 9 页](#)
- [BFD 路由历史记录，第 10 页](#)

关于 BFD 路由

BFD 是一个检测协议，旨在为媒体类型、封装、拓扑和路由协议提供快速转发路径故障检测时间。BFD 可以在单播、点对点模式下对正在两系统之间转发的任何数据协议上运行。数据包在适用于媒体和网络的封装协议负载中携带。

除了快速转发路径故障检测外，BFD 还为网络管理员提供一致的故障检测方法。由于网络管理员可以使用 BFD 按照统一的速率检测转发路径故障，而不是为不同的路由协议呼叫机制采用不同的速率，因此网络分析和计划更简单，重新聚合时间一致且可预测。

BFD 异步模式和回应功能

不管是否启用回应功能，BFD 均可在异步模式下运行。

异步模式

在异步模式下，系统之间会定期发送 BFD 控制数据包，如果某一行中有大量此类数据包未被其他系统接收，则会话将宣布关闭。纯异步模式（无回应功能）很有用，因为它达到特定检测时间所需的数据包数量是回应功能所需数据包数量的一半。

BFD 回应功能

BFD 回应功能将回应数据包从转发引擎发送至直连单跳 BFD 邻居。回应数据包由转发引擎负责发送，并沿同一条路径重新进行转发，以执行检测。另一端的 BFD 会话不参与回应包的实际转发。回应功能和转发引擎负责检测进程，BFD 邻居之间发出的 BFD 控制数据包数量将减少。此

外，由于转发引擎在远程邻居系统上测试转发路径，并未涉及远程系统，因此数据包间的延迟差异增大了。这会导致故障检测时间缩短。

启用回应功能后，BFD可以使用较慢的计时器降低异步会话的速度并减少BFD邻居之间发送的BFD控制数据包的数量，从而降低处理开销，同时提高故障检测速度。



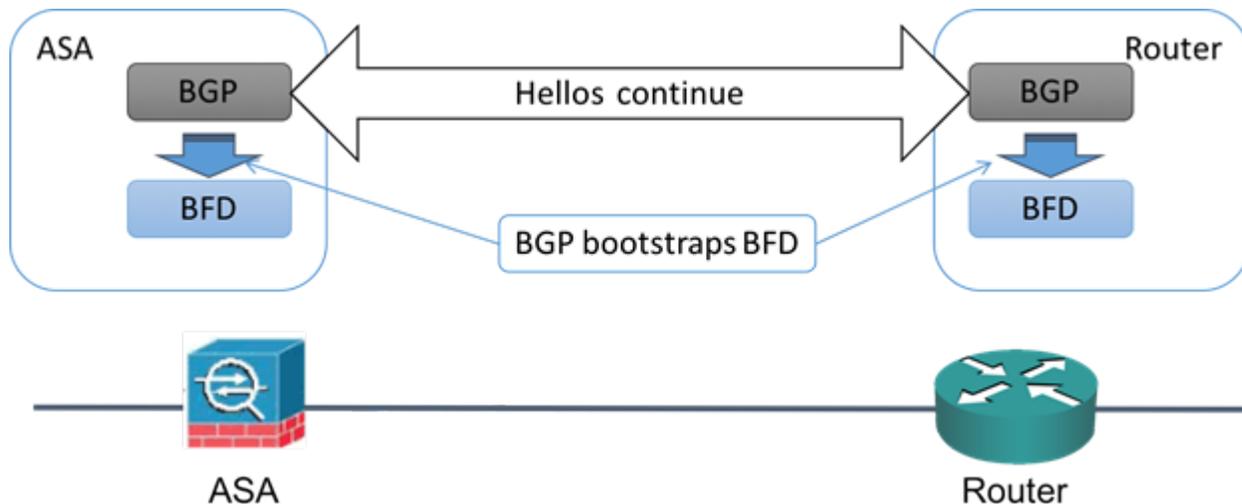
注释 IPv4 多跳或 IPv6 单跳 BFD 邻居不支持回应功能。

您可以在接口级别和路由协议级别启用BFD。您必须在两个系统（BFD对等体）上配置BFD。在接口上并且在相应路由协议的路由器级别启用BFD后，将会创建BFD会话，协商BFD计时器，并且BFD对等体在协商的级别互相发送BFD控制数据包。

BFD 会话设置

以下示例显示ASA和运行边界网关协议(BGP)的相邻路由器。当两台设备启动时，二者之间不会建立BFD会话。

图 1: 建立的 BFD 会话



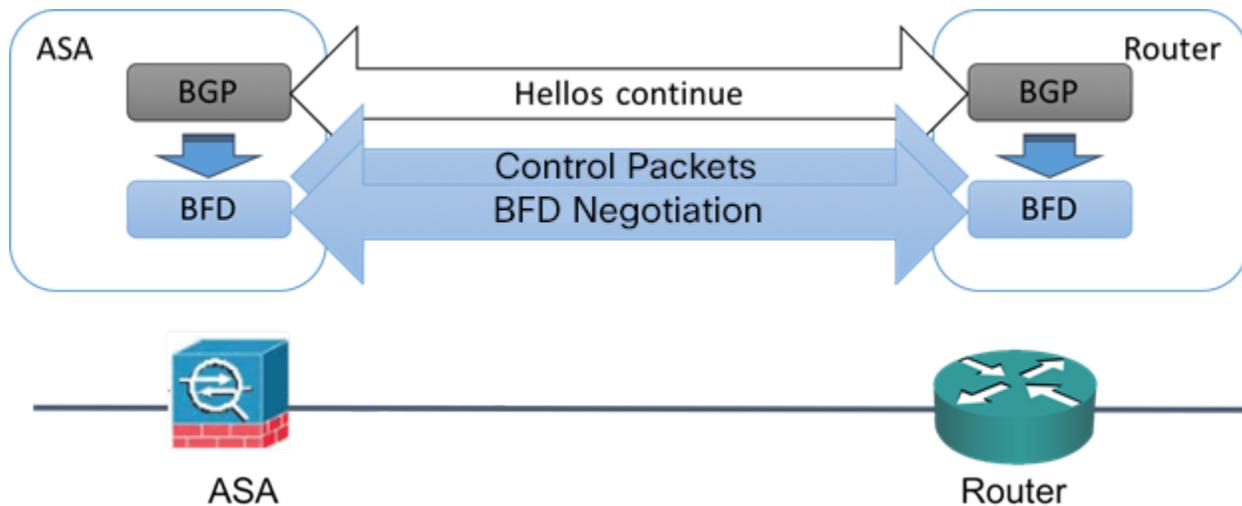
BGP 识别其 BGP 邻居后，会使用邻居的 IP 地址通过引导程序启动 BFD 进程。BFD 不是动态发现其对等体。它依靠配置的路由协议告知它要使用的 IP 地址以及要形成的对等体关系。

路由器上的 BFD 和 ASA 上的 BFD 共同形成 BFD 控制数据包，并开始以一秒的间隔向彼此发送数据包，直到 BFD 会话建立为止。来自任一系统的初始控制数据包都非常相似，例如 Vers、Diag、H、D、P 和 F 位都设置为零，State 设置为 Down。My Discriminator 字段设置为一个在传输设备上唯一的值。Your Discriminator 字段设置为零，因为 BFD 会话尚未建立。TX 和 RX 计时器设置为在设备配置中找到的值。

远程 BFD 设备在会话初始阶段收到 BFD 控制数据包后，会将 My Discriminator 字段中的值复制到自己的 Your Discriminator 字段中，并从 Down 状态过度到 Init 状态，最终进入 Up 状态。一旦两个系统都在各自控制数据包中看到自己的 Discriminator，会话即正式建立。

下图显示了建立的 BFD 连接。

图 2: 未建立 BFD 会话的 BGP



BFD 计时器协商

BFD 设备必须协商 BFD 计时器，以控制和同步 BFD 控制包的发送速率。设备需要确保以下条件，才能协商 BFD 计时器：

- 其对等设备看到包含本地设备的建议计时器的数据包
- 它发送 BFD 控制包的速度永远不会超过被配置为接收这些数据包的对等体
- 对等体发送 BFD 控制包的速度永远不会超过被配置为接收这些数据包的本地系统

Your Discriminator 字段和 H 位的设置足以使远程设备在首次计时器交换期间看到本地设备的数据包。在接收 BFD 控制包后，每个系统都将获得所需最小接收间隔，并将该间隔与其自己的所需最小发送间隔进行比较，然后取两个值中较大者（速度较慢者），并将该值用作其 BFD 数据包的传输速率。两个系统中速度较慢者将决定传输速率。

在协商这些计时器后，可在会话期间随时重新协商它们，而不会导致会话重置。更改其计时器的设备将在所有后续 BFD 控制包上设置 P 位，直到其收到通过远程系统设置了 F 位的 BFD 控制包为止。这种位的交换可以保护数据包，否则它们可能会在传输过程中丢失。



注释 远程系统设置 F 位，并不意味着它将接受新建议的计时器。它表示远程系统已经看到已经更改其中的计时器的数据包。

BFD 故障检测

如果 BFD 会话和计时器已经过协商，则 BFD 对等体按照协商的间隔互相发送 BFD 控制数据包。这些控制数据包作为检测信号，这非常类似于 IGP 呼叫协议，不同之处是速率得到了显著加速。

只要每个 BFD 对等体在配置的检测间隔（所需的最小 RX 间隔）内接收到 BFD 控制数据包，则 BFD 会话会保持，并且与 BFD 关联的任何路由协议均保持其邻接关系。如果 BFD 对等未在此间隔内收到控制数据包，则会向参与该 BFD 会话的所有客户端通知故障情况。路由协议可确定对该信息的适当响应。典型的响应是终止路由协议对等会话和重新收敛，从而绕过出现故障的对等体。

每次 BFD 对等体在 BFD 会话中成功接收到 BFD 控制数据包时，该会话的检测计时器都会重置为零。因此故障检测取决于接收的数据包，而不是接收方上次何时传输数据包。

BFD 部署场景

以下内容介绍了 BFD 在这些特定场景中如何运行。

故障切换

在故障切换场景中，将在主用设备与邻居设备之间建立和保留 BFD 会话。备用设备不会通过邻居保留任何 BFD 会话。当发生故障切换时，新主用设备必须通过邻居发起会话建立，因为主用设备与备用设备之间的会话信息没有同步。

对于无中断重新启动/NSF 场景，客户端 (BGP IPv4/IPv6) 负责通知其邻居关于事件的信息。当邻居收到该信息时，它将保留 RIB 表，直到故障切换完成为止。在故障切换期间，设备上的 BFD 和 BGP 会话将关闭。在故障切换完成后，当 BGP 会话启动时，将在邻居之间建立新的 BFD 会话。

跨网络 EtherChannel 和 L2 集群

在跨网络 EtherChannel 集群场景中，将在主设备与其邻居之间建立和保留 BFD 会话。从属设备不会通过邻居保留任何 BFD 会话。如果由于交换机上的负载均衡而将 BFD 数据包路由到从属设备，则该从属设备必须通过集群链路将此数据包转发到主设备。当发生集群故障恢复时，新主设备必须通过邻居发起会话建立，因为主设备与从属设备之间的会话信息没有同步。

单个接口模式和 L3 集群

在单个接口模式集群场景中，单个设备将通过其邻居保留其 BFD 会话。

BFD 路由准则

情景模式准则

支持单一和多情景模式。

防火墙模式准则

在路由防火墙模式下受支持；支持独立、故障切换和集群模式。在故障切换和集群接口上不支持 BFD。在集群中，仅在主设备上支持此功能。在透明模式下不支持 BFD。

IPv6 规定

IPv6 不支持回送模式。

其他规定

支持 BGP IPv4 和 BGP IPv6 协议。

不支持 OSPFv2、OSPFv3、IS-IS 和 EIGRP 协议。

不支持用于静态路由的 BFD。

不支持传输和隧道上的 BFD。

配置 BFD

本节介绍如何在系统中启用和配置 BFD 路由进程。

过程

步骤 1 创建 BFD 模板，第 5 页。

步骤 2 配置 BFD 接口，第 7 页。

步骤 3 配置 BFD 映射，第 8 页。

创建 BFD 模板

本节介绍创建 BFD 模板和进入 BFD 配置模式所需的步骤。

BFD 模板指定一组 BFD 间隔值。BFD 模板中配置的 BFD 间隔值并不是特定于单个接口。此外，还可以为单跳和多跳会话配置身份验证。可以仅在单跳上启用回应。

过程

步骤 1 通过创建单跳或多跳 BFD 模板在 ASA 上作为路由协议启用 BFD:

```
bfd-template [single-hop | multi-hop] template_name
```

示例:

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1  
ciscoasa(config-bfd)#
```

- **single-hop**- 指定单跳 BFD 模板。
- **multi-hop**- 指定多跳 BFD 模板。

- *template-name* - 指定模板名称。模板名称不能包含空格。

使用 **bfd-template** 命令可创建 BFD 模板并进入 BFD 配置模式。

步骤 2 (可选) 在单跳 BFD 模板上配置回应:

bfd-template single-hop *template_name*

示例:

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa (config-bfd)# echo
```

只能在单跳模板上启用回应模式。BFD 回应不支持 IPv6 BFD 会话。

步骤 3 在 BFD 模板中配置间隔:

interval [**both** *milliseconds* | **microseconds** {**both** | **min-tx**} *microseconds* | **min-tx** *milliseconds*]

示例:

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both** - 最低传输和接收间隔功能。
- *milliseconds* - 间隔以毫秒为单位。范围为 50 到 999。
- **microseconds** - 为 **both** 和 **min-tx** 指定 BFD 间隔 (以毫秒为单位)。
- *microseconds* - 范围介于 50,000 到 999,000 之间。
- **min-tx**- 最低传输间隔功能。

作为 BFD 模板的一部分指定的 BFD 间隔值并不是特定于单个接口。您可以对每个接口应用各自的 BFD 模板。请参阅[配置 BFD 接口](#)，第 7 页。

步骤 4 在 BFD 模板中配置身份验证:

authentication {**md5** | **meticulous-mds** | **meticulous-sha-1** | **sha-1**} [**0**|**8**] *word key-id id*

示例:

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication** - 指定身份验证类型。
- **md5**- 消息摘要 5 (MD5) 身份验证。
- **meticulous-md5** - Meticulous keyed MD5 身份验证。
- **meticulous-sha-1** - Meticulous keyed SHA-1 身份验证。
- **sha-1** - Keyed SHA-1 身份验证。

- **0|8-0** 指定后面是未加密的密码。8 指定后面是已加密的密码。
- **word** - BFD 密码（密钥），单位数密码/密钥，最长 29 个字符。不支持以数字开头后跟空格的密码，例如“0 pass”和“1”均为无效密码。
- **key-id** - 身份验证密钥 ID。
- **id** - 匹配密钥字符串的共享密钥 ID。范围介于 0 到 255 个字符之间。

可以在单跳和多跳模板中配置身份验证。我们建议您配置身份验证，以增强安全性。在每个 BFD 源目标对上必须配置身份验证，而且两台设备上的身份验证参数必须匹配。

配置 BFD 接口

您可以将 BFD 模板绑定至接口，按接口配置基准 BFD 会话参数，然后按接口启用回应模式。

过程

步骤 1 进入接口配置模式：

```
interface interface_id
```

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0  
ciscoasa(config-if)#
```

步骤 2 将 BFD 模板应用到接口：

```
bfd template template-name
```

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0  
ciscoasa(config-if)# bfd template TEMPLATE1
```

即使未使用 **bfd-template** 命令创建模板，也可以在接口下配置模板的名称，但是，该模板会被视为无效，直到您定义该模板。您不必再重新配置模板名称。它会自动变为有效。

步骤 3 配置 BFD 会话参数：

```
bfd interval milliseconds min_rx milliseconds multiplier multiplier-value
```

示例：

```
ciscoasa(config)# interface GigabitEthernet0/0  
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval milliseconds** - 指定将 BFD 控制数据包发送到 BFD 对等体的速率。范围介于 50 到 999 毫秒之间。

- **min_rx milliseconds** - 指定预期从 BFD 对等体接收 BFD 控制数据包的速率。范围介于 50 到 999 毫秒之间。
- **multiplier multiplier-value** - 指定在 BFD 声明对等体不可用并通知第 3 层 BFD 对等体相关故障之前必须错过来自该 BFD 对等体的连续 BFD 控制数据包数。范围为 3 到 50。

步骤 4 在接口上启用 BFD 回应模式。

bfd echo

示例:

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

默认情况下会启用回应模式，但该模式在 BFD IPv6 会话中不受支持。当启用回应模式后，将从 **bfd interval milliseconds min_rx milliseconds** 配置获取最小回应传输级别和所需的最小传输间隔值。

注释 在使用 BFD 回应模式之前，您必须使用 **no ip redirects** 命令禁用 ICMP 重定向消息。这样可以避免 CPU 使用率过高。

配置 BFD 映射

您可以创建包含可与多跳模板关联的目标的 BFD 映射。您必须已配置多跳 BFD 模板。

过程

步骤 1 创建一个多跳 BFD 模板。请参阅[创建 BFD 模板](#)，第 5 页了解相关程序。

步骤 2 将该 BFD 多跳模板与目标的映射相关联:

```
bfd map {ipv4 | ipv6} destination/cdir source/cdire template-name
```

示例:

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** - 配置 IPv4 地址。
- **ipv6** - 配置 IPv6 地址。
- **destination/cdir** - 指定目标前缀/长度。格式为 A.B.C.D/<0-32>。
- **source/cdir** - 指定目标前缀/长度。格式为 X:X:X;X::X/<0-128>。
- **template-name** - 指定与此 BFD 映射关联的多跳模板的名称。

步骤 3（可选）配置 BFD 慢计时器值：

bfd slow-timers [*milliseconds*]

示例：

```
ciscoasa(config)# bfd slow-timers 14000  
ciscoasa(config-bfd)#
```

milliseconds -（可选）BFD 慢计时器值。范围为 1000 到 30000。默认值为 1000。

BFD 监控

可以使用以下命令监控 BFD 路由进程。有关命令输出的示例和说明，请参阅命令参考。

要监控或禁用各种 BFD 路由统计信息，请输入以下其中一个命令：

- **show bfd neighbors**

显示现有 BFD 邻接关系逐行列表。

- **show bfd summary**

显示 BFD、BFD 客户端或 BFD 会话的摘要信息。

- **show bfd drops**

显示 BFD 中已丢弃的数据包数。

- **show bfd map**

显示配置的 BFD 映射。

- **show running-config bfd**

显示所有 BFD 相关的全局配置。

BFD 路由历史记录

表 1: BFD 路由的功能历史记录

功能名称	平台版本	功能信息
BFD 路由支持	9.6(2)	<p>ASA 现在支持 BFD 路由协议。添加了对配置 BFD 模板、接口和映射的支持。还添加了对 BGP 路由协议使用 BFD 的支持。</p> <p>添加了以下命令：bfd echo、bfd interval、bfd map、bfd slow-timers、bfd-template、clear bfd counters、clear conf bfd、neighbor fall-over bfd、show bfd drops、show bfd map、show bfd neighbors、show bfd summary、show running-config bfd</p>