ICS 01.040.35
L 78

YD

中华人民共和国通信行业标准

YD/T 2729-2014

运营级网络地址翻译(NAT)备份技术要求

Technical specification for carrier grade NAT device service backup

2014-10-14 发布　　2014-10-14 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/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：中兴通讯股份有限公司、工业和信息化部电信研究院、中国电信集团公司、上海贝尔股份有限公司、华为技术有限公司。

本标准主要起草人：范　亮、马高峰、马军锋。

运营级网络地址翻译（NAT）备份技术要求

1 范围

本标准规定了对 CGN 设备业务备份技术要求，并对不同应用场景下的特殊要求进行了规定。

本标准适用于 NAT44、DS-Lite AFTR、NAT64 等 CGN 设备。

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 RFC 6052　IPv4/IPv6地址翻译（IPv6 Addressing of IPv4/IPv6 Translators）

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

冷备份　Cool Backup

主用 CGN 设备与备份 CGN 设备间不实时同步用户及业务信息，备份设备上无用户状态信息，当网络或设备故障时，用户需要重新与备用 CGN 设备建立会话的备份方式。

3.1.2

热备份　Hot Backup

主用 CGN 设备与备份 CGN 设备间实时同步用户及业务信息，实时在备份设备的转发层面生成用户的转发表项，状态切换后可以直接转发用户流量。

3.1.3

温备份　Warm Backup

主用 CGN 设备与备份 CGN 设备间实时同步用户及业务信息，但只在备份设备的控制层面保存用户及业务信息，待状态切换后，将用户表项下发到转发层面后转发流量。

3.2 缩略语

下列缩略语适用于本文件。

AFTR	Address Family Transition Router	地址族转换路由器
BIB	Binding Information Base	绑定信息列表
BFD	Bidirectional Forwarding Detection	双向转发检测
BNG	Broadband Network Gateway	宽带网络网关
CGN	Carrier Grade NAT	运行级 NAT
CPE	Customer Premise Equipment	用户驻地设备
ISP	Internet Service Provider	互联网服务提供商

NAT	Network Address Translation	网络地址转换
VRRP	Virtual Router Redundancy Protocol	虚拟路由器冗余协议

4 概述

4.1 CGN 部署方式

由于 IPv4 公网地址的短缺，很多 ISP 希望能够在很多用户之间共享一个 IPv4 公网地址，每个用户被分配一个私网地址，使用一个位于 ISP 网络的 NAT 设备进行私有和公有地址之间的翻译。如图 1 所示，CGN 是一个 NAT 设备，位于用户和 Internet 之间，在数据包经过内部网络与外部网络时，CGN 对 IP 地址和端口号进行翻译。

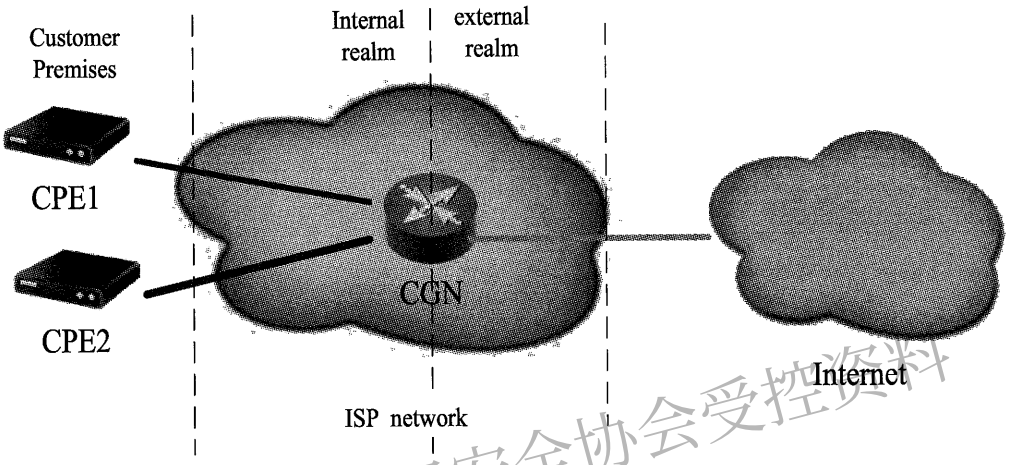

图 1 CGN 部署方式

4.2 CGN 业务备份方案

根据不同场景下的应用需求，高可靠性方案可以分为冷备份、热备份和温备份三类。其中，冷备份适用的环境范围较小，实现较为简单；热备份则提供的可靠性等级更高，也能满足多方面的要求；温备份介于冷备份和热备份之间，只在发生网络故障，需要主备切换时，再将转发表项进行下发，继而转发用户流量， 能最大化利用设备资源。

下面将分章节进行说明。

5 热备份下 CGN 设备的技术要求

5.1 热备份概述

热备份方式下，主备 CGN 设备之间同步用户信息。主 CGN 设备支持将用户信息、会话信息发送给备用 CGN 进行备份，主备设备故障后，备用 CGN 设备切换状态后可以直接转发用户流量，从而维持业务的持续性。

5.2 CGN 热备份组网

根据 CGN 多跳和直连场景，可以分成以下两种组网方式。

多跳场景下：如图 2 所示，两台 CGN 设备之间通过心跳线直连，进行主备选举，主备 CGN 之间还需建立同步信息传送通道，这些信息包含用户信息与会话信息。两台 CGN 设备均与下游设备（比如 CR）建立路由邻居关系，并且能够通过快速路由收敛实现主备切换。

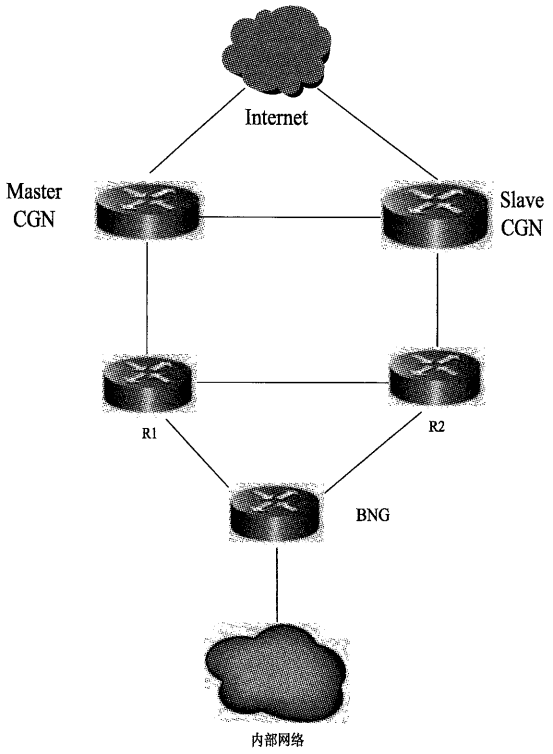

图 2　CGN 多跳组网

直连场景下：如图 3 所示，此场景下主备 CGN 设备通过交换机进行主备选举和用户、会话信息的备份，并使用虚拟 MAC 地址和根据主备状态抑制备用设备等模块的回应，并最终通过交换机的 MAC 表刷新来达到快速切换的效果。

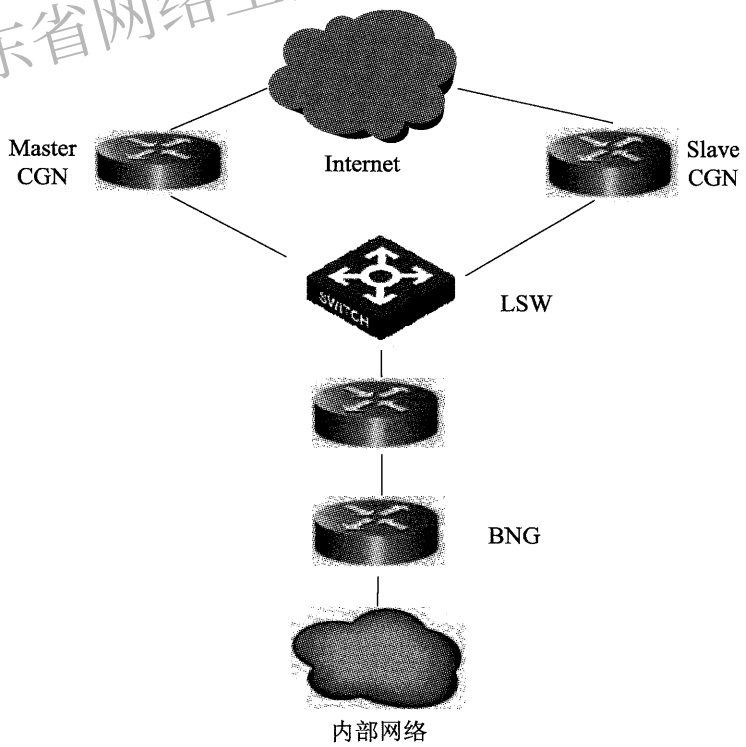

图 3　CGN 单跳组网

上述组网是热备份设备间的典型组网及相关协议的部署。这里需要注意的是，本规范所述的热备份并非仅仅指双机热备份，考虑到部署成本，设备也应支持多机备份的形式，如图 4 所示。

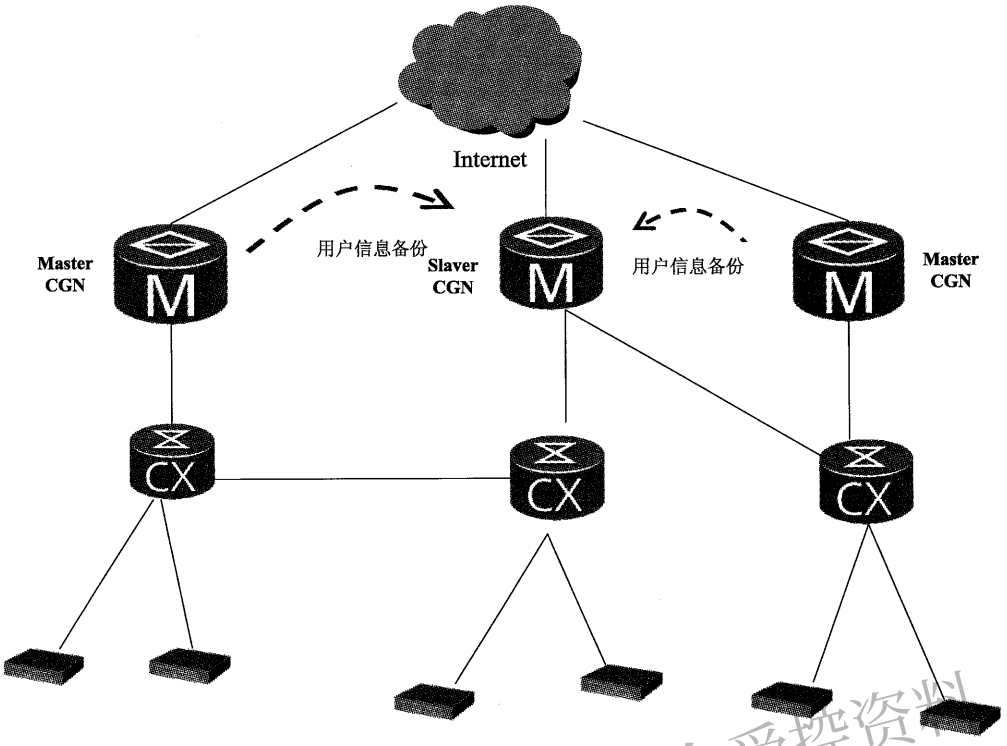

图 4　多机备份

针对具体网络的部署场景在第 9 章中规定。

5.3　CGN 设备热备份原理

5.3.1 信息实时备份

热备份是指主用 CGN 设备与备用 CGN 设备在切换过程中不被用户感知，因此必须在备份设备上保存用户的实时信息，如用户的会话信息、绑定信息和其他业务信息，这样才能使得用户业务不发生中断，维持之前的网络访问权限，并且用户的一些计费信息也不会由于主用 CGN 设备的故障而丢失。下面为信息实时备份的过程：

a）主 CGN 与备份 CGN 之间必须建立同步备份通道、会话备份通道（如 TCP 连接），备份 CGN 接受主 CGN 发送的备份信息报文，可根据不同的备份组建立不同的同步信息传送通道。

b）主 CGN 必须支持将用户信息、会话信息发送给备份 CGN 进行备份，备份 CGN 支持将收到的主 CGN 上的用户信息下发到对应的接口板的功能模块进行同步；备份 CGN 支持通知主 CGN 发送会话备份信息，从而建立热备份环境。

c）应支持控制、数据消息分别传送的方式，为控制消息、用户及业务信息建立不同的信息传送通道。

5.3.2　主备选举

5.3.2.1　直连心跳线

通过备份组的两台 CGN 设备间直连心跳线进行主备选举。通过在主用设备和备用设备之间建立检测链路，并且使用 VRRP 和 BFD 进行实例的主备状态选举，主备 CGN 可以在检测链路上建立备份通道，主用 CGN 设备可以通过备份通道向备用 CGN 设备发送备份信息，当主用 CGN 设备故障的时候，主用

CGN 设备切换到初始状态，备用 CGN 切换到主状态，从而达到切换主备状态的目的。在多跳组网和单跳组网场景下都可以通过直连心跳线进行主备选举，如图 5 和图 6 所示。

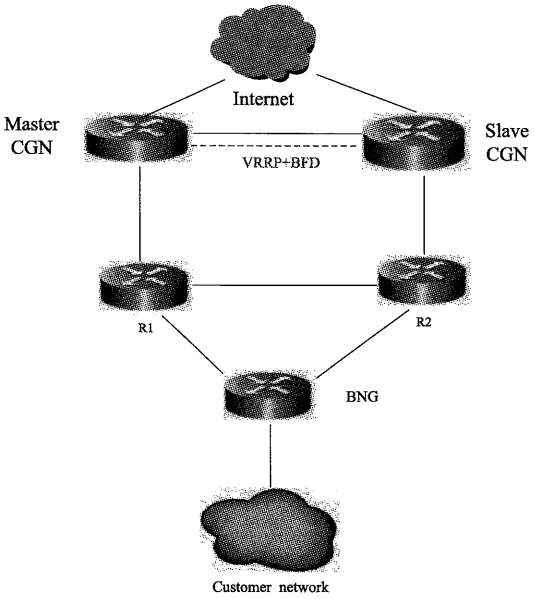

图 5　直连心跳线选举

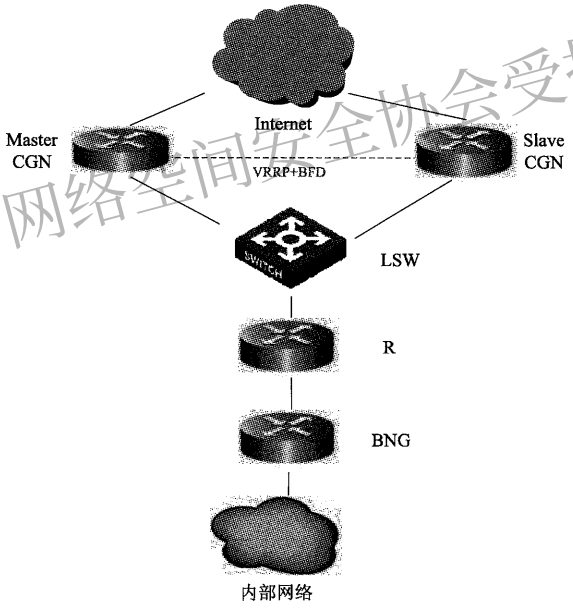

图 6　单跳组网下直连心跳线选举

5.3.2.2　跨交换机

如图 7 所示，CGN 设备将主用、备用设备的用户侧端口或子接口与 VRRP 进行绑定，通过独立子接口或者共用接入业务子接口建立 VRRP 连接，进行主备选举。当与交换机的相关链路出现故障时，进行主备选举。

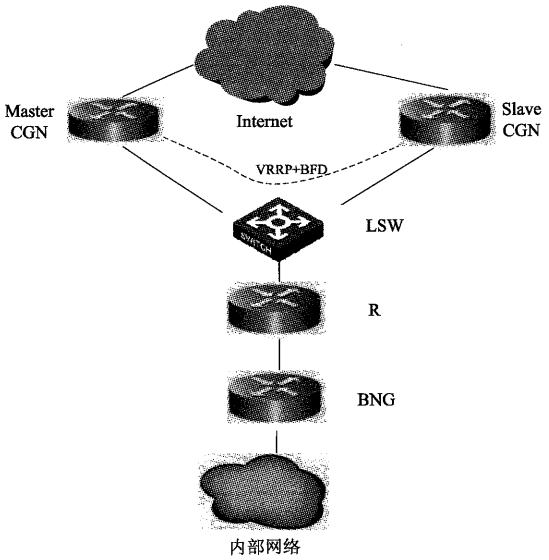

图 7　跨交换机主备选举

5.3.3　主备切换

5.3.3.1　主设备异常触发切换

当主用 CGN 设备故障发生时，将关闭检测链路，同时主备设备发生切换：主用 CGN 设备切切换到初始状态，原备份 CGN 设备检测到检测链路关闭时，由备状态切换为主状态。

图 8 所示为正常工作状态下流量途经的路径；LINK1 表示 NAT 转换前的流量，LINK2 表示 NAT 转换后的流量，Master CGN 进行 NAT 转换工作。

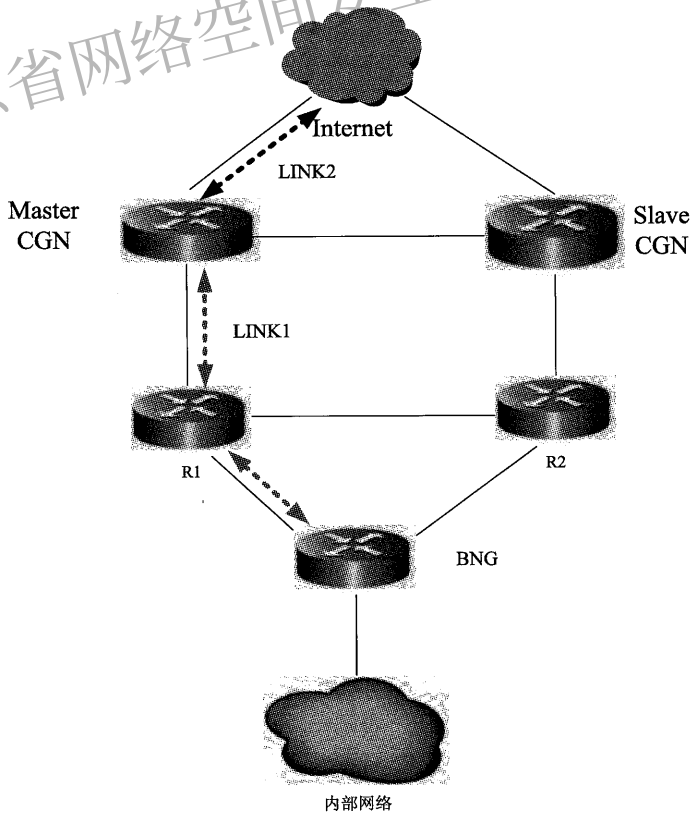

图 8　正常工作

当故障发生后，可能为 LINK1 或者 LINK2 或 LINK1 和 LINK2 同时发生故障，由于在实际情况中 LINK1 和 LINK2 的流量存在通过同一条链路的情况，因此规定当 LINK1 或者 LINK2 只要其中至少一个链路出现故障，则另外一个链路就必须也要使其关闭，否则流量将会在 CGN 设备上丢弃，从而造成用户连接的中断。所以在这种环境下，将 LINK1 和 LINK2 所接入的接口绑定，只要任一接口出现故障时（链路所在接口 down），则将另外的成员口均设置成 down，同时关闭主备 CGN 设备之间的检测链路，并进行主备倒换，同时因为链路接口 down，使得撤销与路由器之间的邻居路由，撤销高优先级的路由，通过快速路由收敛，流量切换到新的主设备，如图 9 所示。

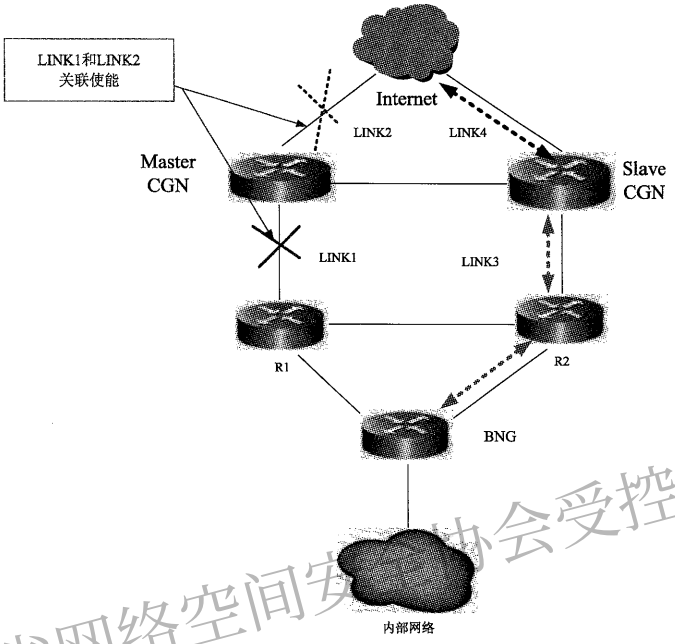

图 9　切换后的流量

5.3.3.2　备设备异常对主设备的影响

备设备所在链路发生故障时，备设备会撤销低优先级的用户侧路由和 NAT 路由，但是由于流量仍然流经主设备，并不会影响用户当前业务。待故障恢复后，备设备通告低优先级的用户侧路由和 NAT 路由。

5.3.4　流量切换

当故障发生时，主备设备发生切换，还需要将主设备上的流量引导到备设备，并由备设备继续为用户提供服务。

5.3.4.1　静态路由方式

如图 10 所示，通过在 CR 配置接口，配置到达 CGN 的静态路由，下一跳指定为 VRRP 的虚拟 IP 地址，则可以通过 VRRP 的虚拟 IP 和交换机实现主备状态的切换和流量的切换，保持状态和流量切换的一致性。交换机上的虚拟 MAC 条目通过 VRRP 的主设备来刷新和保持，当 VRRP 主备切换后，原备份设备升为主用设备，该设备的用户侧端口或子接口必须主动下发 gratuitous ARP，刷新下挂交换机的 MAC 表，则该虚拟 MAC 条目的出接口也转换成到达新主设备的出接口，引导用户上行流量到该设备。

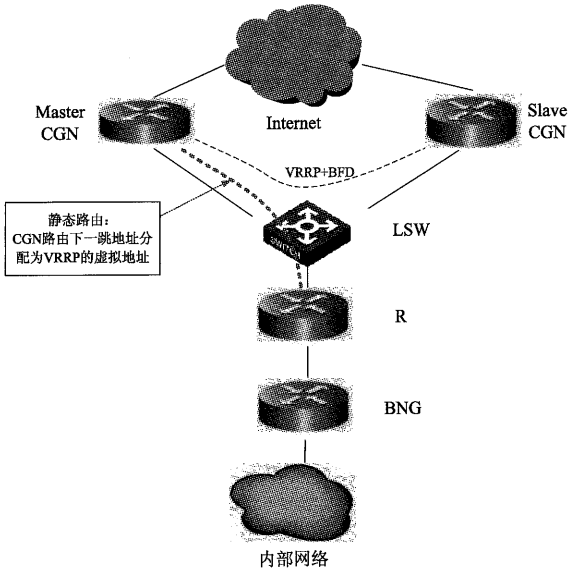

图 10　静态路由方式

用户的下行流量也需要从故障设备引导到备份设备，如图 11 所示。网络侧路由部署主要是 NAT 地址池通过重分配汇聚路由或者通过网段路由，主设备发布高优先级的 NAT 路由，备设备发布低优先级 NAT 路由，当主设备异常时，则进行主备切换，撤销 NAT 路由，使得原先的备设备成为主，通过路由收敛，网络侧下行流量可以继续通过新的主设备流通。

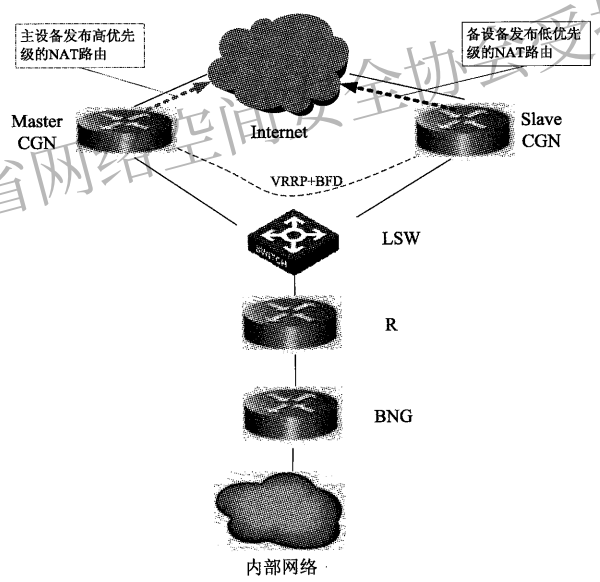

图 11　静态路由方式下行流量引导

5.3.4.2　动态路由方式

5.3.4.2.1　用户侧路由部署

对于每个 CGN 地址，主设备发布高优先级路由，备设备发布低优先级路由，使得 CPE 和主设备建立连接，当主设备异常时，则进行主备切换，同时撤销该 CGN 路由，如图 12 所示，使得原先的备设备成为主用，通过路由收敛，CPE 和新主设备建立起连接，保证流量继续畅通，可以通过配置 IP 路由邻居之间的 BFD 来加速路由收敛，使切换中间态的时间间隔尽量缩短。

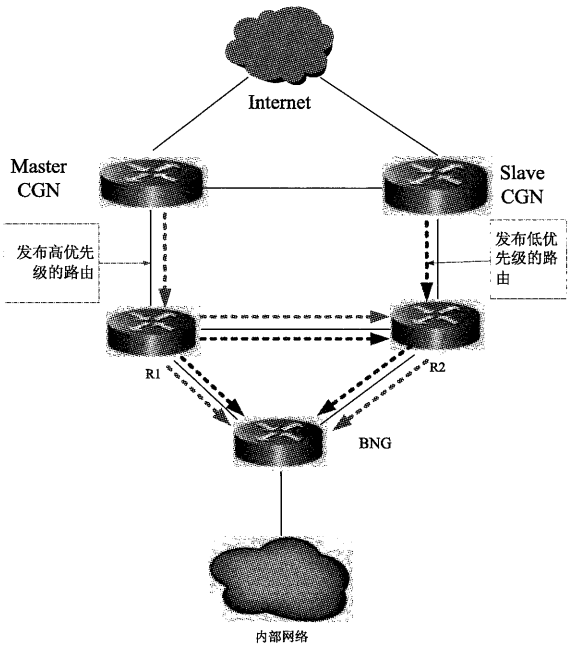

图 12　动态路由用户侧路由

跨交换机组网的环境下，如图 13 所示，主备 CGN 分别通过不同的子接口建立路由邻居，按照图 13 所示的路由通告方式。

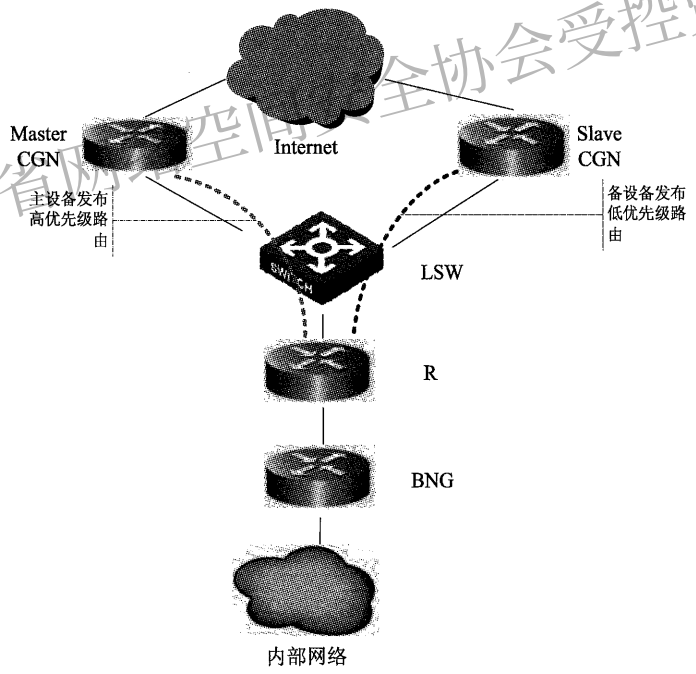

图 13　跨交换机组网用户侧路由发布

5.3.4.2.2　网络侧路由部署

如图 14 所示，网络侧路由部署主要是 NAT 地址池通过重分配汇聚路由或者通过网段路由，主设备发布高优先级的 NAT 路由，备设备发布低优先级 NAT 路由，当主设备异常时，则进行主备切换，撤销

NAT 路由，使得原先的备设备成为主，通过路由收敛，网络侧下行流量可以继续通过新的主设备流通。在这里可以通过配置路由邻居之间的 BFD 来加速路由收敛，使切换中间态的时间间隔尽量缩短。

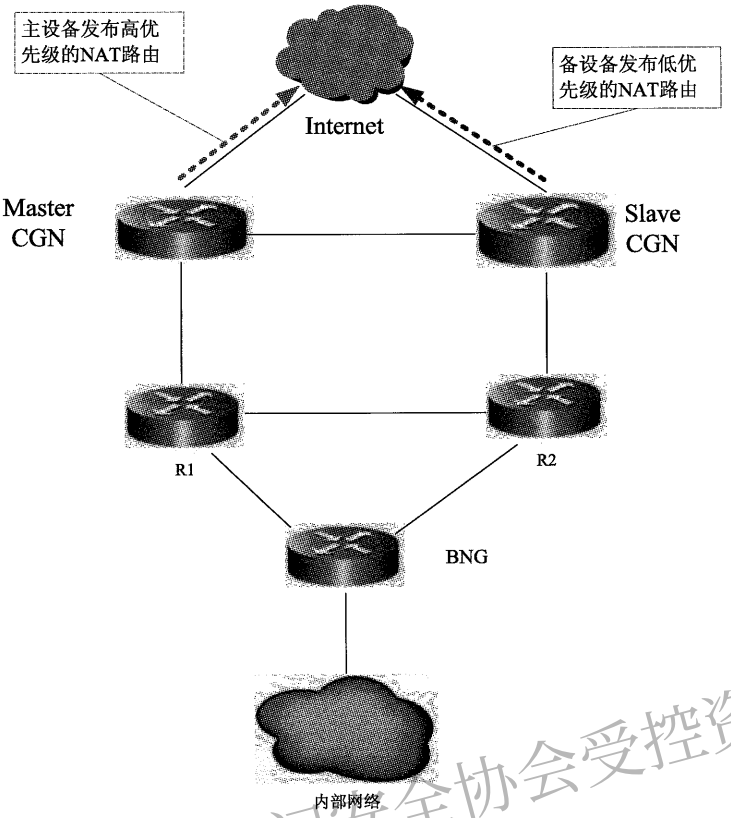

图 14　网络侧路由部署

5.3.5　故障恢复

当故障设备恢复后，需要将用户流量从备用设备回切至主用设备，主用 CGN 设备在故障恢复后需同步用户信息。原主 CGN 设备检测到故障修复时，会重新与原备用 CGN 设备建立检测链路与备份通道，并且原主 CGN 设备变为备份状态，原备 CGN 设备向原主 CGN 设备发送备份信息，然后原主 CGN 设备由备份状态变为主状态。

主备状态切换有命令式手动切换和主备信息协议状态机自动切换两种切换方式：

a）命令触发是指在准备 CGN 设备上手动修改贮备协商信令的优先级或手动配置强制回切命令，实现主备状态切换效果的方式。

b）主备信令协议自动切换，即故障恢复后的自动回切。自动回切的条件包括所有检测为发生故障，则主备信令协议恢复到切换前的状态。

6　冷备份下 CGN 设备的技术要求

6.1　冷备份概述

冷备份方式下，主备 CGN 设备之间没有用户信息同步。主备设备故障后，用户与备用 CGN 设备建立新的会话，而且不必等待主用设备的恢复。冷备份方案无需改动设备，只须改动部分配置，不影响现有 CGN 设备的继续使用，易于实现。

6.2 CGN 冷备份组网

与 CGN 热备份组网相似，CGN 冷备份组网也有 CGN 多跳用户与单跳用户两种组网方式：

多跳场景下：如图 15 所示，主备 CGN 设备之间通过主备信令协议（如 VRRP）进行主备选举，两台 CGN 设备均与下游设备（比如 CR）建立起路由邻居关系，最终通过路由（快速）收敛实现主备切换。

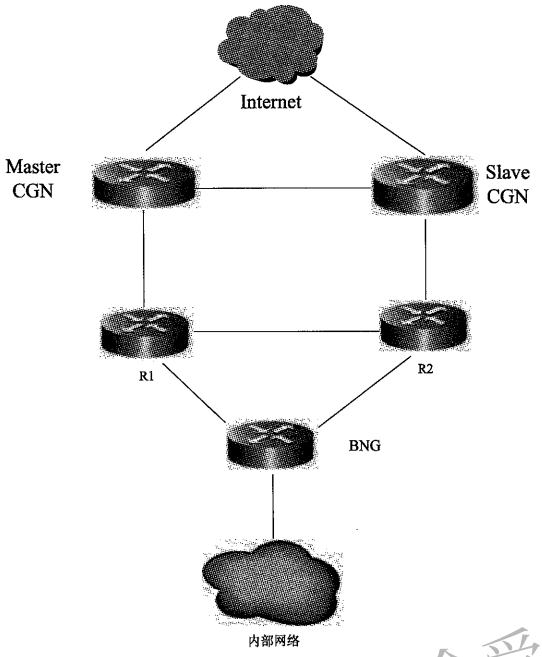

图 15 冷备份多跳组网

单跳场景下：如图 16 所示，主备 CGN 设备通过交换机进行主备选举 ，并使用虚拟 MAC 和根据主备状态抑制备用设备等模块的回应，并最终通过刷新交换机的 MAC 表达到快速切换的效果。

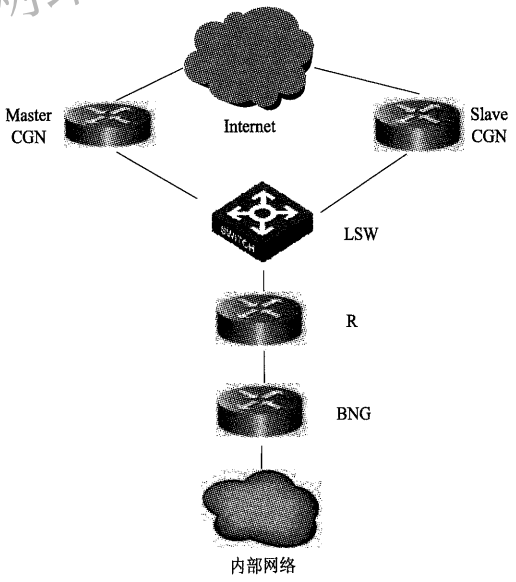

图 16 冷备份单跳组网

6.3 CGN 设备冷备份原理

6.3.1 主备选举

在主备协商冷备份方案中，主备 CGN 设备的通过主备信令协议（如 VRRP）协商主备关系 ，并且可以通过直连心跳线或 CGN 设备的用户侧端口或子接口进行协商。

6.3.1.1 直连心跳线方式

两台 CGN 设备间直连心跳线，如图 17 和图 18 所示，建立 VRRP 链接，通过 VRRP 进行实例的主备状态选举，当主 CGN 设备接口 down 或者删除的时候，则相应降低 VRRP 组优先级，从而达到切换主备状态的目的。

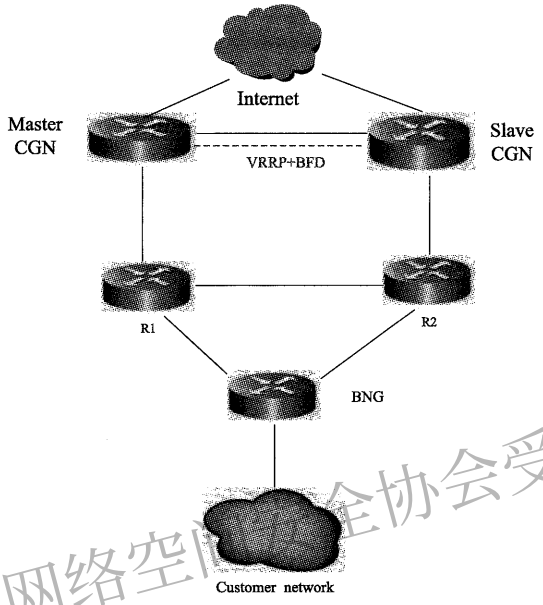

图 17 冷备份多跳直连选举

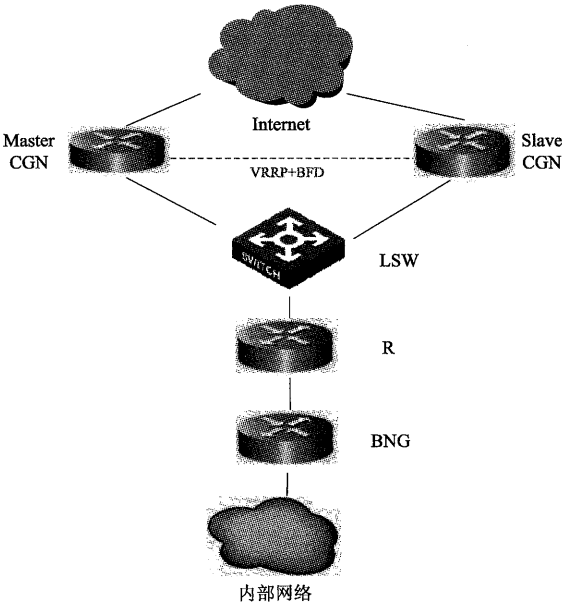

图 18 冷备份单跳直连选举

6.3.1.2 跨交换机状态

这种情形主要是在交换机直连的场景下，如图 19 所示，CGN 设备将主用、备用设备的用户侧端口或子接口与 VRRP 进行绑定，通过独立子接口或者共用接入业务子接口建立 VRRP 连接，进行主备选举。当与交换机的链路出现故障时，发生主备倒换。

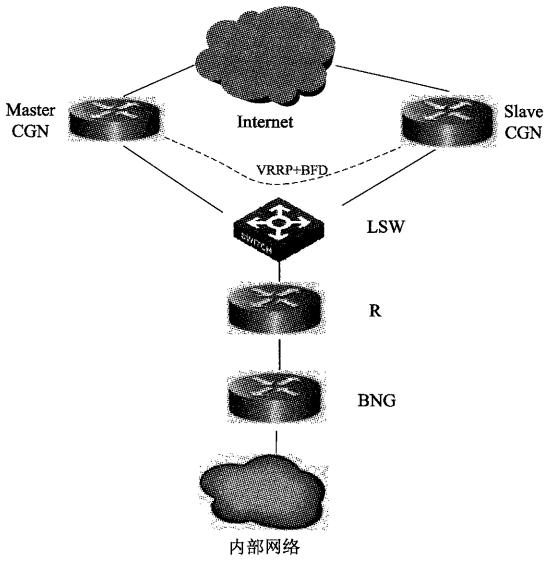

图 19 冷备份跨交换机选举

6.3.2 主备切换

6.3.2.1 主设备异常触发切换

在冷备份状态下，当主用 CGN 设备发生故障时，主备设备进行切换，原备份设备升为主用设备。切换过程热备份切换过程相同。

6.3.2.2 备设备异常对主设备的影响

与热备份相同，备设备异常备设备，会撤销低优先级的路由，但是流量仍然流经主设备，不影响业务。

6.3.3 流量切换

6.3.3.1 静态路由方式

在静态路由方式下冷备份的流量切换与热备相同的，需要注意的是用户业务到达新主用设备后，由于冷备份没有在新主用设备备份用户映射信息，因此需要给用户分配新的映射地址和端口。新主用设备与原主用设备所用的地址池必须使用不同的地址池，主要是为了防止新旧映射之间的混淆。

6.3.3.2 动态路由方式

冷备份的动态路由方式与热备份的动态路由方式相同，区别在于切换到新主用设备后需要重新分配新的映射地址和端口，且新主用设备使用的是不同的地址池。

进行主备切换后，在网络侧，原主设备撤销 NAT 路由，使得原先的备设备成为主，通过路由收敛，网络侧下行流量可以继续通过新的主设备流通。在这里可以通过配置路由邻居之间的 BFD 来加速路由收敛，使切换中间态的时间间隔尽量缩短。

6.3.4 故障恢复

当故障设备恢复后，将用户及流量从备份设备回切至主用设备，回切前需要保证主备在上下行链路都不存在故障。

主备用 CGN 设备利用主备信令协议协商重新恢复到故障发生前状态（通过状态机自动回切、手动更改优先级或手动配置回切命令）。

回切至原主设备后，原主设备重新为用户分配地址和端口，重新建立映射关系。

7 温备份下 CGN 设备的技术要求

温备份与热备份相同，也需要实时在主用CGN设备与备用CGN设备之间同步用户及业务信息，与热备份的区别在于温备份并不将这些信息实时在备份设备的控制层面和转发层面上生成用户的转发表项，而在发生网络故障，需要主备切换时，再将转发表项进行下发，继而转发用户流量

温备份方案由于不要要实时下发转发表项，因此，可以在满规格 N:1 备份的场景中实现温备份方案，如图 20 所示，CGN-2 可以同时作为 CGN-1 和 CGN-3 的备份，假设 CGN-2 和 CGN-3 是接近满规格用户数量的，CGN-2 是无法使用热备份场景为两台设备同时进行备份的。而在温备份场景中，CGN-2 可以实时同步 CGN-1 和 CGN-3 的用户信息，但并不下发转发表，如果 CGN-1 或 CGN-3 发生故障，CGN-2 便接管故障设备 用户。

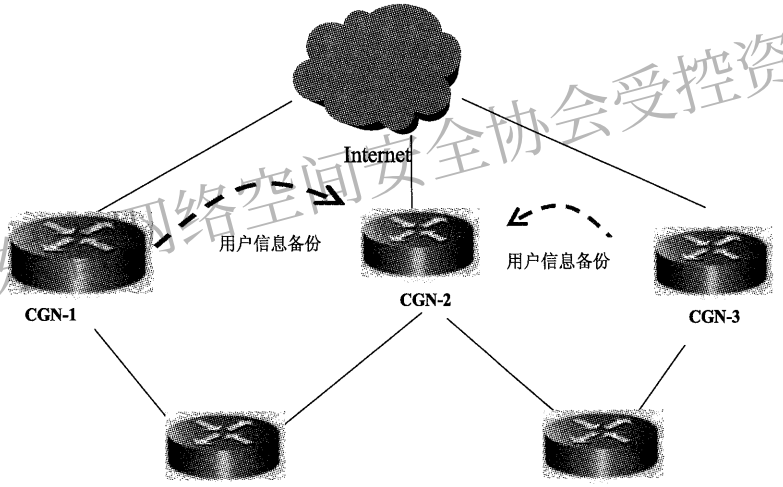

图 20 温备份组网

温备份与热备份处理上述区别以外，应用场景与可用的备份方案与热备份一致。

8 不同场景下 CGN 设备的特殊要求

8.1 轻型双栈（DS-lite）

8.1.1 轻型双栈（DS-lite）信息备份

如果主 CGN 设备采用轻型双栈（DS-lite）网络地址转换技术进行网络地址转换，除了冷备份，热备份和温备份都需要向备份设备实时发送用户的映射绑定信息，主要包括绑定信息和 Session 信息，这些信息包括 IPv6 前缀、子网前缀长度、隧道信息和虚拟专用网络信息等信息。

8.1.1.1 轻型双栈（DS-lite） 绑定信息表的备份

轻型双栈（DS-lite）利用绑定信息表记录映射绑定信息。轻型双栈（DS-lite）维护 UDP、TCP 和 ICMP 三种绑定信息列表。

当轻型双栈（DS-lite）生成或删除一个 TCP/UDP 绑定信息列表时，主用轻型双栈（DS-lite）发送备份信息给备用轻型双栈（DS-lite）设备，备份信息见表 1。

表 1 DS-lite TCP/UDP 绑定信息备份列表

字段名	长度(bit)
TimeStamp	64
B4Address	128
SourceIPv4Address	32
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
protocolIdentifier	8

备份信息表记录了在用户侧 IPv4 地址端口对和网络侧 IPv4 地址端口对之间的一个映射：

（*X*,*x*）<-->(*T*,*t*)

其中 *X* 代表某个 IPv4 地址，*T* 代表 DS-lite 分配的 IPv4 地址，*x* 和 *t* 则都是端口号。备份信息表中 B4Address 表示 B4 用来封装的 IPv4 报文的 IPv6 地址，timestamp 表示备份信息的产生时间,SourceIPv4Address 表示数据包源私有 IPv4 地址；postNATsourceIPv4Address 表示翻译后的公网 IPv4 地址，SourceTransportPort 表示数据包原端口号，postNAPTSourceTransportPort 表示经过翻译后的外网端口号，protocolIdentifier 表示承载的协议。

如果 DS-lite 创建或删除一个 ICMP Queries 等协议的绑定时，主用轻型双栈（DS-lite）发送备份信息给备用轻型双栈（DS-lite）设备，备份信息见表 2。

表 2 的 DS-lite ICMP 绑定信息备份列表

字段名	长度(bit)
timeStamp	64
B4Address	128
SourceIPv4Address	32
ICMPv4Identifier	16
postNATSourceIPv4Address	32
postNATICMPv4Identifier	16
protocolIdentifier	8

备份信息记录描述了在（IPv4 地址，ICMPv4 Identifier）和（IPv4 地址，ICMPv4 Identifier）之间的一个映射：

（*X*, *i*1）<--> (*T*, *i*2)

其中，*X* 代表用户 IPv4 地址，*T* 代表一个 DS-lite 分配的 IPv4 地址，*i*1 是一个 ICMPv4 Identifier，*i*2 是一个 ICMPv4 Identifier。

备份信息表中 B4Address 表示 B4 用来封装的 IPv4 报文的 IPv6 地址， timestamp 表示备份信息的产生时间，SourceIPv4Address 表示原 ICMP 数据包的源地址，ICMPv4Identifier 表示原 ICMP 数据包的标识

号，postNATSourceIPv4Addredd 表示翻译后的公网 IPv4 地址，postNATICMPv4Identifier 表示翻译后的 ICMP 标识符，protocolIdentifier 表示承载的协议。

对于其他协议的备份数据，如果 DS-lite 支持，主用 DS-lite 发送备份信息给备用 DS-lite 设备。

轻型双栈（DS-lite）主用设备需要将绑定信息实时发往备用轻型双栈(DS-lite)设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.1.1.2 轻型双栈（DS-lite Session）的备份

同样，轻型双栈（DS-lite）还需要备份 Session 表的信息，轻型双栈（DS-lite）利用 Session 记录源 IPv4 节点与目的 IPv4 节点之间数据流，并且能起到溯源的作用。当一个轻型双栈（DS-lite ）Session 生成或者删除时，需要记录以下信息，并发送这些信息到相应的备份设备上。

当主用 DS-lite 生成或者删除一个 TCP/UDP Session 时，需要记录信息，并发送这些信息到相应的备份设备上。备份信息见表 3。

表 3 DS-lite TCP/UDP Session 备份列表

字段名	长度(bit)
Timestamp	64
B4Address	128
SourceIPv4Address	32
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
DestinationIPv4Address	32
DestinationTransportPort	16
protocolIdentifier	8

备份信息记录了一组用户 IPv4 地址端口对和网络侧一组 IPv4 地址端口对的映射关系，其关系如下：

（*X,x*）,(*Y,y*) <-->(*T,t*), (*Y,y*)

其中，*X* 是用户侧 IPv4 地址，*T* 和 *Y* 是公网 IPv4 地址，*x, y, t* 是端口号，且 *T* 是 DS-lite 分配的 IPv4 地址。

备份信息表中 B4Address 表示 B4 用来封装的 IPv4 报文的 IPv6 地址，timestamp 表示了备份信息的产生时间，SourceIPv4Address 表示原私网 IPv4 地址，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，SourceTransportPort 表示原端口号，postNATSourceTransportPort 表示经过翻译后的端口号，DestinationIPv4Address 表示目的 IPv4 地址，DestinationTransportPort 表示目的 IPv4 目的端口，protocolIdentifier 表示承载的协议。

当主用 NAT64 生成或者删除一个 ICMP Queries Session 时，需要记录信息，并发送这些信息到相应的备份设备上，备份信息见表 4。

表 4 DS-lite ICMP Session 备份列

字段名	长度(bit)
Timestamp	64
B4Address	128
SourceIPv4Address	32

表 4（续）

字段名	长度(bit)
DestinationIPv4Address	32
ICMPv4Identifier	16
postNATSourceIPv4Address	32
DestinationIPv4Address	32
postNATICMPv4Identifier	16
protocolIdentifier	8

备份信息记录了三元组（IPv4 source address，IPv4 destination address, ICMPv4 Identifier）和三元组（IPv4 source address, IPv4 destination address, ICMPv4 Identifier）之间的映射关系，其关系如下：

（*X*，*Y*, *i*1）<--->（*T*, *Y*，*i*2）

其中 *X* 代表用户侧 IPv4 地址，*T* 和 *Y* 分别代表公网 IPv4 地址，*i*1 为 ICMPv4 Identifier，*i*2 为 ICMPv4 Identifier，且 *T* 是 DS-lite 分配的 IPv4 地址。

备份信息表中 B4Address 表示 B4 用来封装的 IPv4 报文的 IPv6 地址，timestamp 表示了备份信息的产生时间，SourceIPv4Address 表示用户侧 IPv4 地址，DestinationIPv4Address 表示目的地址，ICMPv4Identifier 表示原 ICMPv4 标识符，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，DestinationIPv4address 表示目的地址，postNATICMPv4Identifier 表示翻译后的 ICMPv4 标识符，protocolIdentifier 表示承载的协议。

对于其他协议的数据，如果 DS-lite 支持，主用 DS-lite 发送备份信息给备用 DS-lite 设备。

轻型双栈（DS-lite）主用设备需要将 Session 信息实时发往备用轻型双栈（DS-lite）设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.1.2 轻型双栈（DS-lite）场景下流量的切换

主备切换后，需要将主用 AFTR 设备上的流量引导到备用设备上。

对于每一个 AFTR 地址，主设备发布高优先级路由，备用设备发布低优先级路路由，使得 CPE 与主设备建立起 DS-lite 隧道，当主设备异常时，则进主备切换，并撤销该 AFTR 路由，使得原先的备用设备为主，通过路由收敛，CPE 与备用设备之间建立起一条 DS-lite 隧道，保证 IPv6 流量继续畅通，这里可以通过配置 IPv6 路由邻居之间的 BFDv6 来加速路由收敛，使得切换中间状态的时间间隔尽量缩短。

8.2 NAT44

8.2.1 NAT44 信息备份

如果主 CGN 设备采用 IPv4 到 IPv4 的网络地址转换技术（NAT44）进行报文转换，除了冷备份，热备份和温备份都需要向备份设备实时发送用户的映射绑定信息，主要包括绑定信息和 Session 信息，这些信息需要包括 IPv4 地址虚拟专用网络信息。

8.2.1.1 NAT44 绑定信息的备份

当 NAT44 创建或删除一个绑定实体时，需要记录以下信息，并发送这些信息到相应的备份设备上。

如果 NAT44 创建或删除一个 TCP/UDP 等协议的绑定时，主用 NAT44 发送备份信息给备用 NAT44 设备，备份信息见表 5。

表 5 NAT44 TCP/UDP 绑定信息备份列表

字段名	长度(bit)
TimeStamp	64
SourceIPv4Address	32
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
protocolIdentifier	8

备份信息表记录了在用户侧 IPv4 地址端口对和网络侧 IPv4 地址端口对之间的一个映射：

（*X*,*x*）<-->(*T*,*t*)

其中 *X* 代表某个 IPv4 地址，*T* 代表 NAT44 分配的 IPv4 地址，*x* 和 *t* 都是端口号。备份信息表中 timestamp 表示备份信息的产生时间，SourceIPv4Address 表示用户侧 IPv4 源地址，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，SourceTransportPort 表示用户侧端口号，postNAPTSourceTransportPort 表示经过翻译后的端口号，protocolIdentifier 表示承载的协议。

如果 NAT44 创建或删除一个 ICMP Queries 等协议的绑定时，主用 NAT44 发送备份信息给备用 NAT64 设备，备份信息包括表 6 的内容。

表 6 NAT44 ICMP 绑定信息备份列表

字段名	长度(bit)
timeStamp	64
SourceIPv4Address	32
ICMPv4Identifier	16
postNATSourceIPv4Address	32
postNATICMPv4Identifier	16
protocolIdentifier	8

备份信息记录描述了在（IPv4 地址，ICMPv4 Identifier）和（IPv4 地址，ICMPv4 Identifier）之间的一个映射：

（*X*, *i*1）<--> (*T*, *i*2)

其中，*X* 代表用户 IPv4 地址，*T* 代表一个 DS-lite 分配的 IPv4 地址，*i*1 是一个 ICMPv4 Identifier，*i*2 是一个 ICMPv4 Identifier，

备份信息表中 timestamp 表示备份信息的产生时间，SourceIPv4Address 表示用户侧 IPv4 地址，ICMPv4Identifier 表示用户侧 ICMPv4 标识符，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，postNATICMPv4Identifier 表示翻译后的 ICMPv4 标识符，protocolIdentifier 表示承载的协议。

对于其他协议的数据，如果 NAT44 支持，则主用 NAT44 发送备份信息给备用 NAT44 设备。

NAT44 主用设备需要将 BIB 信息实时发往备用 NAT44 设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.2.1.2 NAT44 Session 的备份

同样，NAT44 还需要备份 Session 表的信息，NAT44 利用 Session 记录源 IPv4 节点与目的 IPv4 节点之间数据流。当一个 NAT44 Session 生成或者删除时，需要记录一下信息，并发送这些信息到相应的备份设备上。

当主用 NAT64 生成或者删除一个 TCP/UDP Session 时，需要记录信息，并发送这些信息到相应的备份设备上，备份信息见表 7。

表 7　NAT44　TCP/UDP Session 备份列表

字段名	长度(bit)
Timestamp	64
SourceIPv4Address	32
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
destinationIPv4Address	32
destinationTransportPort	16

备份信息记录了一组用户 IPv4 地址端口对和网络侧一组 IPv4 地址端口对的映射关系，其关系如下：

（*X,x*）,(*Y,y*)　<-->(*T,t*), (*Y,y*)

其中，*X* 是用户侧的 IPv4 地址，*T* 和 Z 是 IPv4 地址，*x, y, z, t* 是端口号，且 *T* 是 NAT44 分配的 IPv4 地址，*Y'*是代表 IPv4 地址 *Z* 的 IPv6 地址，*Y Y'*由 NAT64 配置的算法根据 IPv4 地址 *Z* 产生。timestamp 表示这个 Session 的生成时间，SourceIPv4Address 表示用户侧私网 IPv4 地址，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，SourceTransportPort 表示用户侧端口号，postNAPTSourcetransportPort 表示经过翻译后的端口号，destinationIPv4Address 表示目的 IPv4 地址，destinationTransPort 表示目的端口号。

当主用生成或者删除一个 ICMP Queries Session 时，需要记录信息，并发送这些信息到相应的备份设备上。备份信息包括表 8 的内容。

表 8　NAT44　ICMP Session 备份列表

字段名	长度(bit)
Timestamp	64
SourceIPv4Address	32
DestinationIPv4Address	32
ICMPv4Identifier	16
postNATSourceIPv4Address	32
DestinationIPv4Address	32
postNATICMPv4Identifier	16

备份信息记录了三元组（IPv4 source address，IPv4 destination address, ICMPv4 Identifier）和三元组（IPv4 source address, IPv4 destination address, ICMPv4 Identifier）之间的映射关系，其关系如下所示：

（*X*，*Y, i*1）　<--> (*T*, *Y*，*i*2)

对于其他协议的数据，如果 NAT64 支持，主用 NAT64 发送备份信息给备用 NAT64 设备。

NAT64 主用设备需要将 BIB 信息实时发往备用 NAT64 设备，发送通道可以是 TCP 等链接，实现信息的实时备份。timestamp 表示备份信息的产生时间，SourceIPv4Address 表示用户侧私网 IPv4 地址，DestinationIPv4Address 表示目的 IPv4 地址，ICMPv4Identifier 表示用户侧 ICMPv 标识符，

postNATSourceIPv4Address 表示经过翻译后的 IPv4 公网地址，DestinationIPv4Address 表示目的 IPv4 地址，postNATICMPv4Identifier 表示经过翻译后的 ICMPv4 标识符，protocolIdentifier 表示承载的协议。

对于其他协议的数据，如果 NAT44 支持，主用 NAT44 发送备份信息给备用 NAT44 设备。

NAT44 主用设备需要将 BIB 信息实时发往备用 NAT44 设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.2.2 NAT44 场景下流量的切换

主备切换后，需要将主用 NAT44 设备上的流量引导到备用设备上。

NAT44 主设备发布高优先级路由，备用设备发布低优先级路由，目的地址为公网地址的数据包将被路由到 NAT44 主设备，当主设备异常时，则进主备切换，并撤销该路由，使得原先的备用设备为主，通过路由收敛，目的地址为公网地址的数据包到达备用设备，保证 IPv4 流量继续畅通。

8.3 NAT64

8.3.1 NAT64 信息备份

如果主 CGN 设备采用 IPv6 到 IPv4 的网络地址转换技术（NAT64）进行报文转换，除了冷备份，热备份和温备份都需要向备份设备实时发送用户的映射绑定信息，主要包括绑定信息和 Session 信息，这些信息至少包括：IPv6 前缀及子网前缀长度、NAT64 前缀和虚拟专用网络信息。

主用 NAT64 设备在生成和删除 BIB 与 Session 时，都需要将此信息实时通知给备用 NAT64。

8.3.1.1 NAT64 BIB 表的备份

NAT64 利用 BIB 表记录映射绑定信息。NAT64 维护三种 BIB，分别为 TCP BIB、UDP BIB、ICMP Queries BIB。

当一个 NAT64 生成或删除一个 TCP/UDP BIB 时，主用 NAT64 发送备份信息给备用 NAT64 设备，备份信息见表 9。

表 9 NAT64 UDP/TCP BIB 备份信息

字段名	长度(bit)
TimeStamp	64
SourceIPv6Address	128
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
protocolIdentifier	8

备份信息表记录了在 IPv6 地址端口对和 IPv4 地址端口对之间的一个映射：

（X',x）<-->(T,t)

其中 X'代表某个 IPv6 地址，T 代表 NAT64 分配的 IPv4 地址，x 和 t 都是端口号。备份信息表中 timestamp 表示备份信息的产生时间，SourceIPv6Address 表示源 IPv6 地址，postNATSourceIPv4Address 表示经过翻译后的公网 IPv4 地址，SourceTransportPort 表示源端口号，PostNAPTSourceTransportPort 表示经过翻译后的端口号，protocolIdentifier 表示所用的传输协议。

当一个 NAT64 生成或删除一个 ICMP Queries BIB 时，主用 NAT64 发送备份信息给备用 NAT64 设备，备份信息见表 10。

表 10 NAT64 ICMP BIB 备份信息

字段名	长度(bit)
timeStamp	64
SourceIPv6Address	128
ICMPv6Identifier	16
postNATSourceIPv4Address	32
ICMPv4Identifier	16
protocolIdentifier	8

备份信息记录描述了在（IPv6 地址，ICMPv6 Identifier）和（IPv4 地址，ICMPv4 Identifier）之间的一个映射：

（*X'*, *i*1）<--> (*T*, *i*2)

其中，*X'*代表某个 IPv6 地址，*T* 代表一个 NAT64 分配的 IPv4 地址，*i*1 是一个 ICMPv6 Identifier，i2 是一个 ICMPv4 Identifier，

备份信息表中 timestamp 表示备份信息的产生时间，SourceIPv6Address 表示源 IPv6 地址，ICMPv6Identifier 表示源 ICMPv6 标识符，postNATSourceIPv4Address 表示经过翻译后的 IPv4 公网地址，ICMPv4Identifier 表示 ICMPv4 标识符。

对于其他协议的数据，如果 NAT64 支持，主用 NAT64 发送备份信息给备用 NAT64 设备。

NAT64 主用设备需要将 BIB 信息实时发往备用 NAT64 设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.3.1.2 NAT64 Session 的备份

当主用 NAT64 生成或者删除一个 TCP/UDP Session 时，需要记录信息，并发送这些信息到相应的备份设备上，备份信息见表 11。

表 11 NAT 64 TCP/UDP Session 备份信息

字段名	长度(bit)
Timestamp	64
SourceIPv6Address	128
postNATSourceIPv4Address	32
SourceTransportPort	16
postNAPTSourceTransportPort	16
destinationIPv6Address	128
postNATDestinationIPv4Address	32
destinationTransportPort	16
postNAPTdestinationTransportPort	16

备份信息记录了一组 IPv6 地址端口对和一组 IPv4 地址端口对的映射关系，其关系如下：

（*X'*,*x*）,(*Y'*,*y*) <--->(*T*,*t*), (*Z*,*z*)

其中，*X'*和 *Y'*是 IPv6 地址，*T* 和 *Z* 是 IPv4 地址，*x, y, z, t* 是端口号，且 *T* 是 NAT64 分配的 IPv4 地址，*Y'*是代表 IPv4 地址 Z 的 IPv6 地址，*Y'*由 NAT64 配置的算法根据 IPv4 地址 *Z* 产生，其具体过程见 IETF RFC6052。

备份信息表中 Timestamp 表示备份信息的生成时间，SourceIPv6Address 表示源 IPv6 地址，postNATSourceIPv4Address 表示经过翻译后的 IPv4 地址，SourceTransportPort 表示源端口号，postNAPTSourceTransportPort 表示经过翻译后的端口号，destinationIPv6Address 表示目的 IPv6 地址，postNATDestinationIPv4Address 表示经过翻译后的目的 Ipv4 地址，destinationTransportPort 表示目的端口号，postNAPTdestinationTransportPort 表示经过翻译后的目的端口号。

当主用 NAT64 生成或者删除一个 ICMP Queries Session 时，需要记录信息，并发送这些信息到相应的备份设备上。备份信息见表 12。

表 12　NAT64 ICMP Session 备份信息

字段名	长度(bit)
Timestamp	64
SourceIPv6Address	128
DestinationIPv6Address	128
ICMPv6Identifier	16
postNATSourceIPv4Address	32
postNATDestinationIPv4Address	32
ICMPv4Identifier	16

备份信息记录了三元组（IPv6 source address，IPv6 destination address, ICMPv6 Identifier）和三元组（IPv4 source address, IPv4 destination address, ICMPv4 Identifier）之间的映射关系，其关系如下：

（*X'*，*Y'*, *i*1） <--> (*T*, *Z*，*i*2)

其中 *X'*和 *Y'*分别代表 IPv6 地址，*T* 和 *Z* 分别代表 IPv4 地址，*i*1 为 ICMPv6 Identifier，*i*2 为 ICMPv4 Identifier，且 *T* 是 NAT64 分配的 IPv4 地址，*Y'*是代表 IPv4 地址 *Z* 的 IPv6 地址，*Y'*由 NAT64 配置的算法根据 IPv4 地址 *Z* 产生，其具体过程见 IETF RFC6052。

备份信息表中 Timestamp 表示备份信息的生成时间，SourceIPv6Address 表示源 IPv6 地址，DestinationIPv6Address 表示目的 IPv6 地址，ICMPv6Identifier 表示 ICMPv6 标识符，postNATSource IPv4Address 表示经过翻译后的公网源 IPv4 地址，postNATDestinationIPv4Address 表示经过翻译后的目的 IPv4 地址，ICMPv4Identifier 表示 ICMPv4 标识符。

对于其他协议的数据，如果 NAT64 支持，主用 NAT64 发送备份信息给备用 NAT64 设备。

NAT64 主用设备需要将 BIB 信息实时发往备用 NAT64 设备，发送通道可以是 TCP 等链接，实现信息的实时备份。

8.3.2　NAT64 场景下流量的切换

主备切换后，需要将主用 NAT64 设备上的流量引导到备用设备上。

在用户侧，NAT64 维护一个 IPv6 地址池，这个 IPv6 地址池由一个或多个 IPv6 前缀组成，我们称之为 Prefix64::/n，根据 IETF RFC6052 的定义，有两种前缀可以用作 Prefix64::/n。

一种是是知名前缀 64:ff9b::/96，IETF RFC6052 将它保留用来代表 IPv6 地址空间中的 IPv4 地址。

一种是网络特定前缀，是指由一个组织分配的 IPv6 前缀，用以创建 IPv4 地址的 IPv6 表示。

对于每一个 IPv6 地址池，NAT64 主设备发布高优先级路由，备用设备发布低优先级路由，目的地址含有这些前缀的 IPv6 数据包将路由到达 NAT64 主设备，当主设备异常时，则进主备切换，并撤销该路由，使得原先的备用设备为主，通过路由收敛，含有 IPv6 地址池中前缀的 IPv6 数据包到达备用设备，保证 IPv6 流量继续畅通。

9 备份场景的分析

9.1 备份场景的选择

根据业务的可靠性要求，在实际部署中，需要根据实际情况，如用户数量情况等，选用 1:1 备份、1+1 备份、*N*:1 备份或 *N*+1 备份 4 种场景中的一种，适用于单独 CGN 设备之间的备份场景。

9.2 1:1 备份场景

1:1 备份是指主备热备环境中，有且只有一个设备处于工作状态，另一设备则处于备份状态。在正常情况下，备份设备上并不接入用户，只有在主用设备出现异常是，才会将用户流量切换到备用设备上。在这种场景下，备份设备有可能长时间处于备份状态，仅与主用设备进行用户信息同步，通常重点局点/宽带用户采用部署采用 1:1 备份方案，以确保重点局点/宽带用户的网络可靠性。

9.3 1+1 备份场景

主备环境下，两台非满负荷工作的设备，在正常情况下各自都维护一部分用户。进行高可靠性部署时，将 CGN A 上某个用户接入端口备份到 CGN B 上某个空闲端口，将 CGN B 上某个用户接入端口备份到 CGN A 上某个空闲端口。在正常情况下，CGNA 与 CGNB 各自维护其主用端口上的用户，当某台 CGN 设备的主用接入端口或该端口与交换机之间的链路出现故障时，将该故障端口上的用户流量切换到它在另一台设备上对应的备份端口，故障恢复后再行回切。

在 1+1 备份场景中，两台 CGN 设备都各自维护用户，在正常情况下都在非满负荷状态下工作，这样能够有效降低设备出现故障的概率。同时，在出现故障时，需要切换的用户数量也比 1:1 备份场景要少，有利于设备稳定性。

1+1 备份场景适用于在同一局址部署多台 CGN 设备，相互备份的情况。

9.4 *N*:1 备份场景

N:1 备份场景指，为若干台 CGN 设备部署一台用于业务备份的 CGN 设备，多块主用 CGN 设备的板卡上的用户备份到备份设备上的一块板卡上。这台备份设备的备份板卡在网络正常的情况下并不负责用户接入，而是仅仅为备份设备与主用设备间做信息同步。当某台主用设备故障的情况下，这台设备上的用户流量会切换到备份设备上，故障恢复后再回切。

多数普通用户局点可以考虑采用 *N*:1 的部署方式，对城域网内宽带用户按照片区划分，一个区域按照规模在区域核心机房部署 1 台~2 台备份 CGN，以提高城域网内普通宽带用户接入的可靠性。

9.5 *N*+1 备份场景

N+1 备份是指，多台主用设备的多块板卡备份到一台备份设备的一块板卡上，同时备份设备的备份板卡也承担正常的用户业务，这样若干台设备互相之间作为备份设备。与 *N*:1 的场景相比，*N*+1 备份场景中用于备份的 CGN 设备在其他 CGN 设备正常时也会承担用户业务，不会造成设备的闲置，提高了设备的利用率。

N+1 备份在同局址内，CGN 设备较少，汇聚交换机也较少的情况下，较容易部署，同时也可以实现所有 BNAS 设备在正常情况下并不满负荷工作，出现网络异常时接管异常端口上的部分用户。但是对于局址内设备较多的情况，局点规划会变得非常复杂。

中华人民共和国
通信行业标准
运营级网络地址翻译(NAT)备份技术要求
YD/T 2729—2014
*
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

*
开本：880×1230　1/16　　2016年12月第1版
印张：1.75　　2016年12月北京第1次印刷
字数：50千字
15115·535
定价：25元
本书如有印装质量问题，请与本社联系　电话：(010)81055492