

ICG 高可用性实践指南

★内部资料、禁止外传★

引擎：R9.0



360 企业安全集团 行为安全子公司

2018 年 10 月

文档修订记录

版本	修订日期	修订人	联系方式	修订概要
v0.1	2018-10-12	赵宇辉		初始草稿；
V1.0	2018-10-16	赵宇辉		发布稿；

❏ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属 360 企业安全集团所有，受到有关产权及版权法保护。任何个人、机构，未经 360 企业安全集团的书面授权许可，不得以任何方式复制或引用本文的任何片断。

● 文档范围

本文包括 360 企业安全集团网康互联网控制网关引擎 R9.0 高可用性（HA）特性的相关介绍及实践建议。

● 期望读者

全体售前、交付、产品与 400 服务人员。

● 格式约定

粗体字 —— 命令和关键字

斜体字 —— 需要用户输入的信息



—— 使用技巧、建议、注意事项和引用信息等



—— 重要信息

【xxxx】 —— WebUI 界面上的菜单项、选项卡、按钮、界面链接（包括主界面、弹出窗口等）

<xxxx> —— WebUI 界面上提供的文本信息，包括单选按钮名称、复选框名称、文本框名称、配置选项名称以及文字描述等。例如，在<安全策略-新建>对话框中进行配置，<源地址>选择“any”。

“→” —— 使用该符号隔开点击对象（菜单项、子菜单、按钮以及链接等），例如，依次点击**【全局配置】→【对象设置】→【网址分类对象】**

目 录

1	ICG 高可用性特性概述	3
1.1	“透明”设备的高可用性	3
1.2	ICG9.0 高可用性（HA）的基本概念	4
1.2.1	网桥模式 HA 的运行模式及设备角色	4
1.2.2	网桥模式 HA 的实现机制	4
1.2.3	实施 HA 的基本要求	6
1.2.4	网关及镜像模式的 HA	6
1.3	ICG9.0HA 与 ICG8.4HA 的对比	6
2	网桥模式 HA 部署场景分析	7
2.1	常见的 HA 部署场景	7
2.2	典型场景 HA 部署	8
2.3	真正意义的“双活”场景	10
2.3.1	使用路由协议实现的“口字形”场景	10
2.3.2	使用路由协议实现的“全互联”场景	11
2.3.3	使用热备协议实现的“主主”场景	12
2.3.4	使用热备协议实现的“主备”场景	13
3	ICG9.0 高可用性（HA）实践中的常见问题	14
3.1	接口联动及 BYPASS 对 HA 的影响	14
3.1.1	接口联动与 HA 的配合问题	14
3.1.2	BYPASS 与 HA 的配合问题	16
3.2	跨三层 MAC 识别特性对 HA 的影响	18
3.3	非对称路由问题	20
4	附录	21
4.1	“口字型”主备模式网络场景流量路径分析	21
4.1.1	正常路径	21
4.1.2	主交换机下行链路故障	22

4.1.3	主交换机上行链路故障.....	23
4.1.4	主防火墙下行链路故障.....	24
4.1.5	主防火墙上行链路故障.....	25
4.2	参考测试用例.....	26

1 ICG 高可用性特性概述

1.1 “透明”设备的高可用性

高可用性（High Availability）技术，通过网络设备的冗余备份，提供了一种最小化网络中由于单点故障（Single Point of Failure）而带来的风险的方法。HA 并不是简单的把一组（通常两个以上）承担相同功能的设备堆砌起来，这其中涉及到设备部署模式、与用户网络环境配合以及设备自身 HA 实现机制等诸多因素。

通常在讨论 HA 问题时，人们常常基于防火墙等一类的网关设备进行讨论，往往会涉及“主备机”、“链路切换”、“状态协商”、“接口监测”等概念。而 ICG 作为网络审计设备，最常用的模式为“透明模式”（网桥模式）；“透明”设备在进行 HA 实践时的关注点和功能要求与网关设备存在着巨大的差异。

因此，在讨论具体 HA 功能及实践之前，我们需要弄清楚“透明”设备的一些特征。顾名思义，“透明”设备首要的特点就是对用户、网络是透明的(Transparent)，即用户以及网络中的其他设备意识不到“透明”设备的存在，因此：

- “透明”设备通常不参与 STP，也不参与动态路由
 - 设备没有直接触发链路切换的能力；只能被动的接受网络中其他设备引起的网络切换；
 - 没有根据流量的有无感知链路是否切换的能力；在负载均衡的链路中处于 HA 状态的两个设备可能同时收到流量；
- 在不与其他设备联动的情况下，没有第三方渠道获取链路情况

因此，对于“透明”设备的高可用性（HA）来说，关注点不在链路的切换，而是两台^①设备的策略同步、用户同步等状态同步上，这包括：

- 1) 管理员对其中一台设备的变更操作，能够及时同步到另一设备；
- 2) 不论何时，流量到达不同的设备能够受到相同的策略管理；
- 3) 不论何时，同一个用户的流量先、后到达不同的设备，有相同的认证状态（不需要重复认证），受到相同的策略管理。

本章在讨论 ICG9.0HA 的基本概念时，也将围绕着策略同步、用户同步展开。

① 此处约定，本文讨论的高可用性（HA）实践，都是指两台 ICG 设备的情况；对于“由于单台设备不满足性能要求，而需要部署多台”的负载均衡场景，不在本文讨论范围之内。

1.2 ICG9.0 高可用性（HA）的基本概念

1.2.1 网桥模式 HA 的运行模式及设备角色

基于 1.1 节的讨论，ICG 网桥模式下的 HA 功能不区分运行模式，设备角色也没有主、备之分。不论实际网络结构如何，是否有流量经过 ICG，两台设备时刻处于“双活”状态。为了便于完成策略的配置及同步，HA 设备分为“主控”、“节点”两种角色，其中：

- 主控设备负责将策略配置同步到节点设备
- 用户上下线状态在主控设备和节点设备之间双向同步

配置页面也相对简单，如图 1 所示：



图 1 ICG9.0 高可用性（HA）配置界面

1.2.2 网桥模式 HA 的实现机制

1.2.2.1 协商机制

由于网桥模式下的 HA 没有设备状态的概念，因此也不存在动态协商的概念；设备角色（主控、节点）在配置时一旦由管理员确认，不会改变。

具体配置时，需要管理员手动指定设备角色、接口，“保存配置”即可。若对端异常或角色冲突，系统将会给出提示，如图 2 所示：



(a)

(b)

图 2 ICG9.0 HA 配置过程

若 HA 配置成功，系统给出工作正常提示，如图 3 所示：

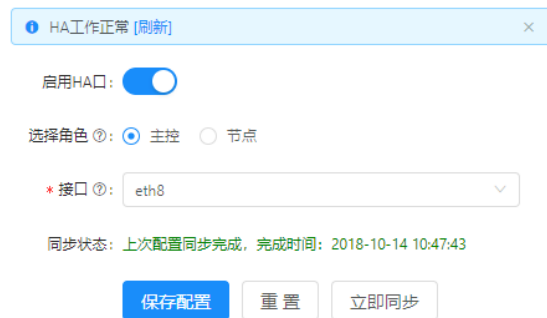
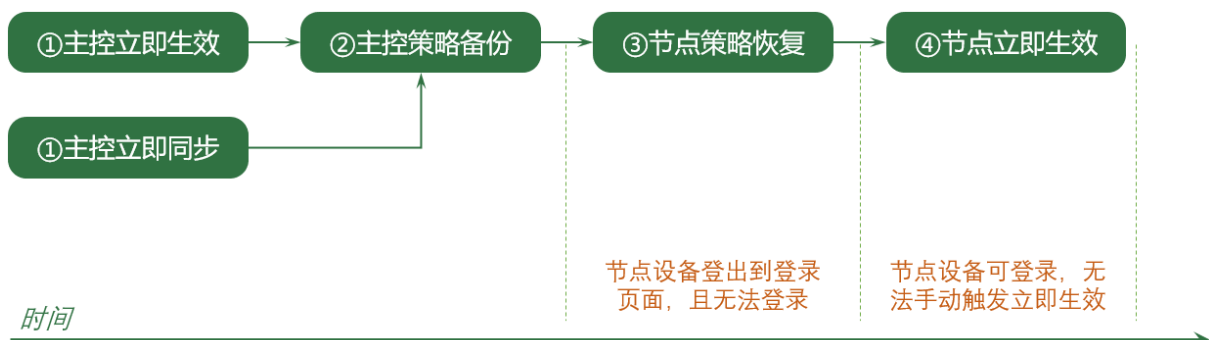


图 3 ICG9.0 HA 配置成功界面

1.2.2.2 同步机制

当前 ICG9.0 的 HA 实现，对于用户状态采取双向实时同步的机制；对于策略配置采取类似于策略备份/恢复的机制，由主控设备向节点设备触发同步，具体过程如下：



主控设备仅在两种情况下向节点设备同步配置：

- 主控设备触发“立即生效”
- 主控设备点击 HA 配置页面“立即同步”按钮

其中，步骤 2、3 均为数据库操作，时间可忽略不计；HA 策略同步的时间主要取决于主控、节点设备的“立即生效”时间，根据策略数量及机型性能的不同，“立即生效”时间可能有所差异。

处于步骤 3 的节点设备将会自动登出到登录页面，并无法登录，如图 4 所示：

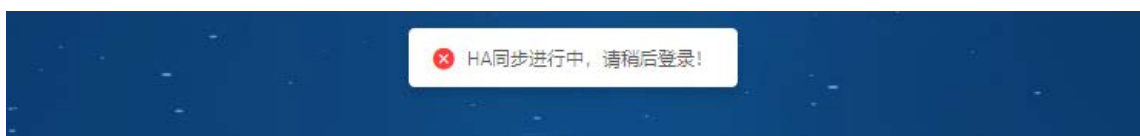


图 4 HA 同步过程中的节点设备

值得注意的是：

- 1) 同步的内容包括所有与策略相关的配置（包括对象等）、用户列表、管理员配置等，不包括网络配置；

- 2) 同步后，节点设备的配置将与主控设备完全一致，其本地配置的策略、用户列表、管理员配置都将被覆盖；
- 3) 部分在同步范围内的操作（如三层交换机配置）不会触发“立即生效”，也就不会触发同步；此时需要通过手动修改其他配置，触发“立即生效”。

1.2.3 实施 HA 的基本要求

ICG9.0 在实施 HA 时，要求两设备具备完全一致的软件版本，包括大小版本号、Hotfix 编号，以保证策略的正常同步。

除此之外，并不要求具备相同的硬件型号和网卡布局^①。

1.2.4 网关及镜像模式的 HA

ICG9.0 对于另外两种常见的部署模式（网关、镜像）同样也支持 HA 的部署，但仅限于策略同步、用户同步。

这里需要特别说明的是，理论上 ICG 网关模式的 HA 应该考虑链路的冗余和切换，类似于防火墙类设备的 HA，但目前 ICG9.0 还没有实现这些功能^②。对于网关模式的用户，启用 HA 特性后仅能实现“温备”的效果，即：保证两台设备的策略配置^③和用户状态完全一致，其中主控设备连接业务线；一旦主控设备出现故障，需要用户管理员手动切换业务线至节点设备。

1.3 ICG9.0HA 与 ICG8.4HA 的对比

与 ICG8.4 版本相比，ICG9.0HA 特性的变化主要体现为支持用户双向同步，这拓展了 HA 特性的适用场景，将在后续章节进行论述。其他方面的差异如下表所示：

	ICG9.0	ICG8.4
设备角色	主控、节点（手动指定）	主机、备机（手动指定）
配置	仅需指定 HA 接口	需要指定主备机 IP 地址
策略同步	主控→节点单向同步	主机→备机单向同步
用户同步	双向同步	主机→备机单向同步

① “透明”模式设备的 HA 只关注策略同步，只要能保证两设备的配置可以同步（具备完全一致的软件版本）就可以实现 HA；由于不同步网络配置，也不关注用户网络链路的状态，因此对于硬件型号和网口数量没有要求。

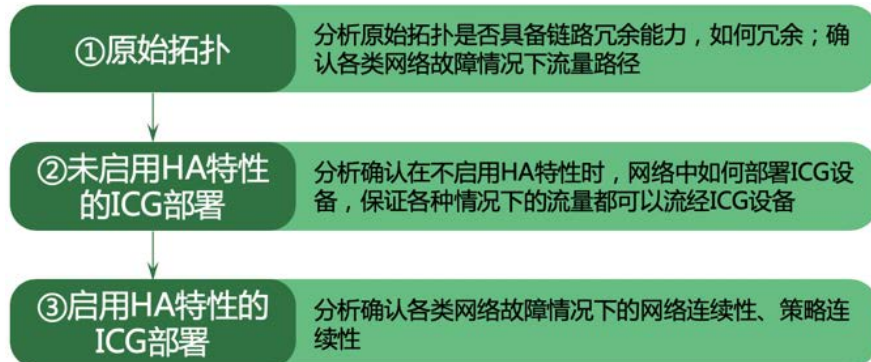
② 后续版本将会考虑实现，以形成完整的 HA 方案。

③ 一般地，“温备”场景下两台设备应具有完全相同的接口地址。

2 网桥模式 HA 部署场景分析

2.1 常见的 HA 部署场景

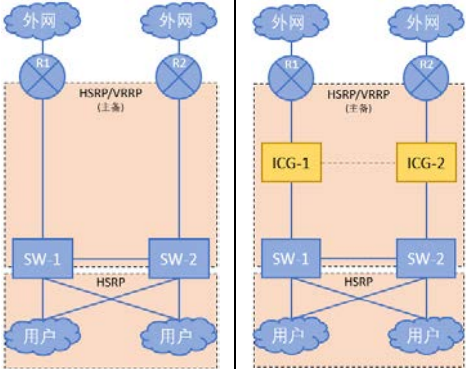
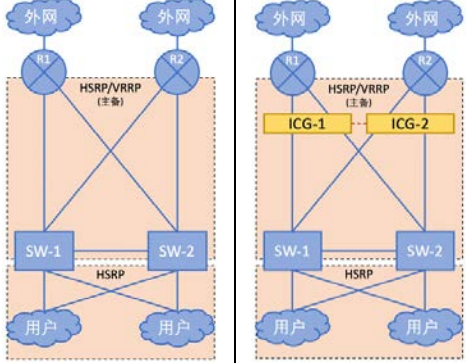
在考虑网桥模式 HA 的部署场景时，应该按照以下过程进行分析：



任何场景的 HA 设计要同时满足：网络连续性、策略连续性（包括审计控制连续性、用户状态连续性、日志记录连续性等）；且两个连续性的保证要自动完成，不能有任何人工干预。一般地，按照原始拓扑是否具备链路冗余能力进行分类，常见的典型场景如下表所示：

	场景分类	原始拓扑	ICG (HA) 部署	场景分析
1	无链路冗余			网络本身不具备链路冗余能力，但客户注重审计完整性，尽可能减少由于 ICG 设备故障造成的网络无审计管理的情况；ICG 上下游交换机通过 STP 实现链路冗余，正常情况下只有一个 ICG 设备承载流量。
2	使用路由协议实现链路冗余			ICG 上下游设备通过路由协议（如 OSPF 等）实现链路的冗余切换；SW-1、SW-2 对内网用户使用主备模式 ^① 的热备协议，用户的第一跳网关只能是 SW-1、SW-2 其中之一；因此，正常情况下只有一个 ICG 设备承载流量。

① 若采用主主模式，两台 ICG 设备会同时承载流量；这是由于在这个场景中，SW-1、SW-2 通过 OSPF 学习到默认路由的下一跳不同（SW-1 下一跳为 R1、SW-2 下一跳为 R2），具体分析请参见 2.3.1 节。

3	使用热备协议实现链路冗余		ICG 上下游的三层设备之间通过主备模式的热备协议（如 VRRP/HSRP）实现链路的冗余切换； 由于 ICG 上游设备为主备模式，因此不论 SW-1、SW-2 对内网用户采取什么模式（主主/主备），正常情况下只有一个 ICG 设备承载流量。
4	（HSRP/VRRP） （主备模式）		与上一场景相比，ICG 上下游设备采用“全互联”结构 ^① ，为了保证审计的完整性 ^② ，ICG 设备需要启用多个网桥；多网桥的 ICG 设备建议部署在近路由器（防火墙） ^③ 端，以确保在一般情况下只有一个 ICG 设备承载流量。

2.2 典型场景 HA 部署

本文以最为常见的“口字型”主备模式网络场景（上表场景 3）为例对 ICG9.0HA 的部署过程及效果进行分析。文中所使用的测试环境如图 5 所示。在这个环境中：

- 两台边界防火墙外网口分别连接两个不同的运营商，各有一个公网地址，图中以 192.168.199.101、192.168.199.102 模拟；
- 防火墙内网口与两台核心交换机的上联口接口（Vlan 接口）处于同一个 Vlan 中；并启用 HA 特性^④，左侧防火墙为主机，右侧防火墙为备机，使用虚拟 IP 作为内网网关；
- 两台核心交换机启用两个 VRRP 实例，分别作为防火墙的回指路由网关和内网用户的下一跳网关；并使得左侧交换机为两 VRRP 实例的主机，右侧交换机为两 VRRP 实例的备机。

① 通常在这类场景中，中间的“全互联”结构都会首先通过 STP 收敛成一个无环网络。

② 这里所说的审计完整性，是指不论流量经过“全互联”结构中的哪一条链路转发，都可以经过 ICG 设备而被审计。

③ 理论上，部署在近交换机端也不影响网络连续性和策略连续性；但这会造成审计日志“非必要”的分散在不同的 ICG 设备上，给管理带来不便，具体分析请参见 2.3.4 节。

④ 关于防火墙的 HA 特性实践，不在本文的讨论范围之内；请参见《防火墙高可用性实践指南》一文。

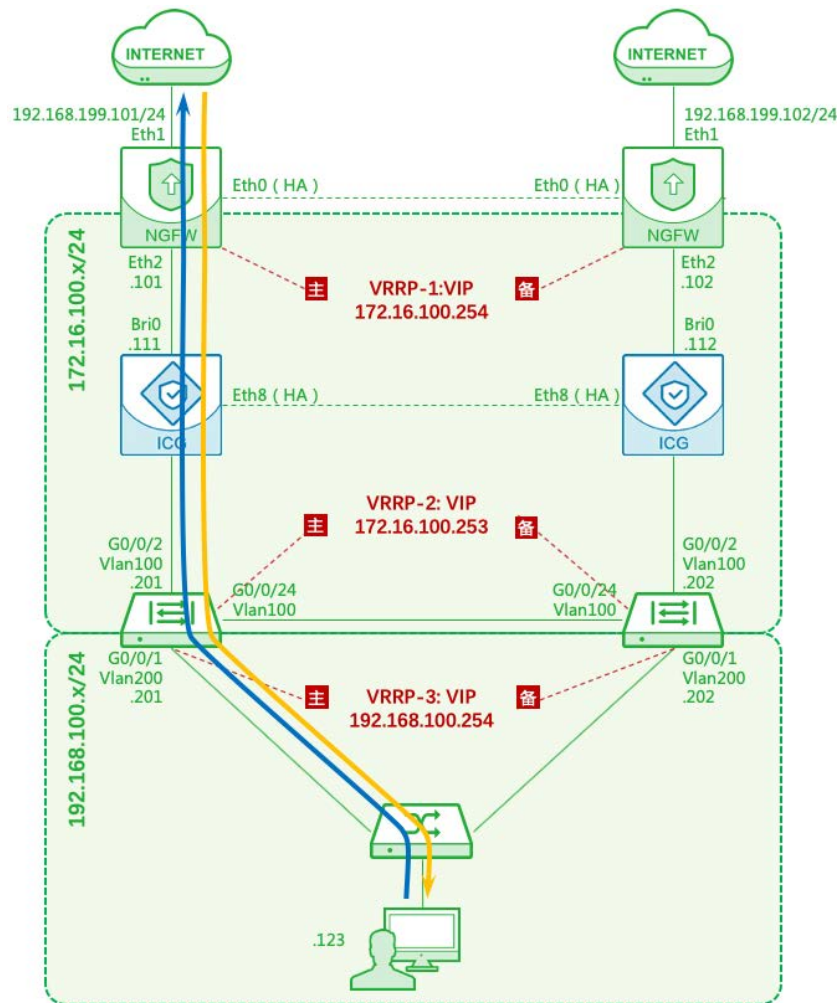


图 5 测试拓扑

正常情况下，内网用户访问互联网的上下行流量路径如图 5 中箭头所示。因此我们定义位于左侧的 ICG 设备为主控设备，右侧的 ICG 设备为节点设备。

ICG9.0HA 的配置方法相对简单，仅需定义设备角色即可，因此上线步骤可参考普通设备的上线过程：

- 1) 配置好主控、分支设备的网络配置（桥口、管理口、路由配置），建议启用“接口联动”特性^①；
- 2) 连接两设备的 HA 线，定义好设备角色后启用 HA 特性；等待设备提示 HA 工作正常，如图 3 所示；
- 3) 按照适当的顺序将两设备割接上线，尽量减少网络中断；在此环境中，可先割接节点设备（右侧），随后割接主控设备（左侧）。

^① 具体分析，请参见 3.1.1 节。

值得注意的是，以上过程假设两台 ICG 设备为全新设备（均无配置）；当我们为一台已经在网运行的 ICG 设备（已经存在策略）额外增加一台全新设备而构成 HA 设备组的时候，务必首先确保原始有策略的设备角色为“主控”，新设备为“节点”。否则会造成策略丢失。

即便是希望新设备为“主控”设备，也需要在同步一次配置之后再进行调整。

关于该场景下各类网络故障情况下的流量路径分析，请参见 4.1 节。

2.3 真正意义的“双活”场景

仔细分析不难发现，2.1、2.2 节所描述的场景中，不论网络结构多么复杂，在最终收敛稳定之后，流量路径只有一种。也就是说，在同一时刻只有一台 ICG 设备承载流量，另一台设备没有流量。如果从有无流量角度来衡量 ICG 设备是否“活跃”的话，这些场景都不属于“双活”场景，使用 ICG8.4 设备都可以支持。

在实际的工程实践中，常见的“双活”场景包括四种，这四种网络结构使用 ICG8.4 版本的 HA 特性就不能很好的满足了，以下来具体分析。

2.3.1 使用路由协议实现的“口字形”场景

在这类场景中，两台核心交换机通过 OSPF 协议学习到的默认路由下一跳不同，根据最短路径原则，SW-1 的下一跳为 R1，SW-2 的下一跳为 R2；与 2.1 节场景 2 不同的是，两台核心交换机对内网用户采用了“主主”模式，如图 6（a）所示：

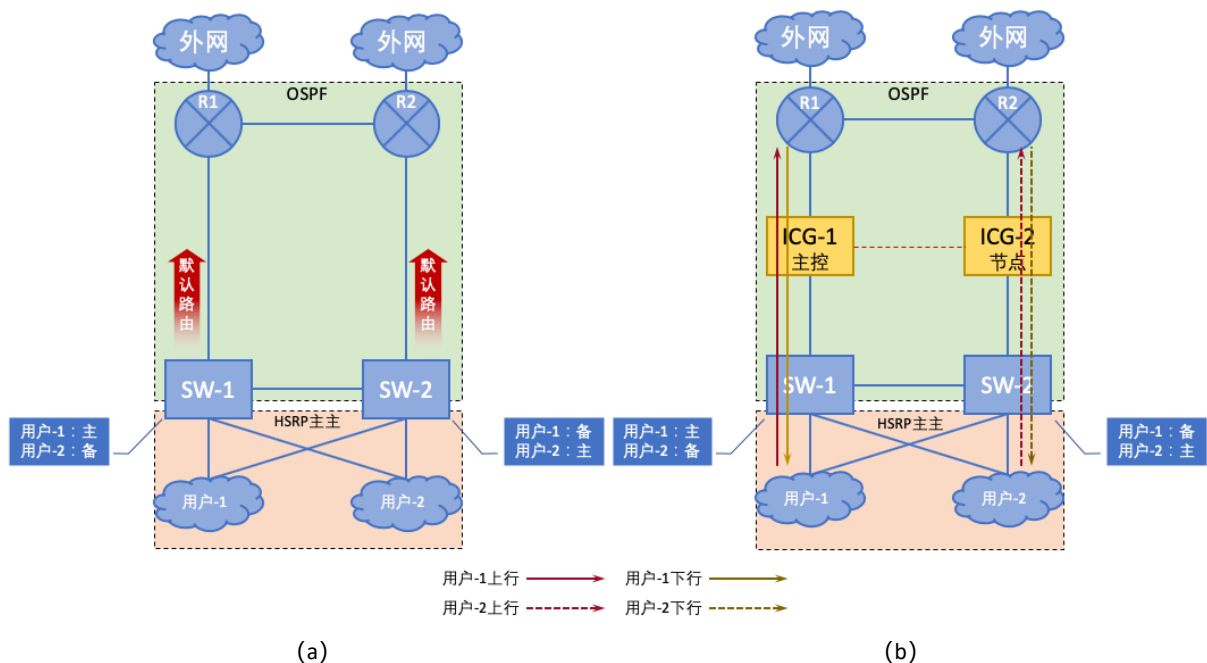


图 6 “双活” 场景 (1)

这就使得不同用户具有不同的流量路径，如图 6（b）所示：

- 用户-1：SW-1 → ICG-1 → R1
- 用户-2：SW-2 → ICG-2 → R2

显然，此时 ICG-1、ICG-2 同时承载流量。当网络发生故障时，OSPF 重新收敛，各用户的流量路径发生变化，如图 7 所示：

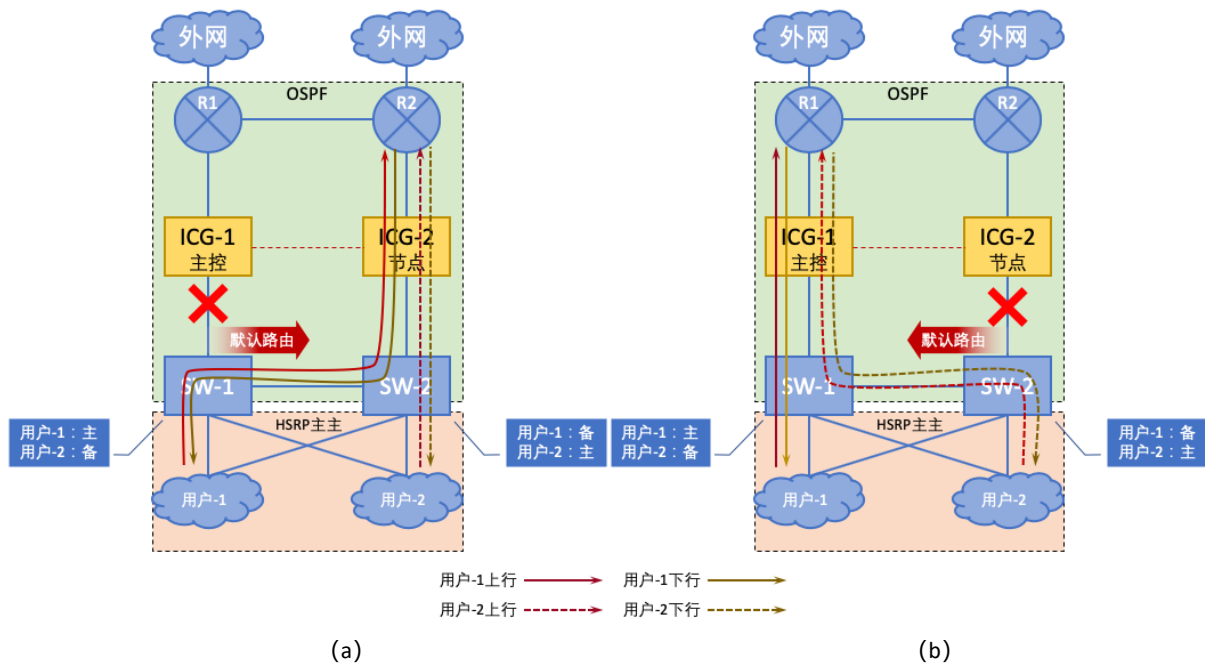


图 7 “双活”场景 (1) 网络故障状态

图 7（a）中，SW-1 上行链路故障，使得用户-1 的路径变为 SW-1 → SW-2 → ICG-2 → R2，由于节点设备存在主控设备上的用户状态，因此流量路径切换后，用户-1 也不需要重新认证。

图 7（b）中，SW-2 上行链路故障，使得用户-2 的路径变为 SW-2 → SW-1 → ICG-1 → R1，由于主控设备存在节点设备上的用户状态（用户双向同步），因此流量路径切换后，用户-2 也不需要重新认证。ICG8.4 的 HA 实现不支持用户双向同步，因此在这个场景下，用户-2 需要重新认证，用户体验较差。

2.3.2 使用路由协议实现的“全互联”场景

在这类场景中，“全互联”结构使得 SW-1、SW-2 具备等效的默认路由，OSPF 会对流量进行负载；因此不论核心交换机对内网用户采用何种模式（主主/主备），用户均可能存在两种路径，如图 8（a）、（b）所示；此时 ICG-1、ICG-2 同时承载流量。

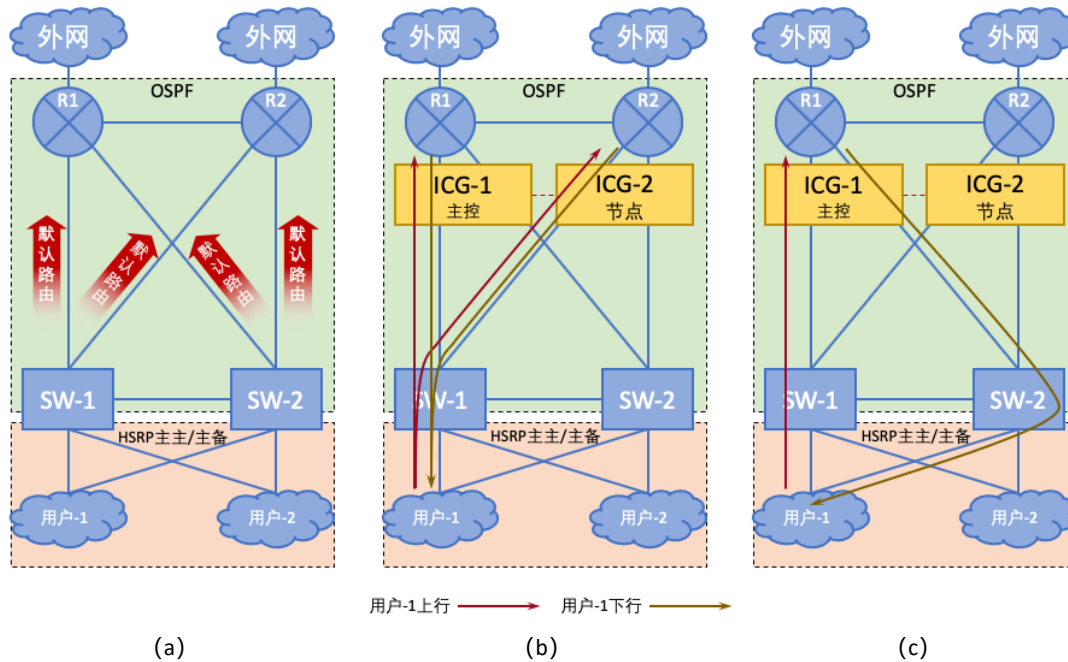


图 8 “双活”场景 (2)

同样地，只有具备双向用户同步特性的 HA 实现才可以支持此类场景。特别要指出的是，与核心交换机一样，R1、R2 也存在等效的内网路由，因此下行流量也可能存在多个路径，如图 8 (c) 所示；由于 ICG 设备部署于近路由器端，因此保证了由同一个路由器转发的流量始终经过同一台 ICG 设备，不影响审计效果。

2.3.3 使用热备协议实现的“主主”场景

此类场景实际上是 2.1 节场景 3 的扩展，边界防火墙下联两个“口字型”结构连接了两个用户区域，同时启用两个 HA 实例分别为不同用户区域提供主备下一跳网关。同样地，不同用户具有不同的流量路径；如图 9 所示：

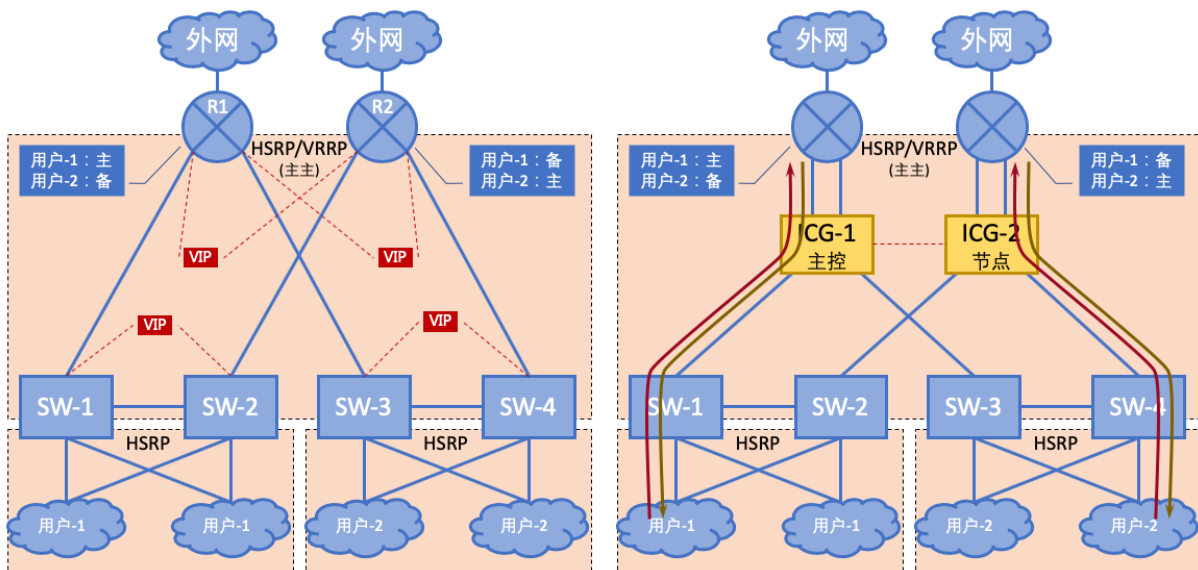


图 9 “双活”场景 (3)

除了图 9 所示的“主主”场景，还有一种通过子接口和 Trunk 链路实现的“主主”场景，如图 10 所示：

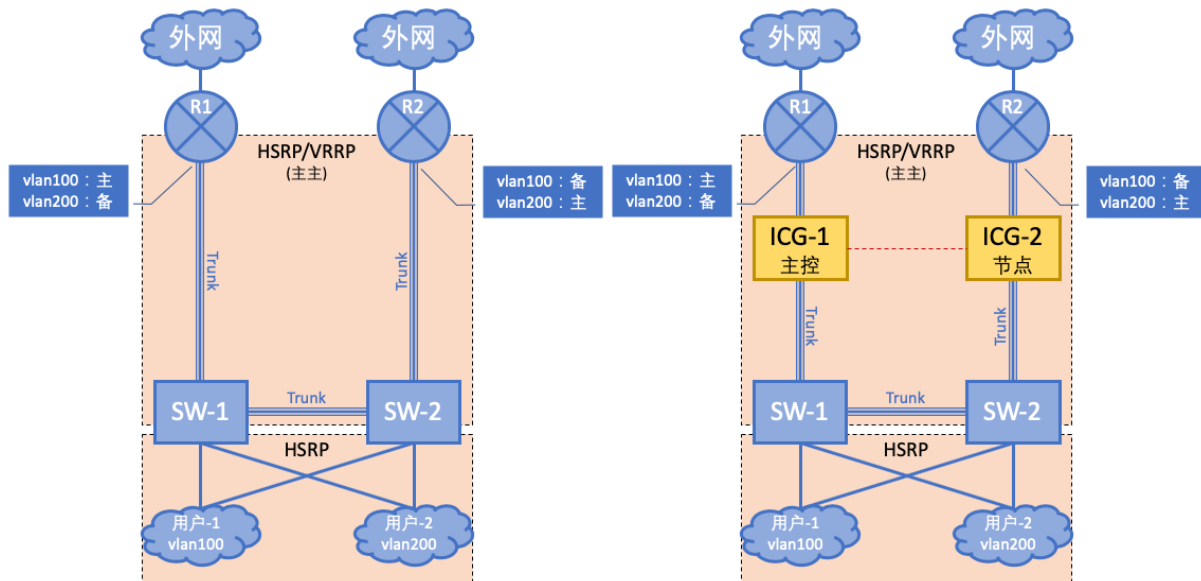


图 10 “双活”场景 (4)

图 9、图 10 的“主主”场景也必须通过具备双向用户同步特性的 HA 进行支持。

2.3.4 使用热备协议实现的“主备”场景

如果将 2.1 节场景 4 中的 ICG 设备部署在近交换机端，且交换机对内网用户采用“主主”模式时，同样会造成两台 ICG 同时承载流量的情况，如图 11 所示：

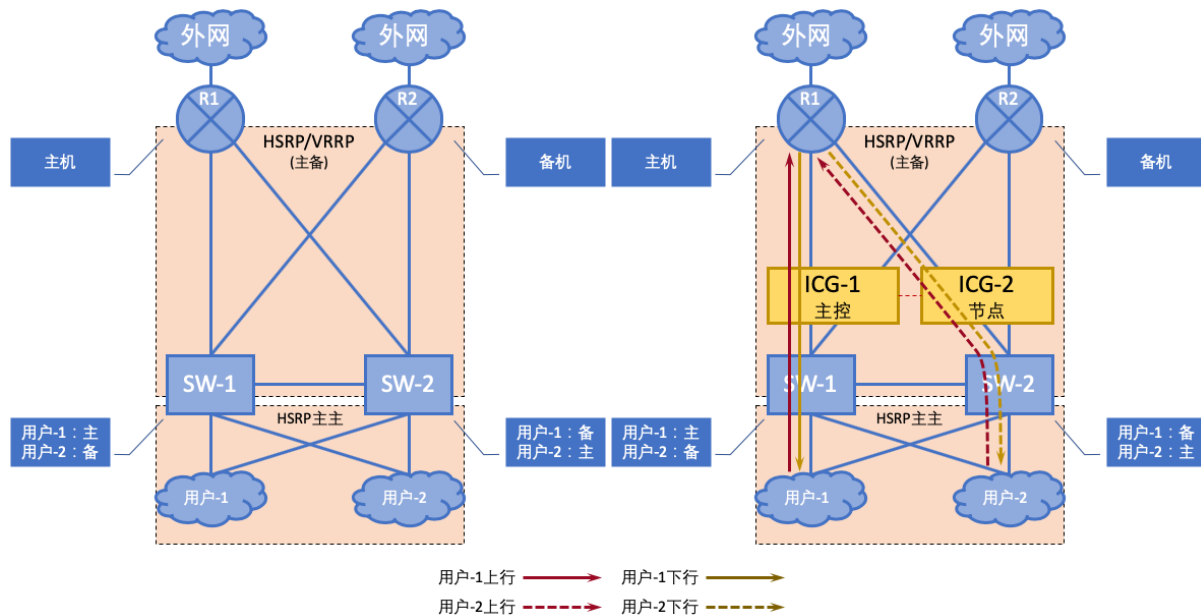


图 11 “双活”场景 (5)

此类场景同样必须通过具备双向用户同步特性的 HA 进行支持。不难发现，这种

部署导致了在网络正常情况下，审计日志分散到两台 ICG 设备当中（两设备同时承载流量），尽管不影响审计效果，但给日常管理带来不便；而这种不便完全可以通过优化 ICG 设备的部署位置来规避，因此这种部署形式并不推荐。

3 ICG9.0 高可用性（HA）实践中的常见问题

3.1 接口联动及 BYPASS 对 HA 的影响

3.1.1 接口联动与 HA 的配合问题

所谓“接口联动”，是指位于同一个网桥的两个接口只能同时处于 up 或同时处于 down 状态的特性。该特性常见于“透明”模式设备的部署场景，特别是在某些与链路状态强相关的场景中尤为重要。

在 HA 的工程实践当中，不启用“接口联动”虽然不会对联通行造成影响；但我们仍然建议始终开启接口联动特性，以使网络获得更好的健壮性，具体表现在：

- 优化流量转发路径，提高流量转发效率

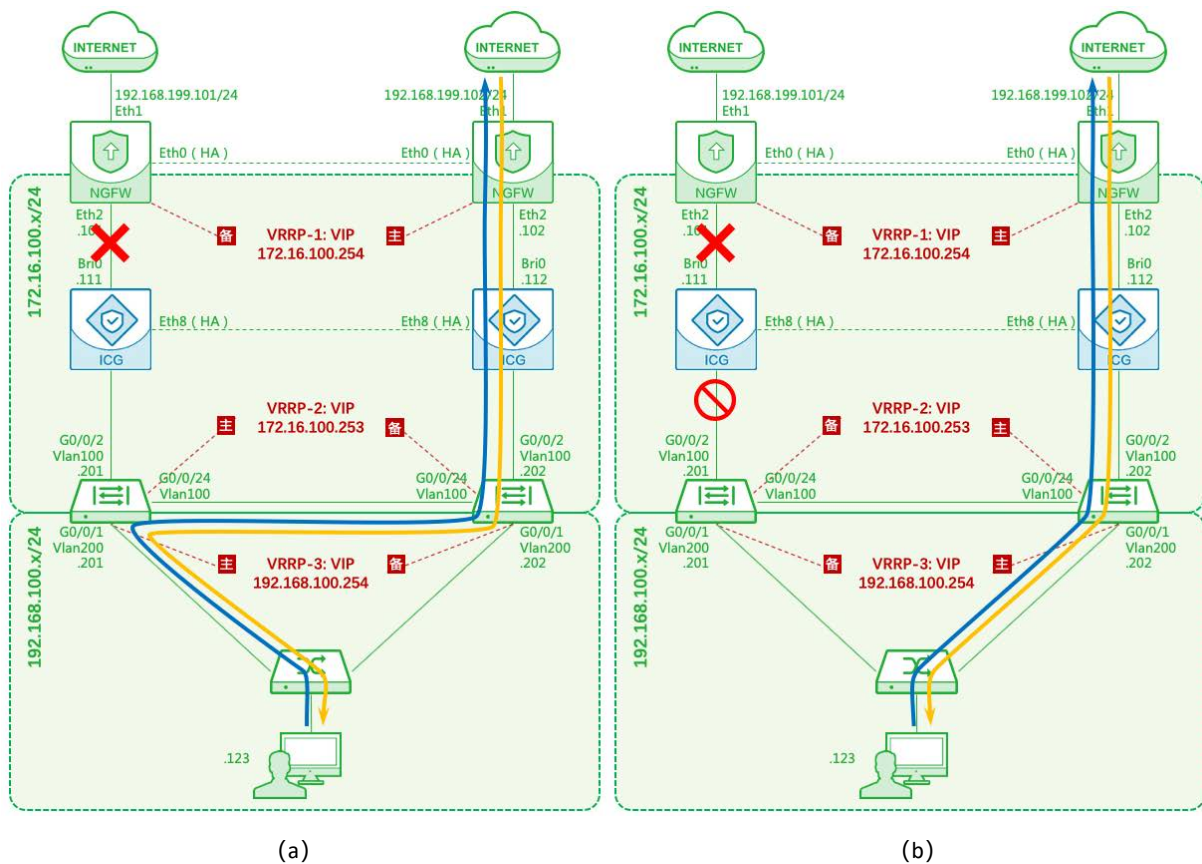


图 12 接口联动场景 (1)

以 2.2 节环境为例，当 ICG 主控设备（左侧）上行链路故障后，防火墙主备机切

换。若 ICG 设备没有启用“接口联动”特性，交换机（左侧）无法感知到链路故障，流量路径将重新收敛为图 12（a）所示。这样虽然没有影响联通性，但流量路径并不是最优化的。

当 ICG 启用“接口联动”特性后，ICG 上行链路故障后，处于同一网桥的下行接口也进入关闭状态；交换机（左侧）感知到链路“故障”后，变更了两个 VRRP 实例的主备状态。最终使得流量路径优化为图 12（b）所示。

➤ 提高某些场景的网络故障响应速度

图 13（a）中，由于交换机（左侧）未感知到链路故障，它仍然是用户的下一跳网关，流量依旧会转发给它。但此时左侧交换机需要等待 OSPF 协议重新收敛，才可以学习到来自于右侧交换机的默认路由，这个时间远远大于 VRRP 的主备切换时间。

当 ICG 启用“接口联动”特性后，链路故障后右侧交换机将成为用户的下一跳网关；由于它已经具备默认路由，因此流量到达右侧交换机后会被立刻转发，网络联通性即刻恢复。经测试，在此场景中，未启用“接口联动”时，网络故障响应时间为 8 个 ping 包，启用“接口联动”后，响应时间仅为 1 个 ping 包。

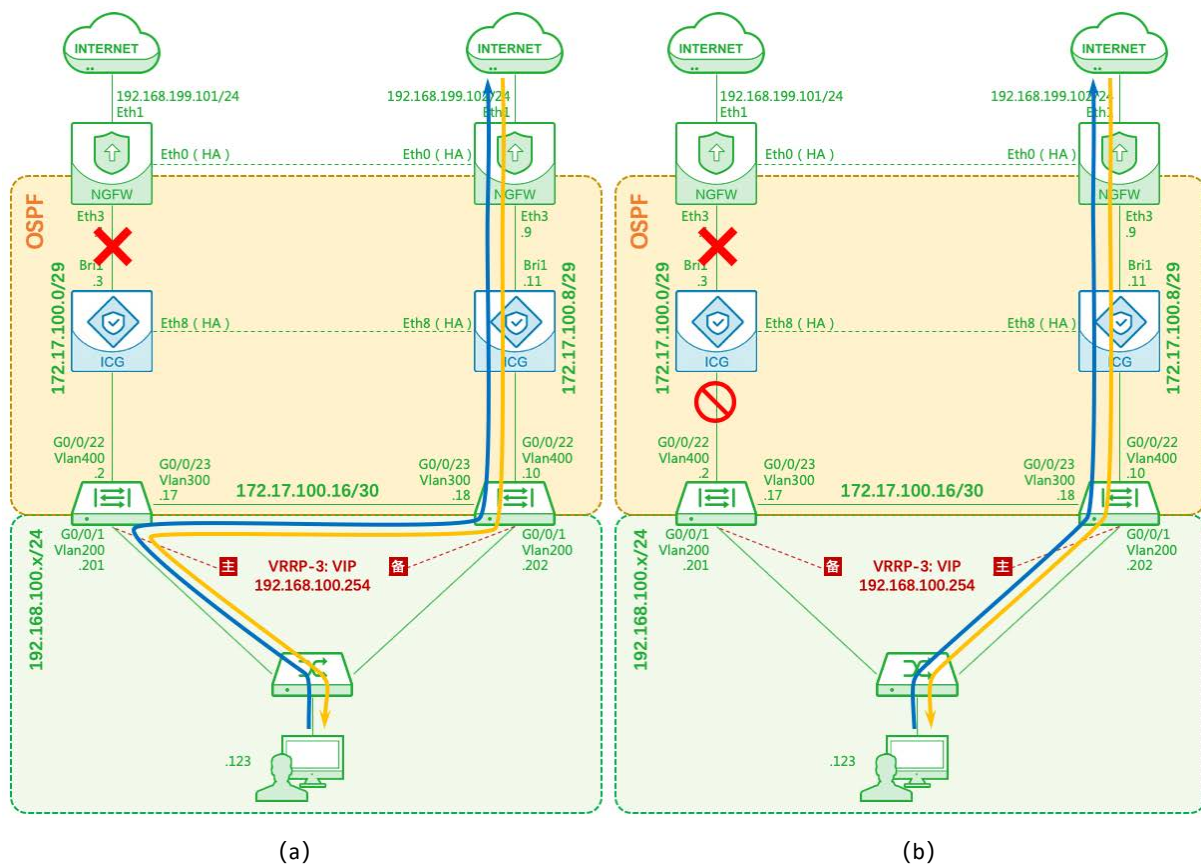


图 13 接口联动场景 (2)

3.1.2 BYPASS 与 HA 的配合问题

“透明”模式设备的 BYPASS 特性并不陌生，它通过将处于同一网桥的一对网口物理联通保证了设备自身故障情况下的网络连续性。但在 HA 实践场景中，我们需要重新考虑这一特性给网络带来的影响。考虑如图 14 所示的场景。

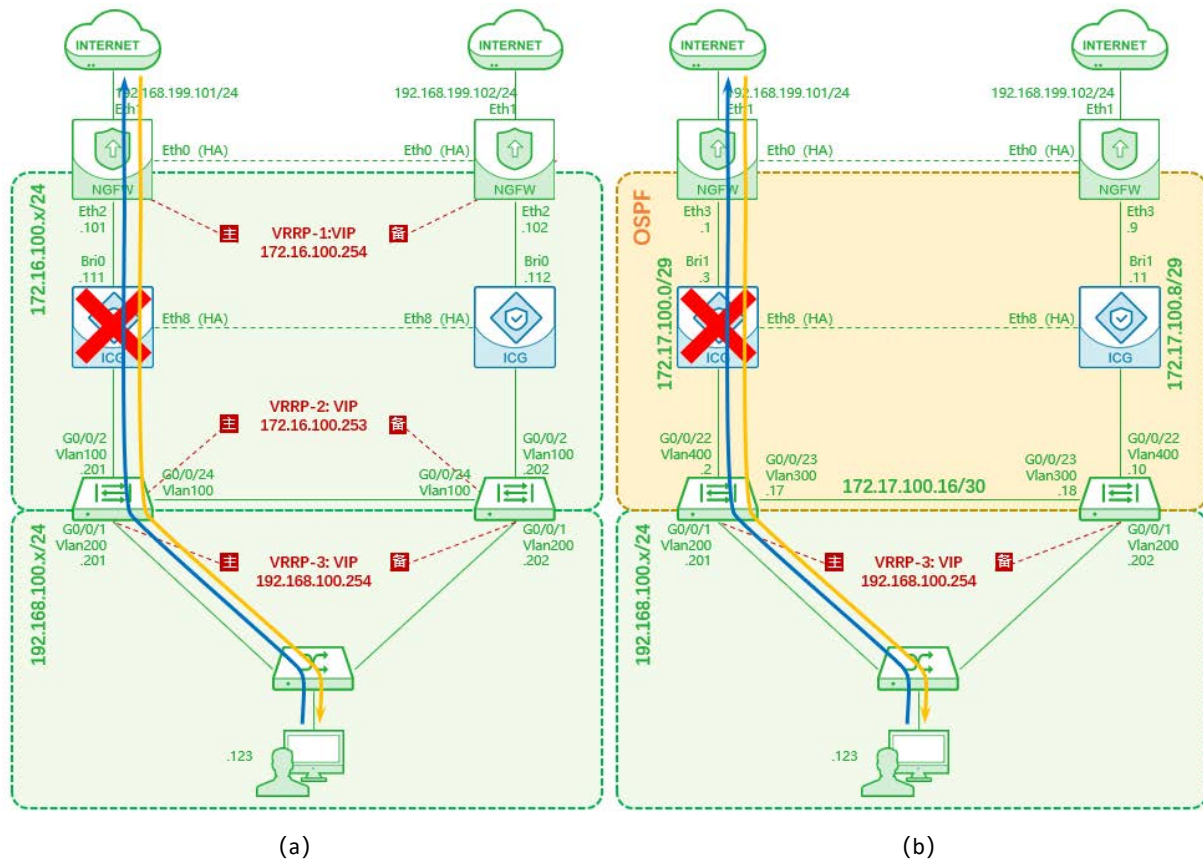


图 14 启用 BYPASS 特性时设备故障后的流量路径 (1)

在该场景中，由于设备启用了 BYPASS 特性，因此设备一旦发生故障会即刻变为“一根导线”；不论客户网络使用何种方式冗余，都不会触发网络重新收敛，流量路径不会发生变化。网络连续性未受影响，但此时流量已经不受任何 ICG 设备的审计管理，策略连续性没有得到保证，这违背了部署 HA 的初衷。

因此，在具体的 HA 实践中可通过以下两种方案之一规避解决这一问题。

➤ 禁用 BYPASS 特性

对于采用内置 BYPASS 装置（电口、光口）的设备来说，可通过【系统配置】→【高级配置】→【系统参数】中的“硬件 BYPASS 开关”选项卡禁用 BYPASS 特性，如图 15 所示。



图 15 硬件 BYPASS 开关

此外，为了保证系统在掉电状态下处于“非 BYPASS”状态^①，需要调整设备 BIOS 的默认配置^②，如图 16 所示：

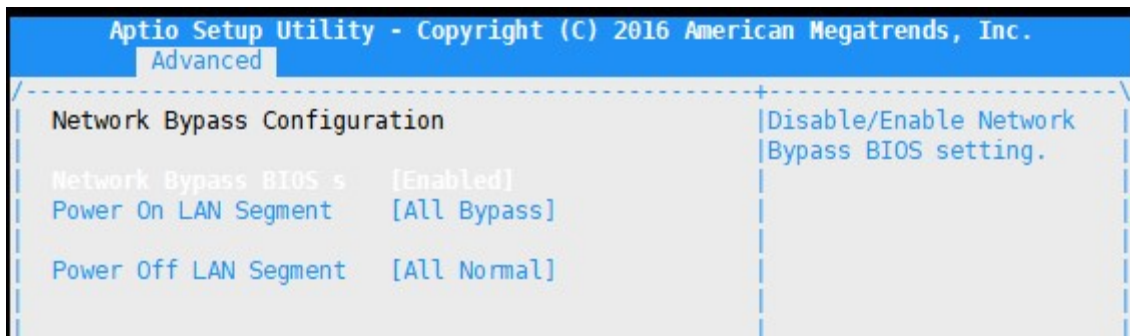


图 16 主板 BIOS 中关于 LAN BYPASS 的配置

默认情况下，Power Off LAN Segment 参数为[All Bypass]，这意味着设备断电后将处于“BYPASS”状态；将其修改为[All Normal]，保存并重启。此时设备断电后将处于“非 BYPASS”状态。

⚠注意：

修改 BIOS 参数的操作涉及设备重启，且需要串口及特殊密码进行操作；因此不建议一线人员自行操作，可优先采取其他方法规避 BYPASS 问题带来的影响。
若项目确实需要，请联系产品及研发人员进行特定支持。

➤ 上游防火墙增加对 ICG 设备桥口地址的监测

对于图 5 所示的场景，可以通过在边界防火墙的“失效监测”中增加对 ICG 主控设备桥口地址的监测来保证策略连续性。

这样，当 ICG 主控设备故障且进入“BYPASS”状态时，由于桥口地址已经“失效”，边界防火墙主备机状态切换，所有流量将通过 ICG 节点设备转发；保证了策略的连续性，如图 17 所示：

① 一般地，具备内置 BYPASS 装置的设备在未上电情况下，会处于 BYPASS 状态；这是由主板 BIOS 中的相关配置决定的。

② 不同硬件平台的 BIOS 配置不尽相同，这里选取一种作为示例。

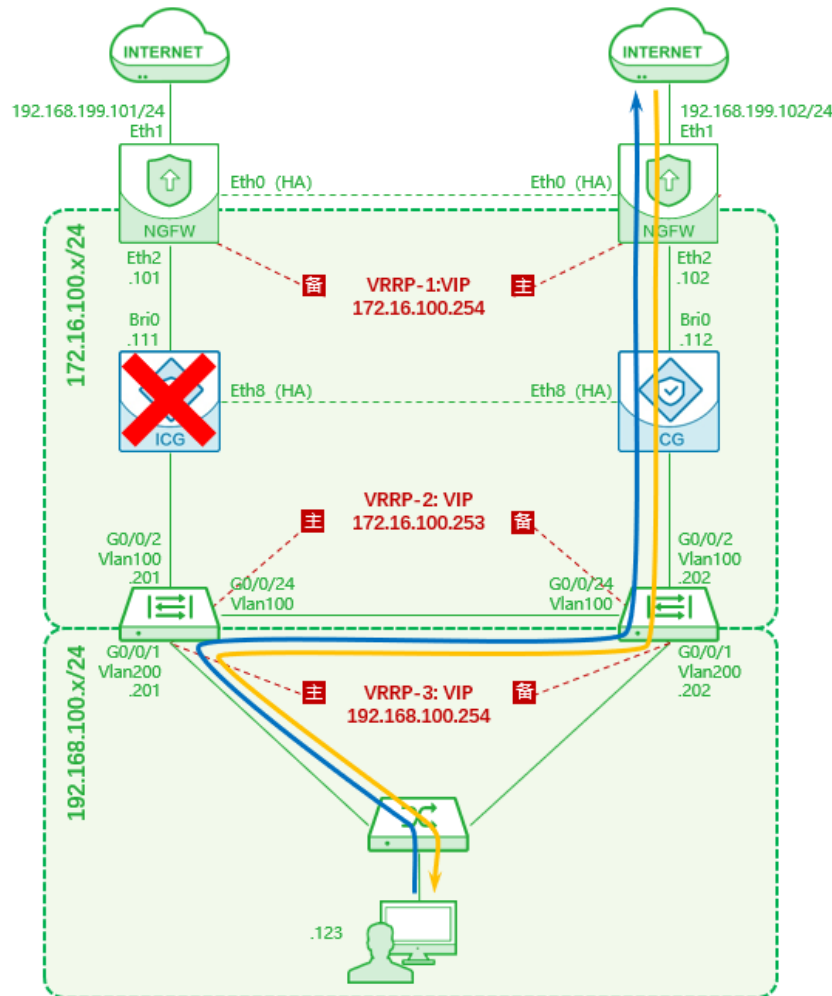


图 17 启用 BYPASS 特性时设备故障后的流量路径 (2)

这种方法特别适用于项目中对于 HA 特性的功能测试。一般地，测试用例常用“直接断电”的方式验证 HA 的效果。若边界防火墙未将 ICG 桥口地址作为监测对象，会出现“直接断电”后流量路径未发生改变，ICG 节点设备无审计日志的情况。这一问题虽然已经不属于 ICG 设备功能的范畴，但也不利于测试用例的正常执行。因此，在执行功能测试时，一线人员要特别注意这些细节。

3.2 跨三层 MAC 识别特性对 HA 的影响

在某些 HA 实践场景中，网络故障后用户流量切换到另外一台 ICG 设备，此时可能会由于用户流量路径的变化而引起上线用户 MAC 地址的变化，导致用户下线。如图 18、图 19 所示。

在启用认证的场景中（如 Web 认证），部分用户会重新认证，违背了部署 HA 的策略连续性原则。

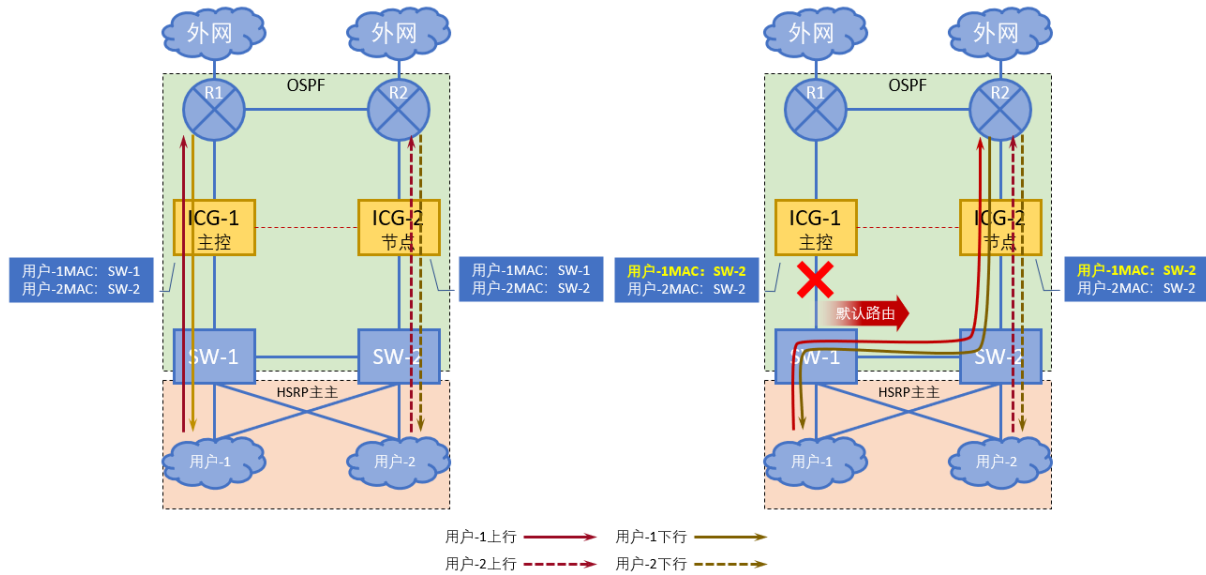


图 18 流量路径变化引起的用户 MAC 地址变化

上线时间	下线时间	用户	IP	认证类型	流量(KB)	动作	下线原因
2018-10-12 10:03:36	2018-10-12 10:04:03	行为安全/产品部/赵光军	192.168.100.123	web本地认证	1	下线	mac变化检查
2018-10-12 09:56:13	2018-10-12 10:02:23	行为安全/产品部/赵光军	192.168.100.123	web本地认证	493,938	下线	mac变化检查
2018-10-12 09:40:07	2018-10-12 09:45:07	192.168.100.123	192.168.100.123	本地自动识别	2,923	下线	无流量下线
2018-10-12 09:35:06	2018-10-12 09:40:06	192.168.100.123	192.168.100.123	本地自动识别	2,943	下线	无流量下线
2018-10-12 09:30:06	2018-10-12 09:35:05	192.168.100.123	192.168.100.123	本地自动识别	2,953	下线	无流量下线
2018-10-12 09:25:04	2018-10-12 09:30:04	192.168.100.123	192.168.100.123	本地自动识别	2,972	下线	无流量下线
2018-10-12 09:20:03	2018-10-12 09:25:03	192.168.100.123	192.168.100.123	本地自动识别	2,933	下线	无流量下线
2018-10-12 09:15:01	2018-10-12 09:20:02	192.168.100.123	192.168.100.123	本地自动识别	2,972	下线	无流量下线
2018-10-12 09:11:58	2018-10-12 09:15:01	192.168.100.123	192.168.100.123	本地自动识别	1,801	下线	无流量下线
2018-10-12 09:10:01	2018-10-12 09:11:55	192.168.100.123	192.168.100.123	本地自动识别	1,193	下线	不符合mac唯一性
2018-10-12 09:05:00	2018-10-12 09:10:00	192.168.100.123	192.168.100.123	本地自动识别	2,963	下线	无流量下线

图 19 由于 MAC 变化的用户下线

在具体 HA 实践中，建议通过以下两种方法之一规避这一问题：

- 关闭“同一 IP，机器变化后认证下线”选项

进入【用户管理】→【认证管理】→【认证高级配置】页面，关闭“同一 IP，机器变化后认证下线”选项，如图 20 所示：

DHCP环境增强配置

IP变动后,不重新认证: ☒

同一IP,机器变化后认证下线: ☐

图 20 认证高级配置

这样，即便上线用户的 MAC 地址发生变化，也不会导致用户下线。保证了策略连续性。

- 启用三层 MAC 识别

通过配置三层交换机，识别到用户真实的 MAC 地址也可以有效解决这一问题。值

得注意的是，配置三层交换机时，应将各链路所有的交换机同时添加到主控、节点 ICG 设备。

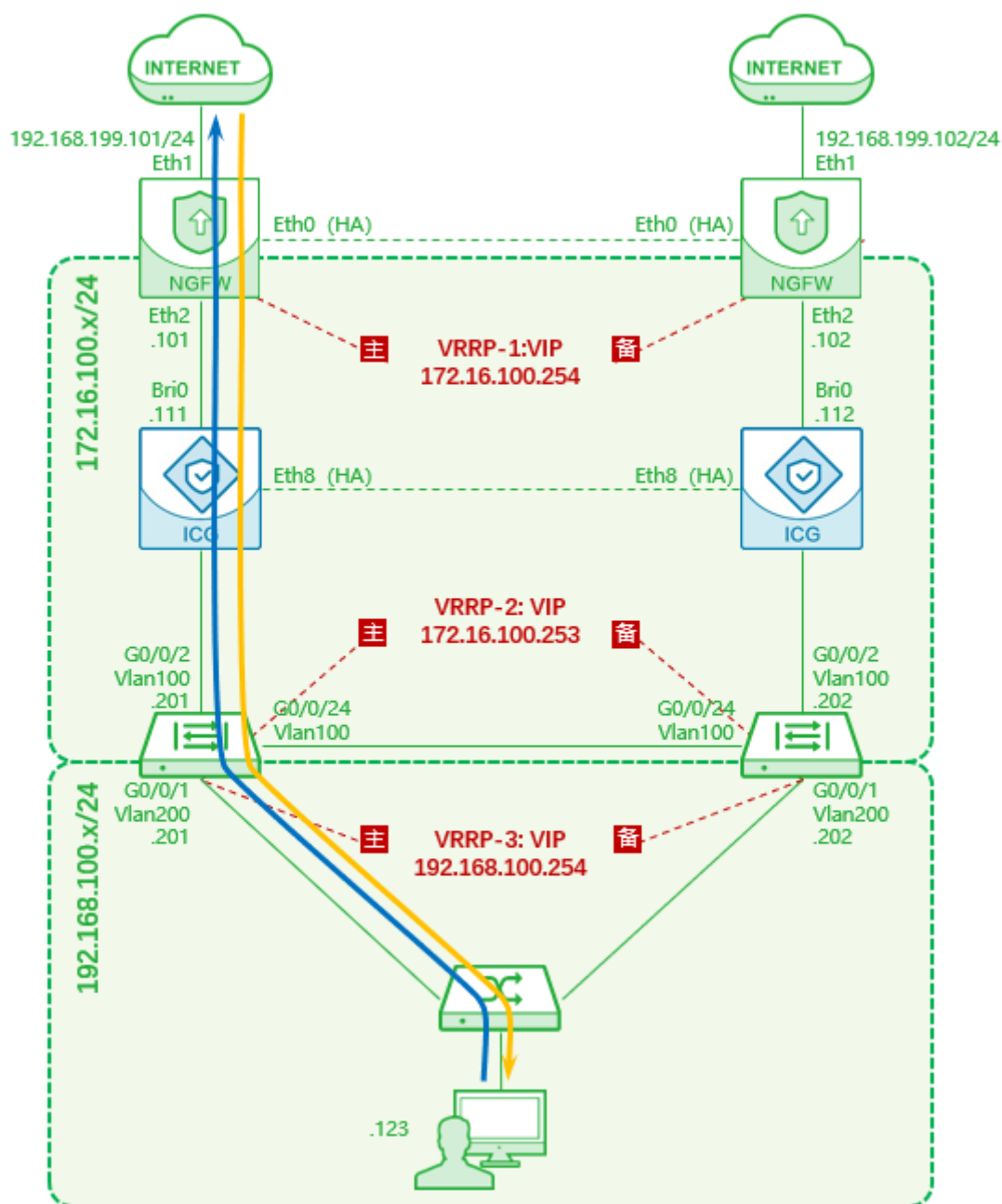
3.3 非对称路由问题

ICG9.0HA 通过主控、节点设备策略、用户的双向同步，保障了网络故障情况下的网络连续性和策略连续性。这些连续性保证的前提，都是用户的上下行流量路径一致。如果用户网络中存在“非对称路由”，导致同一个用户的上、下行流量分配到不同的 ICG 设备，也是无法正常审计的。

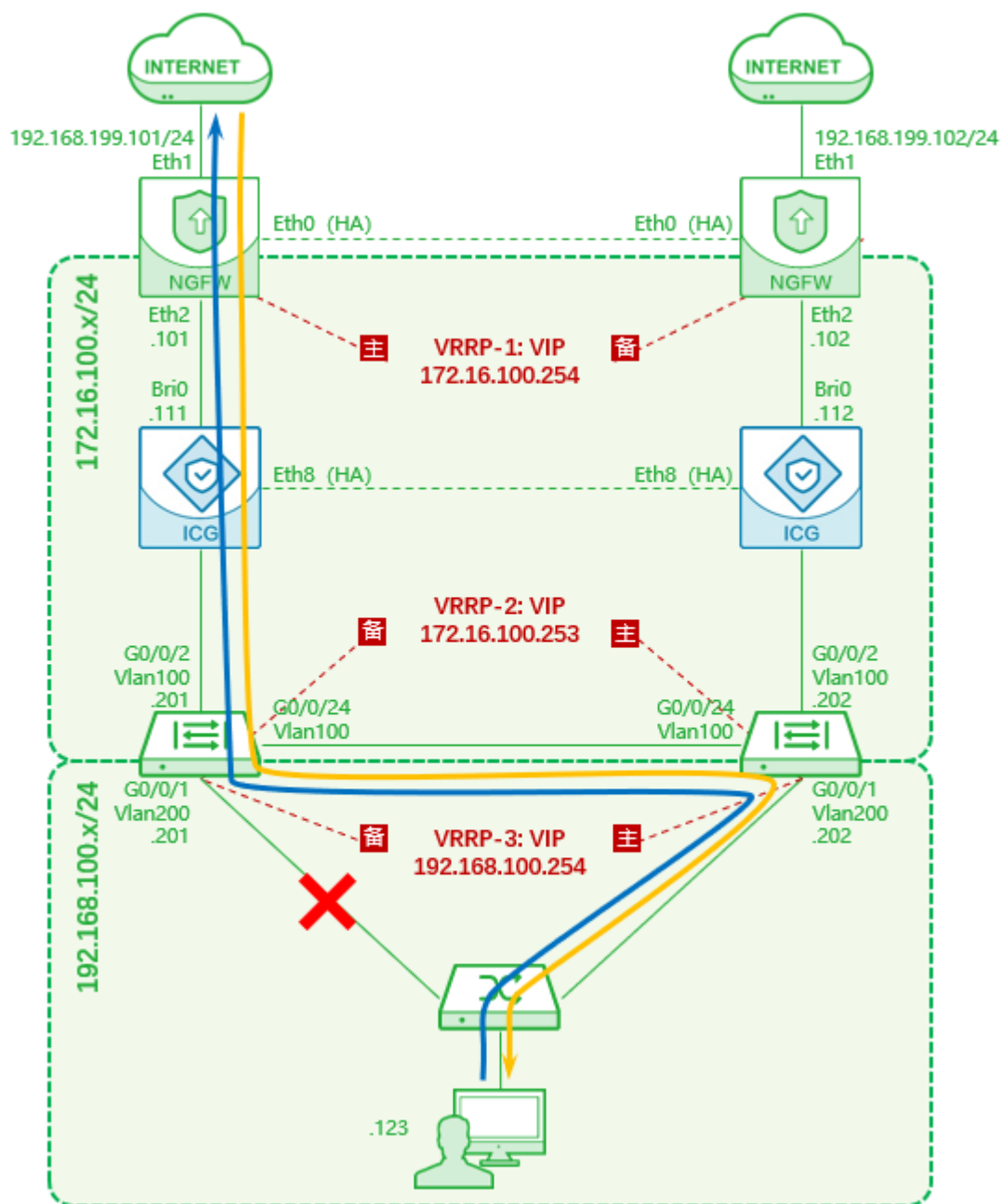
4 附录

4.1 “口字型” 主备模式网络场景流量路径分析

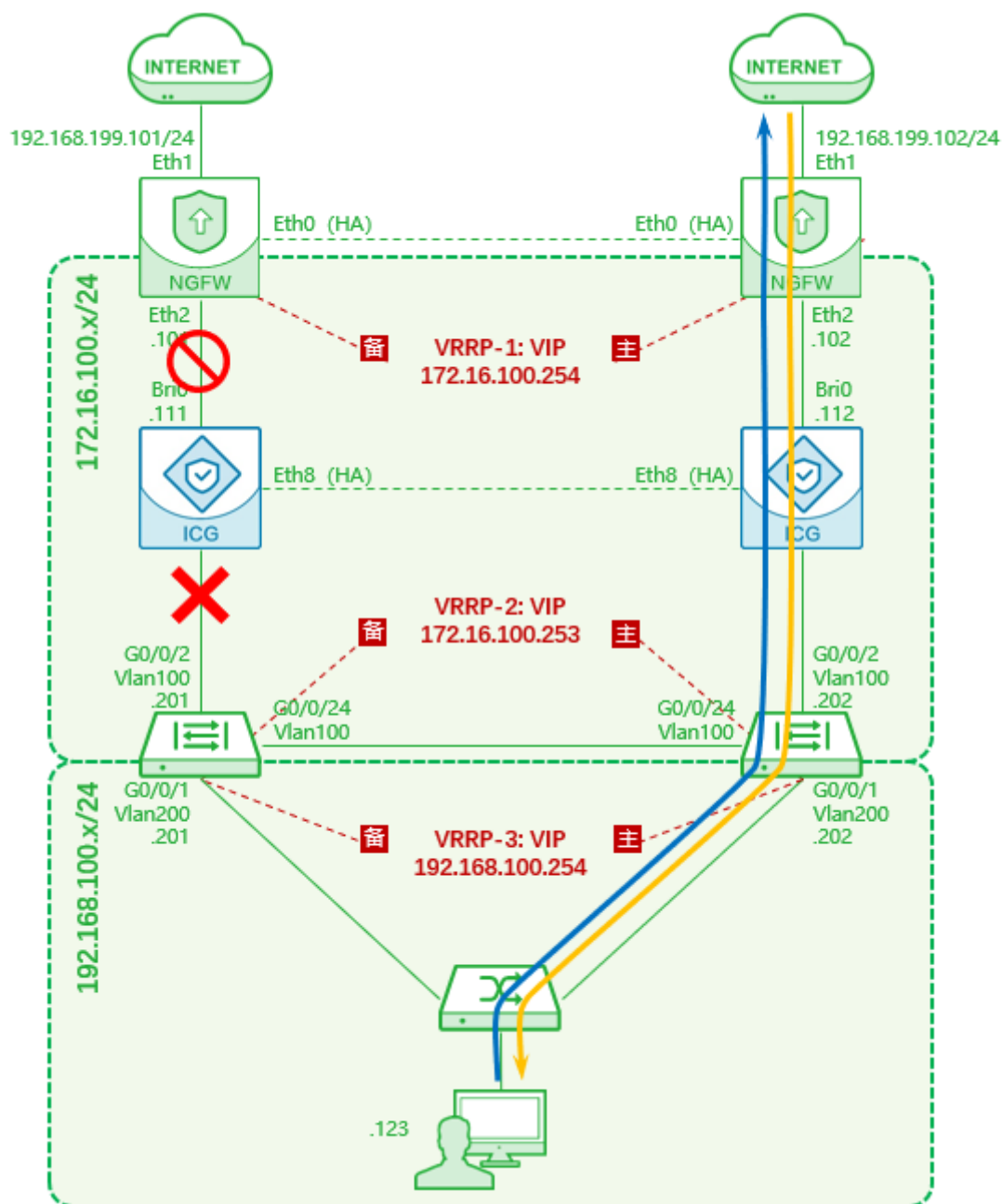
4.1.1 正常路径



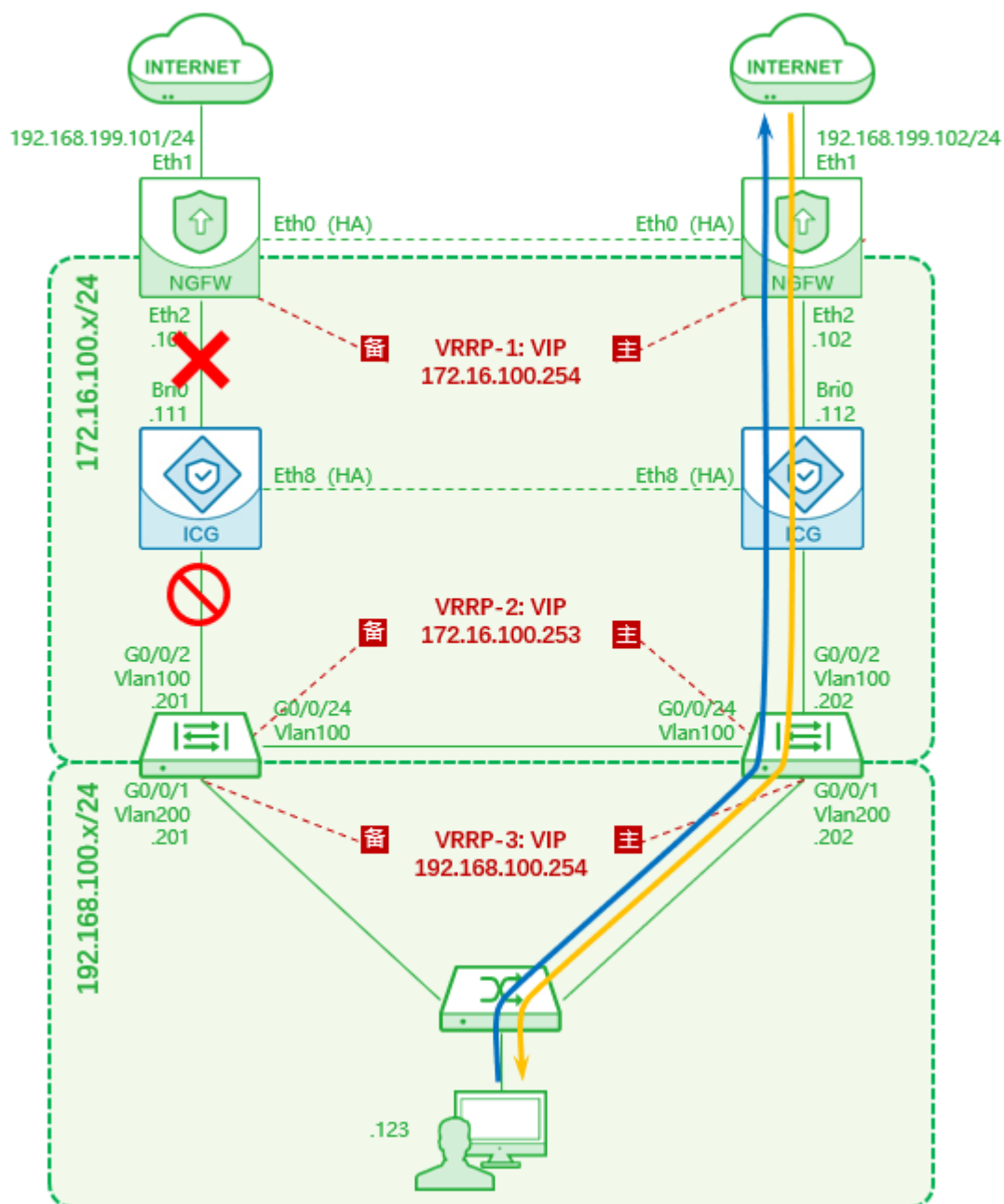
4.1.2 主交换机下行链路故障



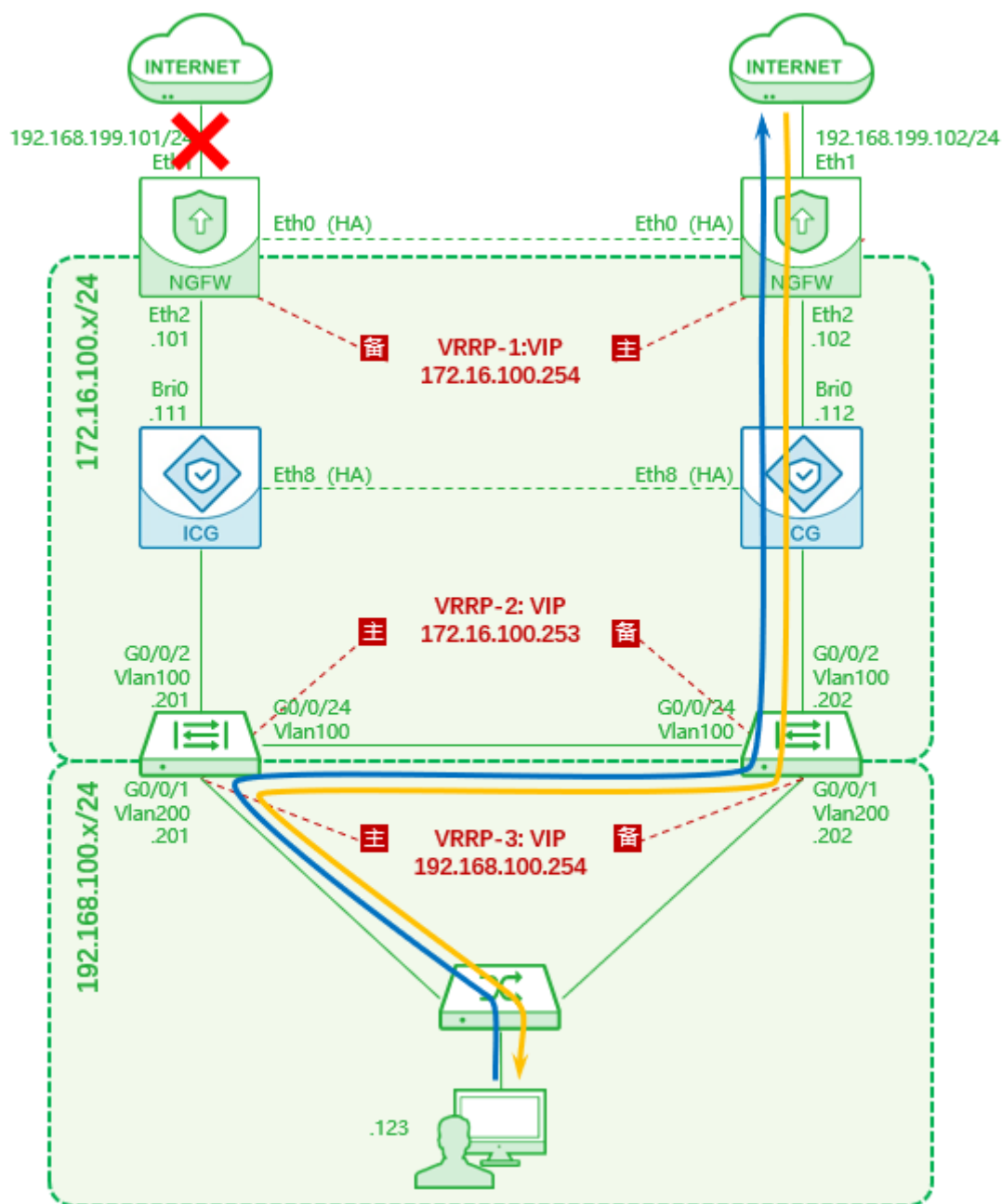
4.1.3 主交换机上行链路故障



4.1.4 主防火墙下行链路故障



4.1.5 主防火墙上行链路故障



4.2 参考测试用例

测试编号：01	
测试项目	高可用性
测试目的	验证 ICG 设备部署于冗余网络中时，在网络故障情况下对于网络连续性 & 策略连续性的保障能力。处于 HA 状态的两台 ICG 设备应该保持策略及上线用户状态的一致。
测试拓扑	
测试方法	<ol style="list-style-type: none"> 按照“测试拓扑”搭建网络环境，并启用 ICG 的高可用性（HA）功能 主控 ICG 启用 Web 认证，并建立两个本地用户，用户名分别为 test1、test2，密码均为 test@123；点击“立即生效” 登录节点 ICG，检查策略及用户配置 用户-1 访问网络，使用 test1 / test@123 登录，并访问网页 观察主控 ICG、节点 ICG 设备的上线用户列表，审计日志 断开主交换机与主控 ICG 设备之间的网线 用户-1 继续访问网络 用户-2 访问网络，使用 test1 / test@123 登录，并访问网页 观察主控 ICG、节点 ICG 设备的上线用户列表，审计日志 恢复主交换机与主控 ICG 设备之间的网线 用户-1、用户-2 继续访问网络 观察主控 ICG、节点 ICG 设备的上线用户列表，审计日志
预期结果	<ol style="list-style-type: none"> 节点 ICG 设备可以登录，可以看到从主控 ICG 设备同步来的审计控制策略及本地用户 弹出认证页面，可以正常登录，并打开网页 主控、节点 ICG 设备的上线用户列表同时存在用户-1（test1）的记录，并显示为在线状态；主控 ICG 可见用户-1 的审计日志，节点 ICG 无审计日志 可以正常访问网络，无需再次认证 弹出认证页面，可以正常登录，并打开网页 主控、节点 ICG 设备的上线用户列表同时存在用户-1（test1）、用户-2（test2）的记录，并显示为在线状态；节点 ICG 可见用户-1 在步骤 7 中产生的审计

	日志，及用户-2 在步骤 8 中产生的审计日志 11. 两用户均可以正常访问网络，无需再次认证 12. 主控、节点 ICG 设备的上线用户列表同时存在用户-1(test1)、用户-2(test2)的记录，并显示为在线状态；主控 ICG 可见用户-1、用户-2 在步骤 11 中产生的审计日志
测试结果	<input checked="" type="checkbox"/> 通过 <input type="checkbox"/> 未通过 <input type="checkbox"/> 未测试
结果确认	参测方： 测评方： 日期：