

中华人民共和国通信行业标准

YD/T 3235—2017

具有双栈内容交换功能的 以太网交换机测试方法

Test method for content switch supporting IPv4/IPv6

2017-04-12 发布

2017-07-01 实施

中华人民共和国工业和信息化部 发布

目 次

前言.....	III
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.....	2
4 设备常规测试.....	3
4.1 设备外观及附件检验.....	3
4.2 电气安全检验.....	3
4.3 供电测试.....	4
4.4 环境测试.....	4
5 接口测试.....	4
5.1 10/100M 以太网接口测试（可选）.....	4
5.2 千兆以太网接口测试.....	4
5.3 万兆以太网接口测试.....	4
5.4 40G 以太网接口测试（可选）.....	4
5.5 100G 以太网接口测试（可选）.....	4
6 二层功能测试.....	5
6.1 VLAN 测试.....	5
6.2 生成树功能测试.....	5
6.3 链路捆绑功能测试.....	5
7 IP 和路由协议测试.....	5
7.1 IPv4 协议测试.....	5
7.2 IPv6 协议测试.....	5
7.3 TCP 和 UDP 协议测试.....	5
7.4 RIPv1/v2 和 OSPFv2 协议测试（可选）.....	5
7.5 RIPng 和 OSPFv3 协议测试（可选）.....	5
8 双栈内容交换功能测试.....	6
8.1 健康检查测试.....	6
8.2 负载均衡测试.....	9
8.3 会话保持测试.....	13
8.4 扩展功能测试（可选）.....	16
9 网络安全功能测试.....	24

10	性能测试	26
10.1	四层性能测试	26
10.2	七层性能测试	29
10.3	长时间稳定性测试	34
11	网络管理功能测试	36
11.1	网管功能测试	36
11.2	SNMPv1/v2 协议测试	38
11.3	SNMPv3 协议测试	38
11.4	通用 Trap 测试	38
11.5	SSH 安全登录测试	38
11.6	计费管理测试	39
12	操作维护测试	39
12.1	日志测试	39
12.2	统计查询和报表功能测试	39
12.3	人机界面测试	39
12.4	操作员维护管理测试	39
12.5	终端管理测试	39
12.6	安全管理测试	40
13	可靠性测试	40
13.1	设备启动时间测试	40
13.2	双机热备功能测试	40
13.3	双机热备中的会话同步功能测试	41
13.4	热插拔可靠性测试（可选）	41
13.5	双机情况下在线升级测试	41

前 言

本标准是具有内容交换的以太网交换设备系列标准之一。该系列标准的结构和名称如下：

——YD/T 1691《具有内容交换功能的以太网交换机设备技术要求》；

——YD/T 1941《具有内容交换功能的以太网交换机设备测试方法》；

——《具有双栈内容交换功能的以太网交换机设备技术要求》；

——《具有双栈内容交换功能的以太网交换机设备测试方法》。

本标准按照 GB/T 1.1—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：中国信息通信研究院、中国移动通信集团有限公司、江苏省邮电规划设计院有限责任公司。

本标准主要起草人：张宇华、杨天乐、马琼芳、顾 戎、房 磊、季智红、王 健、马 可、刘 佳。

具有双栈内容交换功能的以太网交换机测试方法

1 范围

本标准规定了具有内容交换功能的以太网交换机支持 IPv4 和 IPv6 双协议栈的测试方法，包括设备常规测试、接口测试、二层功能测试、IP 和路由协议测试、双栈内容交换功能测试、网络安全功能测试、性能测试、网络管理功能测试、操作维护测试以及可靠性测试等。

本标准适用于具有双栈内容交换功能的以太网交换机或者集成了双栈内容交换功能的网络设备。

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。

YD/T 965—1998 电信终端设备的安全要求和试验方法

YD/T 1287—2013 具有路由功能的以太网交换机测试方法

YD/T 1455—2014 IPv6 网络设备测试方法 核心路由器

YD/T 1941—2009 具有内容交换功能的以太网交换机设备测试方法

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

内容交换 content switch

从传输层到应用层的交换，能够根据传输层到应用层的内容，或者特定信息进行转发、负载均衡和会话保持。

3.1.2

健康检查 health check

对服务器的硬件、软件、网络和服务的探测，以避免某一台或者某些服务器发生故障，造成某些用户连接中断。

3.1.3

负载均衡 load balance

使大量的业务访问在不同服务期间进行分配，保证低性能的服务器不会成为系统的瓶颈，同时使高性能服务器的能力得到充分利用。包括本地服务器群负载均衡和广域网使用的全局负载均衡。

3.1.4

会话保持 session persistence

在一段时间内将同一客户的某一类型请求绑定至同一台服务器上，使得这一时间段中该客户端所有该类型请求均由同一服务器进行处理。

3.1.5

虚拟 IP 地址 virtual IP address

由 IP 地址和 TCP/UDP 应用的端口组成，代表一个地址，为用户的一个或多个目标服务器提供服务，具备提供服务端口转换功能，能够隐藏服务器的真实服务 IP 和端口号。

用户通过虚拟 IP 地址访问网络服务时，请求报文到达 DUT，DUT 根据负载均衡算法从一组真实服务器中选出一台服务器，将报文的目标地址改写成选定服务器的地址，报文的目标端口改写成选定服务器的相应端口，最后将修改后的报文发送给选出的服务器。

3.1.6

具有内容交换功能的以太网交换机 content switch device

具有四至七层交换能力的以太网交换机，能够根据数据流中的传输层至应用层的信息实现对数据流量的交换与分配，在运营商网络中一般位于用户接入点或缓存节点，以及 IDC 的出口处，用以完成负载均衡、会话保持，以及缓存重定向等功能，以合理分配网络带宽及服务器资源。

3.1.7

具有双栈内容交换功能的以太网交换机 content switch supporting IPv4 and IPv6

同时具备 IPv4 和 IPv6 协议处理能力的具有内容交换功能的以太网交换机。

3.2 缩略语

下列缩略语适用于本文件。

AAA	认证、鉴权、计费	Authentication Authorization Accounting
ACL	访问控制列表	Access Control List
BGP	边界网关协议	Border Gateway Protocol
CDN	内容分发网络	Content Distribution Network
DNS	域名服务	Domain Name Service
DUT	被测设备	Device Under Test
FTP	文件传输协议	File Transfer Protocol
GSLB	全局服务器负载均衡	Global Server Load Balance

HTTP	超文本传输协议	Hypertext Transfer Protocol
ICMP	网络控制消息协议	Internet Control Message Protocol
IDC	互联网数据中心	Internet Data Center
LAN	局域网	Local Area Network
LDAP	轻量级目录访问协议	Lightweight Directory Access Protocol
MIB	管理信息库	Management Information Base
NAT	网络地址翻译	Network Address Translation
OSPF	开放最短路径优先协议	Open Shortest Path First
POP	邮局协议	Post Office Protocol
RADIUS	远端用户拨号认证	Remote Authentication Dial In User Service
RIP	路由信息协议	Route Information Protocol
RSTP	快速生成树协议	Rapid Spanning Tree Protocol
RTP	实时传输协议	Real-time Transport Protocol
RTCP	实时传输控制协议	Real-time Transport Control Protocol
SIP	会话发起协议	Session Initiation Protocol
SLB	服务器负载均衡	Server Load Balancing
SMTP	简单邮件传输协议	Simple Mail Transfer Protocol
SNMP	简单网管协议	Simple Network Management Protocol
SSH	安全外壳	Secure Shell
SSL	安全套接字	Secure Socket Layer
STP	生成树协议	Spanning Tree Protocol
TCP	传输控制协议	Transmission Control Protocol
UDP	用户数据报协议	User Datagram Protocol
URL	统一资源定位符	Uniform Resource Locator
VIP	虚拟 IP 地址	Virtual IP Address
VLAN	虚拟局域网	Virtual Local Area Network
WAP	无线应用协议	Wireless Application Protocol

4 设备常规测试

4.1 设备外观及附件检验

设备外观及附件检验见 YD/T 96—1998。

4.2 电气安全检验

电气安全检验见 YD/T 1287—2013 中 8.1。

YD/T 3235—2017

4.3 供电测试

4.3.1 整机功耗

整机功耗检验见 YD/T 1941—2009 中 13.1。

4.3.2 供电变化

供电变化检验见 YD/T 1941—2009 中 13.2。

4.4 环境测试

环境测试见 YD/T 1941—2009 中第 14 章。

5 接口测试

5.1 10/100M 以太网接口测试（可选）

5.1.1 10/100Base-T 接口测试

10/100Base-T 接口测试见 YD/T 1287—2013 中 4.1.1。

5.2 千兆以太网接口测试

5.2.1 1000Base-T 接口测试

1000Base-T 接口测试见 YD/T 1287—2013 中 4.1.4。

5.2.2 1000Base-LX 接口测试

1000Base-LX 接口测试见 YD/T 1287—2013 中 4.1.2。

5.2.3 1000Base-SX 接口测试

1000Base-SX 接口测试见 YD/T 1287—2013 中 4.1.3。

5.3 万兆以太网接口测试

万兆以太网接口测试见 YD/T 1287—2013 中 4.1.5。

5.4 40G 以太网接口测试（可选）

40G 以太网接口测试见 YD/T 1287—2013 中 4.1.6。

5.5 100G 以太网接口测试（可选）

100G 以太网接口测试见 YD/T 1287—2013 中 4.1.7。

6 二层功能测试

6.1 VLAN 测试

6.1.1 VLAN 功能测试

VLAN 功能测试见 YD/T 1941—2009 中 7.3.1。

6.1.2 VLAN 协议测试

VLAN 协议测试见 YD/T 1941—2009 中 7.3.2。

6.2 生成树功能测试

生成树功能测试见 YD/T 1941—2009 中 7.4。

6.3 链路捆绑功能测试

链路捆绑功能测试见 YD/T 1941—2009 中 7.5。

7 IP 和路由协议测试

7.1 IPv4 协议测试

ARP 协议、IP 协议、ICMP 协议、IGMP 协议测试见 YD/T 1287—2013 中 7.1~7.4。

7.2 IPv6 协议测试

IPv6 协议、邻居发现协议、路径 MTU 发现协议、ICMPv6 协议、无状态地址自动配置协议、MLD 协议测试见 YD/T 1455—2014 6.2~6.7。

7.3 TCP 和 UDP 协议测试

TCP 协议、UDP 协议测试见 YD/T 1455—2014 中 6.9 和 6.8。

7.4 RIPv1/v2 和 OSPFv2 协议测试（可选）

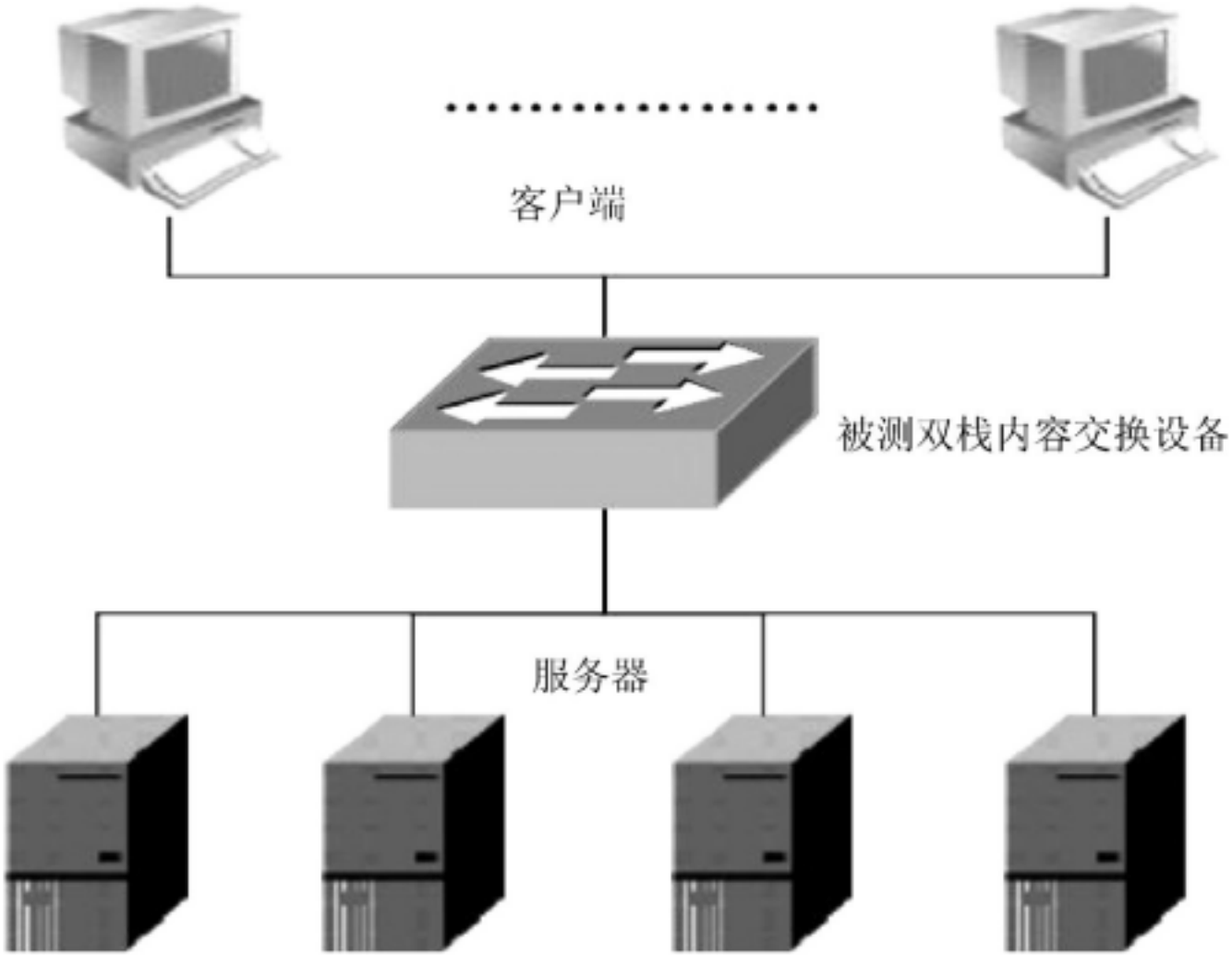
RIPv1/v2 协议、OSPFv2 协议测试见 YD/T 1287—2013 中 7.9~7.10。

7.5 RIPvng 和 OSPFv3 协议测试（可选）

RIPvng 协议、OSPFv3 协议测试见 YD/T 1455—2014 中 7.2 和 7.3。

8 双栈内容交换功能测试

8.1 健康检查测试

测试编号 1.
测试项目：ICMP 服务器健康检查
测试目的：测试 DUT 使用 ICMP 的健康检查方法对服务器的健康检查，能否发现服务器的停机和网络中断等故障
测试配置： <div></div>
测试步骤： <div>1) 配置 DUT 和后台服务器组工作正常，服务器提供 Web 服务并确认可以回应 IPv4 和 IPv6 的 ICMP 包； 2) 客户端有一定的业务请求（大于 1000TPS，TPS：每秒事务数）； 3) DUT 配置 IPv4 和 IPv6 的 ICMP 健康检查，调整频率为每 15 秒检查一次，如果连续 3 次以上服务器没有回应或没有回应相关内容就确认其停止服务； 4) 对 DUT 和服务器之间的接口进行抓包； 5) 拔掉其中某一台服务器的网线，观察 DUT 的健康检查界面； 6) 连接网线，观察 DUT 的健康检查界面</div>
判定原则： <div>1) 抓包显示，DUT 能够按照配置周期性发送 IPv4 和 IPv6 的 ICMP 检测报文； 2) DUT 支持 IPv4 和 IPv6 的 ICMP 服务器健康检查； 3) 步骤 5) 中，DUT 发现服务器故障，记录发现服务器故障的时间，并将所有新发起的请求切换到其它业务服务器，记录相关数据； 4) 步骤 6) 中，DUT 发现服务器恢复，开始给其分配服务，记录发现服务器恢复的时间； 5) 发现服务器故障时间应小于 15×3=45s，发现服务器故障恢复时间应小于 15s</div>

测试编号 2.
测试项目：基于服务的服务器健康检查
测试目的：测试 DUT 使用基于服务的健康检查方法对服务器的健康检查，能否发现服务器的服务已经停止、停机、网络中断等故障

测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，后台服务器组（大于 3）工作正常，提供 Web 服务并确认可以回应 IPv4 和 IPv6 的 ICMP 包； 2) 客户端有一定量的业务请求（大于 1000TPS）； 3) 服务器均提供 <code>http://<服务器 IPv4: 端口>/index.html</code> 的 Web 业务和 <code>http://<服务器 IPv6: 端口>/index.html</code> 的 Web 业务； 4) DUT 配置基于服务的健康检查，调整频率为每 15 秒检查一次，如果连续 3 次以上服务器没有回应或没有回应相关内容就确认其停止服务； 5) 对 DUT 和服务器之间的接口进行抓包； 6) 将服务器 A（其中一台）的 HTTP 服务停止，观察 DUT 的健康检查界面； 7) 恢复服务器 A 的 HTTP 服务，观察 DUT 的健康检查界面，记录发现服务器恢复的时间； 8) 将服务器 B（另一台）提供 HTTP 服务的路径变为 <code>http://<服务器 IPv4: 端口>/abc/index.html</code> 和 <code>http://<服务器 IPv6: 端口>/abc/index.html</code>； 9) 将服务器 B 提供 HTTP 服务的路径恢复为 <code>http://<服务器 IPv4: 端口>/index.html</code> 和 <code>http://<服务器 IPv6: 端口>/index.html</code>；
<p>判定原则：</p> <ol style="list-style-type: none"> 1) 抓包显示，DUT 能够按照配置，周期性发送 IPv4 和 IPv6 的 ICMP、get 请求检查服务器健康状态； 2) DUT 支持基于服务的健康检查； 3) 步骤 6) 中，DUT 发现服务器 A 故障； 4) 步骤 7) 中，DUT 发现服务器 A 恢复； 5) 步骤 8) 中，DUT 发现服务器 B 故障； 6) 步骤 9) 中，DUT 发现服务器 B 恢复； 7) 发现服务器故障时间应小于 $15 \times 3 = 45s$，发现服务器故障恢复时间应小于 15s

测试编号 3.
测试项目：基于内容的服务器健康检查（HTTP）
测试目的：测试 DUT 使用基于内容（HTTP）的健康检查方法对服务器的健康检查，能否发现服务器的服务已经停止、停机、网络中断等故障
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，后台服务器组（大于 3）工作正常，提供 Web 服务并确认可以回应 IPv4 和 IPv6 的 ICMP 包； 2) 客户端有一定量的业务请求（大于 1000TPS）； 3) 服务器均提供 <code>http://<服务器 IPv4: 端口>/index.html</code> 的 Web 业务和 <code>http://<服务器 IPv6: 端口>/index.html</code> 的 Web 业务，并且页面上有“fryuolbg”字符串； 4) DUT 配置基于内容的健康检查，检测网页中如果含有“fryuolbg”字符串，则认为该服务器“健康”，否则反之；调整频率为每 15 秒检查一次，如果连续 3 次以上服务器没有回应或没有回应相关内容就确认其停止服务； 5) 对 DUT 和服务器之间的接口进行抓包； 6) 将服务器 A（其中一台）的 HTTP 服务页面停止，观察 DUT 的健康检查界面； 7) 恢复服务器 A 的 HTTP 服务，观察 DUT 的健康检查界面，记录发现服务器恢复的时间； 8) 将服务器 B（另一台）提供 HTTP 服务的页面内容中的“fryuolbg”变为“fryu-olbg”； 9) 将服务器 B 提供 HTTP 服务的页面内容中的“fryu-olbg”变为“fryuolbg123”；

10) 恢复服务器 B 提供 HTTP 服务的页面内容为 “fryuolbg”
<p>判定原则:</p> <ol style="list-style-type: none"> 1) 抓包显示, DUT 能够按照配置, 周期性发送 IPv4 和 IPv6 的 ICMP、get 请求检查服务器健康状态; 2) DUT 支持基于内容的健康检查; 3) 步骤 6) 中, DUT 发现服务器 A 故障; 4) 步骤 7) 中, DUT 发现服务器 A 正常; 5) 步骤 8) 中, DUT 发现服务器 B 故障; 6) 步骤 9) 中, DUT 发现服务器 B 正常; 7) 步骤 10) 中, DUT 发现服务器 B 正常; 8) 发现服务器故障时间应小于 $15 \times 3 = 45\text{s}$, 发现服务器故障恢复时间应小于 15s
测试编号 4.
测试项目: 基于内容的服务器健康检查 (DNS)
测试目的: 测试 DUT 使用基于内容 (DNS) 的健康检查方法对服务器的健康检查, 能否发现服务器的服务已经停止、停机、网络中断等故障
测试配置: 同测试编号 1
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) DUT 工作正常, 后台服务器组 (大于 3) 工作正常, 提供 DNS 解析服务并确认可以回应 IPv4 和 IPv6 的 ICMP 包; 2) 客户端有一定量的业务请求 (大于 1000QPS, QPS=每秒查询数); 3) 后台 DNS 服务器上配置, 将 www.aaa.com 解析 A 记录为 “10.10.10.10”, AAAA 记录为 “2014: : 2015”; 4) DUT 配置基于内容的健康检查, 检测 www.aaa.com 的解析结果是否为 “10.10.10.10” 和 “2014: : 2015”, 如果是, 则认为该服务器 “健康”, 否则反之; 调整频率为每 15 秒检查一次, 如果连续 3 次以上服务器没有回应或没有回应相关内容就确认其停止服务; 5) 对 DUT 和服务器之间的接口进行抓包; 6) 将服务器 A (其中一台) 的 DNS 服务停止, 观察 DUT 的健康检查界面; 7) 恢复服务器 A 的 DNS 服务, 观察 DUT 的健康检查界面, 记录发现服务器恢复的时间; 8) 将服务器 B (另一台) 提供 DNS 服务中的 www.aaa.com 解析地址变为 “10.10.10.100” 和 “2014: : 2016”; 9) 将服务器 B 提供 DNS 服务中的 www.aaa.com 记录删除。 10) 恢复服务器 B 中 www.aaa.com 记录, 解析地址还原为 “10.10.10.10” 和 “2014: : 2015”。
<p>判定原则:</p> <ol style="list-style-type: none"> 1) 抓包显示, DUT 能够按照配置, 周期性发送 IPv4 和 IPv6 的 ICMP、DNS 请求检测报文; 2) DUT 支持基于内容的健康检查; 3) 步骤 6) 中, DUT 发现服务器 A 故障; 4) 步骤 7) 中, DUT 发现服务器 A 正常; 5) 步骤 8) 中, DUT 发现服务器 B 故障; 6) 步骤 9) 中, DUT 发现服务器 B 故障; 7) 步骤 10) 中, DUT 发现服务器 B 正常; 8) 发现服务器故障时间应小于 $15 \times 3 = 45\text{s}$, 发现服务器故障恢复时间应小于 15s

8.2 负载均衡测试

测试编号 5.
测试项目：轮询负载均衡算法测试
测试目的：测试 DUT 使用轮询法对服务器进行负载均衡的访问分发，在服务器端造成的压力是否确实是均衡的。
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，并配置负载均衡算法为轮询法；后台服务器组数量为 3，工作正常，提供 Web 服务并确认可以回应 ICMP 包。 2) 对 DUT 和服务器之间的接口进行抓包。 3) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 7 个 IPv4 地址作为源 IP 进行测试； b) 第 1 个源 IP 地址的访问速率为 300 页面/s； c) 其余 6 个源 IP 地址的访问速率为 30 页面/s。 4) 查看后台服务器业务的负载均衡情况。 5) 将步骤 3) 中仪表仿真的 7 个 IPv4 地址改为 IPv6 地址，重新测试步骤 3) ~ 步骤 4)，查看后台服务器业务的负载均衡结果
<p>判定原则：</p> <ol style="list-style-type: none"> 1) DUT 将业务按请求到达的顺序平均分给了后台的 3 台服务器，每台服务器的业务请求为 160 页面/s（约数）。 2) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器

测试编号 6.
测试项目：加权负载均衡算法测试
测试目的：测试 DUT 使用加权法对服务器进行负载均衡的访问分发，在服务器端造成的压力是否确实是加权均衡的
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 WEB 服务并确认可以回应 ICMP 包，并配置负载均衡算法为加权法，服务器 A、B、C 提供服务的业务量比例为 3:2:1。 2) 对 DUT 和服务器之间的接口进行抓包。 3) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 7 个 IPv4 地址作为源 IP 进行测试； b) 第 1 个源 IP 地址的访问速率为 300 页面/s； c) 其余 6 个源 IP 地址的访问速率为 30 页面/s。 4) 查看后台服务器业务的负载均衡情况； 5) 将步骤 3) 中仪表仿真的 7 个 IPv4 地址改为 IPv6 地址，重新测试步骤 3) ~ 步骤 4)，查看后台服务器业务的负载均衡结果
<p>判定原则：</p> <ol style="list-style-type: none"> 1) DUT 将业务按请求按照加权算法分给了后台的 3 台服务器，业务请求分别为 240、160、80 页面/s（约数）。 2) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器

测试编号 7.
测试项目：服务器 SNMP 负载均衡算法测试
测试目的：测试 DUT 可以通过 SNMP 从服务器上采集信息，通过对各项指标设定不同的权重进行计算以后，动态产生一个负载均衡的分配比例
测试配置：同测试编号 1
测试步骤： 1) 配置后台服务器可以正常提供服务，并确认可以回复 IPv4 和 IPv6 的 ICMP 包； 2) 在服务器安装 SNMP 代理，并在 DUT 上配置 SNMP 协议； 3) 在 DUT 上配置服务器 SNMP 负载均衡算法，并根据不同指标设定不同权重； 4) DUT 收集后台服务器上的系统性能信息，并根据这些信息作出动态比例的负载均衡； 5) 在客户端发送大量连接请求，DUT 可以根据动态产生的比例进行负载均衡的客户连接请求分发； 6) 检查后台服务器的在线用户数目，应该同动态的比例相一致
判定原则： 1) DUT 会将所有访问负载均衡到后台服务器，并且会根据服务器资源的动态变化的比例进行分发。

测试编号 8.
测试项目：最少连接负载均衡算法测试
测试目的：测试 DUT 可以根据各台服务器目前的实时流量，把后续访问负载均衡到一台并发连接数最小的服务器上去
测试配置：同测试编号 1
测试步骤： 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 Web 服务并确认可以回应 ICMP 包，并配置负载均衡算法为最少连接负载均衡算法，并配置服务器 A、B、C 响应请求的延迟时间分别为 0s、1s、2s。 2) 对 DUT 和服务器之间的接口进行抓包。 3) 使用仪表模拟客户端，以一定压力访问 VIP： a) 仪表仿真 7 个 IPv4 地址作为源 IP 进行测试； b) 第 1 个源 IP 地址的访问速率为 300 页面/s； c) 其余 6 个源 IP 地址的访问速率为 30 页面/s。 4) DUT 将这些客户连接请求发送到当前并发连接数最小的服务器上。 5) 将步骤 3) 中仪表仿真的 7 个 IPv4 地址改为 IPv6 地址，重新测试步骤 3) ~ 步骤 4)，查看后台服务器业务的负载均衡结果
判定原则： 1) DUT 会将所有访问负载均衡到服务器，并且会根据服务器实时并发连接数的动态变化的比例进行分发，并发连接数小的服务器得到更多的新建连接，服务器 A>服务器 B>服务器 C； 2) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。

测试编号 9.
测试项目：Hash 负载均衡算法测试
测试目的：测试 DUT 可以根据业务请求客户端的源 IP 地址和源端口号，通过一定的 Hash 算法将业务请求分配给后台的服务器

测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 Web 服务并确认可以回应 ICMP 包，并配置负载均衡算法为 Hash 负载均衡算法； 2) 对 DUT 和服务器之间的接口进行抓包。 3) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 7 个 IPv4 地址作为源 IP 进行测试，访问速率均为 300 页面/s； b) 第 1 个源 IP 地址访问过程中所有连接的源端口号不变； c) 其余 6 个源 IP 地址访问的源端口号变化。 4) 查看后台服务器业务的负载均衡情况。 5) 将步骤 3) 中仪表仿真的 7 个 IPv4 地址改为 IPv6 地址，重新测试步骤 3) ~ 步骤 4)，查看后台服务器业务的负载均衡结果
<p>判定原则：</p> <ol style="list-style-type: none"> 1) DUT 将业务按预置算法分给了后台的 3 台服务器，业务请求服务数量并不一定均衡； 2) 抓包分析，第 1 个源 IPv4/IPv6 地址所有的请求均被分配到同一台服务器； 3) 抓包分析，其余的每一个源 IPv4/IPv6 地址发出的请求不能都分配到同一台服务器。

测试编号 10.
测试项目：基于源地址映射的负载均衡算法测试
测试目的：测试 DUT 可以根据业务请求客户端的不同源 IP 地址（范围），通过预置条件将业务请求分配给后台不同的服务器
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 Web 服务并确认可以回应 ICMP 包，并配置负载均衡算法为基于源地址映射负载均衡算法，将 192.168.1.0/24 和 2001::/64 的 IP 地址访问分配给服务器 A、192.168.2.0/24 和 2002::/64 的 IP 地址访问分配给服务器 B、192.168.3.0/24 和 2003::/64 的 IP 地址访问分配给服务器 C。 2) 对 DUT 和服务器之间的接口进行抓包。 3) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 3 个 IPv4/IPv6 地址作为源 IP 进行测试； b) 第 1 个源 IP 地址为 192.168.1.20 和 2001::9，访问速率为 100 页面/s； c) 第 2 个源 IP 地址为 192.168.2.41 和 2002::11f，访问速率为 200 页面/s； d) 第 3 个源 IP 地址为 192.168.3.187 和 2003::ff1a，访问速率为 300 页面/s。 4) 查看后台服务器业务的负载均衡情况。
<p>判定原则：</p> <ol style="list-style-type: none"> 1) DUT 将业务按预置算法分给了后台的 3 台服务器，业务请求服务数量分别为 100、200、300 页面/s。 2) 抓包分析，对应源 IPv4/IPv6 地址所有的请求均都分配给同一台服务器

测试编号 11.
测试项目：基于内容的负载均衡算法测试
测试目的：测试 DUT 可以根据业务请求所包含的不同内容，将业务请求分配给后台不同的服务器。

测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 4，工作正常，提供 WEB 服务并确认可以回应 ICMP 包，并配置负载均衡算法为基于请求内容的负载均衡算法，将请求 URL 中含有“FRYU1”的发送给服务器 A，将请求 URL 中含有“FRYU2”的发送给服务器 B，将请求 URL 中含有“FRYU12”的发送给服务器 C，将请求 URL 中含有“FRYU21”的发送给服务器 D； 2) 对 DUT 与服务器之间的接口进行抓包； 3) 使用仪表模拟客户端，以一定压力访问 VIP； 4) 仪表仿真 3 个 IPv4 地址作为源 IP 进行测试，每个源 IP 地址访问 http://VIP/OLBGFRYU1 速率均为 50 页面/s，访问 http://VIP/OLBGFRYU2 速率均为 100 页面/s，访问 http://VIP/OLBGFRYU1212 速率均为 200 页面/s，访问 http://VIP/OLBGFRYU2121 速率均为 400 页面/s； 5) 查看后台服务器业务的负载均衡情况； 6) 将步骤 4) 中仪表仿真的 3 个 IPv4 地址改为 IPv6 地址，重新测试步骤 4) ~ 步骤 5)，查看后台服务器业务的负载均衡结果
<p>判定原则：</p> <ol style="list-style-type: none"> 1) DUT 将业务按预置算法分给了后台的 3 台服务器； 2) 所有请求 http://VIP/OLBGFRYU1 的业务均分配给了服务器 A，访问速率为 150 页面/s； 3) 所有请求 http://VIP/OLBGFRYU2 的业务均分配给了服务器 B，访问速率为 300 页面/s； 4) 所有请求 http://VIP/OLBGFRYU1212 的业务均分配给了服务器 C，访问速率为 600 页面/s； 5) 所有请求 http://VIP/OLBGFRYU2121 的业务均分配给了服务器 D，访问速率为 1200 页面/s

测试编号 12.
测试项目：复合负载均衡算法测试
测试目的：测试 DUT 可以根据多种不同的负载均衡算法的组合，将业务请求分配给后台不同的服务器
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法；DUT 对外提供一个 VIP，后台服务器组数量为 8，分别为 A、B、C、D、E、F、G、H 工作正常，提供 WEB 服务并确认可以回应 ICMP 包。 2) 服务器 H 的请求响应时延为 3s，服务器 G 的请求响应时延为 2s，服务器 F 的请求响应时延为 1s，其它服务器响应时延均为 0s。 3) 配置负载均衡算法为复合负载均衡算法，如下： <ol style="list-style-type: none"> a) 将访问 URL 中含“FRYU1”的请求均分配给服务器 A 和 B，A 和 B 之间的负载均衡策略为轮询法； b) 将重要客户网段 192.168.1.0/24 和 2001::/64 的请求分配给服务器 C 和 D，C 和 D 之间的负载均衡策略为加权法，比例为 1:3； c) 其它访问都按照最小连接算法分配给服务器 E、F、G、H。 4) 对 DUT 与服务器之间的接口进行抓包。 5) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 50 个 IPv4 地址作为源 IP 进行测试； b) 前 10 个源 IP 地址分为 192.168.1.20-192.168.1.29，访问 http://VIP/OLBGFRYU-1 的速率为 400 页面/s，访问 http://VIP/OLBGFRYU1 的速率为 600 页面/s； c) 其它源 IP 地址的范围分为 192.168.10.2-192.168.10.41，访问速率为 800 页面/s。

6) 查看后台服务器业务的负载均衡情况。
7) 将步骤 5) 中仪表仿真的 IPv4 地址改为 IPv6 地址(2001::/64), 重新测试步骤 5) ~ 步骤 6), 查看后台服务器业务的负载均衡结果
判定原则:
1) DUT 将业务按预置算法分给了后台服务器。
2) 业务请求服务数量分别为:
a) 服务器 A 和 B: 300 页面/s;
b) 服务器 C: 100 页面/s;
c) 服务器 D: 300 页面/s;
d) 服务器 E、F、G、H 的总和为 800 页面/s, 服务器 E>服务器 F>服务器 G>服务器 H。
3) 抓包分析, 除了服务器 C 和 D 的请求外, 每一个源 IPv4 和 IPv6 地址发出的请求不能都分配给同一台服务器

8.3 会话保持测试

测试编号 13.
测试项目: 基于源地址的会话保持
测试目的: 测试 DUT 基于源地址的会话保持功能
测试配置: 同测试编号 1
测试步骤:
1) DUT 工作正常, 配置健康检查算法为 ICMP 算法, 负载均衡算法设为轮询法; DUT 对外提供一个 VIP, 后台服务器组数量为 3, 工作正常, 提供 Web 服务并确认可以回应 ICMP 包。
2) DUT 启动会话保持功能, 并设置为基于源地址的会话保持, 配置基于源地址会话保持的有效时间为 3min。
3) 对 DUT 与服务器之间的接口进行抓包。
4) 使用仪表模拟客户端, 访问 VIP:
a) 仪表仿真 100 个 IPv4 地址 (10.1.1.101-10.1.1.200) 作为源 IP 进行测试, 并且 IP 地址采用随机方式 (非顺序性的);
b) 每个源 IP 访问一次 VIP。
5) 查看后台服务器业务的负载均衡结果。
6) 在 3min 以内, 使用仪表模拟客户端, 以源 IP 为 10.1.1.151 对 VIP 进行访问, 访问速率为 300 页面/s。
7) 停止业务请求, 5min 后, 重复步骤 6)。
8) 将步骤 4) 中仪表仿真的 IPv4 地址改为 IPv6 地址, 重新测试步骤 4) ~ 步骤 7), 查看结果。
判定原则:
1) 步骤 4) 中, DUT 将业务按轮询法平均分给了后台的 3 台服务器, 并记录了每台连接对应的源 IP 地址;
2) 步骤 6) 中, 源 IP 为 10.1.1.151 的请求因为其源 IP 地址, 业务请求都分配给了某台服务器, 服务器 A、B、C 的压力并不均衡;
3) 步骤 7) 中, 因会话保持过期, 源 IP 为 10.1.1.151 的请求重新分配给某一台服务器, 其后该地址所有的业务请求又因为会话保持都分配给了该服务器;
4) 步骤 8) 中, IPv6 的测试结果情况基本与 IPv4 相同。

测试编号 14.
测试项目：基于 Cookie 的会话保持
测试目的：测试 DUT 基于 Cookie 的会话保持功能
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法，负载均衡算法设为轮询法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 WEB 服务并确认可以回应 ICMP 包。 2) DUT 启动会话保持功能，并设置为基于 Cookie 的会话保持，配置为 Insert Cookie 模式，即服务器不下发 Cookie，由 DUT 添加 Cookie。 3) DUT 为服务器 A 配置 Cookie-1，为服务器 B 配置 Cookie-2，为服务器 C 配置 Cookie-3（Cookie-1/2/3 表示不同的 Cookie 值，DUT 也可自动生成不同的 Cookie 值）。 4) 对 DUT 与服务器之间的接口进行抓包。 5) 使用仪表模拟客户端，以一定压力访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 100 个 IPv4 地址（10.1.1.101-10.1.1.200）作为源 IP 进行测试，并且 IP 地址采用随机方式（非顺序性的）； b) 访问速率为 900 页面/s，所有请求都不带 Cookie，服务器响应请求的回应带有不同的 Cookie。 6) 查看后台服务器业务的负载均衡情况，保持压力，并存储后台服务器 A 响应时所带的 Cookie-1。 7) 使用仪表模拟客户端，以源 IP 为 10.2.1.151 对 VIP 进行访问，并带上步骤 6) 中存好的 Cookie-1，访问速率为 300 页面/s。 8) 将步骤 5) 中仪表仿真的 IPv4 地址改为 IPv6 地址，重新测试步骤 5)～步骤 7)，查看结果 <p>判定原则：</p> <ol style="list-style-type: none"> 1) 步骤 6) 中，DUT 将业务按轮询法平均分给了后台的 3 台服务器，每台服务器的业务请求为 300 页面/s（约数），并且返回的响应分别含有 Cookie-1、Cookie-2、Cookie-3； 2) 抓包分析，每一个源 IP 地址发出的请求不能都分配给同一台服务器； 3) 步骤 7) 中，源 IP 为 10.2.1.151 的请求因为其带有 Cookie-1，因此业务请求都分配给了服务器 A，服务器 A、B、C 的压力分别为：600 页面/秒、300 页面/秒、300 页面/秒。 4) 步骤 8) 中，IPv6 的测试结果情况基本与 IPv4 相同

测试编号 15.
测试项目：基于 HTTP Header 信息（Calling-ID）的会话保持
测试目的：测试 DUT 基于 HTTP Header 信息（Calling-ID）的会话保持
测试配置：同测试编号 1
<p>测试步骤：</p> <ol style="list-style-type: none"> 1) DUT 工作正常，配置健康检查算法为 ICMP 算法，负载均衡算法设为轮询法；DUT 对外提供一个 VIP，后台服务器组数量为 3，工作正常，提供 WEB 服务并确认可以回应 ICMP 包； 2) DUT 启动会话保持功能，并设置为基于 Calling-ID 进行会话保持； 3) Calling-ID 是用户的手机号，移动用户进行 WAP 浏览时，经过 WAP 网关的 HTTP Session 中 Header 字段带有 Calling-ID； 4) 对 DUT 与服务器之间的接口进行抓包； 5) 使用仪表模拟客户端，访问 VIP： <ol style="list-style-type: none"> a) 仪表仿真 100 个 IPv4 地址（10.1.1.101-10.1.1.200）作为源 IP 进行测试，并且 IP 地址采用随机方式（非顺

<p>序性的)；</p> <p>b) 每个源 IP 的访问均在 HTTP Header 中加入不同的 Calling-ID，代表每个手机号，每个源 IP 访问一次 VIP；</p> <p>c) 仪表配置多个（大于 3）Profile 均使用相同的 IP 地址（10.1.1.222），每个 Profile 的 HTTP Header 中加入不同的 Calling-ID，代表每个手机号，多次访问 VIP。</p> <p>6) 查看后台服务器业务的负载分配情况。</p> <p>7) 使用仪表模拟客户端，以源 IP 为 10.1.1.151 对 VIP 进行访问，并带上步骤 5) 中的 Calling-ID，访问速率为 300 页面/秒。</p> <p>8) 将步骤 5) 中仪表仿真的 IPv4 地址改为 IPv6 地址，重新测试步骤 5) ~ 步骤 7)，查看结果。</p>
<p>判定原则：</p> <p>1) 步骤 5) 中，DUT 将业务按轮询法平均分给了后台的 3 台服务器，并记录了每条连接对应的 Calling-ID；</p> <p>2) 步骤 5) c) 中，同一个源 IP 地址的不同 Profile 发送请求，每个不同的 Calling-ID 第一次访问 VIP 时，都按轮询法分给了后台不同的服务器，接下来的请求就按照 Calling-ID 进行会话保持，不能以源 IP 地址为准进行会话保持；</p> <p>3) 步骤 7) 中，源 IP 为 10.1.1.151 的请求因为其带有特定的 Calling-ID，因此业务请求都分配给了某台服务器，服务器 A、B、C 的压力并不均衡；</p> <p>4) 步骤 8) 中，IPv6 的测试结果情况基本与 IPv4 相同。</p>

测试编号 16.
测试项目：基于 URL 的会话保持
测试目的：测试 DUT 基于 URL 的会话保持功能。
测试配置：同测试编号 1
<p>测试步骤：</p> <p>1) 配置服务器可以正常提供服务，并确认可以回复 ICMP 包；</p> <p>2) 配置 DUT 的负载均衡算法为轮询的负载均衡算法，不启用会话保持；</p> <p>3) 在客户端发送大量连接请求，DUT 能够正常的进行内容交换，将连接请求分发到各个服务器上；</p> <p>4) 启用会话保持，并配置 DUT 的会话保持方式为基于 URL 的会话保持；</p> <p>5) 在客户端发送大量连接请求，DUT 能够正常的进行内容交换，将连接请求分发到各个服务器上；</p> <p>6) 比较在未启用会话保持功能与启用会话保持功能情况下，访问请求的分发情况</p>
<p>判定原则：</p> <p>1) 在启用上述会话保持机制下，访问统一 URL 的关联交易请求应该被分发到同一服务器上</p>

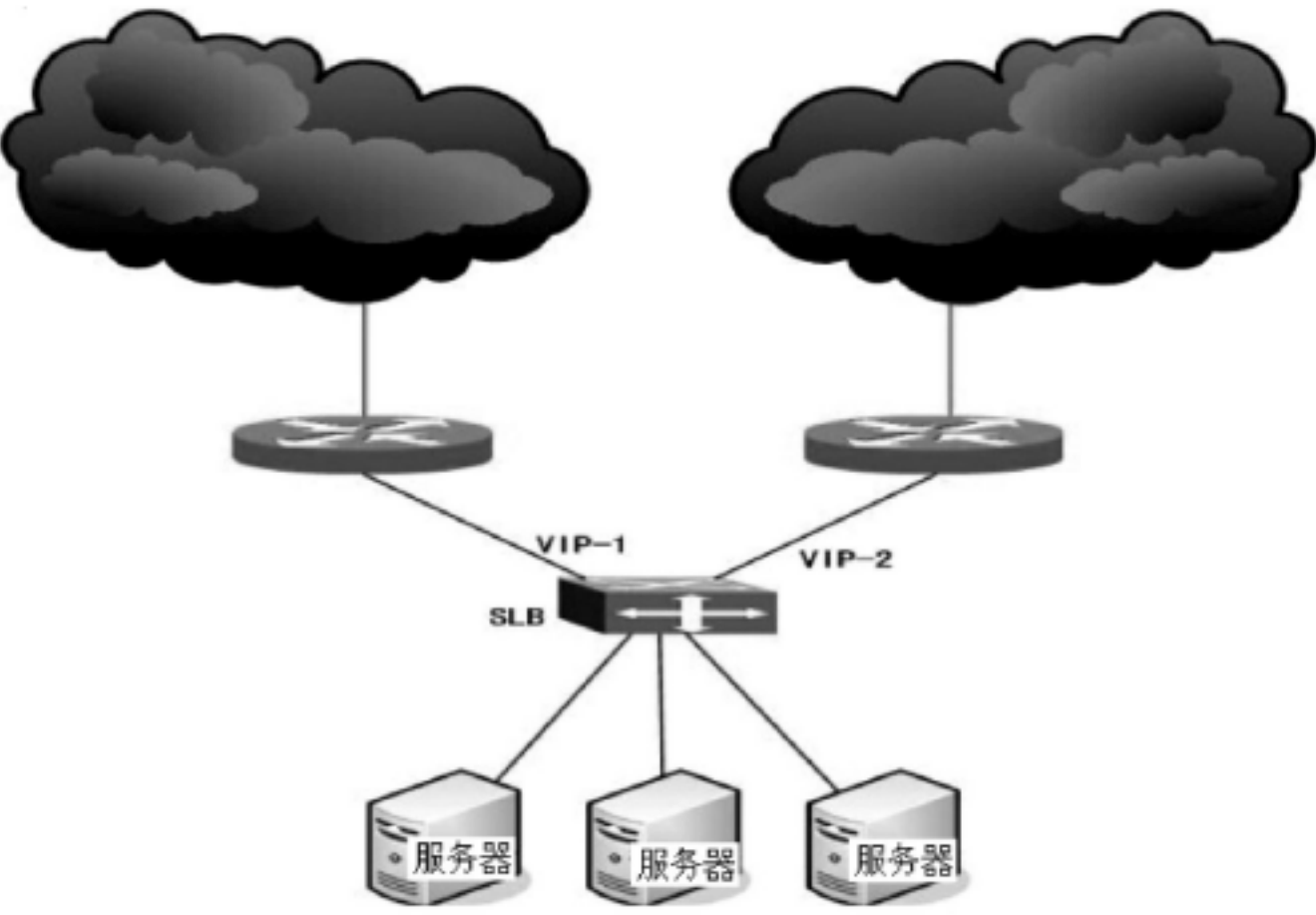
测试编号 17.
测试项目：根据 TCP_Content 或 UDP_Content 的会话保持
测试目的：测试 DUT 可以根据 TCP/UDP 中的特定信息进行分发控制和会话保持
测试配置：同测试编号 1
<p>测试步骤：</p> <p>1) 配置服务器可以正常提供服务，并确认可以回复 ICMP 包；</p> <p>2) 配置 DUT 的负载均衡算法为轮询的负载均衡算法，不启用会话保持；</p> <p>3) 在客户端发送大量连接请求，DUT 能够正常的进行内容交换，将连接请求分发到各个服务器上；</p> <p>4) 启用会话保持，并配置 DUT 的会话保持方式为基于 TCP_Content/UDP_Content 的会话保持；</p>

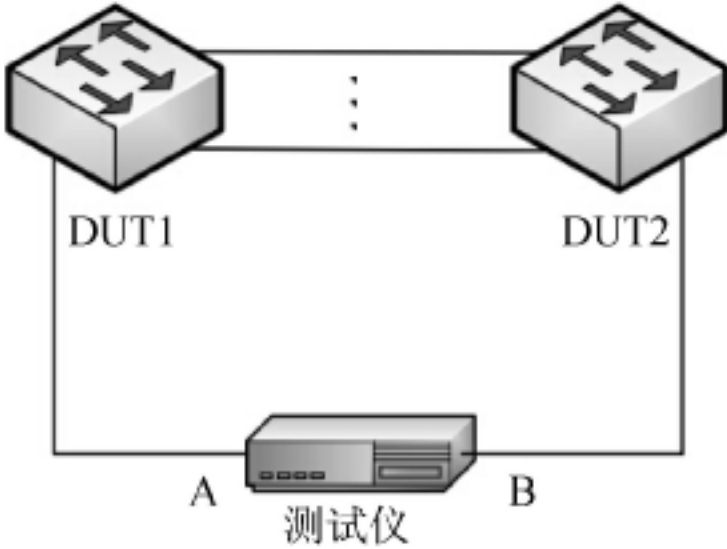
5) 在客户端发送大量连接请求, DUT 能够正常的进行内容交换, 将连接请求分发到各个服务器上;
6) 比较在未启用会话保持功能与启用会话保持功能情况下, 访问请求的分发情况
判定原则:
1) DUT 会将所有访问负载均衡到服务器, 具有相同 TCP/UDP 内容的访问请求被分发到同一服务器上

8.4 扩展功能测试 (可选)

测试编号 18.
测试项目: 多 VIP 测试
测试目的: DUT 支持多个 VIP 地址, 可同时提供多种不同的服务
测试配置: 同测试编号 1
<p>测试步骤:</p> <ol style="list-style-type: none"> 1) DUT 正常工作, 后台服务器组数量为 3, 工作正常, 均可提供 IPv4 和 IPv6 的 Web、FTP 等多种服务并确认可以回应 ICMP 包。 2) 对 DUT 与服务器之间的接口进行抓包。 3) DUT 配置 2 个 VIP (也可多个), 对外提供不同的服务业务。 4) 配置 VIP-1 如下: <ol style="list-style-type: none"> a) 提供 FTP 服务; b) Server Pool: Server-A、Server-B、Server-C; c) 健康检查: ICMP, 所有服务器均健康; d) 负载均衡算法: 轮询法; e) 会话保持: 无。 5) 配置 VIP-2 如下: <ol style="list-style-type: none"> a) 提供 HTTP 服务; b) Server Pool: Server-A、Server-B、Server-C; c) 健康检查: 基于 TCP 80 端口, 所有服务器均健康; d) 负载均衡算法: 最小连接算法; e) 会话保持: 基于 DUT Insert Cookie 方式。 6) 使用仪表模拟大量 IPv4 和 IPv6 客户端, 访问 VIP-1 和 VIP-2; 7) 在 DUT 上将 VIP-1 中的 Server-A 手工 down, Server-A 本身并没有故障, 查看 DUT 工作情况; 8) 对 VIP-1 增加过滤规则, 查看 DUT 工作情况
<p>判定原则:</p> <ol style="list-style-type: none"> 1) 抓包分析, 每一个源 IPv4 和 IPv6 地址发出的请求不能都分配给同一台服务器; 2) 步骤 6) 中, VIP-1 和 VIP-2 工作正常, 并应有两张 Session 表记录设备工作情况; 3) 步骤 7) 中, VIP-1 剩余的流量分给 Server-B 和 Server-C, VIP-2 的业务分配没有任何影响; 4) 步骤 8) 中, VIP-1 和 VIP-2 逻辑上相互独立, 过滤规则只对 VIP-1 有效

测试编号 19.
测试项目: 不同 VIP 不同路由测试
测试目的: 不同的 VIP 拥有不同的路由
测试配置:

	
测试步骤:	<p>1) DUT 正常工作, 后台服务器组数量为 3, 工作正常, 均可提供 IPv4 和 IPv6 的 Web 服务并确认可以回应 ICMP 包;</p> <p>2) 对 DUT 与服务器之间的接口进行抓包;</p> <p>3) DUT 配置 2 个 VIP, 为 VIP-1 和 VIP-2, 对外提供相同业务;</p> <p>4) 为 VIP-1 和 VIP-2 配置不同的默认路由;</p> <p>5) 使用仪表模拟大量 IPv4 和 IPv6 客户端, 访问 VIP-1 和 VIP-2, 且每一个源 IP 地址都访问 VIP-1 和 VIP-2;</p> <p>6) 查看 DUT 的路由信息和工作情况</p>
判定原则:	<p>1) 步骤 6) 中, VIP-1 和 VIP-2 工作正常, 并有不同的默认路由, 并且不同的默认路由应与相应的 VIP 绑定</p>

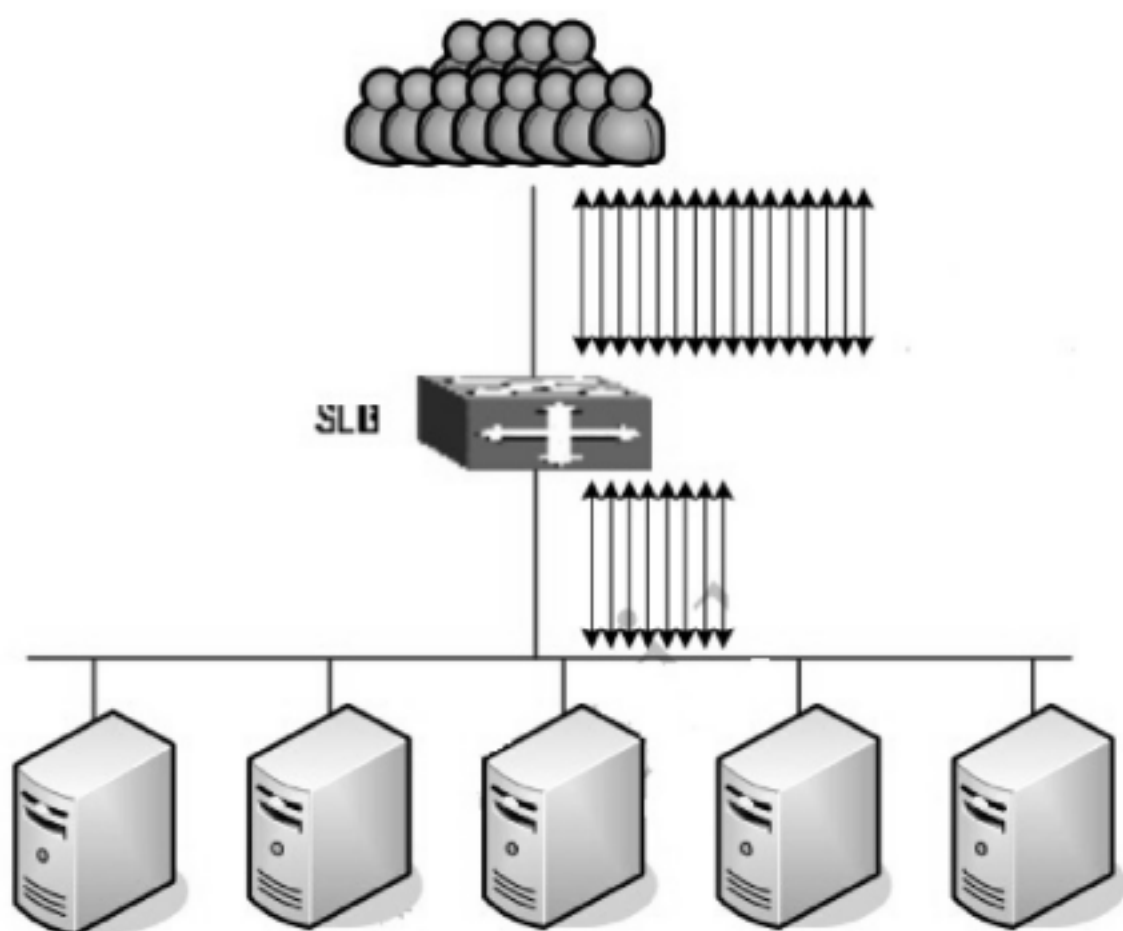
测试编号	20.
测试项目:	链路捆绑测试
测试目的:	验证 DUT 是否支持捆绑, 以及最大捆绑的端口数量
测试配置:	
测试步骤:	<p>1) 按图建立测试环境, 被测设备 (DUT1) 正常工作, 与交换机 (DUT2) 之间多根线连接;</p> <p>2) 根据实际情况可增加仪表与 DUT1、DUT2 之间的连线;</p> <p>3) 采用手工捆绑方式, 在 DUT1 和 DUT2 之间配置设备支持的最大数量的端口捆绑数目 (GE 必测, 10GE 可选测试);</p> <p>4) 由仪表 A 端口 (仿真客户端) 和 B 端口 (仿真后台服务器) 发送 HTTP 协议流量, 流量大小为按捆绑后的链路带宽 70% 以上, 观察各个端口流量情况;</p>

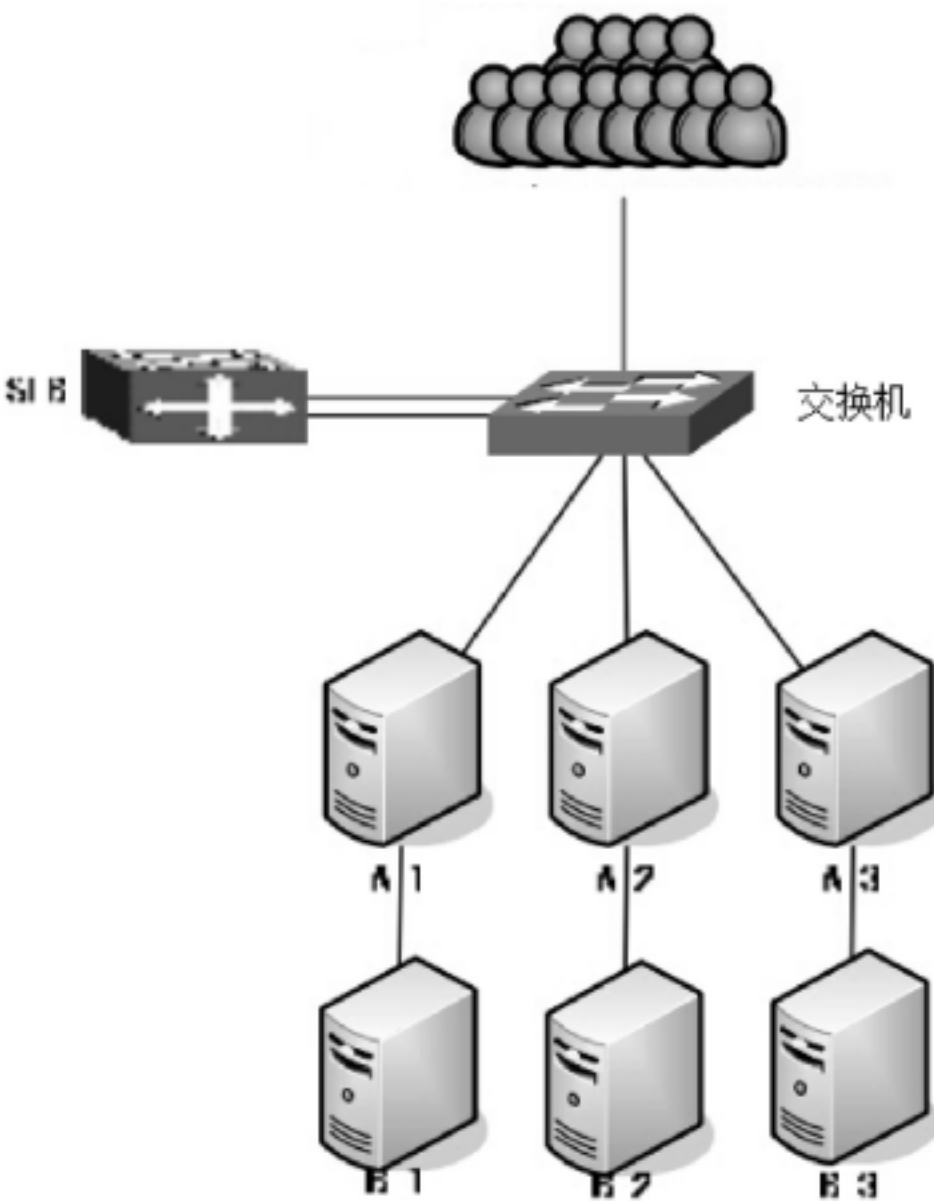
5) 将 DUT1 和 DUT2 之间的链路随机拔掉条, 观察各个端口流量情况
判定原则:
1) DUT 支持端口捆绑;
2) 步骤 4) 中, 捆绑的各个端口流量均匀分配 (按流 Hash);
3) 步骤 5) 中, 业务不受影响, 没有失败的业务请求, 故障链路的流量被其它链路分配承担

测试编号 21.
测试项目: 软关机测试
测试目的: 在维护和更新服务器时, DUT 可以通过手工将后台的某一台服务器“软关机”, 实现不再向该服务器发送任何新请求, 但保持原会话直至结束, 实现服务器的平滑关机。
测试配置: 同测试编号 1
测试步骤:
1) DUT 正常工作, 后台服务器组数量为 3, 工作正常, 均可提供 FTP 服务并确认可以回应 ICMP 包。
2) DUT 健康检查算法为 ICMP 算法, 负载均衡算法为轮询法, 对 DUT 与服务器之间的接口进行抓包。
3) 使用仪表模拟客户端, 以一定压力访问 VIP:
a) 仪表仿真 100 个 IPv4/IPv6 地址作为源 IP 进行测试;
b) 访问速率为 30 页面/秒。
4) 查看后台服务器业务的负载均衡情况。
5) 在 DUT 上将后台的服务器 A “软关机”。
6) 查看后台服务器业务的负载均衡情况
判定原则:
1) 步骤 4) 中, 业务按轮询法分配给后台的 3 台服务器, 负载基本均衡, 均为 10 页面/秒。
2) 步骤 5) 中, 服务器 A 不再有新的连接, 但现有连接继续提供服务, 服务器 A 在 DUT 上的状态为“软 Down”, 整个过程的成功率应为 100%;
3) 步骤 6) 中, 服务器 A 没有新的业务连接, 服务器 B 和 C 分别为 15 页面/秒, 并且当服务器 A 已有连接全部完成后, 服务器 A 在 DUT 上的状态为“Down”

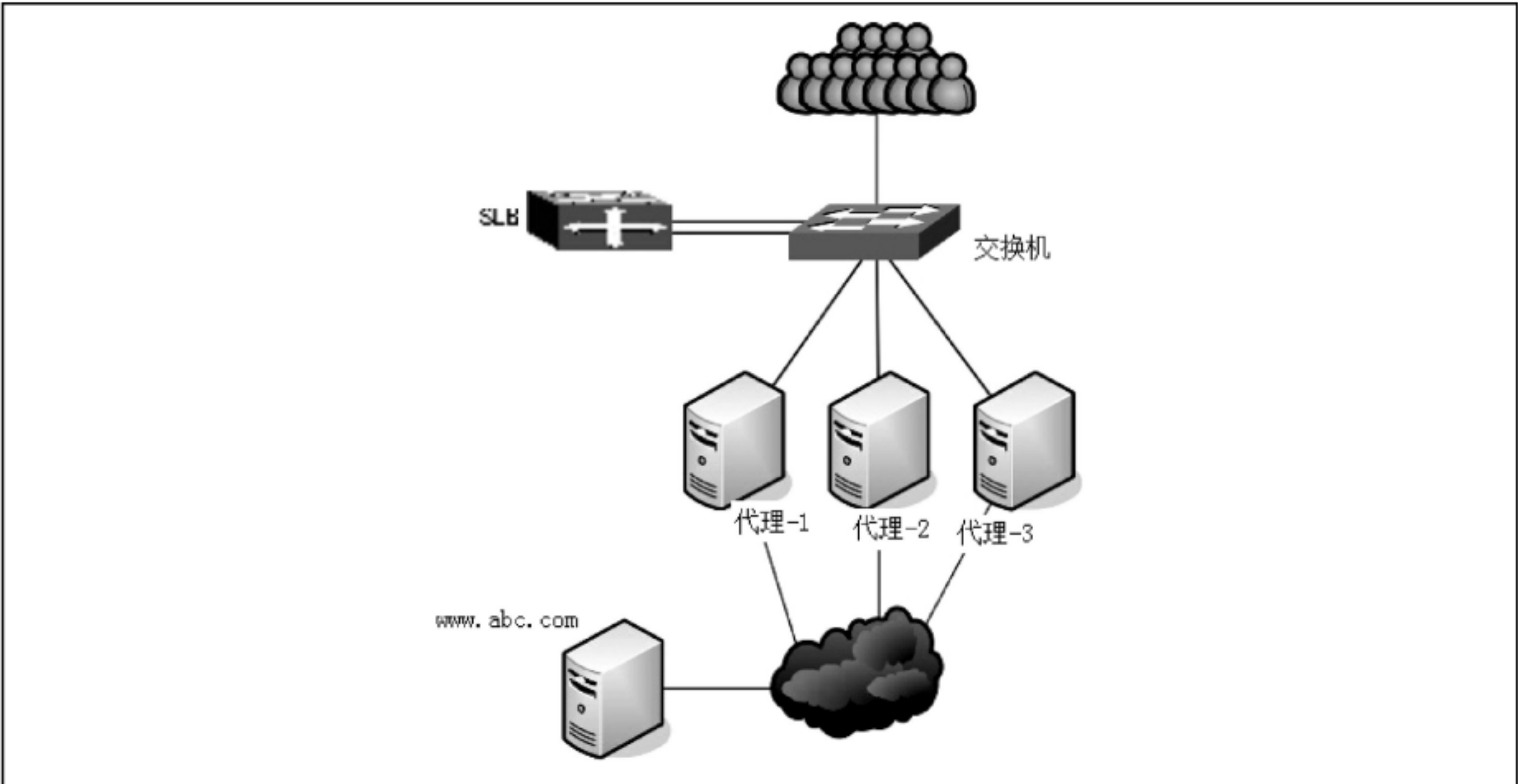
测试编号 22.
测试项目: 温暖上线测试
测试目的: 在维护和更新服务器后, DUT 可以通过手工将后台的某一台服务器“温暖上线”, 实现向该服务器发送新请求逐步增加, 使新服务器的压力缓慢增加到稳定状态, 防止服务器被冲死。
在此定义两个参数:
- 恢复时间: 保证在服务器上线后, DUT 对该设备健康检查通过后, 在一定时间内不向该服务器发客户请求;
- 温暖时间: 保证服务器在恢复时间到期后, 不是马上接收响应负载的全部请求, 而是在一定时间 (>3s) 内逐步增加请求, 直至达到最大值
测试配置: 同测试编号 1
测试步骤:
1) DUT 正常工作, 后台服务器组数量起始为 2, 工作正常, 均可提供 HTTP 服务并确认可以回应 ICMP 包;
2) DUT 健康检查算法为 ICMP 算法, 负载均衡算法为轮询法, DUT 配置恢复时间为 1s, 温暖时间为 3s, 对 DUT 与服务器之间的接口进行抓包。
3) 使用仪表模拟客户端, 以一定压力访问 VIP:

<p>a) 仪表仿真 100 个 IPv4/IPv6 地址作为源 IP 进行测试;</p> <p>b) 访问速率为 900 页面/s。</p> <p>4) 查看后台服务器业务的负载均衡情况。</p> <p>5) 在 DUT 上将第三台服务器 C “温暖上线”。</p> <p>6) 查看后台服务器业务的负载均衡情况。</p>
<p>判定原则:</p> <p>1) 步骤 4) 中, 业务按轮询法分配给后台的 2 台服务器, 负载基本均衡, 均为 450 页面/s。</p> <p>2) 步骤 5) 中, 服务器 C 状态由 “软 UP” 逐步变为 “UP”, 并且服务器 C 在 “软 UP” 后 1s 内没有业务请求, 第 2s~第 5s 服务器 C 压力主检增加到 300 页面/s, 整个过程的成功率应为 100%;</p> <p>3) 步骤 6) 中, 3 台服务器运行稳定, 每台 300 页面/秒。</p>

测试编号 23.
测试项目: 连接复用测试
测试目的: 测试 DUT 是否支持连接复用功能
<p>测试配置:</p> 
<p>测试步骤:</p> <p>1) DUT 工作正常, 后台服务器组数量为 5, 工作正常, 均可提供 HTTP 服务并确认可以回应 ICMP 包。</p> <p>2) DUT 健康检查算法为 ICMP 算法, 负载均衡算法为轮询法, DUT 启用连接复用功能, 对 DUT 与服务器之间的接口进行抓包。</p> <p>3) 使用仪表模拟客户端, 以一定压力访问 VIP:</p> <p>a) 仪表仿真 100 个 IPv4/IPv6 地址作为源 IP 进行测试;</p> <p>b) 访问速率为 10000Connection/s。</p> <p>4) 查看后台服务器业务的负载均衡情况。</p>
<p>判定原则:</p> <p>步骤 4) 中, 业务按轮询法分配给后台的 5 台服务器, 负载基本均衡, DUT 与客户之间的连接为 10000Connection/s, DUT 与服务器之间的连接数总和应远小于 10000Connection/s。</p>

测试编号 24.
测试项目：关联应用健康检查测试
测试目的：DUT 是否支持关联应用的健康检查
测试配置： <div></div>
测试步骤： <div>1) 逻辑拓扑如图，6 台服务器均连接到交换机上；DUT 工作正常，并将业务负载均衡给 A-1、A-2、A-3 三台服务器； 2) A-1、A-2、A-3、B-1、B-2、B-3 均可提供 IPv4 和 IPv6 的 Web 服务并确认可以回应 ICMP 包； 3) 服务器 A-1 是否能够正常提供服务，除了自身外，还依赖服务器 B-1 能够正常工作，A-2、A-3 同理； 4) 配置 DUT 开启关联应用健康检查功能，检查 TCP 80 端口； 5) 对 DUT 与服务端之间的接口进行抓包； 6) 服务器 A-1 和服务端 B-1 均正常，观察 DUT 上服务器 A 的状态； 7) 服务器 A-1 服务关闭，服务器 B-1 正常，观察 DUT 上服务器 A 的状态； 8) 服务器 A-1 服务正常，服务器 B-1 关闭，观察 DUT 上服务器 A 的状态</div>
判定原则： <div>1) 步骤 6) 中，健康检查通过，服务器状态正常； 2) 步骤 7) 中，健康检查不通过，服务器状态为不可用； 3) 步骤 8 中，健康检查不通过，服务器状态为不可用</div>

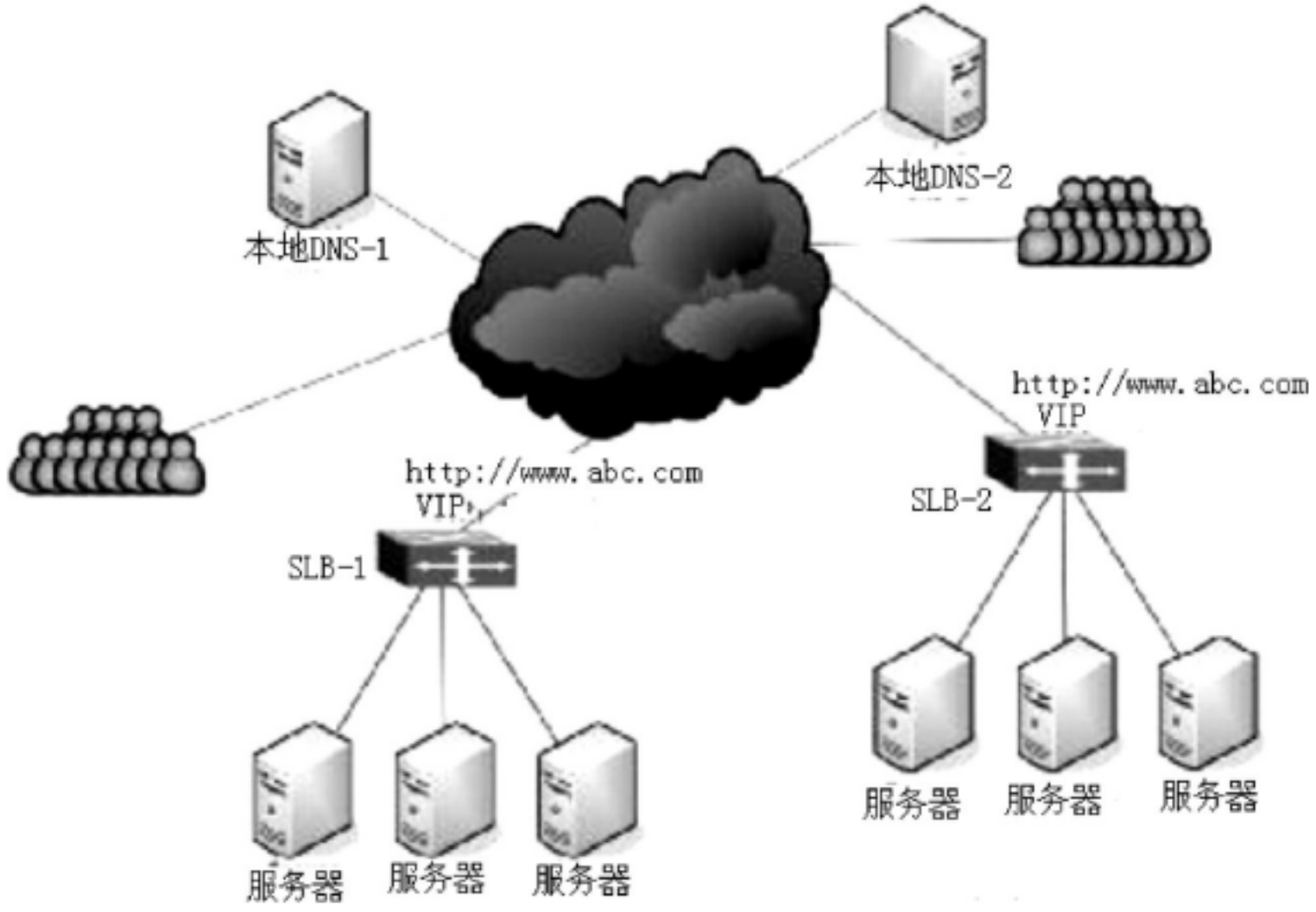
测试编号 25.
测试项目：代理服务器健康检查测试
测试目的：DUT 是否支持代理服务器多站点可用性检查
测试配置：



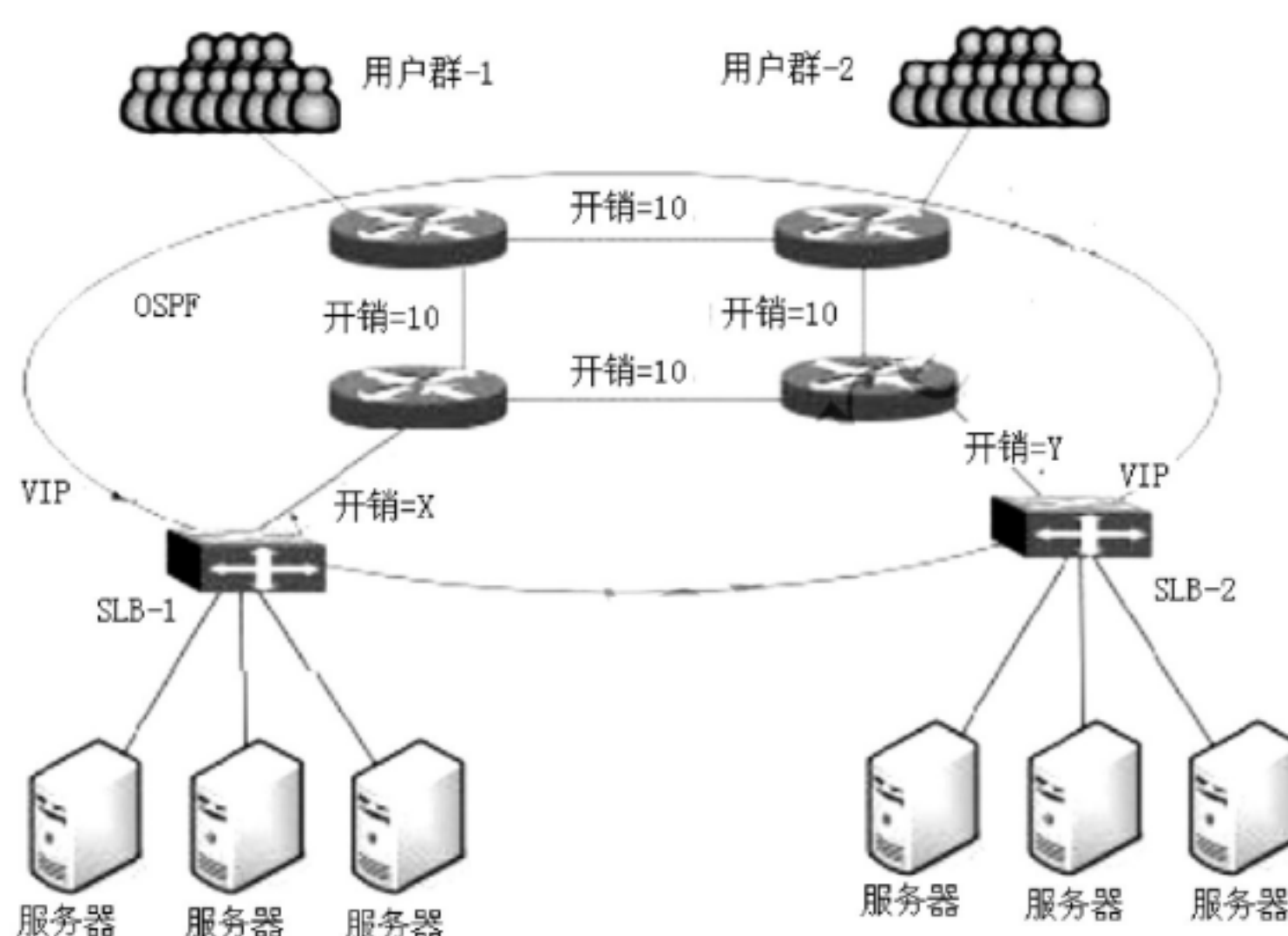
- 测试步骤：
- 1) 逻辑拓扑如图，3 台服务器均连接到交换机上；DUT 工作正常，并将业务负载均衡给 3 台服务器代理-1、代理-2、代理-3；
 - 2) 后台服务器均提供 HTTP 代理服务并确认可以回应 ICMP 包；
 - 3) 因为代理服务器的健康检查需要通过代理检测远端服务器的连通性，因此健康检查不但需要检查代理程序本身的连通性，还需要检查代理服务器与远端服务器的连通性；
 - 4) 配置 DUT，并开启“代理服务器健康检查”功能，即通过后台各个服务器的代理来访问 <http://www.abc.com>，来检查后台服务器的健康状态；
 - 5) 对 DUT 与服务器之间的接口进行抓包；
 - 6) 后面 3 台服务器正常，能通过其代理访问 <http://www.abc.com>，查看 DUT 上 3 台服务器的状态；
 - 7) 将 <http://www.abc.com> 的 Web 服务关闭，查看 DUT 上 3 台服务器的状态；
 - 8) 恢复后，将代理-1 对互联网的连接断掉，但 DUT 与代理-1 之间可达，即 DUT 能够访问代理-1 的代理服务端口，查看 DUT 上 3 台服务器的状态

- 判定原则：
- 1) 步骤 6) 中，健康检查通过，3 台服务器均状态正常；
 - 2) 步骤 7) 中，健康检查不通过，3 台服务器状态为不可用；
 - 3) 步骤 8) 中，Proxy-1 状态为不可用，其它服务器状态正常

测试编号	26.
测试项目：	全局负载均衡测试-DNS 重定向
测试目的：	测试 DUT 是否支持全局负载均衡功能（DNS 重定向）
测试配置：	

	
<p>测试步骤：</p> <ol style="list-style-type: none">1) 两组被测设备，后台服务器组数量均为 3，工作正常，均可提供 IPv4 和 IPv6 的 HTTP 服务并确认可以回应 ICMP 包；2) 授权 DNS 将 <code>http://www.abc.com</code> 的 NS 指向首选“SLB-1: 222.1.1.100 2221::2221”，次选“SLB-2: 211.1.1.100 2222::2222”，即首选由 SLB-1 负责进行最终的 DNS 解析；3) DUT 健康检查算法为 TCP 80 端口检查；全局负载均衡算法为：本地 DNS-1 的请求由 SLB-1 服务，本地 DNS-2 的请求由 SLB-2 服务；本地负载均衡算法为轮询法；4) 对 DUT 与服务器之间的接口进行抓包；5) 使用两台仪表，模拟两个 IPv4/IPv6 用户，本地 DNS 分别为 Local DNS-1、Local DNS-2，访问 <code>http://www.abc.com</code>；6) 查看全局负载均衡的流程是否正确；7) 使用两台仪表，模拟两个群的 IPv4/IPv6 用户分别发送 1000 条/s（本地 DNS-1）和 10000 条/s 秒（本地 DNS-2）的 <code>http://www.abc.com</code> 请求；8) 查看全局负载均衡状况；9) 将 SLB-2 后台所有服务器 down 掉，查看全局负载均衡状况；10) 恢复后，将 SLB-2 down 掉，查看全局负载均衡状况；11) 恢复后，将 SLB-1 后台所有服务器 down 掉，查看全局负载均衡状况；12) 恢复后，将 SLB-1 down 掉，查看全局负载均衡状况。	
<p>判定原则：</p> <ol style="list-style-type: none">1) 抓包分析，每一个源 IPv4 和 IPv6 地址发出的请求不能都分配给同一台服务器；2) 能够实现全局负载均衡，流量分配不一定均衡；3) 一台 down 掉，另一台能够提供保护	

测试编号	27.
测试项目	全局负载均衡测试-IP Anycast
测试目的	测试 DUT 是否支持全局负载均衡功能（IP Anycast）
测试配置	



测试步骤:

- 1) 两组被测设备, 后台服务器组数量均为 3, 工作正常, 均可提供 IPv4 和 IPv6 的 HTTP 服务并确认可以回应 ICMP 包;
- 2) 两台被测设备均开启 OSPF 协议, 与路由器建立邻居关系, 并都发布 211.1.1.100/32 和 2222::2222/128 的路由;
- 3) DUT 健康检查算法为 TCP 80 端口检查, 本地负载均衡算法为轮询法; 配置 OSPF 开销: X=10, Y=10;
- 4) 对 DUT 与服务器之间的接口进行抓包;
- 5) 使用仪表模拟两个群的 IPv4 和 IPv6 用户 (用户群-1 和用户群-2), 如图连接, 分别发送 1000 条/s 和 10000 条/s 的请求, 访问 VIP=211.1.1.100 和 2222::2222;
- 6) 查看全局负载均衡的流程是否正确, 并查看全局负载均衡状况;
- 7) 将 SLB-1 和 SLB-2 后的一台服务器 down 掉, 查看全局负载均衡状况;
- 8) 恢复后, 将 SLB-2 后台所有服务器 down 掉, 查看全局负载均衡状况;
- 9) 恢复后, 将 SLB-2 down 掉, 查看全局负载均衡状况;
- 10) 恢复后, 将 SLB-1 后台所有服务器 down 掉, 查看全局负载均衡状况;
- 11) 恢复后, 将 SLB-1 down 掉, 查看全局负载均衡状况;
- 12) 恢复后, 设置开销 Y=100, 查看全局负载均衡状况

判定原则:

- 1) 抓包分析, 每一个源 IPv4 和 IPv6 地址发出的请求不能都分配给同一台服务器;
- 2) 步骤 6) 中, SLB-1 共承担 1000 条/秒业务, SLB-2 共承担 10000 条/秒业务, 均平均分配给后台 3 个服务器;
- 3) 步骤 7) 中, SLB-1 和 SLB-2 承担的业务量不变, 均平均分配给后台健康的服务器;
- 4) 步骤 8) 和步骤 9) 中, SLB-1 共承担 11000 条/秒业务, 均平均分配给后台 3 个服务器, SLB-2 无业务流量, 并且业务切换过程中会产生失败的交易;
- 5) 步骤 10) 和步骤 11) 中, SLB-2 共承担 11000 条/秒业务, 均平均分配给后台 3 个服务器, SLB-1 无业务流量, 并且业务切换过程中会产生失败的交易;
- 6) 步骤 12) 中, SLB-1 共承担 11000 条/秒业务, 均平均分配给后台 3 个服务器, SLB-2 无业务流量, 并且业务切换过程中不会产生失败的交易。

9 网络安全功能测试

测试编号 28.
测试项目：VIP 端口转换功能测试
测试目的：测试 DUT 服务端口转换功能，能够隐藏服务器的真实服务端口号
测试配置：同测试编号 1
测试步骤： 1) DUT 工作正常，后台服务器组数量为 3，工作正常，均可提供 HTTP 服务并确认可以回应 ICMP 包，且 3 台服务器提供服务的端口号分别为 6666、7777、8888； 2) DUT 的健康检查算法为 ICMP 算法，负载均衡算法为轮询法； 3) DUT 的 VIP 对外提供服务器的 TCP 端口为 80；对 DUT 与服务器之间的接口进行抓包； 4) 使用仪表模拟客户端仿真 IPv4 和 IPv6 用户，以一定压力访问 VIP，查看后台服务器业务的负载均衡情况
判定原则： 1) DUT 将业务按请求到达的顺序平均分给了后台的 3 台服务器，服务正常，成功屏蔽了后台服务器的真实服务端口； 2) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器

测试编号 29.
测试项目：客户端 NAT 功能测试
测试目的：测试 DUT 的 NAT 特性功能
测试配置：同测试编号 1
测试步骤： 1) 在 DUT 上配置客户端地址转换功能，多对一地址转换；后台服务器提供 IPv4 和 IPv6 的 HTTP 业务； 2) 客户端模拟 IPv4 和 IPv6 用户发起 HTTP 业务访问请求； 3) 客户访问成功，并能得到正确的服务； 4) 检查地址转换结果
判定原则： 1) DUT 可以实现对客户端地址的 NAT 转换； 2) 当客户端对服务端发起访问，在通过 DUT 之后，源地址可以转换成指定的一个 IPv4/IPv6 地址

测试编号 30.
测试项目：实时防御攻击功能测试
测试目的：测试 DUT 是否具有实时防御 SynFlood 攻击功能，保证正常的业务不受影响
测试配置：同测试编号 1
测试步骤： 1) DUT 正常工作，后台服务器组数量为 3，工作正常，均可提供 IPv4 和 IPv6 的 HTTP 服务并确认可以回应 ICMP 包； 2) DUT 健康检查算法为 ICMP 算法，负载均衡算法为轮询法； 3) 利用测试仪表产生 IPv4/IPv6 攻击流量，同时利用仪表产生 IPv4/IPv6 正常业务流量（HTTP 连接：10000/s）； 4) 攻击流量和正常流量访问的 TCP 端口号相同，且物理端口上是混合在一起的；

- 5) 观察 DUT 没有启用实时防御 SynFlood 攻击时的情况;
- 6) DUT 设置防 SynFlood 攻击规则, 观察攻击对服务器和 DUT 的影响

判定原则:

- 1) DUT 可以实时防御 SynFlood 攻击, 实现对服务器的保护;
- 2) 记录正常业务不受影响 (100%成功率) 的最大攻击流量;
- 3) 记录正常业务基本不受影响 (95%成功率) 的最大攻击流量;
- 4) 抓包分析, 每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一服务器

测试编号 31.

测试项目: 基本 ACL 测试

测试目的: 测试 DUT 是否支持基于接口 (或 VLAN) 的基本 ACL 功能

测试配置: 同测试编号 1

测试步骤:

- 1) DUT 正常工作, 后台服务器组数量为 3, 工作正常, 均可提供 IPv4 和 IPv6 的 HTTP 服务并确认可以回应 ICMP 包;
- 2) DUT 健康检查算法为 ICMP 算法, 负载均衡算法为轮询法, 配置基本 ACL 过滤功能;
- 3) 在 DUT 某接口/VLAN 上配置 ACL, ACL 可以是 IPv4 和 IPv6 五元组的任意字段和组合;
- 4) 使用仪表从该接口产生受控类型的数据包;
- 5) 检查 ACL 是否生效

判定原则:

DUT 可以实现接口或 VLAN 的基本 ACL 功能

测试编号 32.

测试项目: 高级 ACL 测试

测试目的: 测试 DUT 是否支持高级 ACL 功能

测试配置: 同测试编号 1

测试步骤:

- 1) DUT 正常工作, 后台服务器组数量为 3, 工作正常, 分别为服务器 A、服务器 B 和服务器 C, 均可提供 IPv4 和 IPv6 的 HTTP 服务并确认可以回应 ICMP 包。
- 2) DUT 健康检查算法为 ICMP 算法, 负载均衡算法为轮询法, 对 DUT 与服务器之间的接口进行抓包;
- 3) 使用仪表模拟客户端, 以一定压力访问 VIP:
 - a) 仪表仿真 100 个 IPv4/IPv6 地址作为源 IP 进行测试, 源 IPv4 地址范围为 192.168.1.101-192.168.1.200/24, 源 IPv6 地址范围为 2001::2-2001::65/64, 且源 IP 地址随机产生;
 - b) 控制仪表访问的连接数, 并保持连接数始终为 3000 连接。
- 4) 查看后台服务器业务的负载均衡情况。
- 5) 配置高级 ACL 过滤功能, 设置对服务器 A 进行连接数限制, 对服务器 A 分配的并发连接数不能超过 200 连接。
- 6) 查看后台服务器业务的负载均衡情况。
- 7) 配置高级 ACL 过滤功能, 设置对单个源 IPv4/IPv6 地址进行连接数限制, 源 IP 为 192.168.1.151 和 2001::21 对 VIP 发起的并发连接数不能超过 10 连接。
- 8) 查看后台服务器业务的负载均衡情况。

9) 配置 DUT 启用基于 Cookie 的会话保持，保留上述配置，并且带有自个的 Cookie；
10) 查看后台服务器业务的负载均衡情况
判定原则：
1) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器；
2) 高级 ACL 的策略可以叠加；
3) 步骤 4) 中，3 台服务器均分配 1000 连接；
4) 步骤 6) 中，服务器 A 分配 200 连接，服务器 B、服务器 C 均分配 1400 连接；
5) 步骤 8) 中，服务器 A 分配 200 连接，服务器 B、服务器 C 分配的均略小于 1400 连接，有约为 20 连接的失败业务（192.168.1.151、2001::21 均有 20 连接失败业务）；
6) 步骤 10) 中，由于会话保持功能的启用，符合会话保持条件的连接应不受限制

测试编号 33.
测试项目：带宽管理功能测试
测试目的：测试 DUT 的带宽管理功能，能否针对 IP 地址或服务端口号进行带宽限制管理
测试配置：同测试编号 1
测试步骤：
1) 配置后台服务器提供 IPv4 和 IPv6 的 FTP 服务，并提供一个 100M 文件共下载传输；
2) 客户端 1 和客户端 2 同时进行文件下载，两个客户端具有不同的 IPv4/IPv6 地址；
3) 客户端能够正常下载文件，并记录客户端的下载速度；
4) 在 DUT 上配置基于服务的带宽管理，例如，基于 FTP 服务的带宽管理，保障带宽 200kbit/s，突发带宽 400kbit/s；
5) 在客户端重新下载文件，记录客户端的下载速度；
6) 将 DUT 上的带宽管理改为基于 IPv4/IPv6 地址的带宽管理，对客户端 1 进行带宽管理，重复步骤 3~步骤 5
判定原则：
1) 在 DUT 未对 FTP 服务进行带宽管理时，客户端下载速度高于 400kbit/s；在对 FTP 服务进行带宽管理时，FTP 服务带宽管理策略使 FTP 客户端下载速度高于 200kbit/s，低于 400kbit/s；
2) 在 DUT 未对客户 IPv4/IPv6 地址进行带宽管理时，两个客户端下载速度都高于 400kbit/s；在对客户端 1 的 IPv4/IPv6 地址进行带宽管理时，客户端 1 的下载速度高于 200kbit/s，低于 400kbit/s，客户端 2 的下载速度仍高于 400kbit/s。

10 性能测试

10.1 四层性能测试

测试编号 34.
测试项目：四层每秒新建连接数测试
测试目的：测试 DUT TCP 每秒新建会话处理能力
测试配置：同测试编号 1
测试步骤：
1) 配置 DUT，使 DUT 工作在四层模式，并且进行如下配置：
a) 配置两个 VIP（分别是 IPv4 和 IPv6 的 VIP）；

<ul style="list-style-type: none"> b) 负载均衡算法：轮询法； c) 健康检查算法：ICMP，周期为 3s； d) 会话保持：不开启； e) 负载均衡器开启 SNMP，并且不能开启缓存功能、压缩功能、连接复用功能。 <p>2) 仪表仿真后台服务器组：</p> <ul style="list-style-type: none"> a) 数量为 11（或>11），工作正常； b) 均可提供 HTTP 服务，并确认可以回应 ICMP 包； c) 页面内容分别测试两种：1024Bytes 的静态文本页面和“百度”首页（仪表可采用录制回放等方式实现）。 <p>3) 仪表仿真客户端：</p> <ul style="list-style-type: none"> a) 仪表所有端口应启动“虚拟路由器”功能，禁止仿真的客户端 IP 与 VIP 同一网段或直连； b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机，IP 地址范围尽量大（数量>100000）； c) 客户端的 Think time 均为 0； d) 每一个 Connection 中只有一个 Transaction，即只有一个 get。 <p>4) 配置测试仪表，使其仿真的服务器在收到 HTTP Request 后，立即响应。</p> <p>5) 配置测试仪表，使其仿真的 HTTP 页面如步骤 2) 条件所述。</p> <p>6) 建立新建连接的压力模型，测试 DUT 每秒新建连接数的最大值（稳定值，瞬时峰值无效），达到最大压力后保持压力 15min。</p> <p>7) 记录每秒新建连接数的测试值</p>	<p>判定原则：</p> <ul style="list-style-type: none"> 1) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。 2) DUT 向所有服务器发送周期性（3s）的 ICMP 报文，以检查后台服务器的健康状态。 3) 测试过程中，用真实的客户端（笔记本电脑）发起请求，验证服务的正确性。 4) 业务成功率应>98%。 5) 查看设备会话表，每一条表项至少应有： <ul style="list-style-type: none"> a) VIP 信息； b) 源 IPv4/IPv6 地址； c) 源端口； d) 服务器 ID； e) 有效时长。 6) 测试过程中设备禁止重启，如遇特殊条件（死机等），记录重启和死机次数。
测试编号 35.	
测试项目：四层最大并发连接数测试	
测试目的：测试 DUT TCP 最大并发会话数量	
测试配置：同测试编号 1	
<p>测试步骤：</p> <p>1) 配置 DUT，使 DUT 工作在四层模式，并且进行如下配置：</p> <ul style="list-style-type: none"> a) 配置两个 VIP（分别是 IPv4 和 IPv6 的 VIP）； b) 负载均衡算法：轮询法； c) 健康检查算法：ICMP，周期为 3s； 	

<ul style="list-style-type: none"> d) 会话保持：不开启； e) 负载均衡器开启 SNMP，并且不能开启缓存功能、压缩功能、连接复用功能。 <p>2) 仪表仿真后台服务器组：</p> <ul style="list-style-type: none"> a) 数量为 11（或>11），工作正常； b) 均可提供 HTTP 服务，并确认可以回应 ICMP 包； c) 页面内容为 1024Bytes 的静态文本页面。 <p>3) 仪表仿真客户端：</p> <ul style="list-style-type: none"> a) 仪表所有端口应启动“虚拟路由器”功能，禁止仿真的客户端 IP 与 VIP 同一网段或直连； b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机，IP 地址范围尽量大（数量>100000）； c) 客户端的 Think time 均为 0； d) 每一个 Connection 中只有一个 Transaction，即只有一个 get。 <p>4) 配置测试仪表，使其仿真的服务器在收到 HTTP Request 后，延迟较长时间响应。</p> <p>5) 建立并发连接的压力模型，测试 DUT 最大并发连接数，达到最大压力后保持压力 5min。</p> <p>6) 配置测试仪表，使其仿真的 HTTP 页面如步骤 2) 条件所述。</p> <p>7) 记录最大并发连接数的测试值</p>	<p>判定原则：</p> <ul style="list-style-type: none"> 1) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。 2) DUT 向所有服务器发送周期性（3s）的 ICMP 报文，以检查后台服务器的健康状态。 3) 测试过程中，用真实的客户端（笔记本电脑）发起请求，验证服务的正确性。 4) 业务成功率应为 100%，整个测试过程中应不断有连接成功结束，又有新的连接请求发起。 5) 查看设备会话表，每一条表项至少应有： <ul style="list-style-type: none"> a) VIP 信息； b) 源 IPv4/IPv6 地址； c) 源端口； d) 服务器 ID； e) 有效时长。 6) 测试过程中设备禁止重启，如遇特殊条件（死机等），记录重启和死机次数
测试编号 36.	
测试项目：四层 TCP 最大吞吐能力测试	
测试目的：测试 DUT 支持的最大吞吐能力 goodput（四层性能）	
测试配置：同测试编号 1	
<p>测试步骤：</p> <p>1) 配置 DUT，使 DUT 工作在四层模式，并且进行如下配置：</p> <ul style="list-style-type: none"> a) 配置两个 VIP（分别是 IPv4 和 IPv6 的 VIP）； b) 负载均衡算法：轮询法； c) 健康检查算法：ICMP，周期为 3s； d) 会话保持：不开启； e) 负载均衡器开启 SNMP，并且不能开启缓存功能、压缩功能、连接复用功能。 <p>2) 仪表仿真后台服务器组：</p>	

<p>a) 数量为 11 (或>11), 工作正常;</p> <p>b) 均可提供 HTTP 服务, 并确认可以回应 ICMP 包;</p> <p>c) 页面内容分别测试两种: 512KBytes 的静态文本页面和“新浪”首页 (仪表可采用录制回放等方式实现)。</p> <p>3) 仪表仿真客户端:</p> <p>a) 仪表所有端口应启动“虚拟路由器”功能, 禁止仿真的客户端 IP 与 VIP 同一网段或直连;</p> <p>b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机, IP 地址范围尽量大 (数量>100000);</p> <p>c) 客户端的 Think time 均为 0;</p> <p>d) 每一个 Connection 中只有一个 Transaction, 即只有一个 get。</p> <p>4) 配置测试仪表, 使其仿真的服务器在收到 HTTP Request 后, 立即响应。</p> <p>5) 配置测试仪表, 使其仿真的 HTTP 页面如步骤 2) 条件所述。</p> <p>6) 建立新建连接的压力模型, 测试 DUT 吞吐量 (Goodput) 的最大值 (稳定值, 瞬时峰值无效), 达到最大压力后保持压力 15min。</p> <p>7) 记录最大吞吐能力的测试值</p>
<p>判定原则:</p> <p>1) 抓包分析, 每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。</p> <p>2) DUT 向所有服务器发送周期性 (3s) 的 ICMP 报文, 以检查后台服务器的健康状态。</p> <p>3) 测试过程中, 用真实的客户端 (笔记本电脑) 发起请求, 验证服务的正确性。</p> <p>4) 业务成功率应>98%。</p> <p>5) 查看设备会话表, 每一条表项至少应有:</p> <p>a) VIP 信息;</p> <p>b) 源 IPv4/IPv6 地址;</p> <p>c) 源端口;</p> <p>d) 服务器 ID;</p> <p>e) 有效时长。</p> <p>6) 测试过程中设备禁止重启, 如遇特殊条件 (死机等), 记录重启和死机次数</p>

10.2 七层性能测试

测试编号 37.
测试项目: 七层每秒新建连接数测试
测试目的: 测试 DUT 工作在七层模式下, 每秒新建会话处理能力
测试配置: 同测试编号 1
<p>测试步骤:</p> <p>1) 配置 DUT, 使 DUT 工作在七层模式, 并且进行如下配置:</p> <p>a) 配置两个 VIP (分别是 IPv4 和 IPv6 的 VIP)。</p> <p>b) 负载均衡算法:</p> <p>基于 URL 内容的负载均衡算法;</p> <p>将“get http://vip/sports”的请求分给 Server1;</p> <p>将“get http://vip/news”的请求分给 Server2;</p> <p>将“get http://vip/government”的请求分给 Server3;</p> <p>将“get http://vip/finance”的请求分给 Server4;</p>

将“get http://vip/technology”的请求分给 Server5;

将“get http://vip/shopping”的请求分给 Server6;

将“get http://vip/game”的请求分给 Server7;

将“get http://vip/bbs”的请求分给 Server8;

将“get http://vip/testing”的请求分给 Server9;

将“get http://vip/billing”的请求分给 Server10;

将“get http://vip/travel”的请求分给 Server11;

对于未能匹配上述 URL 内容的连接,则按照轮询法分配给后台 11 台服务器。

c) 健康检查算法: ICMP, 周期为 3s。

d) 会话保持: 基于 Cookie (DUT Insert 模式)。

e) 负载均衡器开启 SNMP, 并且不能开启缓存功能、压缩功能、连接复用功能。

2) 仪表仿真后台服务器组:

a) 数量为 11 (或>11), 工作正常;

b) 均可提供 HTTP 服务, 并确认可以回应 ICMP 包;

c) 页面内容分别测试两种: 1024Bytes 的静态文本页面和“百度”首页 (仪表可采用录制回放等方式实现)。

3) 仪表仿真客户端:

a) 仪表所有端口应启动“虚拟路由器”功能, 禁止仿真的客户端 IP 与 VIP 同一网段或直连;

b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机, IP 地址范围尽量大 (数量>100000);

c) 客户端的 Think time 均为 0。

4) 配置测试仪表, 使其仿真的服务器在收到 HTTP Request 后, 立即响应。

5) 配置测试仪表, 使其仿真的 HTTP 页面如步骤 2) 条件所述。

6) 客户端的配置如下:

a) 每个客户端的 Action List 都含有如下指令:

1 get http://vip/sports

1 get http://vip/news

1 get http://vip/government

1 get http://vip/finance

1 get http://vip/technology

1 get http://vip/shopping

1 get http://vip/game

1 get http://vip/bbs

1 get http://vip/testing

1 get http://vip/billing

1 get http://vip/travel

1 get http://vip/xxxxxxx (x 可以是不匹配上述 URL 的任意值)

b) 客户端之间的上述 Action List 的顺序可以不同, 防止后台服务器的拥塞;

7) 建立新建连接的压力模型, 测试 DUT 每秒新建连接数的最大值 (稳定值, 瞬时峰值无效), 达到最大压力后保持压力 15min;

8) 记录每秒新建连接数的测试值

判定原则:

- 1) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。
- 2) DUT 向所有服务器发送周期性（3s）的 ICMP 报文，以检查后台服务器的健康状态。
- 3) 抓包分析，URL 内容匹配的请求均分配给相应的服务器，对于同一个 Connection 中的多个 Transaction，应根据 URL 内容，分配给后台的对应服务器。
- 4) 服务器的响应应该被 DUT 插入不同的 Cookie 值。
- 5) 测试过程中，用真实的客户端（笔记本电脑）发起请求，验证服务的正确性。
- 6) 业务成功率应>98%。
- 7) 查看设备会话表，每一条表项至少应有：
 - a) VIP 信息；
 - b) 源 IPv4/IPv6 地址；
 - c) 源端口；
 - d) 服务器 ID；
 - e) 有效时长。
- 8) 测试过程中设备禁止重启，如遇特殊条件（死机等），记录重启和死机次数

测试编号 38.

测试项目：七层最大并发连接数测试

测试目的：测试 DUT 工作在七层模式下，最大并发会话数量

测试配置：同测试编号 1

测试步骤：

1) 配置 DUT，使 DUT 工作在七层模式，并且进行如下配置：

a) 配置两个 VIP（分别是 IPv4 和 IPv6 的 VIP）。

b) 负载均衡算法

基于 URL 内容的负载均衡算法：

将“get http://vip/sports”的请求分给 Server1；

将“get http://vip/news”的请求分给 Server2；

将“get http://vip/government”的请求分给 Server3；

将“get http://vip/finance”的请求分给 Server4；

将“get http://vip/technology”的请求分给 Server5；

将“get http://vip/shopping”的请求分给 Server6；

将“get http://vip/game”的请求分给 Server7；

将“get http://vip/bbs”的请求分给 Server8；

将“get http://vip/testing”的请求分给 Server9；

将“get http://vip/billing”的请求分给 Server10；

将“get http://vip/travel”的请求分给 Server11。

对于未能匹配上述 URL 内容的连接，则按照轮询法分配给后台 11 台服务器。

c) 健康检查算法：ICMP，周期为 3s；

d) 会话保持：基于 Cookie（DUT 插入模式）；

e) 负载均衡器开启 SNMP，并且不能开启缓存功能、压缩功能、连接复用功能。

2) 仪表仿真后台服务器组：

<ul style="list-style-type: none"> a) 数量为 11 (或>11), 工作正常; b) 均可提供 HTTP 服务, 并确认可以回应 ICMP 包; c) 页面内容为 1024Bytes 的静态文本页面。 <p>3) 仪表仿真客户端:</p> <ul style="list-style-type: none"> a) 仪表所有端口应启动“虚拟路由器”功能, 禁止仿真的客户端 IP 与 VIP 同一网段或直连; b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机, IP 地址范围尽量大 (数量>100000); c) 客户端的 Think time 均为 0。 <p>4) 配置测试仪表, 使其仿真的服务器在收到 HTTP Request 后, 延迟较长时间响应。</p> <p>5) 配置测试仪表, 使其仿真的 HTTP 页面如步骤 2) 条件所述。</p> <p>6) 客户端的配置如下:</p> <ul style="list-style-type: none"> a) 每个客户端的 Action List 都含有如下指令: <ul style="list-style-type: none"> 1 get http://vip/sports 1 get http://vip/news 1 get http://vip/government 1 get http://vip/finance 1 get http://vip/technology 1 get http://vip/shopping 1 get http://vip/game 1 get http://vip/bbs 1 get http://vip/testing 1 get http://vip/billing 1 get http://vip/travel 1 get http://vip/xxxxxxx (x 可以是不匹配上述 URL 的任意值) b) 客户端之间的上述 Action List 的顺序可以不同, 防止后台服务器的拥塞。 <p>7) 建立并发连接的压力模型, 测试 DUT 最大并发连接数, 达到最大压力后保持压力 5min。</p> <p>8) 记录最大并发连接数的测试值</p>	<p>判定原则:</p> <ul style="list-style-type: none"> 1) 抓包分析, 每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。 2) DUT 向所有服务器发送周期性 (3s) 的 ICMP 报文, 以检查后台服务器的健康状态。 3) 抓包分析, URL 内容匹配的请求均分配给相应的服务器, 对于同一个 Connection 中的多个 Transaction, 应根据 URL 内容, 分配给后台的对应服务器。 4) 服务器的响应应该被 DUT 插入不同的 Cookie 值。 5) 测试过程中, 用真实的客户端 (笔记本电脑) 发起请求, 验证服务的正确性。 6) 业务成功率应为 100%, 整个测试过程中应不断有连接成功结束, 又有新的连接请求发起。 7) 查看设备会话表, 每一条表项至少应有: <ul style="list-style-type: none"> a) VIP 信息; b) 源 IPv4/IPv6 地址; c) 源端口; d) 服务器 ID; e) 有效时长。
--	--

8) 测试过程中设备禁止重启，如遇特殊条件（死机等），记录重启和死机次数

测试编号 39.

测试项目：七层最大吞吐能力测试

测试目的：测试 DUT 工作在七层模式下，最大吞吐能力（goodput）

测试配置：同测试编号 1

测试步骤：

1) 配置 DUT，使 DUT 工作在七层模式，并且进行如下配置：

a) 配置两个 VIP（分别是 IPv4 和 IPv6 的 VIP）；

b) 负载均衡算法

基于 URL 内容的负载均衡算法；

将“get http://vip/sports”的请求分给 Server1；

将“get http://vip/news”的请求分给 Server2；

将“get http://vip/government”的请求分给 Server3；

将“get http://vip/finance”的请求分给 Server4；

将“get http://vip/technology”的请求分给 Server5；

将“get http://vip/shopping”的请求分给 Server6；

将“get http://vip/game”的请求分给 Server7；

将“get http://vip/bbs”的请求分给 Server8；

将“get http://vip/testing”的请求分给 Server9；

将“get http://vip/billing”的请求分给 Server10；

将“get http://vip/travel”的请求分给 Server11。

对于未能匹配上述 URL 内容的连接，则按照轮询法分配给后台 11 台服务器。

c) 健康检查算法：ICMP，周期为 3s；

d) 会话保持：基于 Cookie（DUT 插入模式）；

e) 负载均衡器开启 SNMP，并且不能开启缓存功能、压缩功能、连接复用功能。

2) 仪表仿真后台服务器组：

a) 数量为 11（或>11），工作正常；

b) 均可提供 HTTP 服务，并确认可以回应 ICMP 包；

c) 页面内容分别测试两种：512KBytes 的静态文本页面和“新浪”首页（仪表可采用录制回放等方式实现）。

3) 仪表仿真客户端：

a) 仪表所有端口应启动“虚拟路由器”功能，禁止仿真的客户端 IP 与 VIP 同一网段或直连；

b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机，IP 地址范围尽量大（数量>100000）；

c) 客户端的 Think time 均为 0。

4) 配置测试仪表，使其仿真的服务器在收到 HTTP Request 后，立即响应。

5) 配置测试仪表，使其仿真的 HTTP 页面如步骤 2) 条件所述。

6) 客户端的配置如下：

a) 每个客户端的 Action List 都含有如下指令：

l get http://vip/sports

l get http://vip/news

<div>1 get http://vip/government</div> <div>1 get http://vip/finance</div> <div>1 get http://vip/technology</div> <div>1 get http://vip/shopping</div> <div>1 get http://vip/game</div> <div>1 get http://vip/bbs</div> <div>1 get http://vip/testing</div> <div>1 get http://vip/billing</div> <div>1 get http://vip/travel</div> <div>1 get http://vip/xxxxxxx (x 可以是不匹配上述 URL 的任意值)</div> <div>b) 客户端之间的上述 Action List 的顺序可以不同, 防止后台服务器的拥塞。</div> <div>7) 建立新建连接的压力模型, 测试 DUT 吞吐量 (Goodput) 的最大值 (稳定值, 瞬时峰值无效), 达到最大压力后保持压力 15min。</div> <div>8) 记录最大吞吐能力 Goodput 的测试值</div>
<div>判定原则:</div> <div>1) 抓包分析, 每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。</div> <div>2) DUT 向所有服务器发送周期性 (3s) 的 ICMP 报文, 以检查后台服务器的健康状态。</div> <div>3) 抓包分析, URL 内容匹配的请求均分配给相应的服务器, 对于同一个 Connection 中的多个 Transaction, 应根据 URL 内容, 分配给后台的对应服务器。</div> <div>4) 服务器的响应应该被 DUT 插入不同的 Cookie 值。</div> <div>5) 测试过程中, 用真实的客户端 (笔记本电脑) 发起请求, 验证服务的正确性。</div> <div>6) 业务成功率应>98%。</div> <div>7) 查看设备会话表, 每一条表项至少应有:<div><div>a) VIP 信息;</div><div>b) 源 IPv4/IPv6 地址;</div><div>c) 源端口;</div><div>d) 服务器 ID;</div><div>e) 有效时长。</div></div></div> <div>8) 测试过程中设备禁止重启, 如遇特殊条件 (死机等), 记录重启和死机次数</div>

10.3 长时间稳定性测试

测试编号 40.
测试项目: 长时间稳定性测试
测试目的: 测试 DUT 长时间运行时的稳定性情况
测试配置: 同测试编号 1
<div>测试步骤:</div> <div>1) 配置 DUT, 使 DUT 工作在七层模式, 并且进行如下配置:<div><div>a) 配置两个 VIP (分别是 IPv4 和 IPv6 的 VIP);</div><div>b) 负载均衡算法:<div>基于 URL 内容的负载均衡算法;</div></div></div></div>

将“get http://vip/sports”的请求分给 Server1;

将“get http://vip/news”的请求分给 Server2;

将“get http://vip/government”的请求分给 Server3;

将“get http://vip/finance”的请求分给 Server4;

将“get http://vip/technology”的请求分给 Server5;

将“get http://vip/shopping”的请求分给 Server6;

将“get http://vip/game”的请求分给 Server7;

将“get http://vip/bbs”的请求分给 Server8;

将“get http://vip/testing”的请求分给 Server9;

将“get http://vip/billing”的请求分给 Server10;

将“get http://vip/travel”的请求分给 Server11。

对于未能匹配上述 URL 内容的连接,则按照轮询法分配给后台 11 台服务器。

c) 健康检查算法: ICMP, 周期为 3s。

d) 会话保持: 基于 Cookie (DUT 插入模式)。

e) 负载均衡器开启 SNMP, 并且不能开启缓存功能、压缩功能、连接复用功能。

2) 仪表仿真后台服务器组:

a) 数量为 11 (或>11), 工作正常;

b) 均可提供 HTTP 服务, 并确认可以回应 ICMP 包;

c) 页面内容为“百度”首页 (仪表可采用录制回放等方式实现)。

3) 仪表仿真客户端:

a) 仪表所有端口应启动“虚拟路由器”功能, 禁止仿真的客户端 IP 与 VIP 同一网段或直连;

b) 仪表仿真的源 IPv4/IPv6 地址尽量离散且随机, IP 地址范围尽量大 (数量>100000);

c) 客户端的 Think time 均为 0。

4) 配置测试仪表, 使其仿真的服务器在收到 HTTP Request 后, 立即响应。

5) 配置测试仪表, 使其仿真的 HTTP 页面如步骤 2) 条件所述。

6) 客户端的配置如下:

a) 每个客户端的 Action List 都含有如下指令:

1 get http://vip/sports

1 get http://vip/news

1 get http://vip/government

1 get http://vip/finance

1 get http://vip/technology

1 get http://vip/shopping

1 get http://vip/game

1 get http://vip/bbs

1 get http://vip/testing

1 get http://vip/billing

1 get http://vip/travel


1 get http://vip/xxxxxxx (x 可以是不匹配上述 URL 的任意值)

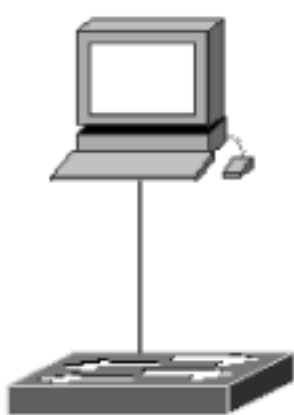
b) 客户端之间的上述 Action List 的顺序可以不同, 防止后台服务器的拥塞;

7) 建立新建连接的压力模型，压力为设备最大值的 90%，运行 10h 以上； 8) 记录业务成功率，以及设备有无宕机、重启等
判定原则： 1) 抓包分析，每一个源 IPv4/IPv6 地址发出的请求不能都分配给同一台服务器。 2) DUT 向所有服务器发送周期性（3s）的 ICMP 报文，以检查后台服务器的健康状态； 3) 抓包分析，URL 内容匹配的请求均分配给相应的服务器，对于同一个 Connection 中的多个 Transaction，应根据 URL 内容，分配给后台的对应服务器。 4) 服务器的响应应该被 DUT Insert 不同的 Cookie 值。 5) 测试过程中，用真实的客户端（笔记本电脑）发起请求，验证服务的正确性。 6) 业务成功率应>98%。 7) 查看设备会话表，每一条表项至少应有： a) VIP 信息； b) 源 IPv4/IPv6 地址； c) 源端口； d) 服务器 ID； e) 有效时长。 8) 测试过程中设备稳定，无宕机、重启

11 网络管理功能测试

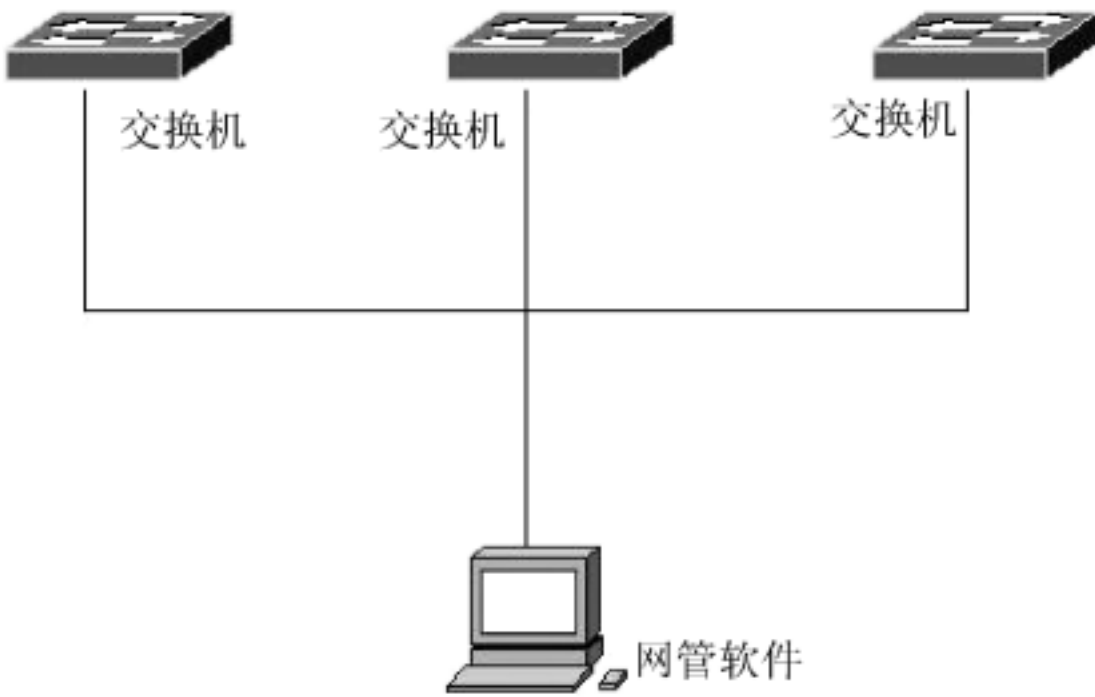
11.1 网管功能测试

测试编号 41.
测试项目：网管操作员越权操作预防的测试
测试目的：网管系统应能设置每个网管操作员的操作权限。越权操作包括低权限的操作员操作高权限才能操作的操作；同权限的操作员间以其他操作员身份进行操作
测试配置： <div></div>
测试步骤： 1) 由最高权限的网管人员配置操作 ID 和操作权限； 2) 由最高权限的网管人员帮助设置或修改操作员密码(或口令)
判定原则： 1) 低权限的操作员操作高权限的操作，应被拒绝并有日志记录； 2) 操作员 ID 和对应的密码不符，应被拒绝并有日志记录； 3) 所有的密码均不能读取或显示

测试编号 42.
测试项目：非网管人员进入系统操作的测试
测试目的：网管系统应具有防止非网管人员进入系统操作的能力
测试配置： <div style="text-align: center;">  <p>局域网交换机</p> </div>
测试步骤： 操作员输入不正确的操作员 ID/口令或密码
判定原则： 不正确的操作员 ID/口令或密码，应不能进入网管系统

测试编号 43.
测试项目：网管系统操作日志的测试
测试目的：日志对网络各种状态有影响的日志、查询能力
测试配置： <div style="text-align: center;">  <p>局域网交换机</p> </div>
测试步骤： <ol style="list-style-type: none"> 1) 查询网管操作日志信息的请求； 2) 网管操作日志信息查询结果的显示
判定原则： <ol style="list-style-type: none"> 1) 网管系统上应能查询对网络操作有影响的操作日志信息； 2) 每条日志信息应包括： <ul style="list-style-type: none"> - 操作员 ID； - 操作日期、时间； - 操作内容。 3) 应提供如按时间、操作员 ID 等方便的查询方式

测试编号 44.
测试项目：集中网管系统对所有设备管理的测试
测试目的：网管系统同时监控多台设备，同时对多台设备进行系统升级能力
测试配置：


测试步骤： 1) 如图配置多台双栈内容交换设备，在客户端安装网管软件； 2) 启动网管系统，查看同一网管界面所监控的设备数； 3) 通过网管软件同时对多台双栈内容交换设备进行系统升级
判定原则： 1) 在网管软件一个视图中同时显示多台双栈内容交换设备； 2) 网管软件同时对多台双栈内容交换设备系统升级成功

测试编号 45.
测试项目：配置文件管理
测试目的：备份设备的配置文件，当所有负载均衡设备故障更换新设备后，仍然能够把原来的配置文件直接恢复在新设备上
测试步骤： 1) 备份运行设备的配置文件到管理工作站上； 2) 更换一台新的设备； 3) 把保存在管理工作站上的原配置文件恢复到新设备上去； 4) 观察新设备的运行情况
判定原则： 新设备上的配置完全恢复，运行正常

11.2 SNMPv1/v2 协议测试

SNMPv1/v2 协议测试见 YD/T 1941—2009 中 9.3。

11.3 SNMPv3 协议测试

SNMPv3 协议测试见 YD/T 1941—2009 中 9.5。

11.4 通用 Trap 测试

通用 Trap 测试见 YD/T 1941—2009 中 9.4。

11.5 SSH 安全登录测试

测试编号 46.
测试项目：SSH 安全登录测试

测试目的：测试 DUT 允许终端通过 SSH 连接，进行管理
测试配置： <div style="text-align: center;">  <p>局域网交换机</p> </div>
测试步骤： <ol style="list-style-type: none"> 1) 在 DUT 上配置通过 SSH 安全登录进行管理； 2) 管理终端通过 SSH 登录到设备； 3) 检查结果
判定原则： DUT 支持 SSH 安全登录

11.6 计费管理测试

计费管理测试见 YD/T 1941—2009 中 9.6。

12 操作维护测试

12.1 日志测试

日志测试见 YD/T 1941—2009 中 10.3。

12.2 统计查询和报表功能测试

统计查询和报表功能测试见 YD/T 1941—2009 中 10.4。

12.3 人机界面测试

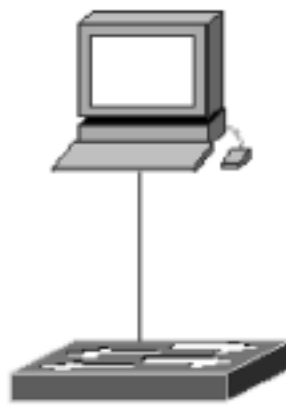
人机界面测试见 YD/T 1941—2009 中 10.5。

12.4 操作员维护管理测试

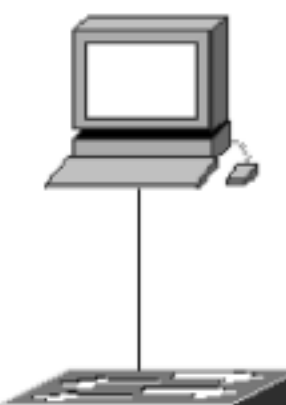
操作员维护管理测试见 YD/T 1941—2009 中 10.6。

12.5 终端管理测试

测试编号 47.
测试项目：终端管理测试
测试目的：测试交换机只允许来自某一源地址的终端进行管理
测试配置：

<div><p>局域网交换机</p></div>
<p>测试步骤：</p> <p>1) 在交换机上配置管理终端地址；</p> <p>2) 检查结果</p>
<p>判定原则：</p> <p>交换机可以配置为只允许来自某一源地址的终端进行配置</p>

12.6 安全管理测试

测试编号 48.
测试项目：安全管理测试
测试目的：测试交换机只允许终端通过特定的物理端口连接，进行管理
<p>测试配置：</p> <div><p>局域网交换机</p></div>
<p>测试步骤：</p> <p>1) 在交换机上配置不同物理端口上的管理权限；</p> <p>2) 管理终端连接不同的物理端口进行管理；</p> <p>3) 检查结果</p>
<p>判定原则：</p> <p>交换机可以在每个物理端口上设置是否可以进行管理，以及管理的方式</p>

13 可靠性测试

13.1 设备启动时间测试

设备启动时间测试见 YD/T 1941—2009 中 12.3。

13.2 双机热备功能测试

双机热备功能测试见 YD/T 1941—2009 中 12.4。

13.3 双机热备中的会话同步功能测试

双机热备中的会话同步功能测试见 YD/T 1941—2009 中 12.5。

13.4 热插拔可靠性测试（可选）

热插拔可靠性测试见 YD/T 1941—2009 中 12.6。

13.5 双机情况下在线升级测试

双机情况下的在线升级测试见 YD/T 1941—2009 中 12.7。
