

ICS 01.040.33

L 78

YD

中华人民共和国通信行业标准

YD/T 2448-2013

公众 IP 网络可靠性 虚拟路由冗余协议 (VRRP) 技术要求

IP network reliability
—Technical requirements of virtual router redundancy protocol

2013-04-25 发布

2013-06-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 概述	2
5 VRRP 协议特征	3
5.1 说明	3
5.2 IP 地址备份	3
5.3 首选路径指示	3
5.4 最小化不必要的业务中断	3
5.5 扩展 LAN 上的高效操作	3
6 VRRP 协议概述	3
7 协议	4
7.1 VRRP 报文格式	4
7.2 IP 字段描述	5
7.3 VRRP 字段描述	6
8 协议状态机	6
8.1 虚拟路由器的参数	6
8.2 定时器	6
8.3 状态迁移表	6
8.4 状态描述	7
9 发送和接收 VRRP 报文	9
9.1 接收 VRRP 报文	9
9.2 VRRP 报文传送	9
9.3 虚拟路由器 MAC 地址	10
10 执行问题	10
10.1 ICMP 重定向	10
10.2 主机 ARP 请求	10
10.3 代理 ARP	10
10.4 可能的转发环回	10
11 安全	10
附录 A (资料性附录) 配置实例	11

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准公众IP网络可靠性系列标准之一。该系列标准预计为：

1. YD/T 2373《公众IP网络可靠性 总体技术要求》；
2. YD/T 2175《公众IP网络可靠性 标记分发协议(LDP)平滑重启动技术要求及测试方法》；
3. YD/T 2176《公众IP网络可靠性 中间系统到中间系统路由交换协议 (IS-IS) 中平滑重启动技术要求及测试方法》；
4. YD/T 1702-2007《公众IP网络可靠性 IP快速重路由技术框架》；
5. YD/T 2416-2012《公众IP网络可靠性 IP快速重路由技术要求》；
6. 《公众IP网络可靠性 RSVP-TE平滑重启动技术要求》；
7. YD/T 2447-2013《公众IP网络可靠性 双向转发检测 (BFD) 机制的技术要求》；
8. YD/T 2448-2013《公众IP网络可靠性 虚拟路由器冗余协议 (VRRP) 技术要求》。

本标准技术内容和 IETF RFC 5798 中涉及 IPv4 上的技术内容保持一致。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

附录A为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院。

本标准起草人：孙明俊、赵 锋、高 巍、蒋晓琳、田 辉。

公众IP网络可靠性

虚拟路由冗余协议（VRRP）技术要求

1 范围

本标准描述了VRRP的特征，设计目标和操作原理，包含VRRP消息格式，协议处理规则和用来监视单个主虚拟路由器收敛情况的状态机，规定了和MAC地址映射相关的操作问题，ARP请求的处理，ICMP重定向消息的产生以及相关的安全问题。

本标准适用于支持VRRP协议的IPv4路由器。

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 1071 计算Internet校验和（Computing the Internet checksum）

IETF RFC 2338 虚拟路由器冗余协议（第一版）（Virtual Router Redundancy Protocol）

3 术语、定义和缩略语

3.1 术语和定义

下列定义和术语适用于本文件。

3.1.1

VRRP 路由器 VRRP Router

运行虚拟路由器冗余协议的路由器。可能包含了一个或多个虚拟路由器。

3.1.2

虚拟路由器 virtual Router

VRRP管理的抽象对象，是共享局域网中主机的默认路由器。包含虚拟路由器标识和一系列位于公共局域网中的相关的IP地址。一个VRRP路由器可能有一个或多个虚拟路由器作为备份。

3.1.3

IP地址拥有者 IP Address Owner

拥有虚拟路由器的IP地址作为真实接口地址的VRRP路由器。该路由器启动后，将会对发送到虚拟路由器任意IP地址的数据包进行响应，比如ICMP ping，TCP连接等。

3.1.4

主IP地址 Primary IP Address

从真实接口地址序列中挑选出的IP地址。常用的选择算法是选择序列中的第一个地址。VRRP通告总是使用主IP地址作为IP包的源地址。

3.1.5

主虚拟路由器 Virtual Router Master

VRRP路由器认为主虚拟路由器负责响应送到虚拟路由器的转发包，同时回答到虚拟地址的ARP请求。需要注意的是，可用的IP地址拥有者应该优先成为主路由器。

3.1.6

虚拟路由器备份 Virtual Router Backup

在当前主虚拟路由器不可用时，其他可用来负责包转发的VRRP路由器序列。

3.2 缩略语

下列缩略语适用于本文件。

ARP	Address Resolution Protocol	地址解析协议
DHCP	Dynamic Host Configuration Protocol	动态主机协议
IANA	internet assigned numbers authority	互联网编号分配机构
ICMP	Internet Control Message Protocol	互联网控制消息协议
IP	Internet Protocol	互联网协议
LAN	Local Area Network	局域网
MAC	Media Access Control	媒体接入控制
OSPF	Open Shortest Path First	开放式最短路径优先
OUI	organizationally unique identifier	组织唯一标识
RIP	Router Information Protocol	路由信息协议
TCP	Transmission Control Protocol	传输控制协议
VRID	Virtual Router ID	虚拟路由器ID
VRRP	Virtual Router Redundancy Protocol	虚拟路由冗余协议

4 概述

网络中的节点可以采用多种方法来决定其到达特定IP目的地的第一跳路由器，包括运行或侦听动态路由协议（例如RIP或OSPF v2），或运行ICMP路由发现客户端，或使用静态配置的缺省路由。

基于管理的开销、处理开销、安全问题以及某些平台上缺乏相应的协议实现等原因，不会再在所有端主机上运行动态路由协议。由于邻居或路由器发现协议需要网络上的所有主机参与，当主机数量很大时，需要设置加大的定时器值来减少网络的协议开销。这导致检测丢失的邻居时延增大，带来长到不可接受的“黑洞”时间。

静态配置的缺省路由减少了配置和处理开销，使用广泛，几乎所有的端点都支持。在部署动态主机配置协议（DHCP）的情况下，通常可以提供端主机的IP地址和缺省网关的配置。但也会导致单故障点，在缺省网关失效时，所有的独立端主机都无法检测到任何可用的替代路径。

虚拟路由器冗余协议（VRRP）设计的目标是消除在静态路由配置环境下固有的单故障点。VRRP规范了一个选举协议，该协议动态的将LAN上的其中一个VRRP路由器赋予虚拟路由器的功能。关联到虚拟路由器的IP地址的VRRP路由器称为主虚拟路由器，路由器转发IP包到这些IP地址。当主路由器变得不可用时，选举过程提供了转发功能的自动倒换。LAN上的任何虚拟路由器的IP地址可以作为端主机的第一跳路由器。VRRP协议的优点就是不需要在每个端主机上配置动态路由或路由发现协议，也可获得缺省路由的较高的可用性。

5 VRRP 协议特征

5.1 说明

本章描述的特征是必须遵守的，用于指导VRRP的设计。

5.2 IP 地址备份

IP地址备份是虚拟路由器冗余备份的主要功能。进行主虚拟路由器选择时，协议应该满足如下描述的附加功能：

- 最小的黑洞持续时间；
- 最小的稳态带宽和处理复杂性；
- 在多种接入局域网技术的基础上支持支持 IP 流量的功能；
- 为满足负载均衡的需求，在一个网络中提供多个可选的虚拟路由器；
- 在一个单独的局域网分片内支持多个逻辑 IP 子网。

5.3 首选路径指示

在一系列冗余路由器中选择主虚拟路由器，一个简单的模型就是为每个路由器赋予相同的优先权，在收敛到其中一个路由器之后就可以认为选择成功。然而，大多数环境下在冗余路由器序列中存在着截然不同的选择（或者选择范围）。例如，优先权可能是基于接入链路的费用或者速度，路由器性能或者可靠性，或者其他策略的考虑。本标准允许路径优先权的表达方式可以以直观方式进行，并保证主虚拟路由器是收敛到当前可用路由器中最优先的一个。

5.4 最小化不必要的业务中断

一旦选定的主虚拟路由器开始工作，主虚拟路由器和备份的虚拟路由器之间的任何不必要的转变都会导致业务的中断。本标准确保在选定主虚拟路由器之后，只要主虚拟路由器工作正常，任何相同或者低优先权的备份路由器不能引发状态迁移。

比如某个路由器变为可用状态时，优先权可能会高于主虚拟路由器，这种环境下上述规定将会非常有用。

5.5 扩展 LAN 上的高效操作

在多接入的LAN上发送IP报文时，需要将IP地址映射为MAC地址。在有学习桥的扩展LAN上，如果启用的虚拟路由器MAC地址没有作为源地址使用过，会引起报文的泛洪发送，对发到虚拟路由器的报文的带宽产生明显影响。为提高该环境下的效率，协议需要遵守以下规定：

- 主路由器发送的报文中的 MAC 地址作为虚拟路由器的源地址，触发站点学习；
- 在路由器变为主虚拟路由器后，立即触发更新站点学习的消息；
- 从主虚拟路由器触发周期性的消息来维持站点学习缓存。

6 VRRP 协议概述

为了提供上述虚拟路由器功能，VRRP规定了一个选择协议。所有协议消息都使用IP组播数据报文，以保证协议运行在各种的LAN接入技术时都能支持IP组播。每个运行VRRP的虚拟路由器都有一个单独的知名MAC地址，本标准仅对使用IEEE 802.48-bit MAC进行映射的情况做出规定。虚拟路由器MAC地址，用作主路由器发出所有周期性VRRP消息的源MAC地址，可用来启动扩展LAN中的桥学习过程。

7.2 IP 字段描述

7.2.1 源地址

报文发出的地址。

7.2.2 目的地址

IANA分配给 VRRP的组播地址是：

224.0.0.18

该地址为本地网组播地址。

路由器在向该目的地址转发数据报文时，必须同时考虑TTL。

7.2.3 TTL

TTL 必须设为255。VRRP路由器收到TTL不等于255的报文时，必须将该报文丢弃。

7.2.4 协议

IANA分配给 VRRP的协议号是112。

7.3 VRRP 字段描述

7.3.1 版本

版本字段规定VRRP的协议版本，本标准为2。

7.3.2 类型

VRRP报文的类型。本版本中只有一个：

1 ADVERTISEMENT

类型为其他的报文必须被丢弃。

7.3.3 虚拟路由器标识 (VRID)

虚拟路由器标识(VRID)字段，是报文所报告的状态的虚拟路由器标识。范围是1-255 (decimal)，无默认值。

7.3.4 优先级

发送报文的VRRP路由器在虚拟路由器中的优先级。较大的值代表较高的优先级。该字段是8比特无符号整数。

拥有虚拟路由器关联地址的VRRP路由器优先级必须是255 (decimal)。

备份的VRRP路由器值必须在1~254 (decimal)之间。默认值为100(decimal)。

优先级值0有特别规定，是当前主虚拟路由器停止参与VRRP，用以触发备份路由器快速切换为主虚拟路由器而无需等待当前主虚拟路由器超时。

7.3.5 Count IP Addr

在VRRP通告中包含的IP地址数量。

7.3.6 认证类型

认证类型字段规定了使用的认证方法。在一个虚拟路由器中认证类型是唯一的。认证类型字段是8比特无符号整数。如果报文中的认证类型未知，或者和本地配置的认证类型不符，该报文必须被丢弃。

认证方法包括：

0(无认证): 使用该认证类型时，VRRP协议的消息交换不需要认证。认证数据字段应为0。

1(保留): 该字段保留以便与IETF RFC 2338兼容。

2(保留): 该字段保留以便与IETF RFC 2338兼容。

7.3.7 通告间隔 (Adver Int)

通告间隔规定ADVERTISEMENTS直接的时间, 单位为秒。默认是1秒。该字段用于配置错误的路由器的故障定位。

7.3.8 校验和 (Checksum)

Checksum字段用来检查VRRP消息的数据完整性, 是VRRP消息16比特长度补码和的补码。为计算校验和, 该字段应设为0。详见IETF RFC 1071。

7.3.9 IP 地址

虚拟路由器关联的一个或多个IP地址。地址数量在"Count IP Adrs"字段规定。这些字段用作配置错误的路由器的故障定位。

7.3.10 认证数据

认证字符串仅用作与IETF RFC2338兼容。在传输时设为0, 接收时丢弃。

8 协议状态机

8.1 虚拟路由器的参数

表1规定了虚拟路由器的参数。

表1 虚拟路由器的参数

VRID	虚拟路由器标识。范围是 1~255 (decimal), 无默认值
Priority	拥有虚拟路由器关联地址的 VRRP 路由器优先级必须是 255。备份的 VRRP 路由器值必须在 1-254 (decimal)之间。默认值为 100(decimal)。优先级值 0 有特别规定, 用于主虚拟路由器之间的状态迁移
IP_Addresses	与主虚拟路由器相关的一个或多个地址, 配置项, 无默认
advertisement_Interval	ADVERTISEMENTS 之间的时间间隔。默认 1s
Skew_Time	偏离 Master_Down_Interval 的时间, 单位为秒。 计算方法: $(256 - \text{Priority}) / 256$
Master_Down_Interval	备份路由器宣布主虚拟路由器停止运行的时间间隔, 单位为秒。 计算方法: $(3 * \text{Advertisement_Interval}) + \text{Skew_time}$
Preempt_Mode	高优先级的备份路由器是否取代低优先级的主虚拟路由器, 值为 True 是允许取代, False 则不允许。默认为 True。 注: 拥有和虚拟路由器相同 IP 地址的路由器可以不受此该模式的影响
Authentication_Type	认证使用的类型。具体的值在 7.3.6 小节规定
Authentication_Data	使用特定 Authentication_Type 的认证数据

8.2 定时器

表2规定了定时器参数。

表2 定时器参数

Master_Down_Timer	Master_Down_Interval 超时没有收到 ADVERTISEMENT 是触发的定时器
Adver_Timer	基于 Advertisement_Interval, 触发 ADVERTISEMENT 发送的定时器

8.3 状态迁移表

图2所示规定了状态迁移图。

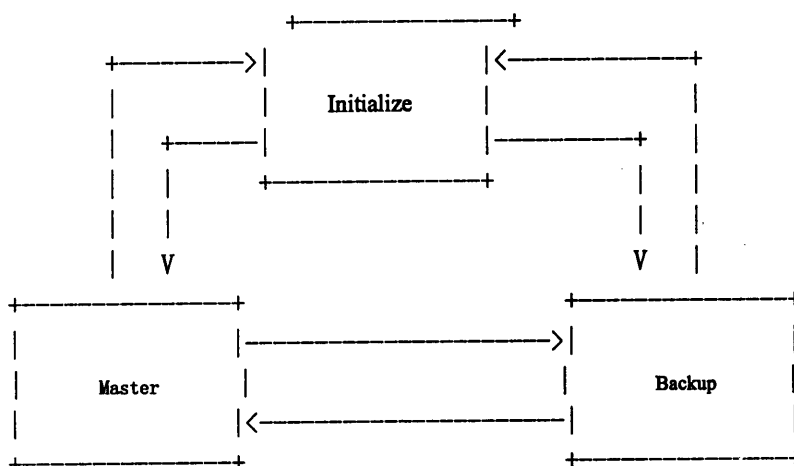


图2 状态迁移图

8.4 状态描述

状态名字使用{状态-名字}格式，报文使用全大写来标识。

VRRP路由器在虚拟路由器选择时需要执行上述状态机。

8.4.1 初始化

该状态用来等待一个Startup事件。如果收到一个Startup事件，那么：

- if Priority = 255 (比如路由器拥有虚拟路由器关联的 IP 地址)
 - 发送ADVERTISEMENT
 - 广播一个gratuitous ARP请求，包含和虚拟路由器IP地址对应的MAC地址
 - 设置Adver_Timer为Advertisement_Interval
 - 变为{Master} state
- else
 - 设置Master_Down_Timer为Master_Down_Interval
 - 变为{Backup}状态
- endif

8.4.2 备份

{Backup}状态的目的是监视主虚拟路由器的可用性和状态。

当在Backup状态时，VRRP路由器必须遵守以下内容：

- 不运行响应对虚拟路由器关联的 IP 地址的 ARP 请求。
- 必须丢弃目的 MAC 地址为虚拟路由器 MAC 地址的报文。
- 不允许接受目的 IP 地址为虚拟路由器的报文。
- 如果收到 Shutdown 事件，那么：
 - 取消Master_Down_Timer
 - 变为{Initialize}状态
 - endif
- If Master_Down_Timer启动，那么：

发送ADVERTISEMENT

对每个关联到虚拟路由器的IP地址发送包含虚拟路由器MAC的gratuitous ARP。

设置Adver_Timer为Advertisement_Interval

转为{Master}状态

endif

If 收到ADVERTISEMENT, 那么:

If ADVERTISEMENT的优先级为0, 那么:

设置Master_Down_Timer为Skew_Time

else:

If Preempt_Mode为False, 或者ADVERTISEMENT的优先级大于或等于本地优先级,

那么:

重设Master_Down_Timer为Master_Down_Interval

else:

丢弃ADVERTISEMENT

endif

endif

endif

8.4.3 主虚拟路由器

当{Master}状态的路由器执行虚拟路由器的转发功能时, 必须按照如下内容操作:

- 必须响应发送到虚拟路由器 IP 地址的 ARP 请求;
- 必须转发目的 MAC 地址是虚拟路由器 MAC 地址的报文;
- 不允许接收发送到虚拟路由器但不是到主虚拟路由器地址的报文;
- 必须接收发送到虚拟路由器但是到主虚拟路由器地址的报文;
- If 收到 Shutdown 事件, 那么:

取消Adver_Timer

发送ADVERTISEMENT, Priority = 0

变为{Initialize}状态

endif

- If Adver_Timer 启动, 那么:

发送ADVERTISEMENT

重设 Adver_Timer为Advertisement_Interval

endif

- If 收到 ADVERTISEMENT, 那么:

If ADVERTISEMENT优先级为0, 那么:

发送ADVERTISEMENT

设置Adver_Timer为Advertisement_Interval

else:

如果ADVERTISEMENT的优先级大于本地优先级

or

If ADVERTISEMENT的优先级等于本地优先级, 发送者的IP地址大于本地IP地址, 那么:

取消Adver_Timer

设置Master_Down_Timer为Master_Down_Interval

变为 {Backup} 状态

else:

丢弃ADVERTISEMENT

endif

endif

endif

9 发送和接收 VRRP 报文

9.1 接收 VRRP 报文

当收到VRRP报文时需要执行如下功能:

- 必须确认IP TTL是255;
- 必须确认VRRP版本为2;
- 必须确认收到的是完整的VRRP报文 (包括固定字段, IP地址, 认证数据);
- 必须确认VRRP checksum;
- 必须确认接收接口配置了VRID, 本地路由器不是IP地址所有者 (优先级为255(decimal));
- 必须确认Auth Type能够匹配到本地配置的认证方法, 执行该认证方法;
- 如果上述检查有一项失败, 接收者必须丢弃报文, 记录该事件, 可能会通过网管报告发生了错误;
- 可能需要确认"Count IP Addr"和配置到VRID的IP地址能否匹配;
- 如果上述检查失败, 接收者应该记录该事件, 可能会通过网管报告检测到错误配置;
- 如果报文不是由地址所有者 (优先级不等于255 (decimal)) 产生的, 接收者必须丢弃该报文;
- 否则继续处理;
- 必须确认Adver Interval和本地虚拟路由器上的配置相同。

如果上述检查失败, 接收者必须丢弃报文, 应该记录该事件, 可能会通过网管报告检测到错误配置。

9.2 VRRP 报文传送

当传送VRRP 报文时, 必须执行以下操作:

- 将虚拟路由器的配置状态填入到 VRRP 报文字段;
- 计算 VRRP 校验和;
- 设置源 MAC 地址为虚拟路由器 MAC 地址;
- 设置源 IP 地址为主 IP 地址接口;
- 设置 IP 协议到 VRRP;
- 发送 VRRP 报文到 VRRP IP 组播组。

注: VRRP报文使用虚拟路由器MAC地址作为源MAC地址, 以保证学习桥可以正确分配虚拟路由器连接的局域网网段。

9.3 虚拟路由器 MAC 地址

虚拟路由器的MAC地址是一个IEEE 802 MAC地址，格式如下：

00-00-5E-00-01-**{VRID}** (in hex in internet standard bit-order)

前3个字节来自IANA分配的OUI。紧接着的两个字节(00-01)表示VRRP协议。**{VRID}**是VRRP虚拟路由器标识。在一个网络上可以提供多达255个路由器。

10 执行问题

10.1 ICMP 重定向

当VRRP运行在一组路由器上时，通常可以使用ICMP重定向。这允许VRRP用在非对称的拓扑环境中。

ICMP重定向的IP源地址应该是决定下一跳路由的终端地址。如果VRRP路由器是主虚拟路由器，需要将报文重定向到其他虚拟路由器，主虚拟路由器需要判断将报文重定向到哪个虚拟路由器地址上，并选择ICMP重定向报文的地址。一个判断方法是检查目的MAC地址。

对称拓扑环境中，如果VRRP用作路由器间的负载均衡，可能需要关闭重定向功能。

10.2 主机 ARP 请求

主机向虚拟路由器的某个IP地址发送ARP请求，必须由主虚拟路由器使用虚拟路由器的虚拟MAC地址进行响应。主虚拟路由器不能使用物理MAC地址进行响应。这样无论哪个路由器作为主虚拟路由器，客户端都可以使用相同的MAC地址。

VRRP路由器重启或者启动时，不能使用物理MAC地址发送ARP消息，只能发送使用虚拟MAC地址的ARP消息。

— 当配置接口时，VRRP路由器应该广播一个 gratuitous ARP 请求，包含接口上每个 IP 地址的虚拟路由器 MAC 地址；

— 系统启动时，初始化 VRRP 操作的接口时，在 IP 地址和虚拟路由器 MAC 地址都配置完成之前，不能发送 gratuitous ARP 请求和 ARP 响应。

10.3 代理 ARP

如果VRRP路由器使用了代理ARP，VRRP路由器必须在代理ARP消息中通过虚拟路由器MAC地址。否则，会导致主机学习到VRRP路由器的真实MAC地址。

10.4 可能的转发环回

VRRP路由器不能将包转发到主虚拟路由器的IP地址，转发这些包可能会导致不必要的流量。如果是在局域网中，终端会收到自己发出的报文，引起转发环回，只能在IP TTL超期才能结束。

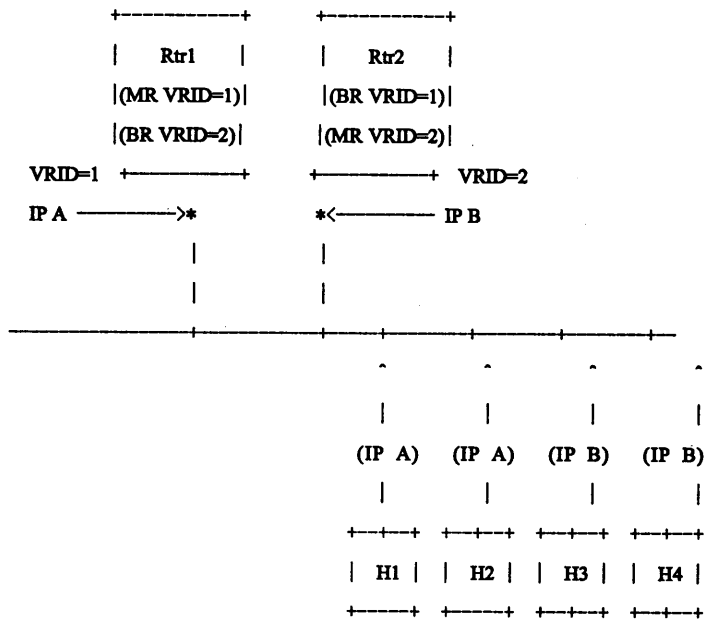
VRRP路由器采取的方法之一，是在进入或者离开MASTER状态时，对每个被采用的IP地址，增加/删除一条拒绝主机路由。

11 安全

VRRP目前不支持认证和加密。

A.2 示例 2

图A.2所示的场景是分别向两个虚拟路由器发送流量。该场景在实际部署时比较常见。



图例:

- +——+——+——+ = 以太网, 令牌环或者FDDI
- H = 主机
- MR = 主虚拟路由器
- BR = 备份虚拟路由器Backup Router
- * = IP 地址
- (IP) = 主机的默认路由器

图A.2 配置实例 2

实例2中一半主机通过Rtr1's IP A配置了静态路由, 另外一般使用Rtr2's IP B。虚拟路由器的配置和上节相同, 增加了第二个虚拟路由器来覆盖Rtr2 (VRID=2, IP_Address=B)拥有的IP地址。

Rtr2宣布时主虚拟路由器, Rtr1作为备份。本场景演示的是提供负载分离的部署情况, 两个路由器都处于可用状态, 用来满足健壮性, 提供完全的冗余备份。

广东省网络空间安全协会受控资料

中华人民共和国
通信行业标准
公众 IP 网络可靠性
虚拟路由冗余协议 (VRRP) 技术要求
YD/T 2448-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街 14 号 A 座
邮政编码: 100061

宝隆元 (北京) 印刷技术有限公司印刷
版权所有 不得翻印

*

开本: 880×1230 1/16 2013 年 5 月第 1 版
印张: 1.25 2013 年 5 月北京第 1 次印刷
字数: 29 千字

15115·96

定价: 20 元

本书如有印装质量问题, 请与本社联系 电话: (010)67114922

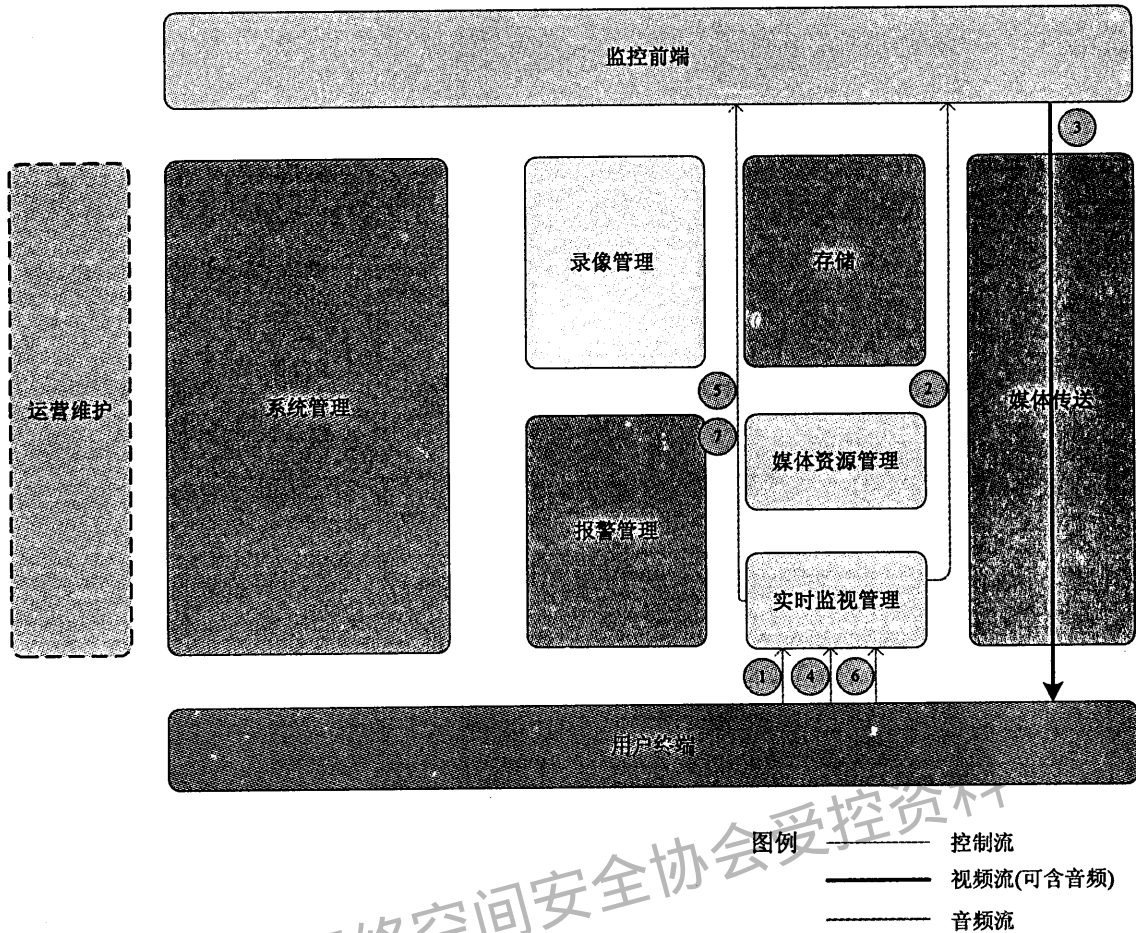


图5 实时视音频监视与云镜控制流程

- 1) 用户向平台请求访问某监控前端，请求信息中，包含监控前端的 ID；
- 2) “实时监视管理”模块检查“监控前端”的状态，确定该用户具有合法的访问权限，并且此监控前端目前可以被访问；
- 3) “实时监视管理”模块建立“监控前端”与“客户端”间的视频连接，客户端上显示实时监视画面；
- 4) 用户发起云镜控制请求，请求信息中包含控制参数；
- 5) “实时监视管理”模块对远程控制的权限进行检查后，向监控前端发送远程控制指令，监控前端于是按指令进行相应的转动；
- 6) 客户端请求停止实时监视；
- 7) “实时监视管理”向监控前端发送指令，拆除视频连接。

7.2 录像与回放

录像与回放流程如图 6 所示。

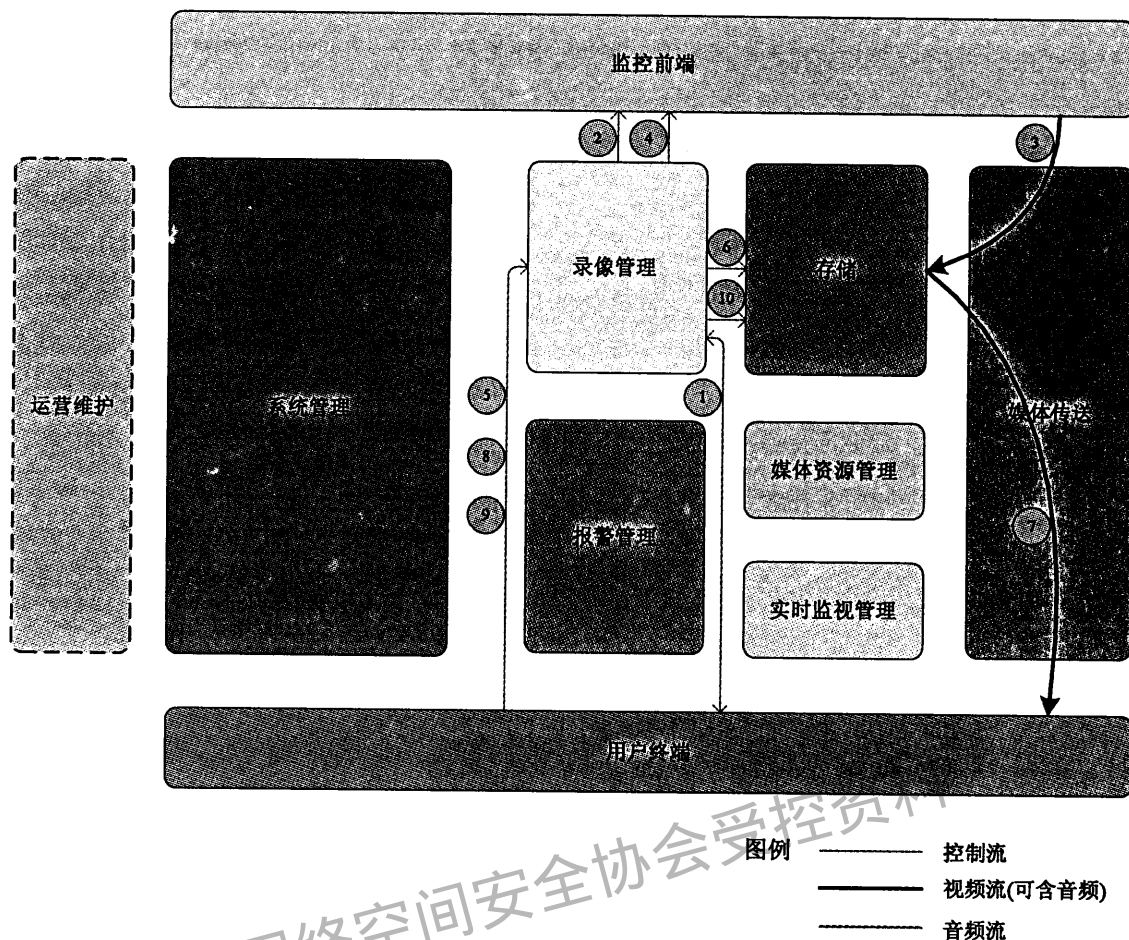


图6 录像与回放流程

- 1) 客户端向“录像管理”模块请求设定录像时间，“录像管理”模块按要求对录像时间进行设定，并给客户端确认回应；
- 2) 经过一段时间后，到了用户设定的录像时间，“录像管理”模块向监控前端发送命令，建立从监控前端到录像存储设备之间的视频通道；
- 3) 视频流从监控前端传送到指定的录像存储设备上；
- 4) 录像时间结束，“录像管理”模块向监控前端发送命令，拆除从监控前端到录像存储设备之间的视频通道；
- 5) 经过一段时间，用户请求回放录像；
- 6) “录像管理”模块向“存储”模块发送指令，建立从录像存储设备到客户端的视频通道；
- 7) 客户端接收到录像存储设备传送的录像视频，开始录像回放；
- 8) 用户请求快进、快退、暂停等操作，平台作出相应的响应；
- 9) 用户请求停止录像回放；
- 10) “录像管理”模块向“存储”模块发送指令，拆除录像存储设备到客户端的视频通道。

7.3 报警与联动

报警与联动流程如图7所示。

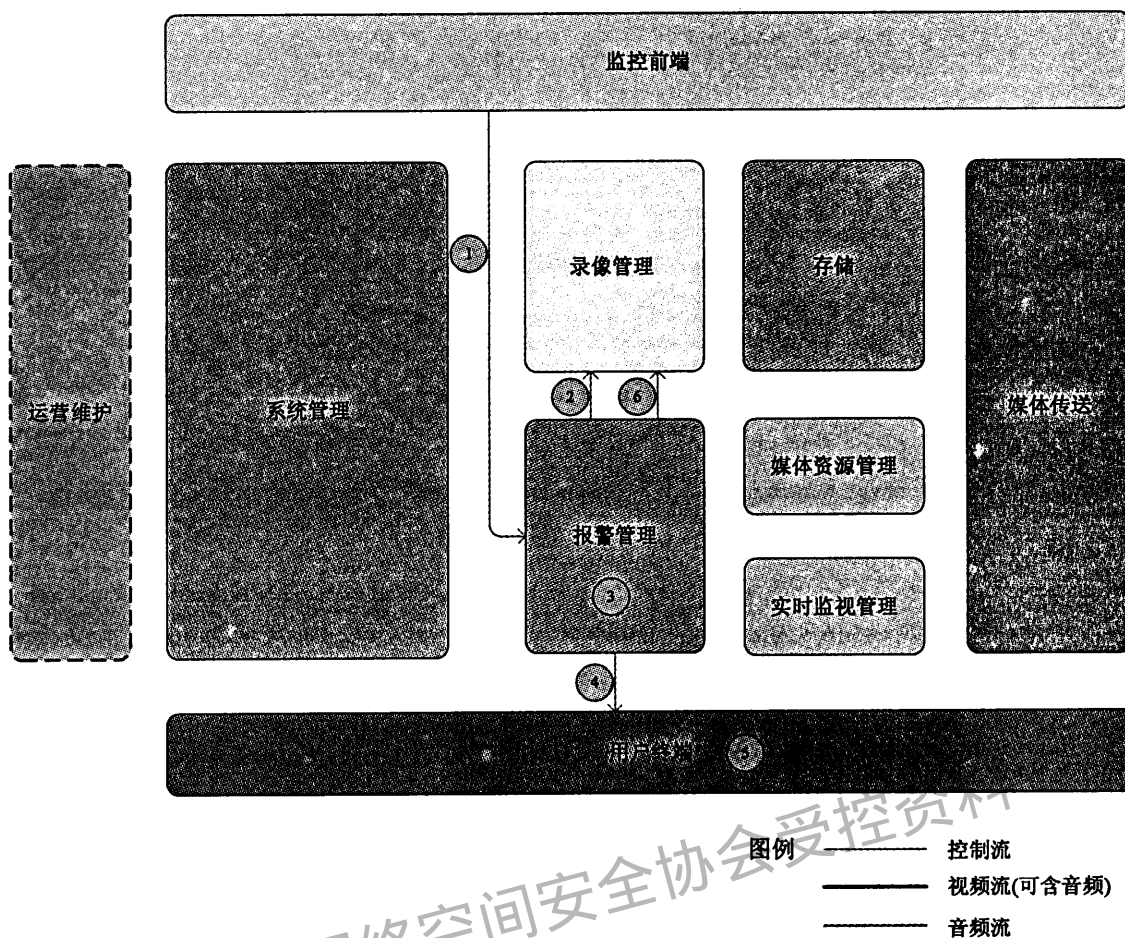


图7 报警与联动流程

- 1) 监控前端接收到报警信号（或经过智能分析，认为报警事件产生），将报警信号发送到报警管理模块；
- 2) 报警管理模块通知录像管理模块开始录像（此过程与前述的录像过程基本相同，从略）；
- 3) 报警管理模块通过多种不同的途径（本业务系统之外的通信方式）向用户发送报警消息；
- 4) 报警管理模块向客户端发送报警信息，要求客户端作出相应处理；
- 5) 客户端作出联动动作（比如，将画面切换到报警设备的联动画面，进行放大显示，并发出报警信息）；
- 6) 经过一定时间，报警管理模块通知录像管理模块停止录像。

8 性能要求

8.1 传输时延

在网络时延小于 500ms 情况下：

端到端实时媒体流传输时延小于 3s。

报警信号传输时延小于 2s。

报警处理信号传输时延小于 2s。

8.2 系统规模

同时在线的监控前端设备数大于 50000。

同时在线的客户端设备数大于 5000。

8.3 视频质量

系统应具备良好的视音频媒体质量，在实时监视与录像回放时，画面清晰流畅，无马赛克，无拖影。

9 编码要求

9.1 视频编码

视频编码可以采用以下一种或多种编码标准：

- AVS 视频；
- MPEG-2；
- MPEG-4；
- H.263；
- H.264。

9.2 音频编码

音频编码与解码采用以下一种或多种编码标准：

- G711；
- G722；
- G723；
- G728；
- G729；
- MP3；
- AMR。

9.3 文本编码

文本消息采用以下编码：

- ISO 8859-1；
- GB2312；
- UTF8。

10 设备编号

系统要求视频监控各平台设备、监控前端和用户按标准进行编号，以实现唯一标识。相应编号规则（十进制编码）如图 8 所示。

图 8 中各代码说明如下：

类别码①：见图 8 说明；

类别码②：用于区分设备为主设备还是外围设备；

1—主设备：视频服务器等负责音视频编码并向网络传送的设备；

2—外部设备：主设备连接的报警等设备。

类别码③：详细前端设备类型；

主设备：

1—DVR；

- 2—视频服务器;
- 3—IP-Camera.

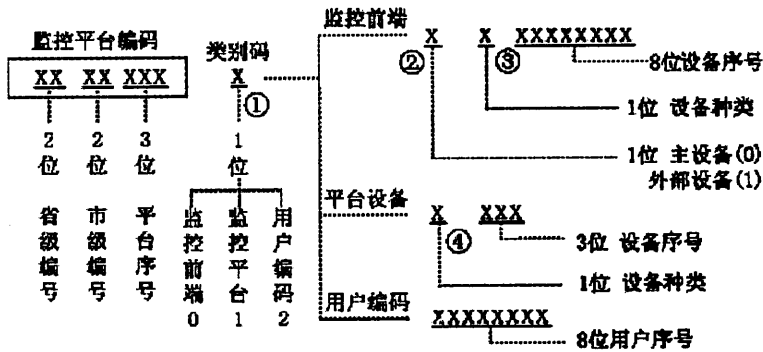


图8 终端编号示意图

外部设备:

- 1—报警采集设备;
- 2—报警输出设备;
- 3—报警采集系统;
- 4—报警联动系统;
- 5—运维支撑系统;
- 6—PSTN 系统;
- 7—统一消息系统;
- 8—其他。

类别码④: 用于区分平台设备类型

- 1—系统管理设备;
- 2—媒体传送设备;
- 3—实时监视管理设备;
- 4—录像管理设备;
- 5—存储设备;
- 6—媒体资源管理设备;
- 7—报警管理设备;
- 8—运营维护设备。

编码原则:

若只建立省级平台, 市级及市级以下编号补零, 平台序号按省级序列序号定;
若建立市级平台, 市级编号由省级运营部门自行确定。

11 通信协议

采用 IP 协议作为承载层(网络层)协议, 传输层采用 TCP 或 UDP 协议。

监控前端与客户端应当支持 PPPoE、DHCP 协议, 支持 DNS。

文件传输协议采用 TFTP、FTP 或 HTTP 协议。

音视频媒体传输采用 RTP、RTSP、RTCP 协议。

控制信令采用 SIP 协议，内容描述采用 SDP 或 XML，业务控制可以采用 HTTP+XML 协议。
网络管理采用 SNMPv2/v3 或 TR069 协议。
组播采用 IGMP 协议。

12 网络管理

网络管理范围包括监控前端设备、客户端设备、业务运营平台所涉及子系统和网络设备的管理。
网络管理必须支持拓扑管理、配置管理（版本管理）、性能管理（统计管理）、故障监控（告警管理）、日志管理、诊断测试等。
网管必须支持冗余，具有良好的稳定性和可靠性。

13 安全要求

13.1 监控前端认证

每个前端设备都应当有一个识别码或用户名、密码，经过认证系统认证授权后，才可以使用登录业务平台，认证方式应支持 AAA 认证方式或 WAP 认证。

13.2 客户端认证

客户端通过可以用户名、密码方式或 WAP 方式，经过认证系统认证授权后，才可以使用登录业务平台。客户端也可以通过 USB Key 登录系统。

13.3 媒体安全

13.3.1 媒体传输安全（可选）

前端设备应当在传输媒体数据前，对数据进行加密处理，以防止数据被未授权的用户访问。媒体的传输加密可以采用以下方式：

- a) 对编码的媒体数据采用标准加密机制，作进一步加密处理；
- b) 采用 IPSec 进行媒体数据传输。

13.3.2 媒体防篡改

在对媒体数据进行编码时，应当采用数字水印技术，对媒体数据增加水印，以防止媒体被非法篡改。

13.3.3 数字版权保护（可选）

应支持在存储监控录像的同时捆绑相应的数字版权管理信息，包括合法内容所有者的情况以及权利信息。

13.4 访问安全

用户只能访问其权限范围内的前端设备，在其权限范围内观看监控录像。

13.5 系统安全

系统应当具备故障及时恢复能力与数据备份机制，尽可能避免结构上的单点故障。

14 计费要求

系统应为业务提供丰富的计费模式。支持各种用户付费方式、计费方式、计费周期、优惠策略的灵活组合。支持灵活多变的费率优惠方式；支持按时长、包月制等多种计费方式；支持对资费的管理；支持增加新的计费策略和方式。

广东省网络空间安全协会受控资料

中华人民共和国
通信行业标准
电信网视频监控系统
第2部分：总体技术要求
YD/T 2455.2-2013

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061

宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16

2013年5月第1版

印张：1.5

2013年5月北京第1次印刷

字数：36千字

15115·104

定价：25元

本书如有印装质量问题，请与本社联系 电话：(010)67114922