VRRP和BGP在校园网中的应用研究

孙光懿[1] 刘 睿[2]

(1. 天津音乐学院网络安全和信息化办公室,天津 300171; 2. 天津音乐学院人事处,天津 300171)

摘要:本文详细阐述了虚拟路由冗余协议(VRRP)和边界网关协议(BGP)的工作原理,制定了在校园网核心层联合部署上述2种协议的网络优化方案,并给出了建立单臂路由、VRRP组、EBGP邻居、IBGP邻居和修改BGP下一跳属性、BGP本地优先级属性、权重属性的具体配置方法,测试后证实该方案很好地解决了当前校园网所面临的主要问题.

关键词:VRRP;BGP;EBGP;IBGP

中图分类号:TP393.9 **DOI**:10.19789/j.1004-9398.2020.04.004

0 引 言

随着教育信息化近20 a的发展,当今校园网已成为各院校重要的基础教学设施.不仅各类应用系统需要依托其运行(如在线教学平台、教务和自动化办公等系统),而且其还对广大师生日常的生活、学习以及教学方式产生了深远影响.当前天津音乐学院(以下简称天音)校园网虽已初具规模,但也存在着如下急需解决的问题:(1)作为校园网枢纽中心的核心层存在明显的单点故障(目前只有1台路由器),一旦出现故障必然造成整个校园网瘫痪.(2)校园网出口链路单一(只有中国教育科研网1条出口链路)且带宽不足,已无法满足广大校园网用户对互联网资源进行访问的需求.(3)校园网对网络故障的自适应能力较差,无论出口链路发生故障或核心层网络设备发生故障,都极有可能造成校园网用户数据流发生堵塞,从而出现访问互联网资源延迟较大甚至无法正常访问的现象.

为了有效解决上述问题,同时也为了最大限度的保证校园网能够安全稳定运行,拟计划采取如下措施:首先,在校园网出口处分别引入中国教育科研网和中国联通2条出口链路(每条链路带宽为500 M);其次,在校园网核心层部署2台高性能路由器;最后,在校园网核心层中联合实施基于虚拟路由冗余协议(virtual router redundancy protocol,VRRP[1-5])和边界网关协议(border gateway protocol,BGP)的网络设计方案.应用VRRP主要是为了实现3层网关冗余与流量负载均衡(在网络正常情况下,校园网内不同网段用户的数据流转发任务,将分别由不同的路由器来负责;如果某台路由器出现故障,那么另一台路由器将承担起全网用户数据流转发任务),从而有效提高校园网核心层的可靠性和2台路由器的利用率.而应用BGP主要是为了对校园网用户数据流进行路由.这样做既可以使网络管理人员更便捷地对校园网用户访问互联网资源的数据流进行有效控制(按照目标地址来选择出口链路),进而提高校园网用户访问互联网资源的速度,又可以大幅提高校园网出口链路的可靠性.

1 VRRP简介

VRRP是一种在局域网中广泛应用的标准网关容错协议,可有效提高3层网关的可靠性.其工作原理与思科私有协议(HSRP)相类似,也是将1组路由器虚拟成1台路由器,并将这台虚拟路由器的IP地址(该IP地址既可以与VRRP组中路由器的真实IP地址相同,又可不同)作为该网段各终端主机的默认网关.通常VRRP具有如下几个特点:(1)与HSRP不同,VRRP是一种开放标准协议,拥有更高的可扩展性与兼容性.如可将VRRP部署在多厂商网络设备环境中,而HSRP只能将其部署在思科网络设备中.(2)VRRP最多可支持建立255个VRRP组,但是每个VRRP组只允许有1台活跃路由器(该路由器负责处理发送到虚拟路由器上的数据包和数据帧),而备用路由器则没有具体数量限制(1台或多台均可以).(3)VRRP拥有较高的安全性,不仅支持明文认证而且还支持IP头认证(IP头

收稿日期:2019-04-09

认证可有效防止报文在传输过程中被修改). 需要特别注意的是,VRRP 组中的路由器只有先建立邻接关系,备用路由器才会收到活跃路由器发送的公告.

2　BGP 简介[6-9]

现实中的互联网是由多自治系统互联所构成的,而自治系统之间的通信则是通过 BGP 来实现的. BGP 是一种运行于 TCP 上的域间路由协议,具有高可靠性、高可扩展性、支持无类域间路由、可变长子网掩码和增量更新等特点. 其主要任务就是确保自治系统之间能够在无环路的情况下交换路由信息. BGP 按照运行位置的不同又可进一步划分为 EBGP 和 IBGP. 二者的主要区别在于:(1) EBGP 无法传递本地优先级属性,而 IBGP 可以传递;(2) EBGP 不涉及 BGP 同步问题,而 IBGP 需要考虑 BGP 同步问题;(3) EBGP 邻居路由器之间必须存在物理链接,而 IBGP 邻居路由器之间只需存在逻辑链接即可;(4) 二者避免路由环路所采取的措施不同(IBGP 通过不允许将从 IBGP 邻居学到的路由再转发给其他 IBGP 邻居这条规则来避免路由环路;而 EBGP 则是通过 AS 路径属性来避免路由环路). 需要特别注意的是:网络管理人员在实际部署 BGP 时,不仅要考虑路由器 CPU 及内存的负载能力(是否能满足日常处理 BGP 更新的需要),而且还要考虑自身对 BGP 的掌握程度.

3　仿真实验

3.1　网络拓扑构建

通过 GNS3 网络仿真平台,虚拟构建出拥有天音校园网(AS32)、中国教育科研网(AS30)、中国联通(AS31)3 个自治系统的大型网络. 其中,天音校园网自治系统由 2 台核心路由器 R3、R4,1 台 2 层交换机 SW1 以及 2 台终端计算机 C1、C2 所组成;中国教育科研网自治系统由其 1 台边界路由器 R1 所组成;中国联通自治系统由其 1 台边界路由器 R2 所组成. 网络拓扑如图 1 所示. 从该网络拓扑中不难看到:首先,校园网内共有 VLAN100、VLAN101 2 个网段且各网段用户之间可以正常通信. 核心层路由器 R3、R4 之间不仅运行 VRRP,而且还采用全互联的方式运行 IBGP. 需要说明的是:通过运行 VRRP,路由器 R3 成为 VLAN100 网段的活跃路由器,同时又成为 VLAN101 网段的备用路由器. 路由器 R4 成为 VLAN101 网段的活跃路由器,同时又成为 VLAN100 网段的备用路由器. 在校园网正常情况下,VLAN100 网段用户数据包的转发任务由核心层路由器 R3 来负责,而 VLAN101 网段用户数据包的转发任务则由核心层路由器 R4 来负责. 采用全互联的方式运行 IBGP 可以有效地避免路由黑洞、减少校园网中 IGP 传播的路由,最大限度地节省校园网带宽. 其次,ISP 边界路由器与校园网核心

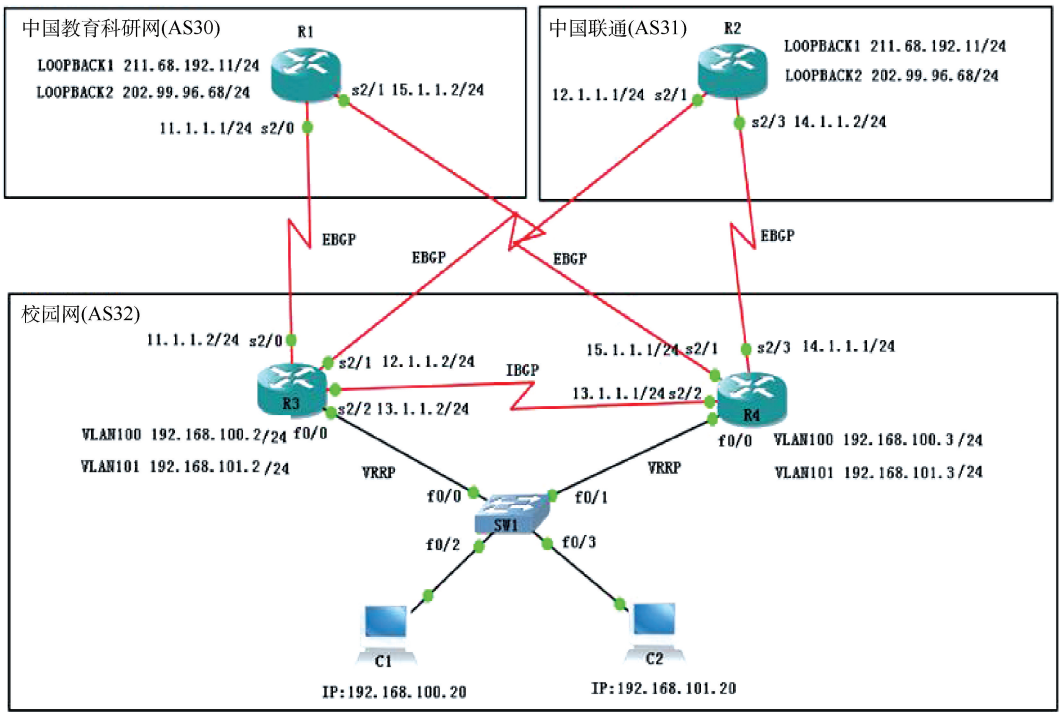


图 1　校园网网络拓扑

层 2 台路由器之间通过物理直连的方式运行 EBGP. 之所以要运行 EBGP 主要是为了让上述 3 个自治系统能够相互交换各自路由信息. 另外,为了实现对校园网用户访问互联网资源的数据流进行有效控制(在出口链路正常的情况下:当校园网用户访问中国教育科研网资源时,数据流经中国教育科研网边界路由器 R1 对目标地址进行访问;当校园网用户访问其他互联网资源时,数据流经中国联通边界路由器 R2 对目标地址进行访问. 在某条出口链路出现故障的情况下:校园网用户访问互联网资源的数据流会从另一条出口链路对目标地址进行访问). 因此,还需在校园网核心层 IBGP 路由器中修改本地优先级及权重属性.

3.2 相关设备 IP 地址分配

本次仿真实验校园网核心层路由器 R3 的 S2/0 接口与 S2/1 接口,分别与路由器 R1 的 S2/0 接口和路由器 R2 的 S2/1 接口相连;核心层路由器 R4 的 S2/1 接口与 S2/3 接口,分别与路由器 R1 的 S2/1 接口和路由器 R2 的 S2/3 接口相连. 相关设备 IP 地址分配方案如表 1 所示.

表 1 相关设备 IP 地址分配方案

设备名称	接口	IP 地址	子网掩码	网关地址
C1	SW1 f0/2	192.168.100.20	255.255.255.0	192.168.100.1
C2	SW1 f0/3	192.168.101.20	255.255.255.0	192.168.101.1
R1	s2/0	11.1.1.1	255.255.255.0	
	s2/1	15.1.1.2	255.255.255.0	
	loopback 1	211.68.192.11	255.255.255.0	
	loopback 2	202.99.96.68	255.255.255.0	
R2	s2/1	12.1.1.1	255.255.255.0	
	s2/3	14.1.1.2	255.255.255.0	
	loopback 1	211.68.192.11	255.255.255.0	
	loopback 2	202.99.96.68	255.255.255.0	
R3	s2/0	11.1.1.2	255.255.255.0	
	s2/1	12.1.1.2	255.255.255.0	
	s2/2	13.1.1.2	255.255.255.0	
	f0/0.1	192.168.100.2	255.255.255.0	
	f0/0.2	192.168.101.2	255.255.255.0	
R4	s2/1	15.1.1.1	255.255.255.0	
	s2/2	13.1.1.2	255.255.255.0	
	s2/3	14.1.1.1	255.255.255.0	
	f0/0.1	192.168.100.3	255.255.255.0	
	f0/0.2	192.168.101.3	255.255.255.0	

3.3 在校园网核心层路由器中部署 VRRP[10-12]

3.3.1 建立 VRRP 组

在校园网核心层路由器 R3、R4 中部署 VRRP,并随之建立了 VRRP100 组与 VRRP101 组. 需要说明的是:VRRP100 组的 IP 地址既为 VLAN100 网段用户的默认网关地址,同理 VRRP101 组的 IP 地址既为 VLAN101 网段用户的默认网关地址. 当校园网用户对外发起访问时,首先需将数据包发往所属网段的默认网关,而后会由 VRRP 组中的活跃路由器对这些数据包进行进一步的处理. 本文给出路由器 R3 中的 VRRP 协议配置过程(路由器 R4 的配置过程与其类似,故省略):

R3 (config-if)#int f0/0.1

R3 (config-subif)#vrrp 100 ip 192.168.100.1/设置 VLAN 100 的网关地址

R3 (config-if)#int f0/0.2

R3 (config-subif)#vrrp 101 ip 192.168.101.1/设置 VLAN 101 的网关地址

3.3.2 配置 VRRP 优先级和抢占特性

为了实现 3 层网关冗余及流量负载均衡,在这里分别将路由器 R3、R4 设置为 VRRP100 组与 VRRP101 组的活跃路由器,同时又分别将二者设置为 VRRP101 组与 VRRP100 组的备用路由器. 这样不仅校园网 3 层网关的可靠性有了大幅度提高,而且校园网流量也实现了负载均衡. 另外,为了避免当 VRRP 组中活跃路由器出现故障时,拥有最高优先级的备用路由器无法成为活跃路由器情况的出现. 因此,有必要为 VRRP 组中的路由器配置抢占特性. 在这里只给出路由器 R3 的配置过程(路由器 R4 的配置过程与其类似,故省略):

R3 (config-subif)#vrrp 100 priority 110//路由器 R3 上的 vrrp 100 组优先级为 110

R3(config-subif) #vrrp 100 preempt//配置抢占特性

R3 (config-subif)#vrrp 101 priority 105 //路由器 R3 上的 vrrp 101 组优先级为 105

R3(config-subif) #vrrp 101 preempt//配置抢占特性

上述配置完成后,查看路由器 R3 中 VRRP 组的工作状态(图 2).

可得以下结论:(1)在 VRRP100 组中,由于路由器 R3 的优先级(110)高于路由器 R4 的优先级(105),因此路由器 R3 成为校园网 VLAN100 网段的活跃路由器;而在 VRRP101 组中,由于路由器 R3 的优先级(105)低于路由器 R4 的优先级(110),因此路由器 R3 成为校园网 VLAN101 网段的备用路由器.(2)校园网 VLAN100 与 VLAN101 网段用户的默认网关地址分别为 192.168.100.1 和 192.168.101.1.

```
R3#sh vrrp bri
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/0.1            100 110 3570       Y  Master  192.168.100.2   192.168.100.1
Fa0/0.2            101 105 3589       Y  Backup  192.168.101.3   192.168.101.1
```

图 2　路由器 R3 中 VRRP 组的工作状态

3.4　配置 BGP[13-15]

3.4.1　建立 EBGP 邻居

校园网核心层路由器 R3、R4 与中国教育科研网边界路由器 R1 及中国联通边界路由器 R2 之间采用物理直连的方式运行 EBGP. 之所以采用该方式运行 EBGP,主要是从 2 台路由器之间能够顺利建立 EBGP 邻接关系角度所考虑的. EBGP 规定,必须要满足以下 3 项条件路由器之间才可建立 EBGP 邻接关系:(1)EBGP 邻居分别位于不同自治系统之中.(2)EBGP 邻居之间必要先建立 TCP 会话,再互相交换 BGP 路由表.(3)neighbor 命令中的 IP 地址必须是可达的. 在这里只给出路由器 R3 与 R1、路由器 R3 与 R2 之间的 EBGP 配置过程,路由器 R4 与 R1、路由器 R4 与 R2 之间的 EBGP 配置过程与其类似,故省略.

(1)配置路由器 R3.

R3(config)#router bgp 32

R3(config-router)#neigh 11.1.1.1 remote-as 30 //指定 EBGP 邻居

R3(config-router)#neigh 12.1.1.1 remote-as 31

R3 (config-router) # neigh 11.1.1.1 update-source s2/0 //指定 EBGP 分组的源 IP 地址

R3 (config-router) # neigh 12.1.1.1 update-source s2/1

(2)配置路由器 R1.

R1(config)#router bgp 30

R1(config-router)#neigh 11.1.1.2 remote-as 32 //指定 EBGP 邻居

R1 (config-router) # neigh 11.1.1.2 update-source s2/0 //指定 EBGP 分组的源 IP 地址

(3)配置路由器 R2.

R2(config)#router bgp 31

R2(config-router)#neigh 11.1.1.2 remote-as 32 //指定 EBGP 邻居

R2 (config-router) # neigh 11.1.1.2 update-source s2/1 //指定 EBGP 分组的源 IP 地址

3.4.2　建立 IBGP 邻居

受互联网 BGP 路由表包含路由条目数量众多的影响,在实际部署 BGP 的过程中,往往不会将其重分发到 IGP 中. 通常的做法是在自治系统内的所有路由器中运行 IBGP 并禁用 BGP 同步. 在这里只给出路由器 R3 配置 IBGP 邻居的过程(路由器 R4 配置 IBGP 邻居的过程与其类似,故省略).

R3(config)#router bgp 32

R3(config-router)#neigh 13.1.1.1 remote-as 32 //指定路由器 R4 为 IBGP 邻居

R3 (config-router) # neigh 13.1.1.1 update-source s2/2

R3 (config-router) # no synchronizat //关闭 BGP 同步

3.4.3　修改 BGP 下一跳属性

下一跳属性是 BGP 的公认强制属性,因此该属性必须出现在 BGP 路由更新之中. 需要注意的是:BGP 默认的下一跳与 IGP 默认的下一跳有所不同. BGP 默认的下一跳为去往目标地址的下一个自治系统入口 IP 地址,而 IGP 默认的下一跳为去往目标地址的下一个路由器接口 IP 地址. 举例来说,如果目标地址位于外部自治系统内,那么本自治系统内的 IBGP 路由器去往目标地址的下一跳就应为外部自治系统入口 IP 地址. 但是这样以来,就极有可能出现 IBGP 路由器丢掉前往目标分组的情况(IBGP 路由器的 IP 路由表中不存在去往外部自治系统入

口 IP 地址的路由). 因此,在部署 BGP 的过程中有必要修改其下一跳属性,将路由更新的源 IP 地址作为其下一跳地址. 在这里只给出在路由器 R3 中修改 BGP 下一跳属性的配置过程:

R3(config-router)#neigh 11. 1. 1. 1 next-hop-self //将路由更新的源 IP 地址作为下一跳地址

R3 (config-router) # neighbor 12. 1. 1. 1 next-hop-self

R3 (config-router) # neighbor 13. 1. 1. 1 next-hop-self

3. 4. 4 修改本地优先级属性

为了实现对路由器 R3 中校园网用户访问互联网资源的数据流进行有效控制,利用路由映射表技术,根据目标地址的不同对其本地优先级属性进行了相应修改. 对于来自中国教育科研网所属目标网段(例如:211. 68. 192. 0/24)的 BGP 路由更新,路由器 R3 将本地优先级设置为 110;对于来自其他目标网段的 BGP 路由更新,路由器 R3 将本地优先级设置为 180. 路由器 R3 的详细配置如下所示:

R3(config-router)#neighbor 11. 1. 1. 1 route-map skk in

R3(config-router)#neighbor 12. 1. 1. 1 route-map lzz in

R3(config)#route-map skk permit 10

R3(config-router-map)#match ip add 10

R3(config-router-map)#set local-prefer 110 //修改本地优先级值为 110

R3(config)#route-map skk permit 16

R3(config)#access-list 10 permit 211. 68. 192. 0 0. 0. 0. 255

R3(config)#route-map lzz permit 10

R3(config-router-map)#match ip add 11

R3(config-router-map)#set local-prefer 180 //修改本地优先级值为 180

R3(config)#access-list 11 deny 211. 68. 192. 0 0. 0. 0. 255 R3(config)#access-list 11 permit any

修改本地优先级属性后,路由器 R3 的 BGP 路由表如图 3 所示. 路由器 R3 去往中国教育科研网目标网段 211. 68. 192. 0/24 时,共有 3 条路由可供选择. 其中本地优先级为 110 且下一跳地址为 11. 1. 1. 1(该地址为中国教育科研网自治系统入口 IP 地址)的这条路由被选为最佳路由;而去往其他目标网段如 202. 99. 96. 0/24 时,同样共有 3 条路由可供选择. 其中本地优先级为 180 且下一跳地址为 12. 1. 1. 1(该地址为中国联通自治系统入口 IP 地址)的这条路由被选为最佳路由.

```
R3#sh ip bgp
BGP table version is 3, local router ID is 13.1.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  202.99.96.0      11.1.1.1                 0             0 30 i
* i                 13.1.1.1                 0    100      0 31 i
*>                  12.1.1.1                 0    180      0 31 i
*> 211.68.192.0     11.1.1.1                 0    110      0 30 i
* i                 13.1.1.1                 0    100      0 30 i
*                   12.1.1.1                 0             0 31 i
```

图 3 路由器 R3 的 BGP 路由表

3. 4. 5 修改权重属性

BGP 有自己独特的路由选择过程,它会首选权重值最高的 BGP 路由为最佳路由. 为了实现对路由器 R4 中校园网用户访问互联网资源的数据流进行有效控制,利用路由映射表技术,根据目标地址的不同对其权重属性进行了相应修改. 对于来自路由器 R1 的中国教育科研网所属目标网段(例如:211. 68. 192. 0/24)的 BGP 路由更新,路由器 R4 将权重值设置为 300;对于来自路由器 R1 其他网段的 BGP 路由更新,路由器 R4 将采用默认权重值;对于来自路由器 R2 的中国教育科研网所属目标网段(例如:211. 68. 192. 0/24)的 BGP 路由更新,路由器 R4 将权重值设置为 101;对于来自路由器 R2 其他网段的 BGP 路由更新,路由器 R4 将权重值设置为 600. 路由器 R4 的详细配置如下所示:

R4(config)#access-list 14 permit 211. 68. 192. 0 0. 0. 0. 255

R4(config-router)#neighbor 15. 1. 1. 2 route-map kk in

R4(config-router)#neighbor 14. 1. 1. 2 route-map kl in

R4(config)#route-map kk permit 10

R4(config-router-map)#match ip add 14

R4(config-router-map)#set weig 300 //修改权重值为 300

R4(config)#route-map kk permit 13

R4(config)#route-map kl permit 10

R4(config-router-map)#match ip add 14

R4(config-router-map)#set weig 101　//修改权重值为 101

R4(config)#route-map kl permit 18

R4(config-router-map)#set weig 600　//修改权重值为 600

修改权重属性后,路由器 R4 的 BGP 路由表图 4 所示. 路由器 R4 去往中国教育科研网目标网段 211.68.192.0/24 同样有 3 条路由可供选择,其中权重值为 300 且下一跳地址为 15.1.1.2(该地址为中国教育科研网自治系统入口 IP 地址)的这条路由被选为最佳路由;而去往其他目标网段如 202.99.96.0/24 时,其中权重值为 600 且下一跳地址为 14.1.1.2(该地址为中国联通自治系统入口 IP 地址)的这条路由被选为最佳路由.

```
R4#sh ip bgp
BGP table version is 4, local router ID is 15.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 202.99.96.0      14.1.1.2                 0             600 31 i
* i                  13.1.1.2                 0    180      0 31 i
*                    15.1.1.2                 0             0 30 i
*  211.68.192.0     14.1.1.2                 0             101 31 i
* i                  13.1.1.2                 0    110      0 30 i
*>                   15.1.1.2                 0             300 30 i
```

图 4　路由器 R4 的 BGP 路由表

4　仿真测试[16]

4.1　网络正常情况下测试

首先,使用 PING 命令测试校园网终端计算机 C1 与 C2 之间的连通性;其次,以终端计算机 C1 为例,使用 trace 命令分别测试访问目标地址 211.68.192.11/24 与 202.99.96.68/24 的路由过程. 最后,使用 sh ip route 命令分别查看路由器 R3 及路由器 R4 的路由表.

(1)测试终端计算机 C1 与 C2 之间的连通性.

VPCS[1] > ping 192.168.101.20

192.168.101.20 icmp_seq = 1 ttl = 254 time = 94.566 ms

192.168.101.20 icmp_seq = 2 ttl = 254 time = 84.387 ms

192.168.101.20 icmp_seq = 2 ttl = 254 time = 63.829 ms

(2)使用 trace 命令分别测试访问中国教育科研网所属目标地址 211.68.192.11/24 和中国联通所属目标地址 202.99.96.68/24 的路由过程.

VPCS[1] > trace 211.68.192.11

trace to 211.68.192.11, 8 hops max, press Ctrl + C to stop

1　192.168.100.2　63.904 ms　10.193 ms　12.603 ms

2　11.1.1.1　59.091 ms

VPCS[1] > trace 202.99.96.68

trace to 202.99.96.68, 8 hops max, press Ctrl + C to stop

1　192.168.100.2　41.704 ms　45.793 ms　31.513 ms

2　12.1.1.1　77.004 ms

(3)使用 sh ip route 命令查看路由器 R3 的路由表(图 5).

(4)使用 sh ip route 命令查看路由器 R4 的路由表(图 6).

```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B     202.99.96.0/24 [20/0] via 12.1.1.1, 08:03:04
B     211.68.192.0/24 [20/0] via 11.1.1.1, 08:02:39
      11.0.0.0/24 is subnetted, 1 subnets
C        11.1.1.0 is directly connected, Serial2/0
      12.0.0.0/24 is subnetted, 1 subnets
C        12.1.1.0 is directly connected, Serial2/1
      13.0.0.0/24 is subnetted, 1 subnets
C        13.1.1.0 is directly connected, Serial2/2
C     192.168.100.0/24 is directly connected, FastEthernet0/0.1
C     192.168.101.0/24 is directly connected, FastEthernet0/0.2
```

图 5　路由器 R3 的路由表

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B     202.99.96.0/24 [20/0] via 14.1.1.2, 07:40:10
B     211.68.192.0/24 [20/0] via 15.1.1.2, 07:40:10
      13.0.0.0/24 is subnetted, 1 subnets
C        13.1.1.0 is directly connected, Serial2/2
      14.0.0.0/24 is subnetted, 1 subnets
C        14.1.1.0 is directly connected, Serial2/3
C     192.168.100.0/24 is directly connected, FastEthernet0/0.1
      15.0.0.0/24 is subnetted, 1 subnets
C        15.1.1.0 is directly connected, Serial2/1
C     192.168.101.0/24 is directly connected, FastEthernet0/0.2
```

图 6　路由器 R4 的路由表

测试后可得以下结论:(1)校园网 VLAN100 网段所属终端计算机 C1 与 VLAN101 网段所属终端计算机 C2 之间可以实现正常通信.(2)实现了校园网3 层网关冗余与流量负载均衡,校园网核心层路由器 R3 不仅是 VLAN100 网段的活跃路由器,而且还是 VLAN101 网段的备用路由器,另一台校园网核心层路由器 R4 不仅是 VLAN100 网段的备用路由器,而且还是 VLAN101 网段的活跃路由器.(3)实现了对校园网用户访问互联网资源的数据流进行有效控制.当终端计算机 C1 访问中国教育科研网资源时,数据流会先被发往 VLAN100 网段的活跃路由器 R3,而后经中国教育科研网边界路由器 R1 到达目标地址.而当终端计算机 C1 访问其他互联网资源时,虽然数据流也会先被发往 VLAN100 网段的活跃路由器 R3,但是需经中国联通边界路由器 R2 到达目标地址.同理,当终端计算机 C2 访问中国教育科研网资源时,数据流会先被发往 VLAN101 网段的活跃路由器 R4,而后经中国教育科研网边界路由器 R1 到达目标地址.而当终端计算机 C2 访问其他互联网资源时,虽然数据流也会先被发往 VLAN101 网段的活跃路由器 R4,但是需经中国联通边界路由器 R2 到达目标地址.

4.2　网络故障情况下测试

在这里模拟中国教育科研网边界路由器 R1 出现故障.与此同时以终端计算机 C1 为例,对其与终端计算机 C2 的连通性以及访问目标地址 211.68.192.11/24 与 202.99.96.68/24 的路由过程进行再次测试,并查看校园网核心层路由器 R3、R4 中 VRRP 组的工作状态.

测试后可得以下结论:(1)VLAN100 网段所属终端计算机 C1 与 VLAN101 网段所属终端计算机 C2 之间仍然可以实现正常通信.(2)校园网核心层路由器 R3、R4 中 VRRP 组的工作状态未发生任何变化.(3)校园网用户仍然可对互联网资源进行正常访问.当终端计算机 C1 访问互连网资源时,数据流会先被发往 VLAN100 网段的活跃路由器 R3,而后经中国联通边界路由器 R2 到达目标地址.同理,当终端计算机 C2 访问互联网资源时,数据流会先被发往 VLAN101 网段的活跃路由器 R4,而后经中国联通边界路由器 R2 到达目标地址.

5　结束语

通过在校园网核心层中联合部署虚拟路由冗余协议和边界网关协议,不仅提高了 3 层网关与出口链路的可靠性,而且还实现了对校园网用户访问互联网资源数据流的有效控制.即使校园网内某台核心交换机或某条出口链路发生故障,校园网用户对互联网资源的访问也不会受到任何影响.校园网经过此次改造后,用户的满意度也有了明显的提升.

参 考 文 献

[1] 崔北亮. CCNA 认证指南(640 - 802)[M]. 北京:电子工业出版社,2009.

[2] KARL S. CCIE 实验指南[M]. 北京:人民邮电出版社,2010:75 - 100.

[3] 王隆杰. 思科网络实验室 CCNP 实验指南[M]. 北京:电子工业出版社,2012.

[4] TEARE D. CCNP router (642 - 902)[M]. 北京:人民邮电出版社, 2011.

[5] TEARE D, VACHON B, GRAZIANI R. CCNP route 300 - 101 学习指南[M]. 北京:人民邮电出版社, 2016.

[6] 孙光懿,郭建忠. VRRP 和 SLA 协议在校园网中的应用[J]. 西华大学学报(自然科学版),2019(2):12 - 18.

[7] 孙光懿. 基于 HSRP 和 STP 协议的网络冗余仿真[J]. 首都师范大学学报(自然科学版),2018,39(3):16 - 23.
[8] 涂朴,赵全军,李斌. 无线自组织网络的改进 MGD 分组调度算法[J]. 首都师范大学学报(自然科学版),2018,39(4):36 - 41.
[9] 孙光懿. 基于 VRRP 和 NAT 多出口校园网可靠性仿真试验设计[J]. 中央民族大学学报(自然科学版),2017,26(3):45 - 53.
[10] 贺聿志,章勇,柳斌. 多链路 BGP 接入方法的探讨[J]. 华中科技大学学报(自然科学版),2016,44(增刊 1):148 - 151.
[11] 李道丰,王高才,王志伟,等. 标准模型下可证明安全的 BGP 路由属性保护机制[J]. 计算机学报,2015,38(4):859 - 871.
[12] 孙杰. BGP 路由策略冲突引发的路由振荡研究[D]. 成都:电子科技大学,2014.
[13] 郑庆棠. 基于仿真平台的典型动态路由协议攻击技术研究[D]. 北京:北京邮电大学,2014.
[14] 陈石,刘金生. BGP 协议防御 DDoS 攻击的方法浅析[J]. 微型机与应用,2016,35(24):5 - 7.
[15] 卢作维. BGP 异常事件与数据业务异常事件的关联分析[D]. 北京:北京邮电大学,2018.
[16] 孙光懿. 基于访问控制列表技术的仿真实验设计[J]. 伊犁师范学院学报(自然科学版),2018,12(3):53 - 58.

Application of VRRP and BGP in Campus Network

SUN Guangyi[1] LIU Rui[2]

(1. Office of Network Security and Information, Tianjin Conservatory of Music, Tianjin 300171;
2. Personnel Department of Tianjin Conservatory of Music, Tianjin 300171)

Abstract: This paper elaborates the working principle of virtual router redundancy protocol (VRRP) and border gateway protocol(BGP) in detail. And the network transformation scheme for the joint deployment of the two protocols in the core layer of the campus network is given. The network optimization scheme of deploying the above two protocols in the core layer of campus network is given. The configuration methods of establishing router-on-a-stick, VRRP group, EBGP neighbor, IBGP neighbor, next-hop attributes of BGP, local priority attributes of BGP and weight attributes are elaborated in detail. After testing, it is proved that this scheme has solved the main problems faced by the current campus network well.

Keywords: VRRP; BGP; EBGP; IBGP