

# 广域网中基于 BGP 专线和 VPN 共享网络系统

## The Research and Realization of Wan Based on VPN And BGP

周晓林 (安徽省气象台 合肥 230031)

丁以英 (安徽气象科技开发中心 合肥 230061)

**摘要:**通过对当今较为流行的基于 BGP 协议的专线宽带和基于 VPN 技术的共享宽带两种方式的研究,在广域网上实现了基于 BGP 路由协议的专线宽带和基于 VPN 技术的共享宽带方式两种数据的数据传输,可根据不同的需求选择不同的组网方式。再在同时拥有 BGP 和 VPN 的局域网的端节点上增加相关路由,实现 BGP 专线和 VPN 共享网络系统互连。

**关键词:**广域网 VPN BGP 路由协议 系统互连

### 1 前言

广域网端到端的对接通常使用路由技术。路由器工作于 OSI 网络七层模型的第三层——网络层,其基本功能可概括为路由和交换。路由是指选择信息传送的最佳路径,以提高通信速度,减轻网络负担,交换是指路由器能够连接不同结构、不同协议的多种网络,在这些网络之间传输信息。广域网技术种类有很多,可根据不同的需求选择不同的组网方式。当今较为流行的有基于 BGP 协议的专线宽带和基于 VPN 技术的共享宽带方式两种方式,下面介绍基于 BGP 路由协议的专线宽带和基于 VPN 技术的共享宽带方式两种方式在本单位数据通信方面的具体应用。

### 2 基于 BGP 路由协议专线方式

广域网的专线方式的路由协议有很多,但在大型网络连通中 BGP 路由协议以其先进的性能为广大用户所采用,下面分别介绍 BGP 基本原理、BGP 邻居、BGP 连接和具体配置。

#### 2.1 BGP 路由协议的基本原理

边界网关协议 BGP (Border Gateway Protocol) 是在自治系统内部使用的路由协议。边界指的是自治系统的边界,用于在自治系统间传播路由信息。BGP 通过在路由信息中增加自治系统路径和其他附属性信息,来构造自治系统的拓扑图,从而消除路由环路,实施用户配置的策略。其着眼点是选择好的路由并控制路由的传播,而不在于发现和计算路由。发现和计算路由是 IGP (内部网关协议) 的事。BGP 要求每一个自

治系统都有一个唯一的编号。从 BGP 的观点来看,整个 Internet 就是通过边界网关连接起来的多个自治系统。

#### 2.2 BGP 邻居

BGP 邻居又称为对等体,可将 BGP 邻居分为两种:第一种是 EBGP 对等体 (External BGP),如果两个交换 BGP 报文的对等体属于不同的自治系统,那么这两个对等体就是 EBGP 对等体,第二种是 IBGP 对等体 (Internal BGP),如果两个交换 BGP 报文的对等体属于相同的自治系统,那么这两个对等体就是 IBGP 对等体。一个自治系统内的不同边界路由器的不同边界路由器之间也要建立 BGP 连接,只有这样才能实现路由信息在整个自治系统内的传递。BGP 中邻居通常通过静态定义,它们依靠建立 TCP 连接形成邻居关系。如果 BGP 的状态是 ESTABLISHED,表明邻居关系已形成。

#### 2.3 BGP 连接

如果两个对等体位于两个自治系统,并且它们之间是直接相连的,就将它们称为 EBGP。位于同一自治系统的 BGP 路由器建立连接,称为 IBGP 连接。此时对等体不需要直接相连,只要 TCP (传输控制协议) 连通就可以了。一条路由在一般情况下是从自治系统内部产生的,它是由某种内部路由协议发现和计算,然后传递到自治系统的边界,再由自治系统边界路由器 (AS-BR) 通过 EBGP 连接传播到其它自治系统中。路由在传播过程中可能会经过若干个自治系统,这些自治系统称为过渡自治系统。若在过渡自治系统内有多个边界路由器,那么这些路由器之间就运行 IBGP 来交换路

由信息。这时内部路由器并不需要知道这些外部路由器,它们只需要在边界路由器之间维护 IP 连通性即可。路由到达自治系统边界后,若内部路由器需要知道这些外部路由,可由自治系统边界路由器将这些路由引入内部路由器协议。外部路由的数量是很大的,通常会超出内部路由器的处理能力,因此引入外部路由时一般需要过滤或集合,以减少路由的数量。

## 2.4 BGP 路由

BGP 执行 3 类路由:自治系统间路由、自治系统内部路由和贯穿自治系统路由。发生在不同自治系统的两个或多个 BGP 路由器之间的路由称为自治系统间路由,这些系统的对等路由器利用 BGP 来维护一致的网络拓扑视图,在自治系统之间通信的 BGP 邻居必须在相同的物理网络之内。Internet 就是使用这种路由的实例,因为它由多个自治系统构成,BGP 一个最重要的用途就是用于为 Internet 中提供最佳路由。发生在同一自治系统的两个或多个 BGP 路由器之间的路由称为自治系统内路由,统一自治系统内的对等路由器使用 BGP 来维护一致的拓扑视图。也可用 BGP 来决定将哪个路由器作为外部自治系统的连接点。贯穿自治系统路由发生在通过不运行 BGP 的自治系统交换数据的两个或多个 BGP 对等路由器间。在贯穿自治系统环境中,使用 BGP 通信的双方都不在自治系统内,BGP 必须与自治系统内使用的路由协议交互以成功地通过该自治系统传输 BGP。

## 2.5 BGP 路由协议具体配置

下面以两台华为 NE08 路由器 (R1、R2) 基于 BGP 路由协议专线方式的设置为例:

安徽省气象台 (R1) 的基本配置

```
sysname behfne08a // R1 系统名称和 password。
```

```
super password level 3 simple huawei
```

```
#
local - user huawei password simple huawei // R1 的
用户名和 password,
```

```
local - user huawei level 3
```

```
#
router id 192.168.205.72 // router id 的 ip address 配
置。
```

```
#
interface Ethernet3/2/0 // 以下为 R1 四个端口的 ip
address 配置。
```

```
ip address 202.16.100.10 255.255.255.0
```

```
interface Ethernet4/2/0
```

```
ip address 202.21.80.161 255.255.255.0 //内网端
口的 ip address
```

```
firewall packet - filter 3000 inbound
```

```
interface Ethernet5/2/0
```

```
ip address 10.129.3.1 255.255.255.0
```

```
interface Serial5/1/0:0
```

```
link - protocol ppp
```

```
description to_babane40a_s33
```

```
ip address 10.129.0.2 255.255.255.252 //外网端
口的 ip address
```

```
#
```

```
interface LoopBack0 // R1 的 LoopBack0 ip address 配
置
```

```
ip address 192.168.205.72 255.255.255.255
```

```
#
```

```
bgp 65015 //启动 BGP,65015 为本地的自治系统号。
```

```
network 10.129.3.0 255.255.255.0 //为 BGP 注入路
由。10.129.3.0 255.255.255.0
```

```
network 172.21.80.0 255.55.255.0 //和 172.21.80.
0 255.55.255.0 为局域网地址。
```

```
peer 192.168.205.1 as - number 65000 //建立 EBGP
邻居,65000 为对端的自治系统号。
```

```
peer 192.168.205.1 ebgp - max - hop 2
```

```
peer 192.168.205.1 connect - interface LoopBak0
```

其它异地城市对接路由器 (R2) 配置方法同上。上面的配置为基本配置,完成基本配置就可以在异地城市通过路由器进行通信。还可以通过路由过滤、BGP 聚合、BGP 反射、BGP 联盟和路由策略等方法来解决实际工作遇到的复杂的通信问题。

## 3 基于 VPN 技术广域网的路由协议设置

近来 VPN 技术采用组建企业虚拟专用网来提高了速率、稳定性、安全性和价格上看具有传统网络无可比拟的优势,已有越来越多的用户,本单位现在就是采用这一技术。下面仅以基于 VPN 技术来实现异地路由器对接。(采用两台华为路由器:R3、R4)其配置要同时支持 GRE 和 IPsec 协议。配置以省气象台:内部网段网号 (202.21.80.0);互连网段网号 (218.22.10.0);

路由器内部端口 IP 地址 (202.21.81.250);路由器 Internet 端口 IP 地址 (218.22.10.171);隧道端口 IP

地址(192.168.1.1)与亳州市气象局:内部网段网号(202.21.95.0);互连网段网号(218.22.248.0);路由器内部端口 IP 地址(202.21.95.254);路由器 Internet 端口 IP 地址(218.22.248.82);隧道端口 IP 地址(192.168.1.2)互连为例。

### 3.1 对于路由器 R3:省气象台端配置如下:

```
access-list normal 101 permit ip 202.21.0.0 0.0.255.255 202.21.0.0 0.0.255.255 (访问控制列表 101,供 Vpn 使用)
```

```
access-list normal 101 deny ip any any (访问控制列表 101,供 Vpn 使用)
```

```
hostname behf (路由器名称)
```

```
crypto IPsec transform tran (设定 IPsec 加密验证组,选择加密方式)
```

```
esp-new hash sha1-hmac-96
```

```
!
```

```
crypto map map_102 10 manual (设定 Vpn 通道验证方式,及验证密码)
```

```
match address 101 (引用访问列表)
```

```
set transform tran(引用转换方式)
```

```
set local-address 192.168.1.1(设置本端地址)
```

```
set peer 192.168.1.2(设置对端地址)
```

```
set session-key inbound esp spi 58102 (设置 SPI)
```

```
set session-key inbound esp string-key bfbz (设置密钥)
```

```
set session-key outbound esp spi 58321
```

```
set session-key outbound esp string-key behf
```

```
!
```

```
interface Ethernet0 (外网接口设置)
```

```
speed auto
```

```
duplex auto
```

```
no loopback
```

```
description internet
```

```
ip address 218.22.10.171 255.255.255.240
```

```
nat inside 110 interface
```

```
!
```

```
interface Ethernet1 (内网接口设置)
```

```
speed auto
```

```
duplex auto
```

```
no loopback
```

```
ip address 202.21.81.250 255.255.255.0
```

```
interface Tunnel102 (设置 Vpn 隧道,引用验证方式)
```

```
encapsulation tunnel
```

```
description bfbz
```

```
ip address 192.168.1.1 255.255.255.252
```

```
crypto map map_102
```

```
tunnel source 218.22.10.171
```

```
tunnel destination 218.22.248.82
```

```
!
```

```
exit
```

```
ip route 0.0.0.0 0.0.0.0 218.22.10.161 preference
```

60 (默认路由)

```
ip route 202.21.95.0 255.255.255.0 Tunnel 102 preference 60 到亳州市气象台路由。!
```

3.2 对于亳州市路由器(R4)配置方法与上述相同,具体配置省略。

## 4 实现 BGP 专线和 VPN 共享网络系统互连

在广域网上实现了基于 BGP 路由协议的专线宽带和基于 VPN 技术的共享宽带两种方式的数据传输之后,需要在配置 BGP 路由协议路由器(R1)上增加路由 network 202.21.95.0 255.55.255.0 和 ip route-static 202.21.95.0 255.255.255.0 202.21.80.161 preference 60;需要在配置 VPN 路由器(R3)上增加一条 ip route 10.129.0.0 255.255.255.0 202.21.80.161 路由,同时在局域网交换机中也要进行必要路由配置(202.21.80.0 和 202.21.81.0 网段之间进行交换)。完成上述路由配置之后,便可以在 BGP 专线和 VPN 共享网络中传输数据,实现系统 BGP 专线和 VPN 共享网络系统互连。

## 5 结束语

广域网中是采用基于 VPN 共享式还是采用 BGP 专线式网络的方式,这要根据具体情况而定,如果申请的线路是共享式宽带,那么采用 VPN 技术是一种很好的选择,这是因为 VPN 是加密的,VPN 数据包在广域网中传输时,广域网上的用户只看到公用的 IP 地址,看不到 VPN 使用的协议;VPN 技术减少租用运营商 WAN 带宽的费用;能使用灵活的拓扑结构,包括全网状连接。如果申请的线路是专线式宽带,那么采用 BGP 技术是一种很好的选择,这是因为 BGP 最重要的用途可体现在为不同城市之间的各类局域网(多个自治系统)中需要在广域网中相互通信的网络中控制路由的

(下转第 82 页)

(上接第 77 页)

传播、提供最佳路由和只发送增加路由,大大减少了传播路由所占用的带宽,适用于广域网上传播大量的路由信息。除此之外,BGP 还有着丰富的路由策略控制手段。

### 参考文献

- 1 周晓林等,《广域网下不同操作系统之间的批文件自动定时互相传输》,成都:计算机应用研究,2005 年增刊。
- 2 SYNGRESS MEDIA 公司著, Cisco 局域网交换配置技

术,机械工业出版社,2000.6。

- 3 蔡晓东,计算机网络技术,西安 西安电子科技大学出版社,1998.2。
- 4 黄永峰、阙勇、刘宪军、权进国等, Windows / Unix / Linux 综合组网技术,北京:清华大学出版社,2002.7。
- 5 华为技术有限公司,《Quidway NetEngine16E/08E/05 路由器用户手册-配置指导二分册》。
- 6 安徽华脉网络有限公司,《VPN 实验系统配置指导手册》。