4 路由技术基础与安全点

4.1 路由理解

简单来说是负责 IP 包的转发，向其它的网络转发

4.2 路由协议

路由协议主要运行于路由器上，路由协议是用来确定到达路径的，它包括 RIP,IGRP(Cisco 私有协议),EIGRP(Cisco 私有协议),OSPF,IS-IS,BGP。起到一个地图凸导航，负责找路的作用。它工作在网络层。

1)RIP、IGRP、EIGRP、OSPF、IS-IS 是内部网关协议(IGP),适用于单个 ISP 的统一路由协议的运行，一般由一个 ISP 运营的网络位于一个 AS(自治系统)内，有统一的 AS number(自治系统号)

2) BGP 是自治系统间的路由协议，是一种外部网关协议，多用于不同 ISP 之间交换路由信息，以及大型企业、政府等具有较大规模的私有网络。

4.3 安全点(共性)

如果在数据包传递过程中，协议出现漏洞，那么容易被人利用，给网络安全造成严重影响。

1) BGP:采用 TCP 传输，会导致出现关于 TCP 的诸多问题，如序列号猜测、SYNFLOOD、拒绝服务、伪造报文等。解决办法：在核心网的出口应用，配置密码认证。相对来说，BGP 协议的安全性较高。

2)OSPF:用的比较多的一种协议，报文超大且领导列表过长，容易消耗资源；upadate 报文攻击；hello 报文攻击；解决办法：增加验证，加密认证机制。设计入侵检测系统。

3)RIPV2:采用明文和密文安全机制，相对来说安全性还可以。

4.4 常见用法

1)接口路由配置

[routeAJinterface GigabitEthernet 0/0/1

[routeA-GigabitEthernet°/0/1Jip address 192.168.20.2255.255.255.224

2)静态路由【路由器、核心交换机】

```
ip route-static 192.168.10.0 255.255.255.0 192.168.20.2
ip route-static 192.168.100.0 255.255.255.0 192.168.20.2
```

3)默认路由【核心交换机配置】

ip route-static 0.0.0.00.0.0.0192.168.20.2

4)策略路由【路由器、核心交换机】

```
# 可以用ACL或IP prefix-list。这里建议ACL，比较简单；而IP prefix-list略显复杂。
[R5]acl 2000
[R5-acl-basic-2000]rule permit source 33.1.1.1 0
[R5-acl-basic-2000]rule permit source 33.2.2.2 0
[R5-acl-basic-2000]rule permit source 33.3.3.3 0
[R5-acl-basic-2000]dis th
[V200R003C00]
#
acl number 2000
 rule 5 permit source 33.1.1.1 0
 rule 10 permit source 33.2.2.2 0
 rule 15 permit source 33.3.3.3 0
#
return
[R5-acl-basic-2000]q
[R5]route-policy ospf permit node 10
Info: New Sequence of this List.
[R5-route-policy]if-match acl 2000
[R5-route-policy]apply cost 10
[R5-route-policy]apply cost-type type-1
[R5-route-policy]dis th
[V200R003C00]
#
route-policy ospf permit node 10
 if-match acl 2000
 apply cost 10
 apply cost-type type-1
#
return
```