组合六（新TOP）

2020年3月15日 10:07

组合六：

理论：NAT-ALG（FTP主动被动模式）、 PPP

项目：如下场景需要进行哪些配置

NAT-ALG（FTP主动被动模式）

FTP协议是一个典型的多通道协议，在其工作过程中，FTP Client和FTP Server之间将会建立两条连接：控制连接和数据连接。

控制连接用来传输FTP指令和参数(用户名、密码、模式协商)，其中就包括建立数据连接所需要的信息（端口信息）；

数据连接用来获取目录及传输数据。

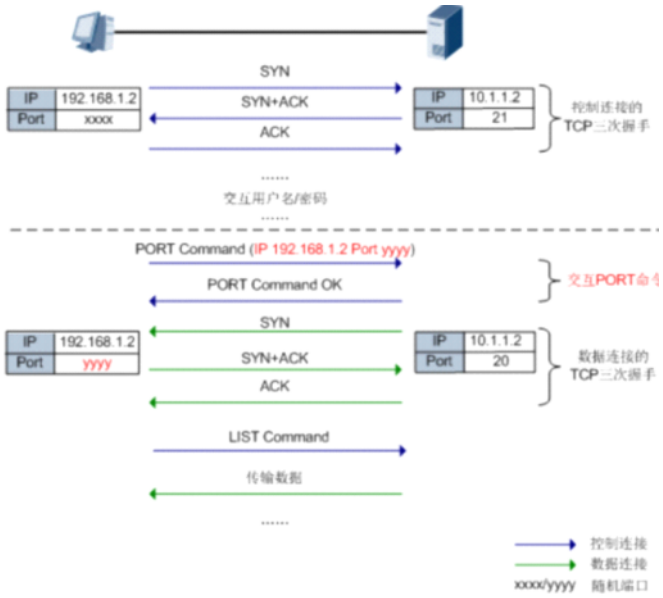
数据连接使用的端口号是在控制连接中临时协商的。

根据数据连接的发起方式FTP协议分为两种工作模式（模式由FTP客户端设置）：主动模式（PORT模式）和被动模式（PASV模式）。

主动模式中，FTP Server主动向FTP Client发起数据连接；

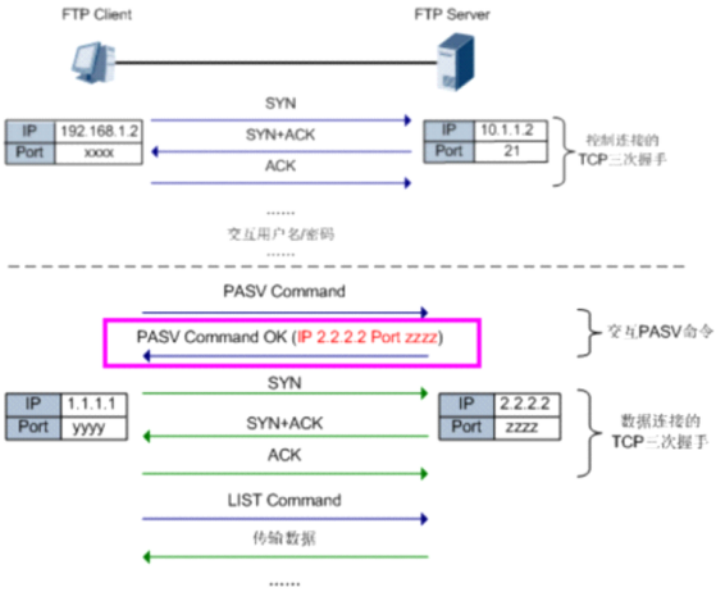
被动模式中，FTP Server被动接收FTP Client发起的数据连接。

主动模式的协议交互流程如下：



首先FTP客户端(源端口号xxxx)向FTP服务器的21端口发起连接建立控制连接，然后客户端通过控制连接发送PORT命令协商客户端使用的数据连接传输端口号（yyyy）。协商成功后，服务器主动使用20端口向客户端的这个端口号发起数据连接

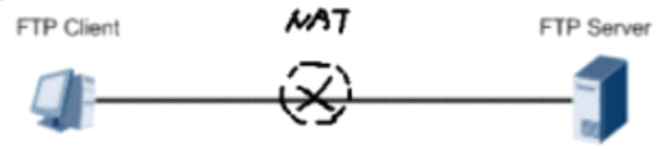
被动模式的协议交互流程如下：



首先FTP客户端(源端口号xxxx)向FTP服务器的21端口发起连接建立控制连接，然后服务器通过控制连接发送PASV命令发送服务器使用的数据连接传输端口号（zzzz）。协商成功后，客户端使用随机端口号yyyy（一般为xxxx+1）向服务器的端口zzzz发起数据连接。

出现的问题：

如图客户端在内网，服务器在外网，路由器部署NAT，且FTP采用主动模式的场景：



客户端通过已经建立好的控制连接发送PORT消息给服务器，告知服务器分配的端口号yyyy，服务器使用20端口访问yyyy建立数据连接，而路由器上并不存在yyyy对应的端口映射表项，所以数据连接无法建立，会出现可以验证用户密码，但是无法获取目录列表的现象。

解决方案：

路由器上开启NAT-ALG（应用层网关），可以识别控制连接中的PORT消息并自动创建yyyy端口的映射表项，保证数据连接可以正常建立

路由器上开启NAT-ALG（应用层网关），可以识别控制连接中的PORT消息并自动创建yyyy端口的映射表项，保证数据连接可以正常建立

PPP-------老题了，不需要多说什么了

分析：

建链过程

LCP------MRU、魔术字、认证、多链路协商

认证-----PAP、 CHAP

NCP-----协商地址、下发地址过程

追问：

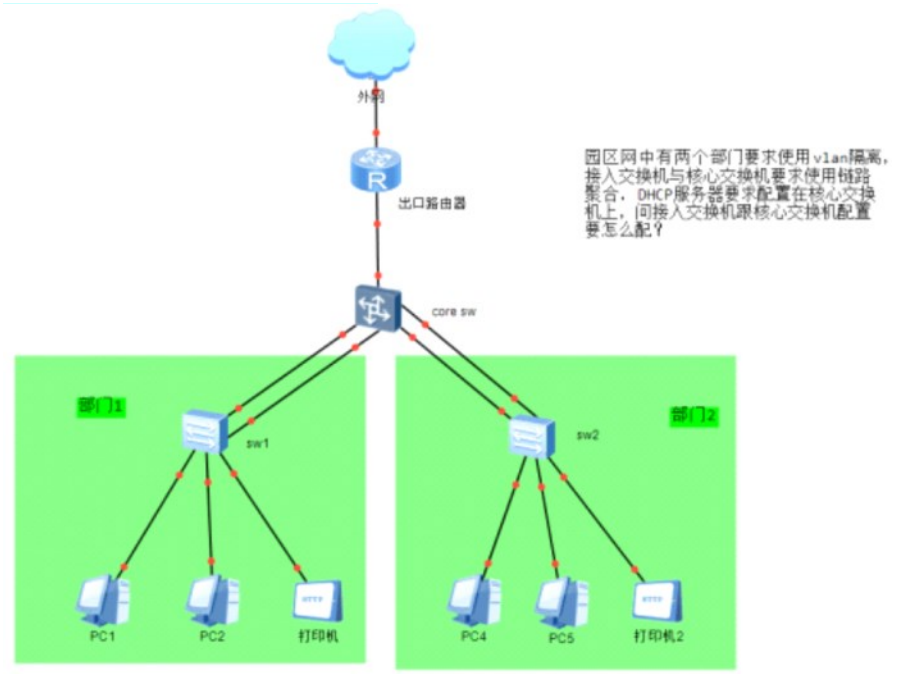
1、 PPPOE

2、 PPPoE的MTU?

3、 PPPoE和NAT如何同时配置?

4、局域网接入如何支持认证？---NAC（网络接入控制）

项目：如下场景需要进行哪些配置



分析：

1、Trunk、Access基本配置没问题

2、Core SW配置VLANif 作为网关 配置DHCP地址池 VLANIF开启dhcp select global，存在打印机则需要保留地址

3、接入交换机开启dhcp snooping，配置信任接口

4、目前网络存在单点故障问题，可以增加SW部署VRRP等技术或者直接堆叠

5、 如果部署多链路、设备互联等技术 还得考虑二层防环技术

自行把相关实验敲一下

追问：

1、内网如何访问外网？

2、如果部署IP电话，接入层如何配置？

3、语音流量的DSCP值一般为多少？---46

4、打印机分配固定IP地址如何配置？

5、 DHCP snooping介绍下？

6、 DHCP服务器如何配置在路由器上，应该注意什么？