[TCP和UDP协议 2](#_Toc643257236)

[TCP 2](#_Toc1757453759)

[UDP 2](#_Toc1500796334)

[TCP的三次握手与四次断开 2](#_Toc259342467)

[UDP 3](#_Toc780892898)

[访问控制列表概述 4](#_Toc1174606877)

[访问控制列表（ACL）： 4](#_Toc85684801)

[扩展访问控制列表 5](#_Toc442721385)

[NAT（网络地址转换） 6](#_Toc535643040)

[NAT的缺点 7](#_Toc1636824479)

[NAT实现方式 7](#_Toc295010009)

[端口多路复用（PAT） 8](#_Toc1001583437)

[NAT两种实现方式的区别： 8](#_Toc1609014226)

## TCP和UDP协议

### 1、TCP

传输控制协议

可靠的、面向连接的协议

传输效率低

### 2、UDP

用户数据报协议

不可靠的、无连接的服务

传输效率高

### TCP的三次握手与四次断开

TCP的应用

|  |  |  |
| --- | --- | --- |
| 端口 | 协议 | 说　　明 |
| 21 | FTP | FTP服务器所开放的控制端口 |
| 23 | TELNET | 用于远程登录，可以远程控制管理目标计算机 |
| 25 | SMTP | SMTP服务器开放的端口，用于发送邮件 |
| 80 | HTTP | 超文本传输协议 |
| 53 | DNS | 域名服务，当用户输入网站的名称后，由DNS负责将它解析成IP地址，这个过程中用到的端口号是53 |

### 三、UDP

1、UDP首部格式

|  |  |
| --- | --- |
| 源端口号（16） | 目标端口号（16） |
| UDP长度（16） | UDP校验和（16） |

UDP长度：用来指出UDP的总长度

校验和：用来完成对UDP数据的差错检验，它是UDP协议提供的唯一的可靠机制

2、UDP端口及应用

|  |  |  |
| --- | --- | --- |
| 端口 | 协议 | 说明 |
| 69 | TFTP | 简单文件传输协议 |
| 123 | NTP | 网络时间协议 |
| 53 | DNS | 域名服务 |

3、UDP的流控和差错控制

UDP缺乏可靠机制

UDP只有校验和来提供差错控制

需要上层协议来提供差错控制：例如TFTP协议

## 访问控制列表概述

### 1、访问控制列表（ACL）：

读取第三层、第四层包头信息

根据预先定义好的规则对包进行过滤

1. 访问控制列表的处理过程

如果匹配第一条规则，则不再往下检查，路由器将决定该数据包允许通过或拒绝通过。

如果不匹配第一条规则，则依次往下检查，直到有任何一条规则匹配。

如果最后没有任何一条规则匹配，则路由器根据默认的规则将丢弃该数据包。

3、访问控制列表的类型：

1. 标准访问控制列表

基于源IP地址过滤数据包

列表号是1～99

### 扩展访问控制列表

基于源IP地址、目的IP地址、指定协议、端口等来过滤数据包

列表号是100～199

二、标准访问控制列表

1、标准访问控制列表的创建

全局：access-list 1 deny 192.168.1.1 0.0.0.0

全局：access-list 1 permit 192.168.1.0 0.0.0.255

通配符掩码：也叫做反码。用二进制数0和1表示，如果某位为1，表明这一位不需要进行匹配操作，如果为0表明需要严格匹配。

隐含拒绝语句：

access-list 1 deny 0.0.0.0 255.255.255.255

1. 将ACL应用于接口

接口模式：ip access-group 列表号 in或out

注：access-list 1 deny 192.168.1.1 0.0.0.0或写为

access-list 1 deny host 192.168.1.1

access-list 1 deny 0.0.0.0 255.255.255.255或写为

access-list 1 deny any

1. 删除已建立的访问控制列表

全局：no access-list 列表号

1. 接口上取消ACL

接口模式：no ip access-group 列表号in 或out

1. 查看访问控制列表

特权：show access-lists

5、删除ACL

全局：no access-list 列表号

注：不能删除单条ACL语句，只能删除整个ACL。

## NAT（网络地址转换）

1. 作用：通过将内部网络的私有IP地址翻译成全球唯一的公网IP地址，使内部网络可以连接到互联网等外部网络上。
2. 优点：

节省公有合法IP地址

处理地址重叠

安全性

### 3、NAT的缺点

延迟增大

配置和维护的复杂性

### 4、NAT实现方式

1. 静态转换

IP地址的对应关系是一对一，而且是不变的，借助静态转换，能实现外部网络对内部网络中某些特设定服务器的访问。

静态NAT配置：

配置接口IP及路由

全局：

Ip nat inside source static 192.168.1.1 61.159.62.131

在内外接口上启用NAT：

出口配置：ip 　nat 　outside

入口配置：ip 　nat 　inside

### 端口多路复用（PAT）

通过改变外出数据包的源IP地址和源端口并进行端口转换，内部网络的所有主机均可共享一个合法IP地址实现互联网的访问，节约IP。

PAT的配置：

全局：ip nat inside source list 1 interface f0/1 overload

Overload 允许多客户端同时使用外网IP进行通信

NAT两种实现方式的区别：

静态转换的对应关系一对一且不变，并没有节约公用IP，只隐藏了主机的真实地址，增加安全性。

端口多路复用可以使所有内部网络主机共享一个合法的外部IP地址，从而最大限度地节约IP地址资源。

开启nat排错功能

Router#debug ip nat

S表示源地址

D表示目的地址

192.168.1.2->61.159.62.130表示将192.168.1.2转换为61.159.62.130

关闭nat排错功能

Router#undebug ip nat