**Morning：**

1. 传输层概述

-作用：提供端口对端口的连接

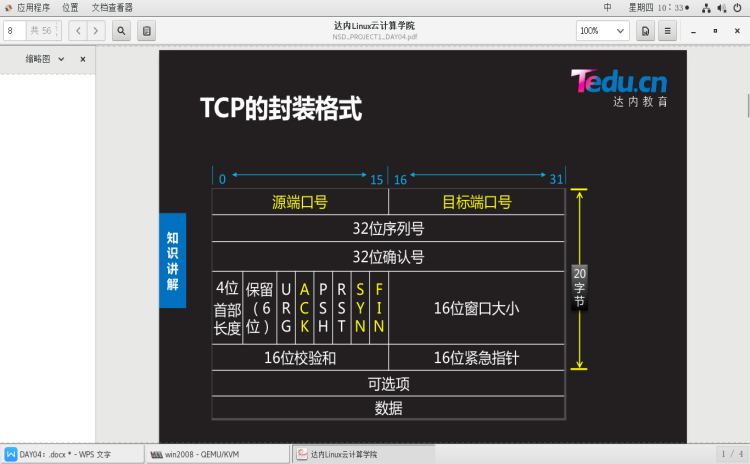
-协议：TCP（传输控制协议）、UDP（用户数据报协议）

TCP：可靠的、面向连接的协议，传输效率低。（数据丢失会要求重发）

UDP：相对不可靠的、无连接的服务，传输效率高

2、TCP

-TCP的封装格式：



SYN：请求连接 ACK：确认连接 FIN：结束连接

-TCP的三次握手：

A：发送 SYN ,请求建立连接(seq=100, ctl=SYN)

B：发送 SYN 、ACK(seq=300, ack=101,ctl=SYN、ACK)

A：发送ACK(seq=101 ack=301,ctl=ACK)

-TCP的四次断开：

A：发送 FIN,请求断开连接 (FIN=1,ACK=1)

B：发送 ACK (ACK=1)

B：发送 FIN,请求断开连接 ( FIN=1,ACK=1) ‘确保数据传输完毕

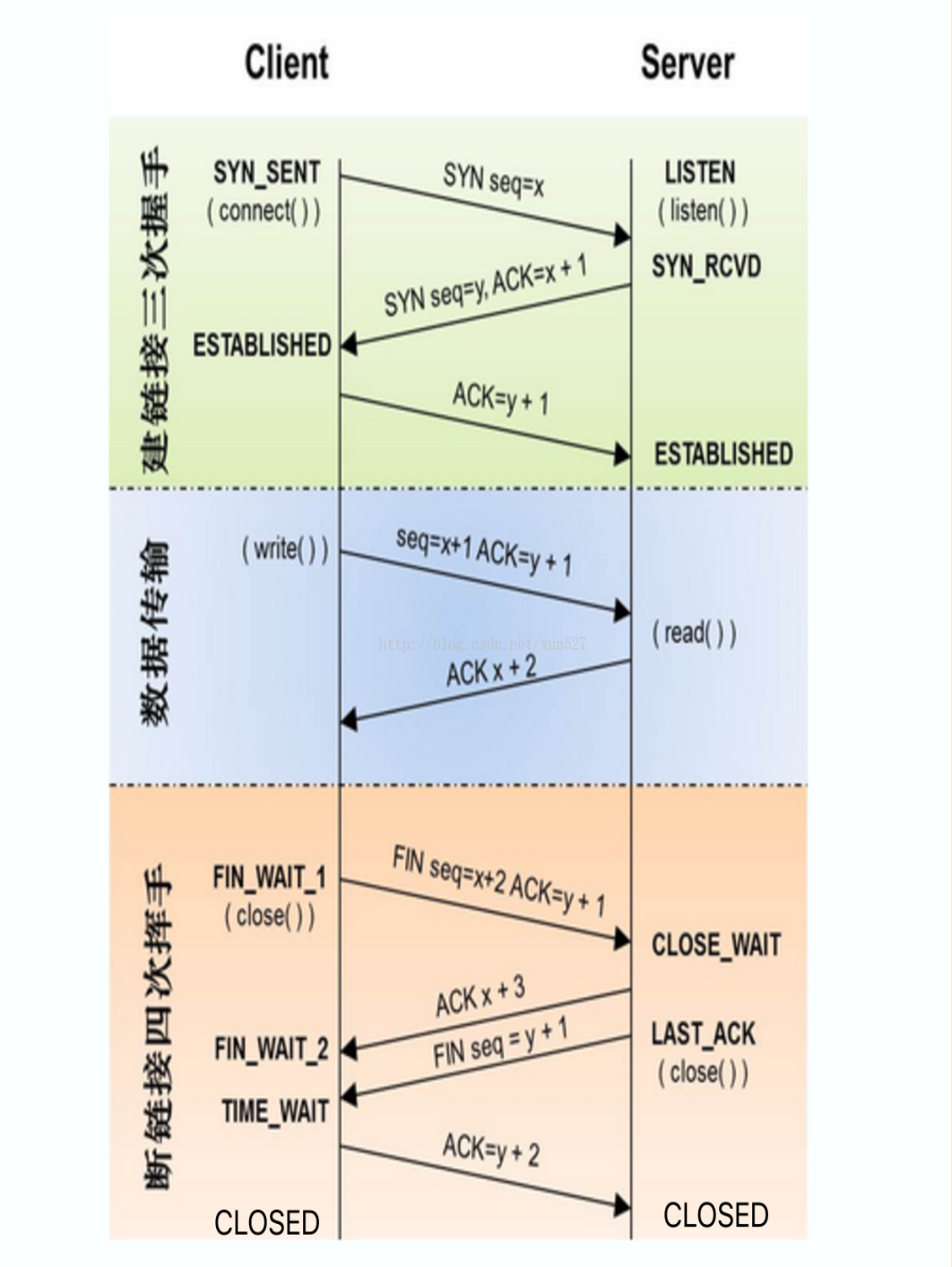
A：发送ACK ( ACK=1)

-TCP的应用：

FTP（21）、SSH（22）、SMTP（25）、DNS（53）、HTTP（80）

#DNS进行迭代查询时使用TCP协议（讲究可靠）

-TCP的十种状态



三次握手：

1）在建立连接之前，B先创建TCB（传输控制块），准备接受客户进程的连接请求，处于LISTEN（监听）状态

2）A首先创建TCB，然后向B发出连接请求，SYN置1，同时选择初始序号seq=x，进入SYN-SEND（同步已发送）状态

3）B收到连接请求后向A发送确认，SYN置1，ACK置1，同时产生一个确认序号ack=x+1。同时随机选择初始序号seq=y，进入SYN-RCVD（同步收到）状态

4）A收到确认连接请求后，ACK置1，确认号ack=y+1，seq=x+1，进入到ESTABLISHED（已建立连接）状态。向B发出确认连接，最后B也进入到ESTABLISHED（已建立连接）状态。

四次断开：

1）A发送一个FIN，用来关闭A到B的数据传送，A进入FIN\_WAIT\_1状态。

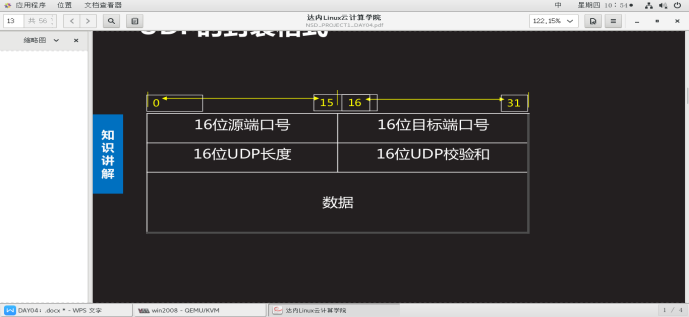
2）B收到FIN后，发送一个ACK给A，确认序号为收到序号+1（与SYN相同，一个FIN占用一个序号），B进入CLOSE\_WAIT状态。

3）B发送一个FIN，用来关闭B到A的数据传送，B进入LAST\_ACK状态。

4）A收到FIN后，A进入TIME\_WAIT状态，接着发送一个ACK给B，确认序号为收到序号+1，B进入CLOSED状态，完成四次挥手。

3、UDP

-UDP的封装格式：



-UDP的应用：

TFTP（69）、DNS（53）、NTP（123）

#DNS进行递归查询时使用UDP协议（讲究效率）

1. 访问控制列表（ACL）

-作用：对第三层（源/目标IP地址）、第四层（源/目标端口）的头部信息，进行数据过滤

-ACL在接口应用的方向：

出：已被路由器处理，正离开路由器接口的数据包；

入：已到达路由器接口的数据包,将被路由器处理。

-ACL的处理过程：

1. 匹配即停止。允许则通过，拒绝则丢弃；
2. 对于思科设备，若无匹配，隐含为拒绝。

-标准ACL：

-基于源IP地址过滤数据包（允许、拒绝或隐含拒绝）

-访问控制列表号是1~99

-拓展ACL：

-基于源IP地址、目的IP地址、指定协议、端口来过滤数据包

-访问控制列表号是100~199

**Afternoon：**

1、标准ACL配置命令

**-创建ACL**

Router(config)#access-list *access-list-number* { permit | deny } *source [ source-wildcard ]*

*‘access-list-number 访问控制列表号1～99*

*’{ permit | deny } 允许/拒绝*

*‘source 源地址主机或网段*

*‘Source-wildcard 反掩码，配合source对主机/网段进行限制*

*例：Router(config)# access-list 1 deny 192.168.1.0 0.0.0.255*

*‘拒绝网段192.168.1.0/24的流量通过*

*Router(config)# access-list 1 permit any ‘允许所有*

*Router(config)# access-list 1 permit host 192.168.1.1‘允许某台主机*

**-将ACL应用于接口(一个接口只能应用1个列表)**

Router(config-if)#(no) ip access-group *access-list-number* {in|out}

*‘(no取消)应用ACL到接口*

*例：Router(config-if)#ip access-group 1 in*

**-查看访问控制列表**

Router(config)# Show access-lists

**-删除ACL**

Router(config)# no access-list *1 ’删除列表号为1的ACL*

2、拓展ACL配置命令：

**-创建ACL**

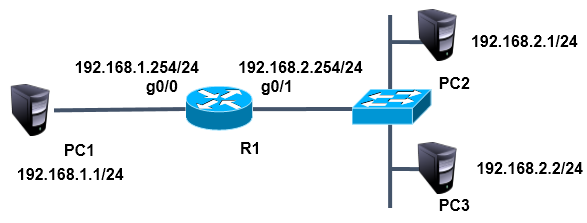
例：Router(config)# access-list 101 deny tcp(传输层协议) 192.168.1.0 0.0.0.255(源地址) host 192.168.2.2(目标地址) eq 80(端口号)

Router(config)# access-list 101 permit ip any any

‘ip协议同时包含TCP/UDP

**-案例**

按照图-3 所示拓扑结构,禁止 pc2 访问 pc1 的 ftp 服务,禁止 pc3 访问 pc1 的 www服务,所有主机的其他服务不受限制



Router(config)#access-list 100 deny tcp host 192.168.2.1 host 192.168.1.1 eq 21

Router(config)#access-list 100 deny tcp host 192.168.2.2 host 192.168.1.1 eq 80

Router(config)#access-list 100 permit ip any any

Router(config)#interface gigabitEthernet 0/1

Router(config-if)#ip access-group 100 in

1. 私有地址：

A类 10.0.0.0～10.255.255.255

B类 172.16.0.0～172.31.255.255

C类 192.168.0.0～192.168.255.255

1. NAT（网络地址转换）

-作用：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外部网络上。

-优点：节省公有合法IP地址；处理地址重叠；安全性

-缺点：延迟较大；配置和维护复杂

-NAT实现方式

**• 静态转换**

特点：IP地址的对应关系是一对一,而且是不变的，适用于服务器。

配置步骤：

1. 设置外部接口的IP地址100.0.0.1/8
2. 设置内部接口的IP地址192.168.1.254/24
3. 建立静态地址转换

*Router(config)#ip nat inside source static 192.168.1.1(私有) 100.0.0.2(公有)*

1. 在内部和外部接口上启动NAT

*Router(config)#interface g0/1*

*Router(config-if)#ip nat outside ‘外部接口启动NAT*

*Router(config)#interface g0/0*

*Router(config-if)#ip nat inside ’内部接口启动NAT*

5）验证

LAN网主机的私有地址可以ping通WAN网主机

WAN网主机可以ping通LAN网主机的公有地址

NAT端口映射：

Router(config)#ip nat inside source static tcp(传输层协议) 192.168.1.1 80(LAN端口号) 100.0.0.2 80(WAN端口号)

‘只能从外部访问100.0.0.2的web服务

**• PAT（端口多路复用）（了解）**

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，用于办公室。

配置步骤：

1）接口IP地址配置

2）使用访问控制列表定义哪些内部主机能做PAT

Router(config)#access-list 1 permit 192.168.1.0 0.0.0.255

1. 确定路由器外部接口

Router(config)#ip nat inside source list 1 interface g 0/1 overload

4）在内部和外部接口上启用NAT

1. 跟踪NAT

Router# debug ip nat ‘开启跟踪NAT，主机ping不通时可用

Router# undebug ’关闭