传输层、应用层

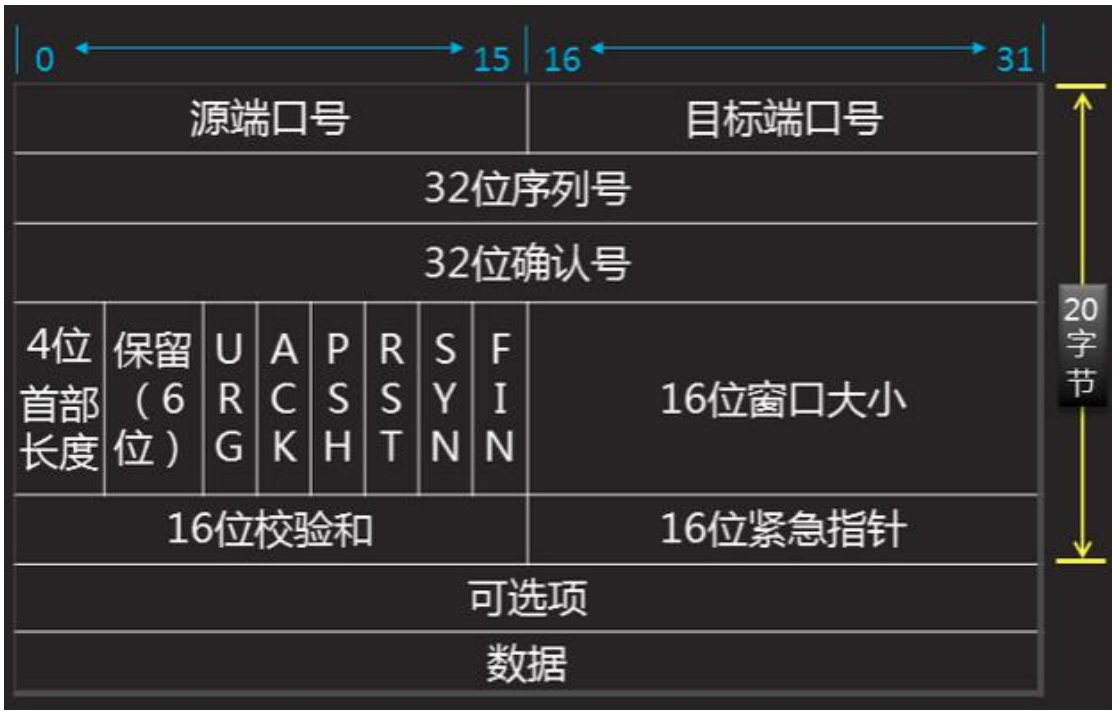
传输层的作用：IP 提供点到点的连接；传输层提供端到端的连接

IP 层找到了这台主机；传输层找到了应用进程

常用的端口号 0～1023（0～65535）

传输层协议：

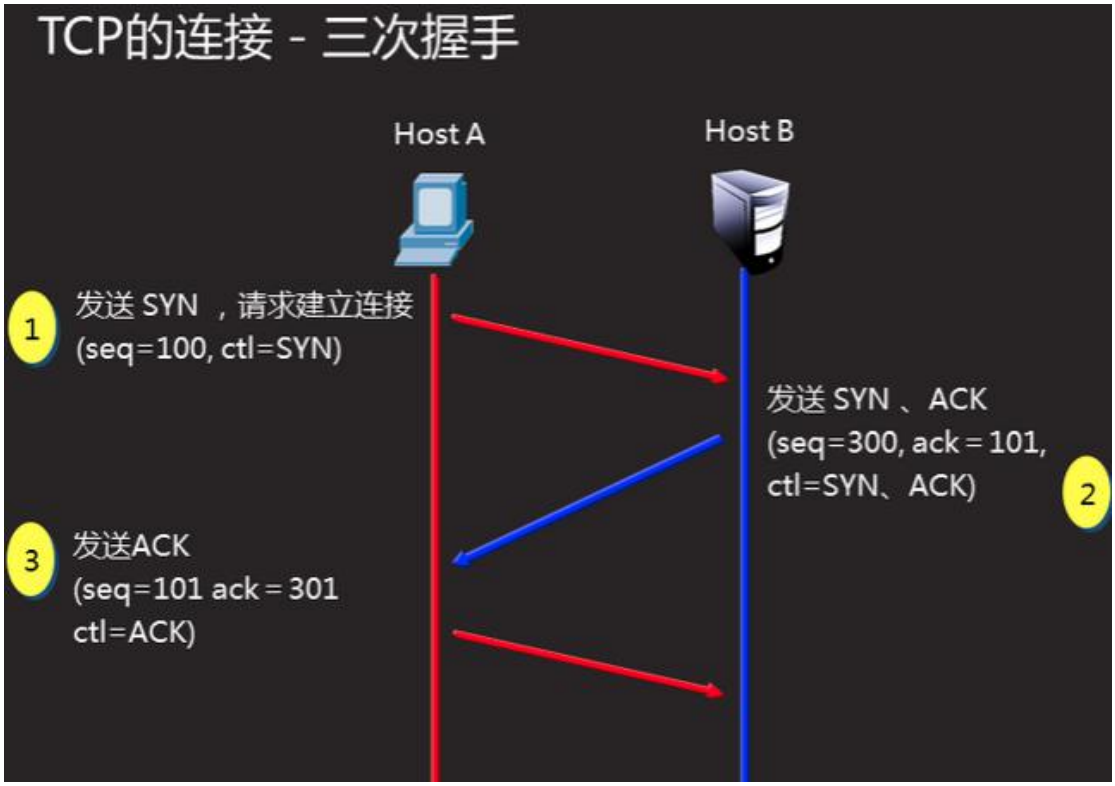
TCP：传输控制协议；可靠的、面向连接的协议；传输效率低
UDP：用户数据报协议；不可靠的、无连接的服务；传输效率高
TCP 的工作原理（可靠性高）【重点】：TCP 的封装格式、连接与断开、流量控制、拥塞控制、差错控制、计时器
TCP 的封装格式



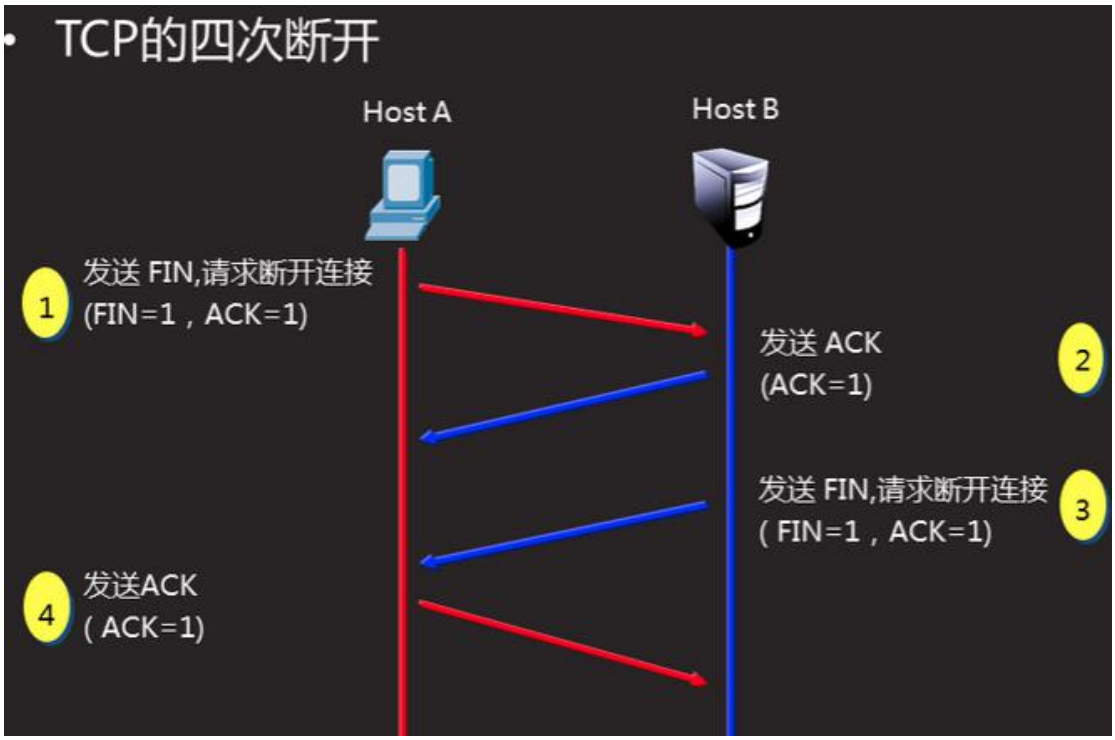
源端口、目标端口
序列号、确认序列号（如序列号为 x 则确认序列号为 x+1）
TCP 首部长度至少 20 字节
控制位：
SYN：建立连接时将这个值设为 1
ACK:当 ACK=1 表示确认，ACK=0 表示确认无效
FIN：FIN=1 表示断开连接请求
RST:RST=1 表示重新建立 TCP 连接
URG：紧急指针有效位
PSH：此标志位为 1 时要求接收方尽快将数据段送达应用层。
窗口值：表示本地可接收数据的数目.当网络通畅时窗口值变大加快传输速度，不稳定时该值减小保证数据的可靠传输，TCP 协议中的流量控制机制就是依靠

变化窗口大小实现的。
校验和：用来做差错控制
紧急指针：和 **URG** 配合使用，当 **URG=1** 时有效

TCP 的三次握手与四次断开



用打电话的方式：A 拿电话拨通 B 的电话（发送 SYN，请求建立连接），B 的电话铃响，接通电话（发送 SYN 建立连接）然后问候 A 喂？（发送 ACK 确认），A 收到 B 的问候后，回复 B（发送 ACK 确认）



用打电话的方式：A 说还有事吗，没事我挂了阿（发送 FIN 请求断开连接），B 收到 A 的请求，回复 A 我没事了（发送 ACK 确认）挂了吧（发送 FIN 请求断开连接），A 说好的，那我挂了哈（发送 ACK 确认）

TCP 的流量控制机制

TCP 使用滑动窗口实现流量控制

实际发送数据的窗口采用发送方和接收方协商的窗口与拥塞窗口中的最小值

TCP 的差错控制

校验和、确认、超时

TCP 的计时器

重传计时器－为了控制丢失的数据段

坚持计时器－为了防止零窗口死锁

保活计时器－防止两个 TCP 之间的连接长时间的空闲

时间等待计时器－连接终止期间使用的,在发送了最后一个 ACK 后，不立即关闭连接，而是等待一段时间，保证能接收到重复的 FIN 数据段

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

UDP

UDP 的封装格式

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

UDP 的应用

端 口	协 议	说 明
69	TFTP	简单文件传输协议
53	DNS	域名服务
123	NTP	网络时间协议
111	RPC	远程过程调用

UDP 的流量和差错控制

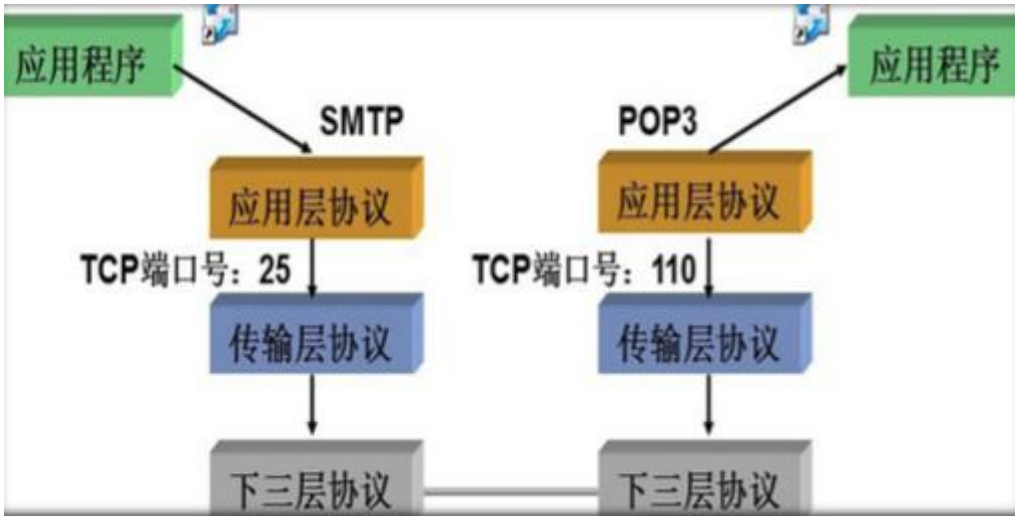
UDP 没有流控机制

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（该协议提供分块传输、分块确认机制，确保数据传输的可靠性）

应用层的作用

与应用程序协同工作，利用基础网络交换应用程序专用的数据



常用的应用层协议

DNS

SMTP 与 POP3

HTTP 与 HTTPS

Telnet

FTP 与 TFTP

//DNS 的功能

Domain Name System 域名系统

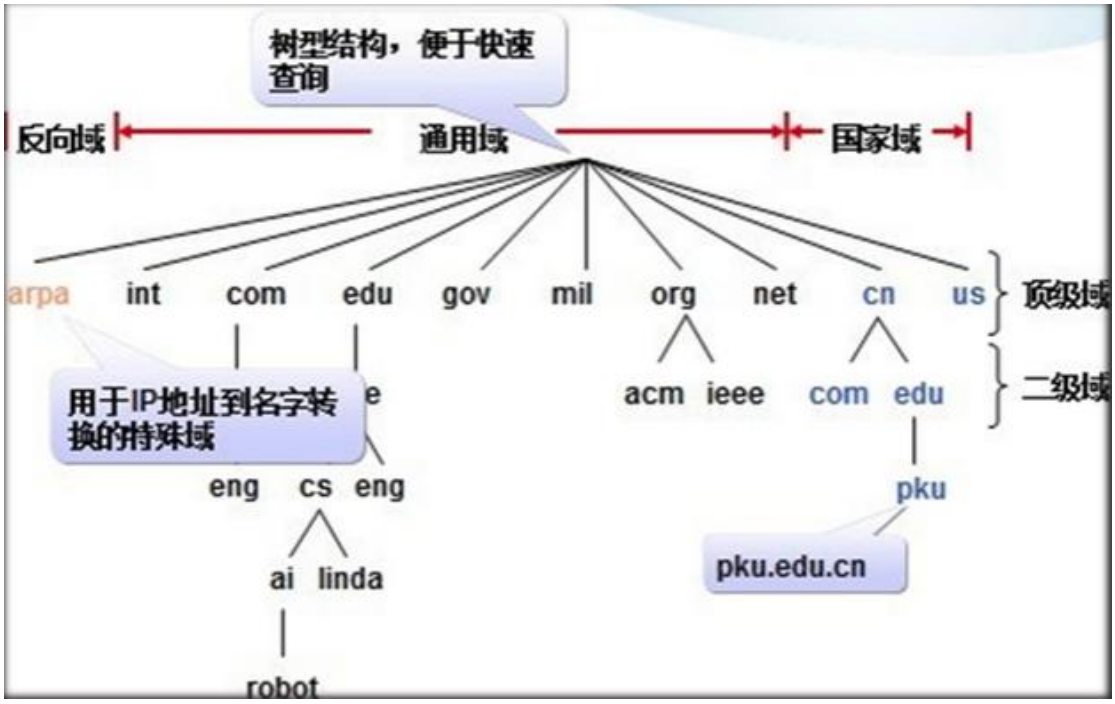
用来完成域名与 IP 地址之间的映射

端口号为 TCP 或 UDP 的 53

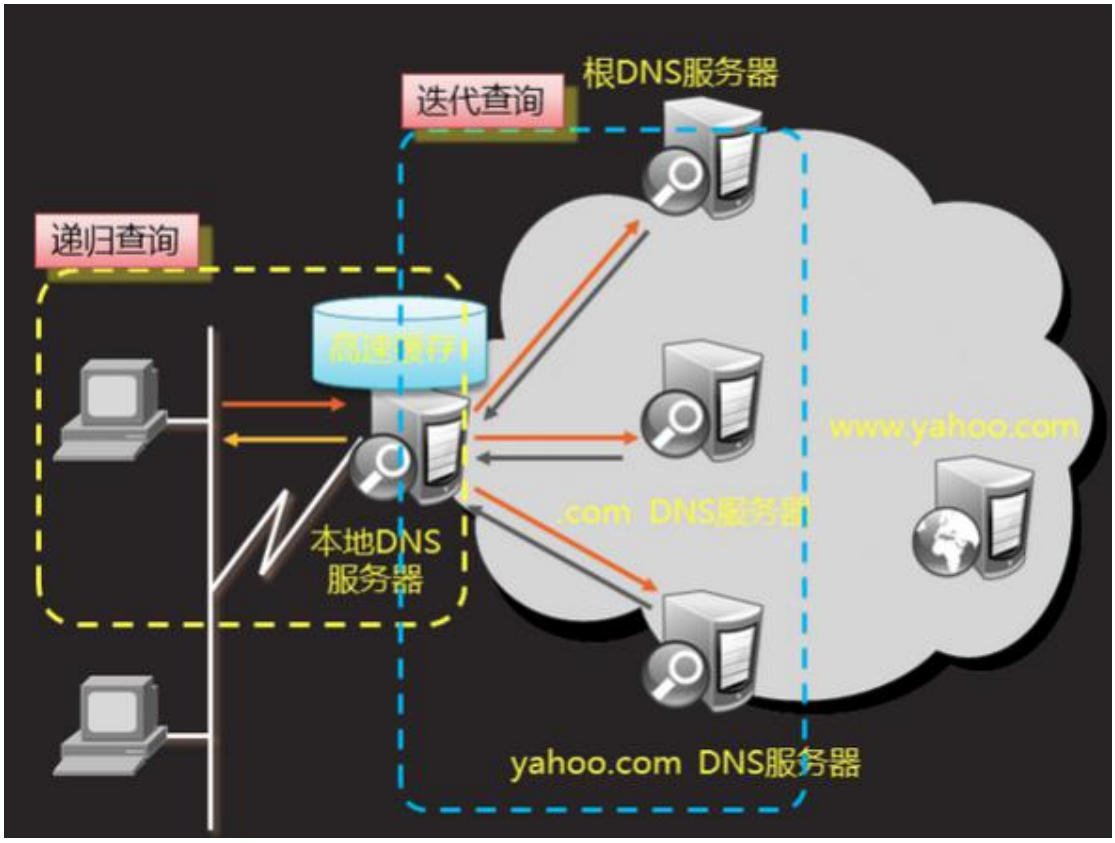
//DNS 名字空间

顶级域有 3 个部分组成：通用域、国家域、反向域
通用域中主要包括：

域后缀	用途描述
.com	商业机构
.edu	教育机构、学校
.gov	政府部门
.int	国际组织
.mil	美国军事网点
.net	网络/计算机相关
.org	其他组织机构、社会团体

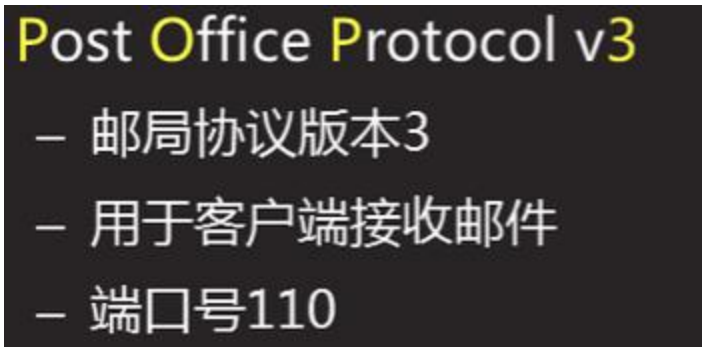


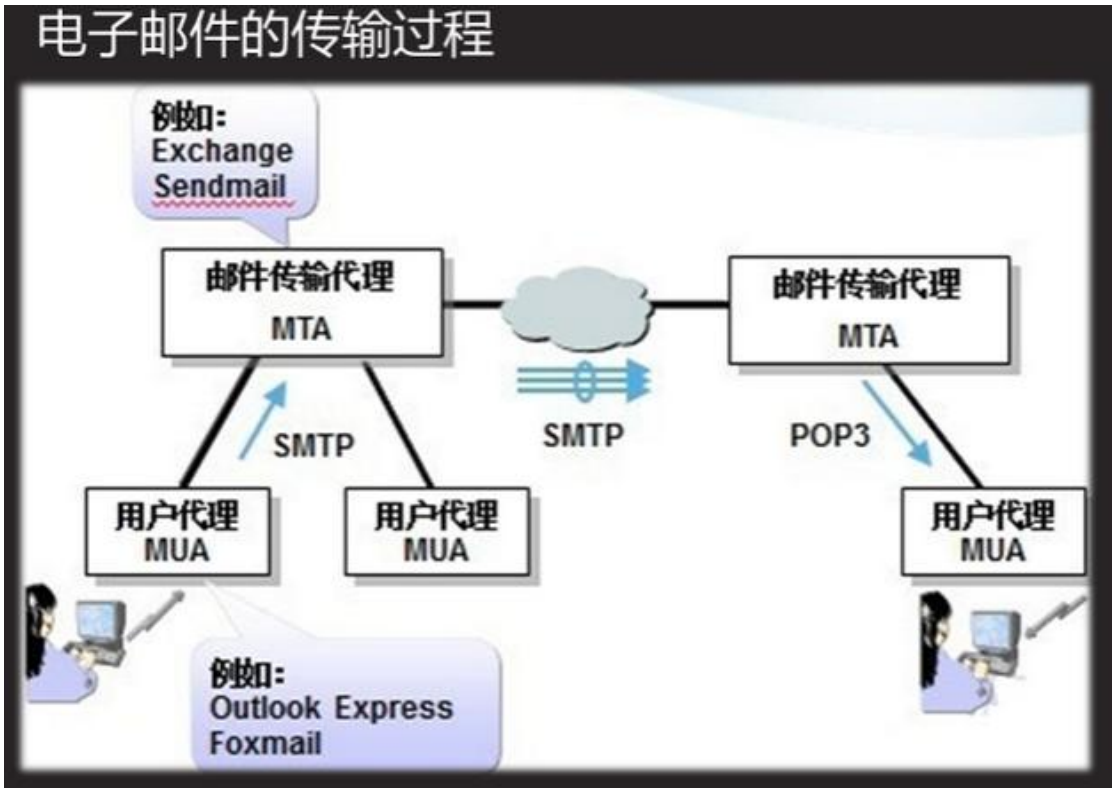
DNS 工作原理



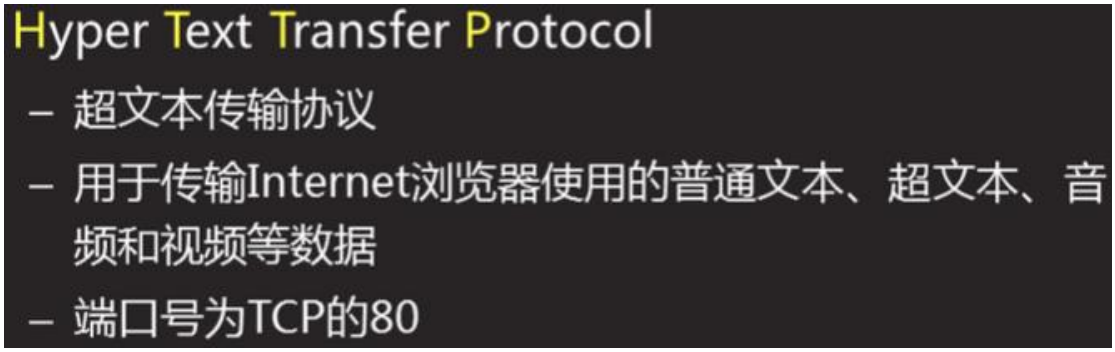
递归解析：本地主机与本地 **DNS** 服务器之间的解析方式，最终会给客户端返回一个结果。
迭代解析：本地 **DNS** 服务器与其他 **DNS** 服务器之间的解析方式。

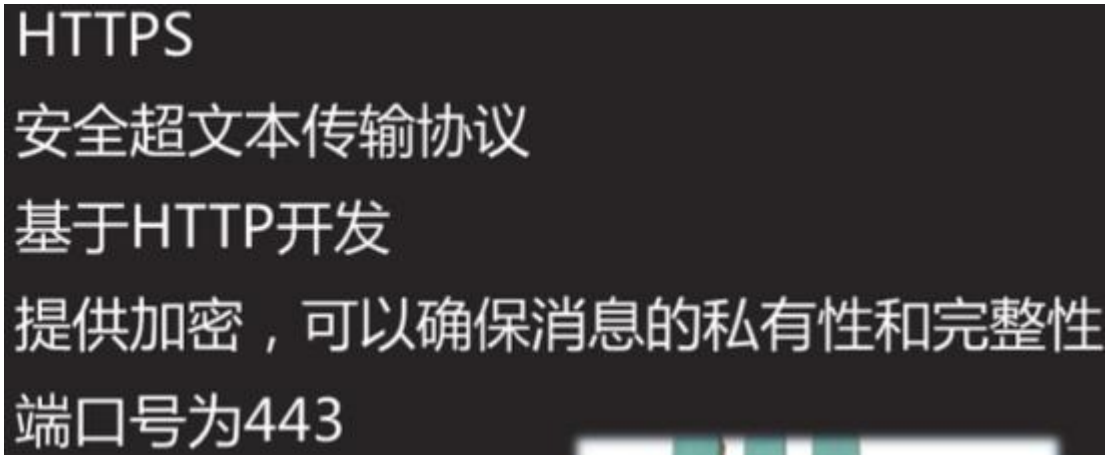
SMTP 与 POP3





HTTP 与 HTTPS





FTP 与 TFTP

File Transfer Protocol

- 文件传输协议
- 使用最为广泛的文件传输应用
- 端口号为TCP 21和20

Trivial File Transfer Protocol

- 简单文件传输协议
- 用来传输一些琐碎的小文件
- 端口号为UDP 69

TFTP工作原理

数据传输是在连接建立和终止之间发生的

文件划分成若干个数据块

- 每一块为512个字节
- 最后一块必须在0 - 511之间

文件传输的可靠性保证

- 由TFTP自行提供流控和差错控制

Telnet

Terminal Network

- 终端网络应用
- 通过文本方式远程管理计算机或路由器/交换机
- 端口号为TCP的23

Telnet的操作

在Windows客户机上操作

– 开始 → 运行：cmd

– 执行：telnet <目标主机地址> [端口号]

示例：

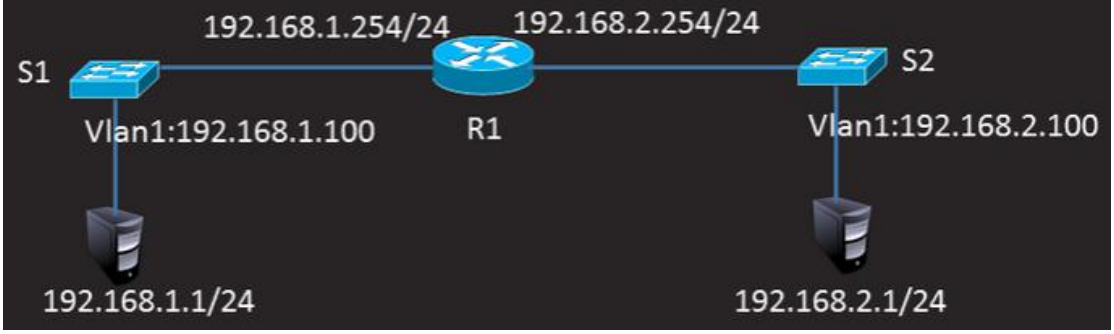
– telnet 192.168.1.100

案例

Telnet远程访问思科交换机、路由器

主机192.168.1.1远程管理S1、R1、S2

主机192.168.2.1远程管理S2、R1、S1



步骤一：Telnet远程访问思科交换机、路由器

1）配置交换机S1的管理IP

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.1.100 255.255.255.0    //交换机管理IP
S1(config-if)#no shutdown
```

2）开启S1的telnet远程管理服务

```
S1(config)#line vty 0 4
S1(config-line)#password 123      //远程管理的密码
S1(config-line)#login
```

3）配置用户模式进入特权模式的密码（明文或密文之一）

```
S1(config)#enable password 456
```

4）按图-1所示的IP配置PC1的IP地址，PC1通过telnet方式远程管理S1

```
PC>telnet 192.168.1.100
Trying 192.168.1.100 ...Open
User Access Verification
Password:                    //输入远程管理密码123
S1>en
S1>enable
Password:                    //输入用户模式进入特模式密码456
S1#                          //通过telnet方式登录到S1的特权模式
```

步骤二：PC1远程管理R1

1）配置路由器R1的接口IP

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.254 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip address 192.168.2.254 255.255.255.0
R1(config-if)#no shutdown
```

2）开启R1的telnet远程管理服务

```
R1(config)#line vty 0 4
R1(config-line)#password 123      //远程管理的密码
R1(config-line)#login
```

3）配置用户模式进入特权模式的密码（明文或密文之一）

```
R1(config)#enable password 456
```

4）PC1通过telnet方式远程管理R1

```
PC>telnet 192.168.1.254
Trying 192.168.1.254 ...Open
User Access Verification
Password:                    //输入远程管理密码123
R1>en
R1>enable
Password:                    //输入用户进入特模式密码456
R1#                          //通过telnet方式登录到R1的特权模式
```

步骤三：PC1远程管理S2

1）配置交换机S2的管理IP

```
S2(config)#interface vlan 1
S2(config-if)#ip address 192.168.2.100 255.255.255.0    //交换机管理IP
S2(config-if)#no shutdown
S2(config-if)#exit
S2(config)#ip default-gateway 192.168.2.254 //不同网段主机远程管理需给交换机配置网关地址
```

2）开启S2的telnet远程管理服务

```
S2(config)#line vty 0 4
S2(config-line)#password 123      //远程管理的密码
S2(config-line)#login
```

3）配置用户模式进入特权模式的密码（明文或密文之一）

```
S2(config)#enable password 456
```

4）PC1通过telnet方式远程管理S2

```
PC>telnet 192.168.2.100
Trying 192.168.2.100 ...Open
User Access Verification
Password:                    //输入远程管理密码123
S2>en
S2>enable
Password:                    //输入用户模式进入特模式密码456
S2#                          //通过telnet方式登录到S2的特权模式
```

////

一般来说，路由器的LAN接口的IP地址就是你所在局域网中的网关。当你所在的局域网的计算机需要和其它局域网中的计算机，或者需要访问互联网的时候，你所在局域网的计算机会先把数据包传输到网关（路由器的LAN接口），然后再由网关进行转发。

举个简单的例子，一套房子内部有三个房间、一个大门，房子可以比喻成你的电脑所在的局域网，三个房间可以比喻成你所在局域网中的三台电脑，房子的大门可以比喻成网关。当你在房子内的一个房间进入另一个房间的时候并不需要经过房子的大门；在局域网中也是一样的，处在同一局域网的中计算机进行通信的时候并不需要用到网关。当你需要到邻居家去玩的时候需要要从你家房子的大门出去；相应的，局域网中的计算机需要和其它局域网中的计算机、和互联网上的计算机进行通信的时候，数据包必须要通过网关才可以到达。

这就是为什么我们在有路由器上网的时候，必须要把计算机中的默认网关地址设置成路由器LAN接口的地址的原因，因为路由器的LAN接口就是你所在网络的网关，你的电脑要上网，数据包必须要经过网关转发出去。目前家用路由器一般使用192.168.1.1和192.168.0.1作为LAN接口的地址，这两个地址也是最常见的网关地址。