网络基本概念

www.huawei.com

HUAWEI

前言

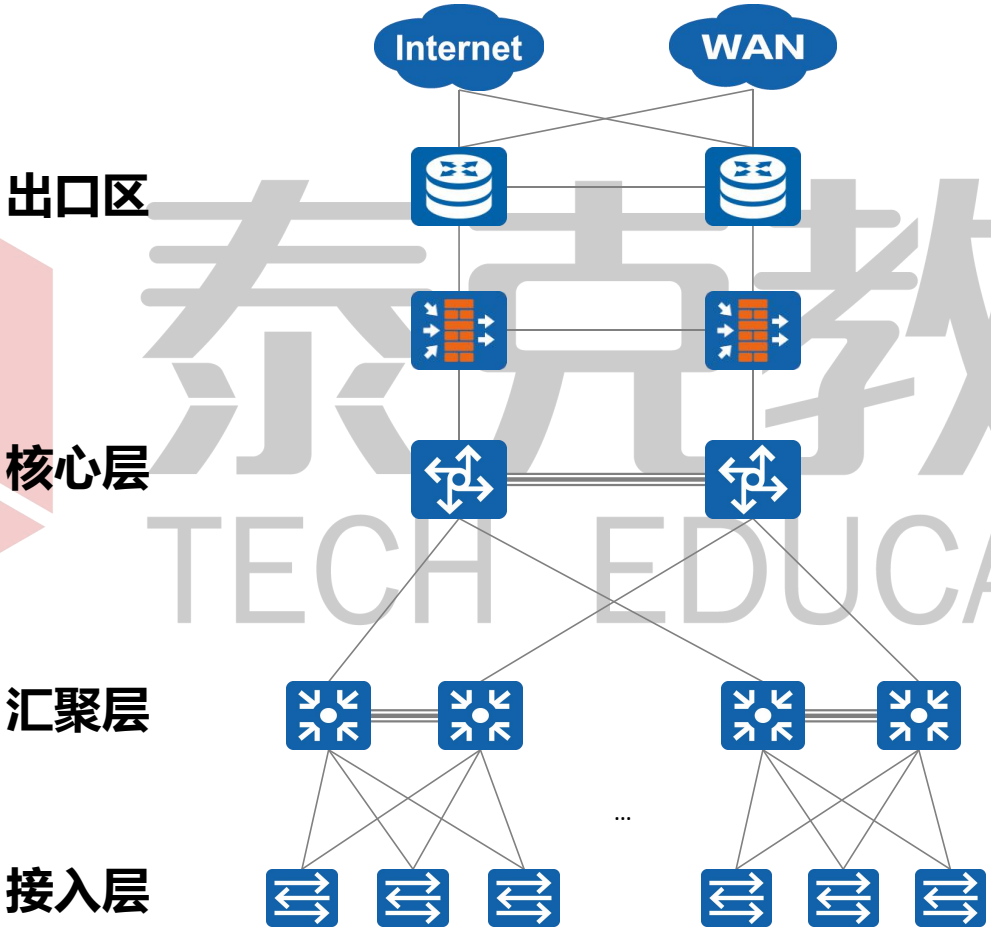
- 在学习安全技术之前，首先我们应该了解网络的基本概念，如网络的基本通信原理，网络的组成和常见的网络协议等。在了解网络协议的基础上，能够理解网络安全威胁，从而部署安全防御策略。

目标

- 学完本课程后，您将能够：
  - 描述TCP/IP的工作原理
  - 描述常见协议的工作原理
  - 描述常见协议可能存在的安全威胁

目录

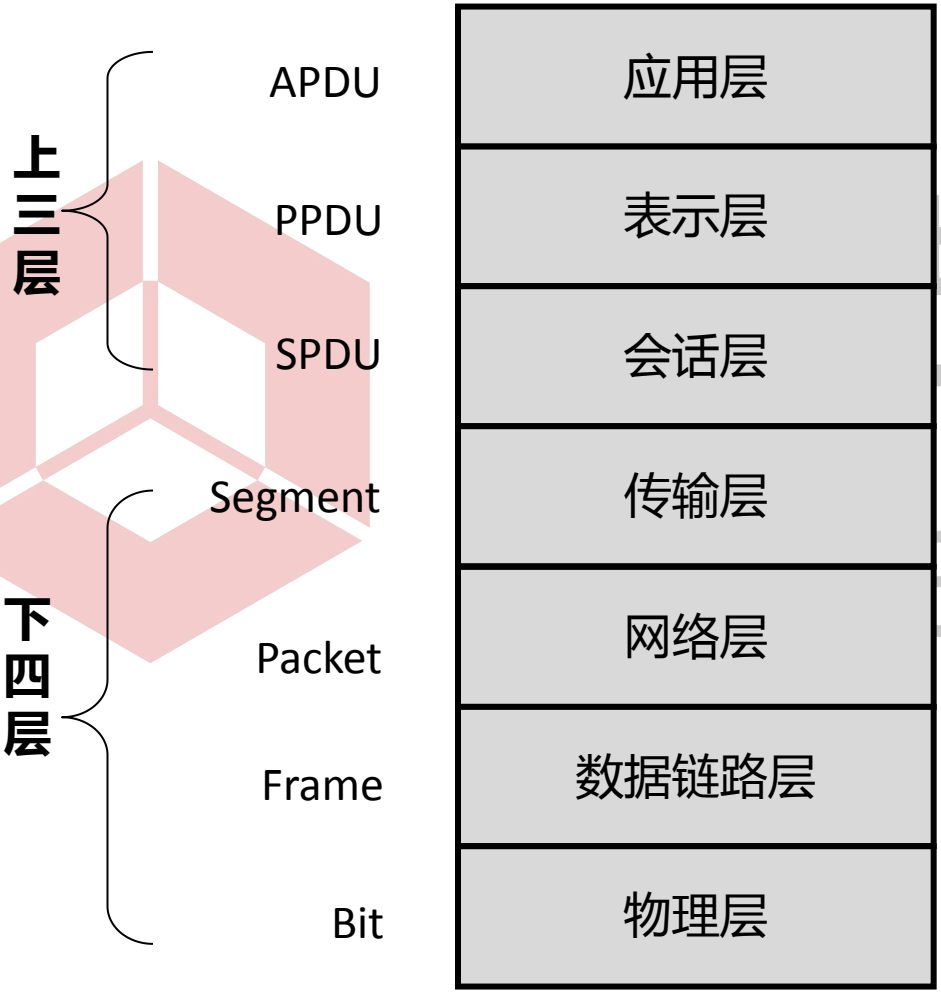
典型园区网络架构



OSI模型的提出

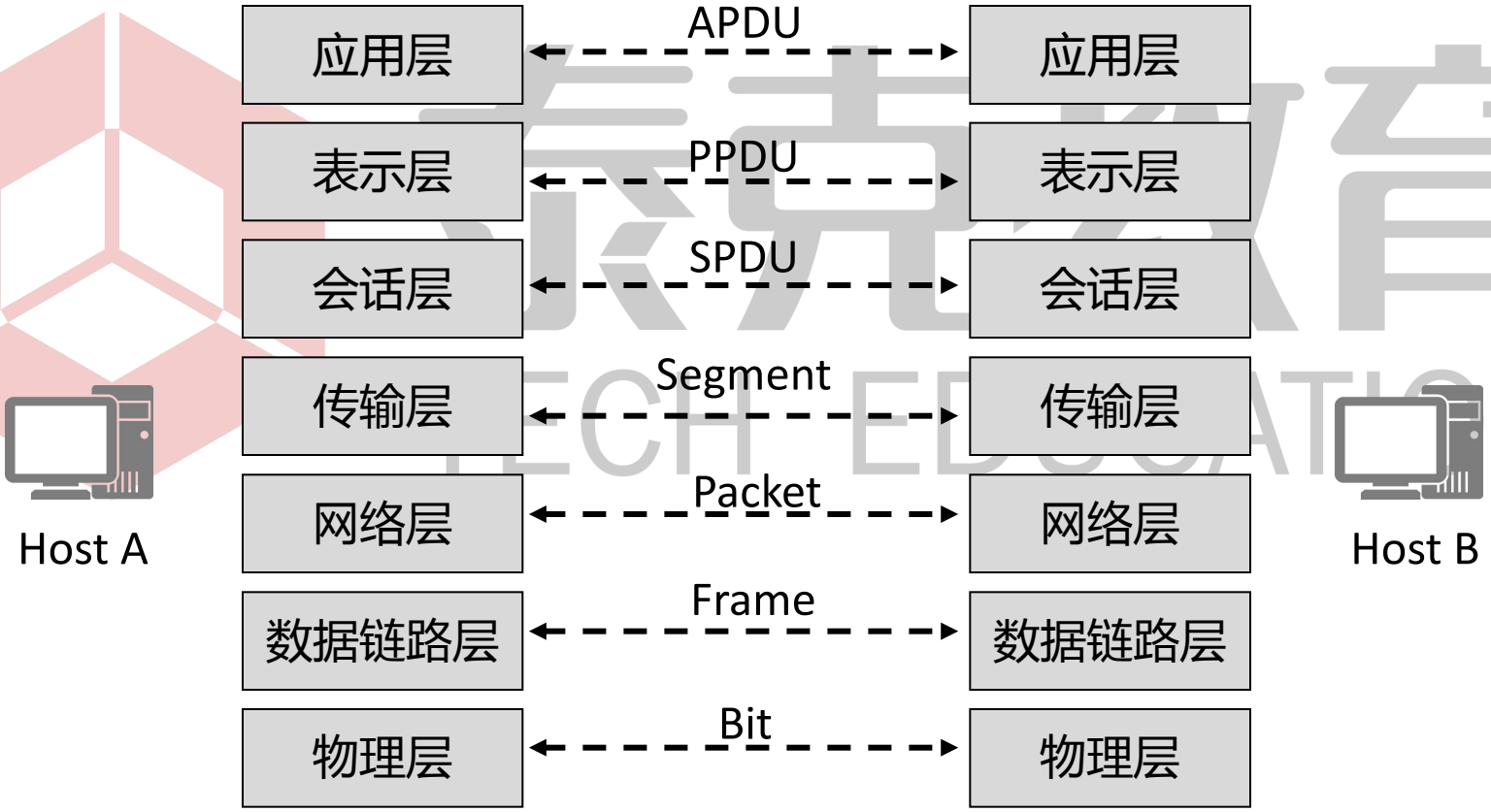
- OSI模型提出的目的
- OSI模型设计原则
- OSI模型的优点

OSI七层模型



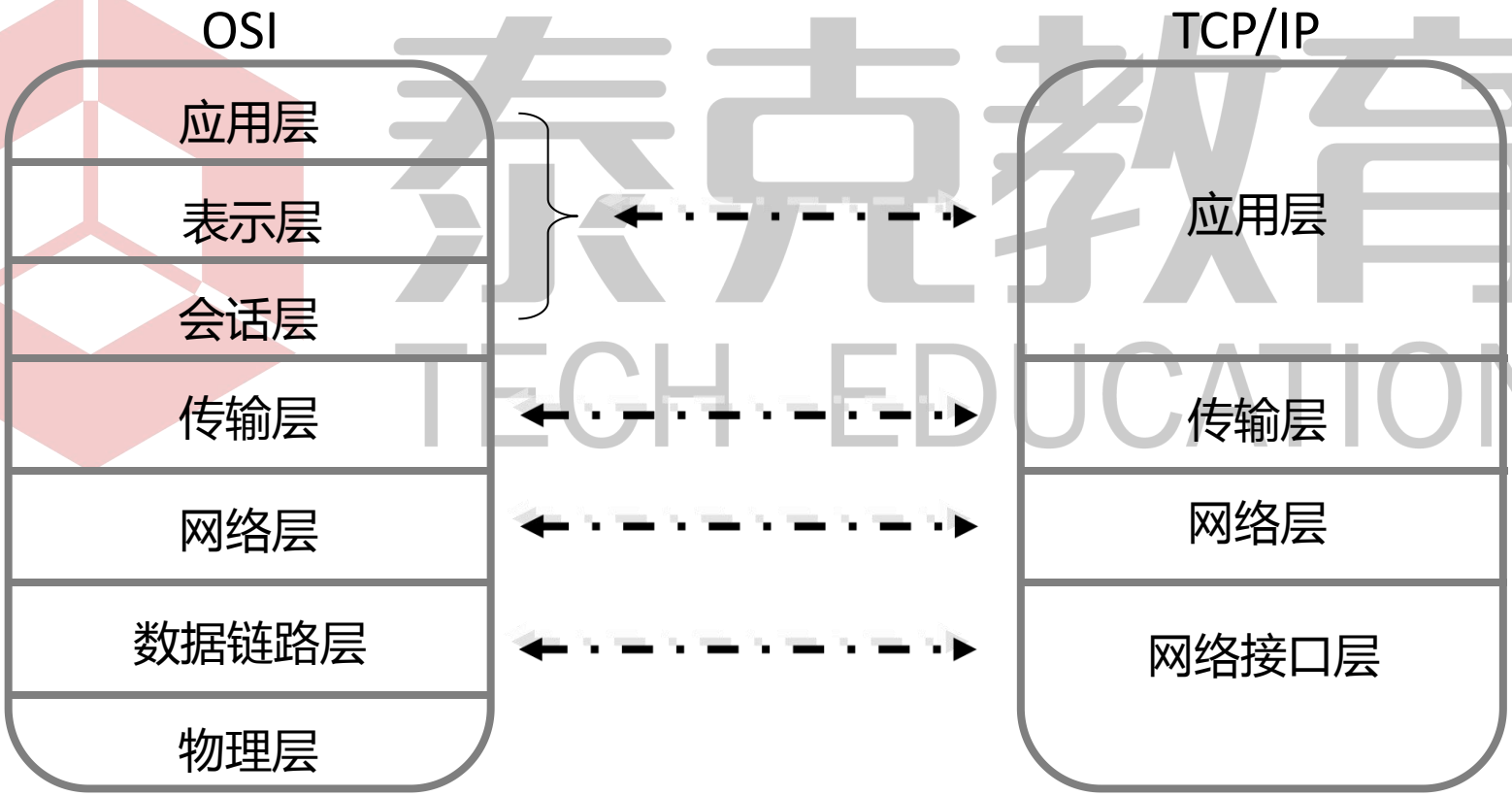
对等层通讯

- 每一层利用下一层提供的服务与对等层通信。

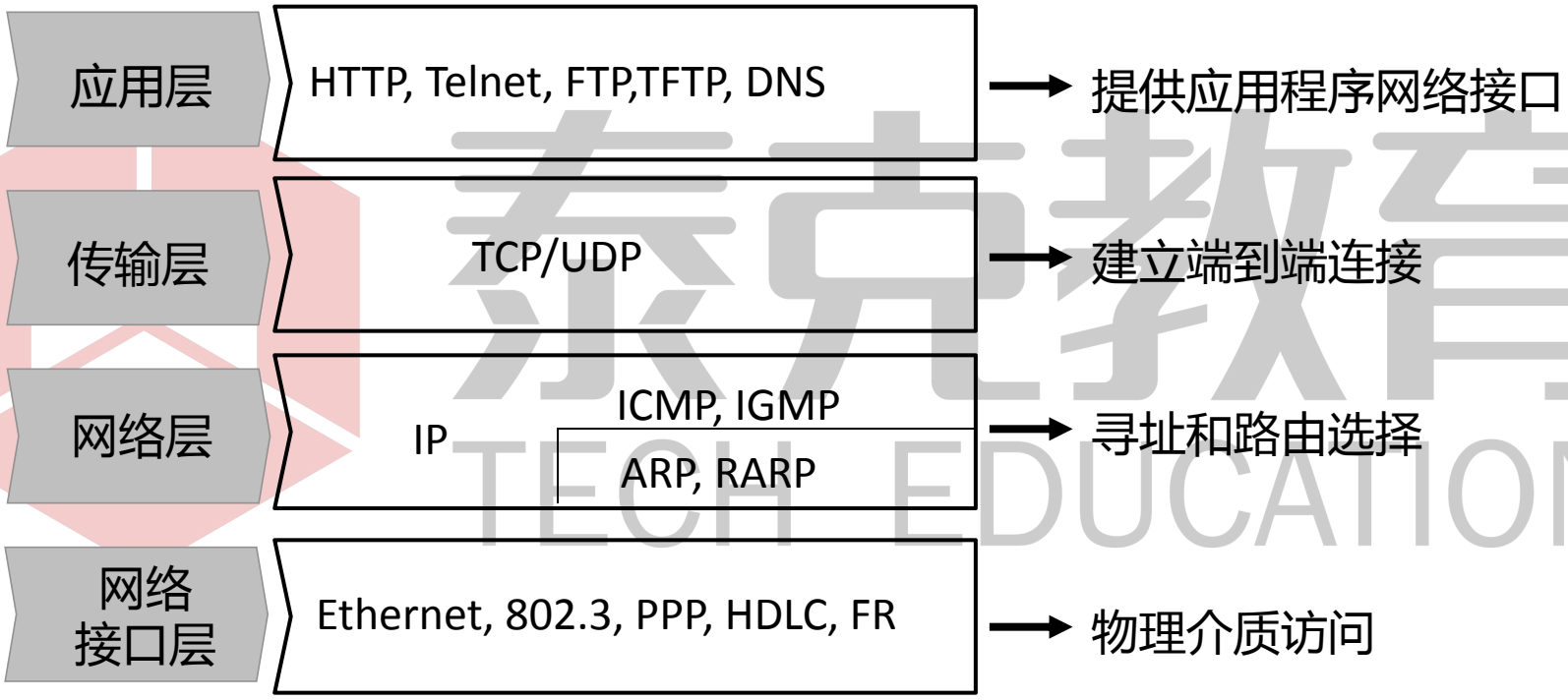


TCP/IP和OSI的对应关系

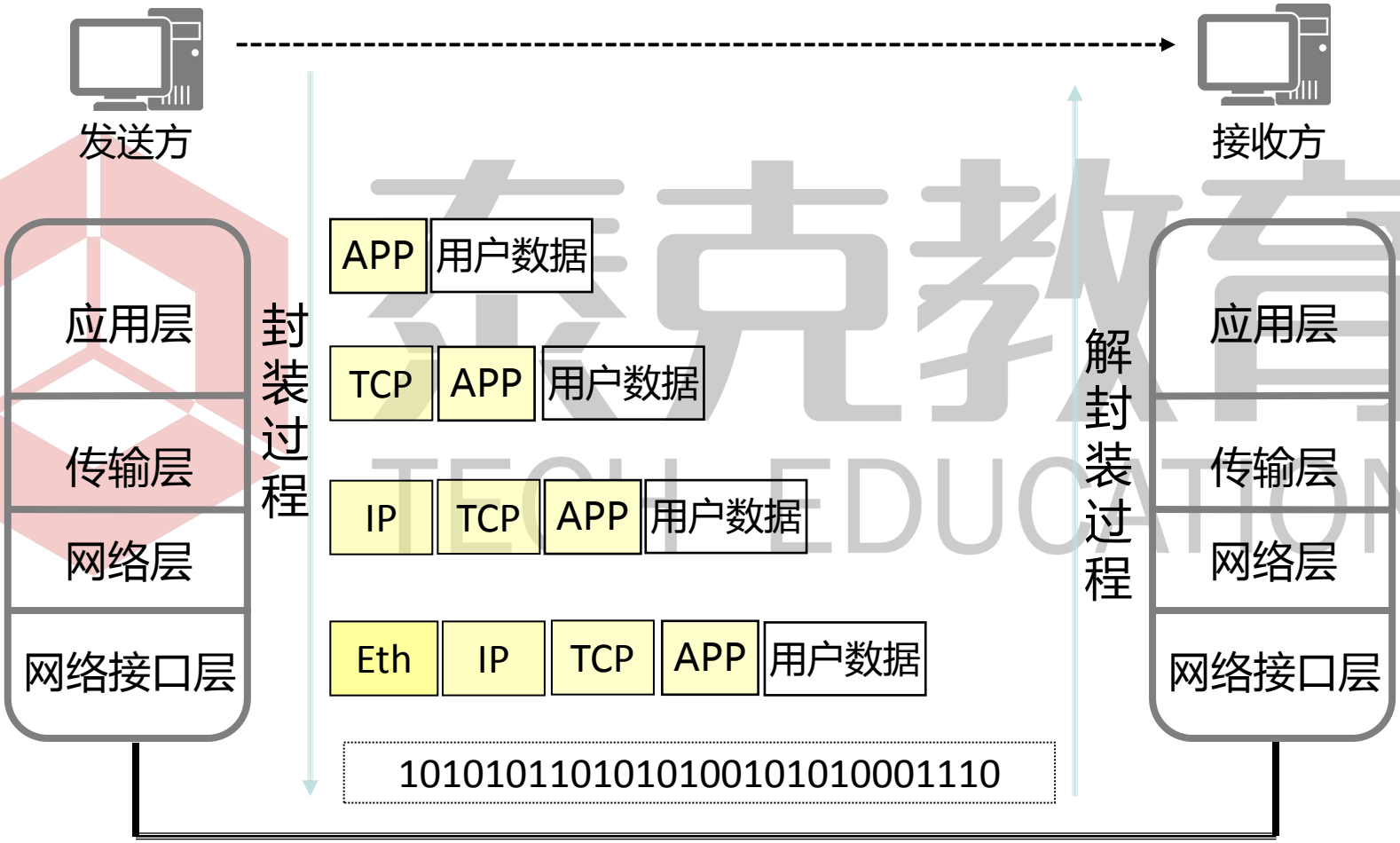
- TCP/IP协议栈具有简单的分层设计，与OSI参考模型有清晰的对应关系。



TCP/IP协议栈各层作用

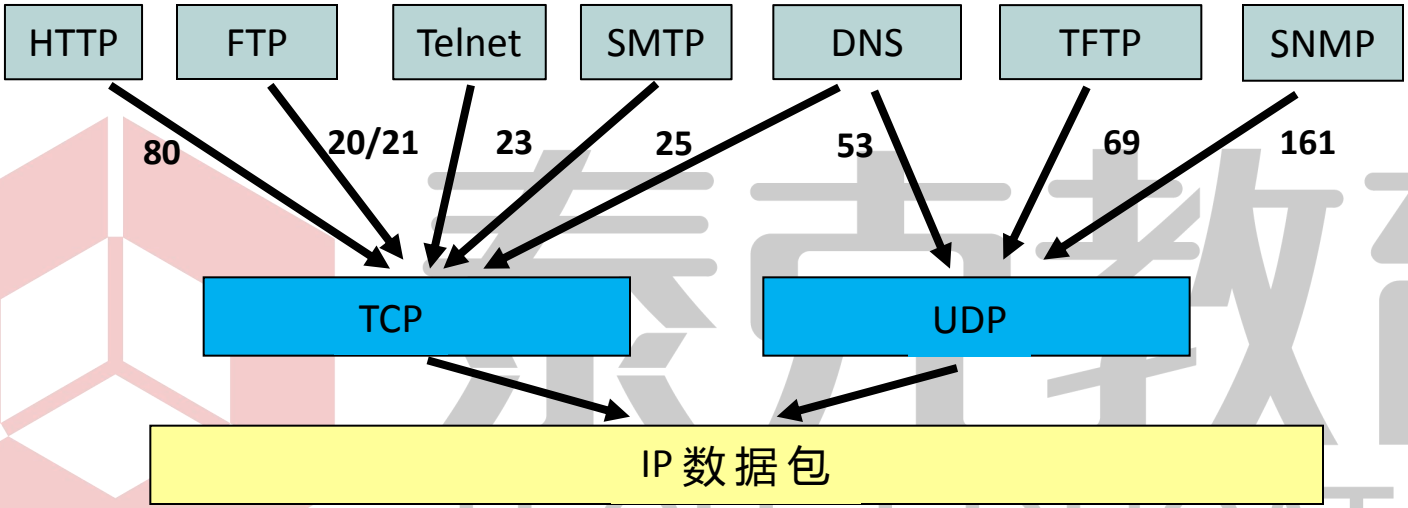


TCP/IP协议栈封装解封装过程



HUAWEI

五元组

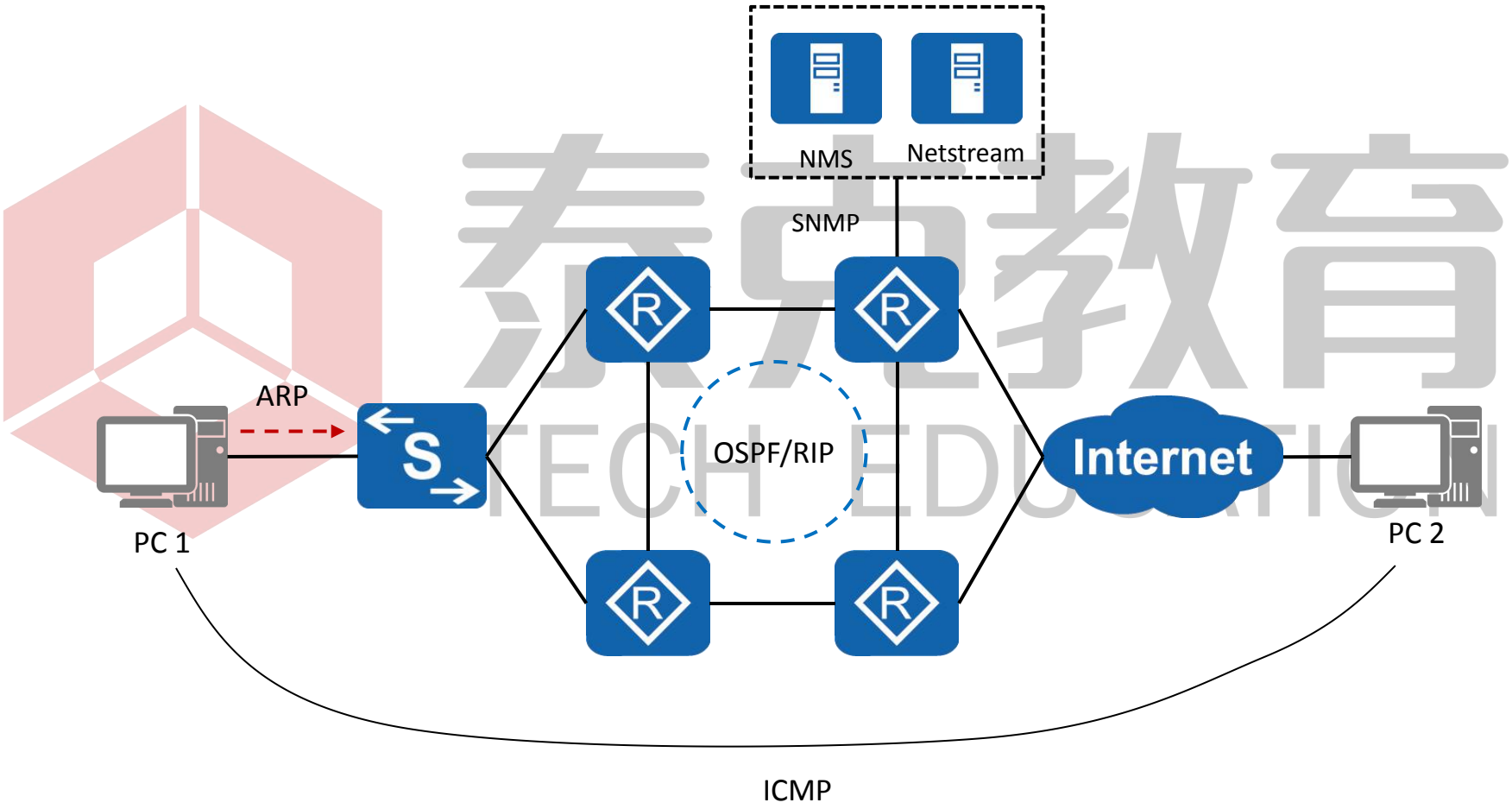


五元组

- 源IP地址 + 目的IP地址 + 协议 + 源端口+目的端口

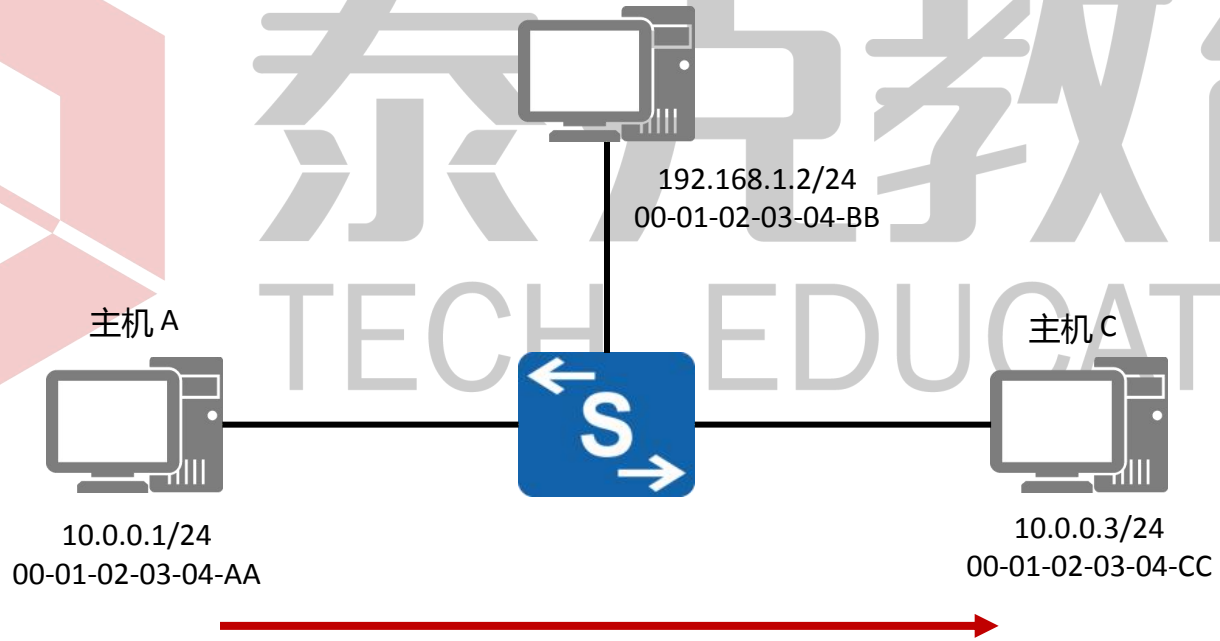
目录

常见网络层协议

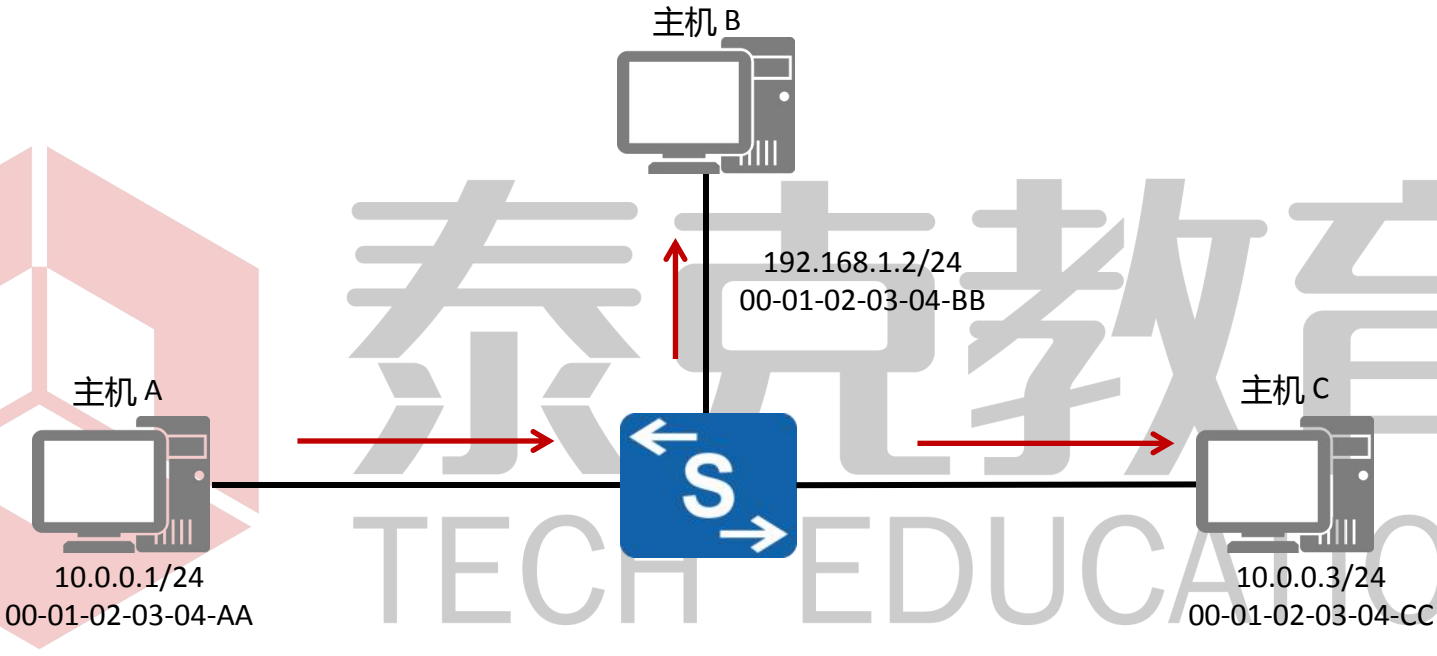


ARP简介

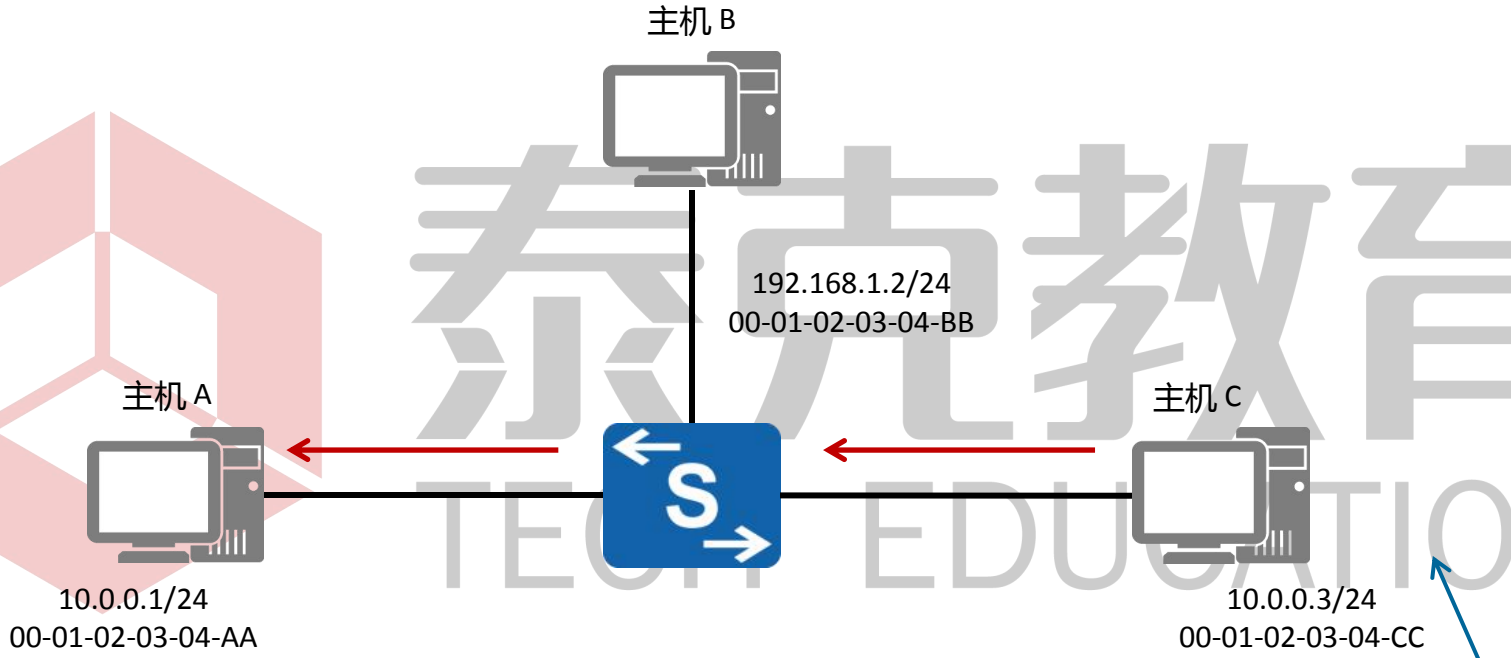
- 主机A发送一个数据包给主机C之前，首先要获取主机C的MAC地址。



ARP请求

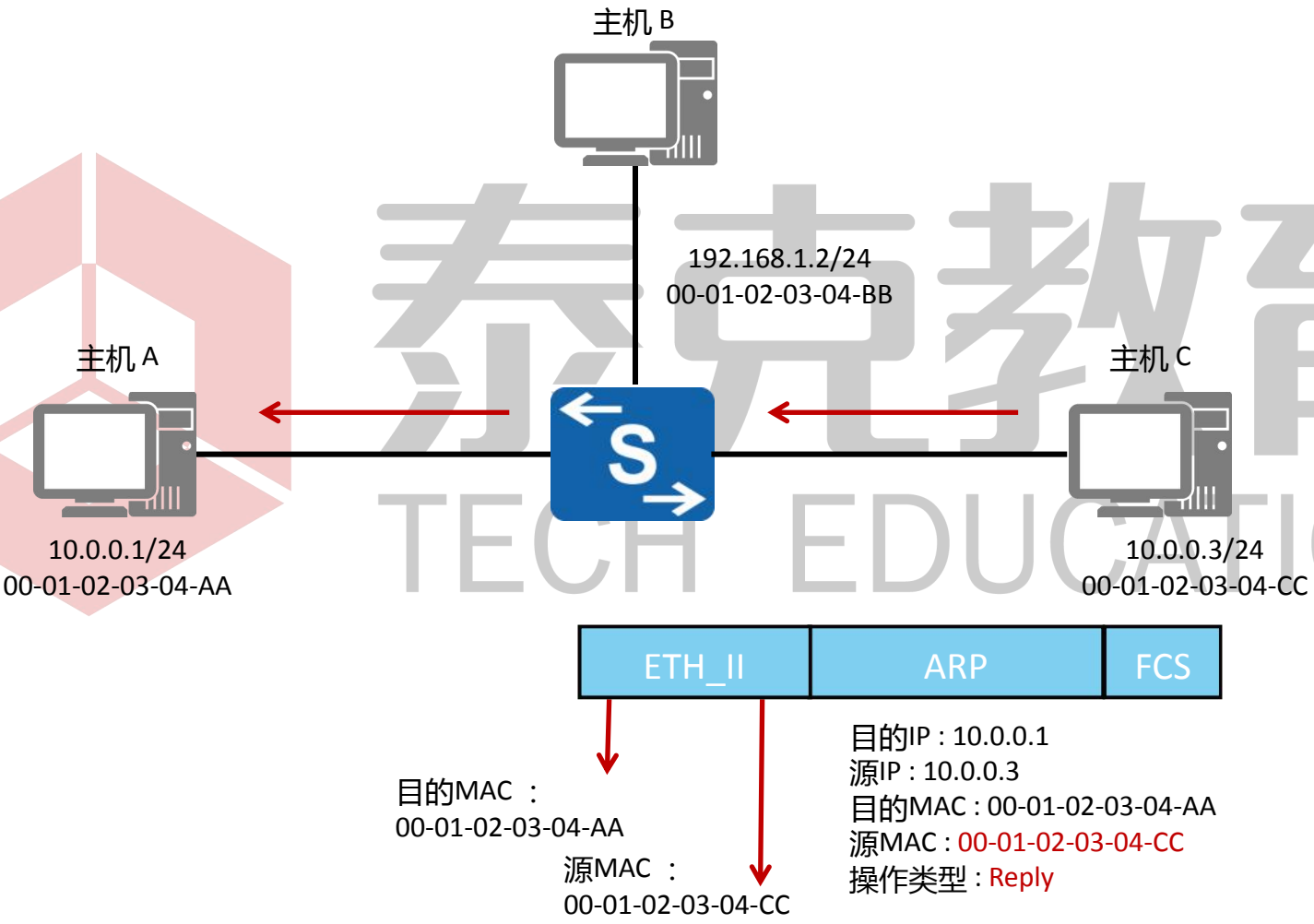


ARP响应（1）



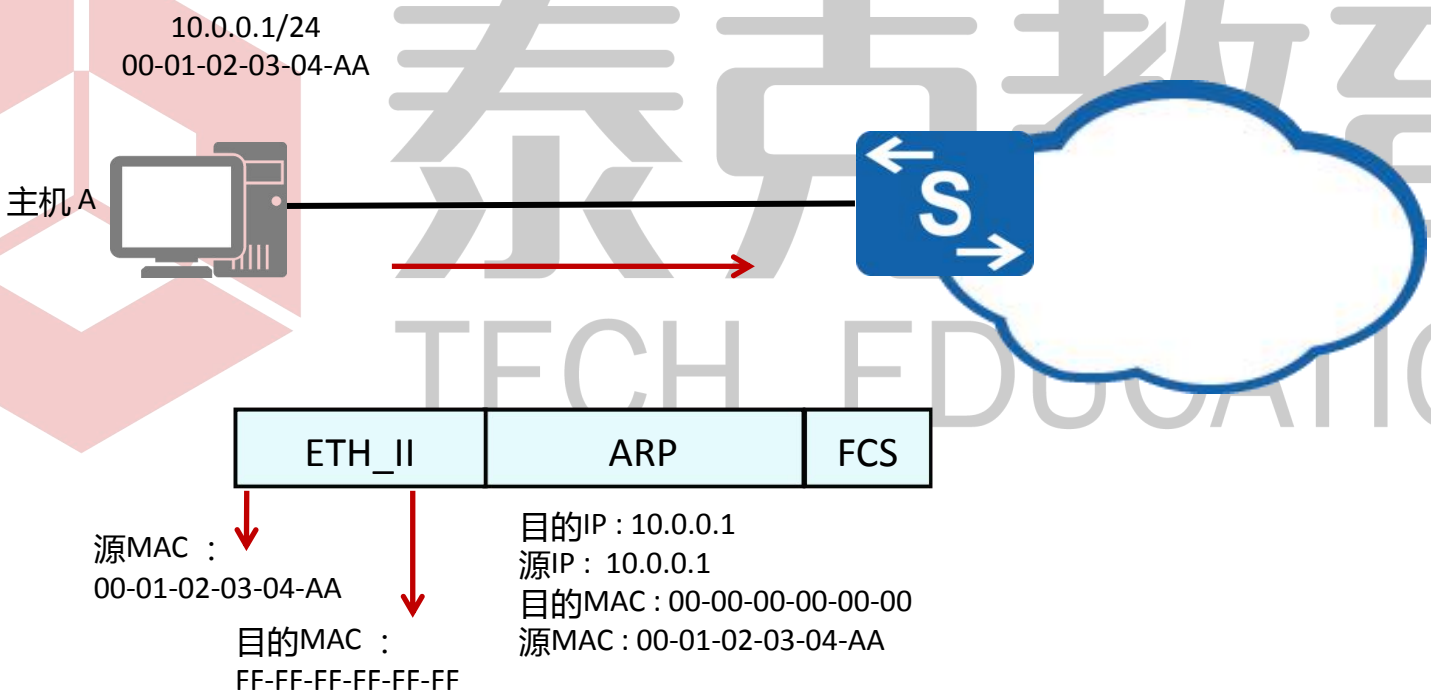

```
Host C>arp -a
Internet address  Physical address      Type
 10.0.0.1         00-01-02-03-04-AA     Dynamic
```

ARP响应 （2）



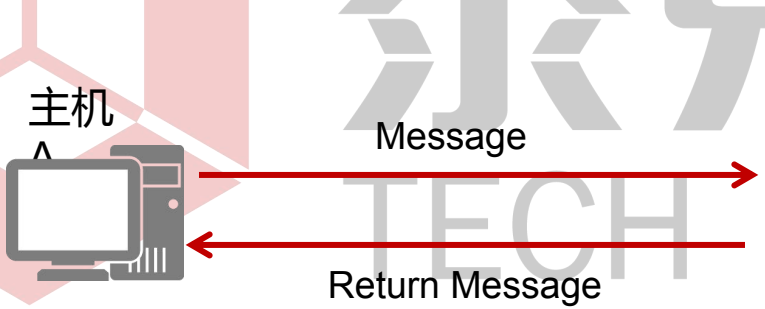
免费ARP

- 免费ARP可以用来探测IP地址是否冲突。

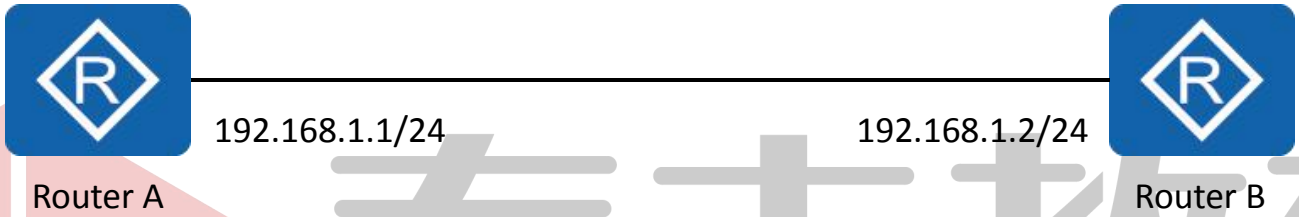


ICMP简介

- ICMP用来传递差错、控制、查询等信息。



ICMP应用 - Ping (1)



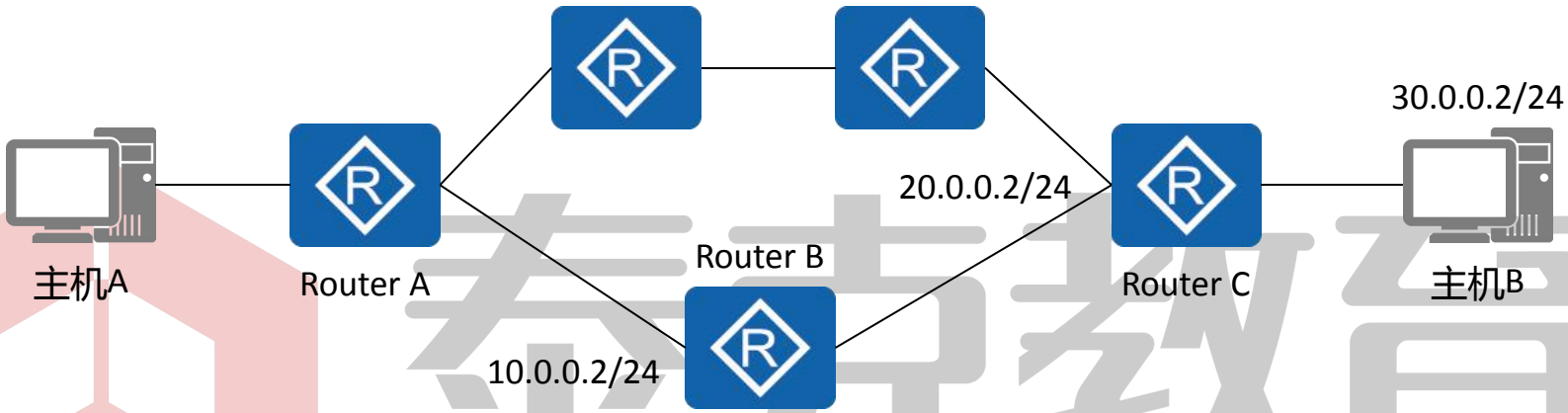

```
<Router A>ping ?
STRING<1-255> IP address or hostname of a remote system
-a            Select source IP address, the default is the IP address of the
              output interface
-c            Specify the number of echo requests to be sent, the default is
              5
-d            Specify the SO_DEBUG option on the socket being used
-f            Set Don't Fragment flag in packet (IPv4-only)
-h            Specify TTL value for echo requests to be sent, the default is
              255
-i            Select the interface sending packets
……
```

ICMP应用 - Ping (2)

```
[Router A]ping 192.168.1.2
  PING 192.168.1.2 : 56  data bytes, press CTRL_C to break
    Reply from 192.168.1.2 : bytes=56 Sequence=1 ttl=255 time=340 ms
    Reply from 192.168.1.2 : bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 192.168.1.2 : bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 192.168.1.2 : bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 192.168.1.2 : bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 192.168.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/88/340 ms
```

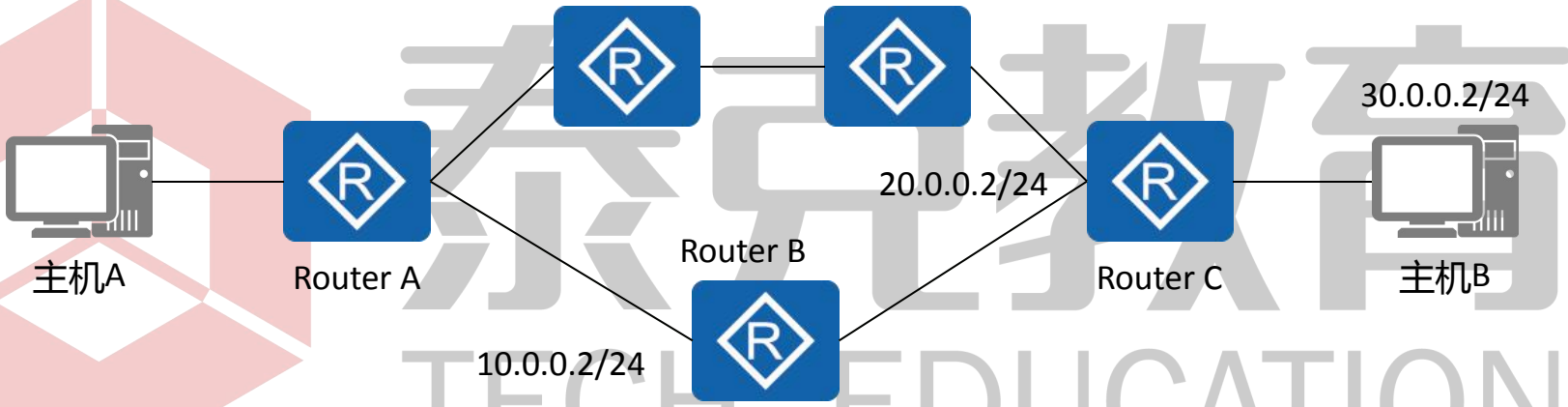
ICMP应用 - Tracert (1)




```
<Router A>tracert ?
STRING<1-255>  IP address or hostname of a remote system
-a             Set source IP address, the default is the IP address of the
               output interface
-f             First time to live, the default is 1
-m             Max time to live, the default is 30
-name          Display the host name of the router on each hop
-p             Destination UDP port number, the default is 33434
-q             Number of probe packet, the default is 3
-s             Specify the length of the packets to be sent. The default
               length is 12 bytes
……
```

ICMP应用 - Tracert (2)

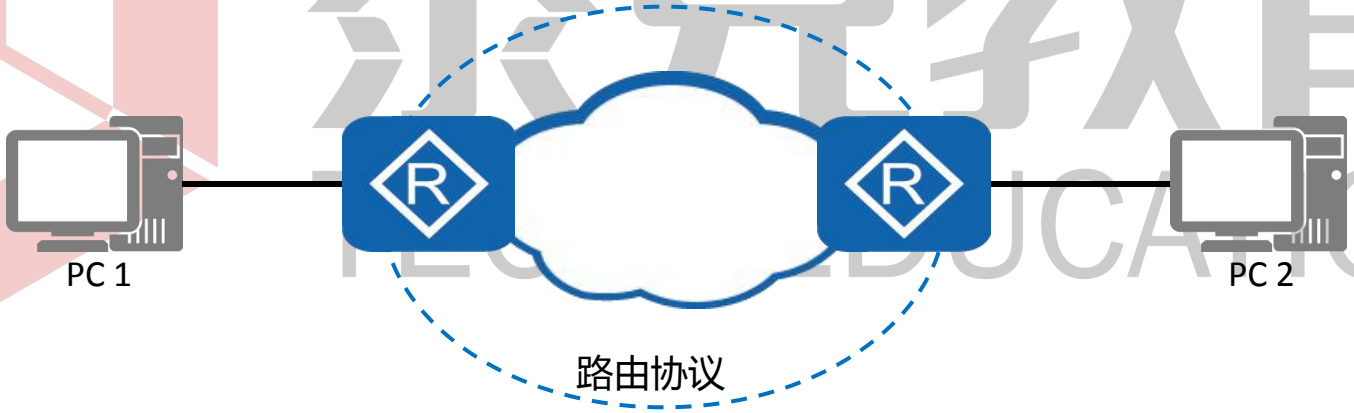
- Tracert显示数据包在网络传输过程中所经过的每一跳。




```
<Router A>tracert 30.0.0.2
Tracert to 30.0.0.2(30.0.0.2), max hops:30, packet length:40, press
CTRL_C to break
 1 10.0.0.2 130 ms  50 ms  40 ms
 2 20.0.0.2 80 ms  60 ms  80 ms
 3 30.0.0.2 80 ms  60 ms  70 ms
```

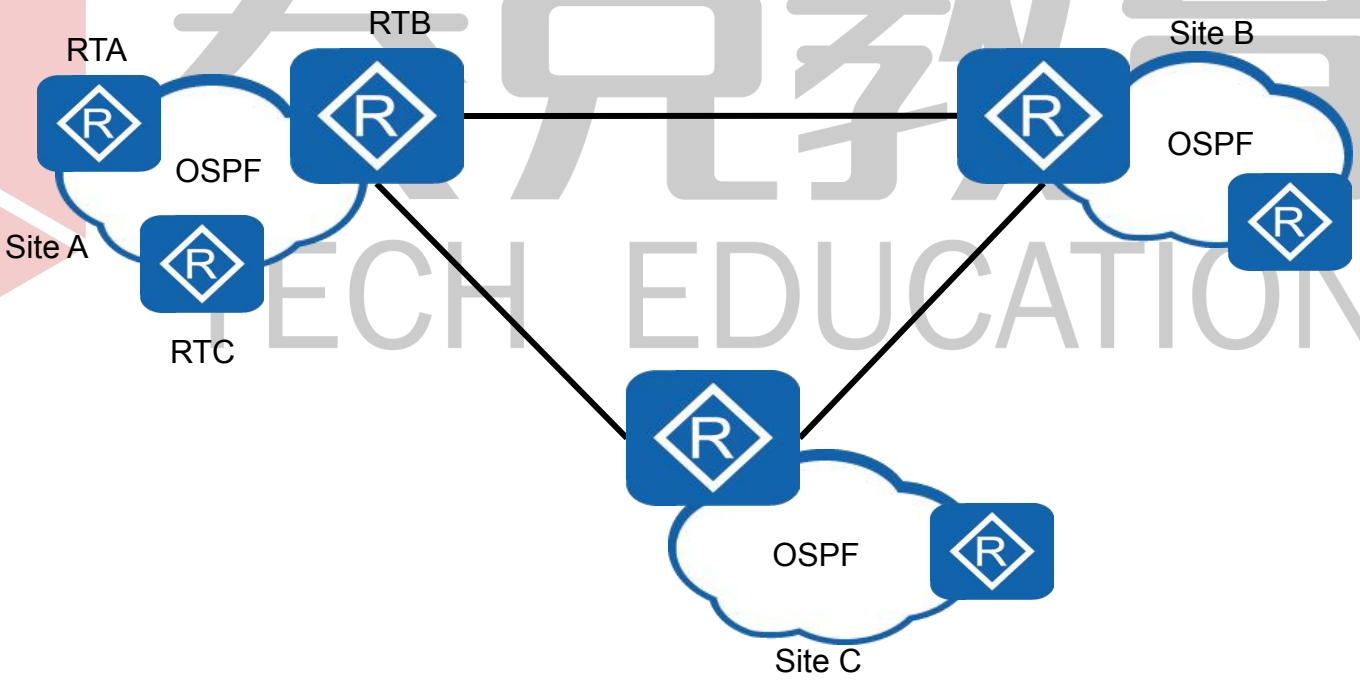
路由协议综述

- 路由是数据通信网络中最基本的要素。路由信息就是指导报文发送的路径信息，路由的过程就是报文转发的过程。



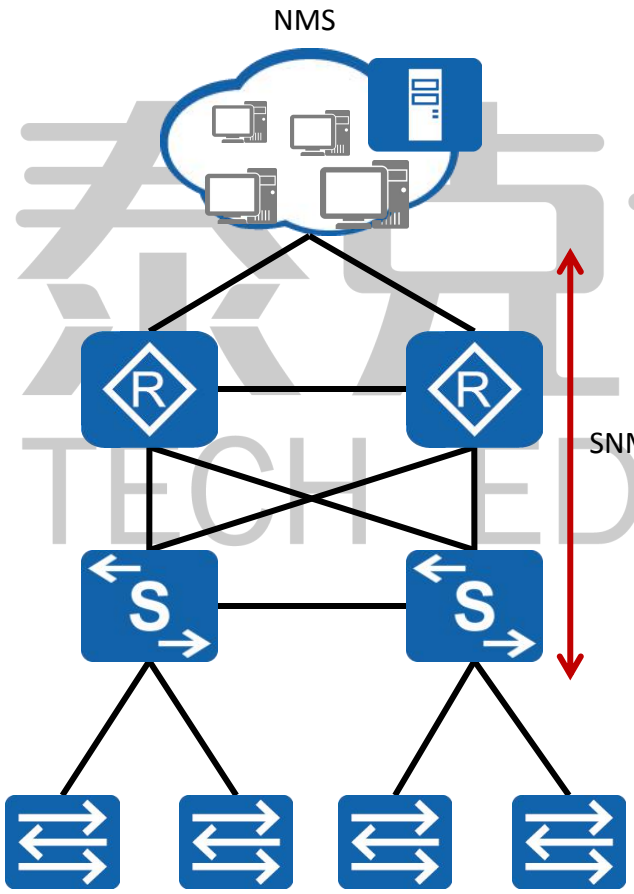
OSPF简介

- 无环路
- 收敛快
- 扩展性好
- 支持认证



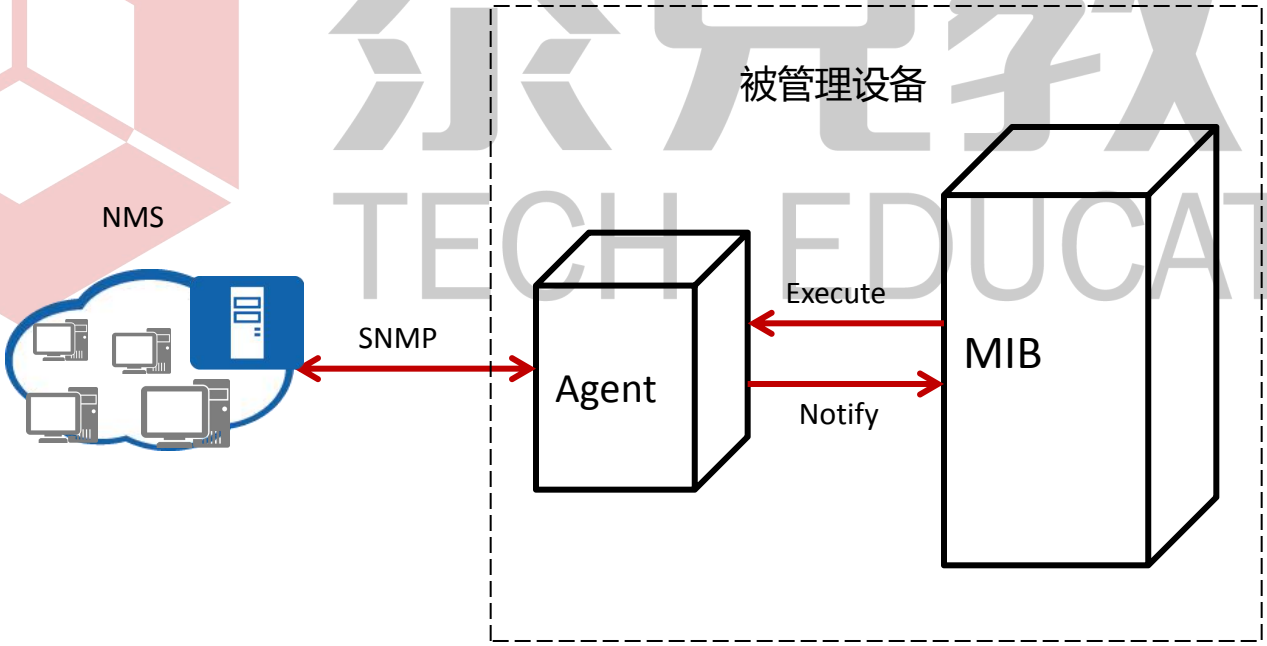
SNMP简介

- SNMP用来在网络管理系统NMS和被管理设备之间传输管理信息。

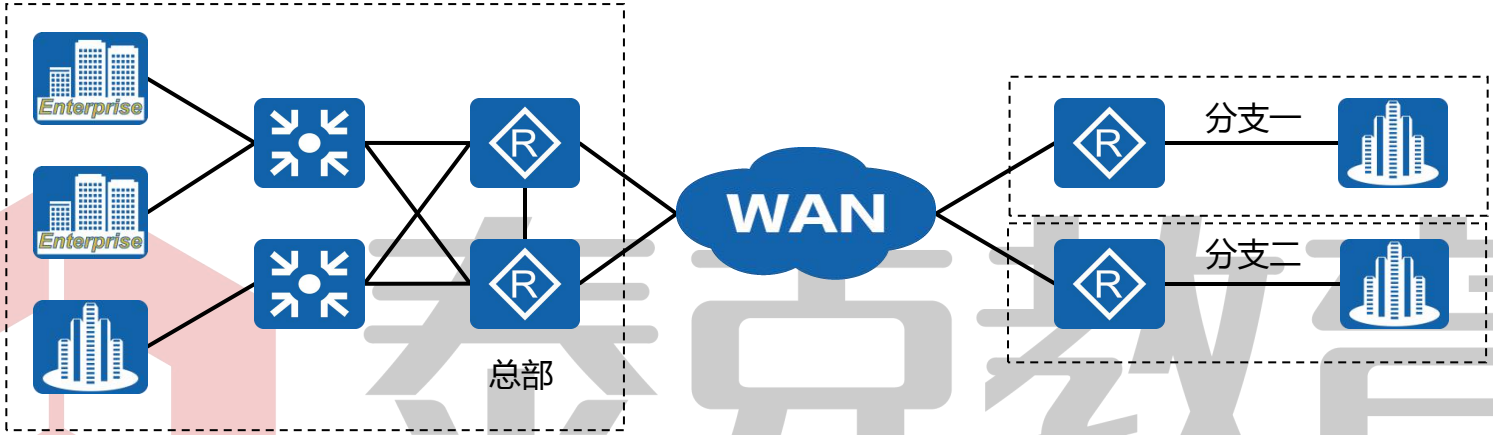


SNMP架构

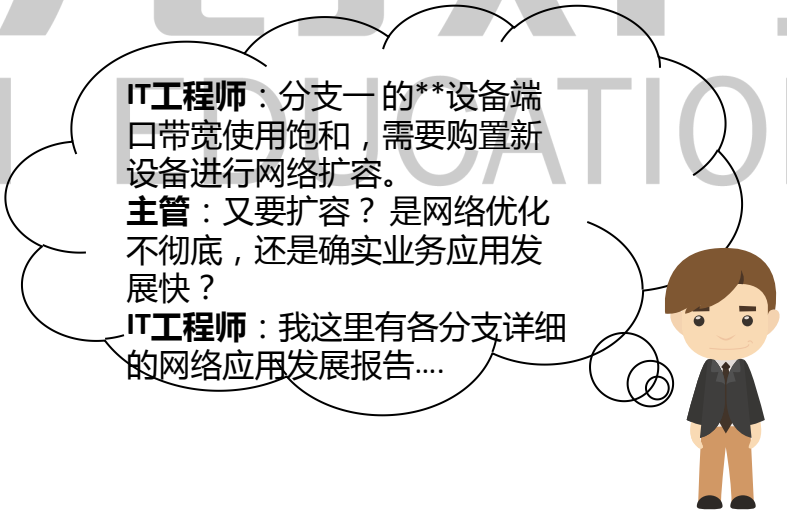
- SNMP包括NMS，Agent和MIB等。
- Agent是被管理设备中的一个代理进程。
- MIB是一个数据库，它包含了被管理设备所维护的变量。



企业网络运维



- 掌握所有分支的流量趋势，主动发现需要扩容的设备和分支。
- 分析分支增加流量的应用分布，找出扩容价值点。
- 整理分支流量变化，合理分配现有网络资源。

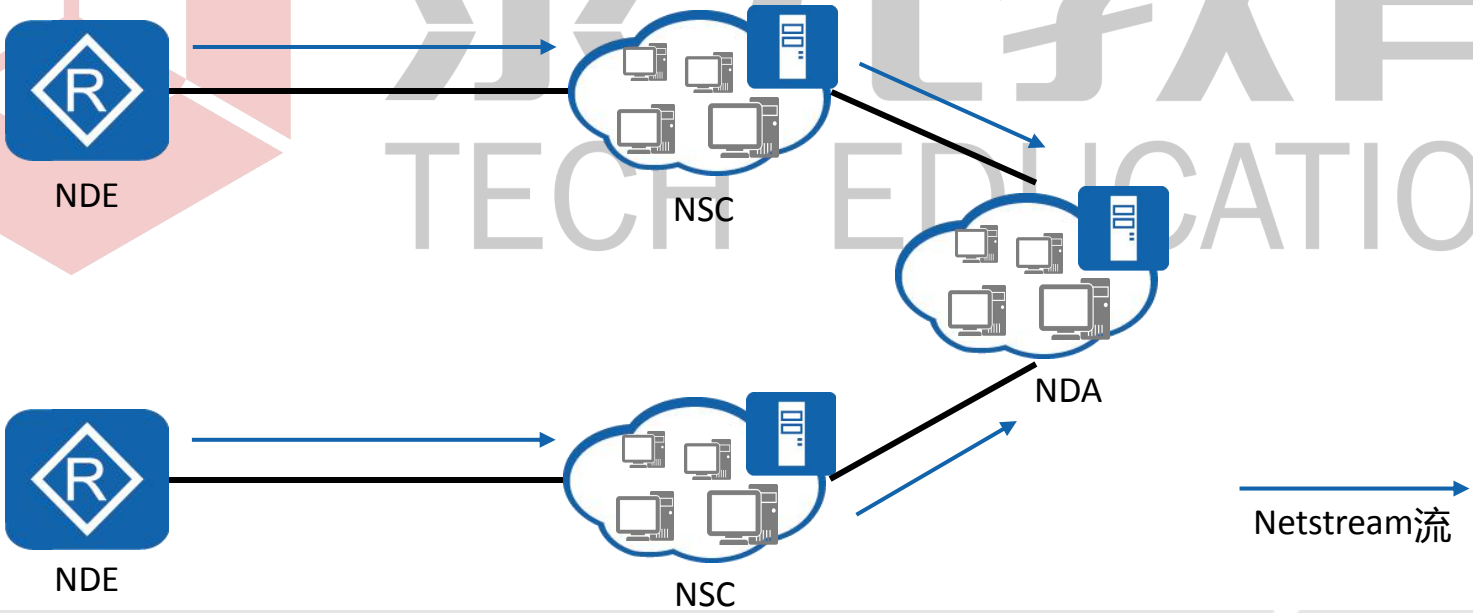


NTA概念及功能

- 基本概念
  - eSight NTA即网流分析系统（Network Traffic Analyzer）是纯软件解决方案，无需硬件探针，不会额外增加用户投资；通过NetFlow、NetStream、sFlow协议，对常见的IP报文进行采集和分析，提供贴近客户的分析报表，能实时准确的监控全网流量，是企业运维管理的一大利器。
- 功能简介
  - eSight NTA提供了一种便捷的网络监控、分析的方法，利用支持NetFlow/NetStream/sFlow等技术的网络设备提供的IP网络流量信息，深入分析全网流量，提供及时的流量分析报告，通过丰富的图表来展示流量分析结果，帮助用户全面了解全网流量，第一时间发现网络异常流量，了解整个网络中的流量分布。

NetStream简介

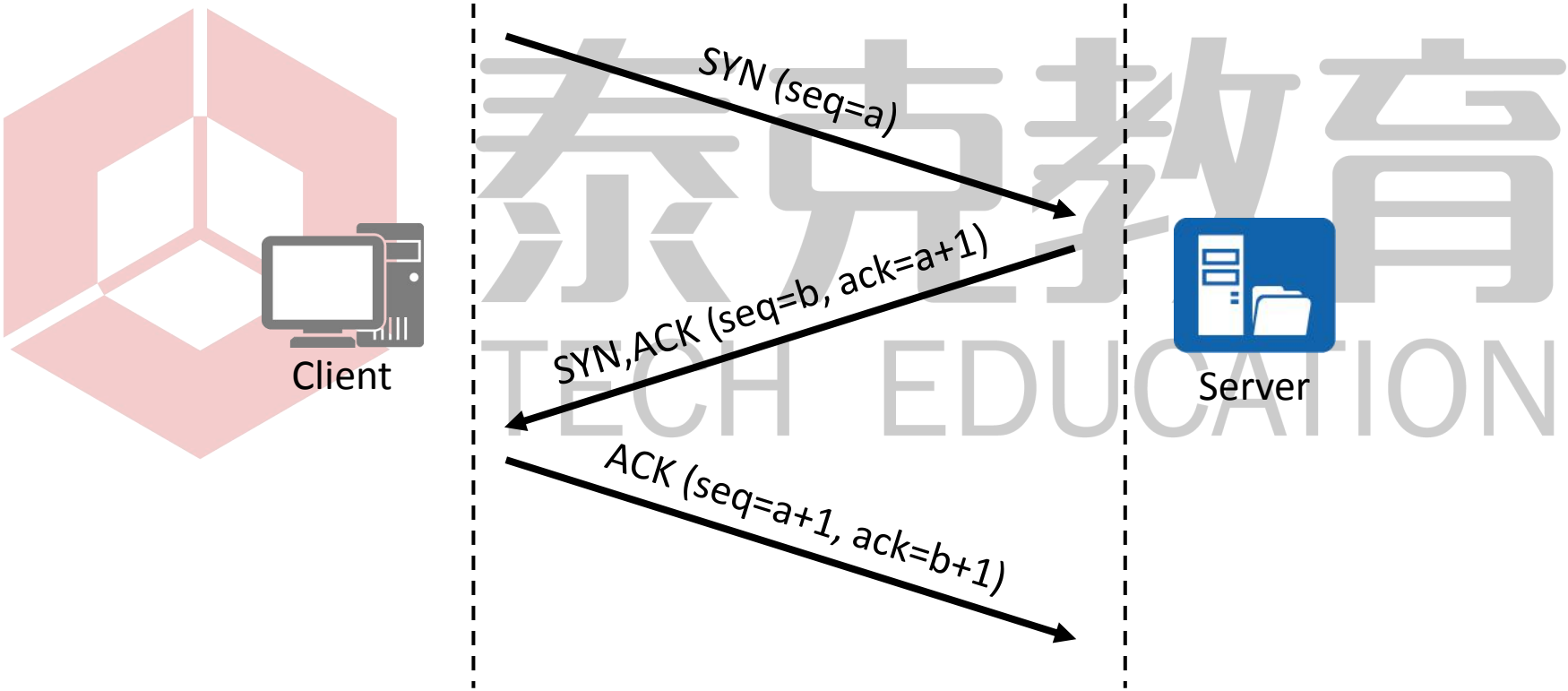
- NetStream是华为技术有限公司的专利技术，是一种网络流信息的统计与发布技术。NDE把获得的统计信息定期向NSC发送，由NSC进行进一步的处理，然后交给后续的NDA进行数据分析，分析的结果为网络计费与规划提供依据。



目录

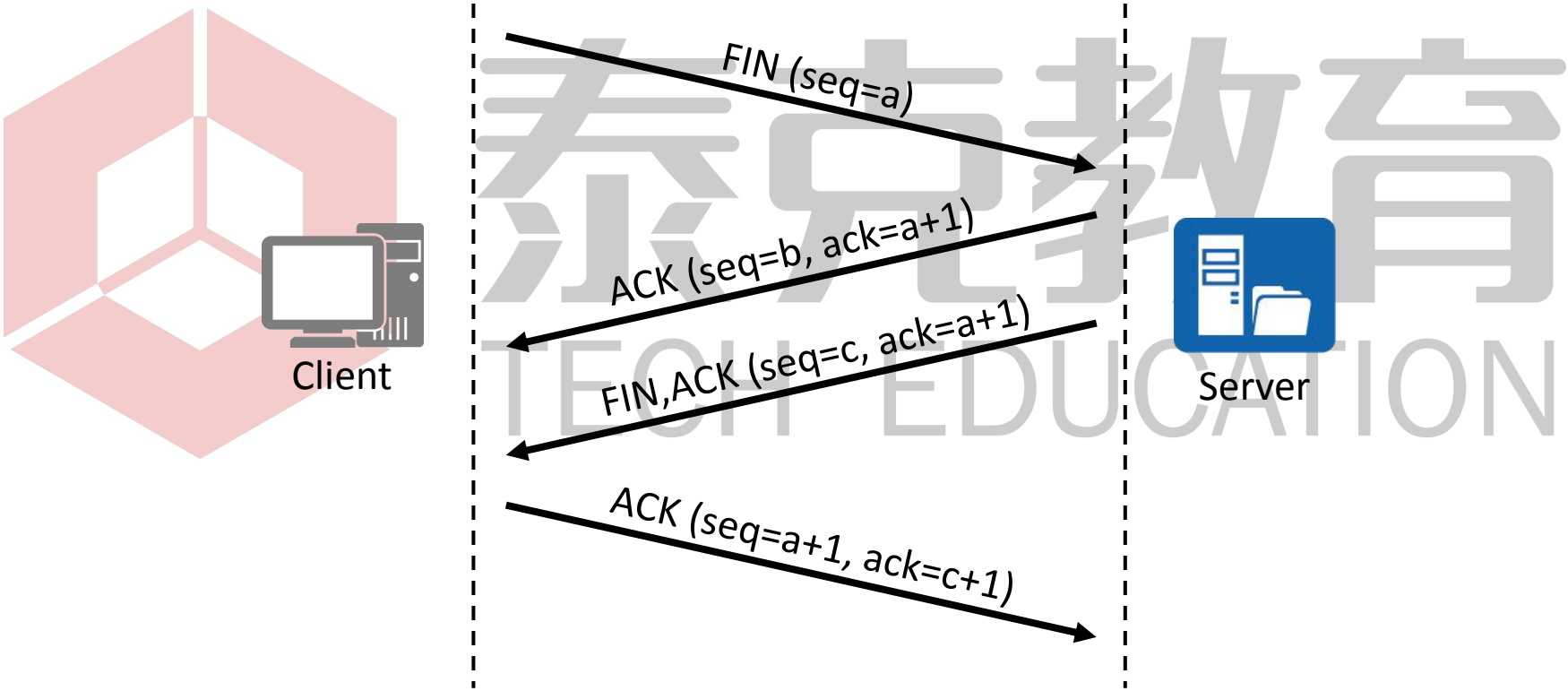
建立TCP连接

- 三次握手



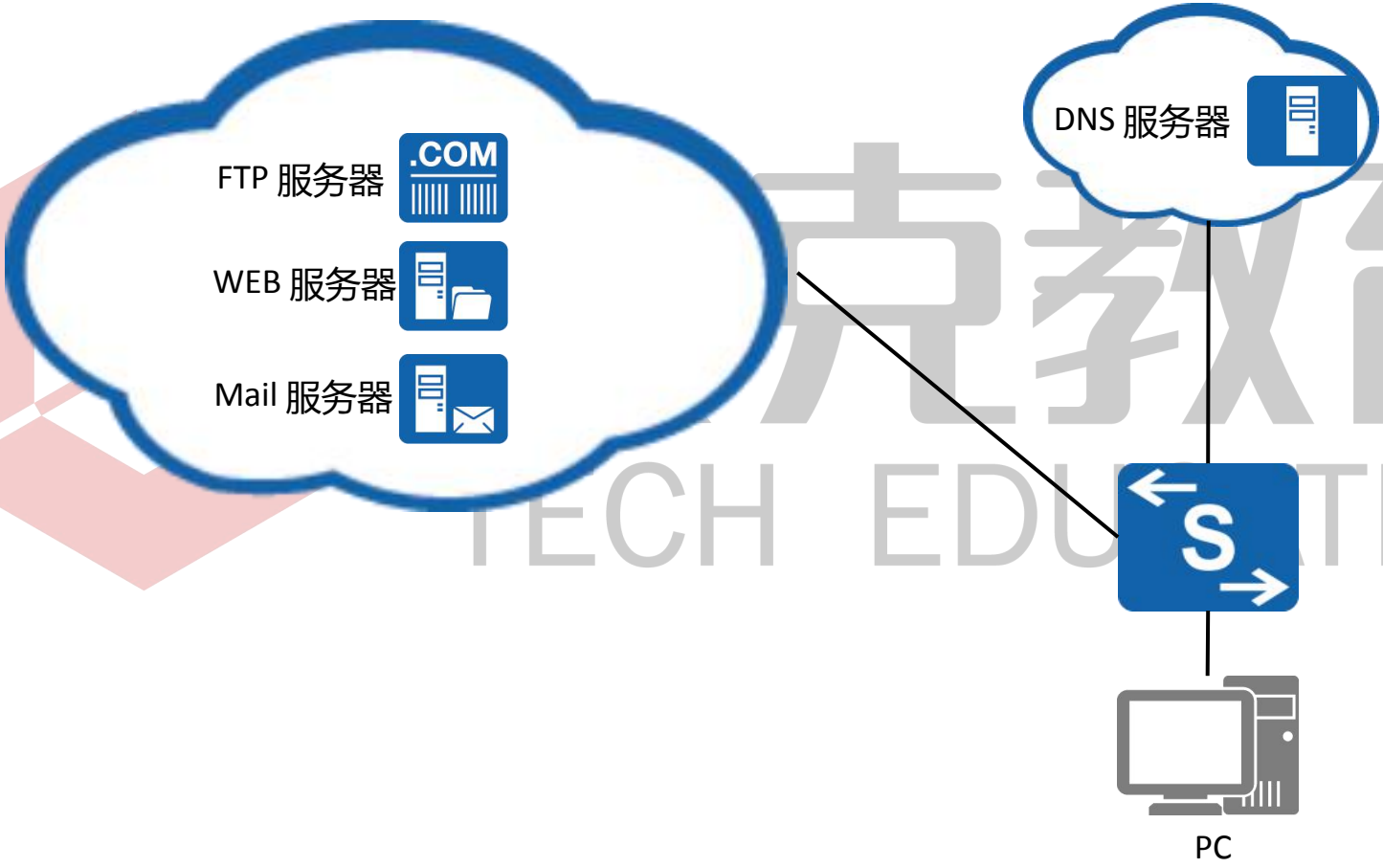
断开TCP连接

- 四次挥手



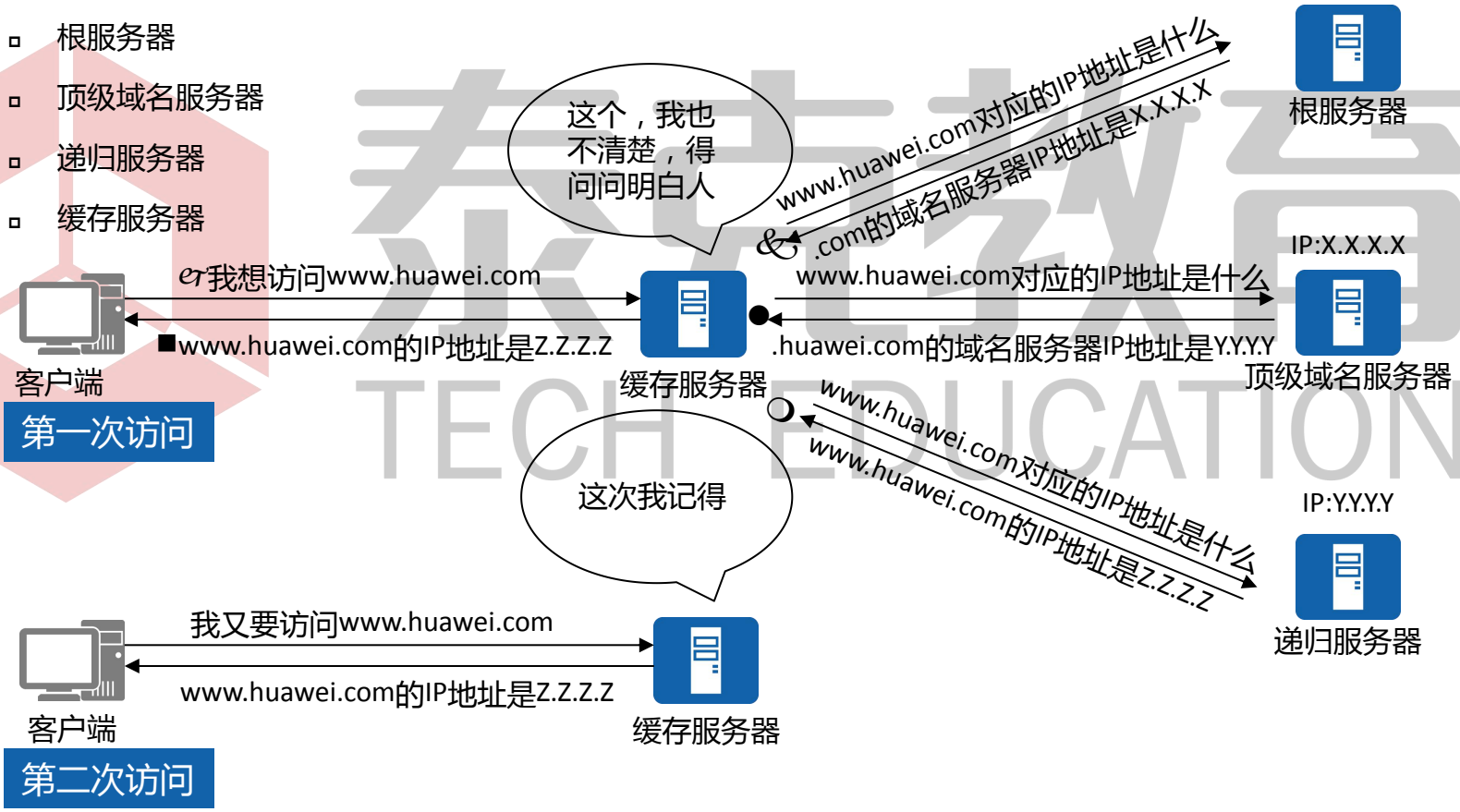
目录

常见应用层协议



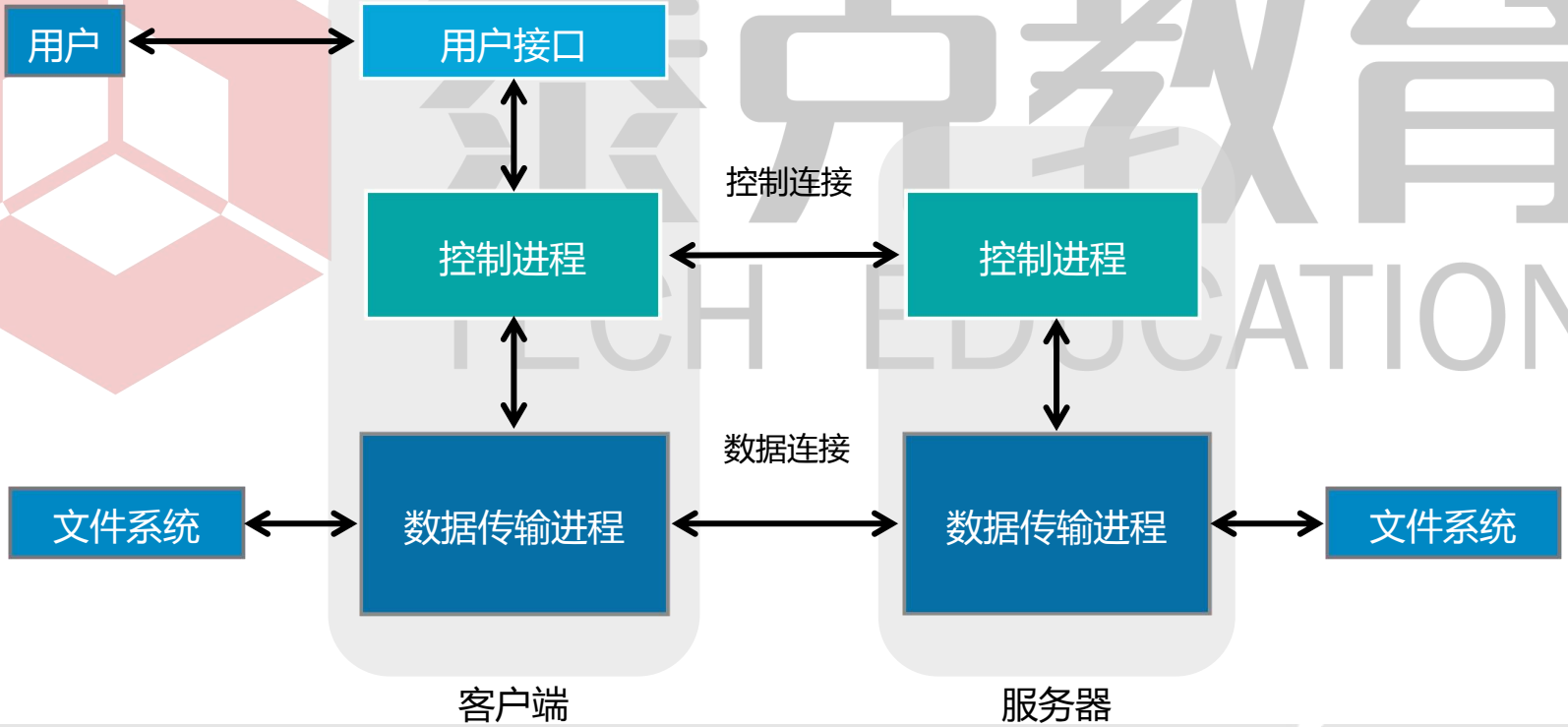
DNS工作原理

- 域名解析要由专门的域名解析系统（Domain Name System，简称DNS）来完成。在DNS系统中，涉及以下几种类型的服务器：
  - 根服务器
  - 顶级域名服务器
  - 递归服务器
  - 缓存服务器



FTP原理

- FTP 提供了一种在服务器和客户机之间上传和下载文件的有效方式。
- 使用FTP传输数据时，需要在服务器和客户机之间建立控制连接和数据连接。



FTP传输模式（1）

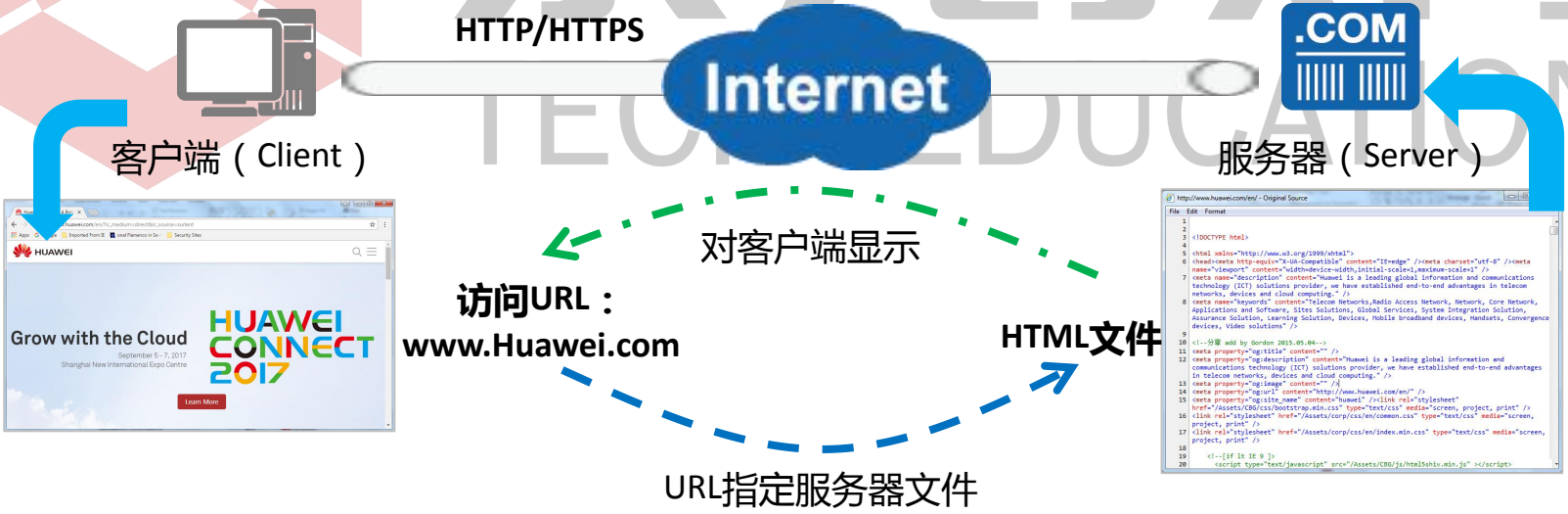
- FTP连接的建立分为主动模式和被动模式，两者的区别在于数据连接是由服务器发起还是由客户端发起。缺省情况下采用主动模式，用户可以通过命令切换。
- 主动模式下FTP连接建立：

FTP传输模式（2）

- 被动模式FTP连接建立:

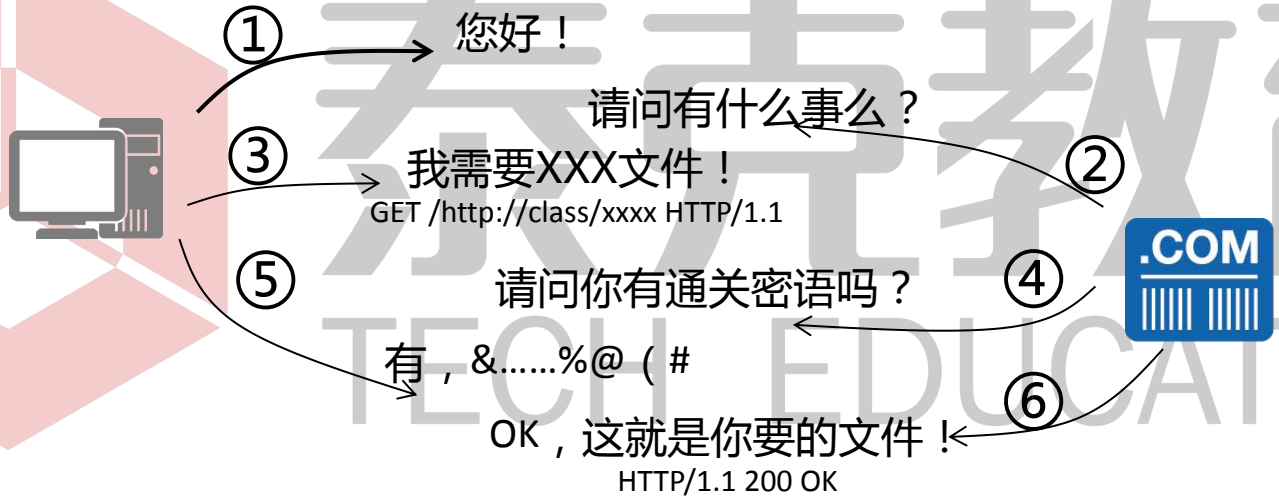
HTTP/HTTPS - Web应用基本组成部分

- Web基于客户端（Client）/服务器（Server）架构实现，包含三个部分：
  - 使用HTML（HyperText Mark-up Language）描述文件
  - 使用URL（Uniform Resource Locator）指定文件的所在
  - 透过HTTP（HyperText Transfer Protocol）协议与服务器沟通



HTTP工作原理

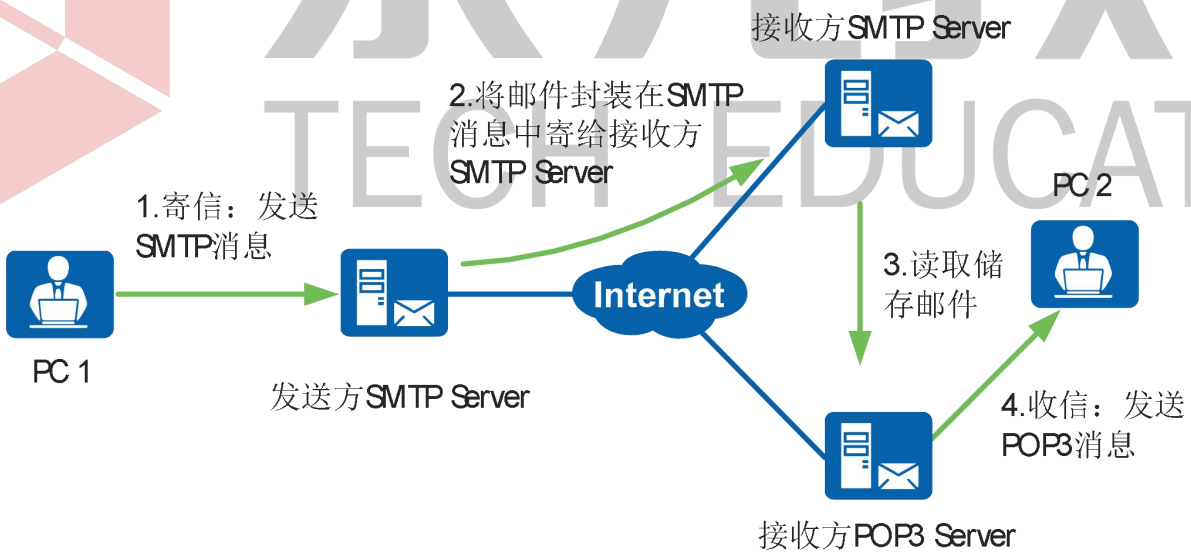
- HTTP（Hypertext Transfer Protocol）是一种无状态的协议，基于简单的请求 - 响应模式（requests/responses）。



- HTTP有两类报文：
  - 请求报文—从客户端向服务器发送请求报文。
  - 响应报文—从服务器到客户端的回答。

SMTP/POP3/IMAP - 邮件收发机制

- SMTP定义了计算机如何将邮件发送到SMTP Server，SMTP Server之间如何中转邮件。
- POP3（Post Office Protocol 3，邮局协议版本3）和IMAP（Internet Mail Access Protocol，交互式邮件存取协议）规定计算机如何通过客户端软件管理、下载邮件服务器上的电子邮件。
- 基于该种方式，网络管理员需要在邮件服务器上部署SMTP服务、POP3服务（或IMAP服务）；终端用户需要在PC上安装邮件客户端软件（例如MicroSoft OutLook、FoxMail等邮件管理软件）。



思考题

1. 以下哪个不属于TCP/IP协议簇？（　）

   A. 数据链路层

   B. 传输层

   C. 会话层

   D. 应用层

2. 以下哪个报文是TCP三次握手的首包？（　）

   A. SYN+ACK

   B. SYN

   C. ACK

   D. FIN

本章总结

- TCP/IP架构
- 常见网络协议介绍

谢谢

www.huawei.com