SANGFOR
深信服科技

计算机网络基础

深信服科技研发专业能力系列课程

讲师介绍

SANGFOR 深信服科技

姓名：翟云箭

部门：创新研究院

联系电话：15521135871
电子邮箱：zhaiyunjian@sangfor.com.cn

职位职称：
研发工程师，项目经理

SANGFOR
深信服科技

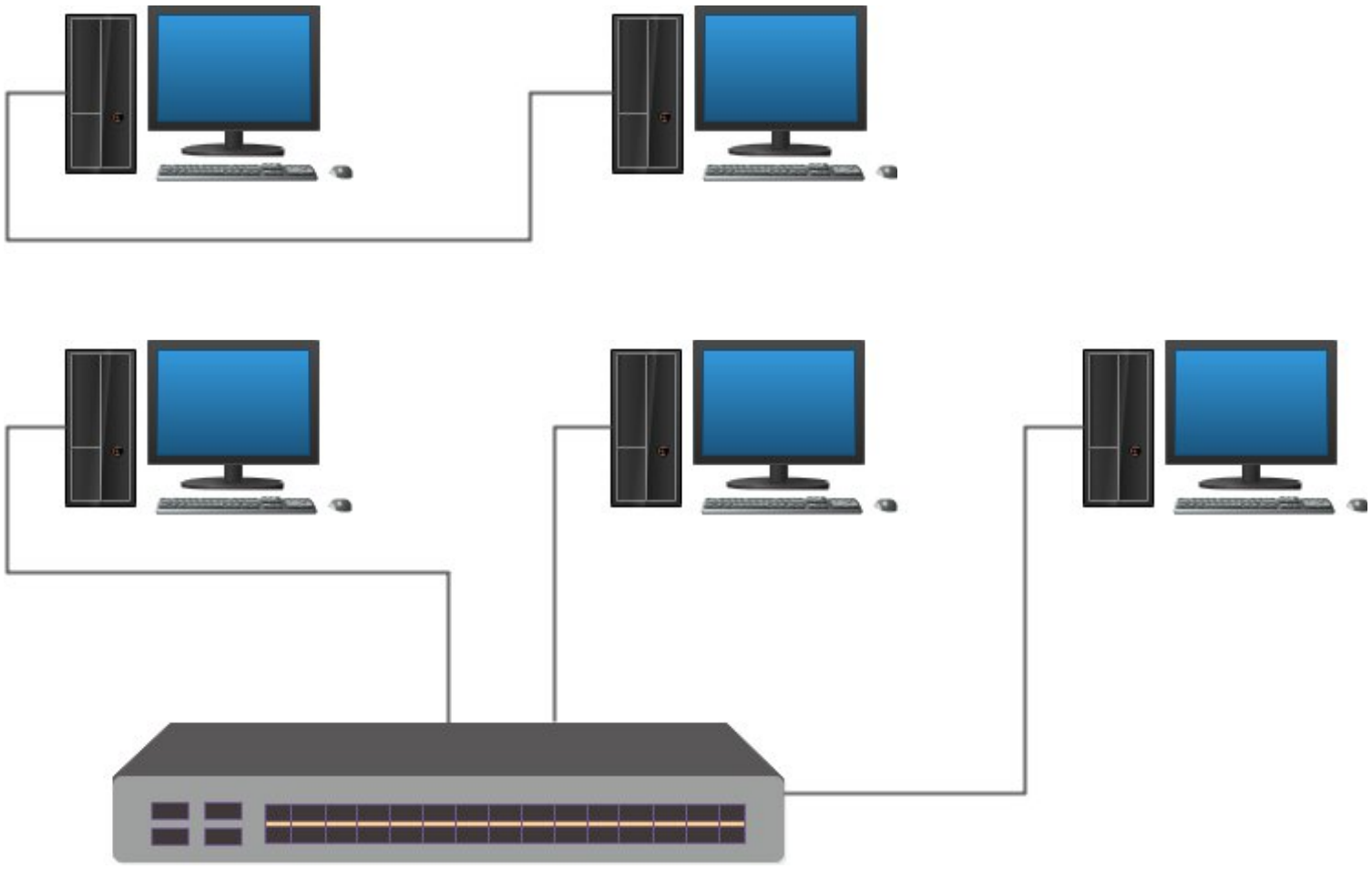
目录

SANGFOR
深信服科技

TCP/IP协议模型

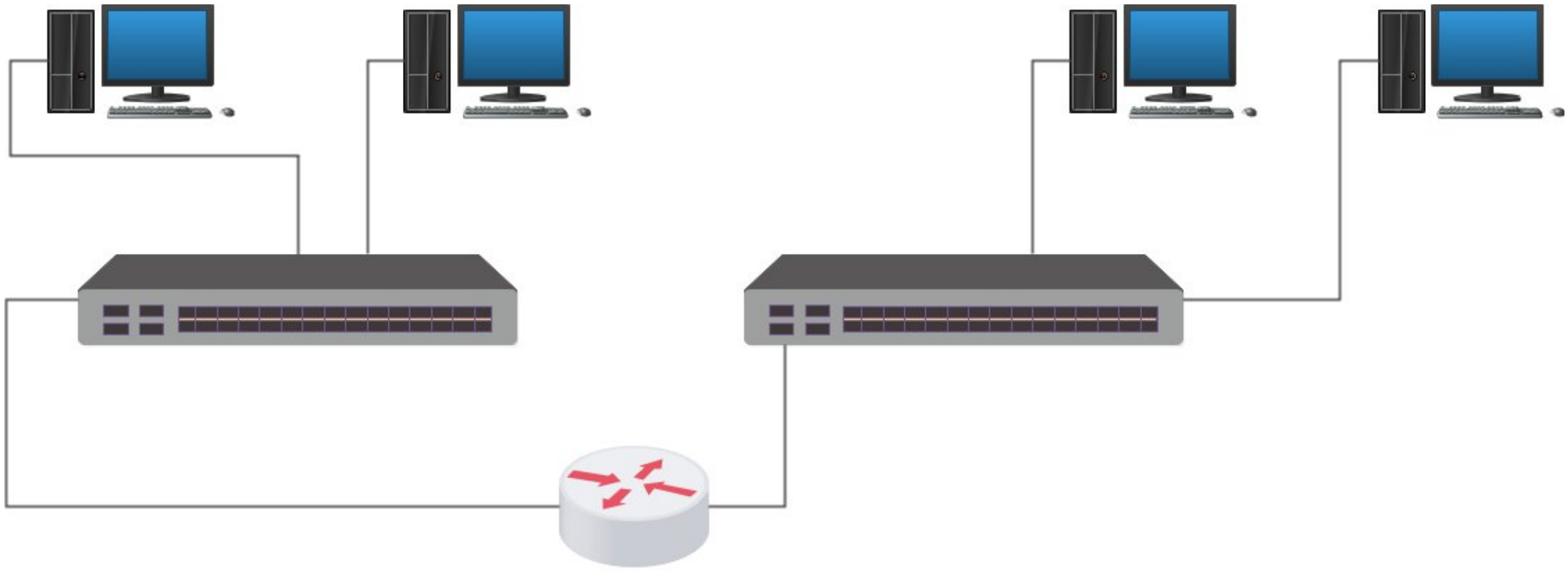
历史

SANGFOR
深信服科技

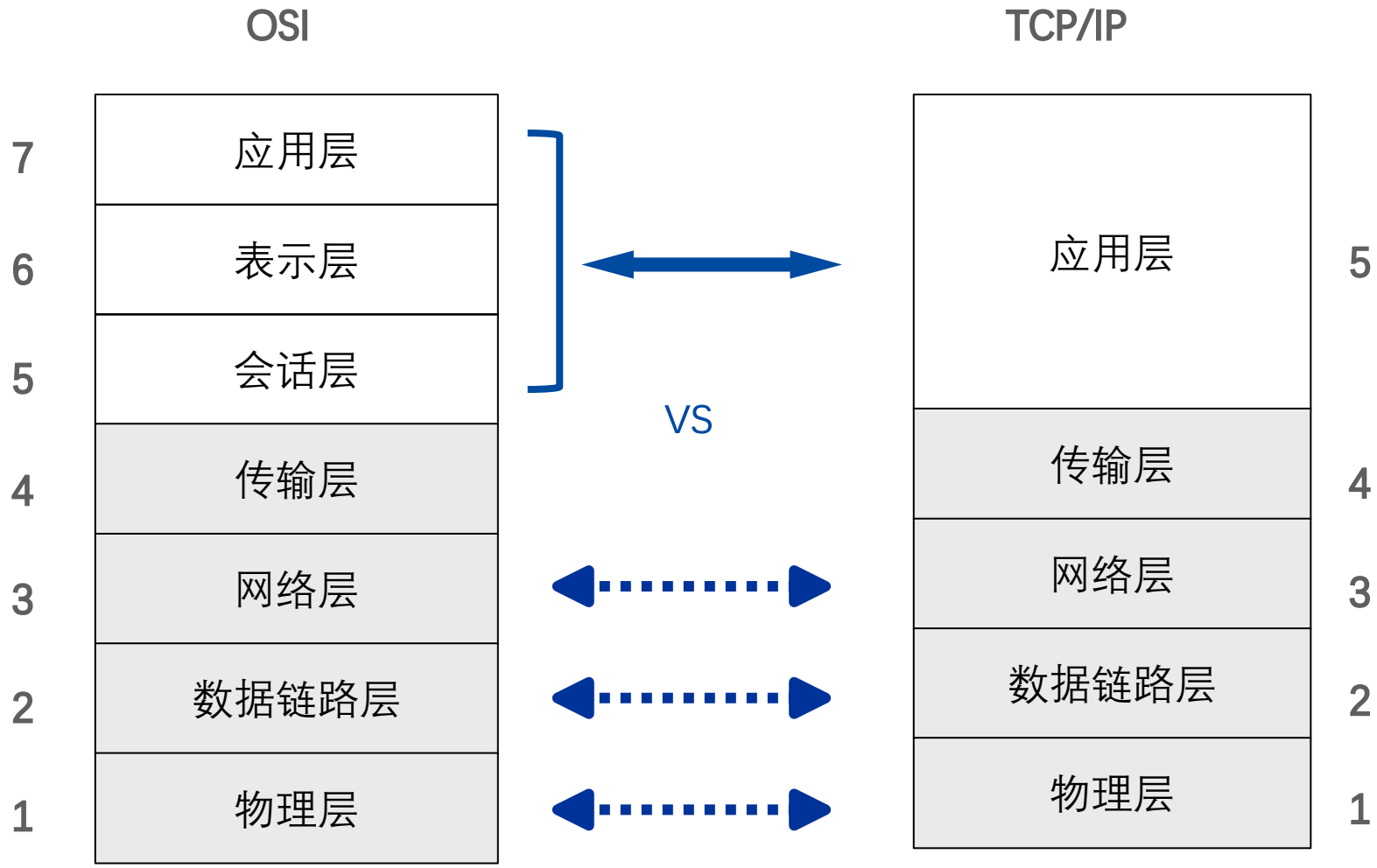


历史

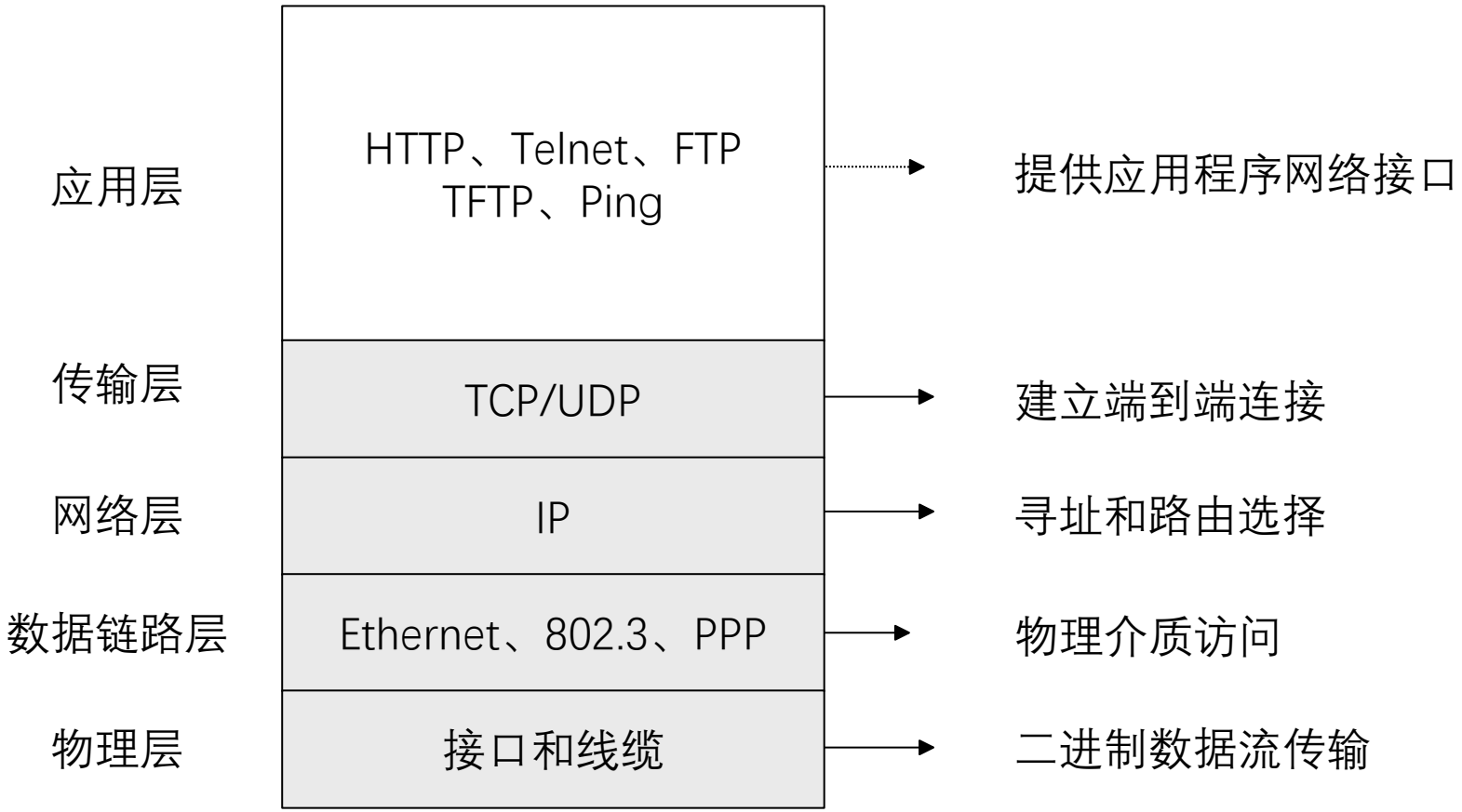
SANGFOR
深信服科技



TCP/IP层次

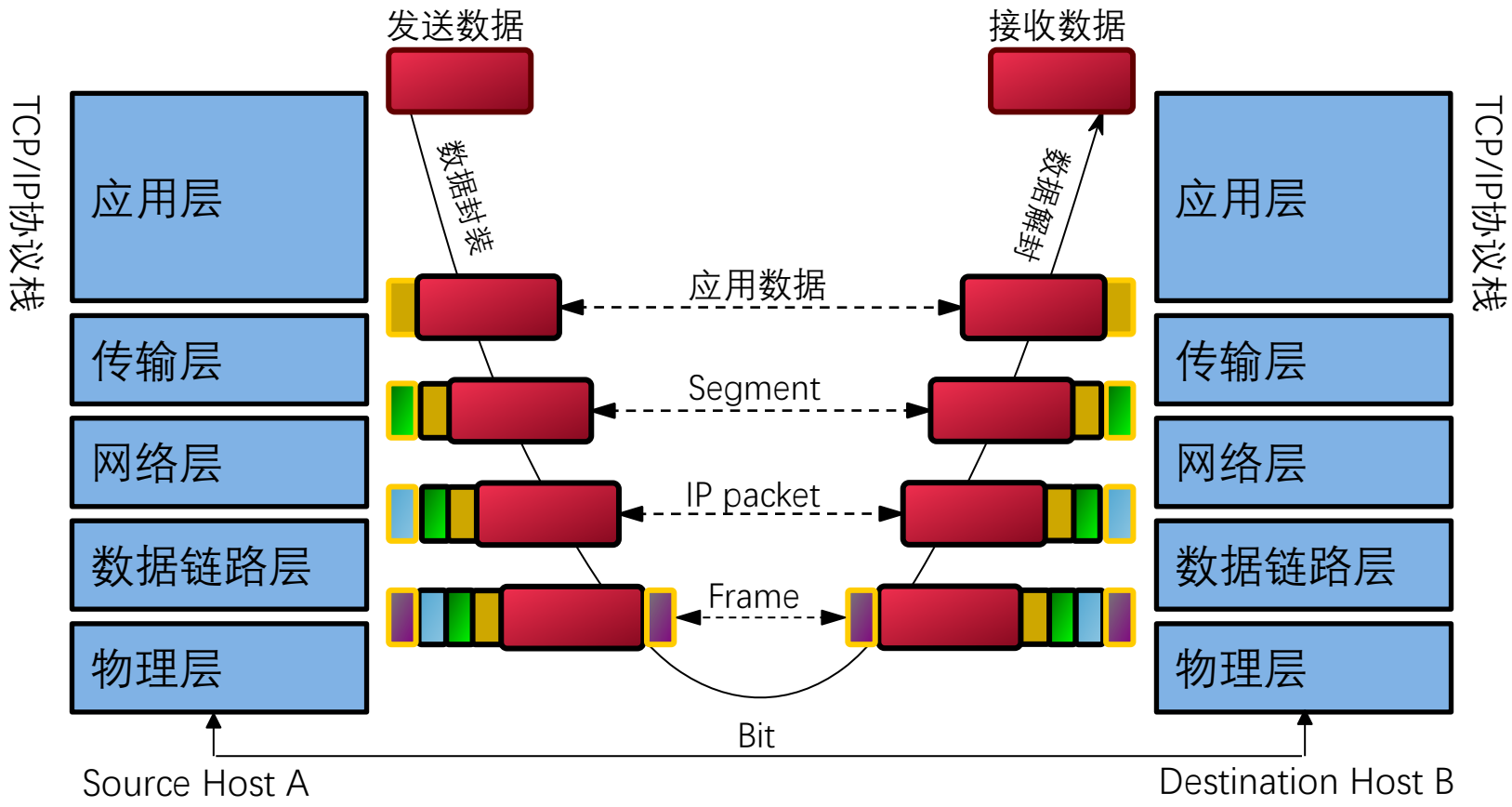

OSI
TCP/IP
7
应用层
6
表示层
5
会话层
4
传输层
3
网络层
2
数据链路层
1
物理层
VS
应用层
5
传输层
4
网络层
3
数据链路层
2
物理层
1

TCP/IP协议栈


应用层
HTTP、Telnet、FTP
TFTP、Ping
提供应用程序网络接口
传输层
TCP/UDP
建立端到端连接
网络层
IP
寻址和路由选择
数据链路层
Ethernet、802.3、PPP
物理介质访问
物理层
接口和线缆
二进制数据流传输

数据包的封装与解封装

- TCP/IP协议是网络设备之间通信规则的正式描述

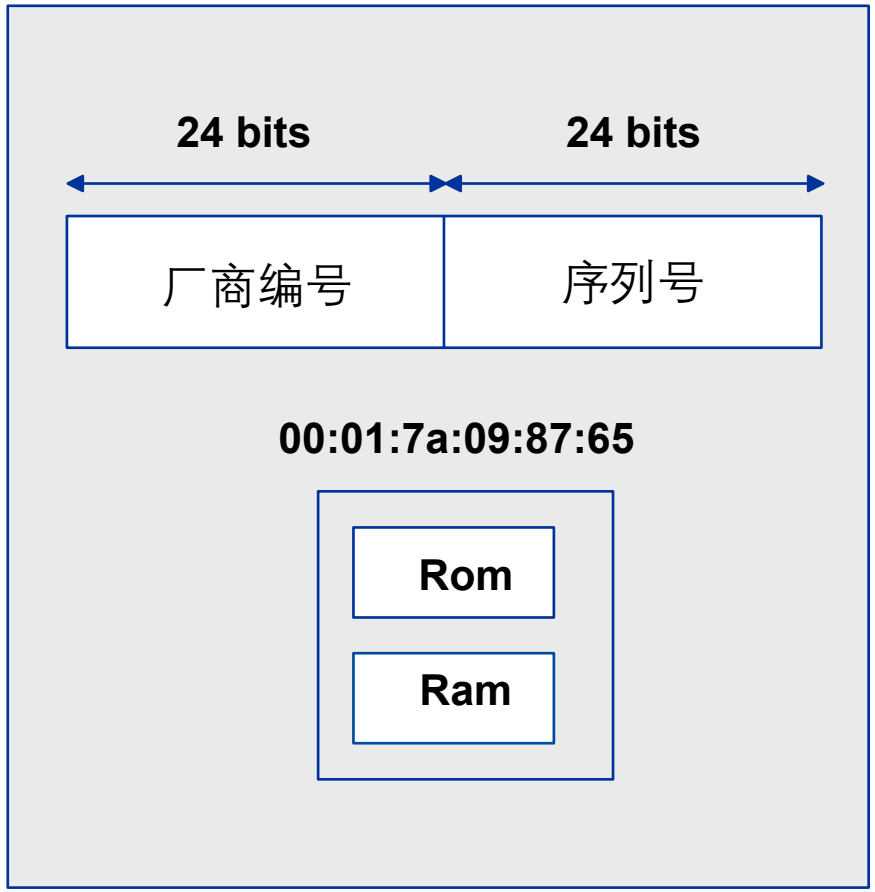


SANGFOR
深信服科技

数据链路层

MAC地址

00:01:7a:09:87:65



ARP地址解析协议

SANGFOR 深信服科技

ARP用来实现以太网中IP地址与MAC地址之间的映射，是以太网通信的基础

根据ARP表项的生成方式不同，可以将ARP表项分为**动态ARP**表项和**静态ARP**表项。两者的区别在于：

- 动态ARP表项由ARP协议通过ARP报文自动生成和维护，可以被老化，可以被新的动态ARP表项更新，也可以被静态ARP表项覆盖。
- 静态ARP表项由网络管理员手工配置生成和维护，不会被老化，也不会被动态ARP表项覆盖。

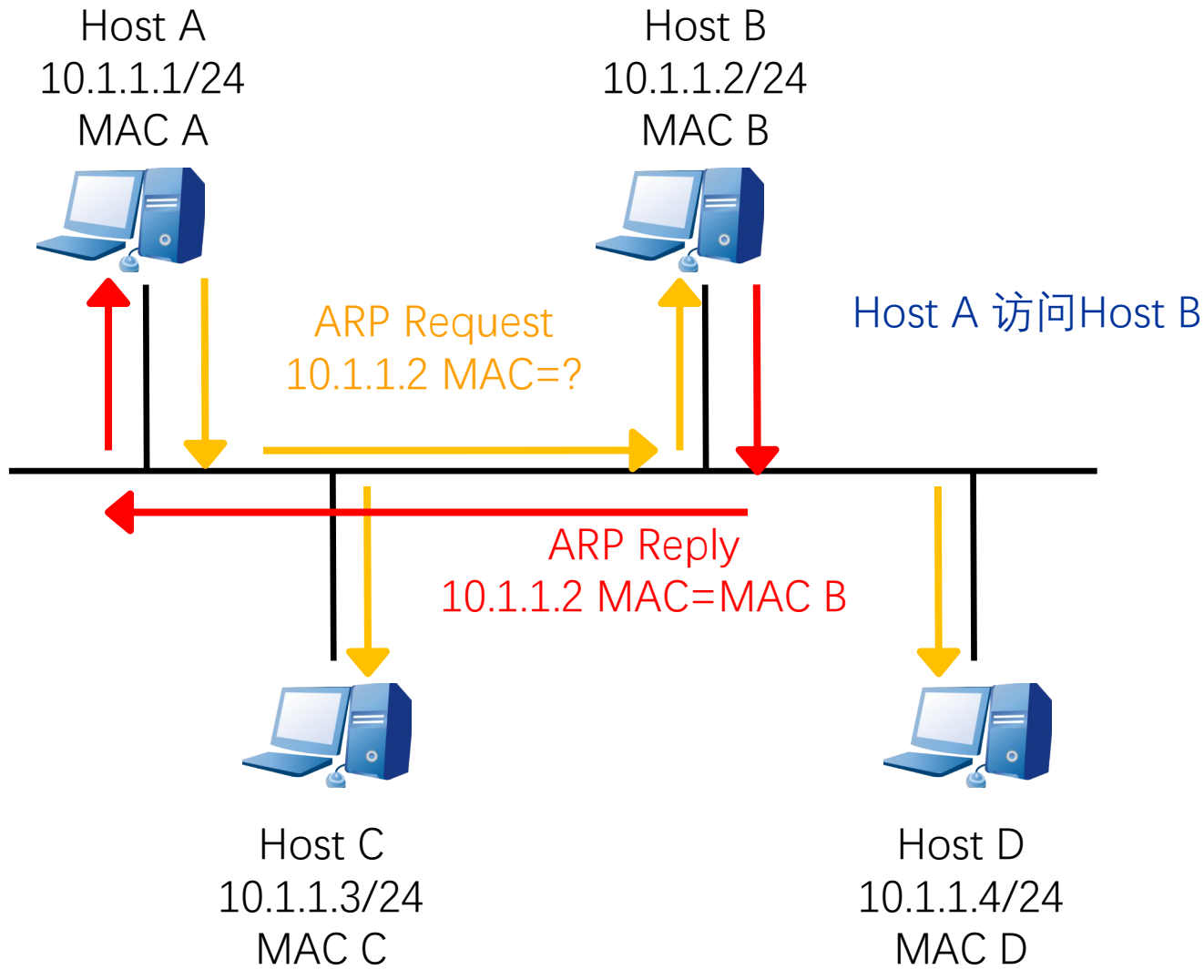
主机在每次发送数据报文前，都会先在ARP表中查找目的IP地址所对应的MAC地址。

- ARP表中有对应的MAC地址时，主机就不会再发送ARP请求报文，而是直接使用该MAC地址。
- ARP表中没有对应的MAC地址时，主机才会广播发送ARP请求报文，请求目的主机的MAC地址。

动态ARP—同网段解析

目的IP与自己在同网段：

- ARP Request （广播）请求MAC
- ARP Reply（单播）回应MAC

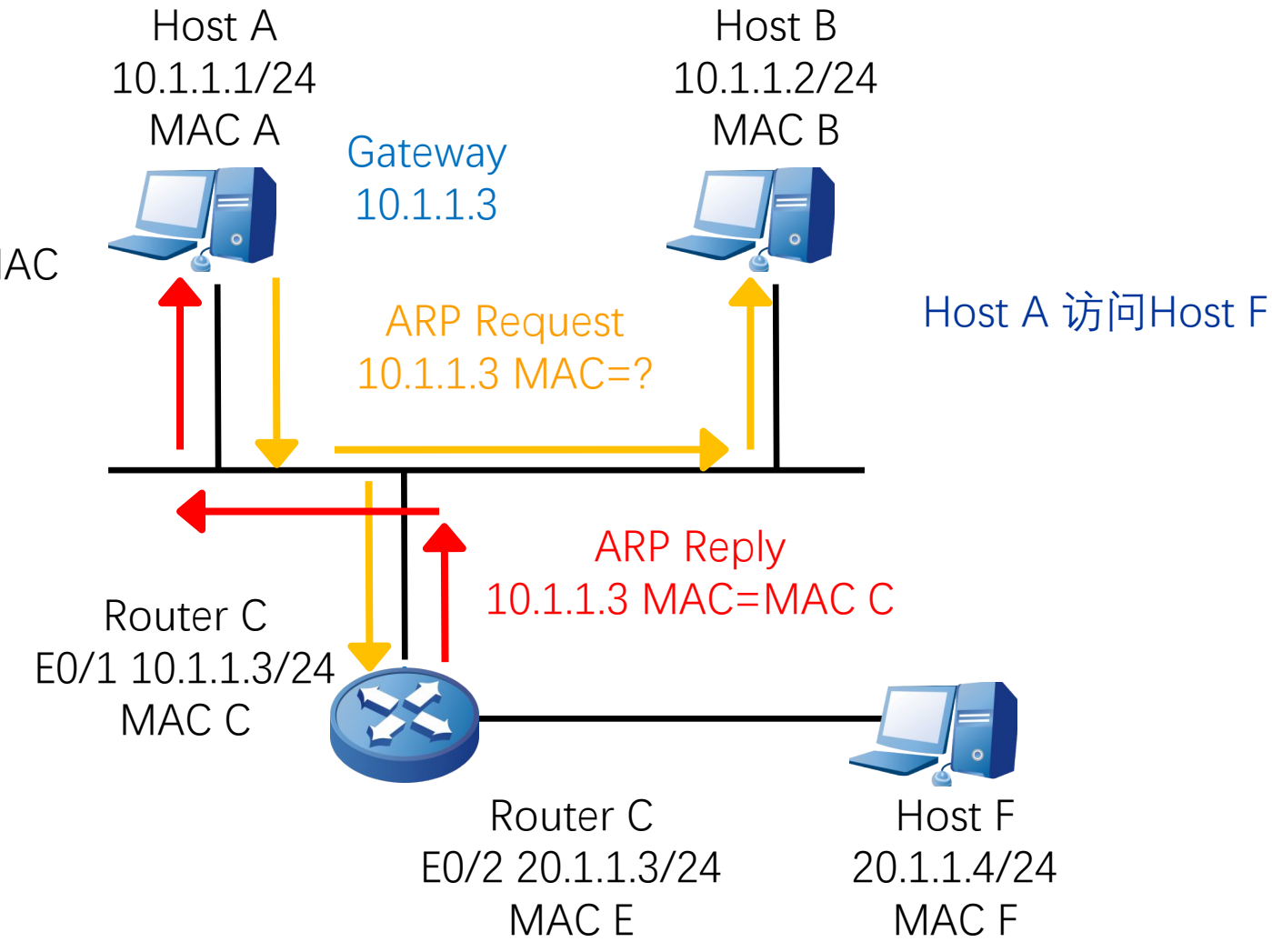


动态ARP—不同网段解析

目的IP与自己在不同网段：

- 数据源端需配置网关IP
- ARP Request （广播）请求网关MAC
- ARP Reply（单播）回应网关MAC

动态ARP表项能被更新，存在老化时间

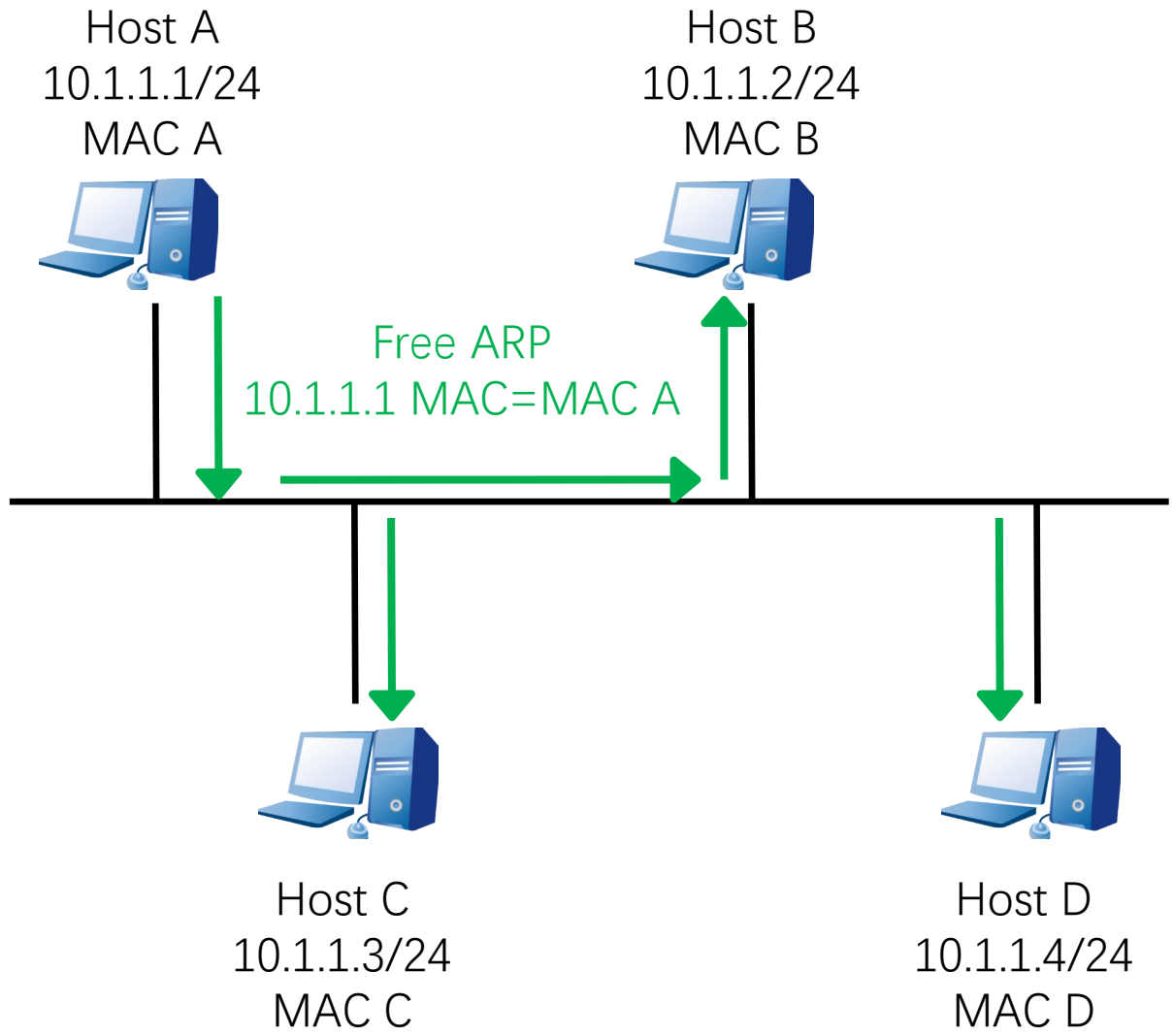


免费ARP

免费ARP通过广播方式通告自己的地址信息

免费ARP主要作用一：

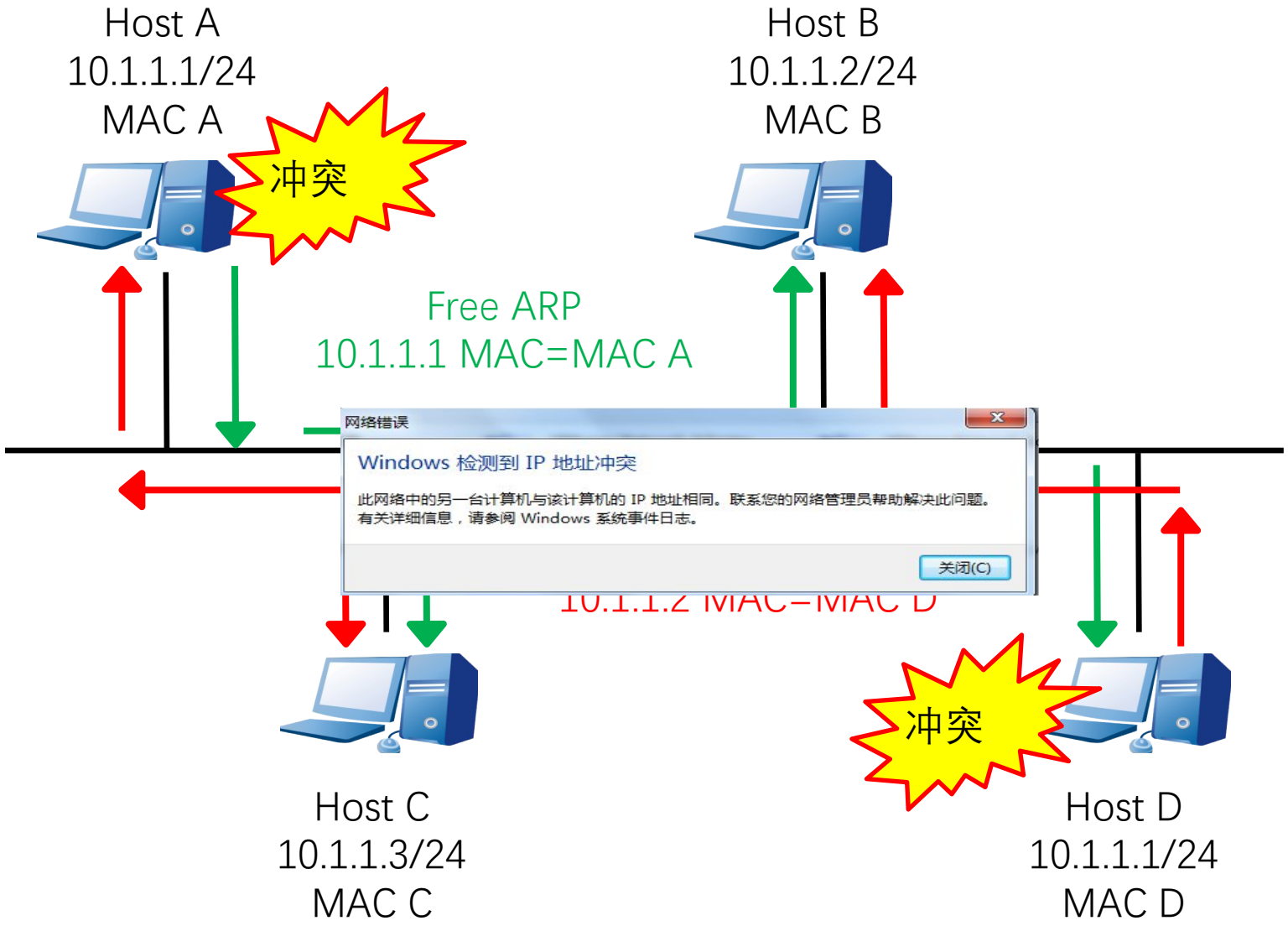
- 主动向网络中通告/更新自己MAC



免费ARP

免费ARP主要作用二：

- IP冲突检测

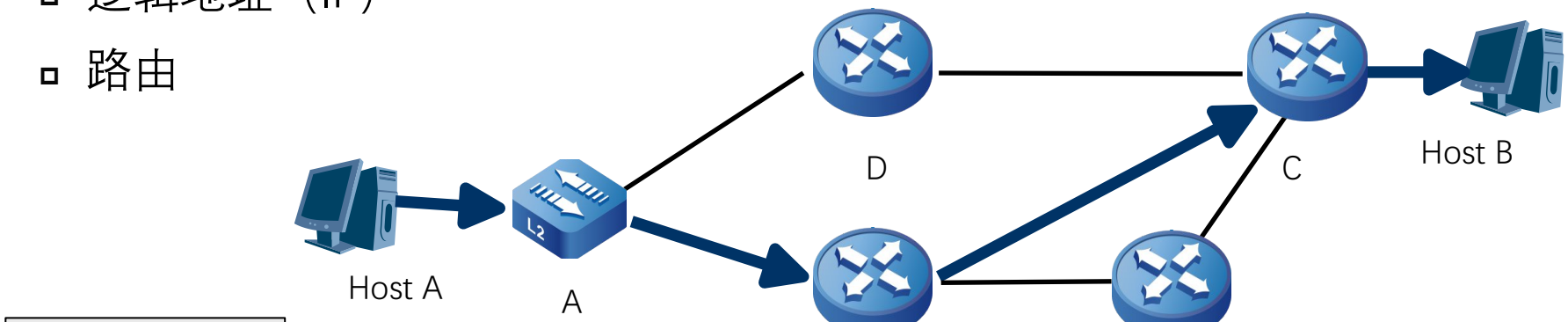


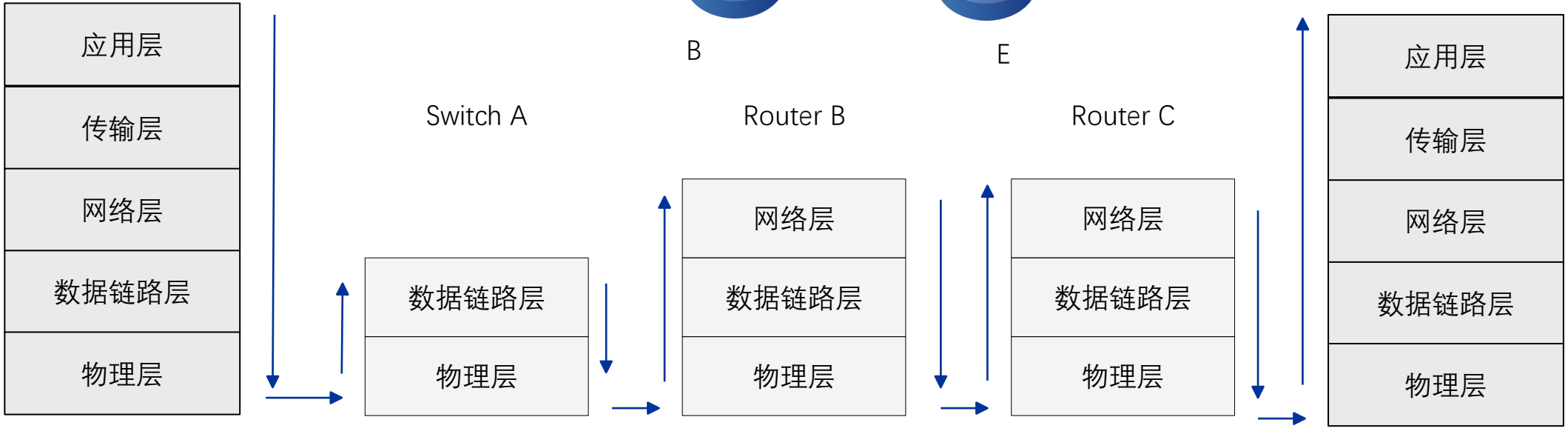
SANGFOR
深信服科技

网络层

网络层

- 网络层的功能：
  - 逻辑地址（IP）
  - 路由





IP地址结构

- IP地址唯一标示一台网络设备，由32个二进制位组成
- IP地址分为两部分：网络部分和主机部分
- IP地址通常采用点分十进制的格式标识
  - 如： 10.1.1.1, 192.168.1.1, etc

路由表

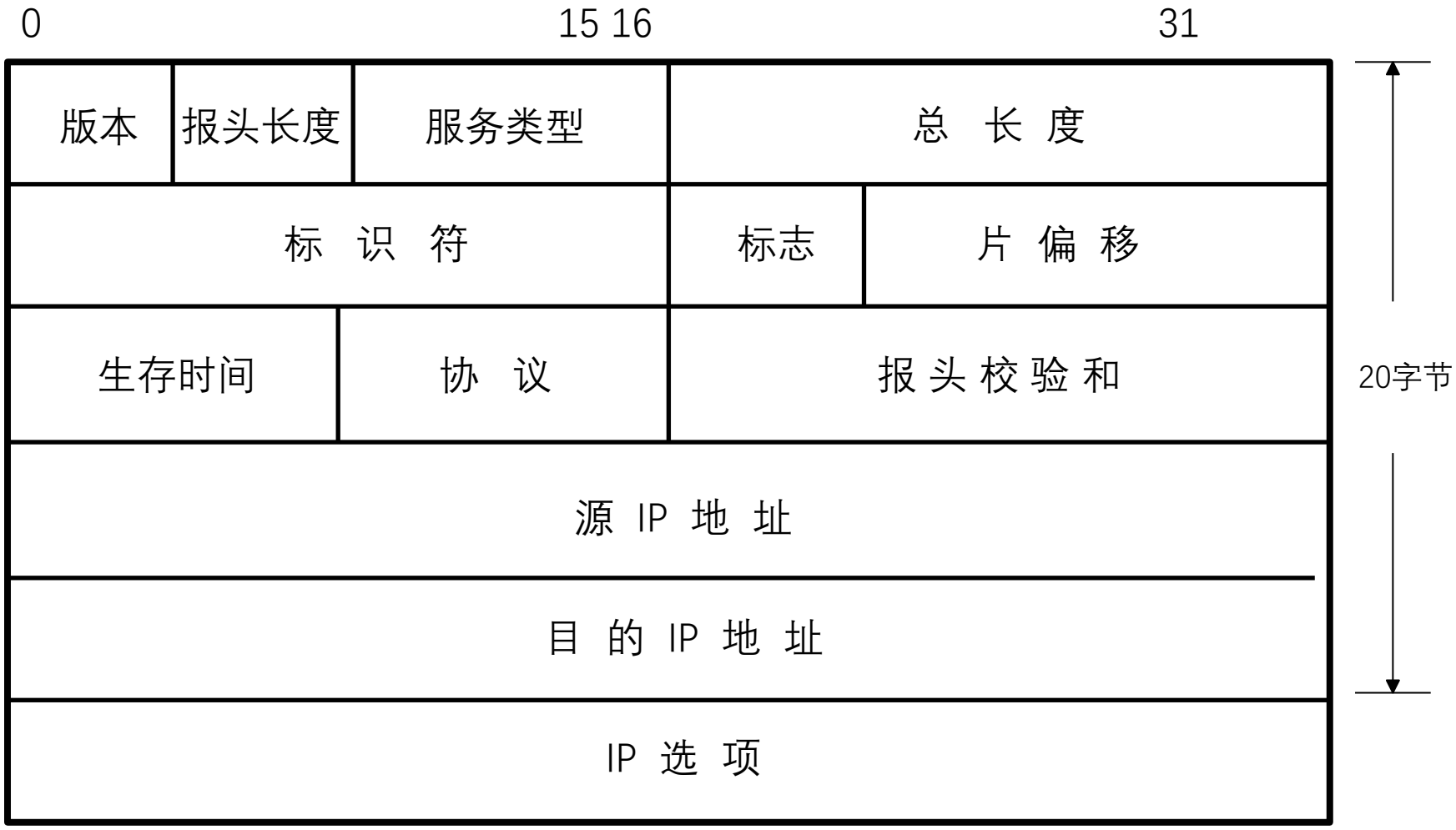
SANGFOR 深信服科技

- 目的地址、网络掩码、输出接口、下一跳IP地址

```
[root@localhost root ]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.83.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
202.202.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
200.200.68.0    0.0.0.0         255.255.252.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     0      0        0 eth0
200.200.0.0     200.200.71.254  255.255.0.0     UG    0      0        0 eth0
127.0.0.0       0.0.0.0         255.0.0.0       U     0      0        0 lo
0.0.0.0         200.200.71.254  0.0.0.0         UG    1      0        0 eth0
```

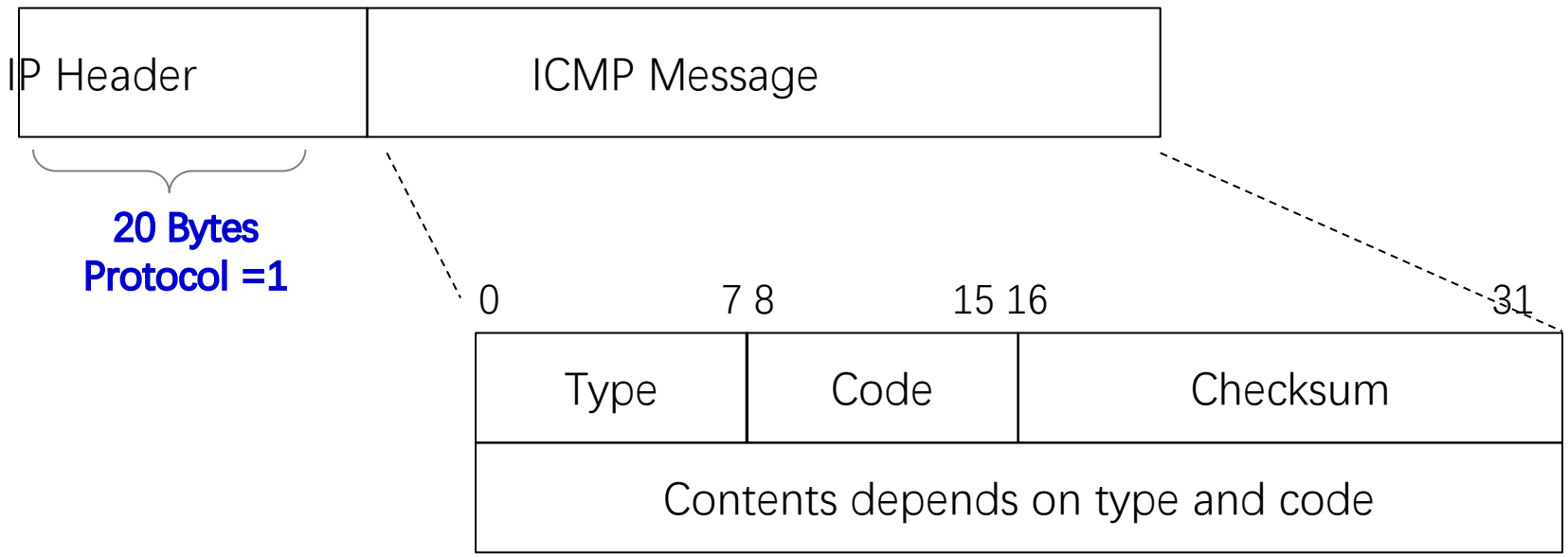
IP报文头部结构

SANGFOR 深信服科技



ICMP协议

- ICMP（Internet Control Message Protocol）是网络层的一个组成部分。它传递差错、控制、查询报文等信息。
- ICMP报文常被IP层或更高层协议及工具使用，如Ping、Tracert



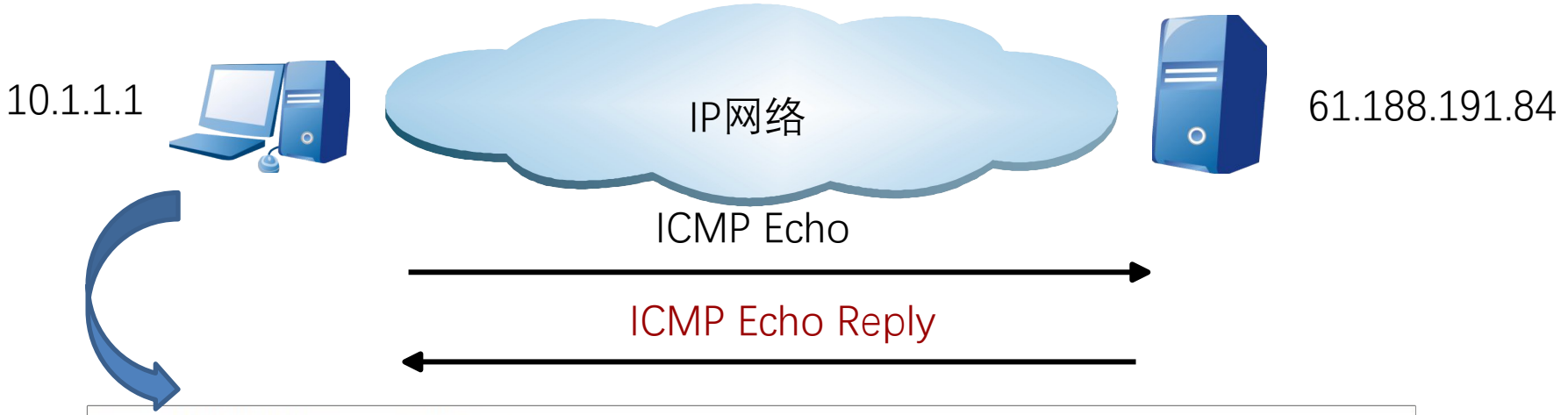
ICMP报文类型

SANGFOR 深信服科技

ICMP常用的几种消息类型：

- 0 Echo Reply 消息
- 3 Destination Unreachable 目的不可达消息
- 5 Redirect重定向消息
- 8 Echo Request 消息
- 11 Time Exceeded超时消息
- 12 Parameter Problem参数问题消息

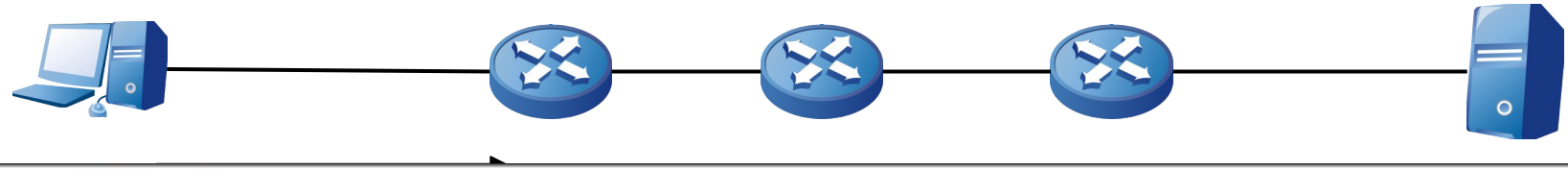
ICMP应用——Ping




```
C:\WINDOWS\system32\cmd.exe

C:\>ping 61.188.191.84

正在 Ping 61.188.191.84 具有 32 字节的数据:
来自 61.188.191.84 的回复: 字节=32 时间=11ms TTL=56
来自 61.188.191.84 的回复: 字节=32 时间=10ms TTL=56
来自 61.188.191.84 的回复: 字节=32 时间=29ms TTL=56
来自 61.188.191.84 的回复: 字节=32 时间=29ms TTL=56

61.188.191.84 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位):
    最短 = 10ms，最长 = 29ms，平均 = 19ms
```

ICMP应用——tracert

SANGFOR 深信服科技



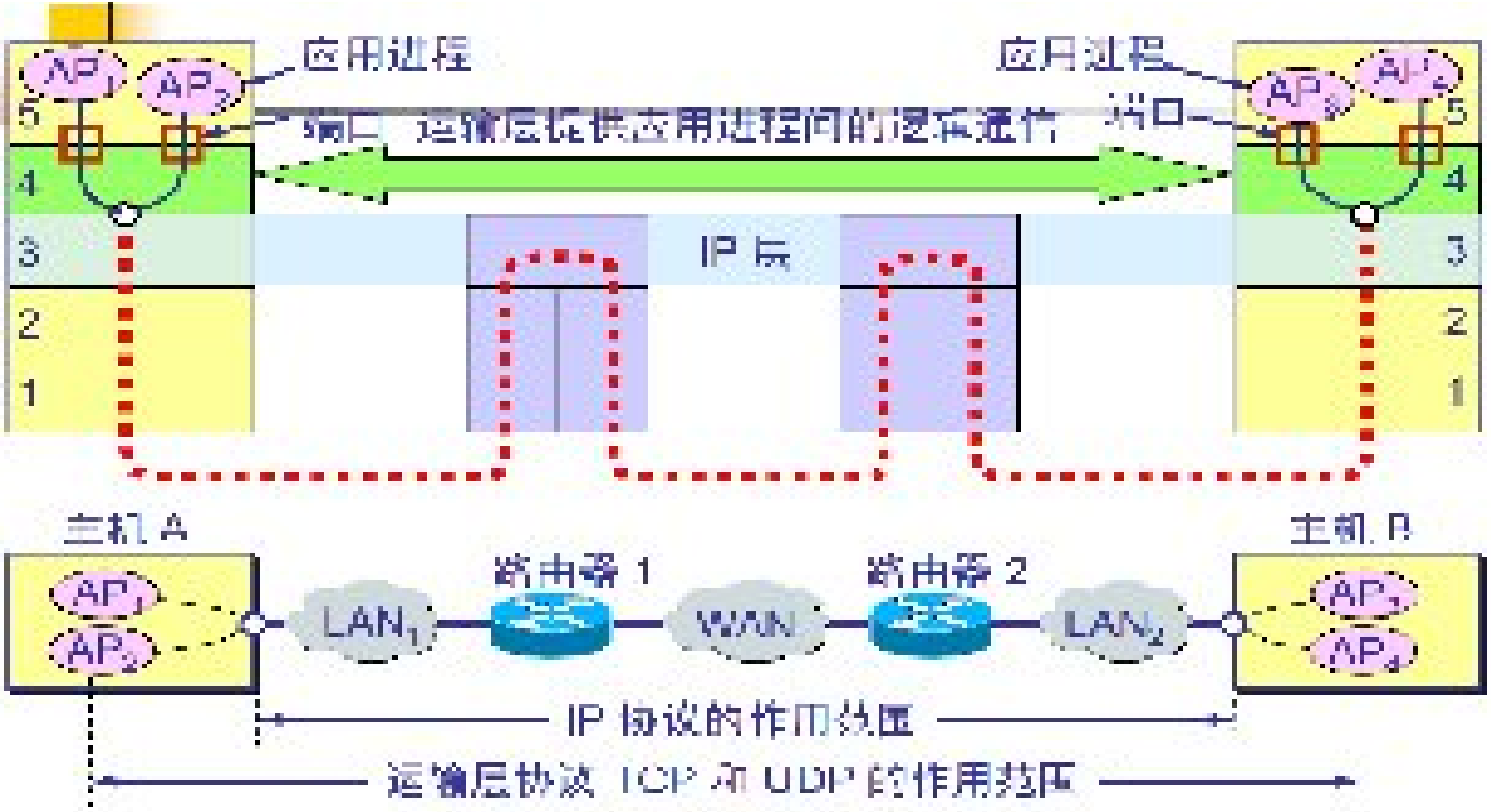
命令提示符

```
C:\> tracert 182.151.192.101

通过最多 30 个跃点跟踪到 182.151.192.101 的路由

  1     2 ms     1 ms     1 ms  192.168.247.254
  2     2 ms     1 ms     1 ms  192.168.7.246
  3     6 ms     3 ms     4 ms  125.71.215.1
  4     9 ms     4 ms     4 ms  182.151.192.101

跟踪完成。
```

SANGFOR
深信服科技

传输层

传输层为相互通信的应用进程提供了逻辑通信



- 运输层为应用进程之间提供端到端的逻辑通信（但网络层是为主机之间提供逻辑通信）。
- 运输层还要对收到的报文进行差错检测。
- 运输层需要有两种不同的运输协议，即面向连接的 TCP 和无连接的 UDP。

传输层协议

SANGFOR 深信服科技

TCP

- 面向连接
- 可靠
- 开销大
- 适用于可靠性要求高的应用

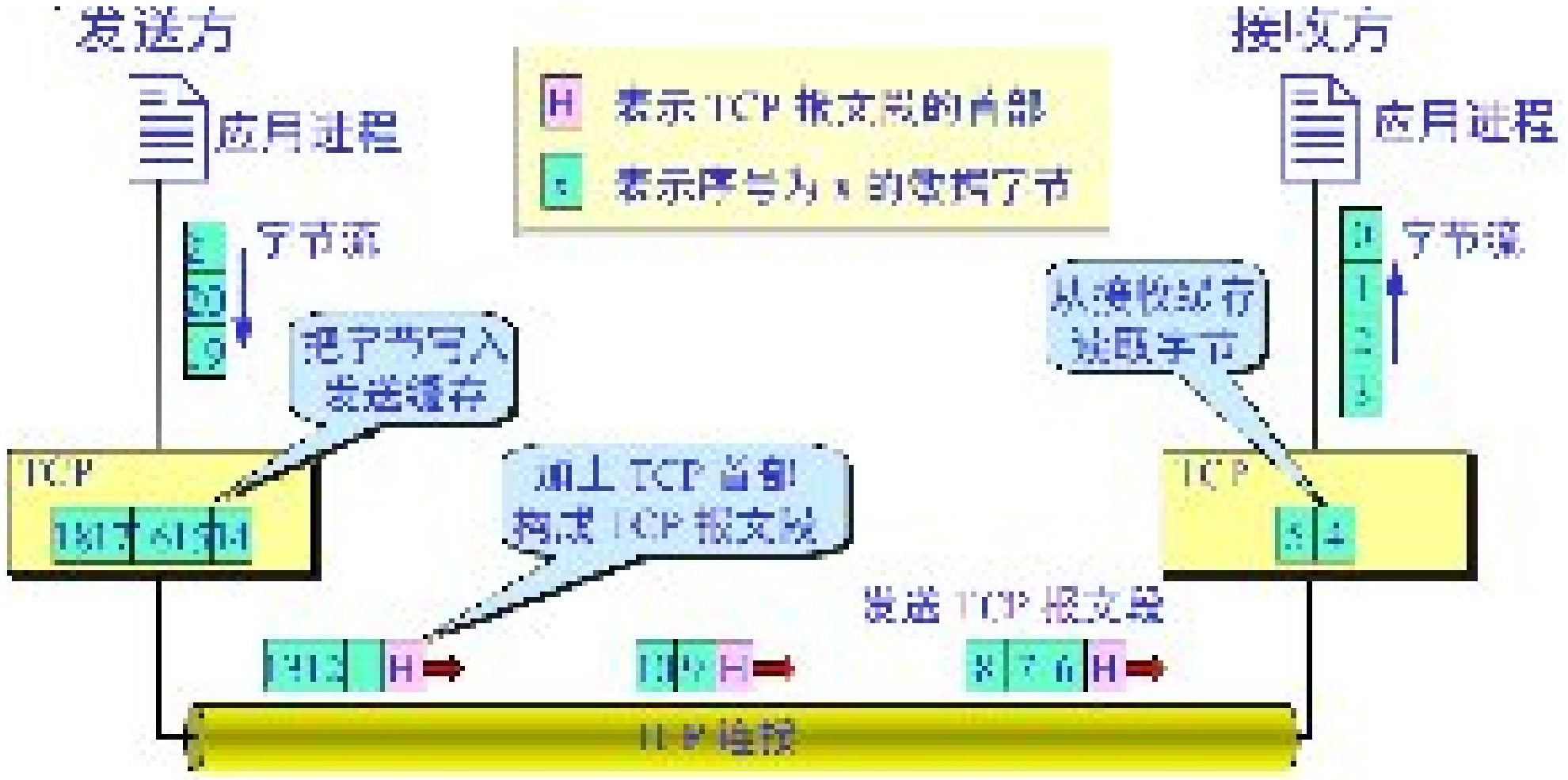
UDP

- 无连接
- 不可靠，可靠性由应用层负责
- 低开销
- 适用于更关注传输效率的应用

TCP 最主要的特点

- TCP 是面向连接的运输层协议。
- 每一条 TCP 连接只能有两个端点(endpoint)，每一条 TCP 连接只能是点对点的（一对一）。
- TCP 提供可靠交付的服务。
- TCP 提供全双工通信。
- 面向字节流。

TCP 面向流的概念

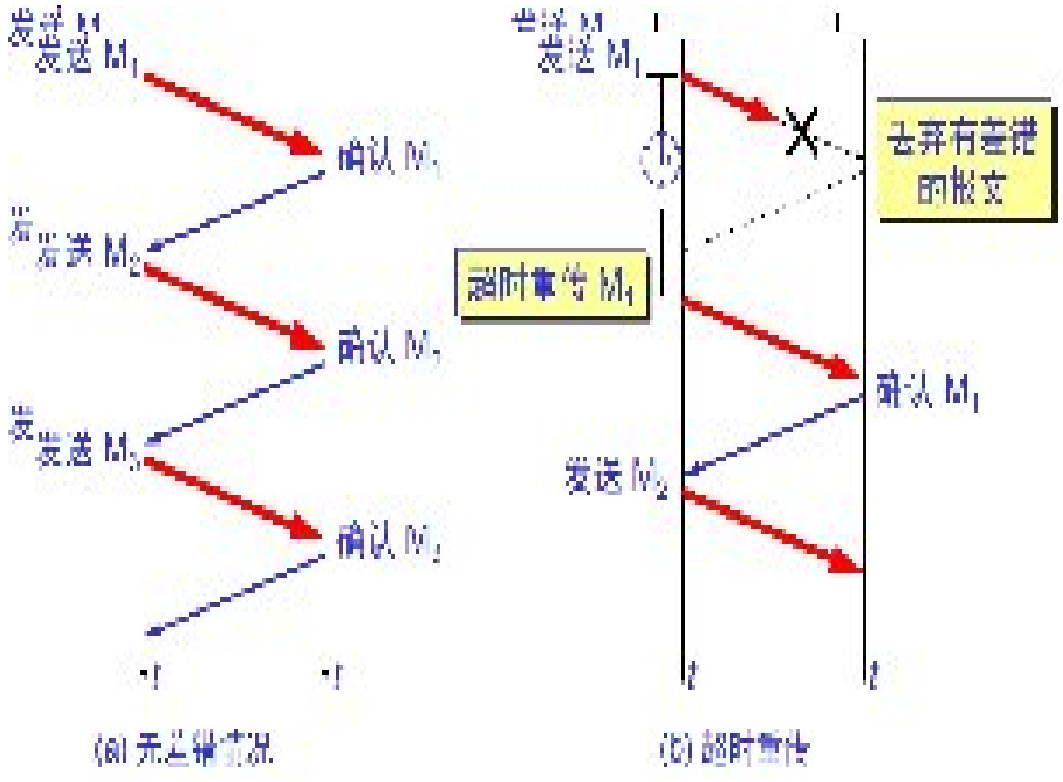


应当注意

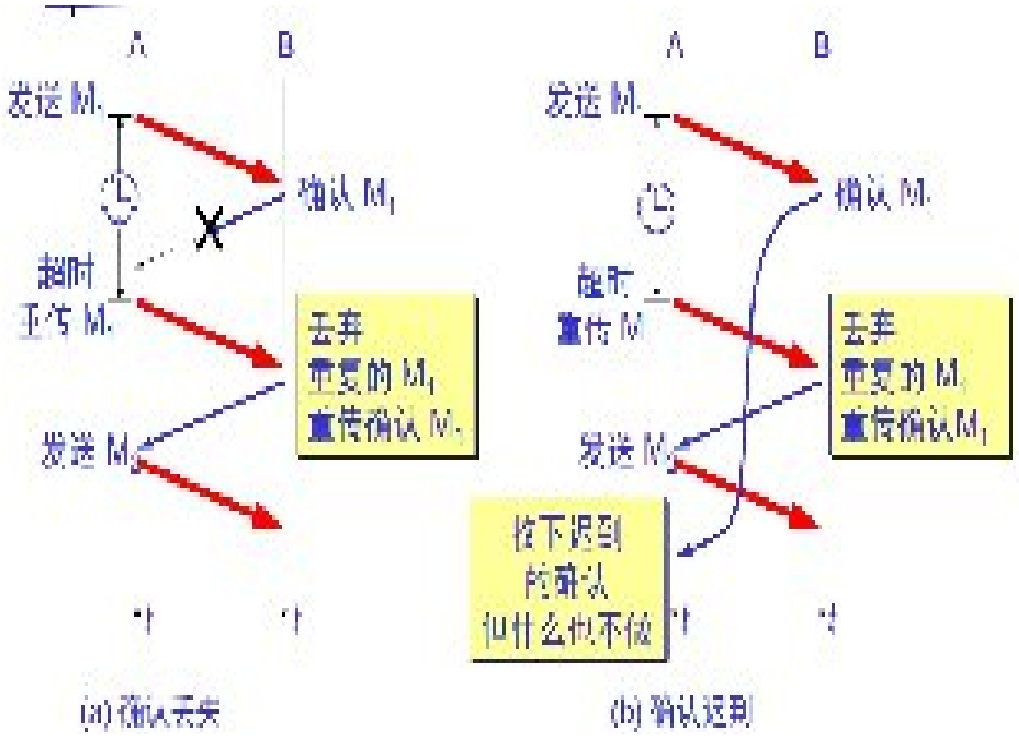
SANGFOR 深信服科技

- TCP 可把太长的数据块划分短一些再传送。TCP 也可等待积累有足够多的字节后再构成报文段发送出去。
- TCP 根据对方给出的窗口值和当前网络拥塞的程度来决定一个报文段应包含多少个字节（UDP 发送的报文长度是应用进程给出的）。
- TCP 可把太长的数据块划分短一些再传送。TCP 也可等待积累有足够多的字节后再构成报文段发送出去。

可靠传输的工作原理



(a) 无差错情况　　(c) 超时重传



(a) 确认丢失　　(b) 确认迟到

可靠传输的实现

SANGFOR 深信服科技

- 使用上述的确认和重传机制，我们就可以在不可靠的传输网络上实现可靠的通信。
- 这种可靠传输协议常称为自动重传请求ARQ (Automatic Repeat reQuest)。
- ARQ 表明重传的请求是自动进行的。接收方不需要请求发送方重传某个出错的分组 。

连续 ARQ 协议

SANGFOR 深信服科技

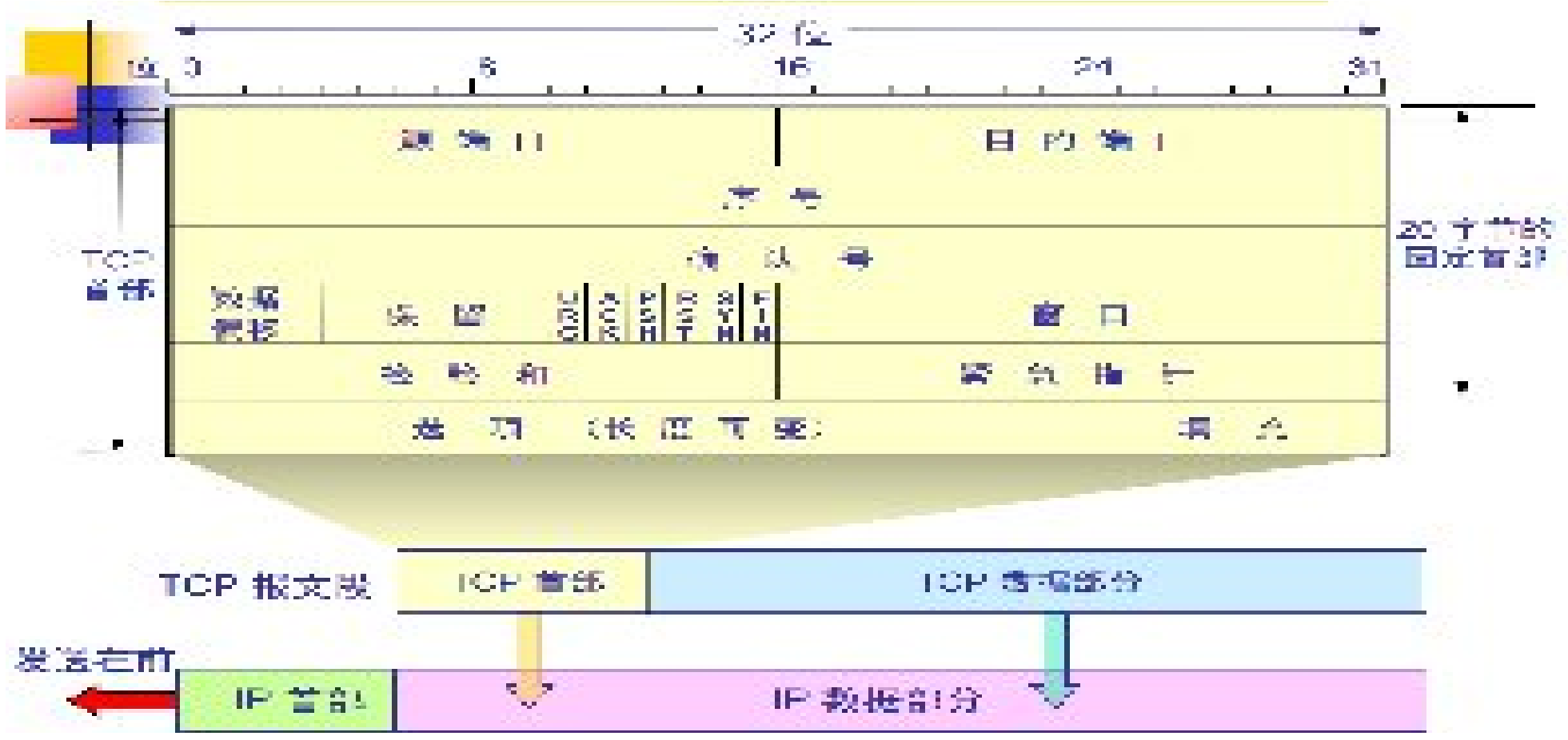
- 接收方一般采用累积确认的方式。即不必对收到的分组逐个发送确认，而是对按序到达的最后一个分组发送确认，这样就表示：到这个分组为止的所有分组都已正确收到了。
- 累积确认有的优点是：容易实现，即使确认丢失也不必重传。缺点是：不能向发送方反映出接收方已经正确收到的所有分组的信息。
- 当通信线路质量不好时，连续 ARQ 协议会带来负面的影响。

TCP 可靠通信的具体实现

SANGFOR 深信服科技

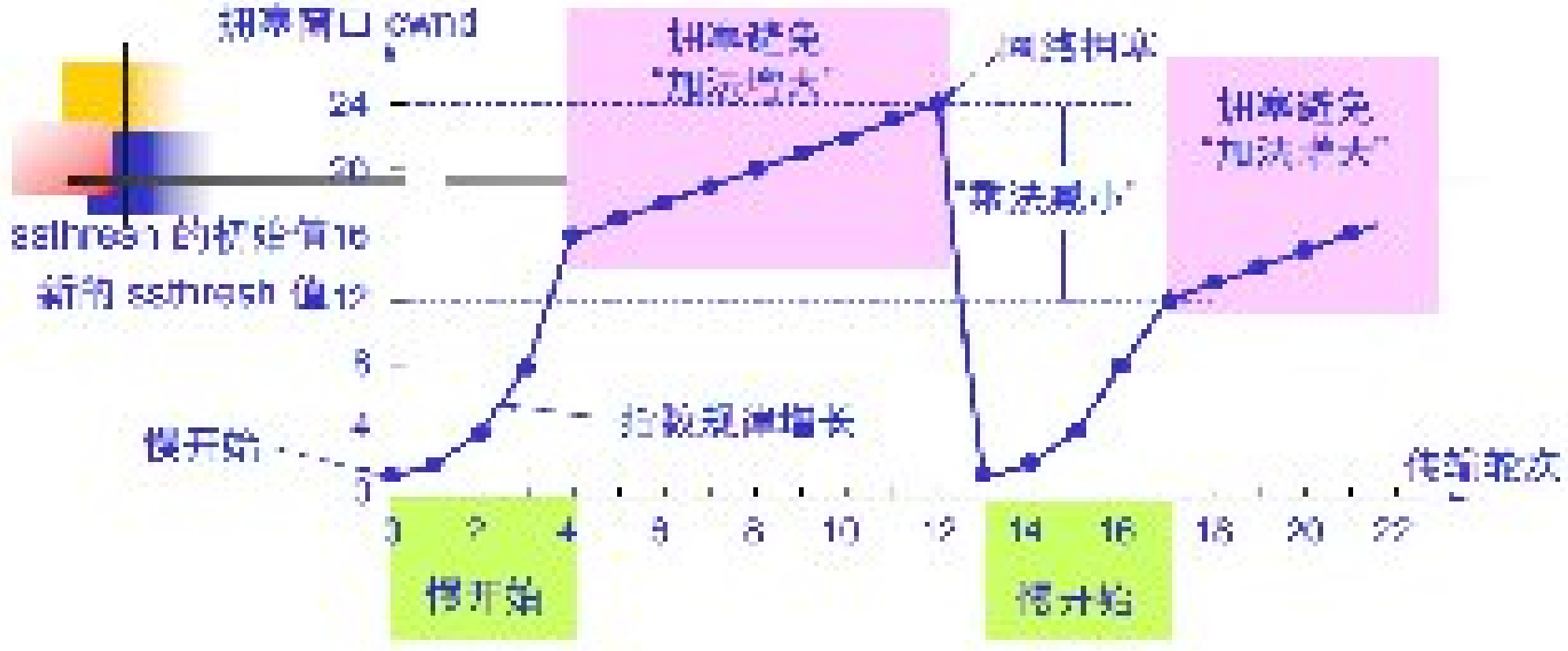
- TCP 连接的每一端都必须设有两个窗口一个发送窗口和一个接收窗口。
- TCP 的可靠传输机制用字节的序号进行控制。TCP 所有的确认都是基于序号而不是基于报文段。
- TCP 两端的四个窗口经常处于动态变化之中。
- TCP连接的往返时间 RTT 也不是固定不变的。需要使用特定的算法估算较为合理的重传时间。

TCP 报文结构



- 选项字段 —— 长度可变。TCP 最初只规定了一种选项，即最大报文段长度 MSS。MSS 告诉对方 TCP：“我的缓存所能接收的报文段的数据字段的最大长度是 MSS 个字节。”

拥塞控制



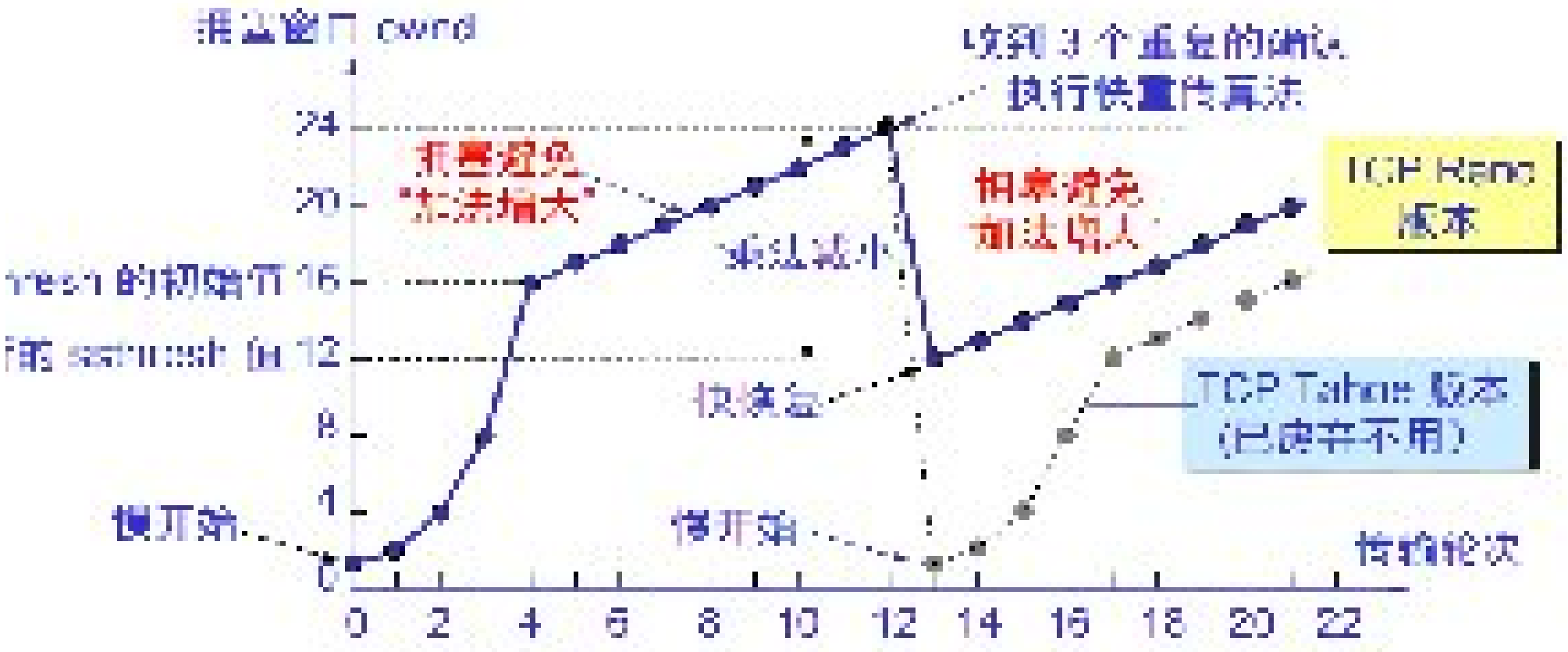
拥塞控制

SANGFOR 深信服科技

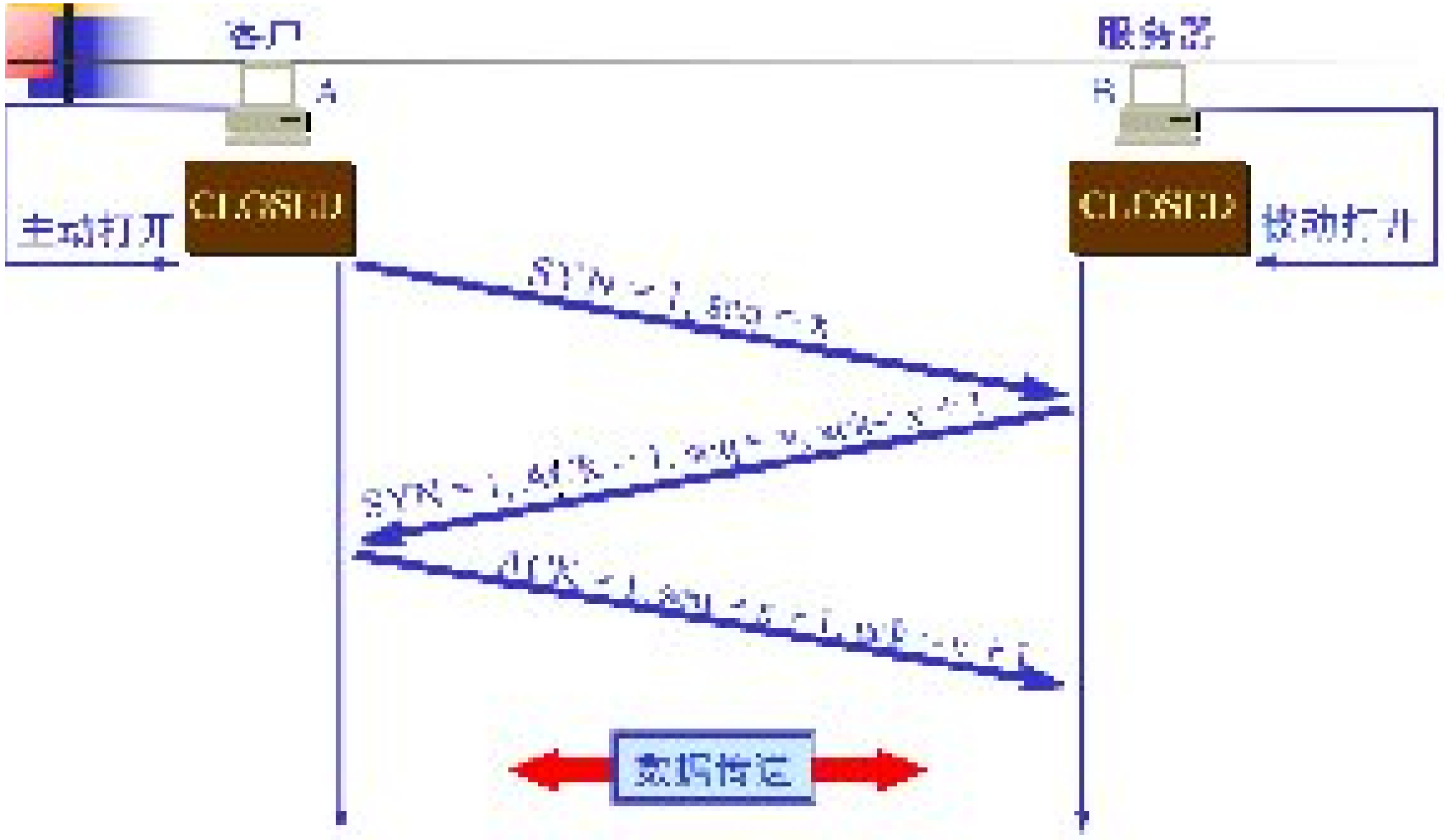
- “乘法减小”是指不论在慢开始阶段还是拥塞避免阶段，只要出现一次超时（即出现一 次 网 络 拥 塞 ），就 把 慢 开 始 门 限 值ssthresh 设置为当前的拥塞窗口值乘以0.5。

- “加法增大”是指执行拥塞避免算法后，在收到对所有报文段的确认后（即经过一个往返时间），就把拥塞窗口 cwnd增加一个MSS 大小，使拥塞窗口缓慢增大，以防止网络过早出现拥塞。

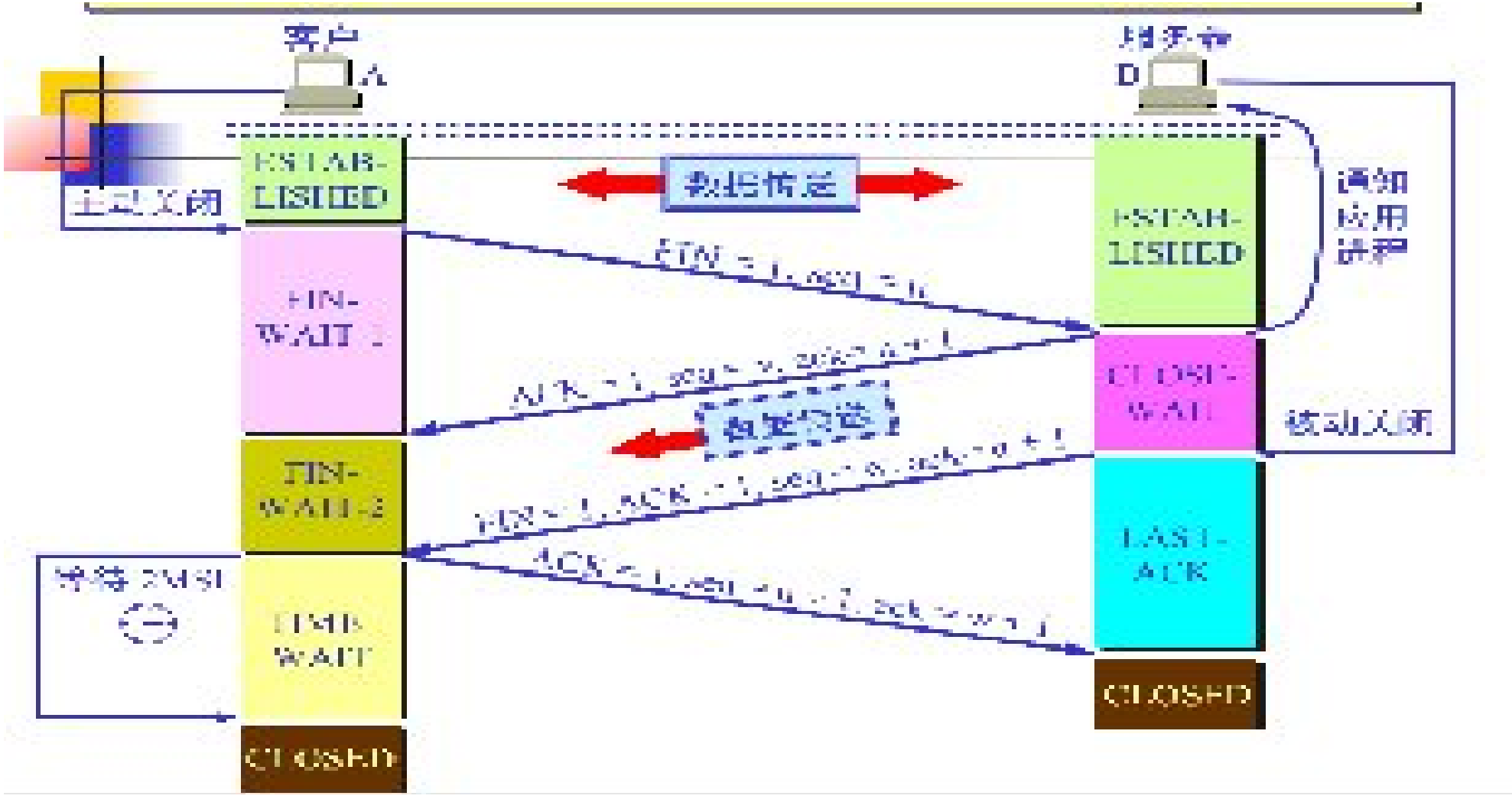
拥塞控制


拥塞窗口 cwnd
24
20
16
12
8
1
0
慢开始
门限减半
快恢复
慢开始
0 2 4 6 8 10 12 14 16 18 20 22
TCP Reno
版本
TCP Tahoe 版本
(已很少不用)

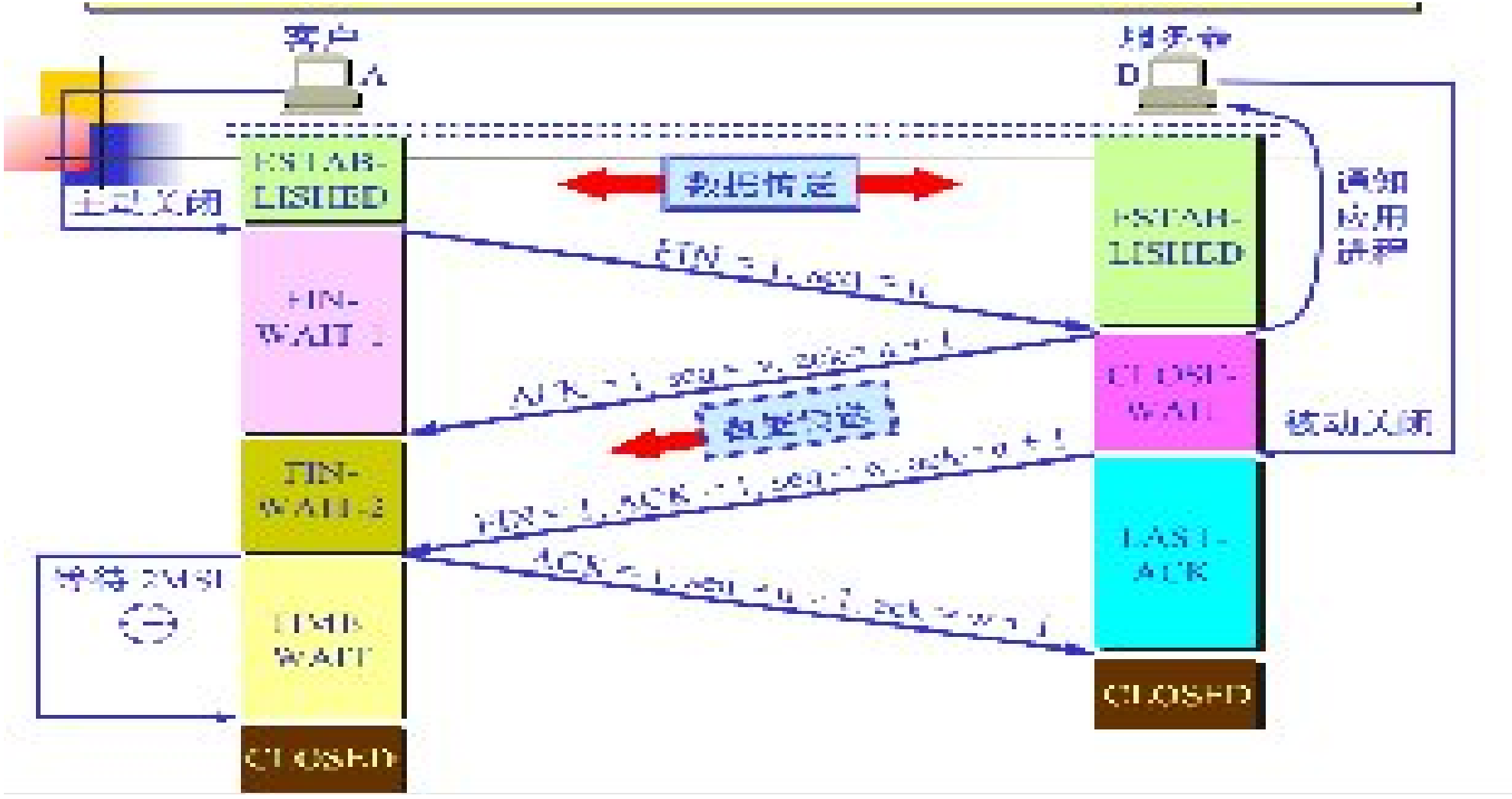
TCP连接



TCP连接释放


客户
A
D
ESTAB-
LISHED
数据传送
ESTAB-
LISHED
通知
应用
进程
FIN-
WAIT
CLOSE-
WAIT
被动关闭
FIN-
WAIT-2
LAST-
ACK
等待 2MSL
TIME-
WAIT
CLOSED
CLOSED

TCP连接释放


客户
A
D
ESTAB-
LISHED
数据传送
ESTAB-
LISHED
通知
应用
进程
FIN-
WAIT
CLOSE-
WAIT
被动关闭
FIN-
WAIT-2
LAST-
ACK
等待 2MSL
TIME-
WAIT
CLOSED
CLOSED

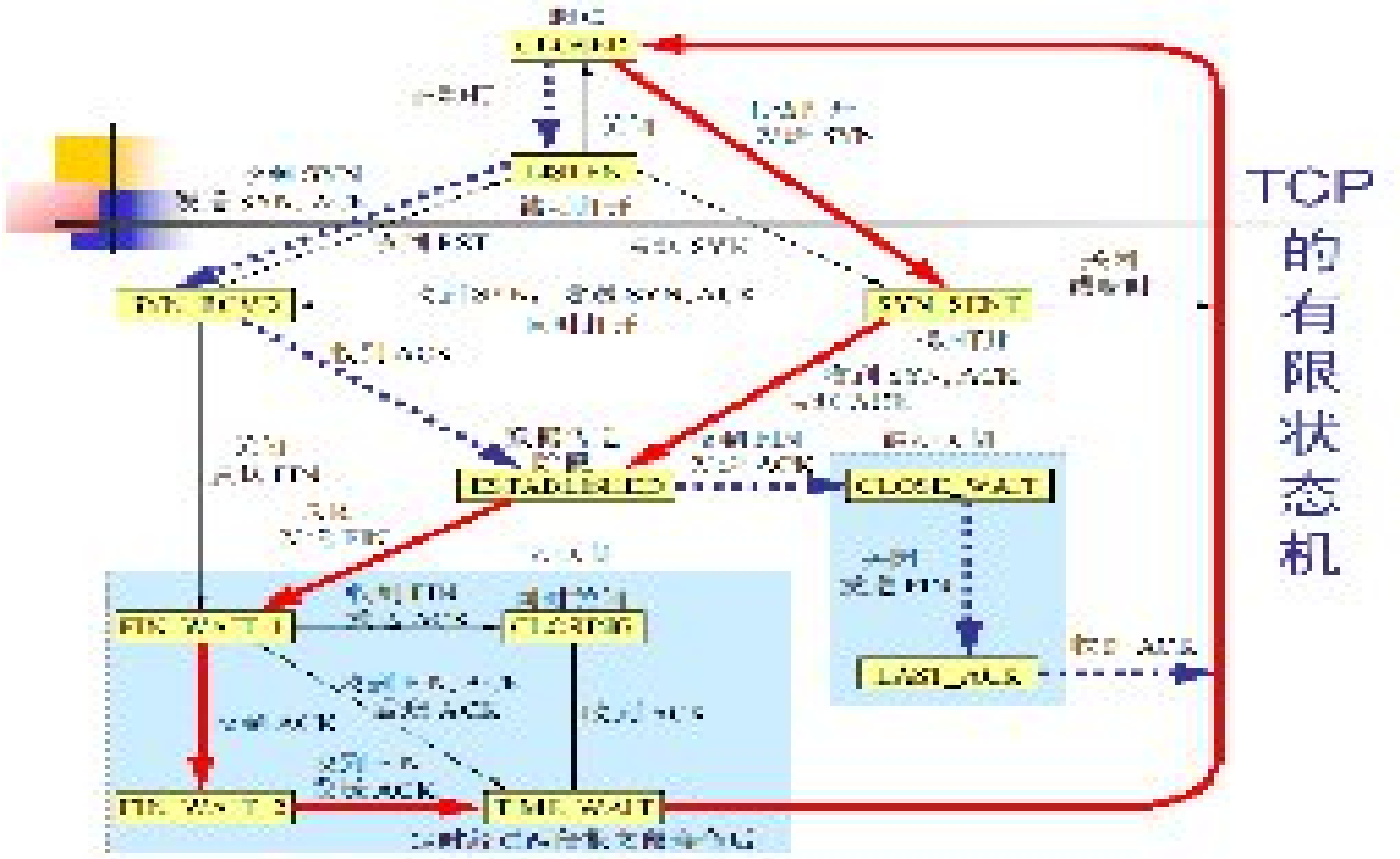
A必须等待2MSL

SANGFOR 深信服科技

- 第一，为了保证 A 发送的最后一个 ACK 报文段能够到达 B。

- 第二，防止“已失效的连接请求报文段”出现在本连接中。A 在发送完最后一个 ACK 报文段后，再经过时间 2MSL，就可以使本连接持续的时间内所产生的所有报文段，都从网络中消失。这样就可以使下一个新的连接中不会出现这种旧的连接请求报文段。

TCP的有限状态机



UDP 的主要特点

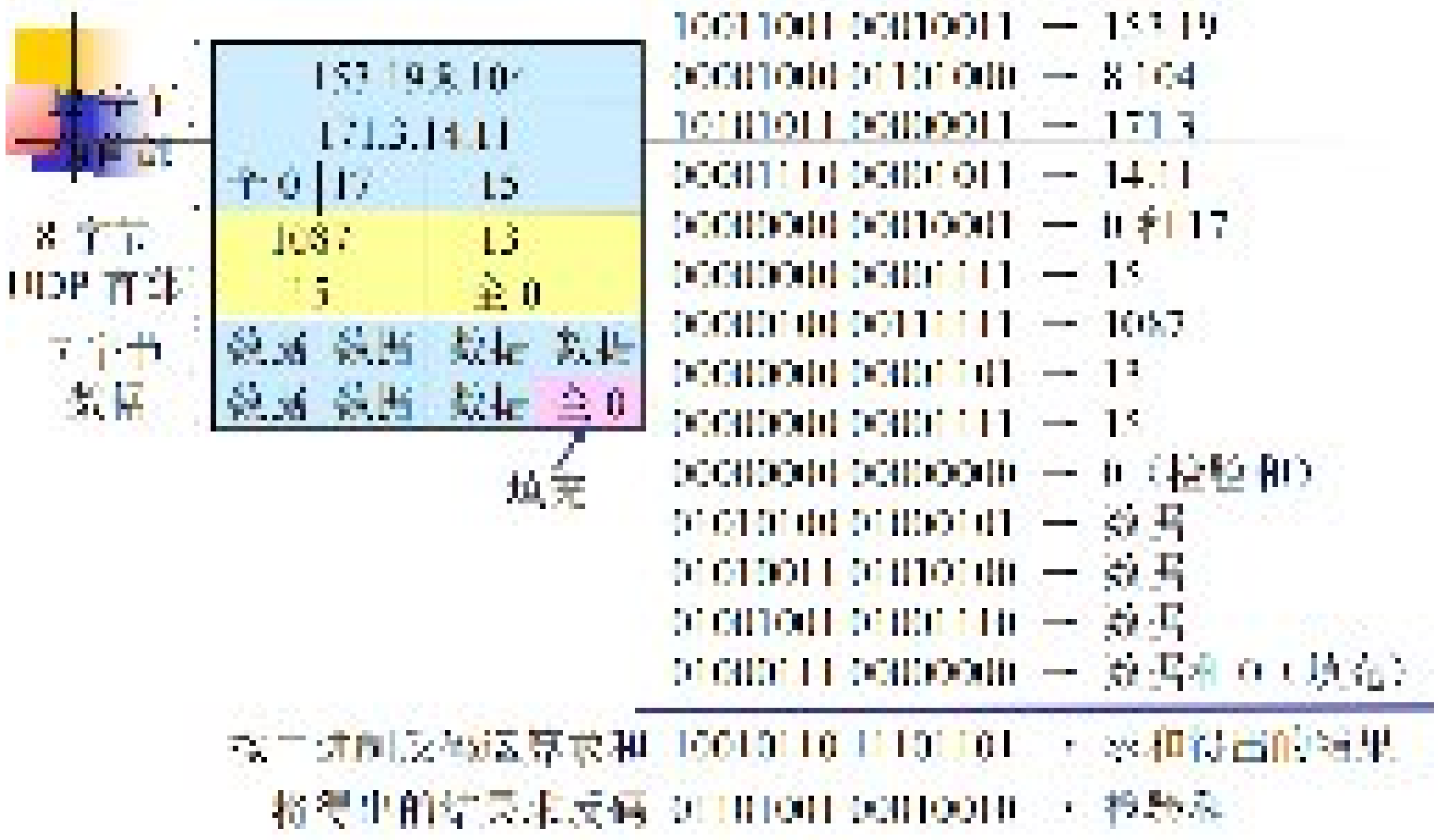
SANGFOR 深信服科技

- UDP 是无连接的，即发送数据之前不需要建立连接。
- UDP 使用尽最大努力交付，即不保证可靠交付，同时也不使用拥塞控制。
- UDP 是面向报文的。UDP 没有拥塞控制，很适合多媒体通信的要求。
- UDP 支持一对一、一对多、多对一和多对多的交互通信。
- UDP 的首部开销小，只有 8 个字节。

UDP 的首部格式


字节
4
4
1
1
2
源 IP 地址
目的 IP 地址
0
17
UDP 长度
字节
12
2
2
2
2
伪首部
源端口
目的端口
长 度
检查和
UDP 用户数据报
首 部
数 据
发送在网
首 部
数 据
IP 数据报

UDP 的首部格式



SANGFOR
深信服科技

应用层

知名应用层协议及端口号

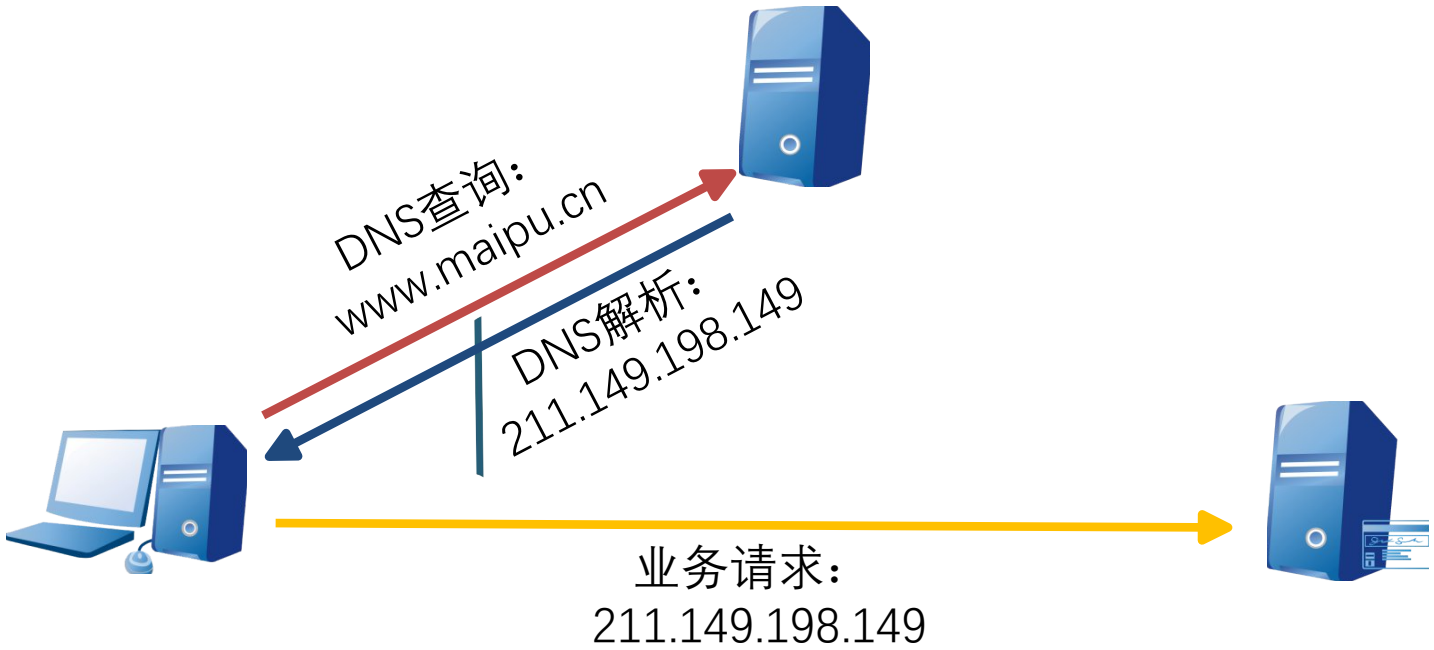
SANGFOR 深信服科技

TCP协议					
协议	端口号	协议	端口号	协议	端口号
FTP		HTTP		SMTP	25
FT-data	20	HTTPS		POP3	110
Telnet		SQL	1433	Tacacs+	49
SSH		Oracel	1521	DNS	

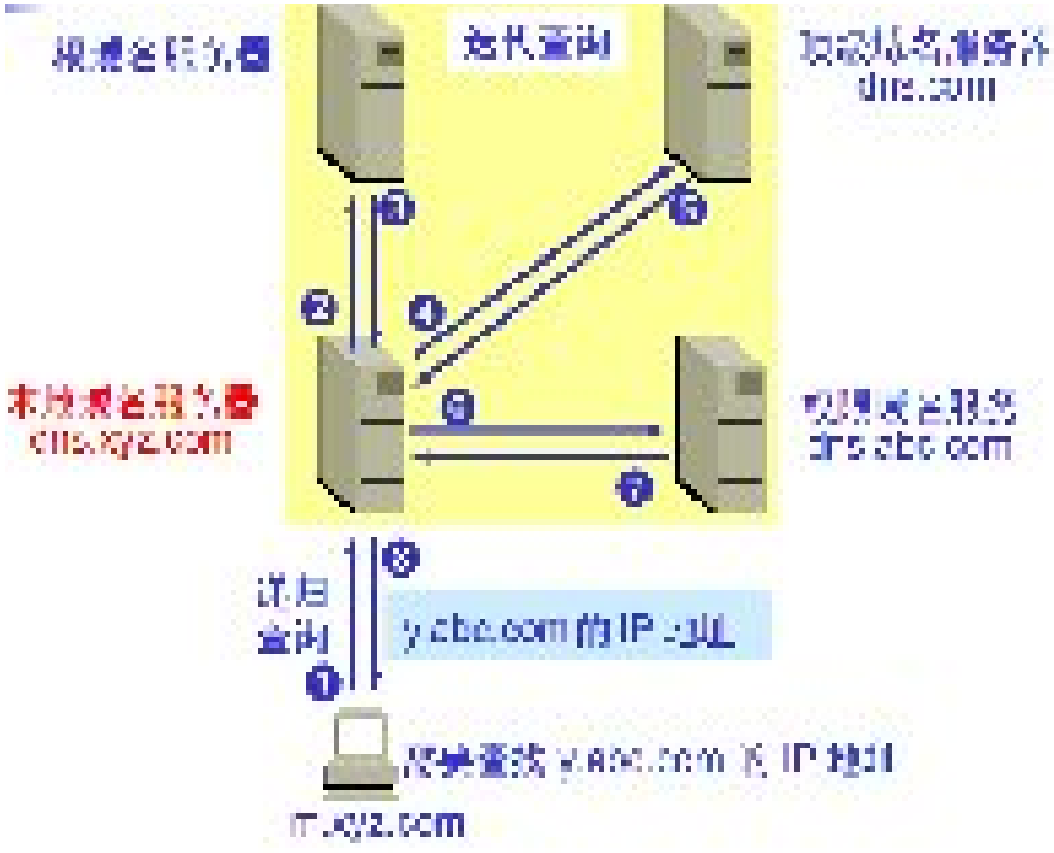
UDP协议					
协议	端口号	协议	端口号	协议	端口号
DHCP	67 68	Radius	1812 1813	WINS	42
TFTP	69	NTP	123	NETBIOS	137 138 139
SNMP	161 162	RIP	520	DNS	

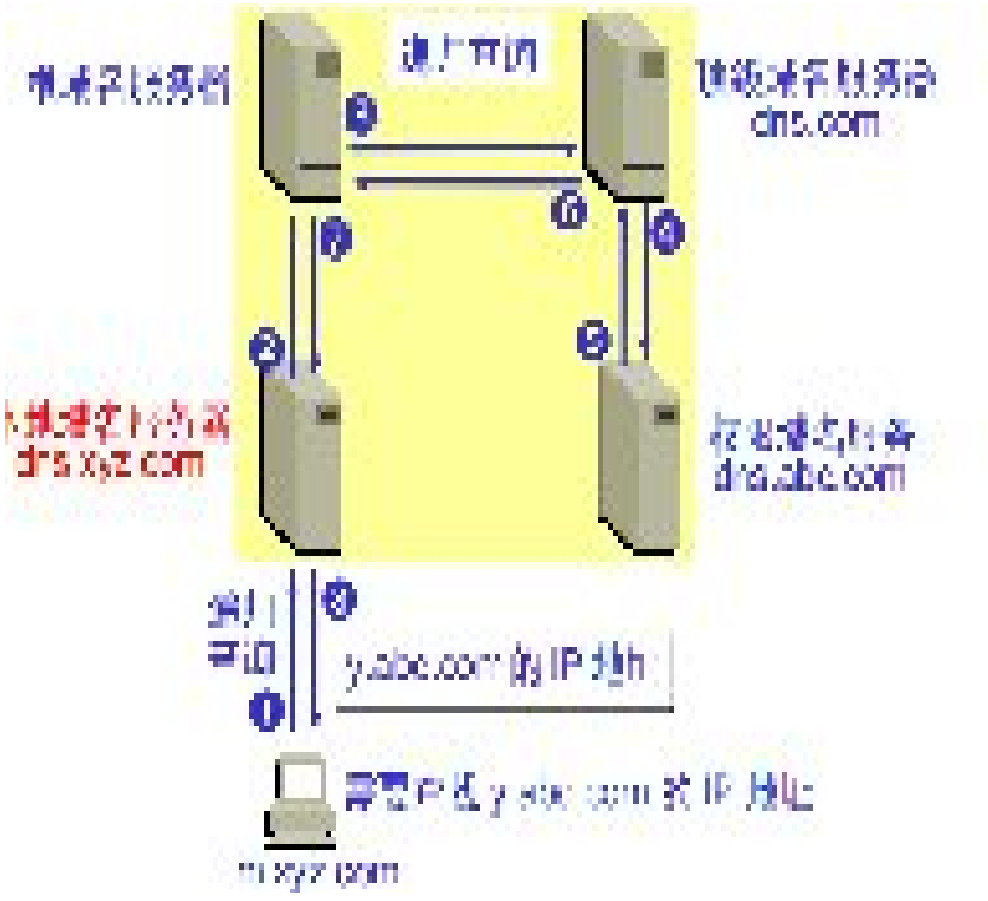
DNS

- DNS的主要作用是通过域名解析为其所对应IP地址

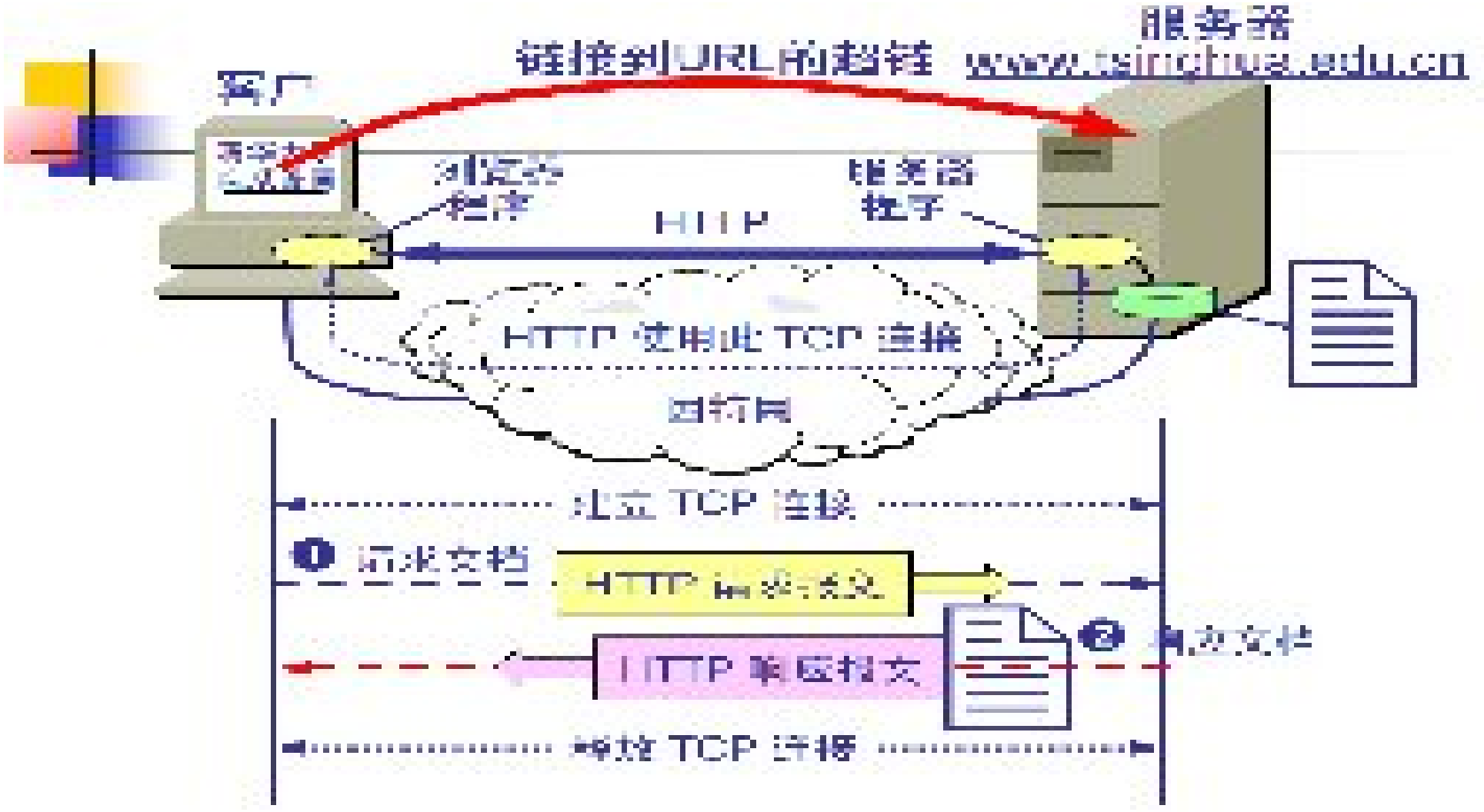


DNS域名的解析过程

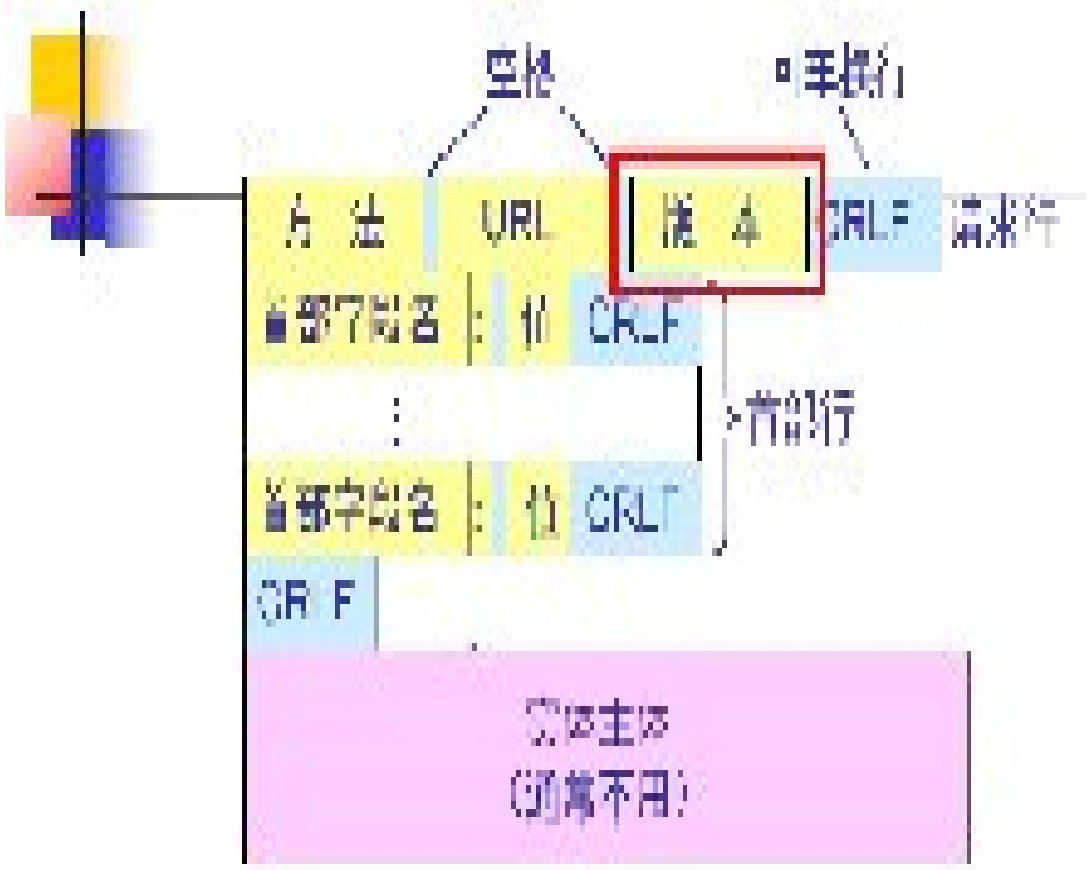




HTTP

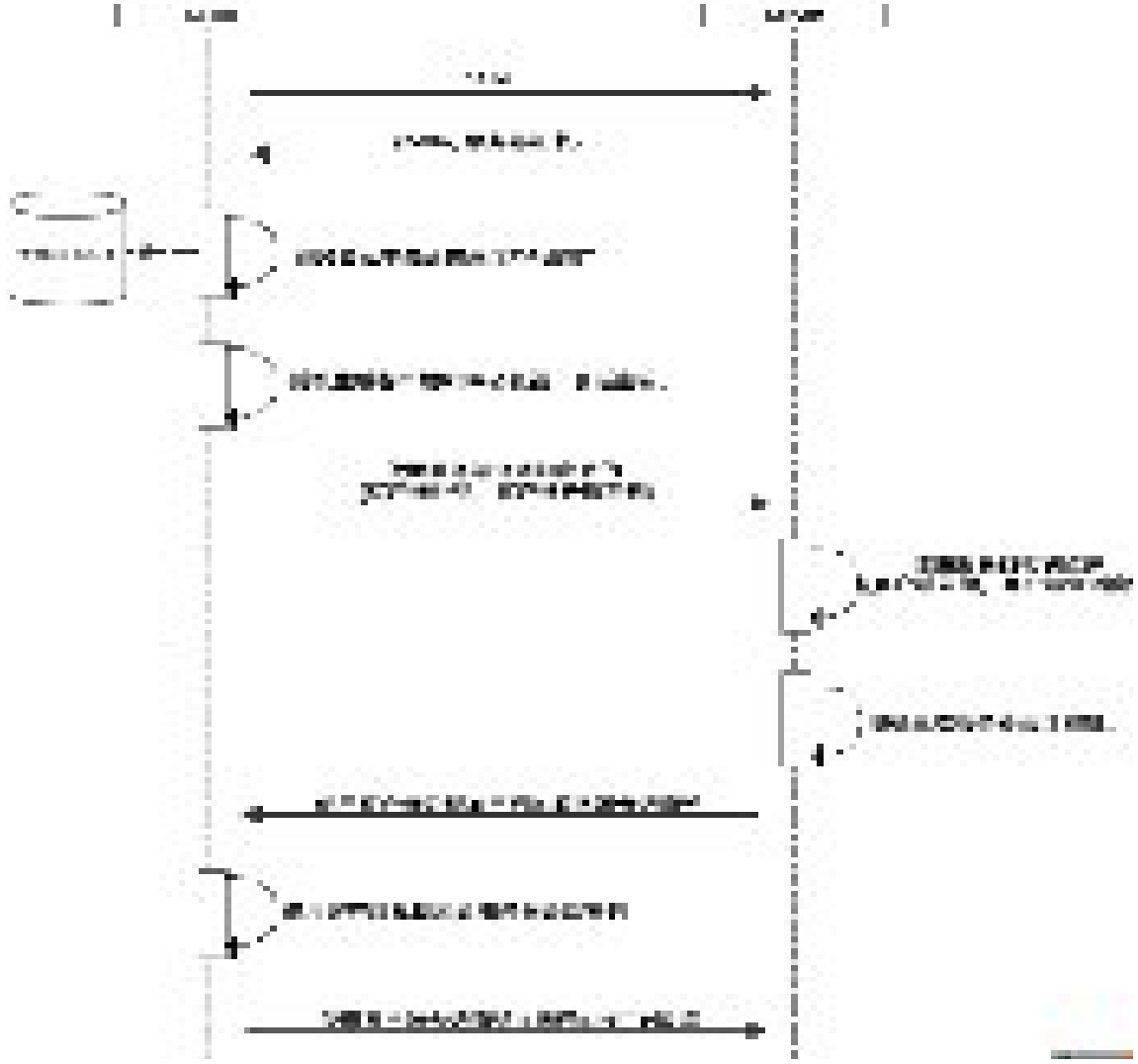

服务器
链接到URL的超链
客户
HTTP
HTTP 使用此 TCP 连接
因特网
建立 TCP 连接
请求文档
HTTP 响应报文
释放 TCP 连接

HTTP 的报文结构


空格
回车换行
方法
URL
版本
CRLF
请求行
首部字段名
值
CRLF
首部行
CRLF
实体主体
(可能不用)


空格
回车换行
版本
状态码
短语
CRLF
状态行
首部字段名
值
CRLF
首部行
CRLF
实体主体

HTTPS

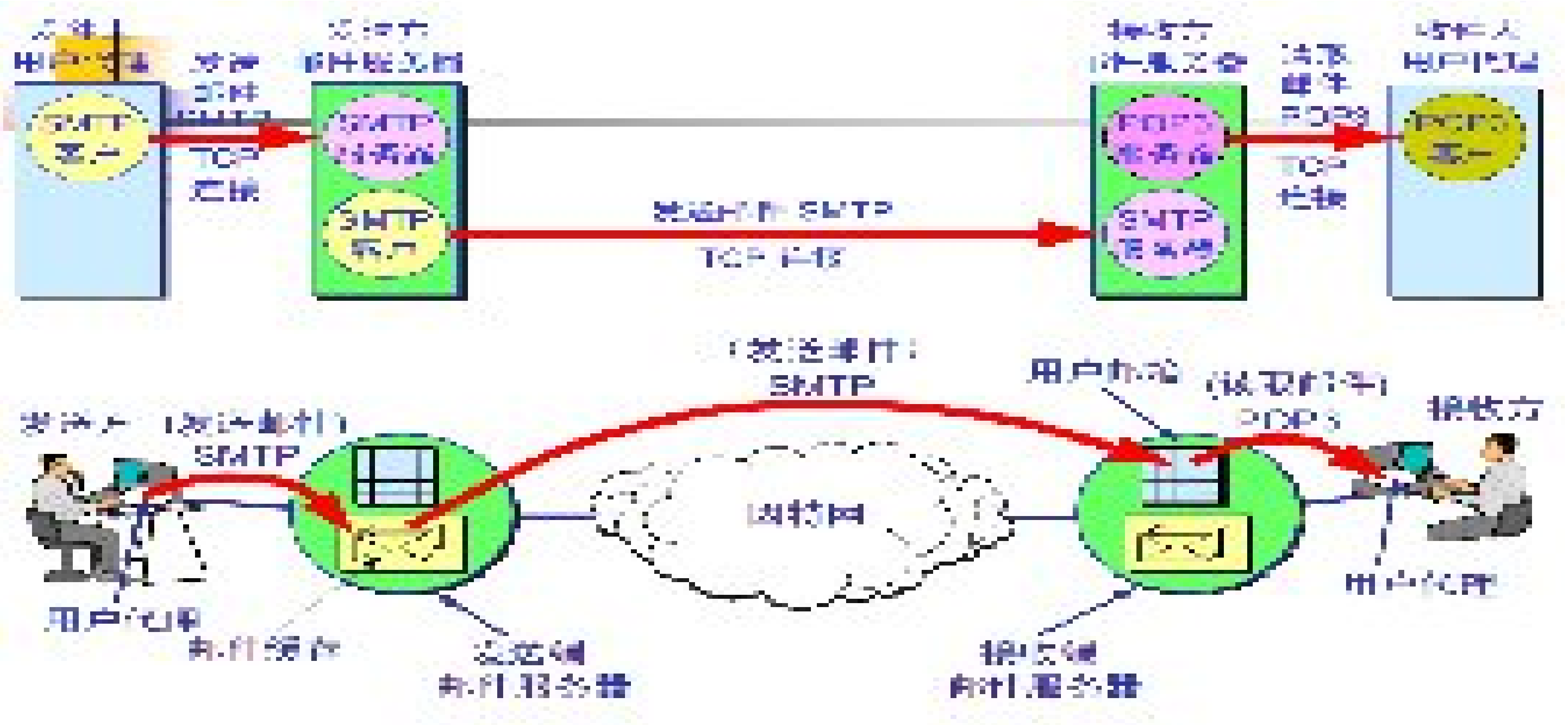


邮件协议

SANGFOR 深信服科技

- 发送邮件的协议：SMTP
- 读取邮件的协议：POP3 和 IMAP
- MIME 在其邮件首部中说明了邮件的数据类型(如文本、声音、图像、视像等)，使用 MIME 可在邮件中同时传送多种类型的数据。

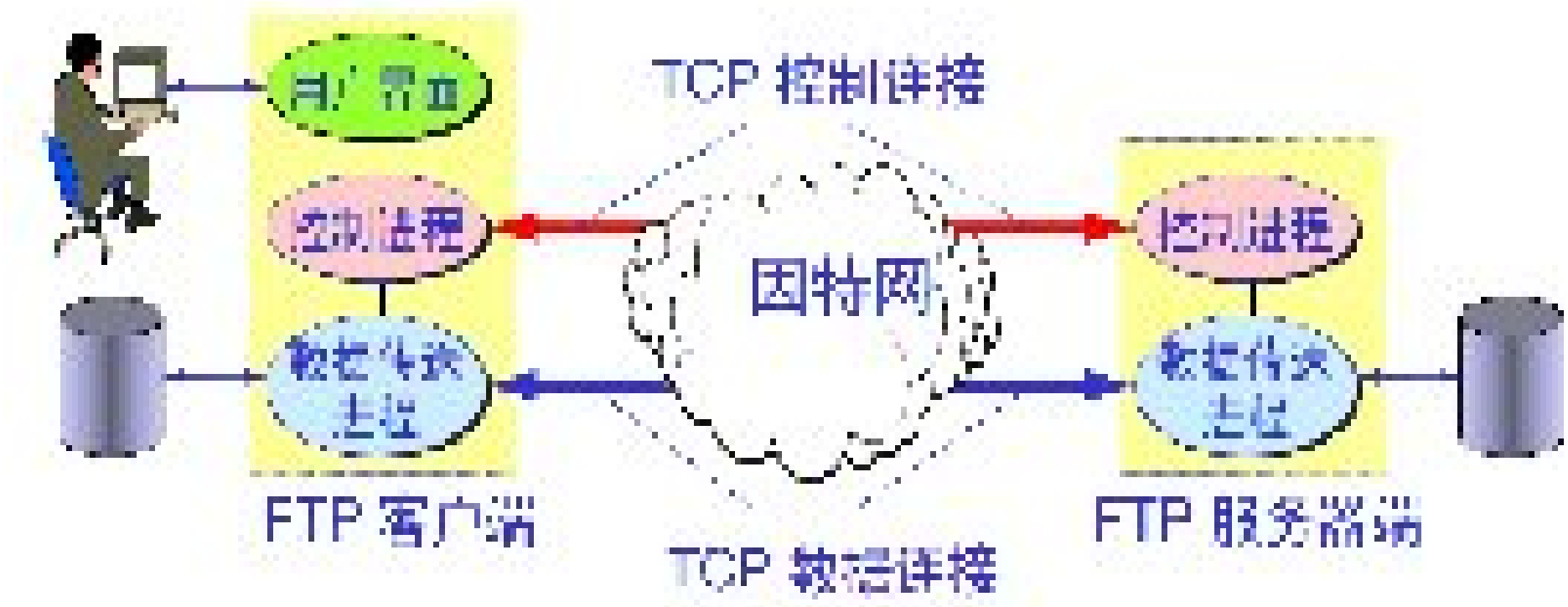
邮件协议



基于万维网的电子邮件

- 电子邮件从 A 发送到网易邮件服务器是使用 HTTP 协议。
- 两个邮件服务器之间的传送使用 SMTP。
- 邮件从新浪邮件服务器传送到 B 是使用HTTP 协议。

FTP



小结

SANGFOR 深信服科技

- TCP/IP协议模型：

历史，协议栈（五层模型，加/解封装），

数据链路层（MAC地址，ARP），

网络层（IP/路由，IPv4头部），

传输层（TCP/UDP，ICMP），

应用层（DNS，HTTP/HTTPS，邮件协议，FTP）。

SANGFOR
深信服科技

THANK YOU

2018深信服科技