# 第一章 企业网络发展历程

## 企业组网基本概念

**1. 核心目标**

* 互联互通：将分散的设备和用户连接成统一网络（如办公网、数据中心网络）。
* 业务支撑：为应用（ERP、视频会议、云服务）提供稳定、安全的传输通道。
* 分层设计：核心层（高速交换）、汇聚层（策略执行）、接入层（用户接入）。
* 典型拓扑：星型（简单易管理）、冗余环型（可靠性）、树型（分层扩展），SD-WAN技术逐渐普及。

**2. 关键设备**

* 防火墙（如深信服NGAF）：实现网络边界安全防护、入侵检测、VPN加密隧道。
* 交换机（核心/接入层）：VLAN划分、STP防环、端口聚合提升带宽。
* 路由器：广域网互联（ISP链路）、动态路由协议（OSPF、BGP）。
* 无线控制器（AC）：AP集中管理、无缝漫游、带宽负载均衡。

**3. 技术延展**

* SD-WAN（深信服aTrust）：优化多链路（如专线+互联网）利用率，提升SaaS（软件即服务，是一种云计算服务模型，允许用户通过互联网访问和使用由第三方提供商托管的应用程序）访问体验。
* 零信任架构（深信服Sangfor Access）：按需认证+动态权限，应对BYOD（Bring Your Own Device）和远程办公安全挑战。

## 网络性能关键指标及影响

表1.1 网络性能关键指标及影响

|  |  |  |  |
| --- | --- | --- | --- |
| **指标** | **定义** | **问题表现** | **解决方案（深信服相关）** |
| 带宽 | 单位时间传输数据量（Mbps） | 视频卡顿、文件下载慢 | 升级专线带宽、部署QoS策略（AD业务引流） |
| 时延 | 数据往返所需时间（ms） | 实时音视频会议卡顿、远程操作延迟高 | 选用低时延链路、部署SD-WAN链路优化 |
| 抖动 | 时延的波动范围 | VoIP通话断续、视频画面马赛克 | 启用QoS流量整形、部署缓存机制 |
| 丢包率 | 丢失数据包占比 | TCP重传导致应用响应慢、实时业务中断 | 检查物理线路、启用前向纠错（FEC）技术 |
| 吞吐量 | 实际有效数据传输速率 | 带宽充足但应用速度慢（协议效率低） | 优化传输协议（如TCP窗口调整） |
| 可用性 | 网络可服务时间比例（99.9%） | 业务不可用导致经济损失 | 部署双机热备、链路冗余（路由器多WAN） |

**1. 带宽（Bandwidth）**

定义：

* 描述单位时间内（通常为秒）网络链路可传输的最大数据量，单位为 Mbps/Gbps。
* 关键点：带宽是“管道容量”，但实际有效传输速率需考虑协议开销（如TCP/IP包头约占比10-20%）。

影响因素：

* 链路类型：专线（高带宽低延迟） vs 互联网（共享带宽，波动大）。
* 协议效率：小包（如VoIP）传输时，协议开销占比更高。
* 设备性能：低端路由器的转发能力可能无法达到标称带宽。

故障现象及案例：

* 现象：用户下载速度慢、视频会议频繁缓冲。
* 案例：某教育机构直播上课时，视频频繁卡顿（带宽为100Mbps但实际并发用户数超500，每个用户需至少2Mbps）。
* 诊断：流量监控（深信服AC）显示带宽利用率峰值达98%，且存在大量P2P下载占用带宽。

解决方案：

* 短效：通过深信服上网行为管理（AC）限制P2P、视频类应用的带宽。
* 长效：升级链路（专线升级至500Mbps），并部署SD-WAN多链路负载均衡，实现带宽叠加。

**2. 时延（Latency）**

定义：

* 数据包从发送端到接收端的单向传输时间（单向时延），或往返时间RTT（Round-Trip Time），单位ms。
* 等级参考：

≤50ms：适用于实时交互（VoIP、视频会议）。

50-200ms：容忍度较高场景（网页浏览、文件传输）。

>200ms：可能引发TCP重传，影响用户体验。

影响因素：

* 物理距离：光缆传输速度约为光速的2/3，跨大洋时延显著增加（如中美海底光缆RTT约150ms）。
* 网络拥塞：路由器队列排队导致时延抖动。
* 协议处理：防火墙深包检测（DPI）会增加处理时延。

故障现象及案例：

* 现象：远程桌面操作卡顿、金融交易系统报单延迟。
* 案例：某跨国企业使用基于TCP的ERP系统，上海访问美国服务器的RTT达300ms，导致SQL查询响应超时。
* 诊断：使用Traceroute工具发现数据经过多跳公网路由器（跨国运营商拥塞）。

解决方案：

* SD-WAN智能选路（深信服aTrust）：绕过拥塞节点，选择低时延路径。
* 协议优化：启用TCP加速（如深信服AD的TCP单边加速技术）。

**3. 抖动（Jitter）**

定义：

* 时延的波动范围（最大时延减最小时延），单位ms，是实时流媒体的关键指标。
* 关键点：抖动越大，接收端需要更大的缓冲（Buffer），但会增加端到端时延。

影响因素：

* 网络拥塞：突发流量导致队列缓冲波动。
* 无线干扰：Wi-Fi信道冲突引发数据重传。
* QoS策略缺失：未对实时流量（如语音）进行优先级标记。

故障现象及案例：

* 现象：VoIP通话断续（对方声音忽快忽慢）、视频会议画面撕裂。
* 案例：某酒店无线网络下客房IPTV频繁卡顿，实测抖动达100ms（因多个AP信道重叠）。
* 诊断：使用无线分析工具（如WirelessMon）发现2.4GHz频段信道利用率超80%。

解决方案：

* 无线优化：调整AP信道至空闲频段（如5GHz），开启无线负载均衡（深信服无线AC）。
* 流量整形：部署QoS策略，为视频流量标记DSCP优先级（EF类）。

**4. 丢包率（Packet Loss Rate）**

定义：

* 传输过程中丢失的数据包占总发送包数的百分比，即使丢包率1%也可能显著降低TCP吞吐量。
* 计算公式：（发送包数 - 接收包数） / 发送包数 × 100%

影响因素：

* 物理层故障：光纤断裂、网口接触不良。
* 网络拥塞：路由器队列溢出导致丢包。
* 安全设备误判：防火墙IP碎片重组失败或IPS误拦截合法流量。

故障现象及案例：

* 现象：文件传输中断、视频通话模糊或断开。
* 案例：某电商大促期间，核心交换机上行端口丢包率突增15%（因TCP突发流量超出交换机缓存）。
* 诊断：通过镜像抓包（Wireshark）发现大量TCP重传（Seq号不连续）。

解决方案：

* 设备调优：增大交换机缓冲区（Buffer Size），开启ECN（显式拥塞通知）。
* 链路冗余：部署深信服多线路接入网关，自动切换故障链路。

**5. 吞吐量（Throughput）**

定义：

* 网络在单位时间内实际传输的有效数据量，单位Mbps。
* 关键点：吞吐量 ≤ 带宽（受协议效率、设备性能、丢包率等多因素影响）。

影响因素：

* 协议开销：TCP/IP头部（20B）+ 以太网帧（18B），小包传输效率低（如总帧长64B：有效数据仅约9%）。
* 窗口大小：TCP接收窗口（RWIN）过小限制吞吐量。
* 设备转发能力：低端交换机使用“存储-转发”（Store-and-Forward）模式会增加处理时延。

故障现象及案例：

* 现象：带宽足够但FTP传输速度不达标、数据库同步缓慢。
* 案例：某银行异地备份中心传输效率仅为理论带宽的30%，因TCP窗口大小默认值（64KB）未优化。
* 诊断：使用iperf3测试，发现吞吐量受窗口限制（带宽延迟积BDP = 带宽 × RTT）。

解决方案：

* 调整TCP参数：增大接收窗口（RWIN）、启用窗口缩放（Window Scaling）。
* 硬件加速：启用深信服防火墙的硬件Offload功能（如SSL解密加速芯片）。

**6. 可用性（Availability）**

定义：

* 网络在指定时间段内可正常服务的时间占比，常用“n个9”表示（如99.99%对应年故障时间52分钟）。
* 计算公式：可用性 = (总时间 - 故障时间) / 总时间 × 100%

影响因素：

* 单点故障：核心交换机/防火墙无冗余。
* 人为误操作：错误配置ACL或路由策略。
* 外部攻击：DDoS导致服务瘫痪。

故障现象及案例：

* 现象：业务间歇性中断、用户无法访问关键系统。
* 案例：某制造企业因单台防火墙故障导致全网断网2小时（可用性下降至99.7%）。
* 诊断：防火墙HA心跳线未正确配置，主备切换失败。

解决方案：

* 高可用架构：部署防火墙双机热备（深信服NGAF支持Active/Standby模式，即双机热备模式，通过两台NGAF防火墙组成主备关系，主设备（Active）处理业务流量，备设备（Standby）实时同步状态但无流量转发。）。
* DDoS防护：启用流量清洗服务（深信服云图与本地设备联动）。

## 企业组网发展阶段问题与解决方案

**1. 小型企业（初始组网）**

* 问题：单台设备性能瓶颈（如路由器转发能力不足）、广播风暴。
* 解决：划分VLAN隔离广播域、升级多核防火墙（如深信服NGFW）。

**2. 中型企业（网络扩张）**

* 问题：多分支机构互联成本高、链路带宽浪费。
* 解决：部署SD-WAN（aTrust）实现智能选路、带宽汇聚和SaaS加速。

**3. 大型企业（数字化转型）**

* 问题：东西向流量激增（数据中心内部）、安全策略难以统一。
* 解决：部署微隔离（深信服EDR联动）、流量可视化分析（日志审计平台）。

**4. 企业上云阶段**

* 问题：混合云网络复杂（本地IDC + 公有云）、安全策略不一致。
* 解决：构建云安全资源池（深信服云镜）、统一管理边界防护策略。

细分：

1. 企业初创阶段：

需求：基础边界防护、端点防护

2. 业务增长阶段：

需求：区域隔离、分级防护、用户认证、行为管理、泄密追踪、移动接入安全

3. 业务扩张阶段：

4. 稳态与敏态业务阶段：

5. 运营管理与服务支撑阶段：

## 家庭组网常用设备与服务

**1. 设备清单：**

* 光猫：光纤信号转换（ISP提供）。
* 无线路由器：NAT转换、无线覆盖（2.4G/5G双频）。
* 电力猫/无线中继器：扩展信号覆盖范围。

NAS设备：家庭私有云存储（如群晖）。

**2. 核心服务：**

* DHCP：自动分配IP地址（避免手动配置错误）。
* UPnP：自动端口映射（支持P2P下载、游戏联机）。
* 家长控制：限制设备上网时间和内容（如深信服家庭版安全网关）。

## 相关考试题

***企业网络发展历程考试***

**1. 我们花钱购买的家庭带宽服务，本质上是购买了什么资源？多选**

**a. 网线**

属物理设备，ISP通常不提供或仅作为配套工具，非本质资源。

**b. 路由器**

路由器：家庭用户需自行购买或租用，亦非ISP服务核心。

**c. 线路带宽**

线路带宽：即购买的数据传输速率（如100Mbps），是用户使用的核心资源。

**d. 公网地址的使用权**

家庭用户通过ISP接入互联网时，需分配IP（通常动态且可能经过NAT），虽多为共享公网IP，但这是连接公网的必备条件。部分ISP收取额外费用提供固定公网IP（如中小企业专线），此时“使用权”更为明确。

·正确答案：c. 线路带宽、d. 公网地址的使用权

**2. 以下哪些业务一般是部署在DMZ区的？多选**

DMZ（Demilitarized Zone）是网络隔离区，用于放置对外提供服务的服务器。

**a. OA (办公系统)**

OA系统通常仅限内部员工访问，需内网隔离保护，部署在内网。

**b. 门户网站**

门户网站需公开访问（如公司官网、产品页面），部署在DMZ区可对外暴露Web服务，同时保护内网安全。

**c. 财务系统**

财务数据高度敏感，需部署在内网（甚至独立安全域），严格限制外部访问。

**d. 邮件系统**

邮件服务器（SMTP/POP3）需与外部通信（接收公网邮件），通常部署在DMZ区；但内部邮件服务可能在内网，需根据具体功能区分。注：若邮件系统的Webmail（如Outlook Web Access）需外网访问，则部署在DMZ；后端数据库仍在内网。

·正确答案：b. 门户网站 和 d. 邮件系统

**3. 终端区一般可以做哪些安全管控措施？多选**

终端区（用户设备区域）

**a. 分级防护**

根据终端敏感度（如高管PC vs 普通员工PC）实施差异化管理（如权限控制、软件安装限制）。

**b. 基础边界防护**

边界防护属于防火墙/网关职能（如NGFW过滤外网流量），与终端无关。

**c. 用户认证**

强制终端用户通过AD域、双因素认证（2FA）登录设备，防止非法接入。

**d. 行为管理**

限制终端用户行为（禁止非法外联、阻断高风险网站）或审计操作日志（文件外发）。

**e. 端点防护**

部署终端杀毒（如EDR）、主机防火墙、漏洞补丁管理，直接防护终端设备。

·正确答案：c. 用户认证、d. 行为管理、e. 端点防护

**4. 以下哪些设备通常部署在运维区？多选**

运维区是用于集中管控IT基础设施（如服务器、网络设备）的关键区域

**a. 堡垒机**

统一运维入口，管控运维人员访问权限，记录操作日志（命令审计、会话录像），部署在运维区。

**b. 基线核查**

用于检查系统安全配置（如弱口令、未修复漏洞、多余端口开放），确保符合安全基线。通常由运维/安全团队操作，部署在运维区进行自动化扫描。

**c. 防病毒服务器**

负责病毒库更新分发及策略管理，一般部署在内网统一管理区（全域终端覆盖），而非运维专用区。

**d. 日志审计**

集中收集全网设备日志（防火墙、服务器、数据库），提供合规分析及异常告警，运维区需直接管理日志系统。

**e. 数据库审计**

监控数据库操作（SQL注入、敏感数据导出），通常与运维区联动（数据库维护需通过堡垒机），可集中部署在运维区。

·正确答案为 a. 堡垒机、b. 基线核查、c. 防病毒服务器、d. 日志审计、e. 数据库审计

**5. 部署在互联网出口的AD设备主要实现以下哪些功能？多选**

AD设备（Application Delivery控制器），常用于优化应用交付，比如负载均衡、SSL加速、流量管理等。互联网出口是内外网交界的区域。

**a. 出栈负载均衡**

优化内网用户访问外网资源（如互联网、SaaS服务）时的链路选择。

**b. 入栈负载均衡**

将外部用户的访问请求（如HTTP/HTTPS）分发到多台内部服务器。

**c. 服务器负载均衡**

属于入栈负载均衡的一种具体实现形式，针对内部服务器群（如Web集群、API网关）。

**d. 泄密追踪**

为安全设备（如DLP、日志审计系统）的职责，AD设备不直接参与泄密溯源。

·正确答案：a. 出栈负载均衡、b. 入栈负载均衡、c. 服务器负载均衡

**6. 以下哪些属于链路聚合（Link Aggregation）的优点？多选**

**a. 提高链路可靠性，避免二层单点故障**

链路聚合将多个物理端口绑定为逻辑通道，当其中一条物理链路故障时，流量自动切换到其他可用链路，避免单点故障。

**b. 提升网络带宽**

聚合后的总带宽为各物理链路带宽之和（如2条1Gbps链路聚合后提供2Gbps带宽）。

**c. 节省交换机接口**

链路聚合需占用多个物理接口（如绑定两个端口），本质是提升带宽/可靠性，并未减少接口使用，反而需预留更多接口资源。

**d. 隔离广播**

广播隔离是VLAN或路由器（广播域分割）的功能，链路聚合仅负责物理带宽与可靠性，不改变广播域范围。

·正确答案：a. 提高链路可靠性，避免二层单点故障 和 b. 提升网络带宽

**7. 以下哪些是衡量网络性能的指标？多选**

**a. 带宽**

（Bandwidth）定义：单位时间内网络链路可传输的最大数据量（如100Mbps），是基础性能指标。

**b. 时延**

（Latency）定义：数据从发送端到接收端的传输时间（如RTT为50ms），直接影响实时业务。

**c. 吞吐量**

（Throughput）定义：实际有效传输的数据速率（如实际测速90Mbps），反映网络真实性能。

**d. 用户量**

（User Count）属于网络规模或负载指标，而非性能的直接度量（用户量增大会间接影响性能）。

·正确答案：a. 带宽、b. 时延、c. 吞吐量

**8. 部分企业级路由器有两个WAN口，其主要作用是什么？多选**

**a. 接入光纤**

光纤只是物理介质的类型（如单模/多模），描述的是传输方式，而非功能。路由器WAN口可能是RJ45（电口）或光纤接口，但接口形式并非本题核心，应排除。

**b. 链路聚合**

链路聚合（LACP）需相同设备间多端口绑定（如交换机互联或服务器接入），而广域网中双WAN口通常连接不同ISP链路（如联通+电信），无法直接聚合（协议、带宽、运营商策略均独立）。企业级路由器一般通过多WAN负载均衡（非链路聚合）实现流量分配，因此此选项不准确。

**c. 增加带宽**

负载均衡实现：双WAN口可同时承载流量（如视频会议走WAN1、网页浏览走WAN2），提升总体带宽利用率。但实际速率上限受单条链路带宽限制（两条100M线路无法合并为200M单线程下载）。

**d. 冗余备份**

主备切换：若主WAN链路故障（如光纤断裂），路由器可自动切换至备用链路，保证业务连续性（如金融交易系统）。

·正确答案：c. 增加带宽、d. 冗余备份

**9. 企业初创阶段内部网络一般需要做如下哪些防护？多选**

**a. 基础边界防护**

初创企业首要需通过防火墙（如NGFW）、NAT等设备阻止外部攻击（端口扫描、暴力破解）。

**b. 用户权限管理**

最小权限原则：限制员工访问敏感数据的权限（如仅允许财务人员访问财务系统），防止数据误操作或泄露。

**c. 数据库审计**

适用阶段：属于高阶安全需求，通常在企业进入成熟期或面临合规性（如GDPR、等保2.0）要求时部署，初创阶段资源有限可暂缓。

**d. 端点防护**

基础安全屏障：部署杀毒软件（如EDR、诺顿）、强制更新补丁，防止病毒/勒索软件通过员工设备侵入内网。

·正确答案：a. 基础边界防护、d. 端点防护

**10. 以下关于虚拟机的说法正确的是？多选**

**a. 一台物理服务器可以虚拟多台虚拟机**

虚拟化技术（如VMware ESXi、Hyper-V）的核心能力是将物理机资源（CPU、内存、磁盘）虚拟化为多台独立虚拟机（VM）。

**b. 虚拟机上需要安装操作系统才能部署服务程序**

虚拟机类似独立计算机，需安装完整的客户机操作系统（如Windows、Linux），之后才能部署服务（如Apache、MySQL）。

对比容器：容器技术（如Docker）共享宿主内核，无需独立OS，如果使用的是容器（如 Docker）或Serverless架构，则可能不需要完整的操作系统。

**c. 虚拟机与虚拟机之间资源、数据相互隔离，互不影响**

虚拟化特性：虚拟化层（Hypervisor）确保各虚拟机资源分配独立，数据存储隔离（如VMDK文件分属不同VM），单VM故障不会波及其他VM或物理机。

**d. 虚拟机崩溃会导致物理机崩溃，服务中断**

虚拟机崩溃仅影响自身服务，物理机或其他VM通常不受影响（除非极端情况，如Hypervisor漏洞或物理硬件故障）。

·正确答案：a. 一台物理服务器可以虚拟多台虚拟机、c. 虚拟机与虚拟机之间资源、数据相互隔离，互不影响

**11. 以下关于桌面云的说法正确的是？多选**

**a. 桌面云能够帮助解决数据安全性的问题**

桌面云将数据和计算资源集中在云端（数据中心），本地终端仅接收图像和传输操作指令，避免数据存储在用户设备（如U盘或本地硬盘）导致的泄露风险。

**b. 桌面云的数据存储在客户数据中心的服务器中**

私有云场景下，数据通常存储在客户自有的数据中心服务器中；公有云场景下（如阿里云桌面服务），数据存在服务商数据中心，但题目未明确区分，应基于常规企业级部署模式判断。

**c. 桌面终端用于传输图像、操作指令、文件数据**

图像：接收并显示云端渲染的桌面画面，如分辨率、刷新率依赖网络传输。

操作指令：将键盘鼠标输入（如点击、快捷键）发送至云端处理。

文件数据：如用户通过终端进行文件上传/下载（如拖拽文件到云桌面，不一定允许下载）时，终端直接参与传输文件内容。

**d. 相比传统PC，桌面云能有效提升运维效率**

核心优势：

统一管理：批量派发镜像更新、修复漏洞，无需逐台操作物理PC。

故障恢复：云端快速重置VM，避免物理设备维修耗时。

·正确答案：a. 桌面云能够帮助解决数据安全性的问题、d. 相比传统PC，桌面云能有效提升运维效率

**12. 以下关于公有云的说法正确的是？多选**

**a. 按需付费**

公有云基于“用多少付多少”（Pay-as-you-go）的模型，如AWS EC2实例按小时计费、存储按GB/月收费。用户无须长期采购硬件，避免资源浪费。

**b. 灵活扩容**

公有云支持动态调整资源规模（如阿里云ECS弹性伸缩组），突发流量时自动扩容，业务低峰期释放资源以节省成本。

**c. 用户投资低**

公有云将CAPEX（资本支出，如购买服务器）转化为OPEX（运营支出），企业无需承担服务器采购和机房建设的高昂成本。

**d. 适合用户的敏态业务**

敏态业务：指需要快速迭代、频繁变更的业务（如互联网电商、AI训练），公有云的弹性算力支持敏捷开发和灰度发布。

对比稳态业务：如传统ERP系统（稳定、低变更），通常更适合私有云或本地部署。

正确答案：a. 按需付费、b. 灵活扩容、c. 用户投资低、d. 适合用户的敏态业务

**13. 深信服能为用户提供哪些安全服务？多选**

**a. 风险评估**

深信服提供完整的安全风险评估，通过对网络架构、资产暴露面、漏洞库匹配等分析，输出风险报告（如高危漏洞、弱密码策略、外网服务暴露）。

典型工具：结合云端威胁情报和本地化扫描引擎，覆盖等保合规及攻击链模拟。

**b. 安全巡检**

定期检查客户安全设备（如防火墙、EDR）的运行状态、策略有效性、日志完整性，确保防护策略与当前威胁匹配（如勒索软件防御规则更新）。

实现方式：支持远程自动化巡检+人工深度分析，提供修复建议。

**c. 安全咨询**

涵盖安全体系建设（如零信任架构规划）、合规性咨询（等保2.0、GDPR）、攻防演练（红蓝对抗）及事件响应（IR）。

**d. 业务系统建设**

业务系统建设（如ERP、OA开发）属于软件开发或IT集成商范畴，深信服作为安全与云计算厂商，核心定位为安全能力输出（如业务系统安全加固），而非全面承接业务系统的开发与部署。

·正确答案：a. 风险评估、b. 安全巡检、c. 安全咨询

**14. 以下哪个接口是家用无线路由器，链接互联网的接口？单选**

**a. WAN口**

（广域网接口）

功能：连接外部网络（如互联网）的入口，通过网线与调制解调器（光猫）相连，接收来自互联网服务提供商（ISP）的网络信号。

示例：家庭宽带安装时，光猫的网线插入路由器WAN口，路由器通过该接口访问公网。

**b. LAN口**

（局域网接口）

用途：连接内部设备（如电脑、打印机），负责内网数据交换。

误区：若误接LAN口至光猫，则路由器无法获取公网IP，导致无法上网。

**c. WLAN**

（无线局域网）

定位：提供无线网络覆盖（如Wi-Fi 6），属于内部通信方式，非物理接口。

**d. USB接口**

功能：扩展外接设备（如硬盘、4G上网卡），非主用互联网接入方式。

·正确答案： a. WAN口

**15. 以下说法错误的是？单选**

**a. 带宽表示单位时间内能够传输的数据总量，单位是bps**

**b. 报文从网络的一端到另一端所需要的时间，时延越低，网络质量越好**

**c. 网络抖动是指网络的最大时延，用来评价网络的稳定性，抖动越小，网络越稳定**

抖动（Jitter）定义为时延的变化率（即不同报文传输时间的波动范围），而非最大时延。抖动越小，时延越稳定（如RTP流媒体中抖动影响音画同步）。若时延在20ms~50ms波动，则抖动为30ms，而非最大时延50ms。

**d. 丢包指一个或多个数据包的数据无法通过网络到达目的地**

·正确答案： c

# 第二章 OSI七层模型

## OSI七层模型的意义

1. 模块化通信：将复杂的网络通信抽象为分层结构，每层专注于特定功能，简化开发与维护。

2. 标准化接口：各层定义标准协议，实现跨厂商设备兼容（如HTTP协议统一全球Web交互）。

3. 故障隔离：分层设计便于定位问题（如传输层丢包与物理层线路断开可快速区分）。

## OSI七层模型各层功能与典型协议/设备

**1. 应用层（Application Layer）**

* 功能：直接面向用户应用，提供网络服务接口（如浏览器访问网页）。
* 典型协议：HTTP（网页）、SMTP（邮件）、FTP（文件传输）、DNS（域名解析）。
* 设备/示例：Web服务器（Nginx）、客户端应用（浏览器）。

示例场景：浏览器输入URL后，应用层发起HTTP请求。

**2. 表示层（Presentation Layer）**

* 功能：数据格式转换（如ASCII→二进制）、加密（SSL/TLS）、压缩（GZIP）。
* 典型协议：JPEG（图片压缩）、MPEG（视频编码）、ASCII（字符编码）。

示例场景：提交登录密码时，表示层加密密码为密文。

**3. 会话层（Session Layer）**

* 功能：建立、管理、终止会话（如远程会议连接）。
* 典型协议：RPC（远程过程调用）、NetBIOS（Windows会话）。

示例场景：视频通话时，会话层维持通话链路稳定。

**4. 传输层（Transport Layer）**

* 功能：端到端数据传输（可靠/不可靠）、流量控制、差错校验。
* 典型协议：TCP（可靠传输）、UDP（高效传输）。
* 核心概念：端口号（标识应用进程，如80→HTTP，443→HTTPS）。

示例场景：下载文件时，TCP确保数据完整无误。

**5. 网络层（Network Layer）**

* 功能：路由寻址（决定数据包路径）、逻辑地址（IP地址）分配。
* 典型协议：IP、ICMP（Ping检测）、BGP（路由协议）。
* 设备：路由器、三层交换机。

示例场景：IP地址决定数据从北京到上海的传输路径。

**6. 数据链路层（Data Link Layer）**

* 功能：物理寻址（MAC地址）、帧同步、差错控制（CRC校验）。
* 典型协议：以太网（Ethernet）、PPP（拨号）、VLAN（虚拟局域网）。
* 设备：交换机、网桥。

示例场景：交换机通过MAC地址转发数据到目标设备。

**7. 物理层（Physical Layer）**

* 功能：物理介质传输（比特流）、电压/光信号转换、接口定义。
* 典型设备：网线（RJ45）、光纤、集线器（Hub）。

示例场景：网线中的电流信号传输“0”和“1”。

## 数据包封装与解封装过程

发送方流程（封装）：

* 应用层 → 生成原始数据（如HTTP请求）。
* 表示层 → 加密/压缩数据。
* 会话层 → 建立会话ID。
* 传输层 → 添加TCP头部（端口号）或UDP头部。
* 网络层 → 添加IP头部（源/目标IP）。
* 数据链路层 → 添加帧头（MAC地址）和CRC校验。
* 物理层 → 转换为比特流并通过网卡发送。

接收方流程（解封装）：

* 物理层 → 接收比特流。
* 数据链路层 → 校验数据帧（MAC地址匹配）。
* 网络层 → 解析IP地址并决定转发。
* 传输层 → 检查端口号并传递到对应应用。
* 上层（会话→应用） → 解密、重组数据，完成应用逻辑。

## TCP与UDP的核心区别与典型应用

表2.1 TCP与UDP的核心区别与典型应用

|  |  |  |
| --- | --- | --- |
| **特性** | **TCP (传输控制协议)** | **UDP (用户数据报协议)** |
| 连接性 | 面向连接（三次握手建立连接） | 无连接 |
| 可靠性 | 可靠（ACK确认、重传机制） | 不可靠（尽力交付，无重传） |
| 数据顺序 | 保证数据顺序 | 不保证顺序 |
| 流量控制 | 滑动窗口机制控制发送速率 | 无流量控制 |
| 拥塞控制 | 慢启动、拥塞避免 | 无拥塞控制 |
| 头部开销 | 大（20字节头部） | 小（8字节头部） |
| 典型应用场景 | 需要数据完整性的场景：  - HTTP/HTTPS  - 文件传输（FTP）  - 邮件（SMTP） | 对实时性要求高的场景：  - 视频会议（Zoom）  - 直播流媒体（RTP）  - DNS查询 |

## 相关考试题

**1. 超文本传输协议HTTP使用的熟知端口号为？单选**

牢记以下常用端口绑定：

20/21 → FTP

22 → SSH

25 → SMTP

53 → DNS

80 → HTTP

443 → HTTPS

3389 → RDP

**a. 21**

21：FTP（文件传输协议）的控制连接端口，用于上传/下载文件。

**b. 25**

25：SMTP（简单邮件传输协议）端口，用于发送邮件（如Outlook配置发件服务器）。

**c. 80**

标准端口：HTTP（HyperText Transfer Protocol）是为未加密的网页通信设计的协议，其默认熟知端口为 80。

典型场景：当在浏览器输入 http://example.com 时，浏览器自动通过 80 端口与服务器建立TCP连接。

**d. 443**

443：HTTPS（加密HTTP）端口，通过SSL/TLS加密数据传输（如网银、支付页面）。

正确答案： c. 80

**2. OSI的结构是()层模型？单选**

可使用口诀辅助记忆：

"All People Seem To Need Data Processing"

“物链网输会示用”

首字母对应：

应用层 (Application)

表示层 (Presentation)

会话层 (Session)

传输层 (Transport)

网络层 (Network)

数据链路层 (Data Link)

物理层 (Physical)

**a. 6**

**b. 7**

**c. 8**

**d. 9**

正确答案： b. 7

**3. 在传输距离相同的条件下，目前哪种介质所支持的信息传输速率最大？单选**

**a. 同轴电缆**

带宽上限（如DOCSIS 4.0为10Gbps下行），且易受电磁干扰（如家用网线靠近电源线时）。

**b. 光纤**

传输原理：光信号通过玻璃/塑料纤维传输，具备更低的信号衰减和抗电磁干扰能力，适合长距离高带宽场景。

带宽潜力：单模光纤理论带宽可达 100Tbps，远超其他介质。实际商用如400Gbps骨干网已广泛应用。

**c. 双绞线**

短距离（100米内）可支持万兆（Cat6a/Cat7），但距离延长后需中继器，速率大幅下降。

**d. 电话线**

传统铜线（如ADSL）最高仅100Mbps，且距离超过3公里时性能急速衰减。

正确答案： b. 光纤

**4. 以下关于TCP协议的描述中，错误的是？单选**

核心能力：TCP通过以下机制保障数据可靠传输：

* 三次握手建立连接（选项c正确）。
* 序列号与确认应答（ACK）：接收方需确认收到的数据包，否则触发超时重传。
* 滑动窗口流量控制：动态调整发送速率，避免接收方缓冲区溢出。
* 拥塞控制算法（如慢启动、拥塞避免）。

局限性：这些机制只能降低丢包概率并重传已丢失的包，但无法完全避免网络故障导致的丢包（如物理链路中断）。

**a. TCP协议使用端口号来区分应用进程**

**b. TCP协议是可靠协议**

**c. TCP协议在开始传输用户数据前会建立TCP三次握手**

**d. TCP协议保障了数据传输过程中不会丢包**

正确答案： d. TCP协议保障了数据传输过程中不会丢包

**5. 在OSI参考模型中，从最底层到最上层的正确顺序是？**

从最底层到最上层的正确顺序为：

物理层 → 数据链路层 → 网络层 → 传输层 → 会话层 → 表示层 → 应用层

**6. 访问支付宝网站的时候使用的是什么协议？单选**

所有涉及敏感信息的网站（银行、支付、社交账号登录）均强制使用HTTPS，HTTP已逐步被淘汰于非敏感场景。

**a. FTP**

用于文件上传/下载（如网站后台更新页面），与用户访问网站流程无关。

**b. HTTPS**

HTTPS = HTTP + SSL/TLS加密：

特征：浏览器显示锁形图标，网址前缀为 https://。

作用：加密数据、验证服务器身份，确保数据完整性。

**c. SMTP**

用于邮件发送（如Outlook发邮件），与网页访问无关。

**d. HTP**

非标准协议，可能为HTTP的笔误，但支付宝不会使用明文HTTP。

正确答案： b. HTTPS

7. 在TCP/IP的传输层中，小于()的端口被用于和现有的服务一一对应？单选

TCP/IP端口分类标准：

* 公认端口（Well-Known Ports）：0~1023，由IANA分配，用于全局性、广泛认可的服务（如HTTP=80、SSH=22）。
* 注册端口（Registered Ports）：1024~49151，组织可申请注册使用（如MySQL=3306），但不强制绑定。
* 动态/私有端口（Dynamic Ports）：49152~65535，客户端临时使用。

**a. 100**

**b. 999**

**c. 65535**

**d. 1024**

正确答案： d. 1024

**8. 以下关于OSI七层模型说法错误的是？单选**

**a. 表示层提供数据格式转换服务**

表示层负责加密、压缩、数据格式转换（如JSON→XML）。

**b. 会话层建立和维护应用程序访问验证和会话**

会话层管理会话生命周期（如SSH登录时维持连接）。

**c. 网络层建立和维护应用程序访问验证和会话**

网络层的核心功能是逻辑寻址（IP地址）和路由选择，确保数据跨网络传输。

**d. 数据链路层建立实体链路链接，通过MAC地址提供可靠数据传输服务**

数据链路层通过MAC地址寻址并提供帧同步，但其主要传输方式是“尽力而为”（如以太网不可靠）。数据链路层通常不保证“可靠性”（可靠性由传输层TCP实现），但某些特殊链路协议（如HDLC）可能支持。

正确答案： c. 网络层建立和维护应用程序访问验证和会话

**9. 以下关于网络层的说法正确的是？单选**

**a. 路由器根据源IP进行路由线路**

错误：路由器的主要路由决策基于目的IP地址，而非源IP地址。

例外：某些高级策略路由（Policy-Based Routing）可能根据源IP调整路径，但题干描述为“网络层的主要说法”，此时默认基础路由机制，而非特殊场景。

**b. 路由选路是一开始就选好的，中途不会改变**

错误：动态路由协议（如OSPF、BGP）会根据网络实时状态（如链路故障、拥塞）动态调整路径。例如，某条光纤切断时，路由表会重新计算最优路径。

**c. 数据包传输的过程中源IP和目的IP每一跳都会改变**

常规路由：源IP和目的IP在整个传输过程中保持不变（如从北京发往上海的IP包，无论经多少个路由器，IP地址始终是源和目的）。

例外：仅在有NAT（网络地址转换）时会改变（如内网IP→公网IP），但NAT是特定场景且非默认路由行为。

**d. 每个路由节点数据包MAC地址都会改变**

链路层特性：每个路由节点在转发数据包时，会替换当前链路的源/目的MAC地址。

核心逻辑：MAC地址仅在本地链路有效，每个局域网（广播域）需要重新封装新的MAC地址。

正确答案： d. 每个路由节点数据包MAC地址都会改变

**10. 下面哪项是OSI模型等参考模型的优点？多选**

**a. 对任何一层的修改不会影响其他层**

各层通过严格定义的接口通信，某一层内部的修改（如协议升级）不影响其他层，前提是接口规范不变。

**b. 通信被划分为更小、更简单的组件，从而有利于组件开发、设计和故障排除**

将复杂通信过程分解为七层，每层专注于单一功能，简化开发（如专注实现传输层协议）和问题定位（逐层排查）。

**c. 通过网络组件标准化支持多厂商联合开发**

OSI模型定义了各层标准协议（如网络层IP），厂商可基于标准开发兼容设备（如Cisco与华为路由器互联）。

**d. 让各类型的网络硬件和软件能够相互通信**

硬件/软件只要遵守同一协议即可通信（如Windows电脑与Linux服务器通过HTTP交互）。

正确答案： a、b、c、d

**11. 以下哪些协议属于应用层协议？多选**

直接面向用户程序，提供网络服务接口（如电子邮件、文件传输、网页浏览）。

**a. HTTPS**

应用层 加密的HTTP协议，用于安全网页访问（如支付宝）。

**b. TCP**

传输层（第四层） 提供可靠传输服务，与端口号绑定（如HTTP基于TCP）。

**c. SMTP**

应用层 邮件发送协议（如Outlook发信到Gmail服务器）。

**d. FTP**

应用层 文件传输协议（如上传网站源码到服务器）。

**e. IP**

网络层（第三层） 逻辑寻址（IP地址）、路由选择的底层协议。

正确答案： a. HTTPS，c. SMTP，d. FTP

**12. 以下说法正确的是？多选**

邮件系统（SMTP/POP3/IMAP）需要确保邮件内容完整无误，需TCP可靠传输。

浏览器（HTTP/HTTPS）加载网页依赖TCP确保所有资源（HTML、图片等）完整到达。

UDP支持低延迟传输，轻微丢包对音视频流畅性影响小，是实时媒体的首选。

**a. 邮件、浏览器等能使用的传输层协议是TCP协议**

**b. 邮件、浏览器等能使用的传输层协议是UDP协议**

**c. 抖音直播、YY语音等使用的传输层协议是TCP协议**

**d. 抖音直播、YY语音等使用的传输层协议是UDP协议**

正确答案： a. 邮件、浏览器等能使用的传输层协议是TCP协议，d. 抖音直播、YY语音等使用的传输层协议是UDP协议

**13. 以下关于端口号的说法正确的是？多选**

**a. 端口号的主要作用之一是区分不同的应用程序**

端口号的本质作用是通过传输层协议（TCP/UDP）区分同一IP地址下不同应用程序的通信（例：浏览器使用80端口、邮件客户端使用25端口）。

**b. 端口号主要包含目的端口号与源端口号两类**

在TCP/UDP的数据包结构中，源端口号（发送方应用程序端口）与目的端口号（接收方应用程序端口）是必填字段，两者缺一不可。

**c. 源端口号是固定的**

源端口通常由客户端动态分配（范围通常为49152~65535），每次连接可能不同。例如，Chrome每次访问网站时可能使用不同源端口（如5001、5002）。

**d. 目的端口号是随机产生的**

目的端口由服务端应用预先定义（如SSH=22、FTP=21），客户端必须明确指定目的端口以访问服务。

正确答案： a. 端口号的主要作用之一是区分不同的应用程序，b. 端口号主要包含目的端口号与源端口号两类

# 第三章 二层通信基础原理与常见问题

## 二层通信的完整过程

**1. 二层通信基础架构**

* 参与设备：同网段内的主机、二层交换机（无路由功能）。
* 通信目标：基于MAC地址直连通信（无需IP路由）。

**2. 详细通信流程**（结合ARP（Address Resolution Protocol, 地址解析协议）与交换机转发）

场景：主机A（IP: 192.168.1.2，MAC: AA） → 主机B（IP: 192.168.1.3，MAC: BB）。

表3.1 二层通信流程示例

|  |  |  |
| --- | --- | --- |
| **步骤** | **过程说明** | **协议/设备角色** |
| 1. ARP请求（广播） | A发送ARP广播报文（目的MAC=FF:FF:FF:FF:FF，询问“谁是192.168.1.3，请告诉AA”） | ARP协议（广播查询目标MAC） |
| 2. 交换机洪泛广播 | 交换机收到广播帧后，向所有端口（除接收端口）洪泛该帧 | 学习MAC地址表，初始所有端口无记录 |
| 3. ARP响应（单播） | B收到ARP请求后，单播回复“我是192.168.1.3，MAC是BB” | ARP协议（单播回应） |
| 4. 交换机学习MAC | 交换机记录B的MAC地址与对应端口，后续通信不再广播 | 交换机MAC地址表更新（MAC→端口映射） |
| 5. 主机A向主机B通信 | A用B的MAC封装数据帧，交换机根据MAC表转发帧到B的端口 | 点对点通信，无需广播 |

**3. 二层交换机工作原理**

MAC地址表：动态学习（源MAC→端口）或静态配置。

转发规则：

* 已知MAC → 定向转发到对应端口。
* 未知MAC → 洪泛到所有端口（广播域内）。
* 广播/组播 → 默认洪泛（广播域内）。

## 二层通信常见问题与解决办法

**1. ARP欺骗（ARP Spoofing）**

* 攻击原理：攻击者伪造ARP响应，声明自己是目标IP的拥有者（例如伪造网关MAC）
* 危害：中间人窃听、流量劫持
* 解决办法：动态ARP检测（DAI）：交换机绑定IP-MAC，拒绝非法ARP报文

**2. 泛洪攻击（MAC Flooding）**

* 攻击原理：攻击者发送大量虚假MAC地址的帧，耗尽交换机MAC地址表容量
* 危害：交换机退化为Hub模式，导致全网广播风暴
* 解决办法：端口安全（Port Security）：限制每端口允许的MAC数量，超出则关闭端口

**3. 二层单点故障**

* 攻击原理：交换网络未配置冗余链路（如单交换机或单链路）
* 危害：链路/设备故障导致全网中断
* 解决办法：生成树协议（STP）：自动阻塞冗余路径，并在主链路失效时激活备用路径

**4. DHCP欺骗（DHCP Spoofing）**

攻击原理：攻击者伪造DHCP（动态主机配置协议，Dynamic Host Configuration Protocol）服务器，分配错误的IP或网关（如DNS指向钓鱼网站）

危害：客户端被引导至恶意网络

解决办法：DHCP Snooping：交换机仅信任指定端口的DHCP响应，拒绝非法服务器

## DHCP的作用与工作原理

**1. DHCP核心作用**

* IP自动分配：为客户端动态分配IP地址、子网掩码、默认网关、DNS等参数。
* 地址管理：防止IP冲突，回收过期IP地址。

**2.** **DHCP四步工作原理**

表3.2 DHCP四步工作原理

|  |  |  |
| --- | --- | --- |
| **步骤** | **报文类型** | **交互过程** |
| Discover | 客户端广播寻找DHCP服务器 | 发送DHCP DISCOVER报文 （源IP=0.0.0.0） |
| Offer | 服务器回应可用IP地址 | 服务器发送DHCP OFFER报文 （包含IP和租期） |
| Request | 客户端确认选择IP | 客户端广播DHCP REQUEST报文 （确认选择） |
| Ack | 服务器最终确认分配 | 服务器发送DHCP ACK完成分配 |

**3. 防御DHCP耗尽攻击（DHCP Starvation）**

* DHCP Snooping：交换机记录合法DHCP服务器端口，并过滤非法Offer报文。
* 限制请求速率：限制客户端每秒DHCP请求次数，防止攻击者快速耗尽地址池。