# 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。

## 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）。