计算机网络

办公室或基地的计算机网络需求取决于机构的预算、规模、容量和整体业务需求。 机构应考虑聘用专业 IT 和网络人员来辅助办公室和分支机构的网络建设。

办公室/基地设置

大多数机构现场都会混合使用几种办公室网络设备。 这些设备可能包括：

与外部互联网服务商的连接 ——与外部互联网服务商 (ISP) 的连接可以采用卫星互联网、电话线或其他互联网服务商专用网络连接形式。

调制解调器 ——调制解调器接收来自互联网服务商的信号，然后将其转换为家庭或办公室网络可用的信号。 调制解调器还包含特定于用户的信息，用于识别、跟踪和监测流量，从而实现安全和计费目的。 如果没有调制解调器，家庭或办公室的网络设备都将无法与外部网络通信。

路由器 ——路由器是一种分割和管理互联网流量的设备，从而让多台计算设备拥有自己的唯一 IP 和 MAC 地址，并能够通过网络，同时与互联网以及在彼此之间通信。 路由器有多种配置和功能。 一些可以监测和控制本地网络的流量，一些具有 WIFI 功能。 要使用的路由器类型将取决于运营需求。

防火墙 ——防火墙是专门用于监测和过滤来自外部网络的互联网内容的设备。 防火墙可用于阻止恶意软件、未经授权的网络入侵，甚至屏蔽组织 IT 政策所不允许的内容。 在简化的网络中，防火墙通常与调制解调器或路由器集成在一起，但如果是高级网络，则可以拥有独立的防火墙，对不同用户设置不同的协议。

交换机 ——网络交换机像是路由器的一种高级形式，可在多个联网设备之间控制和分配互联网流量，同时还能在单个设备级别上进行监测和控制。 交换机还用于过滤、屏蔽和保护内部网络，类似于阻止外部威胁的防火墙。

服务器 ——服务器是在网络中完全专用于储存和共享文件的计算机。 服务器可以像普通台式计算机一样简单，也可以像具有特殊安装要求的大型专业计算设备一样复杂。 近年来，许多机构已开始使用“异地”服务器，在办公室以外的地点（有时是在其他国家）托管及管理文件和数据。 异地服务器是完全可以接受的解决方案，但若服务器用户采用不同的互联网连接方式，最好使用本地服务器。

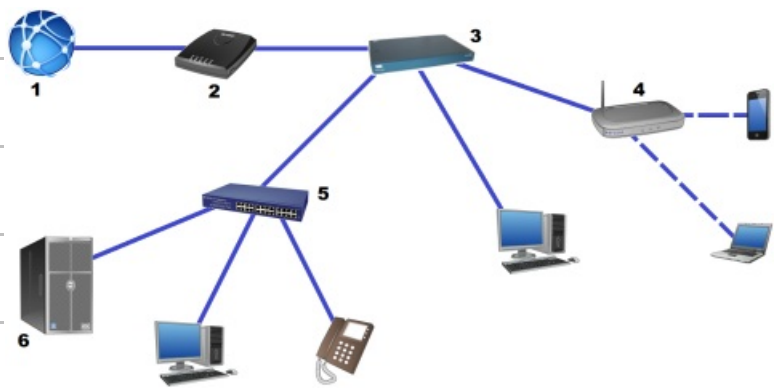
1 外部互联网服务商

2 调制解调器

3 路由器/防火墙

4 WIFI 路由器

5 网络交换机



6 服务器

运营安全

每个本地网络的运营安全要求都应遵循基本的规则。

访问权限控制 ——只有获得授权的人员才能访问网络和计算设备。 所有计算机都应使用密码保护，而且 WIFI 路由器也应要求提供登录凭据。 有些网络允许访客临时访问，而对特殊设置的需求因运营环境而异。

恶意软件 ——网络上的所有计算设备都应安装某种形式的防病毒软件，且操作系统应始终为最新版。 机构应考虑安装可管理设置的防火墙和/或交换机，从而减少网络入侵尝试或恶意软件的传输。

IT 政策 ——各机构应为使用网络的所有员工和用户制定与共享内部 IT 政策。 IT 政策应包括规定可接受行为的规章制度、使用不同类型硬件的规章制度以及惩罚违规行为的指导原则。