第1章

远程网络连接需求

各种网络应用的不断出现对网络提出了越来越高的要求。网络不仅应具备基本的连通性，具备足够的性能和安全性，而且必须是智能而优化的，可以适应复杂的需求和状况。本章将给出远程网络连接的主要需求概况。

1.1 本章目标

学习完本章，应该能够达到以下目标。

(1) 描述远程连接的典型需求分类。

(2) 描述大规模网络对广域连通性的需求。

(3) 描述大规模网络对安全性的需求。

(4) 描述大规模网络对优化性的需求。

1.2 远程连接需求分类

在构造网络的远程连接部分时的需求如下。

(1) 连通性需求。它是计算机网络的基本功能。要通过计算机网络将分散于各地的机构、人员、设施连接起来，必须根据其使用时间、地点、所需带宽，以及可以承受的费用选择适当的连接方式。远程连接的可靠性相对较低，相对更容易发生故障，因此应该对重要的站点和应用配置冗余连接或备份连接。

(2) 安全性需求。由于远程连接超出组织本身的管理范围，构建在其他组织的网络和设施之上，因此面临着更多的安全风险，例如数据遭到窃听、攻击者非法拨号接入等。因此网络必须能够确认接入者的身份，防止远程传输的数据被窃听或伪造，对外隐藏网络内部的细节信息，减少系统的漏洞，防范潜在的攻击风险。

(3) 优化性需求。基于网络的应用日趋多样化，而远程连接的带宽相对较为昂贵，因此更容易发生资源不足的情况。在此种情况下，网络应该有能力辨别出不同的应用类型、用户和数据流，并为其提供适当的资源。

1.3 连通性需求

典型的企业网络由少数园区、少量大/中型分支机构、较多的小型分支机构以及一定数量的 SOHO(Small Office & Home Office)/移动办公人员构成(图 1-1)。其各部分对远程连通性的需求包括。

(1) 园区及大型分支机构之间。作为核心的园区和大型分支机构之间数据传输量大，也经常处于整个网络的核心，其稳定性直接关系到整个网络的稳定性，因此在其互连时经常采用高速、高可靠性的连接方式，如高速专线、高速 MAN 连接、高速分组交换 WAN 连接等。为了进一步提高可靠性，经常采用双线路冗余，甚至从两个以上的运营商租用线路。

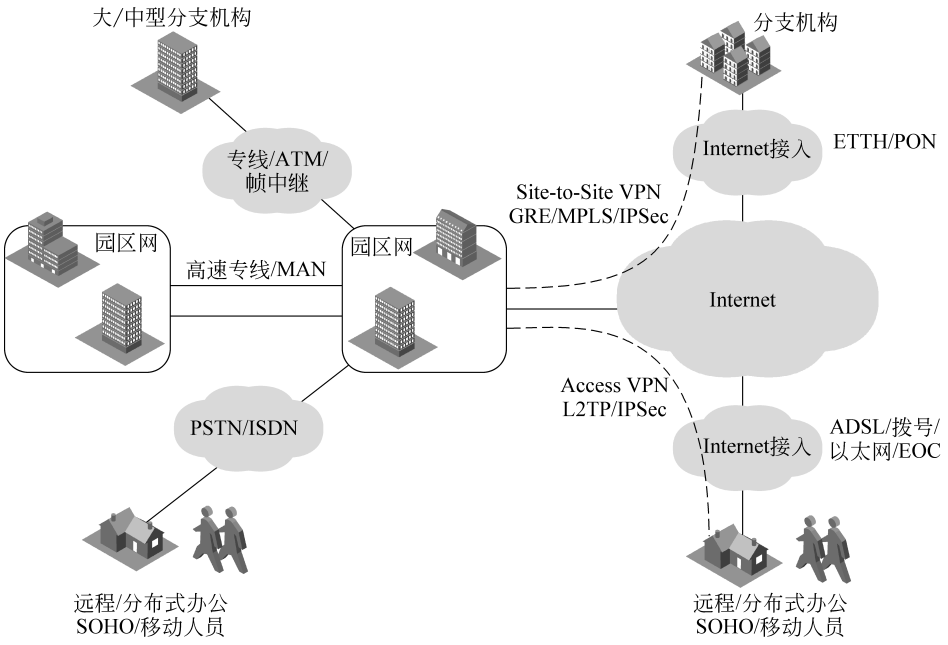

图 1-1　连通性需求

(2) 中型分支机构。中型分支机构的数量多于大型分支机构和园区,数据量和稳定性要求高于小型分支机构。根据费用与性能的平衡,中型分支机构可以采用中低速专线、分组交换技术或 Site-to-Site VPN 技术连接到网络的核心。

(3) 小型分支机构/SOHO/移动办公人员。小型分支机构数量大,数据量低;SOHO/移动办公人员要求随时随地可以接入,并且接入费用应比较低廉。因而它们通常利用无处不在的 Internet 通过 Access VPN 技术接入,或用基于 ISDN/PSTN 的拨号直接接入。

1.4　安全性需求

当今的企业网对安全性的需求越来越高,主要体现在广域传输安全性,节点/站点安全性,以及接入安全性等方面。

首先,由于分散于各地的机构需要通过广域网互相连接,企业的数据必须跨越广域网传送,因而数据的广域传输安全性必须得到保障。对一般的组织而言,直接从运营商租用的专线和分组交换 WAN 连接的安全性较高;而公共网络的安全性较低,在基于公共网络构建的 VPN 中传送的数据容易遭到窃听和篡改,因此通常采用 IPSec 对报文进行完整性检查和加密。

其次,一个组织的数据处理和存储设备实际上都位于各个节点或站点中,因而节点/站点本身的安全性也必须得到保障。对外通告内部的明细路由信息或链路状态信息相当于通告了整个网络的结构,这样做的风险比较大。因而在不同组织之间发布路由时,通常会对发布的路由信息加以控制。

一个有效方法是在组织内部使用私有地址,这种地址无法在公共网络上直接路由。使用通用路由 GRE(Generic Routing Encapsulation)这种 Site-to-Site VPN 技术允许跨越公共网连接使用私有地址的站点。

另一个更安全的方法是在组织内部使用独立的地址空间,这种地址空间可以与外部地址

空间重合，因而无法从外部网络直接访问。BGP/MPLS VPN 技术允许企业、运营商使用完全重合的地址空间构建 VPN，获得更高的节点/站点安全性。

最后，通常每个组织都会有一定数量的人员在外出差或 SOHO 办公，必须允许这些人随时随地接入内部网络，因此保证用户接入安全性就非常重要。允许移动人员远程接入意味着任何人都可以通过相同的远程访问技术连接到组织的网络，要防止这种非法访问，必须对接入用户的身份进行严格验证，并对其授予适当的访问权限。这通常通过基于 RADIUS/TACACS 的 AAA 技术实现。

1.5 优化性需求

与早期仅用于文件和打印共享的局域网不同，当今网络规模不断扩大，其中的应用日益丰富，各种各样的数据共存于同一个网络上。典型企业网的应用及其优化需求（图 1-2）包括以下几个方面。

（1）网络控制：用于实现和维持网络功能的信息，其种类很多，包括链路协议信息、路由协议信息、ICMP、IGMP、STP、VRRP 等。这类信息重要性很高。

（2）网络管理：用于对网络的性能、故障等进行管理的协议通信，如 SNMP 消息。

（3）文件传输：传输量大，占用大量带宽，如 FTP 和文件共享等。

（4）网络存储：日常动态的网络存储数据量是突发的，而定期批量备份的数据通常是集中而大量的。

（5）语音、视频应用数据及相关应用的控制：占用的带宽相对恒定，要求比较稳定的网络服务。类似 IP 音频/视频电话这样的应用要求比较强的实时性，并且其呼叫控制信息要求很强的实时性和可靠性。

（6）远程维护和操作：要求进行实时的交互式操作，这类应用要求操作流畅，因此对延迟比较敏感，如 Telnet 这样的字符交互应用要求的带宽比较低，但使用越来越广泛的图形化远程操作应用对带宽的要求相对较高。

（7）电子交易和 ERP：此类应数据量较小，但对可靠性的要求非常高。

（8）Internet 访问：此类访问主要包括 Web 访问、下载等，其突发性强，带宽需求不稳定，但通常要求并不严格。

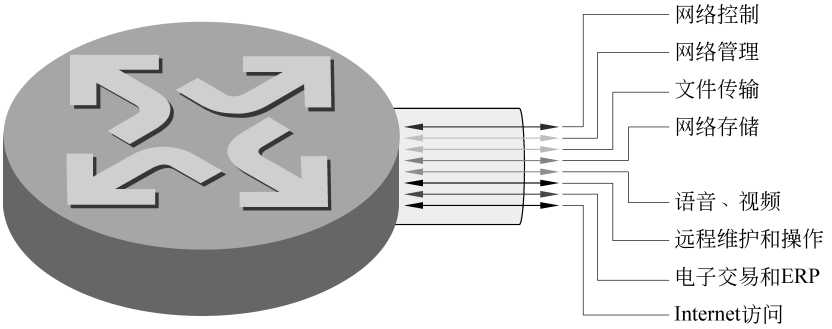

图 1-2 典型企业网的应用及其优化需求

由此可见，各种类型的数据对网络服务的要求有着显著的区别。因此，网络必须能够根据对用户的服务承诺，区分其所发送的报文类型，并根据其特点为其提供不同等级、具有不同特点的服务。这要求网络实现 QoS（Quality of Service，服务质量）。

QoS 是一种对不同的用户、应用类型、数据流提供有差别服务，并可进而保证其获得的网

络资源，提供其所需性能的机制。例如，实现了 QoS 的网络能够对于实时性要求高的 IP 电话音频流报文以最快速度转发；对占用带宽较高的远程容灾备份保证其享有的带宽；对普通用户访问外部网站的流量允许在资源紧缺时部分丢弃，而对网站设计专业人员访问外部网站的流量给予保证等。

1.6　本章总结

（1）远程连接要求以适当的费用提供足够的性能，并确保移动接入的方便性。

（2）远程连接的安全性需求体现在广域传输安全性、节点/站点安全性和接入安全性等方面。

（3）网络应对不同的用户、应用类型、数据流提供有差别服务，并可进而保证其获得的网络资源，提供其所需性能的机制。

1.7　习题和答案

1.7.1　习题

（1）远程网络连接需求包括（　　）。

A. 安全性需求　　B. 优化性需求　　C. 适应性需求　　D. 连通性需求

（2）选择远程网络连接类型时，应考虑其（　　）。

A. 带宽　　B. 费用　　C. 安全性　　D. 可靠性

（3）某公司要求所选取的远程连接线路不可能被窃听，这属于（　　）。

A. 安全性需求　　B. 优化性需求　　C. 连通性需求

（4）某公司要求在带宽不足时优先保证其库存管理应用报文的转发，这属于（　　）。

A. 安全性需求　　B. 优化性需求　　C. 连通性需求

1.7.2　习题答案

（1）ABD　　（2）ABCD　　（3）A　　（4）B