What Is a Virtual Private Network?

A virtual private network (VPN) allows the provisioning of private network services for an Organisation or organizations over a public or shared infrastructure such as the Internet or service provider backbone network. The shared service provider backbone network is known as the VPN backbone and is used to transport traffic for multiple VPNs, as well as possibly non-VPN traffic.

VPNs provisioned using technologies such as Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits (VC) have been available for a long time, but over the past few years IP and IP/Multiprotocol Label Switching (MPLS)-based VPNs have become more and more popular.

This book focuses on describing the deployment of IP- and IP/MPLS-based VPNs. The large number of terms used to categorize and describe the functionality of VPNs has led to a great deal of confusion about what exactly VPNs are and what they can do. The sections that follow cover VPN devices, protocols, technologies, as well as VPN categories and models.

VPN Devices

Before describing the various VPN technologies and models, it is useful to first describe the various customer and provider network devices that are relevant to the discussion.

Devices in the customer network fall into one of two categories:

- **Customer (C) devices**—C devices are simply devices such as routers and switches located within the customer network. These devices do not have direct connectivity to the service provider network. C devices are not aware of the VPN.

- **Customer Edge (CE) devices**—CE devices, as the name suggests, are located at the edge of the customer network and connect to the provider network (via Provider Edge [PE] devices). In CE-based VPNs, CE devices are aware of the VPN. In PE-based VPNs, CE devices are unaware of the VPN.CE devices are either categorized as Customer Edge routers (CE-r), or Customer Edge switches (CE-s).