IP Tunneling and VPNs

Overview

The purpose of this module is to explain Virtual Private Network (VPN) concepts and to overview various L2 and L3 tunneling techniques that allow for implementation of VPNs. The access VPN features in Cisco IOS Release 12.1 are explained along with Layer 2 and Layer 3 tunneling mechanisms.

Objectives

Upon completion of this module, you will be able to perform the following tasks:

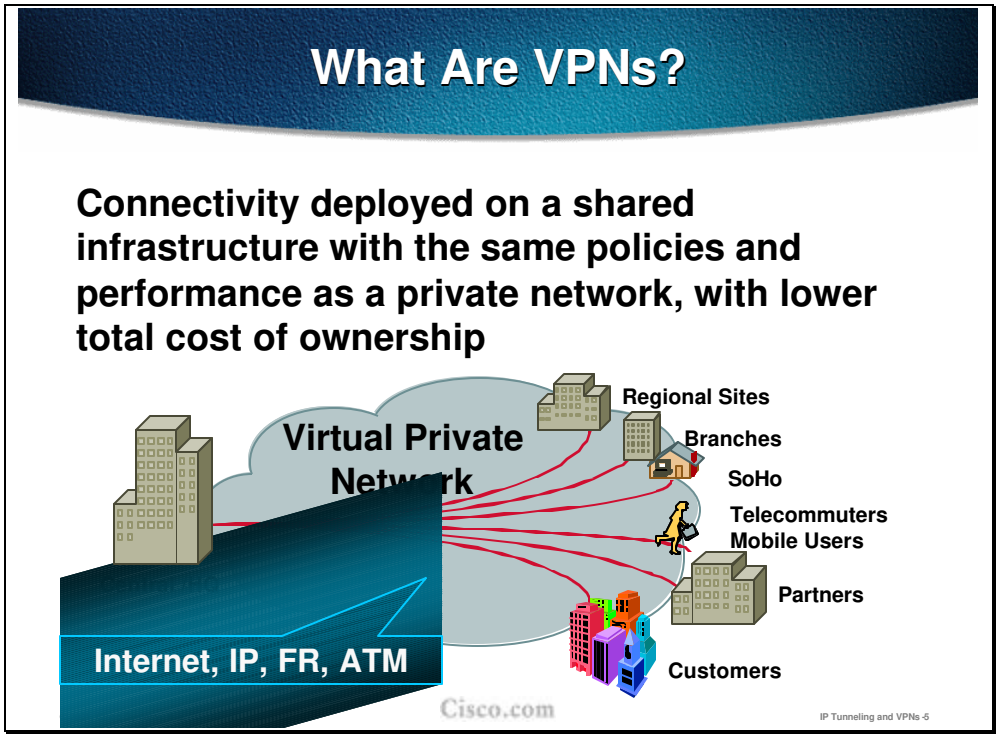
- Explain Virtual Private Network concepts and possibilities
- Describe Layer-2 tunneling features
- Configure support for Microsoft Point-to-Point Tunneling Protocol (PPTP) and Encryption (MPPE)
- Configure L2TP Dial-in and Virtual Private Dial-up Network (VPDN) for dial-in
- Describe and configure GRE Layer-3 tunneling

Introduction to IP VPNs

Objectives

Upon completion of this module, you will be able to perform the following tasks:

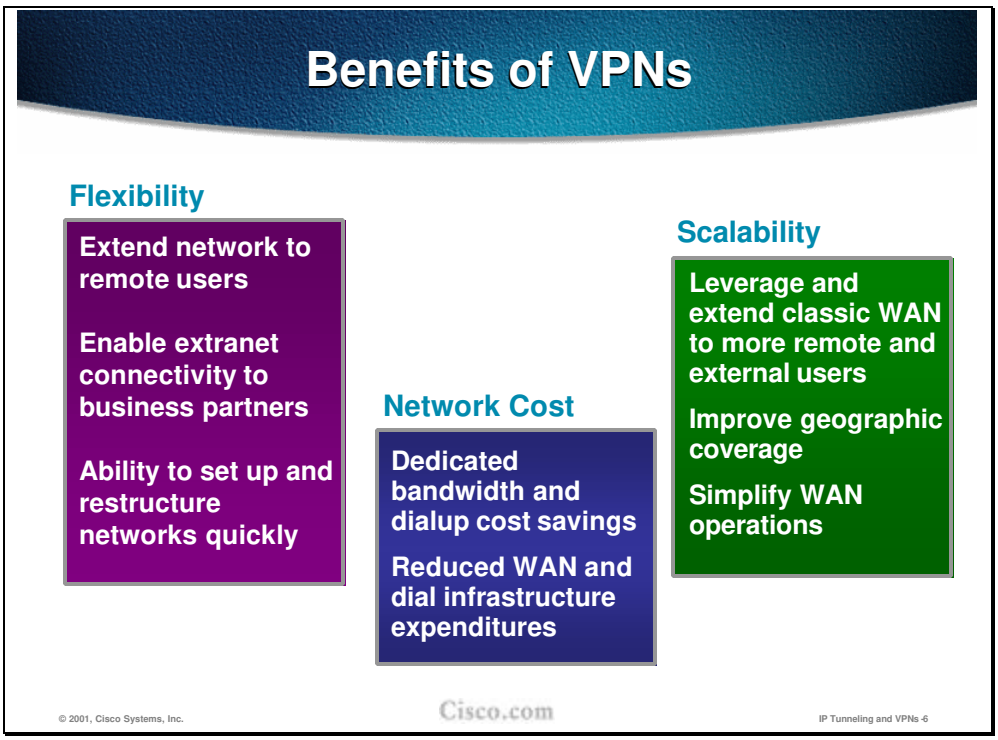
- Define a Virtual Private Network (VPN) and its benefits
- Describe the various types of VPNs:
  - Access, intranet, extranet
  - Layer 2 versus Layer 3
  - Carrier-provided versus not



We will start by defining a VPN.

An academic definition of a VPN is “connectivity deployed on a shared infrastructure with the same policies and performance as a private network, with lower total cost of ownership.”

The infrastructure is public, and can be either the Internet, an IP infrastructure, a Frame Relay network, or an Asynchronous Transfer Mode (ATM) WAN. Our focus today is on the big “I,” the public Internet and IP VPNs, to the exclusion of Frame Relay and ATM.

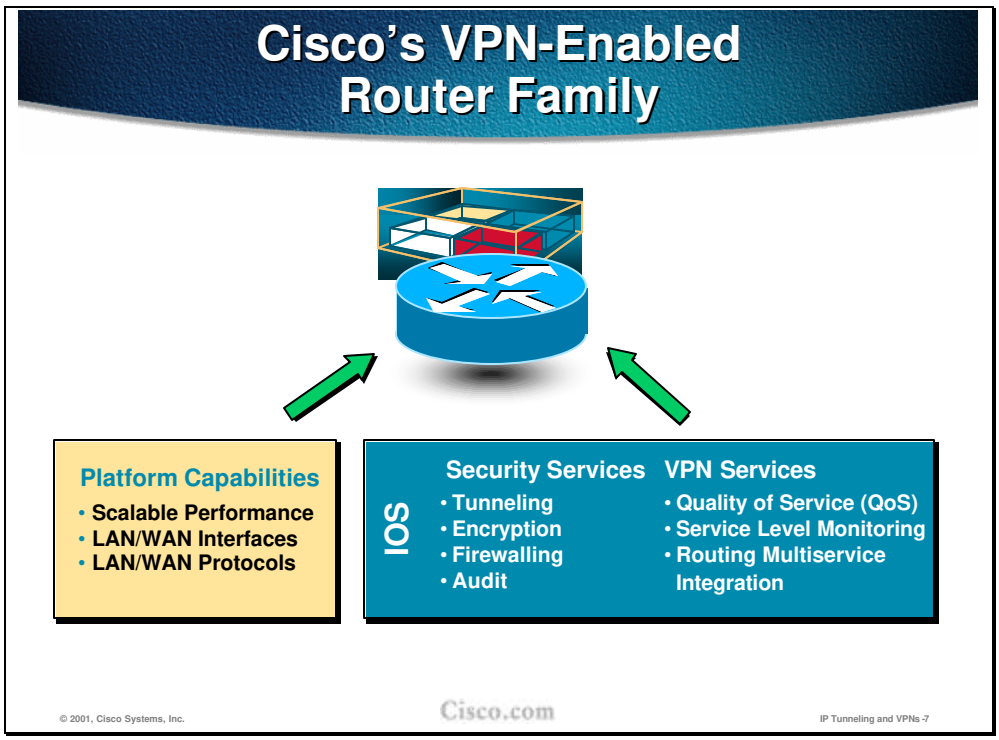


The slide lists some of the benefits of VPNs, which are primarily flexibility, scalability, and lowered cost of communication.

VPNs offer flexiblity as site-to-site and remote-access connections can be set up quickly and over existing infrastructure. A variety of security policies can be provisioned in a VPN, enabling flexible interconnection of different security domains.

VPNs also offer scalability over large areas, as IP transport is universally available. This in turn reduces the number of physical connections and simplifies the underlying structure of a customer WAN.

Lower cost is one of the main reasons for migrating from traditional connectivity options to a VPN connection, as customers may reuse existing links and take advantage of statistical packet multiplexing features of IP networks, used as a VPN transport.



The Cisco hardware and Cisco IOS software provide a full set of VPN tools, not only for just VPNs but for security, management, and all related needs.