1

Introduction

Enterprise Layer 3 (L3) network virtualization enables one physical network to support multiple L3 virtual private networks (L3VPNs). To a group of end users, it appears as if each L3VPN is connected to a dedicated network with its own routing information, quality of service (QoS) parameters, and security and access policies.

This functionality has numerous applications, including:

- Requirements to separate departments and functions within an organization for security or compliance with statutes such as the Sarbanes-Oxley Act or Health Insurance Portability and Accountability Act (HIPAA).
- Mergers and acquisitions in which consolidating disparate networks into one physical infrastructure that supports existing IP address spaces and policies provides economic benefits.
- Airports in which multiple airlines each require an independent network with unique policies, but the airport operator provides only one network infrastructure
- requirements to separate guest networks from internal corporate networks.

For each use case requiring network separation, a L3VPN infrastructure offers the following key benefits over non-virtualized infrastructures or separate physical networks:

- Reduced costs—Multiple user groups with virtual networks benefit from greater statistical multiplexing to provide bandwidth with higher utilization of expensive WAN links.
- A single network enables simpler management and operation of operations, administration, and management (OAM) protocols.
- Security between virtual networks is built in without needing complex access control lists (ACLs) to restrict access for each user group.
- Consolidating network resources into one higher-scale virtualized infrastructure enables more options for improved high availability (HA), including device clustering and multi-homing.