Multiprotocol Label Switching on Cisco Nexus 7000 Series Switches

Multi-Tenancy Challenges in the Data Center

Data centers are at the core of IT infrastructure for today's businesses. They consist of storage, compute and network infrastructure, servicing a variety of applications required by various departments in the organization. With server virtualization and the advent of cloud computing, data centers are undergoing fundamental change in the way they deliver services to the end user. Cloud-based service delivery models such as software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) are increasingly becoming popular, forcing data center architects to take a fresh look at multi-tenancy as a fundamental requirement in next-generation architectures. A major benefit of multi-tenancy is cost effectiveness, for both capital expenditures and operating efficiency, while delivering new services.

Multiprotocol Label Switching (MPLS) services, including Layer 3 VPNs, MPLS traffic engineering, multicast VPNs, and IPv6 Provider Edge (6PE) and IPv6 VPN Provider Edge (6VPE), on Cisco Nexus® 7000 Series Switches address these new requirements in the data center.

Benefits of Deploying MPLS in the Data Center

Main business benefits include:

- Faster introduction of new services
- Reduced operating costs through network consolidation and centralization of services and policy control for a securely segmented network fabric
- Facilitate the addition of new customers, mergers and acquisitions, and regulatory compliance to reach or expand into new markets
- Easy deployment of private and public cloud architectures
- Capability to maintain availability of business services

Main benefits for IT managers include:

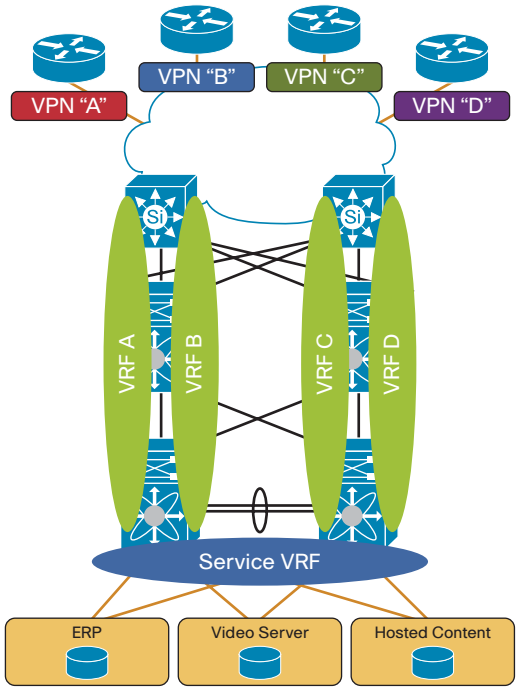
- Network consolidation: MPLS allows enterprises and service providers to deploy multiple services over the same network infrastructure, to increase efficiency and manageability.
- Cloud-ready architecture through secure segmentation: MPLS allows secure segmentation of customer and departmental traffic and enables regulatory compliance while providing security for customer traffic.
- Ease of provisioning and policy control: With a common management for the network infrastructure, administrators can centralize policy control over the network fabric for customers from a central control point and add customer VPNs in a relatively reduced footprint of network devices.
- Network efficiency and bandwidth on demand: Customers can increase the efficiency of the entire network fabric and provide bandwidth flexibility for applications and services on the basis of event-focused demand such as payroll applications and new product launches.

Main MPLS Features on the Cisco Nexus 7000 Series

Layer 3 VPNs

Depending on the industry, vertical, traffic, and customer segmentation is required to extend all the way to the aggregation layer. This need for segmentation may result from regulatory requirements (healthcare, financial, public sector, federal, etc. regulations) or other requirements (XaaS applications for business-to-business (B2B) and business-to-consumer (B2C) environments, etc.). VPNs, along with quality-of-service (QoS) configuration and MPLS Traffic Engineering fast reroute capability, provide traffic segmentation and engineering capabilities in data centers while maintaining Layer 3 convergence and availability over the same infrastructure. The common factor, among all categories, is the capability to segment the traffic and be operationally flexible to adapt to business events—mergers, acquisitions, new product launches, etc.—as well as to engineer the traffic to use the capacity fully without having to be burdened by the capital expenditures (CapEx) and operating expenses (OpEx) associated with growth in the data center (Figure 1).

Figure 1. Deploying shared services using MPLS Layer-3 VPNs



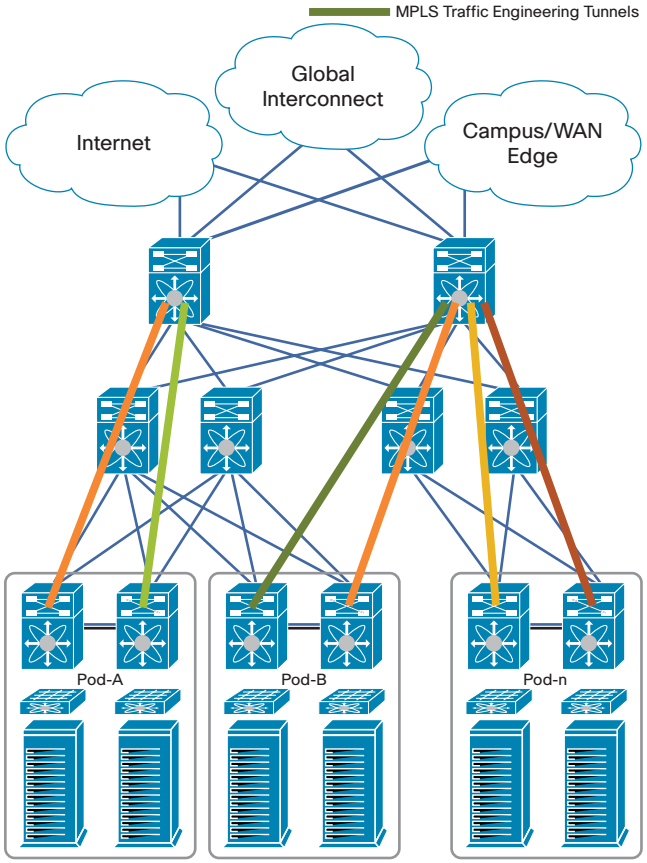
MPLS Traffic Engineering

The capability to respond to event-focused bandwidth demand has been a bottleneck in deploying new revenue-generating services, especially for cloud-based deployments. MPLS traffic engineering enables

Multiprotocol Label Switching on Cisco Nexus 7000 Series Switches

administrators to provide a comprehensive feature set to deploy application-aware paths with specific bandwidth requirements tied to each tunnel, link and node protection, 50-millisecond (ms) fast reroute capability, and efficient utilization of all the network paths (Figure 2).

Figure 2. Deploying highly available applications/services using MPLS Traffic Engineering



Multicast VPNs for IPv4

Video and mobile applications are proliferating over enterprise and hosted or cloud deployments. Multicast VPNs can be deployed along with Layer 3 VPNs to accommodate new applications like video conferencing, collaboration applications, push media, monitoring applications, multiuser domain gaming applications, etc.

6PE and 6VPE

With the exhaustion of IANA IPv4 address space (in February, 2011), enterprises and service providers must look at IPv6 for mandatory new network addressing policy as well as at providing IPv6-based services across the network end to end alongside existing IPv4 networks. This requirement for segmentation and consolidation will be carried over to the IPv6 networks. 6PE and 6VPE provide Layer 3 VPN equivalent functions, enabling the customer to connect IPv6 domains over MPLS networks.

MPLS QoS

The connection-oriented nature of the MPLS framework also provides for QoS features for service assurance for IP traffic. The capability to classify, mark, and police traffic can be applied to MPLS traffic. Differentiated services (DiffServ) models (pipe, short-pipe, and uniform modes) allow control of classification and remarking of traffic, which can be applied to applications that require tighter service-level agreement (SLA) controls.

MPLS High Availability

The Cisco Nexus 7000 Series provides an industry-leading implementation of In-Service Software Upgrade (ISSU), without degradation of performance. This innovation is extended to MPLS functions to provide high availability for MPLS protocols such as Multiprotocol Border Gateway Protocol (MP-BGP) and Label Distribution Protocol (LDP) as well as Resource Reservation Protocol (RSVP). Process restart, graceful restart for protocols, and ISSU are part of the high-availability framework for Layer 3 VPNs, MPLS traffic engineering, Multicast VPN for IPv4 (mVPNv4), and 6PE and 6VPE. In addition, MPLS traffic engineering fast reroute capability as well as Bidirectional Forwarding Detection (BFD)–assisted fast reroute restoration techniques are available as tools to make the network 99.999 percent available.

MPLS Management

The Cisco Nexus 7000 Series provides a comprehensive command-line interface (CLI) framework for ease of operations, in addition to Simple Network Management Protocol (SNMP) MIBs and XML and Network Configuration (NETCONF) protocol for management. MPLS operation, administration, and maintenance (OAM) tools include MIBs, label switched path (LSP) ping and traceroute, and MPLS tunnel ping and traceroute.

Why Cisco Nexus 7000 Series?

The Cisco Nexus Family of switches for data centers provides the network foundation needed to deliver on the Cisco® Data Center 3.0 vision. As Cisco's flagship switching platform, the Cisco Nexus 7000 Series offers innovative solutions to customer challenges with Layer 2 and 3 scalability and virtualization in the data center together with a broad range of services programs to accelerate deployment. It offers exceptional investment protection with the capability to evolve technology in a single chassis. Thousands of customers have deployed the Cisco Nexus 7000 Series as the network platform for their mission-critical data centers.

Why Cisco?

Cisco solutions offer customer success, delivered through a combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction.

For more information, visit:

http://www.cisco.com/go/nexus7000
http://www.cisco.com/go/nxos

C45-647153-00 03/11