Implementing Network Virtualization

5 Day Course
Locations: Mex, D.F.
Date:

Who Needs to Attend

Engineers responsible for designing, implementing, and troubleshooting Network virtualization processes and selection technology work together more efficiently to meet increased service levels.

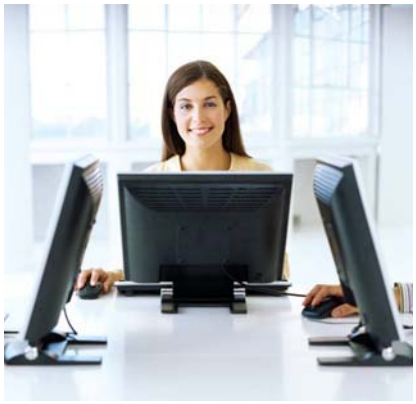
Audience Prerequisites

Experience with and ability to configure routers and LAN switches.

Network professionals with a good working knowledge of TCP/IP protocols.

Experience with basic ability to configure routers and LAN switches security features.

CCNA (recommended but not required).



Network Virtualization course provides design guidance for virtualized enterprise networks and arms network architects with the background necessary to make sound technological choices in the face of different business requirements. As a means of introduction, Network Virtualization lays out the fundamentals of enterprise network design.

Table of Contents

Chapter 1 Business Drivers Behind Enterprise
Network Virtualization
Why Virtualize?
Visitors, Partners, Contractors, and Quarantine Areas
Regulatory Compliance
Secure Service Areas
Network Consolidation
Acquisitions and Mergers
Multitenant Enterprises
Virtual Project Environment: Next-Generation Business Processes

Chapter 2 Designing Scalable Enterprise
Networks
Hierarchical Campus Design
Virtualizing the Campus
WAN Design
WAN Provider Service Offerings
WAN Architecture
WAN Resiliency
WAN Routing Considerations
Securing the WAN
WAN Virtualization

Chapter 3 Basic Virtualized Enterprise
The Virtual Enterprise
Transport Virtualization–VNs
VLANs and Scalability
Virtualizing the Routed Core
The LAN Edge: Authentication and Authorization
Central Services Access: Virtual Network Perimeter

Chapter 4 A Technologies Primer Virtualization:
Theory
Network Device Virtualization
Layer 2: VLANs
Layer 3: VRF Instances
Layer 2 Again: VFIs
Virtual Firewall Contexts
Data-Path Virtualization
Layer 2: 802.1q Trunking
Generic Routing Encapsulation
IPsec
L2TPv3
Label Switched Paths
Data-Path Virtualization Summary
Control-Plane Virtualization–Routing Protocols
VRF-Aware Routing
Multi-Topology Routing

Chapter 5 Infrastructure Segmentation
Architectures: Theory
Hop to Hop
Layer 3 H2H
Single Address Space Alternatives
H2H Summary
Tunnel Overlay for L3VPN
L3VPN Using GRE and IPsec Overlay
Putting It All Together: DMVPN
Tunnel Overlay for Layer 2 VPNs
Layer 2 P2P Overlay Using L2TPv3
Layer 2 P2P Overlay Using MPLS
Layer 2 VPN MP2MP Using MPLS (VPLS)
Peer-Based Model for Layer 3 VPNs
RFC 2547bis the MPLS Way
RFC 2547bis Forwarding-Plane Alternatives
Inter-Autonomous System Connectivity Carrier
Inter-Autonomous System Routing

Implementing Network Virtualization

Why virtualization?

Through virtualization, people, processes and technology work together more efficiently to meet increased service levels.

Virtualization approach and capabilities can help you achieve substantial, long-term benefits from virtualization, including reduced costs, increased agility, and greater energy efficiency.

Chapter 6 Infrastructure Segmentation
Architectures: Practice
Hop-to-Hop VLANs
Layer 3 Hop to Hop
Single Address Space Solutions
Tunnel Overlay for Layer 3 VPNs
GRE Tunnels
Multipoint GRE Tunnels
Mapping Traffic to Tunnels
Resiliency and Routing Considerations
Encryption Considerations
Layer 3 VPNs
RFC 2547bis the MPLS Way
RFC 2547bis over L2TPv3
RFC 2547bis over GRE
IGP Best Practices
BGP Best Practices: Route Reflectors
Layer 2 VPNs
Ethernet over MPLS

Chapter 7 Extending the Virtualized Enterprise over the WAN
WAN Services
IP Services
Layer 2 Circuits
P2P GRE
Multipoint GRE
Dynamic Multipoint VPN
Extending Segmentation over the WAN
MPLS over Layer 2 Circuits
VRF-to-VRF Connections at the Autonomous System Border Routers
MP-eBGP Exchange of Labeled VPN-IPv4 Routes Between Adjacent ASBRs
Multihop MP-eBGP Between Remote Autonomous Systems
Using MPLS over Layer 2 Circuits for Segmented Branch Aggregation
Benefits and Drawbacks
Contracting Multiple IP VPNs
Using CsC for Segmented Branch Aggregation
Benefits and Drawbacks
MPLS over GRE
Benefits and Drawbacks
RFC 2547 VPNs over L2TPv3 Tunnels
Benefits and Drawbacks
VRFs Interconnected by a GRE or DMVPN
Benefits and Drawbacks
RFC 2547 VPNs over DMVPN

Chapter 9 Multicast in a Virtualized Environment
Multicast Introduction
Internet Group Management Protocol (IGMP)
Multicast Routing
Protocol Independent Multicast (PIM)
VRFs and Multicast
Multicast Sourced from an External IP Network
Multicast Across VRFs (mVPN Extranet)
mVPN Transport
Global
Tunnel Overlay
mVPN
Connecting the WAN

Chapter 10 Quality of Service in a Virtualized Environment
QoS Models and Mechanisms: A Review
Differentiated Services
MPLS Quality of Service
Tunnels and Pipes
MPLS Traffic Engineering and Guaranteed Bandwidth
DS-TE and Guaranteed Bandwidth
Do I Really Need This in an Enterprise Network?
QoS Models for Virtualized Networks
One Policy per Group

Chapter 11 The Virtualized Access Layer
Access Layer Switching
Implementing Dynamic Authentication and Authorization
Clientless Authentication
Client-Based Layer 2
Virtualizing the Access Layer
Layer 3 Access