



Q&A

Cisco Network Virtualization

Q. What is network virtualization?

A. Cisco Network Virtualization is the efficient utilization of network resources through logical segmentation of a single physical network. An example of multiple logical networks over a common infrastructure could be different organizational units or departments on a single companywide network. Alternatively, it could be an enterprise customer wanting to differentiate between an employee and vendor and to which resources each has access in the network. Cisco Network Virtualization also fits into the Cisco® Service Oriented Network Architecture (SONA).

Q. How does Cisco Systems® deliver network virtualization services?

A. Cisco has created technologies and products and has produced architecture and design guides to help enterprises implement Cisco Network Virtualization in their campus.

Q. What is the reason for implementing Cisco Network Virtualization?

A. The need for Cisco Network Virtualization comes from multiple factors: regulatory compliance (for example, Sarbanes-Oxley [SOX] and the Health Insurance Portability and Accountability Act of 1996 [HIPAA]), outsourcing, network consolidation because of mergers and acquisitions, and so on. The goal is to reduce total cost of ownership (TCO) by sharing network resources while still maintaining secure separation between organizations, groups, or individuals. Operating multiple physical networks is more expensive in terms of both capital expenditures and operating expenses.

Q. To which areas of the network does infrastructure virtualization apply?

A. Cisco Network Virtualization is applicable to all the primary parts of the network, including the campus, branch, data center, and WAN. These solutions specifically address virtualization in the campus (or enterprise).

Q. Which verticals can benefit from Cisco Network Virtualization?

A. Many verticals can benefit. Some examples include:

- Automotive
- Healthcare
- Financial institutions
- Higher education
- Retail
- Multitenant units

WHAT'S NEW: TECHNOLOGIES

Q. How can customers evolve their architecture to make greater use of Cisco Network Virtualization and SONA?

A. SONA, which includes Cisco Network Virtualization, encompasses both a vision for the evolution of enterprise IT and a pathway to get there. This path is unique for each customer. It is important that the Cisco sales and services teams work closely with each customer to help that customer evolve its architecture, using important capabilities described in the SONA framework in a way and timeframe that best meets the customer's objectives and requirements.

Q. What technologies are involved in delivering Cisco Network Virtualization?

A. Cisco provides several solutions that preserve the benefits of today’s campus design while introducing the capability of segmenting the network into secure virtual networks by overlaying VPN mechanisms onto the existing LAN. These include 802.1x, Network Admission Control (NAC), generic routing encapsulation (GRE) tunnels, virtual routing and forwarding (VRF)-lite, and Multiprotocol Label Switching (MPLS) VPNs. These solutions can address the problems associated with deploying services and security policies in a distributed manner. Whatever their size or security needs, enterprises today can enjoy the benefits of a virtualized campus network with many closed user groups, all on a single physical network.

Q. Which LAN switching platforms support Cisco Network Virtualization solutions?

A. The Cisco Catalyst® 3560, 3750, 4500, and 6500 Series Switches can be used to implement infrastructure virtualization solutions in the enterprise. Table 1 lists platform coverage at a high level.

Table 1. Platform Coverage

Platform	GRE (Hardware)	VRF-lite	MPLS VPN	Multicast Support (for GRE, VRF-lite, and MPLS VPN)
Cisco Catalyst 6500 Series Supervisor Engine 720 and Cisco Catalyst 6500 Supervisor Engine 32	Yes	Yes	Yes	Yes
Cisco Catalyst 4500 Series Supervisor Engine II-Plus, Cisco Catalyst 4000/4500 Supervisor Engine III, Cisco Catalyst 4000/4500 Supervisor Engine IV, and Cisco Catalyst 4000/4500 Supervisor Engine V	No	Yes	No	No
Cisco Catalyst 3550, 3560, and 3750 Series Switches	No	Yes	No	No

Q. What are the benefits of the technologies available to implement path isolation?

A. The primary technologies involved in delivering path isolation in the campus are GRE, VRF-lite, and MPLS.

GRE tunnels represent a fairly simple approach to creating a small number of closed user groups on the campus network. A frequent requirement for corporate IT departments is to provide access to the global Internet for onsite guests or visitors, but to prevent those users from accessing internal sites and resources. Often, the simplest solution is to extend a single “guest” VLAN across a large part of the network. Used in combination with the Cisco VRF-lite feature, GRE tunnels can create a simple, easy-to-administer solution for guest access in any Layer 3 network where Cisco Catalyst 6500 Series Switches and the Cisco Catalyst 6500 Series Supervisor Engine 720 or Cisco Catalyst 6500 Supervisor Engine 32 is deployed. Rather than extending a VLAN across the network to provide guest access, guest traffic is instead isolated to a unique VRF at each distribution layer switch. The traffic is then transported across the corporate LAN through the GRE tunnel to a central device, such as an Internet edge switch. The advantages to this solution include:

- Guest VLANs are prevented from spanning across the corporate switched network (Spanning Tree Protocol domain is not extended over the campus).
- Guest user traffic is isolated from the rest of the corporate LAN traffic.
- The point of ingress for all guest traffic is centralized, making security and quality-of-service (QoS) policies easier to administer.

VRF-lite, a Cisco feature also known as multi-VRF customer edge, provides a solution for campus segmentation by enabling a single routing device to support multiple virtual routers. Each logical router contains its own set of interfaces as well as a routing table and a forwarding table. VRF-lite enables support for scenarios where IP addresses can be overlapped among the VPNs. Each VRF maintains an independent routing domain. This characteristic provides the flexibility of using any IP address space for any given VPN, regardless of whether it overlaps or conflicts with the address spaces of other VPNs. Therefore, each group can independently use private IP addressing, as defined in RFC 1918. In this scenario, Network Address Translation (NAT) is not required. This addressing flexibility is beneficial in



many scenarios. For example, when the networks of acquired companies are merged into a shared LAN, the acquired network can be incorporated into the infrastructure as a separate VPN. In this way, the acquired company's network can preserve its original address space without conflicting with other VPNs. Likewise, this flexibility is beneficial to enterprises that host engineering or development groups, which often need manage their own address space independently.

Another way to segment a campus network for closed user groups is by overlaying MPLS-based, Layer 3 VPNs onto the routed infrastructure of the campus LAN. Like GRE tunnels and VRF-lite, MPLS VPNs provide a secure and dependable way to form logically separated networks on a common physical infrastructure. In MPLS, closed user groups are established through VPNs that are transported independently over the core of the network using labels. The networkwide benefit of this approach is that any VPN can be configured to connect users and resources at any location in the network, without any compromises in performance or network design. Accordingly, MPLS VPNs are the most scalable of the three solutions for Cisco Network Virtualization discussed in this document.

Q. Why is Cisco different?

A. Cisco differentiates itself from most other vendors by adopting a systems-level approach that integrates services throughout the infrastructure. Looking at the Cisco Catalyst switching portfolio, it becomes apparent that a wide range of Layer 3 switches support network virtualization. Other vendors have point solutions that are only applicable for limited areas within the campus network. Cisco Network Virtualization is a primary component of the Cisco SONA framework.

FOR MORE INFORMATION

For more information about Cisco Network Virtualization, visit http://cisco.com/en/US/netsol/ns658/networking_solutions_package.html or contact your local account representative.



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

Printed in USA

C67-350959-00 05/06