Solution Overview

# Network Virtualization for the Campus

**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.**


## SUMMARY

As the demands placed on campus networks have grown in complexity, so has the need for scalable solutions to separate groups of network users and resources into logical partitions. Virtualization of the network provides multiple solutions for centralizing services and security policies while preserving the high-availability, manageability, security, and scalability benefits of the existing campus design. To be effective, these solutions must address the three primary aspects of network virtualization: access control, path isolation, and services edge. Implementing these solutions enables network virtualization to coalesce with the Cisco Systems® Service-Oriented Network Architecture (SONA), creating a solid framework for enterprises to migrate to an Intelligent Information Network.

Utilizing NAC and the IEEE 802.1x protocol, a SONA network delivers identity services, which provide optimal access control. After users gain access to the network, three solutions for path isolation—generic route encapsulation (GRE) tunnels, Virtual Route Forwarding (VRF)-lite, and Multiprotocol Label Switching (MPLS) VPNs—preserve the benefits of today's campus design while introducing the capability of separating the network into secure, virtual networks by overlaying partitioning mechanisms onto the existing LAN. These solutions address the problems associated with deploying services and security policies in a distributed manner. Finally, the centralization of shared services and security policy enforcement dramatically reduces the capital and operational expenses of maintaining different groups' security policies and services within a campus. This centralization also enables consistent policy enforcement throughout the campus.


## CHALLENGE

Design recommendations for campus networks have lacked an elegant way of partitioning network traffic to provide secure, independent environments for closed user groups (Table 1). A number of factors promote the need to create closed user groups, including the following examples:

- **Varying levels of access privileges within an enterprise:** Almost every enterprise needs solutions for granting different levels of access to customers, vendors, and partners as well as employees on the campus LAN.
- **Regulatory compliance:** Some businesses are required by laws or rules to separate segments of a larger organization. For example, in a financial company, banking needs to remain separate from trading.
- **Network simplification for very large enterprises:** In the case of very large campus networks such as airports, hospitals, or universities, the need for security between different groups or departments has in the past required the building and management of separate physical networks, an undertaking that is costly and difficult to manage.
- **Network consolidation:** In mergers and acquisitions, there is often a need to integrate the acquired company's network expeditiously.
- **Outsourcing:** As outsourcing and offshoring proliferate, subcontractors must demonstrate absolute isolation of information between clients. This is especially critical when a contractor services competing companies.
- **Enterprises providing network services:** Retail chains support kiosks for other companies or Internet access for patrons; similarly, airports serving multiple airlines and retailers can use a single network for both isolated and shared services.

**Table 1.** Application Examples of Network Segmentation in Individual Verticals

| Vertical | Examples of Cases for Network Virtualization |
|---|---|
| **Manufacturing** | Production plants (robots, automation of production environment, and so on), administration, sales, video surveillance. |
| **Finance** | Trading floors, administration, mergers. |
| **Government** | Shared buildings and facilities supporting different departments. In some countries the law mandates separate networks between such departments. |
| **Healthcare** | General trend toward hotel service with medical treatment. Separation among medical staff, magnetic resonance imaging (MRI) and other technical equipment, Internet access for patients, media services such as radio and television for patients. |
| **Commercial Real Estate: Multibusiness Campus** | Some resources are shared among groups. Multiple companies on the same campus where different buildings belong to different groups, but all rely on the same core and Internet access. Building automation is administered by the owner and spans across all buildings. |
| **Retail** | Kiosks, public wireless LAN (PWLAN) in branches, RF identification, WLAN devices (for example, older WLAN barcode readers that do not support any WLAN security). |
| **Education** | Separation among students, professors, administrators, and external research groups. Alternatively, individual departments that spread across multiple buildings might require access to their respective server areas. Some resources (Internet, e-mail, and news, for example) might be shared or accessed through a services zone. Building automation, too, must be separated. |

### Campus LAN Evolution

Network virtualization—giving multiple groups access to the same physical network while keeping them logically separate to a degree that they have no visibility into other groups—is a requirement that has challenged network managers for many years. In the 1990s, Layer 2 switching was the defining characteristic of campus LANs, and virtual LANs (VLANs) were the standard for dividing the LAN into separate workgroups within a common infrastructure. The solution was effective and secure, but it did not scale well, nor was it easy to manage as these campus LANs grew.

The introduction of Layer 3 switching in the core and distribution layers helped reduce the scalability, performance, and troubleshooting drawbacks associated with the VLAN-based approach. Layer 3–based campus networks built over the past several years have proven to be scalable and robust and offer high performance. But when it comes to network partitioning and closed user groups, the Layer 3 campus approach has fundamental flaws, and the workarounds have significant limitations. Adding closed user groups in this scenario has meant adding cost and complexity.

## THE SOLUTION: NETWORK VIRTUALIZATION

A scalable solution is needed for keeping groups of users totally separate and centralizing services and security policies while preserving the high-availability, security, and scalability benefits of the campus design. To address this solution, the network design needs to effectively solve the following challenges:

- **Access control:** Help ensure legitimate users and devices are recognized, classified, and authorized entry to their assigned portions of the network.
- **Path isolation:** Help ensure that the substantiated user or device is mapped to the correct secure set of available resources—effectively, the right VPN.
- **Services edge:** Help ensure that the right services are accessible to the legitimate set or sets of users and devices, with centralized policy enforcement.

The Cisco® solution calls for network virtualization, which can be achieved in several ways. Virtualization technologies enable a single physical device or resource to act like it is multiple physical versions of itself and be shared across the network. Network virtualization is a crucial element of the Cisco SONA framework. Cisco SONA uses virtualization technologies to increase use of networked assets such as servers and storage-area networks (SANs). For example, one physical firewall can be configured to perform as multiple virtual firewalls, helping enterprises optimize resources and security investments. Other virtualization strategies include centralized policy management, load balancing, and dynamic allocation. Virtualization enhances agility and improves network efficiency, reducing both capital and operational expenses.

### Access Control: Authentication and Access-Layer Security

Security at the access layer is vital for protecting the campus LAN from external threats. Cisco network virtualization solutions are complemented by features that mitigate threats before they can enter the campus. One such technology is IEEE 802.1X, which is the standard for port authentication. 802.1X forms a solid linkage between users and their associated VPNs, preventing unauthorized straying into off-limits resources. Another complementary technology is Cisco Network Admission Control (NAC). NAC's job is to mitigate threats at the edge and remove harmful traffic before it reaches the distribution or core layers. NAC helps ensure that users do not expose the campus infrastructure to any viruses, worms, or other threats.

### Path Isolation: Layer 3 VPNs

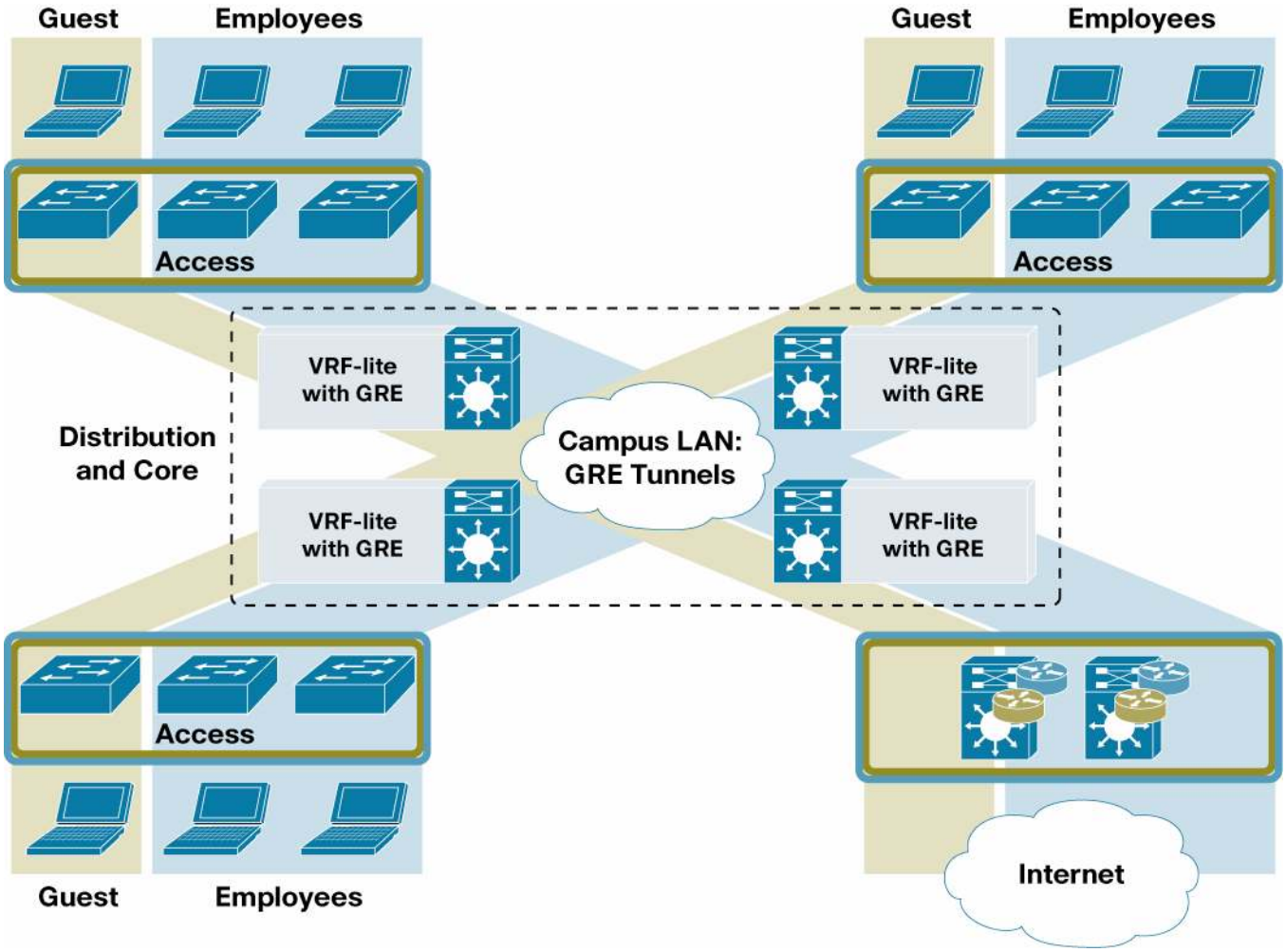
To address network virtualization for the campus, Cisco offers three solutions that are well suited to typical campus network designs and use a mix of Layer 2 and Layer 3 technologies:

- GRE tunnels
- VRF-lite
- MPLS VPNs

#### GRE Tunnels

GRE tunnels present a fairly simple but effective approach to creating closed user groups on the campus network. GRE tunnels are ideally suited as an enterprise solution for hosting "guest" access, wherein companies can provide access to the global Internet for onsite guests or visitors, while preventing those users from accessing internal resources. In Figure 1, GRE tunnels are used in combination with the Cisco VRF-lite feature to create a simple, easy-to-administer solution for guest access.

**Figure 1.** GRE Tunnels Used with VRF-lite




Rather than extending a VLAN across the network to provide guest access, guest traffic is 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 router.

The advantages to this solution include:

- Can span over a typical multilayer campus network (no need for campuswide VLANs).
- 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.
- Can even be extended over the WAN to branches.

One consideration regarding GRE tunnels as a solution for closed user groups is that the tunnels themselves are intense to configure and manage, for which reason the solution is not advisable for more than one or two tunnels. This type of network virtualization is suitable where hub-and-spoke topologies are required.

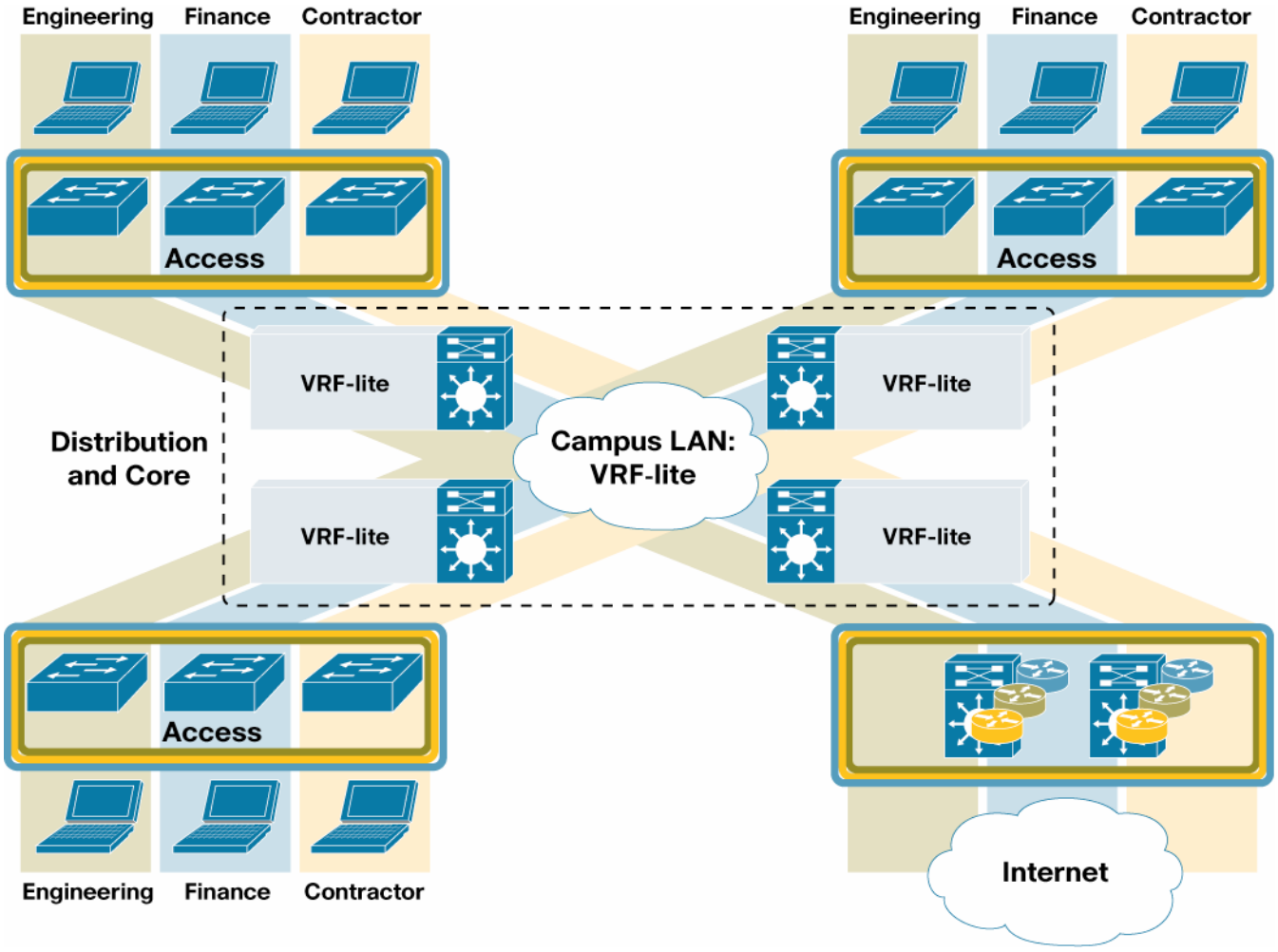
## VRF-lite

VRF-lite, a Cisco feature that also goes by the generic name of Multi-VRF Customer Edge, provides a solution for campus separation by enabling a single routing device to support multiple virtual routers. VRF-lite is effectively a lightweight version of MPLS.

With VRF-lite, network managers enjoy the flexibility of using any IP address space for any given VPN, regardless of whether it overlaps or conflicts with other VPNs' address space. This 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, with little or no interruption to regular business processes on the network.

VRF-lite can be used as an end-to-end solution, as shown in Figure 2, or in conjunction with another solution for closed user groups, as discussed in the next section. In general, VRF-lite is a more scalable solution than GRE tunnels, but it is best suited for networks with four or five segments. It requires manual reconfiguration for every addition, which makes it fairly labor-intensive as a solution.

**Figure 2.** VRF as an End-to-End Solution



## MPLS VPNs

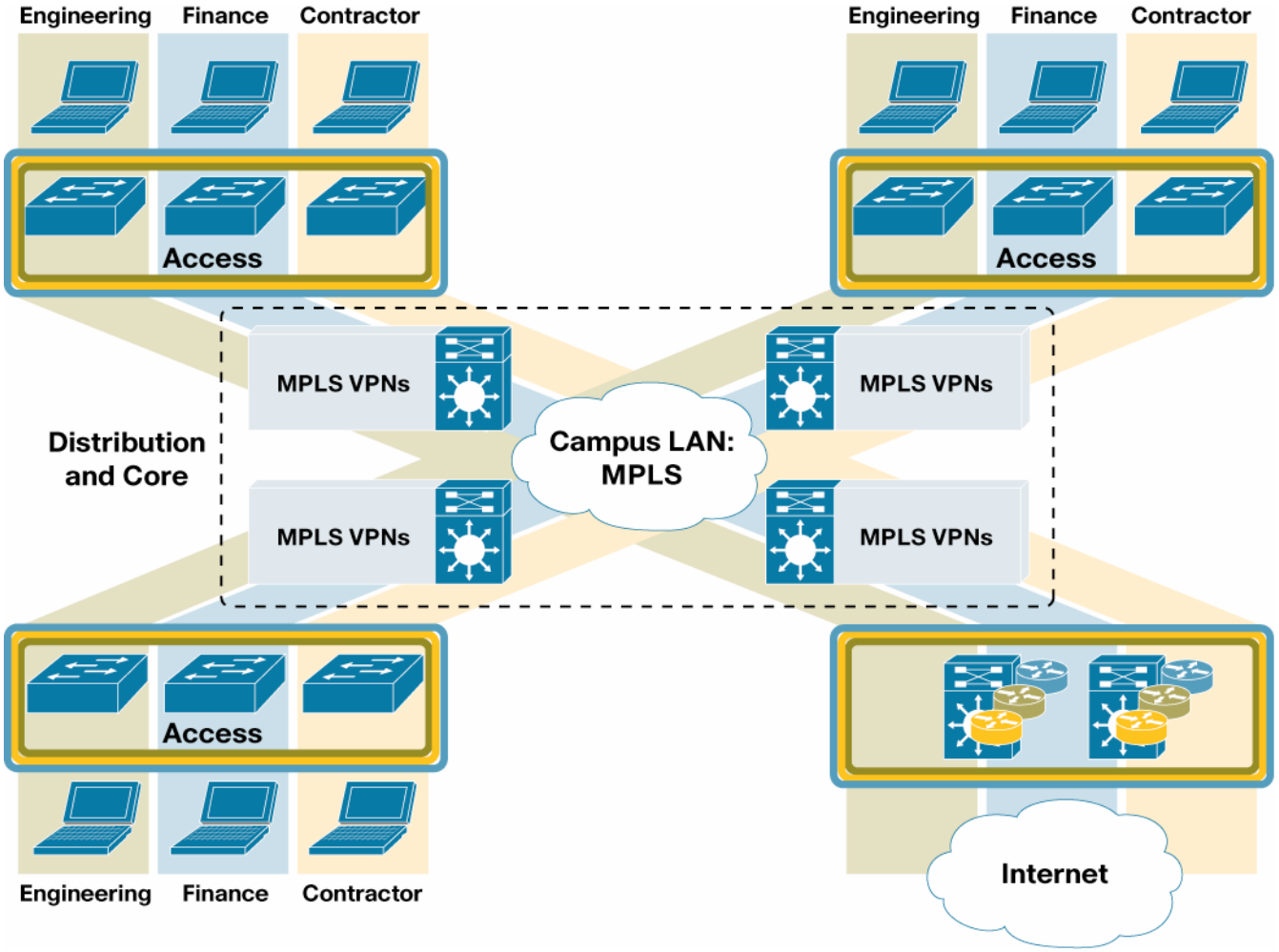
Another way to partition a campus network for closed user groups is MPLS-based Layer 3 VPNs. Like GRE tunnels and VRF-lite, MPLS VPNs provide a secure and dependable way to form logically separated networks on a common physical infrastructure.

Although service providers have made use of MPLS technology for several years, it has not been widely deployed in enterprise networks because of the lack of support for MPLS on LAN switches. But changing business requirements and, in response, new product availability are helping MPLS emerge as a vital technology in the campus infrastructure. With the introduction of MPLS VPN support on the Cisco Catalyst® 6500 Series, MPLS technology became available at an affordable price point for many large enterprises.

MPLS VPNs offer all the benefits of the other solutions discussed in this document (Figure 3). In addition, any MPLS VPN can be configured to connect users and resources at any location in the network, without performance or network design compromises. Accordingly, MPLS VPNs are the most scalable of the three Cisco solutions for network infrastructure virtualization. No manual reconfiguration is needed when groups are added or changed, another factor that adds to its scalable nature and helps keep operating expenses low.

When VLANs are used at the network edge and Layer 3 VPNs in the routed portion of the campus, all the benefits of a hierarchical campus deployment are preserved, while the solution achieves end-to-end scalable segmentation and centralized security and services in the campus LAN. Flexibility of network addressing is another benefit of MPLS VPNs, as with VRF-lite.

**Figure 3.** MPLS VPNs for Any-to-Any Connectivity




### Unified Access for Flexibility

The three Cisco solutions for network virtualization in the campus do not limit users to any specific type of access. Although they work within a single physical network infrastructure, these solutions can easily accommodate mobile users. Whether the solution in use is based on GRE tunnels, VRF-lite, or MPLS VPNs, users can be tied transparently to their closed user groups from wherever they have network access.

### Virtualized Services

Virtualized network services, a crucial element of Cisco network infrastructure virtualization solutions and SONA, can help enterprises achieve efficiencies that can reduce the number of devices required on their networks. Cisco solutions for network virtualization enable centralized services, including:

- Centralized appliances, such as firewalls and intrusion detection systems (IDSs)
- Security policy enforcement
- Traffic monitoring, accounting, and billing
- Shared Internet and WAN access
- Shared data centers

This centralization greatly simplifies and strengthens security enforcement. By helping ensure a single point of access for each VPN, centralized appliances for firewalling and intrusion detection can be shared by many VPNs. A wealth of other services that are common to the different VPNs can also be shared, and doing so can significantly reduce the capital and operational expenses of providing these services.

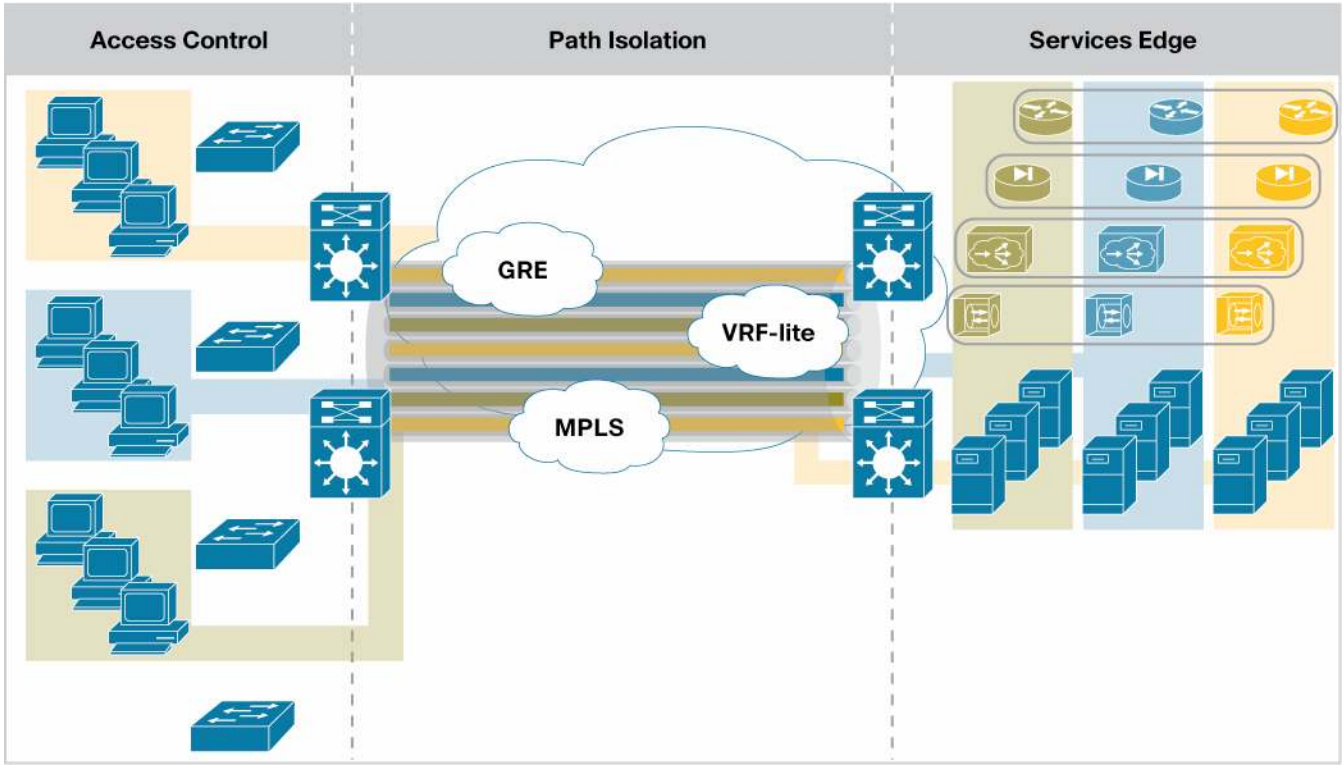
VPNs enable the centralization of security capabilities, which is important, because the enforcement of security policies at a central location simplifies management and lowers operational overhead. It also allows the sharing of security appliances, such as the Cisco Firewall Service Module for Cisco Catalyst 6500 Series Switches, which is VPN-aware and can provide hundreds of virtual firewalls concurrently on a single appliance. With VPN-aware virtual firewalls, each group can enforce its own policies on individual virtual firewalls, while the enterprise owns and maintains a single firewall appliance—lowering total cost of ownership.

## CONCLUSION

In today's evolved networking environments, typical campus network designs use a mix of switching (Layer 2) technologies at the network edge (access) and routing (Layer 3) technologies at the network core (distribution and core layers). Thus, network virtualization can be achieved at the network access layer (Layer 2) by means of VLANs and at the network core (Layer 3) by using GRE tunnels, VRF-lite, and MPLS-based Layer 3 VPNs to partition the routed domain and thus achieve scalable end-to-end virtualization.

With Cisco network virtualization solutions for the campus (Figure 4), enterprises can deploy multiple closed user groups on a single physical infrastructure, while maintaining high standards of security, scalability, manageability, and availability throughout the campus LAN. In light of their virtualized nature and their enablement of centralized services, these solutions form a crucial element of the Cisco SONA framework. A wide range of Cisco Catalyst switches enable enterprises that adopt this framework to use more of their network assets with greater efficiency, allowing them to realize cost savings even as requirements for devices, systems, services, and applications grow.

**Figure 4.** Complete Network Virtualization Solution




**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 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




Printed in the USA C22-347068-00 04/06