



# Comparing Campus and Data Center Switches

## Requirements for Campus and Data Center Switches

Campus and data center switching networks differ in their requirements. An understanding of the two deployments and the specific requirements of each is imperative to choose the right Cisco switch. Each deployment type requires that switches have certain unique features. Table 1 compares the top five requirements for campus and data center switches.

**Table 1.** Top Requirements for Campus and Data Center Switches

Campus Requirements Met by Cisco Catalyst® Family and Cisco IOS® Software	Data Center Requirements Met by Cisco Nexus® Family and Cisco® NX-OS Software
User access control and segmentation	Cloud security and virtual machine awareness
Video intelligence	Virtual machine mobility
Wired and wireless convergence	LAN and SAN convergence
Application visibility	Fabric scalability and resilience
Power over Ethernet (PoE)	Data center consolidation

The rest of this document discusses these features.

## Campus

### User Access Control and Segmentation

A campus or branch office is where users connect to network wired or wirelessly, and every connection point is vulnerable to security breaches. Capabilities to allow access based on business policy, prevent users from interfering with other users and their resources, isolate infected and malicious devices and applications, and track users in the network are crucial features of a campus

switch. Cisco Catalyst switches support IEEE 802.1x and security group tags (SGTs), which automate authentication and network segmentation for user groups and provide access based on user roles. The switches, in conjunction with Cisco Prime™ applications, can help administrators track and monitor every user. Additionally, Cisco Catalyst 6500 Series Switches support Easy Virtual Network (EVN), which simplifies deployment of technologies such as Multiprotocol Label Switching (MPLS), generic routing encapsulation (GRE), and Virtual Routing and Forwarding (VRF)-Lite to segment users and groups in the network.

### Video Intelligence

Globally, business web-based video conferencing traffic is forecasted to grow six fold from 2011 to 2016, a compounded aggregate growth rate (CAGR) of 45 percent<sup>1</sup>. Devices, such as computers, smartphones, cameras, and dedicated Telepresence units, used to send and receive video are proliferating. Helping ensure a consistent experience and the capability to troubleshoot problems are critical in all these scenarios, and the network plays a major role. Cisco Catalyst switches have Medianet features that enable lifecycle video solutions to assess network readiness for video with built-in IP service-level agreement (SLA) tools, automated troubleshooting, and per-flow and per-hop flow metrics to measure such factors as packet loss and network jitter.

### Wired and Wireless Convergence

Controllers to manage wireless access points are ubiquitous in campus and branch-office networks. These controllers can be a physical or virtual appliance or integrated into a LAN switch. The Cisco Catalyst 6500 Series supports the integrated Cisco Wireless Services Module 2 (WISM2). Cisco also has standalone wireless controllers that work in conjunction with the Cisco Catalyst switches.

### Application Visibility

The rising number of different applications places a huge burden on the network. Congestion and outages can occur, and network administrators need an accurate way to track the application traffic flowing through the network to troubleshoot and correct the situation. Cisco Catalyst switches provide Cisco Flexible NetFlow, Network Analysis Modules (NAMs), and Network-Based Application Recognition (NBAR), which comprehensively scan the traffic and offer reports based on protocols, applications, and users.

### Power over Ethernet

PoE is a technology through which power can be delivered to end devices such as IP phones and access points from a connected LAN switch through the LAN cable. Power consumption can also be managed from a central location, which helps conserve energy and reduce costs. Cisco Catalyst switches support PoE, Enhanced PoE (PoE+), and Cisco Universal PoE (Cisco UPOE™), which deliver 15 to 60 watts (W) per port. Cisco EnergyWise™ technology can be used to manage energy consumption of many end devices connected to the switches.

## Data Center

### Cloud Security and Virtual Machine Awareness

As the number of virtual machines increases, so do the challenges of configuring, administering, and troubleshooting the networks that connect them. Because today's networks have both physical and virtual servers on them, visibility and awareness into both environments is critical. Network policies, dictating everything from quality-of-service (QoS) parameters to access control lists (ACLs), define the way that clients and servers, as well as their traffic, is supposed to behave on the network. Historically, these policies were applied to physical switch ports with physical servers connected to them.

1. Cisco VNI Global IP Traffic Forecast, May 2012, at [http://www.cisco.com/web/solutions/sp/vni/vni\\_forecast\\_highlights/index.html](http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html)



As virtual servers move to different servers, on different switches, perhaps in different data centers, deploying and enforcing these policies becomes much more challenging. These challenges spill over into other areas, such as troubleshooting. The Cisco Nexus 1000V Series Switches provide the solution to these problems by providing visibility into the virtual machine environment while extending the features and functions of the Cisco Nexus portfolio. The Cisco Virtual Security Gateway (VSG) and Cisco Adaptive Security Appliance (ASA) for Nexus 1000V Series Switch work with the Cisco Nexus 1000V Series to provide security capabilities such as firewalls, intrusion protection systems (IPS), and VPN. These capabilities can be used for multitenant solutions, thus providing cloud environments with the tools they need to operate securely.

#### Virtual Machine Mobility

**Not only does** the network need awareness of virtual machines; the network needs to enable the movement of virtual machines: between servers, racks, or entire data centers. Virtual machines may need to be moved for several reasons, including providing business continuity, resilience, and workload balancing. The techniques for moving workloads typically do not traverse Layer 3 boundaries: that is, they require Layer 2 adjacency. The challenge with Layer 2 is that it typically requires Spanning Tree Protocol, which often implies stability issues as the environment scales. Features such as Overlay Transport Virtualization (OTV) and Locator/ID Separation Protocol (LISP) effectively address these issues by extending the Layer 2 domain in a way that is scalable and stable and does not rely on spanning tree. Thus, virtual machines can move transparently across data centers, and the environment will remain stable as it scales.

#### LAN and SAN Convergence

Traditional data centers often have separate LAN and SAN infrastructures. However with the evolution of virtualization, the challenges of shrinking data centers, and the additional costs of managing two separate networks,

this model is evolving to a consolidated, single, networking platform. The Cisco Nexus Family of data center switches allows customers to build an infrastructure that allows them to decrease their total cost of ownership (TCO) through the simplification of data center architecture. Through the convergence of the LAN and storage networks, the Cisco Nexus portfolio delivers a high-performance, highly scalable, lossless solution that can carry Ethernet, Fiber Channel, Fiber Channel over Ethernet (FCoE), Small Computer System Interface over IP (iSCSI), and network-attached storage (NAS) traffic. This solution allows reduction in the number of devices managed and maintained, reduced cabling requirements, and more efficient resource utilization, leading to lower power and cooling costs.

#### Fabric Scale and Resilience

To build an agile, highly available infrastructure that delivers both reduced TCO and a solution that can adapt to future needs, you must be able to scale the data center performance and port bandwidth while reducing costs and complexity and to create an architecture that can withstand planned and unplanned downtime. The Cisco Nexus portfolio offers multidimensional scalability for the data center network in switch performance, system scalability, and geographic span, allowing your data center to support more servers and more applications when you need them. Through support for high-density 1, 10, 40, and 100 Gigabit Ethernet connectivity that can be deployed at the aggregation layer, core, top of the rack, middle of the rack, or end of the row and as an embedded virtual switch integrated into your server hypervisor, this highly flexible portfolio enables customers to create the right architecture with the right types of connectivity speeds that they need today, with a solution that can address evolving needs.

When customers couple scalability technologies such as Cisco FabricPath with Cisco Nexus hardware architecture redundancy, Cisco NX-OS process modularity, hitless

In-Service Software Upgrade (ISSU), and self-healing capabilities, customers can take full advantage of a highly available architecture with no service disruption, allowing them to quickly integrate new features, enhancements, and problem fixes, providing a solution that makes zero-impact operations a reality.

#### Data Center Consolidation

The data center is the heart of a business; any downtime (planned or unplanned) can severely affect profitability. Beyond network-based availability, the combination of Cisco Nexus hardware architecture redundancy and Cisco NX-OS process modularity and self-healing capabilities, you can take full advantage of a highly available architecture with no service disruption. Through the solution's capability to help ensure continuous uptime for planned and unplanned maintenance, upgrades, and software certification, and through technologies such as Cisco's ISSU capabilities, you can quickly integrate new features, enhancements, and problem fixes, providing a solution that makes zero-impact operations a reality.

#### Common Features

The campus and data center also require features that are common to both of them, such as simplified management, programmability, high-availability, and Cisco TrustSec® capabilities.

When choosing a Cisco switch for the campus or data center, choose the switch based on the features discussed in this document to gain the greatest benefit and lowest TCO.

#### For More Information

[www.cisco.com/go/switching](http://www.cisco.com/go/switching)