Borderless Network Access

The workspace is changing. It is no longer about working just in our offices or even confined to the country in which we work.

Borderless Networks, a Cisco® next-generation architecture for agile delivery of services and applications, delivers a new workspace experience, connecting anyone, anywhere, using any device, to any resource: securely, reliably, and seamlessly. The Cisco Borderless Networks architecture addresses primary IT and business challenges to help create a truly borderless experience by bringing interactions closer to the employee and customer.

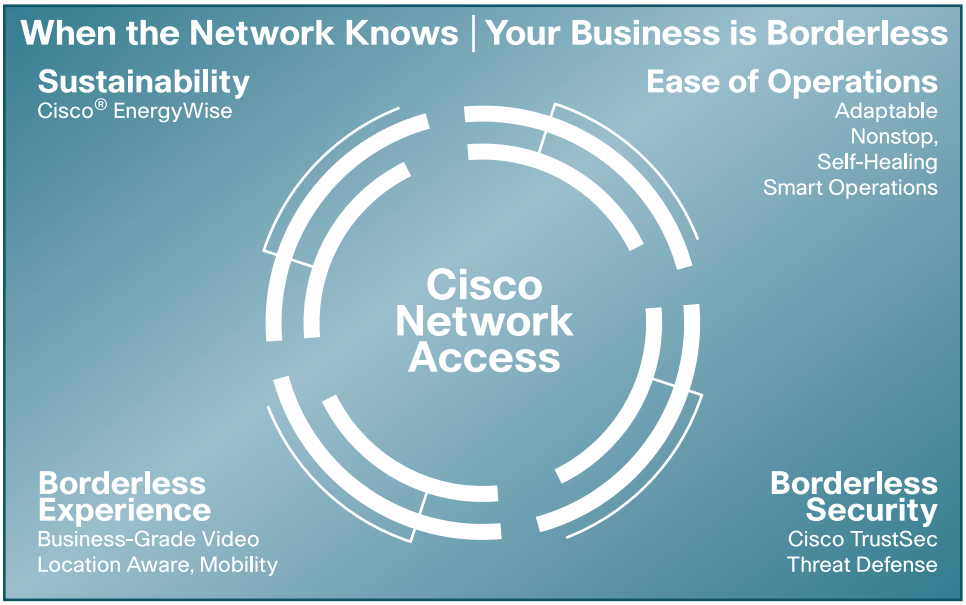
Borderless experience is only possible with intelligent network elements designed to meet the needs of a global workspace with an increasingly mobile workforce. Cisco Borderless Access solutions are a primary component of this architecture, enabling various services such as mobility, security, medianet, and Cisco EnergyWise that simplify operations, increase productivity, and improve operational efficiency. When network access is intelligent and relevant, it knows the identity of the user, as well as where the user is on the network. It knows what is connecting to the network to automatically provision the network for optimal quality of service (QoS) and delivery. It becomes services-aware to optimize user experience. Only with an intelligent access network can your enterprise go borderless securely and smoothly. Your business can save energy, simplify operations with better business efficiency, and enjoy an optimized total cost of ownership.

Cisco network access solutions for the borderless enterprise focus on the following primary areas (Figure 1):

- **Sustainability:** Cisco Catalyst® switching solutions enable greener practices through measurable power efficiency, integrated services, and continuous innovations such as Cisco EnergyWise, an enterprisewide solution that reduces energy costs and greenhouse gas emissions footprint. EnergyWise monitors the power of all Cisco network-connected devices, from Power over Ethernet (PoE) devices to IP-enabled building controllers, generating aggregated power consumption reporting to optimize overall power usage based on user policies.
- **Ease of operations:** Catalyst Smart Operations are a comprehensive set of capabilities that simplify LAN deployment, configuration, and troubleshooting. In addition to adaptive, always-on technologies such as Cisco StackWise® and FlexStack, Smart Operations enable zero-touch installation and replacement of switches, fast upgrade, as well as ease of troubleshooting with reduced operational cost. Cisco Catalyst switches automatically apply the right configuration based on the device connecting to the network (wireless access point, IP phone, video camera, and so on), thus simplifying the network setup and enabling mobility. When Cisco best practices templates are applied, configuration errors are minimized, and network is made operational with minimal setup.
- **Borderless security:** Cisco TrustSec is a foundational component of the Cisco Borderless Security Architecture, which helps securely deliver identity-based business services and applications. TrustSec capabilities include policy-based access control, identity and role-aware networking, data integrity, and confidentiality. In addition, Cisco Catalyst switches offer Cisco Integrated Security Features, an industry-leading solution that provides superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and Address Resolution Protocol [ARP] spoofing). Delivering powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats, Cisco Integrated Security Features provide robust security throughout the network. Furthermore the deployment of end-to-end wired and wireless intrusion prevention system (IPS) solutions also helps to defend against network exploits.

- **Borderless experience:** To enable a borderless experience for end users, it is critical to provide them with ubiquitous connectivity that is secure and reliable, thereby resulting in improved productivity. Although Ethernet-based LAN access has been the primary technology in the enterprise, there has been a significant increase in the adoption of wireless LAN to support the increasingly mobile workforce. With the ratification of 802.11n, WLANs now complement wired LANs where relevant in terms of performance and reliability. Another factor in the borderless experience is the growth in video applications that promote collaboration and reduce costs. Cisco medianet provides the right foundation for delivering business-grade video across the same wired and wireless network used for data and voice. Cisco medianet utilizes access network intelligence to simplify complexity and accelerate deployment of rich-media solutions by allocating resources dynamically to help ensure optimal QoS and delivery.

Figure 1. Four Primary Areas of Cisco Network Access



Sustainability

In response to energy costs, environmental concerns, and government directives, there is an increased need for sustainable and “green” business IT operations. Methods to measure power consumption and control energy output are now the focus of businesses worldwide, with all customers looking to reduce energy costs, increase the efficiency of operations, and consolidate energy management across different devices and communication media.

Cisco EnergyWise is a new energy management architecture that will allow IT operations and facilities to measure and fine-tune power usage to realize significant cost savings. Cisco EnergyWise focuses on reducing power utilization on all devices connected to a Cisco network, ranging from PoE devices such as IP phones and wireless access points to IP-enabled building and lighting controllers. It uses an intelligent network-based approach, allowing IT and building facilities operations to understand, optimize, and control power across an entire corporate infrastructure, potentially affecting any powered device. Cisco Catalyst Switches (including the Cisco Catalyst 2960-S, 3560-X, and 3750-X) support Cisco EnergyWise with additional hardware instrumentation in the Cisco Catalyst 3560-X and 3750-X to provide richer and more granular measurements and controls.

For more details on Cisco EnergyWise, visit:
http://www.cisco.com/en/US/prod/switches/ps5718/ps10195/white_paper_c11-514539.html.

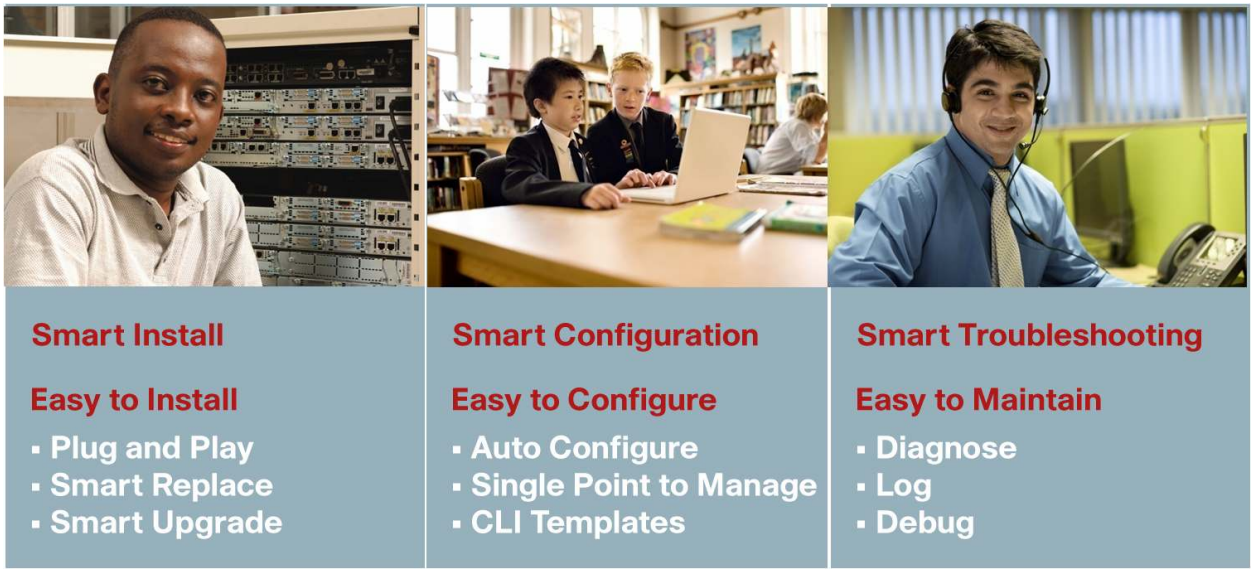
Simplify Switch Deployment and Reduce Costs with Catalyst Smart Operations

Catalyst Smart Operations are a comprehensive set of capabilities to simplify and improve LAN switch and wireless access point deployment, and reduce total cost of ownership. Operational excellence for the enterprise reduces costs and provides network functionality to facilitate next-generation applications. Catalyst Smart Operations help organizations deliver operational excellence and accelerate the way that IT delivers and scales services on the network.

How Do Catalyst Smart Operations Help the Enterprise?

Catalyst Smart Operations make the installation, configuration, replacement, and troubleshooting of a LAN easier and more cost effective by simplifying the operation and deployment of the network. Catalyst Smart Operations include three primary areas: Smart Install, Smart Configuration, and Smart Troubleshooting. Smart Install provides a zero-touch installation of switches onto the network, Smart Configuration provides fast upgrade and zero-touch switch replacement, and Smart Troubleshooting eases the burden of understanding network issues. Figure 2 shows these areas and how they benefit the enterprise.

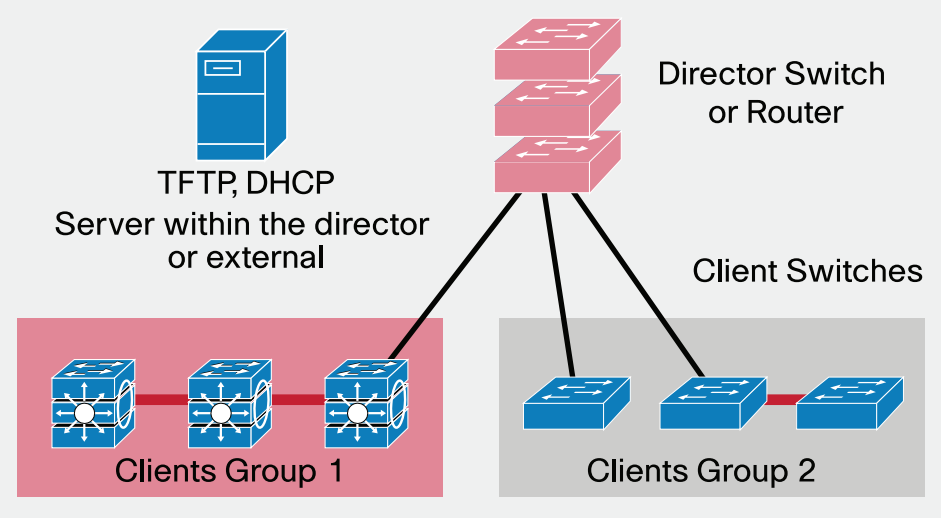
Figure 2. Three Primary Areas of Catalyst Smart Operations



Smart Install: Anyone Can Install a Network

Catalyst Smart Operations utilizes Smart Install to provide smooth plug-and-play technology that installs the Cisco IOS® Software image and switch configuration with minimal user intervention. All the user needs to do is remove the switch from the box, power the switch, and plug it into the network to facilitate smooth network plug and play. Smart Install uses the concept of a director switch, or a switch in the network that helps the installation of other switches. The director switch can be a Cisco Catalyst 3560 or 3750 switch, and the clients, switches that are installed, can be any Catalyst 2960, 3560, or 3750 switch (see Figure 3).

Figure 3. Smart Install-Enabled Network



The director switch is configured with information about images and configuration file locations, and then any switch that attaches to the director will be configured using a Dynamic Host Configuration Protocol (DHCP)-based mechanism. The user needs to specify a DHCP server to allocate IP addresses and a Trivial File Transfer Protocol (TFTP) server for configuration and image file storage. The servers can reside on the director switch or on a third-party server. The director will maintain a list of all switches attached to the network and give user information about those switches including switch type, hostname, IP address, and Cisco IOS Software release. Smart Install can allocate host names and create permanent IP addresses on the client switches, removing the burden of IP address maintenance. The switch groups defined on the director are normally similar switches of the same type, and groups of devices can be upgraded together, facilitating upgrade and change management for the switches.

Smart Configuration: Autoconfigure with Auto SmartPorts

Smart Install is used to install any switch on the network with simple plug and play, but using Auto SmartPorts with Smart Install can make the process of installation faster and easier. Smart Install can download the final switch configuration to a client switch, but this assumes each port will have a predetermined device attached. For example, the first 10 ports are allocated to have IP phones attached, and ports 11 to 20 are allocated for access points, and these need to be predetermined before the switch installation.

Auto SmartPorts have the ability to automatically configure the access ports based on the device that connects to the port. There is no reason to know which device goes into which port, because as devices are attached, they are autodetected, and the port is autoconfigured. Therefore, a base configuration can be downloaded with Smart Install followed by autoconfigured Ethernet ports using Auto SmartPorts as devices attach to the network. The complete installation can be done without knowledge of Cisco IOS Software configuration. Any device with a MAC address organizational unique identifier (OUI), including printers and PCs, or devices that support Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) such as IP phones, access points, and IP cameras can be detected and configured. Also, removal of configuration is possible, and as each devices is removed, the configuration for that device can be removed from the port. This capability allows users to move a device from one port to the other.

Auto SmartPorts configure the port with predefined configurations, encapsulating years of Cisco networking expertise, including security, mobility, IP telephony, availability, QoS, and manageability features with minimal effort and expertise. Auto SmartPorts also includes a macro capability that can be customized by the user. The user can utilize the Cisco built-in macros or customize and create any configuration that is needed to meet the enterprise needs.

Smart Configuration: Configuration Management and Zero-Touch Replacement

The Smart Install director can perform not only the initial installation of switches but also ongoing configuration management; configuration backup; and, in case of emergency, zero-touch switch replacement. The administrator can use the director switch as a single point of management; groups of switches can now be managed from a single point, allowing smooth upgrade or configuration of groups of switches at one time. In addition, any configuration changes made to the client switches will back up automatically and archive to the director or a TFTP server in the network. Two copies of each configuration are archived per switch as part of the Smart Configuration process, providing the latest and previous configuration file. The ability to archive configuration facilitates a zero-touch replacement of any switch that has a problem. The director switch tracks the configuration associated with a client, and therefore, when a faulty switch is replaced, the latest configuration file and Cisco IOS Software image are downloaded to facilitate a zero-touch replacement of switches in the network. It is so easy that any user can remove the faulty switch and replace it with a similar model, and the network will automatically configure the replacement switch.

Smart Configuration: Reduce Operational Costs

Clearly Catalyst Smart Operations reduce costs and ongoing maintenance for switches and attached devices. Table 1 shows a typical return on investment when using Catalyst Smart Operations functionality. Typical cost savings of more than 70 percent can be obtained once Smart Install and Smart Configuration are implemented. The other major advantage of using Catalyst Smart Operations is that the user installing or replacing switches might not need to have intimate knowledge of networking or switching.

Table 1. Cost Savings with Catalyst Smart Operations

Without Cisco Integrated Catalyst Smart Operations

	Amount	Costs*
Equipment to Deploy Annually	100 switches	
Time Per Deployment	1.5 hour/switch	$9000
Number of Updates Annually	4 updates/year	
Time to Update a Network	75 hours/year	

*Average IT Personnel Wage $60/hour

Cost saving with Catalyst Smart Operations

	Amount	Smart Networks	Saving
Time Per Deployment	.25 hour/switch	$1500	83%
Time to Update a Network	20 hours/year	$4800	73%

Cisco StackWise Plus and Cisco FlexStack Stacking: Unify Switches Together

Cisco StackWise and StackWise Plus are the premier innovative stacking technologies from Cisco, which enable a group of switches to act as a single device when connected with stacking cables. The switch stack acts as a unified data and control plane and has increased resiliency and high availability. Cisco StackWise technology provides a method for collectively utilizing the capabilities of a stack of up to nine switches. Individual switches intelligently join to create a single switching unit with a 64-Gbps switching stack interconnect. Switches can be added to and deleted from a working stack without affecting network operation and performance. The switch stack allows subsecond failure recovery and high availability to keep traffic flowing. Also available are cross-stack features such as EtherChannel, allowing high resiliency by utilizing multiple links and switches for traffic forwarding, reducing the risk of network problems. Cisco StackWise Plus is available on Cisco Catalyst 3560 and 3750 Switches. For more information on Cisco StackWise, refer to the StackWise whitepaper.

The Cisco Catalyst 2960-S product family offers Cisco FlexStack stacking. Cisco FlexStack provides true stacking capability, with all switches acting as a single switching unit and unified data plane, with a single IP address similar

to Cisco StackWise. Cisco FlexStack is implemented by adding a stacking module to the Cisco Catalyst 2960-S LAN Base Switch. The new Cisco FlexStack technology allows the stacking of four switches with a stacking throughput of 20 Gbps. The addition and deletion of stack members using a hot-swappable stacking module are possible with the Cisco Catalyst 2960-S Series Switches. Because the module is hot swappable, the addition and deletion of switches to a stack are fast and error free, with automatic imaging and configuration. Also standalone switches, purchased without the stacking capability, can be upgraded with the addition of the stack module and become stack capable. FlexStack stacking does not use a ring protocol such as Cisco StackWise, and therefore, failover times are slower. FlexStack is targeted for users not needing the extensive resiliency and scalability available with StackWise Plus.

Smart Troubleshooting: Isolate and Solve Your Network Issues

Smart Troubleshooting is a set of features and functionality that allow rapid resolution of problems in the network. In general, Cisco IOS Software has an extensive set of command line debugging capabilities that can help customers understand and resolve network issues. Other features that can help with diagnostics include Generic Online Diagnostics (GOLD) and Onboard Failure Logging (OBFL). GOLD allows users to run programmatic tests to determine how well the switch is operating, including the health of hardware components to verify proper operation. Extensive hardware tests can be used to isolate hardware failure or stress test a switch to make sure it is working correctly. OBFL acts like a black box; upon failure of a switch device, OBFL tracks primary parameters within the switch to isolate the problem. The information from OBFL can help improve the products, but also allow customers to understand why a switch had issue and even prevent issues that will happen in the future.

With Catalyst Smart Operations, customers will realize lower operational costs, zero-touch installation, ease of configuration, and simplified switch replacement with faster time to deploy services and network equipment. Cisco is the smart choice in switching, with new innovative ease-of-use capabilities such as Catalyst Smart Operations.

Borderless Security with Intelligent Threat Defense and Cisco TrustSec

Cisco Catalyst switches provide superior Layer 2 threat defense capabilities for mitigating man-in-the-middle attacks (such as MAC, IP, and ARP spoofing). TrustSec, a primary element of borderless security architecture, helps enterprise customers secure their networks, data, and resources with policy-based access control, identity and role-aware networking, data integrity, and confidentiality.

Threat Defense

Cisco Integrated Security Features are an industry-leading solution available on Cisco Catalyst switches that proactively protects your critical network infrastructure irrespective of the access technology. Delivering powerful, easy-to-use tools to effectively prevent the most common and potentially damaging Layer 2 security threats, Cisco Integrated Security Features provides robust security throughout the network.

Cisco Integrated Security Features include the following:

- **Port Security:** Prevents MAC address-flooding attacks by limiting the MAC addresses of stations allowed access to the same physical port. Port Security limits the number of learned MAC addresses to deny MAC address flooding.
- **DHCP Snooping:** Prevents DHCP server spoofing and “man-in-the-middle” attacks with the access switch acting much like a small security firewall between users and the legitimate DHCP server. Network attackers can no longer assign themselves as the default gateway or reroute and monitor traffic flow between the two endpoints.
- **Dynamic ARP Inspection:** Prevents ARP spoofing by helping ensure that the access switch relays only “valid” ARP requests and responses. This capability prevents malicious hosts from invisibly eavesdropping on the conversation between the two endpoints, to glean passwords or data or to listen to IP phone conversations.

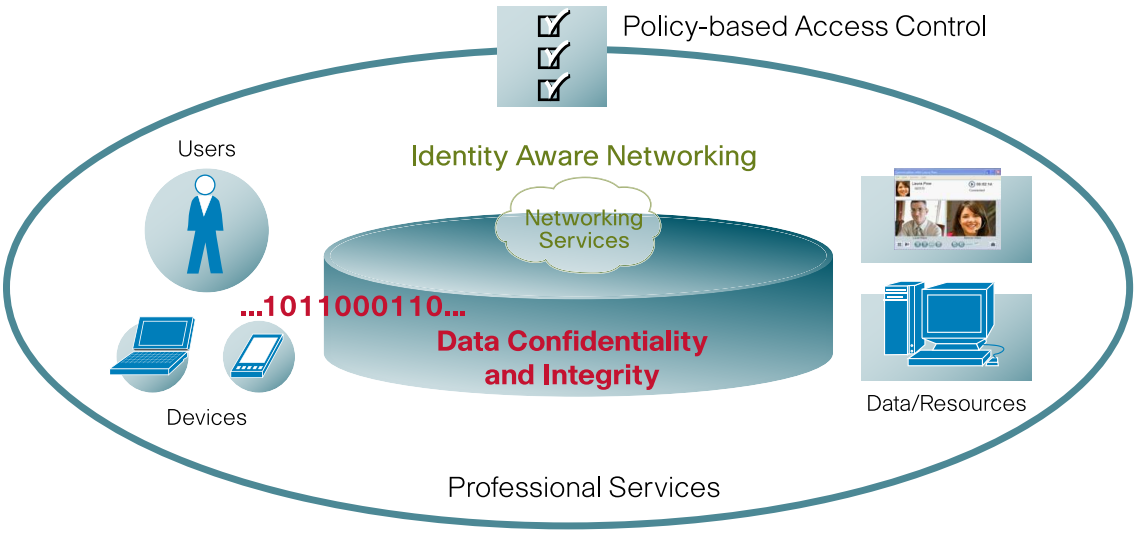
- **IP Source Guard:** Prevents IP host spoofing from attackers and Internet worms assuming a valid user's IP address. IP Source Guard permits forwarding of only packets with valid source addresses.
- **Rogue Detection:** Access points (AP) unmanaged by IT rarely conform to corporate security policy and, as a result, provide easy access to criminals entering a company's network through the WLAN. Customers require smart detection and day-zero remediation of unauthorized or "rogue" access points that will:
  - Immediately disconnect the offending device
  - Accurately pinpoint its location for removal

  For example, an employee plugs in a consumer-grade access point to provide wireless access to members of the team. Unfortunately, attackers discover the consumer-grade access point is using weak encryption and attempt to use it to breach the corporate network. In that situation the wireless LAN controller detects the rogue access point, and the Cisco Wireless Control System (WCS) detaches it from the network by disabling the switch port.

Cisco TrustSec

The Cisco TrustSec solution (Figure 4) secures access to the network, enforces security policies, and delivers standard-based security solutions (such as 802.1X), enabling secure collaboration and policy compliance.

Figure 4. Cisco TrustSec



TrustSec capabilities reflect Cisco thought leadership, innovations, and commitment to customer success. These new capabilities include:

- IEEE 802.1AE MACsec with prestandard 802.1X-REV primary management: An industry leader with prestandard 802.1X-Rev primary management. Available on Cisco Catalyst 3750-X and 3560-X Switches, MACsec provides Layer 2, line-rate Ethernet data confidentiality and integrity on host-facing ports, protecting against man-in-the-middle attacks (snooping, tampering, and replay).
- Flexible authentication that supports multiple authentication mechanisms, including 802.1X, MAC authentication bypass and web authentication, using a single, consistent configuration.
- Open mode that creates a user-friendly environment for 802.1X operations
- Integration of device-profiling technology and guest access handling with Cisco switching to significantly improve security while reducing deployment and operational challenges.
- Comprehensive policy management capabilities such as RADIUS Change of Authorization and downloadable access control list (ACLs).

- 802.1X Supplicant with Network Edge Access Transport (NEAT) enables extended secure access where compact switches in the conference rooms have the same level of security as switches inside the locked wiring closet.
- End-to-end system troubleshooting, monitoring, and reporting capabilities

For more details on Cisco TrustSec, go to: http://www.cisco.com/go/trustsec.

Borderless Experience: Unified Access

Enabling a borderless experience is about providing connectivity to the right person over the right device and at the right time. The goal is to help ensure that end users have a consistent experience when they use collaborative applications such as Cisco Telepresence™ or video conferencing, regardless of the underlying access technology.

With the ratification of the 802.11n standard, wireless networks have attained a maturity that enables them to complement the performance, security, and reliability expected of wired networks. Although WLAN as the primary access technology might be relevant in certain scenarios, the right recommendation is one that strikes a balance between both access methods, taking into account the users' current and future needs in terms of security requirements, reliability numbers, and application demands. The Cisco Ethernet switching portfolio is mobility-ready to help customers take advantage of the 802.11n technology transition. With PoE, Cisco Catalyst series switches can meet the power requirements of dual-radio 802.11n access points, helping ensure better reliability and throughput for users.

The Cisco Catalyst series supports Cisco EnergyWise, an energy management architecture that will allow IT operations, facilities, and plant operations to measure and fine-tune power usage to realize significant cost savings for both wired and wireless access. For 802.11n access points, this technology enables the switching on and off of the access points when coverage is not required during business downtimes.

One logical concern with eliminating the location border in your network is protecting it from intrusion and attack independent of where the attack comes from (that is, wired or wireless clients). The Cisco Catalyst series switches support Cisco TrustSec, which simplifies the deployment of identity services and helps ensure a common policy framework across both networks.

Cisco Catalyst switches simplify WLAN deployment using Catalyst Smart Operations by automatically provisioning the switch when a Cisco access point is connected. Cisco Catalyst switches are shipped with Cisco best practices configuration templates for Cisco access points. When a Cisco access point is detected, Cisco Catalyst switches automatically provision the interface (connected to the access point) with the right settings. Using Cisco best practices templates minimizes operator errors, thus reducing the network setup time.

Cisco is an industry leader in providing intelligent quality of service treatment for all types of traffic. As more and more of your traffic becomes wireless, the challenge is to provide the mobile user with the same experience as the wired user. Cisco innovations such as AutoQoS (to automatically determine and deploy the appropriate QoS policies) and Auto SmartPorts (to dynamically apply QoS policies to a switch port, based on user or device type) significantly lower the cost of operations when deploying quality of service.

Unified Access: Client Monitoring and Troubleshooting

Many studies indicate that network managers spend significant amount of time troubleshooting client issues and root causing the problem. Quicker problem resolution directly affects a company's overall profitability. Client troubleshooting is greatly simplified with the unified solution that helps track assets, devices, and users regardless of whether they are connected wired or wirelessly to the network. With centralized visibility and control enabled by location services, business processes are simplified, thus increasing user productivity.

- Network visibility and control: This solution provides centralized visibility into the location of wired and wireless devices on the network. If a device such as an IP phone is moved from one building to another, the solution dynamically learns the new location, facilitating centralized tracking and enabling emergency services such as E911. It allows tracking of any IP device, including devices connected to Cisco Catalyst switches as well as various wireless assets such as wireless clients, wireless tags, telemetry, interference, and rogue access points.
- Location-assisted client troubleshooting: This feature enables tracking of wired or wireless clients for quick problem resolution. For client connectivity issues, the help desk can use this solution to determine how the client is using the network (connecting from wired or wireless) and to identify the entry into the network, an access port on a switch, or an access point leading to a specific area/location to further narrow down the problem. Also available is historical reporting, which provides more insight into usage patterns.
- Asset tracking and improved security: This feature provides centralized inventory of wired and wireless devices and asset management for improved business processes. Network location service also enables zone-based visibility for asset tracking. Zone or inventory management applications will be able to define zones and monitor the mobile assets entering and exiting the area. The solution alerts network managers when an asset has left the zone or has not been seen for a certain amount of time, increasing responsiveness for security incidents. In addition to detecting rogue access points, this solution can also trace the rogue access point to switch port location (where the rogue is connected) to block the rogue and protect the network.

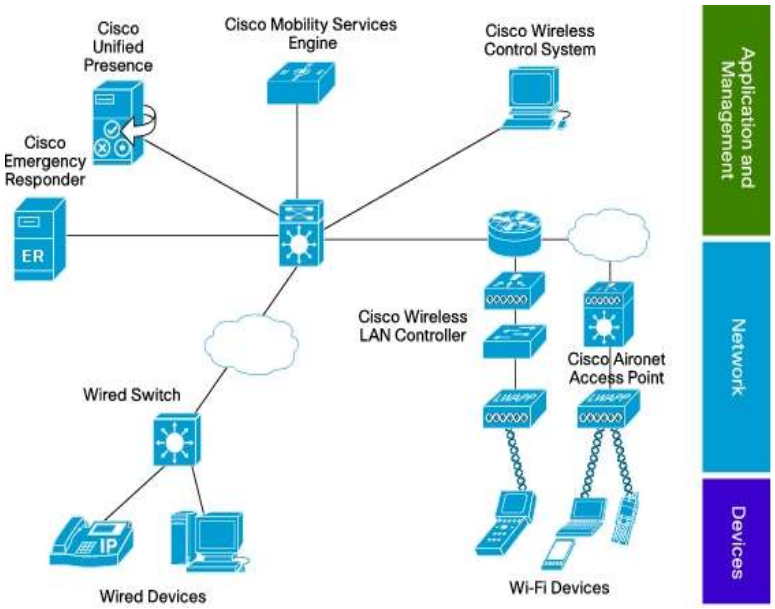
The Cisco Mobility Services Engine (MSE) provides an open API (based on Simple Object Access Protocol [SOAP] and Extensible Markup Language [XML] protocol) for any business application that needs the location data. Several partners have already integrated with Cisco MSE open API for enabling various network security and assurance applications. Access to this API is available to any Cisco technology partner and allows a full integration into the business processes of customers.

Location-based policies allow greater control and visibility. Knowing the location of a wired device provides more intelligence to apply the right set of policies to tracked devices, based not only on the user's credentials, but also on the location of the device. For example, a phone in the lobby of an office building can have different policies from a phone in a conference room or in an employee's office. Today the policies are statically administered, based on an endpoint’s MAC address, not on the location of the endpoint itself.

Network Location Services Architecture

This section focuses on location services for endpoints attached to Cisco Catalyst switches. The overall solution has three components: the Cisco 3300 Series Mobility Services Engine (MSE), WCS, and Cisco Catalyst access switches (Figure 5).

Figure 5. Cisco Network Location Architecture



Cisco 3300 Series MSE

The Cisco 3300 Series MSE tracks the location of wired and wireless devices continuously. It can do this by having the wired and wireless network infrastructure devices (controllers and switches) send location measurement data to the MSE as changes occur in the network. Both wired and wireless network infrastructure connect to the MSE using Network Mobility Service Protocol (NMSP).

In the case of wired switches, the information sent to the MSE is typically the MAC address, switch MAC address, port, IP address, and IEEE 802.1x username (if available). This information is sent whenever a device link changes state. In the case of wireless controllers, the information sent to the MSE is typically the MAC address, IP address, IEEE 802.1x username (if available), and the IEEE 802.11 measurement data necessary to determine the physical location.

Cisco Wireless Control System

The Cisco WCS is the management system for the MSE and provides the administrator with the user interface for common MSE network management functions such as configuration and monitoring. Cisco WCS pinpoints the location of end devices on a floor plan map. In addition to current location, WCS also presents historical information to aid in troubleshooting client connectivity issues.

Cisco Catalyst Switches

Cisco Catalyst switches provide the relevant location information for all the endpoints attached to them. Location information might include the physical address (also known as the civic address) as well as other information about endpoints such as the IP address, MAC address, port, VLAN, and username. Civic location can be configured globally on the switch, with optional information at the interface to indicate specific data such as the room number and cube number. Switches obtain endpoint/user information using features such as IEEE 802.1x, DHCP snooping, Dynamic ARP Inspection (DAI), and IP Source Guard. When an endpoint is plugged into the access switch, the switch can convey information about the endpoint and its location to the central server, Cisco MSE. Additionally, if the endpoint runs the Cisco Discovery Protocol or Link Layer Discovery Protocol (LLDP), more information, such as the version number and serial number, can also be sent to the MSE. Because the endpoint location is derived from the point of attachment in the enterprise network, location services provide dynamic location information, enabling mobility, while optimizing resources and improving operational efficiency.

Borderless Experience: Video

Video-ready edge enables:

- Deterministic user experience
- Resilient video sessions
- Reduced bandwidth utilization
- Secure video systems
- Lower total cost of ownership

Increase in video traffic is beating all expectations of growth. In 2008, the Cisco Visual Networking Index (VNI) predicted Internet traffic will quadruple in 2012. Now, based on the data collected in Q3 2009, Cisco VNI forecast is that peak Internet traffic might grow sevenfold by 2013. Most enterprise IT teams will be expected to deliver the same quality of experience for business-influenced video applications as service providers are delivering for consumers.

What Is Different About Video?

Video traffic has a variable bit rate (VBR) and is bursty. Therefore, enterprise video needs have to be taken into consideration while planning networks, especially with the blurring of lines between wired and wireless access. The bandwidth requirements vary significantly among applications and could vary between sessions (see Table 2). Demands for video streaming and video conference applications are unpredictable and can create unforeseen peaks of traffic.

Table 2. Bandwidth Requirements for Video Applications

Application	Bandwidth	
Desktop	200 KB–1.5 Mb	
Video conference	768 KB–5 Mb	
Cisco TelePresence solution	1.5 Mb–24+ Mb	
Signage	SD 1.5 Mb–5 Mb	HD 5 Mb–8 Mb
Enterprise TV	SD 1.5 Mb–5 Mb	HD 8 Mb–15 Mb
Video surveillance	256k–8+ Mb	

There is a need to optimize the network with effective multicast streaming. High quality of experience will need QoS and a highly available network. Ease of deployment, as well as management of endpoints, applications, and access ports will lead to significant savings.

Video Quality of Service

Video is a high-bandwidth and variable-bandwidth application. Even a few packets lost or delayed can create very ugly artifacts, making the entire screen distorted. In gigabit/10gigabit campus networks, the need for QoS is sometimes overlooked or even challenged. This reaction arises because some network administrators equate QoS with queuing policies only, whereas the QoS toolset extends considerably beyond just queuing tools. Classification, marking, and policing are all important QoS functions that are optimally performed at the access layer (access edge). Cisco Catalyst 2960, 3560, and 3750 Series Switches have a consistent video QoS configuration for all the various enterprise-class video applications. For more information, read Medianet Campus QoS Design.

Video High Availability

High availability creates an enhanced user experience because the video session stays up, even when infrastructure components fail, minimizing disruptions to existing video streams with a highly available access architecture.

The latest innovation on the new Cisco Catalyst 3560-X and 3750-X Series Switches is Cisco StackPower™: a power interconnect system that allows the power supplies in a stack to be shared as a common resource among all the switches. In case of power supply failures, power is maintained for business-critical applications while shedding power for lower-priority devices as defined by the user.

Cisco StackWise and Cisco StackWise Plus technologies create a unified, logical switching architecture through the linkage of multiple, fixed configuration switches. Any switch in the stack can serve as a master, providing the highest reliability for forwarding. Read more at the Cisco StackWise Technology White Paper.

Highly redundant designs are possible with a wide variety of Cisco technologies such as:

- Flex Links allow the switch to provide rapid bidirectional convergence when a primary (forwarding) link fails. Packets are no longer lost, and high quality is maintained on the active video sessions. For more information, read Flex Links.
- Cross-stack EtherChannel allows multiple switches in a stack to create an EtherChannel connection, so that the loss of an individual switch does not affect connectivity for the other switches in the stack.
- Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP) provide rapid spanning tree and also offer the benefit of Layer 2 load balancing and distributed processing. Stacked units behave as a single spanning-tree node.
- Layer 3 Nonstop Forwarding allows for the same level of redundancy at the edge that is available at the core.
- With Unidirectional Link Detection (UDLD), nonworking ports can be detected quickly and shut down, so high availability is maintained.

Bandwidth Utilization Reduced with Multicast

Delivering high-quality live video events over the WAN is one of the most challenging networking tasks. Such live events typically involve high-ranking executives and relay vital business information. In such situations, the event must be delivered right the first time. Unicast networks in particular pose a serious challenge, because congestion on the link from multiple clients attempting to view the live event might result in unacceptable video quality and a disruption of other business-critical applications.

IP Multicast enables multiple receivers to get identical copies of the stream without duplicating the stream on any network link. One or thousands of viewers can get the content with the load on the multicast source always being one stream. This capability is one of the many advantages of IP Multicast on server and network traffic. Cisco is the market leader in the multicast technology with high availability and flexibility. All Catalyst 3750 Series Switches have Smart Multicast, which does not replicate packets within the stack. Cisco IT implemented Single Source Multicast (SSM), a more efficient one-to-many technology. Cisco is the only vendor able to provide a complete end-to-end solution for video and multicast. To read more on how Cisco IT uses IP Multicast to deliver a scalable and cost-effective transport for rich-media delivery, go to this case study. Learn more on enabling multicast at the access.

Securing Video Streams

Like any IP traffic, video over IP is vulnerable to attacks without proper security considerations. Recently researchers from Viper Lab demonstrated how an IP video surveillance system could be tampered with by replacing the crime video with another clip. Then they eavesdropped on a video-over-IP call. Cisco Catalyst switches have built-in security measures that can be easily enabled to protect the video-over-IP traffic. Read more at Cisco Catalyst Integrated Security Features and Cisco TrustSec for protecting infrastructure and using MACsec to encrypt your data.

Lower Total Cost of Ownership

A typical enterprise video deployment involves a large number of device types, each with its own access needs. A variety of video conferencing devices are available, ranging from the Cisco TelePresence solution and other room-based systems to personal HD cameras, video phones, and so on. Then there are digital signage devices with needs different from IP video surveillance.

In a wiring closet switch, there are typically 10+ configuration lines per port per device for an average of thousands of switch ports in an enterprise. Manual adds/moves/changes can be expensive. So most businesses resort to fixed port assignment, which leads to oversubscription and thus a larger capital expense investment. Even with that, global policy changes are very expensive. Cisco Catalyst switches allow for autoconfiguration on device detection. With built-in device detection for IP phones, digital media players, and IP video surveillance cameras (VSCs), and so on, deployments no longer require oversubscription of ports. The IT group now needs to maintain only one configuration per device type for any number of switch ports. Adds/moves/changes are all automated, significantly lowering operational expenses. Read more at Configuring Auto Smartports.

Enabling a Media-Ready WLAN

Cisco delivers a high-performance wireless network as an essential foundation that incorporates advanced technologies such as 802.11n to enable significant enhancements in the throughput and provide reliability and predictability for the media-ready WLAN. These enhancements address the unique requirements demanded by media applications and reduce burden on IT resources. Enabling this experience requires a best-of-class wireless network integrated with a wired network to deliver a truly enterprise-quality video regardless of wired or wireless access.

In addition to a high-performance network, Cisco media-ready networks (medianets) provide intelligence that optimizes video by providing adaptability, prioritization, QoS, resource reservation, monitoring, reliable multicast, and roaming to deliver seamless visual networking experience end-to-end independent of the access technology.

Media-ready wireless expands on the performance of Cisco's 802.11n wireless to deliver innovative features like Cisco VideoStream to ensure smooth, multicast delivery of voice and video applications from the wired network to the wireless network. For more info on Cisco VideoStream technology, visit: http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/ps10325/white_paper_c11-577721.html.

Summary

Cisco Borderless Networks, a Cisco next-generation architecture, deliver a new workspace experience, connecting anyone, anywhere, using any device, to any resource: securely, reliably, and smoothly. Borderless experience is only possible with an intelligent network access designed to meet the needs of a global workspace. Cisco network access is a primary component of this architecture, providing mobility, security, medianet, location, and EnergyWise services for delivering an optimal experience. Intelligent network access provides mobile workspace, secure collaboration, and policy compliance while conserving energy and improving operational efficiency. Intelligent network access enables innovative business models, creating new user experiences that lead to increased customer satisfaction and loyalty.

For More Information

For more information about Cisco Catalyst 3560-X and 3750-X Series Switches, visit http://www.cisco.com/go/3560x and http://www.cisco.com/go/3750x

For more information about Cisco Catalyst 2960-S Series Switches, visit http://www.cisco.com/go/2960

For more information about Cisco Borderless Networks, visit http://www.cisco.com/go/borderless

For more information about the Cisco TrustSec solution, visit http://www.cisco.com/go/trustsec

For more information about Cisco medianet solution, visit https://www.cisco.com/web/solutions/medianet

For more information about Cisco EnergyWise, visit http://www.cisco.com/go/energywise

For more information about the Cisco Context-Aware Mobility solution, visit http://www.cisco.com/go/contextaware

For more information about the Cisco Mobility Services Engine, visit http://www.cisco.com/go/mse

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-577729-00 03/10