Cisco BYOD Solution Components

Revised: August 28, 2014

What's New: The Cisco 3700 and 2700 Series access points, which support 802.11ac, have been validated and added to the Cisco BYOD solution.

Cisco provides a comprehensive BYOD solution architecture, combining elements across the network for a unified approach to secure device access, visibility, and policy control. To solve the many challenges described earlier, a BYOD implementation is not a single product, but should be integrated into an intelligent network.

The following figures show a high-level illustration of the Cisco BYOD solution architecture. The architecture has been separated into campus and branch diagrams simply for ease of viewing. These infrastructure components are explained in detail in the following sections.

Figure 3-1 HIgh-Level BYOD Solution Architecture—Campus View

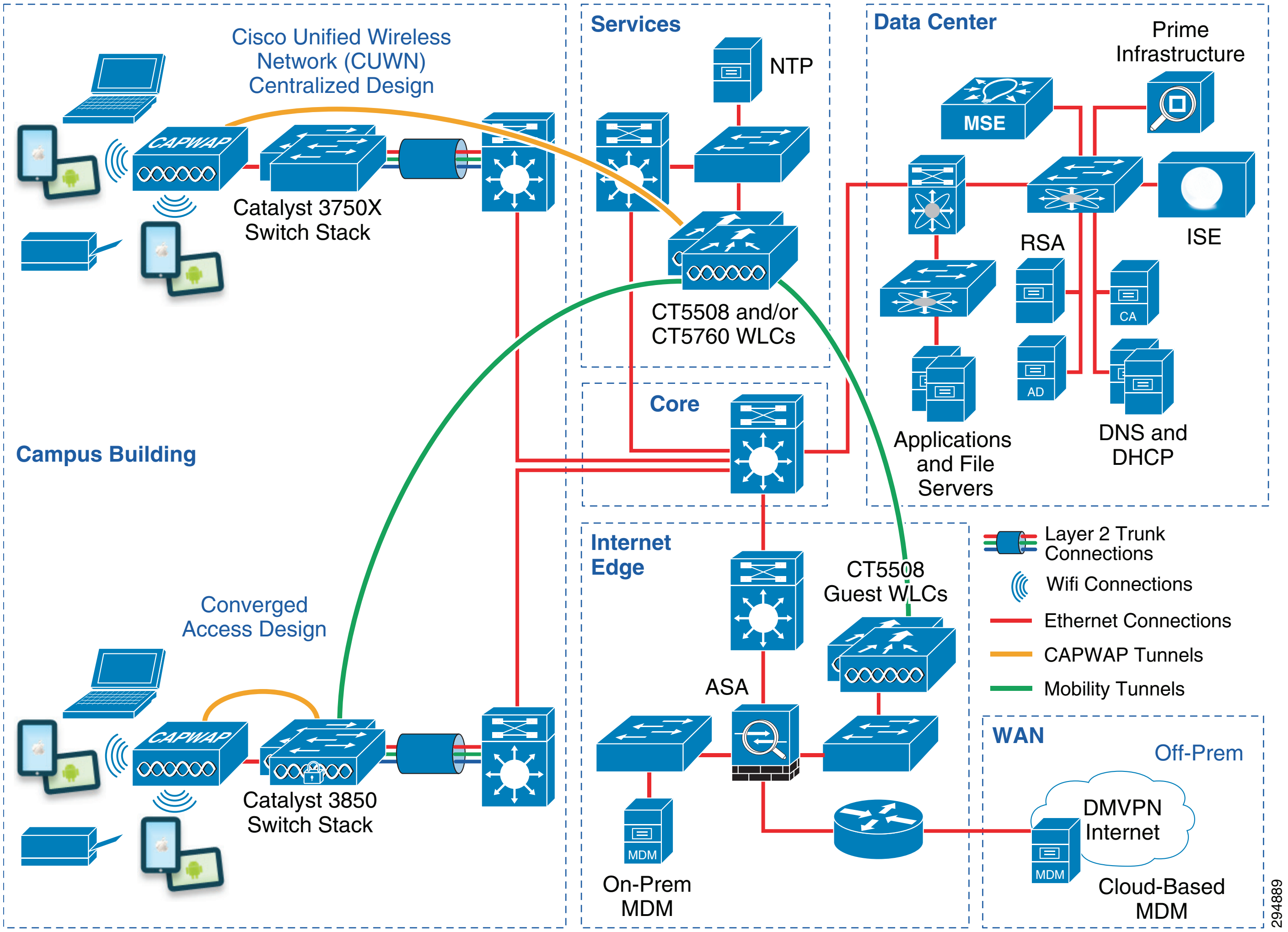
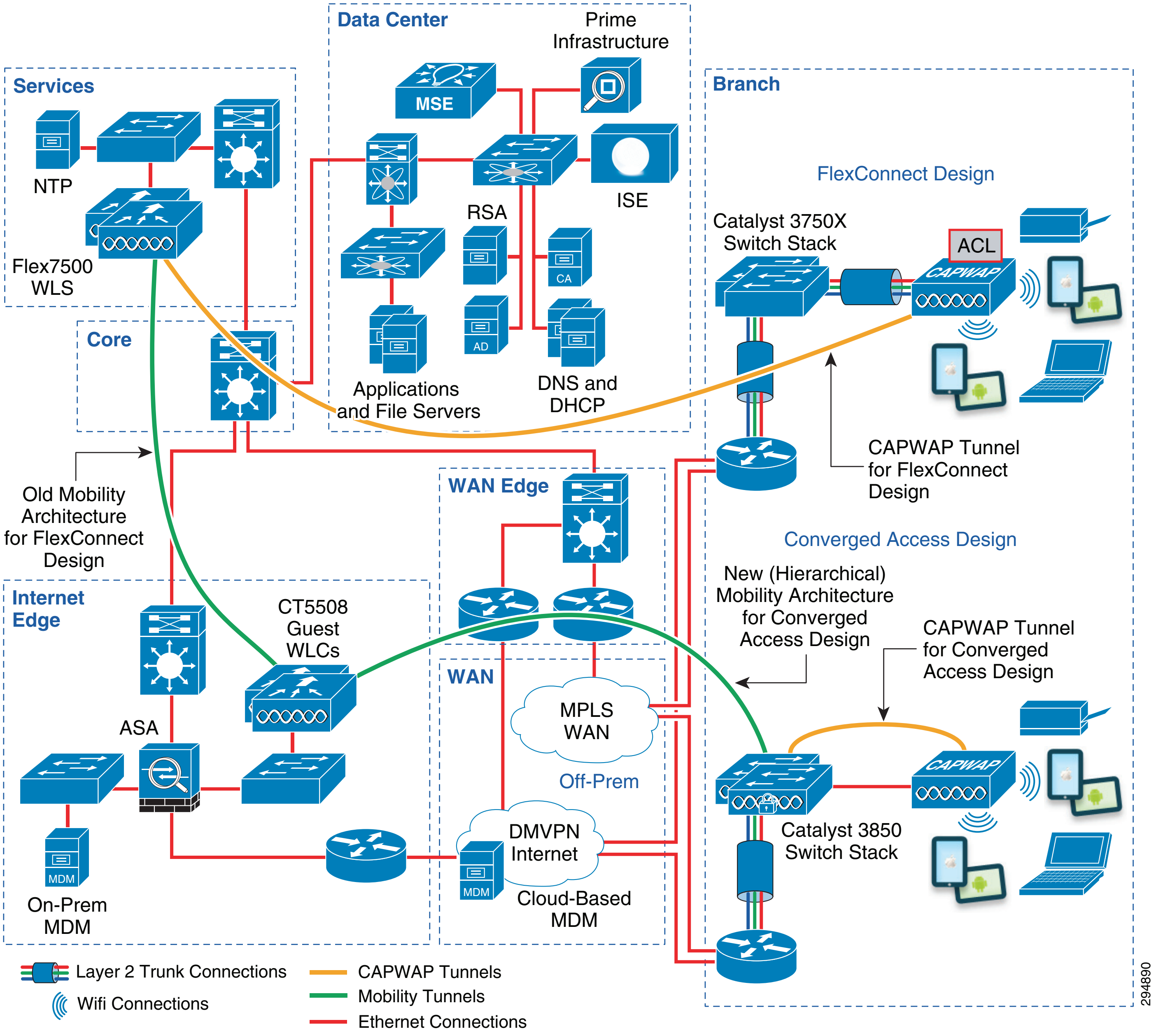


Figure 3-2 High-Level BYOD Branch Solution Architecture—Branch View



Cisco Wireless Infrastructure

The Cisco wireless infrastructure discussed in this design guide consists of Cisco Aironet access points (APs), Cisco wireless LAN controllers (WLCs), Cisco Converged Access switches, and the Cisco Mobility Services Engine (MSE). Each is discussed in the following sections.

Cisco Aironet Access Points

Cisco Aironet access points provide WiFi connectivity for the corporate network and handle authentication requests to the network via 802.1X. The Cisco second generation (G2) access points in this design guide include the Cisco Aironet 3700, 2700, 3600, 2600, and 1600 Series.

Cisco 3700 Series APs are ideal for high-density network environments that use mission-critical, high-performance applications. They feature the industry's first AP with an integrated 802.11ac Wave 1 radio a supporting a 4x4 multiple input, multiple output (MIMO) design with three spatial streams for data rates up to 1.3 Gbps. The flexible, modular design of the Cisco 3700 Series provides expansion capability for a future 802.11ac Wave 2 module and advanced services such as the Wireless Security Module (WSM).

Cisco 2700 Series APs are non-modular dual band (5 GHz and 2.4 GHz) 802.11ac access points optimized for adding capacity and coverage to dense Wi-Fi networks. They feature a 3x4 MIMO design with three spatial streams for a maximum data rate up to 1.3 Gbps.

The Cisco 3700 and 2700 Series APs incorporate the Cisco High-Density Experience (HDX), which includes among other features Cisco CleanAir® with enhanced support for 80-GHz channels and updated ClientLink 3.0 with support for 802.11a/b/g/n/ac. Cisco CleanAir® technology is enabled in hardware for both the Cisco 3700 and 2700 Series APs. Cisco ClientLink 3.0 helps improve performance of clients on the wireless LAN (WLAN).

Cisco 3600 Series access points are ideal for customers looking for best-in-class performance in 802.11n environments with high client density. They feature the industry's first 802.11n 4x4 multiple input multiple output (MIMO) design with three spatial streams for data rates up to 450 Mbps. The flexible, modular design of the Cisco 3600 Series provides expansion capability for emerging technologies such as the 802.11ac module and advanced services such as the Wireless Security Module (WSM).

The 802.11ac module protects the existing investment in wireless infrastructure by extending the capabilities of the Cisco 3600 Series access point to provide 802.11ac Wave 1 support for wireless clients. The field-upgradeable 802.11ac module has its own 5 GHz radio with internal antennas which are separate from the client/data serving 5 GHz and 2.4 GHz radios within the Cisco 3600 Series access point. The 802.11ac module provides 3x3 MIMO with three spatial streams, extending the maximum data rate of the Cisco 3600 Series access point to approximately 1.3 Gbps with the 802.11ac module installed.

The field-upgradeable Wireless Security Module (WSM) has a dedicated 2.4 and 5 GHz radio with its own antennas enabling 7x24 scanning of all wireless channels in the 2.4 and 5 GHz bands. It offloads concurrent support for monitoring and security services—such as Cisco CleanAir® spectrum analysis, wIPS security scanning, rogue detection, context-aware location, and Radio Resource Management (RRM)—from the internal client/data serving radios within the Cisco 3700 or 3600 Series AP to the WSM. This not only allows for better client performance, but also reduces costs by eliminating the need for dedicated monitor mode access points and the Ethernet infrastructure required to connect those devices into the network.

Note The Cisco 3600 Series access point requires 18 Watts of power with the 802.11ac module and 17 Watts of power with the WSM. The Cisco 3700 Series requires 18 Watts of power with the WSM. When powering the access point from a Cisco Catalyst switch, the switch port must support either IEEE 802.3at POE+ or Cisco Universal PoE (UPoE). If powered from a switch port which only supports IEEE 802.11af PoE, the Cisco 3600 Series access point will boot up, however the module will not be activated.

Cisco 2600 Series access points are dual band (5 GHz and 2.4 GHz) 802.11n access points ideal for mid-market small, mid-size, or large enterprise customers looking for mission critical performance. They feature a 3x4 multiple input multiple output (MIMO) design with three spatial streams for a maximum data rate of approximately 450 Mbps.

Cisco Aironet 1600 Series are entry-level dual band (5 GHz and 2.4 GHz) 802.11n access points, designed to address the wireless connectivity needs of small and mid-size enterprise customers. They feature a 3x3 multiple input multiple output (MIMO) design with two spatial streams for a maximum data rate of approximately 300 Mbps.

The Cisco 3600, 2600, and 1600 Series access points support additional technologies, such as Cisco ClientLink 2.0, which help improve performance of clients on the wireless LAN (WLAN). The Cisco 3600 with the 802.11ac module also supports IEEE 802.11ac Wave 1 explicit beamforming for 802.11ac clients which also support the functionality. Cisco CleanAir® technology is also enabled in hardware for both the Cisco 2600 and 3600 Series APs.

Cisco Aironet access points can operate as lightweight or autonomous access points. When functioning as lightweight access points, a wireless LAN controller is required. In this design, the 802.11 MAC layer is essentially split between the AP and the WLC. The WLC provides centralized configuration, management, and control for the access points. All designs in this design guide assume lightweight access points.

Further information regarding Cisco Aironet access points can be found in the following at-a-glance document:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/at_a_glance_c45-636090.pdf

Cisco Wireless LAN Controllers

Cisco Wireless LAN Controllers (WLC) automate wireless configuration and management functions and provide visibility and control of the WLAN. The WLC extends the same access policy and security from the wired network core to the wireless edge while providing a centralized access point configuration. The WLC interacts with the Cisco Identity Services Engine (ISE) to enforce authentication and authorization policies across device endpoints. Multiple WLCs may be managed and monitored by Cisco Prime Infrastructure. Wireless LAN Controller functionality can be within standalone appliances, integrated within Catalyst switch products, or run virtually on Cisco Unified Computing System (UCS). Integrated controller functionality is discussed in Converged Access Campus Design in Chapter 5, "Campus and Branch Network Design for BYOD."

The Cisco wireless LAN controller platforms discussed within this design guide include the Cisco 5508 wireless LAN controller (CT5508), the Cisco Flex 7510 wireless LAN controller, the Cisco 5760 wireless LAN controller (CT5760), and the Cisco Catalyst 3850 Series switch. The Cisco 5508 and Flex 7510 WLC platforms run Cisco Unified Wireless Network (CUWN) software (also referred as AireOS software), while the Cisco 5760 WLC and Catalyst 3850 Series switch run Cisco IOS XE software.

The Cisco 5508 wireless LAN controller is targeted for mid-sized and large single-site enterprises. Within the Cisco BYOD design guide it is deployed within the campus supporting access points operating in centralized (local) mode. The Cisco 5508 WLC supports up to 500 access points and 7,000 clients per controller with a maximum capacity of approximately 8 Gbps.

The Cisco Flex 7510 wireless LAN controller is targeted for enterprise branch environments. Within the Cisco BYOD design guide it is deployed as a remote controller supporting access points operating in FlexConnect mode. The Cisco Flex 7510 WLC supports up to 6,000 access points and 64,000 clients per controller with up to 2,000 FlexConnect groups, each of which can be configured for a branch location.

The Cisco 5760 wireless LAN controller is targeted for large multisite or single-site enterprises or service providers. Within the Cisco BYOD design guide it is deployed within the campus, either supporting access points operating in centralized mode or functioning as a Mobility Controller (MC) in a Converged Access design. The Cisco 5670 WLC supports up to 1,000 access points and 12,000 clients per controller with a maximum capacity of approximately 60 Gbps.

Cisco Catalyst 3850 Series switches are discussed in Cisco Converged Access Switches.

Further information regarding Cisco wireless LAN controller platforms can be found in the following at-a-glance document:
http://www.cisco.com/en/US/prod/collateral/modules/ps2706/at_a_glance_c45-652653.pdf

Cisco Converged Access Switches

Cisco Converged Access switch platforms include the Catalyst 3850 Series and Catalyst 3650 Series. This version of the BYOD design guide only discusses Catalyst 3850 Series switches deployed in both campuses and branches.

Cisco Catalyst 3850 Series switches provide converged wired and wireless network access for devices. As a switch, the Catalyst 3850 provides wired access to the network and handles authentication requests to the network via 802.1X. In addition, the Catalyst 3850 contains wireless LAN controller functionality integrated within the platform. As a wireless controller, it allows for the termination of wireless traffic from access points directly attached to the Catalyst 3850 switch rather than backhauling wireless traffic to a centralized wireless controller. This can provide greater scalability for wireless traffic, as well as provide increased visibility of wireless traffic on the switch. The Catalyst 3850 Series switch supports up to 25 access points and 1000 wireless clients on each switching entity (switch or stack) with a maximum wireless capacity of approximately 40 Gbps (48-port models).

The Catalyst 3850 Series switch interacts with Cisco ISE to enforce authentication and authorization policies across device endpoints, providing a single point of policy enforcement for wired and wireless devices. When deployed at the access-layer within a branch location, the Catalyst 3850 can be configured to function as both a Mobility Controller (MC) and a Mobility Agent (MA), providing full wireless controller functionality. When deployed within a large campus, the Catalyst 3850 can be configured to function as an MA, which allows for the termination of wireless traffic directly on the switch itself. For increased scalability, the MC function, which handles Radio Resource Management (RRM), Cisco CleanAir, and roaming functions, among other things, can be moved to a dedicated CT5760 or CT5508 wireless controller. Both the Catalyst 3850 and the CT5760 wireless controller run IOS XE software, allowing for the full feature richness of Cisco IOS platforms.

Appendix C, "Software Versions" discusses the feature sets and licensing required for wireless controller functionality on the Catalyst 3850 Series platform.

Cisco Mobility Services Engine

The Cisco Mobility Services Engine (MSE) is a platform that helps organizations deliver innovative mobile services and to improve business processes through increased visibility into the network, customized location-based mobile services, and strengthened wireless security. The Cisco MSE supports mobility services software in a modular fashion through applications. The following services are supported along with the required licensing:

- Cisco Base Location Services—Requires Location Services licensing.
- Cisco Connected Mobile Experiences (CMX)—Requires Advanced Location Services licensing.
- Cisco Wireless Intrusion Prevention System (wIPS)—Requires wIPS licensing.

The Cisco MSE is available as a physical appliance or as a virtual appliance with scalability shown in Table 3-1. As of MSE software release 7.4 and above, licensing is based the number of access points supported.

Table 3-1 Mobility Services Engine (MSE) Platforms and Scalability

Platform	Location Services Licensing	Advanced Location Services Licensing	wIPS Licensing	Maximum Number of Tracked Devices
Cisco 3355 MSE Appliance	Up to 2,500 access points	Up to 2,500 access points	Up to 5,000 Monitor Mode (MM) or Enhanced Local Mode (ELM) access points	Up to 25,000 devices
Cisco MSE Virtual Appliance (High-end Virtual Appliance)	Up to 5,000 access points	Up to 5,000 access points	Up to 10,000 MM or ELM access points	Up to 50,000 devices

Chapter 28, "BYOD Network Management and Mobility Services" provides further discussion around the Mobility Services Engine and Cisco wireless technologies that enable the MSE's capabilities.

Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) is a core component of the Cisco BYOD solution architecture. It delivers the necessary services required by enterprise networks, such as Authentication, Authorization, and Accounting (AAA), profiling, posture, and guest management on a common platform. The ISE provides a unified policy platform that ties organizational security policies to business components.

The ISE also empowers the user to be in charge of on-boarding their device through a self-registration portal in line with BYOD policies defined by IT. Users have more flexibility to bring their devices to their network with features such as sponsor-driven guest access, device classification, BYOD on-boarding, and device registration.

The ISE is able to integrate with third-party Mobile Device Managers (MDM) to enforce more granular policies based on device posture received from the MDM compliance rules.

Cisco Adaptive Security Appliance

Cisco Adaptive Security Appliance (ASA) provides traditional edge security functions, including firewall and Intrusion Prevention System (IPS), as well as providing the critical secure VPN (AnyConnect) termination point for mobile devices connecting over the Internet, including home offices, public WiFi hotspots, and 3G/4G mobile networks. The ASA delivers solutions to suit connectivity and mobility requirements for corporate-owned devices as well as employee-owned laptops, tablets, or mobile devices.

Cisco AnyConnect Client

Cisco AnyConnect^{TM} client provides 802.1X supplicant capability on trusted networks and VPN connectivity for devices that access the corporate network from un-trusted networks, including public Internet, public WiFi hotspots, and 3G/4G mobile networks. Deploying and managing a single supplicant client has operational advantages as well as provides a common look, feel, and procedure for users.

In addition, the AnyConnect client can be leveraged to provide device posture assessment of the BYOD device, as well as a degree of policy enforcement and enforcing usage policies.

The AnyConnect client can be provisioned centrally with use of a third-party MDM. This enhances the user experience and reduces the support costs. MDM policy can be configured to manage who is entitled to use AnyConnect.

Cisco Integrated Services Routers

Cisco Integrated Services Routers (ISR), including the ISR 2900 and ISR 3900 families, provide WAN and LAN connectivity for branch and home offices. The LAN includes both wired and wireless access. In addition, ISRs may provide direct connectivity to the Internet and cloud services, application and WAN optimization services, and may also serve as termination points for VPN connections by mobile devices.

Cisco Aggregation Services Routers

Cisco Aggregation Services Routers (ASR), available in various configurations, provide aggregate WAN connectivity at the campus WAN edge. In addition, ASRs may provide direct connectivity to the Internet and cloud services and may also serve as a firewall. The ASR runs Cisco IOS XE software and offers Flexible Packet Matching (FPM) and Application Visibility and Control (AVC).

Cisco Catalyst Switches

Cisco Catalyst® switches, including the Catalyst 3000, Catalyst 4000, and Catalyst 6000 families, provide wired access to the network and handle authentication requests to the network via 802.1X. In addition, when deployed as access switches, they provide power-over-Ethernet (PoE) for devices such as VDI workstations, IP phones, and access points.

Cisco Nexus Series Switches

Cisco Nexus switches, including the Nexus 7000 and 5000 families, serve as the data center switches within the CVD. The Nexus 7000 switches provide 10GE Layer 3 connectivity between the Campus Core, Data Center Core, and Aggregation Layers and 10GE Layer 2 connectivity, utilizing VPC, for the Nexus 5000 switches in the Data Center Access Layer to which all servers are attached.

Cisco Prime Infrastructure

Cisco Prime Infrastructure (PI) is an exciting new offering from Cisco aimed at managing wireless and wired infrastructure while consolidating information from multiple components into one place. While allowing management of the infrastructure, Prime Infrastructure gives a single point to discover who is on the network, what devices they are using, where they are, and when they accessed the network.

Cisco Prime Infrastructure 1.2 is the evolution of Cisco Prime Network Control System 1.1 (NCS). It provides additional infrastructure and wired device management and configuration capabilities while improving on existing capabilities in NCS 1.1.

Cisco Prime Infrastructure interacts with many other components to be a central management and monitoring portal. Prime Infrastructure has integration directly with two other appliance-based Cisco products, the Cisco Mobility Services Engine (MSE) and Identity Services Engine (ISE) for information consolidation. Prime Infrastructure controls, configures, and monitors all Cisco Wireless LAN Controllers (WLCs), and by extension, all Cisco access points (APs) on the network. Prime Infrastructure also configures and monitors Cisco Catalyst switches and Cisco routers.

Secure Access to the Corporate Network

On-boarding for new devices (certificate enrollment and profile provisioning) should be easy for end users with minimal intervention by IT, especially for employee owned devices. Device choice does not mean giving up security. IT needs to establish the minimum security baseline that any device must meet to access the corporate network. This baseline should include WiFi security, VPN access, and add-on software to protect against malware. Proper device authentication is critical to ensure secure on-boarding of new devices and to ensure secure access to other devices on the network. Hence, proper device authentication protects the entire network infrastructure.

Who is accessing the network, *what* device they are using, and *where* they are located need to be considered before implementing a BYOD solution. The user can initiate the provisioning process from a campus or a branch location. This design allows the user to provision and access resources from either location. In the past, a username/password was all that was needed as most employees accessed the network from a wired workstation. Often a simple server was used to collect and authenticate user credentials. As organizations implemented wireless into their network, a unique SSID (Wireless Network name) with a username and password was also needed.

Today, digital certificates and two-factor authentication provide a more secure method to access the network. Typically the end user must download client software to request a certificate and/or provide a secure token for access. One of the challenges with deploying digital certificates to client endpoints is that the user and endpoint may need to access the company's certification authority (CA) server directly (after being authenticated to the corporate network) to manually install the client certificate. This method requires the end user manually install the client certificate and ensuring it is installed in the proper certificate store on the local endpoint.

Deploying digital certificates on non-PC based devices requires a different process as many of these devices do not natively support all the features and functionality needed to create/download and install digital client certificates. As users become more and more mobile, authenticating users and devices accessing the network is an important aspect of BYOD.

Certificate Enrollment and Mobile Device Provisioning

Deploying digital certificates to endpoint devices requires a network infrastructure that provides the security and flexibility to enforce different security policies, regardless of where the connection originates. This solution focuses on providing digital certificate enrollment and provisioning while enforcing different permission levels. This design guide covers Android™ and Apple® iOS™ mobile devices, in addition to Windows 7 and Mac OS X.

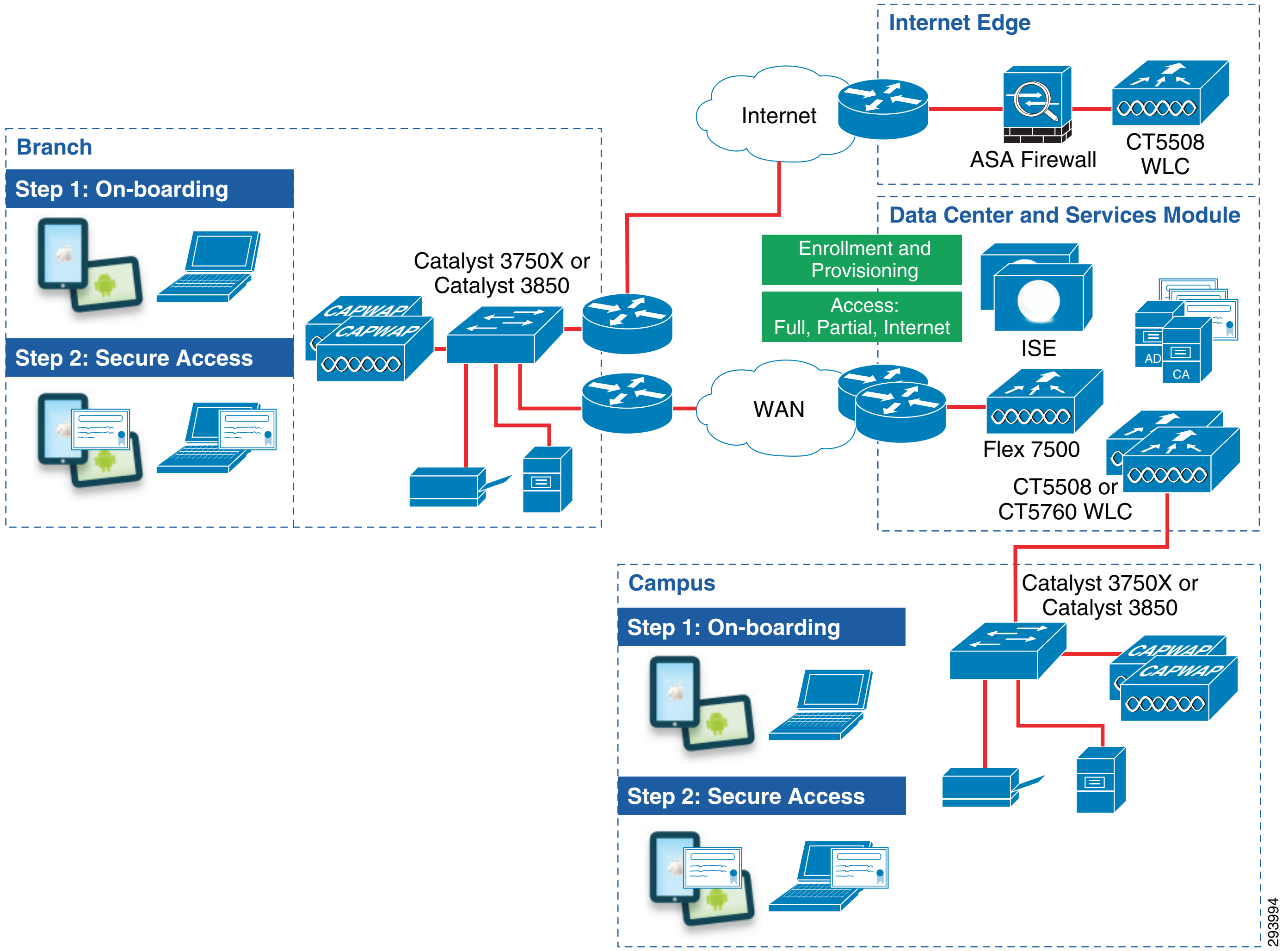
Figure 3-3 highlights the general steps that are followed for this solution when a mobile device connects to the network:

1. A new device connects to a provisioning SSID, referred to as the BYOD_Provisioning SSID. This SSID (open or secured with PEAP) is configured to redirect the user to a guest registration portal.
2. The certificate enrollment and profile provisioning begins after the user is properly authenticated.
3. The provisioning service acquires information about the mobile device and provisions the configuration profile, which includes a WiFi profile with the parameters to connect to a secure SSID, called the BYOD_Employee SSID.
4. For subsequent connections, the device uses the BYOD_Employee SSID and is granted access to network resources based on different ISE authorization rules.

The design guide also covers a single SSID environment, where the same SSID is used for both provisioning and secure access.

Employee devices that do not go through the provisioning process simply connect to a guest SSID, a or dedicated guest-like SSID; which may be configured to provide Internet-only or limited access for guests or employees.

Figure 3-3 Enrollment and Provisioning for Mobile Devices


Internet Edge
Internet
ASA Firewall
CT5508
WLC
Branch
Step 1: On-boarding
Step 2: Secure Access
Catalyst 3750X or
Catalyst 3850
CAPWAP
CAPWAP
Data Center and Services Module
Enrollment and
Provisioning
Access:
Full, Partial, Internet
ISE
AD
CA
WAN
Flex 7500
CT5508 or
CT5760 WLC
Campus
Step 1: On-boarding
Step 2: Secure Access
Catalyst 3750X or
Catalyst 3850
CAPWAP
CAPWAP
293994