Cisco BYOD Solution Components

Revised: August 7, 2013

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

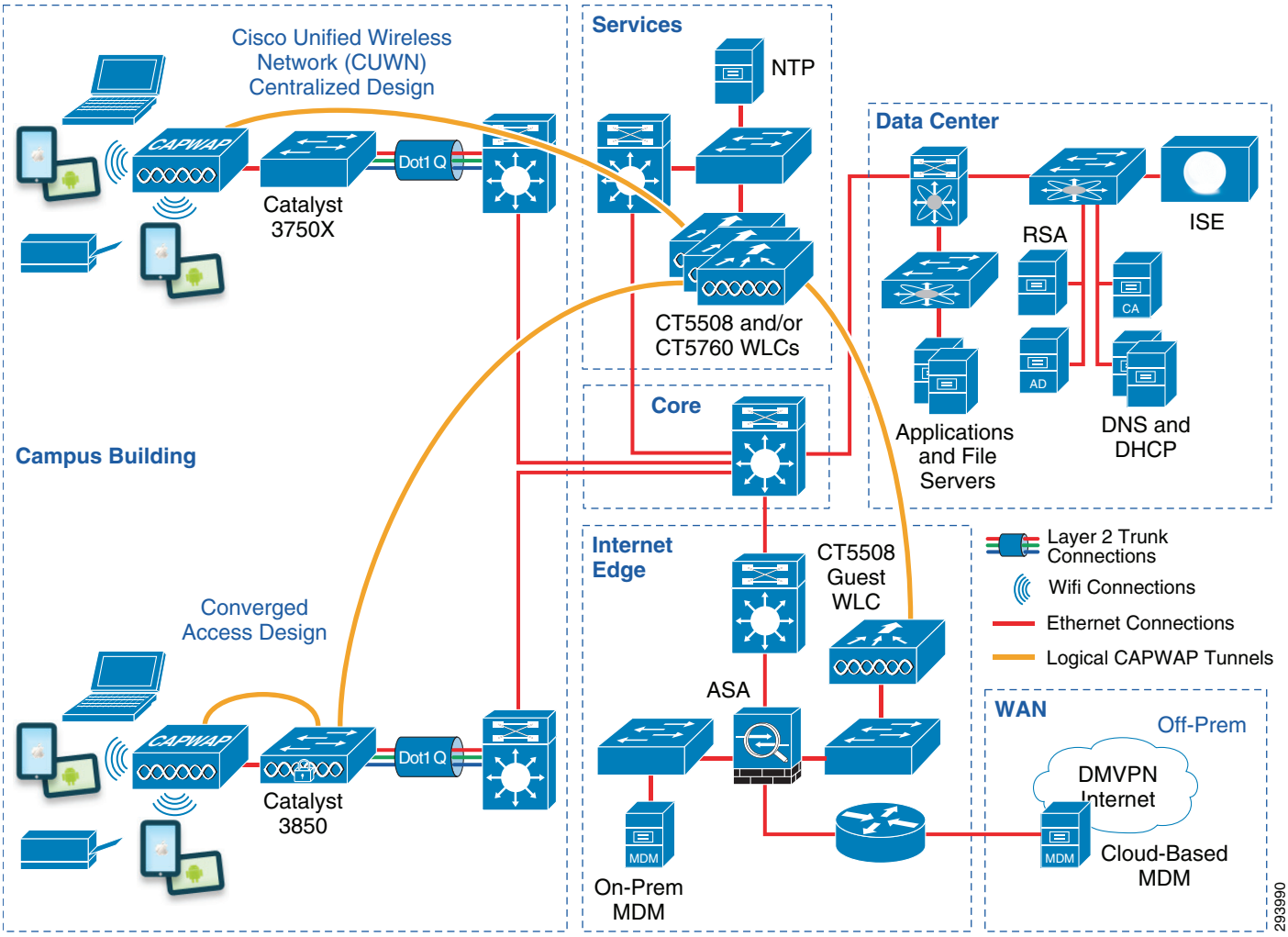
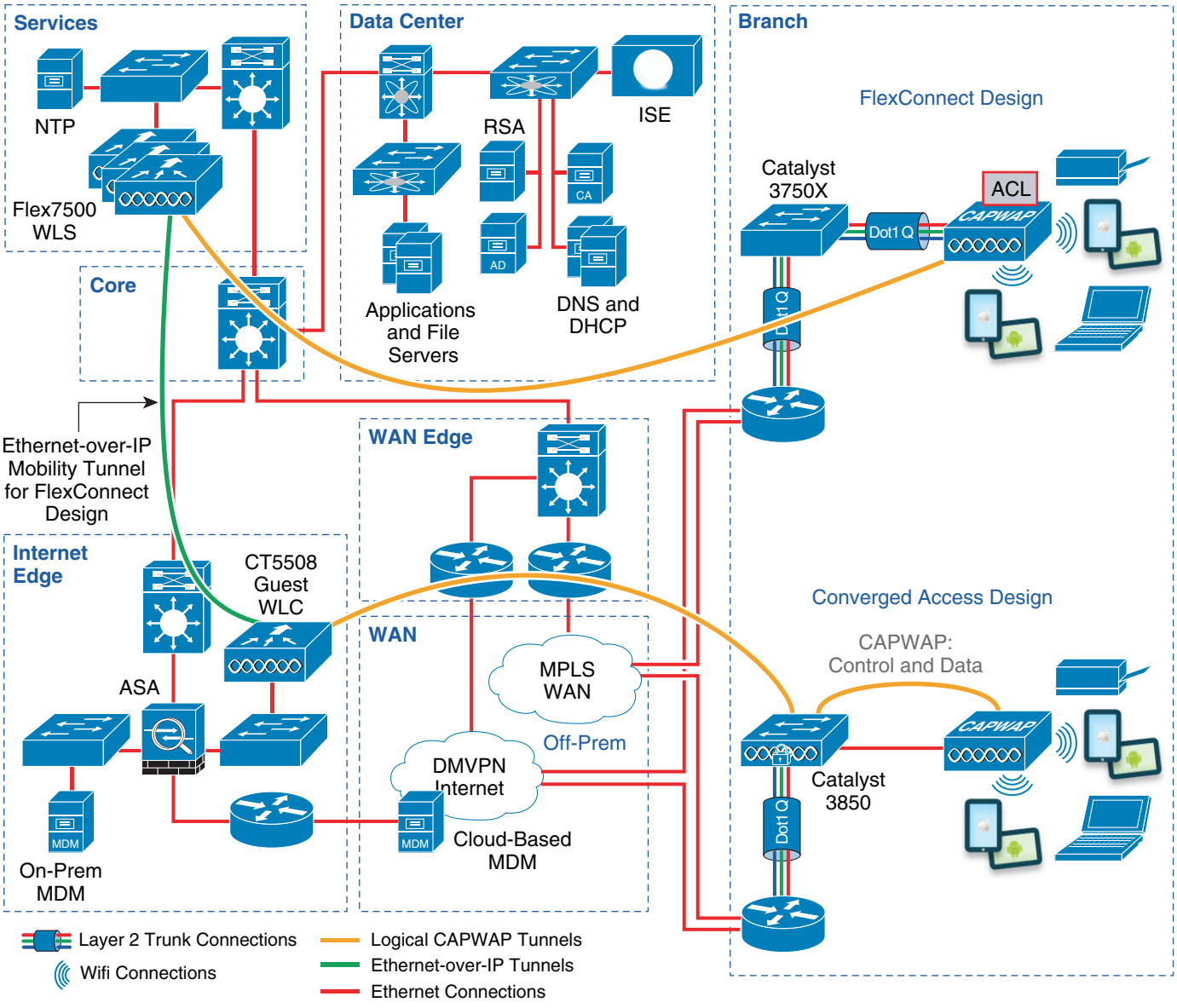


Figure 3-2 High-Level BYOD Branch Solution Architecture—Branch View



Cisco Access Points

Cisco Access Points provide WiFi connectivity for the corporate network and handle authentication requests to the network via 802.1X. In addition, the Cisco Access Points at the branch location can either tunnel all the traffic to the campus or switch traffic locally based on the configuration.

Cisco Wireless Controller

Cisco Wireless LAN Controller (WLC) is used to automate wireless configuration and management functions and to provide the 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."

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™ 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 Converged Access Switches

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 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 a Mobility Agent (MA), which allows for the termination of wireless traffic directly on the switch itself. For increased scalability, the Mobility Controller (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 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