Cisco Universal Wi-Fi for Service Providers, Release 5.0

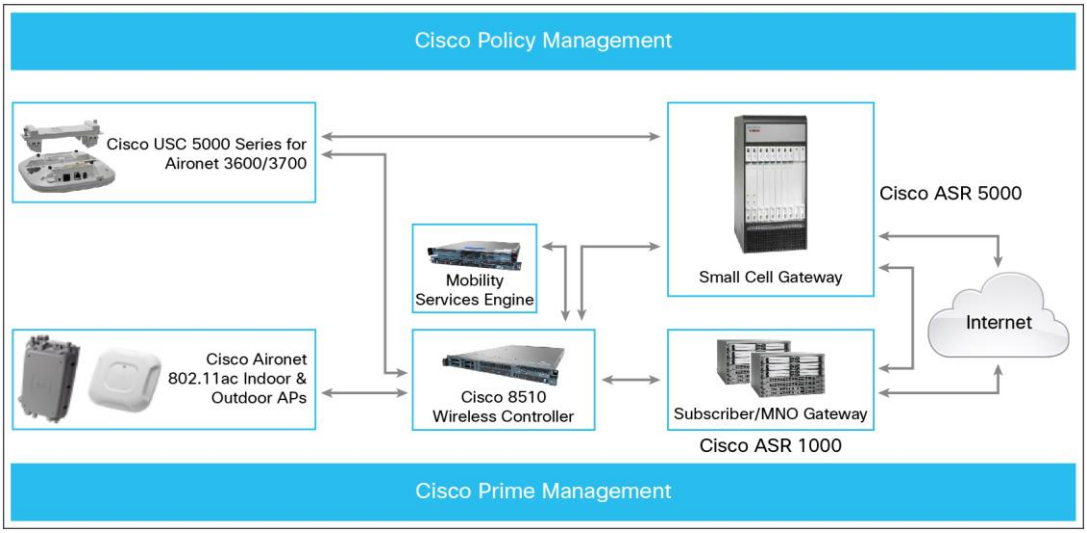
Cisco® Universal Wi-Fi 5.0 gives you everything you need to provide carrier-grade Wi-Fi to your customers. A portfolio of intelligent 802.11ac access points. A secure network intelligence platform. End-to-end, centralized management. Policy control. And an award-winning mobile packet core. Our tested architecture becomes your trusted tool for business and service innovation. A key feature of the Release 5.0 architecture splits the control plane and data plane traffic for improved performance. Release 5.0 also includes advanced virtualized tunneling and Wi-Fi offload configurations for increased scalability and deployment options. These features greatly enhance the Cisco Universal Wi-Fi solution.

The Cisco Universal Wi-Fi solution (Figure 1) includes the following elements:

- A complete portfolio of intelligent 802.11ac access points including the Cisco Aironet® 1530,1550 and 1570 Series for outdoors and the Cisco Aironet® 700, 1700, 2700 and 3700 Series for indoors. Silicon-level integration supports crucial network functions, including interference mitigation, resource management, beamforming, band selection, and voice and video optimization.
- Secure network intelligence and management with carrier-grade network analytics, subscriber management, and policy control provided from the Cisco Wireless Controller, the Cisco Mobility Services Engine (MSE), the Cisco Wireless Access Gateways (WAG), and the Cisco Policy Suite. Cisco WAG configuration options include LMA, iWAG, eWAG and SAMOG-GW. These solution elements give you the flexibility needed to deploy, operate, and manage networks with hundreds of thousands of access points and let you turn on different services by simply pointing and clicking. Real-time analytics and reports are a key feature of Cisco Universal Wi-Fi, providing operators with a tool for offering location-based services. These robust service features help to reduce operating costs through zero-touch provisioning and centralized interference mitigation and troubleshooting for easier network maintenance.
- The Cisco Policy Suite provides a next generation policy management solution that helps customers scale, control, monetize, and personalize services through a flexible and interactive architecture that supports application-centric policy capabilities. The Cisco Policy Suite is a flexible, scalable policy control platform that can be deployed across all access networks.
- The mobile packet core, based on the award-winning Cisco ASR 5000 Series, provides standards-based capabilities that allow operators to transparently and securely integrate Wi-Fi, small cell, and macrocell radio networks through the Cisco ASR 5000 Small Cell Gateway. The Cisco ASR 5000 Series includes common subscriber management, policy, and authentication functions, delivering transparent service integration to Wi-Fi and licensed small cell users. The Cisco ASR 5000 Series Small Cell Gateway is widely deployed today, providing multivendor interoperability.

- Across the Cisco Universal Wi-Fi solution, Cisco Prime is a unified network management platform that supports an intuitive user experience as it integrates operations across Cisco products, technologies, and networks.

Figure 1. Cisco Universal Wi-Fi



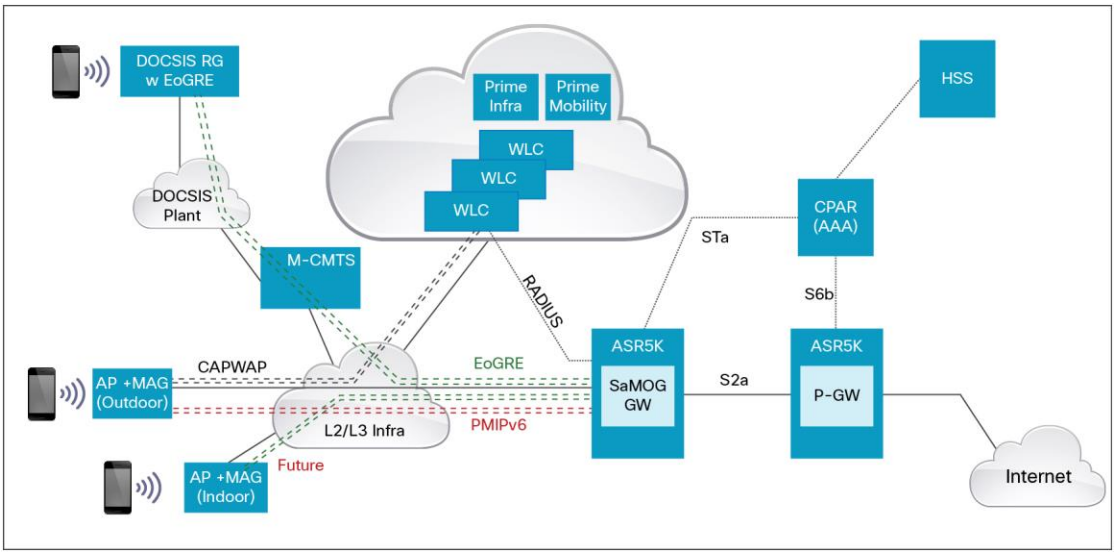
Architecture Models and Use Cases

In this fifth generation release, Cisco Universal Wi-Fi adds support for split control plane/data plane (CP-DP) tunnel deployments using Proxy Mobile IPv6 (PMIPv6), Tier2/3 Internet Access, and Location-based Web Portal Authentication. Previously deployed use cases have been revalidated with newer hardware and software releases.

Split CP-DP Tunneling on Trusted Wi-Fi Access Network

The split control/management plane and data plane architecture is used with PMIPv6 tunneling carried over IPv4 networks. The wireless AP control/management plane will use CAPWAP, whereas the data plane will use an IPv4 generic routing encapsulation (GRE) tunnel, with AP MAG (Mobile Access Gateway) and the Local Mobility Anchor (LMA) on the Cisco ASR 5000 as the tunnel end points. This trusted Wi-Fi architecture provided below (Figure 2) includes both Residential Gateway access via Ethernet over GRE (EoGRE) and AP access via PMIPv6 to the SaMOG (S2a Mobility over GTP) Gateway. The ASR 5000-based SaMOG solution supports Trusted WLAN AAA Proxy (TWAP) for Authentication and Trusted WLAN Access Gateway (TWAG) for data path integration. Future AP MAG tunneling protocols will include EoGRE.

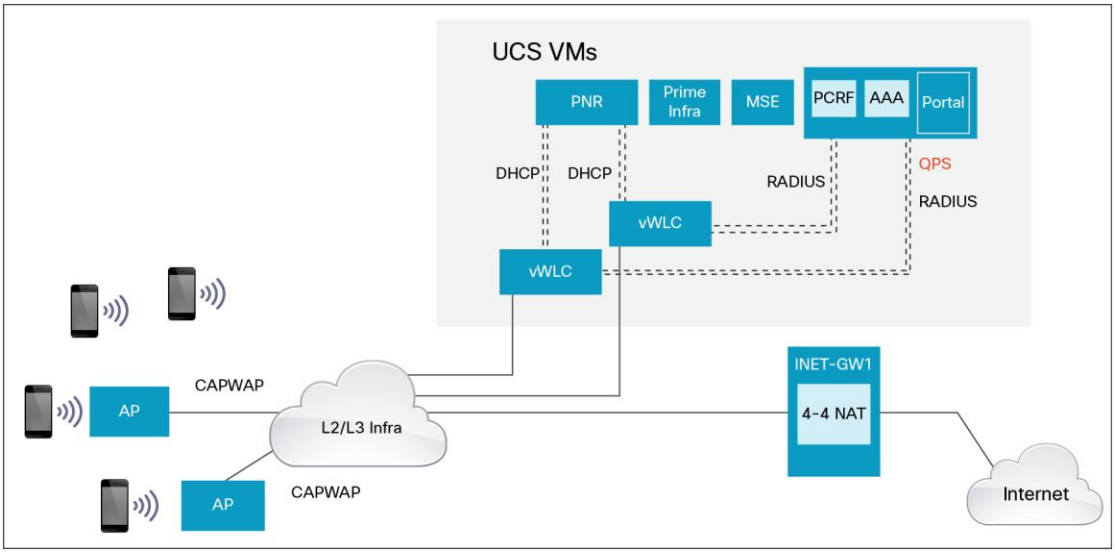
Figure 2. CP-DP Split Architecture



Virtualization for Tier 2/3 Internet Access

Tier 2/3 Internet access is a simplified use case to provide users with Wi-Fi access to the Internet which leverages direct integration of the wireless controller with the Cisco Policy Suite for Web-based authentication. This model makes use of the Cisco Unified Computing System™ (UCS™) and the virtual wireless LAN controller (vWLC) as shown in Figure 3. This model does not make use of a Cisco ASR 1000 or Cisco ASR 5000 WAG and is suited for smaller scale carrier Wi-Fi deployments. The vWLC can achieve a maximum of 500 Mbps throughput and can support up to 200 FlexConnect mode APs. Multiple vWLCs can be loaded onto the Cisco UCS to support larger configurations. Cisco Policy Suite is used in this architecture but other policy servers and/or portals can be integrated into the solution. The addition of a Cloud Services Router 1000v (Virtual Cisco ASR 1000) can be easily added to provide Intelligent Services Gateway and/or NAT functionality as required.

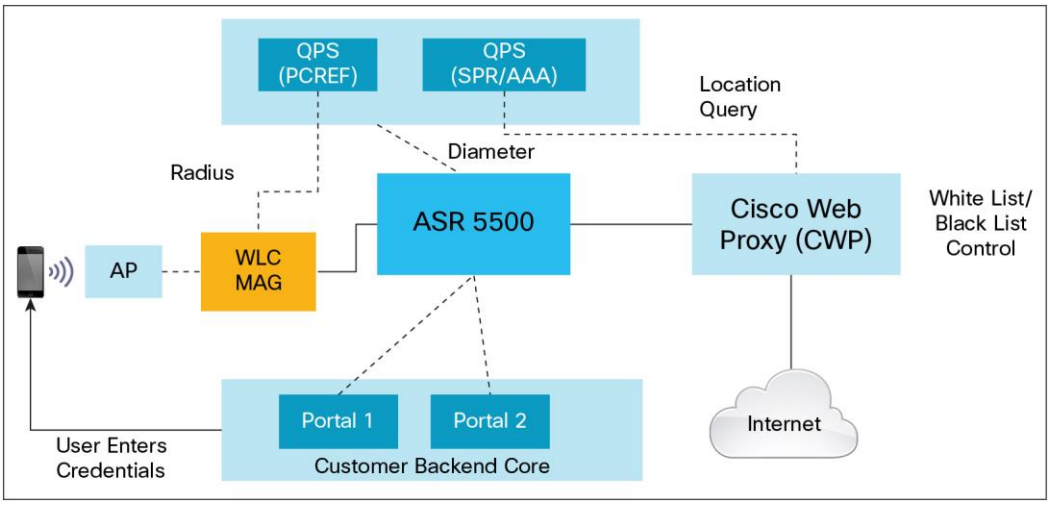
Figure 3. Tier 2/3 Internet Access with Point-of-Presence (PoP) in a Box



Location-Based Web Portal Authentication (with Allowed/Blocked Listing)

There are two main features in this configuration. The first allows the user to easily access the network. If the user device's MAC address is already stored in the AAA server, then the user is automatically connected as an authenticated session (MAC transparent autologon [TAL]). If the user device is not in the AAA server, then the user is redirected to a web portal and queried for their user name and password. The second feature provides the ability for the service provider to control user access to the Internet based on the user's location. This value-added feature utilizes Cisco policy and a Cisco Web Proxy (CWP) server to implement the policy. When a user attempts to access a web page, the request is sent to the CWP that then queries the Cisco Policy Suite database for the AP MAC/SSID pair to which the user is connected. The CWP utilizes this location information to determine if the user is allowed access to the requested web page. If allowed (in the white page list), then the request is sent and the requested page is transmitted to the user (otherwise, the user is not allowed access to the selected white page). If the requested page is not in the white page list, then the user is redirected to a portal for user name/password authentication. If validated, the user is allowed access to the non-allowed list site. The basic configuration of this feature is shown in Figure 4.

Figure 4. Location-Based Web Portal Authentication

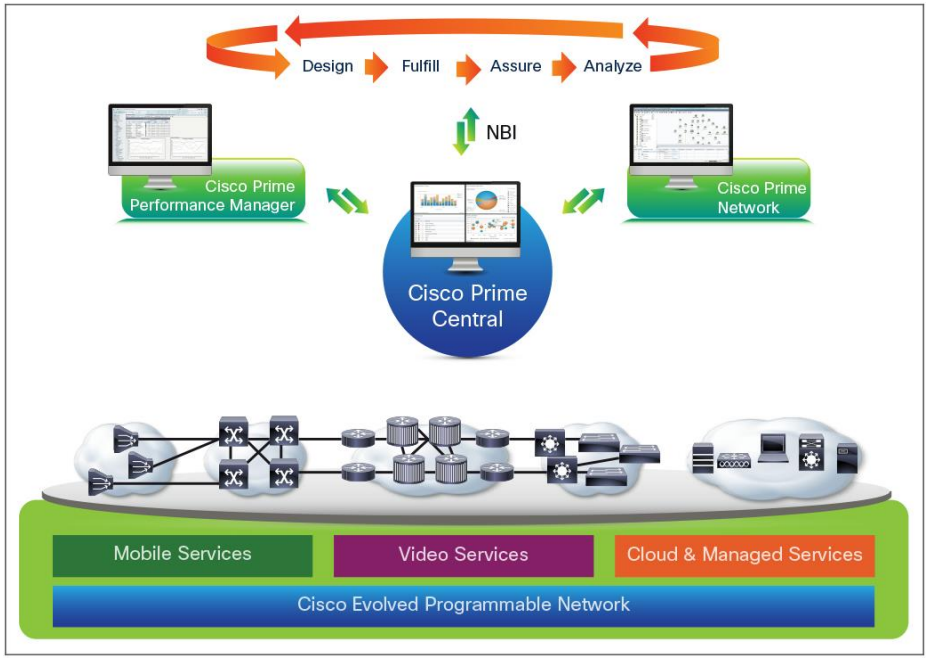


Cisco Prime

Cisco Prime provides a suite of carrier grade tools to address the challenge of operating and managing a complex network infrastructure by providing visibility into network element resources. Cisco Prime (Figure 5) consists of the following main tools:

- **Cisco Prime Infrastructure:** For management of the Cisco Universal Wi-Fi infrastructure and clients.
- **Cisco Prime Central:** Increases efficiencies in network and service lifecycle management tasks through centralized access to integrated operator workflows.
- **Cisco Prime Performance Manager:** Improves quality of service (QoS) by gathering actionable performance statistics across the entire network.
- **Cisco Prime Network:** Provides comprehensive device operation, administration, and fault management for carrier networks and services, supporting multivendor environments.

Figure 5. Cisco Prime Framework



The main use cases and features for the Cisco Universal Wi-Fi Solution 5.0 are shown in Table 1.

Table 1. Cisco Universal Wi-Fi Solution 5.0 Use Case Details

Architecture Models	Use Case Details
Packet Core integration	SAMOG-GW Based • SaMOG PMIPv6 based Split CP-DP on Wi-Fi Access Network • SaMOG based EoGRE Deployment Model • SaMOG 3G Integration Model
Internet Access	• Location Specific Web Authorization using LMA on ASR5500 • Tier2/Tier3 • ASR1K base EoGRE Deployment Model • Prime Carrier Management

Table 2. Cisco Universal Wi-Fi Additional Use Case Detail (Release 4.0 and Earlier)

Packet Core integration	**SAMOG-GW Based** • SaMOG 4G/EPC Integration with EAP-SIM Authentication • SaMOG 4G/EPC Integration with EAP-AKA Authentication **iWAG Based** • EAP-SIM authentication • EAP-SIM authentication with online charging (Gy interface-based) • EAP-PEAP • EAP-TTLS • Inter-MAG mobility for PMIPv6 • Intra-MAG mobility • PMIPv6-MAG, GTPv1, GTPv2 and Cisco ISG coexistence **eWAG Based** • Radius/DHCP proxy • Unclassified MAC or MAC-TAL • DeWAG on with EAP-SIM Authentication - DHCP mode of eWAG (DeWAG)

	PMIPv6-MAG on Wireless Controller • EAP-SIM authentication • Gx-based, web-based authentication from the LMA user device capability

Platforms and Software Releases

Table 2 summarizes Cisco Universal Wi-Fi 5.0 platforms and software releases and provides links to product information.

Table 3. Cisco Universal Wi-Fi Solution 5.0 Platforms and Software Releases

Equipment	Software Release	Product Information
Cisco Aironet Indoor Access Points 700 and 3600 for 802.11n	8.0	Cisco Aironet 700 Series Access Point data sheet Cisco Aironet 3600 Series Access Point data sheet
Cisco Aironet Indoor Access Points 1700, 2700 and 3700 for 802.11ac		Cisco Aironet 1700 Series Access Point data sheet Cisco Aironet 2700 Series Access Point data sheet Cisco Aironet 3700 Series Access Point data sheet
Cisco Aironet Outdoor Access Points 1530 and 1570	8.0	Cisco Aironet 1550 Series Access Point data sheet Cisco Aironet 1570 Series Access Point data sheet
Cisco 8510 Wireless Controller	8.0	Cisco 8510 data sheet
Cisco Mobility Services Engine	8.0	Cisco Mobility Service Engine data sheet
Cisco ASR 1000 Series	3.11	Cisco ASR 1000 data sheet
Cisco ASR 5000 Series	StarOS 16.0	Cisco ASR 5000 data sheet
Cisco Prime Infrastructure (CPI)	2.1	Cisco Prime Infrastructure data sheet
Cisco Policy Suite	PS 6.1.1	Cisco Policy Suite data sheet for Wi-Fi

Cisco Universal Wi-Fi Services Overview

The Cisco Universal Wi-Fi Service portfolio is a comprehensive set of services representing a holistic approach to the total lifecycle of service provider Wi-Fi engagements. Starting with a proof of concept, it covers the end-to-end spectrum of planning, building, optimization, and operation services, each assured by Cisco service level agreements (SLAs). These services are flexible and can be customized.

Cisco Universal Wi-Fi Proof of Concept Service:

- From a cloud-based architecture hosted in a Cisco data center, demonstration of a centralized management system, with zero-touch service fulfillment for rapid deployments of meshed access points

Cisco Universal Wi-Fi RF Plan and Build Service:

- Help to plan and deploy the RF components of the Cisco Universal Wi-Fi solution
- Analysis of architectural readiness, with guidance for selecting and prioritizing locations for Wi-Fi
- RF expertise to obtain the most from your wireless access points
- Coverage and capacity planning
- Post-deployment RF analysis help to ensure deployment success

Cisco Universal Wi-Fi Core Plan and Build Service:

- Help to plan and deploy the core components of the Cisco Universal Wi-Fi solution
- Analysis of architectural readiness and assistance with the SP Wi-Fi deployment design
- Start-to-finish deployment assistance, including mobile subscriber policy enforcement system
- Pre-deployment validation to help ensure deployment success
- Post-deployment knowledge transfers to help ensure your understanding of the solution

Cisco Universal Wi-Fi Solution Support Service (reactive):

- Expert assistance to streamline operation of the Wi-Fi architecture
- Quick isolation and remediation of unplanned service disruptions by specialists
- Tracking and identifying the root cause of disruptive incidents, providing valuable information for design changes and scaling with your mobile subscriber growth

Cisco Universal Wi-Fi Optimization Services (proactive):

- Expert analysis and recommendations for transforming your Wi-Fi architecture into a high-performing, efficient environment
- Help to create a strategy for managing all the critical components of the Cisco Universal Wi-Fi architecture using a suite of Cisco hosted network management applications
- Availability and performance optimization expertise to validate planned design changes
- Collaboration to develop a strategy for managing software releases and changes
- Continuous learning activities that help your IT staff become more self-sufficient

Cisco Universal Wi-Fi Assurance Service (preemptive):

- Extension of the measurement and analytical capabilities of your Cisco Universal Wi-Fi architecture
- Real-time monitoring of a variety of key performance indicators from Cisco network operations center
- Comprehensive analytics using fault, capacity, availability, and performance information to help ensure reliable operations

Cisco Universal Wi-Fi Operate Service (end-to-end platform management):

- Monitoring the managed devices in your environment to help ensure access points and controllers are properly activated and provisioned
- Managing incident and problem resolution
- Identifying operational trends to continually improve performance

For More Information

For more information about the end-to-end Cisco Universal Wi-Fi architecture, services, and product details, please visit cisco.com/go/spwifi.

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 C78-733416-00 12/14