CHAPTER 1

Cisco NCS Overview

This chapter describes the Cisco Unified Network Solution and the Cisco NCS. It contains the following sections:

The Cisco Unified Network Solution

The Cisco Unified Network Solution provides both wired and 802.11 wireless networking solutions for enterprises and service providers. It simplifies the deployment and management of large-scale wired and wireless LANs and enables you to create a unique best-in-class security infrastructure. The operating system manages all client data, communications, and system administration functions, performs radio resource management (RRM) functions, manages system-wide mobility policies using the operating system security solution, and coordinates all security functions using the operating system security framework.

The Cisco Unified Network Solution consists of Cisco Managed Switches, Cisco Unified Wireless Network Controllers (hereafter called *controllers*), and their associated lightweight access points controlled by the operating system, all concurrently managed by any or all of the following operating system user interfaces:

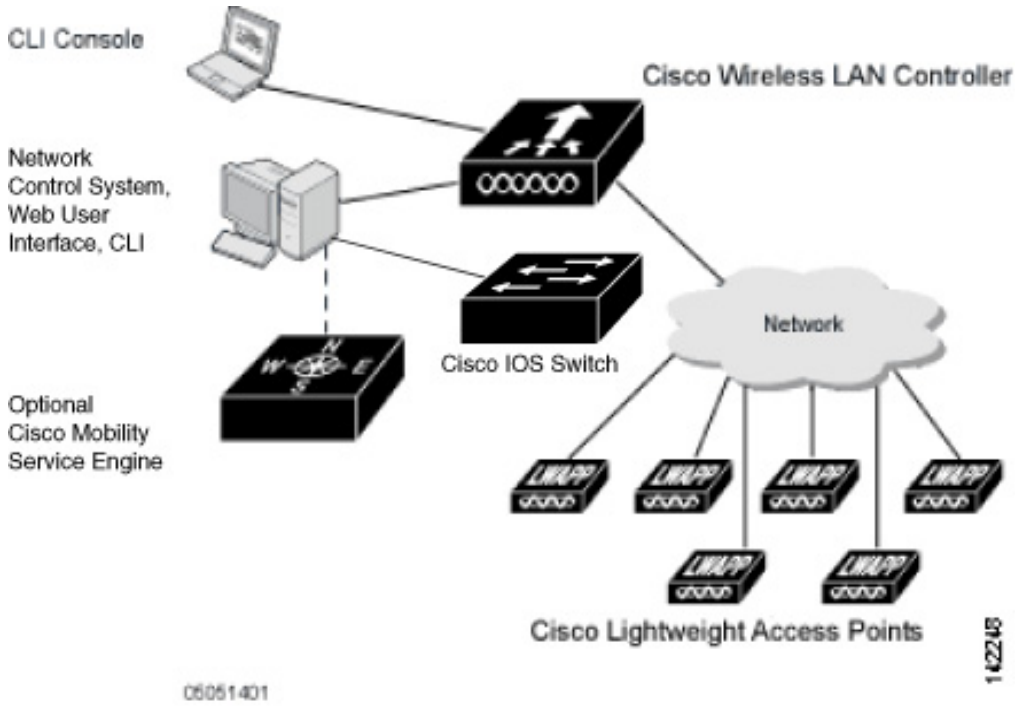
- An HTTPS full-featured web user interface hosted by Cisco controllers can be used to configure and monitor individual controllers.
- A full-featured command-line interface (CLI) can be used to configure and monitor individual controllers.
- NCS can be used to configure and monitor one or more controllers and associated access points. NCS has tools to facilitate large-system monitoring and control. It runs on predefined physical appliance and on specific virtual deployments.
- An industry-standard SNMP V1, V2c, and V3 interface can be used with any SNMP-compliant third-party network management system.

The Cisco Unified Network Solution supports client data services, client monitoring and control, and all rogue access point detection, monitoring, and containment functions. It uses lightweight access points, controllers, and the optional NCS to provide wireless services to enterprises and service providers.

Note Unless specified otherwise, information pertaining to controllers applies to all Cisco Unified Wireless Network Controllers, including but not limited to Cisco 2000 and 2100 Series Unified Wireless Network Controllers, Cisco 4100 Series Unified Wireless Network Controllers, Cisco 4400 Series Unified Wireless Network Controllers, Cisco 5500 Series Wireless LAN Controllers, and controllers within the Cisco Wireless Services Module (WiSM) and Cisco 26/28/37/38*xx* Series Integrated Services Routers.

Figure 1-1 shows the Cisco Unified Network Solution components, which can be simultaneously deployed across multiple floors and buildings.

Figure 1-1 Cisco Unified Network Solution



About NCS

The Cisco Prime Network Control System (NCS) is a Cisco LAN Solution network management tool that adds to the capabilities of the Web User Interface and the command-line interface (CLI). NCS enables you to manage a network of controllers.

NCS enables you to configure and monitor one or more controllers, switches and associated access points. NCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

NCS runs on Red Hat Linux Enterprise Server 5.X 64-bit installations. On Linux, NCS runs as a service, which runs continuously and resumes running after a reboot.

The NCS user interface requires Mozilla Firefox 3.6 or later or Internet Explorer 8 with the Chrome plugin. The administrator defines permissions from the Administration menu, which also enables the administrator to manage user accounts and schedule periodic maintenance tasks.

Note We strongly recommend you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools > Internet Options** and unselecting the **Enable third-party browser extensions** check box on the Advanced tab.

NCS simplifies controller configuration and monitoring and reduces data entry errors. NCS uses the industry-standard SNMP protocol to communicate with the controllers.

NCS also includes the Floor Plan editor which allows you to do the following:

- Vectorized bitmap campus, floor plan, and outdoor area maps.
- Add and change wall types.
- Import the vector wall format maps into the database.

Note The vector files allow the Cisco NCS RF Prediction Tool to make better RF predictions based on more accurate wall and window RF attenuation values.

NCS Licenses

The NCS is deployed through physical or virtual appliance. Use the standard License Center Graphical User Interface to add new licenses, which are locked by the standard Cisco Unique Device Identifier (UDI). When NCS is deployed on a virtual appliance, the licensing is similar to physical appliance, except instead of using a UDI, you will use a Virtual Unique Device Identifier (VUDI).

Note If you want to move licenses from one physical appliance to another, you will need to call the Licensing TAC and rehost the licenses to a new UDI.

NCS License is recognized by the SKU, which is usually attached to every purchase order to clearly identify which software or package is purchased by a customer. The different NCS license options are described in this section. This section contains the following topics:

NCS Evaluation License

NCS can be used in a lab, or in an evaluation with the following license: NCS-DEMO-10. This provides an evaluation license for 10 number of devices, and for a duration of 30 days. If you need a custom device count or duration, please contact your Cisco representative.

NCS Device Count License

NCS uses a single-tier licensing structure that includes all features and functionality in a single tier. Part numbers are purchased based on number of devices to be managed. Part numbers are available to support 50, 100, 500, 1000, 2500, 5000 or 10000 devices; where both an AP and a Switch are considered a single managed device.

NCS Device Count license is of the following:

You can either choose physical appliance or virtual appliance for NCS setup. If you choose the option of ordering the physical appliances, you receive PRIME-NCS-APL-K9 along with a PAK for the license quantity you ordered. That is, if you are ordering L-NCS-1.0-1K with PRIME-NCS-APL-K9 SKU, you receive a physical NCS appliance, plus a PAK for managing 1000 devices.

If you choose the virtual appliance option, download the virtual NCS image and get the L-NCS-1.0-X PAK mailed to you once it has been ordered.

If you want to add more devices into your network, you can get the L-NCS-1.0-X-ADD SKU for X devices. The L-NCS-1.0-X-ADD are identical licenses supplied. The only difference is that these SKUs are for additional licenses and they do not come with physical or virtual activation.

The larger license quantities, specifically 1K, 2.5K, 5K, and 10K are shipped in smaller increments to allow the licenses to be split across different NCS instances.

NCS Upgrade License

The L-NCS-2.0-UPGRADE-X-ADD SKU is used to upgrade NCS 1.X to NCS 2.X. Upgrades come in the following counts: 50, 100, and 500, 1K, 2.5K, 5K and 10K devices.

Once the lower-license level count is equaled or exceeded, the system considers the license for the next level. At this point new, lower-level licenses are not allowed, but additional higher-level licenses are allowed.

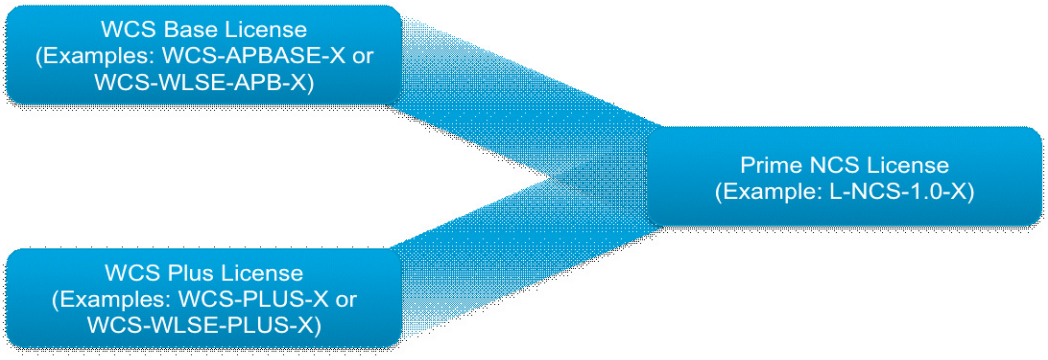
Note that a higher-level system allows lower-level licenses as long as there is no higher-level license or upgrade license present. This allows you to migrate licenses; take care to migrate the licenses in order from the lowest version to the highest version.

Consider a case where you are running NCS 3.0 and you have NCS 1.0, NCS 2.0, and NCS 3.0 licenses. You need to replace the current appliance with a new one and want to move the licenses, but not as part of a backup/restore process. You must first load all NCS 1.0 licenses, an NCS 2.0 Upgrade, the NCS 2.0 licenses, an NCS 3.0 Upgrade, and then all the NCS 3.0 licenses for the licenses to be applied correctly.

NCS Migration License

The NCS uses a single-tier license model. When Cisco WCS BASE or WCS PLUS licenses are being migrated, licenses will be mapped to the new Cisco Prime NCS single-tier model. This is a two stage process.

This section contains the following topics:



The migration licenses that are generated from the Cisco migration portal basically have two levels of plus or base with a count, additionally there could be a spectrum expert license. These licenses are mapped to NCS 1.0 licenses of equivalent counts. For example, a WCS 7.0 Base 500 with Spectrum Expert licenses can be converted to an NCS 1.0 500 device license.

Obtaining the XML file from Existing WCS Deployment

To Obtain the XML file from the existing WCS deployment, follow these steps:

Step 1 Log in to the WCS server (version 7.0.164.0 or higher) and choose **Administration > License Center**.

Note Apply the L-WCS-NCS1-M-K9 License first, before adding the licenses migrated from your WCS installation.

Step 2 From the left sidebar menu, choose **File > WCS File**.

Step 3 Select the WCS license you want to export, and click the **Export** button and save the XML file generated to your local machine.

Uploading the XML file to the Cisco Migration Portal

To upload the generated XML file to the Cisco Migration Portal, follow these steps:

Step 1 Go to: http://www.cisco.com/go/license.

Step 2 Scroll down to the Migration section and click the **Register for Upgrade/Migrate License** link.

Step 3 Choose **NCS 1.0** from the drop-down list, and click **Go to Upgrade/Migration License Portal**.

Step 4 Enter your Product ID and Serial Number.

Step 5 Open the generated XML file in a text editor and copy the contents of the file to the License Text box.

Step 6 Accept the end-user license agreement (EULA), verify your contact information, and click **Continue**.

Step 7 The Cisco Migration Portal generates the new license file and will e-mail the license to you.

Applying the New License to Cisco Prime NCS

As mentioned in step 7 under the "Uploading the XML file to the Cisco Migration Portal" section on page 1-5, the license file is distributed to you in an email from Cisco. Do not edit the contents of the .lic file in any way or you will render the file useless

To apply the New License to Cisco Prime NCS, follow these steps:

Step 1 Log in to the Cisco NCS.

Step 2 Choose **Administration > License Center**.

Step 3 Choose **File > NCS Files.**

Step 4 Click **Add**, and then choose a license file.

Step 5 Click **OK**.

Note Prior to migrating WCS licenses on Cisco Wireless LAN Solution Engine (WLSE), the solution needs to be running Cisco Wireless Control System 7.0.164.0 or later.

Note Cisco WLSE hardware will not support Cisco Prime NCS 1.0. Customers using the WLSE hardware to run WCS are required to purchase either the physical appliance option, or deploy the virtual appliance on your own hardware.

Cisco Unified Network Components

Cisco Unified Network Solutions ensures that your business achieves the highest level of network security and versatility. Cisco Unified Network Solutions empowers your network with the ability to offer secure wireless networking, either within your office for increased mobility or bridging between your office buildings. The following are the different network components in the Cisco Unified Network Solutions:

Cisco Prime NCS

With NCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and wired and wireless LAN systems management. Robust graphical interfaces make wired and wireless LAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make NCS vital to ongoing network operations.

WLAN Controllers

The WLAN Controllers is a highly scalable and flexible platforms that enables system wide services for mission-critical wireless in medium to large-sized enterprises and campus environments. Designed for 802.11n performance and maximum scalability, the WLAN controllers offer enhanced uptime with the ability to simultaneously manage from 5000 access points to 250 access points; superior performance for reliable streaming video and toll quality voice; and improved fault recovery for a consistent mobility experience in the most demanding environments.

NCS supports the Cisco wireless controllers that help reduce the overall operational expenses of Cisco Unified Networks by simplifying network deployment, operations, and management. The following WLAN Controllers are supported in NCS:

- Cisco 2700 Series Location Appliance
- Cisco 2000 Series Wireless LAN Controllers
- Cisco 2100 Series Wireless LAN Controllers
- Cisco 2500 Series Wireless Controllers
- Cisco 4400 Series Wireless LAN Controllers
- Cisco 5500 Series Wireless Controllers
- Catalyst 3750G Wireless LAN Controller Switches
- Cisco Wireless Services Modules (WiSMs) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Services Module 2 (WiSM2) for Cisco Catalyst 6500 Series Switches
- Cisco Wireless Controller on SRE for ISR G2 Routers
- Cisco Flex 7500 Series Wireless Controllers
- Cisco WLAN Controller Network Modules for Cisco Integrated Services Routers

Access Points

NCS supports the industry-leading performance access points for highly secure and reliable wireless connections for both indoor and outdoor environments. NCS supports a broad portfolio of access points targeted to the specific needs of all industries, business types, and topologies.

The following access points are supported in NCS:

- Cisco Aironet 1000, 1040, 1100, 1130, 1140, 1200, 1230, 1240, 1250, 1260, 1310, 1500, 1524, 3500i, 3500e, and 3500p Series Lightweight Access Points.
- Cisco Aironet 801, 1040, 1100, 1130, 1141, 1142, 1200, 1240, 1250, and 1260 Autonomous Access Points.
- Cisco 600 Series OfficeExtend Access Points.
- Cisco Aironet Access Points running Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points protocol (CAPWAP).
- Cisco 1550 Series Mesh Access Points.

Embedded Access Points

NCS supports the AP801, which is the integrated access point on the Cisco 800 Series Integrated Services Routers (ISRs). This access point uses a Cisco IOS software image that is separate from the router Cisco IOS software image. It can operate as an autonomous access point that is configured and managed locally, or it can operate as a centrally managed access point using CAPWAP or LWAPP protocol. The AP801 is preloaded with both an autonomous Cisco IOS release and a recovery image for the unified mode.

When you want to use the AP801 with a controller, you must enable the recovery image for the unified mode on the access point by entering the CLI command on the router in privileged EXEC mode: **service-module wlan-ap 0 bootimage unified**.

Note If the **service-module wlan-ap 0 bootimage unified** command does not work, make sure that the software license is still current.

After enabling the recovery image, enter the CLI command on the router to shut down and reboot the access point: **service-module wlan-ap 0 reload**. After the access point reboots, it discovers the controller, downloads the full CAPWAP or LWAPP software release from the controller, and acts as a lightweight access point.

Note To use the CLI commands mentioned previously, the router must be running Cisco IOS Release 12.4(20)T or later. If you experience any problems, refer to the "Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode" section in the Integrated Services Router configuration guide at this URL: http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/admin_ap.html

To support CAPWAP or LWAPP, the router must be activated with at least the Cisco Advanced IP Services IOS license-grade image. A license is required to upgrade to this Cisco IOS image on the router. See this URL for licensing information:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html

After the AP801 boots up with the recovery image for the unified mode, it requires an IP address to communicate with the controller and to download its unified image and configuration from the controller. The router can provide DHCP server functionality, the DHCP pool to reach the controller, and setup option 43 for the controller IP address in the DHCP pool configuration. Use the following configuration to perform this task.

```
ip dhcp pool pool_name
    network ip_address subnet_mask
    dns-server ip_address
    default-router ip_address
    option 43 hex controller_ip_address_in_hex
Example:
ip dhcp pool embedded-ap-pool
    network 209.165.200.224 255.255.255.224
    dns-server 209.165.200.225
    default-router 209.165.200.226
    option 43 hex f104.0a0a.0a0f /* single WLC IP address (209.165.201.0) in hex format */
```

The AP801 802.11n radio supports lower power levels than the 802.11n radio in the Cisco Aironet 1250 series access points. The AP801 stores the radio power levels and passes them to the controller when the access point joins the controller. The controller uses the supplied values to limit the user configuration.

The AP801 can be used in hybrid-REAP mode. See the "Configuring Hybrid REAP" section on page 12-1 for more information on hybrid REAP.

Note For more information about AP801, refer to the documentation for the Cisco 800 Series ISRs at this URL:http://www.cisco.com/en/US/products/hw/routers/ps380/tsd_products_support_series_home.html.

Access Point Communication Protocols

In controller software release 5.2 or later, Cisco lightweight access points use the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other lightweight access points on the network. Controller software releases prior to 5.2 use the Lightweight Access Point Protocol (LWAPP) for these communications.

CAPWAP, which is based on LWAPP, is a standard, interoperable protocol that enables a controller to manage a collection of wireless access points. CAPWAP is being implemented in controller software release 5.2 for these reasons:

- To provide an upgrade path from Cisco products that use LWAPP to next-generation Cisco products that use CAPWAP
- To manage RFID readers and similar devices
- To enable controllers to interoperate with third-party access points in the future

LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. For example, the controller discovery process and the firmware downloading process when using CAPWAP are the same as when using LWAPP. The one exception is for Layer 2 deployments, which are not supported by CAPWAP.

Deployments can combine CAPWAP and LWAPP software on the controllers. The CAPWAP-enabled software allows access points to join either a controller running CAPWAP or LWAPP. The only exception is the Cisco Aironet 1140 Series Access Point, which supports only CAPWAP and therefore joins only controllers running CAPWAP.

Note The Cisco Aironet 1140 series and 3500 series access points associate only with CAPWAP controllers that run WLC versions 7.0 or later.

This section contains the following topics:

Guidelines and Restrictions for Using CAPWAP

- CAPWAP and LWAPP controllers cannot be used in the same mobility group. Therefore, client mobility between CAPWAP and LWAPP controllers is not supported.
- If your firewall is currently configured to allow traffic only from access points using LWAPP, you must change the rules of the firewall to allow traffic from access points using CAPWAP.

- Make sure that the CAPWAP ports are enabled and are not blocked by an intermediate device that could prevent an access point from joining the controller.
- Any access control lists (ACLs) in your network might need to be modified if CAPWAP uses different ports than LWAPP.

Cisco Wireless LAN Controller Autodiscovery

Controller Autodiscovery is limited to the Cisco WLAN Solution mobility group subnets defined by the operator.

The Cisco Wireless LAN Controller Autodiscovery:

- Allows operators to search for a single controller by IP address.
- Finds the controller on the network within the specified IP address range.
- Automatically enters the controller information into the Cisco NCS database.

Note Controller Autodiscovery can take a long time in a Class C address range. Because of the large number of addresses in a Class B or Class A range, we recommend that you do not attempt Autodiscovery across Class B or Class A ranges.

As access points associate with a controller, the controller immediately transmits the access point information to Cisco NCS, which automatically adds the access point to the database.

Once the access point information is added to the Cisco NCS database, operators can add the access point to the appropriate spot on a Cisco NCS user interface map.

NCS Services

The IT departments within organizations are tasked with meeting increased bandwidth and performance demands, managing a proliferation of new mobile devices, while guaranteeing network access, availability, and regulatory compliance.

Cisco and its partners can work with IT staff to assist with migration to the Cisco Unified Network, making it easier to manage a secure, high-performance, and integrated wired and wireless network that incorporates rich media and diverse mobile devices, including Wi-Fi-enabled phones and tablets.

NCS provides the following Services:

- Cisco Context Aware Service Solution, page 1-10
- Cisco Identity Service Engine Solution, page 1-11
- Cisco Adaptive Wireless Intrusion Prevention Service, page 1-12

Cisco Context Aware Service Solution

Context Aware Service (CAS) provides the capability for a Wi-Fi 802.11a/b/g/n network to determine the location of a person or object with an active Wi-Fi device, such as a wireless client or active RFID tag and/or associated data that can be passed by the end point through the wireless infrastructure to an upstream client.

Context Aware Service (CAS) allows a Mobility Services Engine (MSE) to simultaneously track thousands of mobile assets and clients by retrieving contextual information such as location and availability from Cisco access points.

The collected contextual information can be viewed in GUI format in the NCS User Interface, the centralized WLAN management platform. NCS is the management system that interfaces with the MSE and serves user interface (UI) for the services that the MSE provides.

After installation of MSE and initial configurations are complete, the MSE can communicate with multiple Cisco wireless LAN controllers to collect operator-defined contextual information. You can then use the associated NCS to communicate with each MSE to transfer and display selected data.

You can configure the MSE to collect data for clients, switches, rogue access points, rogue clients, mobile stations, and active RFID asset tags.

With Context-Aware Location Services, administrators can determine the location of any 802.11-based device, as well as the specific type or status of each device. Clients (associated, probing, and so on.), rogue access points, rogue clients, and active tags can all be identified and located by the system. See Context Aware Mobility Solution Deployment Guide for more information.

Note One MSE can be managed by only one NCS, that is, a single MSE cannot be managed by multiple NCS's, but a single NCS can manage multiple MSEs. When the number of devices to be managed exceeds the capacity of a single MSE, you need to deploy multiple, independent MSEs.

Cisco Identity Service Engine Solution

The Cisco Identity Services Engine (ISE) is a next-generation identity and policy-based network access platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations.

The Cisco ISE provides a single console where authentication, authorization, posture, guest, and profiling policies can be created and managed. In addition, policy elements can now be reused across all services, reducing the number of tasks and overhead and bringing consistency to the enterprise.

The Cisco ISE gathers information from devices, the infrastructure, and services to enable organizations to build richer contextual policies that can be enforced centrally across the network. The ISE tracks all clients and devices connected to the network, acting as a single source of information for connected user and device identity and location, as well as the health of the endpoint.

The ability to discover, identify, and monitor all IP-enabled endpoint devices gives IT teams complete visibility of both users and "headless" devices on the corporate network.

The Cisco ISE combines AAA, posture, profiling, and guest management capabilities in a single appliance to enforce dynamic access control. The Identity Services Engine can be deployed across the enterprise infrastructure, supporting 802.1x wired, wireless, and VPN networks.

NCS manages the wired and the wireless clients in the network. When Cisco ISE is used as a RADIUS server to authenticate clients, NCS collects additional information about these clients from Cisco ISE and provides all client relevant information to NCS to be visible in a single console.

When posture profiling is enforced in the network, NCS talks to Cisco ISE to get the posture data for the clients and displays it along with other client attributes. When Cisco ISE is used to profile the clients or an endpoint in the network, NCS collects the profiled data to determine what type of client it is, whether it is an iPhone, iPad, an Android device, or any other device.

Cisco ISE is assisting NCS to monitor and troubleshoot client information, and displays all the relevant information for a client in a single console.

Cisco Adaptive Wireless Intrusion Prevention Service

Maintain a constant awareness of your RF environment to minimize legal liability, protect your brand reputation, and assure regulatory compliance.

Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution.

Cisco Adaptive Wireless Intrusion Prevention Service (wIPS) performs rogue access point, rogue client, and ad-hoc connection detection and mitigation, over-the-air wireless hacking and threat detection, security vulnerability monitoring, performance monitoring and self-optimization, network hardening for proactive prevention of threats and complete wireless security management and reporting.

Cisco's wIPS is made up of the following components that work together to provide a unified security monitoring solution.

- A mobility services engine (MSE) running wIPS software-Serves as the central point of alarm aggregation for all controllers and their respective wIPS monitor mode access points. Alarm information and forensic files are stored on the mobility services engine for archival purposes.
- An wIPS monitor mode access point-Provides constant channel scanning with attack detection and forensics (packet capture) capabilities.
- Local mode access point-Provides wireless service to clients in addition to time-sliced rogue scanning.
- Wireless LAN Controller-Forwards attack information received from wIPS monitor mode access points to the mobility services engine and distributes configuration parameters to access points.
- Network Control System-Provides a centralized management platform for the administrator to configure the wIPS Service on the mobility services engine, push wIPS configurations to the controller, and configure access points in wIPS monitor mode. NCS is also used to view wIPS alarms, forensics, reporting, and to access the attack encyclopedia.