Identity-Based Networking Services

Identity-Based Networking Services Overview

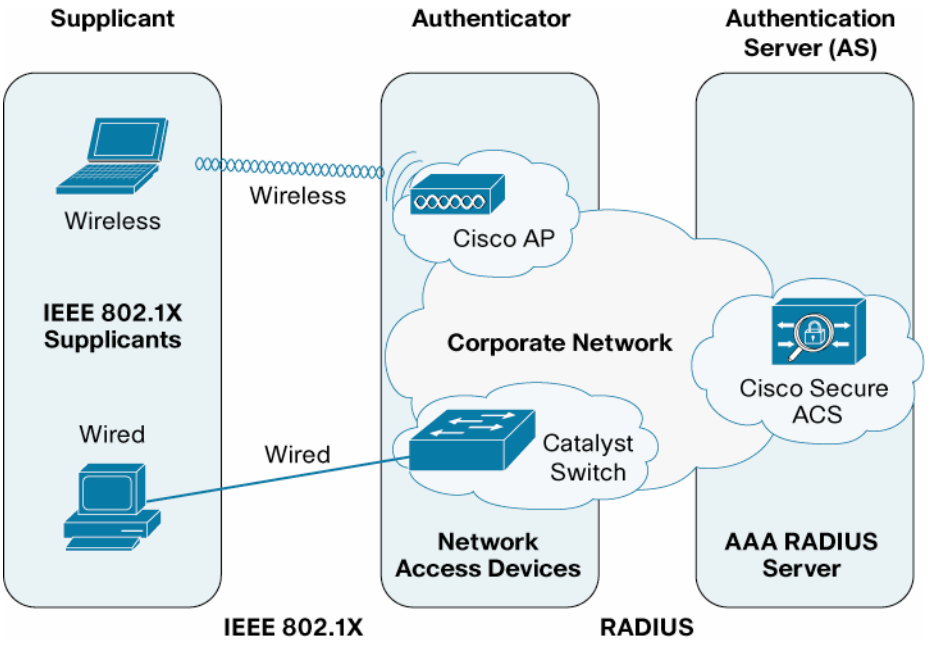
Cisco® Identity-Based Networking Services (IBNS) is an integrated solution that offers authentication, access control, and user policy enforcement to help secure network connectivity and resources. IBNS helps customers increase user productivity, reduce operating costs, increase visibility, and enforce policy compliance.

The three basic components of IBNS are

1. Cisco Catalyst® switches (or wireless access points)
2. Cisco Secure Access Control System (ACS)
3. Cisco Secure Services Client (SSC)

These components, together with an existing identity management infrastructure such as Microsoft Active Directory or LDAP-capable directory, provide policy enforcement at the network edge.

Figure 1. Basic IBNS Component



Cisco IBNS is an easy-to-deploy identity solution that incorporates extensive Cisco testing efforts, including feature development, regression testing, and solutions testing. The IBNS solution is based on real-life customer deployments and provides the following benefits:

- Strong authentication of users and devices on wired and wireless LANs
- Identity feature consistency across Cisco Catalyst switches
- Tight integration between various components in the solution: the authenticator, authentication server, and supplicant

- Architecture that allows a phased deployment approach that gradually introduces identity-based access control
- A solution that has been tested in-house and then hardened with alpha and beta customer testing

The solution also includes deployment and configuration guides.

- Cisco IBNS uses the following software versions:
- Cisco Catalyst 3000 Series Switches: Cisco IOS® Software Release 12.2(50)SE
- Cisco Catalyst 4500 Series Switches: Cisco IOS Software Release 12.2(50)SG
- Cisco Catalyst 6500 Series switches: Cisco IOS Software Release 12.2(33)SXI
- Cisco Secure Access Control System (ACS) Version 5.0
- Cisco Secure Services Client (SSC) Version 5.1
- Microsoft Windows XP and Vista supplicant

Cisco IBNS offers a phased, scenario-based deployment strategy so that customers can roll out the solution with minimal impact to end users. Monitoring, low-impact, and high security deployment modes apply specific combinations of features and configurations to satisfy a particular set of use cases (Table 1). Instead of starting "from scratch," you can follow the guidelines for a particular deployment scenario and then, if necessary, customize it to suit your network requirements.

Table 1. Deployment Modes for Cisco IBNS

Mode	Description
Monitor mode	Provides visibility into access on your network. Includes a pre-access-control deployment assessment and a policy evaluation
Low-impact mode	Reduces known issues with other protocol timeouts and networked services. Enables differentiated access through policy-driven downloadable access control lists (dACLs) based on identity or group.
High security mode	Provides the highest level of LAN-based access security for environments where access cannot be granted without authentication.

For more information about Cisco IBNS, please visit http://www.cisco.com/go/ibns.

Cisco IBNS Software Features

The following Cisco IBNS features are available across Cisco Catalyst switches:

- **Flexible authentication sequencing:** This feature provides a flexible fallback mechanism among IEEE 802.1X, MAC authentication bypass (MAB), and web authentication methods. It also allows switch administrators to control the sequence of the authentication methods. This simplifies identity configuration by providing a single set of configuration commands to handle different types of endpoints connecting to the switch ports. In addition, this feature allows users to configure any authentication method on a standalone basis. For example, MAB can be configured without requiring IEEE 802.1X configuration.
- **IEEE 802.1X with open access:** This feature allows 802.1X and MAB authentication without enforcing any kind of authorization. There is no impact to users or endpoints: They continue to get exactly the same kind of network access that they did before you deployed IBNS. Having visibility into the network gives you insight into who is getting access, who has an operational 802.1X client, who is already known to existing identity stores, and who has credentials, as well as other information.
- **IEEE 802.1X, MAB, and web authentication with downloadable ACLs:** This feature allows ACLs to be downloaded from the Cisco Secure ACS as policy enforcement after authentication using IEEE 802.1X, MAC authentication bypass, or web authentication.

- **Cisco Discovery Protocol enhancement for second-port disconnect:** For IP telephony environments, Cisco Discovery Protocol is enhanced to add a new Type-Length-Value (TLV) for the IP phone to indicate when a PC disconnects from the IP phone. Upon receiving this notification, the switch can clear the authentication session for the PC
- **Inactivity timer for IEEE 802.1X and MAB:** With this local inactivity timer for IEEE 802.1X and MAB, if the authenticated devices stay idle for longer than the defined period, the switch resets the security record of the devices.
- **Multidomain authentication:** This feature allows an IP phone (Cisco or non Cisco) and a PC to authenticate on the same switch port while it places them on appropriate voice and data VLANs.
- **IEEE 802.1X with multiauth:** Multiple authentications allows more than one host to authenticate on an IEEE 802.1X-enabled switch port. With multiauth, each host must authenticate individually before it can gain access to the network resources; this is necessary in a virtualized environment.
- **Centralized web authentication:** This feature allows the switch to redirect users using HTTP URL redirection to a central web authentication server or a guest access server for authentication before accessing the network resources.
- **Common session ID:** IEEE 802.1X and MAB will use a session ID identifier for all 802.1X and MAB authenticated sessions. This session ID will be used for all reporting purposes, such as show commands, MIBs, syslog, and RADIUS messages, and allows users to distinguish messages for one session from others.

The following Cisco IBNS features are available on Cisco Secure ACS 5.0:

- A distributed deployment model that enables large-scale deployments, such as identity deployment in a campus environment
- A powerful, attribute-driven rules-based policy model that addresses complex policy needs in a flexible manner
- Integrated advanced monitoring, reporting, and troubleshooting capabilities for maximum control and visibility
- Improved integration with external identity and policy databases, including Windows Active Directory and Lightweight Directory Access Protocol (LDAP)-accessible databases, simplifying policy configuration and maintenance

The following Cisco IBNS features are available on the Cisco Secure Services Client (SSC):

- A wireless interface that can be disabled when a wired connection is present, eliminating unwanted wireless bridging to the wired network
- An 802.1X identity-based network security framework
- Configuration and enforcement of access policies to protect corporate resources and assets
- Authenticated access to 802.1X wired and wireless LANs

Cisco Secure Access Control System (ACS) 5.0 Ordering Information

Cisco Secure ACS is a next-generation platform for centralized network identity and access control. Cisco Secure ACS 5.0 features a simple yet powerful rule-based policy model and a new, intuitive management interface designed for optimum control and visibility.

Cisco Secure ACS 5.0 is offered as a dedicated appliance, the Cisco 1120 Secure Access Control System, and as software for customers building a virtual infrastructure using VMWare ESX. The appliance and software versions of Cisco Secure ACS 5.0 support the same features. For system specifications, please view the data sheet at http://www.cisco.com/go/acs.

Table 2 lists the part numbers for Cisco Secure ACS hardware and software.

Table 2. Cisco Secure ACS Ordering Information

Part Number	Description
CSACS-1120-K9	Cisco Secure 1120 Appliance with preinstalled Cisco Secure ACS 5.0 and Base license
CSACS-5.0-IENVM-K9	Cisco Secure ACS 5.0 software for VMWare with Base license
CSACS-5-MON-LIC=	Cisco Secure ACS 5.0 Advanced Monitoring and Reporting add-on license
CSACS-5-LRG-LIC=	Cisco Secure ACS 5.0 Large Deployment add-on license

Cisco Secure Services Client Ordering Information

The Cisco Secure Services Client is a software application that enables businesses of all sizes to deploy a single authentication framework across endpoint devices for access to both wired and wireless networks. The Cisco Secure Services Client solution delivers simplified management, robust security, and lower total cost of ownership.

Table 3 lists the part numbers for Cisco Secure Services Client Version 5.1. To download the Cisco Secure Services Client, visit the Cisco Ordering Home Page.

Table 3. Cisco SSC Ordering Information

Part Number	Description
AIR-SC5.0-XP2K	Cisco Secure Services Client (Windows XP/2000)
AIR-SSC-VISTA	Cisco Secure Services Client (Windows Vista)
AIR-SSCFIPS-DRV	Cisco Secure Services Client FIPS drivers (Windows XP only)

Cisco NAC Profiler Ordering Information

The Cisco NAC Profiler enhances the deployment and administration of Cisco IBNS by maintaining a real-time list of all network-attached endpoints, such as IP phones and networked printers.

Table 4. Cisco NAC Profiler Ordering Information

Part Number	Description
NAC3350-PROF-K9	Cisco NAC Profiler Server
NAC3350-CLT-K9=	Cisco NAC Collector License for Cisco NAC 3350 Appliances
NAC3310-CLT-K9=	Cisco NAC Collector License for Cisco NAC 3310 Appliances
NAC3310-PROF-K9	NAC 3310 Profiler-max up to 5K devices
NAC3310-1000C-K9	NAC 3310 Collector-max 1000 devices
NAC3350-3000C-K9	NAC 3350 Collector-max 3000 devices
NAC3350-5000C-K9	NAC 3350 Collector-max 5000 devices
NAC3350-7000C-K9	NAC 3350 Collector-max 7000 devices

For more information on how to order Cisco NAC Profler, including fail-over and device licenses, please visit http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/prod_bulletin0900aecd806b7d69.html

Cisco IBNS Feature Availability for Cisco Catalyst Switches

Table 5 describes the new Cisco IOS® Software-based IBNS features available with enterprise-class Cisco Catalyst switches. All Cisco IOS Software releases are available for order now. Customers interested in purchasing these products can place orders through their normal sales channels.

Table 5. New Cisco IBNS Features for Enterprise-Class Switches

Feature	Cisco IOS Software Release for Catalyst 3000 Series Switches	Cisco IOS Software Release for Catalyst 4500 Series Switches	Cisco IOS Software Release for Catalyst 6500 Series Switches
Flexible authentication sequencing	12.2(50)SE	12.2(50)SG	12.2(33)SXI
IEEE 802.1X with open access	12.2(50)SE	12.2(50)SG	12.2(33)SXI
IEEE 802.1X, MAB, and web authentication with downloadable ACL	12.2(50)SE	12.2(50)SG	12.2(33)SXI
Cisco Discovery Protocol enhancement for second-port disconnect	12.2(50)SE	12.2(50)SG	12.2(33)SXI
Inactivity timer for IEEE 802.1X and MAB	12.2(50)SE	12.2(50)SG	12.2(33)SXI
Multidomain authentication	12.2(25)SEC	12.2(31)SG	12.2(33)SXI
IEEE 802.1X with multiauth	12.2(50)SE	12.2(50)SG	12.2(33)SXI
Centralized web authentication	12.2(50)SE	12.2(50)SG	12.2(33)SXI
Common session ID	12.2(50)SE	12.2(50)SG	12.2(33)SXI

For More Information

For more information about Cisco products, please contact your Cisco account manager or Cisco channel partner.

For more information about Cisco IBNS, go to: http://www.cisco.com/go/ibns

For more information about Cisco Catalyst switches, go to: http://www.cisco.com/go/switches

For more information about Cisco Secure ACS, go to: http://www.cisco.com/go/acs

For more information about Cisco SSC, go to: http://www.cisco.com/en/US/products/ps7034/index.html

For more information about the Cisco NAC Profiler, go to: http://www.cisco.com/en/US/products/ps8464

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 C78-542121-00 06/09