Identity Based Networking Services Overview

Cisco Identity Based Networking Services (IBNS) provides a policy and identity-based framework in which edge devices can deliver flexible and scalable services to subscribers. This module provides information about what Cisco IBNS is and its features and benefits.

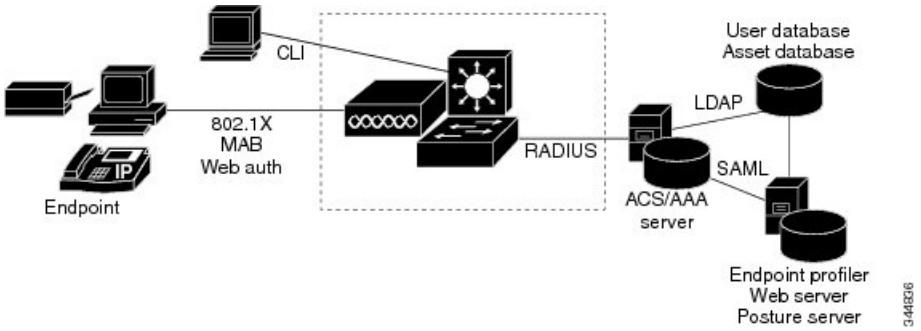
- Understanding Cisco Identity Based Networking Services, on page 1
- Features in Cisco Identity Based Networking Services, on page 2
- Benefits of Cisco Identity Based Networking Services, on page 2
- Web Authentication Support for Common Session ID, on page 3
- Web Authentication Support of IPv6, on page 3
- IP Device Tracking, on page 3
- Feature History for Cisco Identity Based Networking Services Overview, on page 3

Understanding Cisco Identity Based Networking Services

Cisco IBNS feature provides a policy and identity-based framework in which edge devices can deliver flexible and scalable services to subscribers. Cisco IBNS provides an identity-based approach to access management and subscriber management. It offers a consistent way to configure features across technologies, a command interface that allows easy deployment and customization of features, and a robust policy control engine with the ability to apply policies defined locally or received from an external server to enforce policy in the network.

The figure below illustrates a typical deployment of Cisco IBNS in a physically distributed enterprise with a campus, branch offices, and remote workers.

Figure 1: Sample Deployment of Cisco IBNS



By default, the **access-session closed** command is enabled in IBNS 1.0 and as a result, devices cannot perform any pre-authentication actions on the network when using IBNS 1.0. By default, authentication is open in IBNS 2.0, and devices can perform pre-authentication actions on the network. To close authentication on IBNS 2.0, configure the **access-session closed** command in interface-port configuration mode.

Features in Cisco Identity Based Networking Services

Cisco IBNS includes the following features:

- Cisco common classification policy language (C3PL)-based identity configuration
- Concurrent authentication methods on a single session, including IEEE 802.1x (dot1x), MAC authentication bypass (MAB), and web authentication
- Downloadable identity service templates
- Extended RADIUS change of authorization (CoA) support for querying, reauthenticating, and terminating a session, port shutdown and port bounce, and activating and deactivating an identity service template.
- Local authentication using Lightweight Directory Access Protocol (LDAP)
- Locally defined identity control policies
- Locally defined identity service templates
- Per-user inactivity handling across methods
- Web authentication support of common session ID
- Web authentication support of IPv6

Benefits of Cisco Identity Based Networking Services

Identity-based solutions are essential for delivering access control for disparate groups such as employees, contractors, and partners while maintaining low operating expenses. Cisco IBNS provides a consistent approach to operational management through a policy and identity-based infrastructure leading to faster deployment of new features and easier management of switches.

Cisco IBNS provides the following benefits:

- An identity-based framework for session management.
- A robust policy control engine to apply policies defined locally or received from an external AAA server.
- Faster deployment and customization of features across access technologies.
- A simpler and consistent way to configure features across access methods, platforms, and application domains.

Web Authentication Support for Common Session ID

Cisco IBNS allows a single session identifier to be used for web authentication sessions in addition to all 802.1X and MAB authenticated sessions for a client. This session ID is used for all reporting purposes such as show commands, MIBs, and RADIUS messages and allows users to distinguish messages for one session from messages for other sessions. This common session ID is used consistently across all authentication methods and features applied to a session.

Web Authentication Support of IPv6

Cisco IBNS introduces IPv6 support for web authentication. IPv6 is supported for web authentication only when Cisco IBNS is explicitly configured. This means that you must permanently convert your configuration to the Cisco common classification policy language (C3PL) display mode by specifically configuring a Cisco IBNS command such as the **policy-map type control subscriber** command.

IP Device Tracking

IP device tracking can be configured using the Switch Integrated Security Features (SISF) policy. Use the tracking enable command in device tracking configuration mode, to configure device tracking using SISF policy. Use the **show device-tracking** command to display the device tracking configuration.

The following is the sample configuration for device tracking.

```
Device(config)# device-tracking policy sisf_policy
Device(config-device-tracking)# tracking enable
Device(config-device-tracking)# exit
Device(config)# interface GigabitEthernet 3/0/1
Device(config-if)# switchport mode access
Device(config-if)# device-tracking attach-policy sisf_policy
Device(config-if)# end
```

Feature History for Cisco Identity Based Networking Services Overview

This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature History for Cisco Identity Based Networking Services Overview

Release	Feature Name	Feature Information
Cisco IOS XE Everest 16.5.1a	Web Authentication Support of Common Session ID	Allows a single session identifier to be used for all web authentication sessions in addition to 802.1X and MAB authenticated sessions.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to https://cfnng.cisco.com.