Cisco Identity Based Networking Services 2.0 At-a-Glance

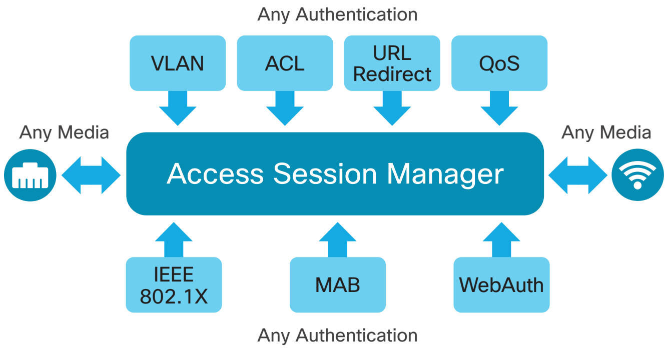
Value of Cisco Identity Based Networking Services (IBNS) 2.0

With the evolution of bring-your-own-device (BYOD) initiatives, a highly mobile global workforce, and virtualized and hybrid data centers, today's enterprise networks have become literally borderless. With diverse work groups–contractors, regular employees, partners, etc.–needing to share the same network infrastructure, a secure and scalable way of granting network access based on identity is a high priority. Network authentication with IEEE 802.1X is fundamental for such deployments, but to address these trends, a more flexible, scalable, and comprehensive solution is required. The current deployment challenges demand an extensible framework that builds on traditional identity-based networking services and can provision enhanced authentication flexibility, local authorizations, role-based access control (RBAC), consistent policy-based access, and the capability to use IPv6 endpoints. Cisco provides a solution: Cisco IBNS 2.0.

Cisco IBNS 2.0

The advanced access session manager, a core component of the Cisco Policy-Aware IBNS architecture, provides a policy- and identity-based framework for flexible and scalable services to secure-access clients (Figure 1). This framework enables provisioning for any authentication with any authorization on any media: wired or wireless. The enhanced policy engine is equipped with a new set of capabilities, and a flexible configuration option, Cisco Common Classification Policy Language (referred to as C3PL), is provisioned, giving administrators more power to define enterprisewide secure access policy.

Figure 1 Cisco IBNS 2.0 Access Session Manager



Benefits

- Identity-based framework for session management
- Robust policy-control engine to apply policies defined locally or received from an external authentication, authorization, and accounting (AAA) server
- Faster deployment and customization of features across access technologies
- Simpler and more consistent way to configure features across access methods, platforms, and application domains

Features

- C3PL-based identity configuration
- Concurrent authentication methods for a single session, including IEEE 802.1X (dot1X), MAC authentication bypass (MAB), and web authentication
- Locally defined & downloadable identity service templates
- Interface templates & Autoconf
- Extended RADIUS change of authorization (CoA) support for session querying, reauthentication, and termination; port shutdown and port bounce; and identity service template activation and deactivation
- Local authentication using Lightweight Directory Access Protocol (LDAP)
- Per-user inactivity handling across methods
- Web authentication support for common session ID
- Web authentication support for IPv6

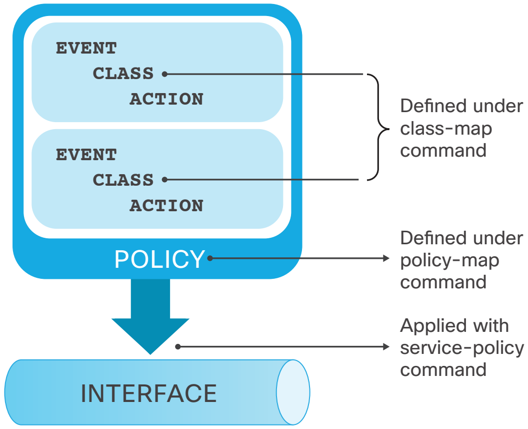
Cisco Policy Language-Based Identity Control with C3PL

The identity control policies define the actions that the access session manager takes in response to specified conditions and endpoint events. A variety of system actions, conditions, and events can be combined using a consistent policy language. For various events, such as session start and session failure, you can specify actions in the control policy. These actions can be performed conditionally for different subscribers based on various match criteria. Control policies are activated on interfaces and typically control the authentication of endpoint identity and the activation of services for sessions.

This new configuration method offers greater flexibility in defining enterprisewide security policies and helps reduce the need to repeat configurations for each port.

Configuring the C3PL policy from the foundation may seem challenging given the various options with which the command set is equipped. To ease this effort, Cisco IOS® Software provides a conversion tool that migrates the existing identity configuration commands on the port to the new policy-mode configurations (Figure 2).

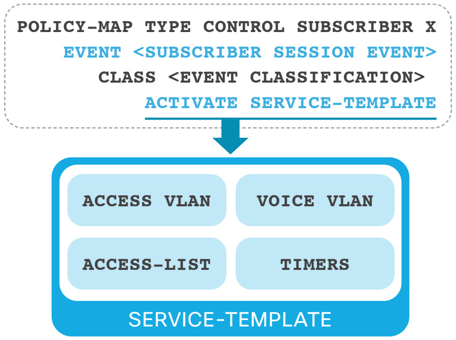
Figure 2 Identity Control Policy Configuration


EVENT
CLASS
ACTION
EVENT
CLASS
ACTION
POLICY
INTERFACE
Defined under class-map command
Defined under policy-map command
Applied with service-policy command

Service Templates

A service template contains a set of service-related attributes or features, such as access control lists (ACLs) and VLAN assignments, which can be activated for one or more subscriber sessions in response to session lifecycle events. Templates simplify the provisioning and maintenance of network session policies in which policies are divided into distinct groups or are role based (Figure 3).

Figure 3 Service Template



```
POLICY-MAP TYPE CONTROL SUBSCRIBER X
    EVENT <SUBSCRIBER SESSION EVENT>
        CLASS <EVENT CLASSIFICATION>
            ACTIVATE SERVICE-TEMPLATE
```

A service template is applied to sessions through its reference in a control policy, through RADIUS CoA requests, or through a user profile or service profile. Service templates also can be downloaded from the RADIUS server or configured locally on the device through the Cisco IOS Software command-line interface (CLI).

Main Use Cases

Concurrent Authentication

Cisco IBNS 2.0 allows the concurrent operation of IEEE 802.1X, MAB, and web authentication methods, making it possible to invoke multiple authentication methods in parallel for a single subscriber session. This capability allows the client-supported method to be completed at the earliest opportunity without the delays associated with serialization.

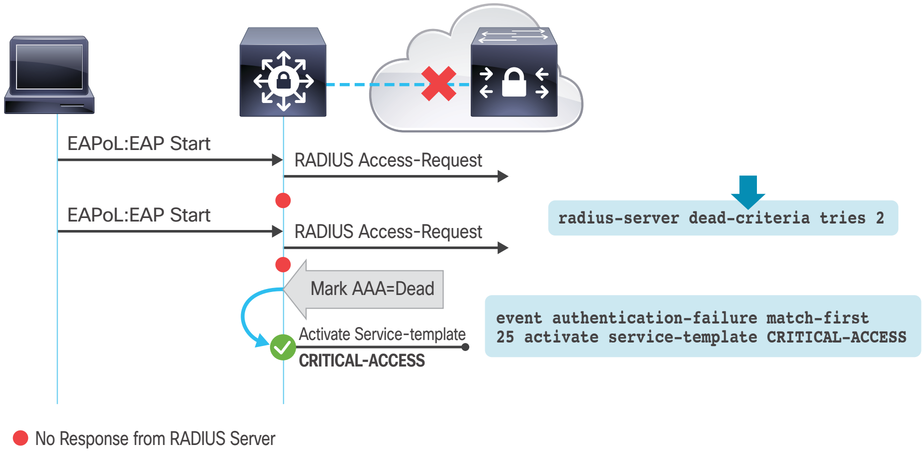
Critical ACL After AAA Failure

Connectivity to the policy server is fundamental for successful network access. If the AAA and RADIUS server infrastructure becomes unavailable because of a failure or unreachable because of network connectivity problems, the network authenticators (switches) may not be able to authorize the end user. Critical VLAN authorization is a remedy that gives the endpoints limited access to the network during an AAA server failure.

A common practice for port authentication is to authorize the user with VLAN and ACL assignments. This type of access permission allows both network segmentation and access control from the enterprise edge. However, the ACL authorization infrastructure requires a pre-authorization ACL to be applied to the port prior to an access session. This requirement prevents the use of critical authorization, in which the user can be given access to a critical VLAN, because the port ACL will block the user’s traffic at ingress to the access network. A comprehensive solution is needed that both authorizes the user with an appropriate VLAN assignment when the AAA infrastructure fails and authorizes an ACL assignment, thereby unblocking the port for access.

The service template and the identity control policy offer options to meet these requirements. A service template can contain IP ACL and VLAN definitions that can be activated during session events (Figure 4).

Figure 4 Critical ACLs



```
radius-server dead-criteria tries 2
```

```
event authentication-failure match-first
25 activate service-template CRITICAL-ACCESS
```

IPv6 Identity

Authenticating IPv6 endpoints and authorizing them for VLAN assignments in closed mode is possible with current Cisco IOS Software. Policy-based Cisco IBNS extends this capability to ACL-based authorization (low-impact mode) and web authentication. In addition, the critical ACL for IPv6 access can be configured for consistency with the IPv6 configuration.

RADIUS Change of Authorization

IBNS 2.0 supports CoA requests to initiate:

- Activation and deactivation of service templates for sessions
- Port bounce
- Port shutdown
- Session querying
- Session reauthentication
- Session termination

CoA for Local Web Authentication

The access session manager can now facilitate CoA for web authentication sessions. All CoA commands that can be run for any authentication session are also applicable for web authentication.

Interface template

Cisco IBNS 2.0 leverages user-definable and reusable templates for interfaces that can be used to manage interface configurations in a simplified manner. Interface template provides an answer to the problem of configuration bloat and manageability problems.

Autoconf

The new AutoConf solution enhances the idea of Auto Smart Port Macros for dynamic device-ID based authorization by leveraging the Policy based IBNS infrastructure and the interface templates. This new framework offers clean and simplified solution for automatic interface configurations at the enterprise edge leveraging the Device sensor and the device classifier features offers for detection and classification of connecting endpoints at the network access.

Web Authentication Support for Common Session ID

Cisco IBNS 2.0 allows a single session identifier to be used for web authentication sessions and for all IEEE 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.

Phased Implementation Strategy

We recommend a phased deployment model for Cisco IBNS that has limited impact on network access while gradually introducing authentication and authorization on the wired network. The phases, in order, are as follows:

- Monitor mode
- Low-impact (or selective-access) mode
- High-security mode

For More Information

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