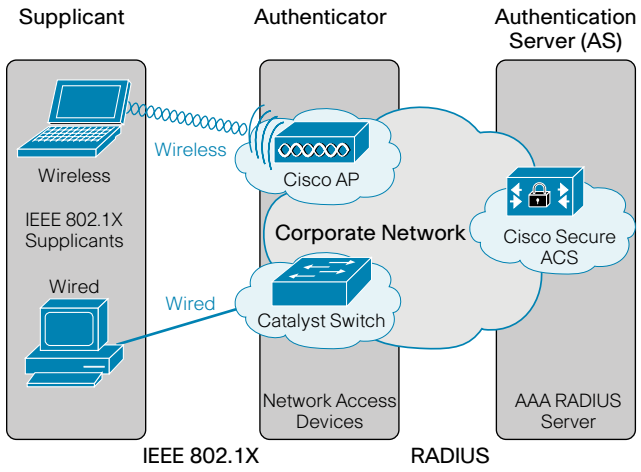
Identity-Based Networking Services (IBNS)

At-A-Glance

What Is the Value of Identity-Based Networking Services (IBNS)?

Cisco® IBNS is the foundation for providing access control to corporate networks. The Cisco IBNS solution is a set of Cisco IOS® Software services designed to enable secure user and host access to enterprise networks powered by Cisco Catalyst® switches and WLANs. Cisco IBNS enables enterprise policy enforcement of all users and hosts, whether managed or unmanaged. The solution promotes authentication to access the network; this authentication also serves as the basis for differentiating users and/or hosts, providing varying levels of access to networked resources based on corporate access policy.

Figure 1.



Cisco IBNS also provides accounting records that can include connection information: who and what connected, IP address, MAC address, port, and authorization information, serving a key role for enabling compliance and security auditing.

The foundation for these services is IEEE 802.1X, a port-based authentication and access control protocol. The three basic components include the client (also known as the "supplicant"), the authenticator (the device the client is attempting to connect to), and the authentication server (a AAA server).

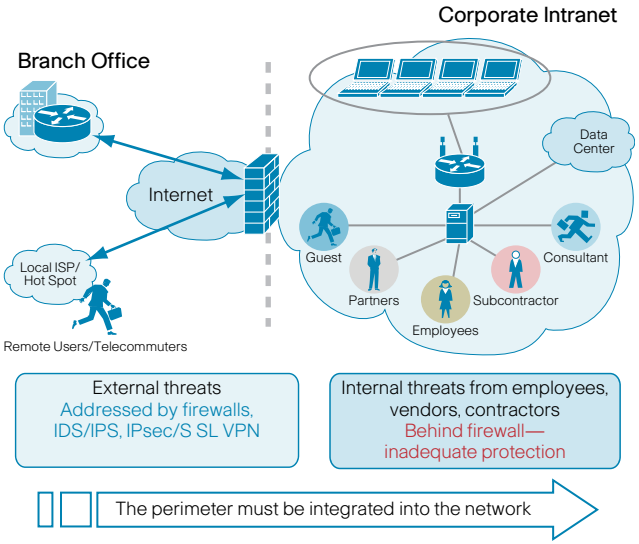
What Problems Does IBNS Help Solve?

Enterprises are continually challenged with reducing costs, increasing productivity, and optimizing operational efficiencies, while increasing revenues and competitiveness. In response to these challenges, enterprises have developed sophisticated business models that rely heavily on a mix of full-time employees, contractors, and partners. Many members of this mixed workforce have direct local intranet access, which increases security risk.

Addressing these potential risks can involve managing access rights on a per-individual port or user basis, which increases operational overhead. Here is the summary for challenges faced by customers today:

- Making network access available to more users without sacrificing security
- Limiting access to network resources while maintaining operational efficiency
- Providing different layers of access for different kinds of users
- Enforcing accountability for actions or usage

Figure 2. Enterprise Access Revolution



How the Trust and Identity System Works

Cisco IBNS enforces policy compliance, controlling port access and tracking users. It asks the questions listed in the table below, and then takes the appropriate actions.

Questions	Actions Taken
Who are you?	Cisco IBNS uses 802.1X or other authentication methods to authenticate the user.
Where can you go?	Based on authentication, the user is placed in the correct workgroup or VLAN.
What service level do you receive?	The user can be given a per-user access control list to explicitly restrict or allow access to specific resources on the network, or given specific QoS priority on the network.
What are you doing?	Using the identity and location of the user, tracking and accounting can be better managed.

Cisco IBNS Solution

Cisco IBNS offers various network identity features, including MAC Authentication Bypass (MAB), web authentication, IEEE 802.1X for link-layer authentication and access control, supplicant, authenticator, and AAA server. The solution offers simplified deployments and IP telephony integration to provide greater flexibility.

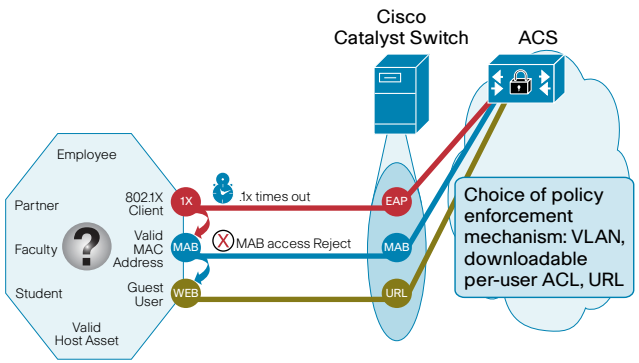
Simplified Deployments

Cisco IBNS has been enhanced to reduce the operational overhead associated with deploying IEEE 802.1X in primarily wired deployments. The main goal is a single-port configuration that can accommodate all potential types of hosts, as well as managed, unmanaged, known, and unknown users. Enhancements include FlexAuth and Open Mode.

FlexAuth allows IT administrators to configure a single port that enables 802.1X, MAC-Auth Bypass (MAB), and/or web-based authentication (WebAuth) in any sequence to accommodate desired authentication requirements. This provides prescriptive authentication and authorization based on the organization's access policies.

Identity-Based Networking Services (IBNS)

Figure 3. Flexible Authentication



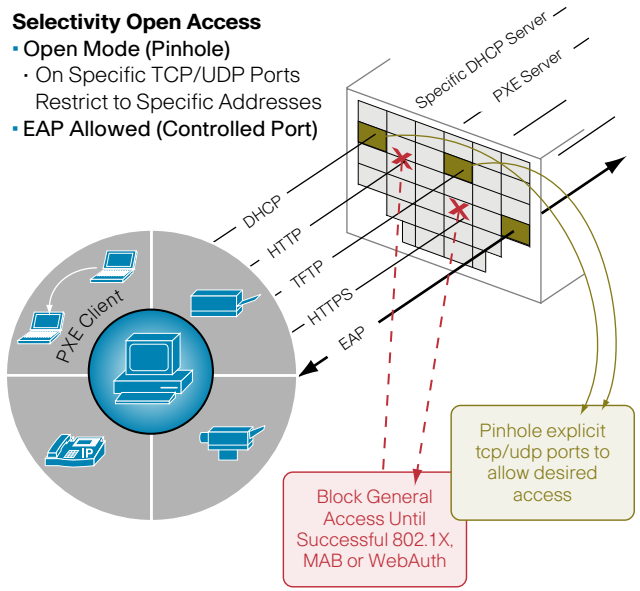
- One configuration addresses all use cases
- Controllable sequence of access control mechanisms, with flexible failure and fallback authorization

Benefit:
- Greater flexibility in defining network access policies

Open Mode provides the IT administrator with the flexibility to selectivity open, or pinhole, certain traffic types through the restricted 802.1X-enabled port. By default, 802.1X acts as a switch port firewall blocking all traffic except Extensible Authentication Protocol over LAN (EAPoL), which is used to carry credentials that authenticate the user or host attempting to connect to the port. Open Mode provides new flexibility to selectively open access to other protocols. The most common use for this is to enable host management operations to function normally in an identity-based access control port implementation. Protocols such as PXE boot, SMS, SUS, and others that assume network connectivity can be allowed to flow through the access controlled port, in a controlled manner. This effectively allows interoperability with any protocol with a defined port number.

Together with FlexAuth and Open Mode, Cisco NAC Profiler helps accelerate and streamline the deployment of 802.1X. The NAC Profiler simplifies the discovery and profiling of all endpoint devices, putting that information into a database that can be utilized by IBNS MAB for non-802.1X endpoint authentication and authorization. It also improves the management of endpoints by managing identity, location, and adds, moves, and changes in these devices following deployment.

Figure 4. 802.1X/MAB—Open Mode



IP Telephony Integration

Multi-Domain Authentication (MDA) allows for the secure deployment of IP telephony, regardless of whether a Cisco or a third-party IP phone is used. IP telephony presents a particular challenge during 802.1X rollouts because a phone is both an endpoint requiring authentication and a device that allows other machines to connect through it to the corporate network.

Cisco Catalyst switches can be configured to secure data and voice VLANs on a single port. With MDA, a phone, with or without a supplicant, is authenticated and subsequently placed in the voice VLAN (or domain). Any device connecting through the phone's Ethernet port is authenticated and then placed in the data VLAN.

To further prevent potential security vulnerabilities, Cisco IBNS offers inactivity timers, and certain models of Cisco IP phones issue Cisco Discovery Protocol notifications and EAP logoffs when PCs disconnect from IP phones. These measures are aimed at removing previously authenticated sessions to prevent unauthorized access.

Authorization

Using Cisco IBNS to prevent unauthorized access to corporate networks is a fundamental risk reduction practice. The nature of basic authentication and authorization serves a vital function in accommodating organizations' access security policies. Cisco IBNS also allows for grouping of users or hosts based on their role in the organization; these groupings should be based on groups with similar sets of privileges. Groupings can be instantiated today using dynamic VLAN assignment, downloadable ACLs, or URL redirect to further restrict access to corporate resources.

Cisco Solution Interoperability

Additionally, the NAC Guest Server can be used for centralized web authentication to allow authentication and authorization for guest users or short-term users, such as partners or subcontractors. The Guest Server offers simple user account administration. This is part of the FlexAuth single-port configuration, and is enabled through URL redirect on the switch port as a fallback to 802.1X and/or MAB.

Additional Information

For more information about the Cisco Identity Based Networking Services solution, visit http://www.cisco.com/go/ibns.