

Cisco Identity-Based Networking Services (IBNS)

Executive Summary

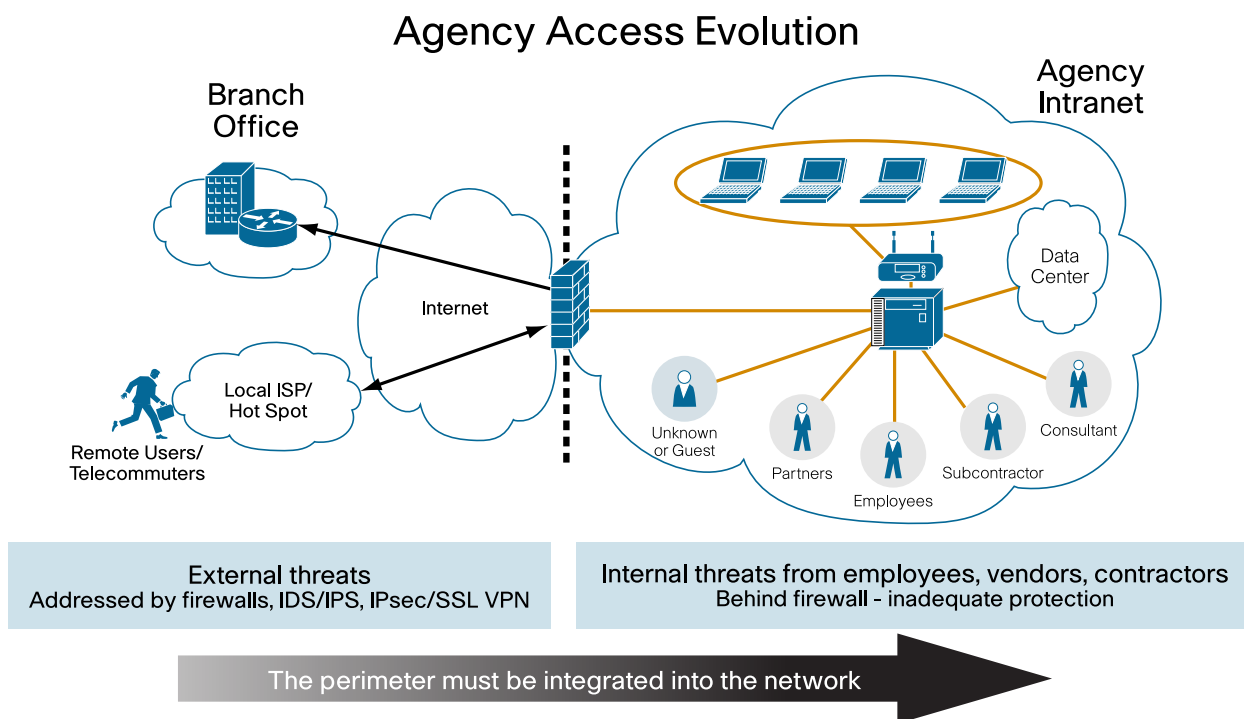
Network security professionals face numerous challenges, but perhaps none is more difficult than the growing need to control devices that are outside the direct management of a network administrator. One of the most common ways that malware enters a company's network is by contractors and employees bringing their own computers, wireless access points, switches, or gaming systems onto the agency network. Typically, clients see a drop of 25% in help desk calls from end users with a properly deployed access control solution. Studies show that the cost of cleaning malware from a device costs an average of \$200 per incident, per device.

With decreased budgets, agencies are challenged to reduce costs, yet they are required to increase productivity and operational efficiency. In response, agencies have developed sophisticated business models that rely heavily on a mix of full-time employees, contractors, and partners. A majority of this mixed workforce has direct local intranet access, thus increasing security risk. Figure 1 shows how network access has evolved for the agency.

Addressing these potential risks can involve managing access rights on a per-individual port or user basis, which increases operational overhead. Summaries of challenges faced by customers today are as follows:

- Making network access available to more users without sacrificing security
- Identifying and accounting for the inventory of devices on your network
- Network virtualization: consolidating multiple physical networks into one logical network
- Limiting access to network resources while maintaining operational efficiency
- Providing cost effective role-based access control
- Enforcing accountability for actions or usage

Figure 1. Agency Access Evolution



IBNS Solutions for the Public Sector

NIST Special Publication 800-53 specifically notes the requirements for 802.1X, which are clearly met with the Cisco IBNS solution detailed below.

- IA-3 Device Identification and Authentication¹

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP] or a Radius server with EAP-Transport Layer Security [TLS] authentication) to identify and authenticate devices on LANs or WANs. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

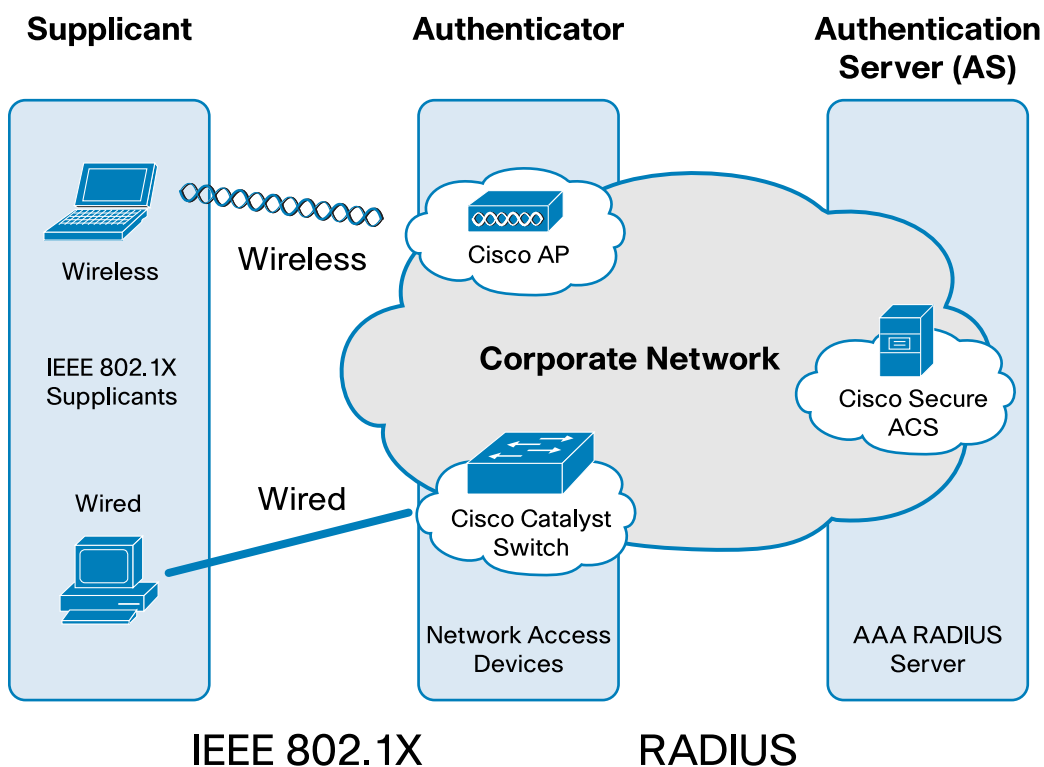
- 1st DISA STIG on Access Control in Support of Information Systems, dated 28 Dec 2008–(AC34.025: CAT I)
The IAO/NSO will ensure either MAC security (with profiling) or 802.1X port authentication is used on all network access ports and configured in accordance with the Network Infrastructure STIG.

The Value of IBNS

Cisco® IBNS is the foundation for providing access control to agency networks. The Cisco IBNS solution is a set of Cisco IOS® Software services designed to enable secure user and host access to agency networks powered by Cisco Catalyst® switches and WLANs. Cisco IBNS enables agency 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 access policy.

¹ NIST SP 800-53 is available to download at <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.

Figure 2. IBNS Overview



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). 802.1X should be the first step in any identity solution and there are several services to build on top of this, including Network Admission Control (NAC), device profiling, guest access, and network virtualization.

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 can be given specific quality of service (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

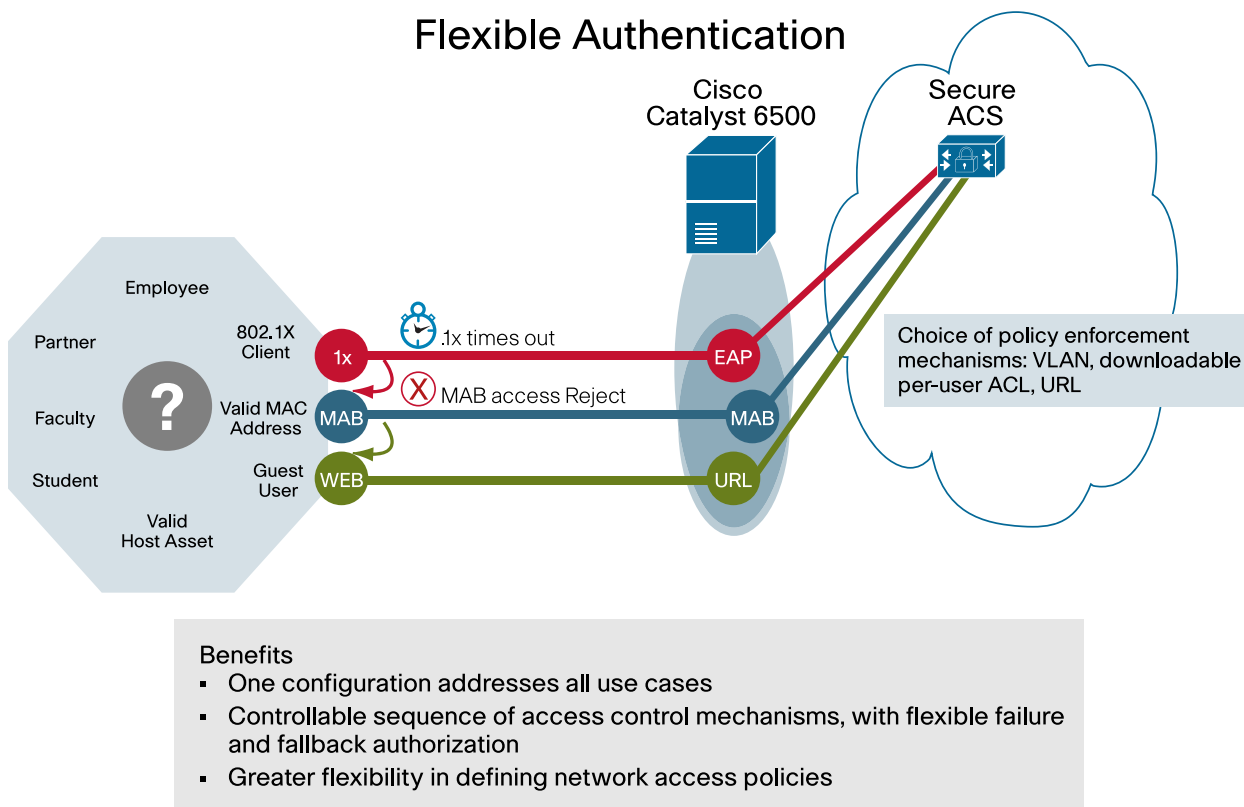
By itself, the IEEE 802.1X standard can be burdensome to deploy. It poses several deployment challenges to organizations, including access for devices without an 802.1X supplicant, continuity of operations with services such as PXE Boot and Wake on LAN, IP telephony integration, and high operational overhead. 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

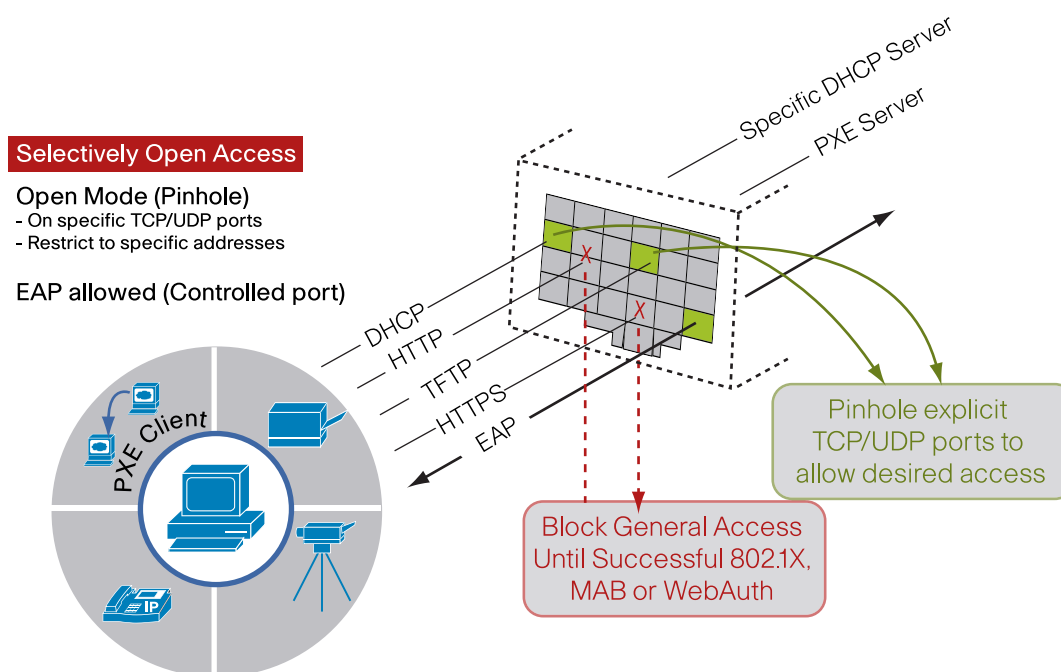
Cisco IBNS has been enhanced to reduce the operational overhead associated with deploying IEEE 802.1X in primarily wired deployments. The main goal is a single-port configuration that can accommodate all potential types of hosts, as well as managed, unmanaged, known, and unknown users. Enhancements include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

Figure 3. IBNS Flexible Authentication



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. In addition, FlexAuth allows deployment of multiple devices behind a single port, yet enforce authentication on a per MAC address basis. This provides prescriptive authentication and authorization based on the organization's access policies.

Open Mode enables the IT administrator to selectively 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.

Figure 4. 802.1X/MAB - Open Mode

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.

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 agency network. With respect to Cisco IP Telephony handsets, 802.1X certificate based authentication is supported directly on the phone.

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 agency 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 access control lists (ACLs), or URL redirect to further restrict access to agency resources. In addition, Cisco IBNS (e.g. Cisco ACS), allows further granularity by deploying rule-based policy

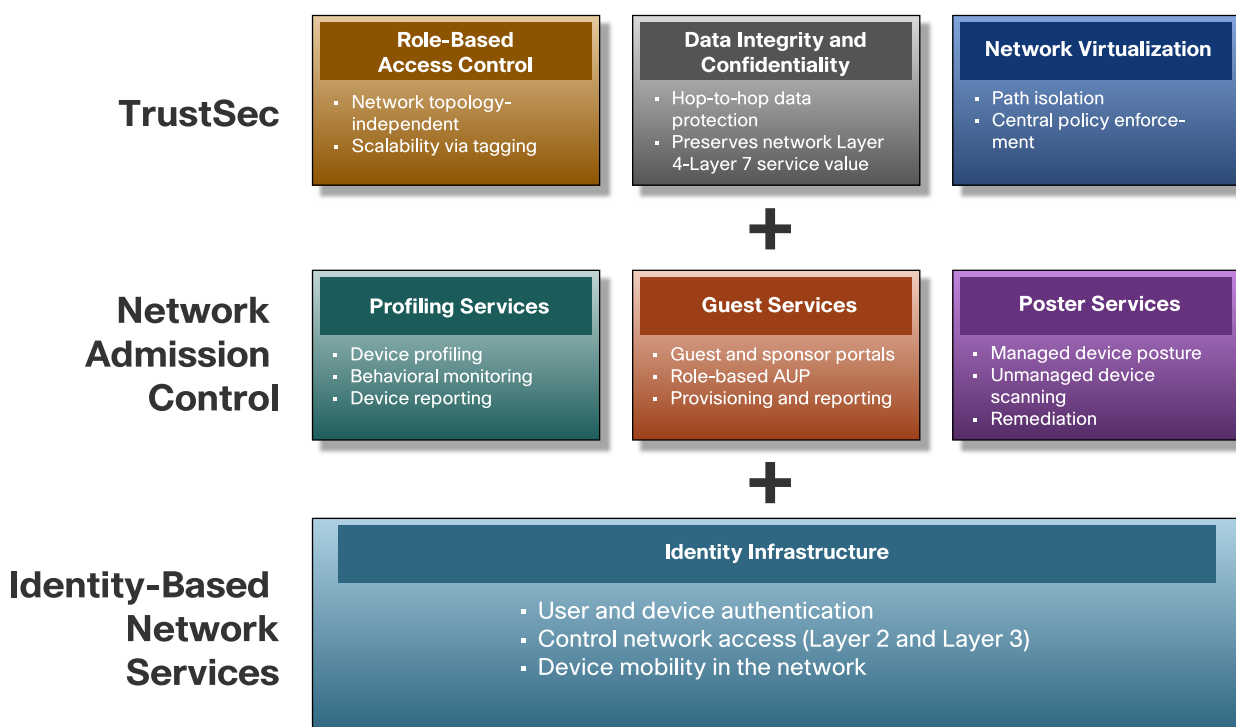
engines to control authorization based on multiple factors such as date, time, location, authentication type, and wired vs. wireless connection.

Post-802.1X Identity Services

Once the 802.1X deployment has been successfully deployed, several useful services can be utilized to offer even greater benefits to your network, including:

- Posture and profiling services: Pre-admission health check of the endpoint, and identity and management of non-PC devices
- Cisco TrustSec: Role-based access control and hop-to-hop encryption
- Network virtualization: Partitioning the physical network into multiple logical networks

Figure 5. Pre and Post Authentication Services



Posture and profiling services—Cisco NAC enforces security policies on all devices requesting network access. Cisco NAC mitigates risks from emerging security threats by allowing only compliant and trusted endpoint devices, such as PCs, servers, and personal digital assistants (PDAs), onto the network. Cisco NAC provides the following benefits:

- **Security policy compliance:** Enables endpoints to conform to security policy, protect infrastructure and employee productivity, secure managed and unmanaged assets, support internal environments and guest access, and tailor policies to your organization's risk level.
- **Investment protection:** Compatible with third-party management applications. Flexible deployment options minimize need for infrastructure upgrades.
- **Risk mitigation:** Reduce risks from viruses, worms, and unauthorized access. Reduce large-scale infrastructure disruptions and integrate with other Cisco Self-Defending Network components to deliver comprehensive security protection.

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.

Cisco TrustSec—Cisco TrustSec significantly reduces the operational costs of managing access control policies and protecting data across agency networks. It does this by building out trusted network segments based on trusted network devices and trusted users. It delivers three fundamental security services:

1. Secure campus access control

Cisco TrustSec uses 802.1X for authentication mechanisms and to access standard directory services and, after successful authentication, maps users and networking devices to specific roles based on criteria such as identity, job function, location, posture, device type, and so on. The role-based access control capability simplifies the scaling of security services and provides a more efficient approach to implementing compliance requirements and security policies.

2. Converged policy framework

With Cisco TrustSec, security policies can be collapsed into a centralized policy engine that acts as a broker between the campus network infrastructure and back-end policy directories, such as Active Directory. Cisco's existing access control system, Cisco Secure ACS, provides policy aggregation and control of this converged policy framework. If deployed along with Cisco NAC, Cisco Secure ACS also interacts with the NAC system to take advantage of endpoint posture, remediation, and other NAC services.

3. Pervasive integrity and confidentiality

Cisco TrustSec adds data protection by securing every data path in the campus switching environment based on digital device certificates and strong encryption based on the IEEE 802.1AE standard. Data confidentiality and integrity is instantiated between devices on a hop-by-hop basis. This allows mission-critical applications such as firewalls, intrusion prevention systems, and content inspection engines to maintain visibility into the packet streams at each switch boundary without disrupting the requirements for data integrity and confidentiality.

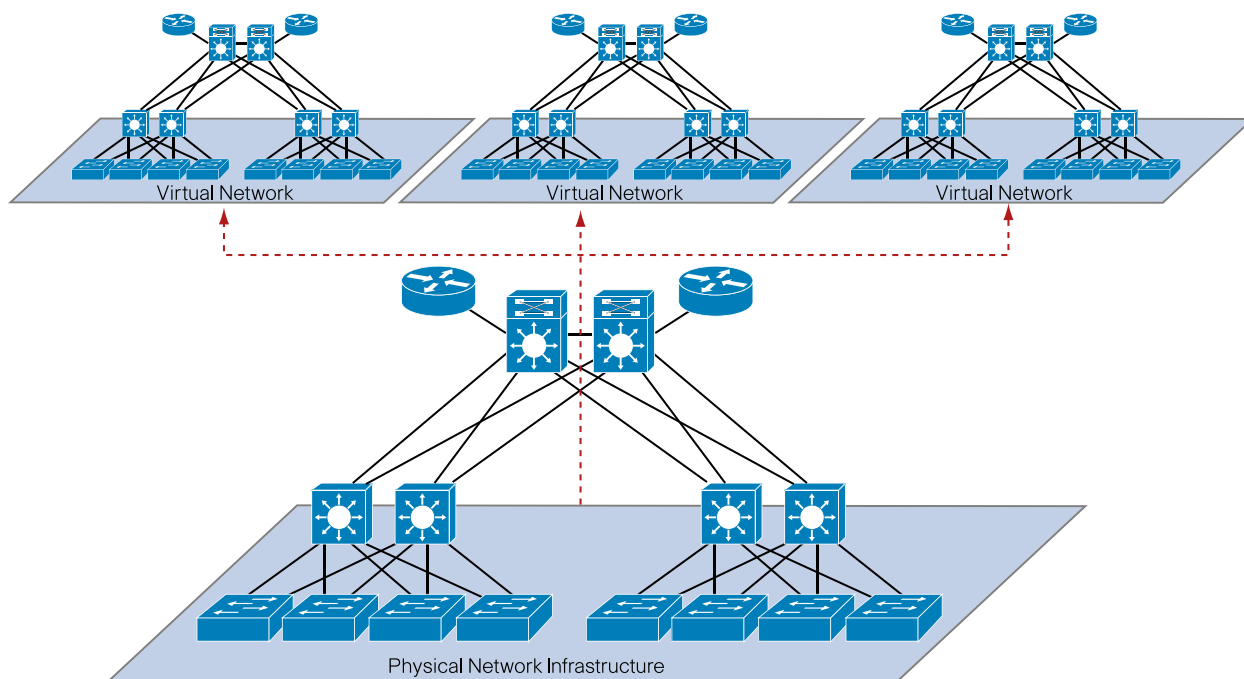
Most access control policies today are managed through ingress filter ACLs that require an understanding of network and application topology. As the network or services change, these ACLs must be modified and propagated throughout the network. It is difficult to keep these ACLs synchronized with agency requirements; as a result, legacy access control implementations typically do not scale.

Cisco TrustSec dramatically reduces the cost of managing access control, shifting from a classic ingress filter model to an ingress tag and egress filter model. Instead of having every entry point understand where every user can and cannot go, administrators can localize access rules to just those areas of the network that understand the policy for a given role. In other words, only those destinations that care about a given role need an ACL policy to deal with that role. This approach allows administrators to implement security policies independent of the location of the user or device. User roles need to be defined only once and are then pervasively and consistently applied across the entire infrastructure.

The Security Association Protocol is a recent Cisco innovation that is based upon the IEEE 802.1Xrev standard. The Security Association Protocol simplifies the key management between links and also facilitates interoperability with other 802.1AE-compatible devices. Cisco TrustSec also carries role information over secured links to make policies and confidentiality pervasive and scalable.

Network Virtualization

Network virtualization refers to the creation of logical isolated network partitions overlaid on top of a common physical infrastructure. Each partition is logically isolated from the others, and must behave and appear as a fully dedicated network to provide privacy, security, and an independent set of policies, service levels, and even routing decisions.

Figure 6. Network Virtualization

Network virtualization provides multiple solutions to business problems and drivers that range from simple to complex. Simple scenarios include agencies that want to provide Internet access to visitors (guest access). The stringent requirement in this case is to allow visitors external Internet access while preventing any possibility of unauthorized connection to the agency internal resources and services. This can be achieved by dedicating a logical “virtual network” to handle the entire guest communication path. Internet access can also be combined with connectivity to a subset of the agency internal resources, as is typical in partner access deployments.

Another simple driver for network virtualization is the creation of a logical partition dedicated to the machines that have been quarantined as a result of a NAC posture validation. In this case, it is essential to guarantee isolation of these devices in a remediation segment of the network, where only access to remediation servers is possible until the process of cleaning and patching the machine is successfully completed.

Complex scenarios include agency IT departments acting as a service provider, offering access to the agency network to many different “customers” that need logical isolation between them. In the future, users belonging to the same logical partitions will be able to communicate with each other and to share dedicated network resources. However, some direct intercommunication between groups may be prohibited. Typical deployment scenarios in this category include retail stores (for example, Best Buy, Albertson’s, Wal-Mart, and so on) that provide on-location network access for kiosks or hotspot providers.

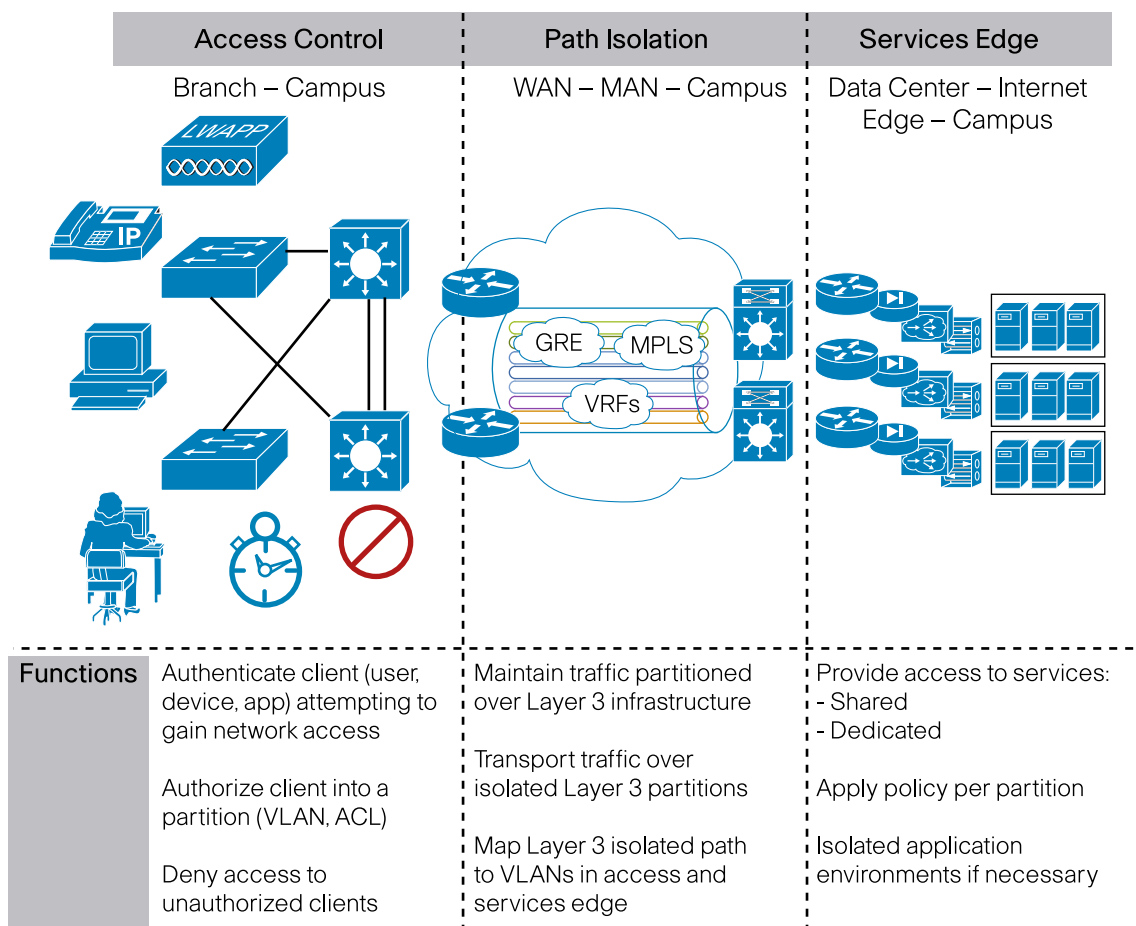
The architecture of an end-to-end network virtualization solution targeted to satisfy the requirements listed above can be separated in the following three logical functional areas:

- Access control
- Path isolation
- Services edge

Each area performs several functions and must interface with the other functional areas to provide the end-to-end solution.

Network Virtualization—Three Functional Areas

Figure 7. Functional Areas of Network Virtualization



When an endpoint is authorized on the network, it can be associated to a specific group that typically corresponds to a separate partition or domain. Thus, 802.1X becomes a valuable tool to determine the mapping of the endpoint to an end-to-end virtual network.

Summary and Conclusion

As network and security administrators are realizing the benefits of 802.1X, they are looking not only for ways to deploy this technology throughout the agency network, but also for additional tools to build on top of the identity framework. In addition, the 802.1X deployment and accompanying services must scale to address today's mobile workforce with multiple access requirements. The financial and operational cost of cleaning malware makes deployment of identity services a requirement, and the use of 802.1X and standards-based access are the critical first step.

There have been issues with the traditional deployment model of 802.1X as specified by IEEE, but Cisco IBNS has built solutions into the infrastructure to simplify these deployments and solve critical problems not addressed by the standard. With the 802.1X baseline identity solution in place, network and security administrators can take advantage of several critical services to lock down networks, including posture and profiling services, Cisco TrustSec for scalable access control and data integrity, and network virtualization to optimize operational efficiencies.

Cisco IBNS Related Links—More Information

http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html

http://www.cisco.com/en/US/products/ps6638/products_ios_protocol_group_home.html

http://www.cisco.com/en/US/products/ps6638/prod_white_papers_list.html

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/whitepaper_C11-530469.html



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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)