

Network Admission Control Framework

Deployment Guide



| | |
|---|-----------|
| Introduction..... | 5 |
| Network Admission Control Overview | 5 |
| Goals of Admission Control | 5 |
| Partnerships..... | 5 |
| Cisco Network Admission Control: Architecture & System Components..... | 6 |
| Architecture Overview | 6 |
| Enforcement:..... | 6 |
| Decision and Remediation: | 7 |
| NAC System Components | 9 |
| Cisco Trust Agent (CTA)..... | 9 |
| CTA Supplicant | 10 |
| Posture Plugins..... | 10 |
| Agentless Hosts..... | 11 |
| Network Access Devices (NADs) | 11 |
| Cisco Secure Access Control Server (ACS) | 12 |
| Remediation Server..... | 12 |
| Posture Validation Server | 13 |
| Audit Server | 13 |
| Reporting..... | 13 |
| Protocols | 14 |
| EAP | 14 |
| EAP-FAST | 14 |
| HCAP | 15 |
| GAME..... | 15 |
| NAC Assessment Methods | 15 |
| NAC L3 IP | 15 |
| NAC L2 IP | 17 |
| NAC L2 802.1x..... | 18 |
| Agentless Hosts..... | 19 |
| Static Exceptions (Whitelisting) | 19 |
| Dynamic Audit..... | 19 |
| NAC Policy Strategies..... | 20 |
| Designing a Network Admission Policy | 20 |
| Policy Creation Requirements | 20 |
| Policy Definition..... | 21 |
| Credentials | 22 |
| Identity Credentials..... | 22 |
| Generic Device Credentials | 22 |
| Microsoft Machine Credentials..... | 22 |
| User Credentials..... | 23 |
| Posture Credentials | 23 |
| Identity versus Posture..... | 24 |
| Network Segmentation and Isolation..... | 24 |
| Segmentation..... | 24 |
| Isolation..... | 24 |

| | |
|--|-----------|
| Default Network Access | 25 |
| NAC Agentless Host (NAH) Options | 25 |
| Static NAD Whitelisting | 25 |
| Centralized ACS Whitelisting | 25 |
| Dynamic Host Audit | 26 |
| Patch Management Integration | 26 |
| Process | 26 |
| Patch-On-Quarantine | 26 |
| NAC Scalability and Availability | 27 |
| Scalability | 27 |
| Users and Hosts | 27 |
| Cisco Secure Access Control Server (ACS) | 28 |
| Protocol Authorization Rates | 28 |
| NAC Timers | 28 |
| Other Scaling Limitations | 29 |
| Scaling Calculations | 29 |
| Load Balancing | 29 |
| IOS RADIUS Server Failover | 30 |
| IOS RADIUS Server Load Balancing | 30 |
| RADIUS Server Load Balancing using Content Services Switch | 30 |
| NAC Design Considerations | 32 |
| NAC Assessment Methods | 32 |
| NAC-L3-IP | 32 |
| NAC-L2-IP | 33 |
| NAC-L2-802.1x | 35 |
| CTA and Windows Boot Sequence | 36 |
| IEEE 802.1x and NAC-L2-IP | 39 |
| NAC Agentless Hosts (NAHs) | 39 |
| NAC-L2/L3-IP and Agentless Hosts | 40 |
| NAC-L2-802.1x and Agentless Hosts | 40 |
| NAH Summary | 41 |
| NAC Enforcement Features and Trade-offs | 42 |
| Network Admission Control Deployment Comparison | 42 |
| NAC Solution Components | 43 |
| Cisco Trust Agent | 43 |
| NADs | 43 |
| Cisco IOS Router | 44 |
| Cisco VPN Concentrators | 44 |
| Cisco Switches | 44 |
| CiscoSecure ACS 4.0 | 44 |
| Performance and Scalability | 44 |
| Management | 45 |
| Other | 45 |
| Directory Services | 45 |
| Authentication Protocol Support | 45 |

| | |
|--|-----------|
| Directory Scaling | 46 |
| Summary | 46 |
| Appendices..... | 47 |
| Acronyms..... | 47 |
| NAC Attribute Reference..... | 53 |
| Attribute Namespace..... | 53 |
| Attribute Data Types..... | 53 |
| Attribute Reference..... | 54 |
| RADIUS Attributes for NAC..... | 56 |
| Identifying NAC Methods in RADIUS Request Attributes | 57 |

Introduction

NETWORK ADMISSION CONTROL OVERVIEW

Network Admission Control (NAC) is a set of technologies and solutions built on an industry initiative led by Cisco Systems®. NAC uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices (PCs, servers, and PDAs, for example) and can restrict the access of noncompliant devices.

The NAC Framework technology integrates an intelligent network infrastructure with solutions from more than 60 manufacturers of leading antivirus and other security and management software solutions.

GOALS OF ADMISSION CONTROL

Previously, users and devices were authenticated as to who or what they were, but not their condition. NAC helps ensure that only healthy client workstations are granted full network access. NAC works with anti-virus, patch management, and personal firewall software to assess the condition, called the posture, of a client before allowing that client network access. NAC helps ensure that a network client has an up-to-date virus signature set, the most current operating system patches, and is not infected. If the client requires an anti-virus signature update or an operating system update, NAC directs the client to complete the necessary updates. If the client has been compromised or if a virus outbreak is occurring on the network, NAC places the client into a quarantined network segment. After the client has completed its update process or disinfection, the client is checked again and returned to a healthy status with normal network access.

PARTNERSHIPS

Cisco has partnered with experts in the anti-virus, patch management, and personal firewall fields to extend the NAC solution to address all areas of concern. All major vendors have signed up for the NAC partner program, which protects the investments that enterprises have already made in security applications. More information about the NAC Partnership program is available at

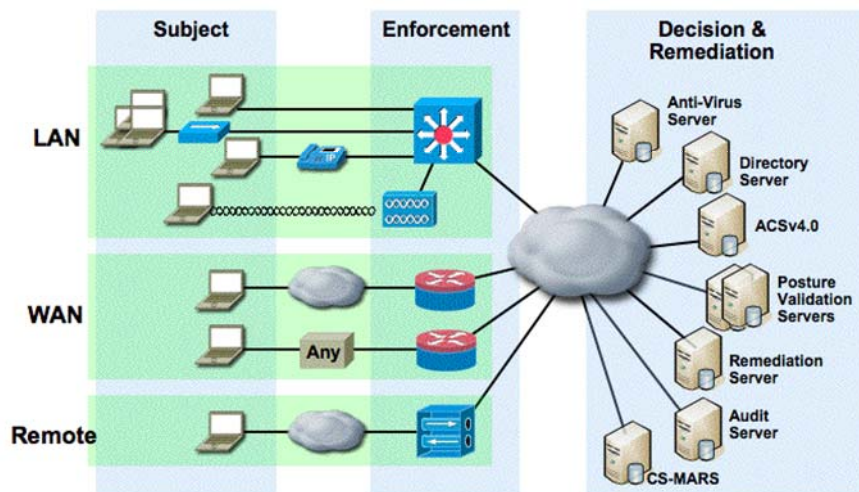
<http://www.cisco.com/en/US/partners/pr46/nac/partners.html>.

Cisco Network Admission Control: Architecture & System Components

Architecture Overview

Cisco NAC assesses the state, or posture, of a host to prevent unauthorized or vulnerable endpoints from accessing the network. Typical hosts are desktop computers, laptops, and servers, but may also include IP phones, network printers, and other network-attached devices.

Figure 1. NAC Deployment Scenarios



Cisco NAC is ubiquitous across all network access methods. Posture information can be gathered and access policy enforced for hosts attempting network access through routers, switches, wireless access points, and VPN concentrators.

The Cisco NAC posture validation process includes these major architectural components.

Subject:

- **Host**—Machine accessing the network on which NAC is enforced
- **Posture Plugin (PP)**—A Cisco or third-party DLL that resides on a host and provides posture credentials to a posture agent residing on the same device.
- **Posture Agent (PA)**—Host agent software that serves as a broker on the host for aggregating credentials from potentially multiple posture plugins and communicating with the network. The Cisco Trust Agent (CTA) is Cisco's implementation of the posture agent.
- **Remediation Client**: A component of a remediation management solution that operates in conjunction with a remediation server to update specific client software such as OS patches.

ENFORCEMENT:

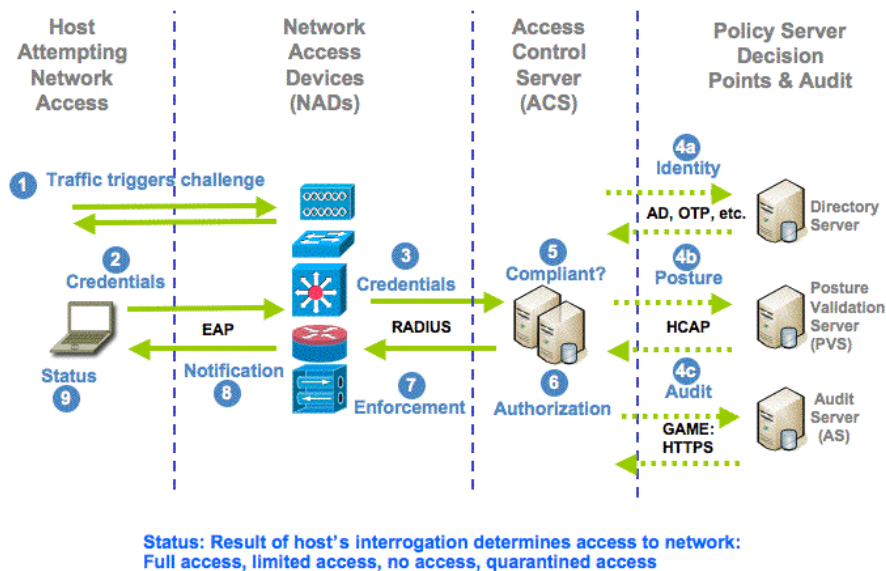
- **Network Access Device (NAD)**—Network devices acting as a NAC enforcement point. These may include Cisco access routers (800-7200), VPN Gateways (VPN3000 series), Catalyst Layer 2 and Layer 3 switches, and wireless access points.

DECISION AND REMEDIATION:

- **AAA Server** (Authentication, Authorization and Accounting Server)—The central policy server that aggregates one or more authentications and/or authorizations into a single system authorization decision and maps this decision to a network access profile for enforcement by the NAD. Cisco Secure Access Control Server (ACS) is Cisco's AAA server product that supports NAC
- **Directory Server**—A centralized directory server for performing user and/or machine authentication. Possible directory services include Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD), Novell Directory Services (NDS), and one-time token password servers (OTP).
- **Posture Validation Server (PVS)**—A posture validation server from one or more third parties acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials from one or more posture plugins against a set of policy rules. Examples include anti-virus servers or security application servers.
- **Remediation Server**—A management solution used to bring non-compliant hosts into compliance. This could be a specialized patch management application or as simple as a web site for distributing software. The better and more efficient your host patching and remediation is, the less risk
- **Audit Server**—A server or software that performs vulnerability assessment (VA) against a host to determine the level of compliance or risk of the host prior to network admission.

The following figure displays the primary NAC components and provides an overview of the authorization process used to grant or deny access to the network.

Figure 2. NAC Components and Authorization Process

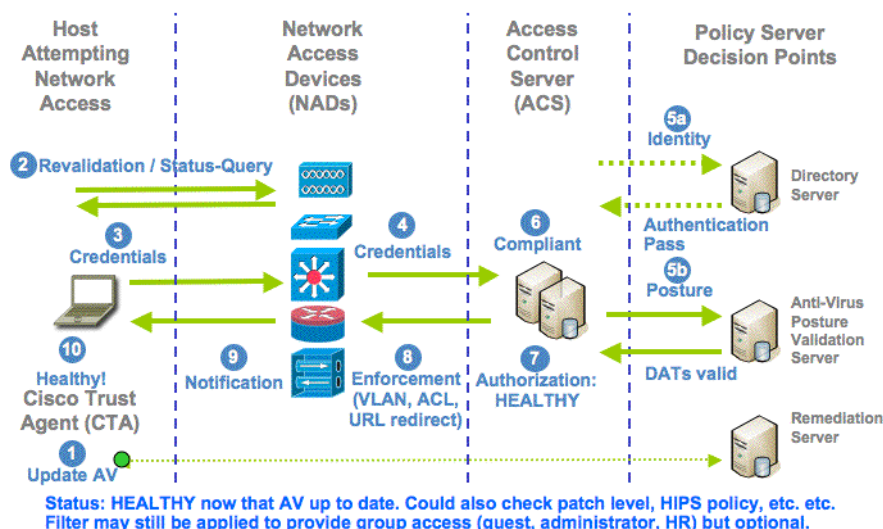


Refer to the numbers in the figure above for each step below describing the NAC authorization process.

1. Posture validation occurs when a NAC-enabled network access device detects a host attempting to connect or use its network resources.
2. Upon detection of a new endpoint, the NAD sets up a communication path between the AAA server (ACS) and the posture agent. After the communication path has been established, the AAA server requests the endpoint for posture credentials from one or more posture plugins.

3. The host responds to the request with its posture credentials from available posture plugins from NAC-compatible software components on the host.
 4. The AAA server either validates the posture information locally or it may in turn delegate parts of the decision to external posture validation servers.
 5. The AAA server aggregates the individual posture results, or posture tokens, from all of the delegate servers to determine the host's overall compliance or system posture token.
 6. The identity authentication and system posture token are then mapped to a network authorization in the network access profile, which consist of RADIUS attributes for timers, VLAN assignments, or downloadable access control lists (ACLs).
 7. These RADIUS attributes are sent to the NAD for enforcement on the host.
 8. The CTA on the host is then sent its posture status for notifying the respective plugins of their individual application posture as well as the entire system posture.
 9. A message may be optionally sent to the user of the host using the CTA's notification dialog so they know their state on the network.
- The following figure displays the primary NAC components and provides an overview of the remediation process used to move a host from quarantine to a healthy state.

Figure 3. NAC Components and Remediation Process from Quarantine to Healthy



Refer to the numbers in the figure above for each step below describing the NAC remediation process.

1. A host that has been placed in the quarantine state is directed to a third party remediation server in order to update its AV software.
2. The Cisco Trust Agent polls the posture plugin for the AV software, discovers there has been a change, and triggers a revalidation from the NAD. The NAD sets up a communication path between the AAA server (ACS) and the posture agent. After the communication path has been established, the AAA server requests the endpoint for posture credentials from one or more posture plugins.
3. The host responds to the request with its posture credentials from available posture plugins from NAC-compatible software components on the host.
4. The AAA server either validates the posture information locally or it may in turn delegate parts of the decision to external posture validation servers.

5. The AAA server aggregates the individual posture results, or posture tokens, from all of the delegate servers to determine the host's overall compliance or system posture token.
6. The identity authentication and system posture token are then mapped to a network authorization in the network access profile which consist of RADIUS attributes for timers, VLAN assignments, or downloadable access control lists (ACLs).
7. These RADIUS attributes are sent to the NAD for enforcement on the host.
8. The CTA on the host is then sent its posture status for notifying the respective plugins of their individual application posture as well as the entire system posture.
9. A message may optionally be sent to the user of the host using the CTA's notification dialog so they know their state on the network.
10. The host's AV software is now up to date and has been verified by AV posture validation server. As a result ACS has moved the host from a quarantine state to a healthy state.

All posture decision points, whether AAA server or PVS, evaluate one or more sets of host credentials in rule-based policy engines which results in one or more application posture token (APTs). An APT represents a compliance check for a given vendor's application on the host. The AAA server then merges all APTs from the delegated PVS and its own policy engine into a single system posture token (SPT) representing the overall compliance of the host. Therefore, if one of the APTs, which compose the overall SPT, fails the compliance check, the overall SPT reflects this. Both APTs and SPTs are represented using the following pre-defined tokens:

Healthy—Host is compliant; no restrictions on network access.

Checkup—Host is within policy but an update is available. Checkup is used to proactively remediate a host to the Healthy state.

Transition—Host posturing is in process; give interim access pending full posture validation. This state is applicable either during host boot when all NAC-enabled applications may not be running or during an audit when posture information has not yet been obtained from the host.

Quarantine—Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection

Infected—Host is an active threat to other hosts; network access should be severely restricted or totally denied all network access.

Unknown—Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined.

Identity authentication and posture validation occurs when a host requests access to a network. Through a Layer 2 or Layer 3 transport method, a network access device (NAD) retrieves posture credentials from the host. The amount of network access granted to the host is determined by its identity and/or level of compliance with posture policy rules. These posture credentials are typically based on the state of the host operating system as well as applications such as anti-virus, firewall, or intrusion detection systems. A sample anti-virus policy that a network administrator might implement with NAC could be "require the anti-virus application from vendor XXX, with scan engine version Y.Y.Y to be enabled and have signature file version Z.Z.Z, otherwise assign a quarantine role and restrict network access for the host to only the anti-virus server."

NAC System Components

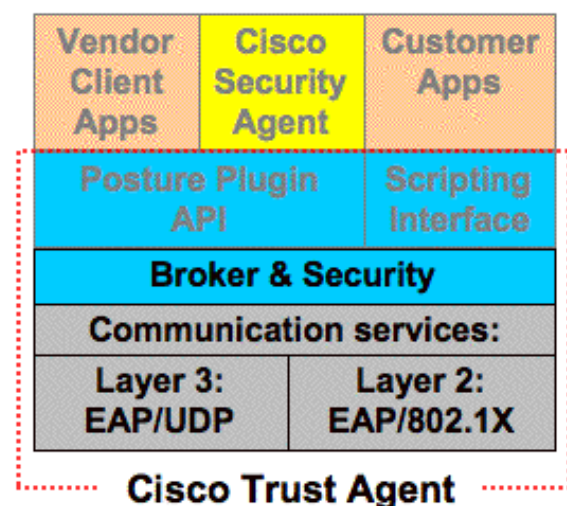
CISCO TRUST AGENT (CTA)

A posture agent (PA) serves as the single point of contact on the host for aggregating credentials from all posture plugins and communicating with the network. This module also provides a trusted relationship with the network for the purposes of exchanging these posture credentials. The Cisco Trust Agent (CTA) is Cisco's posture agent for NAC.

CTA maintains a record of registered posture plugins by both *vendor* (e.g. McAfee, Symantec, Trend Micro, Cisco) and *application type* (e.g. PA, OS, AV, FW, etc). It multiplexes and de-multiplexes posture requests and posture notifications between the posture plugins and

the network. It also determines whether there has been a posture change in the PPs and notifies the NAD using the mechanisms available in the various EAP transports. Note that CTA does not interpret credentials and notifications communicated between the network and a posture plugin or vice versa. The only processing that CTA performs is the necessary multiplexing and de-multiplexing of requests and responses to and from the plugins and network. The Cisco Trust Agent architecture is shown below.

Figure 4. Cisco Trust Agent Architecture



The PA does provide its own plugin to provide credentials about itself, e.g. name and version of the PA, and to provide a minimal set of credentials about the host, e.g. host operating system information. The Posture Agent also supports a notification request to display an informational message to the user.

CTA SUPPLICANT

The CTA supplicant is a NAC-enabled 802.1x supplicant. NAC-enabled means the supplicant is able to use the EAP-FAST protocol to carry both identity and posture information within the 802.1x transport. This allows the supplicant to provide not only user and machine identity, but machine posture information as well.

Currently, the CTA supplicant supports wired interfaces. If wireless support for Cisco NAC is needed, a supplicant that supports both wired and wireless can be obtained from one of the Cisco NAC partners.

POSTURE PLUGINS

A posture plugin is a dynamically loaded library (DLL) that resides on a host and provides posture credentials to a posture agent residing on the same device. There is one posture plugin for each vendor and application type. The plugin acts as an adaptor between the CTA and the respective client software in order to handle posture credentials in posture requests and responses.

Posture credentials provided by a posture plugin may include but are not limited to:

- Software name—Software product name
- Software version—Version of the software product (e.g. 4.2.0.75)
- Software release date—Publication date of the software
- Software enabled/disabled—Whether the software is currently running on the host
- Configuration parameters—May include standard or proprietary application settings and configurations

- **Machine-Posture-State**—Machine Posture State is provided by CTA to inform ACS about the status of the machine when it boots. One of the following three states can be reported: Booting, Running, or Logged in (on Windows platforms).

Posture credentials and notifications received from the Posture Agent include the following:

- **Application Posture Token (APT)**—Posture of the specific application, agent, or software component after posture validation by the AAA server.
- **System Posture Token (SPT)**—Posture of the entire host as a result of validating all credentials (PA, OS, AV, FW, IDS and any others that may be validated)
- (Optional) Information necessary for remediation, e.g. actions to execute, server URL for purposes of remediation

The posture plugin also has the ability to notify the Posture Agent that a change in posture has occurred since the last request for posture credentials from the Posture Agent.

Note: The inter-process communication mechanism between any client software and posture plugin is entirely optional and vendor specific since the Posture Plugin may directly scan registries or files.

AGENTLESS HOSTS

Despite the proliferation of Ethernet as the standard for network connectivity, many Ethernet-enabled devices do not support the IEEE 802.1x supplicant functionality in their native protocol stacks. Such a host is considered to be agentless; it does not have native 802.1x supplicant and therefore is unable to respond to challenges by the network for admission.

There are currently large classes of network-attached devices that fall into this agentless category. While this still includes devices such as desktops and server computers, a larger class includes printers, photocopiers, cameras, phones, sensors, and many other specialized appliances. Reasons for this lack of support include:

- The protocol stack of the host operating system is not supported by the Cisco Trust Agent (CTA) or an 802.1x supplicant.
- The appliance does not have enough storage, memory or CPU.
- The supplicant functionality is available but not enabled by default.
- The host has a personal firewall enabled that blocks Layer 3 (L3) network authentication challenges.

Without a mechanism in the protocol stack to gather identity or posture credentials from these hosts, network admission controls cannot be administered universally, which impacts deployments. To mitigate this, NAC has multiple methods for dealing with agentless hosts involving whitelisting or blacklisting against a static list of IP or MAC addresses. The audit server component has been introduced to the NAC solution to eliminate the maintenance of static lists and rely on dynamic inspection of hosts using vulnerability assessment techniques.

The mechanisms for the handling of agentless hosts are discussed further in this document. Additionally, the configuration details for each of these methods are available in the NAC Configuration Guide.

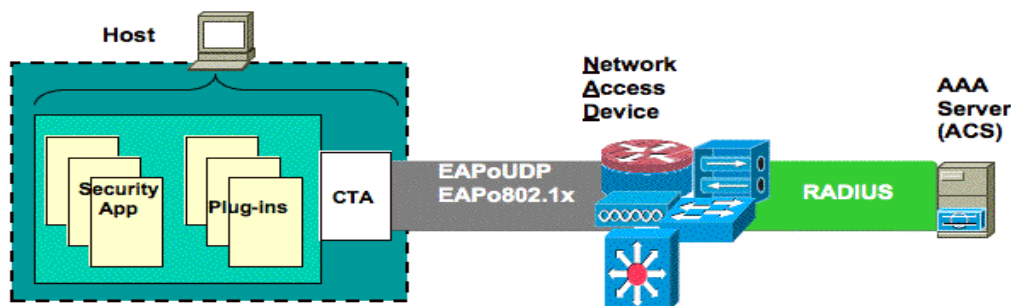
NETWORK ACCESS DEVICES (NADS)

The Network Access Device (NAD) enforces network access based on an authorization policy from the AAA server and communicated via RADIUS attributes.

Upon detection of a host on a Layer 2 (L2) or Layer 3 (L3) port or interface, the NAD attempts to establish communication with a PA on the host before making a request to the AAA server to start the authorization process. Communication between the NAD and PA is done

via an L2 mechanism (802.1x) or an L3 transport (EAPoUDP) depending on the NAD. The PA response is forwarded by the NAD to the AAA server to initiate an access request. After the host trusts the AAA server and they negotiate a secure tunnel, the PA responds with its identity and posture credentials. In this process, the NAD acts as a relay agent between the host and AAA server for all messages in the exchange. When the authorization is completed by the AAA server, the server sends a network access profile to the NAD for enforcement on the host.

Figure 5. Host, NAD, and AAA Server Communication



Between posture validations, the NAD may issue periodic *status queries* to determine that each host using the NAD is still the same device that was first postured and that the host's posture has not changed (EAPoUDP deployments only). This mechanism is a challenge-response protocol that does not involve the AAA server, nor does it require the posture plugins to resend any credentials. It is used to trigger a full posture revalidation with the AAA server when the host's credentials have changed (e.g., to revalidate the host after remediation) or a new host connects with a previously-authorized IP address.

The NAD also supports a local *exception list* based on IP or MAC address so that certain hosts can bypass the posture validation process based on system administrator configuration. Alternatively, they can be configured to query the AAA server for access policies associated with hosts that do not have a Posture Agent installed, also known as agentless hosts.

CISCO SECURE ACCESS CONTROL SERVER (ACS)

The Cisco ACS server is a AAA (authentication, authorization, and accounting) server with RADIUS capabilities that extend beyond identity authentication to handle the authorization of posture credentials from a host. The ACS server then maps the resulting policy decision to a network access profile that is provisioned on the NAD for enforcement. The ACS server can be configured to delegate posture authorization decisions to one or more external *posture validation servers*. This can be performed to improve scalability, delegate the decision for a specific policy domain, or handle proprietary attributes.

The ACS server maintains a record of local and external *policy databases* using vendor and application type of the attributes as a domain or namespace. The ACS server multiplexes and de-multiplexes posture requests and responses to and from these databases. Each policy database has one or more policies, each containing a set of administrator-defined *rules*. Each policy evaluates a set of posture credentials (per vendor and application type) to create an *application posture token* (APT) which defines the compliance level of that component. The ACS server then consolidates all APTs into a final posture assessment called the *system posture token* (SPT), which is the APT that represents the greatest amount of non-compliance. The SPT is then mapped to an access profile that is provisioned to the NAD for enforcement on the host. The APTs, SPT, and any optionally configured user or action *notifications* are also sent to the PA to complete the authorization cycle.

REMEDIATION SERVER

A remediation server is a repository for host software updates that are made available for a host or client to meet policy compliances within an organization. The server may host items such as OS updates, security patches, host agent software, and other software components.

When a host is determined to be in a non-compliant state based on current posture information, the user can be forwarded to a remediation server through URL redirection. There the remediation process can begin by walking the user through the steps for the host to download the necessary software to become compliant with security policy.

A remediation server is often part of a larger remediation solution that includes both server and client portions.

POSTURE VALIDATION SERVER

A posture validation server (PVS) is any server that authorizes sets of posture credentials into one or more APTs. While the ACS server is an instance of a PVS, the term is typically used to describe a delegate server to assist in the authorization of domain-specific posture credentials. For example, an anti-virus (AV) server may act as a PVS for making AV-specific posture decisions since the AV server knows the latest scan engine and signature file versions.

A PVS is expected to implement the following functions using the Host Credential Authorization Protocol (HCAP) for communication between the AAA server and the PVS:

- • Accept a posture credential request from a AAA server or PVS
- • Authorize the credentials against a compliance policy or further delegate them to another PVS
- • Respond to the AAA server with the following:
 - Application Posture Token (APT); the result of validating the posture credentials
 - (Optional) Posture Notifications to aid in domain-specific remediation of the host. Examples include actions to execute, URL of remediation server, etc.

AUDIT SERVER

The newest component in the NAC solution is the audit server, which applies vulnerability assessment (VA) technologies to determine the level of compliance or risk of a host prior to network admission. VA techniques such as network scanning, remote login, or browser-based agents are typically used to gather information that would ordinarily be provided by the IEEE 802.1x supplicant or CTA. The audit server component is supplied by certain vendors in the Cisco NAC Program to give customers the ability to choose a VA vendor and technology that best fits their policy needs and deployment requirements.

The audit server uses the Generic Authorization Message Exchange Protocol to communicate audit information with ACS. ACS is responsible for triggering the audit process for agentless hosts with the audit server. While the audit server is performing the audit process, ACS periodically polls the audit server for an audit decision. When the audit server completes the audit process it reports the posture state of the host to ACS.

For the most current and complete list of vendors and products that integrate with the Cisco NAC Framework, please visit the [Cisco NAC Program](http://www.cisco.com/go/nac/) page on <http://www.cisco.com/go/nac/>.

Reporting

Information on NAC-related events such as failed and passed authentications and the reasons for each can be viewed in the ACS reports. The fields displayed in each report can be customized so that relevant or additional information can be viewed if required. The reports in ACS are a primary means for troubleshooting NAC authentication issues.

In addition, the NAC information in ACS can be exported to the Cisco CS-MARS (Cisco Secure Monitoring Analysis and Response System) appliance. The MARS appliance provides both event correlation as well as a visual insight into the network for NAC events.

Several default reporting options are available for NAC in the MARS appliance. An administrator can either choose to view one of the NAC default reports, such as the total number of current quarantine hosts, as well as create custom reports.

MARS also allows the administrator to quickly view a NAC-related incident and determine where the client is physically located within the network to the level of the specific switch and switchport.

Protocols

The following sections provide descriptions of protocols utilized in Cisco NAC.

EAP

Extensible Authentication Protocol (EAP) is a request and response protocol that is capable of exchanging identity and authentication credentials between a host and AAA server. EAP supports a variety of authentication methods including MSCHAPv2, certificate based authentication, and PKI. EAP is defined in RFC 2284.

Extensions have been made to the EAP protocol for NAC which include the following:

- • **EAP-TLV**
- • **EAPoUDP**

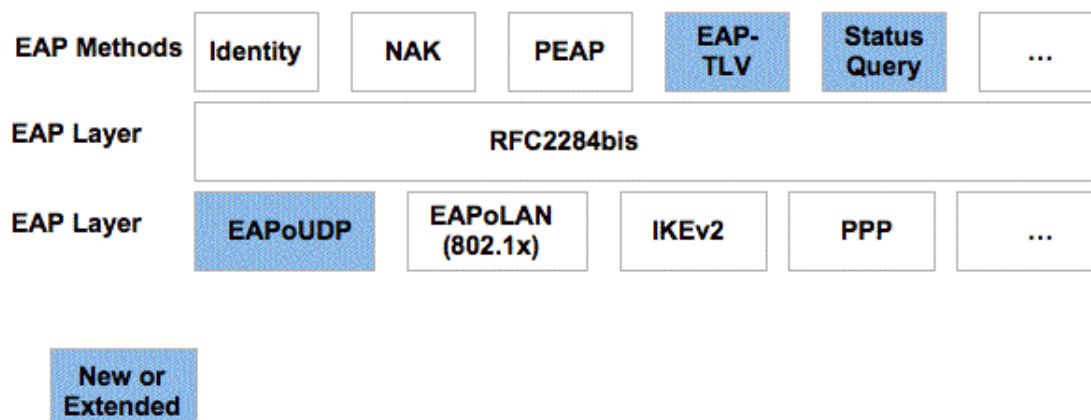
The EAP Type Length Value (EAP-TLV) extension has been added to carry posture credentials, adding posture attribute value pairs (AVPs) and posture notifications.

An extension called Status Query has also been added for NAC. This is a new EAP method for securely querying the status of a peer without a full credential validation. This is a function for NAC L3 IP and NAC L2 IP only.

EAP over UDP (EAPoUDP) provides the capability within the EAP protocol to transport EAP information for NAC L2 IP and NAC L3 IP.

The following figure displays EAP and EAP extension information.

Figure 6. EAP Overview



EAP-FAST

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS based RFC3748 compliant EAP method. A draft for EAP-FAST has been submitted by Cisco to the IETF. The draft is available on the IETF website:

<http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-03.txt>.

The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.

EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process. The tunnel establishment relies on a Protected Access Credential (PAC) that can be provisioned and managed dynamically by EAP-FAST through AAA server.

- Phase 1—Use the PAC to mutually authenticate host and server and establish a secure tunnel.
- Phase 2—Perform client authentication in the established tunnel.
- Optional Phase 0—Used infrequently to enable the client to be dynamically provisioned with a PAC.

Additional information on EAP-FAST and the options available for NAC are discussed in the deployment section of this document.

HCAP

Host Credential Authorization Protocol (HCAP) provides communication between an ACS server and a NAC partner's posture validation servers. HCAP uses an HTTP(S) session to provide secure communication and exchange of EAP-based credentials between ACS and vendor servers.

ACS forwards client credentials to one or more vendor servers and receives posture token response and optional notification messages from each vendor server.

Note: HCAP is the protocol used for communication between ACS and PVS (Posture Validation Servers) such as anti-virus servers.

GAME

Generic Authorization Message Exchange (GAME) provides communication between an ACS server and a NAC partner's audit servers. GAME uses an HTTPS session to provide secure communication and extend the security assertion markup language (SAML) between ACS and a partner audit server.

ACS can trigger the posture validation of agentless hosts (host without CTA) by a partner audit server. The ACS server then polls periodically for audit decision from the audit server. When the audit process is completed the audit server responds to ACS with a posture state for the client or host.

NAC Assessment Methods

Cisco Network Admission Control (NAC) can use a variety of methods to trigger identity and posture validation of hosts attempting to access the network. In most cases the method used is dependent on the existing security policy and the type of Network Access Device through which the host is attempting to connect. The Cisco NAC assessment methods include:

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- IEEE 802.1x and NAC L2 IP
- Agentless Hosts

NAC L3 IP

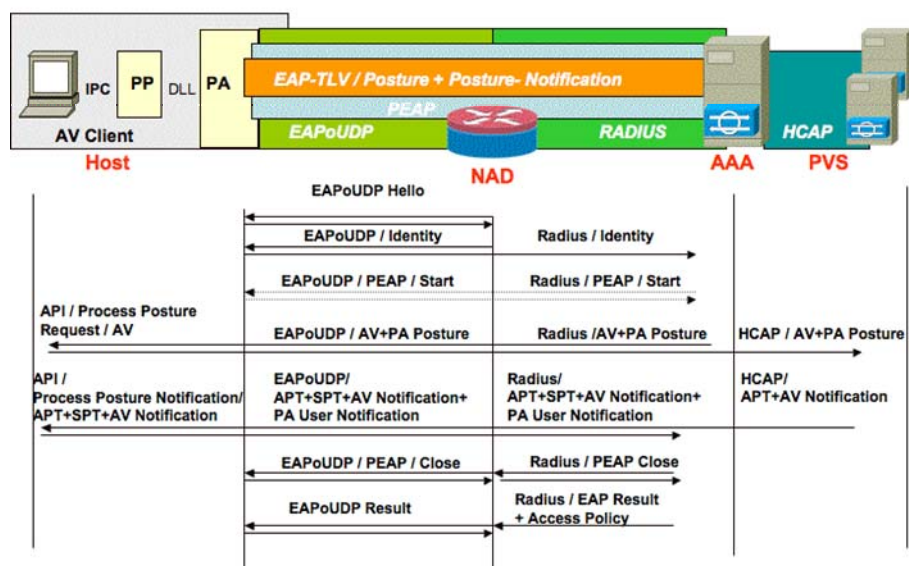
NAC L3 IP was first introduced as part of the initial release of NAC.

The NAC L3 IP posture validation process on a router is triggered when a Layer 3 packet enters the router interface on which NAC L3 IP is configured. Once the NAC process is triggered, the router sends an EOU hello message to which the client host answers with an EOU hello. Now that the NAD and client recognize each other, the NAD asks for the identity of the client. When received, this identity is passed to Cisco Secure ACS in the form of an EAP over RADIUS packet. Cisco Secure ACS then initiates a PEAP session with the client host.

Note: The router acts as a pass-through device at this point, It does not proxy any part of the PEAP session but merely re-encapsulates the PEAP packets from UDP to RADIUS.

Once the PEAP session has been established, Cisco Secure ACS queries the client for credentials from the registered software on the client. This causes the CTA on the client to query the posture plugins that have been registered with CTA for their credentials and attributes. These credentials and attributes are collected and sent to Cisco Secure ACS in the PEAP session. During this initialization phase, the packets received on the router interface are subject to any access list applied on that interface. The access list when coupled with admission control identifies which packets will and will not trigger the admission control process. The following figure shows the details of this process.

Figure 7. NAC L3 IP Posture Validation Process



When Cisco Secure ACS receives the requested credentials from CTA, the ACS server checks the credentials and attributes against the local and external policies in the matched database.

Each policy returns an APT in a single credential back to the client, along with configured actions, which are unique to each posture agent. The most restrictive of the application posture tokens are used as the SPT. The SPT determines the group into which Cisco Secure ACS places the client and the overall posture of that client. The actual enforcement rules are configured in Cisco Secure ACS group policy. Enforcement rules take the form of downloadable ACLs, URL redirection, and timer adjustments. The NAD periodically queries the host to determine if the posture of the host has changed.

The NAD can also enforce a URL redirection to cause a client to automatically go to an AV server for updates when the client attempts web access.

Cisco Secure ACS can be configured to shorten the status query value on the NAD for a particular host to help ensure that the host successfully completes the remediation process. As each application's posture is validated, the application APT returns to a healthy condition and eventually a healthy SPT. If there has been a change, such as a change in DHCP addressing or a changed DHCP client, the

status query process fails and the validation process is restarted. If no response is received from the client, the system can download a default enforcement policy to the NAD to limit the network access of the client depending on the overall network security policy.

NAC L2 IP

NAC L2 IP is similar to NAC L3 IP in that it uses EAP over UDP (EoU) to transport the posture assessment of a host. However, one primary difference with NAC L2 IP is that it is implemented at Layer 3 on a Layer 2 switchport.

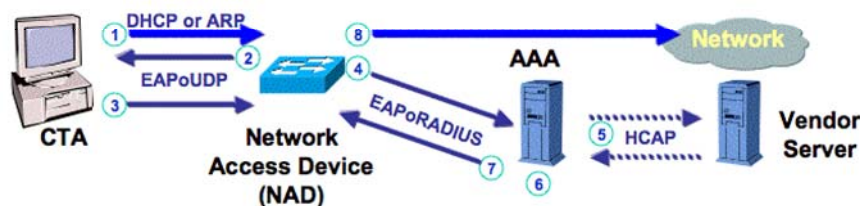
There is also no concept of an intercept ACL for NAC L2 IP. With NAC L2 IP the posture assessment of a host is triggered on the NAD when it receives one of the following from the host:

- DHCP requests
- ARP requests

When the NAD initially receives either a DHCP or ARP request from a host, the NAD starts the EoU handshake and initiates the posture validation process. If the process is triggered based on an incoming DHCP request from the client, it occurs at a somewhat earlier point than the ARP-based trigger.

The following figure illustrates this process between the host, NAD, and ACS server.

Figure 8. Posture Validation Communication Flow



1. DHCP or ARP request triggers NAD.
2. NAD triggers posture validation with CTA (*EAPoUDP*).
3. CTA sends posture credentials to NAD (*EAPoUDP*).
4. NAD sends posture credentials to AAA (*EAPoRADIUS*).
5. AAA can proxy portions of posture authentication to vendor server (*HCAP*).
6. AAA validates posture and determines authorization rights (*Healthy, Checkup, Quarantine*).
7. AAA sends authorization policy to NAD (*ACLs, URL redirection*).
8. Notification may also be sent to applications on host.
9. Host IP access granted (*or denied, restricted, URL redirected*).

After the posture state for the host has been determined by the policy server, enforcement is performed with access control lists (ACLs) on each NAD. A default ACL is configured on the switch to initially restrict network access to only necessary traffic. The default ACL, for example, should permit flows for protocols such as DHCP, DNS, WWW, and any additional default traffic that should be granted access prior to the posture validation of the host. As discussed previously, this differs from the NAC L3 IP concept of an intercept ACL in that it does not specify which traffic triggers a posture validation but rather which traffic should be allowed by default prior to a posture validation of the host. Additional details on configuring the default ACL are covered in the NAC Configuration Guide.

The ACLs for each posture token, such as healthy or quarantine, are defined in ACS as downloadable ACLs. When these ACLs are downloaded to the NAD from ACS, they are prepended to the default ACL configured on the switchport.

Additionally, NAC L2 IP can act as an independent posture validation method to supplement IEEE 802.1x identity validation. Since NAC L2 IP is independent of 802.1x, it can be configured on the same port on which IEEE 802.1x is configured. NAC L2 IP can perform posture validation of a host after the 802.1x user and machine authentication has been performed. This is discussed further in the next section.

NAC L2 802.1X

NAC L2 802.1x leverages 802.1x to provide identity information for user and host authentication with the addition the EAP-FAST protocol to also transport posture information for the host. NAC L2 802.1x triggers the assessment of a host via 802.1x on a Layer 2 switchport.

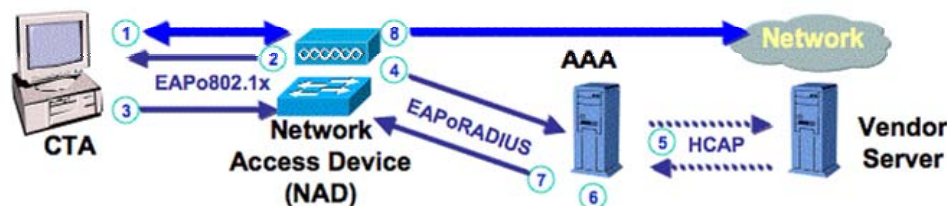
NAC L2 802.1x requires a supplicant that supports EAP-FAST for the EAP method to carry identity and posture information in the TLS tunnel. The CTA embedded supplicant supports EAP-FAST and supports EAP-GTC, EAP-MSCHAPv2, and EAP-TLS for client side authentication.

The identity information provided by 802.1x can include both user and machine information for the host. User and Machine authentication are covered in the deployment considerations section of this document.

Policy enforcement for NAC L2 802.1x is performed via dynamic VLAN assignment on the switch. The VLAN assignment per host is based on the posture token assigned. After ACS determines which posture token to assign to the host, the VLAN information is passed to the switch in RADIUS attributes 64, 65, and 81. It is assumed ACLs have been previously configured to properly segment the VLAN traffic.

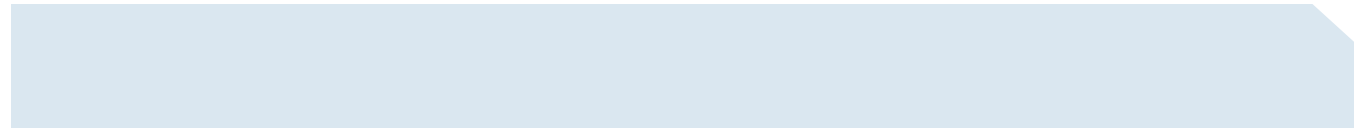
The following figure and steps illustrate the NAC L2 802.1x authentication process.

Figure 9. NAC L2 802.1x



1. 802.1x connection setup between NAD and endpoint.
2. NAD requests credentials from endpoint (*EAPo802.1x*).
3. This may include user, device, and/or posture.
4. CTA, via NAC-capable supplicant, sends credentials to NAD (*EAPo802.1x*).
5. NAD sends credentials to AAA (*EAPoRADIUS*).
6. AAA can proxy portions of posture authentication to vendor server (HCAP).
7. User/device credentials sent to authentication databases (*LDAP, Active Directory, etc.*).
8. AAA validates credentials and determines authorization rights.
9. For example, visitors given GUEST access, unhealthy devices given QUARANTINE access.
10. AAA sends authorization policy to NAD (*VLAN assignment*).
11. Notification may be sent to applications on host also.
12. Host assigned VLAN and may then gain IP access (*or denied, restricted*).

Unlike NAC L2 IP, with NAC L2 802.1x there is no concept of a status-query process from the NAD to the host. The session timeout value is used to initiate the re-authentication process. This value can be locally set on each switch or configured in ACS with RADIUS attribute 27. If the value is set in ACS it automatically overrides the value configured in the switch.



In addition to session timeout, CTA can verify the posture status of the host locally and trigger a posture validation of the host. By default, every five minutes CTA polls the posture plugins on the host to check for a status change in the partner software. If a change has been discovered, the CTA supplicant sends an EAPoL (EAP over LAN) start to the switch to begin re-authentication and posture assessment.

There is a new feature within CTA 2.0 and NAC L2 802.1x called Asynchronous Status Query (ASQ). ASQ allows the security software residing on the host to update and alert CTA, via posture plugins, to any status change involving that software on the host. For example, if the Cisco Security Agent detects a change on the local host, an update is sent to CTA via the posture plugin allowing the CTA supplicant to force a re-assessment of the host by the switch. The Cisco Security Agent is the first software to implement support for the ASQ feature.

Detailed deployment options and considerations for NAC L2 802.1x are discussed below.

AGENTLESS HOSTS

An agentless host is a host that does not have CTA installed and therefore cannot participate in the identity and posture validation process.

An unknown host, in a general sense, is a client without posture agent software loaded. These clients might be IP devices such as IP phones, network printers, or other IP devices. Any PCs or workstations that do not have the CTA or posture agent software loaded are also considered unknown hosts. These workstations may be running MacOS, Solaris, or unsupported versions of windows.

Static Exceptions (Whitelisting)

One way to handle an unknown host is to configure a static policy in Cisco IOS software or centrally in ACS which includes the IP address and the MAC address of the host. Based on the exception created, the host is allowed to bypass the posture validation process to access the network.

Dynamic Audit

A recent addition to NAC is the use of an audit server to perform dynamic auditing of agentless hosts. With dynamic audit a policy is created to trigger the audit or vulnerability scan of an agentless host when they connect to the network. The audit result includes a posture token which is forwarded to ACS and assigned to the host. The host is then granted network access based on the posture token assigned.

The options available to administrators for agentless hosts vary depending on which assessment method(s) is used. This is discussed in the deployment consideration section of this document.

NAC Policy Strategies

NAC is a security solution for enforcing network access using a collaborative security policy for user identity, host identity, and host posture compliance. The NAC Framework may potentially delegate access decisions to multiple security applications for a single authorization decision. Therefore it is important to first understand and create a comprehensive security policy in order to know the goal of your network admission control effort.

Designing a Network Admission Policy

The basis of all authentication, authorization, and accounting (AAA) security technologies is to assess and control who can access what and when and from where and how. Traditionally, the “who” was simply a user and/or host identity in the form of as a username and password, digital certificate, one-time token password, or even biometrics. Cisco Network Admission Control (NAC) has extended AAA authentication beyond user and host identity to include a complete compliance validation of the host’s posture—its hardware and software configuration. With the aid of security applications from the NAC Program, the network may verify the following items before permitting network access:

- The operating system type, version, and patch level
- Registry settings, file existence, and sizes
- Cisco Security Agent (CSA) configuration, and state
- Anti-Virus software version, signature file level, and state
- Personal firewall engine version, rule set, and state
- The existence or absence of specific hardware components

This evolution was necessary since viruses and worms can quickly and easily exploit vulnerabilities, on a large scale, present in unpatched operating systems and applications. This threat can be as much or more of a threat to an organization’s security and survival than a malicious user or hacker. Maintaining a computer system with the latest OS patches and security software updates is critical.

POLICY CREATION REQUIREMENTS

The goal of deploying NAC is to prevent all of the problems associated with unauthorized and non-compliant network hosts. This decision encompasses more than just identity and may involve compliance of the host OS and multiple client-side agents and applications. In larger organizations, the management and operations of identity servers, desktop software, server software, application administration, network security, and support, are handled by separate teams of subject matter experts. Bringing all of these teams together to create and maintain a comprehensive and collaborative security policy can be time consuming and difficult.

A NAC security policy must be collaboratively built and maintained by representatives from your network (LAN, WAN, wireless, remote access, and extranet) and information technology (desktop, server, applications, and support) teams. Decisions that must be made include:

- Who is responsible for policy creation and policy enforcement?
- What are the current requirements for network admission across the company? Are they the same across all access methods (wired, wireless, VPN, extranet, etc.).
- What is your policy on unmanaged or non-standard machines on your network (labs, guests, consultants, extranets, kiosks, etc.)?
- What are your current security policies for authentication and application compliance? Is this enough or do you want to increase the scope of validation?
- How do you do network segmentation now? VLANs? ACLs?

- How often will the policy representatives meet to discuss ongoing policy updates and changes?
- What is the quorum for making changes, however small?
- Do you have management support for business case of enforcing your security policy? Users do not like being managed and you may face backlash.

Once your organization has a basic agreement on the kind of policy desired and how it will be created, you can begin to formally define it.

POLICY DEFINITION

Network admission policies are structured around several basic elements of the authorization decision. The list below explains each one and gives multiple examples of instances or options.

Who—The identity and group of the network access requestor:

User Identity—Differentiated access based on user and group or guest privilege

Host Identity—Differentiated access for corporate asset vs. unmanaged hosts

Host Posture—Hardware and software inventory and security software state

Where—A location with differentiated policy:

Geographic—A city, country, or other region with specific policy rules or laws

Logical—A logical location with unique security requirements such as a lobby, lab, or high security area

When—Contextual access restrictions and logged events for accounting and auditing:

Temporal—Time-of-day, day-of-week, and other time limitations

Quotas—Session limits based on account balance, time, or active instances

Logs—Auditing resource usage and security forensics.

How—The network access method, its protocols, and policy requirements, if any:

LAN—Access via an 802.1x enabled, Layer 2 (L2) switch port

Wireless—Wireless access within and around buildings

WAN—Chokepoints within a Layer 3 (L3) routed network

VPN—Remote access

What—The network privileges and features based on the capability of the access method:

Open—No access requirements or restrictions

Groups—Logical segmentation of the network based on groups or roles

Extranet—Partner connectivity for outsourcing or sharing resources

Utilities—Printing services and other dedicated devices

Guest—Internet-only guest access

Before getting overwhelmed with all possible scenarios within your organization, it is best to start with some simple examples. A security policy does not have to be complicated to be effective.

A simple example would authenticate employees and still allow guests and unauthorized users to access the Internet:

| Who | Where | When | How | What |
|-----------------|-------|------|--|------|
| User: Employees | Any | Any | IEEE 802.1x (wired & wireless) VPN + Token Card | Any |

| | | | | |
|-------------|-----|-----------|------------------|---------------|
| User: Guest | Any | 7am – 6pm | Wireless hotspot | Internet only |
|-------------|-----|-----------|------------------|---------------|

Another company that is more concerned about access to their sensitive records and potential problems with viruses will want a more restrictive policy. This one might be described as “Corporate Asset, Image, and Employee or Else”:

| Who | Where | When | How | What |
|---|-------|------|-----------------|--------------------|
| User: Employees Host: CorporateAssets Posture: OS patches + AV | HQ | Any | NAC L2 802.1x | Any |
| User: Employees Posture: OS patches + AV | VPN | Any | VPN + NAC L3 IP | Any |
| User: CallCenter Host: CorporateAssets Posture: OS patches + AV | India | Any | NAC L2 802.1x | Intranet only |
| Printers | Any | Any | MAC-Auth-Bypass | Print servers only |
| Guest | Any | Any | None | None |

The examples above are very basic, but the combinations of access methods, credential requirements, and partitioning options are still apparent. Document all of the scenarios you need to address, but try to minimize the ways that you handle them. If you must have many different policy options, increase the requirements incrementally in phases to prevent changing too many things at once.

CREDENTIALS

Identity Credentials

Identity is unique name of a person, device, or the combination of both that is recognized by an authentication system. The identity credentials are objects, such as passwords or certificates, used in authentication transaction. In the context of IEEE 802.1x these credentials determine if the authentication system recognizes the 802.1x supplicant on the switch and determines if it has the correct credentials to gain access to the network and what the appropriate authorization is for the supplicant. As has been stated, NAC-L2-802.1x has allowed identity and posture credentials to be passed in one EAP conversation to make an admission decision on both types of credentials. A network administrator needs to understand that when using NAC-L2-802.1x, access is only permitted within ACS when identity credentials successfully authenticate the supplicant. If identity authentication fails, no posture credentials are checked and the supplicant is denied access to the network.

To better understand the functionality of NAC-L2-802.1x, it is important to realize that there are generally two types of identity credentials that can be sent from the supplicant to the NAC system. This has design implications for the device configuration depending on the type of credentials that are being checked.

Generic Device Credentials

The first credential is called a device credential. With this authentication mechanism the machine is authenticated in advance of the user of the computer. This type of credential is used if the device needs to gain access to the network to perform some function before user authentication or if the device is not normally used by end users, such as servers or printers. Device credentials can be stored on the host (such as passwords) that the supplicant can access at device startup in order to authenticate itself to the NAC system.

Microsoft Machine Credentials

In Microsoft environments, Microsoft calls their device credential login mechanism machine authentication. Microsoft introduced the machine authentication facility to allow the client system to authenticate using the identity and credentials of the computer (Active Directory System ID or machine certificate) at boot time so that the client can establish the required secure channel to the domain to update

and participate in the domain group policy object (GPO) model. Machine authentication allows the computer to authenticate itself to the network using 802.1x, just after a PC loads device drivers at boot time.

User Credentials

At boot time, the Windows operating system uses machine authentication to authenticate using 802.1x and to subsequently communicate with Windows domain controllers in order to pull down machine group policies to alleviate the problem of domain GPOs being broken by the introduction of 802.1x.

After the user presses Ctrl+Alt+Delete, the Microsoft Graphical Identification and Authentication (GINA) dialog pops up on the PC for the user to enter their credentials. When GINA is presented, a user can login to the computer or the Windows domain and the username/password used for login can be used as the identity credentials for 802.1x authentication. This second type of credential is commonly referred to as user authentication.

Posture Credentials

Posture credentials are hardware and software attributes conveying status and configuration information that can be used for posture compliance with your security policy. These attributes can be anything that an application vendor and network administrators considers important to check on the client machine. The following table shows examples of the basic data types of attributes that the CTA can send.

| OctetArray | Integer32 | Unsigned32 | String (UTF-8) | IPv4Addr |
|------------|---------------------|---------------------|-------------------------------------|------------------|
| =, != | =, <, >, !=, >=, <= | =, <, >, !=, >=, <= | =, !=, contains, starts with, regex | wildcards & mask |

All NAC credentials—or attributes—are hierarchically organized using a namespace to differentiate the properties of each vendor's applications on a single host. The NAC namespace consists of the vendor, application type, and attribute name, which is often expressed in the following way:

Vendor : Application-Type : Attribute

An example attribute for the Cisco Trust Agent is Cisco:PA:OS-Type. The following chart shows information that is natively available to CTA and examples of what other application posture plugins can provide. Each vendor generally provides attributes common to a particular application type and may also offer additional attributes for proprietary or product-specific features.

| Application: | CTA | CTA | CSA | Anti-Virus |
|--------------|--|--------------------------------------|--|--|
| Vendor: | Cisco | Cisco | Cisco | Various |
| App-Type: | PA | Host | HIP | AV |
| Attributes: | PA-Name PA-Version OS-Type OS-Version OS-Release OS-Kernel-Version Machine-Posture-State | ServicePacks HotFixes HostFQDN | CSAMCName, CSAOperationalState CSAStates CSAVersion TimeSinceLastSuccess fullPoll | Software-Name Software-ID Software-Version Scan-Engine-Version DAT-Version DAT-Date Protection-Enabled |

A network designer needs to be aware that they may need additional application plugins in order to make admission control decisions that support their security policy. For instance, suppose the corporate security policy dictated that a client machine was required to not only have the latest hotfixes for the client OS, but also the latest version of the Anti-Virus DAT file. In this instance the network administrator would need an application plugin to provide this information to CTA and hence would work with their anti-virus vendor to get the appropriate AV plugin for CTA.

IDENTITY VERSUS POSTURE

NAC authorizations move beyond the simple question of identity and group membership to allow differentiated levels of access depending on identity *and* posture. This allows you to prioritize access based on either attribute. Group membership is a fundamental concern for network admission but only when the host posture is healthy. If the host posture is not healthy, the threat of a vulnerable or infected host is enough to warrant overriding the privilege of group identity with restricted access to protect against viruses and worms.

Understanding the authorization priorities between identity and posture is done by creating a table of an organization's identity groups versus posture states. The table is then filled out to show which takes precedence with each of the combinations given a particular security policy. Each group or state is then associated with a specific set of network access rights that control what network behaviors are permitted and denied.

| | Healthy | Quarantine | Unknown |
|-------------|-------------|----------------------|----------------------|
| Employees | Employees | EmployeeQuarantine | EmployeeQuarantine |
| Contractors | Contractors | ContractorQuarantine | ContractorQuarantine |
| Guests | Guests | Guests | Guests |

It is also important to note that not all network access methods are capable of providing both identity and posture credentials. Your deployment choices may be limited by the type of NAC access method as shown in the table below.

| Feature | NAC L2 802.1x | NAC L2 IP | NAC L3 IP |
|-------------------|---------------|-------------|---------------|
| Trigger mechanism | Data Link | DHCP or ARP | Routed Packet |
| Machine Identity | • | | |
| User Identity | • | | |
| Posture | • | • | • |
| Audit | | • | • |

NETWORK SEGMENTATION AND ISOLATION

After an authorization decision is made by the AAA server, it pushes the respective configuration policy to the NAD for enforcement on the host and user. The most common enforcement mechanisms are RADIUS session timers, VLAN assignments, ACLs, URL redirections, and QOS parameters. These mechanisms allow network administrators to enforce their security policy using network segmentation to permit access only to authorized network resources. The enforcement features of the NAD are entirely dependent on the network access method and the NAD's hardware capabilities.

Segmentation

Before implementing NAC, it is important to understand *what* network resources you trying to permit or deny access to and which mechanisms are possible given the capability of your NADs and your network architecture. Using IEEE 802.1x on LAN switches and wireless access points to dynamically assign hosts to VLANs is a common method of network segmentation. This ensures that they can only talk to other resources within the same VLAN and are subject to VLAN ACLs. For VPN and remote access networks, ACLs are used to limit destinations by IP address and protocol. Both mechanisms can effectively segment users and hosts from unauthorized network resources.

Isolation

Segmenting the network according to an identity and posture policy is a fundamental part of a NAC deployment. Just as critical is where in the network you choose to enable NAC to enforce these policies and effectively *isolate* any unauthorized hosts. To do this NAC should be enabled at the very edge of your network to prevent a virus-infected host from touching any other network hosts other than those used for

anti-virus and remediation. Using NAC in the distribution or core of the network might seem like a great way to minimize the number of NAC chokepoints to manage, but it does little to contain a virulent host.

Enabling NAC ubiquitously across all network edges provides the most effective defense, but it can also be used to create additional security zones within your network. NAC can be enabled on routed network interfaces, or chokepoints, to enforce additional security requirements for specific areas of the network.

Default Network Access

Related to isolation, when you create a NAC security policy you must understand your default security policy, that is, what network access is given, if any, when users and hosts are unauthorized. Scenarios involving unauthorized users and hosts cover not only hackers but include guests, contractors, and even legitimate users if there is a failure in AAA services due to scalability or availability. Regardless of the reason, these scenarios leave the users with whatever default network access is provided by the NAD. For a NAC L2 802.1x connection, no access is allowed and for NAC L2/L3 IP only what the default ACL allows is permitted. Depending on your organization's security policy and scenarios, default access may be no access, full access, Internet-only access, some customized set of network services, or all of the above.

NAC AGENTLESS HOST (NAH) OPTIONS

One of the biggest hurdles faced by all NAC deployments is not how to authorize identity and posture credentials but what to do in the absence of them. All of the NAC policies that have been discussed so far assume that all network hosts are able to respond to challenges from the network for identity and posture credentials. There are a large number of network attached devices that do not, cannot, and never will support the various protocols required for network authorization. This class of devices includes everything from network printers and photocopiers to devices with embedded or hardened OSes to PCs with personal firewalls enabled. These devices—called NAC Agentless Hosts—can be handled in several ways and at different levels of the authentication process.

Table 1. NAC Agentless Host (NAH) Summary

| NAH Method | Credentials | Pros | Cons |
|------------------------------|--|---|--|
| Static NAD Whitelisting | MAC / IP address or CDP device type Wildcarding available | Simple, distributed configuration | Weak identity authentication Distributed lists of static addresses to maintain Lack of centralized logging |
| Centralized ACS Whitelisting | MAC / IP addresses Wildcarding available | Centralized address management | Weak identity authentication Static list of addresses to maintain |
| Dynamic Host Audit | Posture from network scan, remote login or browser object download | Dynamic, posture-based assessment No static MAC / IP address lists to maintain | Additional NAC component to manage |

Static NAD Whitelisting

Both Cisco IOS and CatOS offer the ability to statically authenticate a host by its MAC address, IP address or CDP device identity. When a NAD detects a new host, it does not challenge the host if it has a static authorization pre-configured on the NAD. This also means that the ACS never receives a RADIUS request to authenticate this host or record its authorization.

Centralized ACS Whitelisting

If the NAD is unable to statically authorize the host, it may send an agentless requests to ACS if configured to do so. ACS looks up the MAC or IP address in its whitelists, called network access restrictions (NARs), and associates the host to a specific authorization group if found.

Dynamic Host Audit

The ACS may be optionally configured to delegate the authorization of a host to an audit server, a NAC component that uses vulnerability assessment techniques to obtain posture credentials since they cannot be obtained through a normal request/response challenge. This functionality is provided by third party vulnerability assessment vendors which use various techniques to discern the posture of a host. The table below has a summary of the technologies which can be used to determine which techniques will work best for your NAC deployments.

| Technology | Pros | Cons |
|-----------------------------|--|--|
| Network scanning | Fast Works with managed and unmanaged hosts | Limited utility against hosts with a personal firewall |
| Remote login | Read-only login for unobtrusive | Requires administrator account for remote login Not possible with unmanaged hosts |
| Downloadable browser object | Bypasses personal firewalls | Requires user interaction to download the browser object User permissions may limit scope of assessment |

Every organization must address the issue of agentless hosts with NAC and no single NAH method is ideal. Organizations will likely need to utilize multiple NAH methods to effectively handle every admission scenario for agentless devices.

Patch Management Integration

The Cisco NAC Framework provides an architecture and mechanism for authorizing and enforcing network access based on identity and posture credentials in accordance with a security policy. A NAC enabled network does not directly perform the remediation of non-compliant hosts through disinfection, signature file updates, OS patching, and client software distribution. The actual remediation of the host must be performed by the user, a support team, or a patch management solution which may be facilitated by the quarantine network segment. Integrating an automated patch management solution with NAC is a cornerstone for deployment success.

PROCESS

Ideally, an organization's client software distribution strategy and anti-virus services will keep all systems patched and updated in a timely manner. When this happens, all hosts should be admitted to the network with a Healthy posture assessment and segmented solely on the basis of identity. When this update process fails, regardless of the reason, the host will be quarantined by the network and render the host and its user, unproductive on the network. When this happens, the host machine must be remediated as quickly as possible to minimize the impact of quarantining on user productivity and experience.

Expecting all end users to keep their systems invulnerable and virus free is unrealistic, so organizations must have a patching strategy for quarantined hosts. A patching solution can be anything from a support technician that walks over with software CDs to a web server containing all required software to a patch management solution from a patch vendor. It is the responsibility of the security policy team to know what works best to return their users to a Healthy posture state as quickly and efficiently as possible. A dedicated patch management solution from a third party that integrates with NAC to automatically trigger patching upon network quarantine is recommended.

PATCH-ON-QUARANTINE

The Cisco NAC Framework includes an authorization response that can send notifications from the policy servers to the end user, the CTA, and its posture plugins. This allows the user to understand why network access is restricted, to display a web page detailing the current security policy, and to indicate the patch client opened and updates are downloading. It is this kind of collaborative security that is recommended with a tight integration between network enforcement and automated patch on quarantine.

Before investigating patch management solution options you should understand which NAC notification features are important to your deployment. Capabilities include:

- User notification via the CTA popup dialog
- Browser auto-launch via CTA to a specific URL
- Browser URL-redirection to a specific URLs
- Patch client triggered by network authorization or quarantine
- Patch client triggered by patch server notification upon network authorization

From this list you can determine if you have the necessary features to integrate your patch solution or if you need to research solutions from patch vendors. It is important to note that NAC Program participants can have very different levels of integration with the NAC Framework. Some only provide posture credentials via a CTA plugin, while others offer complete integration between ACS and their own posture validation service with HCAP and customized client notifications. It is recommended that you ask each patch vendor what NAC integration options they offer to provide the easiest and most efficient patching solution.

NAC Scalability and Availability

Nearly every network has some form of AAA, but is usually only for VPN or wireless access. NAC changes this and requires authorization upon network ingress for every host and subjects them to ongoing posture revalidations. The increased utilization of the AAA infrastructure has two implications: the AAA servers and their delegates must be scaled for the increased demand and made highly available as a critical network service. Failure to increase both scalability and availability of the AAA infrastructure could result in legitimate users and healthy hosts from being productive.

The NAC Framework architecture was designed for centrally managing an extensible security policy to enforce network access across a very large and heterogeneous network edge. In spite of this design, an understanding of the primary performance factors and anticipated bottlenecks within the architecture is critical for success. This will help you to anticipate which components are the most critical, calculate how many you need, and where to focus your performance tuning efforts.

SCALABILITY

Measuring the scalability of a NAC deployment all comes down to one thing: the number of authorizations completed in a period of time. This is typically rated in transactions per second or TPS.

Users and Hosts

The size of your network, measured in users and hosts, is the first factor in determining the scale of your NAC infrastructure. This provides an initial count for the minimum number of authorizations per day that you can expect on your AAA servers. If your organization's security policy only requires user identity or only host posture to be authenticated, then you do not need to count both.

User behavior throughout the day must also be considered. In a single day a user may connect from home via VPN, come into the office and connect to the LAN, go to meetings and roam wirelessly, go back to their desk, restart their computer after installing updates, and finally check email via VPN before going to bed. Each of these events and more may trigger an additional authorization depending upon the security policy and the protocols used.

Individual users rebooting or roaming throughout the day should average out to a normal load on the AAA services. The real problems come in form of usage spikes, when hundreds or thousands of users request access in a relatively short period of time. It could be as simple as everyone turning on their desktop computer at the start of the day to an unexpected power outage and everything coming back online at the same time. Try to account for these events if they can be anticipated.

Another area of scalability that your users and hosts will impact is on the size of your server and storage systems. Besides the larger volume of transactions, it means more RAM and disk storage on your backend servers. With so many new authentication events and regulations concerning privacy and auditing trails, long term storage needs could grow quickly.

Cisco Secure Access Control Server (ACS)

All requests for network admission must be authorized by the Cisco Secure Access Control Server (ACS), the only AAA server that currently supports all of the NAC protocols and methods. This is because ACS is the central policy engine for coordinating all NAC authorization decisions. For this reason, ACS is the single most important component in the architecture when trying to scale a NAC deployment. There are several factors in the ACS server and security policy that will have a large impact on its ability to scale.

Protocol Authorization Rates

There are many different network authentication protocols to choose from because each one offers different levels of security and features which correspond directly to rates of authentication. Some are very simple and insecure request/response protocols, while others require many roundtrips between the host and AAA server for negotiating an encrypted tunnel and delivering required credentials. Using the authorization rate of your authentication protocols with your TPS count you can calculate the average number of ACS servers are required in your deployment.

NAC Timers

There are a few timers used in NAC that affect the scale of the network. Each timer has a global default value in the Cisco IOS of each NAD. These global IOS values may be overridden first by an IOS configuration command and secondly on a per session basis from the ACS. The use of conservative numbers—long intervals—is recommended at first, then lowering them as authorization performance allows.

Session Timeouts / Revalidations

The Session Timeout (RADIUS attribute 27) triggers a complete revalidation of the user and host credentials in NAC. This is the *most critical* timer affecting AAA scalability since it controls the revalidation period for every host in the network.

EAP-over-UDP Status Queries

The EAP-over-UDP (EoU) protocol is used to challenge hosts for their posture over Layer 3 (L3) connections. In between revalidations from the RADIUS Session Timeout, the NAD initiates a Status Query (SQ) to periodically poll the authorized host. The status query provides three functions:

1. It detects if there is still a host at the previously authorized IP address. There is no way to know if the host has left a layer three network without polling.
2. It cryptographically verifies that the host is the same using the EoU session key provided by the ACS upon authorization. If the verification fails, a revalidation occurs.
3. It asks the Cisco Trust Agent if the posture has changed since the last revalidation or status query. If the posture has changed, the host posture is revalidated.

Status queries are lightweight operations initiated by a NAD against its hosts and have negligible impact on the NAD performance. This timer helps to reduce the need for frequent revalidations with ACS by allowing the NAD to detect posture changes asynchronously within a shorter interval.

Hold Period

NAC agentless hosts that are not authorized with EAP-over-UDP are left with only default network access. When this happens, they are not challenged for their posture again until the hold timer expires. This effectively ignores hosts that repeatedly try to initiate an authorization and create a denial of service attack.

Other Scaling Limitations

There are other limitations in ACS' configuration that do not hurt actual performance but do limit its ability to scale in some deployment scenarios.

- ACS has a maximum of 50,000 addressable entries for network access devices. Rather than using individual IP addresses for each NAD, ranges of IP ranges should be considered. Using a single wildcard entry (*.*.*) is recommended as a best practice to avoid continually updating the list of NADs in the ACS GUI.
- MAC-Auth-Bypass authentications are used in NAC agentless hosts scenarios to match MAC addresses within a whitelist. ACS has a limit of 10,000 MAC addresses per network access profile (NAP).
- ACS can also delegate host posture decisions to audit servers based on MAC address matches. ACS supports up to 1024 MAC addresses per audit server configuration.

Scaling Calculations

The following recommendations provide guidelines on how to scale the Cisco Secure ACS for a Cisco NAC deployment. The number of ACSes required to support a specific size of user database depends on many factors. Assume a minimum of one transaction per day per user on average. Increase the average transaction count based on some of these anticipated timers and behaviors:

- RADIUS session timeout value
- VPN remote access logins
- Multi-homed access on wired and wireless network interfaces
- Wireless roaming
- Restarts due to patches and general operating system and application glitches
- Multiple devices per user (desktops, laptops, PDAs, etc.)
- How often the host posture might change

With this initial count, you can now approximate the number of transactions per day:

$$\text{Transactions_per_Day} = \text{Transactions_per_User_per_Day} \times \text{Number_of_Users}$$

Convert this to TPS by dividing with the number of seconds in a day:

$$\text{Transactions_per_Second} = \text{Transactions_per_Day} / (24 \times 60 \times 60)$$

From this average transaction rate and the ACS authentication protocol performance numbers you can estimate the minimum number of Cisco Secure ACS servers required:

$$\text{ACS_Count} = \text{Transactions_per_Second} / \text{ACS_Protocol_Authorization_Rate}$$

This number is an absolute *minimum* since it is an average for all times of the day, assumes a continual 100% load, and does not account for server downtime due to policy replication, maintenance, and an occasional link down. It is recommended that you divide the final ACS count by 0.4 to account for some of this unknown until actual rates and loads can be verified. Weighting the protocol authorization rates with your mix of network access methods may help to refine the final ACS count.

Load Balancing

To improve the performance of ACS in a NAC-enabled environment, the ACS servers can be configured for load-balancing as well as failover. Load balancing can be configured in one of two ways:

1. IOS RADIUS Server Failover

2. IOS Server Load Balancing (SLB)
3. Load balancing and failover through the use of a Content Services Switch or a Content Services Module

IOS RADIUS Server Failover

Authentication server failover has been possible in IOS since 12.1. The concept requires that multiple RADIUS authentication servers be configured in the device. Figure 1 shows an access router configured with three possible RADIUS servers. If RADIUS server 1 fails, then the router automatically, after a set timeout period, contacts RADIUS server 2 to authenticate the two clients. Similarly, if RADIUS server 2 fails, then the router attempts to authenticate clients using RADIUS server 3. The timeout periods can be configured using the commands below.

There are several command options which provide better control over the performance of the router while attempting authentication:

- **Timeout**—Represents how many seconds a router waits for a reply to a RADIUS request before retransmitting the request. The default value for the timeout is 5.
- **Retransmit**—Specifies the number of times a RADIUS request is resent to a server with a default value of 3.
- **Deadtime**—Represents how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication. The default value for deadtime is 10 minutes.

Configuring appropriate values for these three settings can help improve the authentication performance of the router. To minimize the time required to failover from one ACS server to another, values should be chosen such that they are short enough to initiate failover but not so short that they cause the router to timeout unnecessarily and mark a server as non-responsive. Testing has shown that the default values provide good performance for NAC during ACS failover. If necessary, reduce the retransmit tries from 3 to 2, the timeout from 5 seconds to 3 seconds, and the deadtime to 2 minutes. This provides 6 seconds before the router decides that an ACS server is not responding and moves on to the next server. It also provides 2 minutes for the non-responsive server to recover or restart.

The **aaa group server** command provides a way to group existing server hosts, which makes it possible to select a subset of the configured server hosts and use them for a particular service. More information about configuring multiple RADIUS servers in Cisco IOS can be found at http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d583.html.

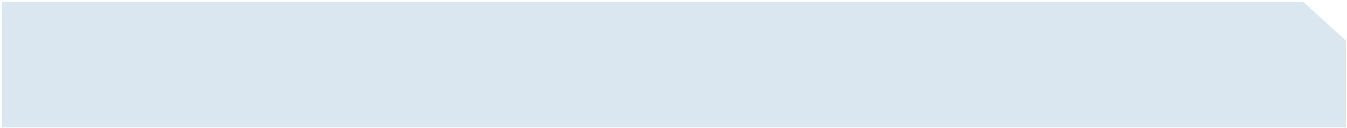
IOS RADIUS Server Load Balancing

RADIUS server load balancing available on the 7200 router and the 6500 series switch platforms can be achieved through IOS. This example utilizes the topology shown in Figure 2 above. In this case the RADIUS servers are placed together into an AAA server group as described above. Additionally, to optimize the performance of the AAA server group for NAC authentication, the load-balancing algorithm should be set to “Weighted Least Connections” (from the default “Weighted Round Robin”).

The above example load balances both RADIUS authentication (occurring over UDP port 1812) and RADIUS accounting (occurring over UDP port 1813). The sticky command specifies that connections from the same client use the same real server, providing that the interval between client connections does not exceed the specified duration. In addition, because both virtual servers are configured with the same sticky group (group 1), and the same server farm (AAAFARM). When a client first accesses one of the virtual servers, that client’s IP address is added to the IOS SLB database for group 1. The client’s IP address is then associated with the physical server chosen for the first RADIUS access request. Subsequent requests from that client for either virtual server always go to the same physical server. The above configuration causes the sticky database to store its entries for 86,400 seconds of inactivity.

RADIUS Server Load Balancing using Content Services Switch

A network load-balancing device such as the Cisco Content Services Switch (CSS) or Cisco Content Switch Module (CSM) can also be employed in a similar fashion to balance authentication requests between the NAC authentication devices and the Cisco Secure ACS



servers. In this configuration the NADs point to the virtual IP address, 192.168.45.1, which is configured on the CSS or CSM to represent the virtual ACS server.

Note: While it is possible to configure failover between sites, the best deployment would include local failover systems on the same LAN. This provides fast, reliable authentication for the local network. Load balancing can be accomplished in the same manner.

- Need for centralized access control versus distributed control at remote sites
- Cisco Secure ACS redundancy
- Geography

NAC Design Considerations

NAC Assessment Methods

Network Admission Control (NAC) is available in a variety of assessment methods in order to apply compliance policies across all network access mediums. Each method may be applied individually per access medium or at multiple locations within the network. A network designer must understand more details of the assessment methods to appropriately select the assessment method that best supports their security policies. There are five main factors in choosing an assessment method.

- Trigger mechanism
- Required credentials
- Authorization capabilities
- Non-responsive Agentless Handling (NAH)
- NAD scaling

This section of the design guide details general design considerations for the NAC assessment methods. Later sections of this design guide detail specific platform considerations for each assessment method. There is a table at the end of this section that summarizes many of the details that are discussed in the following pages.

NAC-L3-IP

NAC-L3-IP was first introduced as part of the initial release of NAC in the summer of 2004.

The primary considerations for NAC-L3-IP with the NAC release on the Catalyst switches is how NAC-L3-IP posture validation process is triggered and its support for NAH. The network designer needs to understand NAC-L3-IP since NAC-L3-IP and NAC-L2-IP are very similar assessment methods, in that both are posture-only credential checks and both support the same authorization capabilities, URL-redirect, and downloadable ACLs.

The first difference has already been summarized in the NAC architecture description earlier in the design guide. NAC-L3-IP is triggered by a Layer 3 packet entering a router interface with an IP admission ACL configured. This is different from NAC-L2-IP, which is triggered by ARP or optionally DHCP traffic on a switch interface. Both have a default security policy implemented by the interface ACL, but NAC-L3-IP can be more flexible in its trigger policy since you can customize the trigger ACL. This allows the network designer options in handling NAH device types (printers, etc.). This trigger difference, along with the platforms that support NAC-L3-IP (IOS software based routers and the VPN3000), means that NAC-L3-IP is mainly positioned for aggregation deployments (WAN, VPN, WLAN, etc.). The current deployment options currently preclude the use of NAC-L3-IP in the distribution layer of a campus infrastructure since the Catalyst Layer 3 switches do not currently support NAC-L3-IP. There is an option to front the distribution layer with a high speed IOS router like the 7200, but this is unacceptable in many cases due to the aggregate throughput of traffic demanded in the distribution layer.

The second difference is the current limitation of NAC-L3-IP in auditing NAH via a partner audit server. The current IOS releases do not support this agentless scenario. This will be supported within 6 months of NAC shipment on IOS based software routers. Other NAC-L3-IP devices, like the VPN 3000, support of audit for NAH is to be determined.

Finally, NAC-L3-IP differs from the other assessment methods in regards to what the parameters are for the scalability of NAD. Since the current devices that support NAC-L3-IP are software based forwarding devices, the primary considerations for NAC scalability fall into the following categories.

- Forwarding performance with NAC-L3-IP

- Memory consumption for NAC-L3-IP simultaneous sessions
- Processor consumption for the session-lifetime and status query timers
- Number of simultaneous NAH that can be handled by the device.

The last two of these scaling factors can be influenced by the network administrator during the design process.

The first scaling factor that can be influenced is the processor consumption of the session-lifetime and status query timers. The session-lifetime timer can be used to make sure that full assessments are done on a frequent basis. If set too low, this timer can cause more frequent posture requests to hit ACS and directly impact ACS's ability to scale posture assessment requests. Hence too low of a session-lifetime timer may require more ACS servers. Also, the status-query timer can be used to quickly detect posture changes or new Layer 3 hosts. Setting the status-query timer too low (either on the NAD or in ACS) can potentially cause high amounts of processor utilization for NADs that are supporting large amounts of devices. This processor utilization can potentially keep the NAD from performing critical control plane functions. With these factors in mind it is recommended that the session-lifetime and status query timers not be altered from the defaults for "healthy" posture assessments. Additionally, it is recommended that these timers should only be changed to a lower value where you want to check the device more frequently for posture assessment changes, such as after a "quarantine" or "infected" posture assessment.

The second scaling factor to be considered is the fact that the current IOS based router platforms have a default of 100 NAH sessions that can concurrently exist on a platform. Once this threshold has been reached, no more EAPoUDP sessions are created by the NAD and have the default interface policy implemented until a EAPoUDP or NAH device is removed from the NAC session table. While it may be uncommon that 100 NAH sessions concurrently exist on a NAC-L3-IP NAD, it may occur when NAC is first being deployed in an environment. For instance, a network administrator may enable NAC on the NAD before CTA has been distributed to the clients. The IOS based platforms allow this value to be changed through the use of the **ip admission ratelimit <100-1000>** command. Since all data plane and control plane traffic is handled by the general purpose CPU on the current NAC-L3-IP platforms, each one of these scaling considerations has platform dependent performance values.

Another design consideration for a network administrator is what to set the termination action on the NAD to after the posture validation timer has expired. It is recommended that the network administrator implement the termination action in ACS via the IETF RADIUS Termination Action Attribute 29. The reason for this recommendation is that without the termination action defined in ACS as "RADIUS request", by default the NAC-L2-IP session is removed from the session table and a connected device defaults back to the default interface ACL security policy until it generates traffic that triggers a full posture assessment. This could potentially interpret application sessions that the client is conducting at the time of the full posture assessment. If the IETF RADIUS Termination Action, Attribute 29, is sent with a RADIUS access-accept, then the NAC session is retained while a full posture assessment is performed. This allows a client to continue an application session during the full posture assessment.

The final recommendation for NAC-L3-IP deployments is that the network administrator initially deploys NAC in an audit mode. In essence, this means that the NAC authorization for initial deployment is the equivalent of a "permit ip any any" for all posture assessment tokens. This recommendation is made to allow the network administrator to minimize the chance that the introduction of NAC into their environment will increase the help desk case load or potentially cause an application outage due to a deny authorization. In an audit mode NAC can still provide invaluable reporting on the compliance level of end devices in addition to identifying NAH.

NAC-L2-IP

As stated earlier, NAC-L2-IP uses EAP over UDP transport similar to NAC-L3-IP and is a posture only credential assessment. Like NAC-L3-IP, the interface ACL is the default policy for the switch port. In some cases the network administrator needs to consider what the correct default interface ACL should permit. For instance, if the NAC-L2-IP port needs to support IP phones then the network administrator will need to consider what ports are necessary for the IP phone to boot and provision itself and add those ports to the interface

ACL. In addition, since the NAC posture assessment is at the ingress to the network, a network administrator may want to consider how the interface ACL affects network functions such as Windows domain login, group policy updates, and login scripts. If for instance the network administrator would like to allow all of these Windows functions, the network administrator may choose to allow the following ports to be added to the interface ACL for NAC-L2-IP.

- 88 kerberos
- 445 domain -smb direct host
- 389 domain ldap
- 123 domain ntp
- 135 domain rpc endpoint mapper
- 1026 domain ntfs

In this fashion the network administrator can allow the Microsoft Windows networking system to continue to function. This seamless integration with the Windows networking environment needs to be balanced against the fact that malware has, in the past, made use of these ports as a way to spread throughout an enterprise. The inclusion or exclusion of any port on the interface ACL is a business risk decision that needs to be made by the network administrator.

As mentioned earlier, a notable difference between NAC-L2-IP and NAC-L3-IP is that NAC-L2-IP is triggered by ARP or DHCP traffic. NAC-L2-IP sessions are active for as long as the host responds to periodic status-query “are you still there?” messages implemented using ARP probes or until they are terminated. A session may be terminated because of the following events:

- ARP probe timeout
- Session terminated by CLI
- Radius Access Accept from the AAA server indicates the session should be deleted on a session timeout

Since the access-control lists on the NAC-L2-IP NADs are implemented in hardware and the number of NAC sessions is limited by hardware on a per platform basis, there are limited design considerations about the impact of load forwarding or simultaneous sessions on the NAC-L2-IP NAD. The primary design considerations for NAC-L2-IP are very similar to NAC-L3-IP regarding processor consumption for session-lifetime and status query timers. The session-lifetime timer has the same impact on ACS scalability in NAC-L2-IP as in NAC-L3-IP. The status query timer also has a direct impact on the control plane CPU utilization. Again setting the status-query timer low (either on the NAD or in the ACS) can potentially cause the switches control plane CPU to have high processor utilization, which can keep the switch from performing critical control plane functions. Again, it is recommended that the posture validation and status query timers not be altered from the defaults for “healthy” posture assessments. Additionally, it is recommended that these timers should only be changed to a lower value where you want to check the device more frequently for posture assessment changes, such as after a “quarantine” or “infected” posture assessment.

Another design consideration is what to set the termination action to on the NAD after the posture validation timer has expired. It is recommended that the network administrator implement the termination action in ACS via the IETF RADIUS Attribute 29. The reason for this recommendation is that without the termination action defined in ACS as “RADIUS request”, by default the NAC-L2-IP session is removed from the session table and a connected device defaults back to the default interface ACL security policy until it generates traffic that triggers a full posture assessment. This could potentially interrupt application sessions that the client is conducting at the time of the full posture assessment. If the IETF RADIUS Attribute 29 – Termination Action is sent with a RADIUS access-accept, then the NAC session is retained while a full posture assessment is performed. This allows a client to continue an application session during the full posture assessment.

One of the main benefits of NAC-L2-IP is that it was designed to support multiple hosts per port. The network administrator needs to be aware that unlike NAC-L3-IP, there are a limited number of hosts per port that can be supported in NAC-L2-IP. Because of hardware implementation differences in different switching platforms, the number of devices per port varies per platform. The number of devices per port for NAC-L2-IP is listed later in the document.

The final recommendation for NAC-L2-IP deployments is exactly the same as for NAC-L3-IP, which is to initially deploy NAC in an audit mode. In essence, this means that the NAC authorization for initial deployment is the equivalent of a “permit ip any any” for all posture assessment tokens. This recommendation is made to allow the network administrator to minimize the chance that the introduction of NAC into their environment will increase the help desk case load or potentially cause an application outage due to a deny authorization. In an audit mode NAC can still provide invaluable reporting on the compliance level of end devices in addition to identifying NAH.

NAC-L2-802.1X

The 802.1x standard specifies both a protocol for carrying EAP messages over a LAN transport, as well as the use of this transport for supporting network admission control on a first-hop L2 port.

Since 802.1x does not have the equivalent of a status query message, the only method by which the NAD can conduct a re-assessment of the client would be to do a full 802.1x transaction by lowering the session-lifetime timer on the NAD. This would create a large amount of overhead on the switch and ACS and is not an optimal solution

NAC requires that a NAD acting as an 802.1x Authenticator can trigger an EAP exchange at the following times:

- When host first connects to network
- Periodically on the switch, trigger a re-authentication to pick up on any changes in AAA posture validation policy (e.g., a new AV signature file has come out)
- On a posture change or a change in authentication credentials on the client, and the client initiates the EAP exchange

With the limitation of the NAD initiating the EAP exchange, CTA now has the capability to signal to the NAC-enabled network that the status of a CTA posture plugin has changed and that the network should reinitiate a identity and posture credential query to compare this changed state to the admissions policy of the NAC network. This is called an “asynchronous status query” in CTA. Asynchronous status query can be initiated by CTA by two methods.

The first method is if a posture plugin has been specifically programmed to trigger CTA to initiate a new EAP exchange by sending an EAPOL-Start message. The Cisco Security Agent (CSA) has implemented this capability in CSA version 4.5.1. In this version there is the ability to trigger an asynchronous status query whenever the operational status of CSA changes. For example, suppose the “healthy” admission policy states that CSA must be operational to access the network. A host accesses the network and passes the admissions policy since CSA was active when the posture credentials were given. Now suppose a malicious (worm or virus) or non-malicious (end user) action disables CSA and causes its operational status to change. This change would trigger an asynchronous notification from CSA to CTA to the CTA supplicant, which would send an EAPOL-Start to the switch. This EAPOL-Start would start an entirely new NAC identity and policy credential validation which would fail to meet the “healthy” admissions policy due to CSA’s operational state being inactive. This would result in another admissions policy, “infected” for instance, to send a new authorization policy (typically a dynamic VLAN assignment) to the switch to isolate that device in some fashion until CSA’s status changes to operational. When CSA’s status does change to operational, this again triggers a NAC identity and posture credential check similar to the sequence described above. When this happens the PC again may meet the “healthy” admission policy and be connected back to the “healthy” VLAN on the switch.

The second method involves an asynchronous status timer in CTA. When this timer expires, a function within CTA is triggered and performs a poll on all the registered posture plugins. If any of the posture plugins reports a status change, CTA sends EAPOL-Start to all

existing sessions. The asynchronous timer is set at 300 seconds. This is a hard coded setting within CTA and cannot be edited by the network administrator.

Similar to NAC-L2-IP, another design consideration is what to set the termination action to on the NAD after the posture validation timer has expired. It is recommended that the network administrator implement the termination action in ACS via the IETF RADIUS Termination Action, Attribute 29. The reason for this recommendation is that without the termination action defined in ACS as “RADIUS request”, by default the NAC-L2-802.1x state machine moves through the following states during a full re-assessment. “authenticated -> disconnected -> connecting -> authenticating -> authenticated”. When the state machine transitions to the “disconnected” state, it denies all traffic on the port except EAPOL. This could potentially interpret application sessions that the client is conducting at the time of the full posture assessment. If the IETF RADIUS– Termination Action, Attribute 29, is sent with a RADIUS access-accept, then the NAC-L2-802.1x state machine moves through the following states “authenticated -> connecting -> authenticating -> authenticated”. Since the “disconnecting” state is never entered, the device continues to accept traffic while a full posture assessment is performed. This allows a client to continue an application session during the full posture assessment.

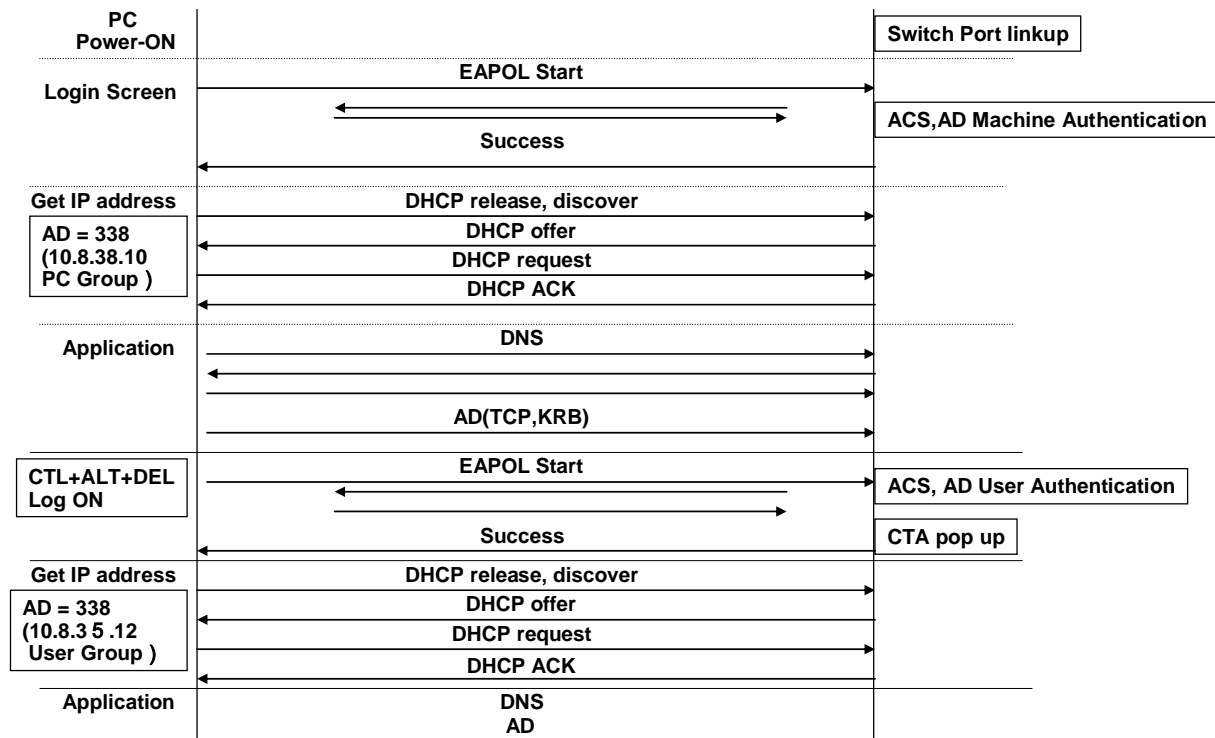
CTA and Windows Boot Sequence

At boot time, the Windows OS uses machine authentication to authenticate using 802.1x and to subsequently communicate with Windows domain controllers to pull down machine group policies to alleviate the problem of domain GPOs being broken by the introduction of 802.1x.

After the GINA is presented, a user can login to the computer or the Windows domain and the username/password used for login can be used as the identity credentials for 802.1x authentication. This is the second type of credential and is commonly referred to as user authentication.

With the introduction of CTA and its included wired supplicant, the boot sequence of the device is similar to the boot sequence using the Windows supplicant, however there are some differences that the network administrator needs to understand these. For example, after each successful authentication and assessment, the CTA supplicant does a network discovery to determine if it needs to renew its IP address due to VLAN assignment. This process is shown in the figure below that graphically depicts the Windows with CTA boot flow.

Windows CTA Boot Flow



Courtesy of Hiromi Mizutani

© 2005 Cisco Systems, Inc. All rights reserved.

1

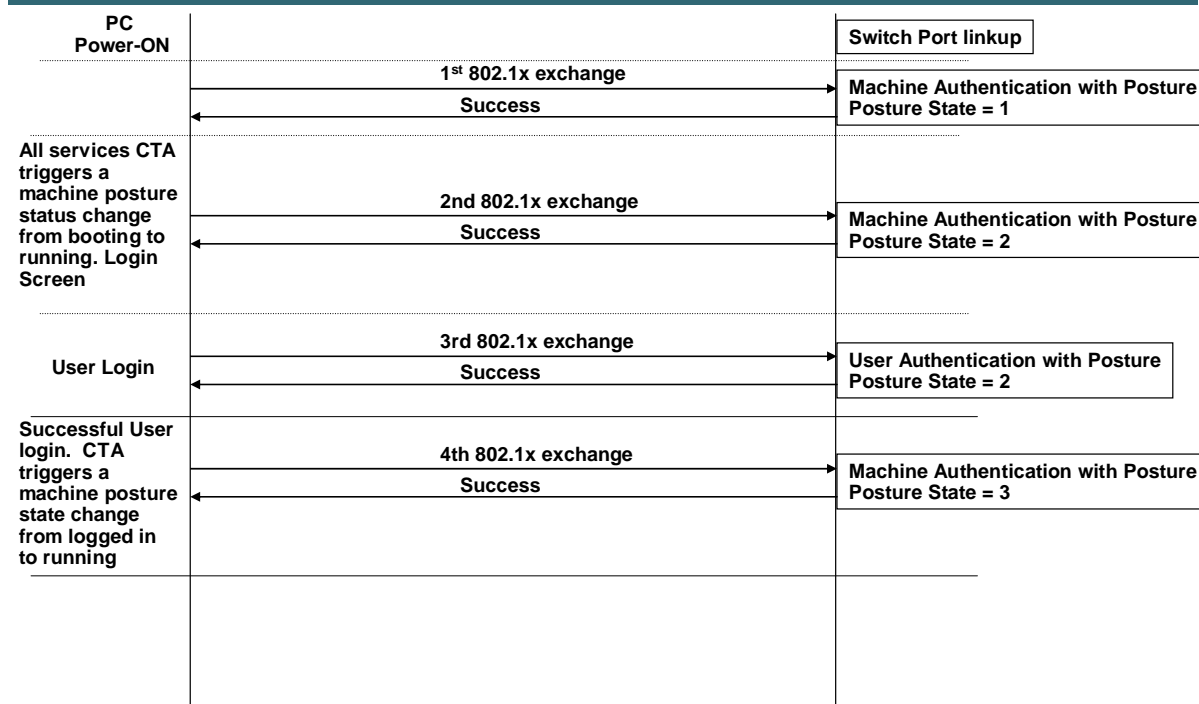
As described earlier, with the introduction of CTA 2.0 there is a new concept of machine posture state that is used to make admission decisions even if application plugin information is not available in the boot process. For instance, you may use the machine-posture-state of booting to only check that AV is installed, since the AV service might not be started at boot time assessment, while you would use the machine posture state of running to check that AV is the correct version and enabled when the service is started.

The use of the machine-posture-state credentials impacts NAC-L2-802.1x because CTA, when queried for machine-posture-state credentials, creates EAPOL-Start traffic to initiate a new posture assessment when it transitions from one machine posture state to another. For instance, if the machine has moved from the booting to running state, CTA generates an EAPOL-Start in the supplicant. The following machine and user authentication scenario with all the machine posture states are shown in the following step-by-step transaction and figure.

- Machine boots.
- Supplicant performs Machine Auth & posture—1st 802.1x exchange.
- All services on the machine complete, thus CTA triggers a posture status change as a result of the machine changing from booting to running.
- Supplicant performs Machine Auth & posture—2nd 802.1x exchange.
- User logs in.
- Supplicant performs user auth & posture—3rd 802.1x exchange.
- Login completes, thus CTA triggers a posture status change as a result of the machine changing from running to logged in.

- Supplicant performs user auth & posture—4th 802.1x exchange.

Windows CTA Boot Flow with Machine Posture



Courtesy of Hiromi Mizutani

© 2005 Cisco Systems, Inc. All rights reserved.

1

As described earlier, CTA uses EAP-FAST to perform machine and user authentication. The network administrator needs to understand how PACs are provisioned to CTA.

EAP-FAST comprises three basic phases:

- Phase 0 (optional)—The PAC is initially distributed to client.
- Phase 1—Using the PAC, a secure tunnel is established.
- Phase 2—The client is authenticated via the secure tunnel.

In the EAP-FAST specification there are two ways to provision the PAC, out-of-band-provisioning or in-band-provisioning. With the NAC-L2-802.1x CTA supplicant you can only provision a PAC with in-band-provisioning. The CTA supplicant only provisions a PAC on the host if the ACS server has been configured to allow in-band-provisioning and if the client side authentication is a successful machine authentication using a certificate assigned to the machine (machine certificate) or a successful user authentication. Out-of-band provisioning is not supported with the NAC-L2-802.x CTA supplicant.

A recommendation for NAC-L2-802.1x deployments is exactly the same as for NAC-L2-IP and NAC-L3-IP, which is that the network administrator initially deploy NAC in an audit mode. In NAC-L2-802.1x this means something slightly different than in the other assessment methods, since in NAC-L2-802.1x the primary authorization of clients is via VLAN assignment. Therefore it is recommended that the network designer either does not return a VLAN assignment, which means that a successful credential check results in access being

granted on the default VLAN of the port, or the network designer returns a VLAN assignment consistently for all posture assessment tokens. This recommendation is made to allow the network administrator to minimize the chance that the introduction of NAC into their environment will increase the help desk case load or potentially cause an application outage due to a deny authorization. It should be noted that if the supplicant fails authentication that the user will always fail the 802.1x transaction and be denied access to the network.

Also, it is recommended that the network designer take an incremental step from an audit-only authorization in NAC-L2-802.1x. There exists a condition within Microsoft networking environments where doing VLAN assignment for both machine and user authentication can cause GPOs and login scripts to potentially fail. If the network designer is only doing VLAN assignment for one of the authentications, machine, or user, then VLAN assignment generally works. When entering into a NAC-L2-802.1x where VLAN assignment may occur for posture as well as identity reasons, it is recommended that the network designer consider only doing VLAN assignment when a posture assessment returns a negative posture token. The reasoning behind this recommendation is the following. If the device successfully passes the identity and posture credential checks and gains access to the network on the native VLAN of the port or a consistent VLAN, then they are assured that normal windows networking functions, GPOs and login scripts function properly. However, if a quarantine or infected token is returned during the identity and posture assessment, then apply the VLAN assignment. There is a possibility this may keep Microsoft network functions from working properly, but it can be argued that if a “quarantine” or “infected” is returned that something fundamentally is wrong with the computing device and therefore some normal functionality can be sacrificed in return for the assurance that the fundamentally broken device is quarantined for remediation.

IEEE 802.1X AND NAC-L2-IP

An additional option for deploying NAC is to leverage an existing IEEE 802.1x supplicant that does not support posture credential checks, such as the native supplicant in Microsoft OSes, to verify the identity credentials of the host and allow the device to gain access to the network. Then NAC-L2-IP can be used to check the posture credentials of the host. This layered approach may be necessary for one of the following reasons.

- There is non-NAC enabled 802.1x supplicant already installed on the host and NAC is being layered on top of the IBNS solution.
- The network administrator requires doing identity and posture credential checks, but also wants to leverage the NAH audit features that are currently only supported in NAC-L2-IP.

Both NAC-L2-IP and 802.1x support can be configured simultaneously on a switch port by switch port basis on the NAD.

The two primary considerations for the network designer are that this deployment method doubles the transaction load on the ACS and that the authorization methods for 802.1x and NAC-L2-IP are disjointed. Both issues can be mitigated by the network designer. The first issue can be mitigated by adding more ACS servers to a server load balancing environment and linearly scaling ACS. The second issue can be mitigated by making sure that all credential checks authorization methods do not overlap. For instance, the network designer can make sure that 802.1x authorization only consists of VLAN assignment and not downloadable ACLs, while NAC-L2-IP can do its authorization with downloadable ACLs.

The configuration details for enabling this solution are discussed in the NAC Configuration Guide.

NAC AGENTLESS HOSTS (NAHS)

There are several methods in NAC to allow network access to hosts that do not or cannot perform NAC or other compliance authorizations. Network attached devices that fall into this category often include printers, scanners, photocopiers, cameras, sensors, badge readers, and specialized equipment. NAH devices may also include computers with unsupported OSes, hardened OSes, embedded OSes, or personal firewalls.

NAC-L2/L3-IP and Agentless Hosts

NAC-L2-IP and NAC-L3-IP provide a great amount of flexibility when dealing with agentless hosts. The following options are available for agentless hosts:

- Static exceptions on the switch
- Static exceptions in ACS
- Audit for agentless hosts (near future for NAC-L3-IP)

Static exceptions can be configured on the switch to allow hosts to bypass the posture validation process based on specified MAC or IP address. CDP static exceptions are also available only for Cisco IP Phones.

Static exceptions can be configured in ACS to allow any specified hosts to bypass the posture validation process based on MAC address. Both individual and wildcard addresses can be specified.

NAC-L2-IP, and in the near future NAC-L3-IP, can also trigger the audit of an agentless host via a partner audit server. After an audit of the host is performed, the audit server provides a posture token to ACS based on the audit results. This in turn is enforced on the NAD with ACLs and URL redirection. This provides an administrator granularity in the decision process on which agentless hosts to allow on the network and what type of access to grant them.

NAC-L2-802.1x and Agentless Hosts

There are several options available to administrators for agentless hosts within NAC-L2-802.1x. They include the following:

- CDP-Based Exception for Cisco IP Telephones
- MAC Authentication Bypass
- Guest VLAN
- Failed Authentication VLAN

Cisco currently has a mechanism for making an exception for Cisco IP Telephones that can generate CDP traffic and identify themselves to the Catalyst switches. With this CDP identification the switch places the Cisco IP Telephone in the voice VLAN and exempt it from the NAC process.

MAC Authentication Bypass is an IBNS feature that is configured on a port basis. The switch makes a RADIUS request to the ACS server with the MAC address of the host connecting to the switch. If the MAC address is found in the internal ACS database, the ACS server replies with an Access-Accept and the host is permitted onto the network. This MAC authentication happens after 802.1x and hence “bypasses” 802.1x’s default security policy of denying access to any device that cannot pass 802.1x authentication. This feature is useful for allowing NAH access to the network. The MAC address OUI can be used to wildcard MAC addresses to allow devices with addresses within the same OUI range to access the network. This is useful for like devices such as printers or terminals that do not have a 802.1x supplicant, but need to be allowed access to the network. Since the MAC Authentication Bypass is dynamic in nature, the network administrator can configure it on all ports in the network and does not have to explicitly not configure it on ports where printers are connected. ***MAC Authentication Bypass is only supported on the Catalyst 6500 at the time of this writing.***

A guest VLAN enables the non-802.1X capable hosts to access the networks that use 802.1X authentication. On a per-port basis you define the guest VLAN to which devices are assigned if they can not speak 802.1x. When you configure an 802.1x guest, all the non-802.1X capable hosts (hosts that do not respond to EAPOL-Identity Request or send an EAPOL-Start) are put in this VLAN. You can configure any VLAN (except for the private VLANs and RSPAN VLANs) as a guest VLAN. If a port is already forwarding on the guest VLAN and you enable 802.1X support on the network interface of the host, the port is immediately moved out of the guest VLAN and the

authenticator waits for authentication to occur. Enabling 802.1X authentication on a port starts the 802.1X protocol. If the host fails to respond to the packets from the authenticator within a certain amount of time, the authenticator puts the port in the guest VLAN. The guest VLANs are supported in both single-authentication mode and multiple-host mode.

Contrast the guest VLAN feature with the authentication failure VLAN feature. On a traditional 802.1X port, the switch does not provide access to the network until the supplicant that is connected to the port is authenticated by verifying its identity information with an authentication server. With an authentication failure VLAN, you can configure the authentication failure VLAN on a per-port basis and after three failed 802.1X authentication attempts by the supplicant, the port is moved to the authentication failure VLAN where the supplicant can access the network. The authentication failure VLAN is independent of the guest VLAN. However, the guest VLAN can be the same VLAN as the authentication failure VLAN. If you do not want to differentiate between the non-802.1X capable hosts and the authentication failed hosts, you may configure both to the same VLAN (either a guest VLAN or an authentication failure VLAN).

The Failed Authentication VLAN does not work with most tunneled EAP- Methods. The reason for this is an original design goal of tunneled methods to avoid man-in-the-middle attacks. With a tunneled method, an EAP-Success (or failure) is passed inside the TLS tunnel from the authentication server to the supplicant. Additionally, an EAPOL-Success (or failure) is passed from the authenticator (switch) to the supplicant. It is a design goal of tunneled methods to insure these two EAP messages are consistent with one another. The only outcome which should be considered a successful authentication is when an EAP-Success sent within the encrypted TLS tunnel is followed by a clear text EAPOL-Success. All other combinations should be considered invalid combinations, both by the supplicant and the authentication server. Because the first EAP-Success is protected within the TLS tunnel channel, its messages cannot be spoofed, whereas clear-text Success and Failure messages can be sent by an attacker. In the failed-auth case, the supplicant receives a failure in the tunnel (or for the tunnel itself), transitions its state machine into a held state, and tries to start the 802.1x state machine over again. Since the supplicant and switch spoke 802.1x on the link, the supplicant always assumes that there is a 802.1x authenticator on the other end of the link and will not perform an IP address request until it receives an access accept. This does not happen since the switch has moved the port into the authorized and forwarding state and will not respond to EAPOL-Starts from the supplicant. PEAPv1 and EAP-FAST are two examples of tunneling protocols that transmit a EAP status message inside the TLS tunnel. Therefore, failed auth will not work with these EAP-methods. However, it should be noted that this is entirely dependent on the supplicant behavior and testing should be done by the network administrator to ensure that Failed-Auth VLAN works with the EAP types and supplicant that the network administrator has decided to deploy on their network.

NAH Summary

All of the NAH options are summarized in the table below.

| Component | Method | Pros | Cons |
|-----------|--|---|---|
| NAD | CDP detection | | |
| NAD | Static MAC address | Address Wildcarding | First-hop only for routers Static list to maintain |
| NAD | Static IP address | Address Wildcarding | Static list to maintain |
| ACS | Network Access Profile filter | Centralized list Address Wildcarding | Static list to maintain |
| ACS | MAC-Authentication-Bypass group mapping | Centralized list Address Wildcarding | Static list to maintain |

NAC ENFORCEMENT FEATURES AND TRADE-OFFS

The tables below summarize the features and tradeoffs of the different assessment methods. The subsequent sections discuss this table in depth, as well as other design considerations for each assessment method and NAH handling.

| Feature | NAC-L2-802.1x | NAC-L2-IP | NAC-L3-IP |
|------------------------|--------------------|-------------|------------------|
| Trigger mechanism | Data Link | DHCP or ARP | Forwarded Packet |
| Machine Identity | √ | | |
| User Identity | √ | | |
| Posture | √ | √ | √ |
| VLAN assignment | √ | | |
| URL-Redirection | | √ | √ |
| Downloadable ACLs | 6500-only (PBACLs) | √ | √ |
| Posture Status Queries | | √ | √ |
| 802.1x Posture Change | √ | | |

NETWORK ADMISSION CONTROL DEPLOYMENT COMPARISON

| Deployment Model | Pros | Cons |
|-------------------------|---|--|
| Identity and Posture | Unified identity & posture with NAC-L2-802.1x L2 enforcement IBNS-compatible | Not supported with NAC-L2-IP and NAC-L3-IP Retail supplicant license for wireless support No audit support (Future) |
| IEEE 802.1x | IBNS-compatible | No posture No audit support |
| Posture Only | NAC-L2-IP and NAC-L3-IP NAH Audit support (NAC-L3-IP in Future) Supplicant optional | No identity |
| IEEE 802.1x and Posture | IBNS-compatible Posture Audit support (NAC-L3-IP in Future) | Disjointed Authorization (posture after VLAN assignment) Twice the load on the ACS server Multiple clients / management complexity |

NAC Solution Components

Cisco Trust Agent

CTA 2.0 is available through:

- Direct distribution on cisco.com
- CSA 4.5.1 through building new agent kit or CSA 5.0 with integrated CTA 2.0 agent kit
- Through various partners (e.g., Trend and InfoExpress)
- We expect partners to integrate CTA compliant technologies into their offerings which would eliminate the need for a separate CTA installation (future)

CTA 2.0 has multiple installation options including:

- Silent installation (separate package)
- With and without NAC-compliant native 802.1x supplicant (separate package)
- With and without scripting interface support (option on installation of all versions)
- All versions provide centralized posture broker, and OS/hotfix information to ACS

There are two components to the trust agent: the posture agent and the 802.1x wired-only supplicant. Deployment considerations for the posture agent are minimal. The primary task is to ensure when CTA is deployed that it includes in the installation directory a “certs” folder which contains the digital certificate of every Cisco Secure ACS installation or a trusted CA in the certificate chain. In any case the certificate authority which signed the certificates must be a trusted root CA on the client system. For this reason self-signed certificates are not recommended for large installations and we recommend deployment of a Public Key Infrastructure. As self-signed certificates have virtually no revocation capability and are valid for a maximum of one year, in large installations this deployment method does not scale and is not considered as secure.

Of special note, the CTA 2.0 client for RedHat Linux does not include an 802.1x supplicant, wired or wireless. In 802.1x environments you must use a IEEE 802.1x supplicant to authenticate the client to the network and then as an additional step carry out posture validation through the CTA. For more information on this deployment method, please refer to the IEEE 802.1x & NAC-L2-IP section.

CTA does not currently support dual-homing the client on redundant links for high availability.

In NAC-L2-802.1x environments CTA polls the plug-ins every 300 seconds for status changes; this is a fixed interval timer. Should the trust agent detect a result change, it triggers the supplicant to restart EPoL validation (EPoL-start).

For more information on CTA deployment, administration, and troubleshooting, please refer to the online documentation at: http://www.cisco.com/en/US/partner/products/ps5923/tsd_products_support_series_home.html.

For general information on CTA 2.0, including latest supported operating systems, please refer to the data sheet at: http://www.cisco.com/en/US/products/ps5923/products_data_sheet0900aecd80119868.html.

NADs

Performance, notably response-time, is critical in any admission controlled environment. Given that on any new connection to the network a device will be postured, it is important to reserve sufficient NAD bandwidth to carry out this interrogation in real-time. Contact your account team to obtain the latest performance data for the NADs you have selected. There are some best practices to generally follow:

- Status-query timers are considered low impact given current performance testing results. Default values are recommended unless higher than average device mobility mandates more aggressive timers which the NAD can support as for example in remote access environments.
- Revalidation timers are the most processor intensive for NADs and ACS. Default values are recommended unless the security policy mandates more aggressive checks and the local NAD can support the load.
- The number of devices per port (switch) or device (router, concentrator, access point) varies depending on platform; validate these values before deploying. In general the permitted density varies depending on what other features are enabled.

In general HTTPS is not supported across any NAD for URL redirection.

In order to mitigate possible Denial of Service attacks by default Cisco IOS NADs, only permit 100 NAC agentless hosts (NAHs) per NAD. In normal operation this is not an issue, however in initial deployment you should follow Cisco best practices and deploy NAC in audit-only mode until sufficient posture compliance has been established; you will likely encounter this limit in high-density or LAN environments. We recommend setting this value higher to meet your initial deployment needs and later reverting to the default value unless local policy requires this as an ongoing requirement (e.g., non-managed device segment where more than 100 devices may exist at any given time). This discussion applies to IOS NADs including NAC-L3-IP routers and NAC-L2-IP switches.

CISCO IOS ROUTER

When enabled, authentication-proxy is triggered *before* EoU. In addition, EoU applied ACLs override those put in place by authentication-proxy and are not user or group aware. NAC-L2-802.1x could be used to provide authentication validation on the switch service module, however the primary method of access policy in this case is VLAN assignment. Hence VLAN ACLs would need to be pre-defined on the switch service module to enforce group-level access control policy.

CISCO VPN CONCENTRATORS

Of note on the 3000 series VPN concentrator, access filters applied based on posture overwrite those based on the user-group mapping; there is no ACL merge.

CISCO SWITCHES

Guidelines that apply to all Cisco Catalyst switches with the associated NAC feature support:

- Currently private VLANs are not supported for dynamic assignment via NAC-L2-802.1x.
- Currently NAC-L2-802.1x on switches does not support Audit (GAME) integration.
- NAC-L2-IP and NAC-L2-802.1x are supported only on access and multivlan access ports (CDP IP Phones only) and not on trunk ports.
- For NAC-L2-IP, given its ARP inspection mechanism, you cannot use a switch as you would a router to sit behind a Layer 3 device and carry out posture validation (normally only the source MAC of the Layer 3 device is visible).
- For NAC-L2-IP any number of L2 hops are permitted between the client and the switch.

CISCOSECURE ACS 4.0

Performance and Scalability

ACS 4.0 database operations migrated from the Windows registry to SQL Sybase. Performance improvements are expected and testing is underway. Please contact your Cisco account team for the latest information.

Ensure sufficient ACS admission bandwidth exists to support your configuration. As called out in the NAD performance discussion, keep revalidation timers to the minimum necessary as this is the most processor intensive function. As a best practice the assumed transaction rate is approximately 10 per second, however this varies dramatically with every configuration (consider latency to backend authentication servers alone, e.g., Active Directory) and as stated based on new pending performance data will likely increase.

Finally, limits are enforced on certain aspects of policy definition. Notably, each instance of a Network Access Profile for which MAC Authentication Bypass is enabled can support a maximum of 10,000 MAC addresses in the local ACS database. Thus if you need more than 10,000 MAC exceptions and wildcarding is not feasible, you have to segment MAB lists on NAP boundaries through NAD device grouping. This limitation applies to both 802.1x/MAB and NAC-L2-IP centralized MAC whitelisting. For NAC-L2-IP, there is also a limit of 1,000 MAC addresses for audit exceptions.

Management

Replication of policy is crucial for scaling policy changes. As initial policy creation is a lengthy process, we highly recommend using the ACS replication features so that centralized policy changes are replicated throughout the Enterprise in a timely matter. This is the most appropriate method to employ to handle rapid policy changes such as to deal with worm or other outbreaks.

In the interest of ease-of-use of troubleshooting NAC configurations, we recommend the definition of a CTA-only policy, namely a NAP which employs an internal policy for which the only required credential is CTA. If for example five types are normally required and for some reason only four are reported by the agent, without this policy the authorization request simply fails and no valuable logging information is generated.

Other

Of special note ACS 4.0, unlike ACS 3.3, no longer supports centralized IP whitelisting for EoU exceptions. If this method is necessary and centralized (via MAB) or local MAC exceptions on each NAD are not ideal, the only remaining option is to use NAD local IP exceptions.

Directory Services

As organizations grow, the use of directory services for centralized and scalable identity management is critical. Besides managing email account names and contact information, they can be used to synchronize identities, passwords, certificates, and other information for network and application authentication. Whenever an authentication request is made, the AAA server delegates the authentication decision to the directory server which returns an acknowledgement and group assignment or a rejection.

Authentication Protocol Support

Nearly all authentication protocols are based on Extensible Authentication Protocol (EAP) for challenge/response communications. EAP protocols support multiple authentication methods for username/password, digital certificate, and one-time-password (OTP) credentials. Unfortunately, not all directory services support all of the EAP-based protocols and methods. Use the tables below to verify which protocols are supported by each NAC method in your deployment and some of the most popular directory servers.

| Protocol | Method | NAC L2 802.1x | NAC L2 IP | NAC L3 IP |
|----------|-----------|---------------------|-----------------|-----------------|
| EAP-FAST | MS-CHAPv2 | • | | |
| | EAP-TLS | • | | |
| | EAP-GTC | • | | |
| PEAP | MS-CHAPv2 | • | | |

Table 2. NAC Method Support of EAP Protocols and Methods

| Database | LEAP | EAP-MD5 | EAP-TLS | PEAP (EAP-GTC) | PEAP (EAP- MSCHAP v2) | EAP-FAST Phase Zero | EAP-FAST Phase Two |
|--------------------------------|------|---------|---------|-------------------|--------------------------------|------------------------|-----------------------|
| ACS Internal | • | • | • | • | • | • | • |
| Windows SAM | • | | | • | • | • | • |
| Windows AD | • | | • | • | • | • | • |
| LDAP | | | • | • | | | • |
| ODBC | • | • | • | • | • | • | • |
| LEAP Proxy RADIUS Server | • | | | • | • | • | • |
| All Token Servers | | | | • | | | |

Table 3. Directory Server Support of EAP Methods

Cisco Secure ACS also supports non-EAP protocols for other AAA requirements. The most basic network challenge protocol is PAP, which is supported by both ACS and Microsoft. However the simplicity of PAP must be balanced against the fact that it sends all credentials unencrypted. Another option is CHAP, which provides a higher level of security than PAP by encrypting passwords when communicating from an end-user client to the AAA client. ARAP support is included to support Apple clients.

Directory Scaling

After compatibility is established, scalability of the directory services infrastructure must be considered. Existing directory server infrastructures are built to handle the load of daily user and machine logins but they may not scale to the load created by NAC revalidations. It may also be necessary to geographically disperse the directory servers throughout your organization to reduce authentication times due to network latency and provide redundancy in the case of server failures.

SUMMARY

NAC Framework dramatically improves security by ensuring that endpoints (laptops, PCs, PDAs, servers, etc.) conform to security policy in order to proactively protect against worms, viruses, spyware, and malware.

NAC Framework also provides broad integration with multivendor security and management software, and enhances existing investments in network infrastructure and vendor software.

Network Admission Control (NAC) is part of the Cisco Self-Defending Network, designed to dramatically improve the network's ability to identify, prevent, and adapt to threats.

Appendices

Acronyms

| Acronym | Description |
|------------|---|
| ACE | Access Control Entry |
| ACK | Acknowledgement |
| ACL | Access Control List |
| ACS | Access Control Server |
| AD | Active Directory (Microsoft) |
| AID | Authority Identity |
| AP | Access Point |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| AV | Anti Virus |
| CAM | Clean Access Manager (CCA) |
| CAS | Clean Access Server (CCA) |
| CCA | Cisco Clean Access |
| CDP | Cisco Discovery Protocol |
| CHAP | Challenge Handshake Authentication Protocol |
| CSA | Cisco Security Agent |
| CTA | Cisco Trust Agent |
| CTASI | CTA Scripting Interface |
| DB | Database |
| DC | Domain Controller (Microsoft) |
| DFS | Distributed File System |
| DHCP | Dynamic Host Configuration Protocol |
| DN | Distinguished Name |
| DNS | Domain Name Service |
| DoS | Denial of Service |
| DOT1X | IEEE 802.1X |
| EAP | Extensible Authentication Protocol |
| EAPOL | EAP over LAN |
| EAPoRADIUS | EAP over RADIUS |
| EAPoUDP | EAP over UDP |
| EOU | EAP Over UDP |
| FAST | Flexible Authentication Secure Tunnel |
| GAME | Generic Authorization Message Exchange |
| GINA | Graphical Identification and Authentication (Microsoft) |
| GPO | Group Policy Object (Microsoft) |
| GTC | Generic Token Card |

| | |
|--------|---|
| HA | High Availability |
| HAL | Hardware Abstraction Layer |
| HCAP | Host Credential Authentication Protocol |
| HIPS | Host Intrusion Prevention System |
| HTTP | Hyper Text Transfer Protocol |
| HTTPS | Hyper Text Transfer Protocol Secured |
| IAS | Internet Access Server (Microsoft) |
| IBNS | Identity Based Networking Services |
| IDS | Intrusion Detection System |
| IID | Initiator Identity |
| IOS | Internetworking Operating System |
| IP | Internet Protocol |
| L2 | Layer 2 |
| L2TP | Layer 2 Tunneling Protocol |
| L3 | Layer 3 |
| LAN | Local Area Network |
| LDAP | Lightweight Directory Access Protocol |
| LEAP | Lightweight Extensible Authentication Protocol |
| MAC | Media Access Control |
| MITM | Man In The Middle |
| MS | Microsoft |
| MSCHAP | Microsoft Challenge Handshake Authentication Protocol |
| MVAP | Multi VLAN Access Ports |
| NAC | Network Admission Control |
| NAD | Network Access Device |
| NAF | Network Access Filter |
| NAH | NAC Agentless Host |
| NAK | Negative Acknowledgement |
| NAR | Network Access Restriction |
| NAT | Network Address Translation |
| NDIS | |
| NDS | Netware Directory Services (Novell) |
| NRH | Non Responding Host |
| NTLM | |
| ODBC | Open Database Connect |
| OOB | Out Of Band |
| OS | Operating System |
| OTP | One Time Password |
| PA | Posture Attribute |
| PAC | Provisioned Access Credential |

| | |
|-------|--|
| PACL | Port ACL |
| PAE | Port Access Entity |
| PBACL | Policy Based ACL |
| PEAP | Protected EAP |
| PKI | Public Key Infrastructure |
| PPTP | |
| PVLAN | Private VLAN |
| QoS | Quality of Service |
| RAC | RADIUS Attribute Component |
| RPC | Remote Procedure Call |
| SAML | Security Assertion Markup Language |
| SIMS | Security Information Management System |
| SLB | Server Load Balancing |
| SMB | Server Message Block |
| SNMP | Simple Network Management Protocol |
| SQ | Status Query |
| SSL | Secure Sockets Layer |
| TCP | Transport Control Protocol |
| TLS | Tunnel Layer Security |
| TLV | Type Length Value |
| UDP | Universal Datagram Protocol |
| URL | Universal Resource Locator |
| VACL | VLAN ACL |
| VLAN | Virtual Local Area Network |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| VSA | Vendor Specific Attribute |
| VVID | Voice VLAN Identifier |
| WAN | Wide Area Network |
| WEP | Wireless Encrypted Protection |
| WLAN | Wireless LAN |
| WoL | Wake on LAN |

| Term | Deprecated Term | Definition |
|---------------|-----------------|--|
| AAA | | Authentication, Authorization, and Accounting server. (Authentication, authorization, and accounting is pronounced "triple a." A AAA server is the central server that aggregates one or more authentication, authorization, or both decisions into a single system-authorization decision, and maps this decision to a network-access profile for enforcement on the NAD. |
| Access-Accept | | Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user. |

| | | |
|---------------------------------------|--|--|
| Access-Challenge | | Response packet from the RADIUS server requesting that the user supply additional information before being authenticated. |
| Access-Reject | | Response packet from the RADIUS server notifying the access server that the user is not authenticated. |
| Access-Request | | Request packet sent to the RADIUS server by the access server requesting authentication of the user. |
| accounting | | Accounting in network management subsystems are responsible for collecting network data relating to resource usage. |
| ACE | | Access Control Entry - An ACL Entry contains a type, a qualifier for the user or group to which the entry refers, and a set of permissions. For some entry types, the qualifier for the group or users is undefined. |
| ACL | | Access Control List. |
| ACS | | Access Control Server or Cisco Secure Access Control Server. |
| Action (ACS) | | |
| Assessment Result (ACS) | | |
| Condition (ACS) | | |
| Condition Set (ACS) | | |
| Credential Type (ACS) | | |
| Credential Validation Databases (ACS) | | |
| Notification String (ACS) | | |
| Posture Assessment (ACS) | | |
| Profile (ACS) | | |
| Rule (ACS) | | |
| Rule Sets (ACS) | | |
| APT, Application Posture Token | | The result of a posture validation check for a given vendor's application. |
| Audit Server | | The server that can determine the posture credentials of a host without relying on the presence of a PA on the host. The server must be able to determine the posture credentials of a host and act as a posture-validation server. |
| authentication | | In network management security, the verification of the identity of a person or a process. |
| authorization | | The method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. |
| AVP, attribute-value pair | | |
| CSA, Cisco Security Agent | | Cisco Security Agent provides threat protection for server and desktop computing systems. It aggregates multiple security functionality, combining host intrusion prevention, distributed firewall, malicious mobile code protection, operating system integrity assurance, and audit log consolidation all within a single agent package. As part of an overall security strategy, Cisco Security Agent enhances Network Admission Control and the SAFE blueprint and extends protection to the endpoint. |

| | | |
|-------------------------------|----------------------------|--|
| CSM, Cisco Security Manager | | |
| CTA, Cisco Trust Agent | CTA Lite, CTA Supplicant | Cisco's implementation of the posture agent is called the CTA and includes the embedded wired-only supplicant |
| CTASI | | CTA Scripting Interface |
| Host | Host | Any machine that attempts to connect to or use the resources of a network. Also referred to as a "host". |
| MAC Exception Handling | MAC Auth Bypass | |
| CS-MARS | | Cisco's Mitigation and Response System (CS-MARS) family of high performance, scalable appliances for threat management, monitoring and mitigation, enable customers to make more effective use of network and security devices by combining network intelligence, context correlation, vector analysis, anomaly detection, hotspot identification and automated mitigation capabilities. |
| NAC | | Network Admission Control. NAC is a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms. NAC is part of the Cisco Self-Defending Network, an initiative to increase network intelligence in order to enable the network to automatically identify, prevent, and adapt to security threats. |
| NAC Partners | Vendors Participants | |
| NAC-L2-802.1x | LAN Port 802.1X, L2 802.1X | |
| NAC-L2-IP | LAN Port IP, L2IP, LPIP | |
| NAC-L3-IP | GWIP | |
| NAD, Network Access Device | | A network access device acts as a policy-enforcement point for the authorized network-access privileges that are granted to a host. |
| NAF, Network Access Filter | | A NAF is a named group of any combination of one or more of the following network elements: IP addresses, AAA clients (network devices), or Network device groups (NDGs). Using a NAF to specify a downloadable IP ACL or Network Access Restriction based on the AAA clients by whom the user may access the network saves you the effort of listing each AAA client explicitly. |
| NAH, NAC Agentless Host | NRH, Non-responsive host | A host that does not have an 802.1x supplicant or CTA installed to perform posture validation. |
| NDG, Network Device Group | | A collection of network devices that act as a single logical group. |
| PA, Posture Agent | | An application that serves as the single point of contact on the host for aggregating posture credentials from potentially multiple posture plugins and securely communicating them to the network. |
| PDP, Policy Decision Point | | Provides facilities for policy management and conditional filters. |
| PEP, Policy Enforcement Point | | ACS acts as the policy enforcement point for policy management. |
| posture credentials | | State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information. |
| plugin, posture plugin | PP, posture plugin | A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization. |
| posture validation | | The authorization of a network endpoint's posture credentials by one or more posture-validation servers and their associated compliance policies. |
| EAP | | |

| | | |
|---|--|--|
| EAP-FAST | | EAP Flexible Authentication via Secure Tunneling. |
| EoU, EAPoUDP | | Extensible Authentication Protocol over User Datagram Protocol. |
| GAME | | Generic Authorization Message Exchange. |
| HCAP | | Host Credential Authorization Protocol. |
| IID, Initiator Identity | | For machine authentication, the IID is the FQDN of the host. (i.e. jdoe-pc.cisco.com). For user authentication the IID is a username. (i.e. jdoe) |
| PEAP | | Protected EAP |
| PV | | Posture Validation. Validates the collection of attributes that describe the general state and health of the user's machine (the "host"). |
| PVS, Policy Server, Vendor Policy Server, Posture Validation Server, External Posture Validation Server | | A Cisco or third-party server used to perform posture validation. A posture-validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules. |
| RAC | | RADIUS Attribute Component. |
| RADIUS | | Remote Authentication Dial-In User Service is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access. |
| SCM | | Switchport Configuration Manager |
| SDM | | Security Device Manager |
| SPT, System Posture Token | | The result of aggregating one or more application posture tokens into a single posture validation result for an Host. |
| token, posture token, posture state | | |
| Token: Healthy | | Host is compliant; no restrictions on network access. |
| Token: Check-up | | Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state. |
| Token: Transition | | Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services may not be running or audit results are not yet available. |
| Token: Quarantine | | Host is out of compliance; restrict network access to a quarantine network for remediation. The host is not an active threat but is vulnerable to a known attack or infection |
| Token: Infected | | Host is an active threat to other hosts; network access should be severely restricted or totally denied all network access. |
| Token: Unknown | | Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined. May also |
| VMS | | |
| VSA, Vendor Specific Attribute | | Most vendors use the VSA to support value-add features. |

NAC Attribute Reference

Attribute Namespace

All NAC attributes are addressed using a namespace based on the vendor and application type. Although each vendor and application type are represented by numbers within the EAP exchange, they are commonly referred to in the following format:

Vendor-ID : Application-Type : Attribute

The Vendor-ID is a 32-bit field containing a globally unique vendor identifier. The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined by the International Assigned Numbers Authority. The Vendor ID for Cisco Systems is 9.

The Application Type is a 16-bit field indicating a globally unique posture application type. The application types currently defined are:

| Vendor | Application Type | Application Type Name | Description |
|--------|------------------|-----------------------|-----------------------------------|
| * | 1 | PA | Posture Agent |
| * | 2 | Host | Host information |
| * | 3 | AV | Anti-Virus |
| * | 4 | FW | Firewall |
| * | 5 | HIPS | Host Intrusion Protection Service |
| * | 6 | Audit | Audit |

Note: For more information on the latest application types, refer to ??? some URL on the NAC Partner pages [Lance - lhayden]

32768-65535—Reserved for local use (this is intended for use by customers who write custom plugins or scripts that are used in a single enterprise and hence need not be globally unique.)

ATTRIBUTE DATA TYPES

| Data Type | Operators | Description |
|-------------|--|---|
| OctetArray | =,!= | The data contains arbitrary data of variable length |
| Integer32 | =,<,>,!>=,>=,<= | 32 bit signed value, in network byte order |
| Unsigned32 | =,<,>,!>=,>=,<= | 32 bit unsigned value, in network byte order |
| String | =,!=, >, <, >=, <=, contains, does not contain, start with, end with, regular-expression | Derived from the OctetArray data type. This is a human readable string represented using the ISO/IEC IS 10646-1 character set with the UTF-8 transformation format [UFT8]. Note 1: For information encoded in 7-bit US-ASCII, the UTF-8 character-set is identical to the US-ASCII character-set. Note 2: UTF-8 may require multiple bytes to represent a single character / code point; thus the length of an UTF8String in octets may be different from the number of characters encoded |
| IPv4Address | Wildcards and mask | Derived from the OctetArray data type. The IPV4Address MUST contain four octets, with the most significant octet first. i.e. "10.11.12.13" IPV4Address= 0A 0B 0C 0D |
| IPv6Address | Wildcards and mask | Derived from the OctetArray data type. The IPV6Address MUST contains 16 octets, with the most significant octet first.i.e. "0A0A:0B0B:0C0C:0D0D:0E0E:0F0F:1010:1111" IPV6Address= 0A 0A 0B 0B 0C 0C 0D 0D 0E 0E 0F 0F 10 10 11 11 |

| | | |
|---------|-------------------|---|
| Time | =,<,>,! =, >=, <= | Derived from the Unsigned32 data type. Represents the number of seconds since January 1, 1970 00:00 UTC |
| Version | =,<,>,! =, >=, <= | Derived from the OctetArray Data Type. The 8 octets are broken up into four 2-octet sets. The two most significant octets contains the major version, the next two octets contains the minor version, the last four octets contain 2 two octet values which are defined by the vendor. Traditionally the third octet is a revision number and the last octet contains the build number. Example: "3.5.1.350" has the value: 00 03 00 05 00 01 01 5E Note: All unused fields MUST be set to 0. |

ATTRIBUTE REFERENCE

The Application-Posture-Token (APT) AVP indicates the result of validating posture request-response AVPs from a particular vendor and application type. This AVP is a Posture Notification AVP and can be sent across the following interfaces in the NAC solution: Client API Posture Notification request, EAP-TLV Posture-Notification request, and HCAP Posture Validation response.

The System-Posture-Token (SPT) AVP indicates the overall result of validating posture request-response AVPs from one or more vendors and application types. This AVP is a Posture Notification AVP and can be sent across the following interfaces in the NAC solution: Client API Posture Notification request, EAP-TLV Posture-Notification request, and HCAP Posture Validation response.

| Vendor (#) | App-Type (#) | Attribute Name | Attr # | Type | Value or Format |
|------------|--------------|---------------------------|--------|------------|---|
| * (any) | * (any) | Application-Posture-Token | 1 | Unsigned32 | 0 = Healthy 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown |
| * (any) | * (any) | System-Posture-Token | 2 | Unsigned32 | 0 = HealthySystem 10 = Checkup 15 = Transition 20 = Quarantine 30 = Infected 100 = Unknown |
| Cisco (9) | PA | PA-Name | 3 | String | Name of the Posture Agent. For Cisco, this is "Cisco Trust Agent" |
| Cisco (9) | PA | PA-Version | 4 | Version | Format: major.minor.revision.build |

| | | | | | |
|-----------|----|-----------------------|-----|-------------------------------|---|
| Cisco (9) | PA | OS-Type | 5 | String | Name of the host operating system: Windows Server 2003 Datacenter Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Web Edition Windows Server 2003 Standard Edition Windows XP Home Edition Windows XP Professional Windows 2000 Datacenter Server Windows 2000 Advanced Server Windows 2000 Server Windows NT Workstation 4.0 Windows NT Server 4.0, Enterprise Edition Windows NT Server 4.0 Windows NT 4.0 Windows NT 3.51 Windows 95 Windows 95 OSR2 Windows 98 Windows 98 SE Windows Me |
| Cisco (9) | PA | OS-Version | 6 | Version | Version of host operating system. Format: major.minor.revision.build |
| Cisco (9) | PA | User-Notification | 7 | String | Value contains one or more characters e.g. "Your anti-virus signature file is out-of-date. Please update your signature file from wwwin- companyxyz..remediation-server.com". |
| Cisco (9) | PA | OS-Kernel | 8 | String | Example: Linux 2.4.20-8 i386 |
| Cisco (9) | PA | Kernel Version | 9 | Version | Version of host operating system. Format: major.minor.revision.build |
| Cisco (9) | OS | Machine-Posture-State | 11 | | This attribute specifies the running state of the machine. 1 - Booting 2 - Running 3 - Logged In |
| Cisco (9) | OS | ServicePacks | 6 | String | Example: ServicePack4 |
| Cisco (9) | OS | HotFixes | 7 | String | Example: [KB12345 Q21345] |
| Cisco (9) | OS | HostFQDN | 8 | String | Example: ghoward-xp1.amer.cisco.com |
| Cisco (9) | OS | Package | 100 | Extended Query Protocol | |
| * (any) | AV | Software-Name | 3 | String | Name of the software product |
| * (any) | AV | Software-ID | 4 | Unsigned32 | Numerical identifier of the software product |
| * (any) | AV | Version | 5 | Version | Version of the software |
| * (any) | AV | Scan-Engine-Version | 6 | Version | Version of the AV scan engine |
| * (any) | AV | DAT-Version | 7 | Version | Value contains version of AV signature file, e.g. 559.0.0.0, 4.5.2.0. |
| * (any) | AV | DAT-Date | 8 | Time | Release time of AV signature file |
| * (any) | AV | Protection-Enabled | 9 | Unsigned32 | 0 = Disabled 1 = Enabled |

| | | | | | |
|-----------|-----|-----------------------------|-------|------------|--|
| * (any) | AV | Action | 10 | String | Format and content are vendor-specific. Maximum length to be supported is 255 chars. |
| Cisco (9) | HIP | CSAVersion | 5 | Version | CSA Version |
| Cisco (9) | HIP | CSAOperationalState | 9 | Unsigned32 | 0 = Disabled 1 = Enabled |
| Cisco (9) | HIP | TimeSinceLastSuccessfulPoll | 11 | Unsigned32 | |
| Cisco (9) | HIP | CSAMCName | 32768 | String | |
| Cisco (9) | HIP | CSAStatus | 32769 | String | Possible values delimited by ' ': global_testmode_on rootkit_detected ipforwarding_on |
| Cisco (9) | HIP | DaysSinceLastSuccessfulPoll | 32770 | Unsigned32 | e.g. 3 |

RADIUS Attributes for NAC

The table below lists all RADIUS attributes, including Cisco vendor-specific attributes (VSAs), relevant to NAC.

| NAC-L2-802.1x | NAC-L2-IP | NAC-L3-IP | # | Attribute Name | Description |
|---------------|-----------|-----------|----|---|---|
| √ | | | 1 | User-Name | Copied from EAP Identity Response in Access Request |
| | √ | √ | 8 | Framed-IP-Address | IP address of host |
| | √ | √ | 26 | Vendor-Specific Cisco (9,1) CiscoSecure-Defined-ACL | ACL name. Automatically sent by ACS. |
| √ | | | 26 | Vendor-Specific Cisco (9,1) sec:pg | Policy-based ACL assignment. Only applies to Catalyst 6000. sec:pg = <group-name> |
| | √ | √ | 26 | Vendor-Specific Cisco (9,1) url-redirect | Redirection URL. url-redirect=<URL> |
| | √ | √ | 26 | Vendor-Specific Cisco (9,1) url-redirect-acl | Apply the named ACL for the redirect URL; ACL must be defined locally on the NAD. Only works on switches with IOS. url-redirect-acl=<ACL-Name> |
| √ | √ | √ | 26 | Vendor-Specific Cisco (9,1) posture-token | Posture token/state name. Automatically sent by ACS. |
| | √ | √ | 26 | Vendor-Specific Cisco (9,1) status-query-timeout | Sets Status Query timer |
| | √ | √ | 26 | Vendor-Specific Cisco (9,1) host-session-id | Session identifier used for auditing. Automatically sent by ACS. |

| | | | | | |
|---|---|---|----|------------------------------------|--|
| ? | √ | √ | 26 | Vendor-Specific Microsoft = 311 | Key for Status Query: MS-MPPE-Recv-Key Automatically sent by ACS. |
| √ | √ | √ | 27 | Session-Timeout | Sets Revalidation Timer (in seconds) |
| √ | √ | √ | 29 | Termination-Action | Action on Session Timeout (0) Default: Terminate session (1) Radius-Request: Re-authenticate |
| √ | | | 64 | Tunnel-Type | 13 = VLAN |
| √ | | | 65 | Tunnel-Medium-Type | 6 = 802 |
| √ | √ | √ | 79 | EAP Message | EAP Request/Response Packet in Access Request and Access Challenge: - EAP Success in Access Accept - EAP Failure in Access Reject |
| ? | ? | ? | 80 | Message Authenticator | HMAC-MD5 to ensure integrity of packet. |
| √ | | | 81 | Tunnel-Private-Group-ID | VLAN name |

Identifying NAC Methods in RADIUS Request Attributes

| RADIUS Attributes | NAC L2 802.1x | NAC L2 IP | NAC L3 IP | NAH / Clientless | MAC- Auth- Bypass |
|------------------------------|------------------------------|--------------------------|--------------------------|-----------------------------|----------------------------------|
| [1] Username | yes | yes | yes | | |
| [6] Service- Type | | | | 10 | 10 |
| [8] Framed IP Address | | yes | yes | | |
| [26/9/1]VSA | | aaa:service=ip_admission | aaa:service=ip_admission | aaa:service=ip_admission | |
| [26/9/1]VSA | | audit-session-id=# | audit-session-id=# | audit-session-id=# | |



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks or trademarks of Cisco Systems, Inc. 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. (0502R)

C07-332601-00 02/06