



GLOSSARY

A

- AAA** Authentication, Authorization, and Accounting server.-(Authentication, authorization, and accounting is pronounced “triple-A.” An 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-Request** Request packet that the access server sends to the RADIUS server requesting authentication of the user.
- Accounting** Accounting in network management subsystems is responsible for collecting network data relating to resource usage.
- Agentless host processing** A method that ACS uses to process authentication requests from hosts that do not have an authentication agent installed, such as Cisco Trust Agent.
- ACL** Access Control List-Each ACL consists of a set of ACL entries.
- 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.
- APT** Application Posture Token-The result of a posture validation check for a given vendor’s application.
- Audit server** A 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.
- AV pair** Attribute-value pair-Encoding that the RADIUS protocol uses to specify an action that the host performs when a condition represented by the attribute value is met.

C

- Cisco Trust Agent** Cisco Trust Agent. The Cisco implementation of the PA.

E

- EAP** Extensible Authentication Protocol-Provides the ability to deploy RADIUS into Ethernet network environments. EAP is defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards.
- EAP-TLS** Extensible Authentication Protocol-Transport Layer Security-Uses the TLS protocol (RFC 2246), which is the latest version of the Secure Socket Layer (SSL) protocol from the IETF. TLS provides a way to use certificates for user and server authentication and for dynamic session key generation.
- Endpoint Device** Any machine that attempts to connect to or use the resources of a network. Also referred to as a host.
- 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.

G

- GAME group feedback** Generic Authorization Message Exchange-A Cisco protocol that is used in the Cisco Network Admission Control (NAC) environment. GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server

H

- Host** Another name for an endpoint device.

L

- LDAP** Lightweight Directory Access Protocol-A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.

M

- MAB** MAC authentication bypass-An authentication method that uses the MAC address of a device to authenticate the device, instead of using an IP address.

N

NAC	Network Admission Control-NAC is a Cisco-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-compliant applications	Applications that integrate with the NAC client. Examples of such applications are Cisco Security Agent and antivirus programs that provide the NAC client with attributes about themselves, such as the version number of a virus definition file.
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), and 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.
NDG	Network Device Group-A collection of network devices that act as a single logical group.
NRH	Nonresponsive host-A host that does not have the Cisco Trust Agent installed to perform posture validation. An NRH is also known as a “agentless” host.

P

PA	Posture Agent-An application that serves as the single point of contact on the host for aggregating posture credentials from potentially multiple posture plug-ins and communicating with 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.
PEAP	Protected Extensible Authentication Protocol-An 802.1x authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft that Cisco Systems, Microsoft, and RSA Security submitted to the IETF.
Posture credentials	State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information.
Posture plug-in	A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization.
PV	Posture Validation-Posture validation validates the collection of attributes that describe the general state and health of the user’s machine (the “host”).

- PVS** Posture Validation Server-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.
- Posture validation** The authorization of a network endpoint's posture credentials by one or more posture-validation servers and their associated compliance policies.

R

- RAC** RADIUS Attribute Component.
- RADIUS** A widely deployed protocol enabling centralized authentication, authorization, and accounting for network access.

V

- VSA** Vendor Specific Attribute-Most vendors use the VSA to support value-added features.