FAQ

Network Admission Control

This is a comprehensive Technical FAQ for Network Admission Control (NAC).

The document covers NAC features and architecture for NAC L3 IP on Cisco IOS routers, NAC L2 IP on Cisco IOS and CatOS switches, and NAC L2 802.1x on Cisco IOS and CatOS switches.

TABLE OF CONTENTS

GENERAL

Q. Does NAC work with non-Cisco devices?

A. No, only Cisco devices support the EAPoUDP protocol.

Q. How do I turn off NAC?

A. Enter the **no ip admission <policy-name>** command on each NAC-enabled interface.

Q. What minimal hardware and software components required to use NAC?

A. There are three primary components to the NAC solution:

- A network endpoint running the Cisco Trust Agent (CTA)
- Cisco network access device (NAD) with NAC enabled on one or more interfaces for network access enforcement
- Cisco Secure Access Control Server (ACS) for endpoint compliance validation.

Q. Which router platforms and IOS versions support NAC?

A. The only IOS release train supporting NAC is Cisco IOS 12.3(8)T or later with the Advanced Security feature sets. For the latest platform support, see http://www.cisco.com/go/nac/.

Router Model	IOS Version
Cisco 83x Series Router	12.3(8)T and later
Cisco 850 Series Routers	12.3(14)T and later
Cisco 870 Series Routers	12.3(14)T and later
Cisco 1700 Series Routers	12.3(8)T and later
Cisco 1800 Series Routers	12.3(8)T and later
Cisco 2600XM	12.3(8)T and later
Cisco 2691 Multiservice Platform	12.3(8)T and later
Cisco 2800 Series Routers	12.3(8)T and later
Cisco 3640 Multiservice Platform	12.3(8)T and later
Cisco 3660-ENT Series Router	12.3(8)T and later
Cisco 3725/3745 Multiservice Access Router	12.3(8)T and later
Cisco 3800 Series Routers	12.3(11)T and later
Cisco 7200 Series	12.3(8)T and later

Q. Which switch platforms support NAC?

A. The table shows support for NAC Framework in IOS and CatOS-based switches:

Switch Model, Supervisor	OS Version	NAC L2 802.1x	NAC L2 IP	NAC L3 IP	NAC Agentless Host
6500—Sup32, 720	Native IOS	–	12.2(18)SXF2	–	NAC L2 IP
6500—Sup2	Native IOS	–	–	–	–
6500—Sup32, 720, Sup2	Hybrid/CatOS	CatOS 8.5	CatOS 8.5	–	–
4000 Series—Sup2+, 3–5	IOS	12.2(25)SG	12.2(25)SG	–	12.2(25)SG (NAC L2 IP)
3550,	IOS IP Services and IP base	12.2(25)SED	12.2(25)SED	–	12.2(25)SED
3750, 3560	IOS—Advanced IP Services, IP Services, IP Base	12.2(25)SED	12.2(25)SED	–	12.2(25)SED
2970	IOS—LAN Base	12.2(25)SED	–	–	–
2960	IOS—LAN Base	12.2(25)SED	–	–	–
2950	IOS	12.1(22)EA6			
	–	–	–		
2940, 2955	IOS	12.1(22)EA6			
	–	–	–		
6500—Sup1A	All	No	No	No	No
5000	All	No	No	No	No
4000/4500	CATOS	No	No	No	No
3500XL	All	No	No	No	No
2900XM	All	No	No	No	No

Q. Is there a document that describes how to configure all of the various NAC components?

A. *Implementing Network Admission Control* and other white papers are available at http://www.cisco.com/go/nac/.

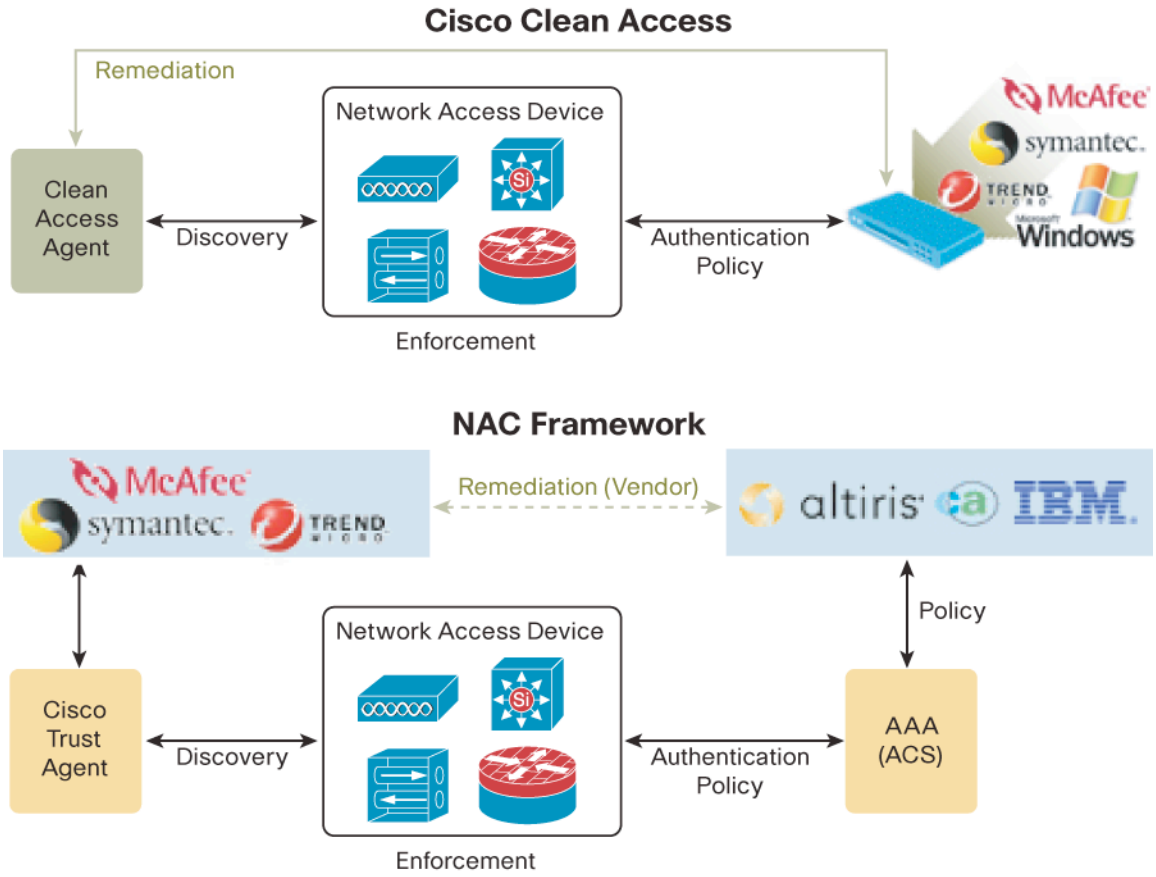
Q. What is the difference between the Cisco Clean Access NAC Appliance and NAC Framework?

A. NAC Framework uses new and existing Cisco network infrastructure and NAC partner products for NAC deployments at Layer 2 and Layer 3, including virtual private networks (VPN) and wireless. For additional information, see the NAC Overview FAQ.

NAC Appliance uses the Cisco Clean Access solution to provide customers with a self contained product that integrates with the network infrastructure. NAC Appliance provides admission control and posture assessment capabilities in network infrastructure that does not support NAC Framework.

This diagram shows the two solutions.

Figure 1.



Q. What are the NAC Posture States? What do they indicate?

A.

- **Healthy**—Host is compliant; no restrictions on network access.
- **Checkup**—Host is within policy but an update is available. Used to proactively remediate a host to the Healthy state.
- **Transition**—Host posturing is in process; give interim access pending full posture validation. This is applicable during the host boot process when all services might not be running or audit results are not yet available.
- **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 endpoint devices; 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.

Q. What is the difference between a Posture Plugin (PP) and a Posture Agent (PA)?

A. The Posture Plugin is a software component on the host that provides posture credentials to the Posture Agent. The Posture Agent also resides on the host and acts as a broker, collecting credentials from the posture plugins on the host and communicating with the network. The Cisco Trust Agent is Cisco Systems's implementation of the posture agent. The Posture Agent can use either EAPoUDP or 802.1x to communicate with the network.

PROTOCOLS

Q. What is EAP?

A. EAP is a request-response protocol defined in RFC 2284.

EAP is used to exchange identity and authentication credentials between a peer and a AAA server. Cisco NAC uses EAPoUDP and EAPoLAN for NAC L2 IP and NAC L2 802.1x.

Q. What extensions have been added to EAP for NAC?

A. The EAP-TLV extension is used to carry posture credentials, including posture Attribute Value Pairs (AVP) and posture notifications.

The Status Query method is used to securely query the posture status of a peer without a full credential revalidation.

Q. What is the port number for EAPoUDP?

A. EAPoUDP uses UDP port 21862

Q. What is EAP-FAST?

A. Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS-based RFC3748-compliant EAP method. Cisco has posted and informational *draft, draft-cam-winget-eap-fast-02.txt*, to the IETF for viewing.

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

Phase 1: Use PAC to mutually authenticate the client 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.

Q. How is EAP-FAST different from PEAP?

A. PEAP provides various strengths, but requires digital certificates, and is not supported on every client device. Like PEAP, EAP-FAST is a tunneled protocol that supports a variety of authentication methods, but it does not require digital certificates and is designed to run on nearly every client device.

Q. Which 802.1x supplicants support EAP-FAST?

A. The wired-only *lite* supplicant in CTA 2.0 supports EAP-FAST. If you need wireless support, the Meetinghouse AEGIS client (supplicant) http://www.mtghouse.com/ supports EAP-FAST.

Q. Which method of PAC provisioning for EAP-FAST does NAC L2 802.1x support?

A. Using the NAC L2 802.1x CTA supplicant, you can provision a PAC with in-band-provisioning. The CTA supplicant only provisions a PAC on the host if the ACS server allows in-band-provisioning. CTA only provisions a PAC on the host if the client-side authentication is a successful machine authentication using a certificate assigned to the machine (machine certificate) or a successful user authentication. The CTA supplicant does not support Out-of-band provisioning with NAC L2 802.1x.

ADMISSION METHODS

Q. What is NAC L2 IP?

A. Similar to the NAC on router platforms, any connected endpoint is assessed for its application postures. No identity-based authentication is involved. Posture is validated, and policy is applied to the enforcement point based on its state of posture. Posture information is carried over the EAP over UDP protocol. Posture validation is triggered by any new ARP request (ARP Inspection) or DHCP binding (DHCP Snooping). Remediation process takes place when posture information does not meet the policy requirement. Traffic from any endpoint violating security policy requirements is restricted by an access control list, which is downloaded from the AAA server. The downloaded ACL is inserted in front of the default port ACL.

Q. Can you provide an ACL example for NAC L2 IP?

A.

```
ip access-list extended interface_acl
 remark Allow EAPoUDP
 permit udp any any eq 21862
 remark Allow DHCP
 permit udp any eq bootpc any eq bootps
 remark Allow DNS
 permit udp any any eq domain
 remark Allow HTTP access to update server
 permit tcp any host 10.0.200.30 eq www
 remark Allow ICMP for test purposes
 permit icmp any any
 remark Implicit Deny
 deny ip any any
```

Q. Do I need a supplicant for NAC L2 IP?

A. No, NAC L2 IP uses EAP over UDP to perform posture checking similar to that of NAC L3 IP.

Q. What is NAC L2 802.1x?

A. This NAC enabled 802.1x deployment method allows user identity, machine identity, and posture validation to be gathered in the 802.1x access control conversation. NAC L2 802.1x uses the EAP-FAST method to exchange this information between the client and server.

Q. Does the current Windows XP supplicant from Microsoft support NAC?

A. No, NAC L2 802.1x, uses EAP-FAST as the EAP method. It has been modified to carry user and machine credentials in a TLS tunnel while also providing posture checking through CTA The MS Windows 802.1x supplicant does not support EAP-FAST and provides no support for posture validation. You can use the MS supplicant to perform user authentication and NAC L2 IP as a supplemental method to provide posture validation if you can not use a NAC enabled supplicant. See the NAC Deployment Guide for additional information.

Q. What is GAME?

A. Generic Authorization Message Exchange. The protocol used for communication between ACS and a partner audit server through an https session extending Security Assertion Markup Language (SAML).

ACS triggers the auditing of NAC Agentless Hosts through the vendor audit server. ACS then polls periodically for audit decisions. The audit server responds with a posture state when the audit is completed.

Q. What is HCAP?

A. Host Credential Authorization Protocol. ACS forwards client EAP-based credentials to one or more vendor servers through one or more HTTP(S) sessions. ACS then receives a posture token response and optional notification messages from each vendor server.

CISCO TRUST AGENT (CTA)

Q. Is CTA required for NAC?

A. Yes, the Cisco Trust Agent (CTA) is required so that NAC can supply the posture credentials of the endpoint. Hosts that cannot run the CTA can be granted access to the network using manually configured exceptions by MAC or IP address on the router or ACS. Exceptions by device types such as Cisco IP phones can also be permitted using CDP on the router.

Q. Where can I download the CTA?

A. If you are a registered Cisco user, you can download the CTA for free from www.cisco.com.

Q. What operating systems and attributes does CTA 2.0 support?

A. This table shows platform and attribute support for CTA 2.0.

CTA Version	OS	Attributes
2.0	• Windows NT 4.0 • Windows 2000 Professional and Server (SP4) • Windows XP Professional (up to SP1) • Windows 2003	• Cisco:PA:PA-Name • Cisco:PA:PA-Version • Cisco:PA:OS-Type • Cisco:PA:OS-Version • Cisco:PA:MachinePostureState
2.0	• Red Hat Linux 9 • Red Hat Enterprise Linux v3	• Cisco:PA:PA-Name • Cisco:PA:OS-Version • Cisco:PA:Kernal-Version • Cisco:PA:MachinePostureState • Cisco:PA:OS-Type • Cisco:PA:OS-Version

Q. What are the differences for each CTA installation file?

A.

CTA .exe Files	Description
ctasetup-win-[version].exe	The installation of this package is considered *noisy*. The end user will be prompted to accept a license agreement, choose the install destination folder, and other general installation options. This package only installs the CTA scripting interface. The supplicant is not installed by using this package.
ctasetup-supplicant-win-[version].exe	The installation of this package is *interactive*. The end user is prompted to accept a license agreement, choose the install destination folder, and other general installation options. This package also can install both the CTA scripting interface and the supplicant. The end user is prompted to select which CTA features to install.
CtaAdminEx-win-[version].exe	The installation of this package is *silent*. You extract the file named ctasilent-win-[version].exe file

CTA .exe Files	Description
	from this package. As the administrator, you accept the license agreement for end users and then deploy the file as a completely silent install that does not prompt the end user for any options. The supplicant is not installed using this package.
CtaAdminEx-supplicant-win-[version].exe	If you use this package, you are choosing to create a silent installation package for the end user. You extract a file named ctasilent-supplicant-win-[version].exe from this package. As the administrator, you accept the license agreement for endusers and then deploy the ctasilent-supplicant-win-[version].exe file as a completely silent install that does not prompt the end user for any options. The supplicant is installed by using this package.

Q. Can CTA 2.0 gather any additional information from MS Windows?

A. Yes, the Host Posture Plugin for Windows can return these attributes: the current Windows Service Pack, the machine name, and the list of hotfixes that have been applied to Windows.

Q. Does CTA 2.0 include an 802.1x supplicant?

A. Yes, CTA includes an 802.1x supplicant that supports only wired 802.1x connections. If you need wireless NAC support you must purchase either the Meetinghouse or Funk supplicants that include NAC wireless support.

Q. I read that CTA 2.0 supports Asynchronous Status Query. What is that?

CTA 2.0 supports Asynchronous Status Query, which gives CTA the ability to signal the Network Access Device (NAD) that something in CTA on the client has changed. The network should initiate an identity and posture status query to compare the changed state to that of the defined admission policy. Asynchronous Status Query works with NAC L2 802.1x.

Q. Which network port does the CTA listen on for NAC challenges?

A. The CTA communicates with the network access device with EAP-over-UDP (EAPoUDP), which uses UDP port number 21862 by default. To change the default EAPoUDP port, edit the ctad.ini configuration file. For all of the ctad.ini configuration file options, see the CTA Administrator Guide.

Whichever port you choose to use, verify that any installed personal firewall software permits incoming traffic to this port. Otherwise, the CTA cannot respond to NAC challenges from the network access device.

Q. Does the CTA have a log file? Where is it? Does it have a size limit?

A. The CTA does have logging capabilities for troubleshooting, but it is disabled by default.

To enable it, go to the CTA configuration directory at C:\Documents and Settings\All Users\Application Data\Cisco Systems\CiscoTrustAgent\, and rename the ctalogd.tmp file to ctalogd.ini. The log file is created under the Logs subdirectory as soon as the CTA receives another EAPoUDP request. If the log file is not created, you might not have renamed the file correctly or the CTA is not receiving EAPoUDP requests. This might be caused by a personal firewall blocking the requests from the network access device.

The default maximum log size is 4mb and can be changed by editing the ctalogd.ini file. When the maximum log size is reached, a new log file is created. Over time, an unlimited number of files are created.

For more log file customizations, see the Event Logging section of the CTA Administrator Guide.

Q. How do I authorize my CTA to talk to another company's ACS server? How do I install a digital certificate from the ACS or root certificate authority for use with the CTA?

A. By default, the CTA trusts any ACS whose digital certificate is signed by any certificate authority (CA) in the certificate chain that already exists in the endpoint's trusted root store (DST, Thawte, or Verisign for example). For self-signed certificates or private CAs, you need to add the certificate manually if you have not already distributed them to your hosts.

So that CTA can import the certificate during installation on the client, create a folder named *certs* in the same directory as the CTA install file (.exe). CTA automatically looks for the .cer in this folder during installation and imports it.

To manually add the certificate to CTA, you can also use the CTACert.exe program provided with CTA. To add a new digital certificate to CTA for ACS or its root certificate authority, Use the command:

```
ctacert.exe /add "cert_path" /store "Root"
```

Note that Root means to store the certificate in the root store and that this operation requires Administrator privileges on the local machine.

Q. How do I restrict the CTA to only communicate to my ACS servers and not to any ACS with a certificate signed by a public CA?

A. There are several options:

Use self-signed certificates for each ACS, and add all of them to each CTA installation. This is generally not a very scalable solution.

Use a private CA (Microsoft Certificate Server) to sign all of your ACS certificates, and to install your private CA public certificate in the Root certificate store of your hosts.

Create and edit a ctad.ini file to restrict the certificates that the CTA accepts according to a matching certificate attributes.

Q. Can I automatically add one or more ACS or root CA certificates when installing CTA?

A. Yes, CTASetup.exe automatically installs all available certificates from a subdirectory named *certs*. Create the directory in the same directory as CTASetup.exe, place your certificates in it, and then run the setup program.

Q. I just installed a posture plugin from your partner *xyz*. How do I know if the plugin is properly registered with the CTA?

A. After a NAC authorization, you can check the CTA log file for processPostureRequests messages (see above on how to enable logging: Does the CTA have a log file? Where is it? Does it have a size limit?). Example CTA log entries are:

```
26  14:37:09.496  11/17/2004  Sev=Info/4  PPMgr/0xE3600006 processPostureRequests returned (8) in
dll C:\Program Files\Common Files\Cisco
Systems\CiscoTrustAgent\Plugins\CiscoSecurityAgentPlugin.dll.
27  14:37:09.496  11/17/2004  Sev=Info/4  PPMgr/0xE3600006 processPostureRequests returned (8) in
dll C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\CiscoHostPlugin.dll.
```

You can also check the ACS Passed Authentications log for logged credentials.

Q. How can I tell if a partner plugin for CTA was properly installed and functioning?

A. Look in C:\Program Files\Common Files\Cisco Systems\CiscoTrustAgent\Plugins\ to verify the plugin is there.

If the plugin is in the folder, you can verify the interaction with CTA by enabling CTA debugging. To do this, edit the ctalogd.ini file:

```
C:\Program Files\Cisco Systems\CiscoTrustAgent\Logging\ctalogd.ini
```

Change the following entries in the file as shown:

```
PPMgr=15
Plugin=15
```

Save and Close the ctalogd.ini file. On the next EoU challenge, you will now see a log file under Logs that has detailed information about the registered plugins.

Q. I am receiving these errors when using the CSUtil.exe to import an ADF file into ACS. Is there a problem with the ADF file?

```
CSUtil v4.0(1.12), Copyright 1997-2005, Cisco Systems Inc
[attr#0]: Error: cannot manually add  attributes with the reserved ID of 1 or 2
[attr#1]: Error: cannot manually add  attributes with the reserved ID of 1 or 2
Attribute 6101:3:1  (Application-Posture-Token) automatically added to  dictionary (DB).
Attribute 6101:3:2 (System-Posture-Token)automatically added to dictionary (DB)
[attr#2]: Attribute 6101:3:3  (Software-Name) added to the dictionary (DB).
```

A. The errors shown in the output are for the APT and the SPT, which is normal. If there were problems importing the ADF, you would not see them in the log file or policy.

Q. What is the maximum user-notification message size that the CTA can display?

A. The CTA v1.0 can display 1000 single-byte characters. ACS limits the user message to 1000 characters.

Q. Does the CTA user-notification dialog support non-ASCII (unicode, multibyte) characters?

A. Yes, the CTA supports the display of UTF-8 encoded character strings. However, ACS currently does not support UTF-8 encoding of messages. Only ASCII characters can be used for the user-notification dialog.

Q. How does the CTA know when a posture change has occurred on the host?

A. During the status query process, CTA checks with the posture plugins for a status change. It is the responsibility of the individual posture plugins to recognize a status change in their respective software applications and agents.

Q. What is the EAP identity that is sent from the PA to initiate the PEAP tunnel? Is it the username, the machine name, or the IP address?

A. The EAP identity sent by the posture agent (PA) to initiate the PEAP tunnel is an empty (null) string. The EAP identity provided within the PEAP tunnel is machine-name:username of the client undergoing NAC authorization. If no user is logged in, the username is replaced with SYSTEM.

Q. Why is the CTA not working with Windows XP?

A. You probably have Windows XP with Service Pack 2. The new firewall feature is blocking the default EAP-over-UDP port (UDP 21862) which is used for NAC. Either disable your Windows firewall or permit traffic to UDP 21862.

Q. How do you single sign-on so that CTA uses the Windows username and password credentials?

A. You configure single sign-on (SSO) by clicking the check box in the CTA deployment profile configuration in the supplicant menu under *User Credentials > Use Single Sign-on for password credentials.* You need to move the xml files to the correct subdirectories and restart the client. By default, the directories created are Cisco Systems, Inc\Cisco Trust Agent 802.1x wired client\profiles\networks and Cisco Systems, Inc\Cisco Trust Agent 802.1x wired client\profiles\policies.

If that has already been done, verify that EAP-GTC is not enabled in the network access profile on ACS. EAP-GTC always prompts for a password from the supplicant.

Q. How do I enable CTA to automatically launch an Internet browser on the client?

A. CTA 2.0 can automatically open the default web browser to a on a client machine when CTA receives a URL that has been predefined in ACS. You can set the URL when defining individual posture validation rules in the notification string field. Filling in the notification string causes CTA to attempt to launch the default web browser to the URL on the client device. For example, you can automatically launch a browser for a quarantine assessment by entering http://x.x.x.x/quarantine.html in the posture assessment notification string of the quarantine rule.

CISCO SECURITY AGENT (CSA)

Q. What versions of CSA support NAC? Do they install the Cisco Trust Agent? What attributes does it provide?

A. This table shows the NAC attributes for different releases of CSA.

CSA Version	CTA Install	Attributes
4.02+	No	• Cisco:Host:ServicePacks • Cisco:Host:Hotfixes • Cisco:HIP:CSAVersion
4.5	Yes	• Cisco:HIP:CSAVersion • Cisco:HIP:CSAOperationalState • Cisco:HIP:CSAMCName • Cisco:HIP:CSAStatus • Cisco:HIP:DaysSinceLastSuccessfulPoll

Q. Can the Cisco Trust Agent use the asynchronous status change to report a status change in CSA to the Network Access Device?

A. Yes, asynchronous status change is supported in CSA 4.5.1. If a change occurs in CSA (for example, user disables CSA) this triggers an asynchronous status query from CSA to the Cisco Trust Agent sending an EAPOL-Start to the Network Access Device. The asynchronous status change feature is only supported with NAC L2 802.1x.

NAC L3 IP (ROUTERS)

Q. Do you have a sample NAC L3 IP configuration for a router?

A. Yes, this is a sample NAC configuration for an 1800 series router with only two interfaces. The client subnet is 192.168.150.0/24, and the server subnet is 192.168.1.0/24. The NAC-specific configuration entries are in bold.

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname NACPack-1800
!
aaa new-model
!
!
aaa authentication login default none
aaa authentication eou default group radius
aaa session-id common
ip subnet-zero
ip cef
!
```

```
!
ip auth-proxy inactivity-timer 5
ip admission inactivity-timer 5
ip admission name NAC eapoudp
!
ip ips po max-events 100
ip domain name cisco.com
ip name-server 192.168.1.5
no ftp-server write-enable
!
!
identity profile eapoudp
 description Exception list for CTA-less devices
 device authorize type cisco ip phone policy NAC_Exempt_Devices
 device authorize ip-address 192.168.150.10 policy NAC_Exempt_Devices
identity policy NAC_Exempt_Devices
 description NAC policy for authorized devices
 access-group ACL_Permit_All
eou clientless username clientless
eou clientless password clientless
eou allow clientless
eou timeout hold-period 60
eou timeout status-query 30
eou timeout revalidation 300
eou logging
!
!
interface FastEthernet0/0
 description NAC Server Network
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description NAC Client Network
 ip address 192.168.150.1 255.255.255.0
 ip access-group ACL_Guest_Access in
 ip admission NAC
 duplex auto
 speed auto
```

```
!
router eigrp 1
 network 192.168.1.0
 network 192.168.150.0
!
ip classless
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended ACL_Guest_Access
 remark Allow EAPoUDP, DHCP, Remediation only for Guest Access
 permit udp any any eq 21862
 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
 permit tcp any host 192.168.1.7 eq www
 deny  ip any 192.168.1.0 0.0.0.255
 permit ip any any
ip access-list extended ACL_NAC_Exempt
 deny  ip any any log
ip access-list extended ACL_Permit_All
 permit ip any any log
!
ip radius source-interface FastEthernet0/0
!
radius-server host 192.168.1.2 auth-port 1645 acct-port 1646
radius-server key cisco123
radius-server vsa send authentication
!
control-plane
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 privilege level 15
 transport input telnet ssh
```

```
line vty 5 15
 privilege level 15
 transport input telnet ssh
!
end
```

Q. What happens to the first packet sent by the host that triggers NAC authorization?

A. This depends on the access control list (ACL) applied to the router interface and any dynamically inserted access control entries (ACEs). If the default ACL denies these packets, they are dropped until the dynamic ACL from the NAC authorization is received and inserted to allow such traffic. The dynamic ACL that is downloaded from ACS is applied to the top of the interface ACL and can either increase or decrease access as needed by the policy.

For this reason, the default interface ACL should allow the minimum level of L3 and L4 network services needed by your hosts, especially when providing guest access. Some of these minimal network services can include:

- EAPoUDP responses (permit udp any any eq 21862)
- DHCP requests (permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps)
- ICMP echo-replies (permit icmp any any)
- DNS requests (permit udp any any eq dns)
- NTP requests (permit udp any any eq ntp)
- Permitting certificate revocation list (CRL) checks
- Spoof mitigation by dropping any packets that are sourced from a different address than the local subnet
- Providing default network access to the Internet for guest users

Note that broadcasts, multicasts, and traffic destined to the router interface are implicitly exempt from posturing. EAPoUDP packets must be permitted by the interface ACL for the router to receive the host's EAPoUDP response!

Q. Can NAC and authentication proxy co-exist on the same interface? If so, which is activated first?

A. Yes, authentication-proxy and NAC can co-exist on the same network interface. Auth-proxy is triggered before NAC. An ACL downloaded to the NAD for NAC overwrites the authentication-proxy ACL.

Q. Does NAC work with EZVPN?

A. Easy VPN server and NAC can co-exist on the same interface. Cisco Easy VPN Client Version 3.6.4 and later supports NAC messages. The encryption and decryption process does not interfere with the NAC processing.

Q. When is the dynamic ACL assigned by NAC removed from the interface ACL?

A. The dynamic ACL entries assigned by NAC are either changed by another posture revalidation or removed after a period of inactivity. This period of inactivity is defined by the inactivity timer (**ip admission inactivity-timer** *minutes*). The default interface ACL then applies to the host until another NAC authorization occurs. The default inactivity period is 60 minutes.

Q. When I use the show eou all command on the NAD, I get different AuthTypes and Posture-Tokens. What do they mean?

A. The **show eou all** command displays the state of NAC sessions that are managed by the NAD.

```
NACPack-1800# show eou all
-----------------------------------------------------------------
Address         Interface       AuthType    Posture-Token Age(min)
-----------------------------------------------------------------
192.168.150.10  FastEthernet0/1 STATIC      -------       1
192.168.150.11  FastEthernet0/1 UNKNOWN     -------       1
192.168.150.12  FastEthernet0/1 Clientless  -------       1
192.168.150.13  FastEthernet0/1 Clientless  Healthy       1
192.168.150.14  FastEthernet0/1 EAP         -------       1
192.168.150.15  FastEthernet0/1 EAP         Healthy       1
192.168.150.16  FastEthernet0/1 EAP         Quarantine    1
```

There are several different Authentication Types (AuthTypes) and Posture Token combinations for NAC as described in the this table:

AuthType	Posture-Token	Status
STATIC	-------	The NAD statically authorized the host using a local identity profile without doing an EAP request over RADIUS to the ACS. Therefore, there is no posture token from the ACS, and the Posture-Token field shows only -------.
UNKNOWN	-------	• The host could not be authorized by the NAD or ACS. There are many possible reasons for this, including: • The host does not have a CTA installed. This could be one of several scenarios: • This is a legitimate nonresponsive host (NRE) that should be permitted by a static router authorization or ACS network access restriction (NAR) • This is an host that should have the CTA (and other agents potentially) and needs remediation • This is a guest user (customer, consultant, and so on.) that is not managed by you. • This host has a personal firewall that is blocking the CTA ability to receive EAPoUDP challenges from the NAD on UDP port 21862. • There is a network-based firewall that is blocking the CTA response to the NAD. • There was a failure in the EAP protocol between the host and ACS. Possible reasons for this failure include: • The host's CTA does not have a digital certificate for the ACS or the root CA of the ACS and refuses to provide its credentials to the ACS via EAP. • The host CTA has a certificate for the ACS or the root CA of the ACS but the subject names do not match the permitted certificates in the CTA ctad.ini file. • The ACS digital certificate has expired. This can be caused by a time synchronization issue on the host or on ACS. • The ACS does not have a digital certificate installed. • The host is not configured as an authorized *clientless* host in the ACS network access restrictions (NARs), resulting in an ACS failed attempt.
Clientless	-------	The host does not have a CTA but was authorized by ACS as a *clientless* host. The posture token name is ------- because it was not defined using the posture-token VSA in the ACS group that the clientless user is assigned to.

AuthType	Posture-Token	Status
Clientless	Healthy	The host does not have a CTA but was authorized by ACS and given a posture of Healthy.
EAP	-------	• The host CTA successfully communicated via EAPoUDP to the ACS. However, the posture-token name was not downloaded to the NAD. This could be because: • The posture token name is not defined by using the posture-token VSA in the ACS group that the clientless user is assigned to. • There is a network access restriction (NAR) preventing a complete authorization. Check the ACS Failed Attempts log (in ACS select Reports and Activities > Failed Attempts) for the reason.
EAP	Healthy	The host was authorized by ACS and given a posture of Healthy.
EAP	Quarantine	The host was authorized by ACS and given a posture of Quarantine.

Q. Does NAC work with HSRP? If the primary router fails, will the secondary router have to revalidate all of the NAC sessions?

A. NAC does work with HSRP. However, there is no stateful failover of NAC session information from one NAD to the other. All hosts are re-validated by the secondary router.

Q. How can I improve the RADIUS failover time caused by a busy AAA server?

A. You can set the **radius-server timeout** <*seconds*> command to shorten the amount of time that IOS waits before marking a server unreachable. The default is 5 seconds.

Use the command **radius-server deadtime** <*minutes*> to tell IOS how long to pass over a server after it is marked unreachable. The default is 0, meaning that IOS never bypasses it, and every new request goes to the first server in the list.

To improve performance and scalability without impacting the user experience, consider using the IOS server load balancing (SLB) feature with multiple ACS servers.

Q. How do I configure the NAD to permit nonresponsive (clientless) hosts?

A. You can use one of these methods to authorize nonresponsive hosts (NREs) on a router that does not have the CTA installed.

The first is to use identity profiles and policies that are configured on the router to statically permit the hosts by IP address or CDP device type.

```
identity profile eapoudp
  description Exception list for non-responsive devices
  device authorize type cisco ip phone policy NAC_Exempt_Devices
  device authorize ip-address 192.168.150.10 policy NAC_Exempt_Devices
identity policy NAC_Exempt_Devices
  description NAC policy for authorized devices
  access-group ACL_Permit_All
ip access-list extended ACL_Permit_All
  permit ip any any log
```

These hosts are shown with STATIC connection types on the router:

```
NACPack-1800# show eou all
------------------------------------------------------------------
Address         Interface        AuthType  Posture-Token  Age(min)
------------------------------------------------------------------
192.168.150.10  FastEthernet0/1  STATIC    -------        1
```

The second method is to have the router make a RADIUS request to the ACS that uses a specific username and password. This user profile in ACS (*clientless*, in this example) is configured with network access restrictions (NARs) to authorize specific hosts without the CTA based on their MAC or IP address. This option is configured on the router with the following commands:

```
eou clientless username clientless
eou clientless password clientless
eou allow clientless
```

Hosts authorized by this clientless method have a CLIENTLESS AuthType:

```
NACPack-1800#show eou all
------------------------------------------------------------------
Address        Interface       AuthType     Posture-Token Age(min)
------------------------------------------------------------------
192.168.150.7  FastEthernet0/1 CLIENTLESS   Unknown       0
```

Note that you must also configure the ACS with the clientless username and password combination as specified.

The third is MAC authentication bypass, which is supported on the Catalyst 6500. MAC-Auth-Bypass is enabled on the 6500, and the list of MAC addresses is specified in ACS. This example assumes that the proper RADIUS configuration has been performed for 802.1x authentication. To enable MAC-Auth-Bypass, use these commands:

```
6506-dut> (enable) set mac-auth-bypass enable
Mac-Auth-Bypass enabled globally.
6506-dut> (enable) set port mac-auth-bypass 2/1 enable
Mac-Auth-Bypass successfully enabled on 2/1.
```

Q. How do I verify that a URL redirection has been applied to a specific host session?

A. URL redirections are optionally applied after a posture validation along with any downloaded ACL. These are useful to either notify or remind a user with a web browser of his posture state and what he must do to become compliant with the network security policy.

Use the **show eou ip** <*ip-address*> command to see if a URL-redirection is applied to a specific host session on the NAD:

```
NACPack-1800#show eou ip 192.168.150.5
Address             : 192.168.150.5
Interface           : FastEthernet0/1
AuthType            : EAP
PostureToken        : Quarantine
Age(min)            : 0
URL Redirect          : http://192.168.1.7/quarantine.htm
ACL Name            : #ACSACL#-IP-Quarantine-41b7a0bf
Revalidation Period : 30 Seconds
Status Query Period : 30 Seconds
```

Q. A URL redirection is assigned to an host session, but it is not redirecting the web browser to the specified URL.

A. URL-redirection will not work in the following situations:

- The NAD HTTP server is disabled. Enable the NAD web server with the command: **ip http server**
- An interface ACL has not been applied to the NAC-enabled interface. Apply an interface ACL to the NAC-enabled interface.
- The ACL entries do not block the client's URL destination host. URL redirection only happens when the destination host requested by the user's browser is blocked by an ACL. If the requested server in the client's original URL is permitted by the ACL, no URL redirection occurs.

Q. When I enable NAC on the router, an ACL named SL_DEF_ACL is created. What is it used for?

A. This is a template ACL that is not applied. The template is created automatically by the advanced security images.

Q. What happens if a posture revalidation occurs while a host is downloading a large file? Will the download have to be restarted?

A. When a NAD performs a posture revalidation with EAPoUDP, it continues to apply the previous level of access until the authorization is complete. If the posture is the same, there is no interruption in the endpoint network flows. If the posture is different and the enforcement rules of the new posture prohibit this type of traffic, the endpoint network flows is interrupted and will likely cause dropped network sessions.

NAC L2 IP (SWITCHES)

Q. What triggers the NAC authentication process on the NAD (switch)?

A. When the NAD first receives either a DHCP request or ARP request from a client.

Q. Do I need an ACL on the switch interface for the client for NAC L2 IP to work?

A. While an interface ACL is not required for NAC L2 IP to function, we recommend using a default ACL on the switch port that only allows a specified type of traffic to pass before authentication can be performed.

Q. Do you have a sample NAC L2 IP configuration for an IOS switch?

A.

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname NAC2Pack-3750
!
aaa new-model
aaa authentication login local_only line
aaa authentication eou default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
!
aaa session-id common
vtp domain NAC
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name nac.cisco.com
ip name-server 10.0.200.10
ip admission name NAC-L2-IP eapoudp
!
ip dhcp snooping vlan 1000
ip dhcp-server 10.0.200.10
ip device tracking
!
eou allow clientless
eou timeout hold-period 3600
eou timeout status-query 10
eou timeout revalidation 3600
eou logging
!
vlan internal allocation policy ascending
!
vlan 10
 name employees
vlan 20
 name contractors
vlan 30
 name utilities
vlan 40
 name guests
vlan 50
```

```
 name healthy
vlan 60
 name checkup
vlan 70
 name transition
vlan 80
 name quarantine
vlan 90
 name infected
vlan 100
 name unknown
vlan 110
 name voice
vlan 200
 name server VLAN
vlan 255
 name NAD MGMT
vlan 1000
 name NAC L2 IP Default VLAN
!
interface GigabitEthernet1/0/2
 description NAC-L2-IP
 switchport access vlan 1000
 switchport mode access
 ip access-group interface_acl in
 spanning-tree portfast
 ip admission NAC-L2-IP
!
interface Vlan10
 description Employees VLAN
 ip address 10.6.10.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan20
 description Contractors VLAN
 ip address 10.6.20.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan30
 description Utilities VLAN
```

```
 ip address 10.6.30.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan40
 description Guests VLAN
 ip address 10.6.40.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan50
 description Healthy VLAN
 ip address 10.6.50.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan60
 description Checkup VLAN
 ip address 10.6.60.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan70
 description Transition VLAN
 ip address 10.6.70.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan80
 description Quarantine VLAN
 ip address 10.6.80.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan90
 description Infected VLAN
 ip address 10.6.90.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan100
 description Unknown VLAN
 ip address 10.6.100.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan110
 description Voice VLAN
```

```
 ip address 10.6.110.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan200
 description Server VLAN
 ip address 10.0.200.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan1000
 description Default Interface VLAN
 ip address 10.6.1.1 255.255.255.0
 ip helper-address 10.0.200.10
!
ip http server
ip http authentication aaa
no ip http secure-server
!
ip radius source-interface GigabitEthernet1/0/24
!
ip access-list extended audit_acl
 permit tcp any any eq www
ip access-list extended interface_acl
 permit udp any any eq 21862
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
ip access-list extended quarantine_url_redir_acl
 deny   tcp any host 10.0.200.30 eq www
 deny   tcp any host 10.0.200.101 eq www
 permit tcp any any eq www
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 include-in-access-req
radius-server host 10.0.200.20 auth-port 1645 acct-port 1646 key cisco123
radius-server source-ports 1645-1646
radius-server vsa send authentication
!
```

Q. Do you have a sample NAC L2 IP configuration for a CatOS switch?

A.

```
#version 8.5(0.123)JAC
!
#Nac
set eou enable
!
#radius
set radius server 10.0.200.20 auth-port 1812 primary
set radius key cisco123
!
set vlan 10 name employees type ethernet mtu 1500 said 100010 state active
set vlan 20 name contractors type ethernet mtu 1500 said 100020 state active
set vlan 30 name utilities type ethernet mtu 1500 said 100030 state active
set vlan 40 name guests type ethernet mtu 1500 said 100040 state active
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active
set vlan 60 name checkup type ethernet mtu 1500 said 100060 state active
set vlan 70 name transition type ethernet mtu 1500 said 100070 state active
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active
set vlan 90 name infected type ethernet mtu 1500 said 100090 state active
set vlan 100 name unknown type ethernet mtu 1500 said 100100 state active
set vlan 110 name voice type ethernet mtu 1500 said 100110 state active
set vlan 2oo name servers type ethernet mtu 1500 said 100110 state active
set vlan 255 name nads_mgmt type ethernet mtu 1500 said 100255 state active
set vlan 1000 name default_L2IP type ethernet mtu 1500 said 100110 state active
!
#acl
!
#security ACLs
clear security acl all
!
set security acl ip nac-l2-ip permit arp
set security acl ip nac-l2-ip permit dhcp-snooping
! Required for CatOS
set security acl ip nac-l2-ip permit arp-inspection any any
set security acl ip nac-l2-ip permit eapoudp
commit security acl all
set security acl map nac-l2-ip 1000
!
```

```
#module 2
set vlan 1000  2/1
set port eou 2/2 auto
!
end
```

Q. How can I verify that a downloadable ACL from ACS had been applied to the switch?

A. Enter the command **show ip access-lists** on the switch. In this example, below you can see that the Heathy_ACL had been downloaded from ACS and applied to the switch.

```
NAC4948#show ip access-lists
Extended IP access interface_acl
    10 permit udp any any eq 21862
    20 permit udp any host 10.0.200.10 eq domain
    30 permit udp any eq bootpc any eq bootps
    40 permit icmp any any
Extended IP access list quarantine_url_redir_acl
    10 deny tcp any host 10.0.200.30 eq www
    30 permit tcp any any eq www
Extended IP access list xACSACLx-IP-Healthy_ACL-433866ab
    10 permit ip any any
```

Q. How can I verify that a downloadable ACL from ACS had been applied to a particular switchport?

A. Enter the command **show ip access-list interface** *x/x* as shown in this example. The client IP address should dynamically replace the source *any* in the ACL.

```
 NAC4948#show ip access-list interface GigE 1/1
IP Admission access control entires (Inbound)
     permit ip host 10.7.1.2 any
```

Q. What is the command "IP Device Tracking" and what is its purpose?

A. The IP device tracking table tracks IP devices and then can generate periodic probes to see if the hosts it is tracking are still present or not. EOU sessions used for LPIP are created and deleted based on hosts appearing and disappearing in the IP device tracking table.

NAC L2 802.1X

Q. What types of credentials are sent from the client with NAC L2 802.1x?

A. In a Microsoft Windows environment two sets of identity credentials can be presented to the network.

The first credential involves the concept of machine authentication where the machine is authenticated before of the user. Microsoft introduced the machine authentication facility to allow the client system to authenticate by using the identity and credentials of the computer at boot time. The client can then establish the required secure channel to update and participate in the domain Group Policy Objects (GPO) model.

Machine authentication allows the computer to authenticate itself to the network by using 802.1x, just after a PC loads device drivers at boot time. The computer can communicate with Windows domain controllers to pull down machine group policies. Domain GPOs are no longer stopped by the introduction of 802.1x.

The second type of credential used for 802.1x is user authentication. After the GINA (login screen) appears, a user can login to the computer or the Windows domain, and the username and password used for login can be used as the identity credentials for 802.1x authentication.

Q. My client unable to authenticate with NAC L2 802.1x, and I do not see the CTA icon in the Windows taskbar?

A. Verify that the CTA installation file that includes the CTA supplicant is installed. If the CTA version with no supplicant was installed, cannot access the supplicant menu, no supplicant icon is shown in the Windows taskbar, and you cannot authenticate by NAC L2 802.1x.

Q. How can I view the 802.1x information for interfaces on the switch?

A.

```
show dot1x all
Dot1x Info for interface GigabitEthernet 1/1
--------------------------------------------------
Supplicant MAC 000d.80cd.cda6
AuthSM State      = AUTHENTICATED
BendSM State      = IDLE
Posture           = Healthy
ReAuthPeriod      = 3600 Seconds (From Authentication Server)
ReAuthAction      = Terminate
TimeToNextReauth  = 3570 Seconds
PortStatus        = AUTHORIZED
MaxReq            = 2
MaxAuthReq        = 2
HostMode          = Single
PortControl       = Auto
ControlDirection  = Both
```

```
QuietPeriod       = 60 Seconds
Re-authentication = Enabled
ReAuthPeriod      = From Authentication Server
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

Q. How can I verify a particular switch port has been placed in the correct VLAN?

A.

```
show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                              active    Ge1/5, Ge1/6, Ge1/7, Ge1/8
                                                    Ge1/9, Ge1/10, Ge1/13, Ge1/15
                                                    Ge1/16, Ge1/17, Ge1/18, Ge1/19
                                                    Ge1/20, Ge1/21, Ge1/22, Ge1/23
                                                    Ge1/24, Gi1/2
10   employees                       active    Ge1/3
20   contractors                      active
30   utilities                             active
40   guests                             active
50   healthy                            active    Ge1/1
60   checkup                           active
70   transition                         active
80   quarantine                       active
90   infected                           active
100  unknown                         active    Ge1/4, Ge1/11, Ge1/14
110  voice                              active
200  servers                           active    Ge1/12
255  nads                               active
```

You can see the client switch port has been placed in VLAN 50 (healthy).

You can also use this interface command to see the switch port information for the interface:

```
show int GigE 1/1 switchport
Name: Ge1/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
```

```
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 50 (healthy)
…output truncated
```

Q. Do you have a sample NAC L2 802.1x configuration for an IOS switch?

A. Yes:

```
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname NAC2Pack-3750
!
!
aaa new-model
aaa authentication login local_only line
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
clock timezone PST -8
switch 1 provision ws-c3750g-24t
vtp domain NAC
vtp mode transparent
ip subnet-zero
ip routing
no ip domain-lookup
ip domain-name nac.cisco.com
ip name-server 10.0.200.10
!
ip dhcp-server 10.0.200.10
!
dot1x system-auth-control
no file verify auto
spanning-tree mode pvst
```

```
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
 name employees
vlan 20
 name contractors
vlan 30
 name utilities
vlan 40
 name guests
vlan 50
 name healthy
vlan 60
 name checkup
vlan 70
 name transition
vlan 80
 name quarantine
vlan 90
 name infected
vlan 100
 name unknown
vlan 110
 name voice
vlan 200
 name servers
vlan 255
 name nads
vlan 1000
 name l2ip
!
interface GigabitEthernet1/0/1
 description NAC-L2-802.1x
 switchport mode access
dot1x reauthentication
dot1x port-control auto
dot1x timeout reauth-period server
spanning-tree portfast
```

```
!!
interface Vlan10
 description Employees VLAN
 ip address 10.6.10.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan20
 description Contractors VLAN
 ip address 10.6.20.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan30
 description Utilities VLAN
 ip address 10.6.30.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan40
 description Guests VLAN
 ip address 10.6.40.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan50
 description Healthy VLAN
 ip address 10.6.50.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan60
 description Checkup VLAN
 ip address 10.6.60.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan70
 description Transition VLAN
 ip address 10.6.70.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan80
 description Quarantine VLAN
 ip address 10.6.80.1 255.255.255.0
 ip helper-address 10.0.200.10
```

```
!
interface Vlan90
 description Infected VLAN
 ip address 10.6.90.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan100
 description Unknown VLAN
 ip address 10.6.100.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan110
 description Voice VLAN
 ip address 10.6.110.1 255.255.255.0
 ip helper-address 10.0.200.10
!
interface Vlan200
 description Servers VLAN
 ip address 10.0.200.1 255.255.255.0
 ip helper-address 10.0.200.10
!

ip http server
ip http authentication aaa
no ip http secure-server
!
ip radius source-interface GigabitEthernet1/0/24
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 include-in-access-req
radius-server host 10.0.200.20 auth-port 1645 acct-port 1646 key cisco123
radius-server source-ports 1645-1646
radius-server vsa send authentication
!
```

Q. Do you have a sample NAC L2 802.1x configuration for an CatOS switch?

A.

```
#version 8.5(0.123)JAC
!
#dot1x
set dot1x radius-keepalive disable
!
!
#radius
set radius server 10.0.200.20 auth-port 1812 primary
set radius key cisco123
!
set vlan 10 name employees type ethernet mtu 1500 said 100010 state active
set vlan 20 name contractors type ethernet mtu 1500 said 100020 state active
set vlan 30 name utilities type ethernet mtu 1500 said 100030 state active
set vlan 40 name guests type ethernet mtu 1500 said 100040 state active
set vlan 50 name healthy type ethernet mtu 1500 said 100050 state active
set vlan 60 name checkup type ethernet mtu 1500 said 100060 state active
set vlan 70 name transition type ethernet mtu 1500 said 100070 state active
set vlan 80 name quarantine type ethernet mtu 1500 said 100080 state active
set vlan 90 name infected type ethernet mtu 1500 said 100090 state active
set vlan 100 name unknown type ethernet mtu 1500 said 100100 state active
set vlan 110 name voice type ethernet mtu 1500 said 100110 state active
set vlan 255 name nads type ethernet mtu 1500 said 100255 state active
!
!
#acl
!
#security ACLs
clear security acl all
#nac_pbacl
set security acl ip nac_pbacl permit arp
set security acl ip nac_pbacl permit arp-inspection any any
set security acl ip nac_pbacl permit dhcp-snooping
set security acl ip nac_pbacl permit udp any any eq 53
set security acl ip nac_pbacl permit ip group healthy_hosts any
set security acl ip nac_pbacl permit ip group quarantine_hosts 10.0.200.0 0.0.0.
255
set security acl ip nac_pbacl permit ip 10.0.200.0 0.0.0.255 group quarantine_ho
```

```
sts
set security acl ip nac_pbacl permit ip group quarantine_hosts host 10.40.80.1
set security acl ip nac_pbacl permit ip host 10.40.80.1 group quarantine_hosts
#
commit security acl all
set security acl map nac_pbacl 80
set security acl map nac_pbacl 50 statistics enable
!
set port dot1x 2/2 port-control auto
```

CISCO SECURE ACCESS CONTROL SERVER (ACS)

Q. What version of ACS supports NAC?

A. ACS version 3.3.1 or later supports NAC L3 IP. ACS version 4.0 and later support NAC L2 IP and NAC L2 802.1x.

Q. ACS 4.0 has new NAC configuration areas that are different from version 3.3.1. What are the differences?

A. The NAC specific configuration has been removed from External User Database area. The Posture Validation *Policy* is configured under the Posture Validation Button.

ACS 4.0 also introduces the concept of Network Access Profiles known as *Access Services*. They are used for incoming Authentication Request Recognition. The Access Services tie Posture Policies and Authorization Components together and are configured under the Network Access Profiles.

Q. Where can I download a free trial of ACS for NAC?

A. A free, 90-day trial of ACS is available for immediate download to registered users at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-eval.

Q. Can NAC policies be replicated between master and slave ACS servers?

A. Yes, in ACS v3.3.1 NAC policies are replicated. However, NAC External Databases are not. Therefore, to replicate the policies, you must manually create any NAC External Databases with the same name on the slave servers to replicate policies. This is documented in ACS 3.3 Release notes.

Q. What are the Cisco vendor specific attributes (VSAs) for controlling a NAC authorization?

A. These vendor-specific attributes (VSAs) within ACS for each user and group are configurable:

- `posture-token:` This is the posture token string that appears in the NAC session
- `status-query-timeout:` This overrides the status query timer in the router
- `url-redirect:` This is the URL for redirecting web browsers.

These are configured in the ACS User or Group Setup under Cisco IOS/PIX RADIUS Attributes in the cisco-av-pair section. An example VSA configuration might be:

```
posture-token=Quarantine
url-redirection=http://remediation.cisco.com/Quarantine/
status-query-timeout=30
```

Note that the VSA names are case sensitive and that they must be all be all lowercase as shown above.

Q. What are the default profile templates that are in ACS 4.0? How do you select one of the templates to start a configuration?

A. There are seven profile templates preconfigured in ACS 4.0.

- NAC L3 IP
- NAC L2 IP
- NAC L2 802.1x
- Microsoft IEEE 802.1x
- Wireless (NAC L2 802.1x)
- Authentication Bypass (802.1x fallback)
- Agentless Host

To select one of the templates, go to Network Access Profiles→Add Template Profile. Select the template that you would like to use as a base for the new profile.

Q. Can I set the revalidation period using a group setting in ACS?

A. Yes, use the IETF RADIUS Attribute #027 Session-Timeout in the IOS/PIX attributes area of the Group configuration.

Q. What is the difference between the status query period and the revalidation period?

A. After the initial posture validation of an endpoint, both the status query period and the revalidation period are configured and enforced by the NAD. You can see each value for a specific EAPoUDP session:

```
NACPack-1800#show eou ip 192.168.150.5
Address             : 192.168.150.5
Interface           : FastEthernet0/1
AuthType            : EAP
PostureToken        : Healthy
Age(min)            : 2
URL Redirect        :
ACL Name            : #ACSACL#-IP-Healthy-41b7a0bf
Revalidation Period : 600 Seconds
Status Query Period : 30 Seconds
```

The status query period triggers a lightweight poll from the NAD to the endpoint at a relatively short interval (less than 300 seconds). The shorter the interval, the more quickly NAC can detect posture changes and respond with the appropriate level of enforcement. A status query accomplishes several goals:

- The status query moves the polling tasks from the ACS to the NAD, reducing the ACS load for posture validation.
- The status query determines if a given endpoint is still on the network, as an IP (L3) router cannot detect at a link level (L2) when an endpoint disconnects. If the endpoint does not respond, the NAC session is deleted from the EAPoUDP table.
- The status query cryptographically confirms that the endpoint is the same one whose posture was previously authorized. This is done using the cryptographic key generated by the PEAP tunnel during the last posture validation. It is necessary because an endpoint with a DHCP-assigned address could leave the network and another host could assume the same IP address. If the keys do not match, the EAPoUDP table entry is deleted on the NAD, and the new endpoint is sent an EAPoUDP request for its posture.

- The status query triggers the CTA to ask each posture plugin if there has been a posture change in their respective agents or applications. The CTA gathers all of the plugin responses and sends the NAD a single status result. If the posture of any application has changed, the NAD performs a posture revalidation.
- The revalidation period is effectively the EAPoUDP session period. When the revalidation period expires, the endpoint posture is no longer valid to the NAD, regardless of the last status query result. The NAD sends a new EAPoUDP challenge to the endpoint, also starting a posture validation by the ACS. Be aware that a relatively low revalidation period (300 seconds or less) can result in a high load on your ACS servers.

Q. Can I create user notification messages in other languages?

A. No. NAC supports UTF-8 encoding of string data types, but the current version of ACS does not support encoding the notification messages to UTF-8.

Q. How can I determine which vendor attributes are stored in the ACS data dictionary?

A. You can list the current NAC data dictionary contents on ACS for Windows with the command:

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -dumpAVP avpdump.txt
```

On the ACS Solution Engine, the attributes can be exported on the System Configuration > CNAC Attributes Management screen by using the Dump Attributes option and downloading the file of attribute definitions.

Q. My version of ACS does not show the NAC credential types and attributes for vendor *xyz*. How do I import new NAC credential types into the ACS data dictionary?

A. You must first obtain the desired attribute description file (*.ini or *.txt) from the specific vendor. The procedure to import new NAC attributes is documented in the ACS for Windows User Guide. On ACS for Windows, the import command is:

```
C:\Program Files\CiscoSecure ACS v3.3\Utils>csutil -addAVP new_avps.ini
```

On the ACS Solution Engine the attributes can be imported from an FTP server on the System Configuration > CNAC Attributes Management screen.

Q. What is the maximum user-notification message size in ACS?

A. ACS limits the user message to 1000 single-byte characters. UTF-8 encoding for double-byte languages is not supported.

Q. What regular expressions are supported by ACS?

A.

- **^ (caret)**—The ^ operator matches the start of a string. For example ^Ci would match the string Cisco or the string Ciena.
- **$ (dollar)**—The $ operator matches the end of a string. For example, co$ would match the string Cisco or the string Tibco.

Q. Can I match a string when using the == and != operators ?

A. The operators == and != are for exact matches of all characters in the string. Verify that the string contents as populated in the ACS Passed Authentications log. Note that some strings can use the | character as a delimiter at the string beginning, the end, or both.

If you only need to check for a substring, use the contains operator instead.

Q. Why does my new profile I created in Network Access Profiles say no under active?

A. You must select active in the Network Access Profile setup page to activate the profile.

Q. How does ACS decide which profile to use when multiple profiles are configured?

A. ACS traverses the ordered list of active Network Access Profiles and maps a RADIUS transaction to a profile. ACS uses a first-match strategy on the first access-request of the transaction.

Q. Does ACS check all of the attributes I have configured?

A. ACS 4.0 only checks the attributes you have selected or checked in the network access profile posture policy configuration.

Q. ACS is rejecting one of my hosts and logging the event to the Failed Attempts log. What is wrong?

A. First look at the Reason field to determine if the failure was caused by any errors in the posture validation such as *No token returned from external server*. Another common message is *No matched mandatory credentials* which is caused by over-specifying the number of mandatory credential types.

We highly recommend that you configure a minimal, CTA-only NAC database with only Cisco:PA as the mandatory credential type. This database should be the last database in the Unknown User Policy's selected database list to prevent a premature match. Any hosts that failover into this database will still need to be quarantined because they will be missing other required credential types. At least they will be identified and quarantined rather than cause a failed attempt.

There are several other messages that can appear in the Failed Attempts log:

Authen-Failure-Code Field	Filter Information Field	Status
`External DB Account Restriction`		There was a problem with the NAC database configuration: • A posture token might not have been received from an external posture validation server (PVS). Verify that the server is properly configured and that the ACS is requesting the correct URL on the PVS. • The mandatory credential types for the configured NAC databases might be too specific. Create a minimal NAC External Database that only requires Cisco:PA as the mandatory credential type. You can at least identify hosts with only the CTA and quarantine them for necessary updates.
`User Access Filtered`	`No Access Filters Passed.`	An attempt was made to filter the endpoint with a network access restriction (NAR), but no match was found so the endpoint was not authorized. This is a rejection of a nonresponsive endpoint (NRE) which might be a guest user or an endpoint in need of a CTA. Update your NARs if the endpoint should be authorized as an NRE.

Q. How do I install partner Attribute Definition files (ADFs) on the ACS appliance?

A. The ACS Solution Engine has a UI screen for importing the NAC ADF files through FTP.

The ADF import screen is located under System Configuration > CNAC Attribute Management, according to the ACS SE v3.3 User Guide.
http://www.cisco.com/en/US/partner/products/sw/secursw/ps5338/products_user_guide_chapter09186a0080233621.html#wp617750

This is an example of the fields defined in a partner ADF.

```
[attr#0]
vendor-id=
vendor-name=
application-id=
application-name=
attribute-id=
attribute-name=
attribute-profile=
attribute-type=
```

Q. How do I configure ACS to check for multiple antivirus agents?

A. Your ACS External NAC databases and policies should be configured similar to the examples below.

Do not forget to configure the respective Database Group Mappings and Unknown User Policy for each NAC database created. The mappings and user policies are necessary for successful NAC authorization.

As an example, here is a multivendor antivirus policy in ACS for NAC:

NAC Databases (see Local Policies below for the policy definitions)

CTA-Only

Mandatory Credential Types	Credential Validation Policies
Cisco:PA	• CTA-Policy • Windows-Basic-Policy

CTA+NAI

Mandatory Credential Types	Credential Validation Policies
Cisco:PA **NAI:AV**	• CTA-Policy • Windows-Basic-Policy • NAI-Policy

CTA+Symantec

Mandatory Credential Types	Credential Validation Policies
Cisco:PA **Symantec:AV**	• CTA-Policy • Windows-Basic-Policy • Symantec-Policy

CTA+Trend

Mandatory Credential Types	Credential Validation Policies
Cisco:PA **Trend:AV**	• CTA-Policy • Windows-Basic-Policy • Trend-Policy

Local Policies (policies can be reused in multiple databases):

CTA-Policy

Rules	Credential Type	Token	Action
Cisco:PA:PA-Version >= 1.0.53	Cisco:PA	Healthy	
Default	Cisco:PA	Quarantine	

Windows-Basic-Policy

Rules	Credential Type	Token	Action
Cisco:PA:OS-Type contains Windows 2000 **Cisco:PA:OS-Version >= 5.0.2195.0**	Cisco:Host*	Healthy	
Cisco:PA:OS-Type contains Windows XP **Cisco:PA:OS-Version >= 5.1.0.0**	Cisco:Host	Healthy	
Default	Cisco:Host	Quarantine	

NAI-Policy

Rules	Credential Type	Token	Action
NAI:AV:Software-Version >= 7.1.0.0 **NAI:AV:Scan-Engine-Version >= 4.3.20** **NAI:AV:Dat-Version >= 4.0.4367.0** **NAI:AV:Protection-Enabled = 1**	NAI:AV	Healthy	
Default	NAI:AV	Quarantine	

Symantec-Policy

Rules	Credential Type	Token	Action
Symantec:AV:Software-Version >= 8.1.0.825 **Symantec:AV:Scan-Engine-Version >= 1.3.0.12** **Symantec:AV:Dat-Version >= 2005.1.20.8** **Symantec:AV:Protection-Enabled = 1**	Symantec:AV	Healthy	
Default	Symantec:AV	Quarantine	

Trend-Policy

Rules	Credential Type	Token	Action
Trend:AV:Software-Version >= 6.5.0.0 **Trend:AV:Scan-Engine-Version >= 7.1.0.1003** **Trend:AV:Dat-Version >= 1.919.0.0** **Trend:AV:Protection-Enabled = 1**	Trend:AV	Healthy	
Default	Trend:AV	Quarantine	

Q. What happens if ACS fails to receive a response from an HCAP posture validation server?

A. If the posture validation server (PVS) fails to respond, ACS responds with an Access-Reject to the router RADIUS request. ACS then logs it in the Failed Attempts log with a log message about not receiving a response from the external PVS. The router then leaves the EoU session in the INIT state for the defined hold period with default network access (whatever is permitted by the NAC-enabled interface ACL). After the hold period expires and the endpoint sends traffic through the router, the NAC authorization process begins again.

PARTNERS

Q. Does company xyz support NAC? Which companies software version support NAC? Which partners are providing reporting solutions for NAC?

A. See the NAC Partner Program site and the NAC Participant List for details about specific vendor support.
http://www.cisco.com/en/US/partners/pr46/nac/partners.html

Q. Does Cisco keep a comprehensive repository of all the NAC attributes for all partners?

A. No, you need to obtain the NAC attributes from your respective vendors.

Q. I do not see the NAC attributes for a vendor in my installation of Cisco Secure ACS. Where do I get them? How do I import them?

A. You must get the NAC attributes from your specific vendor in the form of a .ini or .txt file. These attribute files will be provided with their software. The procedure to import new NAC attributes is documented briefly in the ACS section above and more thoroughly in the ACS User Guide.

ACRONYMS AND TERMS

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

Acronym	Description
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 Addmission Control
NAD	Network Access Device
NAF	Network Access Filter

Acronym	Description
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

Acronym	Description
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	Definition
802.1x, dot1x	IEEE 802.1x. The standard for Layer 2 network authentication. It should not be confused with 802.11a/b/g, which is for wireless networking.
AAA	Authentication, Authorization, and Accounting. Typically, this refers to authorization of users for network access, including dial-up, wireless, VPN, or 802.1x. The central server that aggregates one or more authentication or authorization 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-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 is 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
APT	Application Posture Token. The result of a compliance check for a given vendor’s application, which represents the health of that component. All APTs from a posture validation are merged by the primary PVS to create the SPT.
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.

Term	Definition
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
CS-MARS	Cisco Systems Mitigation and Response System (CS-MARS) family of high performance, scalable appliances for threat management, monitoring and mitigation. Customers can 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.
CTA	Cisco Trust Agent. Cisco product instance of the PA. Includes a PA posture plugin.
CTA, Cisco Trust Agent	Cisco System's implementation of the posture agent is called the CTA and includes the embedded wired-only supplicant
CTASI	CTA Scripting Interface
DAI	Dynamic ARP Inspection
DHCP Snooping	• DHCP snooping is a security feature that provides network security by filtering untrusted DHCP messages and by building and maintaining a DHCP snooping binding database, also referred to as a DHCP snooping binding table. • DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. You use DHCP snooping to differentiate between untrusted interfaces connected to the end user and trusted interfaces connected to the DHCP server or another switch. • DHCP snooping builds a DHCP binding table containing the client IP address, MAC address, port, VLAN number, lease, and binding type. The feature can be enabled on a particular VLAN on the switch. The switch intercepts all DHCP messages bridging within the Layer 2 VLAN domain.
EAP	Extensible Authentication Protocol
EAP-FAST	• Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is a TLS-based RFC 3748- compliant EAP method. • 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.
EAP-FAST	EAP Flexible Authentication by Secure Tunneling
EAP-GTC	EAP Generic Token Card
EAPOL	EAP over LAN
EAP-TLS	EAP Transport Layer Security
Endpoint	Any machine attempting to connect or use the resources of a network
EoU, EAPoUDP	Extensible Authentication Protocol over User Datagram Protocol.
GAME	Generic Authorization Message Exchange
GINA	Graphical Identification and Authentication (Microsoft)
HCAP	Host Credential Authorization Protocol

Term	Definition
Host	Another name for an endpoint device
Host	Any machine that attempts to connect to or use the resources of a network. Also referred to as a host.
IID, Initiator Identity	For machine authentication, the IID is the FQDN of the host. (for example, jdoe-pc.cisco.com). For user authentication, the IID is a username. (for example, jdoe)
MAB	MAC Authentication Bypass (MAC-Auth-Bypass)
Machine Authentication	The machine identity used for authentication is the actual name of the computer as it exists in the Active Directory. The credentials used to authenticate the computer can be password-based or PKI certificate-based, depending on the EAP type used.
MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2
NAC	Network Admission Control. NAC 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 L2 802.1x	Cisco NAC implementation of the 802.1x protocol on CatOS and IOS switches
NAC L2 IP	Layer 2 EAP over UDP support for Cisco switches
NAC L3 IP	Layer 3 EAP over UDP support for Cisco routers
NAD	Network Access Device. A network access device acts as a policy enforcement point for the authorized network access privileges granted to an endpoint device. A NAD can be a Cisco router, switch, access point, or VPN concentrator.
NAF, Network Access Filter	A NAF is a named group of any combination of one or more of these network elements: IP addresses, AAA clients (network devices), or Network device groups (NDGs). A NAF can specify a downloadable IP ACL or Network Access Restriction based on the AAA clients through which the user can access the network. You do not need to list each AAA client explicitly.
NAH	NAC Agentless Host
NAH, NAC Agentless 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
NRH	Nonresponsive Host
PA	Posture Agent. An application that serves as the single point of contact on the endpoint for aggregating posture credentials from potentially multiple posture plugins and communicating with the network. Cisco's posture agent is the Cisco Trust Agent (CTA).
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
PAC	Protected Access Credential
PDP, Policy Decision Point	Provides facilities for policy management and conditional filters
PEAP	Protected EAP
PEAP-GTC	Protected EAP Generic Token Card
PEP, Policy Enforcement Point	ACS acts as the policy enforcement point for policy management
plugin, 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	Current host status and configuration. This can include antivirus levels, hotfixes, OS types, and so on.
posture agent	An application that serves as the single point of contact on the endpoint for aggregating posture credentials

Term	Definition
	from potentially multiple posture plugins and communicating with the network. Cisco's posture agent is the Cisco Trust Agent (CTA).
posture credentials	State information of an endpoint device at a given point in time representing hardware and software (OS and application) information.
posture credentials	State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information.
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 an endpoint device posture credentials by one or more posture validation servers and their associated compliance policies.
posture validation	The authorization of a network endpoint posture credentials by one or more posture-validation servers and their associated compliance policies.
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.
PP	Posture Plugin
PV	Posture Validation. Validates the collection of attributes that describe the general state and health of the user's machine (the host).
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.
PVS, Posture Validation Server, Policy Server, Vendor Policy 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 compliance result for an endpoint device. This is the final posture state resulting from the posture validation of an endpoint.
SPT, System Posture Token	The result of aggregating one or more application posture tokens into a single posture validation result for a host.
Token: Check-up	Host is within policy, but an update is available. Used to proactively remediate a host to the Healthy state.
Token: Healthy	Host is compliant; no restrictions on network access.
Token: Infected	Host is an active threat to other hosts; network should severely restricted or totally deny all network access.
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: Transition	Host posturing is in process; give interim access pending full posture validation. Applicable during host boot when all services might not be running or audit results are not yet available.

Term	Definition
Token: Unknown	Host posture cannot be determined. Quarantine the host and audit or remediate until a definitive posture can be determined.
User Authentication	Method in which user information is verified over 802.1x at the time of login. User Authentication can be performed through either the users active directory (domain) credentials or through credentials provided with a client-side certificate.
VSA, Vendor Specific Attribute	Most vendors use the VSA to support value-add features.

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 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

206616.H_ETMG_KL_1.06

Printed in the USA