WHITE PAPER

Guidelines for the Deployment of Cisco Secure ACS for Windows NT/2000 Servers in a Cisco Catalyst Switch Environment

Introduction

This document presents planning, design, and implementation practices for deploying Cisco Secure Access Control Server (ACS) for Windows NT/2000 servers in support of Cisco Catalyst® Switch networks. It discusses network topology regarding authentication, authorization, and accounting (AAA), user database choices, password protocol choices, access requirements, and capabilities of Cisco Secure ACS.

Factors Influencing Cisco Secure ACS Deployment

Factors that influence how Cisco Secure ACS can be deployed within the enterprise network in support of Cisco Catalyst switches include:

- Network topology
- Security policy
- Network access policy
- Administrative access policy
- User databases

This document will discuss each of these factors.

AAA in a Cisco Catalyst Switch (802.1x/EAPoL) Environment

This paper focuses on the issues specific to deploying Cisco Secure ACS in support of Cisco Catalyst switches. Readers should have a good understanding of AAA concepts and usage. If you are unfamiliar with AAA, you can refer to the following documentation for an introduction to the concepts in this guide:

- *Guidelines for Placing ACS in the Network*
- *Guidelines for Deploying EAP with Cisco Secure ACS for Windows NT/2000 Servers*

Both guides are available at www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml.

Historically, Ethernet-based networks, whether simple broadcast or switched, offered few capabilities for the authentication of devices, or users, to the network. When originally developed, the protocols underpinning Transmission Control Protocol/ Internet Protocol (TCP/IP) over Ethernet—Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP), for example—simply did not address user authentication, authorization, or accounting. The key challenge at the time was connectivity. Advanced security concerns were issues for the future. It is still true today that in the vast majority of organizations any person who can physically attach a computer to the LAN will automatically be granted TCP/IP connectivity to the network without further checks concerning whether such connectivity is appropriate. With the security focus of most organizations having been on the external risks posed by connection to the Internet, relatively uncontrolled IP access has been available on the LAN. With the wider deployment of networks and the accompanying vulnerabilities, most organizations are becoming concerned about this reliance on crude physical security to limit access to their "sensitive" networks, which now includes all them.

The addition of Remote Authentication Dial-In User Service (RADIUS) support to Cisco Catalyst switches means that the user-based access control schemes— long available to control user access to the "point-to-point" links on remote-access routers—are now available on the "broadcast" links of Cisco Catalyst switches. This represents a fundamental breakthrough in the access control schemes that can now be achieved on broadcast or switch-based Ethernet networks. An obvious example of configuration data that an organization might want delivered by RADIUS is the virtual LAN identification for each user.

Extensible Authentication Protocol (EAP), as defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards, represents the technology framework that makes it possible to deploy RADIUS into Ethernet network environments. It also facilitates the adoption of AAA schemes with the security advantages that using such AAA servers confer. The 802.1x standard, also known as EAP over LAN (EAPoL), concerns that part of the wider EAP standard that relates to broadcast media networks. Upon connection, EAPoL provides a "communications channel" between an end user on a client LAN device to the AAA server through the LAN switch. Conceptually, the functionality is very similar to that provided by Point-to-Point Protocol (PPP) servers on point-to-point links. With the addition of AAA support for user access control, all Ethernet LAN connections can be authenticated against the individual user requesting it; only if valid credentials are supplied will network connectivity be provided. In addition, the RADIUS protocol provides for delivery of fine-grained control of the network connectivity to be supplied by switch to the user. Finally, RADIUS provides for the collection of a user's usage statistics of network resources.

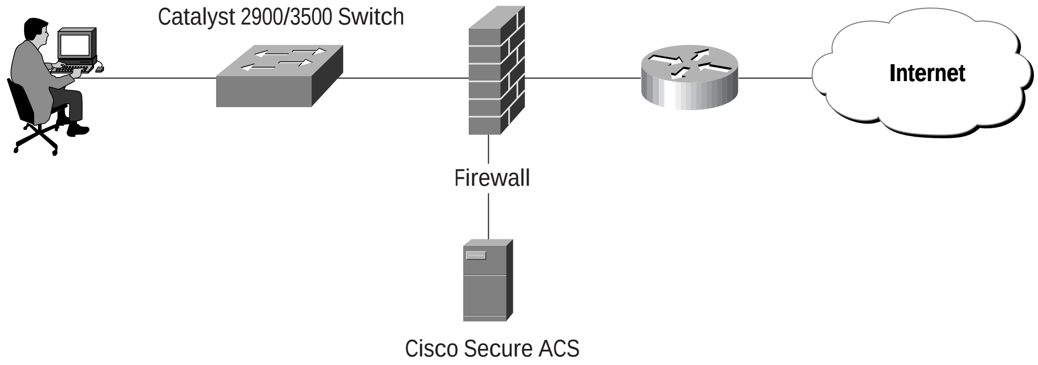
By supporting complex challenge-response dialogues, EAP facilitates the user-based authentication demands of both conventional one-way hashed password authentication schemes such as Challenge Handshake Authentication Protocol (CHAP) and also of more advanced authentication schemes such as Transport Layer Security (TLS), or digital certificates. Moreover, being extensible, additional password protocol schemes such as Microsoft CHAP (MS-CHAP) or Kerberos will almost certainly become supported over time as demand for them grows. The flexible capabilities provided by EAP thus allow deploying organizations to start with less secure but simpler-to-implement authentication protocols and advance to more competent but demanding protocols as requirements dictate. For a more complete explanation of EAP and a discussion of the capabilities and security attributes of the different password protocol schemes supported, see *Guidelines for Deploying EAP with Cisco Secure ACS for Windows NT/2000 Servers.*

Network Topology

How an enterprise network is configured is probably the most important factor in deciding how and where to deploy Cisco Secure ACS. With the complexity and wide geographic dispersion of today's enterprise networks, the decision of how to deploy Cisco Secure ACS may vary widely depending on the network topology into which it is to be deployed.

In the small LAN environment (Figure 1), a single Cisco Secure ACS would usually be located close to the switch. In this environment, the user database is usually small because few switches would require access to the Cisco Secure ACS for AAA so the workload will be modest and only require a single Cisco Secure ACS. Even so, it would be wise to deploy a second server for redundancy, and it should be set up as a replication partner to the primary server because losing the Cisco Secure ACS would prevent users from gaining access to the network. In Figure 1, an Internet connection via firewall and router are included because these are likely to be features of such a network; but they are not strictly related to the Cisco Catalyst AAA setup or required as part of it. It is also worth noting that it is prudent security policy to limit access to the system hosting the Cisco Secure ACS to as small a number of users and devices as necessary. In the illustration, this is achieved by connecting the Cisco Secure ACS host through to a private LAN segment on the firewall; access to this segment would be limited only to the Cisco Catalyst Switch client and those user machines that require Hypertext Transfer Protocol (HTTP) access to the Cisco Secure ACS for administrative purposes. Normal LAN users should not be able to "see" the Cisco Secure ACS at all.

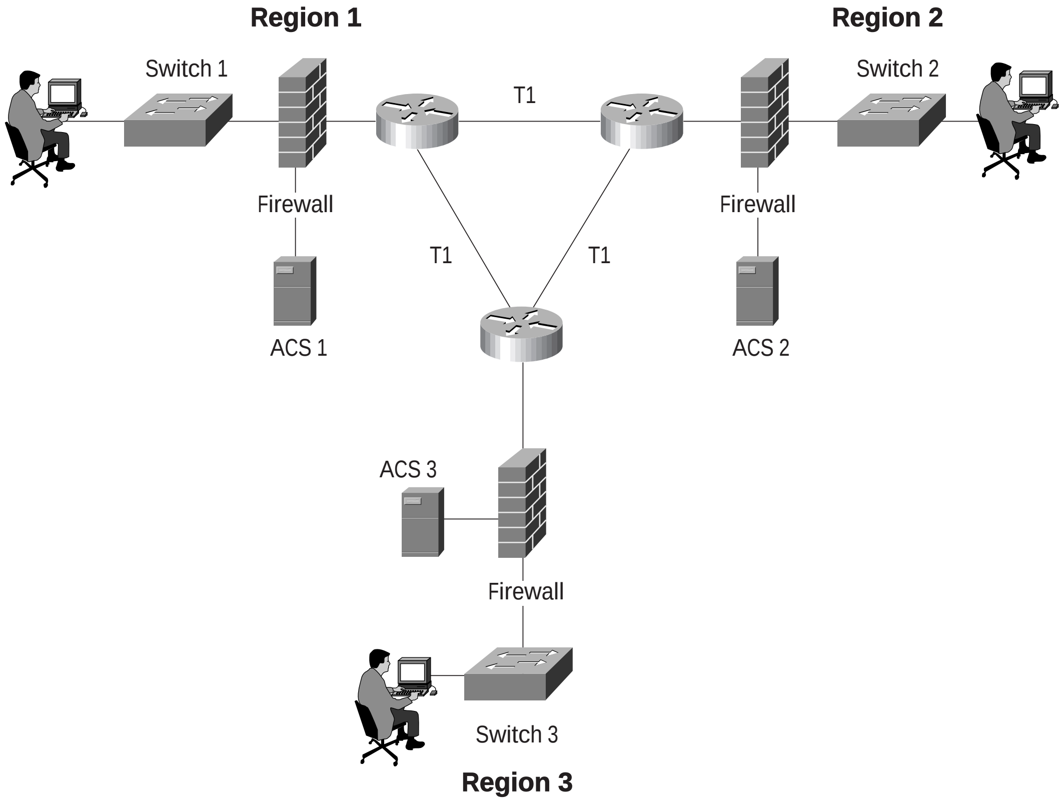
Figure 1 Cisco Secure ACS Deployment in a Small LAN Environment



In a larger network that is geographically dispersed, speed, redundancy, and reliability will be important in determining whether to use a centralized Cisco Secure ACS service or a number of geographically dispersed Cisco Secure ACS units. As with many applications, AAA clients rely upon timely and deterministic responses to their queries. Network speed can be important in deciding how Cisco Secure ACS should be deployed because delays in authentication introduced by the network can result in timeouts at the client side or the switch.

A useful approach in large extended networks, such as for a globally dispersed corporation, is to have at least one Cisco Secure ACS deployed in each major geographical region. Depending upon the quality of the WAN links, these may act as backup partners to servers in other regions to protect against failure of the Cisco Secure ACS in any particular region (Figure 2). In this illustration, Switch 1 is configured with Cisco Secure ACS 1 as its primary AAA server but with Cisco Secure ACS 2 of Region 2 as its secondary. Switch 2 is configured with Cisco Secure ACS 2 as its primary but with Cisco Secure ACS 3 as its secondary. Likewise, Switch 3 uses Cisco Secure ACS 3 as its primary but Cisco Secure ACS 1 as its secondary. In this way, AAA WAN traffic is minimized by using a local Cisco Secure ACS as the primary AAA server, and the number of Cisco Secure ACS units required is also minimized by using the primary Cisco Secure ACS from another region as the secondary when necessary.

Figure 2 Cisco Secure ACS Deployment in a Globally Dispersed Network



The Figure 2 model may be extended further down to campus or even individual site level if reliable high-speed connections between locations are not incorporated or if the performance requirements of the individual sites are such that remotely sited servers may not provide adequate performance. The issues are similar to those relating to providing adequate performance for Web users by means of caching: The greater the performance required, the closer to the user the cache needs to be located, particularly if the intermediate links are slow. It is worth noting, however, that RADIUS— being based on User Datagram Protocol (UDP) and consisting of small challenge and response packets—imposes relatively low bandwidth demands and will not stress a WAN link that has a small amount of usable capacity, even in busy environments. Conversely, attention may need to be paid where virtual private network (VPN) connections between sites using the Internet are employed to provide the link. Although VPN connections save time and money, they do not always provide the deterministic response times and reliability that a dedicated frame relay or T1 link would. If reliable authentication performance is critical to maintaining business functionality—most certainly the case where corporate users are accessing the LAN—the loss of the WAN connection between the switch and the remote Cisco Secure ACS could be catastrophic.

The same issue can be applied to an external database used by the Cisco Secure ACS. The database should be deployed near enough to the Cisco Secure ACS installation to ensure reliable and timely access. See *Guidelines for Placing ACS in the Network* for more in-depth treatment of this issue.

Security Policy

Cisco recommends that every organization that maintains a network develop a security policy, which defines the following minimum policies:

- Preparation
  - Create usage policy statements
  - Conduct a risk analysis
  - Establish a security team structure
- Prevention
  - Approving security changes
  - Monitoring security of your network
- Response
  - Security violations
  - Restoration
  - Review

Several good documents on security policy are located at:

- www.cisco.com/warp/customer/126/secpol.html
- www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/deesp_wp.htm
- www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scdoverv.htm

The introduction of EAP-over-RADIUS support into Cisco Catalyst switches creates an opportunity to enhance an organization's overall security policies. Widely accepted security doctrine maintains that best results will be achieved when any changes in security measures flow down from an overhaul of security policy being translated into specific measures and implementation plans to achieve the new goals. There appears to be no reason to suppose that implementation of AAA-mediated LAN access is an exception to this doctrine.

Network Access Policy

Network access policy is a broad concept. In general, it defines how users can connect to the network and what services they will be provided with when connected to it.

Cisco Secure ACS-based access policy enforcement provides control by using central authentication and authorization of network users. The Cisco Secure ACS database maintains all user IDs, passwords, and privileges (which are held in the form of a RADIUS “access profile”). Upon receipt of a RADIUS access-request packet from the switch on behalf of a particular user, the Cisco Secure ACS first determines which authentication method will be used for that request and then processes it. As noted above, with EAP, the authentication may actually be quite a complex process requiring multiple iterations through a challenge-response dialogue.

The following subsections describe what is required to configure Cisco Secure ACS as the AAA server for a Cisco Catalyst Switch and how to configure the switch to use it.

EAP Type Configuration

The important policy decision regarding authentication in a Cisco Catalyst Switch environment is which EAP authentication type to deploy. The two choices are EAP-Message Digest 5 (MD5) and EAP-TLS. This choice is likely to be influenced by which database is in use as well as by security implications. It is also worth noting that unlike with non-EAP RADIUS devices, where EAP is employed to carry the password protocol traffic over RADIUS, the AAA client device cannot function as policy enforcement point. Enforcement has to be provided by the Cisco Secure ACS because the AAA client device functions as a router of EAP traffic between the end user client and the Cisco Secure ACS; the dialogue is essentially opaque to it. For a description of how to configure which EAP type to be enforced by the Cisco Secure ACS, see Guidelines for *Deploying EAP with Cisco Secure ACS for Windows NT/2000 Servers.*

Cisco Secure ACS RADIUS Profile Configuration

After a user successfully completes the EAP authentication process of whatever type, the Cisco Secure ACS responds to the switch with a RADIUS authentication-accept packet granting that user access to the network. This packet is a fairly standard RADIUS authentication-accept packet and can carry a variety of the usual RADIUS attributes that may be communicated and that will be understood by the Cisco Catalyst Switch. Taken as a whole, the attributes that compose the access-accept packet constitute an “access profile.” Once received by the switch, the attributes are then processed in compliance with the RADIUS RFC and whatever logic is implemented above the level of the protocol. The access profile generally contains user-specific authorization information, such as access control lists (ACLs) to be applied or the VLAN ID to be assigned. For a more complete description of the RADIUS profile and what each attribute means, see the *Cisco Secure ACS 3.0 for Windows 2000/NT Servers User Guide*. For a more complete description of which RADIUS attributes may be configured for consumption by a particular Cisco Catalyst Switch, consult the documentation for that device.

Configuration of the RADIUS profile is performed on the Cisco Secure ACS under the Group Setup section or the User Setup section. For attributes to show up in the Group and User sections, they first have to be configured as required in the Interface Configuration section. The attributes required are as follows:

- [064] Tunnel-Type
- [081] Tunnel-Private-Group-ID

These attributes can be found under the IETF RADIUS Settings section of Interface Control. Checking these boxes causes the appropriate fields to appear on the Group and User pages.

For reasons of administrative scalability, RADIUS profiles are usually configured at the group level rather than one for each user. To configure a VLAN ID to be assigned to all users belonging to a specific group accessing the network through a Cisco Catalyst 4000, 5000, or 6000 Switch, navigate to that group’s page within Cisco Secure ACS and locate the IETF RADIUS settings section. If the steps above on Interface Configuration have been followed, then attributes Tunnel-Type [# 64] and Tunnel-Private-Group-ID [# 81] will appear there for configuration.

To configure these, check the checkbox on the left of both attributes. For the “Tunnel-Type” attribute ensure the first “Tag” list is set to “1” and the corresponding value is set to “VLAN.” Make sure that the second “Tag” list is set to “0.” For the “Tunnel-Private-Group-ID” again make sure the first “Tag” list value is set to “1” and then set the corresponding value field to the appropriate number for the VLAN to be assigned. Again, make sure that the second “Tag” list is set to “0.” In normal usage, RADIUS supports multiple tunnel attribute support tags. When assigning VLAN IDs to a Cisco Catalyst Switch, it will ignore anything with a Tag other than “1.” In other words, only a single VLAN ID may be supplied in each RADIUS response packet to a Cisco Catalyst Switch.

Note: *Cisco Catalyst Switch Support for VLAN Assignment by RADIUS*

Because RADIUS VLAN ID assignment is not supported by Cisco Catalyst 2950 and 3550 switches, assignment of it by the Cisco Secure ACS using RADIUS should not be attempted. Support for VLAN ID to Cisco Catalyst 6000 switches by RADIUS requires Cisco Catalyst Operating System Version 7.2; so provision of the RADIUS VLAN ID attributes to switches running Cisco Catalyst OSv7.1 or earlier should likewise not be attempted.

Cisco Catalyst Switch Configuration

To use RADIUS for per-user port security on a Cisco Catalyst 2950 or 3550 Switch, it needs to be configured as illustrated in Example 1.

Example 1—Sample Cisco IOS Configuration for Ethernet AAA Configuration on a Cisco Catalyst 2950 or 3550 Switch

```
switch#conf t
switch(config)#aaa new-model
switch(config)#radius-server host 10.5.1.197
switch(config)#radius-server key lab
switch(config)#aaa authentication dot1x default group radius
```

To achieve the same thing on a Cisco Catalyst 4000, 5000, or 6000 Switch, it needs to be configured as illustrated in Example 2.

Example 2—Sample Cisco Catalyst OS Configuration for Ethernet AAA Configuration on a Cisco Catalyst 4000, 5000, or 6000 Switch

```
#radius
set radius server 192.168.122.236 auth-port 1812 primary
set radius deadtime 5
set radius timeout 10
set radius retransmit 4
set radius key ABCD123

#dot1x
set dot1x system-auth-control enable
set dot1x re-authperiod 1800
set dot1x re-authentication enable

#accounting
set accounting exec enable start-stop radius
set accounting connect enable start-stop radius
set accounting update new-info
set accounting update periodic 30

#module 2 : 48-port 10/100BaseTX Ethernet
set port dot1x 2/2 port-control auto
set trunk 2/2  off negotiate 1-1005,1025-4094
set spantree portfast 2/2 enable
```

Because of the possibility of changes between releases in the operation of Cisco IOS® Software and Cisco Catalyst OS command-line implementation with regard to AAA, it is always advisable to check the latest configuration guides for the particular switches being configured.

Included at the end of this document is sample debug output produced by a Cisco Catalyst 4000, 5000, or 6000 Series Switch and Cisco Secure ACS for successful authentication attempts for both an EAP-MD5 and an EAP-TLS authentication. These have been annotated for comprehensibility to highlight important items to look for.

Administrative Access Policy

Cisco Catalyst switches represent a widely deployed class of network devices that require management in common with other Cisco Systems network devices. Cisco therefore provides a number of commonly supported mechanisms for managing these devices, including support for the Terminal Access Controller Access Control System (TACACS+) AAA protocol for device administration. For a fuller description of the capabilities and benefits of centralized device configuration control using TACACS+, see *Guidelines for Placing ACS in the Network*.

Separating Administrative and General Users

It is vital to keep the general network user from gaining administrative access to network devices. Even though a general user may not intend to harm the system, inadvertent access may result in significant disruption to the network. Separation of the general user from the administrative user falls into the realm of AAA and Cisco Secure ACS.

The easiest, and recommended, method to perform such separation is to use RADIUS for the general remote-access user and TACACS+ for the administrative user. An administrator, however, may also require remote network access, like the general user. This poses no problem with Cisco Secure ACS. The administrator can have both RADIUS and TACACS+ configurations in Cisco Secure ACS. Using authorization, RADIUS users can have EAPoL (or other network access protocol) as the permitted protocol. Under TACACS+ only the administrator would be configured for shell (exec) access.

For example, if the administrator is connecting to the network as a general user, the switch would use RADIUS as the authenticating and authorizing protocol, and IP-over-Ethernet access “through” the switch would be enabled. Alternatively, if the same administrator connects to the network device to make configuration changes using Telnet, the device would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on Cisco Secure ACS with permission for shell under TACACS+ he would be authorized to log onto that device. This does require that the switch have two separate configurations on Cisco Secure ACS—one for RADIUS and one for TACACS+. An example of a Cisco Catalyst 2950 or 3550 Switch configuration under Cisco IOS Software is shown in Example 3.

Example 3—Sample Cisco IOS Configuration for Separating Ethernet and Shell Logins

```
switch#conf t
switch(config)#aaa new-model
switch(config)#tacacs-server host 10.5.1.198
switch(config)#tacacs-server key lab2
switch(config)#radius-server host 10.5.1.197
switch(config)#radius-server key lab
switch(config)#aaa authentication dot1x default group radius
switch(config)#aaa authentication login default group tacacs+ local
switch(config)#aaa authentication login no_auth none
switch(config)#aaa authentication enable default group tacacs+ none
switch(config)#username admin password adminpass
switch(config)#line console 0
switch(config-line)#login authentication no_auth
```

Conversely, if a general user tried to use a remote-access login into a network device, Cisco Secure ACS would check and approve the username and password, but the authorization process would fail because that user would not have credentials that allow shell/exec access to the device.

User Databases

Aside from the topological considerations, the database is one of the most influential factors involved in making deployment decisions for the Cisco Secure ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of database employed all contribute to how Cisco Secure ACS is used. For a more detailed discussion on user database size implications, see Guidelines for Placing ACS in the Network.

Type of Database

For maximum flexibility, Cisco Secure ACS supports more than 14 database options. For each database type, one or more password protocols are supported, depending upon their respective implementations. Because the EAP RFC only has a mandatory requirement for support for two password protocols—MD5 (CHAP) and TLS—only those databases that are capable of supporting these password protocols may be used with Cisco Catalyst switches. Table 1 shows the options and available features when running Cisco Secure ACS specifically in a Cisco Catalyst Switch environment.

Table 1 Cisco Secure ACS Database Options in Support of Cisco Catalyst Switches

	Features				
Database	PAP	MS-CHAP	EAP-CHAP	EAP-TLS	Group mapping
CSDB			X	X	X
Windows NT/2000 AD				X	X
Novell NDS				X[1]	X[1]
Generic LDAP				X	X
ODBC					
Token server (OTP)					

[1] Only if accessed using generic Lightweight Directory Access Protocol (LDAP)

Cisco Secure ACS Local Database

Cisco Secure ACS provides full feature support for users connected via a Cisco Catalyst Switch when using its internal database. In addition, using the local database provides the maximum speed for authentication. The major drawback of using the local database is that if an organization already has an existing database for users, the databases are discrete and will need to be separately maintained.

Windows NT/2000 AD

To help make use of the investment that many organizations already have in Windows NT/2000, Cisco Secure ACS provides tight integration to those data stores and can take advantage of the work already invested in building the database, without requiring additional input. This eliminates the need for separate databases. (For a fuller discussion of this subject see the Database section of Guidelines for Placing ACS in the Network.) One limitation when using the Windows 2000 database in a Cisco Catalyst Switch environment is that Cisco Secure ACS is unable to support EAP-MD5 (CHAP) authentication against it at this time. (Windows NT/2000 AD does not provide support for MD5-Digest authentication as required for Lightweight Directory Access Protocol (LDAP) Version 3 compliance as defined in IETF RFC 2829.) Fortunately, full support for EAP-TLS is possible, facilitating the more common digital certificate/smart card deployments that most organizations are likely to prefer because of the technical limitations imposed by the CHAP standard.

Generic LDAP

Cisco Secure ACS supports the authentication of users connected to a Cisco Catalyst Switch against records kept in a directory server using LDAP. Because of similarities in the technology employed to integrate Cisco Secure ACS with both LDAP and a Windows 2000 server, the capabilities for both are similar to those available against a Windows 2000 Active Directory server, that is, EAP-TLS. Group mappings are also available, as with Windows NT/2000.

ODBC

Cisco Secure ACS supports authentication against an ODBC-compliant relational database. This enables the use of existing user records stored in a relational database management system (RDBMS). Because the ODBC feature allows password extraction, ODBC can authenticate using EAP-CHAP and EAP-TLS.

White papers for using Cisco Secure ACS with ODBC and LDAP can be accessed at: www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/index.shtml

Novell NDS

Cisco Secure ACS normally integrates with Novell NDS by means of Novell's proprietary network client. If this method is used, no EAP is possible because the technology that NDS employs does not facilitate EAP-MD5 or EAP-TLS authentication. NDS can, however, be configured to provide access via LDAP. If so configured, NDS can be treated as any other generic LDAP server, as described previously, and will support EAP-TLS authentication.

Token card servers (OTP)

No support for one-time password (OTP) authentication is provided over EAP against Cisco Secure ACS in a Cisco Catalyst Switch environment, but it will be added later.

Review

When AAA was conceived, the primary purpose was to provide a centralized point of control for user access via dial-in services to the perimeter of the network while also ensuring that its security was not compromised. The benefits of secured and centrally managed access has resulted in AAA services gradually moving inward from the perimeter. Now, with the development of EAPoL, the benefits have finally reached the very core. When organizations become aware of the security improvements to be attained, we expect that the growth of AAA deployment on corporate LANs will mirror the growth that firewall deployment on corporate Internet connections enjoyed as widespread "'always-on" Internet connectivity became prevalent.

Further discussions of other specific deployment issues will be addressed in documents with AAA information that will be added to the Cisco.com site at www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml

Debug Output for Successful EAP Authentications

The diagnostic logs shown below were collected using:

- A Windows XP client (build 2600)
- A Cisco Catalyst 6500 Switch running Catalyst Operating System Version 7.1(0.39) (Tampa)
- Cisco Secure ACS Version 3.0

To generate debug output from the Cisco Catalyst Switch, use the following commands:

```
set logging console enable
set logging server enable
set logging level radius 7
set logging level security 7
```

To capture debug output on the Cisco Secure ACS, diagnostic logging must be set to maximum (in the System Configuration section, on the Service Control page, under Level of detail, select Full). Output is created in the csradius.log file. For more Cisco Secure ACS debug information, please refer to www.cisco.com/warp/customer/480/9.html

Windows XP Client Operating in EAP-TLS (Certificate) Mode

Cisco Catalyst 6500 (CATOS) of Port Number 2/2 Debug Output EAP-TLS

```
2001 Nov 27 00:52:13 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
2001 Nov 27 00:53:05 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/
  2 is AUTHENTICATING
2001 Nov 27 00:53:05 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:06 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:08 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:08 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:09 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:09 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:09 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:10 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:10 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:11 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:11 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:12 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 00:53:12 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 00:53:13 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is SUCCESS
2001 Nov 27 00:53:13 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is FINISHED
2001 Nov 27 00:53:13 %SECURITY-5-DOT1X_AUTHENTICATION_SUCCESS:Authentication successful for port 2/2
2001 Nov 27 00:53:14 %SECURITY-5-DOT1X_PORT_AUTHORIZED:DOT1X: port 2/2 authorized
2001 Nov 27 00:53:14 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/
  2 is AUTHENTICATED
```

Full Cisco Secure ACS 3.0 RADIUS Debug Recording for EAP-TLS Negotiation with Cisco Catalyst Switch

Note: These are the user and the domain names eaptls3@d3w2k.acslab, located on the Windows 2000 AD External Database

```
Request from host 10.51.117.25:1812 code=1, id=245, length=99 on port 2341
    [001] User-Name                    value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address               value:  10.51.117.25
    [012] Framed-MTU                   value:  1000
    [079] EAP-Message                  value:  .....eaptls3@d3w2k.acslab
    [080] Message-Authenticator        value:  6A 0A E3 64 4C D3 19 F2 AB 66 BB 0E 78 B5 CD 1A
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                  value:  .....
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.1
ExtensionPoint: End of Attribute Set
Sending response code 11, id 245 to 10.51.117.25 on port 2341
    [079] EAP-Message                  value:  .....
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.1
Request from host 10.51.117.25:1812 code=1, id=246, length=186 on port 2341
    [001] User-Name                    value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address               value:  10.51.117.25
    [012] Framed-MTU                   value:  1000
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.1
    [079] EAP-Message
  value:  ...P.....F....A...=..<.]í;.O_.__?1$__.ç*&1S...a.5_G.............d.b.........c..
    [080] Message-Authenticator        value:  A4 0C 14 19 54 C9 C3 81 67 10 C6 45 75 94 C0 74
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                  value:  .=...........J...F......<
.]ƒ?(...öúhº_A_.Z_.._...'H- [_.A{ë..7.&.;m+_.«_.F..._;.6<_.........â......|..*0..&0.._á......#y._.....(0.
  ..*åHå.......0m1.0...*åHå.......tt@cisco.com1.0...U....
US1.0...U....Herzeliya1.0...U....Cisco1.0...U....EMBU1.0...U....EAP
    [079] EAP-Message
  value:  CA0...010905123145Z..030830142409Z0B1.0...*åHå.......fafa@fafa.com1.0...U....Cisco1.0...U....AC
  SBUID170üƒ0...*åHå........üì.0üë.üü._4(..äNyúSëVƒ`_S.#_ísæ#_@.#oDU_X. '_:._û%e.._._/
  Å_*.ö_.ê_müw".*;_Y_ëàe_._._1_.2Så.U,ƒ.._+.)__r_.~f_¬Uóï..üa_..__...\...
    [079] EAP-Message
  value:  .._..O.....ú..70..30...U......>*...uH.kS.º6Gi.4P0ü...U.#.ü_0ü¢.._ºFr. _";*...0_S__N@íqño0m1.0...
  *åHå.......tt@cisco.com1.0...U....1.0...U....Herzeliya1.0...U....Cisco1.0...U....EMBU1.0...U....EAPCA..
   .n_SF9óJÉR_h_}¿0.....U...ü.0ü.0ü.áü_áü.åü»ldap://
    [079] EAP-Message                  value:  /CN=EAPCA,CN=cd-lab210,CN=
CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=d3w2k,DC=acslab?certificateRevocationList?
  base?objectclass=cRLDistributionPoint08á6á4å2http://cd-lab210.d3w2k.acslab/CertEnroll/
  EAPCA.crl0.....+...........0ü.0üÑ..+
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.2
ExtensionPoint: End of Attribute Set
Sending response code 11, id 246 to 10.51.117.25 on port 2341
    [079] EAP-Message                  value:  .=...........J...F......<.]ƒ?(...öúhº_A_.Z_.._...'H
_.A{ë..7.&.;m+_.«_.F..._;.6<_.........â......|..*0..&0.._á......#y._.....(0...*åHå.......0m1.0...*åHå....
  ...tt@cisco.com1.0...U....US1.0...U....Herzeliya1.0...U....Cisco1.0...U....EMBU1.0...U....EAP
    [079] EAP-Message
  value: CA0...010905123145Z..030830142409Z0B1.0...*åHå.......fafa@fafa.com1.0...U....Cisco1.0...U....ACS
  BUID170üƒ0
...*åHå........üì.0üë.üü._4(..äNyúSëVƒ`_S.#_ísæ#_@.#oDU_X. '_:._û%e.._._/
  Å_*.ö_.ê:_müw".*;_Y_ëàe_._._1_.2Så.U,ƒ.._+.)__r_.~f_¬Uóï..üa_..__...\...
    [079] EAP-Message
  value:  .._..O.....ú..70..30...U......>*...u H.kS.º6Gi.4P0ü...U.#.ü_0ü¢.._ºFr. _";*...0_S__N@íqño0m1.0..
  .*åHå.......tt@cisco.com1.0...U....US1.0...U....Herzeliya1.0...U....Cisco1.0...U....EMBU1.0...U....EAPC
  A.. .n_SF9óJÉR_h_}¿0.....U...ü.0ü.0ü.áü_áü.åü»ldap://
    [079] EAP-Message                  value:  /CN=EAPCA,CN=cd-lab210,CN=
CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=d3w2k,DC=acslab?certificateRevocationList?
  base?objectclass=cRLDistributionPoint08á6á4å2http://cd-lab210.d3w2k.acslab/CertEnroll/
  EAPCA.crl0.....+...........0ü.0üÑ..+
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.2
Request from host 10.51.117.25:1812 code=1, id=247, length=112 on port 2341
    [001] User-Name                    value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address               value:  10.51.117.25
    [012] Framed-MTU                   value:  1000
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.2
    [079] EAP-Message                  value:  .=....
    [080] Message-Authenticator        value:  2C 58 B0 70 30 0F 5B 20 99 42 7C 79 92 7C 0E 46
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                  value:  .>...@.....0.åü.ldap:///CN
=EAPCA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=d3w2k,DC=acslab?cACertificate?ba
  se?objectclass=certificationAuthority0U..+.....0.åIhttp://cd-lab210.d3w2k.acslab/CertEnroll/
  cd-lab210.d3w2k.acslab_EAPCA.c
    [079] EAP-Message                  value:  rt0...U.......0.0...U.....
..á0...U.%..0...+.......0!..+.....7.......W.e.b.S.e.r.v.e.r0...*åHå........A._...____.`Pn_...v_Q.._6_.Tº.
  Å_ä.>._...__.ÄX..k.ê_^û___?«ap_C.£_...L0..H0...á.......n_SF9óJÉR_h_}¿0...*åHå.......0m1.0...*åHå.......
  tt@cisco.com1.0...
    [079] EAP-Message                  value:  U....US1.0...U....Herzeliy
a1.0...U....Cisco1.0...U....EMBU1.0...U....EAPCA0...010830142409Z..030830142409Z0m1.0...*åHå.......tt@cis
  co.com1.0...U....US1.0...U....Herzeliya1.0...U....Cisco 1.0...U....EMBU1.0...U....EAPCA0\0...*åHå......
  ..K.0H.A...J__ò|.á.Ä
    [079] EAP-Message                  value:  t_R.4?CI?.U«w.._%».+_ƒ61ïä
L.V..á?T.sZ__.:E._ì/
  _.:_ç.U.....ú..l0..h0...+.....7.......C.A0...U.......F0...U.......0....0...U......_ºFr. _";*...0_S__N@0.
  ....U...ü.0ü.0ü.áü_áü.åü»ldap:///CN=EAPCA,CN=cd-lab210,CN=CDP,CN=Public%20Key%20Services,CN=Service
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.3
ExtensionPoint: End of Attribute Set
Sending response code 11, id 247 to 10.51.117.25 on port 2341
    [079] EAP-Message                  value:  .>...@.....0.åü.ldap:///
  CN =EAPCA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=d3w2k,DC=acslab?cACertifica
  te?base?objectclass=certificationAuthority0U..+.....0.åIhttp://cd-lab210.d3w2k.acslab/CertEnroll/
  cd-lab210.d3w2k.acslab_EAPCA.c
    [079] EAP-Message                  value:  rt0...U.......0.0...U.....
..á0...U.%..0...+.......0!..+.....7.......W.e.b.S.e.r.v.e.r0...*åHå........A._...____.`Pn_...v_Q.._6_.Tº.
  Å_ä.>._...__.ÄX..k.ê_^û___?«ap_C.£_...L0..H0...á.......n_SF9óJÉR_h_}¿0...*åHå.......0m1.0...*åHå.......
  tt@cisco.com1.0...
    [079] EAP-Message
  value:  U....US1.0...U....Herzeliy a1.0...U....Cisco1.0...U....EMBU1.0...U....EAPCA0...010830142409Z..0
  30830142409Z0m1.0...*åHå.......tt@cisco.com1.0...U....US1.0...U....Herzeliya1.0...U....Cisco 1.0...U...
  .EMBU1.0...U....EAPCA0\0...*åHå........K.0H.A...J__ò|.á.Ä
    [079] EAP-Message                  value:  t_R.4?CI?.U«w.._%».+_ƒ61ïä
L.V..á?T.sZ__.:E._ì/
  _.:_ç.U.....ú..l0..h0...+.....7.......C.A0...U.......F0...U.......0....0...U......_ºFr. _";*...0_S__N@0.
  ....U...ü.0ü.0ü.áü_áü.åü»ldap:///CN=EAPCA,CN=cd-lab210,CN=CDP,CN=Public%20Key%20Services,CN=Service
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.3
Request from host 10.51.117.25:1812 code=1, id=248, length=112 on port 2341
    [001] User-Name                    value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address               value:  10.51.117.25
    [012] Framed-MTU                   value:  1000
    [024] State                        value:  CISCO-EAP-CHALLENGE=0.202.77.3
    [079] EAP-Message                         value:  .>....
    [080] Message-Authenticator               value:  49 19 E6 53 9C 73 8C 31 22 18 41 88 9C 33 7E E3
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                         value:  .?. ..s,CN=Configuration,D
C=d3w2k,DC=acslab?certificateRevocationList?base?objectclass=cRLDistributionPoin
t08á6á4å2http://cd-lab210.d3w2k.acslab/CertEnroll/EAPCA.crl0...+.....7.......0..
.*åHå........A...í_p_B.#_._._c.Q...É_¢B .Cm-e.5mw,...W_r.__p.f..."_
    [079] EAP-Message                value:  «__$ó..!_.ä_......................
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.4
ExtensionPoint: End of Attribute Set
Sending response code 11, id 248 to 10.51.117.25 on port 2341
    [079] EAP-Message                value:  .?. ..s,CN=Configuration,D
C=d3w2k,DC=acslab?certificateRevocationList?base?objectclass=cRLDistributionPoint08á6á4å2http://
  cdab210.d3w2k.acslab/CertEnroll/
  EAPCA.crl0...+.....7.......0...*åHå........A...í_p_B.#_._._c.Q...É_¢B .Cm-e.5mw,...W_r.__p.f..."_
    [079] EAP-Message                value:  «__$ó..!_.ä_......................
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.4
Request from host 10.51.117.25:1812 code=1, id=249, length=1610 on port 2341
    [001] User-Name                  value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address             value:  10.51.117.25
    [012] Framed-MTU                 value:  1000
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.4
    [079] EAP-Message                value:  .?._........._.........0
...0..ïá......aR_K......0...*åHå.......0m1.0...*åHå.......tt@cisco.com1.0...U....US1.0...U....Herzeliya1.
  0...U....Cisco1.0...U....EMBU1.0...U....EAPCA0...011029151607Z..021029151607Z0.1.0...U....eaptls30\0...
  *åHå........K.0H.A.
    [079] EAP-Message                value:  _..8`Ño.{5è.ê_)3v._...æW.v
Eá_.åï_q@..w_.@...@O..Ñi.S..ó_Ñ.M ..>í.....ú..f0..b0...U.......á0...+.....7.......U.s.e.r0...U.........j&.
  UÄñ8!_X.._I.(.0ü...U.#.ü_0ü¢.._ºFr. _";*...0_S__N@íqño0m1.0...*åHå.......tt@cisco.com1.0...U....US1.0...
  U....Herzeliya1.0
    [079] EAP-Message
  value:  ...U....Cisco1.0...U....EMBU1.0...U....EAPCA.. n_SF9óJÉR_h_}¿0.....U...ü.0ü.0ü.áü_áü.åü»ldap://
  /CN=EAPCA,
CN=cd-lab210,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=d3w2k,DC=acslab?certificat
  eRevocationList?base?objectclass=cRLDistri
    [079] EAP-Message                value:  butionPoint08á6á4å2http://
cd-lab210.d3w2k.acslab/CertEnroll/EAPCA.crl0.....+..........0ü.0üÑ..+.....0.åü.ldap:///
  CN=EAPCA,CN=AIA,CN=Public%20Key%20Services,CN=Services,CN=Configuration, DC=d3w2k,DC=acslab?cACertifica
  te?base?objectclass=certificationAuth
    [079] EAP-Message                value:  ority0U..+.....0.åIhttp://
cd-lab210.d3w2k.acslab/CertEnroll/
  cdlab210.d3w2k.acslab_EAPCA.crt0)..U.%."0.+.....7.....+.........+.......0/
  ..U...(0&á$..+.....7...á...eaptls3@d3w2k.acslab0...*åHå........A.:ç!.@.<_}bS.I._..lC.m¥_eD1z.E._k__R).7
  .{..ñó..^..u.
    [079] EAP-Message                value:  .X5ïpqS`6{à1L......)7D.^$.
Ü.._¢_b_.l.~..k»_Göë._.ù!'G,...'_ô._.Z}à$.ç"Z_..O.Jço.y_.Y.__.S..dö${[g_W_7.c_<U.2.C...w_F._.w_O_.___¥&R)
  .__.._s.-ò(._)__...B.@wU.y6mH/...DE.___6..\&_ë.*._`ºm__ƒ«N_..i_<_.9u__.ñÄ.01H_._l .!__.......... U
    [080] Message-Authenticator      value:  FD CB 56 B7 43 29 90 76 2A 29 7F 7F BC 82 BB B5
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                value:  .@....
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.5
ExtensionPoint: End of Attribute Set
Sending response code 11, id 249 to 10.51.117.25 on port 2341
    [079] EAP-Message                value:  .@....
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.5
```

```
Request from host 10.51.117.25:1812 code=1, id=250, length=143 on port 2341
    [001] User-Name                  value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address             value:  10.51.117.25
    [012] Framed-MTU                 value:  1000
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.5
    [079] EAP-Message                value:  .@.%..<äZ_...R_..#.J.)¿~rü_ùñ3äLú.â8K
    [080] Message-Authenticator      value:  5D 98 E6 AC 45 EF 04 F9 03 E2 59 0C 8A 49 8C F8
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                value:  .`.5.....+.......... __J.s.._._|w.êf.'}_."ö_..?_yâe..
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.6
ExtensionPoint: End of Attribute Set
Sending response code 11, id 250 to 10.51.117.25 on port 2341
    [079] EAP-Message                value:  .`.5.....+.......... __J.s.._._|w.êf.'}_."ö_..?_yâe..
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.6
Request from host 10.51.117.25:1812 code=1, id=251, length=112 on port 2341
    [001] User-Name                  value:  eaptls3@d3w2k.acslab
    [004] NAS-IP-Address             value:  10.51.117.25
    [012] Framed-MTU                 value:  1000
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.202.77.6
    [079] EAP-Message                value:  .`....
    [080] Message-Authenticator      value:  78 7F 6F 6E E2 65 D7 47 87 78 34 C0 3D FB 52 1A
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [4 - accept_continue]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                value:  .a..
    [026] Vendor-Specific vsa id: 311
          [016] MS-MPPE-Send-Key     value:  ).5.__~._Lá_2ûQ.à.._.>¢m_Æ_ä_#"....å.T_,__M_...¿_.
    [026] Vendor-Specific vsa id: 311
          [017] MS-MPPE-Recv-Key     value:  #Hï$N=XÄ._..u_ì_)_.ƒUá_8.Éí ...ñ¬_..._..___(_»__xë
ExtensionPoint: End of Attribute Set
AuthorExtensionPoint: Initiating scan of configured extension points...
AuthorExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
AuthorExtensionPoint: Supplier [Cisco Downloadable ACLs] not associated with vendor [RADIUS (IETF)], skip
  ping...
Sending response code 2, id 251 to 10.51.117.25 on port 2341
    [064] Tunnel-Type                value:  [T1] 13
    [081] Tunnel-Private-Group-ID    value:  [T1] 2
    [008] Framed-IP-Address          value:  255.255.255.255
    [079] EAP-Message                value:  .a..
    [026] Vendor-Specific vsa id: 311
          [016] MS-MPPE-Send-key     value:  ).5.__~._Lá_2ûQ.à.._.>¢m_Æ_ä_#"....å.T_,__M_...¿_.
    [026] Vendor-Specific vsa id: 311
          [017] MS-MPPE-Recv-Key     value:  #Hï$N=XÄ._..u_ì_)_.ƒUá_8.Éí ...ñ¬_..._..___(_»__xë
```

Windows XP Client Operating in EAP-MD5 (CHAP) Mode

Cisco Catalyst 6500 (CATOS) of Port Number 2/2 Debug Output EAP-MD5

```
2001 Nov 27 02:42:50 %PAGP-5-PORTTOSTP:Port 2/2 joined bridge port 2/2
2001 Nov 27 02:43:24 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/2 is
  AUTHENTICATING
2001 Nov 27 02:43:24 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 02:43:25 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 02:43:25 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 02:43:25 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is SUCCESS
2001 Nov 27 02:43:25 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is FINISHED
2001 Nov 27 02:43:26 %SECURITY-5-DOT1X_AUTHENTICATION_SUCCESS:Authentication successful for port 2/2
2001 Nov 27 02:43:26 %SECURITY-5-DOT1X_PORT_AUTHORIZED:DOT1X: port 2/2 authorized
2001 Nov 27 02:43:26 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/2 is
  AUTHENTICATED
2001 Nov 27 02:44:28 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/2 is
  CONNECTING
2001 Nov 27 02:44:28 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/2 is
  AUTHENTICATING
2001 Nov 27 02:44:28 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 02:44:29 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is REQUEST
2001 Nov 27 02:44:29 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is RESPONSE
2001 Nov 27 02:44:30 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is SUCCESS
2001 Nov 27 02:44:30 %SECURITY-7-DOT1X_BACKEND_STATE:DOT1X: backend state for port 2/2 is FINISHED
2001 Nov 27 02:44:30 %SECURITY-5-DOT1X_AUTHENTICATION_SUCCESS:Authentication successful for port 2/2
2001 Nov 27 02:44:30 %SECURITY-7-DOT1X_AUTHENTICATOR_STATE:DOT1X: authenticator state for port 2/2 is
  AUTHENTICATED
```

Full Cisco Secure ACS 3.0 RADIUS Debug Recording for EAP-MD5 Negotiation with Cisco Catalyst Switch

```
Request from host 10.51.117.25:1812 code=1, id=83, length=71 on port 2341
    [001] User-Name                  value:  eapmd5
    [004] NAS-IP-Address             value:  10.51.117.25
    [012] Framed-MTU                 value:  1000
    [079] EAP-Message                value:  .....eapmd5
    [080] Message-Authenticator      value:  27 9B 21 1D 01 81 0B 82 FB 99 86 0A DE 46 F5 7C
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [11 - challenge]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                value:  .ë....ë_.... èNm__"á`XCD-LAB210
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.203.2f.1
ExtensionPoint: End of Attribute Set
Sending response code 11, id 83 to 10.51.117.25 on port 2341
    [079] EAP-Message                value:  .ë....ë_.... èNm__"á`XCD-LAB210
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.203.2f.1
Request from host 10.51.117.25:1812 code=1, id=84, length=120 on port 2341
    [001] User-Name                  value:  eapmd5
    [004] NAS-IP-Address             value:  10.51.117.25
    [012] Framed-MTU                 value:  1000
    [024] State                      value:  CISCO-EAP-CHALLENGE=0.203.2f.1
    [079] EAP-Message                value:  .ë....k.I.t_.|N.e^X£_deapmd5
    [080] Message-Authenticator      value:  96 0A 35 94 D1 DF B9 B8 DA 03 D7 C4 66 42 A9 22
ExtensionPoint: Initiating scan of configured extension points...
ExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
ExtensionPoint: Calling [AuthenticationExtension] for Supplier [Cisco Generic EAP]
ExtensionPoint: [GenericEAP.dll->AuthenticationExtension] returned [4 - accept_continue]
ExtensionPoint: Start of Attribute Set
    [079] EAP-Message                value:  .ë...
ExtensionPoint: End of Attribute Set
AuthorExtensionPoint: Initiating scan of configured extension points...
AuthorExtensionPoint: Supplier [Cisco Aironet] not associated with vendor [RADIUS (IETF)], skipping...
AuthorExtensionPoint: Supplier [Cisco Downloadable ACLs] not associated with vendor [RADIUS (IETF)], skip
  ping...
Sending response code 2, id 84 to 10.51.117.25 on port 2341
    [064] Tunnel-Type                value:  [T1] 13
    [081] Tunnel-Private-Group-ID    value:  [T1] 2
    [008] Framed-IP-Address          value:  255.255.255.255
    [079] EAP-Message                value:  .ë...
```

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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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

Printed in the USA

12/01 BW7858