

# Guidelines for Placing ACS in the Network



## Introduction

This document discusses planning, design, and implementation practices for deploying Cisco Secure Access Control Server (ACS) for Windows NT/2000 in an enterprise network. It includes discussions about network topology, user base choices, access requirements, integration of external databases, and capabilities of ACS. The information in this document is based on ACS versions 2.6 and 3.0.

## Factors Influencing ACS Deployment

A number of factors influence how ACS is deployed within the enterprise network:

- Network topology
- Remote-access policy
- Security policy
- Administrative access policy
- Database
  - Number of users
  - Type of database
  - Network speed and reliability

## Authentication, Authorization, and Accounting

Cisco Secure ACS for Windows NT/2000 is an authentication, authorization, and accounting (AAA) access control server. ACS provides access control to network access servers through AAA, an architectural framework for configuring a set of three independent security functions consistently. AAA provides a modular way of performing the following services:

- Authentication—Provides the method of identifying users, including login and password dialog, challenge and response, messaging support, and, depending on the security protocol selected, possibly encryption.
- Authorization—Provides the method for remote-access control, including one-time authorization or authorization for each service, per-user account list and profile, support for user groups, and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet.
- Accounting—Provides the method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop times, executed commands (such as Point-to-Point Protocol [PPP]), number of packets, and number of bytes.

ACS uses two distinct protocols for AAA services: Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+).

RADIUS, developed at Livingston (now Lucent), is considered the industry standard for AAA support. In June 1996, Draft 5 of the RADIUS protocol specification was submitted to the Internet Engineering Task Force (IETF). The RADIUS specification (RFC2865) and RADIUS accounting standard (RFC2866) are now the proposed standard protocols. ACS also supports RFC2868 (RADIUS Attributes for Tunnel Protocol Support). The text of the IETF proposed standards is available at the following URLs:

- <http://www.faqs.org/rfcs/rfc2865.html>
- <http://www.faqs.org/rfcs/rfc2866.html>
- <http://www.faqs.org/rfcs/rfc2868.html>

RADIUS provides authentication and authorization in a single step. When the user logs into the network, the NAS prompts the user for a username and a password. The NAS will then send the request to the ACS. The NAS may include a request for access restrictions or per-user configuration information. The RADIUS server returns a single response with authentication approval status and any related access information available.

TACACS+ is the Cisco Systems proprietary AAA protocol. It was originally proposed by C. Finseth at the University of Minnesota as TACACS.

TACACS+ separates the authentication, authorization, and accounting steps. This architecture allows separate authentication solutions that can still use TACACS+ for authorization and accounting. During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine whether the user is granted permission to use a particular command. This provides greater control, compared with RADIUS, over the commands that can be executed on the access server and decouples the authorization process from the authentication mechanism. For example, with TACACS+, it is possible to use Kerberos Protocol authentication and TACACS+ authorization and accounting. After an NAS passes authentication on a Kerberos server, it requests authorization information from a TACACS+ server without having to reauthenticate the NAS by using the TACACS+ authentication mechanism. The NAS informs the TACACS+ server that it has successfully passed authentication on a Kerberos server, and the server then provides authorization information.

An in-depth comparison of TACACS+ and RADIUS can be found at:

- <http://www.cisco.com/warp/public/480/10.html>

RADIUS is generally recommended when providing network access, such as with PPP or virtual private networks (VPNs). TACACS+, though functional as a network access protocol, is recommended for NAS access because of its ability to support more extensive capabilities, such as command filtering.

## Network Topology

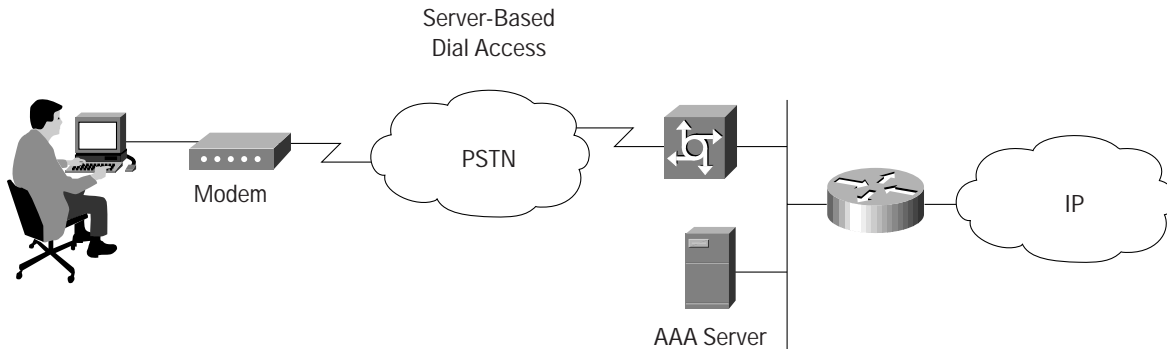
How the enterprise network is configured is probably the single most important factor in deciding how to deploy the ACS. When AAA was first considered, network access was restricted either to devices directly connected to the LAN or remote devices gaining access via modem. Today, enterprise networks can be very complex and, thanks to encryption technologies, can be widely dispersed geographically.

### Dialup Access

In the traditional model of dialup access (a PPP connection), a user employing a modem or Integrated Services Digital Network (ISDN) connection is granted access to an intranet through an NAS. Users may be able to connect only through a single NAS, as in a small business, or may have the option of numerous geographically dispersed access servers.

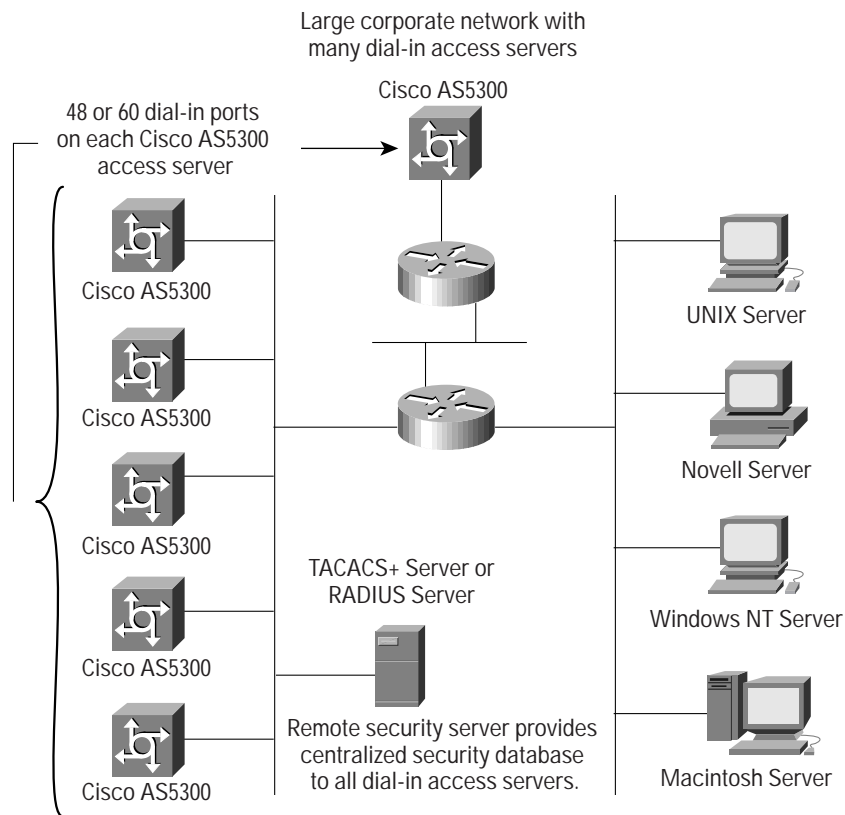
In the small LAN environment (Figure 1), a single ACS is usually located internal to the NAS and is protected from outside access by a firewall and the NAS. In this environment, the user database is usually small, there are few devices that require access to the ACS for AAA, and any database replication is limited to a secondary ACS as a backup.

Figure 1 Small LAN Environment



In a larger dial-in environment, a single ACS installation with a backup may be suitable, too (Figure 2). The suitability of this configuration is dependent on network and server access latency. In this scenario, adding a backup ACS is recommended.

Figure 2 Large Dial-In Network



In a large, geographically dispersed network (Figure 3), where access servers may be located in different parts of a city, in different cities or on different continents, a central ACS may work if network latency is not an issue. But connection reliability over long distances may cause problems. In this case, local ACS installations may be preferable to a central server. If the need for contiguous data is necessary, then database replication or synchronization from a central server may be

necessary. This may be further complicated by the use of external databases (such as NT or Lightweight Directory Access Protocol [LDAP]) used for authentication. Additional security measures may be required to protect the network and user information being forwarded across the WAN. This combines topology and security factors. In this case, the addition of an encrypted connection between regions would be indicated.

Figure 3 Geographically Dispersed Network

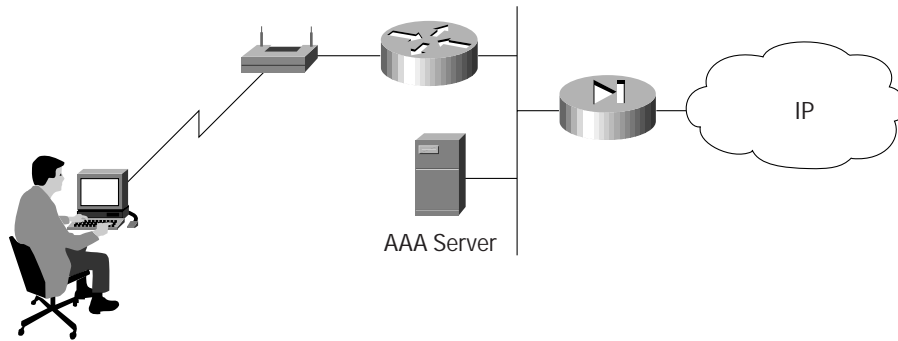


### Wireless Network

The wireless network is a relative newcomer to AAA. The wireless access point (AP), such as the Cisco Aironet® series, provides a bridged connection for mobile clients into the LAN. Authentication is absolutely necessary because of the ease of access to the AP. Encryption is also a necessity because of the ease of eavesdropping on communications. As such, security plays an even bigger role than in the dialup scenario and will be discussed in more detail later.

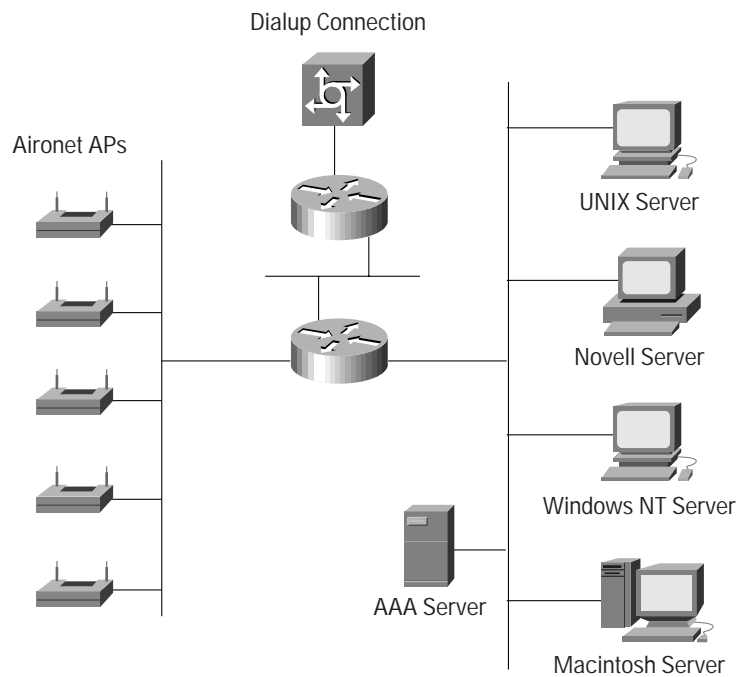
Scaling can be a serious issue in the wireless network. Like the “wired” LAN, the mobility factor of the wireless LAN (WLAN) has similar considerations as the dialup network. Unlike the “wired” LAN, however, the WLAN can be more readily expanded. Although the WLAN technology does have physical limits on the number of users that can be connected through an AP, the number of APs can grow quickly. As with the dialup network, the WLAN can be structured to allow full access for all users, or provide restricted access to different subnets between sites, buildings, floors, or rooms. This brings up a unique issue with the WLAN: the ability of a user to “roam” between APs.

Figure 4 Simple WLAN



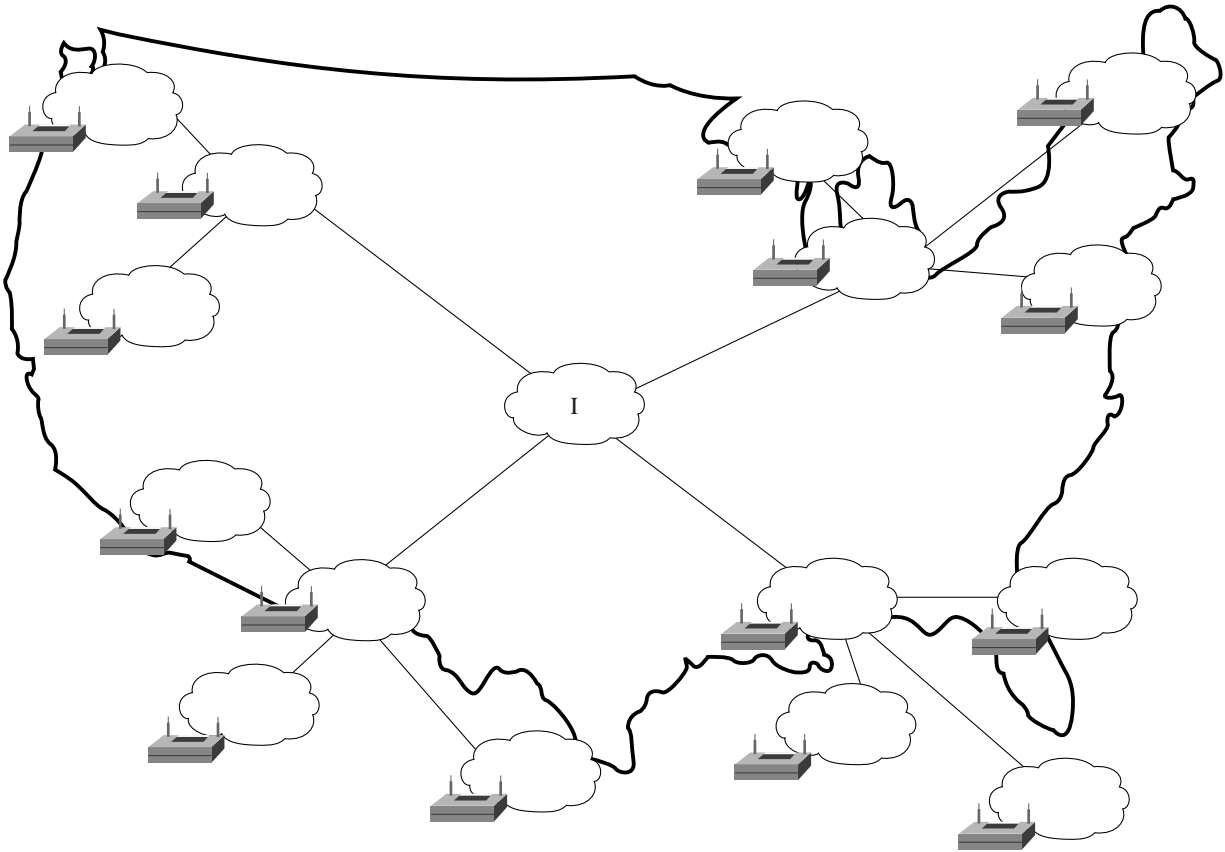
In the simple WLAN, a single AP may be installed (Figure 4). Because there is only one AP, the primary issue is security. In this environment, there is generally a small user base and few network devices to worry about. Providing AAA services to the other devices on the network will not cause any significant additional load on the ACS.

Figure 5 Campus WLAN



In a WLAN in which a number of APs are deployed (Figure 5), as in a large building or a campus environment, the decisions about how to deploy ACS become more complicated. Although Figure 5 shows all APs on the same LAN, they may be distributed throughout the LAN, connected via routers and switches. In the larger geographical distribution of WLANs, the ACS deployment is similar to that of the large regional distribution of dialup LANs (Figure 3). This is particularly true when the regional topology is the campus WLAN (Figure 5). This model starts to change when WLANs are deployed in many small sites that more resemble the simple WLAN (Figure 4). This model may be applicable to a chain of small stores distributed throughout a city or state, nationally, or globally (Figure 6).

Figure 6 Large Deployment of Small Sites



In the Figure 6 model, the decision for authentication from the ACS depends on whether users from the entire network need access on any AP or whether they only require regional or local network access. This factor, along with database type, controls whether local or region ACS installations are required and how database continuity is maintained. In this very large deployment model, security becomes more complicated, too.

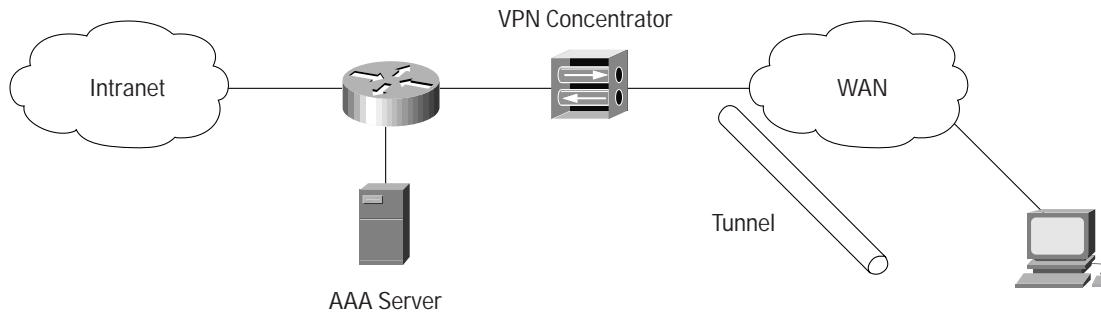
#### Remote Access Using VPN

VPNs use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets (Figure 7).

Benefits of a VPN include:

- **Cost Savings**—By leveraging third-party networks, with VPN technology, organizations no longer have to use expensive leased or Frame Relay lines and are able to connect remote users to their corporate networks through a local Internet service provider (ISP) instead of through expensive 800-number or long-distance calls to resource-consuming modem banks.
- **Security**—VPNs provide the highest level of security using advanced encryption and authentication protocols that protect data from unauthorized access.
- **Scalability**—VPNs allow corporations to use remote access infrastructure within ISPs. Therefore, corporations are able to add a virtually unlimited amount of capacity without adding significant infrastructure.
- **Compatibility with Broadband Technology**—VPNs allow mobile workers, telecommuters, and day extenders to take advantage of high-speed, broadband connectivity, such as DSL and cable, when gaining access to their corporate networks, providing workers significant flexibility and efficiency.

Figure 7 Simple VPN Configuration



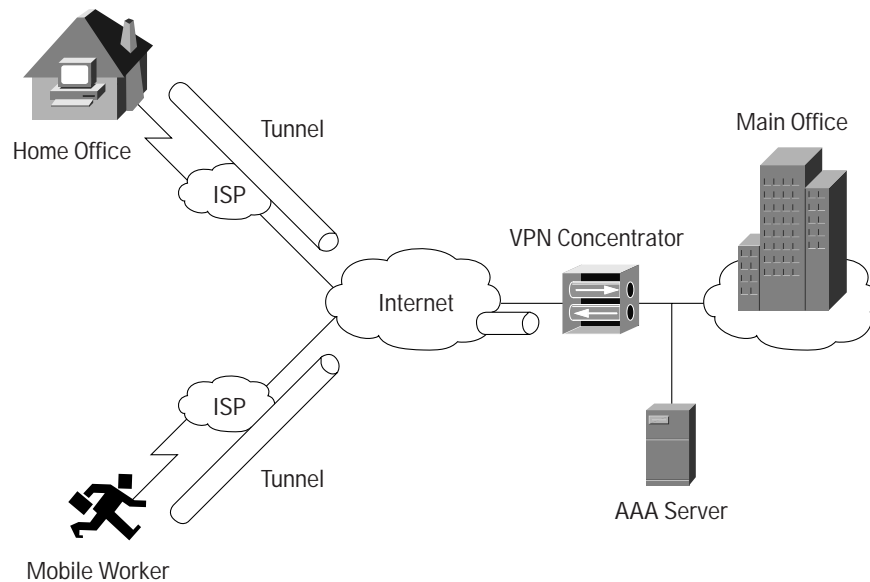
There are two types of VPN access into a network:

**Site-to-Site VPNs**—Extend the classic WAN by providing large-scale encryption between multiple fixed sites such as remote offices and central offices, over a public network, such as the Internet.

**Remote-Access VPNs**—Permit secure, encrypted connections between mobile or remote users and their corporate networks through a third-party network, such as a service provider, through VPN client software.

Generally, site-to-site VPNs can be viewed as a typical WAN connection and are not usually configured to use AAA to secure the initial connection. Remote-access VPNs, however, are similar to classic remote-connection technology (modem or ISDN) and lend themselves to using the AAA model effectively (Figure 8).

Figure 8 Enterprise VPN Solution



A more in-depth discussion of implementing VPN solutions is available at [http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21\\_rg.htm](http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm).

## Remote-Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). This connection may occur in a number of ways. The methods include, but are not limited to, dial-in, ISDN, wireless bridges, and secure Internet connections. Each method has advantages and disadvantages and provides its own challenge to providing AAA services. This closely ties remote-access policy to the enterprise network topology. In addition to the method of access, other decisions, such as specific network routing (access lists), time-of-day access, individual restrictions on NAS access (access control lists), and so on, can also affect how the ACS is deployed.

Remote-access policies can be implemented for employees who telecommute or for mobile users who dial in over an ISDN or a Public Switched Telephone Network (PSTN). Such policies are enforced at the corporate campus with ACS and the access server (AS5300, VPN concentrator, and so on). Inside the enterprise network, remote-access policies can control access for individual employees for wireless access.

ACS remote-access policy provides control by using central authentication and authorization of remote users. The ACS database maintains all user IDs, passwords, and privileges. ACS access policies can be downloaded in the form of access control lists (ACLs) to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

The remote-access policy is part of the overall corporate security policy.

## Security Policy

Cisco Systems recommends that every organization that maintains a network develop a security policy, which should define 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 the following URLs:

- <http://www.cisco.com/warp/public/126/secpol.html>
- [http://www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/deesp\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/deesp_wp.htm)
- [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/secr\\_c/scdoverv.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/secr_c/scdoverv.htm)

## Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to the network devices depends directly on the size of the network and the number of administrators required to maintain it. Local authentication on the NAS can be performed, but it is not very scalable. The use of network management tools can help in large networks, but if local

authentication is used on each device, the policy usually will consist of a single login on the NAS. This does not promote adequate device security. The use of ACS allows for a centralized administrator database, and administrators can be added or deleted at one location. TACACS+ is the recommended AAA protocol choice for controlling NAS administrative access because of its ability to provide per-command control (command filtering) of an NAS administrator's access to the device. RADIUS is not well-suited for this purpose because of the one-time transfer of authorization information at the time of authentication acceptance.

The type of access is also an important consideration. If there are to be different administrative access levels to the NAS, or if a subset of administrators is to be limited to certain systems, ACS can be used with command and NAS filtering to restrict administrators as necessary. To use local authentication restricts the administrative access policy to no login on a device (as previously discussed) or using privilege levels to control access. Controlling access by means of privilege levels is cumbersome and not very scalable. This requires that the privilege levels of specific commands are altered on the NAS and specific privilege levels are defined for the user login. It is also very easy to create more problems by editing the command privilege level. Using command filtering on ACS doesn't require the privilege level of controlled commands be altered. The NAS sends the command to the ACS to be parsed, and ACS determines whether the administrator has permission to use the command (Figure 9). Because the use of AAA allows authentication on any NAS configured for AAA to any administrator on the ACS, NAS filtering can be used to limit access to these devices on a per-NAS basis.

A small network with few network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If more control than what authentication can provide is required, some means of authorization is necessary. As discussed earlier, controlling access using privilege levels can be cumbersome. ACS reduces this problem.

Figure 9 Command Filtering Configuration

**IOS Commands**  
Unmatched Cisco IOS commands  
 Permit  
 Deny

**Command:**  
  
Arguments:  
  
Unlisted arguments  
 Permit  
 Deny

In large enterprise networks, with a large number of devices to administer, the use of the ACS becomes a virtual necessity. Because the administration of many devices requires a larger number of administrators with varying levels of access, the use of local control would create confusion just trying to keep track of the configuration changes required when changing administrators or devices. The use of network management tools, such as CiscoWorks, helps to ease this burden, but

maintaining security is still an issue. Because the ACS can comfortably handle up to 100,000 users, the number of administrators the ACS supports should not be an issue. If there is a large remote-access population using RADIUS for AAA support, the corporate information technology (IT) team should consider a separate ACS system for TACACS+ authentication for the administrator team. This would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If this is not a suitable solution, though, using TACACS+ for administrative (shell/exec) logins and RADIUS for remote network access provides sufficient security for the network devices.

### Separating Administrative and General Users

It is important to keep general network users from accessing network devices. Even though a general user might not intend to disrupt the system, inadvertent access may cause accidental disruption to network access. Separating general users from administrative users falls into the realm of AAA and the 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 issue likely to arise is that an administrator might also require remote network access, like a general user. This poses no problem with ACS. The administrator can have both RADIUS and TACACS+ configurations in ACS. Using authorization, RADIUS users can have PPP (or another network access protocol) set as the permitted protocol. Under TACACS+, only the administrator would be configured to allow shell (exec) access.

For example, if the administrator is dialing into the network as a general user, the NAS would use RADIUS as the authenticating and authorizing protocol and the PPP protocol would be authorized. In turn, if the same administrator is remotely connecting to the network device to make configuration changes, the device would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on ACS with permission for shell under TACACS+, he would be authorized to log onto that device. This does require that the NAS have two separate configurations on ACS, one for RADIUS and one for TACACS+. An example of an NAS configuration under Cisco IOS® Software is provided.

#### Example 1—Sample Cisco IOS Configuration for Separating PPP and Shell Logins

```
aaa new-model
tacacs-server host <ip-address>
tacacs-server key <secret-key>
radius-server host <ip-address>
radius-server key <secret-key>
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username <user> password <password>
line con 0
  login authentication no_tacacs
```

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

### Database

Aside from the topological considerations, the database is one of the most influential factors involved in making deployment decisions for the ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of database employed all contribute to how the ACS is used.

## Number of Users

ACS is designed for the enterprise environment, comfortably handling 80,000 to 100,000 users. This is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be widely distributed geographically and lend itself to using more than one ACS configuration. As discussed in the “Network Topology” section, deploying a single ACS to handle remote regions would not be prudent because of network latency and reliability. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition to this issue, reducing the number of users that a single ACS handles improves performance by lowering the number of logins occurring at any given time and by reducing the load on the database itself.

## Type of Authentication

ACS supports a number of authentication options. Under the current version of ACS, the options include using the local ACS database, using remote authentication via an external database, or synchronizing a remote relational database management system (RDBMS) database with the ACS local database. Table 1 shows the various options and available features.

Table 1 ACS Database Optional

Authentication Method	Features				
	Clear Text	PAP	CHAP	MS-CHAP	Group Mapping
Local	X	X	X	X	X
NT/2000 AD	X	X		X	X
Novell NDS	X	X			X
Generic LDAP	X	X			X
ODBC	X	X	X	X	X
RDBMS using RDBMS-Synchronization	X	X	X	X	X
Token Server (OTP)	X	X			
MCIS	X	X	X	X	X
Remote AAA Server	X	X	*	*	

\* If supported by remote AAA server

Each database option has its own advantages as well as limitations to scalability and performance.

### Local Database

Provides full feature support. Using the local database provides the maximum speed for authentication. It may have regional scalability problems, which can be minimized using database replication. However, replication requires a primary/secondary relationship between ACS systems. Replication keeps AAA servers synchronized by copying selected configuration items from a primary ACS installation over the configuration of a secondary ACS installation, completely replacing those configuration items on the secondary. This restricts maintenance of user accounts to the primary ACS installation. Another drawback is that if an organization has an existing database for users, both databases must be separately maintained.

### Windows NT/2000 AD

In organizations in which a substantial Windows NT/2000 user database already exists, ACS can leverage the work already invested in building the database without any additional input. This eliminates the need for separate databases. When the NAS presents the username to ACS, ACS searches its database to locate a match. If ACS does not find a match and ACS is configured to check the Windows NT/2000 user database, the username and password are forwarded to Windows NT/2000 for authentication against those in the Windows NT/2000 user database. If a match is confirmed, the username (but not the password) is stored in the CiscoSecure user database for future authentication requests. Later authentication requests will

authenticate much faster because ACS goes directly to the Windows NT/2000 user database for authentication. Group mapping allows greater flexibility of user privileges. Authorization privileges assigned to the user's group are then assigned to the user just authenticated. Using Primary Domain Controller (PDC) trust relationships extends the number of users who can be authenticated by ACS. Timeouts may be a problem using PDC trust relationships because of the sometimes-present latency in NT networking. Another problem is that authenticating against the Windows NT/2000 user database does not allow storage of third-party passwords (Challenge Handshake Authentication Protocol [CHAP], for example).

**Novell NDS and Generic LDAP**

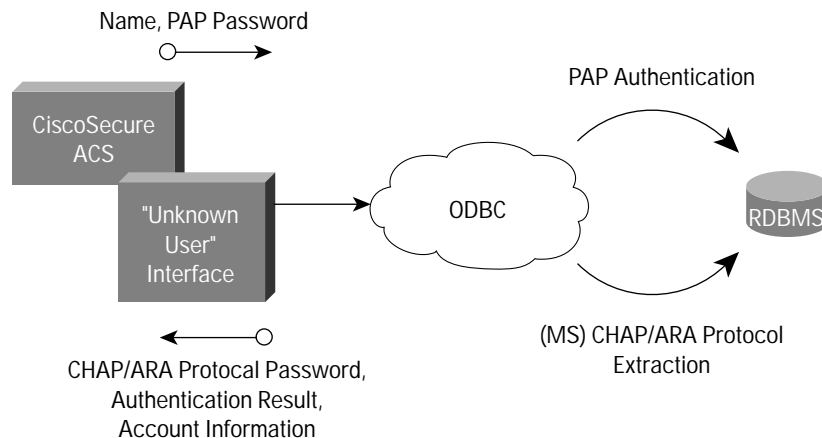
ACS supports authentication of users against records kept in a directory server using LDAP and Novell NetWare Directory Services (NDS). ACS interacts with the most popular directory servers, including Novell and Netscape. Password Authentication Protocol (PAP) and clear text passwords can be used when authenticating against the directory server. These services do not support CHAP or Microsoft CHAP (MS-CHAP). This may be an issue when trying to use network devices that are limited to using one of these protocols (that is, Cisco Aironet wireless). Group mappings are available, as with Windows NT or 2000.

A white paper on LDAP authentication is available at: [http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/ldcsa\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/ldcsa_wp.htm)

**Open DataBase Connectivity**

ACS supports authentication against a relational database that is compliant with Open DataBase Connectivity (ODBC). This enables the use of existing user records. ODBC is a standardized application programming interface (API) that was first developed by Microsoft and is now used by most major database vendors. ODBC now follows the specifications of the Structured Query Language (SQL) Access Group. The Windows ODBC feature enables you to create a Data Source Name (DSN), which specifies the database and other important parameters necessary for communicating with the database. ACS passes the user information to the relational database through the ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns to the CiscoSecure ACS. If the returned values indicate that the username and password provided are valid, ACS grants the user access. Otherwise, ACS denies the user access (Figure 10). Because of the ODBC feature that allows password extraction, ODBC can authenticate clear text, PAP, CHAP, MS-CHAP, and ARA Protocol passwords.

Figure 10 ODBC External Database Authentication



A white paper on LDAP authentication is available at: [http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/exatu\\_wp.htm](http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/exatu_wp.htm).

### RDBMS Synchronization

RDBMS synchronization does not provide remote authentication through an external database, as with NDS or NT. Instead, RDBMS synchronization (or “dbsync”) provides remote configuration of the local database from an ODBC-compliant relational database. This allows the full range of services provided by the local database and the advantages of a separate RDBMS database. It is worth noting that “dbsync” is intended for the advanced client who already has an SQL-based user management and billing system and wants to programmatically push data to the ACS configuration.

### Token Card Servers

Many networks require a token card for one-time password (OTP) authentication. This method is very secure but has several caveats. First, it cannot be combined with encrypted password protocols (CHAP and MS-CHAP). There is no need because of the nature of OTP. However, this causes a problem, as with LDAP and NDS, because of the issue of trying to use network devices that are limited to using one of these protocols (that is, Aironet wireless). Another problem is that group mappings are not available. The token card server should be located reasonably close to the ACS installation because of possible network latency issues.

### Remote AAA Server (Proxy)

Proxy enables ACS to automatically forward an authentication request from an NAS to another AAA server. After the request has been successfully authenticated, the authorization privileges that have been configured for the user on the remote AAA server are passed back to the original ACS, where the user’s profile information is applied for that session on the NAS. This is a very powerful tool that can expand the use of ACS by minimizing the number of users that need to be configured in a locally defined database. Group information, for example, does not need to be maintained on the local ACS. Another advantage is that the organization is not limited to ACS. Other vendors’ AAA products can be used. One drawback is that a user must supply his or her name along with a previously defined string (for example, “mary.smith@corporate.com,” where “@corporate.com” is a character string defined in the server’s Distribution Table as being associated with another specific ACS). Another disadvantage is that it creates a problem when performing NAS filtering. The NAS IP address of the forwarding ACS is used rather than the IP address of the NAS generating the request.

### Network Speed and Reliability

Network speed, also referred to as network latency, and network reliability also play an important role in how ACS is deployed. Delays in authentication can result in timeouts at the client side or the NAS.

The general rule for large, extended networks, such as a globally dispersed corporation, is to have at least one ACS deployed in each region. This may not be adequate if a reliable, high-speed connection between sites is not incorporated. As mentioned in the discussion of VPNs, many corporations are now using secure VPN connections between sites, using the Internet to provide the link. This saves time and money but does not provide the speed and reliability that a dedicated frame or T1 link would provide. If authentication is critical to maintain business functionality, as in the case of a store having cash registers linked via a wireless LAN, the loss of the WAN connection to a remote ACS could be catastrophic.

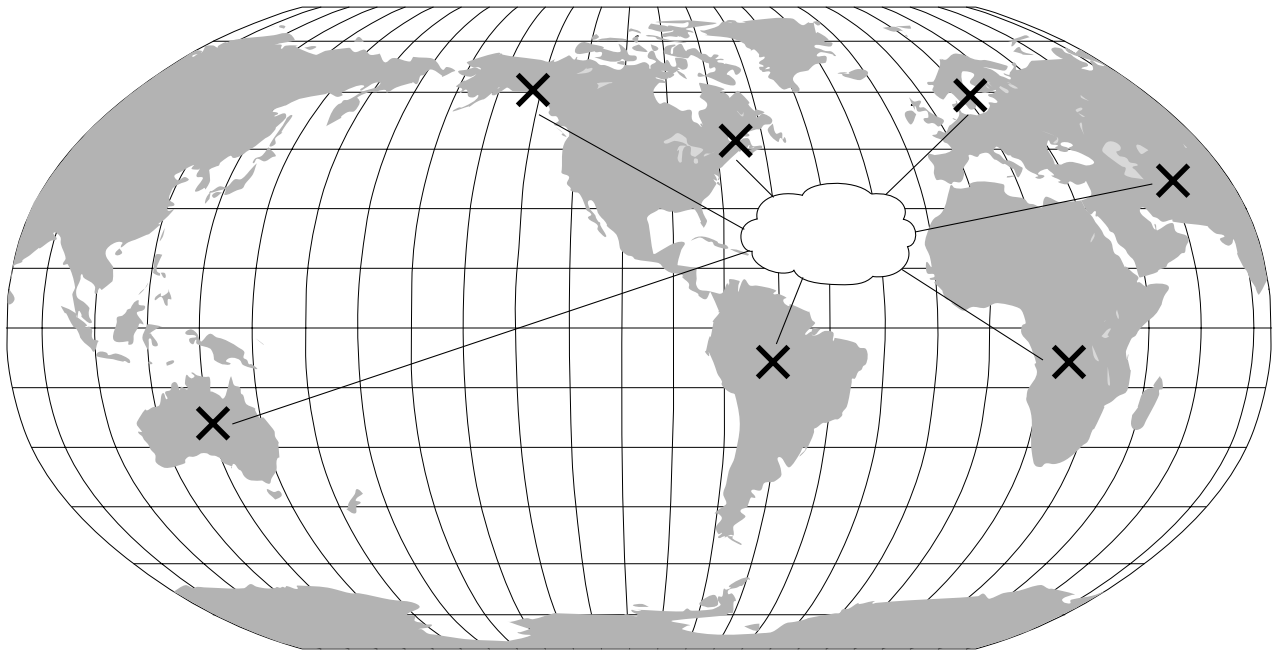
The same issue can be applied to an external database used by the ACS. The database should be deployed near enough to the ACS installation to ensure reliable and timely access. Using a local ACS with a remote database can result in the same problems as using a remote ACS. Another possible problem in this scenario is that a user would experience a timeout problem rather than getting a message that his username could not be authenticated. The NAS would be able to contact ACS, but ACS would wait for a reply that might take a while to receive, if at all. If the ACS were remote, the NAS would time out and try an alternative method to authenticate the user, but in the latter case it is likely that the user’s client program would time out first.

## Review

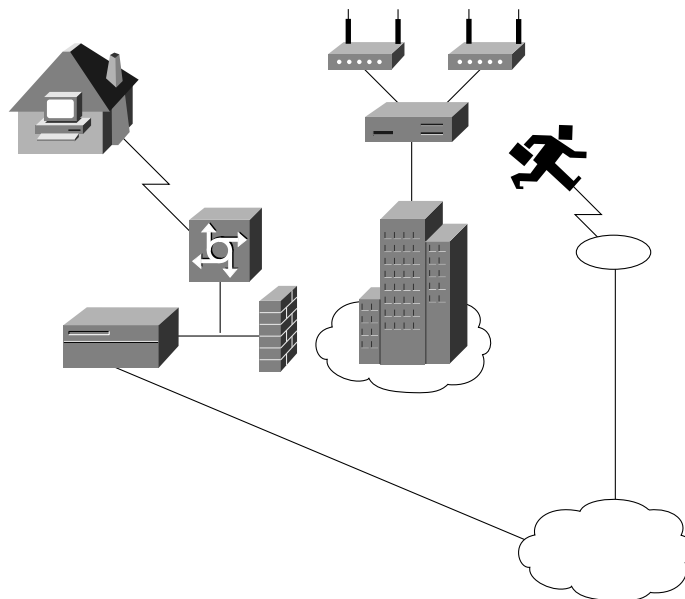
The factors that govern how ACS is deployed are closely interconnected. Network topology is closely tied to network speed and reliability. Access and security policies are tied to network topology and database issues. Almost any combination is possible. When AAA was first conceived, the main purpose was to provide a centralized point of control for user access through dial-in services. As the user base grew and the locations of the access servers were distributed more widely, more capability was required of the AAA server. Regional, then global, requirements became common. Today, ACS is required to provide AAA services for dial-in access, dial-out access, wireless, virtual LAN (VLAN) access, firewalls, VPN concentrators, and administrative control. The list continues to grow. As networks are combined through acquisitions and mergers, multiple databases are increasingly used.

It is possible to have a large, dispersed, mixed environment. A combination of remote access via dial-in and VPN, along with local access via wireless is becoming more popular. Add to the mix local access control via VLAN authentication, and a complex intranet emerges. Figure 11 shows how complex the enterprise network can become. These environments require multiple ACS deployment.

Figure 11 World Deployment Scheme



The black X represents the configuration below in various worldwide locations.



The inclusion of external databases in this topology necessitates the deployment of multiple installations of the database server as well. If different databases are in use, the administrator will have to configure ACS regionally to accommodate the differing formats. For instance, if North America is using LDAP but Asia is using NDS, the North American ACS should check the LDAP database first. It can also be configured to check the Asian NDS database, but because there will be fewer requests to that database, it can be farther down the list in external database configuration. The converse is true for the Asian ACS. If regions share a common database, synchronized installations should be located in each region and served by their

own ACS. In the event that there is a single unified database that is centrally administered, it is recommended that there be multiple ACS and database installations throughout the regions. Database replication and synchronization can then be used to permit timely access to the local LAN.

If a regional topology has no central “campus” but is distributed with similarly sized “mini campuses” that are interconnected with T1, fiber optics, or similar technology, a central ACS can be employed to service the AAA needs of each building. The possibility of the link being compromised is low, and access speeds should be adequate to handle timely authentication.

Further discussions of specific deployment issues, scalability, and performance will be discussed in follow-up documents.



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 Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney  
NSW 2060 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

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](http://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

Copyright © 2001, Cisco Systems, Inc. All rights reserved. Printed in the USA. Aironet, Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0106R) 201762 10/01