White Paper

Deploying Cisco Secure ACS for Windows in a Cisco Aironet Environment

Introduction

Cisco Secure ACS for Windows has long supported the centralization of access control and accounting for dial-up access servers, virtual private networks (VPNs), firewalls, and voice over IP (VoIP) solutions. Starting with Cisco Secure ACS v2.6 for Windows 2000/NT Servers, it supports standards-based IEEE 802.1X authentication of Cisco Aironet® 1200, 1100, 350 and 340 Series Access Points. Starting with Cisco Secure ACS v3.1 for Windows, support is now available for three IEEE 802.1X Extensible Authentication Protocol (EAP) types supported by the Cisco Wireless Security Suite:

- EAP Cisco Wireless (Cisco LEAP)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Protected Extensible Authentication Protocol (PEAP)

Cisco Secure ACS v3.1 also supports concurrent operation of any combination of these three EAP types.

Deployment Overview

You should consider several factors when you are deploying an access control server (ACS) to support wireless networks. Each factor may not be critical in isolation but when combined in the complete deployment, the combination may seriously affect the performance of the wireless LAN (WLAN) and ACS service. Points to consider include:

- Location and number of access points
- Location and number of Cisco Secure ACSs within the network
- Authentication types to be used
- Types of databases to be used and replication and synchronization strategies
- Number of users in each database and the expected access rate
- Need for central or dispersed access control
- Authentication timeouts
- Cisco Secure ACS redundancy

After you have reviewed these factors for your intended design and compared them to the guidelines discussed in this paper, you can design a logical and efficient Cisco Secure ACS deployment for wireless access control.

Performance

Stress testing was performed on Cisco Secure ACS v3.1 to determine the maximum number of authentication requests the Cisco Secure ACS can serve per second. The results were generated using an authentication, authorization, and accounting (AAA) client simulator created internally.

The hardware for testing the ACS system was configured as follows:

Cisco Secure ACS

HP Kayak 1.6 GHz, 256 MB RAM

Cisco Secure ACS v3.1 Internal database with 100,000 users in the database

300 access points

The following test results for LEAP, PEAP and EAP-TLS authentications are raw authentication rates. They do not include network latency, reliability, or user distribution factors.

- Sustained LEAP—90 authentications per second
- Sustained EAP-TLS—32 authentications per second
- Sustained PEAP—32 authentications per second

A significant factor in ACS authentication performance is the Remote Authentication Dial-In User Service (RADIUS) logging level. A high logging level may cause up to a 50 percent degradation of authentication performance.

Note: EAP-TLS testing was performed with "Certificate name comparison" only. Certificate name comparison uses Cisco Secure ACS to verify user identity by comparing the username to the name in the end-user client certificate. Certificate binary comparison uses Cisco Secure ACS to verify user identity by doing a binary comparison with the user certificate.

Scalability

Number of Users

The following recommendations provide guidelines on how to scale the Cisco Secure ACS for a Cisco Aironet wireless deployment. Using the minimum recommended hardware for the Cisco Secure ACS (Pentium III processor, 550 MHz or faster, and 256 megabytes of RAM), it can support 80,000 users in the internal database. Laboratory tests indicate that this number can be increased with the addition of more RAM. Testing shows that with RAM increased to one gigabyte, the Cisco Secure ACS can support 300,000 internal users with performance similar to the standard system supporting 50,000 users. However, the increased database size will affect replication, as discussed in a later section of this document.

The number of Cisco Secure ACSs required to support a specific size of user database depends on several factors including network topology, number of access points, network latency, expected number of users per access point, etc. Table 1 lists these performance factors.

Table 1 ACS Performance Factors

Number of ACS deployments required for a given user base	N_{acs}
Maximum number of authentications per second a single ACS is able to process	M_{aps}
Number of access points connected to the same ACS	N_{ap}
Number of users per access point	N_{users}
Number of retries configured on each access point	N_{retry}
Timeout of the retry (in seconds)	T_{retry}
Rekeying interval (RADIUS attribute 27)	T_{rekey}
Average length of user session	$T_{session}$
Average length of roaming user session	T_{roam}
Percentage of roaming users	P_{roam}
Packet rate	P
Total number of access points	N_{tap}
Safe work load	W_{safe}
Total number of users in the environment	N_{tuser}
Logging level	
Network latency	

In general, the minimum number of Cisco Secure ACSs required to support a given size of user database can be calculated with the following formula:

$$(N_{tuser} / (T_{rekey} * 60)) / (M_{aps} * W_{safe}) = N_{acs}$$

Where:

- N_{acs} is the number of Cisco Secure ACSs required
- N_{tuser} is total number of users in the environment
- T_{rekey} is the rekeying interval in minutes (RADIUS attribute 27)[1]
- M_{aps} is the number of authentication transactions per second
- W_{safe} is a "safe" workload for the ACS indicated as a percent fraction of the total ACS transaction capability

In our case study, we can expect an initial user base of 10,000 LEAP users. Testing has shown that we can expect to have a transaction rate of 90 transactions per second (tps) (Maps in the formula) for authentication only. Assuming a "safe" working load[2] of 40 percent, we can calculate the number of Cisco Secure ACSs required:

$$N_{acs} = (1000/(15*60)) / (90*0.40)$$

$$N_{acs} = 0.31$$

[1] See *Product Bulletin No. 1515*: *Cisco Wireless LAN Security Bulletin* for guidance on determining the correct rekeying interval for a given environment.

[2] The figure for the "safe" working load is derived using several assumptions: (1) provide the ability of any ACS to handle the load from the failover from another ACS; (2) provide the ability to handle "spikes" in authentication load, such as employees arriving first on shift; (3) provide an additional "spare" amount for handling new users. This value is arbitrary in this example. To determine this value, the percentage should include the number of failover ACSs that might be used (100% / # ACS), less some room for new users. The example shows (100%/2)-20% = 40% or 0.40.

Adding 5,000 EAP-TLS users, using the test results of 32 tps for EAP-TLS and keeping the other parameters the same, we get the following ACS requirements for EAP-TLS:

$N_{acs} = (5000/(15*60)) / (32*0.40)$

$N_{acs} = 0.43$

Add these two results together and 0.74 (or 1 rounded) ACS is required to support this user base. To put this in different terms, using the same ratio of 2 to 1 for LEAP to EAP-TLS, a single Cisco Secure ACS can support 21,000 users in a single LAN environment, as shown below.

$(14000/(15*60)) / (90*0.40) = 0.43$

$(7000/(15*60))/(32*0.40) = 0.61$

Total (21000 users per) = 1.04

The higher the safe work load, the higher number of supported users per ACS.

It's important to note, however, that a value of 40 percent for the "safe" working load may not be adequate if all contingencies occur simultaneously.

In the event of a large user base (100,000+), the calculations remain the same. Databases of this size incur other side effects. As mentioned earlier, increased memory helps alleviate performance issues related to database access. Other size-related issues will be discussed later in this document.

Note: The calculations for N_{acs} assume a uniform user density. The deployment designer needs to apply these calculations on a "per location" basis to get a more accurate figure. There will likely be localized "hot spots" where traffic could be many times higher than other areas.

In the case study scenario of 300,000 users, the calculations for the mixed environment for LEAP is:

$N_{acs} = (150000/(15*60))/(90*0.40)$

$N_{acs} = 4.63$

and for EAP-TLS:

$N_{acs} = (150000/(15*60))/ (32*0.40)$

$N_{acs} = 13.02$

The combined number is 18 Cisco Secure ACSs (rounded off). This number assumes a balanced deployment of LEAP and EAP-TLS. The 40 percent "safe" workload provides flexibility in the figures and allows for some growth before adding new servers is required. Similar calculations can be factored in for PEAP.

Additional adjustments to the number of Cisco Secure ACSs can be made by implementing features such as the Temporal Key Integrity Protocol (TKIP)[3]. Using TKIP, the Wired Equivalent Privacy (WEP) rekey timeout interval may be expanded to a maximum of 4 hours and 15 minutes without adversely affecting security (based on current

[3] TKIP defends against an attack on WEP in which the intruder uses the unencrypted initialization vector in encrypted packets to calculate the WEP key. TKIP removes the predictability that an intruder relies on to determine the WEP key by exploiting initialization vectors. See Chapter 4 of the *Cisco Aironet Access Point Software Configuration Guide* for more details.

key vulnerability metrics). With a longer rekey timeout interval, fewer Cisco Secure ACSs are required for the same number of users. Using the original factors for LEAP (above), but using a WEP key timeout of 4 hours (240 minutes) we get the following:

$N_{acs} = (150000/(1240*60))/(90*0.40)$

$N_{acs} = 0.056$

Number of Access Points

To determine the number of access points that a Cisco Secure ACS can manage, start with the assumption that each access point manages about ten WLAN users, then divide that number into the total number of users that can be supported by a Cisco Secure ACS – 21,000. With this formula we have 21,000 divided by 10 or 2100 access points that can be supported by one Cisco Secure ACS. This is the minimum number of access points that can be supported because not all access points will be supporting the maximum number of users at any one time.

Number of Network Access Servers

A Cisco Secure ACS can support up 5000 discrete[4]network access servers (NASs). This number can be increased by the use of the multi-NAS capability of an ACS.

Multi-NAS is a concept that allows one or more addresses to be configured for a given NAS entry. Using multi-NAS, the Cisco Secure ACS can support a theoretical maximum of 255 multiplied by 5000 discrete NAS equaling 1.275 million devices. However, a configuration of 1.275 million devices per Cisco Secure ACS is clearly not realistic. For each octet in the NAS IP address, there are three options:

– Number (ie: a specified number, such as 10.3.157.98)

– Numeric Range (ie: specified low and high numbers of the range in the octet, separated by a hypen, such as 10.3.157.10 – 50.

– Wildcard – An asterisk (*) is used to match all numbers in that octet, such as 10.3.157*.

LAN Versus WAN Deployment

The values calculated above do not take into account the network topology, particularly WAN latency and dependability. Depending on how critical wireless connectivity is to the organization (for example, maintaining connectivity for wireless cash registers in a store is very critical), we recommend that each wired LAN have at least one dedicated ACS. This can be mitigated by either using short, reliable WAN connections, or administratively reducing the degree critical connectivity for these remote devices; for example, meeting rooms where connection reliability is a convenience. A building may have 400 potential users and there may be a cluster of four buildings on the same subnet. One ACS assigned to this subnet will service 1600 users (about one tenth of the number of current users). Other buildings could be on adjacent subnets with reliable WAN connections. Cisco Secure ACSs on adjacent subnets could then be used as secondary systems for backup.

In the event that the WAN connections between buildings in this cluster are short, reliable, and pose no issue of network latency, all of these buildings an all the users can be serviced with two Cisco Secure ACSs. At 40 percent workload, one Cisco Secure ACS would take half of the access points as the primary server, and the other Cisco

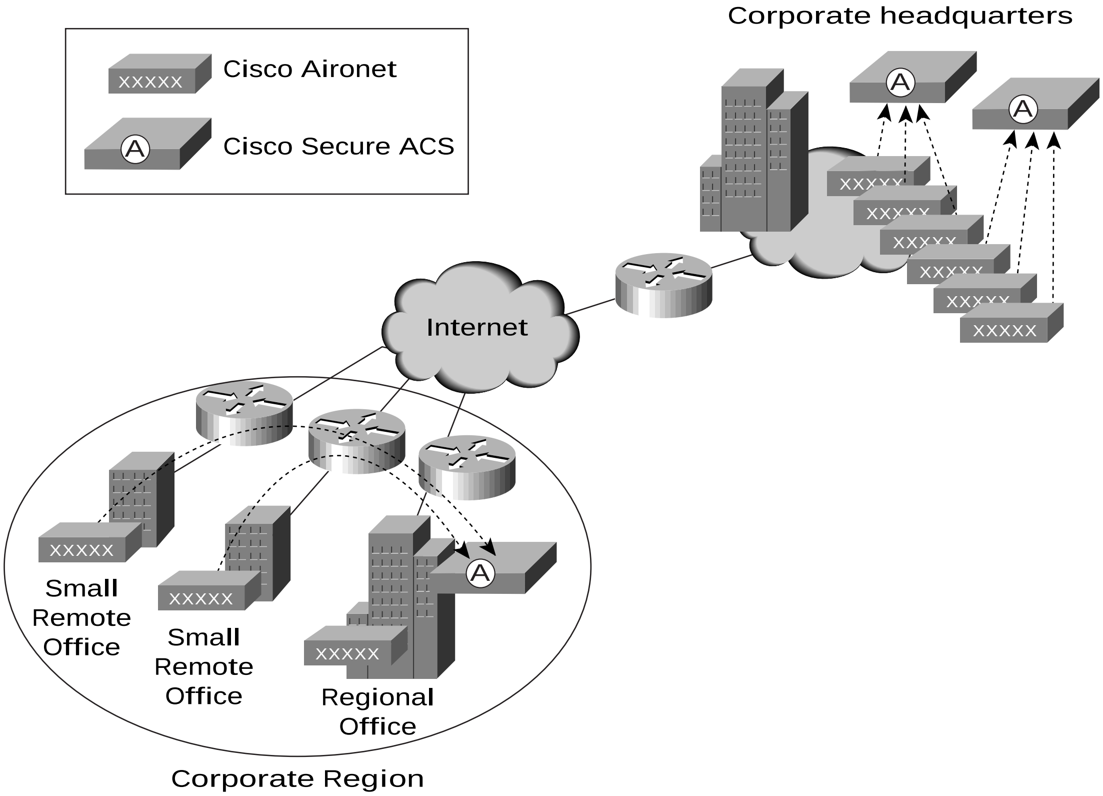
[4] A discrete NAS is a NAS entry configured with a single, non-wildcarded IP address.

Secure ACS would take the remaining access points. Each Cisco Secure ACS would provide backup for the other. Again, at 40 percent load, a failure of one Cisco Secure ACS would only create an 80 percent load on the other Cisco Secure ACS for the duration of the outage. In the case where the WAN is not suitable for authentication connections, we recommend using two or more Cisco Secure ACSs on the LAN in a primary or secondary mode or load balanced.

In the above case study, the 15,000 LEAP/EAP-TLS users will be distributed throughout customer's global network. The number of users at local sites will range from hundreds at the corporate headquarters to less than ten at remote offices. This poses some issues. Figure 1 illustrates one possible solution.

In a given geographical or organizational region, the total number of users may or may not reach a critical level for a Cisco Secure ACS. Small offices would not qualify for separate installations of Cisco Secure ACSs and a regional office may have sufficient reserve capacity. In this case, the small offices can authenticate users across the WAN to the larger regional office. Once again, we should determine that this does not pose a risk to the users in the remote offices. Critical connectivity needs to be assessed against the reliability and throughput to the central Cisco Secure ACS.

Figure 1 Cisco Secure ACS Placement in Regional Settings



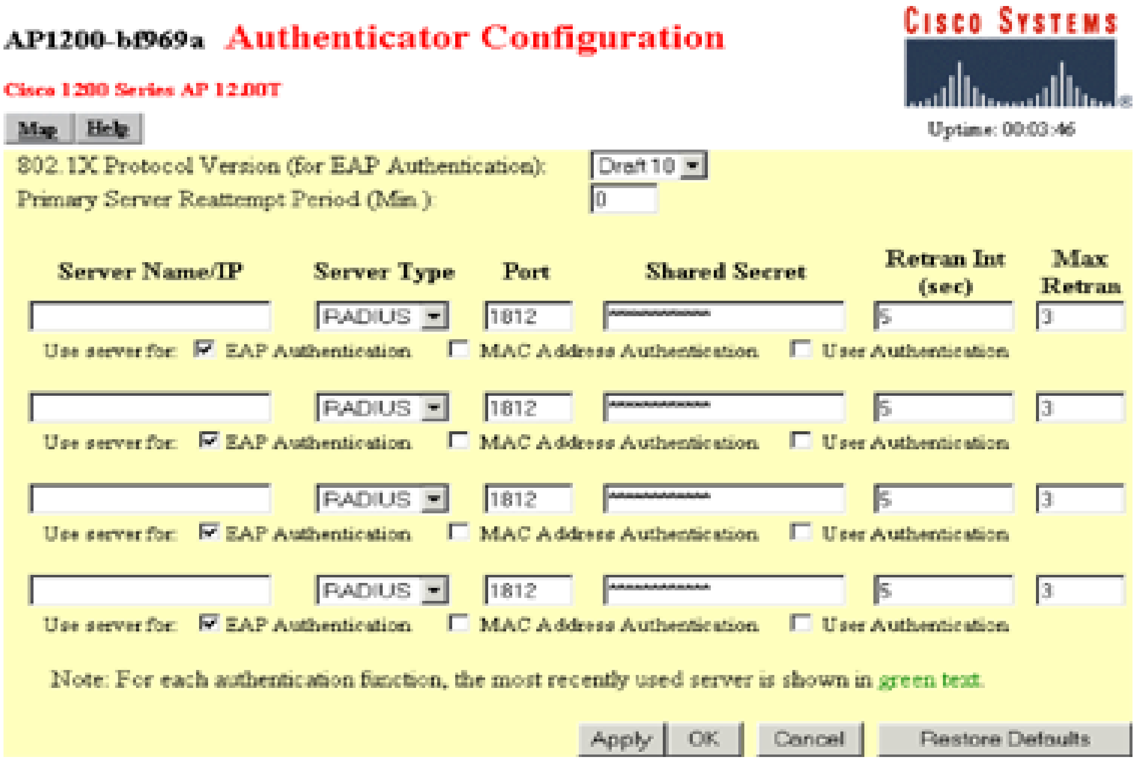
Load-Balancing and Failover

A network load-balancing device such as the Cisco Content Services Switch (CSS) or Cisco LocalDirector content switch can be employed to balance authentication requests between Cisco Secure ACSs. Cisco uses LocalDirector content switches for load balancing and failover for its wireless installation using Cisco Secure ACSs. However, the use of certain features such as accounting may render this approach impractical. It is better to use a simpler method to balance RADIUS traffic between Cisco Secure ACSs.

By convention, most RADIUS clients perform their own failover by maintaining a list of approved RADIUS servers. In the case of the Cisco Aironet access point, this list may contain as many as four RADIUS servers. If you set up more than one server for the same service, the first server in the list is the primary server for that service, and the other servers are used, in the order listed, when the previous server times out. If a backup server responds after the primary server fails, the access point continues to use the backup server for new transactions. Figure 2 shows the configuration window for RADIUS server configuration on the Cisco Aironet access point. Each access point must be configured to apply this failover capability.

Note: Though the example shows failover between sites, the best deployment would include local failover systems on the same LAN. This provides fast, reliable, authentication for the local network. Load balancing can be accomplished in the same manner.

Figure 2 RADIUS Server Configuration on the Cisco Aironet Access Point



AP1200-bf969a Authenticator Configuration

Cisco 1200 Series AP 12.00T

Uptime: 00:03:46

802.1X Protocol Version (for EAP Authentication): Draft 10

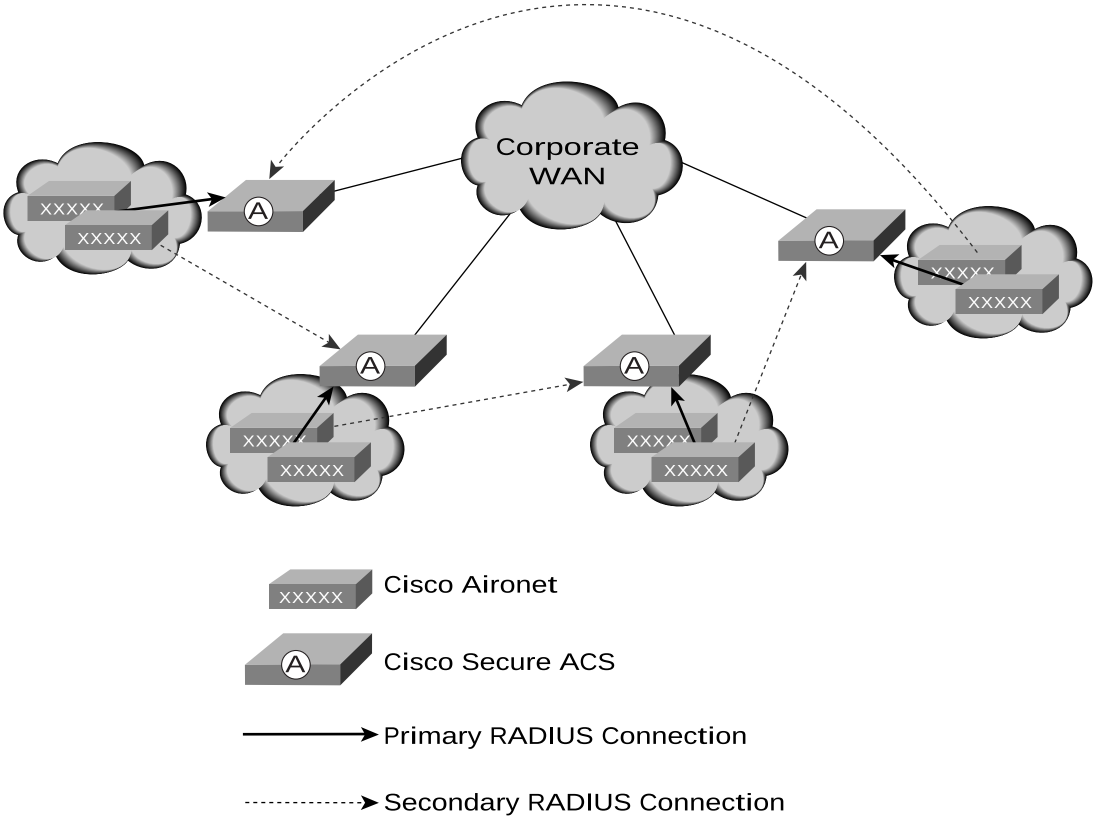
Primary Server Reattempt Period (Min.): 0

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran
	RADIUS	1812	************	5	3
Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication					
	RADIUS	1812	************	5	3
Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication					
	RADIUS	1812	************	5	3
Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication					
	RADIUS	1812	************	5	3
Use server for: ☑ EAP Authentication □ MAC Address Authentication □ User Authentication					

Note: For each authentication function, the most recently used server is shown in green text.

Load balancing on the Cisco Secure ACS is similarly simple. Divide the access points into the same number of groups that there are Cisco Secure ACSs within the local WAN. Point the primary RADIUS server configuration of each access point of each group to the nearest ACS. Point the secondary RADIUS server configuration to the next Cisco Secure ACS, and so on. Figure 3 shows this deployment.

Figure 3 Failover and Load Balancing of ACSs



Database Replication

Database replication replicates selected database information such as user and group information, from a primary Cisco Secure ACS to one or more Cisco Secure ACS backups or clients. Many aspects of system configuration (AAA client tables, groups/profiles, proxy settings, etc.) may be backed up to a secondary using replication. Replication enables the automatic creation of mirror Cisco Secure ACSs. These mirror systems can be used to provide backup redundancy servers, to increase fault-tolerance if the primary system fails. Because of this, the replicated data can be configured. The following aspects of replication are configurable with Cisco Secure ACS:

- Configuration components for replication—What is replicated
- Replication scheduling—When replication takes place
- Replication frequency—How often systems are replicated
- Replication partners—Which systems are replicated
- Client configuration—How the client is to be configured
- Reports and event (error) handling—What information to include in the logs

Some information cannot be replicated (such as IP pool definitions, Cisco Secure ACS certificate and private key files). Database replication does not cover the configuration of external authentication sources. This part of the configuration is not covered because the Cisco Secure ACS functionality relies on the installation of a number of communication dynamic link libraries (DLLs) – installation of these DLLs is determined manually by the system administrator for each case. Database Replication cannot rely on the necessary DLLs being present. Replication of these parts of the Cisco Secure ACS configuration must be done manually.

Caveats

- Any component designated to be replicated to or from another component will be completely overwritten in favor of the replicated component; that is, the replication may be characterized as being destructive master/slave. For example, if the Receive checkbox is selected for user and group database, any user records in the database prior to the replication will be lost when the other Cisco Secure ACS's user database is received.
- Database replication only achieves database synchronization by transforming the slave database into a copy of the master. The data flow in replication is one way and the data on the secondary is overwritten, as described above.
- During the replication process, the authentication service is halted briefly on each of the devices (although not at the same time). On the sender AAA server, service is halted only once at the beginning while the appropriate files and registry information are collated and prepared for sending. On the receiver AAA server, service is halted when the incoming file and registry set is restored. Service is normal while the replication set is being transmitted between servers.

Database Replication Test Results

A sample of the database replication test results is documented in Table 2. Four servers participated in the replication tests. The first three systems ("system 1," "system 2," and "system 3") were co-located in San Jose, California. The fourth system, "remote-server," was located in Netanya, Israel[5]. "System 1" was the primary sever. "System 1" was replicated to "remote-server" and to "system 2". "System 2" was configured to perform "cascade"[6]replication to "system 3". The user database consisted of 100,000 users in 500 user groups, and 5000 AAA clients (NASs). This scenario is represented in Figure 4.

The test results indicate that replication of a large internal database on the LAN takes from 1.5 to 2.0 minutes, while replication of the same database across a long WAN connection takes from 5 to 5.5 minutes. This indicates that when replicating over long distances, care must be made to design a system that minimizes the replication timeouts that

[5] The link between San Jose and Netanya is carried over a private, high-speed, dedicated circuit that passes through the United Kingdom.

[6] “Cascade” replication is where a secondary ACS server receives database replication from a primary ACS server and acts as a primary ACS server to replicate to other secondary ACS servers upon completion of its replication cycle with its primary.

occur during replication. In the case of the long WAN coverage, either system is actually "down"[7]only a short time. Most of the 5 plus minutes is taken up with "transport" time, which does not affect an ACS's ability to perform authentication.

Table 2 Table 2 Database Replication Test Results

	Date	Time	Message	Seconds
System 1	9/20/2002	13:40:22	Outbound replication cycle starting...	
	9/20/2002	13:45:36	Replication to ACS 'remote-server' was successful	314
	9/20/2002	13:45:36	Outbound replication cycle completed	
	9/20/2002	13:53:06	Outbound replication cycle starting...	
	9/20/2002	13:58:34	Replication to ACS 'remote-server' was successful	328
	9/20/2002	13:59:52	Replication to ACS 'System-2' was successful	78
	9/20/2002	13:59:52	Outbound replication cycle completed	
System 2	9/20/2002	13:59:02	Inbound database replication from ACS 'System 1' started	
	9/20/2002	14:00:15	Inbound database replication from ACS 'System 1' completed	73
	9/20/2002	14:00:15	Outbound replication cycle starting...	
	9/20/2002	14:01:57	Replication to ACS 'System 3' was successful	102
	9/20/2002	14:01:57	Outbound replication cycle completed	
System 3	9/20/2002	14:00:48	Inbound database replication from ACS 'System 2' started	
	9/20/2002	14:02:06	Inbound database replication from ACS 'System 2' completed	78

Note: Note: the link speed will affect the complete replication time. However, as stated above, the server is only unavailable while manipulating the database, not during transport. As a result, the transport time does not affect the availability of the server for authentication.

Replication Design

Because database replication in a Cisco Secure ACS is a "top down" approach, using the cascade method minimizes replication-induced downtime on the master server. If the master server is not used for authentication services, but for database maintenance only, the cascade method may not be as critical. However, when traveling across time zones, particularly international time zones, it may be necessary to consider using the cascade method going to remote secondaries. In this case, consider using *At specific times* versus *Automatically triggered cascade* (see Figure 5). This will allow "local" replication to take place during a time that will minimize the impact on user

[7] The server is "down" for authentication only during database changes. For the primary server, this occurs while reading the database and creation of the file used to transport the replicated data. For the secondary server, this occurs while reading the received file and writing to the database. This means that neither server is unavailable at the same time as the other.

authentication. During these long distance replications, replicating to the backup or secondary server first also helps reduce this impact. Figure 6 shows a hypothetical deployment for replication where each region has both a primary and a secondary Cisco Secure ACS deployed. In the scenario, replication is made to the secondary servers to avoid replication downtime to the primary.

Figure 4 Cisco Secure ACS Database Replication Scenario

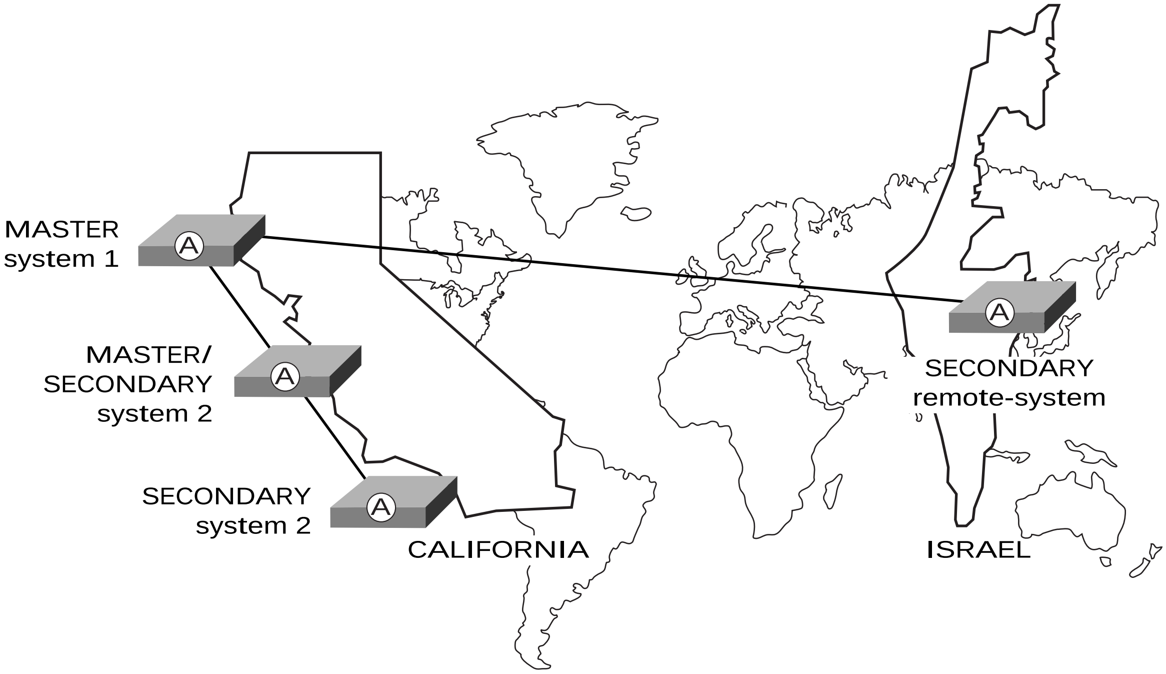
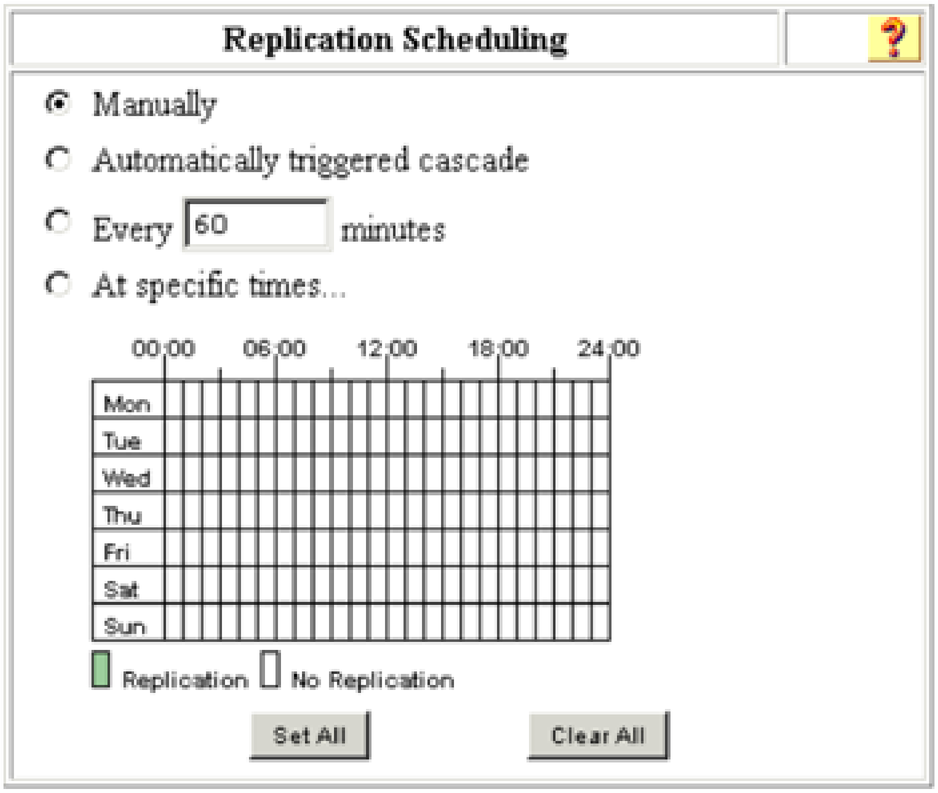


Figure 5 Cisco Secure ACS for Windows Database Replication Scheduling



Replication Scheduling

● Manually

○ Automatically triggered cascade

○ Every 60 minutes

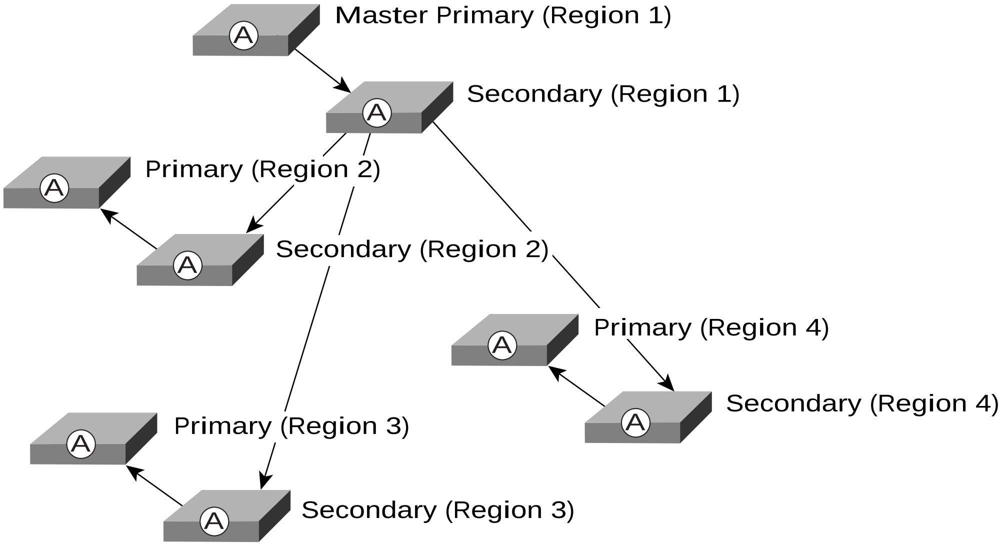
○ At specific times...

00:00 06:00 12:00 18:00 24:00

Mon
Tue
Wed
Thu
Fri
Sat
Sun

🟩 Replication □ No Replication

Figure 6 Cisco Secure ACS for Windows Database Replication Scheduling



An alternative to database replication is the use of Relational Database Management System (RDBMS) synchronization. The RDBMS Synchronization feature enables the updating of the Cisco Secure ACS user database with information from an Open Database Connectivity (ODBC)-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, Cisco Secure ACS reads the file or database via the ODBC connection. RDBMS synchronization supports addition, modification, and deletion for all data items it can access.

More information about RDBMS synchronization is available at:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs31/acsuser/s.htm#xtocid26

Design Implementation at Cisco—An Example

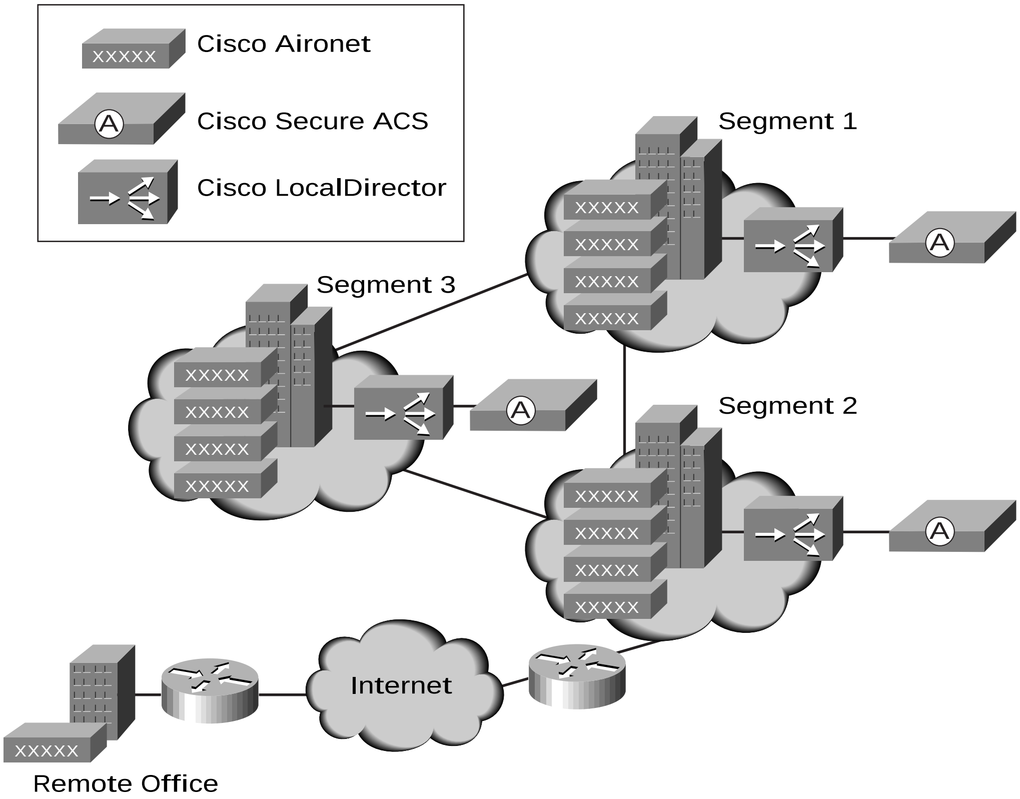
Cisco uses its own technology within its corporate network whenever possible. In the case of wireless technology, Cisco employs Cisco Aironet access points using the Cisco Wireless Security Suite to implement Cisco LEAP and pre-standard TKIP for secure authentication and encryption of all WLAN communication. Cisco Secure ACS is used to provide the RADIUS services required for LEAP. To provide some background and an example of a functioning Cisco Secure ACS deployment with Aironet wireless products, a brief discussion follows of how Cisco has implemented Cisco Secure ACS and Aironet products in its network.

At the Cisco main campus in San Jose, CA buildings are grouped into three segments. Each segment consists of 6 to 19 buildings and all the buildings in the segment are on a common LAN. Each building has six to eight WLAN access points per floor and all the access points in each building are on their own dedicated VLAN. All inter-building and inter-segment network connections use one-gigabyte fiber optic technology. Other Cisco campuses are similarly configured (Figure 7). All wireless connections are designated as secondary network access. Primary network access is through switch ports over wired Ethernet.

Cisco Secure ACS is used to provide LEAP authentication for the access points, and is configured to use Microsoft Active Directory for external database authentication. One Cisco Secure ACS is deployed for each segment of 6 to 19 buildings. A Cisco LocalDirector content switch is placed before each Cisco Secure ACS for load balancing and failover. All Aironet access points are configured with one RADIUS server and the LocalDirector content switch is used for failover. The LocalDirector is used because of the way the deployed version of access point software handles RADIUS failover[8]. As a result, Cisco is not currently using accounting on its wireless network.

[8] Earlier versions of the access point software had a problem with RADIUS failover. If failover occurred, the access point would not check to determine if the primary server was back online. It would remain on the secondary until it was manually reset or the secondary failed, forcing the access point to fail over to the next configured RADIUS server. This is not an issue with the current version of Aironet access point software. Cisco IT is studying the possibility of using the RADIUS client (access point) providing standard RADIUS fail over services (as in IOS) and utilizing accounting.

Figure 7 Cisco Systems Wireless Deployment



For small remote offices, the Cisco Wireless Security Suite provides LEAP and pre-standard TKIP across the WAN to the nearest major campus. Once again, because Cisco's current strategy is for wireless access to be a secondary means of network access, this does not cause a serious problem in the event of a WAN failure.

Recommendations for Cisco Secure ACS Installations with WLANs

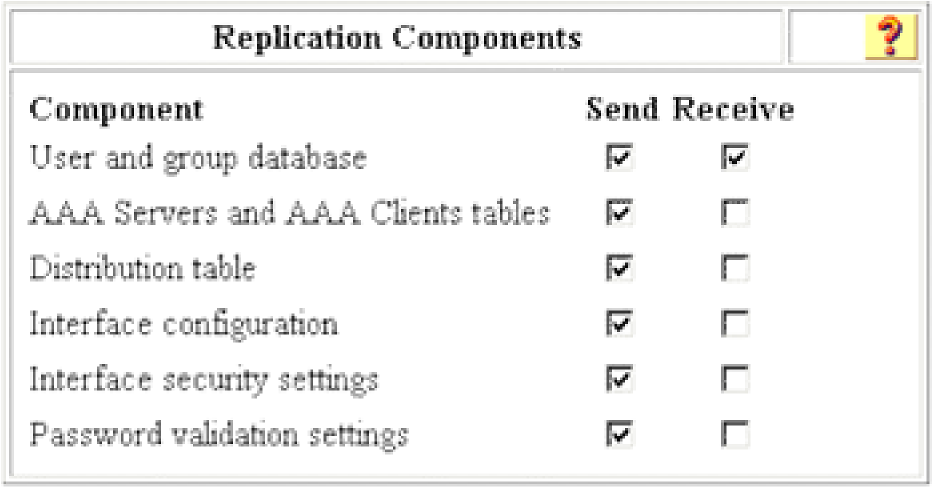
The following recommendations are made based on the current test data.

1. If wireless network access is designed to be a secondary means of accessing the network, a configuration using geographically remote Cisco Secure ACSs as secondary systems for failover authentication is acceptable. In addition, as with the Cisco scenario, remote Cisco Secure ACSs can be successfully used for small remote offices.
2. If wireless network access is designed to be the primary means of accessing the network (critical application), it is recommended that a primary Cisco Secure ACS be placed in each LAN, with consideration of a secondary Cisco Secure ACS at the same location.
3. If a customer will be using the Cisco Secure ACS internal database for user configuration, replication becomes critical factor. There may be issues with how to replicate certain information from the master to the secondary/ masters and out to the rest of the network. In some circumstances the customer needs to replicate user and network data, while in others only user information is to be replicated. Because of the flat nature of the replication

process, a master cannot specify individual replication types. When configured, the master can only replicate one configuration to all secondaries. Our suggestion here is to configure a specific master and secondaries to receive only user data and be the prime source of NAS and other information specific to that region (see Figure 8).

4. Plans must include the growth of wireless LAN deployments in large campuses. Additional Cisco Secure ACSs may need to be deployed. A customer can also consider going over the recommended 40 percent safe workload threshold; however, this may affect usage on the secondaries unless co-located secondaries are deployed. In this case, the only foreseeable benefit is that local authentication will proceed at LAN speeds in the event of failover. If the same Cisco Secure ACS is deployed as a regional or campus primary, better local authentication will be achieved for the served network.

Figure 8 Cisco Secure ACS for Windows Replication Components



Replication Components

Component	Send	Receive
User and group database	☑	☑
AAA Servers and AAA Clients tables	☑	□
Distribution table	☑	□
Interface configuration	☑	□
Interface security settings	☑	□
Password validation settings	☑	□

5. As the wireless user population grows and the distribution of users throughout the global network changes, customers may need to revisit their Cisco Secure ACS deployment strategies. As the user population starts to approach the possible 300,000 limit, performance may degrade. At this point additional memory may be needed (512 KB to 1 MB) on the deployed systems.
6. Using the Cisco Wireless Security Suite pre-standard TKIP to mitigate Wired Equivalent Privacy (WEP) weaknesses is recommended. To implement TKIP, Cisco Aironet wireless client cards are needed for all client devices.
7. Using the CiscoWorks 1105 Wireless LAN Solution Engine for the management of medium and large-scale Aironet deployments is recommended. In addition to providing centralized template-based configuration and firmware updates to facilitate changes on large numbers of access points, it also monitors Cisco Secure ACS LEAP authentication performance.

CISCO SYSTEMS

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

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

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

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco 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