Text Part Number: 78-5269-01 Rev. A0

Release Notes for Cisco User Control Point Version 1.0 (1)

These release notes provide new information that became available after the *Cisco User Control Point Software Installation Guide* and the *Cisco User Control Point Administrator Guide* were printed for Cisco User Control Point (UCP) Version 1.0 (1). Cisco strongly recommends that you review these release notes before installing the software.

This document contains the following sections:

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Obtaining Updated Software

New software or information might become available from Cisco Connection Online (CCO). The new software or information can be obtained at the following URLs:

```
http://www.cisco.com/cgi-bin/tablebuild.pl/ucp
```

and

```
ftp://ftp.cisco.com/cisco/internet/ucp
```

To access CCO, you must be a registered user. After entering your username and password, you will be prompted for an access code. Enter the following:

```
ucpft
```

The next page displays a list of files available for download.

Verifying Package Contents

The UCP package contains the following CD-ROMs:

- Cisco User Control Point
- Cisco Network Control Console
- ActiveWeb Information Broker

The contents of these CD-ROMs are described below. In addition to these 3 software CD-ROMs, there is also a Documentation CD-ROM included, which contains all of the published documentation for Cisco User Control Point as well as other Cisco products.

Contents of the Cisco User Control Point CD-ROM

The contents of this CD-ROM must be installed on a Sun workstation running Solaris 2.5.1. The Cisco User Control Point CD-ROM contains two files: ucp.tar and ucp.txt. The ucp.tar file contains packages for the following:

- UCP UNIX components
- CiscoSecure ACS
- CiscoSecure GRS

The ucp.txt file contains instructions to offload the software to a local disk and begin installation.

Cisco strongly recommends that the contents of this CD-ROM be installed on a machine with the base version of Solaris 2.5.1, with the Solaris patches required for CiscoSecure ACS, which are 103566-25, 103600-18, and 103640-14. Do not install the Solaris patch cluster recommended by Sun. UCP is not supported on a platform with the Sun-recommended Solaris patch cluster.

Note Cisco strongly recommends that the UCP UNIX components be installed in the default directory (/opt/ncp).

Contents of the Cisco Network Control Console CD-ROM

The contents of this CD-ROM must be installed on a Windows NT platform. The Network Control Console installation can be started by clicking the NCC.Setup.exe file. For detailed installation instructions, refer to the *Cisco User Control Point Software Installation Guide*.

Contents of the ActiveWeb Information Broker CD-ROM

The contents of this CD-ROM must be installed on a Sun workstation running Solaris 2.5.1. The ActiveWeb Information Broker CD-ROM contains two files: aw.tar and aw.txt. The aw.tar file contains ActiveWeb 2.1b software including Patch #7. The aw.txt file contains instructions to offload the software to a local disk and begin installation. For detailed installation instructions, refer to the *Cisco User Control Point Software Installation Guide*.

ActiveWeb Patch

After installing ActiveWeb 2.1b, you must apply the ActiveWeb patch (21p7dom.tar.Z).

To apply the ActiveWeb patch, follow these steps:

Step 1 Become superuser on the machine.

Step 2 Stop the broker by entering:

```
/opt/active/bin/S45broker stop
```

Step 3 Change to the /opt/active directory.

Step 4 Copy the extracted patch file (21p7dom.tar.Z) to this directory.

Step 5 Extract the tar file by entering:

```
zcat 21p7dom.tar.Z | tar xf-
```

This will update the necessary binaries and libraries.

Step 6 Start the broker by entering:

```
/opt/active/bin/S45broker start
```

Corrections to the Cisco User Control Point Documentation

This section contains information that became available after the *Cisco User Control Point Software Installation Guide* was issued.

Starting and Stopping the Master Daemon

The command to start or stop the master daemon contains no spaces:

```
S97MasterDaemon
```

It is not correct to use `S97 MasterDaemon`.

Configuring and Starting the Database Adapters

The heading on page 2-22 should read “Configuring and Starting the DS and SMS Database Adapters.”

In Step 3 on page 2-24, for Broker Host, enter the host name or the IP address of the machine running the Standard Broker.

Configuring and Starting the UCP DS Adapter

After Step 5 on page 2-32, continue configuration as follows:

Select LIBDBIPAddr and enter the IP address of the host running CiscoSecure ACS dbServer. If dbServer is running on the same machine as the DSAdapter, enter 0.0.0.0

Configuring PGS for Domain Checking

After Configuring the PGS for Dynamic IP Allocation on page 2-42, configure PGS for domain checking by following these steps:

Step 1 In the Protocol Gateway Properties sheet, click the **Specific** tab.

Step 2 Go to the **GRS** section, and set **RoamingDomainChecking** to 1.

Step 3 Go to the **GRSAccountingRequester** section.

Step 4 In the **primaryserver** parameter, specify the accounting port number and the host name of the GRS server. For example:

```
1846 grs-ultra
```

Step 5 Go to the **GRSRequester** section.

Step 6 In the **primaryserver** parameter, specify the RADIUS port number and the host name of the GRS server. For example:

```
1845 grs-ultra
```

Step 7 Click the **Domains** tab.

Step 8 Click the **New** button, and enter all domains the PGS will proxy.

Note The known clients of the PGS must contain the host names or IP addresses and the shared secret of servers running GRS.

Additional Information Updates

The following items are not described in the published Cisco User Control Point documentation:

- A new IPPoolID feature allows PGS to use NASIPAddress as a key to lookup IPPoolID from the KnownClients table. This allows multiple NASes in different subnets to send requests to a single PGS.
- IPPoolID is supported for Groups (in the CiscoPrivate dictionary under Reply_Attributes). If specified for Group, users in that group do not require it and the Group value overrides the user value.
- The UCP kernel supports a new adaptive round-robin algorithm for load balancing and failover and is effective for PGS to GRS, PGS to AAA, PGS to DHCP, TS to Cache, and Local Cache to Mother Cache interactions.
- A user can be deleted from the CiscoSecure ACS user interface.

Note This does not update the SMS database and will cause the databases to be out of sync. This feature should only be used if there is no SMS interface.

- Data Store enforces the user MaxSessions range between 1 and 50.
- In NCC, DNS ServiceTerminate is set to -1, meaning that a "kill -9"' should not occur if it fails to stop in a few seconds. Depending on the size of the database files, DNS might take up to a minute to stop. If it does not stop after a few minutes, it will need to be manually killed.
- Several utility programs are located in the /opt/ucp/utils directory. You can include this directory in the default path. This directory contains cdump, esnoop (event snooper), accttool (test tool for accounting parser), netflowtool (test tool for netflowparser), and dbtool (an interactive utility for verification and querying the DS).

Storage Mechanisms in the Information Brokers

The Information Broker uses three different storage mechanisms for queuing events:

- Volatile
- Persistent
- Guaranteed

Volatile storage is memory-based; it is fast but vulnerable to power and other failures. This is used for non-critical events, such as Heartbeats from UCP services.

In persistent storage, the broker uses operating system asynchronous I/O to write events to disk. This is used for events that should not be lost. For example, if a UCP service is stopped, all persistent events that it subscribes to are queued in the broker's persistent storage. When the service restarts, the queued events are delivered. In UCP, persistent storage is used for events that involve data transfer to mother caches, IP address assignment and revocation, and RADIUS accounting.

Guaranteed storage uses a two-phase commit process to store events on disk. It is extremely reliable, but very slow. UCP does not use guaranteed storage.

Managing Persistent Queues

ActiveWeb Brokers allocate a fixed file size (currently 256 MB) for persistent events. If not properly managed, this file can fill to capacity. If the file fills up, it must be removed and the broker must be restarted.

Managing Persistent Queues requires some understanding of the behavior, particularly in a test environment, when services are constantly started and stopped or new installations are made.

Each service obtains a persistent client ID from the broker and writes it in its configuration file. On a restart, this client ID is used to reconnect to the original queue.

There might be times, particularly in a test environment, when an existing client ID should be destroyed in order to ensure a clean start. These include:

- When a new release is installed for testing and a cold start of all clients is desired
- When a UCP service is deleted from the NCC

For example, if a UCP service is deleted from NCC, the broker still retains the client ID used by the deleted service. If the client ID is not deleted, the Information Broker continues to queue events for this service, and obsolete or unwanted events consume available broker storage space. Because this might adversely affect the broker's functionality, delete the client IDs of deleted services.

ActiveWeb's Manager utility can be used as follows to delete existing client IDs:

Step 1 Start the ActiveWeb manager utility on any machine where ActiveWeb is installed. Change to the ActiveWeb directory (default: /opt/active/bin) and enter the following:

```
./manager &
```

The manager window appears.

Step 2 Select the host where the broker is running by double-clicking it in the left frame of the manager window.

Step 3 Select the broker to which the service is connected by double-clicking the broker name.

Note Delete clients from the InterComponent and DataTransfer Brokers. You may not need to delete clients from the Heartbeat Broker.

Step 4 Click the **Clients** tab.

Information Broker clients appear in the right frame of the manager utility.

Step 5 Select the client that needs to be deleted.

Note The Group for the client should be Persistent and the Connected status should be No.

Step 6 Click **Delete**.

Assigning NAS-Based IP Pools

A new IPPoolID feature allows PGS to use NASIPAddress as a key to look up IPPoolID from the KnownClients table. To support this feature, the IPPoolID field was added to the PGS Valid Clients table. Under this scenario, the IPPoolID specified in user profile is ignored. This feature is recommended if multiple NASes under different subnets send requests to a single PGW.

There is also a new PGS configuration item: IPPoolBasedOnNASIP. If set to 0, it uses the original design to select the user profile IPPoolID. If set to 1, it uses NAS-Based IPPoolID.

Note If PGS is specified to use IPPoolBasedOnNASIP, and NCC Valid Clients do not specify a IPPoolID for a NAS, PGS will not consider that NAS a valid client.

Adaptive Round-Robin Load Balancing

The UCP kernel has a new adaptive round-robin algorithm for load balancing and failover and is effective for PGS to GRS, PGS to AAA, PGS to DHCP, TS to Cache, and Local Cache to Mother Cache interactions. These are used only by services that use a requester to obtain service from a server. The new configuration items for this are:

```
[NCP]
TicketsPerService = 100
TimeToDetectDeadService = 10
RoundRobinToExternalService = 1
```

TicketsPerService directly determines the round robin cycle time depending on the incoming packet load. This number should not be too large or too small. The default value (100) is recommended.

NCC supports PrimaryServer and SecondaryServer. Additional servers can be specified as “ExternalServer1” to “ExternalServerN” by adding new key/value items in the appropriate requester sections of a service.

Sample DHCP Configuration File (dhcpd.conf)

```
#
# Note that lines beginning with ‘#’ are comments.
#
# Hosts with more than one interface MUST specify a ‘‘server-identifier’’, which
# should be the IP address of the server’s primary network interface, or if there
# is no interface that can be described that way, at least an interface whose
# address isn’t likely to change.

server-identifier chandrup-ultra.cisco.com
option domain-name “cisco.com”;
option domain-name-servers malibu.cisco.com

# Shared network declaration is used to group subnets which share the same
# physical network together. The name is specified so that the shared network can
# be referred to in log messages - it serves no other function.

shared-network CISCO{

# option definitions common to this shared network.
option subnet-mask 255.255.255.224;
default-lease-time 600;

# the time should be the length in seconds that will be assigned to a lease if
# the client requesting the lease # does not ask for a specific expiration time.

max-lease-time 7200;

# One of the two IP subnets that share this physical network. Address ranges can
# be specified for each subnet attached to a shared network. Since these
# subnets share the same physical network, addresses are pooled together, and
# assignments are made without regard to the actual subnet. If the optional
# dynamic-bootp keyword is given in the address range declaration, then addresses
# in that range can be assigned either with the DHCP protocol or the BOOTP
# protocol. Otherwise, only DHCP clients will have addresses allocated from
# the address range. Note that each IP subnet can have its own options specific
# to that subnet. Options that aren’t specified in the subnet are taken from
# the shared network (if any) and then from the global option list.

subnet 204.254.239.0 netmask 255.255.255.224 {
range 204.254.239.10 204.254.239.20;

# The range statement gives the lowest and the highest IP addresses in a
# range. Addresses are dynamically allocated from this range of IP
# addresses

option broadcast-address 204.254.239.31; option routers prelude.fugue.com;
  }
```

```
# The other subnet that shares this physical network

subnet 204.254.239.32 netmask 255.255.255.224 {
   range dynamic-bootp 204.254.239.10 204.254.239.20;
   option broadcast-address 204.254.239.31;
   option routers snarg.fugue.com;
  }
}

# IP subnets that are alone on their physical wire should be declared by
# themselves. ISC dhcpd may still refer to them as shared networks in
# log messages, but this is simply an artifact of the underlying data
# structures. Note that options can be specified in the subnet declaration
# which supersede the global options specified earlier.

subnet 192.5.5.0 netmask 255.255.255.224 {
   range 192.5.5.26 192.5.5.30;
   option name-servers bb.home.vix.com, gw.home.vix.com;
   option domain-name “vix.com”;
   option routers 192.5.5.1;
   option subnet-mask 255.255.255.224;
   option broadcast-address 192.5.5.31;
   default-lease-time 600;
   max-lease-time 7200;
}

# Hosts which require special configuration options can be listed in host
# statements. If no address is specified, the address will be allocated
# dynamically (if possible), but the host-specific information  will
# still come from the host declaration.

host passacaglia {
   hardware ethernet 0:0:c0:5d:bd:95;
   filename “vmunix.passacaglia”;
   server-name “toccata.fugue.com”;
}

# Fixed IP addresses can also be specified for hosts. These addresses should
# not also be listed as being available for dynamic assignment. Hosts for which
# fixed IP addresses have been specified can boot using BOOTP or DHCP. Hosts
# for which no fixed address is specified can only be booted with DHCP, unless
# there is an address range on the subnet to which a BOOTP client is connected
# which has the dynamic-bootp flag  set.

host fantasia {
   hardware ethernet 08:00:07:26:c0:a5;
   fixed-address fantasia.fugue.com;
}

# If a DHCP or BOOTP client is mobile and might be connected to a variety of
# networks, more than one fixed address for that host can be specified. Hosts
# can have fixed addresses on some networks, but receive dynamically allocated
# address on other subnets; in order to support this, a host declaration for
# that client must be given which does not have a fixed address. If a client
# should get different parameters depending on what subnet it boots on, host
# declarations for each such network should be given. Finally, if a domain
# name is given for a host’s fixed address and that domain name evaluates to
# more than one address, the address corresponding to the network to which the
# client is attached, if any, will be assigned.
```

```
host confusia {
   hardware ethernet 02:03:04:05:06:07;
   fixed-address confusia-1.fugue.com, confusia-2.fugue.com;
   filename “vmunix.confusia”;
   server-name “toccata.fugue.com”;
}

host confusia {
   hardware ethernet 02:03:04:05:06:07;
   fixed-address confusia-3.fugue.com;
   filename “vmunix.confusia”;
   server-name “snarg.fugue.com”;
}

host confusia {
   hardware ethernet 02:03:04:05:06:07;
   filename “vmunix.confusia”;
   server-name “bb.home.vix.com”;
}

# The group statement is used to apply one or more parameters to a group of
# declarations. It can be used to group hosts, shared networks, subnets or
# even other groups. Imagine that you have a site with a lot of NCD X-Terminals.
# These terminals come in a variety of  models, and you want to specify the boot
# files for each models. One way to do this would be to have host declarations
# for each server and group them by model:

group {
   filename “Xncd19r”; next-server ncd-booter;
   host ncd1 { hardware ethernet 0:c0:c3:49:2b:57; }
   host ncd4 { hardware ethernet 0:c0:c3:80:fc:32; }
   host ncd8 { hardware ethernet 0:c0:c3:22:46:81; }
}

group {
   filename “Xncd19c”;
   next-server ncd-booter;

   host ncd2 { hardware ethernet 0:c0:c3:88:2d:81; }
   host ncd3 { hardware ethernet 0:c0:c3:00:14:11; }
}

group {
   filename “XncdHMX”;
   next-server ncd-booter;

   host ncd1 { hardware ethernet 0:c0:c3:11:90:23; }
   host ncd4 { hardware ethernet 0:c0:c3:91:a7:8; }
   host ncd8 { hardware ethernet 0:c0:c3:cc:a:8f; }
}
```

Options

The other options that can be specified in the configuration file are:

```
option  domain-name                     “cisco.com”
option  client-identifier               “CLIENT-FOO”
(or)
option  client-identifier               43:4c:49:45:54:2d:46:4f:4f;
option  subnet-mask                     ip-address;
option  time-offset                     nt32;
option  routers                         ip-address [, ip-address ...];
option  time-servers                    ip-address [, ip-address ...];
option  name-servers                    ip-address [, ip-address ...];
option  domain-name-servers             ip-address [, ip-address ...];
option  log-servers                     ip-address [, ip-address ...];
option  cookie-servers                  ip-address [, ip-address ...];
option  lpr-servers                     ip-address [, ip-address ...];
option  impress-servers                 ip-address [, ip-address ...];
option  resource-location-servers       ip-address [, ip-address ...];
option  host-name                       string;
option  boot-size                       uint16;
option  merit-dump                      string;
option  domain-name                     string;
option  swap-server                     ip-address;
option  root-path                       string;
option  ip-forwarding                   flag;
option  non-local-source-routing        flag;
option  policy-filter                   ip-address ip-address [, ip-address ...];
option  max-dgram-reassembly            uint16;
option  default-ip-ttl                  uint8;
option  path-mtu-aging-timeout          uint32;
option  path-mtu-plateau-table          uint16 [, uint16 ....]
option  interface-mtu                   uint16;
option  all-subnets-local               flag;
option  broadcast-address               ip-address;
option  perform-mask-discovery          flag;
option  mask-supplier                   flag;
option  router-discovery                flag;
option  router-solicitation-address     ip-address;
option  static-routes                   ip-address  ip-address [, ip-address ...];
option  trailer-encapsulation           flag;
option  arp-cache-timeout               uint32;
option  ieee802-3-encapsulation         flag;
option  default-tcp-ttl                 uints;
option  tcp-keepalive-interval          uint32;
option  tcp-keepalive-garbage           flag;
option  nis-domain                      string;
option  nis-servers                     ip-address [, ip-address ...];
option  ntp-servers                     ip-address [, ip-address ...];
option  netbios-name-servers            ip-address [, ip-address ...];
option  netbios-dd-server               ip-address [, ip-address ...];
option  netbios-node-type               uint8;
option  netbios-scope                   string;
option  font-servers                    ip-address [, ip-address ...];
option  x-display-manager               ip-address [, ip-address ...];
option  dhcp-client-identifier          data-string;
```

Caveats

This section lists the known problems with UCP and possible workarounds for these problems.

The DSAdapter Does Not Start

The DSAdapter will not start if the UCP installation directory is other than the default (/opt/ncp). UCP UNIX components must be installed in this directory.

Loss of Events During Data Transfer

During bulk transfer of 150,000 user profiles or more, there might be some loss of events (approximately 5 out of 150,000). Although all user profiles usually propagate to the Data Store, some profiles might not propagate to the caches. The workaround is to selectively "update" the user profiles that did not propagate to the caches to trigger their transfer. [CSCdk22457]

Use the cdump utility in the /opt/ncp/utils directory to get the count of user profiles in the master cache. If user profiles are missing from the cache, follow these directions to locate and transfer user profiles that did not propagate.

Step 1 Using SQL*Plus, execute the following SQL statements to dump all the usernames to a file from the Data Store:

```
SQL> SPOOL /tmp/ds.out
SQL> SELECT user_name FROM cd_user_profile WHERE user_name NOT LIKE 'SERVER%'
AND user_name NOT LIKE 'NAS%' AND user-name NOT LIKE 'DICTIONARY%' AND user_name
NOT IN ('superuser', 'unknown_user');
```

Step 2 Edit the /tmp/ds.out file to remove all lines that do not contain usernames.

Step 3 Sort the file as follows:

```
Unix% sort /tmp/ds.out > ds.out.sorted
```

Step 4 Using SQL*Plus, connect to the SMS database and execute the following SQL statements to dump all the usernames to a file:

```
SQL> SPOOL /tmp.sms.out
SQL> SELECT fqdn FROM ncptransfer WHERE AccountStatus=1073741824;
```

Step 5 Sort the file as follows:

```
Unix% sort /tmp/sms.out > sms.out.sorted
```

Step 6 Use the cdump utility in the /opt/ncp/utils directory to dump all the usernames from the master cache:

```
cdump -1 > /tmp/cdump.out
```

Step 7 Use the UNIX utility diff as follows to see any differences in the output from the cache, the Data Store, and the SMS:

```
Unix% diff -b /tmp/sms.out.sorted /tmp/ds.out.sorted
Unix% diff -b /tmp/ds.out.sorted /tmp/cdump.out
```

Step 8 For all the profiles that are missing from the Data Store or the cache, do an "update" propagation from the SMS as follows:

```
SQL> UPDATE NCPTransfer SET AccountStatus = 536870912 WHERE fqdn = 'user-name';
SQL> COMMIT;
```

Data Transfer Fails if the DSAdapter or the SMSAdapter is Down

Data does not propagate if the DSAdapter or the SMSAdapter is down. Also, if any of these services fail during bulk transfer, user profiles will not propagate to the Data Store or the Caches. The workaround is to execute the bulk transfer again or selectively update the user profiles in the SMS database as mentioned in the previous section [CSCdj74071]

Netsys and Oracle Must Be Installed on Different Servers

Installing Netsys and Oracle on the same server can result in unpredictable behavior. For more information, refer to the Netsys documentation.

NSII Doesn’t Stop Netsys Daemons

The Netsys Information bus Interface (NSII) process does not terminate all Netsys processes when Netsys is stopped from the NCC.

This problem does not affect the functionality of the UCP system. [CSCdj76170]

DHCP Slow to Send First Heartbeat

The DHCP service stores its data in the leasedb file. If its leasedb is large, it might take several minutes for DHCP to start and send a heartbeat. This late heartbeat might mislead administrators to think the service did not start correctly. [CSCdj91186]

Shell User Not Supported

Shell users are not supported by this release of UCP. Every user is required to have a Framed-Address attribute defined for it. The Framed-Address field should either contain a valid static IP address or the value 255.255.255.254, indicating that a dynamic IP address is required.

Deletion of a NAS Client

Although the NCC is informed of a NAS deletion when deleted from the CiscoSecure interface, it must be manually deleted from the NCC, and PGS will need to be restarted.

Loss of Events

A service might lose events (in queue and in processing) if a crash occurs or a service is stopped.

Broker Storage Problem

If any unconnected Persistent Queue is present, the broker persistent file will eventually grow to its maximum capacity of 256 MB.

To work around this problem, run the broker manager after restarting any service and delete any unconnected Persistent Queues. [CSCdk00220]

Exception Events by the DSAdapter

The DSAdapter does not publish an exception event when a user profile is added to a group that is not in the Data Store. However, an error is logged in the DSAdapter log file (default: /tmp/dsadapter.log), and the user profile is not added to the Data Store. The workaround is to ensure that all groups exist in the Data Store, before any user profiles are added under them. [CSCdk17846]

Client ID in AWAD Configuration

The Client ID field in the ActiveWeb Access Adapter (AWAD) configuration tab in the NCC should never be modified. If the Client ID field is modified, the AWAD will not connect to the broker. Consequently, the NCC will not receive any heartbeat events. [CSCdk18307]

NCC Shows Incorrect Shared Network Information

If Shared Networks are added or deleted in the DHCP configuration file (dhcpd.conf), the NCC displays the shared network information incorrectly. There is no adverse functional impact on the system. DHCP continues to behave correctly. [CSCdk22527]

Inheritance of HomePoPID Attribute

Group inheritance of the HomePoPID is not supported. Each user must have a HomePoPID specified in its profile. This is enforced by SMSAdapter during data transfer. If this attribute is not present in the user profile, PGS will drop AAA reply packets.

Translation Server Does Not Recognize a Restarted Cache

If a local cache is stopped and restarted, the translation server does not recognize it. To work around the problem, start two local caches. If one of the local caches is stopped and restarted, the translation server will continue to communicate with the second cache. [CSCdk26417]

User Log-On Race Condition

Some race conditions exist due to latency and the distributed nature of transactions. These include:

- If the same user logs on from two different NASes or PoPs within 2 seconds (the PGS event buffering interval), that user will be assigned the same session number. Consequently, the system will permit over-subscription and the user will have two active sessions while the system records 1. However, the two IP addresses will be recorded by the mother cache and freed appropriately.

  This scenario is unlikely.

- If a user logs off and on (new access-request) within 2 seconds, the events might be received out of order by the cache. Consequently, the cache might record the new access-request as a new session because the other session is still active and if maxsession is set for 1, the second request will be rejected.

  Because a delay will be introduced by modems, dialers, the NAS, or the user typing a password, this scenario is also unlikely.

- If a user logs on within 1 second after logging off, the session state or the IP address might be inconsistent in the mother and local caches.

Incorrect User Session Information in the Caches

There are two scenarios where a cache might contain incorrect session information for a user:

- If the Information Broker crashes, and a user logs out before the Information Broker recovers, caches will continue to maintain the state of the user session as logged on. The IP address that was assigned to the user session will not be revoked.
- If a NAS crashes, it will not send Accounting-Stop packets to UCP for all the sessions that were active when it crashed. The caches will continue to maintain the state of these sessions as logged on. The IP addresses that were assigned to these sessions will not be revoked. [CSCdk24273]

Static IP Address Not Dynamically Updated in DNS

The IP addresses of users with Static IP are not dynamically updated in DNS. These need to be added manually to the DNS db zone files. [CSCdj91479]

Troubleshooting Tips and Hints

Deployment of the UCP system involves installation of several software packages on UNIX and Windows platforms. All components must be configured correctly and installed in the correct order for the UCP system to function predictably.

This section provides troubleshooting tips and hints to resolve problems that might have been caused by improper configuration.

CiscoSecure ACS Does Not Start Successfully

Step 1 Verify that the Translation Service (TS) and DSdbAdapter are running before starting the CiscoSecure ACS. When the CiscoSecure ACS starts, you should see profile request/reply events in the ActiveWeb monitor. If the TS needs to be restarted, you might need to change its listening port number (and the corresponding port in acs/CSU/libdb.conf) before restarting. The present port might require up to 2 minutes to become available again.

Step 2 Verify that the number of threads (NumThreads) defined in Translation Service configuration is greater than the number of connections (MaxConnection) defined in /opt/acs/CSU/libdb.conf.

Step 3 Make sure no CiscoSecure ACS processes are running before starting the CiscoSecure ACS.

Step 4 Ensure that the system library, /usr/lib/libresolv.so.2, is present.

Step 5 Look for the following log message:

```
Starting CiscoSecure Processes:
<various servers started...>
ld.so.1: sh: fatal: libw.so.1: can't open file: errno=24
```

If this message appears, make sure fewer than 40 database connections were specified during installation by checking the DB Server Connections entry in the /tmp/cs_install.log file. Cisco recommends no more than 35 database connections.

CiscoSecure ACS Cannot Connect to Database

Step 1 Check the TS log in /tmp/transserv.log to make sure there is no port binding error. The TS listening port should be the same as the value in /opt/acs/CSU/libdb.conf.

Step 2 Make sure there is a server profile defined.

Step 3 If the DSdbAdapter does not receive the PseudoProfileRequest event from the TS when CiscoSecure ACS starts, then stop and restart the ActiveWeb Oracle dbAdapters.

Translation Server Fails to Restart

If the translation server cannot restart after a port binding error, make sure the tcp_close_wait_interval is set to 5 seconds on the machine running the translations server.

To set the tcp_close_wait_interval to 5 seconds, enter the following:

```
ndd -set /dev/tcp tcp_close_wait_interval 5000
```

Authentication Fails

If you see CiscoSecure ACS log files containing an error message “Invalid Attribute 9,140....”, make sure the NAS has the correct NAS dictionary (NCP-vIP-new).

NCC Does Not Start Successfully

Ensure there are no NCC processes running. You must stop all existing NCC processes (Ncc.exe, NccCalc.exe, and Awad.exe) before starting the NCC.

Data Transfer Fails

Step 1 Ensure that the SMSAdapter configuration contains the correct DSAdapter GUID.

Step 2 Ensure that the Group the user belongs to exists in the Data Store. You must define the Group through the CiscoSecure ACS interface before adding users to that group.

Step 3 Check NCC exceptions.

Step 4 Check the SMSAdapter log file to see if the user profile was dropped by SMSAdapter. The log file exists as /tmp/smsadapter.log by default. You may have to turn logging “on” by modifying the SMSAdapter configuration in NCC.

Step 5 Check the DSAdapter log file to see if the user profile was dropped by the DSAdapter. By default, the file exists as /tmp/dsadapter.log. You might have to turn logging “on” by modifying DSAdapter configuration in NCC.

Note The group name is case-sensitive.

Step 6 Ensure all attributes in the user profile exist in the CiscoSecure ACS dictionary and have valid data types.

Step 7 Ensure that the attribute, Home-Pop_ID, is contained in the user profile and has the correct POP name. The user profile might not flow to the POP-level cache if the value of the Home-Pop-ID attribute in the user profile does not match the PopName parameter in the POP-level cache’s configuration.

Note The POP name is case-sensitive.

Step 8 Ensure that the following services are running before transferring data:

- DSAdapter
- SMSAdapter
- SMSdbAdapter (ActiveWeb dbAdapter)
- DSdbAdapter (ActiveWeb dbAdapter)
- Mother Cache(s)
- POP-level cache(s)

Step 9 Ensure that the CiscoSecure ACS is correctly installed or mounted on the machine running the DSAdapter.

Step 10 If all configuration parameters seem correct and user profiles still do not transfer, then stop and restart all pertinent services.

User Does Not Get IP Address

Step 1 Ensure that the IP-Pool-ID attribute defined in the user profile is consistent with the DHCP configuration in dhcpd.conf.

Step 2 The Protocol Gateway Service (PGS) is designed to drop the packet if it requests a dynamic IP address from the DHCP and the IP-Pool-ID subnet is not defined in the dhcpd.conf file.

Dynamic IP Addresses

Step 1 Assign the value 255.255.255.254 to the Framed-Address attribute, along with the right IP-Pool-ID for all users who will be assigned Dynamic IP addresses.

Step 2 Make sure a subnet is defined in the DHCP lease configuration file, dhcpd.conf, corresponding to the IP-Pool-ID.

Next-Session-ID

The attribute, Next-Session-ID, must not be configured as a part of user profiles. This attribute is used for internal communication between UCP services.

DHCP IP-Revocation Logging

If you want to see the freeIP information when the dhcpd daemon revokes IP addresses, set DumpServiceAdapter = 1 in the DHCP configuration through the NCC.

CiscoSecure ACS Tries to Authenticate “unknown user”

This is actually a CiscoSecure ACS feature that should be turned off in the UCP environment. If a request for a nonexistent user comes in, the CiscoSecure ACS, after failing to get the user profile, asks for an “unknown user” profile, which is supposed to be a guest user (like anonymous). This feature can be turned off, as follows:

Step 1 Stop CiscoSecure ACS.

Step 2 Add “NUMBER config defaultuser enable = 0” line in CSU.cfg.

Step 3 Restart CiscoSecure ACS.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems’ primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco’s customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO’s Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco’s Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Cisco Documentation

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the *Cisco User Control Point Software Installation Guide* and *Cisco User Control Point Administrator Guide* publications.

9807R