NN10029-111

Succession Multimedia Communications Portfolio

MCP SIP Application Module

Basics

Standard MCP 1.1 FP1 (02.02) April 2003

NORTEL NETWORKS™

Overview

How this chapter is organized

The SIP Application Module Overview contains the following subsections:

Overview

The SIP Application Module is a service execution engine that provides the following functionality:

- core signaling functionality enabling communication among SIP clients
- SIP proxy server
- Back-to-Back User Agent
- SIP Registration
- CPL interpretation
- Location server
- optional Presence subscription and notification (For more information on the Presence feature, see the *MCP SIP Presence Basics* document.)

The SIP Application Module handles SIP sessions and applications and provides the core services that enable communication between SIP clients. The SIP Application Module is housed on the SIP Application Server.

Functional description

The SIP Application Module includes the following components:

- Back-to-Back User Agent (BBUA)/Proxy Server

  Although the BBUA and Proxy Server are basically two different logical entities within the same physical server, they both act as clients and servers. The SIP Application Module decides on a call-by-call basis whether to process the request as a pure Proxy or BBUA.

  The Proxy Server processes SIP requests and responses, rewrites headers, modifies request-URIs (Universal Resource Indicator), performs location look-up, and forwards requests to SIP clients or other servers in the network.

  The SIP Application Module provides a fully session-stated proxy; in other words, the SIP Application Module maintains a call state for the entire session.

  The BBUA extends the proxy function to perform advanced functions such as

  — originating new calls

  — tearing down existing calls

  — modifying messages

— changing IP addresses in the contact header so that the SIP Application Module remains on the signaling path

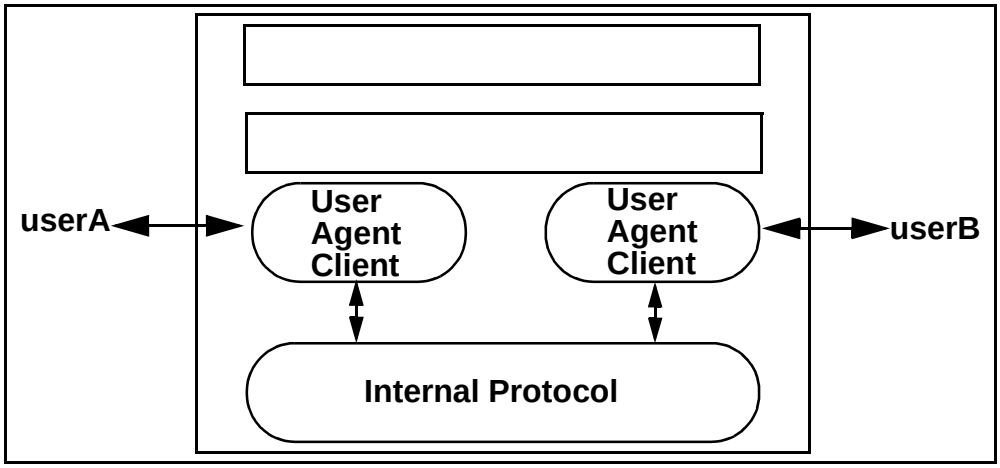
— modifying the Session Description Protocol (SDP) using values supplied by the RTP Media Portal to control media endpoints

— providing advanced screening capabilities

The architecture of a BBUA service consists of two user agent clients linked back-to-back through a proprietary interface.

The BBUA is guaranteed to be on the signaling path of all future requests and responses because it is an endpoint relative to the SIP network components. This is important for services such as billing, which need to be aware of all events that take place on a session. The BBUA in the network also provides a barrier for clients that are not fully SIP compliant and entry and exit points for traffic travelling to and from the public network, including agents behind an enterprise firewall. See Figure 1, “Back-to-Back User Agent service.”

Figure 1 Back-to-Back User Agent service



Routing in a SIP network is based on the same hop-by-hop principle as routing e-mail within the Internet. The next hop for a SIP request is determined by a proxy using the domain or the host part of a SIP URL (user@domain). The terminating proxy determines whether the domain sent in the SIP URL is one of the domains managed by the SIP proxy. Otherwise, the SIP request is forwarded to another Proxy based on the location lookup performed by the SIP Application Module. The SIP Application Module supports routing using table lookup in the SIP database or using the Domain Name Server (DNS) to find a route.

- Redirect Server

  The SIP Application Module decides whether to proxy or redirect the call separately for each individual request. This decision is made based on subscriber service logic. If the decision is to redirect the request, a 302 Response message is returned with a list of alternate locations.

- Registration Server

  The Registration Server performs registration on messages it receives from clients. The Registration Server stores information in the database.

- Location Server

  The Location Server performs location lookup services using domain and user information stored in the database.

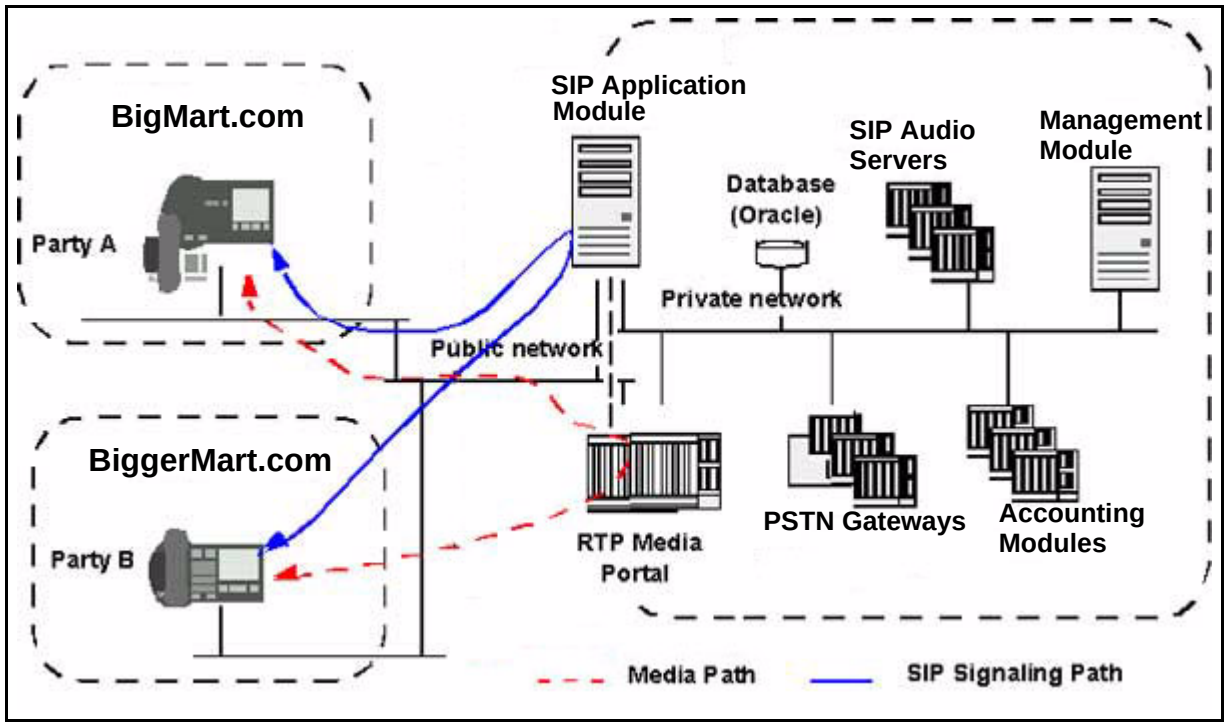
  The SIP Application Module integrates the above logical servers, which are all defined in SIP Draft RFC 2543 (see note for specific reference), into a single server with the enhanced services provided by the Back-to-Back User Agent.

  Note: J. Rosenberg et al, SIP: Session Initiation Protocol, Internet Draft draft-ietf-sip-rfc2543-bis09.txt, IETF, Feb 27, 2002.

Network configuration

The SIP Application Module is configured with two network cards to allow for a network configuration that has a private side and a public side. Figure 2, “Example of network configuration,” shows the SIP Application Module and RTP Media Portal with public ports and ports that are internal to the private network. This network configuration provides security by placing all the components in a private network and exposing only the public signaling and ports to the public network.

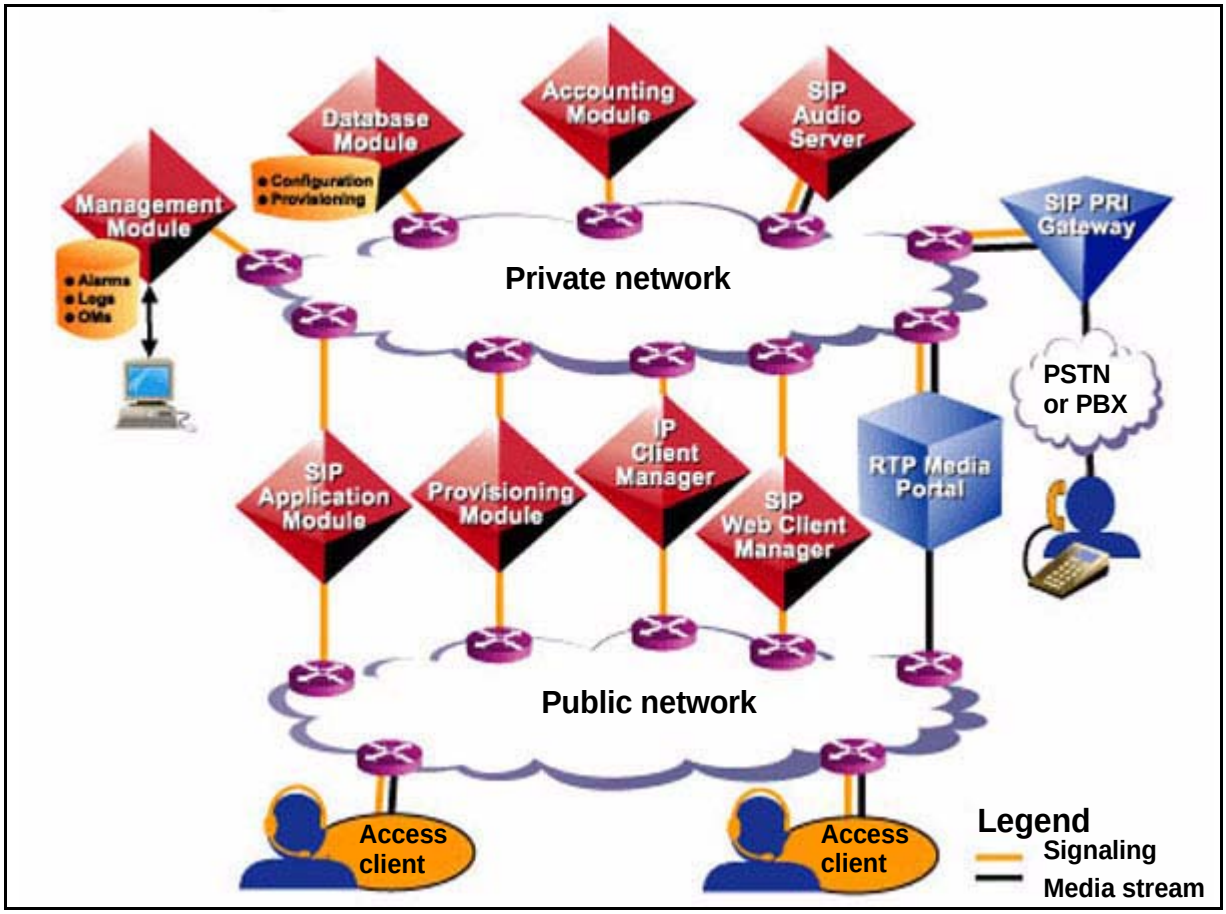
Figure 2 Example of network configuration



Interfaces

The SIP Application Module interfaces with numerous other components. See Figure 3, “Network interfaces.”

Figure 3 Network interfaces



Protocols

The SIP Application Module uses various protocols to support SIP clients, including the Management Module, RTP Media Portal, Database Module, and the PSTN Gateways. The protocols use an IP backbone to connect the components. These interfaces are shown in Figure 3, “Network interfaces.”

Figure 4 Protocols

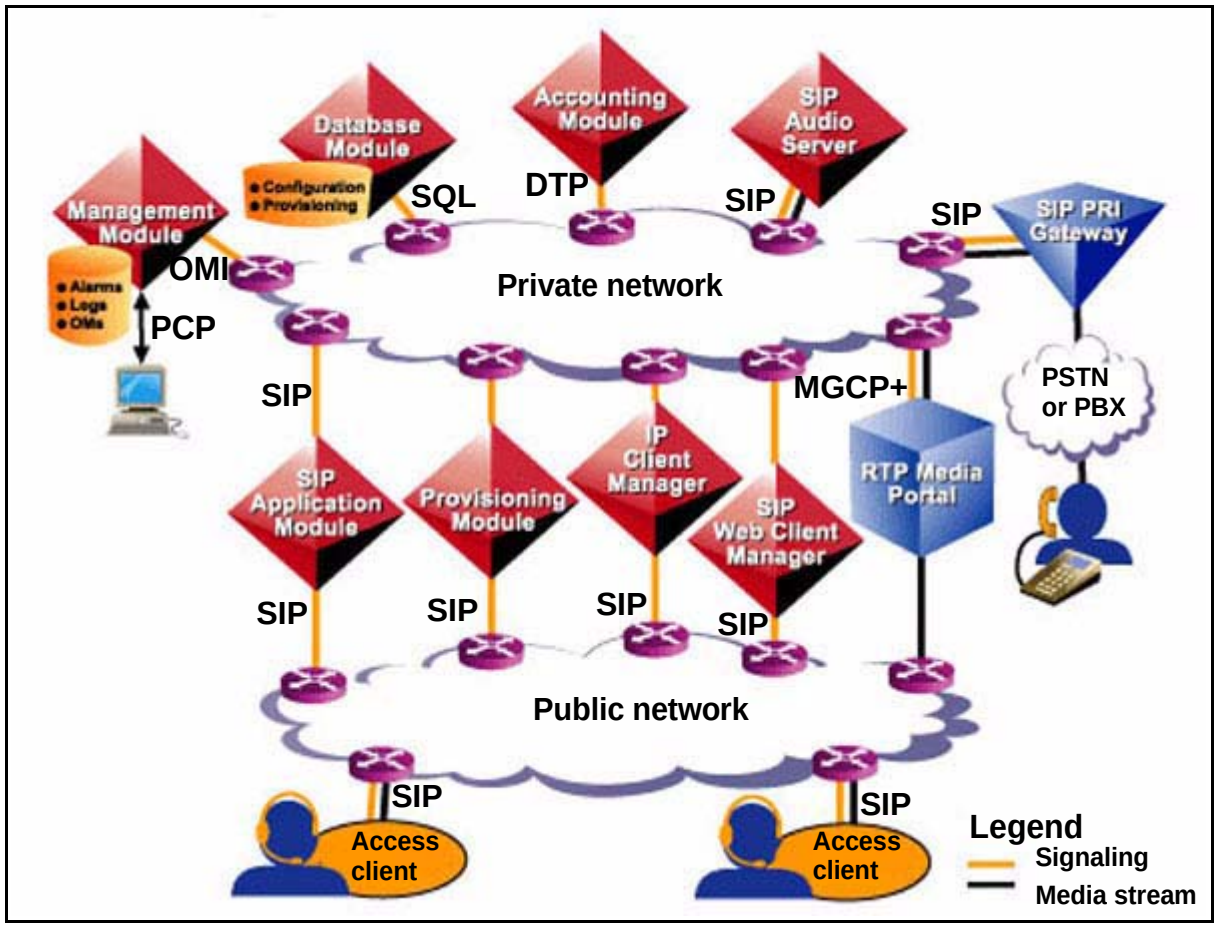


Table 1, “SIP Application Module protocols,” gives details about these interfaces.

Table 1 SIP Application Module protocols

Protocol	Functional component
SQL	Structured Query Language Interface to the Database Module
SIP	Session Initiation Protocol Interface to the • SIP clients • SIP Audio Server • IP Client Manager (IPCM) • SIP PRI Gateway • Web Client Manager
OMI	Open Management Interface Interface to the SIP Management Module
MGCP+	Media Gateway Control Protocol Interface to the RTP Media Portal
PCP	Perfect Channel Protocol for logs and alarms going to the Management Server
DTP	Data Transport Protocol

Note: The external interfaces use an IP network to interconnect the components listed in this table.

Hardware

Refer to Table 2, “Minimum hardware requirements,” for the list of required hardware.

Table 2 Minimum hardware requirements

Sun Netra t 1400(DC) /1405 (AC)	Description
	4-440 Mhz Ultra Sparc II CPUs 4 GB RAM 2-36 GB Ultra SCSI disk drives 1-32X Internal CDROM drive (bootable) 24 GB 4 mm internal tape drive 1 Quad Fast Ethernet PCI card 1 PCI UltraSCSI card AC (t 1405)/DC (t 1400) power supplies

Services and features

The SIP Application Module performs the following services:

- Routing and Translations Services
  - Call Transfer
  - Local termination
  - Foreign termination
  - Redirect
  - Telephony Routing
  - SIP Aliases
  - Multiple Route Termination/SIP Forking feature
  - Call Processing Language (CPL)
- Interworking services
  - Discriminator service
  - Bearer Path Control
  - Privacy Control service

- Service package enforcement
- Authentication services
- Converged PC service
- Network/Address Hiding
- 911 Notification support
- Instant Messaging
- Presence
- Voicemail server interoperability and MWI (message waiting indication) notification
- Registration
- Network address book
- Overload control
- Reliability and fault tolerance

Routing and Translation services

Foreign termination

If an incoming request specifies a domain that is not served by (in other words, is not local to) the SIP Application Module, the SIP Application Module tries to route that request to the appropriate server for that domain.

The first step in this process is to query the DNS SRV, if one is configured in the system, in order to obtain the IP address of the server associated with the foreign domain.

> ***Note:*** A *DNS SRV* extends the basic functionality provided by a traditional domain name server (DNS). It allows a protocol field to be the query for a particular domain and uses that protocol field to provide the correct IP address of the server for the specified protocol. For example, clients may query the server with a domain name of *nortelnetworks.com* and protocol field of *sip*. The DNS SRV would then respond with the IP address of the SIP server for that domain (which may differ from, for example, the H.323 server). This allows a domain to have different servers for different protocols.

If this query fails to find the IP address or if a DNS SRV is not configured, the SIP Application Module attempts to look up the foreign domain in the database to see if an IP address has been provisioned for this foreign domain (see the *SIP Provisioning Client User Guide* for

details). If this step also fails, the SIP Application Module attempts a general DNS A-record lookup to route the request.

Note: The DNS A-record is the traditional response given by a DNS. It translates a domain name into an IP address.

If any of these steps succeed, the SIP Application Module routes the request. If all these methods fail, the SIP Application Module rejects the request.

Call Transfer service
The SIP Application Module handles the transfer on behalf of clients that do not support the call transfer service.

The SIP Application Module supports unattended Call Transfer through the Refer mechanism. Unattended Transfer (or Blind Transfer) refers to cases where the transferor redirects the transferee to the transfer target without first conferring with the transfer target. The transferor receives a Notify message, however, indicating whether the transfer was successful. If it was, the transferor releases the original call. If it was not, the transferor is reconnected to the transferee.

Local termination
The SIP Application Module first determines whether the incoming SIP request terminates to a client in a domain managed by the SIP Application Module. The SIP Application Module performs local routing lookup through the Location Server, which is part of its internal software.

Telephony routing
When the SIP Application Module receives an incoming call, it looks up the callee in the database. If the callee is not in the database but the domain is served and the user portion of the URL is a Telephony routing number, the Telephony routing number is sent through the Telephony routing software within the Location Server.

The Telephony routing software must perform digit translation to find a gateway to terminate a call to. These tables are located in the Database Module. You can provision them through the Provisioning Client. For more information, refer to the *SIP Provisioning Client User Guide* and the *MCP Database Module Basics* document.

The Telephony routing service allows the SIP Application Module to

- provide unique dial plans for each subdomain
- provide routes to gateways or to other domains

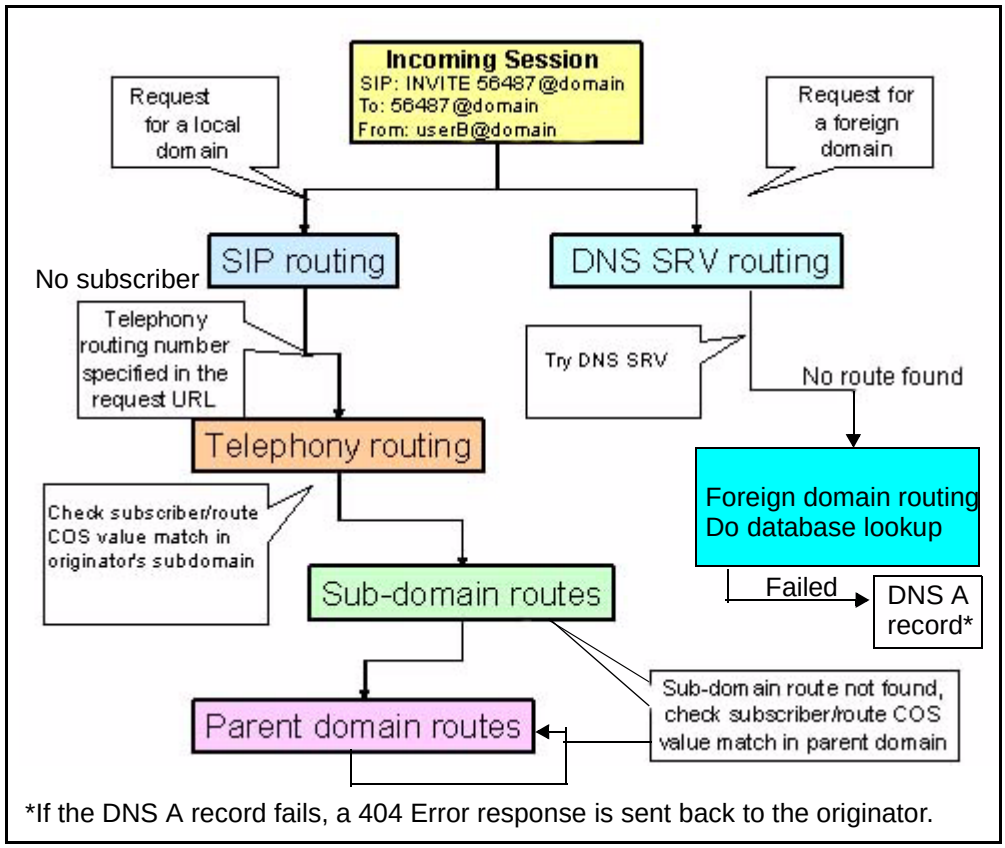
These routes include routes for private digit dial plans, routes to gateways, and telephony-style routing between SIP domains. Multiple lists can reuse the same routes in a route list.

- assign class of service (COS)

  COS is basically used to block particular types of calls, such as international dialing or long-distance dialing. For example, telephones in an office lobby can be restricted to local and emergency calls only in a domain.

Figure 5, “Relationship between Telephony routing stages,” shows the relationship between the telephony routing stages provided by the SIP Application Module. If the COS value of the subscriber and subdomain route do not match, then the SIP Application Module checks the parent for routes with the same or higher COS value.

Figure 5 Relationship between Telephony routing stages



Route lists The Telephony routing service is an enhancement to the Location Server on the SIP Application Module. This enhanced Location Server function has the ability to translate PSTN numbers into

URL addresses specifying an appropriate gateway. It supports the use of digit translation and digit manipulation.

A route list is assigned a single COS. The route list provides the following additional options that can restrict incoming sessions from using the domain's telephony resources:

- allow/block all incoming sessions from other domains
- allow/block all incoming sessions from other subdomains
- redirect session to the originator's domain. This option can be used to redirect an incoming request from another domain that is routing to a restricted route list.

Route lists consist of

- private telephony routes, which are used for private telephony-style digit dial plans
- gateway routes, which provide access to the gateways
- SIP telephony routes, which point to other SIP Application Modules, and SIP domains and subdomains for interdomain routing using telephony-style dial plans

SIP Aliases

Alias URLs can be used to refer to a SIP client in the network. For example, a user "sip: userA@domainX.com" can also be referred to by an alias of "sip:41037@domainX.com".

If an incoming request specifies the "sip:41037@domainX.com" alias in a Request-URI, the alias takes precedence over gateway routing translations, and routing information pertaining to userA is retrieved. If an alias of "sip:41037@domainX.com" is not configured, then gateway routing translations are performed to find out if a terminating gateway exists.

Multiple Route Termination

If a single SIP user is registered at more than one device (PSTN or SIP), forking is used to terminate a session simultaneously or sequentially to multiple devices.

The SIP Application Module interfaces with the SIP database to determine the user routing preference, the routes available, and routing options for a particular user. The user defines these options through the SIP Personal Agent. For additional information on the SIP Personal Agent, refer to the on-product help and *SIP Personal Agent Getting Started Guide.*

With *simultaneous ringing,* the call terminates to multiple routes at the same time. The first terminating route to answer is accepted and the rest of the routes are released.

With *sequential ringing,* the call tries to terminate to only one of several routes at a time. Route advancement occurs whenever an error response is received, a provisionable No Answer timer expires, or a redirect response is received.

Call Processing Language

The SIP Application Module supports the use of the Call Processing Language (CPL), based on the IETF CPL draft, draft-ietf-iptel-cpl.txt. SIP clients can change the behavior of a session using a CPL script that contains general directives for routing a request.

For example, subscribers can include CPL scripts in the body of registration requests that contain instructions for location lookups and call screening, a process that is actually done through the Call Manager in the Personal Agent. Third-party clients can also upload scripts using the Registration mechanism. The Registration function of the SIP Application Module stores the request. When the SIP Application Module is queried for routing information for a subscriber who has valid data stored in the database, the software returns the script along with the routing information. The SIP Application Module applies the CPL script to the returned routes and can eliminate or alter the routes based on the CPL script.

CPL scripts do not support the following:

- Remove location
- Mail option
- Log option

Interworking services

Discriminator service

The SIP Application Module screens requests bound for devices that are not fully SIP compliant, for example, the Communication Server for Enterprise (CSE) 2000. These components cannot process all types of signaling and certain media change requests. Therefore, the SIP Application Module either performs the requested operation or rejects the request and responds with an error response.

The Discriminator service works with various gateways and SIP clients using provisioning facilities implemented by the SIP Application Module. As gateways or SIP clients with limited SIP capability are added to the network, this service can be configured to support these

devices. Information for each component is stored in .xml format to provide flexibility when describing the capabilities of the component.

Bearer Path Control
The SIP Application Module uses the RTP Media Portal to control media streams originating from and terminating to non-compliant SIP devices if they do not support media negotiations. The exception to this occurs when the originating and terminating parties are both the same device type. If both gateways are CSE 2000s, for example, the SIP Application Module does not use the RTP Media Portal.

Privacy Control service
The SIP Application Module supports Privacy Control based on draft-ietf-sip-privacy. This draft defines a mechanism that allows clients to supply a network server with their private user information while at the same time instructing the server not to pass that information outside the boundaries of the trusted network. The information is passed in a Remote-Party-ID header with the privacy indicator set to “full.” The SIP Application Module removes this header any time it forwards the message out over a public network interface.

Service package enforcement
A service package is made up of a user’s enabled network services, such as audio conferencing, and subscriber profile. The service provider defines the available service packages for the domain. The domain provisioner can then assign a specific service package to a subscriber.

Authentication services
The SIP Application Module performs user authentication when the server receives an incoming SIP request. The SIP Application Module supports the challenge-based Digest method for SIP Client-to-Proxy authentication. In Digest authentication, the SIP Application Module challenges a client when a SIP request is received. The SIP Client re-sends a SIP request with a valid password and user name attached. The request types to be authenticated are configurable.

Note: Only US ASCII is supported for user names.

The software performs authentication using the password of the subscriber originating the call. Only subscribers from a local domain actually have a password stored in the database to authenticate against. If a subscriber from a foreign domain (refer to the note below for definitions of these types of domains) places a call and authentication is required for a known foreign domain, the

authentication fails since the database does not have the subscriber's information. As a result, the call is blocked.

Administrators can configure whether they want a call from an unknown foreign domain authenticated or not. System administrators can also specify foreign proxies in the NodalAuth field of the Authentication tab. In this way, no requests originating from those proxies are failed because of authentication.

Note: The following definitions apply:

- *Local Domain*: Local domains are provisioned for and serviced by a particular SIP Application Module. Subscribers for a particular system belong to local domains. Local domains are provisioned through the Provisioning Client.
- *Foreign Domain*: A foreign domain is a domain that is either provisioned as foreign for this SIP Application Module or not provisioned at all for this specific system. It basically represents a domain that is not served.

Converged PC service

The Converged PC service allows end users to use their PCs for the multimedia portion of their communications while using their existing telephony system for voice. The service uses the *simring* feature on an existing telephony system to send mirrored calls to the SIP Application Module through the SIP PRI Gateway. This allows the SIP Application Module to present a call window on the end user's PC when the user's desktop phone rings.

If both parties in a call are Converged users, they will each get a call window from which they can initiate multimedia sessions such as Instant Messaging and collaborative applications between each other.

Some benefits of providing multimedia services using the Converged service are:

- End users can keep using their existing telephone and its capabilities.
- There is no need to replace an existing telephony switch to add multimedia capabilities.

The Converged service adds the following capabilities to the end user's telephony service:

- the ability to manually redirect incoming calls to another party from the PC
- the ability to set up automated enhanced routing and screening of incoming calls based on time of day or based on the calling party's identity
- a call log of all incoming calls
- the ability to send instant messages to the party on the other end of a call
- the ability to start collaborative applications such as shared whiteboard, file transfer, and clipboard transfer with the party on the other end of the call
- the ability to receive a picture ID of the party on the other end of the call

Network/Address Hiding service

The SIP Application Module uses SIP and the Session Description Protocol (SDP) to coordinate the establishment of multimedia sessions for signaling and media, respectively. These protocols embed IP information in their messaging. While Network Address Translation (NAT) devices change port and address information in the IP packet header, most are not currently SIP or SDP aware. IP addresses in these messages are therefore sent out unchanged through the NAT. If the SIP Application Module were to forward these messages on unchanged, sensitive IP information would be given to untrusted clients. In order to remedy this, the SIP Application Module sanitizes the messages before forwarding them.

For IP information in the SIP headers, the SIP Application Module either removes the header (for example, Via headers) or replaces the IP address with the address of the SIP Application Server (for example, Contact header). A media portal is necessary in order to replace the IP information in the SDP headers. The SIP Application Module queries the Media Portal (using MGCP+) for a new IP and port combination to replace the IP and port put there by the client. This effectively anchors the media stream at the Media Portal.

Clients therefore see the SIP Application Module as their signaling endpoint and the Media Portal as their RTP media endpoint. They have no knowledge, and therefore no IP information, about the other client they are in a session with.

The RTP Media Portal handles Network Hiding for the media stream. For information on the RTP Media Portal, refer to the *MCP RTP Media Portal Basics* document.

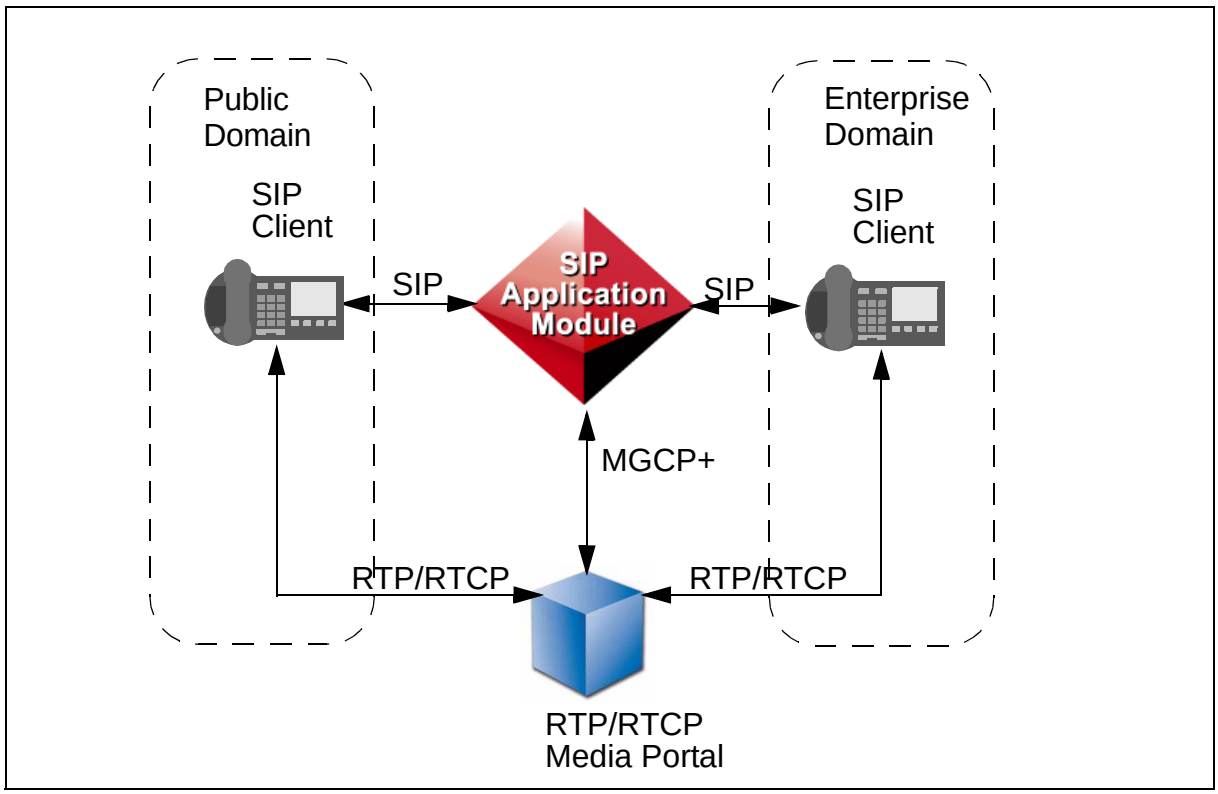
> ***Note:*** The SIP Application Module cannot map SDP information without an RTP Media Portal. It only performs address mapping for SIP header fields. Therefore, SDP passes through untouched. If the server must map SDP address information, then you need an RTP Media Portal.

The SIP Application Module is configured to use an RTP Media Portal to originate and terminate media streams (RTP/RTCP). The SIP Application Module uses extended Media Gateway Control Protocol (MGCP+) to allocate and release resources on the RTP Media Portal for each session as needed.

Enterprise Clients

The SIP Application software uses the RTP Media Portal to hide sensitive IP address information about SIP clients behind a firewall in an Enterprise network. The exception to this occurs when the originator and terminator of the request are both part of the same network. This status is determined by checking the domains in the From header and Request-URI of the SIP Invites. If both SIP clients belong to the same Enterprise network, the SIP Application Module does not use the RTP Media Portal. Administrators can override this behavior by provisioning the *AlwaysUseMediaPortal* domain parameter in the Provisioning Client (for more information about this parameter, see the *SIP Provisioning Client User Guide*). See Figure 6, “RTP Media Portal interworking with Enterprise or foreign clients.”

Figure 6 RTP Media Portal interworking with Enterprise or foreign clients



911 Notification support

The SIP Application Module supports Instant Message notifications to a specified On-Site Notification (OSN) location whenever a user makes a call to an emergency number such as 911. The software provides this service using the same mechanism that allows users to push web pages and/or email links back to the originator of a call. In order to do this, administrators set up (at the Personal Agent) an emergency subscriber for each OSN location and a private telephony route to map the emergency number to this subscriber. Since telephony routes are only unique within a subdomain, you cannot have more than one OSN location for each subdomain.

For each new emergency subscriber that the administrator creates, there must be both

- an emergency number to route to the Public Safety Answering Point (PSAP)
- a SIP subscriber assigned to the OSN location that is to receive the notification.

  Each OSN location must have a specific subscriber assigned, such as sip:guarddeskA@nortelnetworks.com.

For more information and the procedure for setting up Instant Message notifications to emergency numbers, see the *SIP Provisioning Client User Guide.*

Instant Messaging

Instant Messages are routed in parallel only to a subscriber's dynamically registered routes (see “Registration—static and dynamic” on page 24). This is in contrast to session initiation requests, which are subject to CPL routing logic. Upon receipt of an instant message, a client may respond back to the address supplied in the Contact header. This ensures that the response is sent back to the same client device that originally sent the message.

Presence

When a user initially registers, by default their presence status is set to “on-line” in the SIP registration message. Users subscribe to watch the status of other users, and to coordinate the status of their own devices. This information is maintained in an in-memory table on the SIP Application Module (Presence software). The information that is stored in this table includes:

- the user to be watched
- the party requesting the subscription
- the correlation information identifying that particular subscription request
- contact information regarding where to send the notifications that are generated as a result of the subscription being active

When a user changes their presence (for example, to *Busy*), a registration message is automatically sent to the SIP Application Module.

The SIP Application Module then checks its in-memory table to see what their previous presence state was. If the update causes a material change in their presence state, the SIP Application Module looks up which users need to be notified of the change (also in memory). This is done by sending a Notify message to each user at every contact contained in the table. For more information, refer to the *MCP SIP Presence Basics* document.

Voicemail server interoperability and MWI

In order to accomplish voicemail server interoperability and MWI (message waiting indication) notification, the SIP Application Module

transmits the following information over a data link to a voicemail server:

- the called number (terminating party's telephone number)
- the calling number
- the type of call forwarding (for example, due to a busy line, an unanswered call)

This feature also provides an interface to pure IP solutions that use a SIP-enabled voicemail server. In this case, SIP messages provide the context data for each call needed by the voicemail server to record a voicemail message. Thus, a SIP-enabled voicemail server accepts Invites for calls routed to voicemail and sends Notify messages for MWI information. The software uses Real-Time Transport Protocol (RTP) to carry the voice media.

There are two configurations through which the SIP Application Module supports voicemail:

- A pure IP, third-party, SIP-enabled voicemail server that uses RTP to establish the voice path from the subscriber to the voicemail server while SIP provides the setup and MWI information.
- A legacy voicemail server that uses a SIP/PSTN gateway to establish the voice path from the subscriber to the PSTN-based voicemail server. The Simplified Message Desk Interface (SMDI) protocol provides the setup information. The platform uses any voicemail server that supports the SMDI protocol. There are two supported physical connections: a line-based gateway and a PRI/T1-based gateway.

Using either of the above configurations, there are three primary scenarios that this feature considers:

- MESSAGE DEPOSIT: An incoming call for a subscriber gets routed to voicemail because the called subscriber is unavailable, busy, or has all calls forwarded to voicemail.
- MESSAGE NOTIFICATION: The voicemail server sends an MWI status update to the SIP Application Module for a particular subscriber. The SIP Application Module then sends a message to the client(s) to update its MWI display.

  Note: Clients do not store the MWI state. Only the Presence Module stores the state. When a client registers with the proxy

and has messages waiting, the system sends a Notify to the client.

- MESSAGE RETRIEVAL: A subscriber calls the voicemail server for message retrieval. The subscriber is then connected to the voicemail server and accesses the mailbox to retrieve messages.

When you provision the voicemail server, specify which SIP Application Module is the host (see the *Configuration* chapter in this document for details). Only the SIP Application Module that is hosting a particular voicemail server attempts to establish an SMDI connection with that voicemail server.

Note: SMDI is used in certain voicemail configurations to allow the voicemail server to send Message Waiting Indication information to the SIP Application Module. Also when connected to a lines-based voicemail server, the SIP Application Module sends an SMDI message to the voicemail server when a call is being routed to voicemail for message deposit. The SMDI information includes which mailbox the message should be deposited in. Also, the voicemail server periodically sends an SMDI heartbeat message to the SIP Application Module. The SIP Application Module must respond to this message to let the voicemail server know that the SMDI link is still up.

Registration—static and dynamic

Registration can take two forms:

- Static

  Users or administrators can perform static registrations. With static registration, the user can obtain a presence when not logged into the network. The user can obtain a presence and an account in one of the following ways:

  — Using the SIP Provisioning Client, the administrator can add a user account and assign a static route.

  — When users have accounts, they can add contact information, such as PSTN numbers or cell phone numbers, to their routing information.

- Dynamic

  Once a user logs in, re-registration is automatic with the SIP Multimedia PC Client, the SIP Multimedia Web Client, and the IPCM. The IPCM takes care of this re-registration automatically for the i2004. Dynamic registration is automated and behind the scenes.

Network address book

Client Address Book information is stored in the network so that it can be accessed from all clients. The information is downloaded in bulk whenever a client comes on line (either through a Simple Object Access Protocol [SOAP] interface or direct database access depending on the client).

In order to receive updates to the Address Book after the initial download, the client subscribes to the Address Book event package and updates it as needed. Whenever an update is made through the Personal Agent or one of the clients, a Notify message is sent to the client indicating which entries have changed. The client can then incrementally update their view of the information (again either through a SOAP interface or direct database access depending on the client).

A List of Buddies is incorporated as part of the Address Book. Each subscriber must create their own personal Address Book and designate their own Buddies. For each of these specified entries, the client automatically subscribes to their presence event package. This allows them to monitor and update the network presence of each Buddy (for example, online or offline).

Overload control

Overload Control monitors the Incoming Protocol Message Queue Length. If this queue length crosses a configurable threshold value, the system performs Session Blocking, allowing no new incoming requests to process. The system does, however, continue to process requests for an established session. For rejected requests, the system sends a “503 Service Unavailable” response with a Retry-After header, which specifies the amount of time a client should wait before retrying the request.

Note that multiple thresholds may be crossed simultaneously. If this occurs, the appropriate actions are invoked and are not cleared until all aspects of the system have crossed below the assigned threshold value.

Reliability and fault tolerance

The SIP Application Module provides reliability and fault tolerance through multiple SIP Application Modules deployed in an N+M active-standby configuration.

Note: The supported active/standby configurations include:

- a 1+1 configuration (one active plus one standby server), which is the most basic reliable configuration
- an N+M configuration of up to four servers (the sum of N plus M should not exceed 4)
  - a 2+1 (2 active and one standby)
  - 2+2 configuration
  - 3+1 configuration

To accomplish this, all the servers in a reliability group are configured with the same set of NSDs. This gives the standby server the information it needs in case an active server fails. Each server in the group transmits messages indicating its current state. Other servers respond with their current states, including the NSD activated on them.

An initializing server configures itself with one of any inactive NSDs. If all NSDs are active, the initializing server becomes the standby. This prevents conflicts where more than one server is activating simultaneously.

Before activating, the server determines whether it is isolated from critical network resources defined through provisioning. If any of the resources cannot be reached, the server cannot activate and raises an alarm. The alarm clears when the resources become available.

When there are two or more active servers, the group is called a cluster. You can configure both the N+M strategy and the cluster at the Transport Management tab in step 22 in the *Configuration* chapter.

When one of the active SIP Application Modules fails, the passive Module takes over the IP address. The passive Module has now become active and assumes the responsibilities of the failed Module. When this occurs, any sessions already in the active state remain up. This means that calls that have already been established continue and the parties maintain voice path. Any future requests during that session, however, fail (for example, Hold, Retrieve, and Web Pushes) since the session information is no longer available. Any sessions that were not in the active state before the failover are lost. The originating clients of

these sessions either receive no indication or continue to hear an alerting tone for an indefinite period of time.

Manual failover
There are two recommended procedures for manually initiating the fail-over of an active instance to a Standby node: the initiation of discrete LOCK and UNLOCK actions, or the initiation of a restart.

Lock/Unlock If you want to force a fail-over in order to perform maintenance on the "failed" server, then request a LOCK from the Management Console. The LOCK forces the component into a disabled operational state, where it remains until you request an UNLOCK from the Management Console. You can perform any maintenance on the "failed" server while it is LOCKed. Once maintenance is complete, the server can be UNLOCKed from the Management Console, which causes an automatic restart and brings the server back into service.

Restart If you want to simply force an immediate manual fail-over, then you can request a Restart from the Management Console.

WARNING

The N+M reliability strategy provides a highly available service environment. The fail-over mechanisms enable an instance of the SIP Application Module to survive failure condition(s) by migrating to a standby server where it can resume the processing of new sessions.

In such a highly available service environment the failed instance loses all knowledge of sessions started before the fail-over event. Therefore, the stability of these pre-existing sessions cannot be guaranteed. For example:

Sessions involving SIP clients will survive until the clients encounter a "no response" or "unknown call" response to a request on their active session. At that point the clients will release the session and its associated media resources.

Sessions involving the MCP SIP PRI Gateway will survive until there is no response to the SIP PRI Gateway-generated SIP "ping" to the SIP Application Module(s) handling the active sessions on the gateway. If there is no response to the SIP "ping" then the gateway will tear down the associated call and recovers its resources.

Also, sessions involving the MCP RTP Media Portal will not survive a manual fail-over because intentionally LOCKing the SIP Application Module initiates the automatic recovery of all resources (including RTP Media Portal resources) associated with in-progress sessions.

For more information, see the *Configuration* chapter in this document.

OAM&P strategy

The Management Module manages the OAM&P functions for the SIP Application Module. For additional information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

Upgrades

For information on upgrading from one full release to another, refer to the Installation and Commissioning document you receive with the upgrade.

Updating the SIP Application Module software

Administrators can update the software version of the SIP Application Module using the System Management Console. The update can be either an up- or down-version of the software.

Updating the software affects the operation of the component's hosted services during the procedure. This process automatically fills the service property fields of the updated component with the configured values from the previous version.

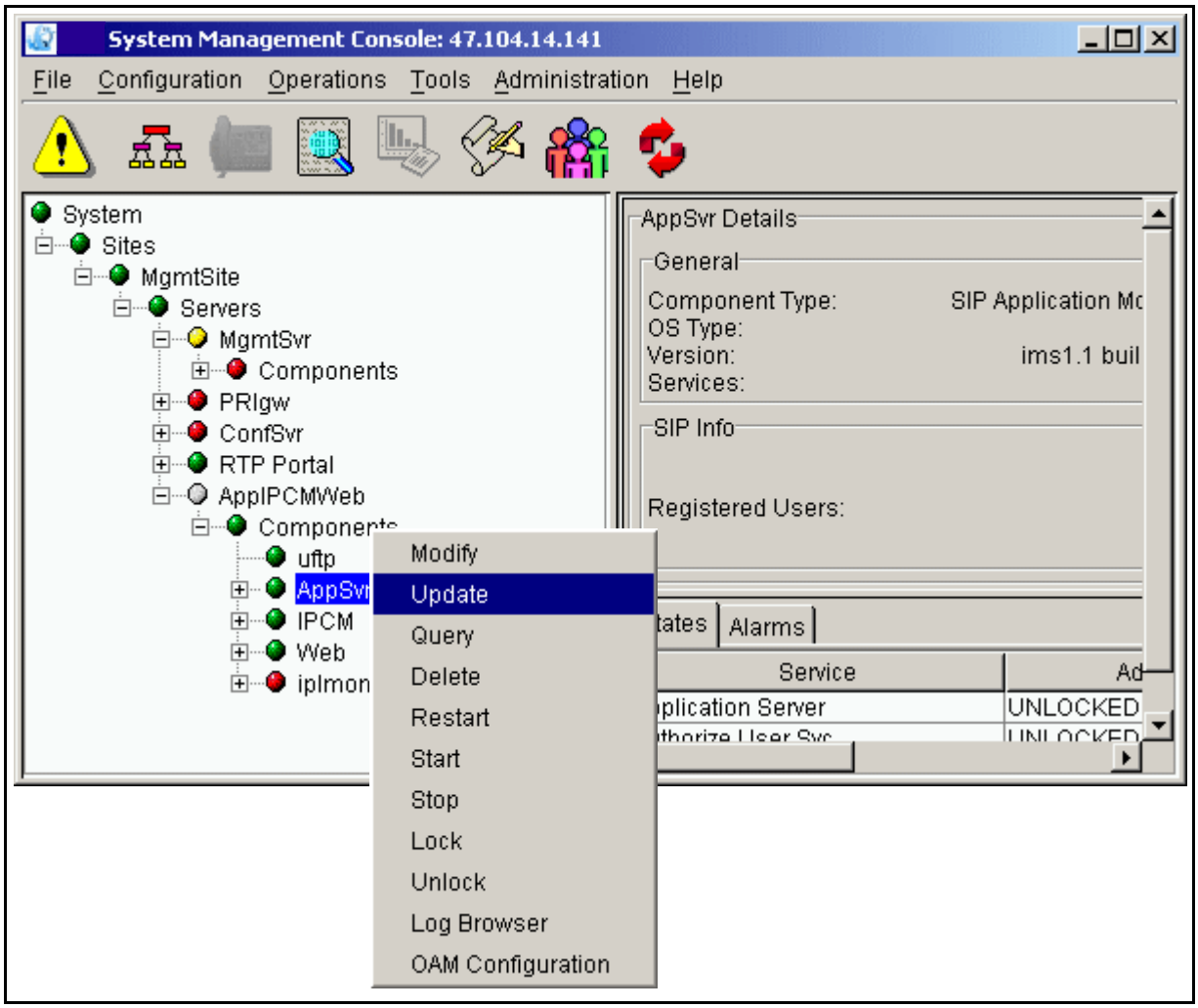
The update introduces new functionality across many components without affecting network stability. If a server update fails, you have a choice to roll back or not. For more information on the update procedure, refer to the *MCP System Management Console Basics* document.

at the System Management Console

1 A load can be either up-versioned or down-versioned. In either case, updating a load from one version to another results in stopping and deleting the previously added version, adding the new version and auto-launching the new version. Therefore, there is no need to manually LOCK and UNLOCK the service. The steps involved in an update are described below.

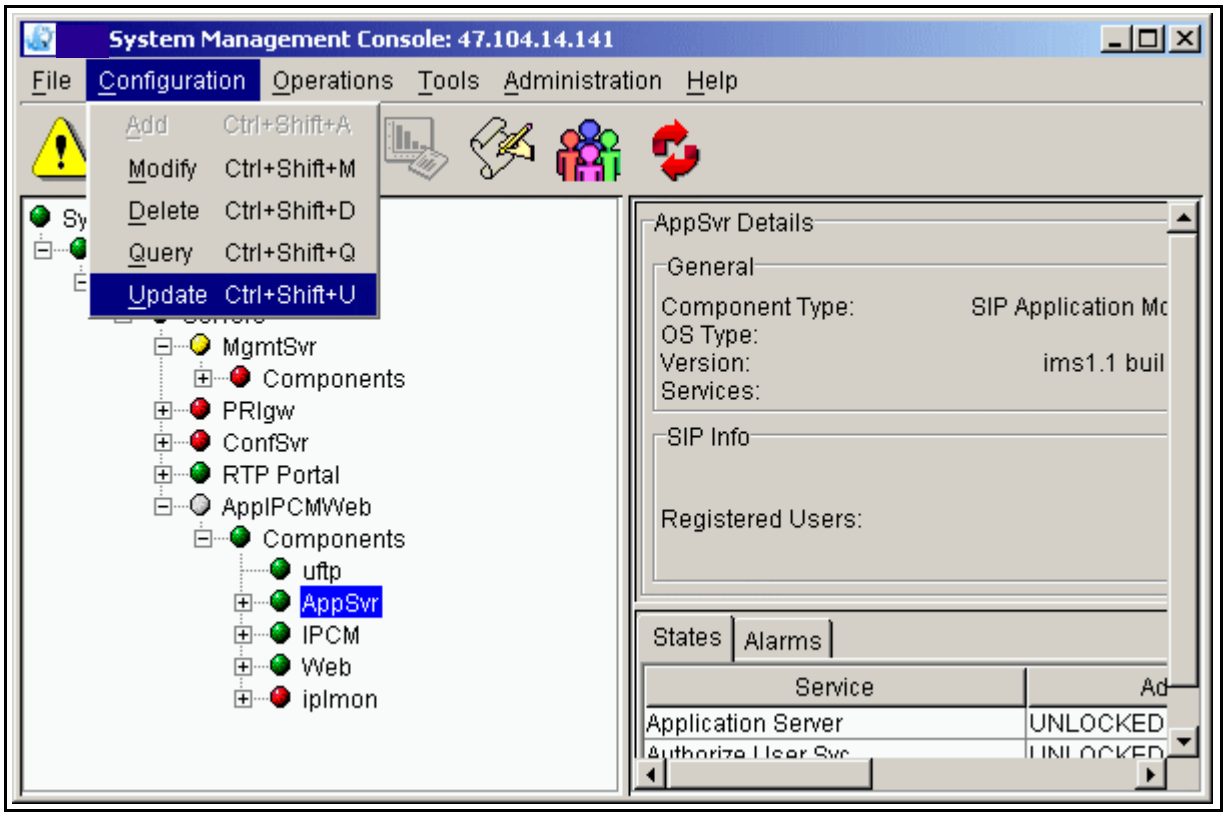
From the System Management Console, under the **Components** folder, select the name configured at deployment, **AppSvr** in the example shown in Figure 1.

Figure 1 Updating the Application Module from the menu tree



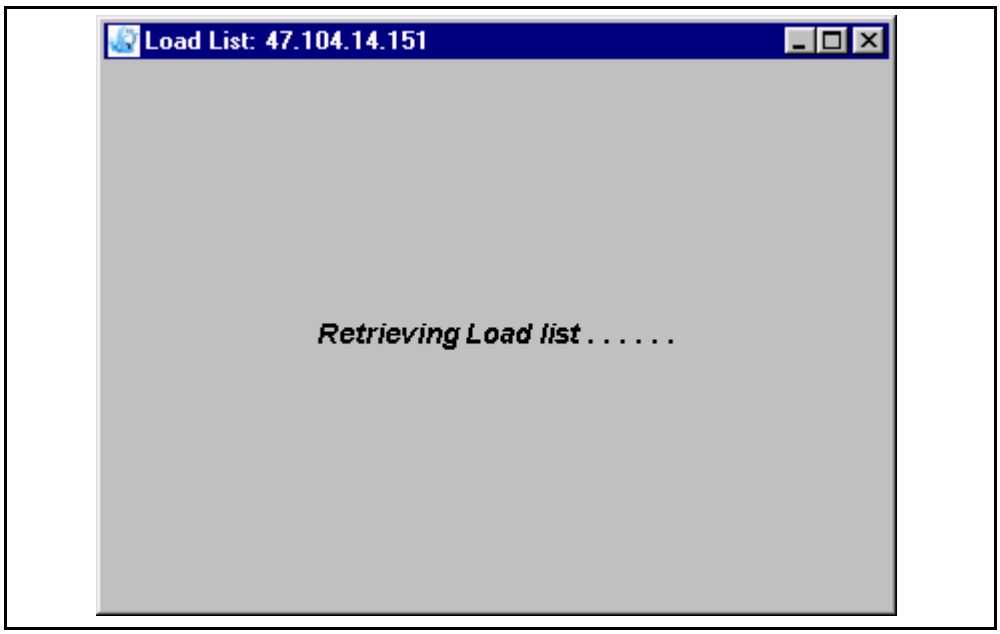
You can also launch the update from the pull-down Configuration menu, as shown.

Figure 2 Updating the SIP Application Module from the pull-down menu



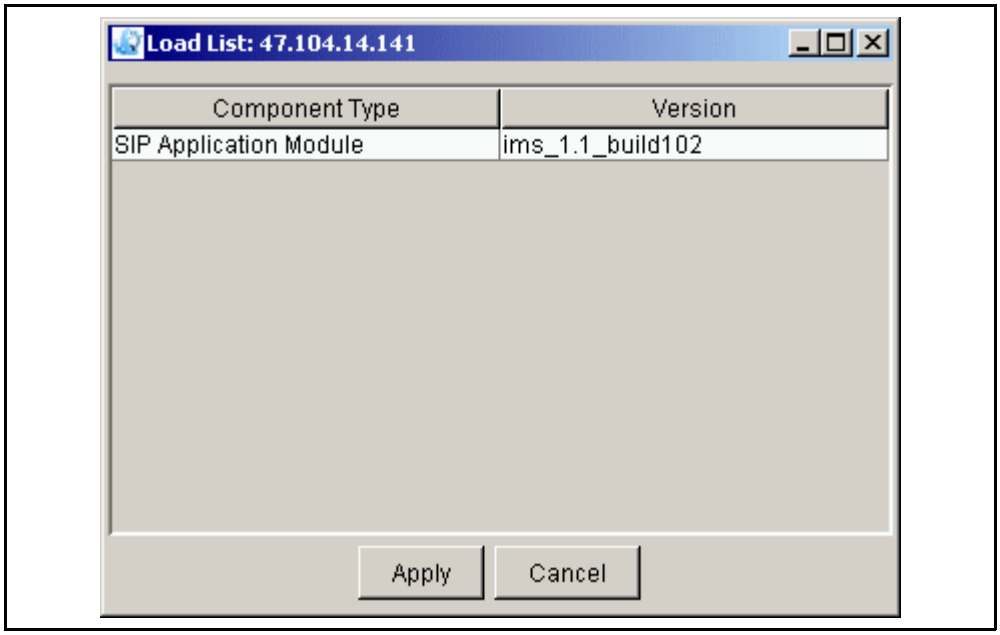
2 Select the **Update** command. The following window appears.

Figure 3 The update window, retrieving the load list



3 Because only versions not currently deployed appear in the loadlist following the **Add->Component** step in the update procedure, multiple versions may not appear for the update operation. You can only do an update from one version to another. Therefore, the window only shows loads that have the same name as the load being updated (see Figure 4, “Load list for updating”).

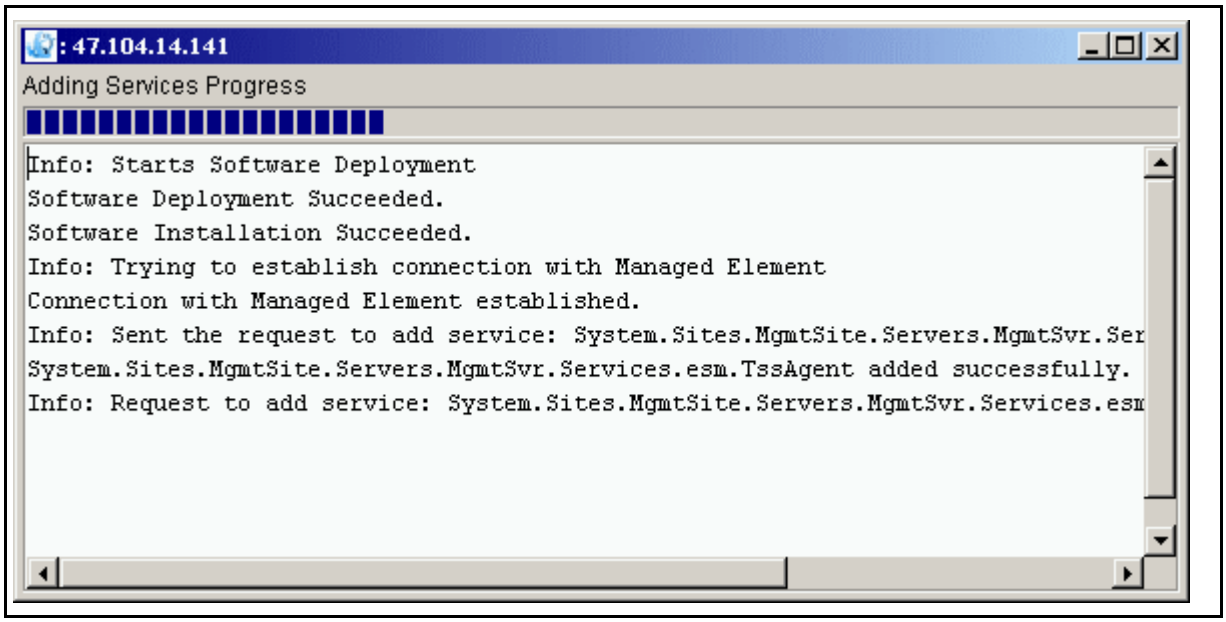
Figure 4 Load list for updating



4 Select the version you want to update. Click on the **Apply** button.

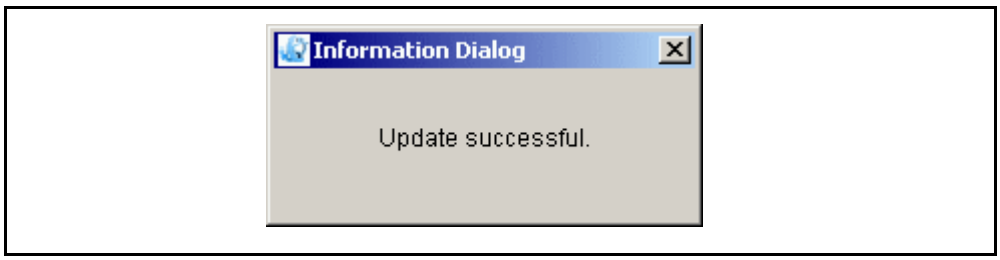
5 The configuration window appears, showing the tabs. Modify all the configuration values you need to modify. Then click on the **Apply** button. The window that appears shows the progress of the update (see Figure 5, “Progress of update”). Each configured managed object (MO) appears as being successfully added onto the managed element (ME).

Figure 5 Progress of update



6 Once the update has completed, the following window appears.

Figure 6 Successful update dialog box



OAM&P strategy

The Management Module manages the OAM&P functions for the SIP Application Module. For additional information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

Fault management

The Management Module manages the faults for the SIP Application Module. For additional information on the Management Module, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

How this chapter is organized

This chapter is organized as follows:

- Alarm clearing procedures
- Recovery procedures

Alarm clearing procedures

Procedure 1 Clearing the SLE701 (SLEE Health Monitor) alarm

at the alarm browser

1 The SIP Application Module raises this warning alarm under one of two conditions:

- The number of application contexts (AC) available for use are inadequate for the level of traffic (in which case the administrator needs to back off the traffic or call the next level of support).

  The SIP Application Module raises this alarm when AC pool use reaches or exceeds 80%. The alarm clears when use drops below 80%.

- There is an error condition that is causing ACs to be consumed at a higher than normal rate. This could be due to a myriad of things; for example, the system might be consuming RetrieveSubscriber ACs at a high rate because the database is overloaded.

Severity is MAJOR. The SLEE is a service processing environment. An AC is a unit of work within that processing

framework. For example, when you register your phone, a number of AC instances are invoked to process the registration.

Procedure 2 Clearing the SMDI101 alarm

at the alarm browser

1 This alarm is raised when the Simplified Message Desk Interface (SMDI) telnet session between the SIP Application Module and a terminal server is lost. The SIP Application Module uses the SMDI protocol to communicate information between itself and a voicemail server. If the connection goes down,

- Message Waiting Indication notification to subscribers stops.
- Calls routed to the voicemail server are not sent to the appropriate mailbox.

However, depending upon the voicemail server's capabilities, the calls may be answered by a default mailbox and the originator can enter the desired mailbox number in which to leave a message. In the same way, users may be able to retrieve their voicemails (for example, they get routed to the default mailbox and are prompted to enter their mailbox). Again, this functionality depends upon the voicemail server being used.

The SIP Application Module repeatedly tries to re-establish the telnet session to the terminal server. If the alarm does not go away in a few minutes, then the terminal server needs to be checked and possibly re-booted. Also, administrators should check the voicemail server to make sure it is running correctly. If problems persist, contact your next level of support.

Configuration

How this chapter is organized

This chapter describes the procedures for configuration required at the service provider premises. This chapter is organized as follows:

  - Svc Pkg Enforcement Service
  - SipFwdAdapter
  - Transport Management
- “Additional SIP TCF Base tab configuration information” on page 90
- “OAM&P strategy” on page 92

Overview

CAUTION

Before making any changes to the base configuration, consult your next level of support.
.

Nortel Networks performs the initial installation and commissioning. Once the installation and commissioning are completed, you can begin to make your system fully operational. The following list identifies some general tasks:

- provision and complete translations to enable voice and trunk services
- configure any additional services, applications, and features that Nortel Networks is not contracted to perform
- complete the installation of clients or add client software for all management interfaces

The SIP Application Module is configured using the System Management Console. For more information, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents. This chapter describes the configurable parameters affecting operation of the SIP Application Module and the procedures for configuration required at the service provider premises.

Deployment from the System Management Console results in the installation of all SIP Application Module-specific software and configuration data on the host machine, and starts the software processes. Undeployment stops the software processes and removes all related software and configuration data. When the deployment is complete, the SIP Application Module should be unlocked, enabled, and available to provide service.

Before a SIP Application Module can be deployed, the server must have been configured at the System Management Console. This server

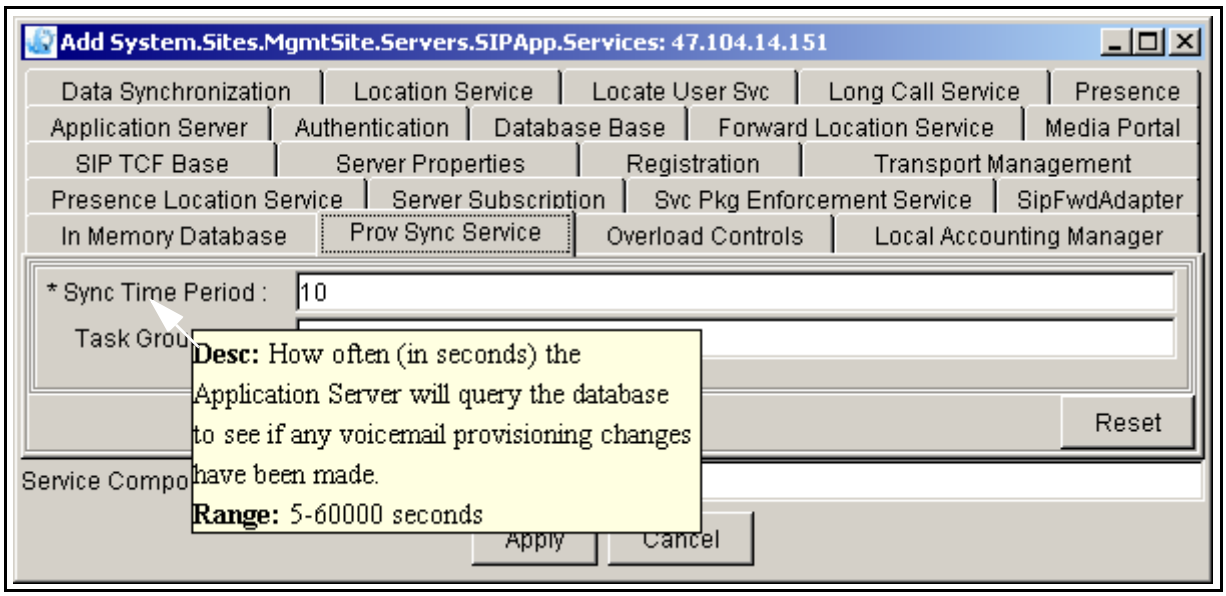
represents the physical hardware on which the SIP Application Module resides. Once the servers are configured, the SIP Application Module can then be deployed.

The SIP Application Module depends on various components that require configuration during the deployment process. In general, most of the SIP Application Module's configuration items can be left with their default values; however, administrators should familiarize themselves with the available options.

Administrators can also find help text with descriptions and acceptable ranges by holding the cursor over the field name as shown in Figure 1, "Displaying help text."

Note: In all tabs, the fields with asterisks (*) require an entry. The grayed-out fields are for information only and cannot be changed. Change all occurrences of the IP address "0.0.0.0" to the proper IP address for your situation.

Figure 1 Displaying help text



Adding a component

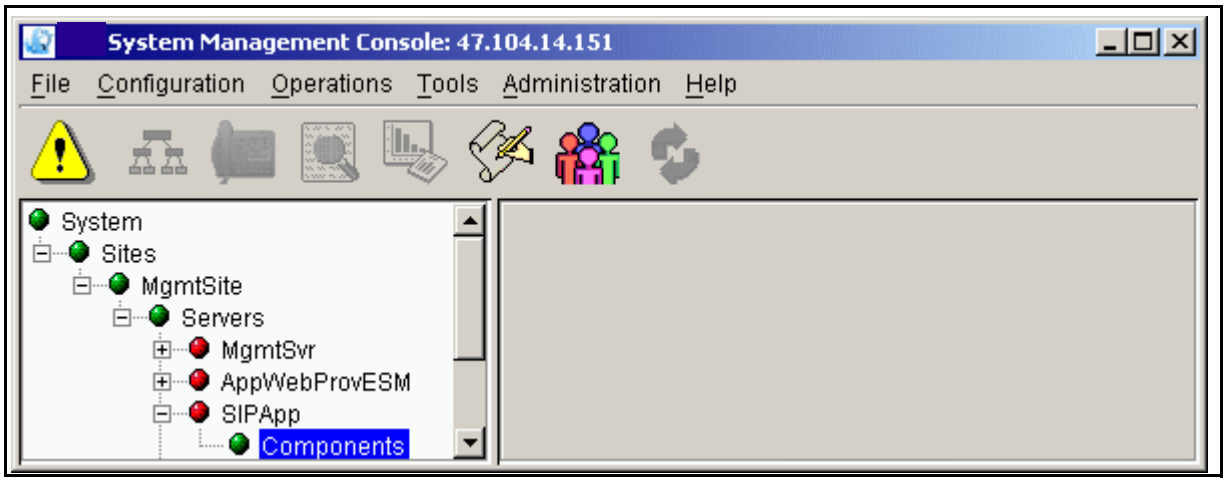
This procedure assumes that the server on which the SIP Application Module will be deployed has already been configured. For example, Figure 3, “Adding a component,” shows the SIP Application Module being deployed onto the previously configured server. For the procedure for adding a server, refer to the *MCP System Management Console Basics.*

Procedure 1 Adding a component

at the System Management Console

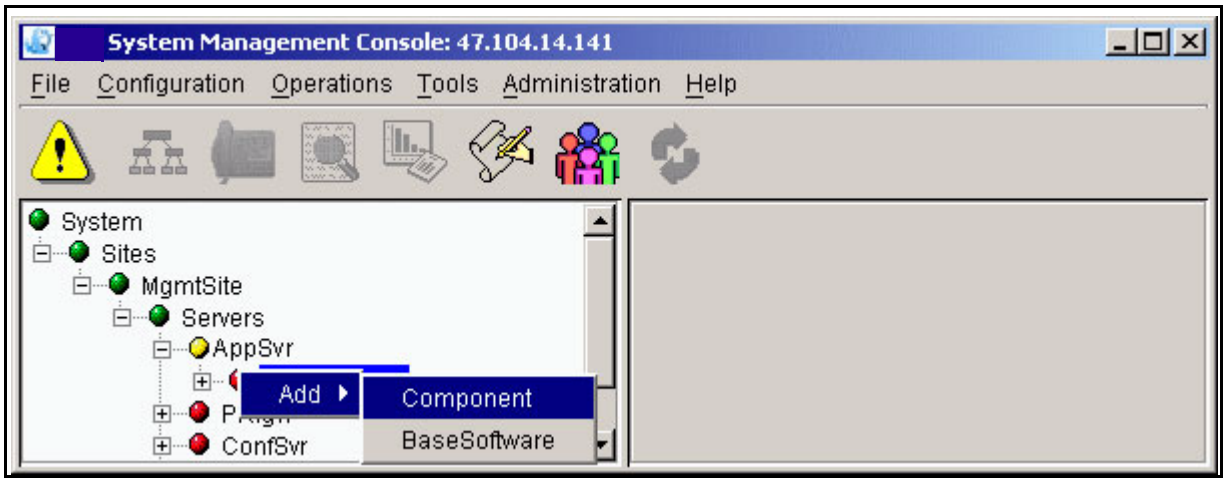
1 To add the SIP Application Module, navigate to and right click on the **Components** item in the Management Console tree structure.

Figure 2 Navigating to the Components file



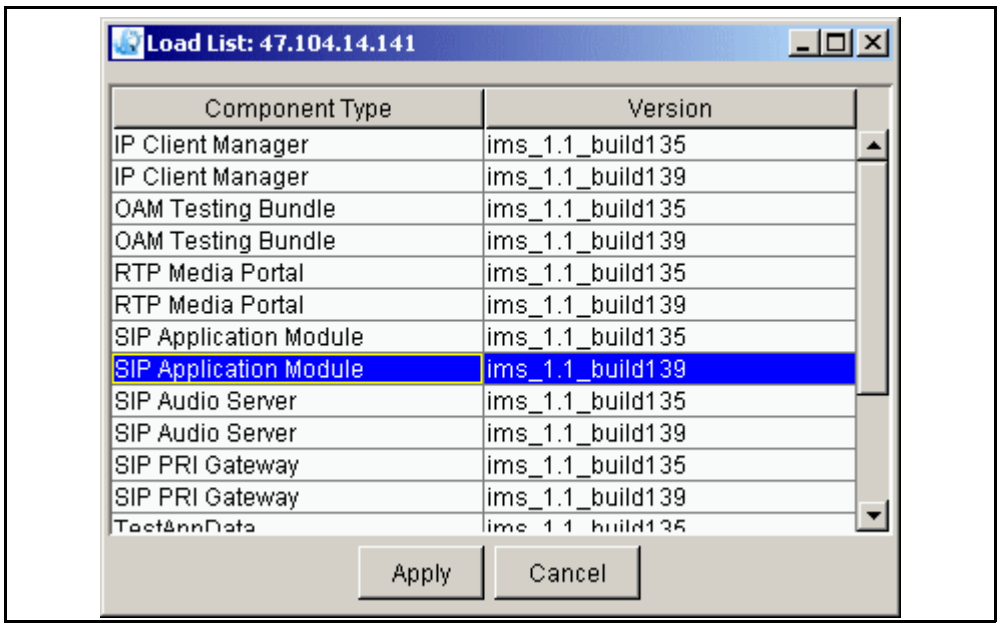
2 Select **Add->Component** as shown.

Figure 3 Adding a component



3 Select the SIP Application Module software load you want from the load list that appears (see Figure 4, “Load list”) and click on the **Apply** button. There may or may not be multiple software loads to choose from.

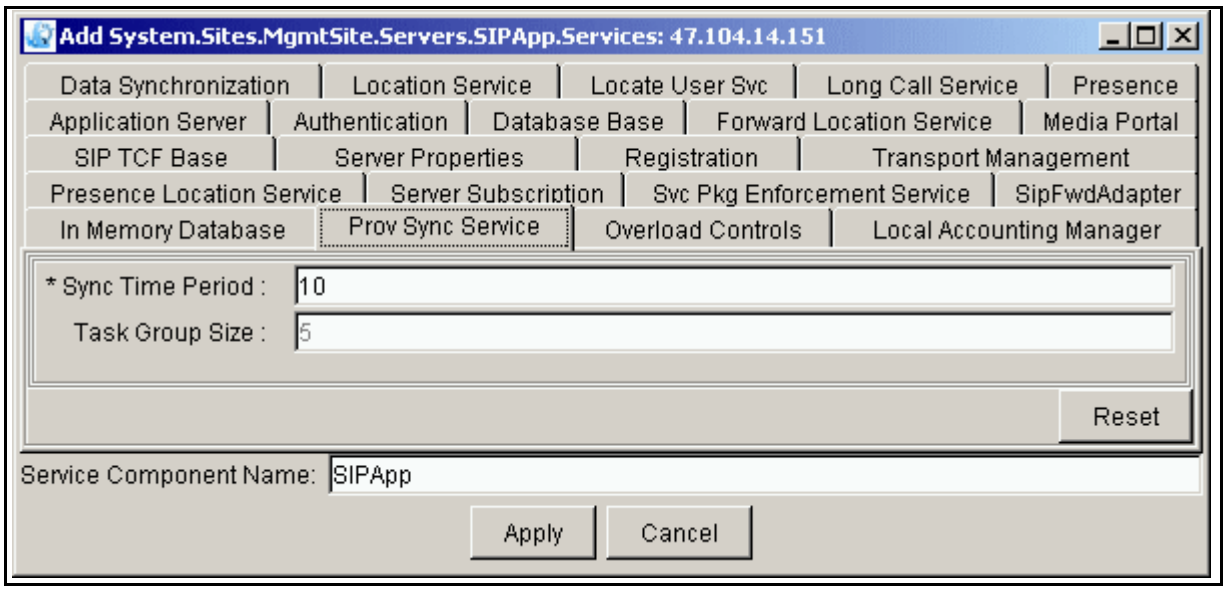
Figure 4 Load list



4 The Configuration window (shown in Figure 5, “Configuration window (top half)”) appears. Once the configuration window appears, enter a label with a maximum of six characters in the Service Component Name field at the bottom. This name must be unique among the components. The following figure shows

an example with the name **SIPApp** entered in the Service Component Name field.

Figure 5 Configuration window (top half)



5

ATTENTION

DO NOT click on **Apply** until you have FINISHED filling in the fields that you need.

Note that there are a number of different tabs in the SIP Application Module configuration window representing the configurable services that the SIP Application Module requires. The following sections describe each tab in detail and provide guidance on how to configure the SIP Application Module. Many of the fields are already filled with default values. Administrators can leave most of the filled-in fields with their default values. Only a few fields need customization.

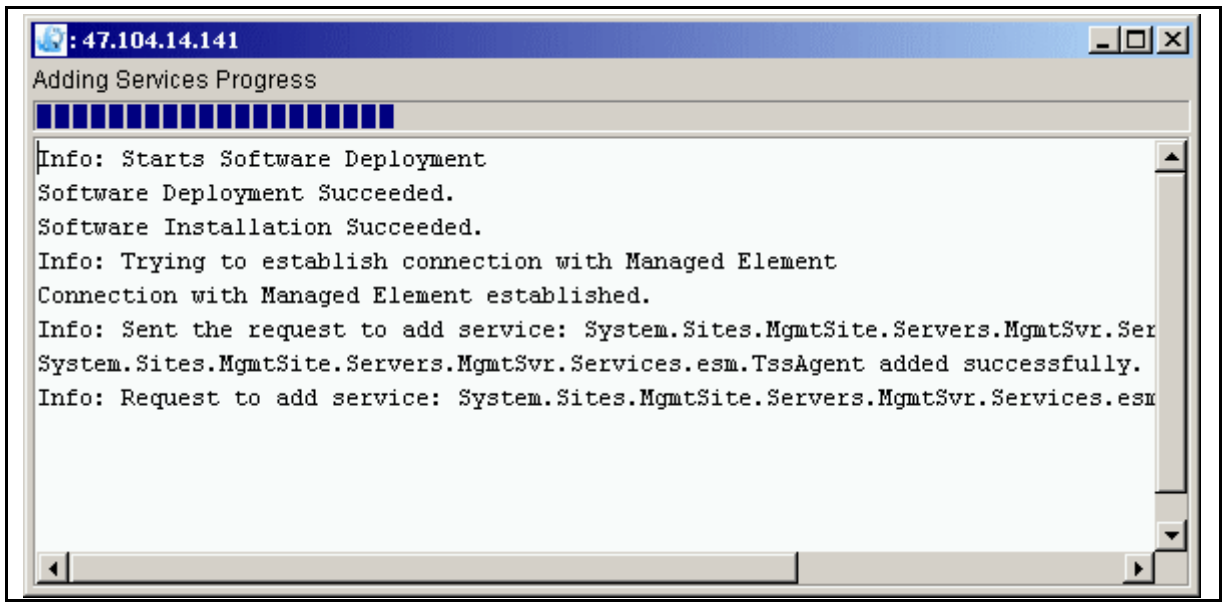
Note: The parameters with asterisks (*) are mandatory. The grayed-out fields are for information only and cannot be changed.

Make any required modifications to any of the tabs. When you have COMPLETED all the tabs, click on the **Apply** button.

6 After you click the **Apply** button, the Management Module begins the deployment and installation of the SIP Application

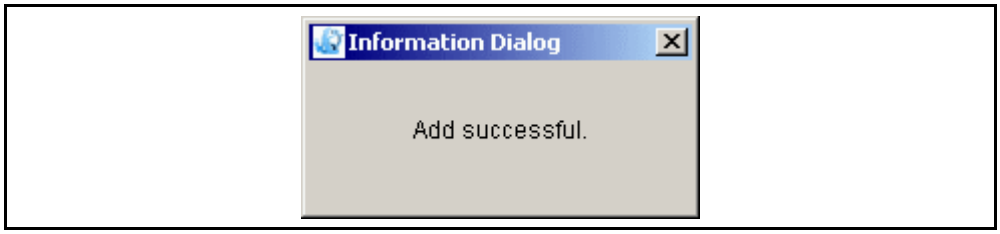
Module. The Adding Services Progress dialog box appears as shown in Figure 6, “Adding Services Progress dialog box.”

Figure 6 Adding Services Progress dialog box



If the deployment is successful, an “Add successful” box appears, as shown in Figure 7, “The Add successful dialog box.”

Figure 7 The Add successful dialog box



If the deployment is not successful, re-examine the configuration tabs and verify that all 0.0.0.0 IP addresses have been replaced with the correct IP address. Verify other non-default parameters for accuracy. The SIP Application Module and all of its services must be unlocked and enabled. There must be no alarms.

After deployment and installation, the Management Module configures services according to values entered in the configuration tabs during step 4.

Configuring the SIP Application Module tabs

The following sections describe the configuration tabs in detail. The tables following the figures describe the fields shown in the figures.

Note: These tabs do NOT have to be completed in this particular order. The following order is only for example.

Procedure 2 Completing the tab fields

at the System Management Console

1 Click on the Application Server tab. The Application Server tab allows the SIP Application Module to set high-level data, such as the title of the server instance, the managed domains, and the private IP address of the server.

Figure 8 Completing the Application Server tab fields

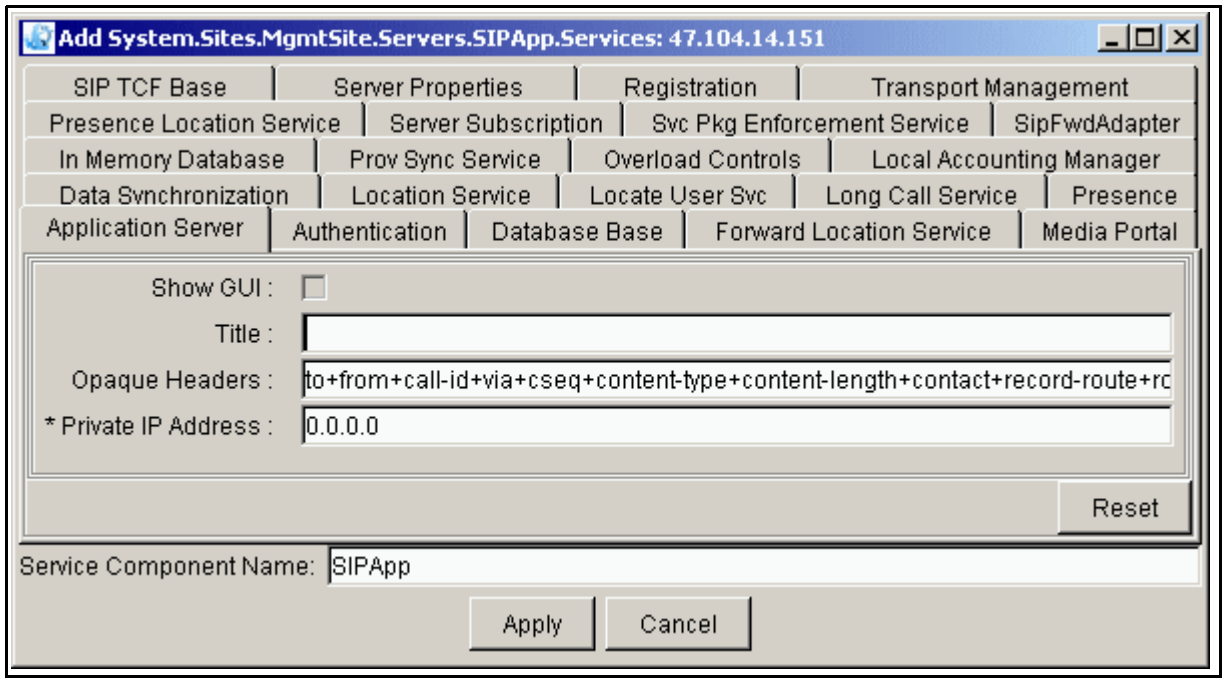


Table 3 Application Server tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Show GUI	Type=checkbox Default=unchecked	This is a read-only field.
Title	Type=string Range=0-64 characters	This field contains the title of this Server instance.

Table 3 Application Server tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Opaque Headers	Type=string Range=0-2048 characters Default=to+from+call-id+via+ cseq+content-type+content-length+contact+record-route+ route+proxy- require+rseq	This field contains a “+” delimited list of headers that should not be passed through the server.
Private IP Address	Type=valid IP address Range=0-4096 numbers or blank Default=0.0.0.0	This field contains the private IP address of the server. ***Note:*** Do not leave this field blank or the software will not deploy.

2 Click on the Long Call Service tab. The Long Call Service tab allows the service provider to set the length of time between endpoint audits. The Long Call Service detects abandoned calls and releases the resources used by such calls.

Figure 9 Completing the Long Call Service tab fields

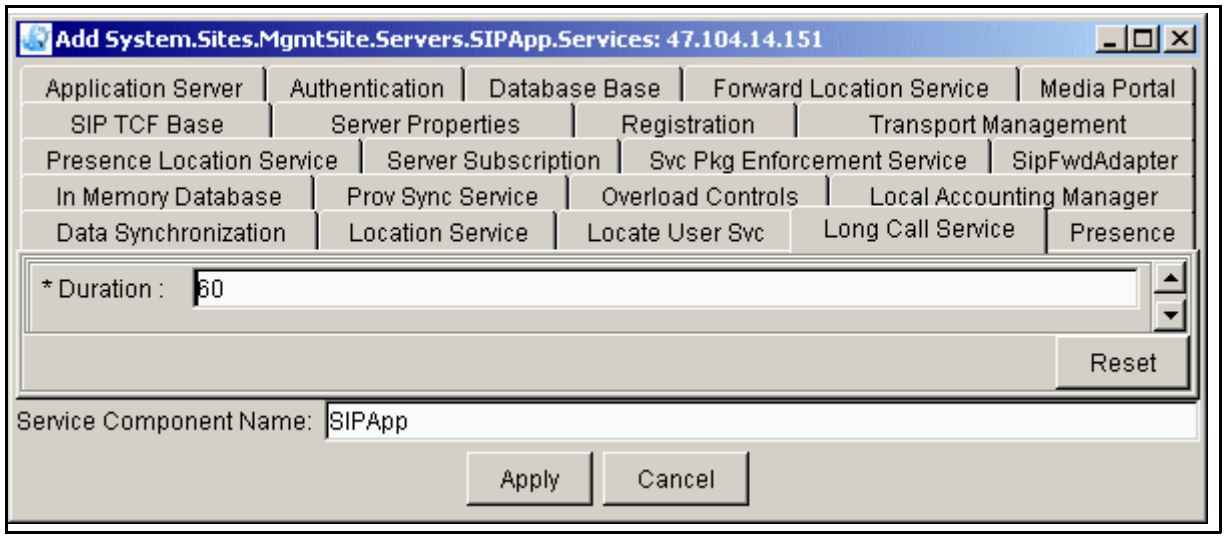


Table 4 Long Call Service tab field descriptions

Field	Value	Description
Duration	Type: Integer Range: 0–Max_Integer Default: 60 minutes	This field shows the length of time in minutes between endpoint audits and is used to detect abandoned calls. A value of zero deactivates it. The recommended value is 10 (minutes). If the SIP Application Module detects an abandoned call at the endpoint audit, it drops the resources for that leg.

3 Click on the Presence tab. This tab allows the service provider to configure context and expiration information for the Presence service.

Figure 10 Completing the Presence tab fields

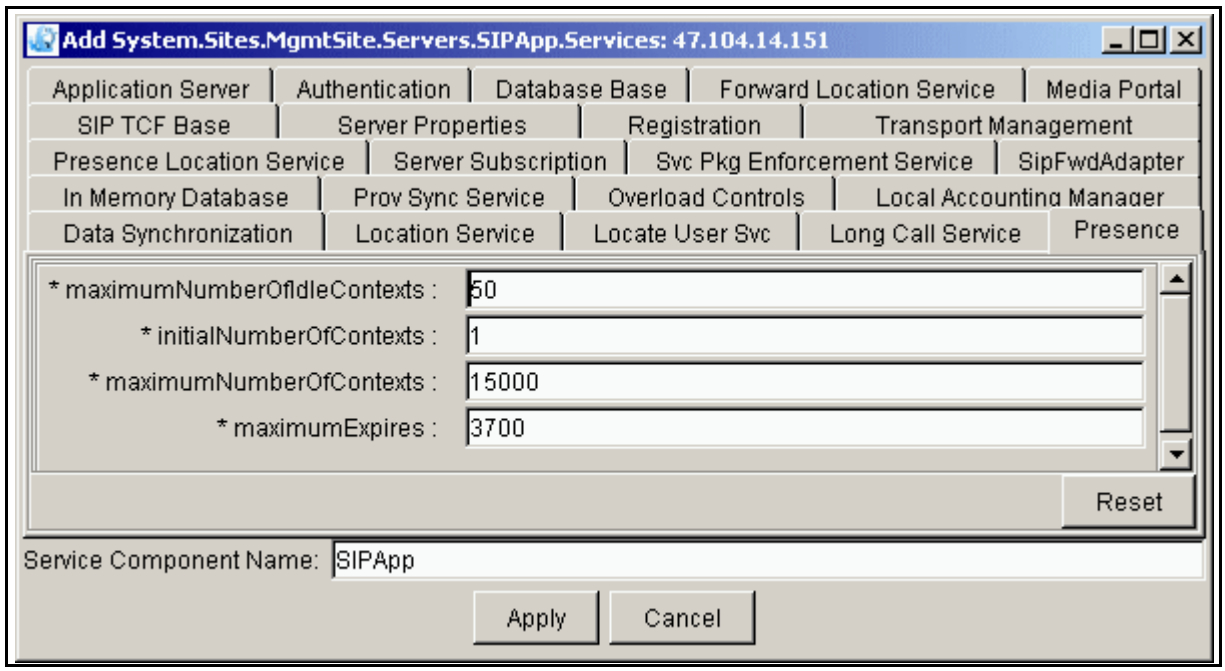


Table 5 Presence tab field descriptions

Field	Value	Description
maximumNumber OfIdleContexts	Type=integer Range=1-10000 Default=50	This field indicates the maximum number of idle contexts at any time. This should not exceed the maximum number of contexts.
initialNumberOfContexts	Type=integer Range=1-10000 Default=1	This field indicates the initial number of contexts to create. This should not exceed the maximum number of contexts.
maximumNumberOf Contexts	Type=integer Range=1-15000 Default=15000	This field indicates the maximum number of contexts to create.
maximum Expires	Type=integer Range=60-86400 Default=3700	This read-only field contains the maximum allowable expiration value for a presence subscription request, in seconds.

4 Click on the Presence Location Service tab. This tab allows the service provider to configure the use of off-board Location Servers for routing.

Figure 11 Completing the Presence Location Service tab fields

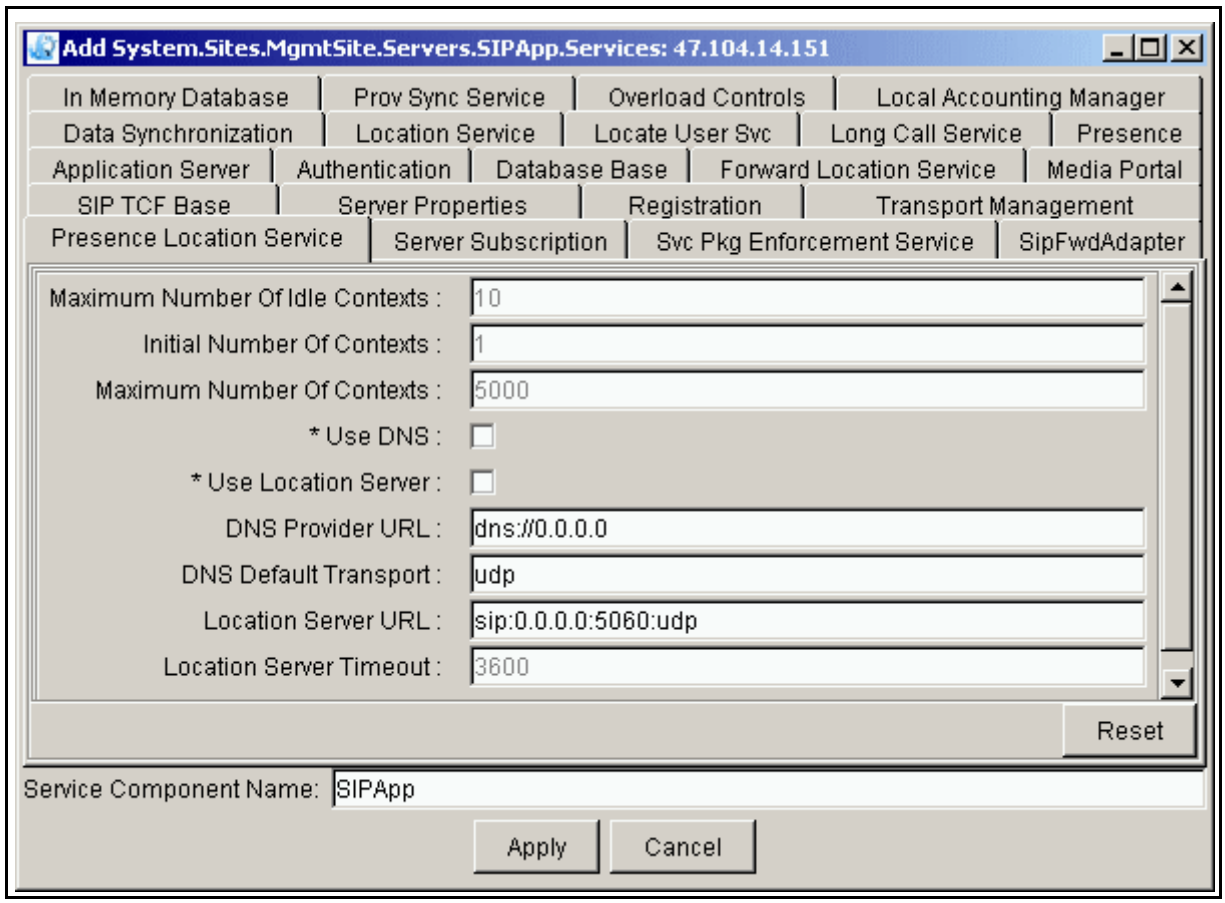


Table 6 Presence Location Service tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Maximum Number of Idle Contexts	Type=integer Range=1-100 numbers Default=10	This read-only field contains the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
Initial Number of Contexts	Type=integer Range=1-100 numbers Default=1	This read-only field contains the initial number of contexts to create. It should not exceed the maximum number of contexts.

Table 6 Presence Location Service tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Maximum Number Of Contexts	Type=integer Range=1-10000 numbers Default=5000	This read-only field contains the maximum number of contexts to create.
Use DNS	Type=checkbox Default=unchecked	Turns DNS server functionality on and off.
Use Location Server	Type=checkbox Default=unchecked	Turns Location Server functionality on and off.
DNS Provider URL	Type=string Range=1-1024 numbers Default=dns://0.0.0.0	This field indicates the address of the DNS Server format >dns://0.0.0.0
DNS Default Transport	Type=string Range=udp, tcp Default=udp	Transport type used to communicate with the DNS server.
Location Server URL	Type=string Default=sip://0.0.0.0:5060:udp	This is the address of the Location Server.
Location Server Timeout	Type=string Default=3600	This field is not used.

5 Click on the Authentication tab. The Authentication tab enables or disables authentication for requests and sets additional authentication information.

Figure 12 Completing the Authentication tab fields

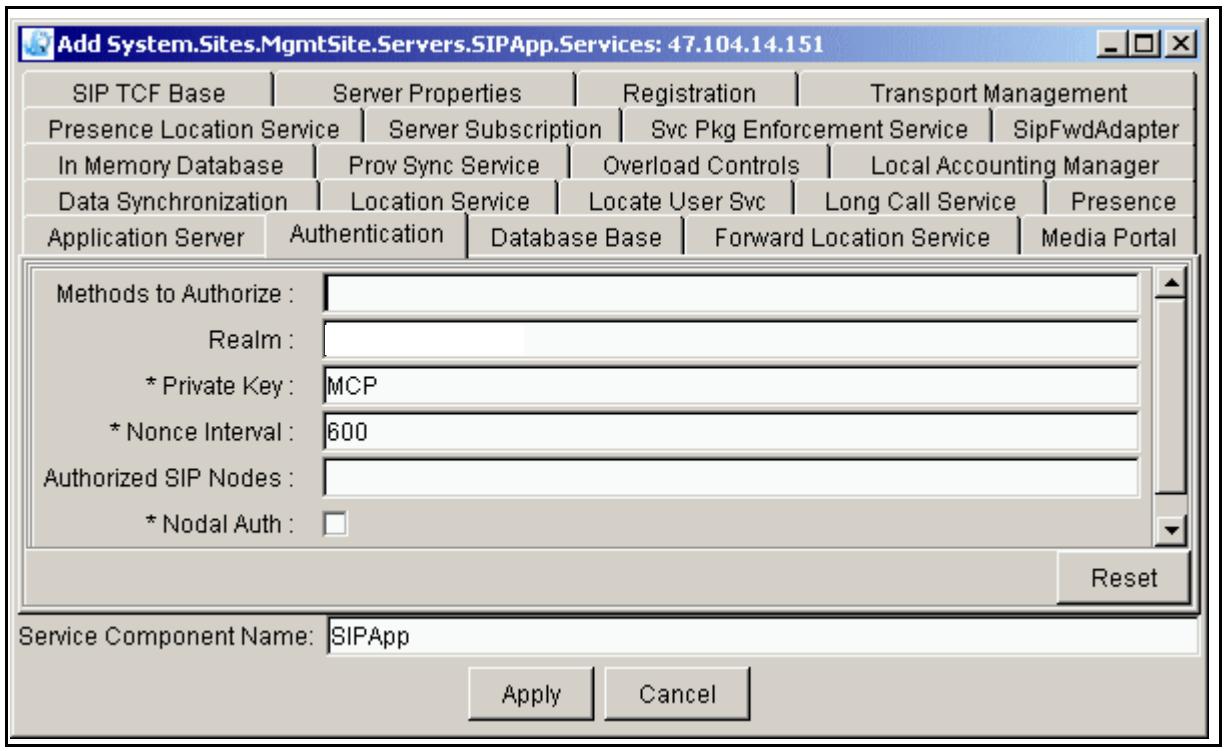


Table 7 Authentication tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Methods to Authorize	Type=string Default=register	This field indicates which SIP methods to authenticate.
Realm	Type=string Range=0-256 characters	This field indicates the string that is displayed to the user to indicate what realm they need to supply a password for.
Private Key	Type=string Range=0-256 characters Default=MCP	An extra key used to uniquely generate authentication challenges.
Nonce Interval	Type=integer Range=10000- 600000 milliseconds Default=600	The software uses this field to determine how long to wait (in milliseconds) for a response to a challenge with a specific nonce value before generating a new nonce value.

Table 7 Authentication tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Authorized SIP Nodes	Type=IP address Range=0-2000 numbers	This field contains a + -delimited list IP addresses. Use the SIP PRI Gateway and SIP Audio Server addresses.
Nodal Auth	Type=checkbox Default=unchecked	When this field is checked, the SIP Application Module redirects requests. When unchecked, this field authenticates requests and only the SIP PRI Gateway and SIP Audio Server listed in the previous field can send INVITE messages to the SIP Application Module without authentication. Nortel Networks recommends that you do not change this field.

6 Click on the Media Portal tab. This tab allows the service provider to set port and firewall information pertaining to the Media Portal.

Figure 13 Completing the Media Portal tab fields

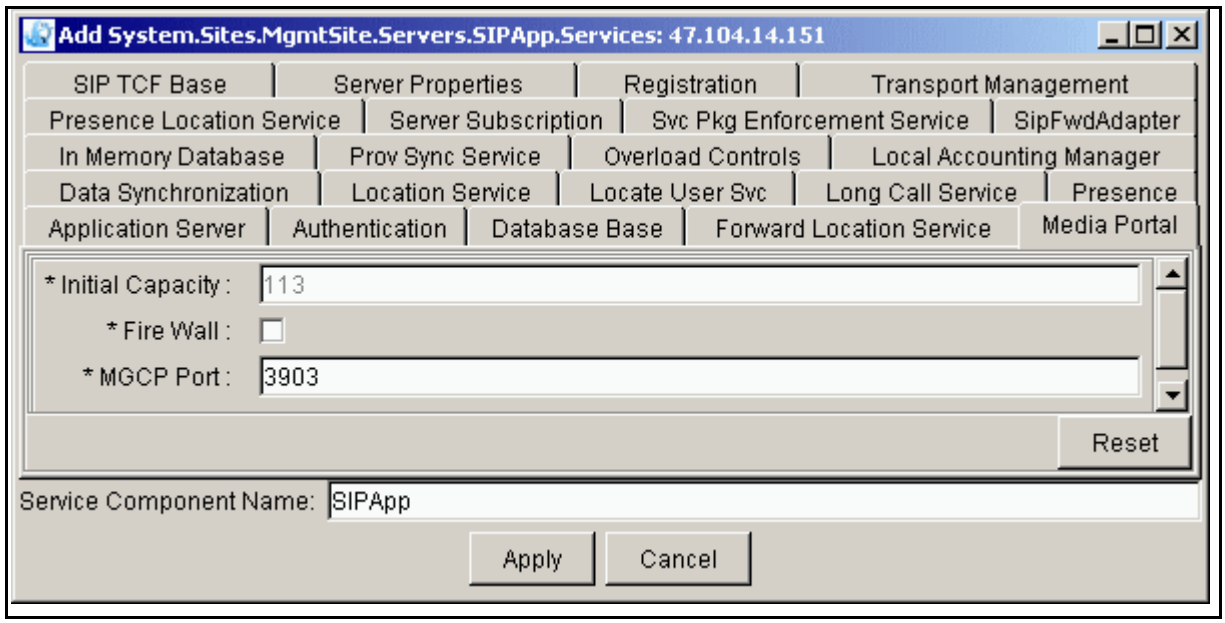


Table 8 Media Portal tab field descriptions

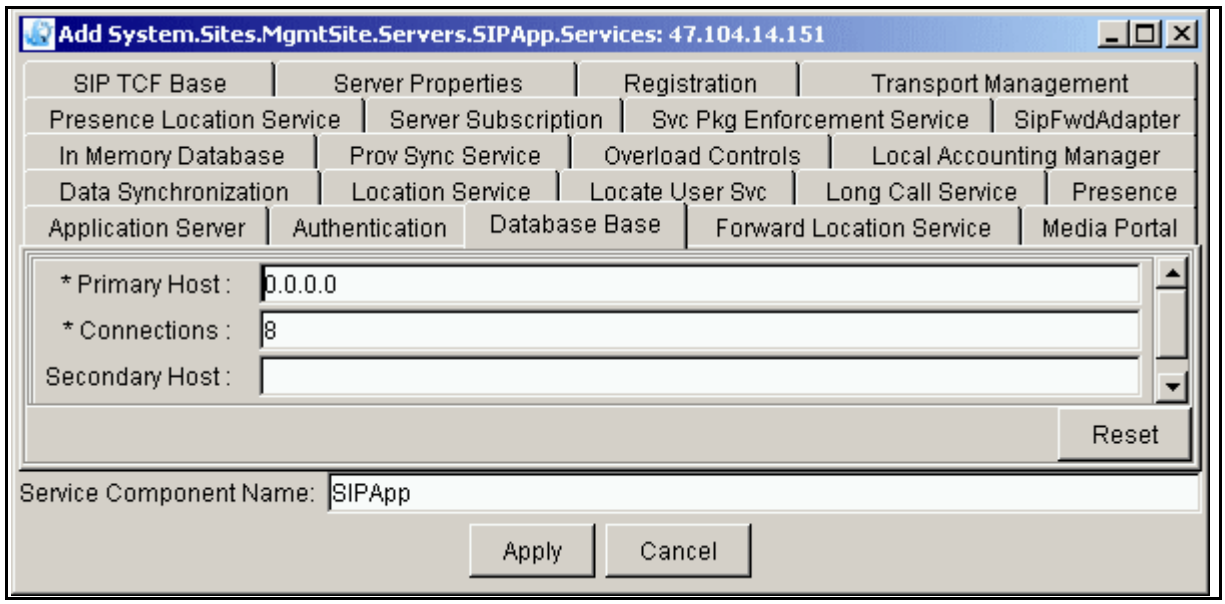
Field	Value	Description
Initial Capacity	Type=integer Range=113-16384 Default=113	This field is not used.
Fire Wall	Type=checkbox Default=unchecked	This field is not used.
MGCP Port	Type=integer Range=1025-65535 Default=3903	This field indicates the UDP Communications port number where the Media Portal sends and receives MGCP+ messages.

7 Click on the Database Base tab.

General properties for the SIP Application Module's connection to the database are defined in the Database Base tab. See the *MCP Database Module Basics* document for more information and field descriptions. Modifications to the Database Base require that the Database Base be locked. A lock of the Database base releases all SIP Application Module resources associated with the Database Base. When released, these

resources are removed from the SIP Application Module's local cache. When the Database Base is unlocked, all SIP Application Module resources must be reallocated causing a re-read of the resources from the database. This tab also contains connection information for the database.

Figure 14 Completing the Database Base tab fields



Note: See the *MCP Database Module Basics* document for field descriptions.

8 Click on the Locate User Svc tab. This tab allows administrators to configure the use of off-board Location Servers for routing.

Figure 15 Completing the Locate User Svc tab fields

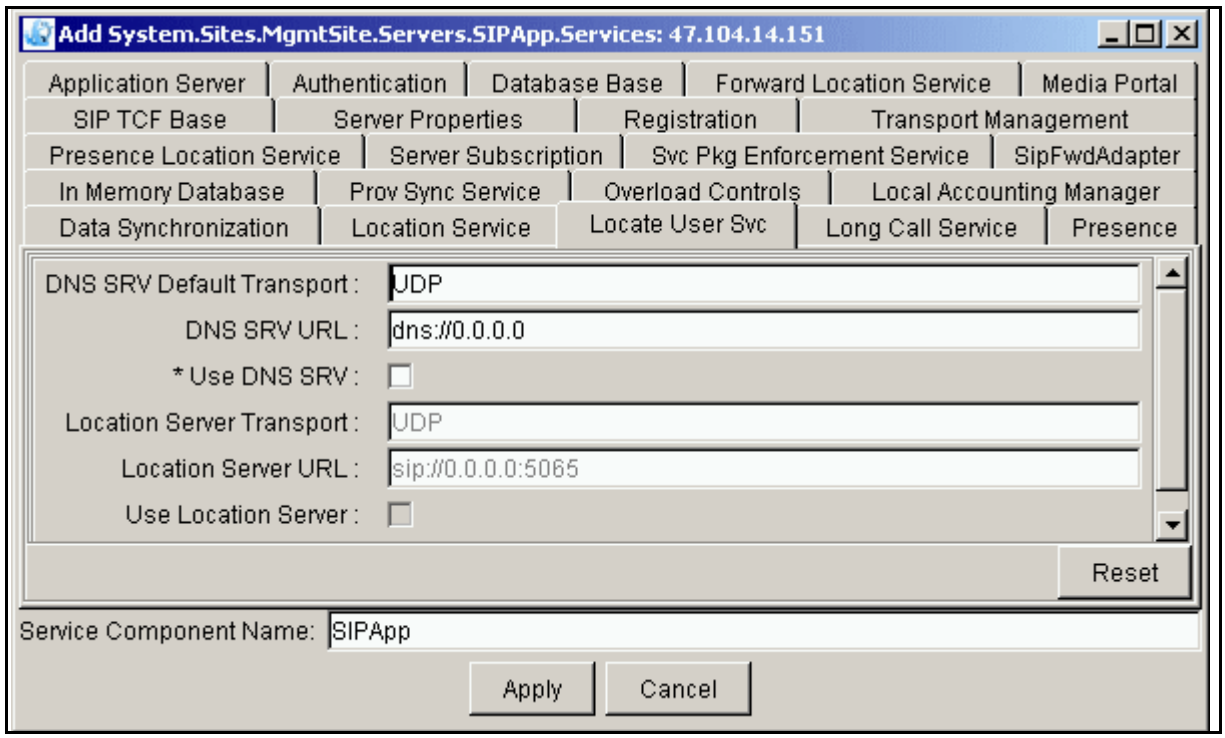


Table 9 Locate User Svc tab field descriptions (Sheet 1 of 2)

Field	Value	Description
DNS SRV Default Transport	Type=string Range=UDP, TCP Default=UDP	This field indicates the transport type used to communicate with the DNS SRV server.
DNS SRV URL	Type=string Range=1-64 numbers Default=dns://0.0.0.0	This field indicates the address of the DNS SRV server.
Use DNS SRV	Type=checkbox Default=unchecked	If box is checked, then enter a URL in the DNS SRV URL field. Prefix that URL with dns://.
Location Server Transport	Type=string Default=UDP	This read-only field contains the transport type used to communicate with the Location Server.

Table 9 Locate User Svc tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Location Server URL	Range=1-64 numbers Default=sip://0.0.0.0:5065	This field indicates the address of the Location Server.
Use Location Server	Type=checkbox Default=unchecked	This field is not used.

9 Click on the Data Synchronization tab. This tab allows the service provider to set the context and expiration information relating to the synchronization of in-memory and persistent data.

Figure 16 Completing the Data Synchronization tab fields

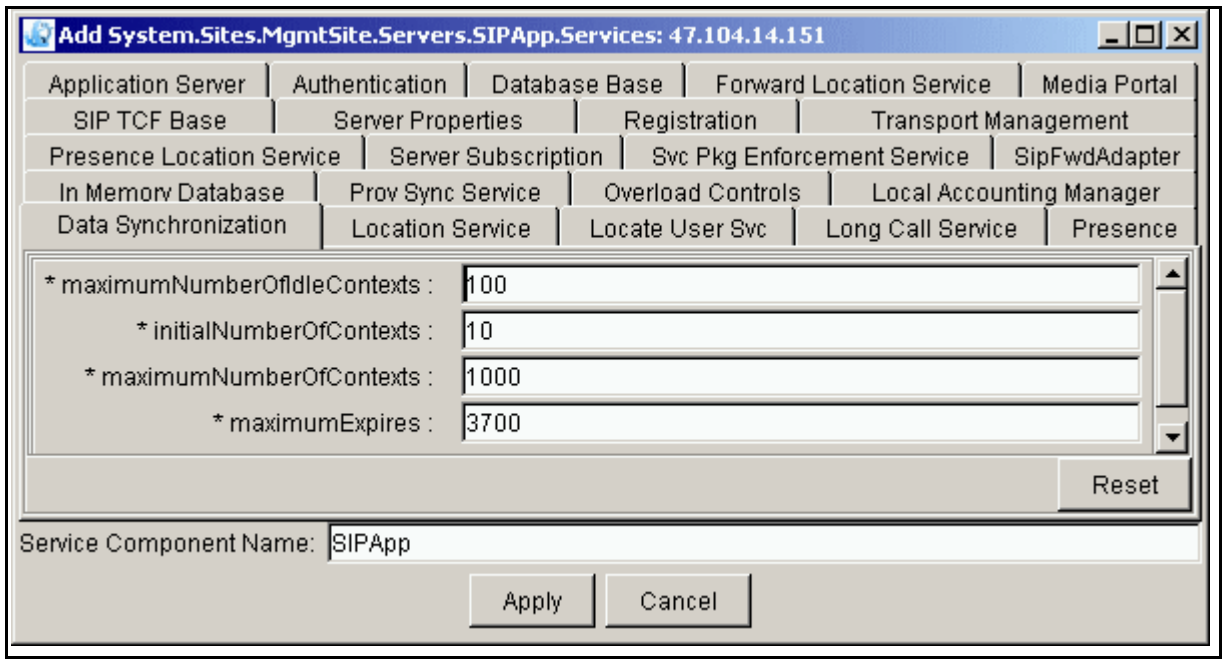


Table 10 Data Synchronization tab field descriptions

Field	Value	Description
maximumNumberofIdleContexts	Type=integer Range=1-10000 numbers Default=100	This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
initialNumberofContexts	Type=integer Range=1-10000 numbers Default=10	This is the initial number of contexts to create. It should not exceed the maximum number of contexts.
maximumNumberOfContexts	Type=integer Range=1-10000 numbers Default=1000	This is the maximum number of contexts to create.
maximumExpires	Type=integer Range=60- 86400 seconds Default=3700	This is the maximum allowable expiration value for a DataSync subscription request, in seconds.

10 Click on the Prov Sync Service tab. The **Prov Sync Service** parameter forwards provisioning modifications on user and device records to the SIP Application Module whenever modifications occur or when additions or deletions are made.

The Prov Sync Service tab allows the SIP Application Module to keep its configuration data updated with any changes that are made through the Provisioning Client web page. This tab also allows service providers to set how often the SIP Application Module queries the database for provisioning changes.

Modifications to this tab require that the Prov Sync Service be locked.

Figure 17 Completing the Prov Sync Service tab fields

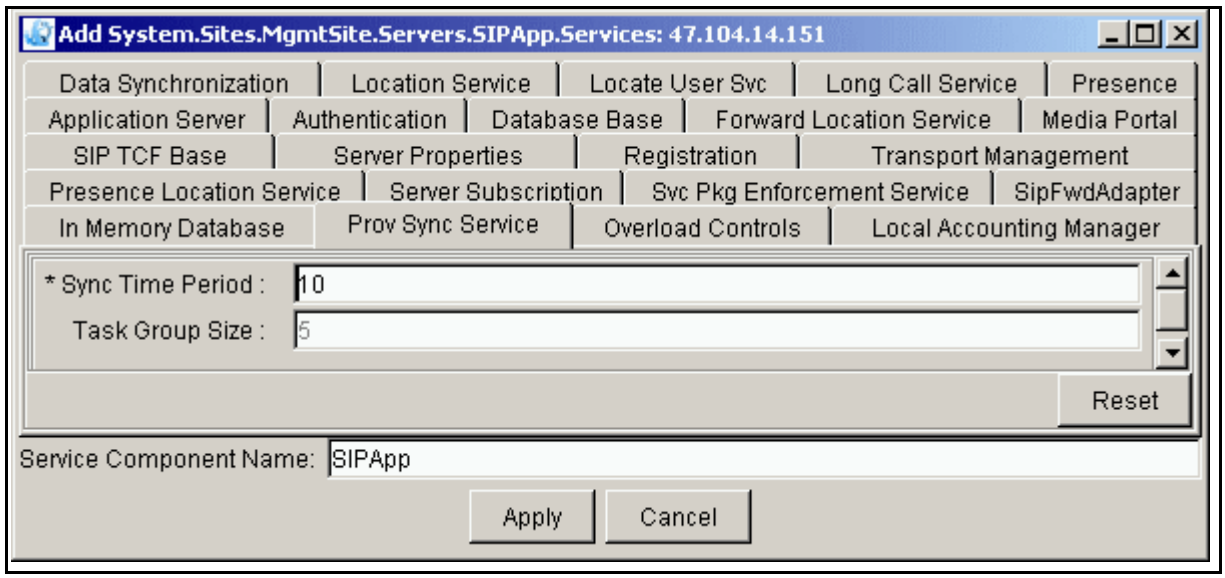


Table 11 Prov Sync Service tab field descriptions

Field	Value	Description
Sync Time Period	Type=integer Range=5-60000 seconds Default=10	This field indicates how often (in seconds) the SIP Application Module queries the database for provisioning changes.
Task Group Size	Type=integer Default=5	This is a read-only field.

11 Click on the Overload Controls tab. This tab allows the service provider to set threshold alarm information and system resource collection intervals.

Figure 18 Completing the Overload Controls tab fields

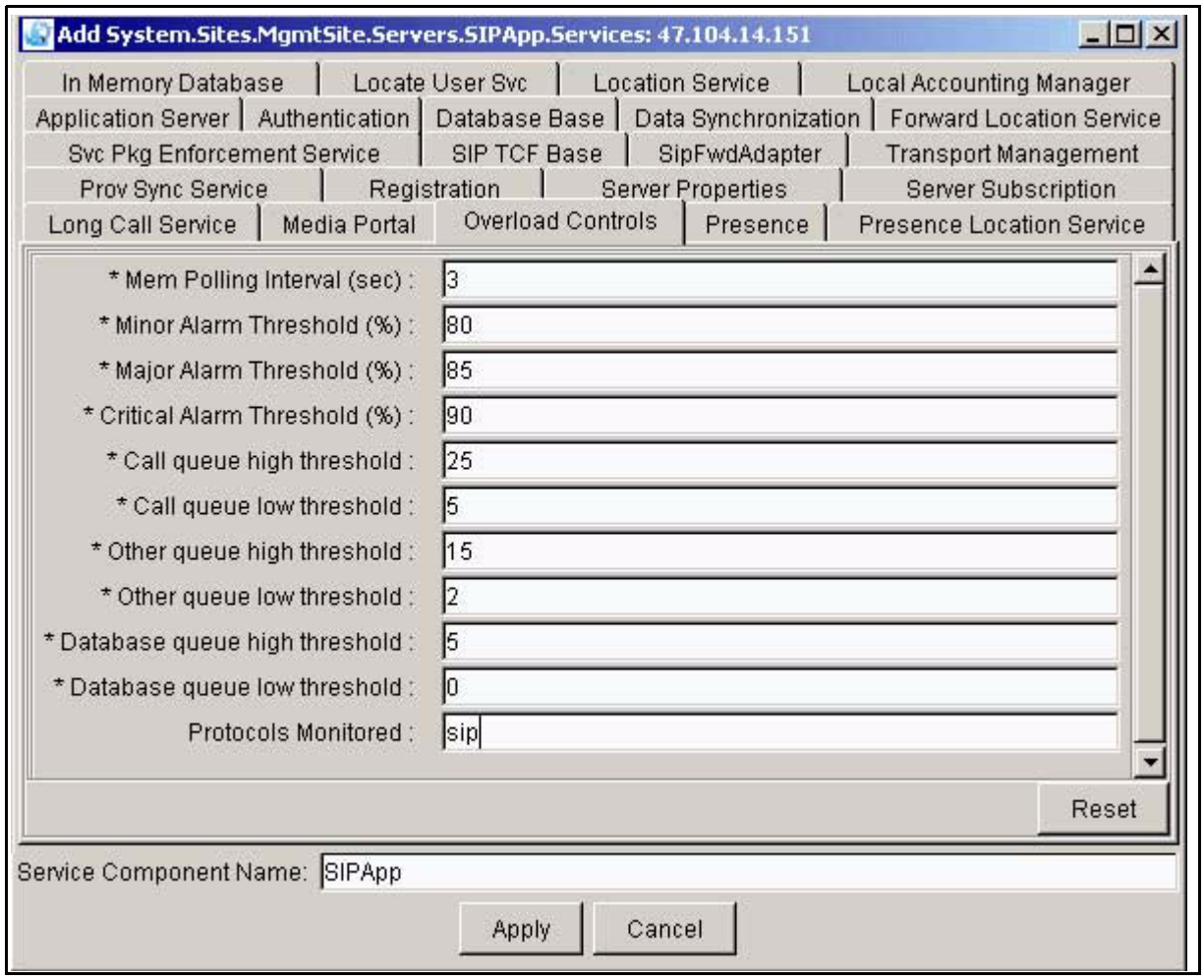


Table 12 Overload Controls tab field descriptions (Sheet 1 of 2)

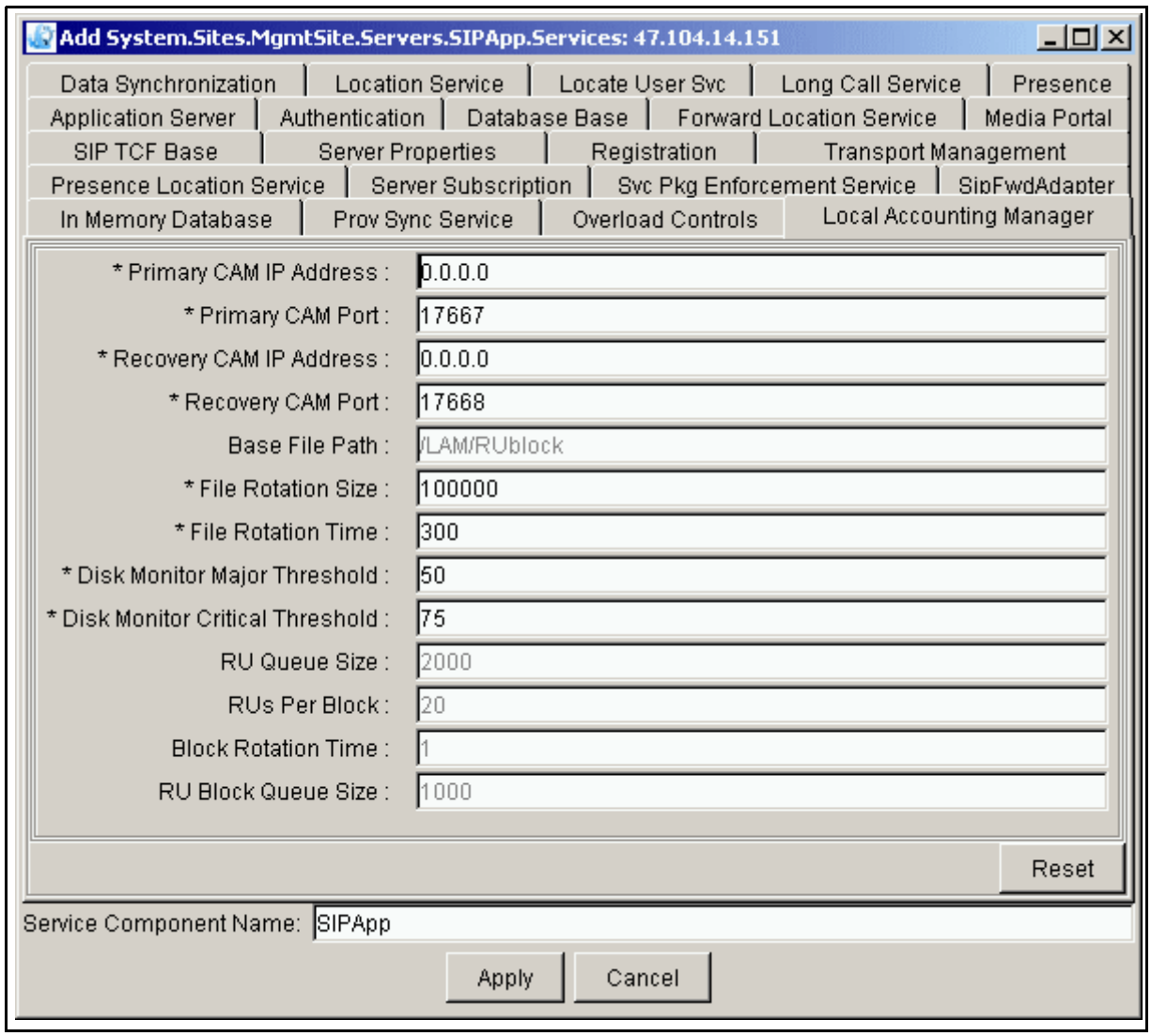
Field	Value	Description
Mem Polling Interval (sec)	Type=integer Range=a positive integer Default=3	This field indicates the number of seconds to wait in between checks on memory usage.
Minor Alarm Threshold (%)	Type=integer Range=0-100 numbers Default=80	This field indicates the threshold at which Minor overload is encountered for both CPU and memory.

Table 12 Overload Controls tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Major Alarm Threshold (%)	Type=integer Range=0-100 numbers Default=85	This field indicates the threshold at which a Major overload is encountered for both CPU and memory.
Critical Alarm Threshold (%)	Type=integer Range=0-100 numbers Default=90	This field indicates the threshold at which a Critical overload is encountered for both CPU and memory.
Call queue high threshold	Type=integer Range=1-500 numbers Default=25	This field contains the number of elements in the queue that, if exceeded, causes the system to disallow new calls.
Call queue low threshold	Type=integer Range=0-500 numbers Default=5	This field contains the number of elements in the queue that causes the system to allow new calls.
Other queue high threshold	Type=integer Range=1-500 numbers Default=15	This field contains the number of elements in the queue that, if exceeded, causes the system to disallow other session types, such as registrations, instant messages, or subscriptions.
Other queue low threshold	Type=integer Range=0-500 numbers Default=2	This field contains the number of elements in the queue that causes the system to allow other session types.
Database queue high threshold	Type=integer Range=1-500 numbers Default=5	This field contains the number of elements in the queue that, if exceeded, causes a cluster overload.
Database queue low threshold	Type=integer Range=0-500 numbers Default=0	This field contains the number of elements in the queue that causes the cluster overload to clear.
Protocols Monitored	Type=string Range=0-1024 characters Default=sip	Plus sign (+)-delimited list of protocols whose IO queues are monitored for excessive delays.

12 Click on the Local Accounting Manager tab. For more information on the Local Accounting Manager tab fields, see the *MCP Accounting Module Basics* document. This tab contains information pertaining to the Accounting Manager and billing records, including IP addresses, ports, file rotation size and time, and recording unit queue size.

Figure 19 Completing the Local Accounting Manager tab fields



13 Click on the In Memory Database tab. This tab allows the service provider to set information relating to local domains, event subscriptions, and the nonce used for authentication.

Figure 20 Completing the In Memory Database tab fields

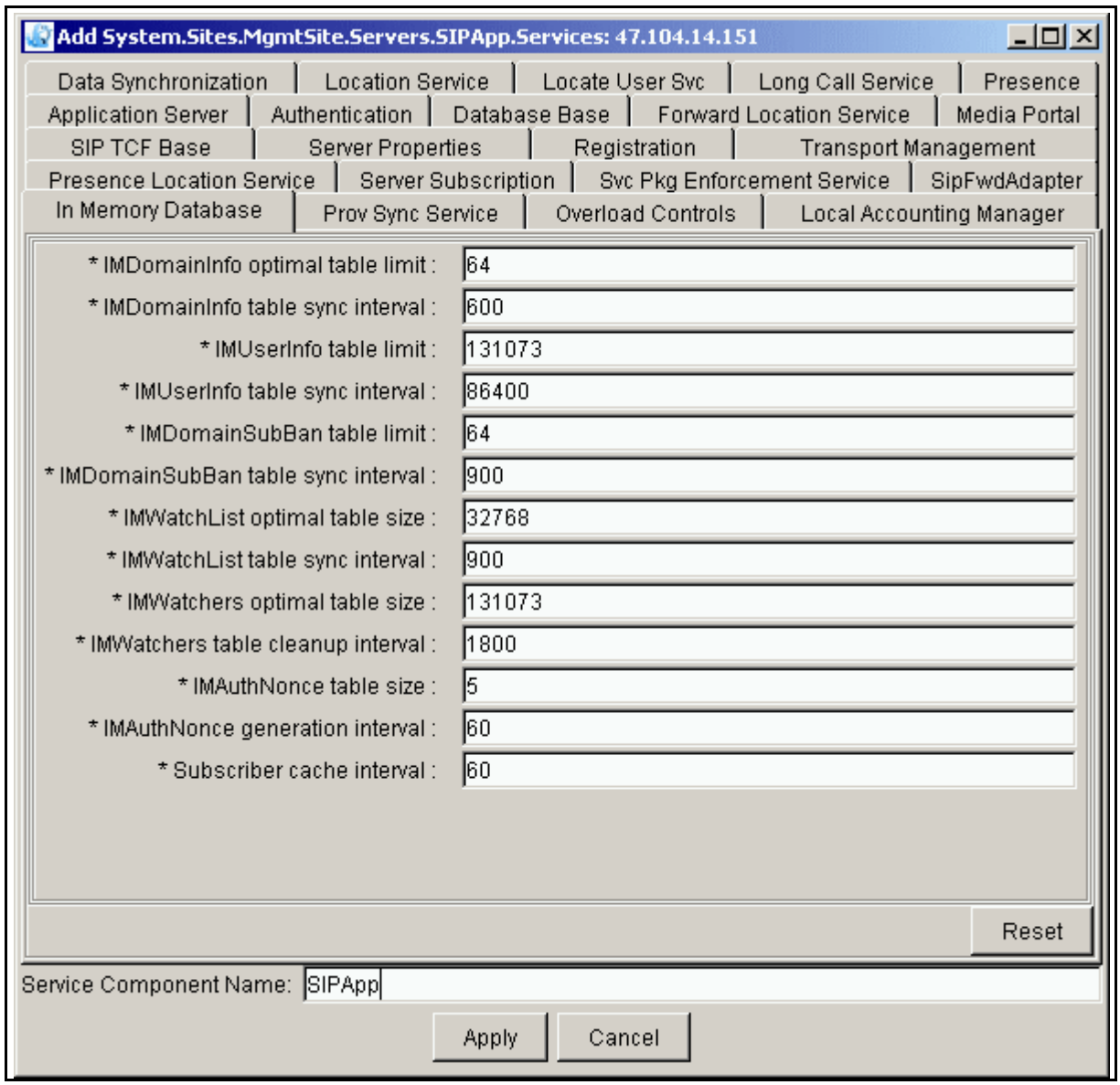


Table 13 In Memory Database tab field descriptions (Sheet 1 of 2)

Field	Value	Description
IMDomainInfo optimal table limit	Type=integer Range=16-MaxInt numbers Default=64	Set this to the number of domains and subdomains you expect to have.
IMDomainInfo table sync interval	Type=integer Range=300- 3600 numbers Default=600	Set this to however often you want the system to scan for changes to domain provisioning.
IMUserInfo table limit	Type=integer Range=32768-MaxInt numbers Default=131073	Set this to the number of users you expect to host.
IMUserInfo table sync interval	Type=integer Range=1800- 86400 numbers Default=1800	Set this to however often you want the system to scan for changes to the user's provisioned presence information.
IMDomainSubBan table limit	Type=integer Range=16-MaxInt numbers Default=64	Set this to the number of domains and subdomains you expect to have.
IMDomainSubBan table sync interval	Type=integer Range=300-86400 numbers Default=900	Set this to however often (in seconds) the SIP Application Module checks the database for changes in the domain ban information.
IMWatchList optimal table size	Type=integer Range=32768-MaxInt numbers Default=32768	Set this to the total number of user ban list entries you expect.
IMWatchList table sync interval	Type=integer Range=300-1800 numbers Default=900	Set this to however often (in seconds) the SIP Application Module checks the database for changes in the user ban information.

Table 13 In Memory Database tab field descriptions (Sheet 2 of 2)

Field	Value	Description
IMWatchers optimal table size	Type=integer Range=65536-MaxInt numbers Default=131073	Set this to the number of subscriptions expected at any interval in time.
IMWatchers table cleanup interval	Type=integer Range=300 to 86400 numbers Default=1800	Set this to however often (in seconds) you want the system to clear out any expired event subscriptions.
IMAuthNonce table size	Type=integer Range=1-10 numbers Default=5	Set how many nonces you want the system to keep for authentication.
IMAuthNonce generation interval	Type=integer Default=60	Sets how often (in seconds) the system creates a new nonce. This is a read-only field.
Subscriber cache interval	Type=integer Range=60-3600 numbers Default=60	Set this to however long you want the system to cache, in memory, subscriber information from the database, in seconds.

14 Click on the Location Service tab. This tab allows the service provider to configure the use of off-board Location Servers for routing.

Figure 21 Completing the Location Service tab fields

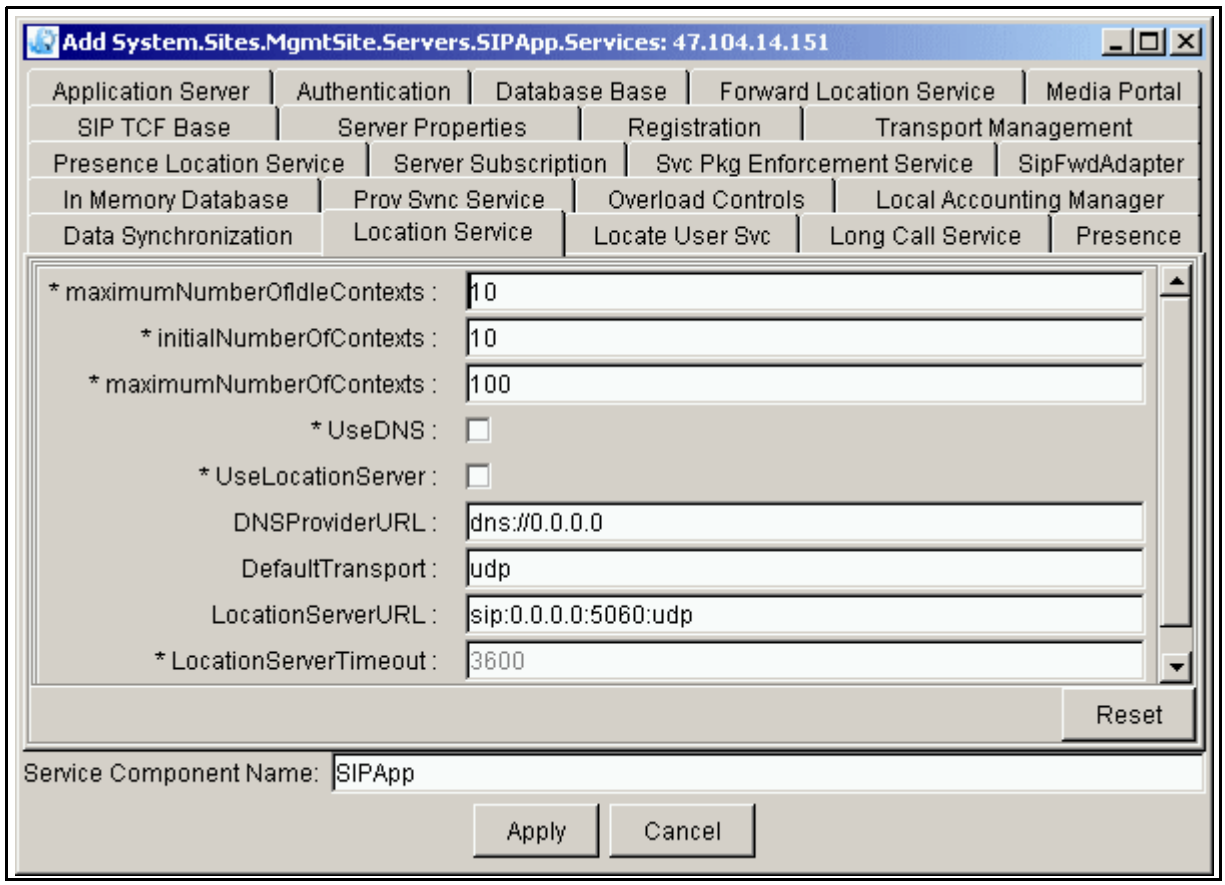


Table 14 Location Service tab field descriptions (Sheet 1 of 2)

Field	Value	Description
maximumNumberOf IdleContexts	Type=integer Range=1-512 numbers Default=10	This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
initialNumberOf Contexts	Type=integer Range=1-512 numbers Default=10	This is the initial number of contexts to create. It should not exceed the maximum number of contexts.

Table 14 Location Service tab field descriptions (Sheet 2 of 2)

Field	Value	Description
maximumNumberOf Contexts	Type=integer Range=1-512 numbers Default=100	This is the maximum number of contexts to create.
UseDNS	Type=checkbox Default=unchecked	Turns DNS server functionality on and off.
UseLocationServer	Type=checkbox Default=unchecked	Turns Location server functionality on and off.
DNSProviderURL	Type=string Range=0-1024 numbers Default=dns://0.0.0.0	This is the address of the DNS server.
DefaultTransport	Type=string Range=udp or tcp Default=udp	Transport type used to communicate with the DNS server.
LocationServerURL	Type=string Range=0-1024 numbers Default=sip://0.0.0.0:5060:udp	This is the address of the Location Server.
LocationServerTimeout	Type=integer Default=3600	This is a read-only field.

15 Click on the Forward Location Service tab. This tab allows the service provider to configure the use of off-board Location Servers for routing.

Figure 22 Completing the Forward Location Service tab fields

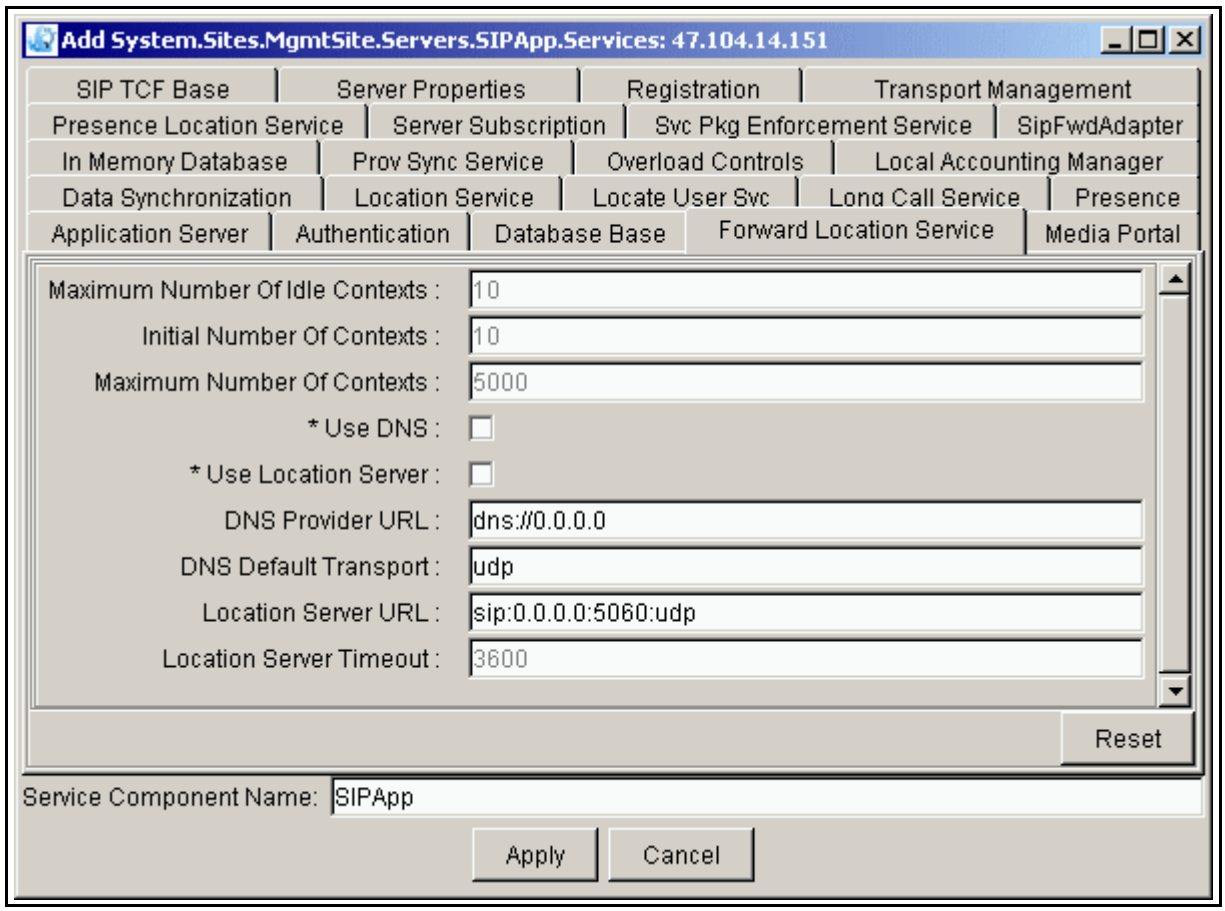


Table 15 Forward Location Service tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Maximum Number of Idle Contexts	Type=integer Range=1-100 numbers Default=10	This is a read-only field. This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
Initial Number of Contexts	Type=integer Range=1-100 numbers Default=10	This is a read-only field. This is the initial number of contexts to create. It should not exceed the maximum number of contexts.

Table 15 Forward Location Service tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Maximum Number Of Contexts	Type=integer Range=1-100 numbers Default=150	This is a read-only field. This is the maximum number of contexts to create.
Use DNS	Type=checkbox Default=unchecked	Turns DNS server functionality on and off. Check this field if you are using the DNSSvr service to resolve foreign domains.
Use Location Server	Type=checkbox Default=unchecked	Turns Location Server functionality on and off.
DNS Provider URL	Type=string Range=1-1024 numbers Default=dns://0.0.0.0	This field indicates the address of the DNS Server format >dns://0.0.0.0
DNS Default Transport	Type=string Range=udp, tcp Default=udp	Transport type used to communicate with the DNS server.
Location Server URL	Type=string Default=sip://0.0.0.0:5060:udp	This is the address of the Location Server.
Location Server Timeout	Type=string Default=3600	This field is only used with an offboard Location Server. This timeout value tells the Application Server how long to wait for an answer from the Location Server. If it didn't receive one in this time, the request would be failed.

16 Click on the Registration tab. This tab contains registration context information as well as the valid maximum expiration value for registrations.

Figure 23 Completing the Registration tab fields

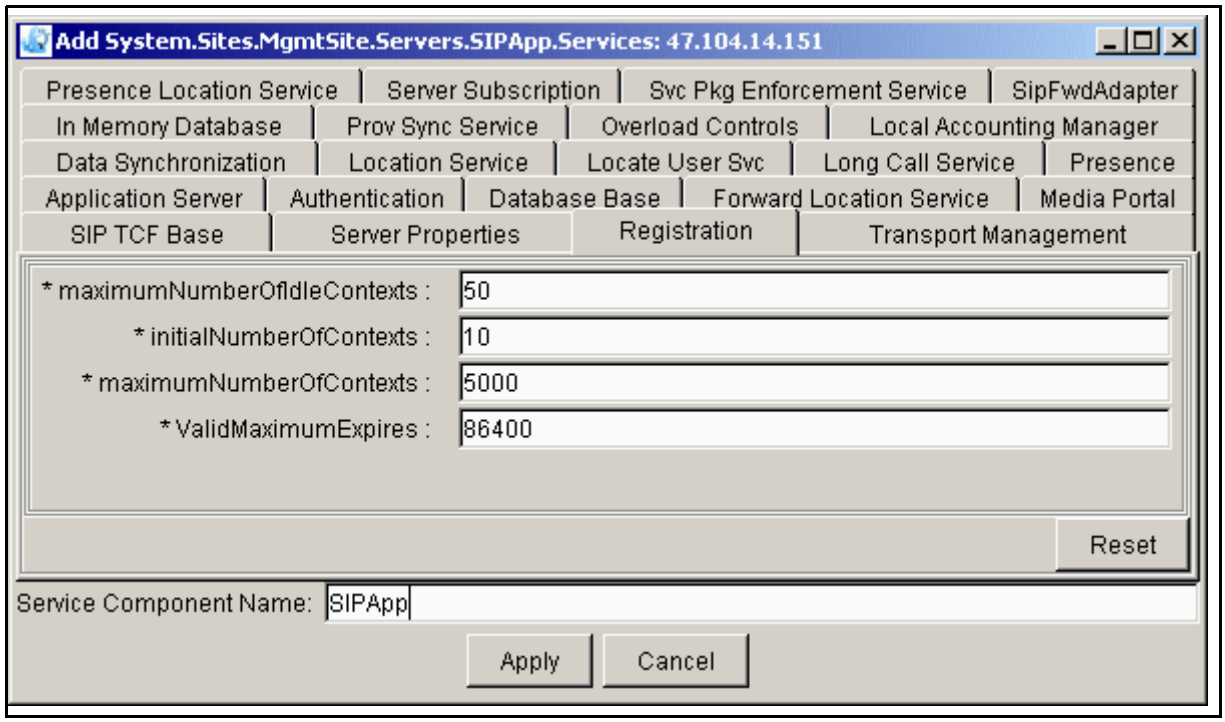


Table 16 Registration tab field descriptions

Field	Value	Description
maximumNumberOf IdleContexts	Type=integer Range=1-10000 numbers Default=50	This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
initialNumberOf Contexts	Type=integer Range=1-10000 numbers Default=10	This is the initial number of contexts to create. It should not exceed the maximum number of contexts.
maximumNumberOf Contexts	Type=integer Range=1-10000 numbers Default=5000	This is the maximum number of contexts to create.
Valid Maximum Expires	Type=integer Range=60-86400 numbers Default=86400	This is the maximum allowable expiration value for a registration request, in seconds.

17 Click on the Server Properties tab. This tab allows the service provider to set the system properties for the server.

Figure 24 Completing the Server Properties tab fields

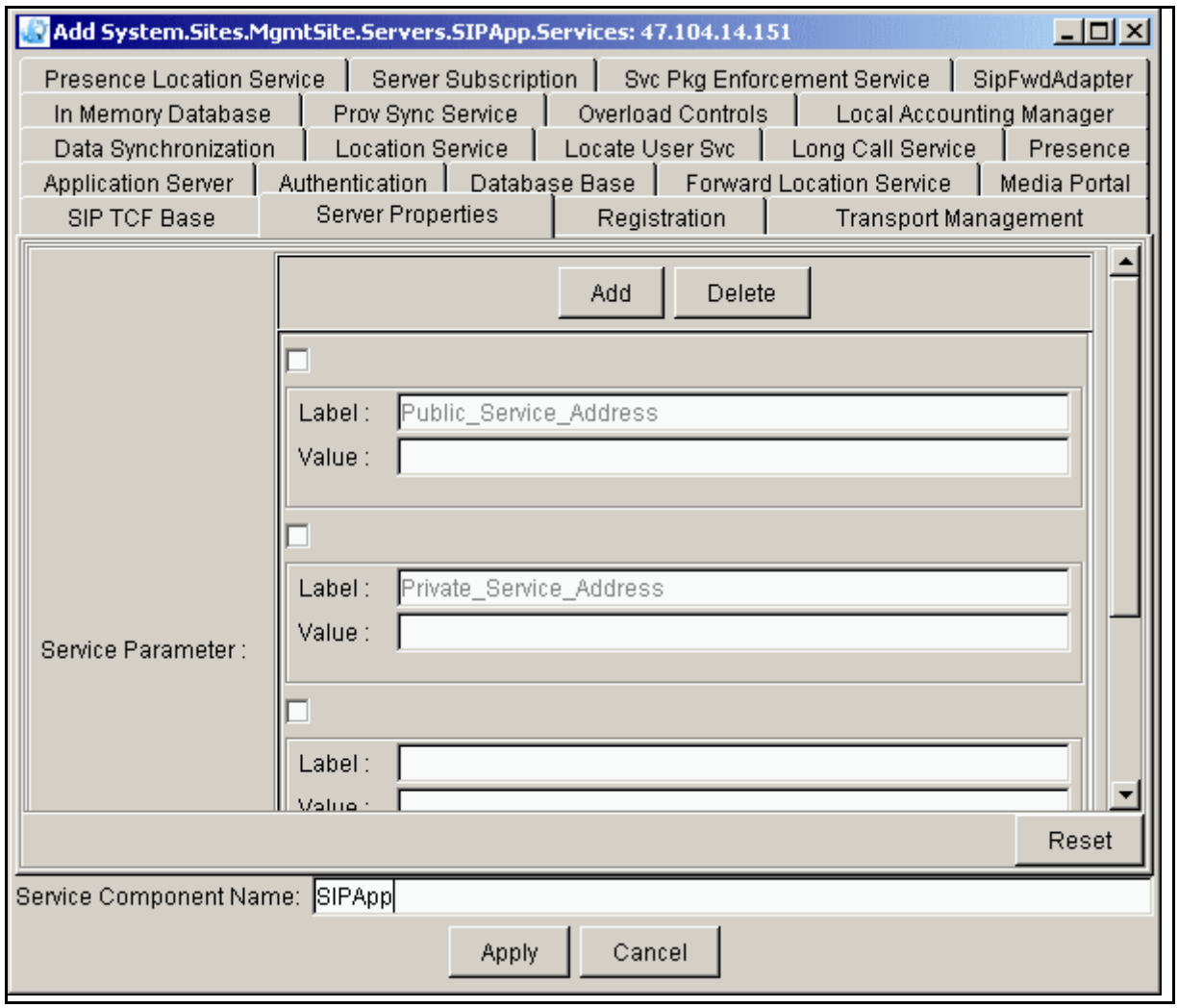


Table 17 Server Properties tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Label:	Type=string Range=1-80 characters Default=Public_Service_Address	This is a label that identifies the public address for the server.
Value	Type=string in the form of a valid IP address (x.x.x.x)	This field contains an IP address.

Table 17 Server Properties tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Label:	Type=string Range=N/A Default=Private_Service_Address	This is a label that identifies the private address for the Server. Only add an entry for a standalone configuration.
Value:	Type=string in the form of an IP address (x.x.x.x)	This field contains the private machine logical IP address of the SIP Application Module assigned to the label just above this field.
Label:	Type=string Range=1-80 characters Default=blank	This field contains a unique label to reference the value to the field directly below assigned below. Enter **server.gateways**. Only add an entry for redundant configurations.
Value:	Type=string Range=1-80 characters Default=blank	This field contains the nodes that the software needs to check upon boot up of this SIP Application Module. This value is assigned to the label just above this field.
Label:	Type=string Range=1-25 characters Default=blank	This field contains a unique label to reference the value. Enter **server.blade.host.label** for interworking with the RTP Media Portal. See Table 22, “Transport Management tab field descriptions,” on page 79, which contains the actual value of *private_static_address*. In other words, this is where a numeric IP address is assigned to the label *private_static_address*. The label *server.blade.host.label* has a value which is another label (*private_static_address*) whose value in turn is defined in the Transport Management tab.
Value:	Type=string Range=1-25 characters Default=blank	This field should contain the string *private_static_address*.

18 Click on the Server Subscription tab. This tab contains a list of the provisioning servers that the SIP Application Module can communicate with, as well as the context limits.

Figure 25 Completing the Server Subscription tab fields

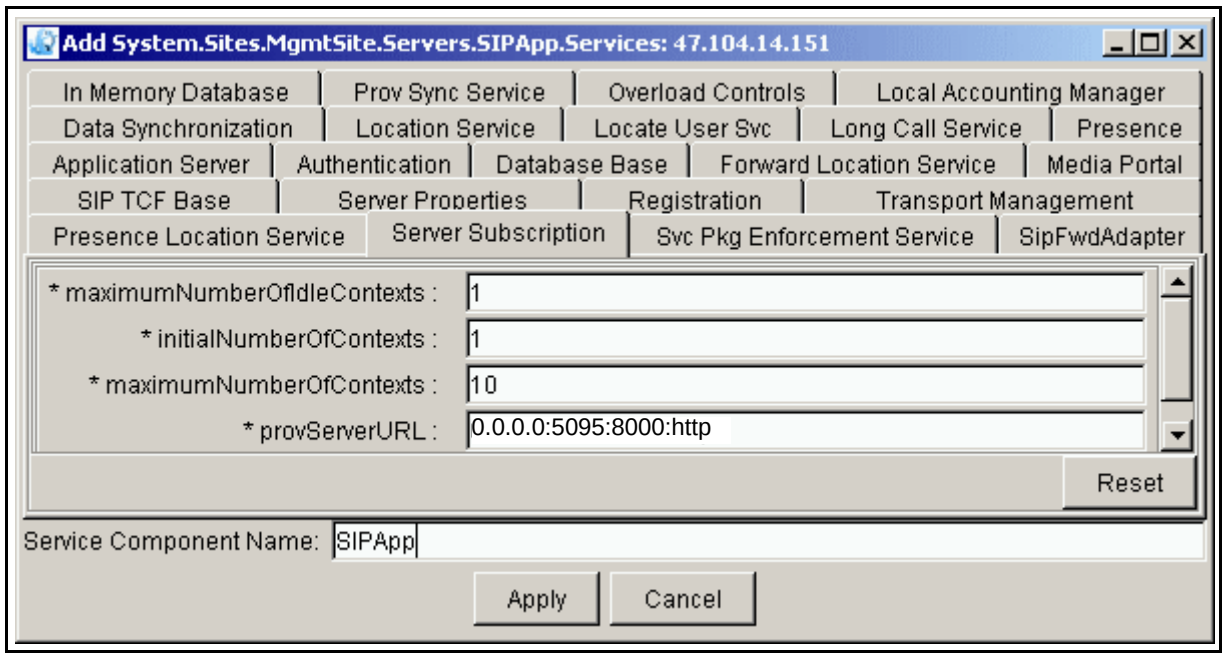


Table 18 Server Subscription tab field descriptions (Sheet 1 of 2)

Field	Value	Description
maximumNumberOf IdleContexts	Type=integer Range=1-10000 numbers Default=1	This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
initialNumberOf Contexts	Type=integer Range=1-10000 numbers Default=1	This is the initial number of contexts to create. It should not exceed the maximum number of contexts.

Table 18 Server Subscription tab field descriptions (Sheet 2 of 2)

Field	Value	Description
maximumNumberOf Contexts	Type=integer Range=1-10000 numbers Default=10	This is the maximum number of contexts to create. The range is 1 to 10000.
provServerURL	Type=string Range=0-4096 characters Default=0.0.0.0:5095:8000:http	The comma-delimited list of Provisioning Modules this server is to communicate with. Format is [IP ADDR]:[SIP PORT]:[HTTP PORT]:[PROTOCOL].

19 Click on the SIP TCF Base tab. The SIP TCF Base provides support for the SIP protocol. The SIP Application Module is one of several components that use the SIP TCF Base. See “Additional SIP TCF Base tab configuration information” on page 90 for more information. The SIP TCF Base contains many parameters pertaining to the SIP Application Module’s transport configuration. It includes information regarding the transport IP addresses/ports, timers, number of redirects, and retransmission, among other items. Modifications to the SIP TCF Base tab require that the SIP TCF Base be locked.

Figure 26 Completing the SIP TCF Base tab fields

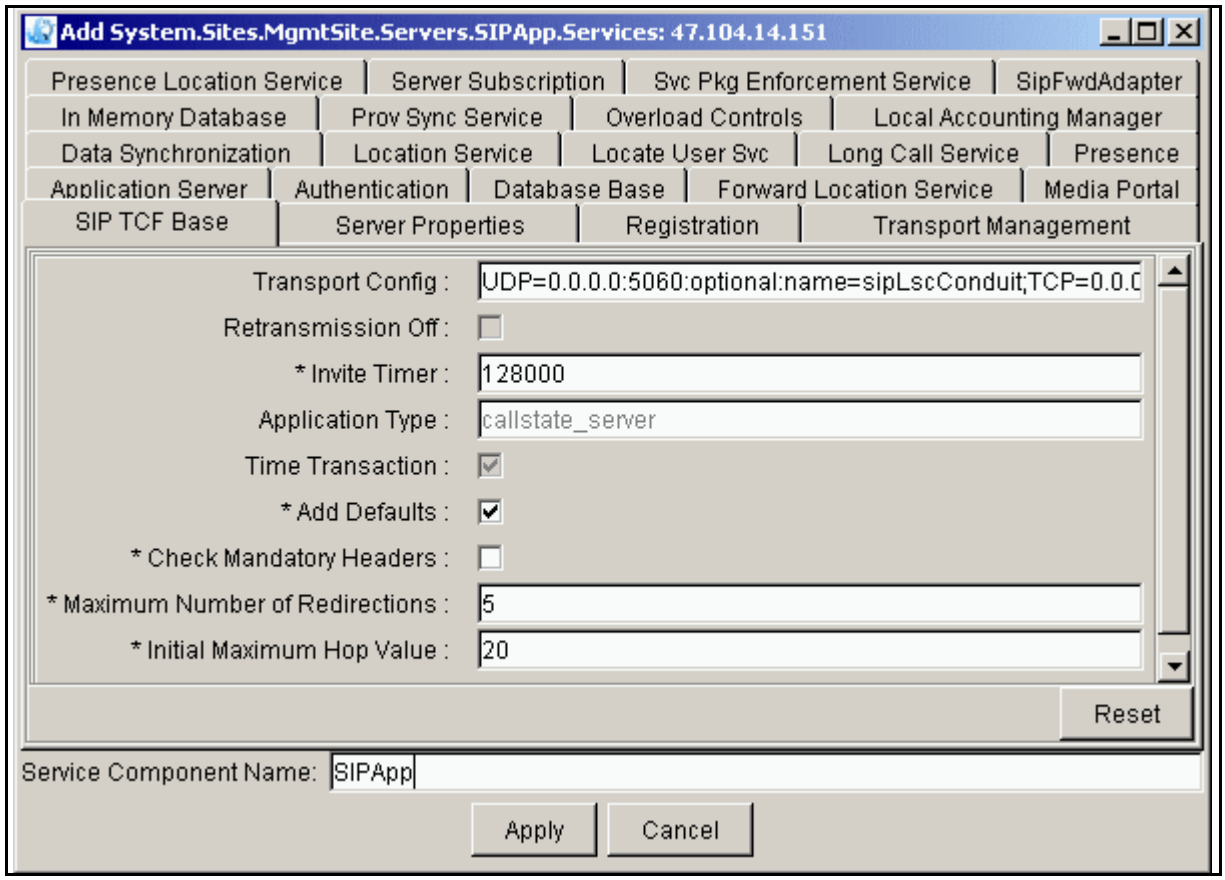


Table 19 SIP TCF Base tab field descriptions (Sheet 1 of 2)

Field	Value	Description
Transport Config	Type=string Default=UDP=0.0.0.0:5060:optional:name=sipLscConduit;TCP=0.0.0.0:5060:optional:name=sipLscConduit	Specifies the transport, IP addresses, and ports. Includes both the public and private interfaces. If your system consists of only public IPs, do NOT duplicate the string. This field indicates the public IPs for the UDP and TCP portions only. Transports can appear more than once. Use this field only for a standalone system. Enter the machine logical IP address of the SIP Application Module. For redundant configurations, leave this field blank.
Retransmission Off	Type=checkbox Default=unchecked	This is a read-only field that controls SIP retransmissions.

Table 19 SIP TCF Base tab field descriptions (Sheet 2 of 2)

Field	Value	Description
Invite Timer	Type=integer Range=120000-3600000 numbers Default=128000	This controls the maximum time in milliseconds to wait for an INVITE to receive a Final Response after receiving a provisional Response.
Application Type	Type=string Range=callstate_server, stateful_server, stateless_server, user_agent Default=callstate_server	This is the type of SIP Server on the node.
Time Transaction	Type=checkbox Default=checked	This field specifies whether the SIP transactions should be timed. This field is read only.
Add Defaults	Type=checkbox Default=checked Recommendation is to check the box.	Specifies whether to fill in missing mandatory headers with default values in the SDP message bodies.
Check Mandatory Headers	Type=checkbox Default=unchecked Recommendation is NOT to check the box.	Controls whether the mandatory SDP headers are checked for presence in the SDP messages.
Maximum Number of Redirections	Type=integer Range=3-10 numbers Default=5	Maximum number of redirections allowed before a request is dropped.
Initial Maximum Hop Value	Type=integer Range=5-50 numbers Default=20	Maximum number of hops allowed before a request is dropped.

20 Click on the Svc Pkg Enforcement Service tab. This tab allows the service provider to toggle on and off the enforcement of audio conferencing and voicemail settings based on the user's service packages.

Figure 27 Completing the Svc Pkg Enforcement Service tab fields

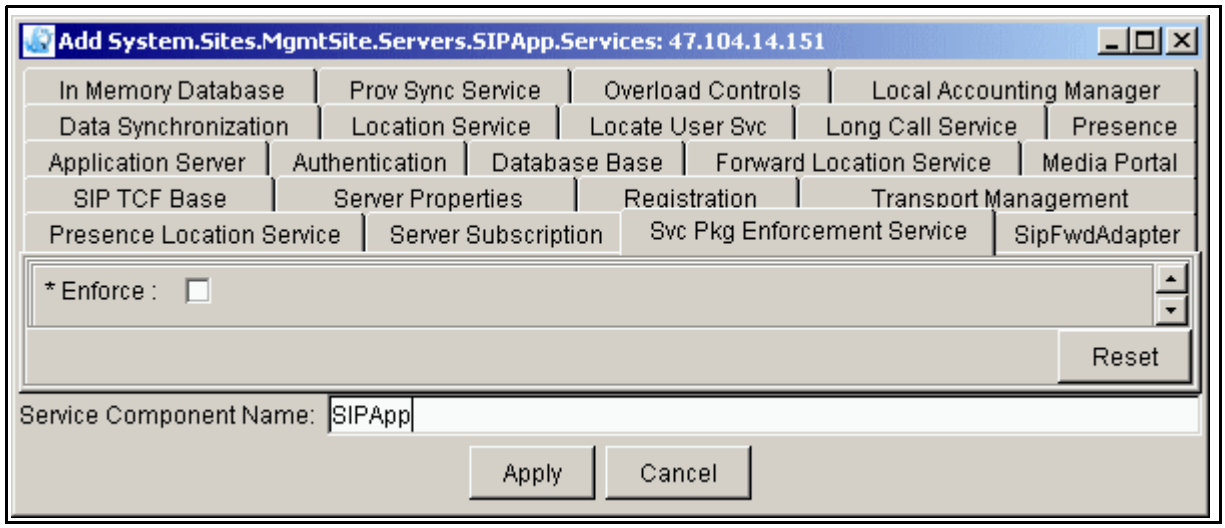


Table 20 Svc Pkg Enforcement Service tab field descriptions

Field	Value	Description
Enforce	Type=checkbox Default=unchecked	Turns on or off the server-based enforcement of Audio Conferencing and Voice Mail services based on users' Service Package settings. If you are only using clients, it is not necessary to check the box since the clients will perform the enforcement. If there are third-party clients, you may want to check the box so that the SIP Application Server will enforce the service package.

21 Click on the SipFwdAdapter tab. This tab allows the service provider to set the valid events that the SIP Application Module will process and determines whether or not the SIP Application Server will or will not forward messages to a foreign server.

Figure 28 Completing the SipFwdAdapter tab fields

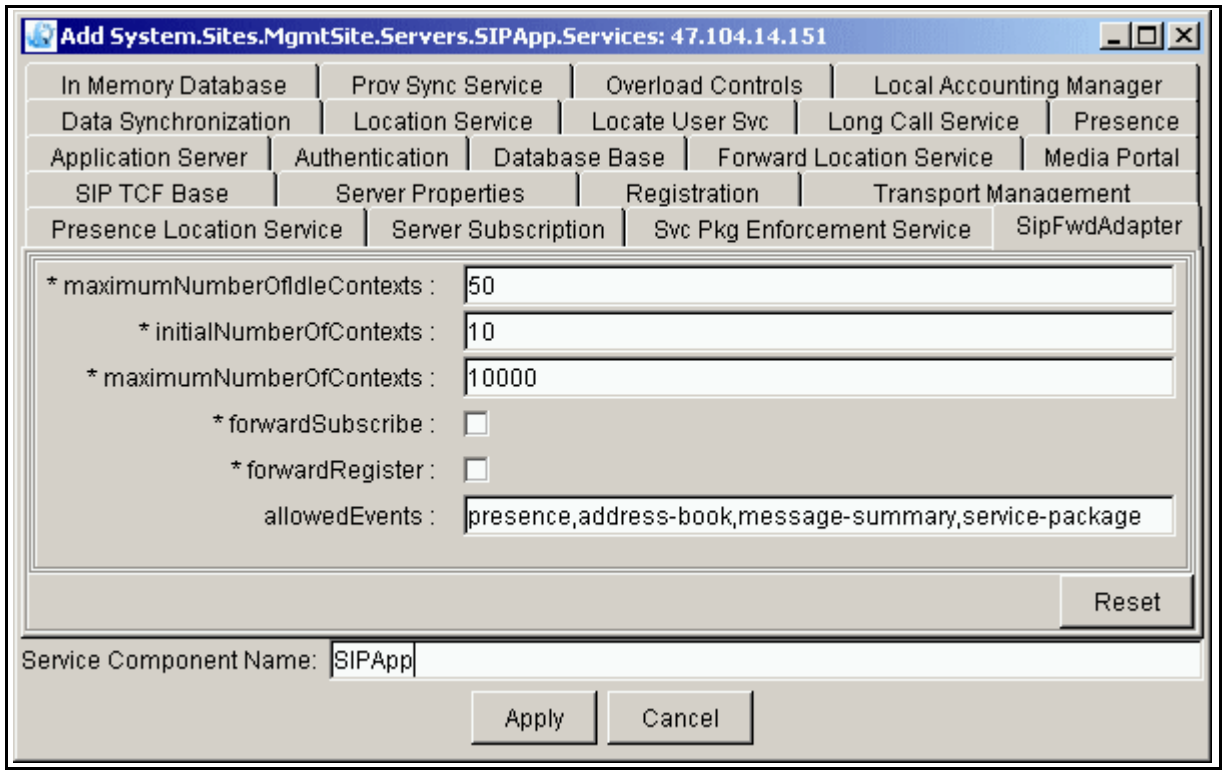


Table 21 SipFwdAdapter tab field descriptions (Sheet 1 of 2)

Field	Value	Description
maximumNumberOf IdleContexts	Type=integer Range=1-10000 numbers Default=50	This is the maximum number of idle contexts at any time. It should not exceed the maximum number of contexts.
initialNumberOf Contexts	Type=integer Range=1-10000 numbers Default=10	This is the initial number of contexts to create. It should not exceed the maximum number of contexts.
maximumNumberOf Contexts	Type=integer Range=1-10000 numbers Default=5000	This is the maximum number of contexts to create.

Table 21 SipFwdAdapter tab field descriptions (Sheet 2 of 2)

Field	Value	Description
forwardSubscribe	Type=checkbox Default=unchecked	If box is checked, the system allows subscribe messages to be forwarded.
forwardRegister	Type=checkbox Default=unchecked	If box is checked, the system allows register messages to be forwarded.
allowedEvents	Type=string Range=0-512 characters Default= presence, address-book, message-summary, service-package	This field indicates the valid event packages for the SIP Application Module to process.

22 Click on the Transport Management tab. This tab has a number of subfields. The next series of screens and tables give information on what data to enter and where to enter it. For more information on the function of this tab, see the section following, “Transport Management: Active-Hot Standby Server Heartbeat Mechanism” on page 87. This tab contains a large number of server and network service parameters that set protocols, transports, ports, and heartbeat information.

Figure 29 Completing the Transport Management tab fields

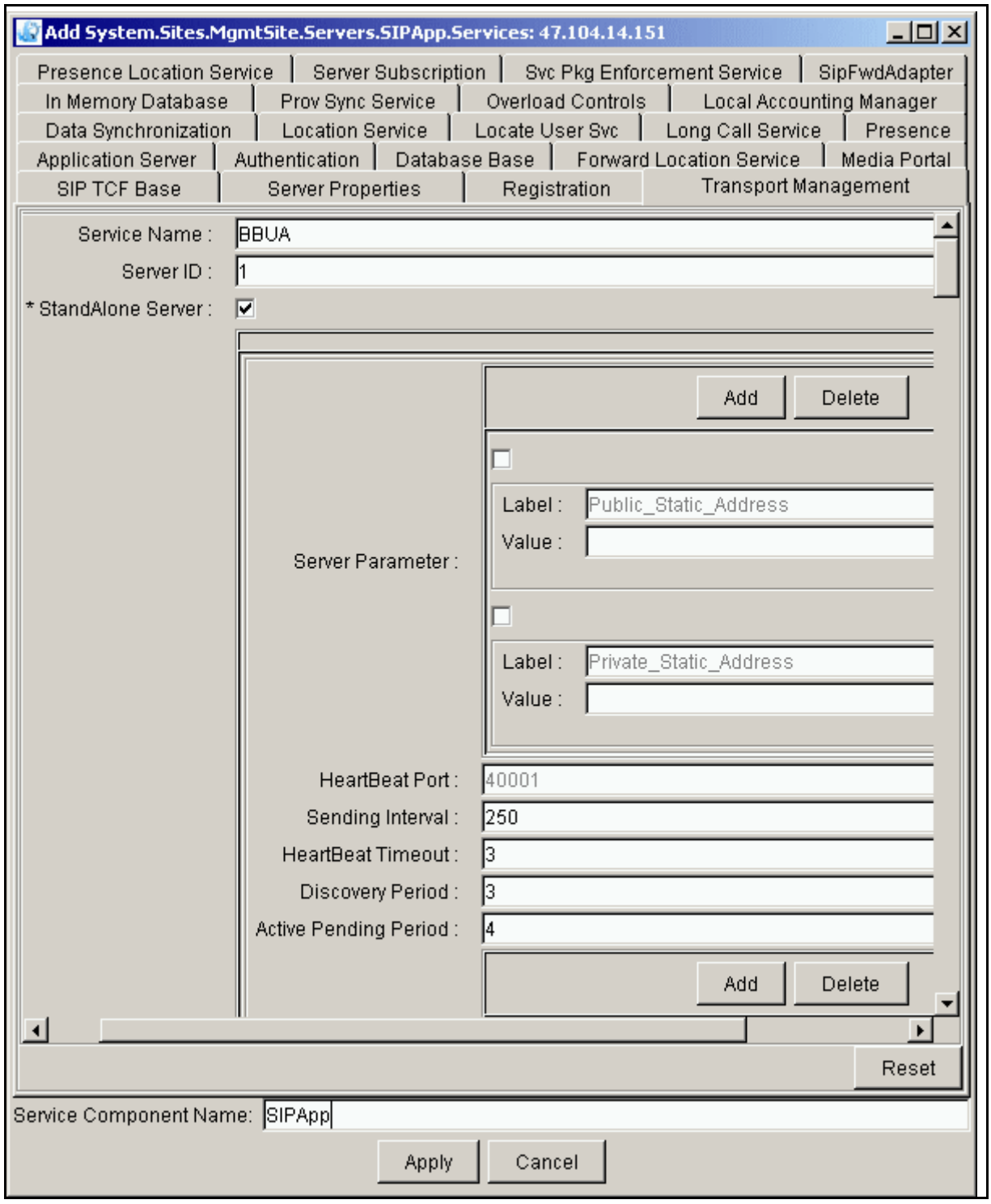


Table 22 Transport Management tab field descriptions (Sheet 1 of 3)

Field	Value	Description
Service Name	Type=string Range=1-20 characters Default=BBUA	This field indicates the name of the service this Reliability Manager is supporting.
Server ID	Type=integer Range=1-4 numbers Default=1	This field indicates the ID number for this server.
StandAlone Server	Type=checkbox Default=checked	Is the server standalone or part of a reliable group? Check the box if the server is standalone.
Label	Type=string Range=1-15 characters Default=Public_Static_Address	This field contains a unique label that references the value.
Value	Type=string in form of an IP address	This field contains the value to assign this label (IP address).
Label	Type=string Range=1-15 characters Default=Private_Static_Address	This is a unique label that references the value.
Value	Type=string in the form of an IP address	This field contains the value to assign this label (IP address).

Table 22 Transport Management tab field descriptions (Sheet 2 of 3)

Field	Value	Description
Label	Type=string Range=1-15 alphanumeric characters Default=Service_Node_Name	This is the name by which the CS 2000 knows an MCP server. This name has to be assigned to the service instance in the N+M configuration so it cannot be the node name of the platform. In addition it must contain no special characters like "_" or "-". It is defined in one of two places when the node is deployed from the management server. If the server is running as part of an N+M cluster then each service instance is defined as a service parameter in each Network Service Description (NSD) in the Transport Management tab. Each NSD has to define a unique service name. This is done by adding a service name of "Service_Node_Name" in the label field and the desired node name in the Value part. This information must then be datafilled in the CS 2000 as the name and IP from the NSD. If the system is not running the N+M then the service name needs to be added to the "Server Properties" tab. This information also needs to be entered on the CS 2000.
Value	Type=string in the form of an IP address Range=<host name of node>	This field contains the value to assign this label (IP address).
HeartBeat Port	Type=integer Range=40001 Default=40001	This is the port for all servers to use to send or receive reliability messages. This is a read-only field.
Sending Interval	Type=integer Range=50-2000 numbers Default=250	This is the interval in milliseconds between reliability messages.

Table 22 Transport Management tab field descriptions (Sheet 3 of 3)

Field	Value	Description
HeartBeat Timeout	Type=integer Range=1-10 numbers Default=3	This is the number of seconds before a server is declared failed.
Discovery Period	Type=integer Range=2-60 numbers Default=3	This is the number of seconds a server stays in Discovery Mode.
Active Pending Period	Type=integer Range=2-10 numbers Default=4	This is the number of seconds a server stays in Active Pending Mode.

Figure 30 Transport Management tab subfields, cont'd

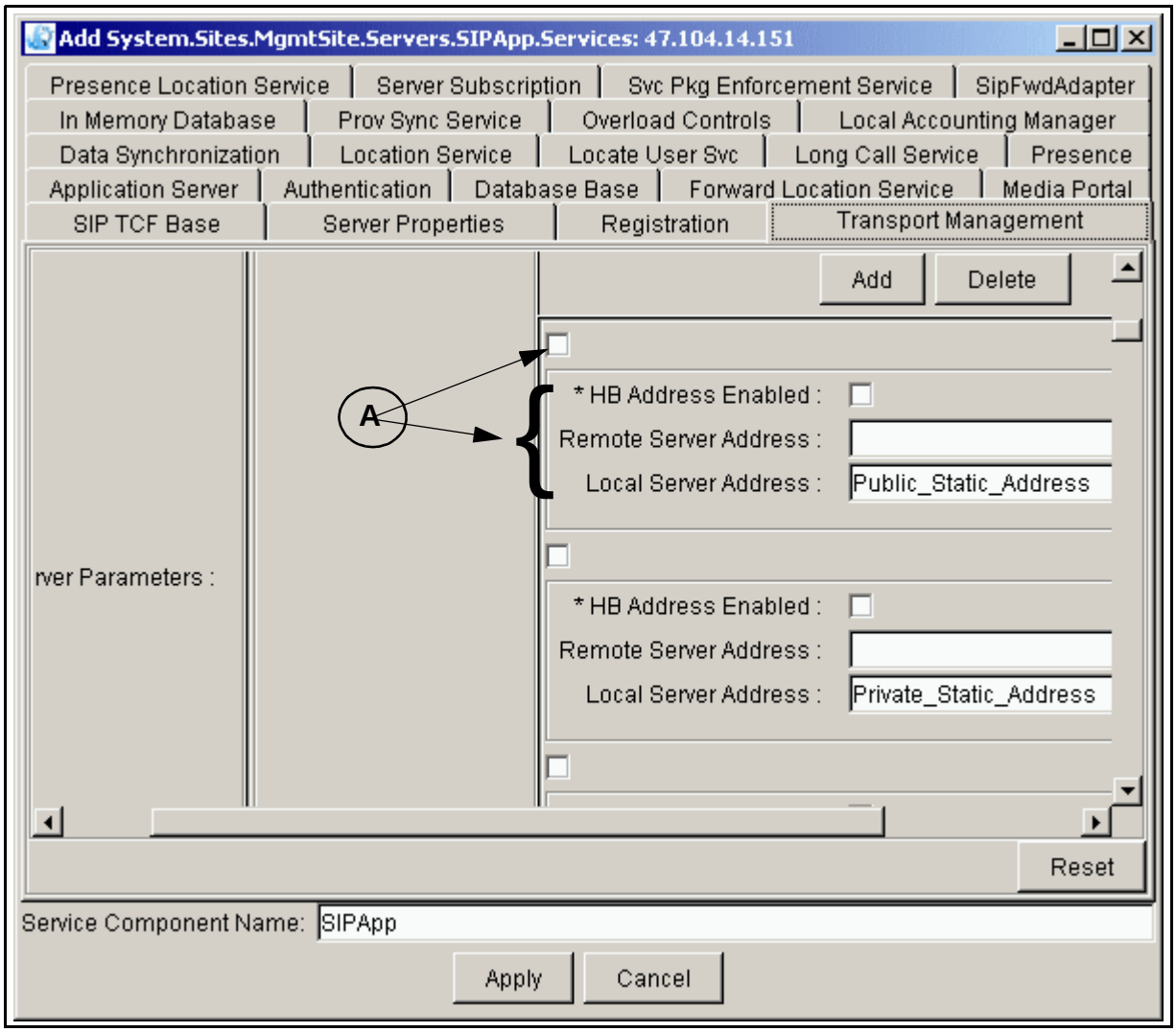


Table 23 Transport Management tab subfield descriptions, cont'd (Sheet 1 of 2)

Field	Value	Description
A	Type=checkbox Default=unchecked	Use these checkboxes when you want to delete a checkbox's relevant section, indicated by a bracket in the figure above.
HB Address: HB Address Enabled	Type=checkbox Default=unchecked	Check this checkbox to indicate that the address is enabled.

Table 23 Transport Management tab subfield descriptions, cont'd (Sheet 2 of 2)

Field	Value	Description
HB Address: Remote Server Address	Type=string in the form of a valid IP address	This is the reliable IP address for a group server.
HB Address: Local Server Address	Type=string Range=1-50 characters Default=Private_Static_Address, Public_ Static_Address	This is the reliable IP address for a group server.

Figure 31 Transport Management tab subfields, cont'd

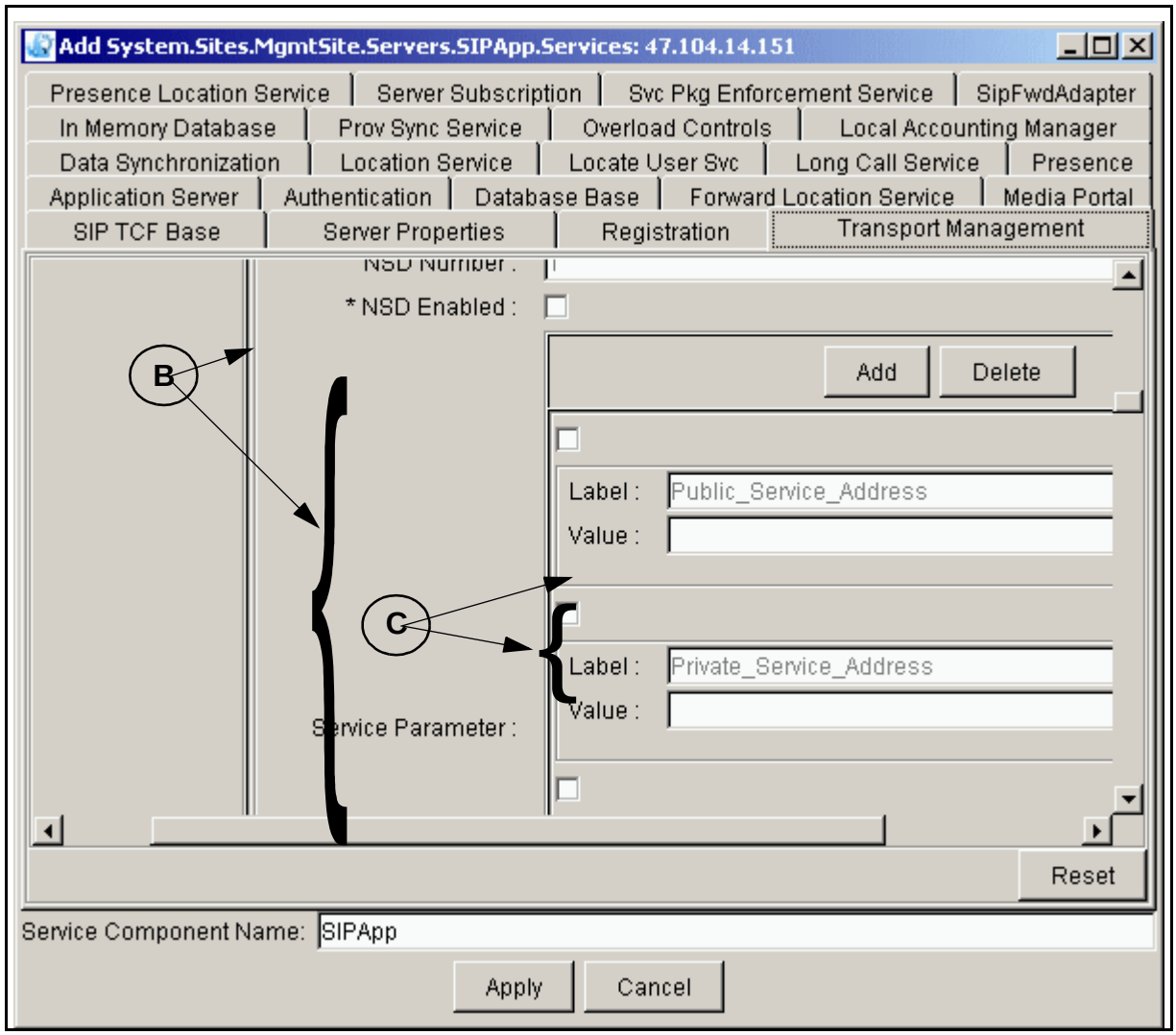


Table 24 Transport Management tab subfield descriptions, cont'd (Sheet 1 of 2)

Field	Value	Description
B/C	Type=checkbox Default=unchecked	Use these checkboxes when you want to delete a checkbox's relevant section, indicated by the brackets in the figure above.
NSD Number	Type=integer Range=1-3 numbers Default=1	This is the unique number for this Network Service Descriptor (NSD).

Table 24 Transport Management tab subfield descriptions, cont'd (Sheet 2 of 2)

Field	Value	Description
NSD Enabled	Type=checkbox Default=unchecked	Check the box if this NSD is enabled.
Service Parameter: Label	Type=string Range=1-15 characters Default=Private_Service_Address, Public_Service_Address	This is a unique label that references the value.
Service Parameter: Value	Type=string in the form of a valid IP address Range=1-15 numbers	This field contains the value to assign this label (IP address).

Figure 32 Transport Management tab subfields, cont'd

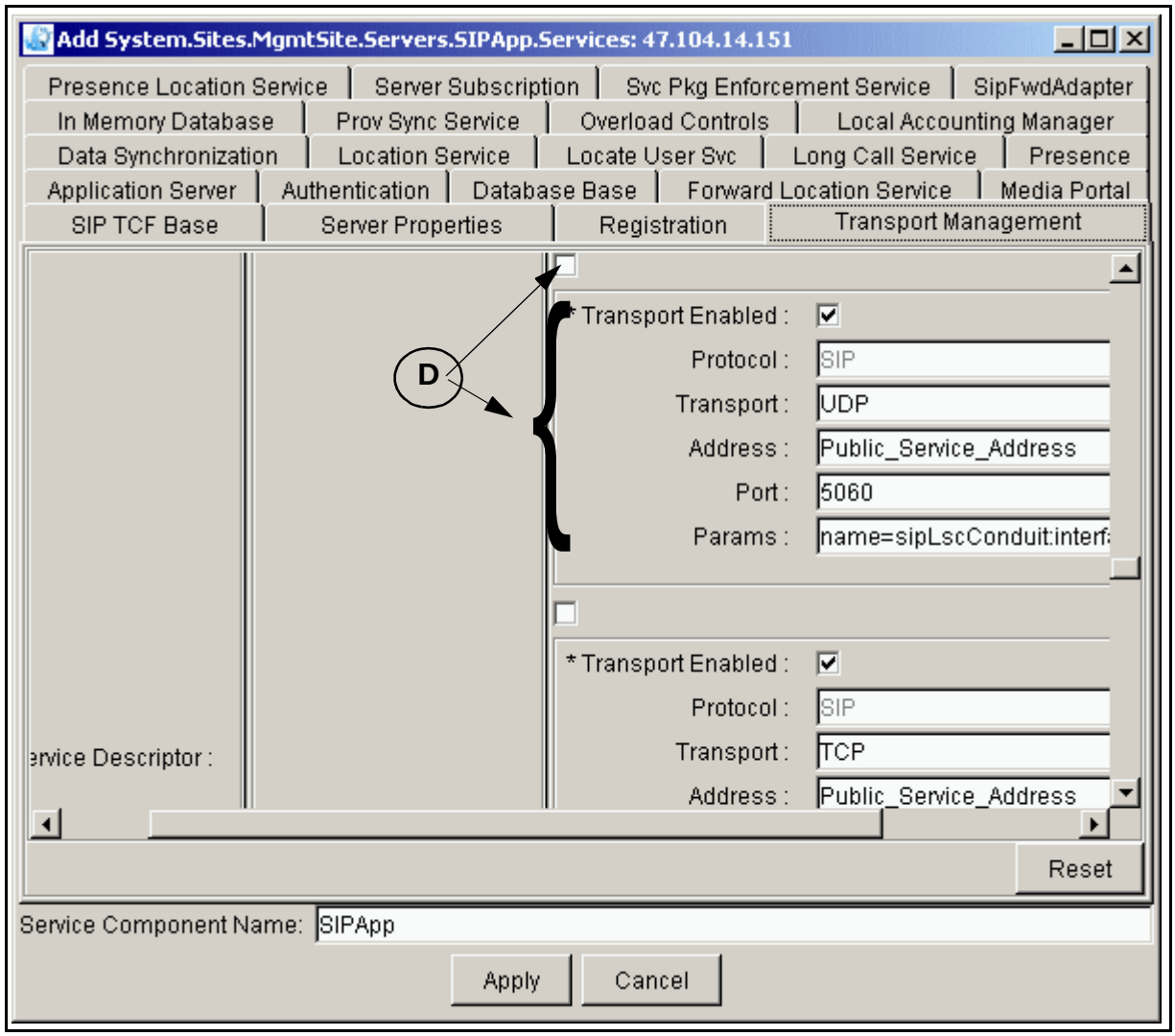


Table 25 Transport Management tab subfield descriptions, continued

Field	Value	Description
D	Type=checkbox Default=unchecked	Use this checkbox when you want to delete a checkbox's relevant section, indicated by the bracket in the figure above.
Interface Configuration: Transport Enabled	Type=checkbox Default=checked	Check the box if this Transport is enabled.
Interface Configuration: Protocol	Type=string Default=SIP	This is the protocol this interface supports.
Interface Configuration: Transport	Type=string Range=TCP or UDP Default=UDP	This is the transport for this interface.
Interface Configuration: Address	Type=string Range=1-50 characters Default=Private_Service_Address, Public_Service_Address	This is the service IP address label.
Interface Configuration: Port	Type=string Range=1024-65535 numbers Default=5060	This is the port for this interface. The range is 1024 to 65535.
Interface Configuration: Params	Type=string Default=name=sipLscConduit:interface=qfe0	These are the optional parameters for this interface.
Note: Scroll down to repeat entries in these subfields as needed.		

Transport Management: Active-Hot Standby Server Heartbeat Mechanism

The Transport Manager (referred to as the reliability managed object) is responsible for the heartbeat communication and state maintenance between the Application Modules. This software is responsible for monitoring the health and communicating the status of a Network Service Descriptor (NSD) across servers. Status communication and heartbeating occurs across all provisioned interfaces.

The heartbeat data in the Transport Manager defines a server group. Each server in a group includes provisioning for the static public and private address of every other server in that group. Each server in a

group consisting of four servers has provisioning for three public static heartbeat addresses and three private static heartbeat addresses.

The only time when this condition may not hold is when a new server is being introduced into an existing group that is currently providing service. In this case, the new server is provisioned with the information for all the other servers while the other servers are not yet updated with provisioning for the new server.

The reliability manager is configured by provisioning of engineering- and network-related parameters. The engineering parameters determine the timeout intervals and failure detection thresholds. The NSD parameters define the visible network interfaces used by the reliable services. The reliability manager service defines all the NSD data for the set of servers.

Note that checkboxes exist within several of the configuration data areas to enable or disable use of the data. In some cases, not all items are provisioned. For these cases, do not select those checkboxes.

The provisioning also allows for the use of label/value pairs. Where noted, you can use an address label in place of an explict address. This capability simplifies the configuration process where the same data are provisioned multiple times. For the Transport Manager configuration, the Module Parameter label/value pairs are values associated with the entire component (the SIP Application Module). The Service Parameters apply only to the service instance.

The default configuration includes, in the Server Parameter fields, Public_Static_Address and Private_Static_Address labels. These refer to the fixed IP addresses of the server. In the Network Service Descriptor area, the Service Parameter label/value pairs define the Public_Service_Address and the Private_Service_Address. These labels refer to the service addresses for a particular service instance that could be enabled on any one of many servers in the service NSD group.

Active-standby server group configuration

Configuration of an active-standby server group occurs as part of the normal deployment process. When servers are deployed, the administrator is prompted for configuration data specific to that component. During deployment, the administrator will see a configuration tab called Transport Manager. There is one set of fields for the engineering parameter data, one set of fields for the Heartbeat Parameters, and multiple sets of fields for the NSD data.

Each NSD bean describes the network interfaces and protocols to be managed by the service being deployed under normal operating conditions. Configuration of the servers in the active-standby group occurs independently. The system manager is not aware of any relationship between the servers. Therefore, take care to configure the server group so that the reliability service functions properly.

When using the reliability manager, the administrator must ensure that conflicts with other managed-objects do not occur. Configuration data for the reliability manager replaces similar configuration data that may have previously been found in the configuration data of other managed-objects. The reliability manager internally launches network services by communicating with other managed-objects in the system (through the service registry). The reliability manager passes this data to the transport controller during system initialization and state transitions.

When provisioning for reliability, leave the SIP transport parameters in the SIP Configuration tab blank. A set of equivalent fields are provisioned in the Transport Management dialog box instead. All other provisioning is unaffected.

The SIP Application Module, when running in reliable mode, requires public and private service addresses for each service instance (a service instance is a “virtual” application server that can exist on one of any number of physical servers). These service addresses are what other clients and servers use to communicate with the application server instances (note that the Management Module is configured to use the static addresses of the previous section).

A 1+1 reliable SIP Application Module configuration (one active and one standby server with one service instance) needs seven addresses on the public network and seven addresses on the private network (total for both servers).

Configuration of the NSD is what defines those SIP Application Module network services that require reliability. If there are two physical servers in a 1+1 configuration, there must be one active NSD. Each active NSD describes the SIP services to activate on an active server. The servers in the group negotiate which NSDs each will activate. The server that finds all NSDs already activated automatically becomes a standby server.

Each enabled NSD must define a unique public and private service address and may define other instance specific properties. Note that the public and private service address tag values (their provisioned IP addresses) should be different from the provisioned static addresses.

Additional SIP TCF Base tab configuration information

This section contains additional configuration information for the IP and port properties under the SIP TCF Base tab.

TCF Config details

SIP server protocol, network, and ports are started based on the information in this parameter. The TCF Config syntax for this parameter follows:

```
<transport>=<host address>:<host port>:<optional
parameters>
```

You can define multiple transports by continuing this format with a semicolon separator.

The supported transports for SIP are UDP, TCP, and SSL. The format of the optional parameter in the configuration string is specific to each supported transport type and, for some transports, configuration information in the optional parameter is mandatory.

For TCF Config parameter values, refer to Table 26, “UDP/TCP/SSL Config values.”

Table 26 UDP/TCP/SSL Config values

Parameter	Value	Description
Host Address	IP v4 address	This field contains the address of the host on which you want the connection to open.
Host Port	Integer	This field contains the port on which to open the connection. The standard port for SIP is 5050.
Optional	hostaddr:<IPv4>	The hostaddr value specifies the primary public address of the SIP Application Module.

TCF Config parameter example 1, UDP, TCP

Example

```
UDP=192.168.0.1:5060;TCP=192.168.0.1:5060
```

Note: Do not use the IP addresses from this example in your network.

This example creates a general SIP server for TCP and UDP and starts execution of two SIP server ports on network address 192.168.0.1. The first server uses UDP/IP transport listening on port 5060. The second server uses TCP/IP accepting connections on port 5060.

```
UDP=192.168.0.1:5060:hostaddr:47.249.32.64
```

This example creates a SIP server for UDP on all interfaces on port 5060. This must be used on all application servers that span public/private networks.

This example creates an SSL server that can be used for secure communications with an SSL client application.

Example

```
UDP=192.168.0.1:5060;TCP=192.168.0.1:5060;SSL=192
.168.0.1:7020
```

Note: Do not use the IP addresses from this example in your network.

This example combines the five previous examples into one example that shows all transport services starting together on a single SIP server.

Note 1: Each transport specification is separated by a semicolon.

Note 2: Be sure to avoid address and port conflicts, which can cause service startup failure, and require re-configuration and server restart.

Retransmission Off parameter

When Retransmission Off is false, the SIP server follows the retransmission policies identified by the RFC 2543 (see note for specific reference) specification for SIP.

Note: J. Rosenberg et al, SIP: Session Initiation Protocol, Internet Draft draft-ietf-sip-rfc2543-bis09.txt, IETF, Feb 27, 2002.

When Retransmission Off is true, the SIP server does not retransmit SIP messages. This value is not changeable.

Invite Timer parameter

The Invite Timer value specifies the number of milliseconds a non-finalized SIP Invite transaction can remain open before it is forced closed. A SIP Invite transaction, having received a provisional response and waiting on a final response, is allowed to persist only as

long as this timer setting. Expiration of this timer causes resources allocated to the transaction to be released. Activation of this timer is controlled by the Time Transaction parameter.

When the Time Transaction value is true, the default value of 128,000 mS is used.

Time Transaction parameter

When the Time Transaction value is true, all transactions are timed. Invite transactions are forced closed and the Invite Timer duration has expired. For all other transactions, the time-out duration is fixed at 64000 mS.

Add Defaults parameter

When the Add Defaults value is set to true, SDP message bodies in SIP messages with missing mandatory SDP headers are regenerated with default mandatory headers. This occurs when messages are proxied through the SIP Application Module.

Note 1: Set this parameter to true when downstream servers fully support the SDP specification.

Note 2: Set this parameter to false when downstream servers do not fully support the SDP specification.

Check Mandatory Headers parameter

When the Check Mandatory Headers value is true, SDP messages are screened for required header content.

Note: Missing headers cause message rejection.

When the Check Mandatory Headers value is false, SDP messages are not screened for required header content.

OAM&P strategy

The SIP Application Module is fully integrated with the Management Module. Perform all configuration at the Management Console window. For additional information on the Management Module, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

Accounting management

The SIP Application Module does not do any accounting management. For more information on accounting, please see the *MCP Accounting Module Basics* document.

Performance management

The Management Module manages the performance functions for the SIP Application Module. For additional information on the Management Module, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

Security and Administration

How this chapter is organized

This chapter is organized as follows:

Security

The SIP Application Module with Back-to-Back User Agent functionality controls the Media Portal (Media NAT) over an MGCP-type protocol. The SIP Application Module ensures security of clients and the network in the following ways:

- Uses MGCP+ to communicate with the Media Portal (over the private LAN) to control which ports are opened or closed.
- All signaling traffic traverses the SIP Application Module. It is the only node to which clients terminate SIP signaling.
- Hides address assigned by the Enterprise NAT from other users.
- Helps maintain connection to clients through NAT and/or firewall by the keep-alive mechanism.
- Provides client authentication.
- Port 5060 is the only port required to be opened on the public interface.
- The SIP Application Module is managed from the private LAN. A management interface is not available from the public interface.

OAM&P strategy

The Management Module performs the security and administrative functions for the SIP Application Module. For additional information on the Management Module, refer to the *MCP Management Module Basics* and the *MCP System Management Console Basics* documents.

Appendix A: Basic call flows

Using SIP as the signaling protocol to establish a communication path between endpoints, the SIP Application Module provides the following call services:

- Voice plus video
- Call transfer
- Authentication

The following sections provide sample diagrams and descriptions of the call flows that enable these specific services. For an overview of a basic call flow, see the *MCP Basics* document.

Voice plus video

Figure 1, “Client-to-client voice plus video diagram,”and Figure 2, “Client-to-client voice plus video call flow,” show the basic call flow for a client-to-client voice-plus-video call. Each client in the diagram has a *User Agent*. The SIP Application Module provides Back-to-Back User Agent service, treating each SIP call as an independent Ingress and Egress leg. A detailed, step-by-step illustration follows this diagram.

Figure 1 Client-to-client voice plus video diagram

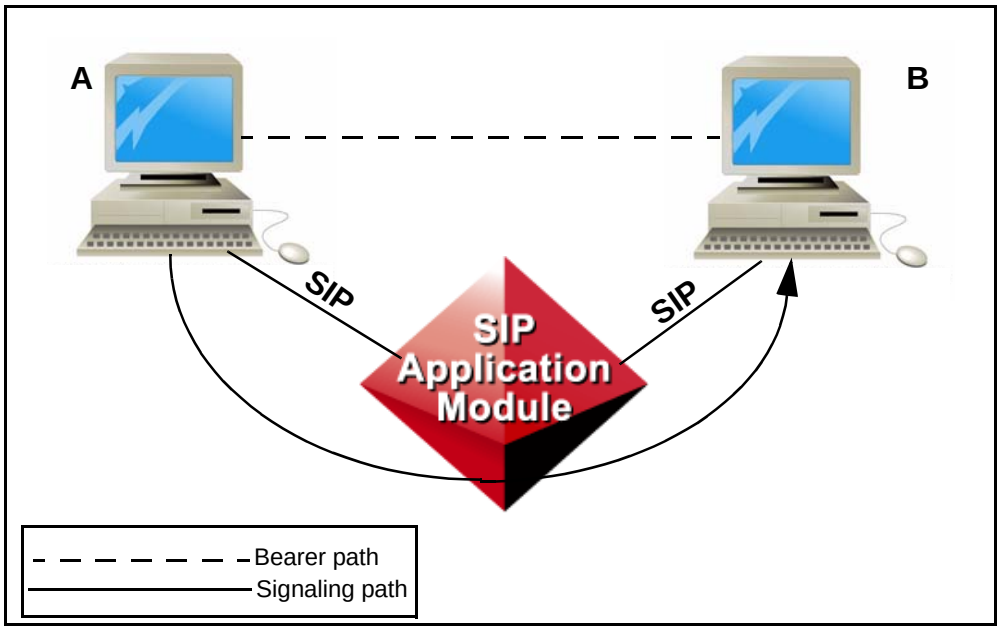
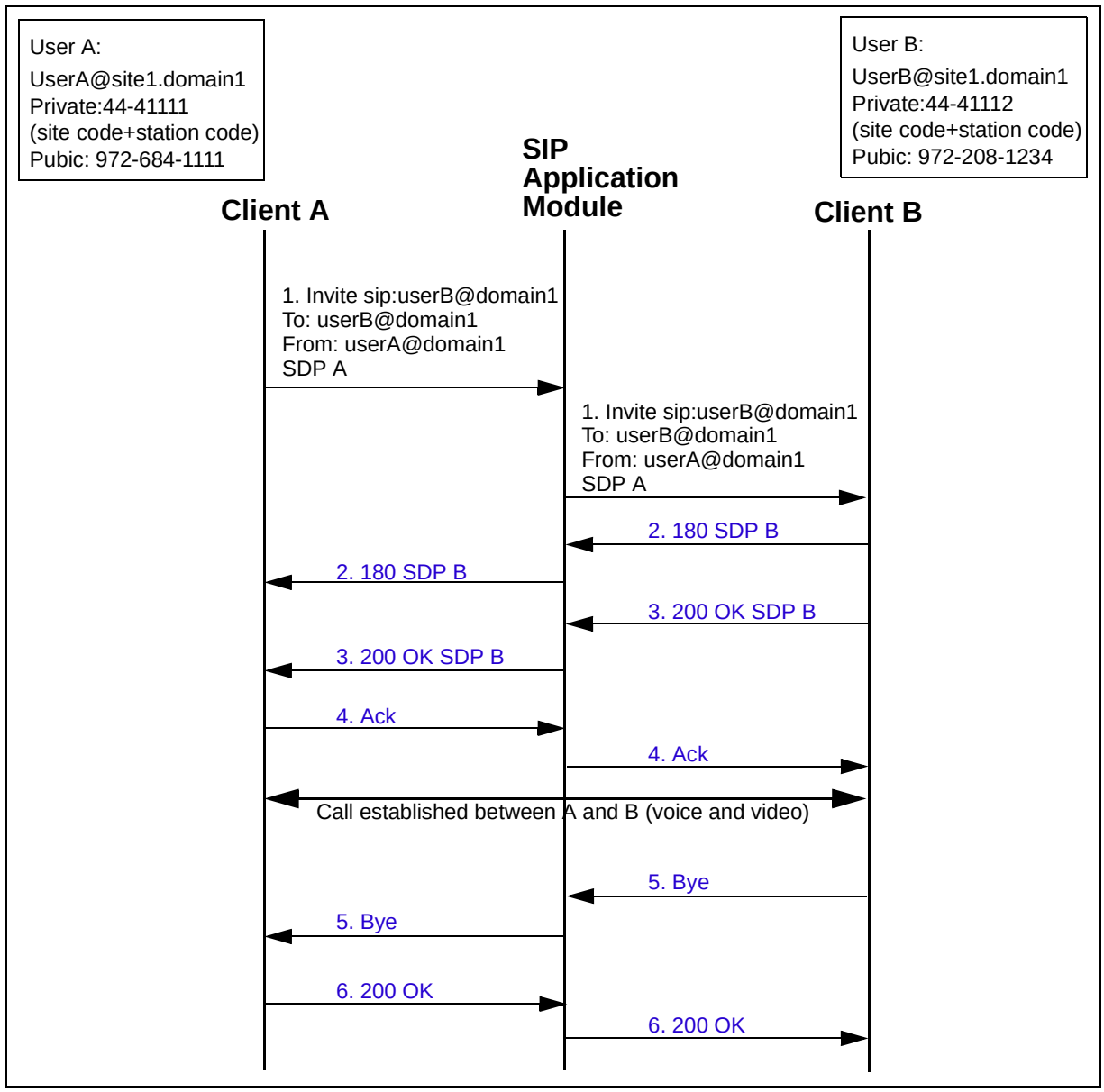


Figure 2 Client-to-client voice plus video call flow



The following steps provide more detail about the call flow:

1. Client A sends an Invite to Client B.
2. Client B responds with 180 SDP (Session Description Protocol)
3. Client B responds with 200 OK.

4. Client A sends an ACK message to the SIP Application module, which sends the ACK on to Client B.

   Note: The terminating client starts sending packets. The connection is established.

5. Client B sends Bye to end the call.
6. Client A responds with a 200 OK.

Call transfer

Figure 3, “Call transfer to client diagram,”and Figure 4, “Call transfer (blind) to client call flow,” show the basic call flow for a call transfer. A detailed, step-by-step illustration follows these diagrams.

Figure 3 Call transfer to client diagram

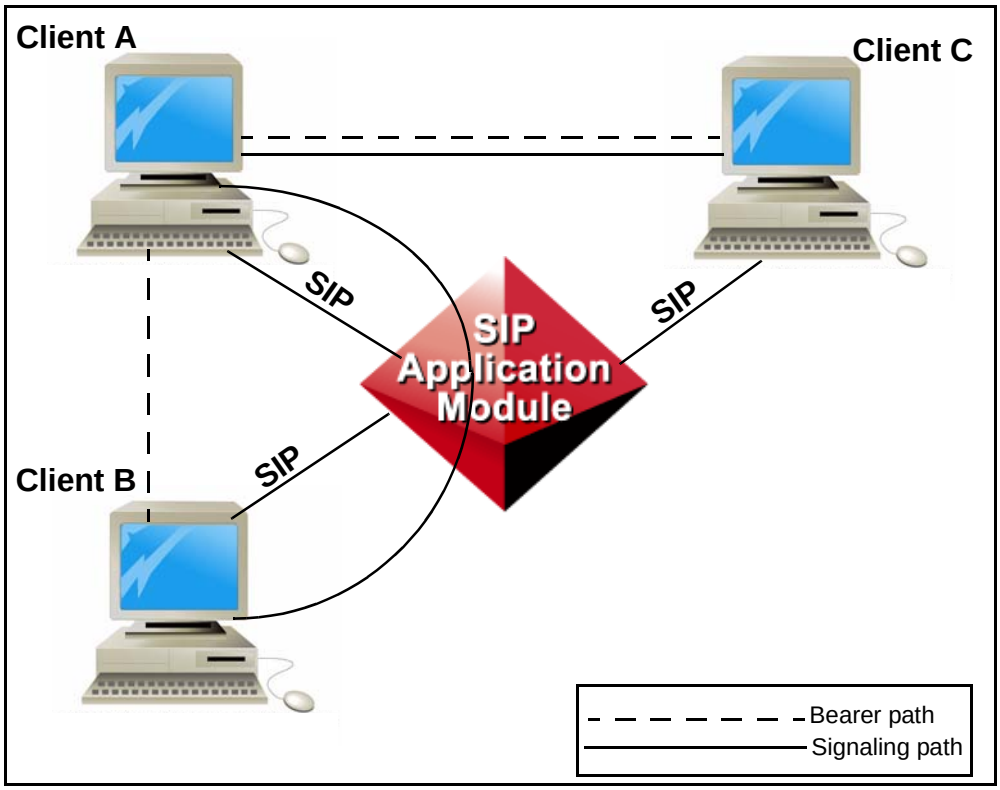
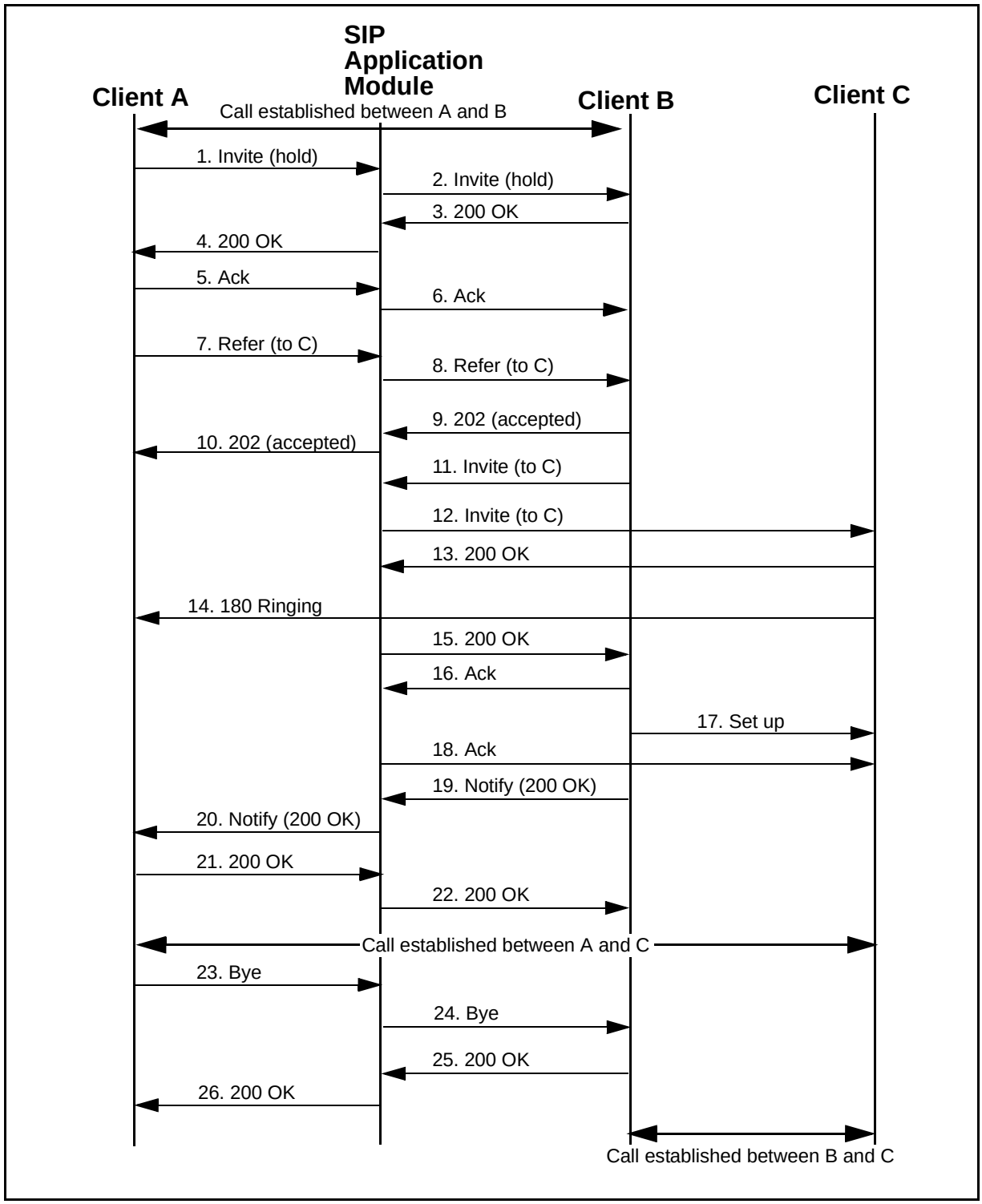


Figure 4 Call transfer (blind) to client call flow

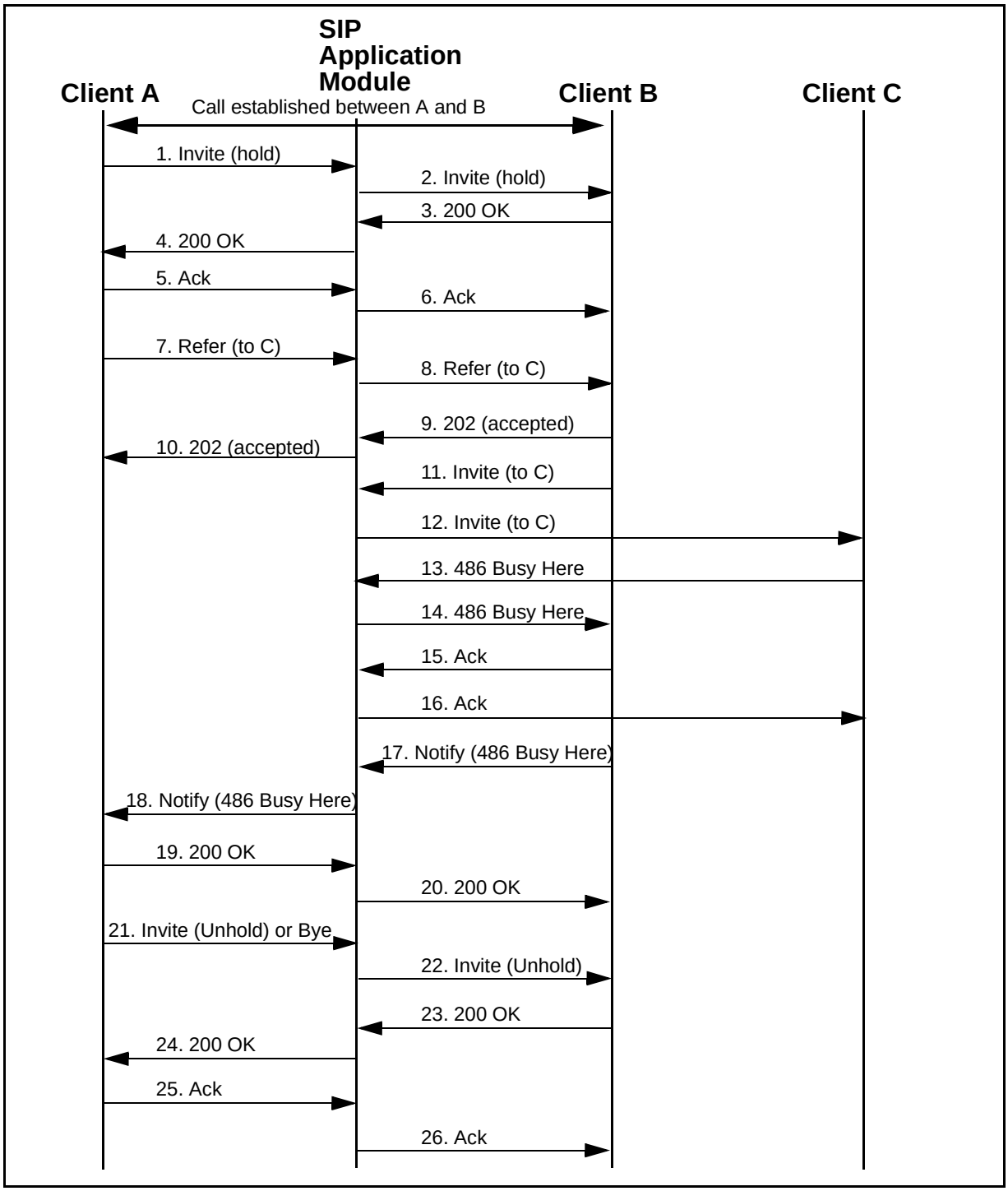


The following steps provide more detail about the call flow:

1. Client A initiates the transfer of B to C. A selects blind transfer.
2. The SIP Application Module sends a Hold to B.
3. Client B sends a 200 OK message back to the SIP Application Module. The 200 OK messages contain an Allow Header, which lists the SIP methods that the client being transferred supports. If Refer is in that list, then Refer is used for the transfer; otherwise, Bye-Also is used.
4. SIP Application Module sends a 200 OK message back to Client A.
5. Ack message from Client A to the SIP Application Module.
6. Ack message from the SIP Application Module to Client B.
7. Client A sends Refer-to header with C's information in it and a Referred-by header with A's information in it.
8. The SIP Application Module sends the Refer message to B.
9. 200 Accepted
10. 200 Accepted
11. The SIP Application Module sends an Invite to B to establish the new call between B and C.
12. Invite to C.
13. 200 OK
14. Ringing (SIP) – SIP/2.0 180 Ringing (SIP clients do not send SDP in the 180)
15. 200 OK
16. Ack
17. New media connection is set up between B and C.
18. Ack
19. Client B notifies the SIP Application Module.
20. The SIP Application Module notifies Client A.
21. Client A sends a 200 OK.
22. SIP Application Module sends a 200 OK to Client B.
23. Client A hangs up.

Figure 5, "Failed call transfer call flow,"and the steps following the figure show the call flow for a failed transfer.

Figure 5 Failed call transfer call flow



The following steps provide more detail about the call flow:

1. Client A initiates the transfer of B to C. A selects blind transfer.
2. The SIP Application Module sends a Hold to B.
3. Client B sends a 200 OK message back to the SIP Application Module. The 200 OK messages contain an Allow Header, which lists the SIP methods that the client being transferred supports. If Refer is in that list, then Refer is used for the transfer; otherwise, Bye-Also is used.
4. SIP Application Module sends a 200 OK message back to Client A.
5. Ack message from Client A to the SIP Application Module.
6. Ack message from the SIP Application Module to Client B.
7. Client A sends Refer-to header with C's information in it and a Referred-by header with A's information in it.
8. The SIP Application Module sends the Refer message to B.
9. 200 Accepted
10. 200 Accepted
11. The SIP Application Module sends an Invite to B to establish the new call between B and C.
12. Invite to C.
13. SIP Application Module receives a 486 Busy Here response from Client C. This response could be any type of 4xx, 5xx, or 6xx error message.
14. The SIP Application Module sends a Notify message to Client B. The body of the Notify message contains the 486 Busy Here, in this example
15. Client B responds with an Ack.
16. The SIP Application Module sends an Ack to Client C.
17. Client B Notifies Client A, through the SIP Application Module, that Client C is Busy.
18. Notify goes to Client A.
19. Client A responds with a 200 OK.
20. 200 OK to Client B.
21. There are now two possibilities:
    - Invite (Unhold): Client A can re-establish the call to Client B, in which case steps 22-26 apply.
    - Bye: Client A can hang up, in which case this is the last step.

22. SIP Application Module sends an Invite (Unhold) to Client B.
23. Client B responds with a 200 OK.
24. The SIP Application Module sends the Invite to Client A.
25. Client A responds with an Ack.
26. The SIP Application Module sends an Ack to Client B and the call is re-established.

Authentication

Figure 6, “Authentication diagram,”and Figure 7, “Authentication call flow,” show the basic call flow for Authentication. You can configure the SIP Application Module to support Authentication on Invite or Authentication on Registration. Following these diagrams is a detailed, step-by-step example of Authentication on Registration.

Figure 6 Authentication diagram

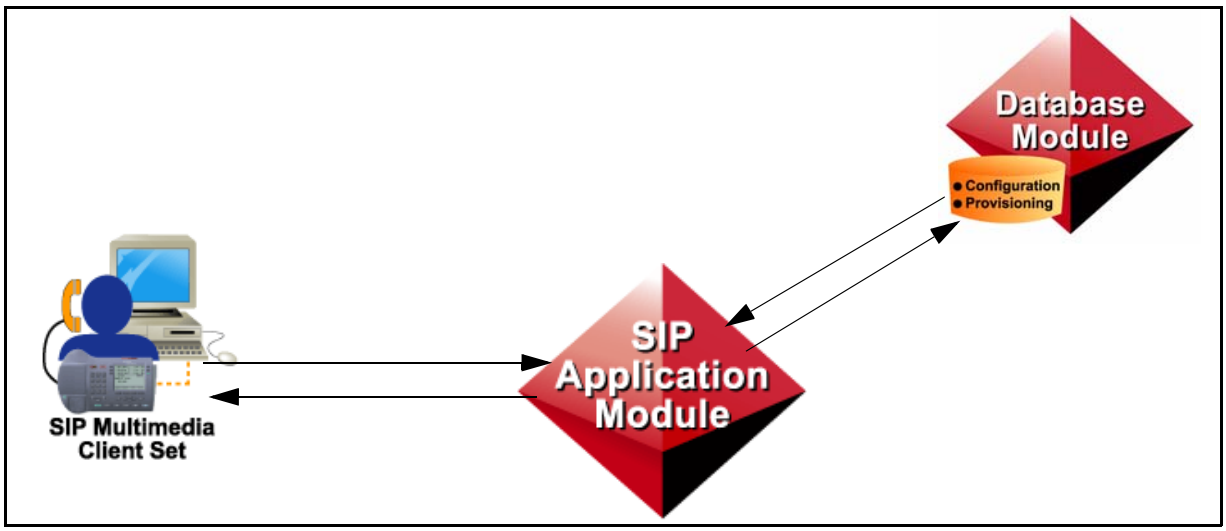
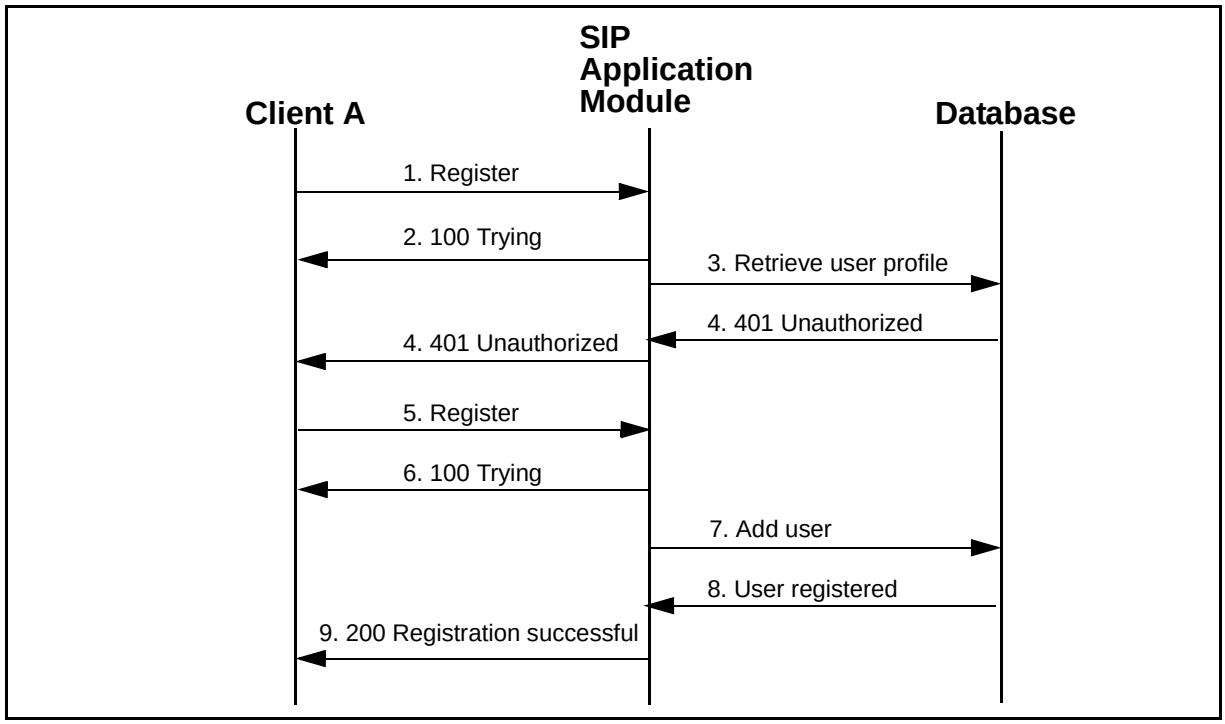


Figure 7 Authentication call flow



The following steps provide more detail about the call flow:

1. Client A sends a Register (SIP) message to the SIP Application Module.

   Initial requests never contain the user's credentials (basically, the initial request just contains a password). Client A makes the request, the SIP Application Server rejects it and gives them a piece of information called a nonce in the 401 Unauthorized message. The client takes that nonce and uses it to encrypt their password information and sends this back in the second request.

2. The SIP Application Module returns a 100 Trying message to Client A, then

3. The SIP Application Module attempts to retrieve the FROM party's subscriber information to see if they've been marked as INACTIVE in the system. This also causes the information to be cached at the SIP Application Server, so the same dip is not made to the database on the subsequent registration attempt. This profile information allows the system to determine what their password is in order to authenticate them.

4. In this case, the Database Module has returned a 401 Unauthorized message to the SIP Application Module, which sends the information on to Client A.

5. Client A sends another Register (SIP) message to the SIP Application Module.
6. Again, the SIP Application Module returns a 100 Trying message to Client A.
7. The SIP Application Module tells the Database Module to add this user to the registration tables (SQL).
8. The Database Module tells the SIP Application Module that the user is registered (SQL). Nothing is returned unless there is an error. If there is no error code, the registration worked.
9. The SIP Application Module then contacts Client A with a successful registration message (200 Registration Successful).

Succession Multimedia Communications Portfolio

MCP SIP Application Module

Basics

Publication number: NN10029-111
Product release: MCP 1.1 FP1 Standard
Document release: Standard MCP 1.1 FP1 (02.02)
Date: April 2003
Printed in the United States of America.

NORTEL NETWORKS™