



Key Elements of a Successful SIP Device Provisioning System

A white paper by Incognito Software
April, 2006

Key Elements of a Successful SIP Device Provisioning System

Introduction	2
Why SIP is Essential for Next-Generation Networks	3
Secure, Automated SIP Device Provisioning	3
Integration with OSS and Billing Systems	5
TFTP Clustering for Increased Performance and Reliability	5
Provisioning SIP User Agents	6
Conclusions	6

Many VoIP providers and broadband operators are managing one static configuration file per customer or group of customers. This isn't viable for large SIP-based networks

Introduction

Today's VoIP and broadband multimedia services require proper configuration of VoIP phones, ATAs (Analog Telephone Adapters), MTAs (Multimedia Termination Adapters), and other SIP devices. The provisioning function, which involves transfer of configuration files to those devices, is crucial to deploying new services.

Many VoIP providers and broadband operators are managing one static configuration file per customer. This isn't viable for large SIP-based networks, where device variables and subscriber data are undergoing constant change, necessitating dynamic "on-the-fly" generation of device configuration files.

The purpose of Session Initiation Protocol (SIP) is to initialize, synchronize, modify, and terminate data, voice, and video sessions. SIP doesn't transmit the contents of a media session; that is handled by other protocols. The value of SIP is in its mobility. SIP allows multimedia sessions to span a user's home and third-party IP networks.

SIP-based devices require sophisticated configuration files in order to activate service. Configuration information includes customer name, password, telephone number, ring tone, class of service, QoS (Quality of Service), SIP URI, SIP proxy server, call server FQDN (Fully Qualified Domain Name) or IP address, and other parameters.

The VoIP provider or broadband operator must promptly send updated configuration files to the SIP device whenever a customer needs to activate or modify a service. Requests like these can number in the thousands per day for large networks.

This paper provides an overview of SIP and why specialized provisioning of SIP devices is required.

SIP offers a unique set of capabilities that enables cable MSOs, wireline carriers, and wireless operators to expand their services without major investments in infrastructure.

Why SIP is Essential for Next-Generation Networks

In a traditional PSTN telephone network, basic endpoints communicate over an intelligent, hardware-dependent transport infrastructure and only the telephone company can introduce new services.

By contrast, SIP and the Internet put the intelligence at the endpoints, which communicate over simple transport links. Any provider, not just the telephone company, can develop new services without upgrading transport infrastructures.

Cable MSOs, wireline carriers, and wireless operators can quickly offer innovative new information and entertainment service packages without major infrastructure investments. SIP offers:

- **Mobility:** A user can communicate over home and third-party networks because sessions are initiated and routed through the user's universal address identifier (URI) and network-based servers: proxy servers for call routing, registrar servers for current location, and re-direct servers for call forwarding.
- **Simplified Universal Address:** The SIP framework routes a request to a URI's contact points based on information about the user's preferences, presence (availability), and location.
- **Distributed Intelligence via User Agents:** For each individual call or peer-to-peer session, SIP endpoints known as User Agents (UAs) negotiate the media and protocol extensions to be used, so that any type of conversation (voice, video, messaging) is possible.
- **Quality of Service:** SIP lets you set QoS levels for any service, not just voice. This allows data packets from the selected service (interactive gaming, music, video, voice) to be transmitted at a higher priority over other data so that packets aren't delayed or dropped, preventing noise, distortion, or lags.

Secure, Automated SIP Device Provisioning

To complete service activation, the VoIP or broadband provider must assign the SIP ATA or MTA an IP address, a DNS server for looking up domain names, and a configuration file.

The process of provisioning or activating SIP endpoints varies across VoIP and broadband providers based on the nature the operator's business model and the nature of the SIP endpoints themselves.

Pre-Provisioning and Self-Registration Business Models

Some VoIP and broadband service providers operate independently of the physical network and distribute SIP ATAs or MTAs to subscribers via retail outlets or online. In this business model, the service provider creates a static configuration file for each SIP device before distribution and, thus, before service activation. There is little or no subscriber involvement in this type of service activation process – the subscriber cannot self-register online, for example.

The process of provisioning or activating SIP endpoints varies across VoIP and broadband providers based on the nature the operator's business model and the nature of the SIP endpoints themselves.

However, even if self-registration isn't available, at some point, the service provider must deliver updated SIP configuration files to devices in the field.

If the configuration files are static, the subscriber cannot easily effect changes. Additionally, the VoIP or broadband provider must manually create, store, and track each individual device's configuration file, leading to the unsustainable situation of trying to generate and retain data on hundreds of thousands of device configuration files. Even in the smallest broadband networks, it's a burden to store each configuration file associated with each subscriber device.

In order to handle thousands to millions of subscribers requesting service setup or changes, a service provider must have automated device provisioning software that can process device variables and subscriber data and generate each configuration file dynamically, "on-the-fly" – at the time the device and associated service package requires activation – with no file retention required. This process also provides complete security, since only a device with knowledge of the correct filename, initiating a request from the correct IP address, is allowed to download that file. The file is not written to disk so it cannot be hijacked, and the file creation algorithm can be set to change every 30 minutes.

Both auto-provisioning and pre-provisioning capabilities are important aspects of this approach. In an auto-provisioning scenario, a subscriber self-registers before the provisioning software configures the device and activates service.

In pre-provisioning, the software records the pre-assigned device and client class so that it can automatically assign the appropriate service level and activate the device without additional registration.

Both auto-provisioning and pre-provisioning require automatic rules-based processing so that service providers can easily apply criteria-based formulas across large numbers of subscribers and devices.

Variable SIP Configuration File Formats

Since there have been no standards approved for SIP device configuration (unlike DOCSIS®), each device manufacturer has created their own configuration file format and uses different encryption algorithms to encode the files.

This added complexity can affect cost and time-to-market for new SIP-based services, so service providers need to eliminate the manual effort involved.

They can do this with automated SIP device provisioning software that, first, gives customer service representatives templates to enter basic service and device parameters including telephone numbers and other unique identifiers, and second, dynamically generates the appropriate configuration file based on the parameters entered.

Automated provisioning software can overcome the challenges associated with lack of standards for SIP device configuration.

By correlating the device type with the service bundled selected, automated provisioning software can perform dynamic on-the-fly generation of each device configuration file. Ideally the software can automatically create various file formats for a wide assortment of devices from multiple vendors: modems, VoIP phones, residential gateways, and standalone MTAs and embedded MTAs (eMTAs). Each configuration file must contain the appropriate parameters and formats that comply with the specific requirements of each device.

The provisioning software must transfer these files from operator headquarters over the IP network to the SIP device awaiting configuration. The software can use different methods such as TFTP transfer or HTTP transfer.

Integration with OSS and Billing Systems

The device provisioning software needs to interface to a service provider's existing OSS systems responsible for subscriber records and billing. These interfaces allows the provisioning software to activate SIP endpoints with the appropriate customer name, URI, telephone number, ring tone, QoS, SIP proxy server (if not discovered via DHCP or DNS), call server FQDN or IP address, encryption, username, password, and other information the SIP ATA or MTA may require.

TFTP Clustering for Increased Performance and Reliability

One way a VoIP or broadband provider can achieve maximum revenue assurance is through TFTP server clustering.

To perform dynamic generation of configuration files, the provisioning software's DHCP server sends the IP address of a TFTP (Trivial File Transfer Protocol) server and a filename to the requesting SIP device. The SIP device can then contact the TFTP server to request that file by name, and the TFTP server creates an on-the-fly configuration file based on the configuration information embedded in the filename itself.

The TFTP system must be constantly available to serve customer requests, preferably through server redundancy, and be scalable to accommodate an enormous number of files and transfers. For example, the TFTP system must create a configuration file for each new service activation as well as handle a large volume of file transfers to provision SIP devices coming online simultaneously after a power outage.

One industry-proven TFTP clustering system allows a master TFTP server to have multiple TFTP slaves. The system can cluster up to 255 synchronized TFTP servers with each master configuring up to 16 slaves.

The DHCP server synchronizes file generation data across the TFTP servers and performs load balancing of the TFTP cluster. To reduce the workload on each TFTP server, the network operator can assign specific "weights" to individual TFTP servers to take into account varying hardware and performance capabilities. The DHCP server

The TFTP service must be highly available and scalable to accommodate an enormous number of files and transfers.

Provisioning software should support the SIP User Agent Profile Delivery Framework.

can then send clients the IP address of a more heavily weighted TFTP service more often than less heavily weighted TFTP services.

The DHCP server collects status updates at regular intervals from all TFTP servers in the cluster. If the DHCP service fails to receive a status update within the required interval, it assumes that the associated TFTP is unavailable and routes TFTP file requests to one of the other servers in the cluster.

Provisioning SIP User Agents

Any VoIP or broadband operator's provisioning software should support the SIP User Agent Profile Delivery Framework.

UAs are logical entities: clients that initiate requests (such as VoIP phones), servers that respond to requests, or client/server combinations.

This framework allows a SIP UA client, such as a VoIP phone, to be completely provisioned even behind NAT gateways or on foreign networks.

The phone discovers its provisioning server using a DNS lookup or DHCP Option for SIP, and then subscribes to the provisioning server with a SIP "SUBSCRIBE" message to the server's IP address or FQDN. The provisioning software examines the SUBSCRIBE message and responds to the client UA with an available client data profile. Because the client profile is in XML format, it is supported by any UA protocol. For each configuration change, the client UA sends a "NOTIFY" message back to the provisioning server. The UA operates in "Config-Allow" mode, choosing a protocol for device configuration to occur: TFTP, HTTP, or HTTPS.

Conclusions

Successful SIP-based VoIP and broadband service deployments depend on device provisioning software that can handle the specific requirements of SIP: dynamic generation of configuration files, large volumes of requests for configuration files, integration with OSS systems, and the SIP UA delivery framework.

Contact:

Incognito Software Inc.
Phone: 604.688.4332 or US/Canada toll free 800.877.1856
Fax: 604.688.4339
Email: sales@incognito.com
Web: <http://www.incognito.com>