



Device Provisioning in Cable Environments

A white paper by Incognito Software
August, 2006

Device Provisioning in Cable Environments

Introduction	2
Auto-Provisioning and Pre-Provisioning	2
Components Involved in Device Provisioning	3
First Steps in SIP, DOCSIS®, and PacketCable™ Provisioning	4
TFTP or HTTP to Complete Device Provisioning.....	4
TFTP Clustering for Increasing Performance and Reliability	6
Conclusion.....	7

Key requirements for automated device provisioning software are scalability, reliability, and responsiveness.

Introduction

Automated provisioning software reduces the costs and time-to-market for triple-play or quad-play deployment by automatically configuring and updating customer premises equipment (CPE) such as modems, multimedia terminal adapters (MTAs), VoIP phones, gateways, and set top boxes. The software removes the complexity of subscriber activation including the need to send a technician to the subscriber's home.

In today's high-growth broadband environments, the key requirements for automated provisioning software are scalability, reliability, and responsiveness.

The software needs to bring subscribers online quickly and support continued subscriber growth. It must free up the service provider's administrative resources, facilitating superior customer service.

To fulfill all these responsibilities, provisioning systems must precisely manage IP addresses, DNS servers, users, and devices across the entire network.

Auto-Provisioning and Pre-Provisioning

Service activation requires the assignment of an IP address, a DNS server for looking up domain names, and a device configuration file.

Service activation involves the assignment of several parameters to the modem, MTA, or other access device at the subscriber site: an IP address, a DNS server for looking up domain names, and a configuration file. After the modem or MTA comes online, each CPE connected to the modem or MTA ("behind" the modem or MTA) can also receive its own IP address.

In order to handle thousands to millions of subscribers requesting service setup or changes, both auto-provisioning and pre-provisioning capabilities are essential. In an auto-provisioning scenario, a subscriber must self-register before the provisioning software can configure the device and activate service.

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

The provisioning software must be able to allocate IP addresses to CPE based on desired class of service, device type, subscriber status (new vs. existing), and ISP in a multiple-ISP environment.

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

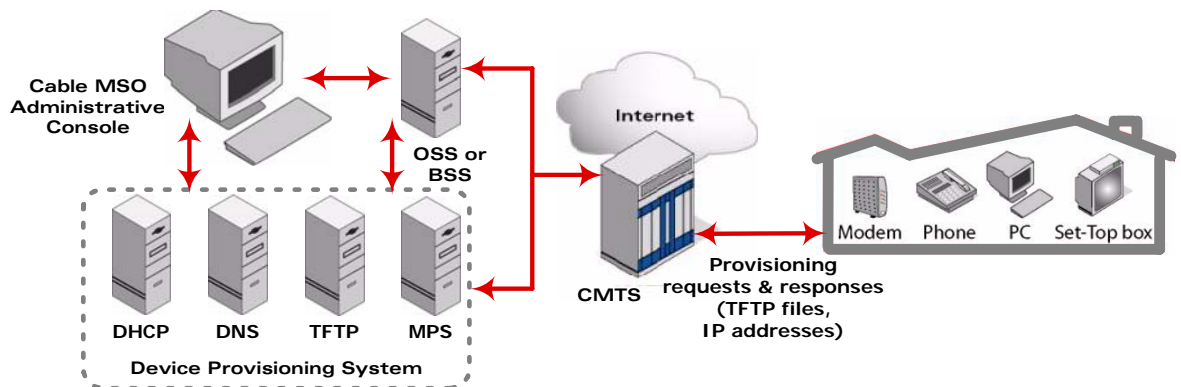
Components Involved in Device Provisioning

A cable operator's device provisioning system makes use of a variety of protocols and network elements.

All IP data packets between the device provisioning software and subscriber site must pass through the CMTS (Cable Modem Termination System) at the operator's headend facility. The CMTS routes IP data traffic between an Ethernet network (the cable operator's internal network or the general Internet) and the hybrid fiber-coax (HFC) network that connects the cable headend with subscriber site modem.

Similarly, at the subscriber site, all IP communications intended for CPE must pass through the modem or MTA because the modem provides the interface between the analog RF signals on the HFC network and the digital devices. In other words, the modem *modulates* digital IP data from the CPE onto analog RF signals for transmission over the HFC network, and in the other direction, *demodulates* analog RF signals from the HFC network into digital IP data packets for the CPE.

Cable systems use DHCP for assigning IP addresses, but they typically use different protocols for diagnostics and transfer of configuration files.



The cable operator's provisioning system uses DHCP protocol to assign IP addresses and configuration filenames to modems or MTAs. It also uses TFTP (Trivial File Transfer Protocol) or HTTP (Hyper Text Transfer Protocol) for transfer of device configuration files, SNMP (Simple Network Management Protocol) for status and performance monitoring, and syslog for logging.

After the provisioning software configures the modem or MTA, the other CPE can also receive their own IP addresses from the provisioning system's DHCP server. The DHCP server provisions the

CPE based on the remote ID (the cable modem's MAC address) that the CMTS inserts into the DHCP packets.

The provisioning system also provides Time-of-Day (ToD) functions so that each device can accurately time-stamp its communications messages, such as DHCP requests, and error logs.

First Steps in SIP, DOCSIS®, and PacketCable™ Provisioning

When the subscriber switches on the modem or MTA, the device asks the provisioning software at operator headquarters (via the CMTS) for an IP address and configuration information. The provisioning software must validate the device's hardware MAC address or other DHCP option data against the device database.

The provisioning software's DHCP server is responsible for granting the device an IP address and a DNS server identifier. In DOCSIS and some SIP implementations, the DHCP server also sends a TFTP or HTTP server name, and a TFTP or HTTP configuration filename. In PacketCable implementations, the provisioning software transfers the TFTP server and filename via SNMP protocol.

An extra step is involved if the subscriber still needs to register the device with the broadband provider. In this case, the provisioning software's DHCP server first gives the modem limited access to the operator's network, with an IP address and a DNS identifier so the modem can be redirected to a web site that facilitates service activation. Once the subscriber completes the request for service and billing information, the subscriber's modem is added to the proper "client class" according to the level of service they paid for, and the software tells the modem to reboot. Finally, when the modem has rebooted, the provisioning software grants the modem an IP address, DNS server, a TFTP or HTTP configuration filename and/or a TFTP or HTTP server name.

TFTP or HTTP to Complete Device Provisioning

After receiving the TFTP or HTTP filename and/or server name, the modem requests the file from the TFTP or HTTP server, which can dynamically generate the configuration file based on the appropriate service parameters. This automated generation of a customized file minimizes the operator's effort in responding to personalized service requests.

Although some SIP-based MTAs and eMTAs learn the configuration filename through DHCP, other SIP devices don't receive a filename and instead receive TFTP or HTTP configuration files encrypted with the SIP device's encryption key, which is pre-defined at the factory.

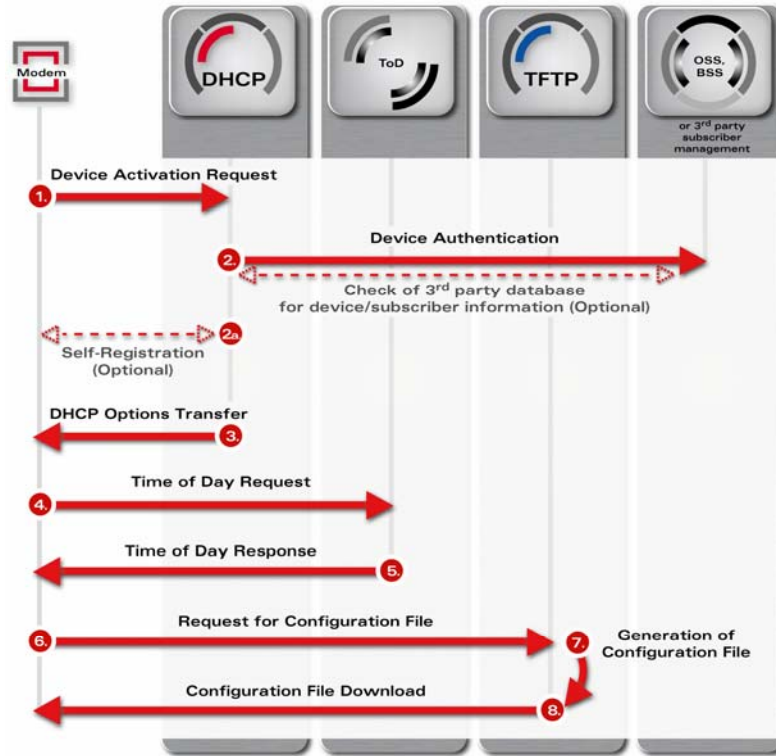
The modem now has full access to the Internet as specified in operator's billing database. In addition, the operator can quickly and easily change service levels or collect technical information about device operation for troubleshooting purposes.

HTTP file configuration is similar. To download the encrypted configuration file from the provisioning software at boot time, the device places an HTTP GET request to the HTTP server. The returned file is an XML document.

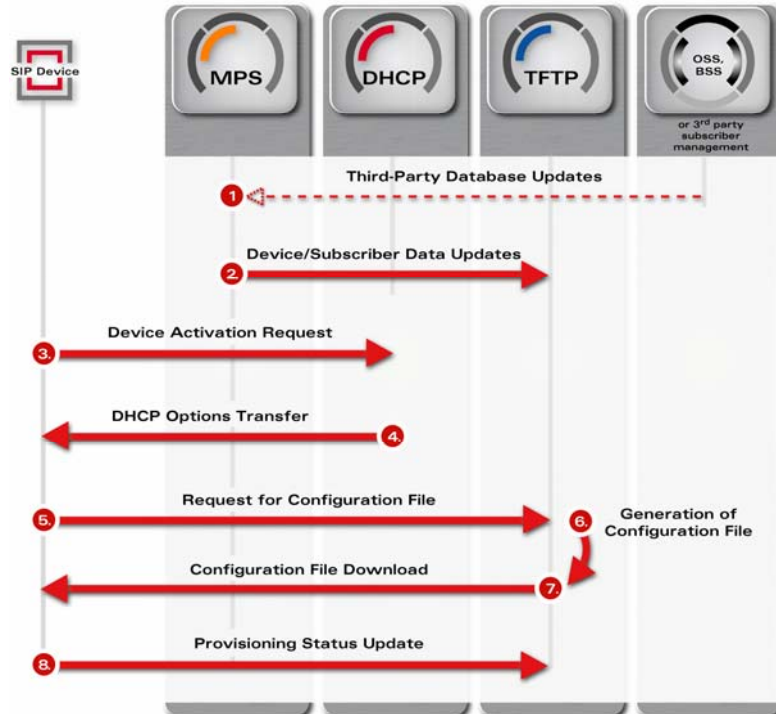
SIP, DOCSIS, and PacketCable devices typically use TFTP or HTTP file transfer for device configuration.

Examples of DOCSIS, PacketCable, and SIP device provisioning sequences are shown below.

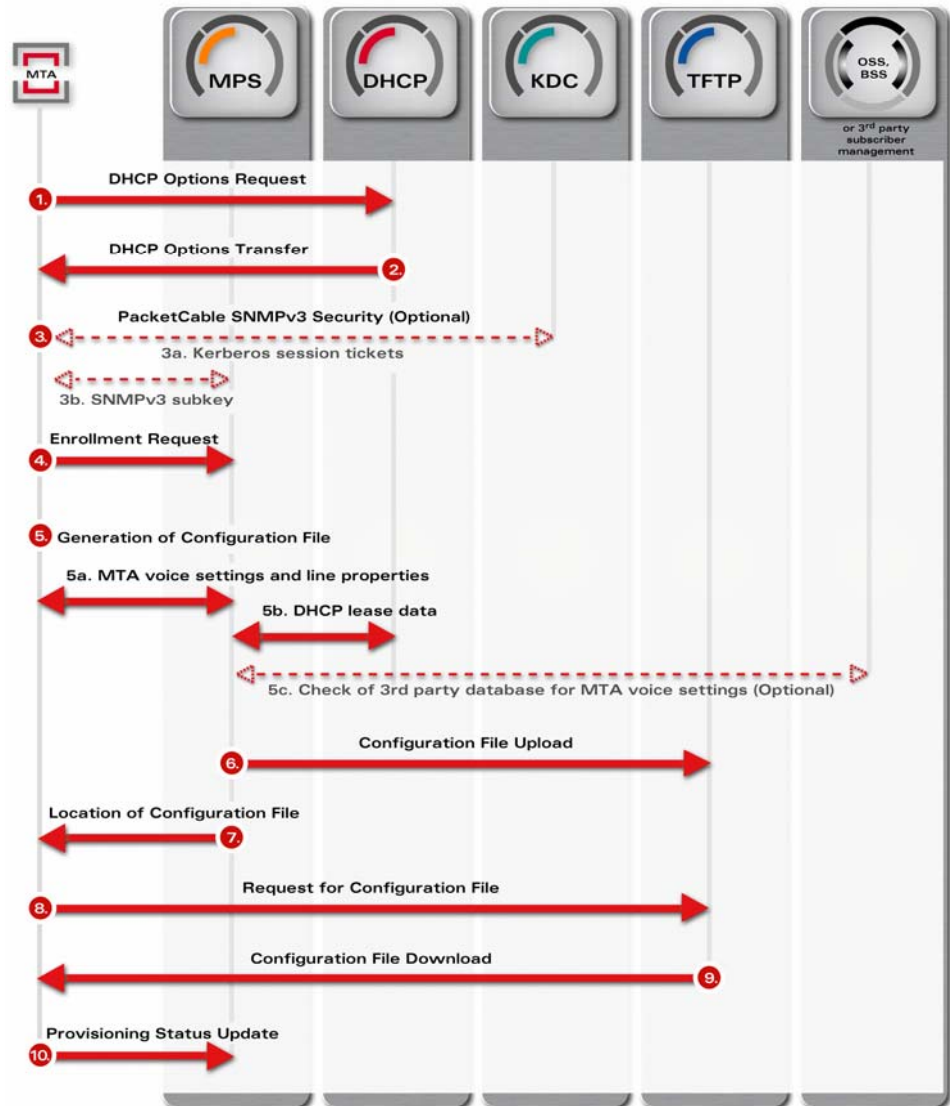
DOCSIS Device Provisioning Sequence Example:



SIP Device Provisioning Sequence Example:



PacketCable Device Provisioning Sequence Example (Secure PacketCable):



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

TFTP Clustering for Increasing Performance and Reliability

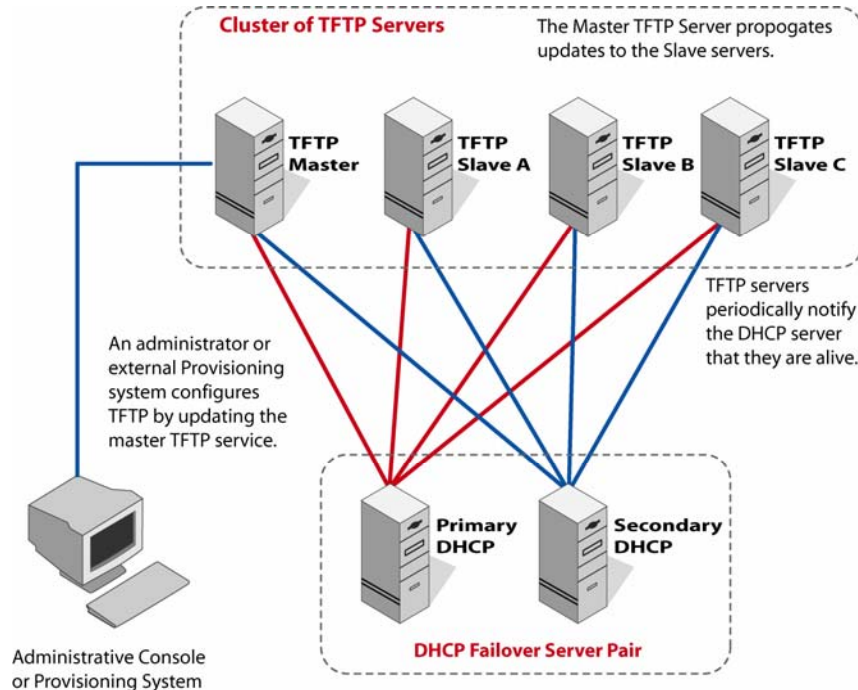
One way a broadband provider using TFTP can achieve maximum revenue assurance is through TFTP server clustering.

A TFTP system must always be ready to handle customer requests – it creates a configuration file for each new service activation and handles a large volume of file transfers, especially when thousands of devices come online simultaneously after a power outage.

An industry-proven TFTP clustering system allows a master server to have multiple slave servers and provides redundancy for high reliability. In this system, an operator can cluster up to 255

synchronized TFTP servers with each master configuring up to 16 slaves.

For maximum performance, a DHCP server or other provisioning server performs load balancing and file synchronization across the TFTP cluster. The administrator first assigns specific “weights” to individual servers to reduce the workload on each TFTP server and take into account varying hardware and performance capabilities. The more heavily weighted TFTP server then receives client requests more often than the less heavily weighted TFTP servers.



The TFTP servers also issue status updates so that if one fails, any requests for files are routed to one of the other servers in the cluster.

Conclusion

Cable MSOs can further develop high-margin revenue streams and control the costs of deployment with device provisioning solutions optimized for the needs of VoIP, IP video, and gaming service roll-outs. Especially with the movement towards all-IP networks, it's become essential to incorporate highly responsive, scalable, and reliable DHCP, DNS, and TFTP/HTTP software to set up and manage millions of CPE devices and potentially billions of IP addresses and domains.

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>