LINKSYS®
A Division of Cisco Systems, Inc.

Linksys SPA Provisioning Guide

Version 3.01

Corporate Headquarters

Linksys
121 Theory Drive
Irvine, CA 92617
USA
http://www.linksys.com
Tel: 949 823-1200
800 546-5797
Fax: 949 823-1100

CISCO SYSTEMS

Linksys SPA Provisioning Guide

Disclaimer – Please Read:

This document contains implementation examples and techniques using Linksys, a division of Cisco Systems, Inc. and, in some instances, other company's technology and products and is a recommendation only and does not constitute any legal arrangement between Linksys, a division of Cisco Systems, Inc. and the reader, either written or implied. The conclusions reached and recommendations and statements made are based on generic network, service and application requirements and should be regarded as a guide to assist you in forming your own opinions and decision regarding your particular situation. As well, Linksys reserves the right to change the features and functionalities for products described in this document at any time. These changes may involve changes to the described solutions over time.

Use of Proprietary Information and Copyright Notice:

LINKSYS®
A Division of Cisco Systems, Inc.

CONTENTS

Contents

LINKSYS®
A Division of Cisco Systems, Inc.

Preface

This guide describes the provisioning of Linksys Voice over IP (VoIP) products. It contains the following sections:

Document Audience

This document is written for service providers who offer services using Linksys VoIP products and specifically for administrative staff responsible for remote provisioning and preprovisioning Linksys devices.

Linksys VoIP Products

The following summarizes the Linksys VoIP products that can be remotely provisioned or preprovisioned using the information provided in this document.

- SPA9000—IP PBX with Auto-Attendant; can be used with the SPA400, which provides a SIP-PSTN gateway
- Linksys Analog Telephone Adapters (ATAs):
  - PAP2T—Voice adapter with two FXS ports
  - SPA1001—Small VoIP adapter
  - SPA2102—Voice adapter with router
  - SPA3102—Voice adapter with router and PSTN connectivity
  - SPA8000—Voice adapter supporting up to eight FXS connections
  - AG310—ADSL2+ gateway with VoIP and PSTN connectivity

- WAG310G—Wireless-G ADSL2+ gateway with VoIP and PSTN connectivity
- RTP300—IP router with two FXS ports
- WRP400—Wireless-G ADSL gateway with two FXS ports
- WRTP54G—Wireless-G IP router with two FXS ports
- WRT54GP2—Wireless-G IP router with two FXS ports
- WAG54GP2—Wireless-G ADSL gateway with two FXS ports

- SPA900 Series IP phones:
  - SPA901—One line, small, affordable, no display
  - SPA921—One-line business phone
  - SPA922—One-line business phone with Power over Ethernet (PoE) support and an extra Ethernet port for connecting another device to the LAN
  - SPA941—Default is two lines, upgradeable to four lines
  - SPA942—Default is two lines, upgradeable to four lines. Power over Ethernet (PoE) support and an extra Ethernet port for connecting another device to the LAN
  - SPA962—Six lines, hi-res color display. Power over Ethernet (PoE) support and an extra Ethernet port for connecting another device to the LAN

Note A Linksys VoIP device that supports the remote provisioning options described in this document is referred to generically as a SPA.

How This Document is Organized

This document is divided into the following chapters and appendices.

Chapter	Contents
Chapter 1, “Provisioning Linksys VoIP Devices”	This chapter introduces Linksys VoIP products.
Chapter 2, “Creating Provisioning Scripts”	This chapter describes how to work with Linksys provisioning scripts and configuration profiles.
Chapter 3, “Provisioning Tutorial”	This chapter provides step-by-step procedures for using the scripting language to create a configuration profile.
Chapter 4, “Provisioning Field Reference”	This chapter provides a systematic reference for each parameter on the Provisioning tab of the administration web server.
Appendix A, “Acronyms”	This appendix provides the expansion of acronyms used in this document.
Appendix B, “Glossary”	This appendix defines the terms used in this document.

Document Conventions

The following are the typographic conventions used in this document.

Typographic Element	Meaning
Boldface	Indicates an option on a menu or a literal value to be entered in a field.
<parameter>	Angle brackets (<>) are used to identify parameters that appear on the configuration pages of the Linksys device administration web server. The index at the end of this document contains an alphabetical listing of each parameter, hyperlinked to the appropriate table in Chapter 4, "Provisioning Field Reference"
Italic	Indicates a variable that should be replaced with a literal value.
Monospaced Font	Indicates code samples or system output.

Related Documentation

The following documentation provides additional information about features and functionality of Linksys ATAs:

- *AA Quick Guide*
- *IVR Quick Guide*
- *SPA Provisioning Guide*

The following documentation describes how to use other Linksys Voice System products:

- *SPA9000 Administrator Guide*
- *LVS CTI Integration Guide*
- *LVS Integration with ITSP Hosted Voicemail Guide*
- *SPA900 Series IP Phones Administrator Guide*
- *SPA 2.0 ATA Administrator Guide*
- *Linksys Voice over IP Product Guide: SIP CPE for Massive Scale Deployment*

Technical Support

Technical support contact information for authorized Linksys Voice System partners is as follows:

- LVS Phone Support (requires an authorized partner PIN)

  888 333-0244 Hours: 4am-6pm PST, 7 days a week
- E-mail support

  voipsupport@linksys.com

LINKSYS®
A Division of Cisco Systems, Inc.

CHAPTER 1

Provisioning Linksys VoIP Devices

This chapter describes the features and functionality available when provisioning Linksys VoIP devices and explains the setup required. It includes the following sections:

Note A Linksys VoIP device is generically referred to in this document as a SPA. Unless otherwise noted, the instructions in this document apply equally to the SPA9000, Linksys Analog Telephone Adapters (ATAs), and SPA900 Series IP phones.

Residential Deployment Provisioning Requirements

Linksys ATAs, such as the PAP2T, are primarily intended for high-volume deployments by VoIP service providers to residential and small business customers. In this scenario, units are likely to be widely distributed across the Internet, connected through routers and firewalls at the customer premises.

Further, ATAs can also serve as terminal nodes in business or enterprise environments, where the units may be operated within a self-contained LAN environment.

The ATA can be seen as a remote extension of the service provider back-end equipment. In essence, it replaces the traditional physical analog telephone line connection from a customer premise to a central office with a virtual connection, which relies on broadband Internet service to extend the central office phone line termination into the customer premises.

The ATA can assume responsibility for many of the functions that were traditionally handled at the central office. At a minimum, the ATA serves as a media conversion endpoint, offering the consumer a telephone port analogous to a traditional phone line terminal.

Remote management and configuration is required to efficiently ensure proper operation of the ATA at the customer premises. ATA configuration varies according to the individual customer and with the same customer over a period of time.

The ATA must be configured to match the account service parameters for the individual customer. Also, configuration may need to be modified because of newly introduced service provider features, modifications in the service provider network, or firmware upgrades in the endpoint.

This customized, ongoing configuration is supported by the following features of Linksys ATAs:

- Reliable remote control of the endpoint,
- Encryption of the communication controlling the endpoint,
- Streamlined endpoint account binding.

Remote Endpoint Control

The service provider must be able to modify configuration parameters in the ATA after the unit has been deployed to the customer premises. The service provider must also be able to upgrade the endpoint firmware remotely, and both of these operations must be reliable.

In a residential deployment, the endpoint itself is typically connected in a local network, and accesses the Internet through a router using network address translation (NAT). For enhanced security, the router may attempt to block unauthorized incoming packets by implementing symmetric NAT, a packet filtering strategy which severely restricts the packets that are allowed to enter the protected network from the Internet.

Communication Encryption

The configuration parameters communicated to the endpoint may contain authorization codes or other information should not be revealed to the customer. This may be required to protect the service provider from unauthorized activity by the customer. It is also necessary to protect the customer from unauthorized use of the account by other customers.

For this reason, the service provider may wish to encrypt the configuration profile communication between the provisioning server and the endpoint, in addition to restricting access to the ATA administration web server.

Provisioning Overview

Linksys VoIP products support secure remote provisioning and firmware upgrades. Configuration profiles can be generated using common, open source tools, facilitating integration into service provider provisioning systems. Supported transport protocols include TFTP, HTTP, and HTTPS with client certificates. Linksys provisioning solutions are designed for high-volume residential deployment, where each SPA typically resides in a separate LAN environment connected to the Internet with a NAT device.

Note This Provisioning Guide is intended to supplement the product administration guides, which provide definitions and usage guidelines for each parameter available for a specific device.

The SPA can be configured to resync its internal configuration state to a remote profile periodically and on power up. Starting with firmware release 2.0, 256-bit symmetric key encryption of profiles is supported. In addition, an unprovisioned SPA can receive an encrypted profile specifically targeted for that device without requiring an explicit key. Release 2.0 supports a secure first-time provisioning mechanism using SSL functionality.

Note Remote customization (RC) units are introduced with Release 5.x. RC units are customized by Linksys so when the unit is started, it tries to contact the Linksys provisioning server to download its customized profile.

User intervention is not required to initiate or complete a profile update or firmware upgrade. Remote firmware upgrade is achieved via TFTP or HTTP, but not using HTTPS because the firmware does not contain sensitive information that can be read by a customer. The SPA upgrade logic is capable of automating multi-stage upgrades, if intermediate upgrades are required to reach a future upgrade state from an older release. .A profile resync is only attempted when the SPA is idle, because this may trigger a software reboot.

General purpose parameters are provided to help service providers manage the provisioning process. Each SPA can be configured to periodically contact a normal provisioning server (NPS). Communication wit the NPS does not require the use of a secure protocol because the updated profile is encrypted by a shared secret key. The NPS can be a standard TFTP, HTTP or HTTPS server.

Initial Provisioning

Linksys ATAs provide convenient mechanisms for initial provisioning, based on two deployment models:

- Retail distribution, where the customer purchases the ATA separately from the VoIP service
- Bulk distribution, where the service provider issues the ATA to the customer as part of the VoIP service contract

In the first model, the customer purchases the ATA from a retail outlet, and subsequently requests VoIP service from the service provider, for use with that adapter. The service provider must then support secure remote configuration of the unit.

In the second model, the service provider acquires adapters in bulk quantity, and either preprovisions the adapters in-house or purchases RC units from Linksys.

Deploying RC Units

The in-house preprovisioning step can be eliminated by using RC units. Customization of RC units reduces the need to handle the units prior to shipping to end customers. It also discourages the use of the SPA with a different service.

The MAC address of each RC unit is associated with a customized profile for the customer who purchased each unit on a provisioning server maintained by Linksys. The RC unit is preprovisioned by Linksys with the connection information for the Linksys provisioning server. When the RC unit is started, it tries to contact the Linksys provisioning server and download its customized profile.

The status of customization for an RC unit can be determined by viewing the Customization parameter in the Product Information section of the Info tab. An RC unit that has not been provisioned displays Pending. An RC unit that has been provisioned displays the name of the company that owns the unit. If the unit is not an RC unit the web page displays Not Customized.

Linksys offers RC units to service providers for volume deployments of SPA endpoints. Through customization, the manufacturing default values of a select number of parameters can be customized to meet the needs of individual service providers.

The following is a sample template for an RC unit:

```
Restricted Access Domain "domain.com, domain1.com, domain2.com";
Primary_DNS                * "x.y.w.z";
Secondary_DNS              * "a.b.c.d";
Provision_Enable           * "Yes";
Resync_Periodic            * "30";
Resync_Error_Retry_Delay   * "30";
Profile_Rule   * "http://prov.domain.com/sipura/profile?id=$MA";
```

The Restricted Access Domain parameter is configured with the actual domain names of up to a maximum of five domains. The Primary_DNS and Secondary_DNS parameters are configured with the actual domain names or IP addresses of the DNS servers available to the RC unit.

Redundant Provisioning Servers

The provisioning server may be specified as an IP address or as a fully qualified domain name (FQDN). The use of a FQDN facilitates the deployment of redundant provisioning servers. When the provisioning server is identified through a FQDN, the SPA attempts to resolve the FQDN to an IP address through DNS. Only DNS A-records are supported for provisioning; DNS SRV address resolution is not available for provisioning. The SPA continues to process A-records until the first server responds. If no server associated with the A-records responds, the SPA logs an error to the syslog server.

Retail Provisioning

The SPA firmware includes an administration web server that displays SPA internal configuration and accepts new configuration parameter values. The server also accepts a special URL command syntax for performing remote profile resync and firmware upgrade operations.

In a retail distribution model, a customer purchases a Linksys voice endpoint device, and subsequently subscribes to a particular service. The customer first signs on to the service and establishes a VoIP account, possibly through an online portal. Subsequently, the customer binds the particular device to the assigned service account.

To do so, the unprovisioned SPA is instructed to resync with a specific provisioning server through a resync URL command. The URL command typically includes an account PIN number or alphanumeric code to associate the device with the new account.

In the following example, a device at the DHCP-assigned IP address 192.168.1.102 is instructed to provision itself to the SuperVoIP service:

```
http://192.168.1.102/admin/resync?https://prov.supervoip.com/linksys-init/1234abcd
```

In this example, 1234abcd is the PIN number of the new account. The remote provisioning server is configured to associate the SPA that is performing the resync request with the new account, based on the URL and the supplied PIN. Through this initial resync operation, the SPA is configured in a single step, and is automatically directed to resync thereafter to a permanent URL on the server. For example:

```
https://prov.supervoip.com/linksys
```

For both initial and permanent access, the provisioning server relies on the SPA client certificate for authentication and supplies correct configuration parameter values based on the associated service account.

Automatic In-House Preprovisioning

Using the administration web server and issuing a resync URL is convenient for a customer in the retail deployment model, but it is not as convenient for preprovisioning a large number of units.

The SPA supports a more convenient mechanism for in-house preprovisioning. With the factory default configuration, a SPA automatically tries to resync to a specific file on a TFTP server, whose IP address is offered as one of the DHCP-provided parameters. This lets a service provider connect each new SPA to a LAN environment configured to preprovision SPAs. Any new SPA connected to this LAN automatically resyncs to the local TFTP server, initializing its internal state in preparation for deployment. Among other parameters, this preprovisioning step configures the URL of the SPA provisioning server.

Subsequently, when a new customer signs up for service, the preprovisioned SPA can be simply bar-code scanned, to record its MAC address or serial number, before being shipped to the customer. Upon receiving the unit, the customer connects the unit to the broadband link, possibly through a router. On power-up the SPA already knows the server to contact for its periodic resync update.

Configuration Access Control

Besides configuration parameters that control resync and upgrade behavior, the SPA provides mechanisms for restricting end-user access to various parameters.

The SPA firmware provides specific privileges for login to a User account and an Admin account. The Admin account is designed to give the service provider configuration access to the SPA, while the User account is designed to give limited and configurable control to the end user of the device.

The User account provides access to basic interactive voice response (IVR) functions and to a subset of the administration web server parameters. The Admin account provides full access to all IVR functions and to all administration web server parameterse.

The User and Admin accounts can be independently password protected. The configuration parameters available to the User account are completely configurable in the SPA, on a parameter-by-parameter basis. Optionally, user access to the SPA administration web server can be totally disabled. The manufacturing reset control using the IVR can also be disabled, via provisioning.

The Internet domains accessed by the SPA for resync, upgrades, and SIP registration for Line 1 can be restricted. These and other features are described in detail in administration guides for each product.

SPA Configuration Profiles

The SPA configuration profile defines the parameter values for a specific SPA device. The configuration profile can be used in two formats:

- Open (XML-style) format
- Proprietary, plain-text format

The XML-style format lets you use standard tools to compile the parameters and values. To protect confidential information contained in the configuration profile, this type of file is generally delivered from the provisioning server to the SPA over a secure channel provided by HTTPS.

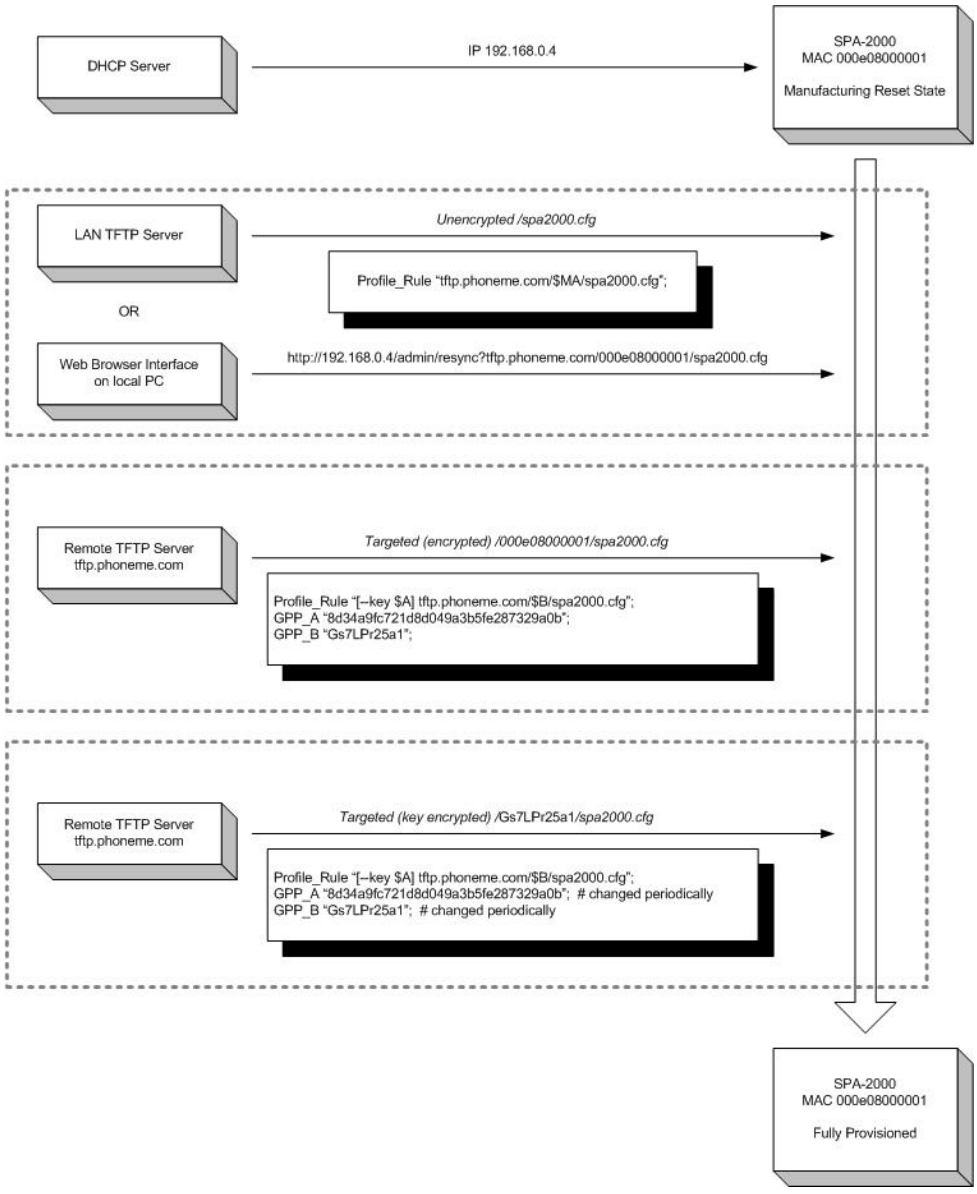
The plain-text configuration file uses a proprietary format, which can be encrypted to prevent unauthorized use of confidential information. By convention, the profile is named with the extension .cfg (for example, spa2102.cfg). The Linksys Profile Compiler (SPC) tool is provided for compiling the

plain-text file containing parameter-value pairs into an encrypted CFG file. The SPC tool is available from Linksys for the Win32 environment (spc.exe) and Linux-i386-elf environment (spc-linux-i386-static). Availability of the SPC tool for the OpenBSD environment is available on a case-by-case basis.

SPA Provisioning Flow

Firmware release 1.0 provides basic features in support of secure provisioning. This section describes the high-level provisioning flow supported by release 1.0 in the context of a service provider application. The SPA provisioning flow is illustrated in Figure 1-1.

Figure 1-1 SPA Provisioning Flow



At a high level, the provisioning process involves four provisioning states described in Table 1-1.

Table 1-1 Provisioning States

Flow Step	Step Description
MFG-RESET	Manufacturing reset Performing manufacturing reset on the SPA returns the device to a fully unprovisioned state. All configurable parameters regain their manufacturing default values. Manufacturing reset can be performed from any state through the IVR sequence ****RESET#1# Allowing the end user to perform manufacturing reset guarantees that the device can always be returned to an accessible state.
SP-CUST	Service provider customization The provisioning parameters are customized for a particular service provider network. The Profile_Rule parameter must be configured in this step to point to a device specific configuration profile, using a service provider specific provisioning server. This can be accomplished in one of three ways: • Auto-configuration via local DHCP server. A TFTP server name or IPv4 address is specified by DHCP on he local network. The indicated TFTP server carries the desired Profile_Rule entry in the CFG file /spa2102.cfg • Enter a resync URL. An end-user opens a browser onto the SPA web server, explicitly requesting a resync to a specific TFTP server, using this URL syntax: http://x.x.x.x/admin/resync?prvserv/spa2102.cfg where x.x.x.x is the IP address of the specific SPA and prvserv is the target TFTP server, followed by a profile path. • Edit Profile_Rule parameter. Open the provisioning pane on the SPA web interface, and enter the TFTP URL in the Profile_Rule parameter: for example, prserv/spa2102.cfg. The spa2102.cfg file modifies the Profile_Rule to contact a specific TFTP server, and request a MAC-address specific CFG file. For example, the following entry contacts a specific provisioning server, requesting a new profile unique to this unit: Profile_Rule tftp.callme.com/profile/$MA/spa2102.cfg;

Table 1-1 Provisioning States (continued)

SEC-PRV-1	Secure Provisioning—Initial Configuration
	The initial device-unique CFG file should be targeted to each SPA by compiling the CFG file with the spc --target option. This provides an initial level of encryption that does not require the exchange of keys.
	The initial device-unique CFG file should reconfigure the profile parameters to enable stronger encryption, by programming a 256-bit encryption key, and pointing to a randomly generated TFTP directory. For example, the CFG file might contain:
	`Profile_Rule [--key $A] tftp.callme.com/profile/$B/spa2102.cfg;`
	`GPP_A 8e4ca259…;  # 256 bit key`
	`GPP_B Gp3sqLn…;  # random CFG file path directory`

SEC-PRV-2	Secure Provisioning—Full Configuration The subsequent profile resync operations retrieve 256-bit encrypted CFG files, which maintain the SPA in a state synchronized to the provisioning server. All remaining SPA parameters are configured and maintained through this strongly encrypted profile. The encryption key and random directory location can be changed periodically for extra security.

Using HTTPS

The SPA provides a reliable and secure provisioning strategy based on HTTPS requests from the SPA to the provisioning server, using both server and client certificates for authenticating the client to the server and the server to the client.

To use HTTPS with Linksys SPA units, you must generate a Certificate Signing Request (CSR) and submit it to Linksys. Linksys generates a certificate for installation on the provisioning server that is accepted by the SPA units when they seek to establish an HTTPS connection with the provisioning server. This procedure is described in the "Enabling HTTPS" section on page 1-13.

How HTTPS Works

Starting with firmware release 2.0.6 , the SPA implements SSL, which lets the SPA client to connect to servers using HTTPS.

HTTPS encrypts the communication between the client and the server, protecting the message contents from other intervening network devices. The encryption method for the body of the communication between client and server is based on symmetric key cryptography. With symmetric key cryptography, a single secret key is shared by the client and the server over a secure channel protected by Public/Private key encryption.

Messages encrypted by the secret key can only be decrypted using the same key. HTTPS supports a wide range of symmetric encryption algorithms. The SPA implements up to 256-bit symmetric encryption, using the American Encryption Standard (AES), in addition to 128-bit RC4.

HTTPS also provides for the authentication of the server and the client engaged in a secure transaction. This feature ensures that the provisioning server and an individual client cannot be spoofed by other devices on the network. This is an essential capability in the context of remote endpoint provisioning.

Server and client authentication is performed using public/private key encryption, using certificates containing the public key. Text encrypted with a public key can be decrypted only by its corresponding private key (and vice versa). The SPA supports the RSA algorithm for public/private key cryptography.

Certificates are authenticated in the context of a certificate chain. A certificate authority lies at the root of the chain, with all other certificates depending on the root authority for authority.

Server Certificates

Each secure provisioning server is issued an SSL server certificate, directly signed by Linksys. The firmware running on the SPA clients recognizes only these certificates as valid. The clients try to authenticate the server certificate when connecting via HTTPS, and reject any server certificate not signed by Linksys.

This mechanism protects the service provider from unauthorized access to the SPA endpoint, or any attempt to spoof the provisioning server. This might allow the attacker to reprovision the SPA, to gain configuration information, or to use a different VoIP service. Without the private key corresponding to a valid server certificate, the attacker is unable to establish communication with a Linksys SPA.

Client Certificates

In addition to a direct attack on the SPA, an attacker might attempt to contact a provisioning server using a standard web browser, or other HTTPS client, to obtain the SPA configuration profile from the provisioning server. To prevent this kind of attack, each SPA also carries a unique client certificate, also signed by Linksys, including identifying information about each individual endpoint. A certificate authority root certificate capable of authenticating the device client certificate is given to each service provider. This authentication path allows the provisioning server to reject unauthorized requests for configuration profiles.

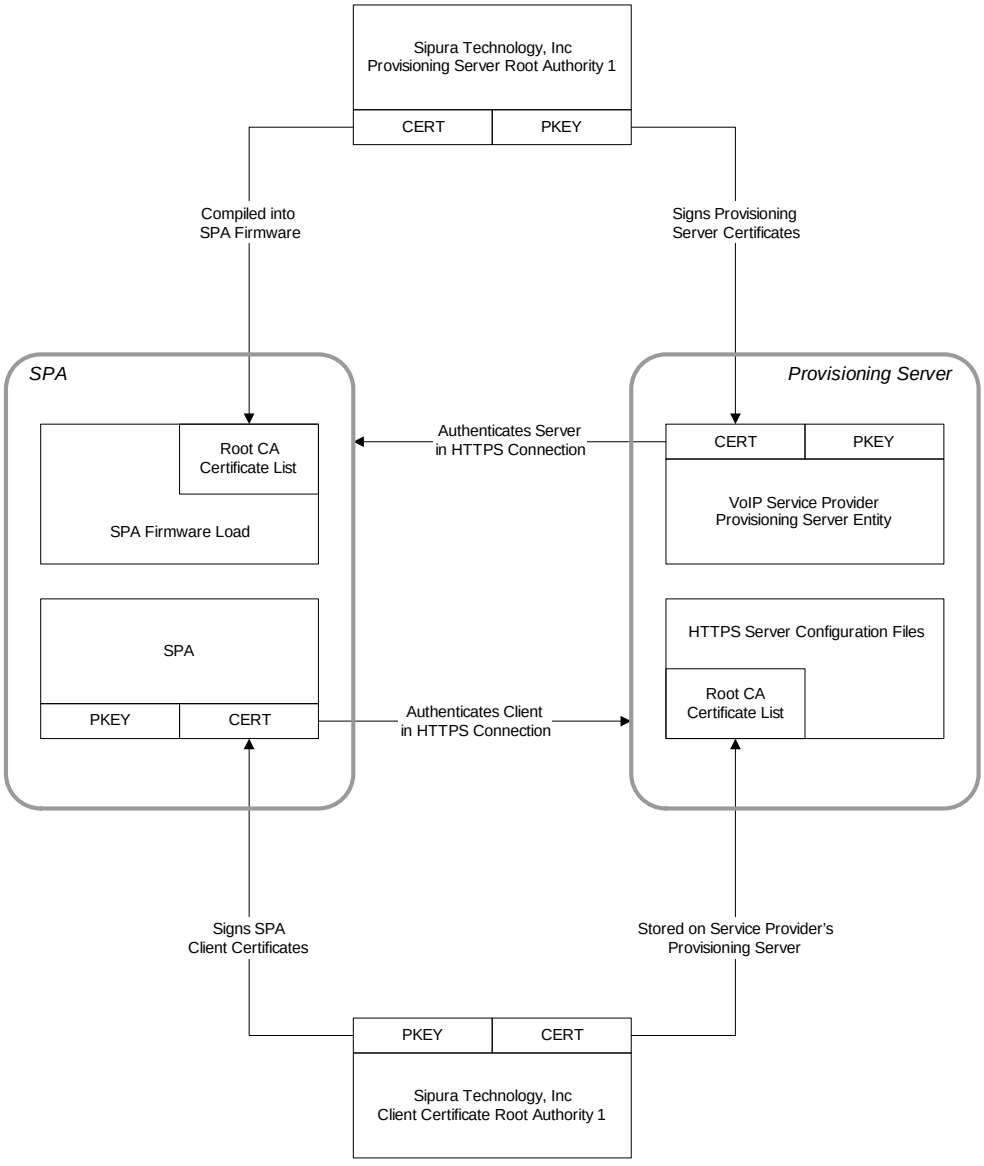
Linksys Certificate Chain Structure

The combination of server certificates and client certificates ensures the secure communication between a remote SPA and its provisioning server. Figure 1-2 illustrates the relationship and placement of certificates, public/private key pairs, and signing root authorities, among the Linksys client, the provisioning server, and the Linksys certification authority.

The upper half of the diagram shows the Linksys Provisioning Server Root Authority, used to sign individual provisioning server certificates. The corresponding root certificate is compiled into all firmware releases at or above 2.0.6, allowing the SPA endpoints to authenticate authorized provisioning servers.

Figure 1-2 SPA Configuration and Provisioning Certificate Chain

SPA Configuration-Provisioning Certificate Chain



As indicated in the lower half of the diagram, a Linksys Client Certificate Root Authority signs each unique certificate. The corresponding root certificate is made available to service providers for client authentication purposes.

Provisioning Setup

This section describes setup requirements for provisioning a SPA and includes the following topics:

License Keys

Certain products within the SPA product family provide for premium features. Enabling these features requires a license key. This key is unique per feature and device. To enable a premium feature in any device, the corresponding key needs to be programmed into the <License_Keys> parameter. Once programmed, the feature remains enabled permanently. License_Keys is a write-only parameter that always appears empty when read. Contact Linksys for further information or to obtain license keys.

Software Tools

The following software tools are useful for provisioning Linksys ATAs :

- Open source gzip compression utility, used when generating configuration profiles
- Open source OpenSSL software package: for profile encryption and HTTPS operations
- Scripting language with CGI scripting support, such as the open source Perl language tools: to test dynamic generation of profiles and one-step remote provisioning using HTTPS
- Ethernet packet analyzer (such as the freely downloadable Ethereal/Wireshark): to verify secure exchanges between provisioning servers and Linksys voice devices
- The ssldump utility: for monitoring HTTPS transactions

Server Configuration

Provisioning requires the availability of servers, which for testing purposes can be installed and run on a local PC:

- TFTP (UDP port 69)
- HTTP (TCP port 80)
- HTTPS (TCP port 443)
- Syslog (UDP port 514)

To troubleshoot server configuration, it is helpful to install a separate client for each type of server on a different host.

TFTP

TFTP is convenient for managing small deployments of SPA units within an office LAN environment. It is also useful for in-house preprovisioning of SPAs in preparation for remote deployment. However, once deployed remotely, HTTP offers greater provisioning reliability, given NAT and router protection mechanisms.

The SPA is able to obtain a TFTP server IP address directly from the DHCP server through DHCP option 66. If this is done, a Profile_Rule need be configured only with the profile filepath on that TFTP server. The Profile_Rule provided with the factory default configuration is as follows:

```
/spa$PSN.cfg
```

For example, on a SPA2102, this expands to /spa2102.cfg, which means that the unit resyncs to this file on the local TFTP server, if that is specified via DHCP option 66. Note that the specified filepath is relative to the TFTP server virtual root directory.

HTTP

The SPA behaves like a browser requesting web pages from any remote Internet site. This provides a reliable means of reaching the provisioning server, even when a customer router implements symmetric NAT or other protection mechanisms. HTTP and HTTPS works more reliably than TFTP in remote deployments, especially when the deployed units are connected behind residential firewalls or NAT-enabled routers.

As an alternative to HTTPS, the SPA can resync to a configuration profile using HTTP. In this case, a separate explicit profile encryption can be used to protect confidential information. The SPA supports 256-bit AES in CBC mode to pre-encrypt individual profiles. These encrypted profiles can be downloaded by the SPA using HTTP without danger of unauthorized use of confidential information in the configuration profile. This resync mode may be useful to reduce the computational load on the provisioning server required when using HTTPS for every resync request.

In a small deployment within a single LAN environment, it is common to rely on a simple TFTP server for provisioning of network devices. Linksys voice devices support TFTP for both provisioning resync and firmware upgrade operations. TFTP is especially useful for the in-house preprovisioning of a large number of un-provisioned devices.

Basic HTTP-based SPA provisioning relies on the HTTP GET method for retrieving configuration profiles. Typically, this means that a configuration file is pre-generated for each deployed SPA, and these files are stored within an HTTP server directory. When the server receives the GET request, it simply returns the file specified in the GET request header.

Alternatively, the requested URL can invoke a CGI script (still using the GET method). In this case, the configuration profile might be generated dynamically, perhaps by querying a customer database and producing the profile on-the-fly.

In the case of CGI handling resync requests, the SPA also supports the HTTP POST method as a mechanism to request the resync configuration data. The SPA can be configured to convey certain status and identification information to the server within the body of the HTTP POST request. The server can use this information to help generate a desired response configuration file, or store the status information for later analysis and tracking.

As part of both GET and POST requests, the SPA automatically includes basic identifying information in the request header, in the User-Agent field. The supplied information conveys manufacturer, product name, current firmware version, and product serial number.

For example, the following is the User-Agent request field from a SPA2102:

```
User-Agent: Linksys/SPA-2102-2.0.5 (88012BA01234)
```

Enabling HTTPS

For increased security managing remotely deployed units, the SPA supports HTTPS for provisioning. To this end, each newly manufactured SPA carries a unique SLL Client Certificate (and associated private key), in addition to a Linksys CA server root certificate. The latter allow the SPA to recognize authorized provisioning servers, and reject non-authorized servers. On the other hand, the client certificate allows the provisioning server to identify the individual SPA issuing the request.

In order for a service provider to manage SPA deployment using HTTPS, a server certificate needs to be generated for each provisioning server to which the SPA resyncs using HTTPS. The server certificate must be signed by the Linksys Server CA Root Key, whose certificate is carried by all deployed units. To obtain a signed server certificate, the service provider must forward a certificate signing request to Linksys, which signs and returns the server certificate for installation on the provisioning server.

The provisioning server certificate must contain in the subject Common Name (CN field) the FQDN of the host running the server. It may optionally contain additional information following the host FQDN, separated by a / character. The following are examples of CN entries that would be accepted as valid by the SPA:

```
CN=sprov.callme.com
CN=pv.telco.net/mailto:admin@telco.net
CN=prof.voice.com/info@voice.com
```

In addition to verifying the certificate chain of the provisioning server certificate, the SPA tests the server IP address against a DNS lookup of the server name specified in the server certificate.

A certificate signing request can be generated using the OpenSSL utility. The following shows an example of the **openssl** command that produces a 1024-bit RSA public/private key pair and a certificate signing request:

```
openssl req -new -out provserver.csr
```

This command generates the server private key in privkey.pem and a corresponding certificate signing request in provserver.csr. In this example, the service provider keeps privkey.pem secret and submits provserver.csr to Linksys for signing. Upon receiving the provserver.csr file, Linksys generates provserver.crt, the signed server certificate.

In addition, Linksys also provides a Linksys CA Client Root Certificate to the service provider. This root certificate certifies the authenticity of the client certificate carried by each SPA.

The unique client certificate offered by each SPA during an HTTPS session carries identifying information embedded in its subject field. This information can be made available by the HTTPS server to a CGI script invoked to handle secure requests. In particular, the certificate subject indicates the unit product name (OU element), MAC address (S element), and serial number (L element). The following is an example of these elements from a SPA2102 client certificate subject field:

```
OU=SPA-2102, L=88012BA01234, S=000e08abcdef
```

Early SPA units, manufactured before firmware 2.0.x, do not contain individual SSL client certificates. When these units are upgraded to a firmware release in the 2.0.x tree, they become capable of connecting to a secure server using HTTPS, but are only able to supply a generic client certificate if requested to do so by the server. This generic certificate contains the following information in the SPA identifying fields:

```
OU=Linksys.com, L=Linksysgeneric, S=Linksysgeneric
```

To determine if a SPA carries an individualized certificate use the $CCERT provisioning macro variable, whose value expands to either Installed or Not Installed, according to the presence or absence of a unique client certificate. In the case of a generic certificate, it is possible to obtain the serial number of the unit from the HTTP request header, in the User-Agent field.

HTTPS servers can be configured to request SSL certificates from connecting clients. If enabled, the server can verify the client certificate chain using the Linksys CA Client Root Certificate supplied by Linksys. It can then provide the certificate information to a CGI for further processing.

The location for storing certificates may vary. For example, on a Apache installation, the file paths for storing the provisioning server signed certificate, its associated private key, and the Linksys CA client root certificate are likely to be as follows:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.crt

# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/provserver.key

# Certificate Authority (CA):
SSLCACertificateFile /etc/httpd/conf/spacroot.crt
```

Refer to the documentation provided for an HTTPS server for specific information.

Firmware release 2.0.6 supports the following cipher suites for SSL connection to a server using HTTPS. Future release updates may implement additional cipher suites.

Table 1-2 Cipher Suites Supported for Connecting to an HTTPS Server

Numeric Code	Cipher Suite
0x0039	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
0x0035	TLS_RSA_WITH_AES_256_CBC_SHA
0x0033	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
0x002f	TLS_RSA_WITH_AES_128_CBC_SHA
0x0005	TLS_RSA_WITH_RC4_128_SHA
0x0004	TLS_RSA_WITH_RC4_128_MD5
0x0062	TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
0x0060	TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
0x0003	TLS_RSA_EXPORT_WITH_RC4_40_MD5

Syslog Server

If a syslog server is configured on the SPA (using the <Syslog_Server> or <Debug_Server> parameters), the resync and upgrade operations log messages to the syslog server. A message can be generated at the start of a remote file request (configuration profile or firmware load), and at the conclusion of the operation (with either success or failure).

The logged messages themselves are configured in the following parameters:

For profile resync:

- Log_Resync_Request_Msg
- Log_Resync_Success_Msg
- Log_Resync_Failure_Msg

For firmware upgrades:

- Log_Upgrade_Request_Msg
- Log_Upgrade_Success_Msg
- Log_Upgrade_Failure_Msg

These parameters are macro expanded into the actual syslog messages.

Where to Go From Here

The following table summarizes the location of specific information in this document for completing different provisioning tasks.

To Do This ...	Refer to ...
Learn to work with Linksys provisioning scripts and configuration profiles.	Chapter 2, “Creating Provisioning Scripts”
Review step-by-step procedures for using the scripting language to create a configuration profile.	Chapter 3, “Provisioning Tutorial”
Refer to the function and usage of each parameter on the Provisioning tab of the administration web server.	Chapter 4, “Provisioning Field Reference”
Look up the expansion for an acronyms use in this document.	Appendix A, “Acronyms”
Define a term used in this document.	Appendix B, “Glossary”

LINKSYS®
A Division of Cisco Systems, Inc.

CHAPTER 2

Creating Provisioning Scripts

This chapter describes the Linksys provisioning script and includes the following sections:

SPA Configuration File

The SPA configuration profile defines the parameter values for a specific SPA device. The profile lets you determine the value for each parameter used by the SPA and also to determine the user access to each parameter: hidden, read-only, or read-write. Any parameters not specified by a profile are left at the factory default values.

The SPA accepts a configuration profile in two formats:

- Open (XML-style) format
- Proprietary, plain-text format

The XML-style format lets you use standard tools to compile the parameters and values. To protect confidential information contained in the configuration profile, this file is generally delivered from the provisioning server to the SPA over a secure channel, provided by HTTPS. A complete example XML profile can be generated using the Linksys profile compiler tool (see the "SPA Configuration Profile Compiler" section on page 2-6), using the following command:

```
spc --sample-xml sample.txt
```

The plain-text configuration file uses a proprietary format, which can be encrypted to prevent unauthorized use of confidential information. By convention, the profile is named with the extension .cfg (for example, spa2102.cfg). The Linksys Profile Compiler (SPC) tool is used to compile the plain-text file containing parameter-value pairs into an encrypted CFG file. The SPC tool is available from Linksys for the Win32 environment (spc.exe) and Linux-i386-elf environment (spc-linux-i386-static). Availability of the SPC tool for the OpenBSD environment is available on a case-by-case basis.

Open Format Configuration File

A configuration file in open, XML-style format can be sent from the provisioning server to the SPA during a resync operation without compiling them into a binary object.

The SPA can accept configuration formats generated by standard tools. This eases development of back-end provisioning server software to generate SPA configuration profiles from existing databases.

The SPA configuration profile open format consists of a text file (with XML-like syntax), optionally compressed using the gzip deflate algorithm (RFC1951), and further optionally encrypted using 256-bit AES symmetric key encryption.

The XML profile syntax consists of an XML-style hierarchy of elements, with element attributes and values. Opening element tags need to be properly matched by corresponding closing element tags. Empty element tags are allowed. Element tags are case sensitive. Comments are allowed, using standard XML syntax. Leading and trailing white space is removed from the parameter value. New lines within a value are converted to spaces.

The SPA recognizes elements with proper SPA parameter names, when encapsulated in the special <flat-profile> element. In addition, the SPA also recognizes arbitrary, configurable aliases for a limited number of parameter names. The <flat-profile> element itself can in turn be encapsulated within other arbitrary elements.

Unrecognized element names are ignored by the SPA. Any parameters not specified by a profile are left unchanged in the SPA. If the XML file contains multiple occurrences of the same parameter tag, the last such occurrence overrides any earlier ones. To avoid inadvertently overriding configuration values for a parameter, it is recommended that at most one instance of a parameter be specified in any one profile.

Element attributes are allowed. Their value must be enclosed by double quotes. All such attributes are ignored by the SPA, except for the user-access attribute: ua.

The user-access attribute defines access to the administration web server for a specific parameter by the User account. Access by the Admin account is unaffected by this attribute.

The ua attribute, if present, must have one of the following values:

- na—no access
- ro—read-only
- rw—read/write

If the user-access attribute (ua) is not specified in an element tag, the factory default user access is applied for the corresponding parameter.

An XML header of the form <? . . . ?> is allowed, but is ignored by the SPA.

As an example, the following profile would be accepted by the SPA. It supplies the values of three provisioning parameters.

```
Basic XML Profile FormatBasic XML Profile Format
```

Example 2-1 Basic XML Profile Format

```
<flat-profile>
<Resync_On_Reset> Yes
  </Resync_On_Reset>
<Resync_Periodic> 7200
  </Resync_Periodic>
<Profile_Rule>
    tftp://prov.telco.com:6900/Linksys/config/spa2102.cfg
```

```
  </Profile_Rule>
</flat-profile>
```

The profiles in Example 2-1 and Example 2-2 are functionally equivalent. Example 2-2 contains additional information and comments, which are ignored by the SPA. Also, in Example 2-2 the <flat-profile> element is encapsulating within the <top-level> element. Such extra encapsulation is allowed, and the parameters within it are still recognized.

Example 2-2 XML Profile with Comments

```
<?xml version='1.0'?>
<top-level>
<!-- Unrecognized element 'generator' is ignored by SPA -->
<generator> Telco Profile Compiler v.1.2
  </generator>
<!-- Unrecognized flat-profile attribute 'device' is ignored by SPA -->
<flat-profile device="Linksys">
<!-- three parameters are specified by this profile -->
<Resync_On_Reset> Yes
    </Resync_On_Reset>
<Resync_Periodic> 7200
    </Resync_Periodic>
<Profile_Rule>
      tftp://prov.telco.com:6900/Linksys/config/spa2102.cfg
    </Profile_Rule>
</flat-profile>
</top-level>
```

The SPA recognizes and translates basic XML character escapes, including escapes for those shown in Table 2-1.

Table 2-1

Special Character	XML Escape Sequence
& (ampersand)	&amp;
< (less than)	&lt;
> (greater than)	&gt;
' (apostrophe)	&apos;
" (double quote)	&quot;

Numeric character escapes, using decimal and hexadecimal values (s.a. `&#40;` and `&#x2e;`), are also translated.

Note The SPA firmware does not support the full Unicode character set, but only the ASCII subset.

The profile in Example 2-3illustrates character escapes. This example defines an information hotline dial plan, which sets the Dial_Plan[1] parameter equal to (S0 <:18005551212>).

Example 2-3 Dial Plan Example

```
<flat-profile>
 <Dial_Plan_1_>
    ( S0 &lt;:18005551212&gt; )
  </Dial_Plan_1_>
```

```
</flat-profile>
```

The element names that are recognized by the SPA can be derived from the SPA administration web server field names as follows:

- Append [*n*] to each of the numbered parameters, where *n* is the line, user, or extension number (for example Dial_Plan[1] and Dial_Plan[2]).
- Replace spaces plus any of the following special characters with underscores:
  - [ ] ( ) /

This is illustrated by Example 2-4, which also illustrates setting user access privileges, using the ua attribute.

Example 2-4 Using Numbers and Spaces in an XML Profile

```
<flat-profile>

  <!-- This sets the SIP TOS/DiffServ Value[1] parameter to be user not-accessible -->
  <SIP_TOS_DiffServ_Value_1_   ua="na"/>

  <!-- This sets the Dial Plan[1] parameter to be user read-only -->
  <Dial_Plan_1_   ua="ro"/>

  <!-- This sets Dial Plan[2] parameter to be user read-write -->
  <Dial_Plan_2_   ua="rw"/>

</flat-profile>
```

The SPA processes empty elements and elements with empty values differently. If an element tag is specified within an empty element form, than the current value of the corresponding parameter is left unchanged. On the other hand, if the element tag is used within an opening and a closing element, with no value between them, then the corresponding parameter is set to an empty string. This is illustrated in Example 2-5.

Example 2-5 Empty Elements vs. Empty Strings

```
<flat-profile>

  <!-- GPP_A will be set to an empty string -->

  <GPP_A>
  </GPP_A>

  <!-- GPP_B will remain unchanged -->

  <GPP_B/>

</flat-profile>
```

Using the empty element form is useful when specifying a read/write parameter (ua=rw). This allows the end user to set and maintain specific values (such as User 1 and User 2 settings), while preventing the profile from overwriting the user-supplied values during a resync operation.

Example 2-6 Empty Elements Preserve User-Configured Values

```
<flat-profile>

  <!-- End-user manages these parameters, values are not changed by this profile -->
```

```
  <Speed_Dial_2_2_  ua="rw"/>
  <Speed_Dial_3_2_  ua="rw"/>
  <Speed_Dial_4_2_  ua="rw"/>
  <Speed_Dial_5_2_  ua="rw"/>
  <Speed_Dial_6_2_  ua="rw"/>
  <Speed_Dial_7_2_  ua="rw"/>
  <Speed_Dial_8_2_  ua="rw"/>
  <Speed_Dial_9_2_  ua="rw"/>

</flat-profile>
```

Configuration File Compression

Optionally, the XML configuration profile can be compressed to reduce the network load on the provisioning server. The supported compression method is the gzip deflate algorithm (RFC1951). The gzip utility and a compression library that implements the same algorithm (zlib) are readily available from Internet sites.

To identify when compression is applied, the SPA expects the compressed file to contain a gzip compatible header, as generated by invoking the gzip utility on the original XML file.

For example, if profile.xml is a valid profile, the file profile.xml.gz is also accepted. This example be generated with either of the following commands:

Example 2-7 Compressing the Configuration Profile

```
# first invocation, replaces original file with compressed file:

gzip profile.xml

# second invocation, leaves original file in place, produces new compressed file:

cat profile.xml | gzip > profile.xml.gz
```

The SPA inspects the downloaded file header to determine the format of the file. The choice of file name is not significant and any convention that is convenient for the service provider can be used.

File Encryption

An XML configuration profile can be encrypted using symmetric key encryption, whether or not it is already compressed. The supported encryption algorithm is the American Encryption Standard (AES), using 256-bit keys, applied in cipher block chaining mode.

Note Compression must precede encryption for the SPA to recognize a compressed and encrypted XML profile. First generate the XML, then compress with gzip, and finally encrypt.

The OpenSSL encryption tool, available for download from various Internet sites, can be used to perform the encryption. Note that support for 256-bit AES encryption may require recompilation of the tool (so as to enable the AES code). The SPA firmware has been tested against version openssl-0.9.7c.

If encrypted, the profile expects the file to have the same format as generated by the following command:

Example 2-8 Encrypting the Configuration Profile

```
# example encryption key = SecretPhrase1234

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml -out profile.cfg

# analogous invocation for a compressed xml file

openssl enc -e -aes-256-cbc -k SecretPhrase1234 -in profile.xml.gz -out profile.cfg
```

A lower case –k precedes the secret key, which can be any plain text phrase and is used to generate a random 64-bit salt. Then, in combination with the secret specified with the –k argument, it derives a random 128-bit initial vector, and the actual 256-bit encryption key.

When this form of encryption is used to encrypt a configuration profile, the SPA needs to be informed of the secret key value to decrypt the file. This value is specified as a qualifier in the pertinent profile URL. The syntax is as follows, using an explicit URL:

```
[--key "SecretPhrase1234"] http://prov.telco.com/path/profile.cfg
```

This is programmed using one of the Profile_Rule parameters. The key must be preprovisioned into the unit at an earlier time. This bootstrap of the secret key can be accomplished securely using HTTPS.

Preencrypting configuration profiles offline with symmetric key encryption allows the use of HTTP for resyncing profiles. The provisioning server only needs to use HTTPS to handle initial provisioning of SPAs after deployment. This reduces the load on the HTTPS server in large scale deployments.

The final file name does not need to follow a specific format, but it is conventional to end the name with the .cfg extension to indicate that it is a configuration profile.

SPA Configuration Profile Compiler

The SPA also accepts configuration profiles in binary format. The SPA configuration profile compiler is a translation tool (spc.exe) that translates a plain-text format into the required binary format.

Appendix C, "Example SPA Configuration Profile" provides an example of a typical SPA2102 configuration text file. Other ATAs are similar. However, the SPA3102 has a number of unique parameters.

The SPC tool expects a semicolon, ;", to separate each parameter definition. If a parameter is not defined in the configuration profile, the current value for that parameter is retained by the SPA.

The SPC tool is available from Linksys upon request in binary executable format in the following versions:

- spc.exe—Windows 32-bit PC environment
- spc-linux-i386-static—Linux ELF environment

Versions of the SPC tool for other platforms may be available by special request.

The profile compiler can generate different types of configuration files, using different types of encryption.

- Generic, non-targeted CFG file, without an explicit key
- Targeted (**--target** option), also encrypts the CFG file without an explicit key, but uses the MAC address of the target SPA, and only that SPA can decode it
- Explicit key-based encryption of the CFG file.

A generic, non-targeted CFG file is accepted as valid by any SPA that resyncs to it. The following command generates a basic CFG file:

```
spc spa2102.txt spa2102.cfg
```

This example compiles the plain-text spa2102.txt file into the binary spa2102.cfg file understood by the SPA2102. The **--scramble** option performs encryption that does not require the explicit transmission of a key to the target SPA. It requires one randomizing argument. For example,

```
spc --scramble SomeSecretPhrase spa2102.txt spa2102.cfg
```

The resulting encrypted spa2102.cfg is accepted as valid by any SPA that resyncs to it.

The **--target** option also encrypts the CFG file without the need to explicitly transmit a key, but does so in such a way that only the target SPA can decode it. Targeted CFG files provide a basic level of security. This command uses the MAC address of the target SPA as an argument. For example,

```
spc --target 000e08aabbcc spa2102.txt spa2102.cfg
```

This command uses the MAC address 000e08aabbcc, and only the SPA with that MAC address is able to decrypt and process the generated spa2102.cfg profile. Any other SPA attempting to resync to this file rejects it as unreadable.

The third option performs an explicit key-based encryption of the CFG file. This option requires that the key used to encrypt the file be preprovisioned in the target SPA, so that it can be decoded.

Two algorithms are available for this type of encryption:

- RC4 (**--rc4**)
- AES (**--aes**)

In addition, the key can be specified either explicitly as a hexadecimal digit sequence (**--hex-key**) or by hashing a secret phrase (**--ascii-key**). With the **--hex-key** option, the key can be up to 256 bits in length. With the **--ascii-key** option the generated key is 128 bits.

The following examples illustrate explicit key-based encryption.

```
spc --rc4 --ascii-key apple4sale spa2102.txt spa2102.cfg
spc --aes --ascii-key lucky777 spa2102.txt spa2102.cfg
spc --aes --ascii-key "my secret phrase" spa2102.txt spa2102.cfg
spc --aes --hex-key 8d23fe7...a5c29 spa2102.txt spa2102.cfg
```

Any combination of scrambling, targeting, and explicit-key encrypting can be applied to a CFG file, as shown by the following example:

```
spc --target 000e08aaa010 --aes --ascii-key VerySecret a.txt a.cfg
```

After each compilation, SPC prints a final status message. Syntax error messages are also printed if a compilation is not successful.

The status and error messages printed by SPC are suppressed with the **--quiet** command line option. Messages can be redirected to a file with the **--log** *file_name* option. In the latter case, the SPC command itself is also printed in the log file, preceded by a timestamp.

```
spc --quiet . . .
spc --log prov.log . . .
```

SPC can also be used to generate sample configuration source files (for both plain text and XML formats), corresponding to the accompanying firmware release. The commands for producing sample files are as follows:

```
# sample plain.txt to be used as source file for eventual spc compilation:
```

```
spc --sample-profile plain.txt

# sample config.xml to be fed directly to an SPA running 2.0.6 or above:

spc --sample-xml config.xml
```

Proprietary Plain-Text Configuration File

The plain-text format is an alternative to the open format and is the only format recognized by firmware releases prior to 2.0.6.

Source Text Syntax

The syntax of the plain-text file accepted by SPC is a series of parameter-value pairs, with the value enclosed in double quotes. Each parameter-value pair is followed by a semicolon (for example, parameter_name “parameter_value”;). If no quoted value is specified for a parameter (or if a parameter specification is missing entirely from the plain-text file) the value of the parameter remains unchanged in the SPA.

The syntax also controls the User account access to the parameter in the administration web server. An optional exclamation point or question mark, immediately following the parameter name, indicates the parameter should be read-write or user read-only for the User account.

If neither mark is present, the parameter is made inaccessible to the user from the web server pages. Note that this syntax has no effect on the Admin account access to the parameter. If the parameter specification is missing entirely from the plain-text file, the User account access to the parameter remains unchanged in the SPA.

If the plain-text file contains multiple occurrences of the same parameter-value specification, the last occurrence overrides any earlier ones. To avoid accidentally overwriting configuration values, it is recommended that no more than one specification for each parameter be included in one profile.

Parameter names in the plain-text file must match the corresponding names appearing in the SPA web interface, with the following modifications:

- Spaces between words are replaced by underscores, for example Multi_Word_Parameter
- Parameters with a numeric identifier use a bracketed index syntax to identify the line, extension, or user (for example, Line_Enable[1] and Line_Enable[2]).
- Comments are delimited by a # character up to the end-of-line. Blank lines can be used for readability.

The following illustrates the format for each parameter-value pair:

```
Parameter_name [ ‘?’ | ‘!’ ] [“quoted_parameter_value_string”] ‘;’
```

Boolean parameter values are asserted by any one of the values {Yes | yes | Enable | enable | 1}. They are deasserted by any one of the values {No | no | Disable | disable | 0}.

The following are examples of plain-text file entries:

```
# These parameter names are for illustration only

Feature_Enable      ! “Enable” ;   # user read-write, but force the value to Enable
Another_Parameter   ? “3600”   ;   # user read-only
Hidden_Parameter      “abc123” ;   # user not-accessible
```

```
Some_Entry          !          ;    # user read-write, leaves value unchanged
```

Multiple plain text files can be spliced together to generate the source for the final binary CFG file. This is accomplished using the **import** directive at the start of a new line followed by one or more spaces and the file name to splice into the stream of parameter-value pairs. File splicing can be nested several files deep.

For example, the file base.txt contains the following:

```
Param1 "base value 1" ;
Param2 "base value 2" ;
```

The file spa1234.txt contains the following lines:

```
import base.txt
Param1 "new value overrides base" ;
Param7 "particular value 7" ;
```

When compiled, spa1234.txt becomes:

```
Param1 "base value 1" ;
Param2 "base value 2" ;
Param1 "new value overrides base" ;
Param7 "particular value 7" ;
```

Comments

During development and scripting, it is often convenient to temporarily disable a provisioning parameter by entering a # character at the start of the parameter value. This effectively comments-out the remaining text in that parameter.

For example, a Profile_Rule with the value "`# http://192.168.1.200/sample.cfg`" is equivalent to an empty Profile_Rule. The # character comment-mechanism applies to the Profile_Rule*, Upgrade_Rule, and Resync_Trigger_* parameters.

Macro Expansion

Several provisioning parameters undergo macro expansion internally prior to being evaluated. This preevaluation step provides greater flexibility controlling the resync and upgrade activities of the SPA.

The parameter groups which undergo macro expansion before evaluation are as follows:

- Resync_Trigger_*
- Profile_Rule*
- Log_Resync_*
- Upgrade_Rule
- Log_Upgrade_*

Under certain conditions, some general purpose parameters (GPP_*) also undergo macro expansion, as explicitly indicated in the Optional Resync Arguments section.

During macro expansion, expressions of the form $NAME and $(NAME) are replaced by the contents of the named variables. See the "Macro Expansion Variables" section on page 4-7 for the complete list of variables available for macro expansion. These include general purpose parameters, several product identifiers, certain event timers, and provisioning state values.

For example, for a SPA with MAC address 000E08012345, the expression:

```
spa$(MAU)config.cfg
```

macro-expands into the following string:

```
spa000E08012345config.cfg
```

If a macro name is not recognized, it remains unexpanded. For example,

```
The name STRANGE is not recognized as a valid macro name, while MAU is recognized as a
valid macro name; so the expression:

spa$STRANGE$MAU.cfg

macro-expands into the string:

spa$STRANGE000E08012345.cfg
```

Macro expansion is not applied recursively. For example, $$MAU" expands into $MAU" (the $$ is expanded), and not 000E08ABCDEF", for a SPA with the indicated MAC address.

The special purpose parameters (GPP_SA through GPP_SD), whose contents are mapped to the macro expressions $SA through $SD, are only macro expanded as the argument of the **--key** option in a resync URL.

Also, the macro expression can qualify the expansion so that only a substring of the macro variable is used instead of its full value, such as a portion of the MAC address.

The syntax for substring macro expansion is $(NAME:p) and $(NAME:p:q), where p and q are non-negative integers. The resulting expansion results in the macro variable substring starting at character offset p, and of length q (or till end-of-string if q is not specified). For example, for an SPA with MAC address 000E08012345, the expression $(MAU:4) macro-expands into the string 08012345, while the expression $(MAU:8:2) macro-expands into the string 23

Conditional Expressions

Conditional expressions can trigger resync events and select from alternative URLs for resync and upgrade operations.

Conditional expressions consist of a list of comparisons, separated by the **and** operator. All comparisons must be satisfied for the condition to be true.

Each comparison can relate one of three types of literals: integer values, software or hardware version numbers, and doubled-quoted strings.

Note that version numbers take the form of three non-negative integers separated by periods (major, minor, and build numbers), plus an optional alphanumeric string in parentheses. No intervening spaces are allowed.

The following are examples of valid version numbers:

```
1.0.31(b)
1.0.33
2.0.3(G)
2.0.3(0412s)
```

```
2.0.6
```

Quoted strings can be compared for equality or inequality. Integers and version numbers can also be compared arithmetically. The comparison operators can be expressed as symbols or as acronyms, as indicated in the table below. Acronyms are particularly convenient when expressing the condition in an XML-style profile.

Table 2-2 Comparison Operators for Conditional Expressions

Operator	Alternate Syntax	Description	Applicable to Integer and Version Operands	Applicable to Quoted String Operands
=	eq	equal to	Yes	Yes
!=	ne	not equal to	Yes	Yes
<	lt	less than	Yes	No
<=	le	less than or equal to	Yes	No
>	gt	greater than	Yes	No
>=	ge	greater than or equal to	Yes	No

For legacy support to firmware versions prior to 2.0.6, the not-equal-to operator can also be expressed as a single ! character (in place of the two-character != string).

Conditional expressions typically involve macro-expanded variables. For example,

```
$REGTMR1 gt 300 and $PRVTMR gt 1200 and "$EXTIP" ne ""

$SWVER ge 2.0.6 and "$CCERT" eq "Installed"
```

It is important to enclose macro variables in double quotes where a string literal is expected. Do not do so doing so where a number or version number is expected.

For legacy support of firmware versions prior to 2.0.6, a relational expression with no left-hand-side operand assumes $SWVER as the implicit left-hand-side. For example, ! 1.0.33 is equivalent to: $SWVER != 1.0.33.

When used in the context of the Profile_Rule* and Upgrade_Rule parameters, conditional expressions must be enclosed within the syntax "(expr)?" as in the following upgrade rule example:

```
( $SWVER ne 2.0.6 )? http://ps.tell.com/sw/spa021024.bin
```

On the other hand, the syntax above using parentheses should not be used when configuring the Resync_Trigger_* parameters.

Assignment Expressions

Arbitrary parameters can be pre-assigned values within the context of Profile_Rule* and Upgrade_Rule parameter. This causes the assignment to be performed before the profile if retrieved.

The syntax for performing these assignments is a list of individual parameter assignments, enclosed within parentheses (assignments)!, with each assignment taking the form:

ParameterXMLName = "Value" ;

Note that the recognized parameter names correspond to the names as for XML-based profiles.

Any parameter can be assigned a new value in this way, and macro-expansion applies. For example, the following is a valid assignment expression:

```
( User_ID_1_ = "uid$B" ; GPP_C = "" ; GPP_D = "$MA" ; )!
```

For conciseness, the general purpose parameters GPP_A through GPP_P can also be referred to by the single lowercase letters a through p. The example above is equivalent to the following:

```
( User_ID_1_ = "uid$B" ; c = "" ; d = "$MA" ; )!
```

White space can optionally be used for readability.

URL Syntax

Standard URL syntax is used to specify how to retrieve configuration files and firmware loads in Profile_Rule* and Upgrade_Rule parameters, respectively. The syntax is as follows:

```
[ scheme:// ] [ server [:port]] filepath
```

Where scheme is one of the following values:

- tftp
- http
- http

If scheme is omitted, tftp is assumed. The server can be a DNS-recognized host name or a numeric IP address. The port is the destination UDP or TCP port number. The filepath must begin with the root directory (/). In other words, it must be an absolute path.

If server is missing, then the tftp server specified through DHCP (option 66) is used instead.

If port is missing, then the standard port for the specified scheme is used instead (tftp uses UDP port 69, http uses TCP port 80, https uses TCP port 443). A filepath must be present. It need not necessarily refer to a static file, but can indicate dynamic content obtained through CGI.

Macro expansion applies within URLs. The following are examples of valid URLs:

```
/$MA.cfg
/Linksys/spa021025.bin
192.168.1.130/profiles/init.cfg
tftp://prov.call.com/cpe/Linksys$MA.cfg
http://neptune.speak.net:8080/prov/$D/$E.cfg
https://secure.me.com/profile?Linksys
```

Optional Resync Arguments

The URLs entered in Profile_Rule* parameters may be preceded by optional arguments, collectively enclosed by square brackets. The recognized options are key, post, and alias.

key

The **key** option is used to specify an encryption key. It is required to decrypt profiles which have been encrypted with an explicit key. The key itself is specified as a (possibly quoted) string following the term **--key**.

Some usage examples:

```
[--key VerySecretValue]
[--key "my secret phrase"]
[--key a37d2fb9055c1d04883a0745eb0917a4]
```

The bracketed optional arguments are macro expanded. In particular, note that the special purpose parameters GPP_SA through GPP_SD are only macro expanded into their macro variables $SA through $SD when used as arguments of the key option, as in the following examples:

```
[--key $SC]
[--key "$SD"]
```

In the case of XML-style profiles, the argument to **--key** must be the same as the argument to the **-k** option given to **openssl**.

In the case of SPC compiled profiles, the argument to **--key** must be the same as the argument to either the **--ascii-key** or the **--hex-key** options, as given to SPC.

post

The **post** option provides an alternative access method for the http and https schemes. If left unspecified, the SPA performs an HTTP GET operation, when contacting the provisioning server. If specified, on the other hand, the SPA performs an HTTP POST operation.

The body of the POST is generated from the contents of one of the general purpose parameters, GPP_A through GPP_P, with macro expansion applied. The GPP_* parameter to use is indicated by a single lowercase letter (a through p) given as argument to the term **--post**.

Using POST provides a convenient alternative to the GET method when arbitrary state or identifying information needs to be supplied from the SPA to the server, as part of periodic resyncs.

For example, GPP_F could contain the following POST body template:

```
Product = "$PN"; MAC_Addr = "$MA"; Ser_Num = "$SN"; SW_Ver = "$SWVER";
```

Then, a URL option such as the following would use the POST method to convey the information to the server in the body of the profile request message (shown here with an accompanying URL):

```
[--post f ] http://ps.one.com/cpe/resyncs?
```

alias

The **alias** option provides a flexible means of recognizing alternative parameter names in XML-based configuration profiles. This is useful in cases where part of the configuration profile is obtained from a customer database form that uses different terminology than expected by the SPA.

For example, a customer XML profile specifies the SIP registration parameters: name, number, auth-secret, enclosed in an XML element hierarchy as follows:

```
<CPE>
  <SIP-Credentials>
    <name>J. Smith</name>
    <number>14085551234</number>
    <auth-secret>732091751563sfd</auth-secret>
  <SIP-Credentials>
</CPE>
```

To map these three parameters directly to the SPA Display_Name_1_, User_ID_1_, and Password_1_ parameters (Line 1), enter this mapping in a general purpose parameter (for example, GPP_M):

```
/CPE/SIP-Credentials/name = /flat-profile/Display_Name_1_ ;
/CPE/SIP-Credentials/number = /flat-profile/User_ID_1_ ;
/CPE/SIP-Credentials/auth-secret = /flat-profile/Password_1_ ;
```

Then, request the customer credentials profile with the following URL option (showing an example URL for completeness):

```
[--alias m ] http://acct.voipservice.net/credentials/spa$MA.xml
```

Upon receiving the profile, the SPA would apply the indicated translations, assigning J. Smith to Display_Name_1_, 14085551234 to User_ID_1_, and 732091751563sfd to Password_1_.

The **alias** option matches only the left-hand-side of an alias as much as specified by the configured alias map. The element itself can be nested further. In the example above, GPP_M could have contained the following instead:

```
/SIP-Credentials/name = /flat-profile/Display_Name_1_ ;
/SIP-Credentials/number = /flat-profile/User_ID_1_ ;
/auth-secret = /flat-profile/Password_1_ ;
```

In general, it is best to specify enough enclosing elements to ensure an unambiguous translation.

The **alias** option is designed to recognize a limited number of critical parameters. Up to 30 parameters can be remapped this way.

Combining Options

Multiple URL options can be combined, by enclosing them within the same set of square brackets. The following are examples of valid URL option strings:

```
[--post j --alias k]
[--key "SymmetricSecret" --alias a]
[--key "$SB" --post g]
[--alias a --key abracadabra321 --post c]
```

Using Provisioning Parameters

This section describes the provisioning parameters broadly organized according to function. It includes the following topics:

General Purpose Parameters

The general purpose parameters GPP_* are used as free string registers when configuring the SPA to interact with a particular provisioning server solution. The GPP_* parameters are empty by default. They can be configured to contain diverse values, including the following:

- Encryption keys
- URLs
- Multistage provisioning status information
- Post request templates
- Parameter name alias maps
- Partial string values, eventually combined into complete parameter values.

The GPP_* parameters are available for macro expansion within other provisioning parameters. For this purpose, single-letter upper-case macro names (A through P) are sufficient to identify the contents of GPP_A through GPP_P. Also, the two-letter upper-case macro names SA through SD identify GPP_SA through GPP_SD as a special case when used as arguments of the **key** URL option.

For example, if GPP_A contains the string ABC, and GPP_B contains 123, the expression AB macro expands into ABC123.

Enables

All profile resync and firmware upgrade operations are controlled by the Provision_Enable and Upgrade_Enable parameters. These parameters control resyncs and upgrades independently of each other. These parameters also control resync and upgrade URL commands issued through the SPA administration web server. Both of these parameters are set to yes by default.

In addition, the Resync_From_SIP parameter controls requests for resync operations via a SIP NOTIFY event sent from the service provider proxy server to the SPA. If enabled, the proxy can request a resync by sending a SIP NOTIFY message containing the Event: resync header to the SPA.

The SPA challenges the request with a 401 response, and expects an authenticated subsequent request before honoring the resync request from the proxy. The Event: reboot_now and Event: restart_now headers perform cold and warm restarts, respectively, are also challenged.

The two remaining enables are Resync_On_Reset and Resync_After_Upgrade_Attempt. These determine if the SPA performs a resync operation after power-up software reboots and after each upgrade attempt.

When enabling Resync_On_Reset, the SPA introduces a random delay following the boot-up sequence before actually performing the reset. The delay is a random time up to the value specified in Resync_Random_Delay (in seconds). In a pool of SPA units, all of which are simultaneously powered up, this introduces a spread in the times at which each unit initiates a resync request to the provisioning server. This feature can be useful in a large residential deployment, in the case of a regional power failures.

Triggers

The SPA is designed to resync with the provisioning server periodically. The resync interval is configured in Resync_Periodic (seconds). If this value is left empty, the SPA does not resync periodically.

The resync typically takes place when the voice lines are idle. In case a SPA voice line is active when a resync is due, the SPA delays the resync procedure until the line becomes idle again. However, it waits no longer than Forced_Resync_Delay (seconds). A resync may cause configuration parameter values to change. This, in turn, causes a firmware reboot, which terminates any voice connection active at the time of the resync.

If a resync operation fails because the SPA was unable to retrieve a profile from the server, if the downloaded file is corrupt, or an internal error occurs, the SPA tries to resync again after a time specified in Resync_Error_Retry_Delay (seconds). If Resync_Error_Retry_Delay is set to 0, the SPA does not try to resync again following a failed resync attempt.

When upgrading, if an upgrade fails, a retry is performed after Upgrade_Error_Retry_Delay seconds.

Two configurable parameters are available to conditionally trigger a resync: Resync_Trigger_1 and Resync_Trigger_2. Each of these parameters can be programmed with a conditional expression (which undergoes macro expansion). If the condition in any of these parameters evaluates to true, a resync operation is triggered, as though the periodic resync timer had expired.

The following example condition triggers a resync if Line 1 failed to register for more than 5 minutes (300 seconds), and at least 10 minutes (600 seconds) have elapsed since the last resync attempt.

```
$REGTMR1 gt 300 and $PRVTMR ge 600
```

Configurable Schedules

Profile resyncs and upgrades provide for automatic retries in case of failure, in addition to periodic configuration updates. Time intervals are specified via three parameters, which are usually specified as a specific interval duration, in seconds. Starting with firmware version 3, these parameters allow the application-level (macro time scale) retry schedule to be configured. These provisioning parameters are:

- Resync_Periodic
- Resync_Error_Retry_Delay
- Upgrade_Error_Retry_Delay

These parameters accept a single delay value (seconds). The new extended syntax allows for a comma-separated list of consecutive delay elements. Each delay element consists of a deterministic delay value, optionally followed by a plus sign and an additional numeric value, which bounds a random extra delay. The last element in the sequence is implicitly repeated forever. For example,

```
Resync_Periodic            =  7200
Resync_Error_Retry_Delay   =  1800,3600,7200,14400
```

In this example, the SPA periodically resyncs every two hours. In case of resync failure, the SPA retries in 30 minutes, then again in 1 more hour, then after two more hours, and then after four more hours, continuing at four-hour intervals until it successfully resyncs.

The following is another example:

```
Resync_Periodic            =  3600+600
Resync_Error_Retry_Delay   =  1800+300,3600+600,7200+900
```

In this example, the SPA periodically resyncs every hour (plus an additional random delay of up to 10 minutes). In case of resync failure, the SPA retries in 30 minutes (plus up to five minutes more).

If it fails again, it waits an additional hour (plus up to 10 minutes). If again unsuccessful, it waits two more hours (plus up to 15 minutes), and so also thereafter, until it successfully resyncs.

The following is another example:

```
Upgrade_Error_Retry_Delay  =  1800,3600,7200,14400+3600
```

In this example, if a remote upgrade attempt fails, the SPA retries the upgrade in 30 minutes, then again after one more hour, then in two hours. If it still fails, it subsequently retries every four to five hours, until it succeeds.

Profile Rules

The SPA provides multiple remote configuration profile parameters (Profile_Rule*). This means that each resync operation can retrieve multiple files, potentially managed by different servers.

In the simplest scenario, the SPA resyncs periodically to a single profile on a central server, which updates all pertinent internal parameters. Alternatively, the profile can be split between different files. One file is common for all the SPAs in a deployment, while a separate file is provided that is unique for each account. Encryption keys and certificate information could be supplied by still another profile, stored on a separate server.

Whenever a resync operation is due, the SPA evaluates the four Profile_Rule* parameters in sequence:

1. Profile_Rule
2. Profile_Rule_B
3. Profile_Rule_C
4. Profile_Rule_D

Each evaluation may result in a profile being retrieved from a remote provisioning server, possibly updating some number of internal parameters. If any of these evaluations fails, the resync sequence is interrupted, and is retried again from the beginning specified by the Resync_Error_Retry_Delay parameter (seconds). If all evaluations succeed, the SPA waits for the second specified by the Resync_Periodic parameter, and then resync once more.

The contents of each Profile_Rule* parameter consist of a set of alternatives. The alternatives are separated by the | character. Each alternative consists of a conditional expression, an assignment expression, a profile URL, and any associated URL options. All these components are optional within each alternative. The following are the valid combinations, and the order in which they must appear, if present:

```
[ conditional-expr ] [ assignment-expr ] [[ options ] URL ]
```

Within each Profile_Rule* parameter, all of the alternatives except the last one must provide a conditional expression. This expression is evaluated and processed as follows:

1. Conditions are evaluated from left to right, until one is found that evaluates as true (or until one alternative is found with no conditional expression)
2. Any accompanying assignment expression is evaluated, if present
3. If a URL is specified as part of that alternative, an attempt is made to download the profile located at the specified URL, and update the internal parameters accordingly.

If all alternatives have conditional expressions, and none evaluates to true (or if the whole profile rule is empty), then the entire Profile_Rule* parameter is skipped, and the next profile rule parameter in the sequence is evaluated.

The following are some examples of valid programming for a single Profile_Rule* parameter.

The following example resyncs unconditionally to the profile at the specified URL, performing an http GET request to the remote provisioning server.

```
http://remote.server.com/Linksys/$MA.cfg
```

In the following example, the SPA resyncs to two different URLs, depending on the registration state of Line 1. In case of lost registration, the SPA performs an HTTP POST to a CGI script, transmitting the contents of the macro expanded GPP_A (which may provide additional information on the state of the SPA).

```
($REGTMR1 eq 0)? http://p.tel.com/has-reg.cfg
| [--post a] http://p.tel.com/lost-reg?
```

In the following example, the SPA resyncs to the same server, but provides additional information if a certificate is not installed in the unit (for legacy pre-2.0 units).

```
("$CCERT" eq "Installed")? https://p.tel.com/config?
| https://p.tel.com/config?Linksys$MAU
```

In the following example, Line 1 is disabled until GPP_A is set equal to Provisioned through the first URL. Afterwards, it resyncs to the second URL.

```
("$A" ne "Provisioned")? (Line_Enable_1_ = "No";)! https://p.tel.com/init-prov
| https://p.tel.com/configs
```

In the following example, the profile returned by the server is assumed to contain XML element tags that need to be remapped to proper SPA parameter names by the aliases map stored in GPP_B.

```
[--alias b] https://p.tel.com/account/spa$MA.xml
```

A resync is typically considered unsuccessful if a requested profile is not received from the server. This default behavior can be overridden by the parameter Resync_Fails_On_FNF. If Resync_Fails_On_FNF is set to No, then the SPA accepts a file-not-found response from the server as a successful resync. The default value for Resync_Fails_On_FNF is Yes.

Report Rule

The SPA provides a mechanism for reporting its current internal configuration to the provisioning server. This is useful for development and debugging. The report syntax is similar to the XML profile. All provisionable parameters are included, except for the values of passwords, keys, and the GPP_SA to GPP_SD parameters, which are not shown.

The Report_Rule parameter is evaluated like a profile rule parameter. In other words, it accepts a URL, optionally qualified with a bracketed expression. The URL specifies the target destination for the report and an encryption key can be included as an option.

The URL scheme can be TFTP, HTTP, or HTTPS. When using TFTP, the operation performed is TFTP PUT. In the case of HTTP and HTTPS, the operation performed is HTTP POST.

If an encryption key is specified, the report is encrypted using 256-bit AES in CBC mode. The encrypted report can be decrypted with the following OpenSSL (or equivalent) command:

```
openssl enc -d -aes-256-cbc -k secretphrase -in rep.xml.enc -out rep.xml
```

The following is an example of the corresponding Report_Rule configuration:

```
[ --key secretphrase ] http://prov.serv.net/spa/$MA/rep.xml.enc
```

Once the report rule is configured, an actual report can be generated and transmitted by sending the SPA a SIP NOTIFY message, with the Event: report type. The SIP NOTIFY request is handled like other SIP notifies, with the SPA requiring authentication from the requesting server before honoring the request to issue a report. Each SIP NOTIFY report request generates one attempt to transmit the report. Retries are not supported.

Upgrade Rule

The SPA provides one configurable remote upgrade parameter, Upgrade_Rule. This parameter accepts a syntax similar to the profile rule parameters. URL options not supported for upgrades, but conditional expressions and assignment expressions can be used. If conditional expressions are used, the parameter can be populated with multiple alternatives, separated by the | character. The syntax for each alternative is as follows:

```
[ conditional-expr ] [ assignment-expr ] URL
```

As in the case of Profile_Rule* parameters, the Upgrade_Rule parameter evaluates each alternative until a conditional expression is satisfied or an alternative has no conditional expression. The accompanying assignment expression is evaluated, if specified. Then, an upgrade to the specified URL is attempted.

If the Upgrade_Rule contains a URL without a conditional expression, the SPA upgrades to the firmware image specified by the URL. Subsequently, it does not attempt to upgrade again until either the rule itself is modified or the effective combination of scheme + server + port + filepath is changed, following macro expansion and evaluation of the rule.

In order to attempt a firmware upgrade, the SPA disables audio at the start of the procedure, and reboots at the end of the procedure. For this reason, an upgrade driven by the contents of Upgrade_Rule is only automatically initiated by the SPA if any voice line is currently inactive.

For example,

```
http://p.tel.com/firmware/spa021025.bin
```

In this example, the Upgrade_Rule upgrades the firmware to the image stored at the indicated URL. The following is another example:

```
("$F" ne "beta-customer")? http://p.tel.com/firmware/spa021025.bin
| http://p.tel.com/firmware/spa-test-0527s.bin
```

This example directs the unit to load one of two images, based on the contents of a general purpose parameter, GPP_F.

The SPA can enforce a downgrade limit with respect to firmware revision number. This can be useful as a customization option. If a valid firmware revision number is configured in the parameter Downgrade_Rev_Limit, the SPA rejects upgrade attempts for firmware versions earlier than the specified limit.

Data Types

The data types used with configuration profile parameters are as follows:

- Uns<n>—Unsigned n-bit value, where n = 8, 16, or 32. It can be specified in decimal or hex format such as 12 or 0x18 as long as the value can fit into n bits.
- Sig<n>—Signed n-bit value. It can be specified in decimal or hex format. Negative values must be preceded by a "-" sign. A + sign before positive value is optional.
- Str<n>—A generic string with up to n non-reserved characters.
- Float<n>—A floating point value with up to n decimal places.
- Time<n>—Time duration in seconds, with up to n decimal places. Extra decimal places specified are ignored.
- PwrLevel—Power level expressed in dBm with 1 decimal place, such as –13.5 or 1.5 (dBm).
- Bool—Boolean value of either "yes" or "no."
- {a,b,c,…}—A choice among a, b, c, …
- IP—IP Address in the form of x.x.x.x, where x between 0 and 255. For example 10.1.2.100.
- Port—TCP/UDP Port number (0-65535). It can be specified in decimal of hex format.
- UserID—User ID as appeared in a URL; up to 63 characters.
- FQDN—Fully Qualified Domain Name, such as "sip.Linksys.com:5060", or "109.12.14.12:12345". It can contain up to 63 characters.
- Phone—A phone number string, such as 14081234567, *69, *72, 345678, or a generic URL such as 1234@10.10.10.100:5068, or jsmith@Linksys.com. It can contain up to 39 characters.
- ActCode—Activation code for a supplementary service, such as *69. It can contain up to 7 characters.
- PhTmplt—A phone number template. Each template may contain one or more patterns separated by a ",". White space at the beginning of each pattern is ignored. "?" and "*" represent wildcard characters. To represent literally use %xx. For example, %2a represents *. It can contain up to 39 characters. Examples: "1408*, 1510*", "1408123????, 555?1.".
- RscTmplt—A template of SIP Response Status Code, such as "404, 5*", "61?", "407, 408, 487, 481". It can contain up to 39 characters.
- CadScript—A mini-script that specifies the cadence parameters of a signal. Up to 127 characters. Syntax: $S_1[;S_2]$, where:
  $S_i=D_i(on_{i,1}/off_{i,1}[,on_{i,2}/off_{i,2}[,on_{i,3}/off_{i,3}[,on_{i,4}/off_{i,4}[,on_{i,5}/off_{i,5}[,on_{i,6}/off_{i,6}]]]]])$ and is known as a *section*, $on_{i,j}$ and $off_{i,j}$ are the on/off duration in seconds of a *segment* and i = 1 or 2, and j = 1 to 6. D_i is the total duration of the section in seconds. All durations can have up to three decimal places to provide 1 ms resolution. The wildcard character "*" stands for infinite duration. The segments within a section are played in order and repeated until the total duration is played.

  Example 1:

```
60(2/4)

Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60 s
Number of Segments = 1
Segment 1: On=2s, Off=4s

Total Ring Length = 60s
```

  Example 2—Distinctive ring (short,short,short,long):

```
60(.2/.2,.2/.2,.2/.2,1/4)
```

```
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 60s
Number of Segments = 4
Segment 1: On=0.2s, Off=0.2s
Segment 2: On=0.2s, Off=0.2s
Segment 3: On=0.2s, Off=0.2s
Segment 4: On=1.0s, Off=4.0s

Total Ring Length = 60s
```

- FreqScript—A mini-script that specifics the frequency and level parameters of a tone. Up to 127 characters. Syntax: $F_1@L_1[,F_2@_{L2}[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$, where F_1–F_6 are frequency in Hz (unsigned integers only) and L_1–L_6 are corresponding levels in dBm (with up to 1 decimal places). White spaces before and after the comma are allowed (but not recommended).

  Example 1—Call Waiting Tone:

```
440@-10

Number of Frequencies = 1
   Frequency 2 = 440 Hz at -10 dBm
```

  Example 2—Dial Tone:

```
350@-19,440@-19

Number of Frequencies = 2
   Frequency 1 = 350 Hz at -19 dBm
   Frequency 2 = 440 Hz at -19 dBm
```

- ToneScript—A mini-script that specifies the frequency, level and cadence parameters of a call progress tone. May contain up to 127 characters. Syntax: FreqScript;Z_1[;Z_2]. The section Z_1 is similar to the S_1 section in a CadScript except that each on/off segment is followed by a frequency components parameter: $Z_1 = D_1(on_{i,1}/off_{i,1}/f_{i,1}[,on_{i,2}/off_{i,2}/f_{i,2}\ [,on_{i,3}/off_{i,3}/f_{i,3}\ [,on_{i,4}/off_{i,4}/f_{i,4}\ [,on_{i,5}/off_{i,5}/f_{i,5}\ [,on_{i,6}/off_{i,6}/f_{i,6}]]]]])$, where $fi,j = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]$ and $1 < n_k < 6$ indicates which of the frequency components given in the FreqScript are used in that segment; if more than one frequency component is used in a segment, the components are summed together.

  Example 1—Dial tone:

```
350@-19,440@-19;10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 10 s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 10s
```

  Example 2—Stutter tone:

```
350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)

Number of Frequencies = 2
Frequency 1 = 350 Hz at -19 dBm
Frequency 2 = 440 Hz at -19 dBm
Number of Cadence Sections = 2
Cadence Section 1: Section Length = 2s
Number of Segments = 1
Segment 1: On=0.1s, Off=0.1s with Frequencies 1 and 2
```

```
Cadence Section 2: Section Length = 10s
Number of Segments = 1
Segment 1: On=forever, with Frequencies 1 and 2

Total Tone Length = 12s
```

Example 3—SIT tone:

```
985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)

Number of Frequencies = 3
Frequency 1 = 985 Hz at -16 dBm
Frequency 2 = 1428 Hz at -16 dBm
Frequency 3 = 1777 Hz at -16 dBm
Number of Cadence Sections = 1
Cadence Section 1: Section Length = 20s
Number of Segments = 4
Segment 1: On=0.38s, Off=0s, with Frequency 1
Segment 2: On=0.38s, Off=0s, with Frequency 2
Segment 3: On=0.38s, Off=0s, with Frequency 3
Segment 4: On=0s, Off=4s, with no frequency components

Total Tone Length = 20s
```

- ProvisioningRuleSyntax—Scripting syntax used to define configuration resync and firmware upgrade rules.
- DialPlanScript—Scripting syntax used to specify Line 1 and Line 2 dial plans.

Notes:

- <Par Name> represents a configuration parameter name. In a profile, the corresponding tag is formed by replacing the space with an underscore “_”, such as **Par_Name**.
- An empty default value field implies an empty string < **“”** >.
- The SPA continues to use the last configured values for tags that are not present in a given profile.
- Templates are compared in the order given. The first, *not the closest*, match is selected. The parameter name must match exactly.
- If more than one definition for a parameter is given in a configuration file, the last such definition in the file is the one that takes effect in the SPA.
- A parameter specification with an empty parameter value forces the parameter back to its default value. To specify an empty string instead, use the empty string **“”** as the parameter value.

LINKSYS®
A Division of Cisco Systems, Inc.

CHAPTER 3

Provisioning Tutorial

This chapter describes the procedures for transferring configuration profiles between the SPA and the provisioning server and includes the following sections:

For information about creating configuration profiles, refer to Chapter 2, “Creating Provisioning Scripts.”

Preparation

The examples presented in this chapter require the availability of one or more servers. For the purposes of this tutorial, these can be installed and run on a local PC. To troubleshoot server configuration, it is helpful to install clients for each type of server on a separate server machine. That establishes proper server operation independent of the interaction with Linksys VoIP devices.

The pertinent servers include: Syslog (UDP port 514), TFTP (UDP port 69), HTTP (TCP port 80), HTTPS (TCP port 443). For generating configuration profiles, it is useful to install the open source gzip compression utility. For profile encryption and HTTPS operations, you can install the open source OpenSSL software package. In addition, to test dynamic generation of profiles and one-step remote provisioning using HTTPS, a scripting language with CGI scripting support, such as the open source Perl language tools, is recommended.

Finally, to verify secure exchanges between provisioning servers and Linksys voice devices, it is useful to install an Ethernet packet sniffer (such as the freely downloadable Ethereal/Wireshark). For HTTPS transactions, you can use the ssldump utility.

A Linksys VoIP device (SPA) can retrieve a configuration profile from a provisioning server and update its internal configuration accordingly. SPAs accept two different profile formats, one based on an open published syntax, and one based on an unpublished binary definition. The open configuration profile format uses a simple XML-like syntax. The binary format is generated by converting a plain text file using the SPA Profile Compiler (SPC).

The examples in this tutorial use configuration profiles with XML-style syntax. To use the proprietary plain-text format, you need to convert the files using SPC before they can be used. This procedure is described in the “Proprietary Profile Format” section on page 3-13.

Basic Resync

This section demonstrates the basic resync functionality of Linksys VoIP devices. It includes the following topics:

TFTP Resync

The SPA supports multiple network protocols for retrieving configuration profiles. The most basic profile transfer protocol is TFTP (RFC1350). TFTP is widely used for the provisioning of network devices within private LAN networks. Although not recommended for deployments of endpoints across the Internet, it can be convenient for deployment within small organizations, for in-house preprovisioning, and for development and testing.

The following configuration profile format uses the XML-style syntax:

```
<flat-profile>
  <GPP_A> 12345678
  </GPP_A>
</flat-profile>
```

The `<flat-profile>` element tag encloses all parameter elements to be recognized by the SPA. The example above defines one parameter value, the first general purpose parameter (GPP_A), with a value of 12345678.

Exercise

Step 1 Within a LAN environment connect a PC and an SPA to a hub, switch, or small router.

Step 2 Connect an analog phone to the Phone 1 port of the SPA.

Step 3 On the PC, install and activate a TFTP server.

Step 4 Using a text editor, create the configuration profile and save it with the name `basic.txt` in the virtual root directory of the installed TFTP server.

Step 5 If possible, verify that the TFTP server is properly configured by requesting the basic.txt file using a TFTP client other than the SPA itself.

Preferably, the TFTP client should be running on a separate host from the server.

Step 6 Using the analog phone, obtain the local IP address of the SPA (IVR menu ****** 110 #**).

If the SPA configuration has been modified since it was manufactured, perform manufacturing reset on it using the IVR RESET option (******** 73738#).

Step 7 Open the PC web browser on the SPA admin/advanced configuration page.

For example, if the SPA IP address is 192.168.1.100):

http://192.168.1.100/admin/advanced

Step 8 The Provisioning tab in the admin/advanced page contains a number of configurable parameters specific to provisioning. Select the Provisioning tab, and inspect the values of the general purpose parameters GPP_A through GPP_P.

These should be empty.

Step 9 To resync the test SPA to the `basic.txt` configuration profile, open the following URL from the PC browser.

Assuming the PC IP address is 192.168.1.200:

http://192.168.1.100/admin/resync?tftp://192.168.1.200/basic.txt

This resync URL method is designed for development and testing. When it receives this command, the SPA at address 192.168.1.100 requests the file `basic.txt` from the TFTP server at IP address 192.168.1.200. It then parses the downloaded file and updates the GPP_A parameter with the value 12345678.

Step 10 Verify that the parameter was correctly updated by refreshing the admin/advanced page on the PC web browser and selecting the Provisioning tab on that page.

The GPP_A parameter should now contain the value 12345678.

Syslog

The SPA sends a syslog message to a syslog server when the SPA is about to resync to a provisioning server and after the resync has either completed or failed. This server is identified in the web server administration (admin/advanced, System tab, Syslog_Server parameter). It is instructive to configure the syslog server IP address into the SPA and observe the messages generated during each exercise.

Exercise

Step 1 Install and activate a syslog server on the local PC.

Step 2 Program the PC IP address into the Syslog_Server parameter, and submit the change.

Click the **System** tab and enter the value of your local syslog server into the Syslog_Server parameter.

Step 3 Repeat the TFTP Resync operation described in the previous exercise.

The SPA generates two syslog messages during the resync. The first indicates that a request is in progress. The second marks success or failure of the resync.

Step 4 Verify that your syslog server received messages such as the following:

```
SPA-2102 00:0e:08:ab:cd:ef -- Requesting resync tftp://192.168.1.200/basic.txt
SPA-2102 00:0e:08:ab:cd:ef -- Successful resync tftp://192.168.1.200/basic.txt
```

More detailed messages are available by programming the Debug_Server parameter (instead of the Syslog_Server parameter) with the IP address of the syslog server, and setting the Debug_Level to a value between 0 and 3 (3 being the most verbose).

The contents of these messages can be configured using the following parameters:

- Log_Resync_Request_Msg
- Log_Resync_Success_Msg

- Log_Resync_Failure_Msg.

If any of these parameters are cleared, the corresponding syslog message is not generated.

Occasionally, it may also be informative to capture an Ethernet packet trace of the interaction between the SPA and the provisioning server. You can run the Ethernet packet analyzer (such as Ethereal/Wireshark) on a PC connected through a hub to the same subnet as the SPA.

Automatic Resync

When a SPA is deployed remotely or as part of an internal company deployment, it may need to resync periodically to the service provider provisioning server, to ensure that any customer profile configuration changes made on the server are propagated to the endpoint, without requiring an explicit resync request to the endpoint.

To cause the SPA to automatically and periodically resync to a server, a configuration profile URL is defined using the Profile_Rule parameter, and a resync period is defined using the Resync_Periodic parameter.

Exercise

Step 1 Using the PC web browser, open the SPA admin/advanced page, Provisioning tab.

Step 2 Define the Profile_Rule parameter.

Step 3 The following value assumes a TFTP server IP address of 192.168.1.200:

```
tftp://192.168.1.200/basic.txt
```

Step 4 In the Resync_Periodic parameter enter a small value for testing such as **30** (meaning 30 seconds).

Step 5 Click **Submit all Changes**.

With the new parameter settings, the SPA now resyncs to the configuration file specified by the URL twice a minute.

Step 6 Observe the resulting messages in the SPA syslog trace.

Step 7 Ensure that the Resync_On_Reset parameter is set to **yes**.

Step 8 Power cycle the SPA.

The SPA also automatically resyncs to the provisioning server whenever it is power-cycled.

If the resync operation fails for any reason, such as if the server is not responding, the unit waits the number of seconds defined in Resync_Error_Retry_Delay before attempting to resync again. If Resync_Error_Retry_Delay is zero, the SPA does not try to resync following a failed resync attempt.

Step 9 (Optional) Verify that the value of Resync_Error_Retry_Delay is set to a small number, such as **30**, disable the TFTP server, and observe the results in the syslog trace.

Unique Profiles and Macro Expansion

In a large deployment, each SPA needs to be configured with distinct values for specific parameters, such as User_ID or Display_Name. This requires the service provider to generate distinct profiles, one for each deployed SPA. Each SPA, in turn, must be configured to resync to its own profile, according to some predetermined profile naming convention.

The SPA profile URL syntax can include identifying information specific to each SPA (such as MAC address and serial number) via macro expansion of built-in variables. This eliminates the need to specify these values within each SPA profile.

The SPA profile rule undergoes macro expansion internally before being applied. The macro expansion understands a number of values including the following:

- $MA expands to the unit MAC address, using lower case hex digits (for example, 000e08abcdef)
- $SN expands to the unit Serial Number (for example, 88012BA01234)

Exercise

Step 1 Obtain the MAC address of the test SPA from its product label.

This is a 12-digit number, using lower case hex digits, beginning with 000308, such as 000e08aabbcc.

Step 2 Copy the basic.txt configuration file to a new file named spa_*mac_address*.cfg and place the new file in the virtual root directory of the TFTP server.

Replace *mac_address* with the actual MAC address of the SPA.

Step 3 Open the SPA admin/advanced page, Provisioning tab.

Step 4 Enter the following value in the Profile_Rule parameter:

tftp://192.168.1.200/spa$MA.cfg

Step 5 Click **Submit All Changes**.

This causes an immediate reboot and resync.

When the next resync occurs, the SPA retrieves the new file by expanding the $MA macro expression into its own MAC address.

Several other values can be macro expanded in this way, including all the general purpose parameters, (GPP_A through GPP_P) These can be referenced as $A through $P. Macro expansion is not limited to the URL file name, but can also be applied to any portion of the profile rule parameter.

For a complete list of variables available for macro expansion, see the "Macro Expansion Variables" section on page 4-7.

URL Resolution

The profile URL can contain a provisioning server name instead of an explicit IP address. In this case, the SPA performs a DNS lookup to resolve the name.

A non-standard server port can be specified in the URL, using the standard syntax :port following the server name.

Also, the configuration profile can be stored in a subdirectory of the server virtual root directory. Again, this is specified using standard URL notation.

For example, the following is a valid Profile_Rule that requests the file spa2102.cfg, in the server subdirectory /Linksys/config, for the TFTP server running on host prov.telco.com, which listens for connection on port 6900.

```
tftp://prov.telco.com:6900/Linksys/config/spa2102.cfg
```

Again, macro expansion can be used anywhere in the URL. This can be convenient in organizing a directory of profiles on the server for the deployed SPA devices. For example, a profile subdirectory name might be supplied for each SPA in a dedicated general purpose parameter, with its value referred within a common profile rule via macro expansion.

For example, GPP_B has the following definition:

```
Dj6Lmp23Q
```

The Profile_Rule has this value:

```
tftp://prov.telco.com/Linksys/$B/$MA.cfg
```

Then, when resyncing, this SPA (assuming a MAC address of 000e08012345) requests the profile at the following URL:

```
tftp://prov.telco.com/Linksys/Dj6Lmp23Q/000e08012345.cfg
```

HTTP GET Resync

HTTP provides a more reliable resync mechanism than TFTP because it is better at establishing a TCP connection between a SPA client behind a firewall or NAT device and a remote provisioning server on the Internet. In addition, HTTP servers offer improved filtering and logging features compared to TFTP servers, which helps to regulate and track connections.

On the SPA client side, using HTTP (with the GET method) simply means changing TFTP to HTTP in the URL defined in the Profile_Rule parameter.

On the server side, the service provider must install and configure the HTTP server. The SPA does not require any special configuration setting on the server to be able to resync using HTTP. If a standard web browser can retrieve a profile from a particular server using HTTP, the SPA should be able to do so as well.

Exercise

Step 1 Install an HTTP server on the local PC or other accessible host.

The open source Apache server can be downloaded from the Internet.

Step 2 Copy the basic.txt configuration profile from the earlier exercises onto the virtual root directory of the installed server.

Step 3 Verify proper server installation (and file access of basic.txt) by accessing the profile using a standard web browser.

Step 4 Modify the Profile_Rule of the test SPA to point to the HTTP server in place of the TFTP server, so as to download its profile periodically.

For example, assuming the HTTP server is at 192.168.1.300, enter the following value:

```
http://192.168.1.200/basic.txt
```

Step 5 Observe the syslog messages sent by the SPA.

The periodic resyncs should now be obtaining the profile from the HTTP server.

Also, the server should be logging each request if connection logging is enabled in the server configuration.

Step 6 In the HTTP server logs, observe how information identifying the test SPA appears in the log of user agents.

This should include the SPA manufacturer, product name, current firmware version, and serial number.

Secure Resync

This section demonstrates the preferred mechanisms available on the SPA for securing the provisioning process. It includes the following topics:

Basic HTTPS Resync

HTTPS adds SSL to HTTP for remote provisioning so that:

- The SPA can authenticate the provisioning server
- The provisioning server can authenticate the SPA
- The confidentiality of information exchanged between the SPA and the provisioning server is ensured through encryption

SSL generates and exchanges secret (symmetric) keys for each connection between the SPA and the server, using public/private key pairs preinstalled in the SPA and the provisioning server.

On the client side, using HTTPS (with the GET method), simply requires changing the definition of the URL in the Profile_Rule parameter from **http** to **https**. On the server side, the service provider must install and set up the HTTPS server.

In addition, an SSL server certificate signed by Linksys must be installed on the SPA provisioning server. The SPA devices cannot resync to a server using HTTPS, unless the server supplies a Linksys-signed server certificate.

Exercise

Step 1 Install an HTTPS server on a host whose IP address is known to the network DNS server, through normal hostname translation.

The open source Apache server can be configured to operate as an HTTPS server, when installed with the open source mod_ssl package.

Step 2 Generate a server Certificate Signing Request for the server.

Step 3 For this step, you may need to install the open source OpenSSL package or equivalent software. If using OpenSSL, the command to generate the basic CSR file is as follows:

```
openssl req -new -out provserver.csr
```

This command generates a public/private key pair, which is saved in the privkey.pem file.

Step 4 Submit the CSR file (provserver.csr) to Linksys for signing.

A signed server certificate is returned (provserver.cert) along with a Linksys CA Client Root Certificate, spacroot.cert.

Step 5 Store the signed server certificate, the private key pair file, and the client root certificate in the appropriate locations on the server.

In the case of an Apache installation on Linux, these locations are typically as follows:

```
# Server Certificate:
SSLCertificateFile /etc/httpd/conf/provserver.cert
# Server Private Key:
SSLCertificateKeyFile /etc/httpd/conf/pivkey.pem
# Certificate Authority:
SSLCACertificateFile /etc/httpd/conf/spacroot.cert
```

Step 6 Restart the server.

Step 7 Copy the basic.txt configuration profile from the earlier exercises onto the virtual root directory of the HTTPS server.

Step 8 Verify proper server operation by downloading basic.txt from the HTTPS server, using a standard browser from the local PC.

Step 9 Inspect the server certificate supplied by the server.

The browser probably does not recognize it as valid unless the browser has been preconfigured to accept Linksys as a root CA. However, SPA devices expect the certificate to be signed this way.

Step 10 Modify the Profile_Rule of the test SPA to contain a reference to the HTTPS server in place of the HTTP server, for example:

https://my.server.com/basic.txt

This example assumes the name of the HTTPS server is my.server.com.

Step 11 Click **Submit All Changes**.

Step 12 Observe the syslog trace sent by the SPA.

The syslog message should indicate that the resync obtained the profile from the HTTPS server.

Step 13 (Optional) Use an Ethernet protocol analyzer on the SPA subnet to verify that the packets are encrypted.

Step 14 In this exercise, client certificate verification is not yet enabled, use a browser to request the profile stored in basic.txt.

At this point, the connection between SPA and server is encrypted. However, the transfer is not secure because any client can connect to the server and request the file, given knowledge of the file name and directory location. For secure resync, the server must also authenticate the client, as demonstrated in the next exercise.

HTTPS With Client Certificate Authentication

In the factory default configuration, the server does not request SSL client certificates from clients. After changing the configuration to enable client authentication, the server requires a client certificate to authenticate the SPA before accepting a connection request.

Because of this, the resync operation in this exercise cannot be independently tested using a browser lacking the proper credentials. Nevertheless, the SSL key exchange within the HTTPS connection between the test SPA and the server can be observed using the ssldump utility. The utility trace shows the interaction between client and server.

Exercise

Step 1 Enable client certificate authentication on the HTTPS server.

Step 2 In Apache (v.2), set the following in the server configuration file:

```
SSLVerifyClient  require
```

Also ensure that the spacroot.cert has been stored as shown in the previous exercise.

Step 3 Restart the HTTPS server and observe the syslog trace from the SPA.

Each resync to the server now performs symmetric authentication, so that both server and client certificates are verified before the profile is transferred.

Step 4 Using ssldump, capture a resync connection between the SPA and the HTTPS server.

If client certificate verification is properly enabled on the server, the ssldump trace shows the symmetric exchange of certificates (first server-to-client, then client-to-server) before the encrypted packets containing the profile.

With client authentication enabled, only a SPA with a MAC address matching a valid client certificate can request the profile from the provisioning server. A request from an ordinary browser or other unauthorized device is rejected by the server.

HTTPS Client Filtering and Dynamic Content

If the HTTPS server is configured to require client certificates, the information in each certificate identifies the resyncing SPA and supplies it with the correct configuration information.

The HTTPS server makes the certificate information available to CGI scripts (or compiled CGI programs) invoked as part of the resync request. For the purpose of illustration, this exercise uses the open source Perl scripting language, and assumes that Apache (v.2) is used as the HTTPS server.

Exercise

Step 1 Install Perl on the host running the HTTPS server.

Step 2 Generate the following Perl reflector script:

```
#!/usr/bin/perl -wT
use strict;
print "Content-Type: text/plain\n\n";
print "<flat-profile><GPP_D>";
```

```
print "OU=$ENV{'SSL_CLIENT_I_DN_OU'},\n";
print "L=$ENV{'SSL_CLIENT_I_DN_L'},\n";
print "S=$ENV{'SSL_CLIENT_I_DN_S'}\n";

print "</GPP_D></flat-profile>";
```

Step 3 Save this file with the file name reflect.pl, with executable permission (chmod 755 on Linux), in the CGI scripts directory of the HTTPS server.

Step 4 Verify accessibility of CGI scripts on the server (as in /cgi-bin/…).

Step 5 Modify the Profile_Rule on the test SPA to resync to the reflector script, as in the following example:

```
https://prov.server.com/cgi-bin/reflect.pl?
```

Step 6 Click **Submit All Changes**.

Step 7 Observe the SPA syslog trace to ensure a successful resync.

Step 8 Open the SPA admin/advanced page, Provisioning tab.

Step 9 Verify that the GPP_D parameter contains the information captured by the script.

This information contains the SPA product name, MAC address, and serial number if the test SPA carries a unique certificate from the manufacturer, or else generic strings if it is a unit manufactured before firmware release 2.0.

A similar script could be used to determine information about the resyncing SPA and then provide it with appropriate configuration parameter values.

Profile Formats

This section demonstrates the generation of configuration profiles. To explain the functionality in this section, TFTP from a local PC is used as the resync method, although HTTP or HTTPS can be used for testing as well, if it is convenient. This section includes the following topics:

Profile Compression

A configuration profile in XML format can become quite large if all parameters are individually specified by the profile. To reduce the load on the provisioning server, the SPA supports compression of the XML file, using the deflate compression format used by the gzip utility (RFC 1951).

Exercise

Step 1 Install gzip on the local PC.

Step 2 Compress the basic.txt profile from earlier exercises, by invoking gzip from the command line:

```
gzip basic.txt
```

This generates the deflated file basic.txt.gz.

Step 3 Save the deflated file in the TFTP server virtual root directory.

Step 4 Modify the Profile_Rule on the test SPA to resync to the deflated file in place of the original XML file, as in the following example:

```
tftp://192.168.1.200/basic.txt.gz
```

Step 5 Click **Submit All Changes**.

Step 6 Observe the syslog trace from the SPA.

Upon resync, the new file is downloaded by the SPA and used to update its parameters.

The file size of such a small profile is not reduced by gzip. Compression is only useful with larger profiles.

For integration into customized back-end provisioning server solutions, the open source zlib compression library can be used in place of the standalone gzip utility to perform the profile compression. However, the SPA expects the file to contain a valid gzip header.

Profile Encryption

A compressed or uncompressed profile can be encrypted. This is useful when the confidentiality of the profile information is of particular concern, such as when using TFTP or HTTP for communication between SPA clients and the provisioning server.

The SPA supports symmetric key encryption using the 256-bit AES algorithm. This encryption can be performed using the open source OpenSSL package.

Exercise

Step 1 Install OpenSSL on a local PC.

This may require recompilation to enable the AES code.

Step 2 Starting from the XML profile in basic.txt, generate an encrypted file with the following command:

```
openssl enc -aes-256-cbc -k MyOwnSecret -in basic.txt -out basic.cfg
```

The compressed basic.txt.gz file could be used instead because the XML profile can be both compressed and encrypted.

Step 3 Store the encrypted file basic.cfg in the TFTP server virtual root directory.

Step 4 Modify the Profile_Rule on the test SPA to resync to the encrypted file in place of the original XML file. The encryption key is made known to the SPA with the following URL option:

```
[--key MyOwnSecret ] tftp://192.168.1.200/basic.cfg
```

Step 5 Click **Submit All Changes**.

Step 6 Observe the syslog trace from the SPA.

On resync, the new file is downloaded by the SPA and used to update its parameters.

Partitioned Profiles

The SPA download multiple separate profiles during each resync. This allows managing different kinds of profile information on separate servers and maintaining common configuration parameter values separate from account specific values.

Exercise

Step 1 Create a new XML profile, basic2.txt, that specifies a value for a distinct parameter from the earlier exercises.

For instance, the file can contain the following:

```
<flat-profile><GPP_B>ABCD</GPP_B></flat-profile>
```

Step 2 Store the basic2.txt profile in the TFTP server virtual root directory.

Step 3 Leave the first profile rule as in any the earlier exercises, but configure the second profile rule (Profile_Rule_B) to point to the new file:

```
tftp://192.168.1.200/basic2.txt
```

Step 4 Click **Submit All Changes**.

The SPA now resyncs to both the first and second profiles, in that order, whenever a resync operation is due.

Step 5 Observe the SPA syslog trace to confirm the expected behavior.

Parameter Name Aliases

When generating an XML profile for the SPA, it may be convenient to assign names to certain configuration parameters that are different from the canonical names recognized by the SPA. For example, a customer account database may generate XML element tags for a customer telephone number and SIP registration password with names such as SIP-number and SIP-password. These names can be mapped to the SPA canonical names (User_ID_1_ and Password_1_) before being applied to SPA Line 1.

In many instances, the back-end provisioning solution used by the service provider can perform this mapping. However, the SPA itself can remap the parameter names internally. To do this, an alias map is defined and stored in one of the general purpose provisioning parameters. Then, the profile rule which invokes the resync is directed to remap the non-canonical XML elements as specified by the alias map.

Exercise

Step 1 Generate a profile named customer.XML containing the proprietary customer-account XML form indicated in the following example:

```
<customer-account>
```

```
  <SIP-number> 17775551234
  </SIP-number>
  <SIP-password> 512835907884
  </SIP-password>
</customer-account>
```

Step 2 Store the file in the TFTP server virtual root directory.

Step 3 Open the test SPA web interface on the admin/advanced page, Provisioning tab, and edit GPP_A to contain the alias map indicated above (do not enter new lines through the web interface, instead simply enter each alias consecutively).

```
/customer-account/SIP-number = /flat-profile/User_ID_1_ ;
/customer-account/SIP-password = /flat-profile/Password_1_ ;
```

Step 4 Edit the Profile_Rule to point to the new XML profile, and also specify the alias map as a URL option, as follows:

```
[--alias a ] tftp://192.168.1.200/customer.xml
```

Step 5 Click **Submit All Changes**.

When the SPA resyncs, it receives the XML profile, remaps the elements, as indicated by the alias map, and populates the User_ID_1_ and Password_1_ parameters.

Step 6 View the Line 1 tab to verify the new configuration.

Note The SPA supports alias remapping of a limited number of parameters. It is not meant to rename all parameters in its configuration.

Proprietary Profile Format

Firmware releases prior to 2.0.6 do not recognize the XML-based profiles described so far in this chapter. Instead, the Linksys Profile Compiler tool (SPC) converts a text-based profile definition into a proprietary binary format understood by earlier versions of the firmware. The tool provides its own options for encrypting the resulting binary profile.

The text-based profile understood by SPC uses a different syntax from the XML profile presented earlier. It consists of a list of parameter-value pairs, with the value in double quotes. Other minor syntax and parameter naming differences also apply. The following example specifies values for two Line 1 parameters:

Exercise

Step 1 Obtain the SPC utility from Linksys.

Executables are available for the Windows Win32 environment, Linux ELF, and OpenBSD.

Step 2 Generate the text profile account.txt containing the two-line profile shown in the following example:

```
User_ID[1] “17775551234” ;
Password[1] “512835907884” ;
```

Step 3 Compile the text profile into a binary file, account.cfg, using the following command:

```
spc account.txt account.cfg
```

Step 4 Store account.cfg in the TFTP server virtual root directory.

Step 5 Modify the test SPA profile rule to point to the new profile:

```
tftp://192.168.1.200/account.cfg
```

Step 6 Click **Submit All Changes**.

Upon resync, the SPA retrieves the new file, recognizes its binary format and updates the two specified parameters.

Step 7 Observe the syslog messages sent by the SPA during resync.

LINKSYS®
A Division of Cisco Systems, Inc.

CHAPTER 4

Provisioning Field Reference

This chapter provides a listing of the parameters provided on the administration web server Provisioning tab, which can be used in configuration profile scripts. It includes the following sections:

The Provisioning parameters described in this chapter are recognized by the SPA beginning with firmware release 2.0.6.

For a complete list of all the parameters available through the administration web server, and which can be used in configuration profiles, refer to the administration guide for each product.

Configuration Profile Parameters

The following table defines the function and usage of each parameter in the Configuration Profile Parameters section under the Provisioning tab.

Table 4-1 Configuration Profile Parameters

Parameter Name	Description and Default Value
Provision_Enable	Controls all resync actions independently of firmware upgrade actions. Set to yes to enable remote provisioning. The default is Yes.
Resync_On_Reset	Triggers a resync after every reboot except for reboots caused by parameter updates and firmware upgrades. The default is Yes.

Table 4-1 Configuration Profile Parameters (continued)

Parameter Name	Description and Default Value
Resync_Random_Delay	The maximum value for a random time interval that the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. This parameter is in units of 20 seconds; the default value of 2 represents 40 seconds. This feature is disabled when this parameter is set to zero. This feature can be used to prevent an overload of the provisioning server when a large number of devices power-on simultaneously. The default is 2 (40 seconds).
Resync_Periodic	The time interval between periodic resyncs with the provisioning server. The associated resync timer is active only after the first successful sync with the server. Set this parameter to zero to disable periodic resyncing. The default is 3600 seconds.
Resync_Error_Retry_Delay	Resync retry interval (in seconds) applied in case of resync failure. The device has an error retry timer that activates if the previous attempt to sync with the provisioning server fails. The device waits to contact the server again until the timer counts down to zero. This parameter is the value that is initially loaded into the error retry timer. If this parameter is set to zero, the device immediately retries to sync with the provisioning server following a failed attempt. The default is 3600 seconds.

Table 4-1 Configuration Profile Parameters (continued)

Parameter Name	Description and Default Value
Forced_Resync_Delay	Maximum delay (in seconds) the SPA waits before performing a resync. The device does not resync while one of its phone lines is active. Because a resync can take several seconds, it is desirable to wait until the device has been idle for an extended period before resyncing. This allows a user to make calls in succession without interruption. The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero. The default is 14,400 seconds.
Resync_From_SIP	Enables a resync to be triggered via a SIP NOTIFY message. The default is Yes.
Resync_After_Upgrade_Attempt	Triggers a resync after every firmware upgrade attempt. The default is Yes.
Resync_Trigger_1 Resync_Trigger_2	Configurable resync trigger conditions. A resync is triggered when the logic equation in these parameters evaluates to TRUE. The default is (empty).
Resync_Fails_On_FNF	Determines whether a file-not-found response from the provisioning server constitutes a successful or a failed resync. A failed resync activates the error resync timer. The default is Yes.
Profile_Rule	This parameter is a profile script that evaluates to the provisioning resync command. The command is a TCP/IP operation and an associated URL. The TCP/IP operation can be TFTP, HTTP, or HTTPS. If the command is not specified, TFTP is assumed, and the address of the TFTP server is obtained through DHCP option 66. In the URL, either the IP address or the FQDN of the server can be specified. The file name can have macros, such as $MA, which expands to the device MAC address. The default is /spa$PSN.cfg.

Table 4-1 Configuration Profile Parameters (continued)

Parameter Name	Description and Default Value
Profile_Rule_B Profile_Rule_C Profile_Rule_D	Defines second, third, and fourth resync commands and associated profile URLs. These profile scripts are executed sequentially after the primary Profile Rule resync operation has completed. If a resync is triggered and Profile Rule is blank, Profile Rule B, C, and D are still evaluated and executed. The default is (empty).
Log_Resync_Request_Msg	This parameter contains the message that is sent to the Syslog server at the start of a resync attempt. The default is $PN $MAC – Requesting resync $SCHEME://$SERVIP:$PORT$PATH.
Log_Resync_Success_Msg	Syslog message issued upon successful completion of a resync attempt. The default is $PN $MAC – Successful resync $SCHEME://$SERVIP:$PORT$PATH -- $ERR.
Log_Resync_Failure_Msg	Syslog message issued after a failed resync attempt. The default is $PN $MAC – Resync failed: $ERR.
Report_Rule	The target URL to which configuration reports are sent. This parameter has the same syntax as the Profile_Rule parameter, and resolves to a TCP/IP command with an associated URL. A configuration report is generated in response to an authenticated SIP NOTIFY message, with Event: report. The report is an XML file containing the name and value of all the device parameters. This parameter may optionally contain an encryption key. For example: `[ --key $K ] tftp://ps.callhome.net/$MA/rep.xml.enc` The default is (empty).

Firmware Upgrade Parameters

The following table defines the function and usage of each parameter in the Firmware Upgrade section of the Provisioning tab.

Table 4-2 Firmware Upgrade Parameters

Parameter Name	Description and Default Value
Upgrade_Enable	Enables firmware upgrade operations independently of resync actions. The default is Yes.
Upgrade_Error_Retry_Delay	The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero. The default is 3600 seconds.
Downgrade_Rev_Limit	Enforces a lower limit on the acceptable version number during a firmware upgrade or downgrade. The device does not complete a firmware upgrade operation unless the firmware version is greater than or equal to this parameter. The default is (empty).
Upgrade_Rule	This parameter is a firmware upgrade script with the same syntax as Profile_Rule. Defines upgrade conditions and associated firmware URLs. The default is (empty).
Log_Upgrade_Request_Msg	Syslog message issued at the start of a firmware upgrade attempt. The default is $PN $MAC -- Requesting upgrade $SCHEME://$SERVIP:$PORT$PATH.
Log_Upgrade_Success_Msg	Syslog message issued after a firmware upgrade attempt completes successfully. The default is $PN $MAC -- Successful upgrade $SCHEME://$SERVIP:$PORT$PATH -- $ERR.
Log_Upgrade_Failure_Msg	Syslog message issued after a failed firmware upgrade attempt. The default is $PN $MAC -- Upgrade failed: $ERR.
License Keys	This field is empty.

General Purpose Parameters

The following table defines the function and usage of each parameter in the General Purpose Parameters section of the Provisioning tab.

Table 4-3 General Purpose Parameters

Parameter Name	Description and Default Value
GPP_SA GPP_SB GPP_SC GPP_SD	Special purpose provisioning parameters, designed to hold encryption keys and passwords. To ensure the integrity of the encryption mechanism, these parameters must be kept secret. Therefore these parameters are not displayed on the device configuration web page, and they are not included in the configuration report sent in response to a SIP NOTIFY command. The default is (empty)
GPP_A GPP_B GPP_C GPP_D GPP_E GPP_F GPP_G GPP_H GPP_I GPP_J GPP_K GPP_L GPP_M GPP_N GPP_O GPP_P	General purpose provisioning parameters. These parameter can be used as variables in provisioning and upgrade rules. They are referenced by prepending the variable name with a '$' character, such as $GPP_A. The default is (empty)

Macro Expansion Variables

The following macro variables are recognized within the following provisioning parameters:

- Profile_Rule
- Profile_Rule_*
- Resync_Trigger_*
- Log_Resync_*
- Upgrade_Rule
- Log_Upgrade_*
- GPP_* (under specific conditions)

Within these parameters, syntax types, such as $NAME or $(NAME), are recognized and expanded.

Macro variable substrings can be specified with the notation $(NAME:p) and $(NAME:p:q), where p and q are non-negative integers (available in revision 2.0.11 and above). The resulting macro expansion is the substring starting at character offset p, with length q (or else till end-of-string if q is not specified). For example, if GPP_A contains ABCDEF, then $(A:2) expands to CDEF, and $(A:2:3) expands to CDE.

An unrecognized name is not translated, and the $NAME or $(NAME) form remains unchanged in the parameter value after expansion. Table 4-4 summarizes the macro expansion variables.

Table 4-4 Macro Expansion Variables

Macro Name	Macro Expansion
$	The form $$ expands to a single $ character.
A through P	Replaced by the contents of the general purpose parameters GPP_A through GPP_P.
SA through SD	Replaced by the contents of the special purpose parameters GPP_SA through GPP_SD. These parameters are meant to hold keys or passwords used in provisioning. Note that $SA through $SD are only recognized as arguments to the optional resync URL qualifier **--key**, as in the following example: `[--key $SA] http://ps.callme.com/profiles/abcdefg.cfg` These variables are not expanded outside of this limited context.
MA	MAC address using lower case hex digits, for example, 000e08aabbcc.
MAU	MAC address using upper case hex digits, for example 000E08AABBCC.
MAC	MAC address using lower case hex digits, and colons to separate hex digit pairs, for example 00:0e:08:aa:bb:cc.
PN	Product Name, for example SPA2102.

Table 4-4 Macro Expansion Variables (continued)

Macro Name	Macro Expansion
PSN	Product Series Number, for example 2102.
SN	Serial Number string, for example 88012BA01234.
CCERT	SSL Client Certificate status: Installed or Not Installed.
IP	IP address of the SPA within its local subnet, for example 192.168.1.100.
EXTIP	External IP of the SPA, as seen on the Internet, for example 66.43.16.52.
SWVER	Software version string, for example 2.0.6(b).
HWVER	Hardware version string, for example 1.88.1.
PRVST	Provisioning State, a numeric string: • -1 = explicit resync request, • 0 = power-up resync, • 1 = periodic resync, • 2 = resync failed, retry attempt
UPGST	Upgrade State, a numeric string: • 1 = first upgrade attempt, • 2 = upgrade failed, retry attempt
UPGERR	Result message (ERR) of previous upgrade attempt, for example http_get failed.
PRVTMR	Seconds since last resync attempt.
UPGTMR	Seconds since last upgrade attempt.
REGTMR1	Seconds since Line 1 lost registration with SIP server.
REGTMR2	Seconds since Line 2 lost registration with SIP server.
UPGCOND	Legacy macro name, always expands to true in firmware rev 2.0.6 and above.
SCHEME	File access scheme, one of TFTP, HTTP, or HTTPS, as obtained after parsing resync or upgrade URL.
METH	Deprecated alias for SCHEME, do not use.
SERV	Request target server host name, as obtained after parsing resync or upgrade URL.
SERVIP	Request target server IP address, as obtained after parsing resync or upgrade URL, possibly following DNS lookup.

Table 4-4 Macro Expansion Variables (continued)

Macro Name	Macro Expansion
PORT	Request target UDP/TCP port, as obtained after parsing resync or upgrade URL.
PATH	Request target file path, as obtained after parsing resync or upgrade URL.
ERR	Result message of resync or upgrade attempt. Only useful in generating result syslog messages. The value is preserved in the UPGERR variable in the case of upgrade attempts.
UID1	The contents of the Line 1 User_ID configuration parameter (Firmware 2.0.11 and above).
UID2	The contents of the Line 2 User_ID configuration parameter (Firmware 2.0.11 and above).
ISCUST	Value=1 if unit is customized, 0 otherwise; customization status viewable on WebUI Info page.

Internal Error Codes

The SPA defines a number of internal error codes (X00–X99) to facilitate configuration in providing finer control over the behavior of the unit under certain error conditions. They can be viewed in Table 4-5.

Table 4-5 Error Code Definitions

Error Code	Description
X00	Transport layer (or ICMP) error when sending a SIP request.
X20	SIP request times out while waiting for a response.
X40	General SIP protocol error (for example, unacceptable codec in SDP in 200 and ACK messages, or times out while waiting for ACK).
X60	Dialed number invalid according to given dial plan.

LINKSYS®
A Division of Cisco Systems, Inc.

APPENDIX A

Acronyms

A/D	Analog To Digital Converter
ANC	Anonymous Call
B2BUA	Back to Back User Agent
Bool	Boolean Values. Specified as yes and no, or 1 and 0 in the profile
CA	Certificate Authority
CAS	CPE Alert Signal
CDR	Call Detail Record
CID	Caller ID
CIDCW	Call Waiting Caller ID
CNG	Comfort Noise Generation
CPC	Calling Party Control
CPE	Customer Premises Equipment
CWCID	Call Waiting Caller ID
CWT	Call Waiting Tone
D/A	Digital to Analog Converter
dB	decibel
dBm	dB with respect to 1 milliwatt
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DRAM	Dynamic Random Access Memory
DSL	Digital Subscriber Loop
DSP	Digital Signal Processor
DTAS	Data Terminal Alert Signal (same as CAS)
DTMF	Dual Tone Multiple Frequency
FQDN	Fully Qualified Domain Name
FSK	Frequency Shift Keying
FXS	Foreign eXchange Station

GW	Gateway
ITU	International Telecommunication Union
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
ILEC	Incumbent Local Exchange Carrier
IP	Internet Protocol
ISP	Internet Service Provider
ITSP	IP Telephony Service Provider
IVR	Interactive Voice Response
LAN	Local Area Network
LBR	Low Bit Rate
LBRC	Low Bit Rate Codec
MC	Mini-Certificate
MGCP	Media Gateway Control Protocol
MOH	Music On Hold
MOS	Mean Opinion Score (1-5, the higher the better)
ms	Millisecond
MSA	Music Source Adaptor
MWI	Message Waiting Indication
OSI	Open Switching Interval
PCB	Printed Circuit Board
PR	Polarity Reversal
PS	Provisioning Server
PSQM	Perceptual Speech Quality Measurement (1-5, the lower the better)
PSTN	Public Switched Telephone Network
NAT	Network Address Translation
OOB	Out-of-band
REQT	(SIP) Request Message
RESP	(SIP) Response Message
RSC	(SIP) Response Status Code, such as 404, 302, 600
RTP	Real Time Protocol
RTT	Round Trip Time
SAS	Streaming Audio Server
SDP	Session Description Protocol

SDRAM	Synchronous DRAM
sec	seconds
SIP	Session Initiation Protocol
SLA	Shared line appearance
SLIC	Subscriber Line Interface Circuit
SP	Service Provider
SPA	Linksys Phone Adaptor
SSL	Secure Socket Layer
TFTP	Trivial File Transfer Protocol
TCP	Transmission Control Protocol
UA	User Agent
uC	Micro-controller
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VM	Voicemail
VMWI	Visual Message Waiting Indication/Indicator
VQ	Voice Quality
WAN	Wide Area Network
XML	Extensible Markup Language

LINKSYS®
A Division of Cisco Systems, Inc.

APPENDIX B

Glossary

ACD (Automatic Call Distribution)—A switching system designed to allocate incoming calls to certain positions or agents in the order received and to hold calls not ready to be handled (often with a recorded announcement).

Area code—A 3-digit code used in North America to identify a specific geographic telephone location. The first digit can be any number between 2 and 9. The second and third digits can be any number.

Billing increment—The division by which the call is rounded. In the field it is common to see full-minute billing on the local invoice while 6-second rounding is the choice of most long-distance providers that bill their customers directly.

Blocked calls—Caused by an insufficient network facility that does not have enough lines to allow calls to reach a given destination. May also pertain to a call from an originating number that is blocked by the receiving telephone number.

Bundled service—Offering various services as a complete package.

Call completion—The point at which a dialed number is answered.

Call termination—The point at which a call is disconnected.

CDR (Call Detail Records)—A software program attached to a VoIP/telephone system that records information about the telephone number activity.

Carrier's carrier—Companies that build fiber optic and microwave networks primarily selling to resellers and carriers. Their main focus is on the wholesale and not the retail market.

Casual access—When customers choose not to use their primary carriers to process the long-distance call being made. The customer dials the carrier 101XXXX number.

CO (Central Office)—Switching center for the local exchange carrier.

Centrex—This service is offered by the LEC to the end user. The feature-rich Centrex line offers the same features and benefits as a PBX to a customer without the capital investment or maintenance charges. The LEC charges a monthly fee to the customer, who must agree to sign a term agreement.

Circuits—The communication path(s) that carry calls between two points on a network.

Customer Premise Equipment—The only part of the telecommunications system that the customer comes into direct contact with. Example of such pieces of equipment are telephones, key systems, PBXs, voice-mail systems, and call accounting systems as well as wiring telephone jacks. The standard for this equipment is set by the FCC, and the equipment is supplied by an interconnect company.

Dedicated access—Customers have direct access to the long-distance provider via a special circuit (T1 or private lines). The circuit is hardwired from the customer site to the POP and does not pass through the LEC switch. The dial tone is provided from the long-distance carrier.

Dedicated Access Line (DAL)—Provided by the local exchange carrier. An access line from the customer telephone equipment directly to the long-distance company switch or POP.

Demarcation point—This is where the LEC ownership and responsibility (wiring, equipment) ends and the customer responsibilities begin.

Direct Inward Dialing (DID)—Allows an incoming call to bypass the attendant and ring directly to an extension. Available on most PBX systems and a feature of Centrex service.

Dual Tone Multifrequency (DTMF)—Better known as the push button keypad. DTMF replaces dial pulses with electronically produced tones for network signaling.

Enhanced service—Services that are provided in addition to basic long distance and accessed by way of a touchtone phone through a series of menus.

Exchange code (NXX)—The first three digits of a phone number.

Flat-rate pricing—The customer is charged one rate (sometimes two rates, one for peak and one for off-peak) rather than a mileage-sensitive program rate.

IXC (Interexchange Carrier)—A long-distance provider that maintains its own switching equipment.

IVR (Interactive Voice Response)—Provides a mechanism for information to be stored and retrieved using voice and a touchtone telephone.

Local loop—The local telephone company provides the transmission facility from the customer to the telephone company office, which is engineered to carry voice and/or data.

North American Numbering Plan (NANP)—How telephone numbers are identified in North America. The telephone number can be identified based on their three separate components: (NPA), (NXX), and (XXXX).

PIN (Personal Identification Code)—A customer calling/billing code for prepaid and pay-as-you-go calling cards.

Private Branch Exchange—Advanced phone system commonly used by the medium to larger customer. It allows the customer to perform a variety of in-house routing (inside calling). The dial tone that is heard when the customer picks up the phone is an internal dial tone.

SS7 (Linksys device Signaling Number 7)—Technology used by large carriers to increase the reliability and speed of transmission between switches.

Switch (switching)—Equipment that connects and routes calls and provides other interim functions such as least cost routing, IVR, and voicemail. It performs the traffic cop function of telecommunications via automated management decisions.

Touchtone (DTMF)—The tone recognized by a push button (touchtone) telephone.

Unified messaging— Platform that lets users send, receive, and manage all e-mail, voice, and fax messages from any telephone, PC, or information device.

Voicemail—A system that allows storage and retrieval of voice messages through voice-mail boxes.

LINKSYS®
A Division of Cisco Systems, Inc.

APPENDIX C

Example SPA Configuration Profile

What follows is a *sample* profile. An up-to-date profile template can be obtained from the SPC tool, with the command line invocation spc --sample-profile sample.txt.

```
# ***
# *** Linksys SPA Series Configuration Parameters
# ***


# *** System Configuration

Restricted_Access_Domains          "" ;
Enable_Web_Server                  "Yes" ;
Web_Server_Port                    "80" ;
Enable_Web_Admin_Access            "Yes" ;
Admin_Passwd                       "" ;
User_Password                    ! "" ;

# *** Internet Connection Type

DHCP                             ! "Yes" ;
Static_IP                        ! "" ;
NetMask                          ! "" ;
Gateway                          ! "" ;

# *** Optional Network Configuration

HostName                         ! "" ;
Domain                           ! "" ;
Primary_DNS                      ! "" ;
Secondary_DNS                    ! "" ;
DNS_Server_Order                   "Manual" ;  # options: Manual/Manual,DHCP/DHCP,Manual
DNS_Query_Mode                     "Parallel" ;  # options: Parallel/Sequential
Syslog_Server                      "" ;
Debug_Server                       "" ;
Debug_Level                        "0" ;  # options: 0/1/2/3
Primary_NTP_Server                 "" ;
Secondary_NTP_Server               "" ;

# *** Configuration Profile

Provision_Enable                   "Yes" ;
Resync_On_Reset                    "Yes" ;
Resync_Random_Delay                "2" ;
Resync_Periodic                    "3600" ;
Resync_Error_Retry_Delay           "3600" ;
Forced_Resync_Delay                "14400" ;
```

```
Resync_From_SIP                     "Yes" ;
Resync_After_Upgrade_Attempt        "Yes" ;
Resync_Trigger_1                    "" ;
Resync_Trigger_2                    "" ;
Profile_Rule                        "/spa$PSN.cfg" ;
Profile_Rule_B                      "" ;
Profile_Rule_C                      "" ;
Profile_Rule_D                      "" ;
Log_Resync_Request_Msg              "$PN $MAC -- Requesting resync
$SCHEME://$SERVIP:$PORT$PATH" ;
Log_Resync_Success_Msg              "$PN $MAC -- Successful resync
$SCHEME://$SERVIP:$PORT$PATH" ;
Log_Resync_Failure_Msg              "$PN $MAC -- Resync failed: $ERR" ;

# *** Firmware Upgrade

Upgrade_Enable                      "Yes" ;
Upgrade_Error_Retry_Delay           "3600" ;
Downgrade_Rev_Limit                 "" ;
Upgrade_Rule                        "" ;
Log_Upgrade_Request_Msg             "$PN $MAC -- Requesting upgrade
$SCHEME://$SERVIP:$PORT$PATH" ;
Log_Upgrade_Success_Msg             "$PN $MAC -- Successful upgrade
$SCHEME://$SERVIP:$PORT$PATH -- $ERR" ;
Log_Upgrade_Failure_Msg             "$PN $MAC -- Upgrade failed: $ERR" ;

# *** General Purpose Parameters

GPP_A                               "" ;
GPP_B                               "" ;
GPP_C                               "" ;
GPP_D                               "" ;
GPP_E                               "" ;
GPP_F                               "" ;
GPP_G                               "" ;
GPP_H                               "" ;
GPP_I                               "" ;
GPP_J                               "" ;
GPP_K                               "" ;
GPP_L                               "" ;
GPP_M                               "" ;
GPP_N                               "" ;
GPP_O                               "" ;
GPP_P                               "" ;
GPP_SA                              "" ;
GPP_SB                              "" ;
GPP_SC                              "" ;
GPP_SD                              "" ;

# *** SIP Parameters

Max_Forward                         "70" ;
Max_Redirection                     "5" ;
Max_Auth                            "2" ;
SIP_User_Agent_Name                 "$VERSION" ;
SIP_Server_Name                     "$VERSION" ;
SIP_Accept_Language                 "" ;
DTMF_Relay_MIME_Type                "application/dtmf-relay" ;
Hook_Flash_MIME_Type                "application/hook-flash" ;
Remove_Last_Reg                     "No" ;
Use_Compact_Header                  "No" ;
```

```
# *** SIP Timer Values (sec)

SIP_T1                          ".5" ;
SIP_T2                          "4" ;
SIP_T4                          "5" ;
SIP_Timer_B                     "32" ;
SIP_Timer_F                     "32" ;
SIP_Timer_H                     "32" ;
SIP_Timer_D                     "32" ;
SIP_Timer_J                     "32" ;
INVITE_Expires                  "240" ;
ReINVITE_Expires                "30" ;
Reg_Min_Expires                 "1" ;
Reg_Max_Expires                 "7200" ;
Reg_Retry_Intvl                 "30" ;
Reg_Retry_Long_Intvl            "1200" ;

# *** Response Status Code Handling

SIT1_RSC                        "" ;
SIT2_RSC                        "" ;
SIT3_RSC                        "" ;
SIT4_RSC                        "" ;
Try_Backup_RSC                  "" ;
Retry_Reg_RSC                   "" ;

# *** RTP Parameters

RTP_Port_Min                    "16384" ;
RTP_Port_Max                    "16482" ;
RTP_Packet_Size                 "0.030" ;
Max_RTP_ICMP_Err                "0" ;
RTCP_Tx_Interval                "0" ;

# *** SDP Payload Types

NSE_Dynamic_Payload             "100" ;
AVT_Dynamic_Payload             "101" ;
G726r16_Dynamic_Payload         "98" ;
G726r24_Dynamic_Payload         "97" ;
G726r40_Dynamic_Payload         "96" ;
G729b_Dynamic_Payload           "99" ;
NSE_Codec_Name                  "NSE" ;
AVT_Codec_Name                  "telephone-event" ;
G711u_Codec_Name                "PCMU" ;
G711a_Codec_Name                "PCMA" ;
G726r16_Codec_Name              "G726-16" ;
G726r24_Codec_Name              "G726-24" ;
G726r32_Codec_Name              "G726-32" ;
G726r40_Codec_Name              "G726-40" ;
G729a_Codec_Name                "G729a" ;
G729b_Codec_Name                "G729ab" ;
G723_Codec_Name                 "G723" ;

# *** NAT Support Parameters

Handle_VIA_received             "No" ;
Handle_VIA_rport                "No" ;
Insert_VIA_received             "No" ;
Insert_VIA_rport                "No" ;
Substitute_VIA_Addr             "No" ;
Send_Resp_To_Src_Port           "No" ;
```

```
STUN_Enable                         "No" ;
STUN_Test_Enable                    "No" ;
STUN_Server                         "" ;
EXT_IP                              "" ;
EXT_RTP_Port_Min                    "" ;
NAT_Keep_Alive_Intvl                "15" ;

# ***

Line_Enable[1]                      "Yes" ;
SAS_Enable[1]                       "No" ;
MOH_Server[1]                       "" ;
SAS_DLG_Refresh_Intvl[1]            "30" ;
NAT_Mapping_Enable[1]               "No" ;
SAS_Inbound_RTP_Sink[1]             "" ;
SIP_Port[1]                         "5060" ;
NAT_Keep_Alive_Enable[1]            "No" ;
EXT_SIP_Port[1]                     "" ;
NAT_Keep_Alive_Msg[1]               "$NOTIFY" ;
SIP_TOS/DiffServ_Value[1]           "0x68" ;
NAT_Keep_Alive_Dest[1]              "$PROXY" ;
RTP_TOS/DiffServ_Value[1]           "0xb8" ;
SIP_Debug_Option[1]                 "none" ;  # options: none/1-line/1-line excl. OPT/1-line
excl. NTFY/1-line excl. REG/1-line excl. OPT|NTFY|REG/full/full excl. OPT/full excl.
NTFY/full excl. REG/full excl. OPT|NTFY|REG
Network_Jitter_Level[1]             "high" ;  # options: low/medium/high/very high
SIP_100REL_Enable[1]                "No" ;
Blind_Attn-Xfer_Enable[1]           "No" ;
SIP_Proxy-Require[1]                "" ;
Auth_Resync-Reboot[1]               "Yes" ;
SIP_Remote-Party-ID[1]              "No" ;

# *** Proxy and Registration

Proxy[1]                            "" ;
Use_Outbound_Proxy[1]               "No" ;
Outbound_Proxy[1]                   "" ;
Use_OB_Proxy_In_Dialog[1]           "Yes" ;
Register[1]                         "Yes" ;
Make_Call_Without_Reg[1]            "No" ;
Register_Expires[1]                 "3600" ;
Ans_Call_Without_Reg[1]             "No" ;
Use_DNS_SRV[1]                      "No" ;
DNS_SRV_Auto_Prefix[1]              "No" ;
Proxy_Fallback_Intvl[1]             "3600" ;

# *** Subscriber Information

Display_Name[1]                     "" ;
User_ID[1]                          "" ;
Password[1]                         "" ;
Use_Auth_ID[1]                      "No" ;
Auth_ID[1]                          "" ;
Mini_Certificate[1]                 "" ;
SRTP_Private_Key[1]                 "" ;

# *** Supplementary Service Subscription

Call_Waiting_Serv[1]                "Yes" ;
Block_CID_Serv[1]                   "Yes" ;
Block_ANC_Serv[1]                   "Yes" ;
Dist_Ring_Serv[1]                   "Yes" ;
```

```
Cfwd_All_Serv[1]                    "Yes" ;
Cfwd_Busy_Serv[1]                   "Yes" ;
Cfwd_No_Ans_Serv[1]                 "Yes" ;
Cfwd_Sel_Serv[1]                    "Yes" ;
Cfwd_Last_Serv[1]                   "Yes" ;
Block_Last_Serv[1]                  "Yes" ;
Accept_Last_Serv[1]                 "Yes" ;
DND_Serv[1]                         "Yes" ;
CID_Serv[1]                         "Yes" ;
CWCID_Serv[1]                       "Yes" ;
Call_Return_Serv[1]                 "Yes" ;
Call_Back_Serv[1]                   "Yes" ;
Three_Way_Call_Serv[1]              "Yes" ;
Three_Way_Conf_Serv[1]              "Yes" ;
Attn_Transfer_Serv[1]               "Yes" ;
Unattn_Transfer_Serv[1]             "Yes" ;
MWI_Serv[1]                         "Yes" ;
VMWI_Serv[1]                        "Yes" ;
Speed_Dial_Serv[1]                  "Yes" ;
Secure_Call_Serv[1]                 "Yes" ;
Referral_Serv[1]                    "Yes" ;
Feature_Dial_Serv[1]                "Yes" ;

# *** Audio Configuration

Preferred_Codec[1]                  "G711u" ;  # options:
G711u/G711a/G726-16/G726-24/G726-32/G726-40/G729a/G723
Silence_Supp_Enable[1]              "No" ;
Use_Pref_Codec_Only[1]              "No" ;
Echo_Canc_Enable[1]                 "Yes" ;
G729a_Enable[1]                     "Yes" ;
Echo_Canc_Adapt_Enable[1]           "Yes" ;
G723_Enable[1]                      "Yes" ;
Echo_Supp_Enable[1]                 "Yes" ;
G726-16_Enable[1]                   "Yes" ;
FAX_CED_Detect_Enable[1]            "Yes" ;
G726-24_Enable[1]                   "Yes" ;
FAX_CNG_Detect_Enable[1]            "Yes" ;
G726-32_Enable[1]                   "Yes" ;
FAX_Passthru_Codec[1]               "G711u" ;  # options: G711u/G711a
G726-40_Enable[1]                   "Yes" ;
FAX_Codec_Symmetric[1]              "Yes" ;
DTMF_Tx_Method[1]                   "Auto" ;  # options: InBand/AVT/INFO/Auto
FAX_Passthru_Method[1]              "NSE" ;  # options: None/NSE/ReINVITE
Hook_Flash_Tx_Method[1]             "None" ;  # options: None/AVT/INFO
FAX_Process_NSE[1]                  "Yes" ;
Release_Unused_Codec[1]             "Yes" ;

# *** Dial Plan

Dial_Plan[1]
"(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)" ;
Enable_IP_Dialing[1]                "No" ;

# *** FXS Port Polarity Configuration

Idle_Polarity[1]                    "Forward" ;  # options: Forward/Reverse
Caller_Conn_Polarity[1]             "Forward" ;  # options: Forward/Reverse
Callee_Conn_Polarity[1]             "Forward" ;  # options: Forward/Reverse

# *** Call Forward Settings
```

```
Cfwd_All_Dest[1]                ! "" ;
Cfwd_Busy_Dest[1]               ! "" ;
Cfwd_No_Ans_Dest[1]             ! "" ;
Cfwd_No_Ans_Delay[1]            ! "20" ;

# *** Selective Call Forward Settings

Cfwd_Sel1_Caller[1]             ! "" ;
Cfwd_Sel1_Dest[1]               ! "" ;
Cfwd_Sel2_Caller[1]             ! "" ;
Cfwd_Sel2_Dest[1]               ! "" ;
Cfwd_Sel3_Caller[1]             ! "" ;
Cfwd_Sel3_Dest[1]               ! "" ;
Cfwd_Sel4_Caller[1]             ! "" ;
Cfwd_Sel4_Dest[1]               ! "" ;
Cfwd_Sel5_Caller[1]             ! "" ;
Cfwd_Sel5_Dest[1]               ! "" ;
Cfwd_Sel6_Caller[1]             ! "" ;
Cfwd_Sel6_Dest[1]               ! "" ;
Cfwd_Sel7_Caller[1]             ! "" ;
Cfwd_Sel7_Dest[1]               ! "" ;
Cfwd_Sel8_Caller[1]             ! "" ;
Cfwd_Sel8_Dest[1]               ! "" ;
Cfwd_Last_Caller[1]             ! "" ;
Cfwd_Last_Dest[1]               ! "" ;
Block_Last_Caller[1]            ! "" ;
Accept_Last_Caller[1]           ! "" ;

# *** Speed Dial Settings

Speed_Dial_2[1]                 ! "" ;
Speed_Dial_3[1]                 ! "" ;
Speed_Dial_4[1]                 ! "" ;
Speed_Dial_5[1]                 ! "" ;
Speed_Dial_6[1]                 ! "" ;
Speed_Dial_7[1]                 ! "" ;
Speed_Dial_8[1]                 ! "" ;
Speed_Dial_9[1]                 ! "" ;

# *** Supplementary Service Settings

CW_Setting[1]                   ! "Yes" ;
Block_CID_Setting[1]            ! "No" ;
Block_ANC_Setting[1]            ! "No" ;
DND_Setting[1]                  ! "No" ;
CID_Setting[1]                  ! "Yes" ;
CWCID_Setting[1]                ! "Yes" ;
Dist_Ring_Setting[1]            ! "Yes" ;
Secure_Call_Setting[1]            "No" ;

# *** Distinctive Ring Settings

Ring1_Caller[1]                 ! "" ;
Ring2_Caller[1]                 ! "" ;
Ring3_Caller[1]                 ! "" ;
Ring4_Caller[1]                 ! "" ;
Ring5_Caller[1]                 ! "" ;
Ring6_Caller[1]                 ! "" ;
Ring7_Caller[1]                 ! "" ;
Ring8_Caller[1]                 ! "" ;

# *** Ring Settings
```

```
Default_Ring[1]                 ! "1" ;  # options: 1/2/3/4/5/6/7/8
Default_CWT[1]                  ! "1" ;  # options: 1/2/3/4/5/6/7/8
Hold_Reminder_Ring[1]           ! "8" ;  # options: 1/2/3/4/5/6/7/8/none
Call_Back_Ring[1]               ! "7" ;  # options: 1/2/3/4/5/6/7/8
Cfwd_Ring_Splash_Len[1]         ! "0" ;
Cblk_Ring_Splash_Len[1]         ! "0" ;
VMWI_Ring_Splash_Len[1]         ! ".5" ;
VMWI_Ring_Policy[1]              "New VM Available" ;  # options: New VM Available/New VM
Becomes Available/New VM Arrives
Ring_On_No_New_VM[1]             "No" ;

# ***

Line_Enable[2]                   "Yes" ;
SAS_Enable[2]                    "No" ;
MOH_Server[2]                    "" ;
SAS_DLG_Refresh_Intvl[2]         "30" ;
NAT_Mapping_Enable[2]            "No" ;
SAS_Inbound_RTP_Sink[2]          "" ;
SIP_Port[2]                      "5061" ;
NAT_Keep_Alive_Enable[2]         "No" ;
EXT_SIP_Port[2]                  "" ;
NAT_Keep_Alive_Msg[2]            "$NOTIFY" ;
SIP_TOS/DiffServ_Value[2]        "0x68" ;
NAT_Keep_Alive_Dest[2]           "$PROXY" ;
RTP_TOS/DiffServ_Value[2]        "0xb8" ;
SIP_Debug_Option[2]              "none" ;  # options: none/1-line/1-line excl. OPT/1-line
excl. NTFY/1-line excl. REG/1-line excl. OPT|NTFY|REG/full/full excl. OPT/full excl.
NTFY/full excl. REG/full excl. OPT|NTFY|REG
Network_Jitter_Level[2]          "high" ;  # options: low/medium/high/very high
SIP_100REL_Enable[2]             "No" ;
Blind_Attn-Xfer_Enable[2]        "No" ;
SIP_Proxy-Require[2]             "" ;
Auth_Resync-Reboot[2]            "Yes" ;
SIP_Remote-Party-ID[2]           "No" ;

# *** Proxy and Registration

Proxy[2]                         "" ;
Use_Outbound_Proxy[2]            "No" ;
Outbound_Proxy[2]                "" ;
Use_OB_Proxy_In_Dialog[2]        "Yes" ;
Register[2]                      "Yes" ;
Make_Call_Without_Reg[2]         "No" ;
Register_Expires[2]              "3600" ;
Ans_Call_Without_Reg[2]          "No" ;
Use_DNS_SRV[2]                   "No" ;
DNS_SRV_Auto_Prefix[2]           "No" ;
Proxy_Fallback_Intvl[2]          "3600" ;

# *** Subscriber Information

Display_Name[2]                  "" ;
User_ID[2]                       "" ;
Password[2]                      "" ;
Use_Auth_ID[2]                   "No" ;
Auth_ID[2]                       "" ;
Mini_Certificate[2]              "" ;
SRTP_Private_Key[2]              "" ;

# *** Supplementary Service Subscription
```

```
Call_Waiting_Serv[2]              "Yes" ;
Block_CID_Serv[2]                 "Yes" ;
Block_ANC_Serv[2]                 "Yes" ;
Dist_Ring_Serv[2]                 "Yes" ;
Cfwd_All_Serv[2]                  "Yes" ;
Cfwd_Busy_Serv[2]                 "Yes" ;
Cfwd_No_Ans_Serv[2]               "Yes" ;
Cfwd_Sel_Serv[2]                  "Yes" ;
Cfwd_Last_Serv[2]                 "Yes" ;
Block_Last_Serv[2]                "Yes" ;
Accept_Last_Serv[2]               "Yes" ;
DND_Serv[2]                       "Yes" ;
CID_Serv[2]                       "Yes" ;
CWCID_Serv[2]                     "Yes" ;
Call_Return_Serv[2]               "Yes" ;
Call_Back_Serv[2]                 "Yes" ;
Three_Way_Call_Serv[2]            "Yes" ;
Three_Way_Conf_Serv[2]            "Yes" ;
Attn_Transfer_Serv[2]             "Yes" ;
Unattn_Transfer_Serv[2]           "Yes" ;
MWI_Serv[2]                       "Yes" ;
VMWI_Serv[2]                      "Yes" ;
Speed_Dial_Serv[2]                "Yes" ;
Secure_Call_Serv[2]               "Yes" ;
Referral_Serv[2]                  "Yes" ;
Feature_Dial_Serv[2]              "Yes" ;

# *** Audio Configuration

Preferred_Codec[2]                "G711u" ;  # options:
G711u/G711a/G726-16/G726-24/G726-32/G726-40/G729a/G723
Silence_Supp_Enable[2]            "No" ;
Use_Pref_Codec_Only[2]            "No" ;
Echo_Canc_Enable[2]               "Yes" ;
G729a_Enable[2]                   "Yes" ;
Echo_Canc_Adapt_Enable[2]         "Yes" ;
G723_Enable[2]                    "Yes" ;
Echo_Supp_Enable[2]               "Yes" ;
G726-16_Enable[2]                 "Yes" ;
FAX_CED_Detect_Enable[2]          "Yes" ;
G726-24_Enable[2]                 "Yes" ;
FAX_CNG_Detect_Enable[2]          "Yes" ;
G726-32_Enable[2]                 "Yes" ;
FAX_Passthru_Codec[2]             "G711u" ;  # options: G711u/G711a
G726-40_Enable[2]                 "Yes" ;
FAX_Codec_Symmetric[2]            "Yes" ;
DTMF_Tx_Method[2]                 "Auto" ;  # options: InBand/AVT/INFO/Auto
FAX_Passthru_Method[2]            "NSE" ;  # options: None/NSE/ReINVITE
Hook_Flash_Tx_Method[2]           "None" ;  # options: None/AVT/INFO
FAX_Process_NSE[2]                "Yes" ;
Release_Unused_Codec[2]           "Yes" ;

# *** Dial Plan

Dial_Plan[2]
"(*xx|[3469]11|0|00|[2-9]xxxxxx|1xxx[2-9]xxxxxxS0|xxxxxxxxxxx.)" ;
Enable_IP_Dialing[2]              "No" ;

# *** FXS Port Polarity Configuration

Idle_Polarity[2]                  "Forward" ;  # options: Forward/Reverse
```

```
Caller_Conn_Polarity[2]           "Forward" ;  # options: Forward/Reverse
Callee_Conn_Polarity[2]           "Forward" ;  # options: Forward/Reverse

# *** Call Forward Settings

Cfwd_All_Dest[2]                ! "" ;
Cfwd_Busy_Dest[2]               ! "" ;
Cfwd_No_Ans_Dest[2]             ! "" ;
Cfwd_No_Ans_Delay[2]            ! "20" ;

# *** Selective Call Forward Settings

Cfwd_Sel1_Caller[2]             ! "" ;
Cfwd_Sel1_Dest[2]               ! "" ;
Cfwd_Sel2_Caller[2]             ! "" ;
Cfwd_Sel2_Dest[2]               ! "" ;
Cfwd_Sel3_Caller[2]             ! "" ;
Cfwd_Sel3_Dest[2]               ! "" ;
Cfwd_Sel4_Caller[2]             ! "" ;
Cfwd_Sel4_Dest[2]               ! "" ;
Cfwd_Sel5_Caller[2]             ! "" ;
Cfwd_Sel5_Dest[2]               ! "" ;
Cfwd_Sel6_Caller[2]             ! "" ;
Cfwd_Sel6_Dest[2]               ! "" ;
Cfwd_Sel7_Caller[2]             ! "" ;
Cfwd_Sel7_Dest[2]               ! "" ;
Cfwd_Sel8_Caller[2]             ! "" ;
Cfwd_Last_Caller[2]             ! "" ;Cfwd_Sel8_Dest[2]               ! "" ;
Cfwd_Last_Dest[2]               ! "" ;
Block_Last_Caller[2]            ! "" ;
Accept_Last_Caller[2]           ! "" ;

# *** Speed Dial Settings

Speed_Dial_2[2]                 ! "" ;
Speed_Dial_3[2]                 ! "" ;
Speed_Dial_4[2]                 ! "" ;
Speed_Dial_5[2]                 ! "" ;
Speed_Dial_6[2]                 ! "" ;
Speed_Dial_7[2]                 ! "" ;
Speed_Dial_8[2]                 ! "" ;
Speed_Dial_9[2]                 ! "" ;

# *** Supplementary Service Settings

CW_Setting[2]                   ! "Yes" ;
Block_CID_Setting[2]            ! "No" ;
Block_ANC_Setting[2]            ! "No" ;
DND_Setting[2]                  ! "No" ;
CID_Setting[2]                  ! "Yes" ;
CWCID_Setting[2]                ! "Yes" ;
Dist_Ring_Setting[2]            ! "Yes" ;
Secure_Call_Setting[2]            "No" ;

# *** Distinctive Ring Settings

Ring1_Caller[2]                 ! "" ;
Ring2_Caller[2]                 ! "" ;
Ring3_Caller[2]                 ! "" ;
Ring4_Caller[2]                 ! "" ;
Ring5_Caller[2]                 ! "" ;
Ring6_Caller[2]                 ! "" ;
```

```
Ring7_Caller[2]                 ! "" ;
Ring8_Caller[2]                 ! "" ;

# *** Ring Settings

Default_Ring[2]                 ! "1" ;  # options: 1/2/3/4/5/6/7/8
Default_CWT[2]                  ! "1" ;  # options: 1/2/3/4/5/6/7/8
Hold_Reminder_Ring[2]           ! "8" ;  # options: 1/2/3/4/5/6/7/8/none
Call_Back_Ring[2]               ! "7" ;  # options: 1/2/3/4/5/6/7/8
Cfwd_Ring_Splash_Len[2]         ! "0" ;
Cblk_Ring_Splash_Len[2]         ! "0" ;
VMWI_Ring_Splash_Len[2]         ! ".5" ;
VMWI_Ring_Policy[2]              "New VM Available" ;  # options: New VM Available/New VM
Becomes Available/New VM Arrives
Ring_On_No_New_VM[2]             "No" ;

# *** Call Progress Tones

Dial_Tone                         "350@-19,440@-19;10(*/0/1+2)" ;
Second_Dial_Tone                  "420@-19,520@-19;10(*/0/1+2)" ;
Outside_Dial_Tone                 "420@-16;10(*/0/1)" ;
Prompt_Tone                       "520@-19,620@-19;10(*/0/1+2)" ;
Busy_Tone                         "480@-19,620@-19;10(.5/.5/1+2)" ;
Reorder_Tone                      "480@-19,620@-19;10(.25/.25/1+2)" ;
Off_Hook_Warning_Tone             "480@-10,620@0;10(.125/.125/1+2)" ;
Ring_Back_Tone                    "440@-19,480@-19;*(2/4/1+2)" ;
Confirm_Tone                      "600@-16;1(.25/.25/1)" ;
SIT1_Tone
"985@-16,1428@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)" ;
SIT2_Tone
"914@-16,1371@-16,1777@-16;20(.274/0/1,.274/0/2,.380/0/3,0/4/0)" ;
SIT3_Tone
"914@-16,1371@-16,1777@-16;20(.380/0/1,.380/0/2,.380/0/3,0/4/0)" ;
SIT4_Tone
"985@-16,1371@-16,1777@-16;20(.380/0/1,.274/0/2,.380/0/3,0/4/0)" ;
MWI_Dial_Tone                    "350@-19,440@-19;2(.1/.1/1+2);10(*/0/1+2)" ;
Cfwd_Dial_Tone                   "350@-19,440@-19;2(.2/.2/1+2);10(*/0/1+2)" ;
Holding_Tone                     "600@-19;*(.1/.1/1,.1/.1/1,.1/9.5/1)" ;
Conference_Tone                  "350@-19;20(.1/.1/1,.1/9.7/1)" ;
Secure_Call_Indication_Tone      "397@-19,507@-19;15(0/2/0,.2/.1/1,.1/2.1/2)" ;

# *** Distinctive Ring Patterns

Ring1_Cadence                    "60(2/4)" ;
Ring2_Cadence                    "60(.3/.2,1/.2,.3/4)" ;
Ring3_Cadence                    "60(.8/.4,.8/4)" ;
Ring4_Cadence                    "60(.4/.2,.3/.2,.8/4)" ;
Ring5_Cadence                    "60(.2/.2,.2/.2,.2/.2,1/4)" ;
Ring6_Cadence                    "60(.2/.4,.2/.4,.2/4)" ;
Ring7_Cadence                    "60(.4/.2,.4/.2,.4/4)" ;
Ring8_Cadence                    "60(0.25/9.75)" ;

# *** Distinctive Call Waiting Tone Patterns

CWT1_Cadence                     "30(.3/9.7)" ;
CWT2_Cadence                     "30(.1/.1, .1/9.7)" ;
CWT3_Cadence                     "30(.1/.1, .3/.1, .1/9.3)" ;
CWT4_Cadence                     "30(.1/.1,.1/.1,.1/9.5)" ;
CWT5_Cadence                     "30(.3/.1,.1/.1,.3/9.1)" ;
CWT6_Cadence                     "30(.1/.1,.3/.2,.3/9.1)" ;
CWT7_Cadence                     "30(.3/.1,.3/.1,.1/9.1)" ;
CWT8_Cadence                     "2.3(.3/2)" ;
```

```
# *** Distinctive Ring/CWT Pattern Names

Ring1_Name                          "Bellcore-r1" ;
Ring2_Name                          "Bellcore-r2" ;
Ring3_Name                          "Bellcore-r3" ;
Ring4_Name                          "Bellcore-r4" ;
Ring5_Name                          "Bellcore-r5" ;
Ring6_Name                          "Bellcore-r6" ;
Ring7_Name                          "Bellcore-r7" ;
Ring8_Name                          "Bellcore-r8" ;

# *** Ring and Call Waiting Tone Spec

Ring_Waveform                       "Sinusoid" ;  # options: Sinusoid/Trapezoid
Ring_Frequency                      "25" ;
Ring_Voltage                        "70" ;
CWT_Frequency                       "440@-10" ;

# *** Control Timer Values (sec)

Hook_Flash_Timer_Min                ".1" ;
Hook_Flash_Timer_Max                ".9" ;
Callee_On_Hook_Delay                "0" ;
Reorder_Delay                       "5" ;
Call_Back_Expires                   "1800" ;
Call_Back_Retry_Intvl               "30" ;
Call_Back_Delay                     ".5" ;
VMWI_Refresh_Intvl                  "30" ;
Interdigit_Long_Timer               "10" ;
Interdigit_Short_Timer              "3" ;
CPC_Delay                           "2" ;
CPC_Duration                        "0" ;

# *** Vertical Service Activation Codes

Call_Return_Code                    "*69" ;
Blind_Transfer_Code                 "*98" ;
Call_Back_Act_Code                  "*66" ;
Call_Back_Deact_Code                "*86" ;
Cfwd_All_Act_Code                   "*72" ;
Cfwd_All_Deact_Code                 "*73" ;
Cfwd_Busy_Act_Code                  "*90" ;
Cfwd_Busy_Deact_Code                "*91" ;
Cfwd_No_Ans_Act_Code                "*92" ;
Cfwd_No_Ans_Deact_Code              "*93" ;
Cfwd_Last_Act_Code                  "*63" ;
Cfwd_Last_Deact_Code                "*83" ;
Block_Last_Act_Code                 "*60" ;
Block_Last_Deact_Code               "*80" ;
Accept_Last_Act_Code                "*64" ;
Accept_Last_Deact_Code              "*84" ;
CW_Act_Code                         "*56" ;
CW_Deact_Code                       "*57" ;
CW_Per_Call_Act_Code                "*71" ;
CW_Per_Call_Deact_Code              "*70" ;
Block_CID_Act_Code                  "*67" ;
Block_CID_Deact_Code                "*68" ;
Block_CID_Per_Call_Act_Code         "*81" ;
Block_CID_Per_Call_Deact_Code       "*82" ;
Block_ANC_Act_Code                  "*77" ;
Block_ANC_Deact_Code                "*87" ;
```

```
DND_Act_Code                        "*78" ;
DND_Deact_Code                      "*79" ;
CID_Act_Code                        "*65" ;
CID_Deact_Code                      "*85" ;
CWCID_Act_Code                      "*25" ;
CWCID_Deact_Code                    "*45" ;
Dist_Ring_Act_Code                  "*26" ;
Dist_Ring_Deact_Code                "*46" ;
Speed_Dial_Act_Code                 "*74" ;
Secure_All_Call_Act_Code            "*16" ;
Secure_No_Call_Act_Code             "*17" ;
Secure_One_Call_Act_Code            "*18" ;
Secure_One_Call_Deact_Code          "*19" ;
Referral_Services_Codes             "" ;
Feature_Dial_Services_Codes         "" ;

# *** Outbound Call Codec Selection Codes

Prefer_G711u_Code                   "*017110" ;
Force_G711u_Code                    "*027110" ;
Prefer_G711a_Code                   "*017111" ;
Force_G711a_Code                    "*027111" ;
Prefer_G723_Code                    "*01723" ;
Force_G723_Code                     "*02723" ;
Prefer_G726r16_Code                 "*0172616" ;
Force_G726r16_Code                  "*0272616" ;
Prefer_G726r24_Code                 "*0172624" ;
Force_G726r24_Code                  "*0272624" ;
Prefer_G726r32_Code                 "*0172632" ;
Force_G726r32_Code                  "*0272632" ;
Prefer_G726r40_Code                 "*0172640" ;
Force_G726r40_Code                  "*0272640" ;
Prefer_G729a_Code                   "*01729" ;
Force_G729a_Code                    "*02729" ;

# *** Miscellaneous

Set_Local_Date_(mm/dd)              "" ;
Set_Local_Time_(HH/mm)              "" ;
Time_Zone                           "GMT-07:00" ;  # options:
GMT-12:00/GMT-11:00/GMT-10:00/GMT-09:00/GMT-08:00/GMT-07:00/GMT-06:00/GMT-05:00/GMT-04:00/
GMT-03:30/GMT-03:00/GMT-02:00/GMT-01:00/GMT/GMT+01:00/GMT+02:00/GMT+03:00/GMT+03:30/GMT+04
:00/GMT+05:00/GMT+05:30/GMT+05:45/GMT+06:00/GMT+06:30/GMT+07:00/GMT+08:00/GMT+09:00/GMT+09
:30/GMT+10:00/GMT+11:00/GMT+12:00/GMT+13:00
FXS_Port_Impedance                  "600" ;  # options:
600/900/600+2.16uF/900+2.16uF/270+750||150nF/220+820||120nF/220+820||115nF/370+620||310nF
FXS_Port_Input_Gain                 "-3" ;
FXS_Port_Output_Gain                "-3" ;
DTMF_Playback_Level                 "-16" ;
DTMF_Playback_Length                ".1" ;
Detect_ABCD                         "Yes" ;
Playback_ABCD                       "Yes" ;
Caller_ID_Method                    "Bellcore(N.Amer,China)" ;  # options:
Bellcore(N.Amer,China)/DTMF(Finland,Sweden)/DTMF(Denmark)/ETSI DTMF/ETSI DTMF With PR/ETSI
DTMF After Ring/ETSI FSK/ETSI FSK With PR(UK)
FXS_Port_Power_Limit                "3" ;  # options: 1/2/3/4/5/6/7/8
Protect_IVR_FactoryReset            "No" ;
```

LINKSYS®
A Division of Cisco Systems, Inc.

INDEX

Symbols

Numerics

A

B

C

D

E

N

O

P

R

S

T

U

W

X