



ADMINISTRATOR- HANDBUCH

**Cisco Services Ready-Plattformen der
Serie SRP500 (SRP520-Modelle)**

Cisco und das Cisco Logo sind Marken von Cisco Systems, Inc. und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Cisco Marken finden Sie unter www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1005R)

Kapitel 1: Einführung der Services Ready-Plattform der Serie SRP500 (SRP520-Modelle) 10

Funktionsübersicht	10
Produktübersicht	11
Modellnummern	11
Vorderseite	11
Vorderseite der SRP521W	11
Vorderseite der SRP526W/SRP527W	12
LEDs auf der Vorderseite	12
Rückseite	13
Rückseite der SRP521W	13
Rückseite der SRP526W/SRP527W	13
Beschreibung der Rückseite	14
Seitenansicht	15
Draufsicht	16
Standardeinstellungen	17

Kapitel 2: Erste Schritte im Konfigurationsprogramm 18

Anmelden beim Konfigurationsprogramm	18
Überblick über das Konfigurationsprogramm	19
Bereiche des Hauptfensters	19
Symbole im Konfigurationsprogramm	20

Kapitel 3: Das Schnelleinrichtungsmenü 21

Basic Configuration Setup (Grundlegende Konfigurationseinrichtung)	21
WAN Setup (Ethernet) (WAN-Einrichtung (Ethernet))	21
WAN Setup (ADSL) (WAN-Einrichtung (ADSL))	22
LAN Setup (LAN-Einrichtung)	22
Wireless Setup (Wireless-Einrichtung)	23
Remote Provisioning (Remote-Bereitstellung)	23
Advanced Configuration Setup (Erweiterte Konfigurationseinrichtung)	24
Sprachkommunikation	24
Mobile Network Setup (Mobilnetzeinrichtung)	24

Firewall	24
NAT	24
Kapitel 4: Einrichten der Schnittstellen auf der Services Ready-Plattform	25
Einrichten der WAN-Schnittstelle	25
Internet Setup (Interneteinrichtung)	26
Hinzufügen einer Subschnittstelle	29
Kapselungseinstellungen	32
IPoA-Einstellungen	32
PPPoE-Einstellungen	33
PPPoA-Einstellungen	34
Internetoptionen	35
Mobile Network (Mobilnetz)	36
Ausfallsicherung und Wiederherstellung	40
Einrichten der VLAN-Schnittstellen und LAN-Ports	42
DHCP-Server	42
VLAN-Einstellungen	46
Porteinstellungen	48
Einrichten des Wireless LAN	49
Basic Wireless Settings (Grundlegende Wireless-Einstellungen)	50
Wi-Fi Protected Setup	56
WPS-Methode 1	57
WPS-Methode 2	57
WPS-Methode 3	57
Wireless MAC Filter (Wireless-MAC-Filter)	58
Erweiterte Wireless-Einstellungen	60
WMM-Einstellung	63
Verwenden der Verwaltungsschnittstelle	64
Kapitel 5: Konfigurieren des Netzwerks	65
Routing	66
Static Routes (Statische Routen)	66
RIP (RIP)	67

Intervlan Routing (Intervlan-Routing)	69
NAT	69
NAT Setting (NAT-Einstellung)	70
Port Forwarding (Portweiterleitung)	70
Port Range Triggering (Portbereich-Triggering)	72
QoS	75
QoS Bandwidth Control (QoS-Bandbreitensteuerung)	75
QoS Policy (QoS-Richtlinie)	77
CoS To Queue (CoS für Warteschlangen)	79
DSCP To Queue (DSCP zu Warteschlange)	79
Firewall	80
Firewall Filter (Firewall-Filter)	80
Internet Access Control (Internet-Zugriffssteuerung)	82
PPPoE Relay (PPPoE-Relay)	85
DDNS	86
DMZ	89
IGMP (IGMP)	90
UPnP	91
CDP Setting (CDP-Einstellung)	92

Kapitel 6: Sprache konfigurieren 94

Konfigurieren von Sprachdiensten	94
Funktion der Sprach-Ports	94
SRP-Sprachfunktionen	95
Unterstützte Codecs	95
SIP-Proxy-Redundanz	96
Weitere SRP-Sprachfunktionen	97
Registrieren beim Service Provider	103
Verwalten von Anrufer-ID-Diensten	105
Optimieren der Faxdurchgangsraten	107
Fehlerbehebung: Fax	108
Pausenunterdrückung und Erzeugung von Komfortauschen	109

Konfigurieren von Wählplänen	110
Allgemeines zu Wählplänen	110
Zahlenfolgen	110
Beispiele für Ziffernfolgen	112
Annahme und Übertragung der gewählten Ziffern	114
Wählplan-Timer (Off-Hook-Timer)	115
Syntax für den Wählplan-Timer	116
Beispiele für den Wählplan-Timer	116
Langer Inter-Digit-Timer (Timer für unvollständige Eingaben)	117
Syntax für den langen Inter-Digit-Timer	117
Beispiel für den langen Inter-Digit-Timer	117
Kurzer Inter-Digit-Timer (Timer für vollständige Eingaben)	117
Syntax für den kurzen Inter-Digit-Timer	118
Beispiele für den kurzen Inter-Digit-Timer	118
Bearbeiten von Wählplänen	118
Eingeben des Wählplans für Leitungsschnittstellen	118
Zurücksetzen der Kontrolltimer	119
Umsetzung von sicheren Anrufen	120
Aktivieren von sicheren Anrufen	120
Ausführliche Informationen zu sicheren Anrufen	121
Verwendung von Mini-Zertifikaten	122
Erzeugen von Mini-Zertifikaten	123
Konfigurieren von Spracheinstellungen	124
Seite Info (Infos)	124
Product Information (Produktinformationen)	124
System Status (Systemstatus)	125
Line Status (Status der Leitung)	126
Seite System (System)	130
Systemkonfiguration	130
Weitere Einstellungen	130
Seite SIP (SIP)	131
SIP-Parameter	131
SIP-Timer-Werte	134
Behandlung von Antwortstatuscodes	136
RTP Parameters (RTP-Parameter)	137
SDP-Payload-Typen	139
Parameter NAT-Unterstützung	141
Seite Provisioning (Bereitstellung)	144
Konfigurationsprofil	144

Firmware Upgrade (Firmware-Upgrade)	148
Allgemeine Parameter	149
Seite Regional (Regional)	150
Festlegen von Rufton-, Kadenz- und Tonskripten	150
Anruffortschrittstöne	152
Unterschiedliche Klingeltöne	155
Unterschiedliche Anklopftöne	156
Namen für unterschiedliche Klingel-/CWT-Töne	157
Spezifikationen für Klingel- und Anklopftöne	158
Kontrolltimerwerte (Sek.)	159
Vertikale Dienstaktivierungscodes	162
Vertikale Dienstankündigungscodes	170
Codec-Auswahlcodes für ausgehende Anrufe	170
Weitere Bestimmungen	171
Seiten Line (1–2) (Leitung 1-2)	174
Leitung aktivieren	175
Streaming-Audio-Server (SAS)	175
NAT-Einstellungen	177
Netzwerkeinstellungen	177
SIP-Einstellungen	179
Anruffunktionseinstellungen	184
Proxy und Registrierung	185
Teilnehmerinformationen	187
Supplementary Service Subscription (Abonnement für ergänzende Dienste)	188
Audiokonfiguration	192
Wählplan	197
Konfiguration der FXS-Portpolarität	198
Benutzerseiten (1–2)	199
Einstellungen Anrufweiterleitung	199
Einstellungen zur Weiterleitung ausgewählter Anrufe	200
Kurzwahleinstellungen	200
Einstellungen für ergänzende Dienste	201
Einstellungen für unterschiedliche Klingeltöne	203
Einstellungen für den Klingelton	203
Kapitel 7: VPN-Konfiguration	204
IKE-Richtlinie	204
IPSec-Richtlinie	207

GRE-Tunnel	211
VPN-Passthrough	213
Cisco VPN Server	214
Konfigurieren von Benutzern	217

Kapitel 8: Verwaltungseinstellungen 220

Web Access Management (Webzugangsverwaltung)	221
Remote-Management	223
TR069	223
SNMP	225
SNMP-Portbeschreibungen	227
Local TFTP (Lokales TFTP)	228
Time Setup (Zeiteinrichtung)	229
Setup Wizard (Installationsassistent)	230
Benutzerliste	231
User Privilege Control (Benutzerberechtigungssteuerung)	232
Protokollierung	232
Factory Defaults (Werkseitige Einstellungen)	233
Firmware Upgrade (Firmware-Upgrade)	234
Datensicherung und -wiederherstellung	234
Backup Configuration (Konfiguration sichern)	235
Restore Configuration (Konfiguration wiederherstellen)	235
Reboot (Neu starten)	235
Status	236
Switch Setting (Switch-Einstellung)	236

Kapitel 9: Verwenden der Diagnose für die Services Ready-Plattform 238

Ping Test (Ping-Test)	238
Traceroute Test (Traceroute-Test)	239
Detect Active LAN Clients (Aktive LAN-Clients erkennen)	239

Kapitel 10: Anzeigen des Status der Services Ready-Plattformen	240
Router-Einstellungen	241
Firewall Status (Firewall-Status)	242
Interface Information (Schnittstelleninformationen)	244
Wireless Network Status (Wireless-Netzwerk-Status)	245
Wireless Client Information (Informationen zum Wireless-Client)	246
Mobile Network Status (Mobilnetzstatus)	247
DHCP Server Information (DHCP-Serverinformationen)	249
QoS Status (QoS-Status)	250
Routing Table (Routing-Tabelle)	251
ARP Table (ARP-Tabelle)	252
RIP Status (RIP-Status)	252
IGMP Status (IGMP-Status)	253
VPN Status (VPN-Status)	253
CDP Neighbor Information (CDP-Nachbarinformationen)	254
Anhang A: Technische Daten	255
Anhang B: Weiterführende Informationen	257

Einführung der Services Ready-Plattform der Serie SRP500 (SRP520-Modelle)

Vielen Dank, dass Sie sich für die Cisco Services Ready-Plattformen der Serie SRP500 (SRP520-Modelle) entschieden haben. Die Geräte der Serie SRP500 sind flexible Geräte, die kleinen und mittleren Unternehmen die Möglichkeit geben, verschiedene Dienste von Service Providern zu nutzen, beispielsweise hochwertige Datendienste, gehostete Sprachdienste und Sicherheitsservices.

In diesem Kapitel erhalten Sie erste Informationen zu Ihrem neuen Gerät. Folgende Themen sind enthalten:

- **Funktionsübersicht**
- **Produktübersicht**

Informationen zur physischen Installation der SRP und zur Verwendung des Installationsassistenten für die Konfiguration des Geräts finden Sie in der Schnellstartanleitung für die Cisco Services Ready-Plattformen der Serie SRP500 (SRP520-Modelle) unter: www.cisco.com/go/srp500/

Funktionsübersicht

Vielen Dank, dass Sie sich für die Cisco Services Ready-Plattform der Serie SRP500 (SRP520-Modelle) entschieden haben.

Die SRP500-Plattformen umfassen die folgenden Funktionen:

- Intelligente Funktionen zur Unterstützung von Sprach-, Daten-, Sicherheits- und Anwendungsdiensten
- Branchenführender SIP-Stack (Session Initiation Protocol) für klare, hochwertige Sprachdienste
- Kompatibilität mit häufig eingesetzten Soft-Switches und Sprach-Gateways
- Integrierte Sicherheit, VPN-Funktionen und ein Wireless Access Point (802.11n)
- Standardbasierte Bereitstellung für einen optimierten Einsatz

Produktübersicht

In diesem Abschnitt werden die SRP-Modellnummern aufgeführt und die Vorder-, Rück- und Seitenansichten des Geräts dargestellt.

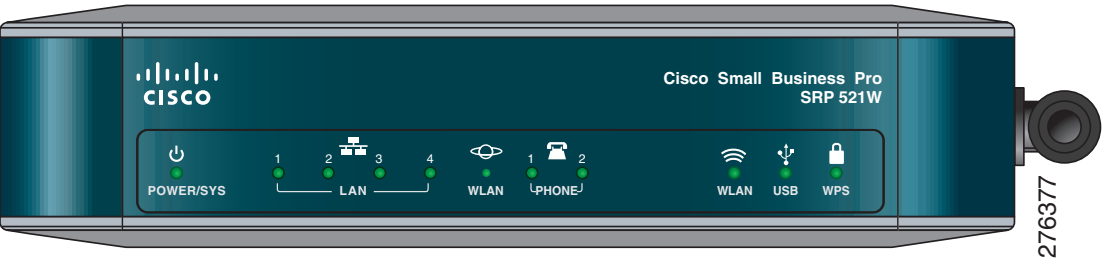
Modellnummern

In der folgenden Tabelle werden die SRP520-Modellnummern erläutert:

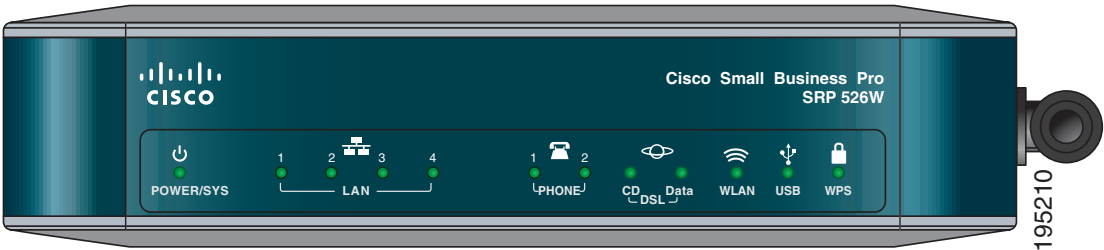
Modell	Beschreibung
SRP521W	Fast Ethernet WAN 2 Telefon-Ports (FXS), 1 Line-Port (FXO), 1 WAN-Port (10/100), 4 LAN-Ports (10/100), 1 USB-2.0-Port, 802.11n und Wi-Fi Protected Setup (WPS)
SRP526W	ADSL2+ Annex B (ADSL über ISDN) 2 Telefon-Ports (FXS), 1 Line-Port (FXO), 1 DSL-Port, 4 LAN-Ports (10/100), 1 USB-2.0-Port, 802.11n und Wi-Fi Protected Setup (WPS)
SRP527W	ADSL2+ Annex A/M (ADSL über POTS) 2 Telefon-Ports (FXS), 1 Line-Port (FXO), 1 DSL-Port, 4 LAN-Ports (10/100), 1 USB-2.0-Port, 802.11n und Wi-Fi Protected Setup (WPS)

Vorderseite

Vorderseite der SRP521W



Vorderseite der SRP526W/SRP527W



LEDs auf der Vorderseite

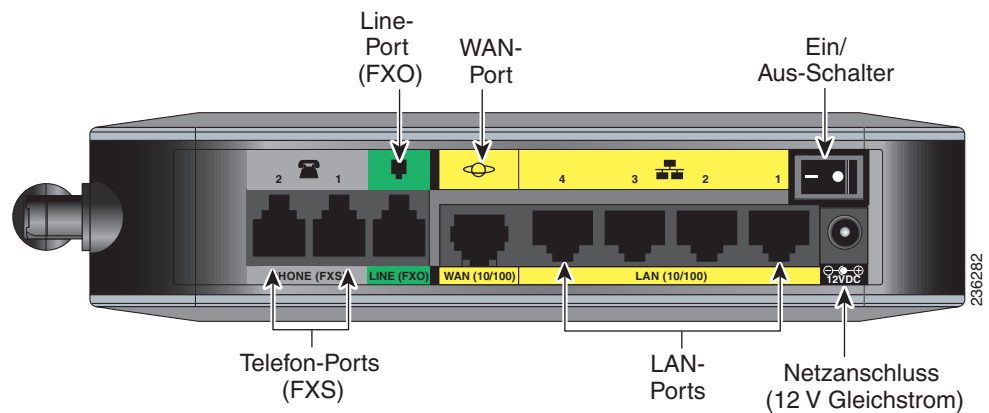
In der folgenden Tabelle werden die LEDs auf der Vorderseite der SRP erläutert. Diese LEDs werden für die Überwachung der Systemaktivität verwendet.

LEDs (grün)	Beschreibung
POWER/SYS (STROM/SYSTEM)	Leuchtet, wenn die SRP erfolgreich gestartet wurde und betriebsbereit ist. Blinkt, wenn die SRP startet.
LAN-Ports (1 bis 4)	Leuchtet, wenn eine Verbindung hergestellt wurde. Blinkt, wenn auf dem LAN-Port Aktivitäten verzeichnet werden.
WAN-Port (nur für SRP521W)	Leuchtet, wenn eine Verbindung hergestellt wurde. Blinkt, wenn auf dem WAN-Port Aktivitäten verzeichnet werden.
Telefon-Ports (FXS) (1 bis 2)	Leuchtet, wenn eine Verbindung hergestellt wurde. Blinkt, wenn auf dem Telefon-Port Aktivitäten verzeichnet werden.
DSL CD	Blinkt, wenn ein DSL-Dienst erkannt wird. Leuchtet grün, wenn synchronisiert wird.
DSL-Daten (nur für SRP 526W/527W)	Blinkt, wenn DSL-Aktivitäten verzeichnet werden.
WLAN	Leuchtet, wenn der Funk gestartet wird und aktiv ist. Blinkt, wenn auf dem WLAN-Port Wireless-Aktivitäten verzeichnet werden.
USB-Port	Leuchtet, wenn das verbundene USB-Gerät aktiv ist. Blinkt, wenn bei einem Gerät ein Fehler verzeichnet oder es nicht unterstützt wird.
WPS-Taste	Leuchtet, wenn Wi-Fi Protected Setup (WPS) aktiv ist. Ein langsames grünes Blinken gibt an, dass die Funktion eingerichtet wird. Ein schnelles grünes Blinken weist auf einen Einrichtungsfehler hin.

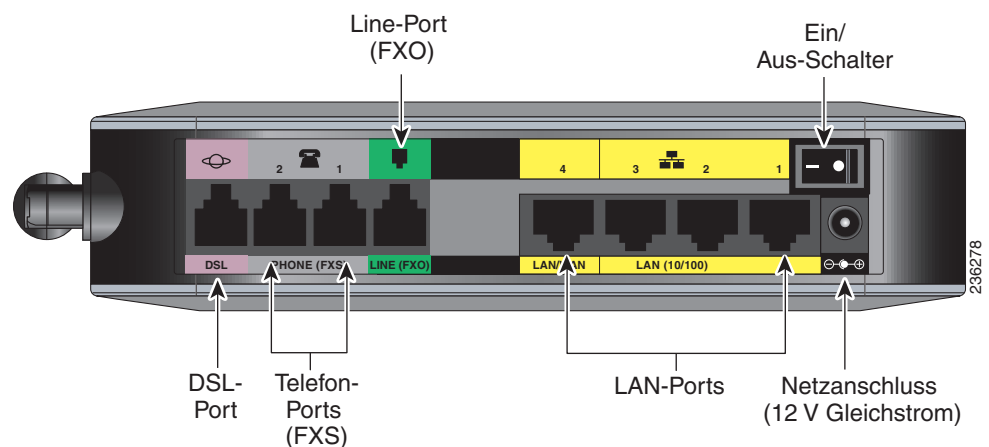
Rückseite

Auf der Rückseite werden die Netzwerkgeräte angeschlossen. Die jeweiligen Ports auf der Rückseite sind vom Modell abhängig.

Rückseite der SRP521W



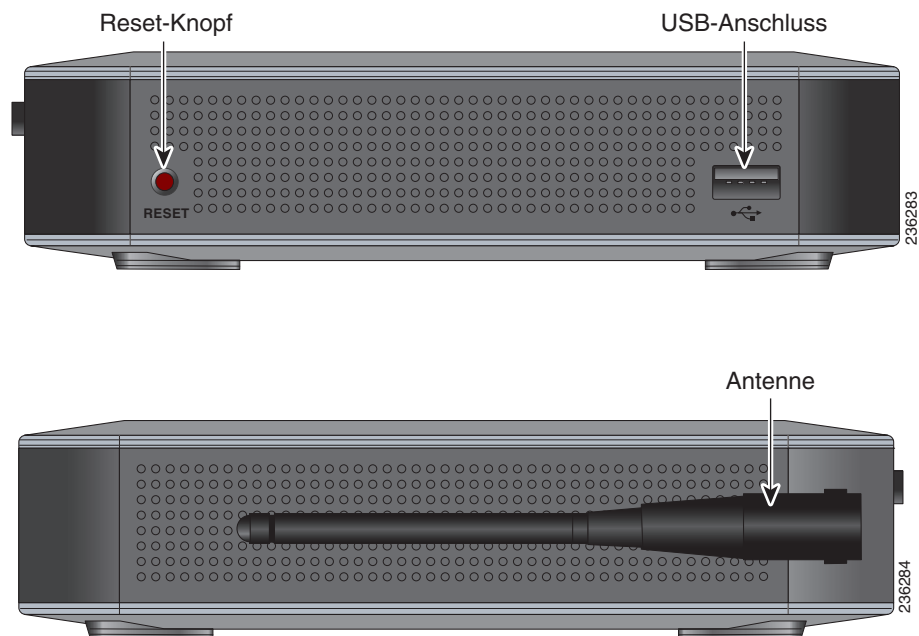
Rückseite der SRP526W/SRP527W



Beschreibung der Rückseite

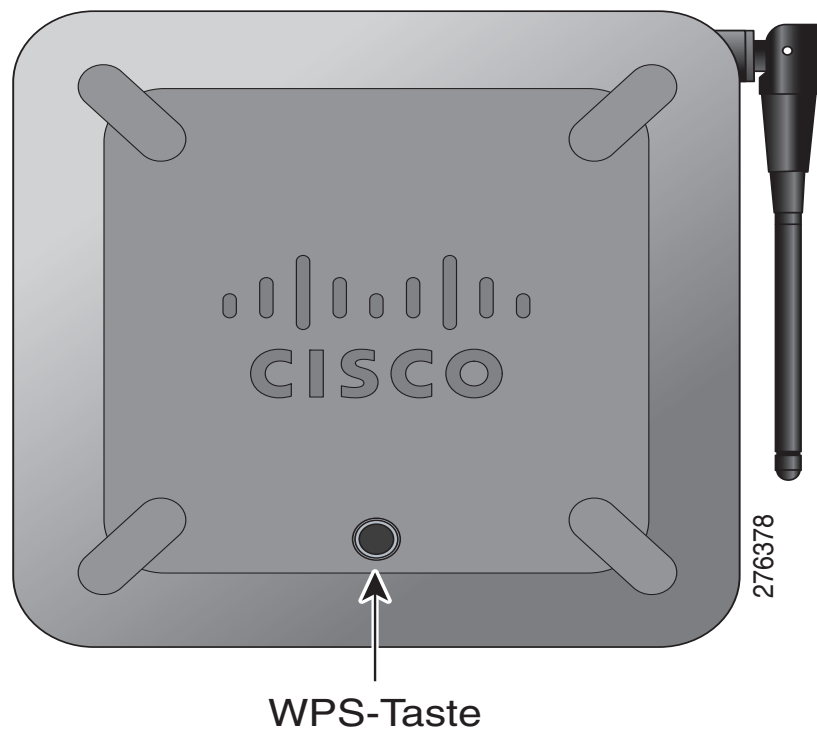
Funktion	Beschreibung
DSL-Port nur für SRP526/SRP527W	Verbindet die SRP mit der DSL-Leitung.
Telefon-Ports (FXS)(1 bis 2)	Stellt eine direkte Verbindung zu einem analogen Telefon, einem Faxgerät o. ä. her. Wenn für ein Analogtelefon eine separate Leitung erforderlich ist, müssen Sie ggf. einen Klingeladapter zwischen der SRP und dem Telefon anbringen, damit das Telefon bei eingehenden Anrufen klingelt.
Line-Port (FXO)	Stellt eine Verbindung zu einem öffentlichen Telefonnetz (dem analogen Telefondienst) her, das ein herkömmliches Telefon nutzt.
WAN-Port (10/100) nur SRP521W	Verbindet die SRP mit dem WAN (Wide Area Network).
LAN-Ports (10/100) (1 bis 4)	Stellt eine Verbindung zu einem per Kabel angeschlossenen Computer und anderen verkabelten Netzwerkgeräten her.
Ein/Aus-Schalter	Schaltet die SRP ein oder aus.
Netzanschluss (12 V Gleichstrom)	Stellt eine Verbindung zum mitgelieferten Netzteil her.

Seitenansicht



Funktion	Beschreibung
Reset-Taste	Halten Sie diese Taste 5 Sekunden lang gedrückt, um die SRP zurückzusetzen. Halten Sie diese Taste 10 Sekunden lang gedrückt, um die SRP auf die werkseitigen Einstellungen zurückzusetzen. Führen Sie zum Drücken dieser Taste eine Büroklammer oder einen ähnlichen Gegenstand in die Öffnung ein.
USB-Port	Stellt eine Verbindung zu einem kompatiblen USB-Modem her. Weitere Informationen zum Anschließen der SRP an einen USB-Anschluss finden Sie unter Mobile Network (Mobilnetz), Seite 36.
Antenne	Wi-Fi-Antenne

Draufsicht



Funktion	Beschreibung
WPS-Taste	Zur automatischen Konfiguration der Wireless-Sicherheit für Geräte, die Wi-Fi Protected Setup (WPS) unterstützen. Halten Sie für die Konfiguration von WPS diese Taste gedrückt, bis die WPS-LED blinkt. Stellen Sie sicher, dass sich das Gerät während der Einrichtung in der Nähe der SRP befindet.

Standardeinstellungen

Parameter	Wert
Geräte-IP	192.168.15.1
Benutzername	cisco
Passwort	cisco
Administrator-Benutzername	admin
Administrator-Passwort	admin
DHCP-Bereich	192.168.15.100 bis 149
Daten-VLAN	VLAN 1
Sprach-VLAN	VLAN 100, auf den Cisco VoIP-Telefonen über CDP veröffentlicht

Erste Schritte im Konfigurationsprogramm

In diesem Kapitel wird die Konfiguration und Verwendung des Konfigurationsprogramms für die Services Ready-Plattform erläutert. Dabei handelt es sich um ein webbasiertes Programm, mit dem Sie Ihre SRP (Services Ready-Plattform) verwalten und bereitstellen.

Dieses Kapitel enthält die folgenden Abschnitte:

- **Anmelden beim Konfigurationsprogramm**
- **Überblick über das Konfigurationsprogramm**

Anmelden beim Konfigurationsprogramm

In diesem Abschnitt wird erläutert, wie Sie sich beim Konfigurationsprogramm für die Services Ready-Plattform anmelden.

SCHRITT 1 Verbinden Sie einen Computer mit einem verfügbaren LAN-Port der SRP. Standardmäßig wird der Computer zum DHCP-Client der SRP und erhält eine IP-Adresse aus dem Bereich 192.168.15.x.

SCHRITT 2 Starten Sie einen Webbrowser.

Geben Sie in die Adressleiste **http://192.168.15.1** ein. Dies ist die Standardadresse der SRP.

SCHRITT 3 Wenn das Anmeldefenster geöffnet wird, geben Sie Benutzernamen und Passwort für die Anmeldung als Administrator ein.

Der Standardbenutzername lautet **admin**.
Das Standardpasswort lautet **admin**.

HINWEIS Bei Passwörtern muss die Groß- und Kleinschreibung beachtet werden.

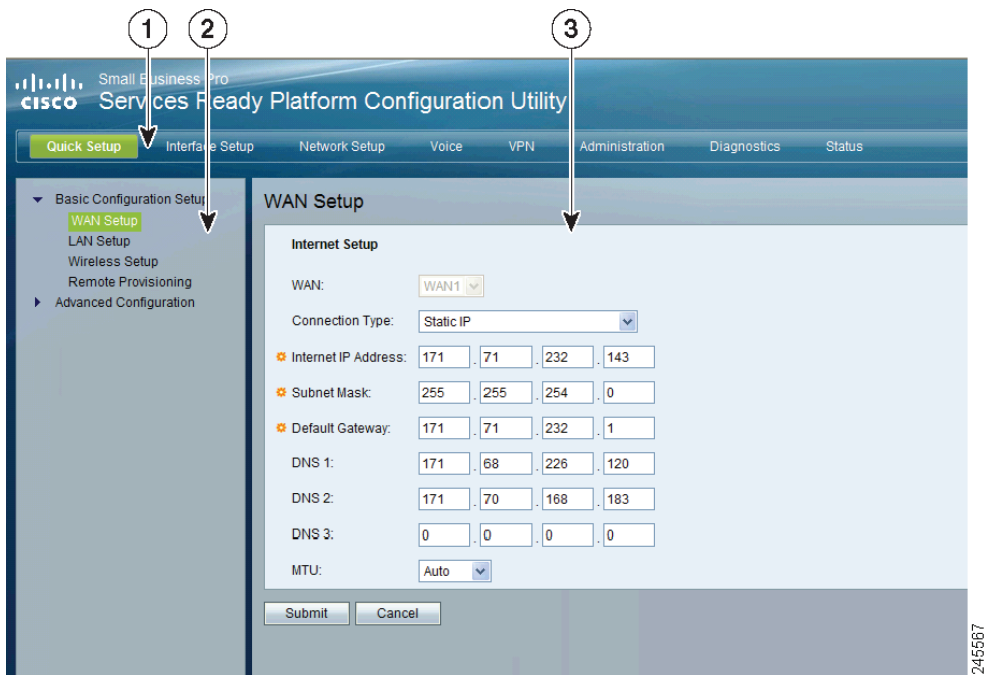
HINWEIS Wenn Sie sich als **cisco** (mit dem Passwort **cisco**) anmelden, wird automatisch der **Setup Wizard** (Installationsassistent) gestartet. Wenn Sie sich als **admin** anmelden, können Sie den Setup Wizard (Installationsassistenten) starten, indem Sie auf **Administration > Setup Wizard** (Verwaltung > Installationsassistent) klicken.

SCHRITT 4 Klicken Sie auf **Log In** (Anmelden). Das Konfigurationsprogramm der Services Ready-Plattform wird geöffnet.

Überblick über das Konfigurationsprogramm

Bereiche des Hauptfensters

In diesem Bereich werden die wichtigsten Menüleisten und Symbole erläutert, die im Konfigurationsprogramm verwendet werden.



Nummer	Komponente	Beschreibung
1	Menüleiste	Enthält die wichtigsten Funktionskategorien. Klicken Sie auf ein Menüelement, um zu einer anderen Kategorie zu wechseln.

Nummer	Komponente	Beschreibung
2	Navigationsbereich	Ermöglicht eine einfache Navigation durch die konfigurierbaren Gerätefunktionen. Die Hauptelemente lassen sich erweitern und zeigen dann Unterfunktionen an. Klicken Sie auf das Dreieck neben dem Titel der Hauptelemente, um ihre Elemente zu erweitern oder zu verkleinern. Klicken Sie auf den Titel einer Funktion oder Unterfunktion, um sie zu öffnen.
3	Hauptinhalt	In diesem Bereich wird der Hauptinhalt der jeweiligen Funktion angezeigt.

Symbole im Konfigurationsprogramm

Das Konfigurationsprogramm verfügt über Symbole und Schaltflächen für häufig verwendete Konfigurationsoptionen. In der folgenden Tabelle werden diese Symbole erläutert:

Symbol	Beschreibung
 Edit (Bearbeiten)	Mit dem Symbol zum Bearbeiten können Sie ein vorhandenes Element in einer Liste bearbeiten. Klicken Sie nach Durchführung Ihrer Änderungen auf Submit (Senden), um die Änderungen zu speichern.
 Add Item (Element hinzufügen)	Mit dem Symbol zum Hinzufügen von Elementen können Sie einer Liste ein Element hinzufügen. Klicken Sie nach Erstellen eines neuen Elements auf Submit (Senden), um das neue Element zu speichern.
 Delete Item (Element löschen)	Mit dem Symbol zum Löschen von Elementen können Sie ein Element aus einer Liste löschen. Klicken Sie nach Löschen eines Elements auf Submit (Senden), um die Änderungen zu speichern.
 Increment/Decrement (Erhöhen/Verringern)	Mit den Symbolen zum Erhöhen und Verringern können Sie numerische Werte ändern. Klicken Sie auf +, um einen Wert zu erhöhen, und auf -, um einen Wert zu verringern. Klicken Sie auf Submit (Senden), um Ihre Änderungen zu speichern.

Das Schnelleinrichtungsmenü

In diesem Kapitel wird erläutert, wie Sie über das Schnelleinrichtungsmenü die wichtigsten Verbindungseinstellungen für die Services Ready-Plattformen konfigurieren. Folgende Themen sind enthalten:

- **Basic Configuration Setup (Grundlegende Konfigurationseinrichtung)**
- **Advanced Configuration Setup (Erweiterte Konfigurationseinrichtung)**

Das Menü **Quick Setup** (Schnelleinrichtung) wird standardmäßig angezeigt, wenn Sie sich zum ersten Mal bei der SRP anmelden. Auf diesen Einrichtungseiten können Sie besonders schnell und einfach die Grundeinstellungen des Geräts festlegen. Außerdem finden Sie praktische Verknüpfungen zu den Funktionen des Konfigurationsprogramms.

Um auf diese Seiten zuzugreifen, klicken Sie in der Menüleiste des Konfigurationsprogramms auf **Quick Setup > Basic Configuration Setup** (Schnelleinrichtung > Grundlegende Konfigurationseinrichtung).

Basic Configuration Setup (Grundlegende Konfigurationseinrichtung)

In der grundlegenden Konfigurationseinrichtung können Sie für die SRP Einstellungen für WAN, LAN, Wireless und Remote-Bereitstellung definieren.

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Quick Setup > Basic Configuration Setup** (Schnelleinrichtung > Grundlegende Konfigurationseinrichtung).

WAN Setup (Ethernet) (WAN-Einrichtung (Ethernet))

Auf der Seite für die WAN-Einrichtung können Sie Ihre Ethernet-WAN-Schnittstelle konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Quick Setup > WAN Setup** (Schnelleinrichtung > WAN-Einrichtung). Das Fenster *WAN Setup* (WAN-Einrichtung) wird geöffnet.
- SCHRITT 2** Geben Sie den Internetverbindungstyp wie vom Internet Service Provider (ISP) vorgegeben ein.
- SCHRITT 3** Legen Sie die Einstellungen für den Verbindungstyp wie unter **Hinzufügen einer Subchnittstelle, Seite 29** beschrieben fest.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

WAN Setup (ADSL) (WAN-Einrichtung (ADSL))

Auf der Seite für die WAN-Einrichtung können Sie Ihre ADSL-WAN-Schnittstelle konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Quick Setup > WAN Setup** (Schnelleinrichtung > WAN-Einrichtung).
- SCHRITT 2** Das Fenster *WAN Setup* (WAN-Einrichtung) wird geöffnet.
- SCHRITT 3** Geben Sie die VC- und IP-Einstellungen wie unter **Internet Setup (Interneteinrichtung), Seite 26** beschrieben ein.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

LAN Setup (LAN-Einrichtung)

Auf der Seite für die LAN-Einrichtung können Sie die LAN-Schnittstelle konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Quick Setup > LAN Setup** (Schnelleinrichtung > LAN-Einrichtung). Das Fenster *LAN Setup* (LAN-Einrichtung) wird geöffnet.
- SCHRITT 2** Geben Sie die IP- und DHCP-Servereinstellungen des Routers für das LAN ein. Detaillierte Beschreibungen zu diesen Feldern finden Sie im Abschnitt zu DHCP unter **Einrichten der VLAN-Schnittstellen und LAN-Ports, Seite 42**.
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Wireless Setup (Wireless-Einrichtung)

Auf der Seite für die Wireless-Einrichtung können Sie das Wireless-Netzwerk konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Quick Setup > Wireless Setup** (Schnelleinrichtung > Wireless-Einrichtung). Das Fenster *Wireless Setup* (Wireless-Einrichtung) wird geöffnet.
- SCHRITT 2** Legen Sie die Einstellungen für das Wireless-Netzwerk wie unter **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)**, [Seite 50](#) beschrieben fest.
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Remote Provisioning (Remote-Bereitstellung)

Auf der Seite für TR-069 können Sie die Kommunikation mit einem Auto-Configuration Server (ACS) über das TR-069-CPE-WAN-Management-Protokoll (CWMP) konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Quick Setup > Remote Provisioning** (Schnelleinrichtung > Remote-Bereitstellung). Das Fenster *Remote Provisioning* (Remote-Bereitstellung) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Enabled** (Aktiviert), um die Remote-Bereitstellung zu aktivieren.
- SCHRITT 3** Legen Sie die Einstellungen für die Remote-Bereitstellung wie unter **Remote-Management**, [Seite 223](#) definiert fest.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Advanced Configuration Setup (Erweiterte Konfigurationseinrichtung)

Über die Funktionen in der erweiterten Konfigurationseinrichtung können Sie erweiterte Einstellungen für Sprache, Mobilnetzeinrichtung, Firewall und NAT festlegen.

Um auf diese Seite zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Quick Setup > Advanced Configuration Setup** (Schnelleinrichtung > Erweiterte Konfigurationseinrichtung).

Sprachkommunikation

Mit der Sprachoption können Sie die Sprachdienste und -einstellungen anzeigen und verwalten. Weitere Informationen finden Sie unter **Sprache konfigurieren, auf Seite 94**.

Mobile Network Setup (Mobilnetzeinrichtung)

Mit der Sprachoption können Sie die Sprachdienste und -einstellungen anzeigen und verwalten. Weitere Informationen finden Sie unter **Mobile Network (Mobilnetz), auf Seite 36**.

Firewall

Mit der Firewall-Option können Sie die Firewall-Filtereinstellungen verwalten. Weitere Informationen finden Sie unter **Firewall, auf Seite 80**.

NAT

Mit der NAT-Option können Sie die NAT-Einstellungen (Network Address Translation) verwalten. Weitere Informationen finden Sie unter **NAT, auf Seite 69**.

Einrichten der Schnittstellen auf der Services Ready-Plattform

In diesem Kapitel wird erläutert, wie Sie die Schnittstellen für die SRP einrichten. Folgende Themen sind enthalten:

- **Einrichten der WAN-Schnittstelle**
- **Einrichten der VLAN-Schnittstellen und LAN-Ports**
- **Einrichten des Wireless LAN**
- **Verwenden der Verwaltungsschnittstelle**

Um auf diese Seiten zuzugreifen, klicken Sie in der Menüleiste des Konfigurationsprogramms auf **Interface Setup** (Schnittstelleneinrichtung).

Einrichten der WAN-Schnittstelle

In diesem Abschnitt wird erläutert, wie Sie die WAN-Schnittstelleneinstellungen für die SRP einschließlich der folgenden Funktionen einrichten:

- **Internet Setup (Interneteinrichtung)**
- **Kapselungseinstellungen**
- **Mobile Network (Mobilnetz)**
- **Ausfallsicherung und Wiederherstellung**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Interface Setup > WAN** (Schnittstelleneinrichtung > WAN).

Internet Setup (Interneteinrichtung)

Auf der Seite für die Interneteinrichtung können Sie die Einstellungen für das WAN-Netzwerk konfigurieren.

HINWEIS Es wird empfohlen, dass Sie nach der Konfiguration der Schnittstelleneinstellungen ein neues Passwort für die SRP festlegen. Weitere Informationen dazu finden Sie unter **Benutzerliste, Seite 231**. Durch diese Vorsichtsmaßnahme können Sie die Sicherheit erhöhen und nicht autorisierte Zugriffe auf und Änderungen an der SRP vermeiden.

SCHRITT 1 Klicken Sie auf **Interface Setup > WAN > Internet Setup** (Schnittstelleneinrichtung > WAN > Interneteinrichtung). Das Fenster *Internet Setup* (Interneteinrichtung) wird geöffnet.

In der Liste für die WAN-Schnittstellen werden die Standardroute, der Schnittstellentyp, der Typ der Internetverbindung und die IP-Adresse für die einzelnen Schnittstellen angezeigt.

SCHRITT 2 Um die WAN-Schnittstelleneinstellungen zu konfigurieren, klicken Sie in der Schnittstellenspalte auf den Link zur WAN-Schnittstelle.

SCHRITT 3 Konfigurieren Sie die Parameter für die physischen Schnittstellen.

- Wählen Sie für eine DSL-Schnittstelle aus der Dropdown-Liste ein DSL-Protokoll aus. Wenn Sie wissen, welcher Modulationstyp am besten geeignet ist, oder wenn die SRP Probleme bei der Erkennung der richtigen Modulation hat, legen Sie einen Modulationstyp fest. Die DSL-Standardmodulation ist MultiMode (empfohlen).
- Wählen Sie für eine Ethernet-Schnittstelle die Einstellung für die Flusskontrolle (standardmäßig aktiviert), die Schnittstellengeschwindigkeit und die Duplexeinstellungen (standardmäßig **Auto-negotiate** (Automatische Aushandlung)) aus, oder überschreiben Sie die von der Schnittstelle verwendete MAC-Adresse. Um die MAC-Adresse des Computers zu verwenden, von dem aus Sie die SRP konfigurieren, klicken Sie auf **Clone Your PC's MAC** (MAC-Adresse des PCs klonen).

SCHRITT 4 Konfigurieren Sie die Schnittstellenadressierung.

- a. Klicken Sie in der Liste für die WAN-Schnittstellen neben der Schnittstelle, die Sie konfigurieren möchten, auf das Bleistiftsymbol für **Edit** (Bearbeiten).

Das Fenster für die Einstellungen der Interneteinrichtung wird geöffnet.

- b. Konfigurieren Sie die VC-Einstellungen wie in der Tabelle **VC-Einstellungen** unten definiert.

Abhängig vom ausgewählten Kapselungstyp wirken sich die verfügbaren Optionen auf die anderen, auf der Seite angezeigten Optionen aus. Weitere Informationen finden Sie unter **Kapselungseinstellungen, Seite 32**.

- c. Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern.

VC-Einstellungen	
Feld	Beschreibung
Multiplexing (Multiplexing)	Definiert die Vorgehensweise, mit der die verschiedenen Protokolle innerhalb eines DSL Virtual Circuit gehandhabt werden. Sie können zwischen der LLC-Kapselung (Logical Link Control), die auch LLC-SNAP genannt wird, und dem VC-Multiplexing (Virtual Channel), das auch VC-Mux genannt wird, auswählen.
QoS Type (QoS-Typ)	Wählen Sie die QoS-Methode (Quality of Service) für DSL aus, die Ihr ISP für Ihre Leitung verwendet: Unspecified Bit Rate (UBR, Nicht spezifizierte Bitrate), Constant Bit Rate (CBR, Konstante Bitrate), Real-Time Variable Bit Rate (RTVBR, Echtzeit-Variablen-Bitrate) oder Non-Real-Time Variable Bit Rate (NRTVBR, Nicht-Echtzeit-Variablen-Bitrate). CBR bietet die beste Garantie für geringe Latenz. UBR bietet gar keine Garantie für geringe Latenz, wird jedoch für die meisten Breitbanddatendienste verwendet. ▪ Pcr Rate (PCR-Rate) – Wenn QoS auf CBR, VBR_RT oder VBR_NRT gesetzt ist, geben Sie die Peak Cell Rate (PCR, Höchste Zellenrate) in Zellen pro Sekunde an. ▪ Scr Rate (SCR-Rate) – Wenn QoS auf VBR_NRT oder VBR_RT gesetzt ist, geben Sie die Sustained Cell Rate (SCR, Dauerhafte Zellenrate) in Zellen pro Sekunde an. ▪ MBS (MBS) – Wenn QoS auf VBR_NRT oder VBR_RT gesetzt ist, geben Sie die MBS in Zellen pro Sekunde an. ▪ CDTV (CDTV) – Wenn QoS auf CBR, VBR_NRT oder VBR_RT gesetzt ist, geben Sie die CDTV in Zellen pro Sekunde an.
VPI/VCI Auto Detect (Automatische VPI/VCI-Erkennung)	Verwenden Sie diese Option, um die automatische Erkennung der VPI- und VCI-Werte, die Ihre Leitung zum ATM-Netzwerk identifiziert, zu aktivieren oder zu deaktivieren. Virtual Path Identifier (VPI, Virtuelle Pfaderkennung) und Virtual Channel Identifier (VCI, Virtuelle Kanalerkennung) sind Werte, mit denen Ihre Leistung im ATM-Netzwerk Ihres ISP identifiziert wird. Die SRP erkennt automatisch die auf den folgenden VC-Paaren verfügbaren DSL-Dienste: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, 8/59, 0/38.

SCHRITT 5 Um eine Ethernet-Subschnittstelle zu konfigurieren, klicken Sie neben der WAN-Schnittstelle auf das Bleistiftsymbol für **Edit** (Bearbeiten). Geben Sie die Einstellungen wie unter **Hinzufügen einer Subschnittstelle, Seite 29** beschrieben ein.

SCHRITT 6 Wählen Sie die Standardroute für die Schnittstelle aus, die Sie konfigurieren. Die Standardroute für Sprachdaten ist **Default Voice Route** (Standardsprachroute).

HINWEIS Wenn Sie die Ausfallsicherungsfunktion für die Schnittstelle verwenden, wählt die Schnittstellenstandardroute automatisch die Subschnittstelle aus, über die der Verkehr weitergegeben wird, der von einer fehlgeschlagenen Schnittstelle umgeleitet wurde.

SCHRITT 7 Wählen Sie, um die Schnittstelleninformationen anzuzeigen, aus der Liste der WAN-Schnittstellen eine WAN-Schnittstelle aus. Im Bereich der WAN-Schnittstellendetails werden Informationen zur Schnittstelle angezeigt, wie in der Tabelle unten beschrieben.

Detaileinstellungen für die WAN-Schnittstelle	
Name	Wert
Link Status (Linkstatus)	Schnittstellenstatus: verbunden oder nicht verbunden
IP-Adresse	Öffentliche IP-Adresse der Schnittstelle
Netmask (Netzmaske)	Subnetzmaske
Gateway	IP-Adresse des ISP-Servers
Hostname	Hostname (falls zutreffend)
Domain Name (Domänenname)	Domänenname (falls zutreffend)
MTU Type (MTU-Typ)	Auto (Automatisch) oder Custom (Benutzerdefiniert)
MTU Size (MTU-Größe)	Aktuelle MTU-Größe: Dieser Wert ist leer, falls Auto (Automatisch) eingestellt ist.
DNS 1,2,3 (DNS 1, 2, 3)	IP-Adressen der DNS-Server (falls konfiguriert)
VLAN Encapsulation (VLAN-Kapselung)	Wenn diese Option aktiviert ist, wird dem ausgehenden Verkehr ein IEEE-802.1q-VLAN-Header hinzugefügt, sodass einige Service Provider die Servicequalität auf Grundlage zugehöriger IEEE-802.1p-Prioritätswerte steuern können.
VLAN-ID	Verwendete VLAN-ID, falls die VLAN-Kapselung aktiviert ist

Hinzufügen einer Subschnittstelle

Im Fenster für die Interneteinrichtung können Sie auf der Seite mit der Liste für die WAN-Schnittstellen der SRP eine Subschnittstelle hinzufügen. Diese Optionen entsprechen denen für die Konfiguration einer WAN-Hauptschnittstelle, mit der Ausnahme, dass Sie für PPTP oder L2TP keine Ethernet-Subschnittstelle konfigurieren können.

Die SRP unterstützt für jeden physischen Port mehrere logische Schnittstellen. Für Ethernet-Ports werden VLAN-Schnittstellen als Teil eines IEEE-802.1p-Trunks erstellt. Auf ADSL-Schnittstellen können mehrere PVCs erstellt werden.

Die SRP unterstützt bis zu fünf VLANs, die als Local Area VLANs oder WAN-Subschnittstellen verwendet werden können. Auf einer ADSL-Schnittstelle können bis zu vier PVCs konfiguriert werden.

SCHRITT 1 Um eine neue logische Internetverbindung hinzuzufügen, wählen Sie auf der Seite für die Interneteinrichtung das WAN der obersten Ebene aus, und klicken Sie auf das Seitensymbol für **Add** (Hinzufügen). Das Fenster *Internet Setup* (Interneteinrichtung) für die neue Internetverbindung wird geöffnet.

SCHRITT 2 Wählen Sie den für Ihren ISP erforderlichen Verbindungstyp wie in der Tabelle **Ethernet-Einstellungen für die WAN-Schnittstelle** definiert aus.

SCHRITT 3 Wählen Sie aus der Dropdown-Liste eine MTU-Option aus. Wenn von Ihrem ISP aus keine Änderung erforderlich ist, wird empfohlen, die MTU-Methode auf **Auto** (Automatisch) zu setzen, sodass das Sprachsystem die Größe automatisch auswählen kann. Die Standardgröße beträgt 1500 Byte.

Um eine andere MTU-Größe festzulegen, wählen Sie in der Dropdown-Liste die Option **Custom** (Benutzerdefiniert) aus, und geben Sie die Größe in Byte ein. Die Standardgröße für Ethernet-Netzwerke beträgt 1500 Byte. Für PPPoE-Verbindungen beträgt die Standardgröße 1492 Byte.

SCHRITT 4 Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern.

Die neue Verbindung wird auf der Seite für die Interneteinrichtung der Liste der WAN-Schnittstellen hinzugefügt.

Ethernet-Einstellungen für die WAN-Schnittstelle	
Feld	Beschreibung
WAN	WAN1 ist die Schnittstellenidentität für den WAN-Port der SRP. Dieser Wert kann nicht geändert werden.
VLAN-ID	Die VLAN-Identität für die Schnittstelle oder Subschnittstelle. Dieser Wert kann nicht mehr geändert werden, sobald die Schnittstelle erstellt wurde.
Connection Type (Verbindungstyp)	Typ der vom ISP bereitgestellten Internetverbindung
	Automatic Configuration/DHCP (Automatische Konfiguration/DHCP) Ein häufig für Kabelmodems verwendeter Verbindungstyp. Wählen Sie diese Option aus, wenn Ihr ISP beim Herstellen einer Verbindung automatisch eine IP-Adresse zuweist. Für diesen Verbindungstyp sind keine weiteren Informationen erforderlich.
	Static IP (Statische IP) Wählen Sie diese Option aus, wenn Ihr ISP Ihnen eine statische (dauerhafte) IP-Adresse zuweist und keine dynamische Zuweisung nutzt. Geben Sie die zugewiesene IP-Adresse, Subnetzmaske und IP-Adresse des Standard-Gateways ein.

Ethernet-Einstellungen für die WAN-Schnittstelle	
Feld	Beschreibung
	PPPoE Wählen Sie diese Option aus, wenn Ihr ISP PPPoE (Point-to-Point Protocol over Ethernet) verwendet. Geben Sie Benutzernamen und Passwort für Ihr ISP-Konto und ggf. den Servicenamen ein. Wählen Sie die Option Connect on Demand (Auf Aufforderung verbinden) oder Keep Alive (Erhalten) aus. Connect on Demand (Auf Aufforderung verbinden) Öffnet nur dann eine Verbindung, wenn ein Benutzer versucht, eine Internetverbindung herzustellen. Die Verbindung endet automatisch, wenn sie länger inaktiv ist als über Max Idle Time (Max. Leerlaufzeit) in Minuten festgelegt. Diese Option wird empfohlen, wenn Ihre Abrechnung nach Dauer der Verbindung erfolgt. BEMERKUNG Computer senden häufig Informationen über das Internet, selbst wenn gerade kein E-Mail- oder Browserprogramm genutzt wird. Dadurch bleibt eine Sitzung möglicherweise länger als erwartet aktiv. Keep Alive (Erhalten) Erhält die Verbindung zum Internet unbegrenzt, auch wenn keine Daten gesendet oder empfangen werden.
	PPTP Wählen Sie diese Option aus, wenn Ihr ISP PPTP (Point-to-Point-Tunneling Protocol) verwendet. Geben Sie die IP-Adresse des PPTP-Servers sowie Benutzernamen und Passwort für Ihr Konto ein. Wenn Ihr Service Provider keine dynamischen IP-Adressen zuweist, deaktivieren Sie DHCP, und geben Sie die für Ihr Konto bereitgestellten Daten für Adresse, Maske und Gateway ein. Wählen Sie die Option Connect on Demand (Auf Aufforderung verbinden) oder Keep Alive (Erhalten) aus.

Ethernet-Einstellungen für die WAN-Schnittstelle	
Feld	Beschreibung
	L2TP Wählen Sie diese Option aus, wenn Ihr ISP L2TP (Layer 2 Tunneling Protocol) verwendet und Ihnen eine statische IP-Adresse zugewiesen hat. Geben Sie die IP-Adresse des L2TP-Servers sowie Benutzername und Passwort für Ihr Konto ein. Wenn Ihr Service Provider keine dynamischen IP-Adressen zuweist, deaktivieren Sie DHCP, und geben Sie die für Ihr Konto bereitgestellten Daten für Adresse, Maske und Gateway ein. Wählen Sie die Option Connect on Demand (Auf Aufforderung verbinden) oder Keep Alive (Erhalten) aus.
Maximum Transmission Unit (MTU) (Maximale Übertragungseinheit (MTU))	Die Größe des größten Pakets (in Byte), das über das Netzwerk gesendet werden darf. Dieser Wert beträgt üblicherweise 1500 Byte, muss jedoch für einige Breitbanddienste evtl. niedriger sein. Fragen Sie Ihren Service Provider nach den jeweiligen Anforderungen.
Static DNS 1-3 (Statische DNS 1 bis 3)	(Optional) Geben Sie die IP-Adressen von bis zu drei DNS-Servern (Domain Name System) ein, oder lassen Sie die Felder leer, sodass dynamisch ein DNS-Server zugewiesen wird.

Kapselungseinstellungen

In diesem Abschnitt werden die ADSL-Kapselungseinstellungen erläutert, die Sie auf der Seite für die Interneteinrichtung in den VC-Einstellungen auswählen können.

Die Kapselung ist das Protokoll, das zwischen Ihrem Breitband-Gateway und den Servern des ISP eingesetzt wird. Die meisten Kapselungen sind in Internetstandards definiert, die Requests for Comments (RFC) genannt werden. Zwei wurden vom Point-to-Point Protocol (PPP) abgeleitet: PPP over Ethernet (PPPoE) und PPP over ATM (PPPoA).

IPoA-Einstellungen

Wählen Sie IPoA für die direkte Kapselung von IP-Verkehr über den DSL ATM Virtual Circuit aus. Geben Sie die von Ihrem ISP bereitgestellten Informationen ein: IP-Adresse, Subnetzmaske und IP-Adresse für das Standard-Gateway. Sie können ggf. auch die IP-Adressen des primären und sekundären DNS-Servers eingeben.

IPoA-Einstellungen	
Feld	Beschreibung
Internet IP Address and Subnet Mask (Internet-IP-Adresse und Subnetzmaske)	Die IP-Adresse und Subnetzmaske der SRP, wie für externe Benutzer im Internet (einschließlich des ISP) sichtbar. Diese Informationen erhalten Sie von Ihrem ISP.
Standard-Gateway	Ihr ISP stellt die IP-Adresse des Gateways bereit.
Primary/Secondary DNS (Primärer/ sekundärer DNS)	Zur Definition eines oder mehrerer DNS-Server. Die SRP verwendet diese, um Domännennamen für logisch konfigurierte Funktionen aufzulösen und kann sie auch über DHCP an lokale Clients weitergeben.

PPPoE-Einstellungen

Wählen Sie PPPoE aus, um über Ethernet gekapseltes PPP über den DSL ATM Virtual Circuit auszuführen. Geben Sie den Benutzernamen und das Passwort ein, das Sie von Ihrem ISP erhalten haben. Sie können ggf. auch einen PPP-Dienstnamen angeben, wenn Ihr Service Provider diesen bereitstellt.

PPPoE-Einstellungen	
Feld	Beschreibung
Username and Password (Benutzername und Passwort)	Die Zeichenfolgen, die Sie von Ihrem ISP erhalten haben. Der Benutzername kann auch „Username“, „Anmeldename“ oder „Anmeldung“ heißen.
Servicename	Eine für einige ISPs erforderliche Zeichenfolge. Geben Sie diese nur ein, wenn Ihr ISP dies verlangt.
Connect on Demand (Auf Aufforderung verbinden)	Verbindet das Breitband-Gateway mit Ihrem ISP, wenn eine Verbindung erforderlich ist, und trennt die Verbindung wieder, wenn die Leitung eine bestimmte Zeit lang inaktiv ist. Sie können die maximale Inaktivitätsdauer anpassen. Die Standardeinstellung ist 20 Minuten. Die Alternative zu dieser Einstellung ist Keep Alive (Erhalten). In den meisten Fällen können Sie sich für eine Option entscheiden, ohne Ihren ISP fragen zu müssen.

PPPoE-Einstellungen	
Feld	Beschreibung
Keep Alive (Erhalten)	Erhält die Verbindung zum ISP ununterbrochen aufrecht. Wenn die Verbindung für eine bestimmte Anzahl an Sekunden abgebaut wird (der sogenannte „Wahlwiederholungszeitraum“), versucht das Gateway automatisch, sie erneut herzustellen. Der Standardzeitraum für die Wahlwiederholung ist 20 Sekunden.
Enable MTU/MRU greater than 1492 (MTU/MRU über 1492 aktivieren)	Zusätzliche Headerinformationen in PPPoE-Verbindungen über ADSL, mit denen die maximale Paketgröße für einen Sendevorgang auf 1492 Byte festgelegt wird. Aktivieren Sie diese Einstellung nur, wenn Sie vom ISP dazu aufgefordert werden.

PPPoA-Einstellungen

Wählen Sie PPPoA aus, um PPP direkt über den DSL ATM Virtual Circuit auszuführen. Geben Sie den Benutzernamen und das Passwort ein, das Sie von Ihrem ISP erhalten haben.

PPPoA-Einstellungen	
Feld	Beschreibung
Username and Password (Benutzername und Passwort)	Die Zeichenfolgen, die Sie von Ihrem ISP erhalten haben. Der Benutzername kann auch „Username“, „Anmeldename“ oder „Anmeldung“ heißen.
Connect on Demand (Auf Aufforderung verbinden)	Verbindet das Breitband-Gateway mit Ihrem ISP, wenn eine Verbindung erforderlich ist, und trennt die Verbindung wieder, wenn die Leitung eine bestimmte Zeit lang inaktiv ist. Verbindung und Verbindungstrennung geschehen automatisch. Sie können die maximale Inaktivitätsdauer anpassen. Die Standardeinstellung ist 20 Minuten. Die Alternative zu dieser Einstellung ist Keep Alive (Erhalten). In den meisten Fällen können Sie sich für eine Option entscheiden, ohne Ihren ISP fragen zu müssen.
Keep Alive (Erhalten)	Erhält die Verbindung zum ISP ununterbrochen aufrecht. Wenn die Verbindung für eine bestimmte Anzahl an Sekunden abgebaut wird (der sogenannte „Wahlwiederholungszeitraum“), versucht das Gateway automatisch, sie erneut herzustellen. Der Standardzeitraum für die Wahlwiederholung ist 20 Sekunden.

Internetoptionen

Auf der Seite für die Internetoptionen können Sie die für die Internetverbindung konfigurierten Daten ergänzen.

SCHRITT 1 Klicken Sie auf **Interface Setup > WAN > Internet Option** (Schnittstelleneinrichtung > WAN > Internetoption). Das Fenster *Internet Option* (Internetoption) wird geöffnet.

SCHRITT 2 Geben Sie den Hostnamen und Domännennamen (falls vom ISP bereitgestellt) ein.

SCHRITT 3 Geben Sie die IP-Adressen für bis zu drei DNS-Server ein.

HINWEIS Für die SRP können DNS-Serverinformationen in verschiedenen Kontexten festgelegt werden, damit so Ihre persönlichen Anforderungen erfüllt werden.

Für jede WAN-Schnittstelle kann die statische oder dynamische Konfiguration der primären, sekundären und tertiären verbindungsspezifischen Server festgelegt werden. Sie können in den Internetoptionen die primären, sekundären und tertiären Server auch statisch konfigurieren.

Um zu bestimmen, welche Server für die interne Namensauflösung verwendet werden, nimmt die SRP die ersten drei Adressen aus einer Liste, die sie in der folgenden Reihenfolge erstellt:

- Primäre Server aus den Internetoptionen WAN1, WAN2 und dann 3G
- Sekundäre Server aus den Internetoptionen WAN1, WAN2 und dann 3G
- Tertiäre Server aus den Internetoptionen WAN1, WAN2 und dann 3G

SCHRITT 4 Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern.

Internetoptionen	
Feld	Beschreibung
Hostname	Von Ihrem ISP bereitgestellter Hostname
Domain Name (Domänenname)	Von Ihrem ISP bereitgestellter Domänenname
Static DNS 1–3 (Statische DNS 1 bis 3)	Geben Sie die IP-Adressen für bis zu drei DNS-Server ein.

Mobile Network (Mobilnetz)

Auf der Seite für das Mobilnetz können Sie konfigurieren, dass die SRP eine Verbindung zu einem mobilen USB-Breitbandmodem herstellt, das über die USB-Schnittstelle angeschlossen ist. Weitere Informationen zu kompatiblen Modems finden Sie unter www.cisco.com/go/srp500.

-
- SCHRITT 1** Klicken Sie auf **Interface Setup > Mobile Network** (Schnittstelleneinrichtung > Mobilnetz). Das Fenster *Mobile Network* (Mobilnetz) wird geöffnet.
- SCHRITT 2** Stellen Sie eine Verbindung zum USB-Modem her. Wenn die Karte von der SRP unterstützt wird, wird sie automatisch erkannt und auf der Seite für das Mobilnetz angezeigt.
- SCHRITT 3** Wählen Sie den Verbindungsmodus **Auto** (Automatisch) oder **Manual** (Manuell) aus. Der Standardmodus ist **Auto** (Automatisch).
- Wenn das Modem automatisch eine Verbindung herstellen soll, wählen Sie **Auto** (Automatisch) aus.
 - Um die Modemverbindung manuell herzustellen und zu trennen, wählen Sie **Manual** (Manuell) aus.
- HINWEIS** Die Ethernet-Verbindungswiederherstellung funktioniert nur im Verbindungsmodus **Auto** (Automatisch). Wenn Sie **Auto** (Automatisch) auswählen, müssen Sie auch **Connect on Demand** (Auf Aufforderung verbinden) oder **Keep Alive** (Erhalten) aktivieren.
- SCHRITT 4** Stellen Sie sicher, dass im Feld für den Kartenstatus der Status der Mobilkarte angezeigt wird.
- SCHRITT 5** Wählen Sie, falls erforderlich, für die Konfiguration der Schnittstelle ein Tunneling-Protokoll aus.
- SCHRITT 6** Ändern Sie, falls erforderlich, im Bereich **Mobile Network Setup** (Mobilnetzeinrichtung) die Einstellungen des Mobilnetzes.
- HINWEIS** Um die Mobilnetzkarte manuell einrichten zu können, müssen Sie im Feld für den Konfigurationsmodus auf die Option **Manual** (Manuell) klicken.
- SCHRITT 7** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Feld	Beschreibung
Connect Mode (Verbindungsmodus)	Wählen Sie den Modus Auto (Automatisch) oder Manual (Manuell) aus. Wenn Sie den manuellen Modus auswählen, müssen Sie auf das Konfigurationsprogramm zugreifen, um über die Mobilverbindung eine Internetverbindung herzustellen. Klicken Sie auf Connect (Verbinden), um bei Bedarf eine Verbindung herzustellen. Klicken Sie auf Disconnect (Verbindung trennen), um die Verbindung zu trennen. BEMERKUNG Die Ethernet-Verbindungswiederherstellung und die Ausfallsicherung für die Schnittstellenverbindung funktionieren nur, wenn der Verbindungsmodus auf Auto (Automatisch) festgelegt ist. Wenn Sie Auto (Automatisch) auswählen, müssen Sie auch Connect on Demand (Auf Aufforderung verbinden) oder Keep Alive (Erhalten) aktivieren.
Connect on Demand (Auf Aufforderung verbinden)	Wählen Sie diese Option aus, wenn die SRP die Internetverbindung beenden soll, nachdem sie eine bestimmte Zeit lang inaktiv war (maximale Leerlaufzeit). Wenn die Internetverbindung aufgrund von Inaktivität getrennt wird, gibt diese Option dem Modem die Möglichkeit, automatisch erneut eine Verbindung herzustellen, wenn ein Benutzer wieder versucht, auf das Internet zuzugreifen. Geben Sie im Feld Max Idle Time (Max. Leerlaufzeit) die Anzahl der Minuten ein, die vergehen können, bis die Internetverbindung getrennt wird. Der Standardzeitraum für diese Einstellung ist 5 Minuten.
Tunneling-Protokoll	Das Tunneling-Protokoll (PPTP/L2TP) wird über ein USB-Modem und mit den folgenden Methoden unterstützt. ▪ NONE (KEINE): Wählen Sie diese Option aus, um das Tunneling-Protokoll zu deaktivieren. ▪ PPTP/L2TP: Wählen Sie, je nach dem Dienst, den Sie verwenden möchten, PPTP oder L2TP aus. Sie müssen auch die IP-Adresse des Servers, den Benutzernamen und das Passwort angeben. ▪ Follow Ethernet WAN configure (Gemäß Ethernet-WAN-Konfiguration): Wählen Sie diese Option aus, damit sich das Tunneling-Protokoll an die Konfiguration des Ethernet-WAN hält.

Feld	Beschreibung
Card Status (Kartenstatus)	Zeigt den aktuellen Status der Modemverbindung an, also ob es initialisiert, verbunden oder getrennt wird bzw. ist. Ggf. werden die folgenden Meldungen angezeigt: ▪ Please set APN manually (APN manuell festlegen) Wird angezeigt, wenn die SRP den APN des Betreibers im automatischen Modus nicht bestimmen kann ▪ Searching for service... (Nach Dienst suchen ...) ▪ no SIM card (Keine SIM-Karte) ▪ SIM locked (SIM gesperrt) ▪ SIM busy (SIM beschäftigt) ▪ SIM ready (SIM bereit) ▪ pin code needed (PIN erforderlich) ▪ pin code error (PIN-Fehler) ▪ Card is locked (Karte gesperrt) ▪ Card is not activated (Karte nicht aktiviert) ▪ Card initialized error (Karte verursacht Fehler) ▪ error (Fehler) BEMERKUNG Wenn der Verbindungsmodus auf Manual (Manuell) gesetzt ist, können Sie auf eine Schaltfläche klicken, um das Modem zu verbinden bzw. dessen Verbindung zu trennen.
Configure Mode (Konfigurationsmodus)	Die SRP erkennt automatisch unterstützte Modems und zeigt eine Liste entsprechender Standardkonfigurationen an. Wenn Sie eine dieser Einstellungen überschreiben müssen (mit Ausnahme der SIM-PIN), wählen Sie den manuellen Konfigurationsmodus aus.
Card Model (Kartenmodell)	Das Modell der Datenkarte, die über USB angeschlossen ist. Nicht unterstützte Karten werden als nicht erkannt angezeigt.
Access Point Name (APN) (Name des Access Point (APN))	Das Internetnetzwerk, mit dem sich das Mobilgerät verbindet. Geben Sie den Namen des Access Point ein, den Sie von Ihrem Mobilfunkanbieter erhalten haben.

Feld	Beschreibung
Dial Number (Wählnummer)	Die Wählnummer für die Internetverbindung. Geben Sie die Wählnummer ein, die Sie von Ihrem Mobilfunkanbieter erhalten haben.
Username/ Password (Benutzername/ Passwort)	Benutzername und Passwort, die Sie von Ihrem Mobilfunkanbieter erhalten haben
SIM PIN (SIM-PIN)	Der PIN-Code für die SIM-Karte. Geben Sie hier Ihre SIM-PIN ein. Dieses Feld wird nur für GSM-Karten angezeigt.
Servername	Name des Servers für die Internetverbindung (falls von ISP bereitgestellt)
Authentifizierung	Der Authentifizierungstyp Ihres Service Providers. Wählen Sie ihn aus der Dropdown-Liste aus. Die Standardeinstellung ist Auto. Wenn Sie den erforderlichen Authentifizierungstyp nicht kennen, belassen Sie die Standardeinstellung.
Service Type (Servicetyp)	Wählen Sie basierend auf dem Dienstsinal Ihrer Region den am häufigsten verfügbaren Verbindungstyp für Mobildatendienste aus. Wenn an Ihrem Standort nur ein Mobildatendienst unterstützt wird, können Sie Ihre bevorzugte Option begrenzen, sodass sich die Zeiten für die Verbindungseinrichtung verringern. Die erste Auswahl sucht immer nach einem HSPDA/3G/UMTS-Dienst oder wechselt automatisch zu GPRS, falls dieses Netz verfügbar ist.

Ausfallsicherung und Wiederherstellung

Eine Internetverbindung kann über den WAN-Port oder ein Wireless-Modem, das am USB-Port angeschlossen ist, hergestellt werden. Weitere Details zu kompatiblen USB-Modemgeräten finden Sie unter www.cisco.com/go/srp500.

Es können zwar gleichzeitig ein Ethernet- und ein USB-Modem angeschlossen werden, doch eine Verbindung kann immer nur über eines der beiden Geräte hergestellt werden. Wenn die Internetverbindung fehlschlägt, versucht die SRP automatisch, eine andere Verbindung über eine andere Schnittstelle herzustellen. Diese Funktion wird *Ausfallsicherung* genannt. Wenn die ursprüngliche Internetverbindung wiederhergestellt wird, wird der ursprüngliche Pfad erneut verwendet und die Sicherungsverbindung fallen gelassen. Diese Funktion wird *Wiederherstellung* genannt.

SCHRITT 1 Klicken Sie auf **Interface Setup** > **Failover & Recovery** (Schnittstelleneinrichtung > Ausfallsicherung und Wiederherstellung). Das Fenster *Failover & Recovery* (Ausfallsicherung und Wiederherstellung) wird geöffnet.

SCHRITT 2 Klicken Sie auf **Enabled** (Aktiviert), um die Verbindungswiederherstellung zu aktivieren.

Wenn diese Funktion aktiviert ist, setzt die SRP die Ethernet-Schnittstelle auf die höchste Priorität und aktiviert außerdem die Ausfallsicherung für die Schnittstellenverbindung. Wenn die Internetverbindung fehlschlägt, versucht die SRP automatisch, die Mobilnetzverbindung über die USB-Schnittstelle zu starten (falls verfügbar). Ist die Internetverbindung dann wiederhergestellt, kehrt die SRP automatisch zu dieser ursprünglichen Verbindung zurück und beendet die Verbindung über die Sicherungsschnittstelle.

HINWEIS Der Mobilverbindungsmodus muss auf **Auto** (Automatisch) gesetzt sein, damit die Ethernet-Verbindungswiederherstellung genutzt werden kann.

SCHRITT 3 Geben Sie einen Zeitüberschreitungswert für die Ausfallsicherung ein.

SCHRITT 4 Wählen Sie im Bereich für die Site der Ausfallsicherungsprüfung eine Site aus, auf der die Ausfallsicherungsprüfung vorgenommen werden soll. Verwenden Sie entweder das nächste Hop-Gateway, oder geben Sie die IP-Adresse für eine benutzerdefinierte Site ein.

SCHRITT 5 Ändern Sie die Priorität der WAN-Schnittstellen, indem Sie auf **Up** (Nach oben) oder **Down** (Nach unten) klicken.

SCHRITT 6 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für Ausfallsicherung und Wiederherstellung

Feld	Beschreibung
Connection Recovery (Verbindungs- wiederherstellung)	Aktivieren Sie diese Option, um sicherzustellen, dass Ihre primäre Internetverbindung gesichert ist.
Interface Connection Failover (Ausfallsicherung für die Schnittstellen- verbindung)	Die Ausfallsicherungserkennung funktioniert über das Ermitteln der physischen Verbindung und/oder des Vorhandenseins von Datenverkehr auf der Internetverbindung. Wenn die Verbindung inaktiv ist, versucht die SRP, ein Ziel anzupingen. Wenn auf das Ping-Signal keine Antwort folgt, nimmt die SRP an, dass die Verbindung unterbrochen ist, und versucht, eine Verbindung über eine andere Schnittstelle herzustellen.
Timeout (Zeitüberschreitung)	Das Zeitintervall, nach dem die SRP den Status der Internetverbindung ermittelt. Der Standardwert ist 60 Sekunden.
Connection Validation Site (Verbindungs- prüfungssite)	Ping-Ziel für die SRP, um den Status der Internetverbindung zu ermitteln. Standardmäßig pingt die SRP die NTP-Server (Network Time Protocol) an. Hier können Sie eine andere IP-Adresse als Ziel angeben.
WAN Interfaces (WAN- Schnittstellen)	Stellt Informationen zum aktuellen Status der Ethernet-Internetverbindung und der Mobilnetzverbindung bereit. Klicken Sie auf den Hyperlink für den Status, um die Details anzuzeigen. Sie können auch die Priorität der Schnittstelle konfigurieren, indem Sie auf die Pfeile nach unten oder oben klicken. Beachten Sie, dass die Prioritätseinstellung für die Schnittstelle nur konfigurierbar ist, wenn die Ethernet-Verbindungswiederherstellung deaktiviert ist.

Einrichten der VLAN-Schnittstellen und LAN-Ports

In diesem Abschnitt wird erläutert, wie Sie die VLAN- und LAN-Ports der SRP einrichten. Folgende Themen sind enthalten:

- **DHCP-Server**
- **VLAN-Einstellungen**
- **Porteinstellungen**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Interface Setup > LAN** (Schnittstelleneinrichtung > LAN).

DHCP-Server

Um die SRP als DHCP-Server zu konfigurieren, müssen Sie zuerst auf der entsprechenden Seite einen DHCP-Server erstellen. Aktivieren Sie ihn anschließend, indem Sie ihn einer VLAN-Schnittstelle zuweisen.

HINWEIS Beim Erstellen eines DHCP-Servers müssen Sie außerdem die IP-Adresse und Maske für die VLAN-Schnittstelle angeben, der er zugewiesen ist. Wenn Sie einen DHCP-Server keiner VLAN-Schnittstelle zuweisen, werden die IP-Adressoptionen direkt über die VLAN-Einstellungen konfiguriert.

Auf der Seite für den DHCP-Server können Sie DHCP Lease-Pools erstellen, Leases für bestimmte Hosts reservieren, Standardrouten definieren und DHCP-Optionswerte festlegen.

- SCHRITT 1** Klicken Sie auf **Interface Setup > LAN > DHCP Server** (Schnittstelleneinrichtung > LAN > DHCP-Server). Das Fenster *DHCP Server* (DHCP-Server) wird geöffnet.
- SCHRITT 2** Um die Informationen zu einem DHCP-Eintrag anzuzeigen, klicken Sie in der **DHCP List** (DHCP-Liste) auf das entsprechende Element. Die DHCP-Informationen werden in der Tabelle mit den DHCP-Details angezeigt.
- SCHRITT 3** Um einen DHCP-Eintrag der DHCP-Liste hinzuzufügen oder einen Eintrag daraus zu löschen, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten) oder auf das X-Symbol für **Delete** (Löschen).
- SCHRITT 4** Um einen neuen DHCP-Server-Pool zu erstellen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster *DHCP Server* (DHCP-Server) für den neuen Eintrag wird geöffnet.
- SCHRITT 5** Geben Sie unter **Router IP** (Router-IP) den **DHCP Name** (DHCP-Namen) und die **Local IP Address/Subnet Mask** (Lokale IP-Adresse/Subnetzmaske) ein.
- SCHRITT 6** Konfigurieren Sie die DHCP-Servereinstellungen wie in der Tabelle **DHCP-Servereinstellungen** definiert.
- SCHRITT 7** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

DHCP-Servereinstellungen	
Feld	Beschreibung
Router IP (Router-IP)	
DHCP Name (DHCP-Name)	Beschriftung, mit der die DHCP-Serverkonfiguration identifiziert wird, und die verwendet wird, um den Dienst einer VLAN-Schnittstelle zuzuweisen
Local IP Address/ Subnet Mask (Lokale IP-Adresse/ Subnetzmaske)	IP-Adresse und Subnetzmaske, mit der die VLAN-Schnittstelle, der diese DHCP-Regel zugewiesen wird, konfiguriert wird
DHCP Server Setting (DHCP-Servereinstellung)	
Show DHCP Reservation (DHCP-Reservierung anzeigen)	Klicken Sie auf diese Schaltfläche, um die DHCP-Reservierungen zu prüfen und zu bearbeiten. Klicken Sie erneut auf die Schaltfläche, um die Reservierungstabellen auszublenden.
WAN-Schnittstelle	Wählen Sie die WAN-Schnittstelle aus, über die die zugehörigen DHCP-Daten, insbesondere die DNS-Informationen, abgerufen werden.

DHCP-Servereinstellungen	
Feld	Beschreibung
Option 66 (Option 66)	Stellt den Hosts, für die diese Option erforderlich ist, die Adressinformationen des bereitstellenden Servers zur Verfügung. Die Serverinformationen können wie folgt definiert werden: ▪ Local TFTP Server (Lokaler TFTP-Server): Die SRP verwendet ihren eigenen TFTP-Server für die Bereitstellungsdateien, sodass sie ihre eigene, lokale IP-Adresse an den Client ausgibt. ▪ Remote TFTP Server (Entfernter TFTP-Server): Wenn die SRP mit dieser Methode konfiguriert wurde, verwendet sie die Serverinformationen, die sie über ihre WAN-Schnittstelle und Option 66 empfangen hat, wenn der lokale Client Anforderungen sendet. ▪ Manual TFTP Server (Manueller TFTP-Server): Ermöglicht die manuelle Konfiguration einer Konfigurationsserveradresse. Diese Option wird zwar üblicherweise verwendet, um eine IP-Adresse oder einen vollständig qualifizierten Hostnamen bereitzustellen, aber die SRP akzeptiert auch eine vollständige URL und bietet sie selbst (einschließlich Protokoll, Pfad und Dateiname) an, um so die Anforderungen bestimmter Clients zu erfüllen.
Option 67 (Option 67)	Stellt den Hosts, für die diese Option erforderlich ist, einen Konfigurations-/Bootstrap-Dateinamen zur Verfügung. Diese Option wird gemeinsam mit Option 66 verwendet, damit der Client eine passende TFTP-Anforderung für die Datei senden kann.

DHCP-Servereinstellungen	
Feld	Beschreibung
DNS Proxy (DNS-Proxy)	Wenn der DNS-Proxy aktiviert ist, erhalten lokale Clients für ihre DNS-Anforderungen die lokale IP-Adresse der SRP. Die SRP leitet diese Anforderungen an die DNS-Server weiter, für die sie konfiguriert wurde. Einen wichtigen Hinweis zu DNS finden Sie unter Internet Setup (Interneteinrichtung), Seite 26. Wenn der DNS-Proxy deaktiviert ist, werden den DHCP-Clients die DNS-Serverinformationen wie folgt bereitgestellt: ▪ Wenn die statische DNS-Adresse im entsprechenden Feld konfiguriert ist, wird den Clients nur dieser Server zur Verfügung gestellt. ▪ Wenn die statische DNS-Adresse nicht konfiguriert ist, werden bis zu drei Server angeboten, zuerst aus der allgemeinen Konfiguration der Internetoptionen und anschließend aus der oben festgelegten WAN-Schnittstelle.
Starting IP Address (IP-Startadresse)	Erste IP-Adresse in diesem Pool
Maximum DHCP Users (Höchstanzahl der DHCP-Benutzer)	Höchstanzahl der Geräte, denen der DHCP-Server IP-Adressen zuweisen soll. Diese Zahl ist von der Subnetzmaske und der IP-Startadresse abhängig. Sie darf nicht über 1024 liegen. Der Standardwert lautet 50.
IP Address Range (IP-Adressbereich)	Zeigt den Bereich der DHCP-Adressen an
Client Lease Time (Client-Lease-Zeit)	Die Zeitdauer, während der eine Adresse an einen Client geleast wird. Geben Sie den Lease-Zeitraum in Minuten ein. Der Standardwert ist 0 Minuten, d. h. einen Tag.
Static DNS (Statische DNS)	Definiert eine DNS-Serveradresse, die die DHCP-Clients direkt für die Namensauflösung verwenden. Diese Option ist nur erforderlich, wenn die DNS-Proxy-Funktion für diesen DHCP-Server deaktiviert ist. Das Feld wird ausgeblendet, wenn der DNS-Proxy aktiviert ist.
Windows Internet Naming Service (WINS)	Verwaltet in Windows die Auflösung von Hostname in Adresse. Geben Sie, falls Sie einen WINS-Server verwenden, die IP-Adresse des Servers ein. Lassen Sie das Feld andernfalls leer.

VLAN-Einstellungen

Auf dieser Seite werden die VLAN-Einstellungen konfiguriert. Wenn Sie auf **Add Entry** (Eintrag hinzufügen) klicken, können Sie ein weiteres VLAN erstellen.

-
- SCHRITT 1** Klicken Sie auf **Interface Setup > LAN > VLAN Setting** (Schnittstelleneinrichtung > LAN > VLAN-Einstellung). Das Fenster *VLAN Setting* (VLAN-Einstellung) wird geöffnet.
- Auf dieser Seite können Sie die Liste der konfigurierten VLANs anzeigen, ein VLAN hinzufügen oder löschen und die Details für ein ausgewähltes VLAN anzeigen.
- SCHRITT 2** Um einen VLAN-Eintrag aus der VLAN-Liste zu bearbeiten oder zu löschen, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten) oder auf das X-Symbol für **Delete** (Löschen).
- SCHRITT 3** Um die Informationen für einen VLAN-Eintrag anzuzeigen, klicken Sie auf eines der Elemente in der **VLAN Details List** (VLAN-Detailliste). Die VLAN-Informationen für den DHCP-Pool werden in der Tabelle **VLAN Details** (VLAN-Details) angezeigt.
- SCHRITT 4** Um ein neues VLAN zu erstellen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster *VLAN Settings* (VLAN-Einstellungen) für den neuen Eintrag wird geöffnet.
- SCHRITT 5** Geben Sie die VLAN-Einstellungen für den neuen Eintrag wie in der Tabelle **VLAN-Einstellungen** definiert ein.
- SCHRITT 6** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
- SCHRITT 7** Klicken Sie auf **Add Entry** (Eintrag hinzufügen), um die Seite zum Hinzufügen eines VLANs zu öffnen. Auf dieser Seite können Sie einen VLAN-Eintrag hinzufügen.
- SCHRITT 8** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

VLAN-Einstellungen

Feld	Beschreibung
VLAN-Name	Bridge- oder VLAN-Name
VLAN-ID	Bridge- oder VLAN-ID
Voice VLAN (Sprach-VLAN)	Klicken Sie auf dieses Feld, wenn Sie die Sprachfunktion nutzen möchten. Verwenden Sie diese Option nur im VLAN-Modus.
Adresstyp	Der Adresstyp legt fest, wie die VLAN-IP-Schnittstelle konfiguriert wird. - Wählen Sie None (Keine), wenn keine IP-Schnittstelle erforderlich ist. Dies ist üblicherweise der Fall, wenn die Bridge-Funktion nur für Ports eingesetzt wird. - Wählen Sie Static IP Address (Statische IP-Adresse) aus, um manuell eine Adresse für die Schnittstelle zu definieren. - Wählen Sie Dynamic IP Address (Dynamische IP-Adresse) aus, um eine Adresse von einem DHCP-Server im lokalen Netzwerk anzufordern. - Wählen Sie DHCP Server (DHCP-Server) aus, um einen zuvor auf dieser Schnittstelle konfigurierten DHCP-Serverdienst zu aktivieren. In diesem Fall wird die IP-Adresse des VLANs von der DHCP-Serverkonfiguration abgeleitet.
Available Interface (Verfügbare Schnittstelle)	Die verfügbaren Schnittstellen, die dem VLAN hinzugefügt werden können. Um eine Schnittstelle in die Liste der hinzugefügten Schnittstellen zu verschieben, klicken Sie auf die entsprechende Schnittstelle und anschließend auf die Taste mit dem Pfeil nach rechts (>). Um alle Schnittstellen gemeinsam zu verschieben, klicken Sie auf die Taste mit dem doppelten Pfeil nach rechts (>>).
Added Interface (Hinzugefügte Schnittstelle)	Schnittstellen, die als Mitglieder der VLAN-Bridge ausgewählt wurden. Um eine Schnittstelle aus dieser Liste zu entfernen, klicken Sie auf die entsprechende Schnittstelle und anschließend auf die Taste mit dem Pfeil nach links (<). Um alle Schnittstellen gemeinsam zu entfernen, klicken Sie auf die Taste mit dem doppelten Pfeil nach links (<<).

Porteinstellungen

Über die Seite mit den Porteinstellungen können Sie die LAN-Portattribute festlegen, die Porteinstellungen bearbeiten und anzeigen.

- SCHRITT 1** Klicken Sie auf **Interface Setup > LAN > Port Setting** (Schnittstelleneinrichtung > LAN > Porteinstellung). Das Fenster *Port Setting* (Porteinstellung) wird geöffnet.
- SCHRITT 2** Legen Sie die Einstellungen für Flusskontrolle und Geschwindigkeitsduplex wie in der Tabelle **Porteinstellungen** definiert fest. Sie können diese Einstellungen nur für die LAN-Ports 1 bis 4 konfigurieren.
- SCHRITT 3** Um die Portinformationen anzuzeigen, klicken Sie in der Portliste auf die entsprechenden Elemente. Die Portinformationen werden in der Tabelle mit den Portdetails angezeigt.
- SCHRITT 4** Um einen Porteintrag zu bearbeiten, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten). Das Fenster für die VLAN-Porteinstellungen wird geöffnet.
- SCHRITT 5** Konfigurieren Sie die Porteinstellungen wie in der Tabelle **Porteinstellungen** definiert.
- SCHRITT 6** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Porteinstellungen

Feld	Beschreibung
Mode (Modus)	Beschreibt das aktuell konfigurierte Verhalten des Ports ▪ Desktop mode (Desktopmodus): Stellt angeschlossenen Geräten den Zugriff auf ein einzelnes Daten-VLAN zur Verfügung, für die die SRP DHCP-Dienste bereitstellt. Eingehender Verkehr vom Host kann markiert oder unmarkiert sein. Ausgehender Verkehr zum Host ist unmarkiert. ▪ IP Phone + Desktop mode (IP-Telefon- und Desktopmodus): Der Port wird mit einem Daten-VLAN für den nativen Zugang und einem Sprach-VLAN für die Verwendung mit einem angeschlossenen IP-Telefon konfiguriert. Für die Weitergabe von Sprach-VLAN-Informationen an das Telefon wird CDP eingesetzt.

Porteinstellungen	
Feld	Beschreibung
Enabled Flow Control (Flusssteuerung aktiviert)	Ein Mechanismus für die temporäre Beendigung der Datenübertragung auf dieser physischen Schnittstelle. Beispiel: Es kann eine Situation auftreten, in der eine Sendestation (ein Computer) Daten schneller überträgt als ein anderes Element des Netzwerks (einschließlich der Empfangsstation) die Daten empfangen kann. Das überlastete Netzwerkelement sendet einen PAUSE-Frame, wodurch die Übertragung des Absenders für einen bestimmten Zeitraum angehalten wird. Um diese Funktion zu aktivieren, müssen Sie das Kontrollkästchen markieren. Standardmäßig ist diese Option deaktiviert.
Speed Duplex (Geschwindigkeitsduplex)	Wählen Sie den Duplexmodus aus. Sie können Auto-negotiate (Automatische Aushandlung), 10 Half (10 Halb), 10 Full (10 Voll), 100 Half (100 Halb) und 100 Full (100 Voll) auswählen. Die Standardeinstellung ist Auto-negotiate (Automatische Aushandlung).
Port Details (Portdetails)	Zeigt detaillierte Informationen zu den Ports an

Einrichten des Wireless LAN

In diesen Abschnitten wird die Konfiguration der Wireless-LAN-Einstellungen für die SRP erläutert. Folgende Themen sind enthalten:

- **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)**
- **Wi-Fi Protected Setup**
- **Wireless MAC Filter (Wireless-MAC-Filter)**
- **Erweiterte Wireless-Einstellungen**
- **WMM-Einstellung**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Interface Setup > Wi-Fi Settings** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen).

Basic Wireless Settings (Grundlegende Wireless-Einstellungen)

Auf der Seite für die grundlegenden Wireless-Einstellungen können Sie den integrierten Wireless Access Point der SRP und vier Wireless-Netzwerke konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Interface Setup > Wi-Fi Settings > Basic Wireless Settings** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen > Grundlegende Wireless-Einstellungen). Das Fenster *Basic Wireless Settings* (Grundlegende Wireless-Einstellungen) wird geöffnet.
- SCHRITT 2** Konfigurieren Sie die Wireless-Netzwerkeinstellungen wie in der Tabelle **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)** definiert. Wenn Sie fertig sind, klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
- SCHRITT 3** Wählen Sie den Netzwerkmodus zum Einschalten des Funks aus, und klicken Sie auf **Apply** (Anwenden).
- SCHRITT 4** Konfigurieren Sie die Netzwerksicherheitseinstellungen für jede SSID. Klicken Sie im Bereich für die Wireless-Tabelle in der Spalte **Security** (Sicherheit) auf den Link **Edit** (Bearbeiten). Das Fenster für die Wireless-Sicherheit wird geöffnet.
- SCHRITT 5** Wählen Sie in der Dropdown-Liste den Sicherheitsmodus aus. Standardmäßig ist diese Option deaktiviert.

Wenn Sie einen Sicherheitsmodus aktivieren, wird ein Fenster geöffnet, in dem die Sicherheitseinstellungen für diesen Modus definiert werden (Authentifizierungstyp, Verschlüsselung, Passphrase usw.). Geben Sie die Sicherheitseinstellungen wie in der Tabelle **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)** definiert ein, und klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Sie kehren zur Seite mit den grundlegenden Wireless-Einstellungen zurück.

Basic Wireless Settings (Grundlegende Wireless-Einstellungen)	
Feld	Beschreibung
Network Mode (Netzwerkmodus)	Wählen Sie den Wireless-Modus basierend auf den Gerättypen im Netzwerk aus. BEMERKUNG Der Wireless Access Point ist standardmäßig deaktiviert, um die Netzwerksicherheit zu gewährleisten. Sie müssen einen aktiven Netzwerkmodus auswählen, um ihn zu aktivieren. Erst dann können Sie weitere Konfigurationseinstellungen vornehmen. - Wenn Sie Wireless-N-, Wireless-G- und Wireless-B-Geräte im Netzwerk haben, wählen Sie Mixed (Gemischt) aus. - Wenn Sie nur Wireless-G- und Wireless-B-Geräte im Netzwerk haben, wählen Sie BG-Mixed (BG Gemischt) aus. - Wenn Sie nur Wireless-N-Geräte haben, wählen Sie Wireless-N Only (Nur Wireless-N) aus. - Wenn Sie nur Wireless-G-Geräte haben, wählen Sie Wireless-G Only (Nur Wireless-G) aus. - Wenn Sie nur Wireless-B-Geräte haben, wählen Sie Wireless-B Only (Nur Wireless-B) aus. - Wenn Sie den integrierten Wireless Access Point nicht verwenden möchten, wählen Sie Disabled (Deaktiviert) aus.
Radio Band (Frequenzbereich)	Wählen Sie die Wireless-Bandbreite für das Netzwerk aus. Es stehen drei Optionen zur Auswahl: Auto (Automatisch), Standard-20MHz Channel (Standard – 20-MHz-Kanal) und Wide-40MHz Channel (Breit – 40-MHz-Kanal). Die Standardeinstellung ist Standard-20MHz Channel (Standard – 20-MHz-Kanal). Die Wide-Channel-Bandkonfiguration steht nur für Wireless-N-Netzwerke und -Clients zur Verfügung. Wenn der Wide-Channel-Modus für gemischte Netzwerke ausgewählt wird, steht die Standard-Channel-Verwendung weiterhin für Wireless -B- und Wireless-G-Clients zur Verfügung.
Wide Channel	Wenn Sie für die Funkfrequenzeinstellung die Option Wide-40MHz Channel (Breit – 40-MHz-Kanal) ausgewählt haben, steht diese Einstellung für Ihren primären Wireless-N-Kanal zur Verfügung. Wählen Sie aus der Dropdown-Liste einen beliebigen Kanal aus. Wenn automatisch eine Funkfrequenz ausgewählt wird, wird der Wide Channel ebenfalls automatisch ausgewählt.

Basic Wireless Settings (Grundlegende Wireless-Einstellungen)	
Feld	Beschreibung
Standard Channel	Wenn Sie Wide-40MHz Channel (Breit – 40-MHz-Kanal) oder Standard -20MHz Channel (Standard – 20-MHz-Kanal) für die Funkfrequenzeinstellung ausgewählt haben, steht diese entsprechende Einstellung zur Verfügung. Wählen Sie den Kanal für das Wireless-N-, Wireless-G- und Wireless-B-Netzwerk aus. Wenn Sie für die Funkfrequenzeinstellung Wide-40MHz Channel (Breit – 40-MHz-Kanal) ausgewählt haben, ist der Standardkanal ein sekundärer Kanal für Wireless-N. Der Standardwert ist Kanal 11. Wenn automatisch eine Funkfrequenz ausgewählt wird, wird der Standardkanal ebenfalls automatisch ausgewählt.
Wireless Table (Wireless-Tabelle)	
Wireless Network Name (SSID) (Wireless-Netzwerknamen (SSID))	Name des Netzwerks, das die Clients für die Verbindung verwenden Standardmäßig heißt das Wireless-Netzwerk „cisco-data“ und ist mit dem Standard-VLAN verbunden. Um das Wireless-Standardnetzwerk umzubenennen, legen Sie einen eindeutigen Wireless-Netzwerknamen fest, bei dem Sie auf die Groß- und Kleinschreibung achten und bis zu 32 Zeichen (beliebige Zeichen auf der Tastatur) eingeben. Das zweite Wireless-Standardnetzwerk hat den Standardnamen „cisco-voice“ und ist mit dem Sprach-VLAN verbunden. Um ein zweites Wireless-Netzwerk zu erstellen, geben Sie in der SSID2-Einstellung einen eindeutigen Wireless-Netzwerknamen ein. Um dieses Netzwerk zu aktivieren, wählen Sie Enabled Network (Netzwerk aktiviert) aus. BEMERKUNG Möglicherweise ist Ihr ISP oder ITSP für die Steuerung der SSID2-Einstellungen verantwortlich. Weitere Informationen erhalten Sie von Ihrem ISP oder ITSP.
SSID1/2/3/4 (SSID1/2/3/4)	Der Netzwerkname, der von allen Geräten in einem Wireless-Netzwerk gemeinsam genutzt wird. Die SRP unterstützt bis zu vier Wireless-Netzwerke. Standardmäßig ist das erste und zweite Wireless-Netzwerk aktiviert. Falls erforderlich, können Sie zwei weitere Wireless-Netzwerke aktivieren. Für jedes Wireless-Netzwerk müssen Sie den Wireless-Netzwerknamen (SSID), den Broadcast-Netzwerknamen und die Option zum Aktivieren des Netzwerks konfigurieren.

Basic Wireless Settings (Grundlegende Wireless-Einstellungen)	
Feld	Beschreibung
Broadcast Network Name (Broadcast-Netzwerkname)	Wenn Wireless-Clients die lokale Umgebung auf verfügbare Wireless-Netzwerke prüfen, erkennen sie die SSIDs, die von Wireless-Netzwerken in der Umgebung übertragen werden. Wenn Sie die SSID übertragen möchten, lassen Sie das Kontrollkästchen aktiviert. Wenn Sie die SSID nicht übertragen möchten, deaktivieren Sie das Kontrollkästchen. In diesem Fall müssen die Wireless-Benutzer die SSID kennen, um eine Verbindung zum Netzwerk herstellen zu können.
Enabled Network (Netzwerk aktiviert)	Um das Wireless-Netzwerk zu aktivieren, markieren Sie das Kontrollkästchen. Um das Wireless-Netzwerk zu deaktivieren, entfernen Sie die Markierung des Kontrollkästchens.

Feld	Beschreibung
Wireless Security Settings (Wireless-Sicherheitseinstellungen – Um hierauf zuzugreifen, klicken Sie für alle konfigurierten SSIDs auf Edit Security (Sicherheit bearbeiten).)	
Security Mode (Sicherheitsmodus)	Wählen Sie die Sicherheitsmethode für das Wireless-Netzwerk aus. Die SRP unterstützt die folgenden Sicherheitsmodusoptionen: WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise und WEP. WPA steht für „Wi-Fi Protected Access“, einen stärkeren Sicherheitsstandard als die WEP-Verschlüsselung. WEP steht für „Wired Equivalent Privacy“. Wenn Sie keine Wireless-Sicherheit verwenden möchten, belassen Sie die Standardeinstellung, Disabled (Deaktiviert). Es wird empfohlen, dass Sie die höchste von Ihrem Wireless-Client-Gerät unterstützte Sicherheitsebene einsetzen.
WEP Security Mode Settings (Einstellungen für den WEP-Sicherheitsmodus)	
WEP	Eine grundlegende Verschlüsselungsmethode, die nicht so sicher ist wie WPA. WEP ist ggf. erforderlich, wenn die Netzwerkgeräte WPA nicht unterstützen.
Authentication Type (Authentifizierungstyp)	Wählen Sie Auto (Automatisch) oder Shared Key (Gemeinsam verwendeter Schlüssel) aus. Wenn Sie die Option Auto (Automatisch) verwenden, ist das Netzwerk geöffnet, und jedes Gerät, ob mit oder ohne gemeinsam verwendeten Schlüssel, kann hinzugefügt werden. Bei der Authentifizierung über den gemeinsam verwendeten Schlüssel muss der Client den Schlüssel angeben, den Sie auf dieser Seite festlegen.

Feld	Beschreibung
Verschlüsselung	Wählen Sie eine WEP-Verschlüsselungsmethode aus: 64-Bit, 10 Hexadezimalziffern oder 128-Bit, 26 Hexadezimalziffern. Der Standard ist 64-Bit, 10 Hexadezimalziffern. Höhere Verschlüsselungsebenen führen zu besserer Sicherheit, doch aufgrund ihrer Komplexität können Sie die Leistung des Netzwerks beeinträchtigen.
Passphrase (Passphrase)	Geben Sie eine Passphrase ein, um die WEP-Schlüssel automatisch zu erstellen. Klicken Sie dann auf Generate (Generieren). Es werden gültige Schlüssel angezeigt.
Key 1-4 (Schlüssel 1 bis 4)	Wenn Sie keine Passphrase eingeben, müssen Sie die WEP-Schlüssel manuell eingeben. Wenn Sie die 64-Bit-WEP-Verschlüsselung auswählen, muss der Schlüssel genau 5 ASCII- oder 10 Hexadezimalzeichen lang sein. Wenn Sie die 128-Bit-WEP-Verschlüsselung auswählen, muss der Schlüssel genau 13 ASCII- oder 26 Hexadezimalzeichen lang sein. Gültige Hexadezimalzeichen sind 0 bis 9 und A bis F. BEMERKUNG Die SRP unterstützt einen einzigen WEP-Schlüssel für den Access Point. Wenn mehrere SSIDs mit WEP konfiguriert werden, müssen Sie denselben Schlüssel verwenden.
TX Key (TX-Schlüssel)	Wählen Sie den zu verwendenden TX-Schlüssel (Übertragungsschlüssel) aus. Der Standardwert lautet 1.
WPA Personal Mode Settings (Einstellungen für den persönlichen WEP-Modus)	
WPA Personal (Persönliches WPA)	Diese Option bietet eine höhere Wireless-Sicherheit durch eine erweiterte Verschlüsselung (TKIP oder AES).
WPA Algorithms (WPA-Algorithmen)	WPA unterstützt zwei Verschlüsselungsmethoden, TKIP und AES, mit dynamischen Verschlüsselungsschlüsseln. Wählen Sie als Algorithmustyp entweder AES oder TKIP aus. Der Standard ist TKIP.
WPA Shared Key (Gemeinsam verwendeter WPA-Schlüssel)	Geben Sie eine Passphrase mit 8 bis 63 Zeichen ein.
Group Key Renewal (Gruppenschlüsselerneuerung)	Geben Sie ein Intervall in Sekunden ein, um festzulegen, wie oft die SRP die Verschlüsselungsschlüssel ändern soll. Der Standardzeitraum für die Gruppenschlüsselerneuerung beträgt 3600 Sekunden, also 1 Stunde.

Feld	Beschreibung
WPA2 Personal Mode Settings (Einstellungen für den persönlichen WPA2-Modus)	
WPA2 Personal (Persönliches WPA2)	Diese Option bietet durch eine erweiterte Verschlüsselung (AES oder TKIP + AES) eine hohe Wireless-Sicherheit.
WPA Algorithms (WPA-Algorithmen)	WPA2 unterstützt die beiden Verschlüsselungsmethoden TKIP und AES mit dynamischen Verschlüsselungsschlüsseln. Wählen Sie als Algorithmustyp entweder AES oder TKIP + AES aus. Der Standard ist TKIP + AES.
WPA Shared Key (Gemeinsam verwendeter WPA-Schlüssel)	Geben Sie eine Passphrase mit 8 bis 63 Zeichen ein.
Group Key Renewal (Gruppenschlüsselerneuerung)	Geben Sie ein Intervall in Sekunden ein, um festzulegen, wie oft die SRP die Verschlüsselungsschlüssel ändern soll. Der Standardzeitraum für die Gruppenschlüsselerneuerung beträgt 3600 Sekunden, also 1 Stunde.
Einstellungen für WPA und WPA2 Enterprise	
WPA Enterprise (WPA Enterprise)	Bei dieser Option wird WPA gemeinsam mit einem erreichbaren RADIUS-Server verwendet. Wenn Sie über zwei RADIUS-Server verfügen, legen Sie einen davon als primären und den anderen als sekundären Server für Sicherungszwecke fest.
WPA2 Enterprise (WPA2 Enterprise)	Bei dieser Option wird WPA2 gemeinsam mit einem erreichbaren RADIUS-Server verwendet. Wenn Sie über zwei RADIUS-Server verfügen, legen Sie einen davon als primären und den anderen als sekundären Server für Sicherungszwecke fest.
WPA Algorithms (WPA-Algorithmen)	WPA und WPA2 unterstützen die beiden Verschlüsselungsmethoden TKIP und AES mit dynamischen Verschlüsselungsschlüsseln. Wählen Sie als Algorithmustyp entweder AES oder TKIP aus. Der Standard für WPA ist TKIP. Der Standard für WPA2 ist AES.

Feld	Beschreibung
Primary RADIUS Server (Primärer RADIUS-Server)	▪ RADIUS Server (RADIUS-Server): Geben Sie die IP-Adresse des RADIUS-Servers ein. ▪ RADIUS Port (RADIUS-Port): Geben Sie die Portnummer des RADIUS-Servers ein. Der Standardwert lautet 1812. ▪ Shared Secret (Gemeinsam verwendeter, geheimer Schlüssel): Geben Sie den Schlüssel ein, den die SRP und der Server gemeinsam verwenden. Der Schlüssel kann aus 8 bis 63 ASCII-Zeichen oder 64 Hexadezimalzeichen bestehen.
Secondary RADIUS Server (Sekundärer RADIUS-Server)	▪ RADIUS Server Address (RADIUS-Serveradresse): Geben Sie die IP-Adresse des RADIUS-Servers ein. ▪ RADIUS Port (RADIUS-Port): Geben Sie die Portnummer des RADIUS-Servers ein. ▪ Shared Secret (Gemeinsam verwendeter, geheimer Schlüssel): Geben Sie den Schlüssel ein, den die SRP und der Server gemeinsam verwenden. Der Schlüssel kann aus 8 bis 63 ASCII-Zeichen oder 64 Hexadezimalzeichen bestehen.
Key Renewal Timeout (Zeitüberschreitung für Schlüssel-erneuerung)	Geben Sie ein Intervall in Sekunden ein, um festzulegen, wie oft die SRP die Verschlüsselungsschlüssel ändern soll. Der Standardzeitraum für die Gruppenschlüssel-erneuerung beträgt 3600 Sekunden, also 1 Stunde.

Wi-Fi Protected Setup

Auf der Seite für Wi-Fi Protected Setup können Sie die Wireless-Sicherheit für Ihre Wireless-Netzwerke automatisch konfigurieren.

HINWEIS Stellen Sie sicher, dass sich das WPS-Client-Gerät während der Einrichtung in der Nähe der SRP befindet.

SCHRITT 1 Klicken Sie auf **Interface Setup > Wi-Fi Settings > Wi-Fi Protected Setup** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen > Wi-Fi Protected Setup). Das Fenster für Wi-Fi Protected Setup wird geöffnet.

SCHRITT 2 Um WPS für eine einzelne SSID zu aktivieren, wählen Sie aus der Dropdown-Liste den Namen des Wireless-Netzwerks, das Sie konfigurieren möchten. Die Standard-Daten-SSID ist „cisco-data“. Die Standard-Sprach-SSID ist „cisco-voice“.

SCHRITT 3 WPS ist standardmäßig aktiviert. Wählen Sie **Disabled** (Deaktiviert), wenn Sie diese Funktion für das ausgewählte VLAN nicht verwenden möchten.

- SCHRITT 4** Wählen Sie eine Methode für Wi-Fi Protected Setup aus. Der aktuelle Status für Wi-Fi Protected Setup wird unten auf der Seite angezeigt.

Es stehen drei Methoden zur Konfiguration der Wireless-Einstellungen über WPS zur Verfügung. Verwenden Sie die Methode, die für das zu konfigurierende Client-Gerät geeignet ist.

WPS-Methode 1

Verwenden Sie diese Methode, wenn das Client-Gerät über eine Taste für Wi-Fi Protected Setup verfügt.

- SCHRITT 1** Klicken oder drücken Sie auf dem Client-Gerät auf die Taste **Wi-Fi Protected Setup** (Wi-Fi Protected Setup).
- SCHRITT 2** Klicken Sie auf dieser Seite auf **Wi-Fi Protected Setup** (Wi-Fi Protected Setup), oder drücken Sie die Taste für Wi-Fi Protected Setup auf der Oberseite des SRP520, falls dieser mit der aktuell ausgewählten SSID verbunden ist. Weitere Informationen finden Sie unter **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)**, Seite 50.
- SCHRITT 3** Klicken Sie nach der Konfiguration des Client-Geräts auf **OK**. Weitere Anweisungen erhalten Sie über das Client-Gerät oder dessen Dokumentation.

WPS-Methode 2

Verwenden Sie diese Methode, wenn das Client-Gerät über eine PIN-Taste für Wi-Fi Protected Setup verfügt.

- SCHRITT 1** Geben Sie im Feld auf dieser Seite die PIN-Nummer ein.
- SCHRITT 2** Klicken Sie auf **Register** (Registrieren).
- SCHRITT 3** Klicken Sie nach der Konfiguration des Client-Geräts auf **OK**. Weitere Anweisungen erhalten Sie über das Client-Gerät oder dessen Dokumentation.

WPS-Methode 3

Verwenden Sie diese Methode, wenn das Client-Gerät die PIN-Nummer der SRP benötigt.

- SCHRITT 1** Geben Sie die auf dieser Seite aufgeführte PIN-Nummer ein. (Sie finden sie auch auf dem Etikett auf der Unterseite der SRP)
- SCHRITT 2** Klicken Sie nach der Konfiguration des Client-Geräts auf **OK**. Weitere Anweisungen erhalten Sie über das Client-Gerät oder dessen Dokumentation.

Wireless MAC Filter (Wireless-MAC-Filter)

Auf der Seite für den Wireless-MAC-Filter können Sie die MAC-Adressen der Wireless-Geräte festlegen, denen die SRP den Zugriff erlaubt bzw. die sie blockiert.

-
- SCHRITT 1** Klicken Sie auf **Interface Setup > Wi-Fi Settings > Wireless MAC Filter** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen > Wireless-MAC-Filter). Das Fenster *Wireless MAC Filter* (Wireless-MAC-Filter) wird geöffnet.
- SCHRITT 2** Wählen Sie aus der Dropdown-Liste eine SSID aus, und legen Sie die MAC-Filtereinstellungen fest, die auf die SSID angewendet werden sollen. Die Standard-SSID für Daten ist „cisco-data“, für Sprache „cisco-voice“.
- SCHRITT 3** Um die Wireless-Benutzer nach MAC-Adresse zu filtern und den Zugriff zu erlauben oder zu blockieren, wählen Sie **Enable** (Aktivieren) aus. Die Standardeinstellung lautet Deaktivieren.
- SCHRITT 4** Wählen Sie im Bereich **Access Restriction** (Zugriffsbeschränkung) die Option **Prevent** (Verhindern) oder **Permit** (Zulassen) aus.
- SCHRITT 5** Wenn die Option für den Wireless-MAC-Filter aktiviert ist, können Sie auf **Show Client List** (Client-Liste anzeigen) klicken, um die Seite mit der Liste der Wireless-Clients anzuzeigen. Hier werden Computer und andere Geräte aufgeführt, die momentan mit dem Wireless-Netzwerk verbunden sind. Die Liste kann nach Client-Name, Schnittstelle, IP-Adresse, MAC-Adresse und Status gefiltert werden.
- SCHRITT 6** Wählen Sie für ein Gerät, das Sie der Liste hinzufügen möchten, **Save to MAC Address Filter List** (In MAC-Adressfilterliste speichern) aus, und klicken Sie auf **Add** (Hinzufügen). Um die aktuellsten Daten abzurufen, klicken Sie auf **Refresh** (Aktualisieren). Um diese Seite zu schließen und zur Seite für den Wireless-MAC-Filter zurückzukehren, klicken Sie auf **Close** (Schließen).
- HINWEIS** Der Wireless-Zugriff kann über die MAC-Adressen der Wireless-Geräte, die innerhalb des Netzwerkradius senden, gefiltert werden.
- SCHRITT 7** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Einstellungen für den Wireless-MAC-Filter	
Feld	Beschreibung
Wireless MAC Filter (Wireless-MAC-Filter)	
Select a SSID (SSID auswählen)	Wählen Sie den Namen des Wireless-Netzwerks aus, das Sie konfigurieren möchten. Die Standard-SSID für Daten ist „cisco-data“, für Sprache „cisco-voice“.
Enabled/Disabled (Aktiviert/Deaktiviert)	Um die Wireless-Benutzer nach MAC-Adresse zu filtern und den Zugriff zu erlauben oder zu blockieren, wählen Sie Enabled (Aktiviert) aus. Standardmäßig ist diese Option deaktiviert.
Access Restriction (Zugriffsbeschränkung)	
Prevent (Verhindern)	Wählen Sie diese Option aus, um den Wireless-Zugriff der Clients, die Sie in der MAC-Adresstabelle speichern, zu blockieren. Dies ist die Standardeinstellung.
Permit (Zulassen)	Wählen Sie diese Option aus, wenn Sie nur den in der MAC-Adresstabelle festgelegten Clients den Wireless-Zugriff erlauben wollen.
Show Client List (Client-Liste anzeigen)	Klicken Sie auf diese Schaltfläche, um eine Liste der Computer und anderer Geräte anzuzeigen, die mit diesem Wireless-Netzwerk verbunden sind. Um einen aufgeführten Client der MAC-Adresstabelle hinzuzufügen, markieren Sie das Kontrollkästchen Save to MAC Address Filter List (In MAC-Adressfilterliste speichern), und klicken Sie auf Add (Hinzufügen). Um die Client-Liste auszublenden, klicken Sie auf Hide Client List (Client-Liste ausblenden).
MAC Address Table (MAC-Adresstabelle)	
01-32 (01 bis 32)	Geben Sie die MAC-Adresse der Geräte ein, deren Wireless-Zugriff Sie blockieren oder zulassen möchten.

Erweiterte Wireless-Einstellungen

Auf der Seite für die Wireless-Einstellungen können Sie erweiterte Wireless-Funktionen für die SRP konfigurieren.

HINWEIS Diese Einstellungen sollten nur von einem erfahrenen Administrator festgelegt werden. Bevor Sie diese Einstellungen konfigurieren, müssen Sie sicherstellen, dass die Wireless-Funktion auf der SRP aktiviert ist. Weitere Informationen finden Sie unter **Basic Wireless Settings (Grundlegende Wireless-Einstellungen)**, Seite 50.

- SCHRITT 1** Klicken Sie auf **Interface Setup > Wi-Fi Settings > Advanced Wireless Settings** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen > Erweiterte Wireless-Einstellungen). Das Fenster *Advanced Wireless* (Erweiterte Wireless-Einstellungen) wird geöffnet.
- SCHRITT 2** Um den RTS-Schwellenwert zu konfigurieren, wählen Sie aus der Dropdown-Liste eine SSID aus.
- SCHRITT 3** Geben Sie im Feld für den RTS-Schwellenwert einen Wert ein. Wenn inkonsistente Datenflüsse zu verzeichnen sind, geben Sie nur leichte Verringerungen ein. Als Standardwert wird 2347 empfohlen.
- SCHRITT 4** Ändern Sie im Bereich für die globalen Einstellungen die Einstellungen wie gewünscht und in der Tabelle **Erweiterte Wireless-Einstellungen** definiert. Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Erweiterte Wireless-Einstellungen	
Feld	Beschreibung
Advanced Wireless Setup (Erweiterte Wireless-Einrichtung)	
Select a SSID (SSID auswählen)	Wählen Sie den Namen des Wireless-Netzwerks aus, das Sie konfigurieren möchten. Die Standard-Daten-SSID ist „cisco-data“. Die Standard-Sprach-SSID ist „cisco-voice“.

Erweiterte Wireless-Einstellungen	
Feld	Beschreibung
RTS Threshold (RTS-Schwellenwert)	Die SRP sendet RTS-Frames (Request to Send) an eine Empfangsstation und verhandelt das Senden eines Daten-Frames. Nach Empfangen eines RTS antwortet die Wireless-Station mit einem CTS-Frame (Clear to Send), um der SRP zu signalisieren, dass die Übertragung beginnen kann. Wenn inkonsistente Datenflüsse zu verzeichnen sind, können Sie diesen Schwellenwert anpassen. Es wird nur eine leichte Verringerung in Bezug auf den Standardwert 2347 empfohlen. Wenn ein Netzwerkpaket kleiner als die voreingestellte RTS-Schwellenwertgröße ist, wird der RTS/CTS-Mechanismus nicht aktiviert. Der RTS-Schwellenwert sollte auf dem Standardwert 2347 belassen werden.
Global Settings (Globale Einstellungen)	
AP Isolation (AP-Isolierung)	Isoliert alle Wireless-Clients und Wireless-Geräte voneinander. Die Wireless-Geräte können mit der SRP kommunizieren, aber nicht mit anderen Wireless-Geräten im Netzwerk. Wählen Sie Enabled (Aktiviert) aus, um diese Option zu verwenden. Standardmäßig ist die AP-Isolierung deaktiviert.
Basic Rate (Basisrate)	Eine Reihe von Raten, mit denen die SRP Daten übertragen kann. Die SRP kündigt den anderen Wireless-Geräten im Netzwerk ihre Basisrate an, sodass diese wiederum ihre beste Rate für die Übertragung auswählen können. Die Standardeinstellung ist Default (Standard), mit der die SRP mit allen Wireless-Standardraten übertragen kann (1 – 2 Mbit/s, 5,5 Mbit/s, 11 Mbit/s, 18 Mbit/s und 24 Mbit/s). Für ältere Wireless-Technologien kann 1 – 2 Mbit/s ausgewählt werden. Über All (Alle) kann die SRP für ihre Übertragung alle Wireless-Raten verwenden. Die Basisrate entspricht nicht der tatsächlichen Rate der Datenübertragung. Um die Rate der Datenübertragung für die SRP festzulegen, müssen Sie die Einstellung Transmission Rate (Übertragungsrate) definieren.

Erweiterte Wireless-Einstellungen	
Feld	Beschreibung
N Transmission Rate (N-Übertragungsrate)	Legen Sie die Datenübertragungsrate abhängig von der Geschwindigkeit des Wireless-N-Netzwerks fest. Wählen Sie aus verschiedenen Übertragungsgeschwindigkeiten aus, oder legen Sie Auto (Automatisch) fest, damit die SRP automatisch die schnellstmögliche Datenrate nutzt und die Funktion Auto-Fallback (Automatisches Fallback) aktiviert. Über diese Option wird die bestmögliche Verbindungsgeschwindigkeit zwischen der SRP und einem Wireless-Client ausgehandelt. Die Standardeinstellung ist Auto.
Transmission Rate (Übertragungsrate)	Legen Sie die Datenübertragungsrate je nach der Geschwindigkeit des Wireless-Netzwerks fest. Wählen Sie aus verschiedenen Übertragungsgeschwindigkeiten aus, oder legen Sie Auto (Automatisch) fest, damit die SRP automatisch die schnellstmögliche Datenrate nutzt und die Funktion Auto-Fallback (Automatisches Fallback) aktiviert. Über diese Option wird die bestmögliche Verbindungsgeschwindigkeit zwischen der SRP und einem Wireless-Client ausgehandelt. Die Standardeinstellung ist Auto.
CTS Protection Mode (CTS-Schutzmodus)	Die SRP verwendet automatisch den CTS-Schutzmodus (Clear-To-Send), wenn die Wireless-N- und Wireless-G-Produkte schwerwiegende Probleme entdecken und in einer Umgebung mit starkem 802.11b-Verkehr keine Daten an die SRP senden können. Diese Funktion steigert die Fähigkeit der SRP, alle Wireless-N- und Wireless-G-Übertragungen zu empfangen, kann jedoch die allgemeine Leistung beeinträchtigen. Die Standardeinstellung ist Auto.
DTIM Interval (DTIM-Intervall)	Dieser Wert zwischen 1 und 255 gibt das Intervall für die Delivery Traffic Indication Message (DTIM) an. Ein DTIM-Feld ist ein Countdown-Feld, das die Clients über das nächste Fenster für das Abhören von Broadcast- und Multicast-Meldungen informiert. Wenn die SRP Broadcast- oder Multicast-Meldungen für verbundene Clients gepuffert hat, sendet sie die nächste DTIM im Einklang mit dem DTIM-Intervallwert. Die Clients hören die Beacons und wachen auf, um die Broadcast- und Multicast-Meldungen zu empfangen. Der Standardwert lautet 1.

Erweiterte Wireless-Einstellungen	
Feld	Beschreibung
Fragmentation Threshold (Fragmentierungsschwellenwert)	Mit diesem Wert wird die Maximalgröße eines Pakets festgelegt. Ist diese erreicht, werden Daten in mehrere Pakete aufgeteilt (fragmentiert). Wenn viele Paketfehler auftreten, können Sie den Fragmentierungsschwellenwert leicht erhöhen. Setzen Sie den Fragmentierungsschwellenwert zu hoch, ist möglicherweise eine schlechte Netzwerkleistung die Folge. Es wird nur eine leichte Verringerung in Bezug auf den Standardwert empfohlen. In den meisten Fällen sollte der Standardwert 2346 beibehalten werden.
Beacon Interval (Beacon-Intervall)	Geben Sie einen Wert zwischen 40 und 3500 Millisekunden ein. Der Wert für das Beacon-Intervall gibt an, wie häufig das Signal gesendet wird. Ein Beacon ist eine Paketübertragung der SRP, mit der das Wireless-Netzwerk synchronisiert wird. Der Standardwert lautet 100.
Power Control (Leistungssteuerung)	Wählen Sie den hohen, mittleren oder niedrigen Wert, um den Bereich des Wireless-Netzwerks festzulegen. Der Standard ist der hohe Wert, eine normale Leistungseinstellung.

WMM-Einstellung

Auf der Seite für die WMM-Einstellung konfigurieren Sie die Unterstützung für WMM-Geräte (Wi-Fi Multimedia) im Netzwerk.

- SCHRITT 1** Klicken Sie auf **Interface Setup > Wi-Fi Settings > WMM Setting** (Schnittstelleneinrichtung > Wi-Fi-Einstellungen > WMM-Einstellung). Das Fenster *WMM Setting* (WMM-Einstellung) wird geöffnet.
- SCHRITT 2** Wenn andere Geräte im Netzwerk vorhanden sind, die WMM unterstützen, belassen Sie die Standardeinstellung **Enabled** (Aktiviert).
- SCHRITT 3** Wählen Sie für **No Acknowledgement** (Keine Bestätigung) die Option **Enabled** (Aktiviert) aus, um die Bestätigungsfunktion zu deaktivieren, sodass die SRP bei einem Fehler Daten nicht erneut sendet. Standardmäßig ist diese Option deaktiviert.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Verwenden der Verwaltungsschnittstelle

Auf der Seite für die Verwaltungsschnittstelle legen Sie die Loopback-Schnittstellen fest, die für Routing-Aktualisierungen und einige Protokolle verwendet werden können. Sie können bis zu zwei Loopback-Schnittstellen definieren.

SCHRITT 1 Klicken Sie auf **Interface Setup > Management Interface** (Schnittstelleneinrichtung > Verwaltungsschnittstelle). Das Fenster *Management Interface* (Verwaltungsschnittstelle) wird geöffnet.

SCHRITT 2 Um einen Eintrag in der Liste der Loopback-Schnittstellen zu bearbeiten, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten).

Das Fenster *Manually Adding Loopback* (Loopback manuell hinzufügen) wird geöffnet.

SCHRITT 3 Geben Sie die IP-Adresse ein, die für die Loopback-Schnittstelle verwendet werden soll. Die Adresse darf sich mit keiner anderen, auf der SRP konfigurierten Schnittstelle überschneiden.

HINWEIS Die für die Loopback-Schnittstelle verwendete IP-Adresse übernimmt die Subnetzmaske 255.255.255.255.

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Konfigurieren des Netzwerks

In diesem Kapitel wird erläutert, wie Sie die Netzwerkeinstellungen für die Services Ready-Plattformen konfigurieren. Folgende Themen sind enthalten:

- **Routing**
- **NAT**
- **Port Range Triggering (Portbereich-Triggering)**
- **Firewall**
- **PPPoE Relay (PPPoE-Relay)**
- **DDNS**
- **IGMP (IGMP)**
- **UPnP**
- **CDP Setting (CDP-Einstellung)**

Klicken Sie in der Menüleiste des Konfigurationsprogramms auf die Registerkarte **Network Setup** (Netzwerkeinrichtung).

Routing

In diesem Abschnitt wird erläutert, wie Sie auf der SRP verschiedene Routing-Typen konfigurieren:

- **Static Routes (Statische Routen)**
- **RIP (RIP)**
- **Intervlan Routing (Intervlan-Routing)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Network Setup > Routing** (Netzwerkeinrichtung > Routing).

Static Routes (Statische Routen)

Auf der Seite für statische Routen konfigurieren Sie statische Routen für den Netzwerkverkehr.

SCHRITT 1 Klicken Sie auf **Network Setup > Routing > Static Routes** (Netzwerkeinrichtung > Routing > Statische Routen). Das Fenster *Static Routes* (Statische Routen) wird geöffnet.

Auf dieser Seite können Sie die Liste der aktuellen statischen Routen sowie Details zu einer ausgewählten Route anzeigen lassen. Oder fügen Sie der Liste eine neue statische Route hinzu.

SCHRITT 2 Klicken Sie zum Hinzufügen einer statischen Route auf **Add Entry** (Eintrag hinzufügen).

Das Fenster *Static Routing* (Statische Routen) für den neuen Eintrag wird geöffnet.

SCHRITT 3 Geben Sie einen Namen für die neue Route ein.

SCHRITT 4 Geben Sie die IP-Zieladresse und die Subnetzmaske für das gewünschte Netzwerk bzw. den gewünschten Host ein, dem Sie eine statische Route zuweisen möchten.

SCHRITT 5 Geben Sie die IP-Adresse des Gateways ein, das den Kontakt zwischen der SRP und dem gewünschten Netzwerk bzw. Host ermöglicht.

SCHRITT 6 Wählen Sie die Schnittstelle für diese Route aus.

SCHRITT 7 Klicken Sie auf **Senden**, um Ihre Änderungen zu speichern.

Einstellungen für statische Routen	
Feld	Beschreibung
Enter Route Name (Routennamen eingeben)	Geben Sie einen Namen für die statische Route ein.
Destination Subnet (Zielsubnetz)	IP-Adresse des Netzwerks oder Hosts, dem sie eine statische Route zuweisen möchten
Subnet Mask (Subnetzmaske)	Legt fest, bei welchem Teil einer IP-Adresse es sich um den Netzwerk- und den Host-Teil handelt
Gateway	Geben Sie die IP-Adresse des Gateway-Geräts ein, das den Kontakt zwischen der SRP und dem gewünschten Netzwerk bzw. Host ermöglicht.
Schnittstelle	Legt fest, ob sich die IP-Zieladresse im LAN- und Wireless-Netzwerk (internes verkabeltes und kabelloses Netzwerk) oder im Internet (WAN) befindet.

RIP (RIP)

Auf den Seiten für das Routing Information Protocol (RIP) können Sie für die SRP dynamische Routen festlegen. Dieses Protokoll können Sie aktivieren, damit sich die angegebenen Schnittstellen automatisch an physische Änderungen in der Netzwerkanordnung anpassen können und damit sie Routing-Tabellen mit anderen Routern austauschen können. Die SRP legt die Route der Netzwerkpakete auf Grundlage der geringsten Zahl von Hops zwischen Quelle und Ziel fest.

SCHRITT 1 Klicken Sie auf **Network Setup > Routing > RIP** (Netzwerkeinrichtung > Routing > RIP). Das Fenster *RIP (RIP)* wird geöffnet.

SCHRITT 2 Um RIP (dynamisches Routing) zu aktivieren, wählen Sie **Enabled** (Aktiviert) aus. Standardmäßig ist diese Option deaktiviert.

SCHRITT 3 Wenn Sie RIP aktivieren, wählen Sie die RIP-Version und die Zeitüberschreitungswerte wie in der Tabelle **RIP-Einstellungen** definiert aus.

Auf der SRP können Sie festlegen, welche Netzwerke am Routing-Protokoll teilnehmen sollen, entweder nach Schnittstelle oder nach Subnetz der IP-Adresse.

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

RIP-Einstellungen	
Feld	Beschreibung
RIP List (RIP-Liste)	Interface (Schnittstelle): Zeigt die Liste der Schnittstellen an. RIP Enabled (RIP aktiviert): Wählen Sie diese Option aus, um RIP für die Schnittstelle zu aktivieren oder zu deaktivieren. Passive Mode (Passivmodus): Über die Passivmodus-Schnittstelle werden alle empfangenen Pakete normal verarbeitet. Multicast- oder Unicast-RIP-Pakete werden nur an RIP-Nachbarn gesendet. Um den Passivmodus auszuwählen, wählen Sie im Fenster mit den RIP-Konfigurationseinstellungen die Option Enabled (Aktiviert) aus. Authentication (Authentifizierung): Wenn Sie Pakete mit RIP Version 2 senden und empfangen, können Sie für eine Schnittstelle eine RIP-Authentifizierung auswählen. Die SRP unterstützt für Schnittstellen zwei Authentifizierungsmodi: Simple Password Authentication (Einfache Passwortauthentifizierung) und MD5 Authentication (MD5-Authentifizierung). BEMERKUNG: RIP Version 1 unterstützt die Authentifizierung nicht.
RIP Version (RIP-Version)	Um die Pakettypen, die übertragen werden können, zu begrenzen, wählen Sie Version 1 (Version 1) oder Version 2 (Version 2) aus. Wählen Sie andernfalls RIP v1/v2 (RIP-Version 1 und 2) aus, um Pakete der Version 1 und 2 übertragen zu können.
RIP Timer (RIP-Timer)	Für die Regulierung seiner Leistung nutzt RIP Timer. Dazu gehören ein Aktualisierungs-Timer, ein Zeitüberschreitungs-Timer und ein Lösch-Timer für Routen. Update (Aktualisieren): Geben Sie an, wie oft die SRP Routing-Aktualisierungen senden soll. Die Voreinstellung ist 30 Sekunden. Timeout (Zeitüberschreitung): Geben Sie an, wie oft die SRP Routing-Aktualisierungen von den jeweiligen Routern aus der Routing-Tabelle erwarten soll. Wird dieser Wert überschritten, wird die Route als nicht erreichbar angesehen. Die Route wird erst aus der Routing-Tabelle gelöscht, wenn der Lösch-Timer abläuft. Flush (Löschen): Geben Sie an, wie lange die SRP auf eine Aktualisierung wartet, bevor eine Route aus der Routing-Tabelle gelöscht wird.

RIP-Einstellungen	
Feld	Beschreibung
RIP By (RIP über)	Wählen Sie aus, ob RIP über eine Schnittstelle oder ein IP-Subnetz aktiviert werden soll.
RIP List (RIP-Liste)	Zeigt die RIP-Einstellungen aller SRP-Schnittstellen an. Um die Einstellungen zu bearbeiten, klicken Sie auf das Bleistiftsymbol für Edit (Bearbeiten).

Intervlan Routing (Intervlan-Routing)

Durch die Konfiguration von VLANs können Sie die Größe der Broadcast-Domäne besser steuern und lokalen Verkehr im lokalen Bereich halten. Wenn jedoch eine Endstation in einem VLAN mit einer Endstation in einem anderen VLAN kommunizieren muss, ist die Intervlan-Kommunikation erforderlich. Diese Kommunikation wird durch Intervlan-Routing ermöglicht.

HINWEIS Falls Sie einen Wireless-Gastzugang konfiguriert haben, wird das Intervlan-Routing nicht auf dem Gast-VLAN genutzt.

SCHRITT 1 Klicken Sie auf **Network Setup > Routing > Intervlan Routing** (Netzwerkeinrichtung > Routing > Intervlan-Routing). Das Fenster *Intervlan Routing* (Intervlan-Routing) wird geöffnet.

SCHRITT 2 Um das Intervlan-Routing zu aktivieren, wählen Sie **Enabled** (Aktiviert) aus. Dies ist die Standardeinstellung. Um Intervlan-Routing zu deaktivieren, wählen Sie **Disabled** (Deaktiviert) aus.

SCHRITT 3 Klicken Sie ggf. auf **Senden**, um Ihre Änderungen zu speichern.

NAT

In diesem Abschnitt wird erläutert, wie Sie die NAT-Einstellungen (Network Address Translation) für die SRP einrichten. Folgende Themen sind enthalten:

- **NAT Setting (NAT-Einstellung)**
- **Port Forwarding (Portweiterleitung)**
- **Port Range Triggering (Portbereich-Triggering)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Network Setup > NAT** (Netzwerkeinrichtung > NAT).

NAT Setting (NAT-Einstellung)

Auf der Seite für NAT können Sie das NAT-Routing aktivieren und deaktivieren, über das die SRP die Netzwerkverbindung ins Internet hosten kann.

-
- SCHRITT 1** Klicken Sie auf **Network Setup > NAT > NAT Setting** (Netzwerkeinrichtung > NAT > NAT-Einstellung). Das Fenster *NAT Setting* (NAT-Einstellung) wird geöffnet.
- SCHRITT 2** Um NAT zu aktivieren, klicken Sie auf **Enabled** (Aktiviert). Dies ist die Standardeinstellung. Um NAT zu deaktivieren, klicken Sie auf **Disabled** (Deaktiviert). Standardmäßig sind alle ALGs deaktiviert.
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Port Forwarding (Portweiterleitung)

Die Seite für die Portweiterleitung ist nützlich, wenn Ihr Netzwerk Netzwerkdienste (Internetanwendungen) wie Web, E-Mail, FTP, Videokonferenzen oder Spiele hostet. Für jeden Dienst wird der Internet-Datenverkehr nach Anwendung (IP-Port) an die internen Server weitergeleitet, die diese Dienste hosten.

Mit der Portweiterleitung kann die SRP Pakete, die an die WAN-Schnittstelle und einen bestimmten Anwendungsport oder einen Portbereich adressiert sind, an ein internes Gerät im LAN weiterleiten. Wenn Sie beispielsweise im SRP-LAN einen Webserver haben, können Sie die Portweiterleitung für alle Anfragen an Port 80 festlegen, damit diese umgewandelt und an die IP-Adresse des internen Webserver gesendet werden.

Wenn Sie auf **Add Entry** (Eintrag hinzufügen) klicken, können Sie einen zusätzlichen Eintrag für einen weiteren Netzdienst hinzufügen. Um einen Eintrag zu bearbeiten, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten).

- HINWEIS** Um die korrekte Weiterleitung des Datenverkehrs sicherzustellen, müssen lokale Server entweder mit einer statischen IP-Adresse konfiguriert werden, oder ihnen muss über DHCP eine reservierte IP-Adresse zugewiesen werden. Auf der Seite **Interface Setup > LAN > DHCP Server** (Schnittstelleneinrichtung > LAN > DHCP-Server) können Sie IP-Adressen reservieren. Weitere Informationen finden Sie unter **DHCP-Server, Seite 42**.

-
- SCHRITT 1** Klicken Sie auf **Network Setup > NAT > Port Forwarding** (Netzwerkeinrichtung > NAT > Portweiterleitung). Das Fenster *Port Forwarding* (Portweiterleitung) wird geöffnet.
- SCHRITT 2** Um einen Eintrag hinzuzufügen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster zum manuellen Hinzufügen einer Portweiterleitung wird geöffnet.

SCHRITT 3 Geben Sie die Einstellungen für die Portweiterleitung wie in der Tabelle **Einstellungen für die Portweiterleitung** definiert ein.

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für die Portweiterleitung	
Feld	Beschreibung
Port Forwarding Type (Portweiterleitungstyp)	Wählen Sie aus der Dropdown-Liste den Typ der Portweiterleitung aus. Wählen Sie Single Port Forwarding (Weiterleitung über einzelnen Port) aus, um den Datenverkehr für einen festgelegten Port auf den gleichen oder einen anderen Port des Zielservers im LAN weiterzuleiten. Wählen Sie Port Range Forwarding (Weiterleitung über Portbereich) aus, um den Datenverkehr an einen Portbereich an die gleichen Ports auf dem Zielserver im LAN weiterzuleiten. Weitere Informationen zu den erforderlichen Ports oder Portbereichen finden Sie in der Dokumentation der entsprechenden Internetanwendung.
Name der Anwendung	Wählen Sie für die Weiterleitung über einen einzelnen Port aus der Dropdown-Liste eine gemeinsame Anwendung aus (z. B. Telnet oder DNS). Um eine Anwendung einzugeben, die nicht in der Liste gespeichert ist, wählen Sie Add a new name (Neuen Namen hinzufügen) aus, und geben Sie den Namen einer neuen Anwendung ein.
Enter a Name (Namen eingeben)	Geben Sie für die Weiterleitung über einen einzelnen Port den Namen der neuen Anwendung ein.
WAN Interface Name (WAN-Schnittstellennamen)	Wählen Sie die WAN-Schnittstelle aus, an die der Datenverkehr ursprünglich adressiert ist.
External Port (Externer Port)	Geben Sie für die Weiterleitung über einen einzelnen Port die Portnummer ein, die externe Clients für die Herstellung einer Verbindung zum internen Server verwenden sollen.

Einstellungen für die Portweiterleitung	
Feld	Beschreibung
Internal Port (Interner Port)	Geben Sie für die Weiterleitung über einen einzelnen Port die Portnummer ein, die die SRP für die Weiterleitung von Datenverkehr an den internen Server verwenden soll. Aus Gründen der Einfachheit sind die internen und externen Portnummern häufig gleich. Abweichende externe Portnummern können jedoch genutzt werden, um Datenverkehr desselben Anwendungstyps, der für unterschiedliche interne Server vorgesehen ist, zu unterscheiden oder um durch nicht standardisierte Ports den Datenschutz zu erhöhen.
Protokoll	Wählen Sie die Protokolle aus, die weitergeleitet werden sollen: TCP, UDP oder beide.
IP-Adresse	Geben Sie die IP-Adresse des lokalen Servers ein, der den weitergeleiteten Datenverkehr empfangen soll.
Aktiviert	Klicken Sie auf Enabled (Aktiviert), um diese Weiterleitungsregel zu aktivieren. Standardmäßig ist diese Option deaktiviert.

Port Range Triggering (Portbereich-Triggering)

Über die Seite für das Portbereich-Triggering kann die SRP ausgehende Daten auf bestimmte Portnummern überwachen und dynamisch eine Weiterleitungsregel erstellen, um zurückkehrenden Datenverkehr an den lokalen Client zu leiten, der die Anfrage gestellt hatte.

Für das Portbereich-Triggering muss der lokale Client keine feste IP-Adresse verwenden. Der Datenverkehr für einen bestimmten Port kann immer nur an einen lokalen Client weitergeleitet werden.

SCHRITT 1 Klicken Sie auf **Network Setup > NAT > Port Range Triggering** (Netzwerkeinrichtung > NAT > Portbereich-Triggering). Das Fenster *Port Range Triggering* (Portbereich-Triggering) wird geöffnet.

Auf dieser Seite können Sie in der entsprechenden Liste die vorhandenen Einträge für das Portbereich-Triggering und Details zu einem ausgewählten Eintrag anzeigen.

SCHRITT 2 Um einen vorhandenen Eintrag zu bearbeiten, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten).

SCHRITT 3 Um einen neuen Eintrag für das Portbereich-Triggering einzugeben, klicken Sie auf **Add Entry** (Eintrag hinzufügen).

Das Fenster *Port Range Triggering* (Portbereich-Triggering) wird geöffnet.

SCHRITT 4 Geben Sie die Einstellungen für das Portbereich-Triggering wie in der Tabelle **Einstellungen für das Portbereich-Triggering** definiert ein.

SCHRITT 5 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für das Portbereich-Triggering	
Feld	Beschreibung
Name der Anwendung	Geben Sie zur Bezeichnung der Anwendung in der Liste für das Portbereich-Triggering einen Namen ein.
WAN	Wählen Sie die WAN-Schnittstelle aus, über die die Trigger-Ports erkannt werden sollen.
LAN	Wählen Sie das LAN aus, in dem sich der Computer befindet und an das der weitergeleitete Datenverkehr gesendet werden soll.
Triggered Range (Ausgelöster Bereich)	Geben Sie die Start- und End-Portnummern des ausgelösten Portbereichs ein. Wenn ein lokaler Client eine ausgehende Verbindung zu einem Port in diesem Bereich herstellt, öffnet die SRP die Ports, die in den Feldern für den Weiterleitungsbereich eingegeben sind, wieder für den ursprünglichen Client. Die entsprechenden Portnummern finden Sie in der Dokumentation der Internetanwendung.

Einstellungen für das Portbereich-Triggering	
Feld	Beschreibung
Forwarded Range (Weiterleitungsbereich)	Geben Sie die Start- und End-Portnummern des Weiterleitungsbereichs ein. Diese Ports werden geöffnet, wenn eine ausgehende Verbindung mit einem der Ports, die in den Feldern für den Weiterleitungsbereich eingegeben sind, hergestellt wird. Die entsprechenden Portnummern finden Sie in der Dokumentation der Internetanwendung.
Protokoll	Wählen Sie aus der Dropdown-Liste einen Protokolltyp aus (TCP, UDP oder beide).
Enable (Aktivieren)	Klicken Sie auf Enable (Aktivieren), um die definierten Anwendungen zu aktivieren. Standardmäßig ist diese Option deaktiviert.

QoS

In diesem Abschnitt wird erläutert, wie Sie QoS-Einstellungen (Quality of Service) für die SRP konfigurieren. Folgende Themen sind enthalten:

- **QoS Bandwidth Control (QoS-Bandbreitensteuerung)**
- **QoS Policy (QoS-Richtlinie)**
- **CoS To Queue (CoS für Warteschlangen)**
- **DSCP To Queue (DSCP zu Warteschlange)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Network Setup > QoS** (Netzwerkeinrichtung > QoS).

QoS Bandwidth Control (QoS-Bandbreitensteuerung)

Über die Seite für die QoS-Bandbreitensteuerung kann die SRP die Upstream-Datenübertragungen begrenzen, um den Bestimmungen des Breitbanddienstes zu entsprechen.

-
- SCHRITT 1** Klicken Sie auf **Network Setup > QoS > Bandwidth Control** (Netzwerkeinrichtung > QoS > Bandbreitensteuerung). Das Fenster *QoS Bandwidth Control* (QoS-Bandbreitensteuerung) wird geöffnet.
- SCHRITT 2** Klicken Sie neben der Schnittstelle, für die Sie die Bandbreitensteuerung aktivieren möchten, auf **Enabled** (Aktiviert). Deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren. Standardmäßig ist diese Option deaktiviert.
- SCHRITT 3** Um die verfügbare Bandbreite für die einzelnen physischen Schnittstellen zu konfigurieren, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten). Das Fenster *Bandwidth Shaping Control* (Bandbreitengestaltungssteuerung) wird geöffnet.
- SCHRITT 4** Geben Sie die Werte für die Bandbreitengestaltungssteuerung wie in der Tabelle **Einstellungen für die Bandbreitengestaltungssteuerung** definiert ein.
- SCHRITT 5** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Einstellungen für die Bandbreitengestaltungssteuerung	
Feld	Beschreibung
Upstream Bandwidth (Upstream-Bandbreite)	Geben Sie die maximal verfügbare Upstream-Bandbreite für den verbundenen Breitbanddienst ein. Der Standardwert für Ethernet-Schnittstellen ist 100.000 Kbit/s. BEMERKUNG Wenn Sie diesen Wert höher setzen, als die verfügbare Bandbreite es zulässt, kann es passieren, dass im Netzwerk des Service Provider Datenpakete willkürlich blockiert werden.
Strict High Priority Queue (Warteschlange mit höchster Priorität)	Definiert die erforderliche Bandbreite für Datenverkehr mit höchster Priorität. Der Datenverkehr aus der Warteschlange mit der höchsten Priorität innerhalb dieser Rate, wird vor dem Datenverkehr aller anderen Warteschlangen übertragen.
High, Medium, Normal, Low (Hoch, Mittel, Normal, Niedrig)	Geben Sie die relative Priorität oder Gewichtung der Warteschlangen mit hoher, mittlerer, normaler und niedriger Priorität an. Die Warteschlangengewichtung legt die relative Menge an Bandbreite fest, die dem Datenverkehr in den jeweiligen Warteschlangen in Zeiträumen mit hohem Datenaufkommen zugesichert wird. In der Spalte für die Bandbreite wird dieser Wert unter Berücksichtigung der Bandbreite mit höchster Priorität angezeigt. Um die relative Gewichtung der Warteschlangen zu ändern, klicken Sie auf die Plus- (+) oder Minus-Schaltfläche (-). Sind keine Daten mit höchster Priorität vorhanden, werden die Daten aus diesen Warteschlangen auf der Grundlage eines gewichteten Round-Robin-Verfahrens verarbeitet. BEMERKUNG Die Bandbreitenwerte auf dieser Seite geben den geringsten zugesicherten Durchsatz an, der unter Lastbedingungen für die einzelnen Warteschlangen verfügbar ist. Höhere Verkehrsraten können ggf. verzeichnet werden, wenn andere Warteschlangen nicht voll ausgenutzt werden.

QoS Policy (QoS-Richtlinie)

Auf der Seite für die QoS-Richtlinie werden Regeln für die Klassifizierung, Warteschlangeneinrichtung und Markierung des Datenverkehrs von LAN-zu-WAN-Schnittstellen konfiguriert. Es stehen verschiedene Klassifizierungsmethoden zur Auswahl, damit der Datenverkehr jederzeit mit der richtigen Priorität versehen werden kann.

- SCHRITT 1** Klicken Sie auf **Network Setup > QoS > QoS Policy** (Netzwerkeinrichtung > QoS > QoS-Richtlinie). Das Fenster *QoS Policy* (QoS-Richtlinie) wird geöffnet.
- SCHRITT 2** Um eine vorhandene Regel zu bearbeiten, klicken Sie auf das Bleistiftsymbol für **Edit** (Bearbeiten).
- SCHRITT 3** Klicken Sie zum Hinzufügen einer neuen Richtlinie auf **Add Entry** (Eintrag hinzufügen).
- Das Fenster *QoS Priority Setting* (QoS-Prioritätseinstellung) wird geöffnet.
- SCHRITT 4** Wählen Sie aus der Dropdown-Liste die QoS-Kategorie aus (Anwendung, MAC-Adresse, Ethernet-Port oder VLAN).
- SCHRITT 5** Geben Sie die Richtlinieneinstellungen für die jeweilige Kategorie wie in der Tabelle **QoS-Richtlinieneinstellungen: Klassifizierung** definiert ein.
- SCHRITT 6** Geben Sie die QoS-Warteschlangen- und Markierungseinstellungen für die festgelegte Kategorie ein.
- SCHRITT 7** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

QoS-Richtlinieneinstellungen: Klassifizierung	
Application Category (Anwendungskategorie)	
Applications/ Name (Anwendungen/ Name)	Wählen Sie aus der Dropdown-Liste eine Standardanwendung aus. Um eine Anwendung einzugeben, die nicht in der Liste gespeichert ist, wählen Sie Add a New Application (Neue Anwendung hinzufügen) aus, und geben Sie den Namen der neuen Anwendung ein.
LAN	Wählen Sie das Quell-LAN aus.
Port Range (Portbereich)	Geben Sie den Port oder Portbereich sowie das Protokoll (TCP, UDP oder beide) ein, mit denen die erforderliche Anwendung definiert wird. Sie können bis zu drei Portbereiche pro Regel festlegen. Einzelne Ports können definiert werden, indem Sie denselben Wert für den Bereichsanfang und das Bereichsende eingeben. Weitere Informationen finden Sie in der Dokumentation der Internetanwendung.

MAC Address Category (MAC-Adresskategorie)	
Name	Geben Sie einen Namen für die Beschreibung dieser Regel ein.
LAN	Wählen Sie das Quell-LAN aus.
MAC-Adresse	Geben Sie die MAC-Adresse des Quellgeräts im folgenden Format ein: xx:xx:xx:xx:xx:xx
Ethernet Port Category (Ethernet-Portkategorie)	
Name	Geben Sie einen Namen für den Ethernet-Port ein. Beispiel: Ethernet-Port1.
LAN	Wählen Sie das Quell-LAN aus.
Ethernet	Wählen Sie den Ethernet-Quellport aus.
VLAN Category (VLAN-Kategorie)	
Name	Geben Sie den Namen des Ethernet-Ports ein. Beispiel: daten_Lan
VLAN	Wählen Sie das Quell-VLAN aus.
IP-Adresse	
Name	Geben Sie einen Namen für die Beschreibung dieser Regel ein.
Destination IP (Ziel-IP)	Geben Sie die IP-Zieladresse oder das Zielnetzwerk ein, das den Datenverkehr für diese Regel klassifiziert.
Destination Mask (Zielmaske)	Geben Sie die Maske für die IP-Zieladresse oder das Zielnetzwerk ein.
LAN	Wählen Sie das Quell-LAN aus.
QoS-Richtlinieneinstellungen: Warteschlangen	
Priorität	Wählen Sie die Warteschlangenpriorität für diesen Datenverkehr aus: Strict (Streng), High (Hoch), Medium (Mittel), Normal (Normal) oder Low (Niedrig).

CoS To Queue (CoS für Warteschlangen)

Auf der Seite **CoS To Queue** (CoS für Warteschlangen) können Sie festlegen, wie Datenverkehr auf der Grundlage von Ethernet-CoS-Einstellungen (Class of Service) in Warteschlangen eingeordnet werden soll.

SCHRITT 1 Klicken Sie auf **Network Setup > QoS > CoS To Queue** (Netzwerkeinrichtung > QoS > CoS für Warteschlangen). Das Fenster *CoS To Queue* (CoS für Warteschlangen) wird geöffnet.

SCHRITT 2 Ändern Sie die Prioritätseinstellungen für die einzelnen VLAN-CoS-Werte wie erforderlich.

Die Werte der VLAN (CoS)-Prioritätsmarkierungen (0 bis 7) werden der Router-Warteschlange zugewiesen, wobei 0 der geringste und 7 der höchste Wert ist.

SCHRITT 3 Wählen Sie aus der Dropdown-Liste eine Prioritätsebene aus.

Mit der Priorität wird die Warteschlange für die Datenweiterleitung festgelegt, der der CoS-Wert zugewiesen wird.

Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

DSCP To Queue (DSCP zu Warteschlange)

Über die Seite **DSCP To Queue** (DSCP zu Warteschlange) wird der Datenverkehr auf Grundlage des DSCP-Werts (Differentiated Services Code Point) im eingehenden Paket (DSCP) einer Warteschlange zugewiesen.

SCHRITT 1 Klicken Sie auf **Network Setup > QoS > DSCP To Queue** (Netzwerkeinrichtung > QoS > DSCP zu Warteschlange). Das Fenster *DSCP To Queue* (DSCP zu Warteschlange) wird geöffnet.

SCHRITT 2 Ändern Sie die Prioritätseinstellungen für die einzelnen IP-DiffServ-Werte wie erforderlich.

SCHRITT 3 Wählen Sie aus der Dropdown-Liste eine Prioritätsebene aus. Mit der Priorität wird die Warteschlange für die Datenweiterleitung festgelegt, der der DSCP-Wert zugewiesen wird. Zur Auswahl stehen die Prioritäten **Strict** (Streng), **High** (Hoch), **Medium** (Mittel), **Normal** (Normal) und **Low** (Niedrig).

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Firewall

In diesem Abschnitt wird erläutert, wie Sie die Firewall-Einstellungen für die SRP konfigurieren: Folgende Themen sind enthalten:

- **Firewall Filter (Firewall-Filter)**
- **Internet Access Control (Internet-Zugriffssteuerung)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Network Setup > Firewall** (Netzwerkeinrichtung > Firewall).

Firewall Filter (Firewall-Filter)

Auf der Seite für den Firewall-Filter können Sie für die SRP Firewall-Schutzfilter einrichten. Die Firewall verbessert die Netzwerksicherheit und nutzt Stateful Packet Inspection (SPI), um Datenpakete zu analysieren, die im Netzwerk eintreffen.

- SCHRITT 1** Klicken Sie auf **Network Setup > Firewall > Firewall Filter** (Netzwerkeinrichtung > Firewall > Firewall-Filter). Das Fenster *Firewall* (Firewall) wird geöffnet.
- SCHRITT 2** Wählen Sie **Enabled** (Aktiviert) aus, um den SPI-Firewall-Schutz zu aktivieren. Die Firewall ist standardmäßig aktiviert.
- SCHRITT 3** Geben Sie die Internet- und Web-Filteroptionen wie in der Tabelle **Einstellungen für den Firewall-Filter** definiert ein.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für den Firewall-Filter	
Feld	Beschreibung
SPI Firewall Protection (SPI-Firewall-Schutz)	Um einen Firewall-Schutz zu aktivieren, wählen Sie Enabled (Aktiviert) aus. Die Standardeinstellung ist Enabled (Aktiviert).

Internet Filter Options (Internet-Filteroptionen)	
Filter Anonymous Internet Requests (Anonyme Internetanfragen filtern)	Wenn Sie diese Option aktivieren, kann Ihr Netzwerk nicht „gepingt“ oder von anderen Internetbenutzern entdeckt werden. Auch Ihre Netzwerk-Ports werden ausgeblendet. Dadurch wird es externen Benutzern erschwert, in Ihr Netzwerk einzudringen. Dieser Filter ist standardmäßig aktiviert. Wählen Sie Disabled (Deaktiviert) aus, um anonyme Internetanfragen zuzulassen.
Filter Internet NAT Redirection (Internet-NAT-Umleitung filtern)	Diese Funktion hindert lokale Clients daran, über aktive Portweiterleitungsregeln auf lokale Dienste zuzugreifen (d. h. lokale Clients können nicht die öffentliche IP-Adresse des Routers verwenden, um auf lokale Dienste zuzugreifen, was ansonsten möglich wäre, wenn sie über das Internet verbunden wären). Lokale Clients können aber weiterhin über private Adressen auf einen lokalen Dienst zugreifen. Dieser Filter ist standardmäßig deaktiviert. Wählen Sie Enabled (Aktiviert) aus, um die Internet-NAT-Umleitung zu aktivieren, oder Disabled (Deaktiviert), um die Funktion zu deaktivieren.
Filter IDENT (Port 113) (Filter-IDENT (Port 113))	Verhindert, dass Port 113 von Geräten außerhalb des lokalen Netzwerks gescannt wird. Dieser Filter ist standardmäßig aktiviert. Wählen Sie Enabled (Aktiviert) aus, um Port 113 zu filtern, oder Disabled (Deaktiviert), um die Funktion zu deaktivieren.
Filter DoS Attack (DoS-Angriff filtern)	Schützt die SRP vor Denial-of-Service-Angriffen.

Web Filter Settings (Web-Filtereinstellungen)	
Proxy	Die Verwendung von WAN-Proxy-Servern kann die Sicherheit des Netzwerks beeinträchtigen. Durch Aktivierung des Proxy-Filters wird der Zugriff auf alle WAN-Proxy-Server verhindert. Um die Proxy-Filterung zu aktivieren, müssen Sie das Kontrollkästchen aktivieren. Dieser Filter ist standardmäßig deaktiviert.
Java	Java ist eine Programmiersprache für Websites. Wenn Sie Java filtern, verhindern Sie den Zugriff auf Websites im Internet, die mit dieser Programmiersprache erstellt wurden. Um die Java-Filterung zu aktivieren, müssen Sie das Kontrollkästchen markieren. Dieser Filter ist standardmäßig deaktiviert.
ActiveX	ActiveX ist eine Programmiersprache für Websites. Wenn Sie ActiveX filtern, verhindern Sie den Zugriff auf Websites im Internet, die diese Programmiersprache verwenden. Um die ActiveX-Filterung zu aktivieren, müssen Sie das Kontrollkästchen markieren. Dieser Filter ist standardmäßig deaktiviert.
Cookies (Cookies)	Cookies sind Blöcke aus Daten, die auf Ihrem Computer gespeichert und von Websites verwendet werden, wenn Sie mit diesen interagieren. Um Cookies zu filtern, müssen Sie das Kontrollkästchen markieren. Dieser Filter ist standardmäßig deaktiviert.
Filter Port (Port filtern)	Geben Sie die HTTP-Portnummer ein, die bei Verwendung einer der oben genannten Filter gescannt wird. Standardmäßig ist dies Port 80.

Internet Access Control (Internet-Zugriffssteuerung)

Auf der Seite für die Internet-Zugriffssteuerung können Sie Regeln für die Steuerung des Benutzerzugriffs auf das Internet (LAN zu WAN) festlegen.

SCHRITT 1 Klicken Sie auf **Network Setup > Firewall > Internet Access Control** (Netzwerkeinrichtung > Firewall > Internet-Zugriffssteuerung). Das Fenster *Internet Access Control* (Internet-Zugriffssteuerung) wird geöffnet.

In diesem Fenster können Sie vorhandene Richtliniendetails anzeigen, Richtlinien bearbeiten und neue Richtlinien hinzufügen.

- SCHRITT 2** Um eine Richtlinie für den Internetzugriff hinzuzufügen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster *Internet Access Control settings* (Einstellungen für die Internet-Zugriffssteuerung) für die neue Richtlinie wird geöffnet.
- SCHRITT 3** Geben Sie einen Namen für die Richtlinie für Internetzugriff ein.
- SCHRITT 4** Klicken Sie auf **Enabled** (Aktiviert), um die Internet-Zugriffssteuerung zu aktivieren.
- SCHRITT 5** Klicken Sie ggf. auf **Show Edit List** (Bearbeitungsliste anzeigen), um die Richtlinien für MAC-Adresse, IP-Adresse und IP-Adressbereich anzuzeigen.
- SCHRITT 6** Wählen Sie im Bereich für die Zeitplanung die Tage und Uhrzeiten aus, zu denen diese Richtlinie umgesetzt werden soll.
- SCHRITT 7** Wählen Sie nach Erfordernis weitere Sperroptionen aus.
- SCHRITT 8** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für die Internet-Zugriffssteuerung	
Feld	Beschreibung
Enter Policy Name (Richtliniennamen eingeben)	Geben Sie einen Namen für die Richtlinie ein.
Status	Um diese Richtlinie zu aktivieren, klicken Sie auf Enabled (Aktiviert). Um diese Richtlinie zu deaktivieren, klicken Sie auf Disabled (Deaktiviert). Standardmäßig ist diese Option deaktiviert.
From, To (Von, Bis)	Sie können die Regel auf den gesamten Datenverkehr anwenden, indem Sie From All, To All (Von: Alle, Bis: Alle) auswählen. Oder begrenzen Sie die Regel auf bestimmte Schnittstellen, z. B. From VLAN1 to WAN1 (Von VLAN1 bis WAN1).
Applied PCs (Gültige PCs) (optional)	Um die Richtlinien nur auf bestimmte Computer anzuwenden, klicken Sie auf Show Edit List (Bearbeitungsliste anzeigen). Geben Sie dann die einzelnen Computer an, indem Sie die MAC- oder IP-Adresse festlegen. Sie können auch Gruppen aus Computern festlegen, indem Sie bis zu zwei IP-Adressbereiche eingeben.

Zeitplan	
Tage	Wählen Sie aus, an welchen Tagen diese Richtlinie aktiv sein soll. Wählen Sie die einzelnen oder aber alle Tage aus. Geben Sie einen Stundenbereich mit Start- und Endzeit ein, oder wählen Sie 24 Stunden aus.
Zeiten	Wählen Sie aus, zu welchen Uhrzeiten diese Richtlinie aktiv sein soll. Geben Sie einen Stundenbereich mit Start- und Endzeit ein, oder wählen Sie 24 Stunden aus.
Aktion	
Blocking Everything (Alles blockieren)	Aktivieren Sie dieses Kontrollkästchen, um den Internetverkehr zu blockieren, der den auf dieser Seite festgelegten Kriterien entspricht. Deaktivieren Sie das Kontrollkästchen, um eine oder mehrere der anderen Filteroptionen auszuwählen.
Blocking by URL and Keyword (Nach URL und Schlüsselwörtern blockieren)	Aktivieren Sie dieses Kontrollkästchen, damit die Benutzer nicht auf bestimmte URLs oder auf URLs mit bestimmten Schlüsselwörtern zugreifen können. Geben Sie bis zu vier URLs und bis zu sechs Schlüsselwörter ein.
Blocking by Destination IP Address (Nach IP-Zieladresse blockieren)	Aktivieren Sie dieses Kontrollkästchen, damit Benutzer bestimmte IP-Adressen nicht benutzen können. Geben Sie bis zu vier IP-Adressen ein.
Blocking by Application (Nach Anwendung blockieren)	Aktivieren Sie dieses Kontrollkästchen, damit Benutzer auf bestimmte Internetdienste nicht zugreifen können, zum Beispiel FTP oder Telnet. (Pro Richtlinie können Sie bis zu drei Anwendungen blockieren.) Klicken Sie in der Anwendungsliste auf die Anwendung, die Sie blockieren möchten. Klicken Sie anschließend auf den Doppelpfeil nach rechts (>>), um die Anwendung in die Liste der blockierten Anwendungen zu verschieben. Um eine Anwendung aus der Liste der blockierten Anwendungen zu entfernen, markieren Sie sie, und klicken Sie anschließend auf den Doppelpfeil nach links (<<).

Modify Application (Anwendung bearbeiten)	Wenn die Anwendung, die Sie blockieren möchten, nicht aufgeführt wird oder Sie die Einstellungen eines Dienstes bearbeiten möchten, geben Sie den Namen der Anwendung in das Feld Application Name (Anwendungsname) ein. Geben Sie den Portbereich in das Feld Port Range (Portbereich) ein. Wählen Sie das Protokoll aus der Dropdown-Liste mit den Protokollen aus. Klicken Sie anschließend auf Add Entry (Eintrag hinzufügen). Um einen Dienst zu bearbeiten, wählen Sie ihn aus der Anwendungsliste aus. Ändern Sie den Namen, den Portbereich und/oder die Protokolleinstellungen, und klicken Sie anschließend auf das Bleistiftsymbol für Edit (Bearbeiten). Um einen Dienst zu löschen, wählen Sie ihn aus der Anwendungsliste aus. Klicken Sie dann auf das X für Delete (Löschen).
--	---

PPPoE Relay (PPPoE-Relay)

Auf der Seite für das PPPoE-Relay können Sie die Einstellungen für das PPPoE-Relay festlegen. Die PPPoE-Relay-Funktion hört bestimmte LAN-Schnittstellen auf PPP-Verkehr ab und leitet ihn an das festgelegte WAN weiter. Frames, die im WAN empfangen werden, werden per Relay an den Client zurückgesendet, der die Sitzung im LAN gestartet hat.

SCHRITT 1 Klicken Sie auf **Network Setup > PPPoE Relay** (Netzwerkeinrichtung > PPPoE-Relay). Das Fenster *PPPoE Relay* (PPPoE-Relay) wird geöffnet.

Auf dieser Seite können Sie Relays anzeigen, hinzufügen und bearbeiten.

SCHRITT 2 Klicken Sie zum Hinzufügen eines PPPoE-Relays auf **Add Entry** (Eintrag hinzufügen). Das Fenster *PPPoE Relay Add* (PPPoE-Relay hinzufügen) wird geöffnet.

SCHRITT 3 Um ein PPPoE-Relay für das Internet zu aktivieren, klicken Sie auf **Enabled** (Aktiviert).

SCHRITT 4 Wählen Sie die WAN- und LAN-Schnittstelle für diese Regel aus.

SCHRITT 5 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für das PPPoE-Relay	
Feld	Beschreibung
WAN-Schnittstelle	Wählen Sie die WAN-Schnittstelle für diese Regel aus. Beispiel: WAN1 oder WAN2.
LAN Interface (LAN-Schnittstelle)	Wählen Sie die LAN-Schnittstelle für diese Regel aus. Beispiel: VLAN1 oder VLAN100.
PPPoE Relay Status (PPPoE-Relay-Status)	Aktiviert einen L2TP-Zugriffskonzentrator (LAC), um aktive Erkennungs- und Dienstausswahlfunktionalitäten für einen Steuerkanal mit PPP over Ethernet (PPPoE über ein Layer 2 Tunneling Protocol (L2TP)) an einen L2TP-Netzwerkserver (LNS) oder Tunnel-Switch (Multihop-Knoten) weiterzuleiten. Diese Relay-Funktionalität ermöglicht es dem LNS oder Tunnel-Switch, seine angebotenen Dienste dem Client anzukündigen, sodass eine umfassende Steuerung der Dienste zwischen dem LNS und einem PPPoE-Client möglich ist.

DDNS

Auf der Seite für das dynamische DNS (DDNS) können Sie einen Internetdienst festlegen, der es Routern mit nicht statischen, öffentlichen IP-Adressen erlaubt, über Internet-Domännennamen gefunden zu werden. Wenn eine neue IP-Adresse zugewiesen wird, aktualisiert die SRP den DDNS-Dienst, um sicherzustellen, dass der zugehörige Domänenname als dieser neue Wert aufgelöst wird. Dies erleichtert den Remote-Zugriff.

HINWEIS Um DDNS verwenden zu können, müssen Sie ein Konto bei einem DDNS-Provider einrichten, zum Beispiel bei DynDNS.com oder TZO.com.

- SCHRITT 1** Klicken Sie auf **Network Setup > DDNS** (Netzwerkeinrichtung > DDNS). Das Fenster **DDNS** (DDNS) wird geöffnet.
- SCHRITT 2** Wählen Sie aus der Dropdown-Liste einen DDNS-Dienst aus. Sie können **DynDNS.org** oder **TZO.com** auswählen. Das Fenster für den DDNS-Dienst wird geöffnet.
- SCHRITT 3** Geben Sie die Informationen für den ausgewählten Dienst ein, wie in der Tabelle **Einstellungen für den DDNS-Dienst** definiert.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für den DDNS-Dienst	
Feld	Beschreibung
DDNS Service (DDNS-Dienst)	Wählen Sie aus der Dropdown-Liste den Provider für den DDNS-Dienst aus. Sie können DynDNS.org oder TZO.com auswählen. Der DDNS-Dienst ist standardmäßig deaktiviert. BEMERKUNG Sie müssen ein Konto bei einem dieser Provider eröffnen, bevor Sie den Dienst verwenden können.
DynDNS.org Settings (Einstellungen für DynDNS.org)	
Benutzername	Geben Sie den Benutzernamen von DynDNS.org ein.
Passwort	Geben Sie das Passwort von DynDNS.org ein.
Hostname	Geben Sie Ihren Hostnamen ein. Beispiel: name.dyndns.org
System	Wählen Sie den verwendeten DynDNS-Dienst aus. Sie können Dynamic (Dynamisch), Static (Statisch) oder Custom (Benutzerdefiniert) auswählen.
Mail Exchange (Mailaustausch) (optional)	Geben Sie die Adresse des Mailaustauschservers ein, sodass E-Mails, die an die DynDNS-Adresse gerichtet sind, direkt auf den Mailserver geleitet werden.

Mail Exchange (Backup MX) (Mailaustausch (Sicherung))	Diese Option gibt Ihnen die Möglichkeit, den Mailaustauschserver als Sicherung zu verwenden. Um sie zu aktivieren, wählen Sie Enabled (Aktiviert) aus. Wenn Sie nicht sicher sind, welche Einstellung am besten ist, wählen Sie Disabled (Deaktiviert) aus. Dies ist die Standardeinstellung.
Wildcard (Platzhalter)	Diese Option gibt Ihnen die Möglichkeit, in der DDNS-Adresse einen Platzhalter zu verwenden. Wenn Ihre DDNS-Adresse beispielsweise meineadresse.dyndns.org lautet und Sie die Platzhalteroption aktivieren, können Sie auch x.meineadresse.dyndns.org verwenden, wobei x der Platzhalter ist. Um Platzhalter zu aktivieren, klicken Sie auf Enabled (Aktiviert). Wenn Sie für diesen Dienst nicht angemeldet sind oder sich nicht sicher sind, wählen Sie Disabled (Deaktiviert) aus. Dies ist die Standardeinstellung.
Internet IP Address (Internet-IP-Adresse)	Zeigt die aktuelle IP-Adresse an
Status	Zeigt den DDNS-Status an
Aktualisieren	Klicken Sie auf diese Schaltfläche, um manuell eine Aktualisierung zu starten.
TZO.org Settings (Einstellungen für TZO.org)	
E-Mail-Adresse	Geben Sie die E-Mail-Adresse für Ihr TZO-Konto ein.
TZO Key (TZO-Schlüssel)	Geben Sie den Schlüssel für Ihr TZO-Konto ein.
Domain Name (Domänenname)	Geben Sie Ihren Hostnamen ein. Beispiel: name.dyndns.org
Internet IP Address (Internet-IP-Adresse)	Zeigt die aktuelle IP-Adresse an
Status	Zeigt den DDNS-Status an
Aktualisieren	Klicken Sie auf diese Schaltfläche, um manuell eine Aktualisierung zu starten.

DMZ

DMZ gibt einem lokalen Benutzer die Möglichkeit, für die Verwendung eines speziellen Diensts eine offene Verbindung zum Internet herzustellen, z. B. für ein Online-Spiel oder eine Videokonferenz. Das DMZ-Hosting leitet alle Ports gleichzeitig an einen Computer weiter. Die Weiterleitung über einen Portbereich ist sicherer, da sie nur die Ports öffnet, die geöffnet werden müssen, während durch das DMZ-Hosting alle Ports eines Computers für das Internet geöffnet werden.

Bei allen Computern, deren Ports weitergeleitet werden, muss die DHCP-Client-Funktion deaktiviert sein, und ihnen sollte eine neue statische IP-Adresse zugewiesen werden, da sich die IP-Adressen bei Verwendung der DHCP-Funktion ändern können.

SCHRITT 1 Klicken Sie auf der Registerkarte auf **Network Setup** (Netzwerkeinrichtung) und anschließend im Navigationsfenster auf **DMZ** (DMZ). Das Fenster *DMZ* (DMZ) wird geöffnet.

SCHRITT 1 Klicken Sie auf **Network Setup > DMZ** (Netzwerkeinrichtung > DMZ). Das Fenster *DMZ* (DMZ) wird geöffnet.

Auf dieser Seite können Sie vorhandene DMZ-Elemente und ihren Status anzeigen, DMZ-Elemente bearbeiten und neue hinzufügen.

SCHRITT 2 Um das DMZ-Hosting zuzulassen, verwenden Sie die Standardeinstellung, **Enabled** (Aktiviert). Wählen Sie andernfalls **Disabled** (Deaktiviert) aus.

SCHRITT 3 Geben Sie die IP-Quelladresse und die IP-Zieladresse oder MAC-Adresse an.

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Feld	Beschreibung
Status	Um diese Funktion zu aktivieren, wählen Sie Enabled (Aktiviert) aus. Um das DMZ-Hosting zu deaktivieren, klicken Sie auf Disabled (Deaktiviert).
Source IP Address (IP-Quelladresse)	Wenn eine beliebige IP-Adresse als Quelle dienen soll, wählen Sie Any IP Address (Beliebige IP-Adresse) aus. Wenn Sie eine IP-Adresse oder einen IP-Adressbereich als Quelle festlegen möchten, klicken Sie auf die zweite Optionsschaltfläche, und geben Sie die IP-Adresse(n) in die angezeigten Felder ein.

Feld	Beschreibung
Zieladresse	Um den DMZ-Host nach IP-Adresse zu bestimmen, wählen Sie die entsprechende Option aus, und geben Sie die IP-Adresse in das Feld ein. Wenn Sie den DMZ-Host nach MAC-Adresse bestimmen möchten, wählen Sie die entsprechende Option aus, und geben Sie die MAC-Adresse in das Feld ein. Um diese Informationen abzurufen, klicken Sie auf die Schaltfläche für die DHCP-Client-Tabelle.
Show DHCP Client Table (DHCP-Client-Tabelle anzeigen)	In der DHCP-Client-Tabelle werden Computer und andere Geräte angezeigt, denen der Router IP-Adressen zugewiesen hat.

IGMP (IGMP)

Auf der Seite für IGMP können Sie Einstellungen für das IGMP-Protokoll (Internet Group Management Protocol) konfigurieren. IGMP ist ein Signalprotokoll, das IP-Multicasting für IPTV unterstützt. Verwenden Sie IGMP beispielsweise, wenn Sie Internet Protocol Television (IPTV) mit mehreren Setup-Boxen nutzen, die auf demselben lokalen Netzwerk gleichzeitig verschiedene Videodatenströme übertragen.

-
- SCHRITT 1** Klicken Sie auf **Network Setup > IGMP** (Netzwerkeinrichtung > IGMP). Das Fenster *IGMP (IGMP)* wird geöffnet.
- SCHRITT 2** Um über die SRP Multicast-Datenverkehr für eine Multimedia-Anwendung zuzulassen, verwenden Sie die Standardeinstellung **Enabled** (Aktiviert).
- SCHRITT 3** Wählen Sie die Version aus, die unterstützt werden soll, **IGMP v1** oder **IGMP v2**. Wenn Sie nicht sicher sind, welche Version unterstützt werden soll, wählen Sie die Standardeinstellung IGMP v2 aus.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Feld	Beschreibung
Support IGMP Version (Unterstützte IGMP-Version)	Wählen Sie aus der Dropdown-Liste die gewünschte Version aus. Sie können IGMP v1 oder IGMP v2 auswählen. Wenn Sie nicht sicher sind, welche Version unterstützt werden soll, verwenden Sie die Standardeinstellung IGMP v2.
IGMP Proxy (IGMP-Proxy)	Um den IGMP-Proxy zu aktivieren, wählen Sie Enabled (Aktiviert) aus. Dadurch kann Multicast-Datenverkehr für Ihre Multimedia-Anwendungen über die SRP geleitet werden.
Immediate Leave (Sofort wechseln)	Wählen Sie Enabled (Aktiviert) aus, wenn Sie IPTV-Anwendungen verwenden und den Kanalwechsel ohne Verzögerung ermöglichen möchten. Verwenden Sie andernfalls die Standardeinstellung Disabled (Deaktiviert).

UPnP

Auf der Seite für UPnP können Sie das UPnP-Protokoll aktivieren. Das UPnP-Protokoll (Universal Plug and Play) gibt lokalen Geräten die Möglichkeit, die SRP zu entdecken und bestimmte Konfigurationen zu steuern.

-
- SCHRITT 1** Klicken Sie auf **Network Setup > UPnP** (Netzwerkeinrichtung > UPnP). Das Fenster *UPnP* (UPnP) wird geöffnet.
- SCHRITT 2** Um UPnP zu verwenden, wählen Sie die Standardeinstellung **Enabled** (Aktiviert) aus.
- SCHRITT 3** Konfigurieren Sie die Verwendung von UPnP anhand der Funktionen in der Tabelle **UPnP-Einstellungen**.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

UPnP-Einstellungen	
Feld	Beschreibung
UPnP	Um UPnP zu aktivieren, wählen Sie die Standardeinstellung Enabled (Aktiviert) aus. Wählen Sie andernfalls Disabled (Deaktiviert) aus.
Allow Users to Configure (Benutzerkonfiguration zulässig)	Wenn diese Option aktiviert ist (Standard), können lokale Clients UPnP verwenden, um die Konfiguration und das Verhalten der SRP zu ändern. Wenn Clients die SRP über UPnP nur erkennen sollen, wählen Sie Disabled (Deaktiviert) aus.
Keep UPnP Configurations After System Reboot (UPnP-Konfigurationen nach Systemneustart beibehalten)	Wenn diese Option aktiviert ist, speichert die SRP die von Clients vorgenommenen Konfigurationsänderungen auch über einen Systemneustart hinweg. Standardmäßig ist diese Option deaktiviert.
Allow Users to Disable Internet Access (Benutzer dürfen Internetzugriff deaktivieren)	Wenn diese Option aktiviert ist, können lokale Clients die SRP-Internetverbindung über UPnP aktivieren und deaktivieren. Standardmäßig ist diese Option deaktiviert.

CDP Setting (CDP-Einstellung)

Auf der Seite für CDP können Sie die CDP-Einstellungen (Cisco Discovery Protocol) im Netzwerk festlegen. CDP ist ein Protokoll zur Geräteerkennung auf Linkebene, das auf allen Cisco Geräten zur Verfügung steht. Alle für CDP aktivierten Geräte senden regelmäßig Nachrichten an eine Multicast-Adresse und hören die regelmäßigen Nachrichten anderer Geräte ab, um Informationen über ihre Umgebung zu sammeln.

SCHRITT 1 Klicken Sie auf **Network Setup > CDP Setting** (Netzwerkeinrichtung > CDP-Einstellung). Das Fenster *CDP Setting* (CDP-Einstellung) wird geöffnet.

Sie können CDP auf einigen, allen oder keiner der SRP-Ethernet-Schnittstellen aktivieren. Cisco empfiehlt die Standardeinstellung, **Per Port** (Nach Port), wodurch CDP nur auf LAN-Ports aktiviert wird.

SCHRITT 2 Geben Sie die CDP-Timer-Werte und die Portteilnahme wie in der Tabelle **CDP-Einstellungen** definiert an.

SCHRITT 3 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

CDP-Einstellungen

Feld	Beschreibung
CDP	Diese Option steuert, ob CDP auf einigen, allen oder keiner der SRP-Ethernet-Schnittstellen ausgeführt wird. Standardmäßig wird die CDP-Einstellung nach Port festgelegt (empfohlen).
CDP Timer (CDP-Timer)	Geben Sie an, in welchem Abstand aufeinanderfolgende CDP-Pakete gesendet werden sollen. Sie können einen Wert zwischen 5 und 900 Sekunden eingeben. Die Voreinstellung ist 60 Sekunden.
CDP Hold Timer (CDP-Halte-Timer)	Diese Option steuert, ob CDP auf einigen, allen oder keiner der SRP-Ethernet-Schnittstellen ausgeführt wird. Sie können einen Wert zwischen 10 und 255 Sekunden eingeben. Die Voreinstellung ist 80 Sekunden.
Interface List (Schnittstellenliste)	Aktivieren Sie das Kontrollkästchen, um auszuwählen, auf welchen Schnittstellen CDP ausgeführt wird.

Sprache konfigurieren

In diesem Kapitel wird die Konfiguration von Spracheinstellungen und -diensten für die Services Ready-Plattformen beschrieben. Folgende Abschnitte sind enthalten:

- **Konfigurieren von Sprachdiensten**
- **Konfigurieren von Spracheinstellungen**

Konfigurieren von Sprachdiensten

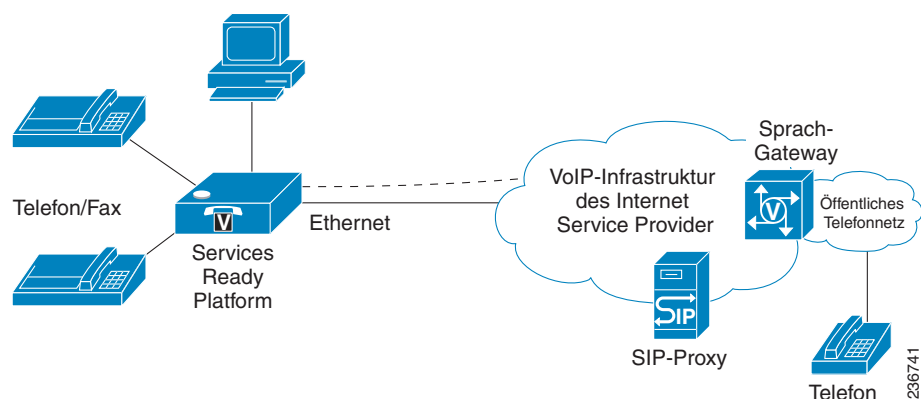
In diesem Abschnitt wird beschrieben, wie Sie Ihre SRP konfigurieren müssen, um den Ansprüchen der Kunden in Bezug auf Sprachdienste zu entsprechen. Folgende Themen sind enthalten:

- **Funktion der Sprach-Ports**
- **Verwalten von Anrufer-ID-Diensten**
- **Pausenunterdrückung und Erzeugung von Komfortaustauschen**
- **Konfigurieren von Wählplänen**
- **Umsetzung von sicheren Anrufen**

Funktion der Sprach-Ports

Die SRP520 verfügt über mehrere Sprach-Ports, die Anrufe aus lokal angeschlossenen Analogtelefonen oder Faxgeräten über SIP-basierte Internet-Telefondienste ermöglichen. Neben den vier FXS-Ports zum Anschluss von Telefonen bietet die SRP auch einen FXO-Port mit einer Leitung. Dank diesem Port können Telefonate über das Telefonnetz auch dann geführt werden, wenn ein Fehler in der Breitbandverbindung auftritt oder sogar wenn die SRP ausfällt.

Hinweis: Der SRP520-Line-Port ist eine passive Schnittstelle, die das öffentliche Telefonnetz (PSTN) im Fall von Störungen mit dem FXS-Port 1 verbindet. Unter normalen Betriebsbedingungen können Anrufe nicht dynamisch an diese Schnittstelle geleitet werden.



Die SRP erhält den Status jedes Anrufs, der über die FXS-Schnittstelle erfolgt, und reagiert entsprechend auf Benutzereingaben (beispielsweise Abheben/Auflegen (sog. On-Hook/Off-Hook) oder Rückfrage (sog. Hook-Flash)). Da die SRP das Session Initiation Protocol (SIP) verwendet, ist sie mit den meisten Internettelefonie-Angeboten der Service Provider kompatibel.

SRP-Sprachfunktionen

Die SRP verfügt über programmierbare Sprach-Ports mit vollem Funktionsumfang, die innerhalb einer großen Vielzahl von Konfigurationsparametern kundenspezifisch bereitgestellt werden können. Im folgenden Abschnitt werden die Faktoren beschrieben, die mitunter für die Sprachqualität ausschlaggebend sind:

- **Unterstützte Codecs**
- **SIP-Proxy-Redundanz**
- **Weitere SRP-Sprachfunktionen**

Unterstützte Codecs

Die SRP-Sprach-Ports unterstützen die folgenden Codecs:

Codec	Beschreibung
G.711 (A-Law und μ -Law)	Codecs mit sehr niedriger Komplexität, die nicht komprimierte, digitalisierte 64 Kbit/s-Sprachübertragungen bei einem bis zehn 5 ms-Sprach-Frames pro Paket unterstützen. Diese Codecs bieten die höchste Sprachqualität über Schmalband und nutzen die größte Bandbreite aller verfügbaren Codecs.

G.726-32	Codec mit niedriger Komplexität, der komprimierte, digitalisierte 32 Kbit/s-Sprachübertragungen bei einem bis zehn 10 ms-Sprach-Frames pro Paket unterstützt. Dieser Codec liefert eine hohe Sprachqualität.
G.729a	ITU G.729-Sprachkodierungsalgorithmus, der zur Komprimierung von digitalisierter Sprache verwendet wird. G.729a ist eine Version des G.729 mit verringerter Komplexität, der ungefähr halb so viel Verarbeitungsleistung wie G.729 benötigt. Die G.729- und G.729a-Bitströme sind zwar miteinander kompatibel und interoperabel, jedoch nicht identisch.

Der Administrator kann die jeweils bevorzugten Codecs für die Leitungen auswählen. Weitere Informationen finden Sie unter [Audiokonfiguration, Seite 192](#).

Darüber hinaus hängt die Aushandlung des optimalen Sprachcodecs in manchen Fällen davon ab, inwieweit ein Gerät einen Codec-Namen mit dem von der Gegenstelle verwendeten Codec abgleichen kann. Sie können die verschiedenen Codecs einzeln benennen, sodass die SRP den Codec mit der Gegenstelle erfolgreich aushandeln kann. Weitere Informationen finden Sie unter [Audiokonfiguration, Seite 192](#).

SIP-Proxy-Redundanz

Für gewöhnlich erfolgen in handelsüblichen IP-Telefonie-Bereitstellungen alle Anrufe über einen SIP-Proxyserver. Ein typischer SIP-Proxyserver kann tausende Teilnehmer bewältigen. Es ist wichtig, einen Backup-Server vorzusehen, sodass ein aktiver Server für Wartungsarbeiten vorübergehend ausgetauscht werden kann. Da die SRP die Verwendung von Backup-SIP-Proxyservers (über DNS SRV) unterstützt, werden Dienstausschfallzeiten gering gehalten.

Sie können die Proxy-Redundanz auf einfache Weise unterstützen, indem Sie Ihren DNS-Server mit einer Liste von SIP-Proxyadressen konfigurieren. Sie können die SRP derart instruieren, dass sie einen SIP-Proxyserver in einer in der SIP-Nachricht benannten Domäne kontaktiert. Die SRP fordert vom DNS-Server eine Liste der Hosts in der entsprechenden Domäne an, die SIP-Services bereitstellt. Wenn ein Eintrag vorhanden ist, gibt der DNS-Server einen SRV-Eintrag zurück. Dieser enthält eine Liste der SIP-Proxyserver für die Domäne samt deren Hostnamen, Priorität, Überwachungsports und ähnlichem. Die SRP versucht, die Liste der Hosts in der Reihenfolge der festgelegten Priorität zu kontaktieren.

Wenn die SRP derzeit einen Proxyserver mit niedrigerer Priorität verwendet, testet sie den Proxy mit der höheren Priorität regelmäßig, um zu sehen, ob dieser wieder am Netz ist, und schaltet nach Möglichkeit zurück zum Proxy mit der höheren Priorität. Die SIP-Proxy-Redundanz wird im Konfigurationsprogramm der Services Ready-Plattform auf den Seiten **Line** (Leitung) (1-4) konfiguriert. Weitere Informationen finden Sie unter **Seiten Line (1–2) (Leitung 1-2), Seite 174**.

Weitere SRP-Sprachfunktionen

In der folgenden Tabelle sind weitere Sprachfunktionen zusammengefasst, die von der SRP bereitgestellt werden.

Funktion	Beschreibung
Pausenunterdrückung	Mit der Funktion der Sprachpausenerkennung (VAD) mit Pausenunterdrückung kann die Anzahl der vom Netz unterstützten Anrufe erhöht werden, indem die durchschnittliche Bandbreite, die für einen einzelnen Anruf erforderlich ist, verringert wird. Die VAD bedient sich zur Unterscheidung zwischen Sprachsignalen und Nichtsprachsignalen eines komplexen Algorithmus. Auf Basis der aktuellen und bisherigen Statistik bestimmt der VAD-Algorithmus, ob es sich um Sprache handelt oder nicht. Wenn der VAD-Algorithmus festlegt, dass es sich nicht um Sprache handelt, werden die Funktionen für Pausenunterdrückung und die Erzeugung von Komfortauschen aktiviert. Hierzu wird die natürliche Stille, die bei einer Zweierverbindung für gewöhnlich auftritt, entfernt und nicht übertragen. Die IP-Bandbreite wird nur beansprucht, wenn eine Person spricht. Während der stillen Phasen eines Telefonats steht zusätzliche Bandbreite für andere Sprachanrufe oder für Datenverkehr zur Verfügung, da die stillen Pakete nicht über das Netz übertragen werden. Bei der Erzeugung von Komfortauschen wird ein weißes Hintergrundrauschen (Geräusch) künstlich erzeugt um die Anrufer zu versichern, dass die Verbindung auch während der stillen Phasen des Telefonats bestehen bleibt. Wird kein Komfortauschen eingesetzt, so denkt der Anrufer aufgrund der durch VAD und Pausenunterdrückung erzeugten „Totenstille“ möglicherweise, dass die Verbindung unterbrochen wurde.

Funktion	Beschreibung
Modem-/FAX-Passthrough	- Der Modem-Passthrough-Modus kann nur dann aktiviert werden, wenn die im Modem Line Toggle Code festgelegte Nummer vorab gewählt wird. Weitere Informationen finden Sie unter Seite Regional (Regional), Seite 150. - Der FAX-Passthrough-Modus wird aktiviert, wenn ein CED/CNG-Ton oder ein NSE-Ereignis erkannt wird. - Die Echokompensation ist im Modem-Passthrough-Modus automatisch deaktiviert. - Die Echokompensation (ECAN) ist im FAX-Passthrough-Modus deaktiviert, wenn der Parameter FAX Disable ECAN (ECAN für FAX deaktivieren) auf der Registerkarte Line 1 (Leitung 1) oder Line 2 (Leitung 2) für diese Leitung auf Yes (Ja) festgelegt ist (in diesem Fall entspricht FAX-Passthrough dem Modem-Passthrough). - Die Funktionen Anklopfen und Pausenunterdrückung sind sowohl bei FAX- als auch bei Modem-Passthrough automatisch deaktiviert. Darüber hinaus ist die Out-of-Band-DTMF-Übertragung während Modem- oder FAX-Passthrough deaktiviert.
Adaptiver Jitter-Puffer	Die SRP kann eingehende Sprachpakete puffern und somit die Auswirkungen auf variable Netzverzögerungen minimieren. Dieser Prozess wird als Jitter-Puffern bezeichnet. Die Größe des Jitter-Puffers passt sich spezifisch an die sich ändernden Netzbedingungen an. Für jede Leitung des Dienstes stellt die SRP die Kontrolleinstellung Network Jitter Level (Stärke des Jitters im Netzwerk) bereit. Die Stärke des Jitters bestimmt, wie stark die SRP versucht, den Jitter-Puffer im Verlauf der Zeit zu verkleinern, um eine niedrigere Gesamtverzögerung zu erzielen. Je stärker der Jitter, desto langsamer fällt die Verkleinerung aus. Je schwächer der Jitter, desto schneller fällt die Verkleinerung aus. Der adaptive Jitter-Puffer wird auf den Seiten Line (Leitung) konfiguriert. Weitere Informationen finden Sie unter Seiten Line (1–2) (Leitung 1-2), Seite 174.

Funktion	Beschreibung
Sichere Anrufe	Ein Benutzer kann ausgehende Anrufe durch Verschlüsseln der Audiopakete in beide Richtungen sichern, sofern er von einem Service Provider oder Administrator dazu berechtigt wurde.
Einstellbare Audio-Frames pro Paket	Mit dieser Funktion kann der Benutzer die Anzahl an Audio-Frames, die in einem RTP-Paket enthalten sind, festlegen. Pakete können 1 bis 10 Audiopakete enthalten. Mit steigender Anzahl an Paketen sinkt zwar die beanspruchte Bandbreite, allerdings wird auch die Verzögerung erhöht und die Sprachqualität möglicherweise beeinträchtigt. RTP-Pakete werden auf der Seite SIP konfiguriert. Weitere Informationen finden Sie unter Seite SIP (SIP) , Seite 131 .
DTMF-Relay	Die SRP kann DTMF-Ziffern als Out-of-Band-Ereignisse vermitteln und somit die Zifferntreue bewahren. Dadurch kann die Zuverlässigkeit der DTMF-Übertragung, die für viele IVR-Anwendungen wie DFÜ-Banking oder Fluginformationen erforderlich ist, gesteigert werden. DTMF Relay (DTMF-Relay) wird im Parameter DTMF Tx Mode (DTMF-Übertragungsmodus) auf den Seiten Lines (Leitungen) konfiguriert. Weitere Informationen finden Sie unter Seiten Line (1–2) (Leitung 1-2) , Seite 174 .
Anruffortschrittstöne	Bei der SRP können die Tonsignale zur Signalisierung des Anruffortsschritts konfiguriert werden. Diese Tonsignale werden auf der SRP lokal generiert, sodass ein Endbenutzer über den Status (beispielsweise Rückruf) informiert wird. Die Parameter für jede Tonart (beispielsweise ein Freizeichen, das einem Endbenutzer vorgespielt wird) können Frequenz und Amplitude jeder Komponente sowie Kadenzinformationen umfassen. Die Anruffortschrittstöne werden auf der Seite Regional (Regional) konfiguriert. Siehe Seite Regional (Regional) , Seite 150 .
Anruffortschrittston-Passthrough	Mit dieser Funktion kann der Benutzer die Anruffortschrittstöne (beispielsweise Ruftöne), die vom Netzwerk der Gegenstelle generiert werden, hören.

Funktion	Beschreibung
Echokompensation	Eine Impedanzabweichung zwischen Telefon und dem Telefon-Port des IP-Telefonie-Gateways kann zu einem Nahecho führen. Die SRP verfügt über eine Nahechokompensation, die eine Impedanzabweichung kompensiert. Die SRP stellt ferner eine Echosperrung mit Comfort Noise Generator (CNG) bereit, sodass Sie kein Echo mehr erkennen können. Die Echokompensation wird auf den Seiten Line (Leitung) konfiguriert. Weitere Informationen finden Sie unter Seiten Line (1–2) (Leitung 1–2), Seite 174.
Signalisieren von Rückfrageereignissen	Die SRP kann dem Proxy während eines verbundenen Anrufs Rückfrageereignisse (Hook-Flash-Ereignis) signalisieren. Mit dieser Funktion können über Mehrplatzlösungen (Third Party Call Control) erweiterte Dienste für aktive Gespräche zur Verfügung gestellt werden. Abhängig von den Funktionen, die vom Service Provider im Rahmen der Mehrplatzlösung angeboten werden, können die folgenden ATA-Funktionen deaktiviert werden, um dem Softswitch ein Hook-Flash-Ereignis korrekt zu signalisieren. ▪ Anklopf-Service: Bezieht sich auf den Parameter Call Waiting Service (Anklopfdienst) auf den Seiten Line (Leitungen). ▪ Service für Dreierkonferenz: Bezieht sich auf den Parameter Three-Way Conf Serv (Dienst für Dreierkonferenzen) auf den Seiten Line (Leitungen). ▪ Service für Dreiergespräche: Bezieht sich auf den Parameter Three-Way Call Serv (Dienst für Dreiergespräche) auf den Seiten Line (Leitungen). Sie können die für die Erkennung einer Rückfrage zulässige Zeitspanne im Rahmen des Parameters Hook Flash Timer (Hook-Flash-Timer) auf der Seite Regional (Regional) konfigurieren. Weitere Informationen finden Sie unter Seite Regional (Regional), Seite 150.

Funktion	Beschreibung
Konfigurierbarer Wählplan mit Interdigit-Timern	Die SRP bietet drei konfigurierbare Interdigit-Timer: ▪ Initial Timeout (T) (Ursprüngliche Zeitüberschreitung (T)): Signalisiert, dass das Telefon aufgelegt ist und bislang noch keine Ziffer gedrückt wurde. ▪ Long Timeout (L) (Lange Zeitüberschreitung (L)): Signalisiert das Ende einer Zifferneingabe; in diesem Fall wird keine Eingabe weiterer Ziffern mehr erwartet. ▪ Short Timeout (S) (Kurze Zeitüberschreitung (S)): Wird zwischen Ziffern verwendet; d. h. nachdem eine Ziffer gedrückt wurde, verhindert ein kurzer Zeitüberschreitungswert, dass die Ziffer ein zweites Mal erkannt wird. Weitere Informationen erhalten Sie unter Konfigurieren von Wählplänen, Seite 110.
Polaritätssteuerung	Bei der SRP können Sie die Polarität bei Anrufverbindung und Anruftrennung einstellen. Diese Funktion ist erforderlich, damit einige Fernsprechezahlensysteme und Anrufbeantworter unterstützt werden können. Die Polaritätssteuerung wird auf den Seiten Line (Leitung) konfiguriert. Weitere Informationen finden Sie unter Seiten Line (1–2) (Leitung 1-2), Seite 174.
Steuerung der anrufenden Partei	Die Steuerung der anrufenden Partei (Calling Party Control, CPC) signalisiert dem Gerät des angerufenen Teilnehmers, dass der Anrufer während einer bestehenden Verbindung aufgelegt hat, indem die Spannung zwischen a- und b-Ader vorübergehend entfernt wird. Diese Funktion ist bei automatischen Anrufbeantwortern nützlich. Diese wissen dann, wann die Verbindung zu trennen ist. Die CPC wird auf der Seite Regional (Regional) konfiguriert. Weitere Informationen finden Sie unter Seite Regional (Regional), Seite 150.

Funktion	Beschreibung
Berichtgenerierung und Ereignisprotokollierung	Die SRP stellt eine Reihe von Status- und Fehlerberichten bereit, um Service Provider bei der Problemdiagnose und Leistungsbewertung ihrer Services zu unterstützen. Die Informationen können von einem autorisierten Agenten abgerufen werden, beispielsweise über HTTP-Digest-Authentifizierung. Die Informationen können in Form einer XML-Seite oder HTML-Seite bereitgestellt werden. Die Berichtgenerierung und Ereignisprotokollierung werden auf der Seite System (System) konfiguriert. Weitere Informationen finden Sie unter Seite System (System), Seite 130.
Syslog- und Debug-Server-Einträge	Syslog- und Debug-Server-Einträge bieten ausführlichere Informationen als die Berichtgenerierung und Ereignisprotokollierung. Anhand der Konfigurationsparameter können Sie auf der SRP auswählen, welche Art von Aktivität/ Ereignissen Sie protokollieren möchten. Die Syslog- und Debug-Server ermöglichen, dass die erfassten Informationen an einen Syslog-Server gesendet werden. Syslog- und Debug-Server-Einträge werden auf der Seite System (System) konfiguriert. Weitere Informationen finden Sie unter Seite System (System), Seite 130.
SIP über TLS	Die SRP ermöglicht die Nutzung von SIP über TLS (Transport Layer Security). SIP über TLS dient dazu, böswillige Aktivitäten zu unterbinden. Zu diesem Zweck werden die SIP-Nachrichten zwischen Service Provider und Endbenutzer verschlüsselt. SIP über TLS funktioniert über das gängige standardisierte TLS-Protokoll. Bei SIP über TLS werden nur die Signalisierungsnachrichten und nicht die Medien verschlüsselt. Mit einem separaten Sicherheitsprotokoll wie Secure Real-Time Transport Protocol (SRTP) können Sprachpakete verschlüsselt werden. SIP über TLS wird im Parameter SIP Transport (SIP-Transport) auf den Seiten Line (Leitung) konfiguriert. Weitere Informationen finden Sie unter Seiten Line (1–2) (Leitung 1–2), Seite 174.

Registrieren beim Service Provider

Damit Sie einen Internet-Telefoniedienst nutzen können, müssen Sie Ihre SRP zunächst beim Internet-Telefonie Service Provider (ITSP) registrieren.

HINWEIS Dazu muss jede Leitungs-Registerkarte separat konfiguriert werden. Jede Leitungs-Registerkarte kann für einen unterschiedlichen ITSP konfiguriert werden.

- SCHRITT 1** Melden Sie sich beim Konfigurationsprogramm an. Sie werden aufgefordert, die administrativen Anmeldedaten einzugeben, die Sie von Ihrem Service Provider erhalten haben. Benutzername und Passwort lauten gemäß Standardeinstellung **admin**.
- SCHRITT 2** Klicken Sie im Menü **Voice (Sprache)** auf **Line (Line 1-2)** (Leitung 1-2), und wählen Sie die Leitungsschnittstelle aus, die Sie ändern möchten.
- SCHRITT 3** Geben Sie im Abschnitt **Proxy and Registration** (Proxy und Registrierung) den Proxy ein.
- SCHRITT 4** Geben Sie im Abschnitt **Subscriber Information** (Teilnehmerinformationen) Benutzer-ID und Passwort ein.

HINWEIS Dies sind die Mindesteinstellungen für die meisten ITSP-Verbindungen. Geben Sie die erforderlichen Kontoinformationen gemäß Ihrem ITSP ein.

- SCHRITT 5** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern. Der Sprachdienst wird neu gestartet.

SCHRITT 6 Mit den folgenden Schritten können Sie den Fortschritt überprüfen:

- a. Klicken Sie im Navigationsbereich **Voice** (Sprache) auf **Info** (Info). Blättern Sie nach unten, bis Sie zum Abschnitt **Line** (Leitung) für die von Ihnen konfigurierte Leitung gelangen. Vergewissern Sie sich, dass die Leitung registriert wurde.
 - b. Rufen Sie über ein externes Telefon die Ihnen von Ihrem ITSP zugewiesene Telefonnummer an. Wenn Sie die Standardeinstellungen nicht verändert haben, sollte das Telefon läuten. Wenn Sie abheben, können Sie ein Gespräch in Zweiwege-Audio führen.
 - c. Wenn die Leitung nicht registriert ist, aktualisieren Sie Ihren Browser mehrere Male, da es einen Moment dauern kann, bis die Registrierung abgeschlossen ist. Überprüfen Sie auch, ob der DNS korrekt konfiguriert ist.
-

Verwalten von Anrufer-ID-Diensten

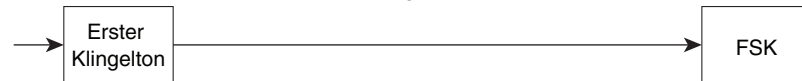
Das Verfahren zur Auswahl der Anrufer-ID (CID) hängt von Ihrem Bereich bzw. Ihrer Region ab. Sie finden diese Option auf der Seite **Sprache > Regional** im Bereich **Miscellaneous** (Weitere Bestimmungen). Sie können die CID mit den folgenden Parametern konfigurieren.

Anrufer-ID-Verfahren
Bellcore (Nordamerika, China): CID, CIDCW und VMWI. FSK wird nach erstem Klingelton gesendet (entspricht der ETSI FSK nach dem ersten Klingelton) (keine Polaritätsumkehr oder DTAS). Dies ist die Standardeinstellung.
DTMF (Finnland, Schweden) : nur CID. DTMF wird nach der Polaritätsumkehr (ohne DTAS) sowie vor dem ersten Klingelton gesendet.
DTMF (Dänemark) : nur CID. DTMF wird vor dem ersten Klingelton ohne Polaritätsumkehr und DTAS gesendet.
ETSI DTMF: nur CID. DTMF wird nach DTAS (und ohne Polaritätsumkehr) und vor dem ersten Klingelton gesendet.
ETSI DTMF mit PR: nur CID. DTMF wird nach der Polaritätsumkehr und DTAS sowie vor dem ersten Klingelton gesendet.
ETSI DTMF nach Klingelton: nur CID. DTMF wird nach dem ersten Klingelton gesendet (ohne Polaritätsumkehr oder DTAS).
ETSI FSK: CID, CIDCW und VMWI. FSK wird nach DTAS (aber ohne Polaritätsumkehr) und vor dem ersten Klingelton gesendet. Wartet auf Bestätigung von CPE nach DTAS für CIDCW.
ETSI FSK mit PR (GB): CID, CIDCW und VMWI. FSK wird nach der Polaritätsumkehr und DTAS sowie vor dem ersten Klingelton gesendet. Wartet auf Bestätigung von CPE nach DTAS für CIDCW. Polaritätsumkehr erfolgt nur, wenn das Gerät aufgelegt ist.
DTMF (Dänemark) mit PR: nur CID. DTMF wird nach der Polaritätsumkehr (ohne DTAS) sowie vor dem ersten Klingelton gesendet.
Anrufer-ID-FSK-Standard
Die SRP unterstützt Bell 202- und v.23-Standards für die Generierung von Anrufer-IDs. Legen Sie den FSK-Standard fest, den Sie verwenden möchten (Bell 202 oder v.23). Die Standardeinstellung ist Bell 202.

Es gibt drei Arten von Anrufer-IDs:

- **On-Hook-Anrufer-ID, mit Klingelton verbunden:** Diese Anrufer-ID wird für eingehende Anrufe genutzt, wenn das zugehörige Telefon aufgelegt ist. Siehe folgende Abbildungen (a) – (c). Alle CID-Verfahren können auf diese CID-Art angewandt werden.
- **On-Hook-Anrufer-ID, nicht mit Klingelton verbunden:** Diese Anrufer-ID wird verwendet, um das VMWI-Signal an das Telefon zu senden, damit die Leuchtanzeige für neue Nachrichten an- bzw. ausgeschaltet wird (siehe Abbildung 1 (d) und (e)). Diese Funktion ist nur bei FSK-basierten CID-Verfahren verfügbar (Bellcore, ETSI FSK und ETSI FSK mit PR).
- **Off-Hook-Anrufer-ID:** Diese Anrufer-ID wird verwendet, um die Anrufer-ID bei eingehenden Anrufen bereitzustellen, wenn das zugehörige Telefon abgehoben wurde (siehe folgende Abbildung). Es kann sich hierbei einerseits um die Anrufer-ID im Rahmen der Anklopffunktion (CIDCW) handeln, andererseits kann der Benutzer damit auch darüber in Kenntnis gesetzt werden, dass die Identität des Teilnehmers am anderen Ende geändert oder aktualisiert wurde (beispielsweise aufgrund einer Rufübergabe). Diese Funktion ist nur bei FSK-basierten CID-Verfahren verfügbar (Bellcore, ETSI FSK und ETSI FSK mit PR).

a) Bellcore/ETSI On-Hook-Nach-Klingelton-FSK



b) ETSI On-Hook-Nach-Klingelton-DTMF



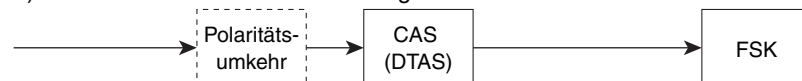
c) ETSI On-Hook-Vor-Klingelton-FSK/DTMF



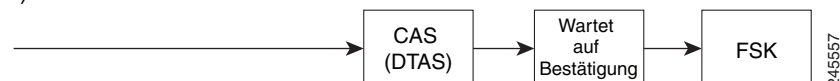
d) Bellcore On-Hook-FSK mit/ohne Klingelton



e) ETSI On-Hook-FSK mit/ohne Klingelton



f) Bellcore/ETSI Off-Hook-FSK



245557

Optimieren der Faxdurchgangsraten

Bei Faxübertragungen über IP-Netzwerke kann es sogar beim T.38-Standard, der von der SRP unterstützt wird, zu Problemen kommen. Sie können auf ihrer SRP diverse Einstellungen vornehmen, um Ihre Faxdurchgangsraten zu verbessern.

SCHRITT 1 Stellen Sie sicher, dass Sie über ausreichend Bandbreite für Uplink und Downlink verfügen.

- Für ein G.711-Fallback werden ungefähr 100 Kbit/s empfohlen.
- Planen Sie für T.38 zumindest 50 Kbit/s ein.

SCHRITT 2 Sie können auf Ihrer SRP auf der Registerkarte **Line** (Leitung) die folgenden Einstellungen vornehmen, um die G.711-Fallback-Faxdurchgangsraten zu optimieren:

- **Network Jitter Buffer (Netzwerk-Jitter-Puffer):** sehr hoch
- **Jitter buffer adjustment (Jitter-Puffer-Anpassung):** deaktivieren
- **Call Waiting (Anklopfen):** aus
- **3 Way Calling (3-Wege-Anruf):** aus
- **Echo Cancellor (Echokompensation):** aus
- **Silence suppression (Pausenunterdrückung):** aus
- **Preferred Codec (Bevorzugter Codec):** G.711
- **Use pref. codec only (Nur bevorzugten Codec verwenden):** ja

Wenn Sie für die PSTN-Terminierung einen Cisco Media Gateway verwenden, deaktivieren Sie T.38 (Fax-Relay) und aktivieren Sie das Modem-Passthrough. Beispiel:

```
modem passthrough nse payload-type 110 codec g711ulaw
fax rate disable
fax protocol passthrough g711ulaw
```

SCHRITT 3 Aktivieren Sie das T.38-Fax auf der SRP. Konfigurieren Sie dazu auf der Registerkarte **Line** (Leitung) für den FXS-Port, an den das FAX-Gerät angeschlossen ist, die folgenden Parameter:

```
FAX_Passthru_Method: ReINVITE
```

HINWEIS Wenn der Aufbau eines T.38-Anrufs fehlschlägt, kehrt der Anruf automatisch zum G.711-Fallback zurück.

SCHRITT 4 Wenn Sie einen Cisco Media Gateway verwenden, nehmen Sie die folgenden Einstellungen vor:

Vergewissern Sie sich, dass das Cisco Gateway für T.38 mit dem SPA-Dial Peer korrekt konfiguriert wurde. Beispiel:

```
fax protocol T.38
fax rate voice
fax-relay ecm disable
fax nsf 000000
no vad
```

Fehlerbehebung: Fax

Wenn Sie Probleme beim Senden oder Empfangen von Faxnachrichten haben, gehen Sie wie folgt vor:

SCHRITT 1 Vergewissern Sie sich, dass Ihr Faxgerät auf eine Geschwindigkeit zwischen 7200 und 14400 eingestellt ist.

SCHRITT 2 Senden Sie ein Testfax in einer kontrollierten Umgebung zwischen zwei ATAs.

SCHRITT 3 Ermitteln Sie die Erfolgsrate.

SCHRITT 4 Überwachen Sie das Netzwerk, und führen Sie eine Statistik für Jitter, Verlust und Verzögerung.

SCHRITT 5 Wenn das Senden und Empfangen von Faxen nur teilweise nicht funktioniert, machen Sie eine Kopie der SRP-Konfiguration. Laden Sie dazu die folgende Datei herunter. Sie können diese dann an den technischen Support senden.

http://<SRP_IP_Address>/admin/config.xml&xuser=admin&xpassword=<admin_password>

Wenn Sie einen Webbrowser verwenden, wählen Sie die Option **view source** (Quelle anzeigen) für die nächste Seite, und speichern Sie diese Datei lokal.

SCHRITT 6 Aktivieren und zeichnen Sie die Debug-Liste auf.

HINWEIS Sie können Daten auch über einen Sniffer aufzeichnen.

SCHRITT 7 Identifizieren Sie den Typ des Faxgeräts, das an das Gerät angeschlossen ist.

SCHRITT 8 Wenden Sie sich an den technischen Support:

- Wenn Sie ein Endbenutzer von VoIP-Produkten sind, wenden Sie sich an den Vertriebspartner oder den Internet-Telefonie Service Provider (ITSP), der die Geräte zur Verfügung gestellt hat.
 - Wenn Sie ein autorisierter Cisco Partner sind, wenden Sie sich unter www.cisco.com/support an den technischen Support von Cisco.
-

Pausenunterdrückung und Erzeugung von Komfortauschen

Mit der Funktion der Sprachpausenerkennung (VAD) mit Pausenunterdrückung kann die Anzahl der vom Netz unterstützten Anrufe erhöht werden, indem die Bandbreite, die für einen einzelnen Anruf erforderlich ist, verringert wird. Die VAD bedient sich zur Unterscheidung zwischen Sprachsignalen und Nichtsprachsignalen eines komplexen Algorithmus. Auf Basis der aktuellen und bisherigen Statistik bestimmt der VAD-Algorithmus, ob es sich um Sprache handelt oder nicht. Wenn der VAD-Algorithmus festlegt, dass es sich nicht um Sprache handelt, werden die Funktionen für Pausenunterdrückung und die Erzeugung von Komfortauschen aktiviert. Dabei wird die Übertragung der natürlichen Stille, die bei einer Zweierverbindung für gewöhnlich auftritt, unterdrückt. Die IP-Bandbreite wird daher nur beansprucht, wenn eine Person spricht. Während der stillen Phasen eines Telefonats steht zusätzliche Bandbreite für andere Sprachanrufe oder für Datenverkehr zur Verfügung, da die stillen Pakete nicht über das Netz übertragen werden.

Bei der Erzeugung von Komfortauschen wird ein weißes Hintergrundrauschen (Geräusch) künstlich erzeugt um die Anrufer zu versichern, dass die Verbindung auch während der stillen Phasen des Telefonats bestehen bleibt. Wird kein Komfortauschen eingesetzt, so denkt der Anrufer aufgrund der durch VAD und Pausenunterdrückung erzeugten „Totenstille“ möglicherweise, dass die Verbindung unterbrochen wurde.

Die Pausenunterdrückung wird auf den Seiten **Line (1-2)** (Leitung 1-2) konfiguriert. Registerkarten. Weitere Informationen finden Sie unter **Seiten Line (1-2) (Leitung 1-2), Seite 174**.

Konfigurieren von Wählplänen

Wählpläne bestimmen, wie gewählte Ziffern interpretiert und übertragen werden. Darüber hinaus legen sie fest, ob die gewählte Nummer akzeptiert oder zurückgewiesen wird. Mit einem Wählplan können Sie den Wählvorgang vereinfachen oder gewisse Anruftypen wie Ferngespräche oder internationale Anrufe blockieren. Dieser Abschnitt enthält Informationen, die Sie zum Verständnis von Wählplänen benötigen. Ferner sind Verfahren beschrieben, mit denen Sie Ihre eigenen Wählpläne konfigurieren können. Dieser Abschnitt enthält die folgenden Themen:

- **Allgemeines zu Wählplänen**
- **Bearbeiten von Wählplänen**

Allgemeines zu Wählplänen

Dieser Abschnitt enthält Informationen darüber, wie Wählpläne umgesetzt werden. Entsprechende Informationen finden Sie unter folgenden Themen:

- **Zahlenfolgen**
- **Beispiele für Ziffernfolgen**
- **Annahme und Übertragung der gewählten Ziffern**
- **Wählplan-Timer (Off-Hook-Timer)**
- **Langer Inter-Digit-Timer (Timer für unvollständige Eingaben)**
- **Kurzer Inter-Digit-Timer (Timer für vollständige Eingaben)**

Zahlenfolgen

Ein Wählplan umfasst eine Reihe aus Zeichenfolgen, die durch das Zeichen „|“ voneinander getrennt sind. Die Gesamtheit der Folgen wird durch Klammern begrenzt. Jede Zahlenfolge innerhalb des Wählplans enthält eine Reihe von Elementen, die den vom Benutzer gedrückten Tasten individuell zugewiesen sind.

HINWEIS Leerzeichen werden ignoriert, können aber zur Verbesserung der Lesbarkeit verwendet werden.

Zahlenfolge	Funktion
0 1 2 3 4 5 6 7 8 9 0 * #	Geben Sie ein beliebiges dieser Zeichen ein, um eine Taste festzulegen, die der Benutzer auf der Telefontastatur drücken muss.
x	Geben Sie x ein, um es für eine beliebige Taste auf der Telefontastatur festzulegen.
[Folge]	Geben Sie Zeichen in eckigen Klammern ein, um eine Liste akzeptierter Tasteneingaben festzulegen. Der Benutzer kann eine beliebige der in der Liste angeführten Tasten drücken. ▪ Numerischer Bereich: Wenn Sie beispielsweise [2-9] eingeben, kann der Benutzer eine Ziffer zwischen 2 und 9 drücken. ▪ Numerischer Bereich mit anderen Zeichen: Wenn Sie beispielsweise [35-8*] eingeben, kann der Benutzer 3, 5, 6, 7, 8 oder * drücken.
. (Punkt)	Geben Sie einen Punkt für die Elementwiederholung ein. Der Wählplan akzeptiert null oder mehrere Eingaben der jeweiligen Ziffer. Bei 01. beispielsweise kann der Benutzer 0, 01, 011, 0111 usw. eingeben.
<dialled:substituted>	Mit diesem Format können Sie anzeigen, dass gewisse gewählte Ziffern durch andere Zeichen ersetzt werden, wenn die Folge übertragen wird. Die gewählten Ziffern können aus null oder mehreren Zeichen bestehen. BEISPIEL 1: <8:1650>xxxxxxxx Wenn der Benutzer 8 und danach eine siebenstellige Zahl eingibt, dann wird die gewählte 8 vom System automatisch durch 1650 ersetzt. Wenn der Benutzer 85550112 wählt, überträgt das System 16505550112. BEISPIEL 2: <:1>xxxxxxxxxxxx In diesem Beispiel werden keine Ziffern ersetzt. Wenn der Benutzer eine 10-stellige Zahlenfolge eingibt, wird die Zahl 1 am Beginn der Folge hinzugefügt. Wenn der Benutzer 9725550112 wählt, überträgt das System 19725550112.

Zahlenfolge	Funktion
, (Komma)	Setzen Sie zwischen Ziffern ein Komma, um nach der vom Benutzer eingegebenen Folge einen Wählton für eine „Amtsleitung“ abzuspielen. BEISPIEL: 9, 1xxxxxxxxxx Der Wählton für eine „Amtsleitung“ ertönt, nachdem der Benutzer 9 gedrückt hat, und wird beendet, wenn der Benutzer 1 drückt.
! (Ausrufezeichen)	Mit einem Ausrufezeichen können Sie ein Muster einer Wählfolge verbieten. BEISPIEL: 1900xxxxxxxx! Das System weist jede 11-stellige Folge zurück, die mit 1900 beginnt.
*xx	Geben Sie ein Sternchen ein, um dem Benutzer die Eingabe eines 2-stelligen Sternchencodes zu ermöglichen.
S0 oder L0	Mit S0 können Sie den kurzen Inter-Digit-Timer auf 0 Sekunden verringern, mit L0 den langen Inter-Digit-Timer.

Beispiele für Ziffernfolgen

In den folgenden Beispielen sind Ziffernfolgen angeführt, die Sie in einen Wählplan eingeben können.

Bei einer vollständigen Wählplaneingabe werden die Folgen durch einen senkrechten Strich (|) voneinander getrennt, und der gesamte Satz von Folgen steht in Klammern.

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

Nebenstellen auf Ihrem System

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

[1-8]xx Ermöglicht einem Benutzer die Eingabe einer beliebigen 3-stelligen Nummer, die mit einer Ziffer zwischen 1 und 8 beginnt. Wenn Ihr System 4-stellige Nebenstellen verwendet, geben Sie stattdessen diese Folge ein: **[1-8]xxx**.

Lokale Einwahl mit 7-stelliger Nummer

BEISPIEL: ([1-8]xx | 9, **xxxxxxx** | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]111)

9, xxxxxxxx Nachdem ein Benutzer 9 gedrückt hat, ertönt der externe Wählton. Der Benutzer kann dann eine beliebige 7-stellige Nummer wählen, wie bei einem lokalen Anruf.

Lokale Einwahl mit 3-stelliger Ortsvorwahl und einer 7-stelligen lokalen Nummer

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]**xxxxxxxxx** | 8, <:1212>xxxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

9, <:1>[2-9]xxxxxxxxx Dieses Beispiel ist nützlich, wenn eine Ortsvorwahl erforderlich ist. Nachdem ein Benutzer 9 gedrückt hat, ertönt der externe Wählton. Der Benutzer muss eine 10-stellige Nummer eingeben, die mit einer Ziffer zwischen 2 und 9 beginnt. Das System fügt das Präfix 1 automatisch ein, bevor die Nummer an den Betreiber übertragen wird.

Lokale Einwahl mit automatisch eingefügter 3-stelliger Ortsvorwahl

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>**xxxxxxxxx** | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

8, <:1212>xxxxxxxxx Dieses Beispiel ist nützlich, wenn der Betreiber die Eingabe einer lokalen Ortsvorwahl erfordert, die Mehrheit der Anrufe aber auf eine Ortsvorwahl laufen. Nachdem der Benutzer 8 gedrückt hat, ertönt ein externer Wählton. Der Benutzer kann eine beliebige 7-stellige Nummer eingeben. Das System fügt das Präfix 1 und die Ortsvorwahl 212 automatisch ein, bevor die Nummer an den Betreiber übertragen wird.

USA: Ferngespräche

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxxxx | 9, 1 [2-9] **xxxxxxxxx** | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | 0 | [49]11)

9, 1 [2-9] xxxxxxxxxxxx Nachdem der Benutzer 9 gedrückt hat, ertönt der externe Wählton. Der Benutzer kann eine beliebige 11-stellige Nummer eingeben, die mit 1 beginnt und auf die eine Ziffer zwischen 2 und 9 folgt.

Blockierte Nummern

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxx | 8, <:1212>xxxxxxxxx | 9, 1 [2-9] xxxxxxxxxxxx | 9, 1 900 **xxxxxxxx** ! | 9, 011xxxxxx. | 0 | [49]11)

9, 1 900 xxxxxxxx ! Diese Ziffernfolge ist nützlich, wenn Sie Benutzer daran hindern möchten, Nummern zu wählen, die mit hohen Gebühren oder unangemessenem Inhalt verbunden sind, beispielsweise die 1-900er-Nummern in den USA. Nachdem der Benutzer 9 gedrückt hat, ertönt der externe Wählton. Wenn der Benutzer eine 11-stellige Nummer eingibt, die mit den Ziffern 1900 beginnt, wird der Anruf zurückgewiesen.

USA: Internationale Anrufe

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | **9, 011xxxxxx.** | 0 | [49]11)

9, 011xxxxxx. Nachdem der Benutzer 9 gedrückt hat, ertönt ein externer Wählton. Der Benutzer kann eine beliebige Nummer eingeben, die mit 011 beginnt, wie beispielsweise bei internationalen Anrufen aus den USA.

Informationsgespräche

BEISPIEL: ([1-8]xx | 9, xxxxxxxx | 9, <:1>[2-9]xxxxxxxxxx | 8, <:1212>xxxxxxxx | 9, 1 [2-9] xxxxxxxxxxx | 9, 1 900 xxxxxxxx ! | 9, 011xxxxxx. | **0 | [49]11**)

0 | [49]11 Dieses Beispiel enthält 2-stellige Folgen, die durch einen senkrechten Strich voneinander getrennt sind. Mit der ersten Folge kann ein Benutzer 0 für einen Betreiber wählen. Mit der zweiten Folge kann der Benutzer 411 für lokale Informationen oder 911 für Notrufdienste eingeben.

Annahme und Übertragung der gewählten Ziffern

Wenn ein Benutzer eine Reihe von Ziffern wählt, wird jede Folge im Wählplan als potenzielle Übereinstimmung getestet. Die übereinstimmenden Folgen bilden einen Satz aus Kandidaten-Ziffernfolgen. Je mehr Ziffern der Benutzer eingibt, desto stärker verringert sich der Kandidatensatz, bis nur eine oder keine gültigen vorhanden sind. Wenn ein Terminierungsereignis auftritt, akzeptiert die SRP die vom Benutzer eingegebene Folge und initiiert einen Anruf oder weist die Folge als ungültig zurück. Wenn die gewählte Folge ungültig ist, ertönt ein Reorder-Ton (schnelles Besetztzeichen).

In der folgenden Tabelle wird erläutert, wie Terminierungsereignisse verarbeitet werden.

Terminierungsereignis	Verarbeitung
Die gewählten Ziffern stimmen mit keiner Folge im Wählplan überein.	Die Nummer wird zurückgewiesen.
Die gewählten Ziffern stimmen genau mit einer Folge im Wählplan überein.	▪ Wenn die Folge laut Wählplan zulässig ist, wird die Nummer akzeptiert und gemäß Wählplan übertragen. ▪ Wenn die Folge laut Wählplan blockiert ist, wird die Nummer zurückgewiesen.
Eine Zeitüberschreitung tritt auf.	Die Nummer wird zurückgewiesen, wenn innerhalb des vom entsprechenden Inter-Digit-Timer festgelegten Zeitraums für die gewählten Ziffern im Wählplan keine Ziffernfolge als Entsprechung gefunden werden kann. ▪ Der lange Inter-Digit-Timer kommt zur Anwendung, wenn die gewählten Ziffern mit keiner Ziffernfolge im Wählplan übereinstimmen. Der Standardwert ist 10 Sekunden. ▪ Der kurze Inter-Digit-Timer wird verwendet, wenn die gewählten Ziffern mit einer oder mehreren Kandidatenfolgen im Wählplan übereinstimmen. Der Standardwert ist 3 Sekunden.
Der Benutzer drückt die #-Taste.	▪ Wenn die Folge vollständig und laut Wählplan zulässig ist, wird die Nummer akzeptiert und gemäß Wählplan übertragen. ▪ Wenn die Folge unvollständig oder laut Wählplan blockiert ist, wird die Nummer zurückgewiesen.

Wählplan-Timer (Off-Hook-Timer)

Sie können sich den Wählplan-Timer als Off-Hook-Timer vorstellen. Dieser Timer startet mit dem Zählen, wenn das Telefon abgehoben wird. Wenn innerhalb der festgelegten Anzahl von Sekunden keine Ziffern gewählt werden, läuft der Timer ab und die Nulleingabe wird evaluiert. Wenn Sie keine spezielle Wählplanfolge für eine zulässige Nulleingabe festgelegt haben, wird der Anruf zurückgewiesen. Der Standardwert ist 5.

Syntax für den Wählplan-Timer

SYNTAX: (*P**S*<:*n*> | *Wählplan*)

- *s*: Anzahl von Sekunden; wenn nach *P* keine Nummer mehr eingegeben wird, kommt der Standardtimer von 5 Sekunden zur Anwendung.
- *n*: (optional): Die Nummer zur automatischen Übertragung, wenn der Timer abläuft; Sie können eine gültige Nummer eingeben. Es sind keine Platzhalter zulässig, da die Nummer wie angezeigt übertragen wird. Wenn Sie die Nummernsubstitution <*n*> auslassen, dann ertönt nach der festgelegten Anzahl an Sekunden ein Reorder-Ton (schnelles Besetztzeichen).

Beispiele für den Wählplan-Timer

- **Räumen Sie den Benutzern mehr Zeit ein, um mit dem Wählen zu beginnen, nachdem der Hörer abgenommen wurde.**

BEISPIEL: (*P***9** | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2 9]xxxxxxxxxx | 9,8,011xx. | 9,8,xx.|[1-8]xx)

P9 Nachdem der Benutzer das Telefon abgehoben hat, bleiben ihm 9 Sekunden, um mit dem Wählen zu beginnen. Wenn innerhalb der 9 Sekunden keine Ziffern gedrückt werden, ertönt ein Reorder-Ton (schnelles Besetztzeichen). Wenn Sie einen längeren Zeitraum einstellen, haben die Benutzer mehr Zeit, um die Ziffern einzugeben.

- **Erstellen einer Hotline für alle Folgen am Systemwählplan**

BEISPIEL: (*P***9<:23>** | (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8.011xx. | 9,8,xx.|[1-8]xx)

P9<:23> Nachdem der Benutzer das Telefon abgehoben hat, bleiben ihm 9 Sekunden, um mit dem Wählen zu beginnen. Wenn innerhalb der 9 Sekunden keine Ziffern gedrückt werden, wird der Anruf automatisch an die Nebenstelle 23 weitergeleitet.

- **Erstellen einer Hotline auf einer Schaltfläche Line (Leitung) für eine Nebenstelle**

BEISPIEL: (*P***0 <:1000>**)

Wenn Sie den Timer auf 0 Sekunden einstellen, wird der Anruf beim Abheben des Telefons automatisch an die festgelegte Nebenstelle weitergeleitet.

Langer Inter-Digit-Timer (Timer für unvollständige Eingaben)

Sie können sich diesen Timer als Timer für unvollständige Eingaben vorstellen. Dieser Timer misst das Intervall zwischen gewählten Ziffern. Dieser wird angewandt, solange die gewählten Ziffern mit keiner Ziffernfolge im Wählplan übereinstimmen. Wenn der Benutzer innerhalb der festgelegten Anzahl von Sekunden keine weitere Ziffer eingibt, wird die Eingabe als unvollständig bewertet und der Anruf zurückgewiesen. Der Standardwert ist 10 Sekunden.

HINWEIS In diesem Abschnitt wird erklärt, wie Sie einen Timer im Rahmen eines Wählplans bearbeiten können. Alternativ können Sie den Kontrolltimer ändern, der die standardmäßigen Inter-Digit-Timer für alle Anrufe steuert. Weitere Informationen finden Sie unter [Zurücksetzen der Kontrolltimer, Seite 119](#).

Syntax für den langen Inter-Digit-Timer

SYNTAX: `L:S, ( Wählplan)`

s: Anzahl von Sekunden; wenn nach `L`: keine Nummer mehr eingegeben wird, kommt der Standardtimer von 5 Sekunden zur Anwendung. Die Timerfolge wird links neben der öffnenden Klammer für den Wählplan angezeigt.

Beispiel für den langen Inter-Digit-Timer

BEISPIEL: `L:15, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8.011xx. | 9,8,xx. | [1-8]xx)`

L:15, Mit diesem Wählplan kann der Benutzer zwischen der Eingabe von Ziffern bis zu 15 Sekunden Pause einlegen, bevor der lange Inter-Digit-Timer abläuft.

Kurzer Inter-Digit-Timer (Timer für vollständige Eingaben)

Sie können sich diesen Timer als Timer für vollständige Eingaben vorstellen. Dieser Timer misst das Intervall zwischen gewählten Ziffern. Er wird angewandt, solange die gewählten Ziffern mit zumindest einer Ziffernfolge im Wählplan übereinstimmen. Wenn der Benutzer innerhalb der festgelegten Anzahl von Sekunden keine weitere Ziffer eingibt, wird die Eingabe evaluiert. Wenn die Eingabe gültig ist, wird der Anruf fortgesetzt. Wenn Sie nicht gültig ist, wird der Anruf zurückgewiesen. Der Standardwert ist 3 Sekunden.

Syntax für den kurzen Inter-Digit-Timer

SYNTAX 1: S:s, (Wählplan)

Mit dieser Syntax können Sie die neuen Einstellungen auf den gesamten Wählplan in Klammern anwenden.

• **SYNTAX 2:** Folge Ss

Mit dieser Syntax können Sie die neuen Einstellungen auf eine bestimmte Wählfolge anwenden.

s: Anzahl von Sekunden; wenn nach s keine Nummer mehr eingegeben wird, kommt der Standardtimer von 5 Sekunden zur Anwendung.

Beispiele für den kurzen Inter-Digit-Timer

- Stellen Sie den Timer für den gesamten Wählplan ein.

BEISPIEL: **S:6**, (9,8<:1408>[2-9]xxxxxx | 9,8,1[2-9]xxxxxxxxxx | 9,8.011xx.
| 9,8,xx.|[1-8]xx)

S:6, Wenn der Benutzer eine Nummer bei abgehobenem Telefon eingibt, kann er zwischen der Eingabe der Ziffern eine Pause von bis zu 15 Sekunden einlegen, bevor der kurze Inter-Digit-Timer abläuft.

- Legen Sie einen Instant-Timer für eine bestimmte Folge im Wählplan fest.

BEISPIEL: (9,8<:1408>[2-9]xxxxxx | **9,8,1[2-9]xxxxxxxxxS0** | 9,8.011xx.
| 9,8,xx.|[1-8]xx)

9,8,1[2-9]xxxxxxxxxS0 Wenn der Timer auf 0 eingestellt ist, wird der Anruf automatisch weitergeleitet, nachdem der Benutzer die letzte Ziffer der Sequenz gewählt hat.

Bearbeiten von Wählplänen

Sie können Wählpläne bearbeiten und die Kontrolltimer ändern.

Eingeben des Wählplans für Leitungsschnittstellen

Mit diesem Wählplan können Sie Leitziffern aus einer gewählten Nummer entfernen, bevor Sie an den Betreiber übertragen wird.

-
- SCHRITT 1** Melden Sie sich beim Konfigurationsprogramm an. Sie werden aufgefordert, die administrativen Anmeldedaten einzugeben, die Sie von Ihrem Service Provider erhalten haben. Benutzername und Passwort lauten gemäß Standardeinstellung **admin**.
- SCHRITT 2** Klicken Sie im Menü **Voice** (Sprache) auf **Line (Line 1-2)** (Leitung 1-2), und wählen Sie die Leitungsschnittstelle aus, die Sie ändern möchten.
- SCHRITT 3** Blättern Sie nach unten, bis Sie zum Abschnitt *Dial Plan* (Wählplan) gelangen.
- SCHRITT 4** Geben Sie die Ziffernfolgen im Feld **Dial Plan** (Wählplan) ein. Weitere Informationen finden Sie unter **Allgemeines zu Wählplänen, Seite 110**.
- SCHRITT 5** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Zurücksetzen der Kontrolltimer

Mit dem folgenden Verfahren können Sie die Standardeinstellungen der Timer für alle Anrufe zurücksetzen.

-
- HINWEIS** Bearbeiten Sie den Wählplan, um eine Timereinstellung für nur eine bestimmte Ziffernfolge oder einen bestimmten Anruftyp zu bearbeiten. Weitere Informationen finden Sie unter **Allgemeines zu Wählplänen, Seite 110**.
-

-
- SCHRITT 1** Melden Sie sich beim Konfigurationsprogramm an. Sie werden aufgefordert, die administrativen Anmeldedaten einzugeben, die Sie von Ihrem Service Provider erhalten haben. Benutzername und Passwort lauten gemäß Standardeinstellung **admin**.
- SCHRITT 2** Klicken Sie im Menü **Voice** (Sprache) auf **Regional** (Regional).
- SCHRITT 3** Blättern Sie nach unten, bis Sie zum Abschnitt *Control Timer Values* (Kontrolltimerwerte) gelangen.
- SCHRITT 4** Geben Sie in den Feldern *Interdigit Long Timer* (Langer Inter-Digit-Timer) und *Interdigit Short Timer* (Kurzer Inter-Digit-Timer) die gewünschten Werte ein. Schlagen Sie hierzu in den Definitionen zu Beginn dieses Abschnitts nach.
-

Umsetzung von sicheren Anrufen

In diesem Abschnitt wird die Umsetzung von sicheren Anrufen mit der SRP beschrieben. Folgende Abschnitte sind enthalten:

- **Aktivieren von sicheren Anrufen**
- **Ausführliche Informationen zu sicheren Anrufen**
- **Verwendung von Mini-Zertifikaten**
- **Erzeugen von Mini-Zertifikaten**

HINWEIS Es handelt sich hierbei um ein Thema, das nur für erfahrene Installationsanwender gedacht ist.

Aktivieren von sicheren Anrufen

Ein sicherer Anruf wird in zwei Schritten umgesetzt. Der erste Schritt unterscheidet sich nicht vom normalen Verbindungsaufbau. Der zweite Schritt beginnt nach dem normalen Verbindungsaufbau, wenn beide Seiten zum Streamen von RTP-Paketen bereit sind.

Beim zweiten Schritt erfolgt zwischen beiden Parteien ein Informationsaustausch, um zu bestimmen, ob der aktuelle Anruf in den sicheren Modus geschaltet werden kann. Die Informationen werden mittels in den Nachrichtentext von SIP-INFO-Anfragen eingebetteter base64-Kodierung übertragen, und die Antworten werden in einem proprietären Format übertragen. Wenn die zweite Stufe erfolgreich war, gibt die SRP kurz einen speziellen kurzen Hinweistext aus, um beiden Parteien zu signalisieren, dass der Anruf nun sicher ist und der RTP-Verkehr in beiden Richtungen verschlüsselt wird.

Wenn das Telefon des Benutzers die Anrufer-ID im Rahmen der Anklopffunktion (CIDCW) unterstützt und dieser Dienst aktiviert ist, wird die CID mit den aus dem Mini-Zertifikat der Gegenseite extrahierten Informationen aktualisiert. Dem Feld **Name** (Name) der CID wird ein \$-Symbol vorangestellt. Beide Parteien können Namen und Nummer verifizieren, um die Identität der Gegenseite sicherzustellen.

Der signierende Agent ist implizit und muss für alle Geräte, die auf sicherem Wege miteinander kommunizieren, gleich sein. Der öffentliche Schlüssel des signierenden Agenten wird vom Administrator in der SRP vorkonfiguriert. Mit diesem Schlüssel verifiziert die SRP das Mini-Zertifikat ihres Peers. Das Mini-Zertifikat ist gültig, wenn es noch nicht abgelaufen ist und eine gültige Signatur aufweist.

Die Standardkonfiguration der SRP kann derart eingestellt werden, dass alle ausgehenden Anrufe entweder sicher oder nicht sicher sind. Bei standardmäßig sicheren Anrufen kann der Benutzer die Sicherheit deaktivieren. Hierzu muss er vor der Eingabe der Zielnummer *19 drücken. Bei standardmäßig nicht sicheren Anrufen kann der Benutzer einen sicheren ausgehenden Anruf führen. Hierzu muss er vor der Eingabe der Zielnummer *18 drücken. Der Benutzer kann die Sicherheit von eingehenden Anrufen allerdings nicht festlegen. Dies hängt allein davon ab, ob der Anrufer die Sicherheit aktiviert oder deaktiviert hat.

Die SRP geht nicht in den sicheren Modus über, wenn die CID des Mini-Zertifikats der angerufenen Partei nicht mit der beim ausgehenden Anruf verwendeten Benutzer-ID übereinstimmt. Die SRP führt diese Überprüfung durch, nachdem sie das Mini-Zertifikat von der angerufenen Partei erhalten hat.

Ausführliche Informationen zu sicheren Anrufen

Der zweite Schritt des Aufbaus eines sicheren Anrufs kann bei genauerer Betrachtung in zwei weitere Schritte unterteilt werden.

SCHRITT 1 Der Anrufer sendet eine „Caller Hello“-Nachricht (base64-kodiert und in den Nachrichtentext einer SIP-INFO-Anfrage eingebettet) an die angerufene Partei, die die folgenden Informationen enthält:

- Nachrichten-ID (4B)
- Version und Markierungen (4B)
- SSRC des verschlüsselten Stroms (4B)
- Mini-Zertifikat (252B)

Nach Erhalt einer gültigen „Caller Hello“-Nachricht antwortet die angerufene Partei mit einer „Callee Hello“-Nachricht (base64-kodiert und in den Nachrichtentext einer SIP-Antwort auf die INFO-Anfrage des Anrufers eingebettet), die ähnliche Informationen enthält. Der Anrufer überprüft dann die „Callee Hello“-Nachricht und fährt bei gültiger Nachricht mit dem nächsten Schritt fort.

SCHRITT 2 Der Anrufer sendet der angerufenen Partei die „Caller Final“-Nachricht, die die folgenden Informationen enthält:

- Nachrichten-ID (4B)
 - Verschlüsselter Hauptschlüssel (16B oder 128b)
 - Verschlüsseltes Master-Salt (16B oder 128b)
-

Verwendung von Mini-Zertifikaten

Hauptschlüssel und Master-Salt sind mit dem öffentlichen Schlüssel aus dem Mini-Zertifikat der angerufenen Partei verschlüsselt. Hauptschlüssel und Master-Salt werden von beiden Parteien verwendet, um Sitzungsschlüssel abzuleiten, mit denen dann die in der Folge gesendeten RTP-Pakete verschlüsselt werden. Die angerufene Partei reagiert dann mit einer „Callee Final“-Nachricht (einer leeren Nachricht).

Das Mini-Zertifikat (MC) enthält die folgenden Informationen:

- Benutzername (32B)
- Benutzer-ID oder Telefonnummer (16B)
- Ablaufdatum (12B)
- Öffentlicher Schlüssel (512b oder 64B)
- Signatur (1024b oder 512B)

Das MC verfügt über einen öffentlichen 512-Bit-Schlüssel, der für den Aufbau von sicheren Anrufen verwendet wird. Der Administrator muss jedem Teilnehmer des Dienstes für sichere Anrufe ein MC und den entsprechenden öffentlichen 512-Bit-Schlüssel zur Verfügung stellen. Das MC ist mit einem privaten 1024-Bit-Schlüssel des Service Provider signiert, der als Zertifizierungsstelle (CA) des MC dient. Darüber hinaus muss der das MC signierende öffentliche 1024-Bit-Schlüssel der Zertifizierungsstelle auch für jeden Teilnehmer bereitgestellt werden.

Mit dem öffentlichen Schlüssel der Zertifizierungsstelle wird das von anderen Teilnehmer empfangene MC verifiziert. Bei ungültigem MC wird der Anruf nicht in den sicheren Modus überstellt. Das MC und der öffentliche Schlüssel (1024 Bit) der Zertifizierungsstelle werden konkateniert und in den einzelnen Parameter „Mini Certificate“ (Mini-Zertifikat) base64-kodiert. Der private 512-Bit-Schlüssel ist in den Parameter „SRTP Private Key“ (Privater SRTP-Schlüssel) base64-kodiert und sollte wie ein Passwort geheim gehalten werden. (Mini Certificate und SRTP Private Key werden auf den Seiten **Line (1-4)** (Leitung 1-4) konfiguriert.)

Der Aufbau eines sicheren Anrufs basiert auf dem Austausch von Informationen, die in den Nachrichtentexten von SIP-INFO-Anfragen bzw. -Antworten eingebettet sind. Aus diesem Grund muss der Service Provider sicherstellen, dass SIP INFO-Nachrichten das Netzwerk durchlaufen können, ohne dass deren Nachrichtentext geändert wird.

Erzeugen von Mini-Zertifikaten

Cisco stellt einen Mini-Zertifikat-Generator bereit, mit dem Mini-Zertifikate und private Schlüssel erzeugt werden können. Wenn Sie auf dieses Tool zugreifen möchten, wenden Sie sich bitte an einen Cisco Mitarbeiter.

Der Mini-Zertifikat-Generator verwendet die folgende Syntax:

```
gen_mc ca-key user-name user-id expire-date
```

Hierbei gilt:

- **ca-key** ist eine Textdatei, die die Paare des base64-kodierten privaten 1024-Bit-Schlüssels der Zertifizierungsstelle bzw. öffentlichen Schlüssels enthält, mit denen das MC signiert bzw. verifiziert wird. Hier ein Beispiel:

```
9CC9aYU1X51JuU+EBZmi3AmcqE9U1LxEOWopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qq
e3VgYxWCQNa335YCNdsenASeBxuMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS
TYk2TZYTccnZ75TuTjj13qvYs=5nEtOrkCa84/mEwl3D9tSvVLyIiwQ+u/
Hd+C8u5SNk7hsAUZaA9TqH8Iw0J/
IqSrsf6scsmundY5j7Z5mK5J9uBxSB8t8vamFGD0pF4zhNtbrVvIXKI9kmp4vph1C5jzO9gDfs3M
F+zjyYrVUFdM+pXtDBxmM+fGUfrpAuXb7/k=
```

- **user-name** steht für den Namen des Teilnehmers, beispielsweise „Max Mustermann“. Die maximale Länge ist 32 Zeichen.
- **user-id** steht für die Benutzer-ID des Teilnehmers, die mit der im Rahmen des INVITE beim Durchführen des Anrufs verwendeten Benutzer-ID genau übereinstimmen muss, beispielsweise „14083331234“. Die maximale Länge ist 16 Zeichen.
- **expire-date** steht für das Ablaufdatum des MC, beispielsweise „00:00:00 1/1/34“ 34=2034). Intern ist das Datum als fixe 12B-Zeichenfolge kodiert: 000000010134.

Das Tool erzeugt die Parameter „Mini-Certificate“ (Mini-Zertifikat) und „SRTP-Private Key“ (Privater SRTP-Schlüssel), die für die Benutzer sodann bereitgestellt werden können.

Beispiel:

```
gen_mc ca_key „Max Mustermann“ 14085551234 „00:00:00 1/1/34“
```

Bei diesem Beispiel werden das folgende Mini-Zertifikat und der folgende private SRTP-Schlüssel erzeugt:

```
<Mini-Certificate>
Sm9lIFNtaXR0AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAxNDA4NTU1MTIzNAAAAAAAAAMDAwMDAwMDEw
MTM0O0vJakde2vVMF3Rw4pPXL7lAgIagMpbLSAG2+++YlSqt198Cp9rP/
xMGffoPmDKGx6JftkQ5sxLcuwgxpXpxkeXvpZKlYlpsb28L4Rhg5qZA+Gqj1hDFCmG6dffZ9SJhx
ES767G0JIS+N81QBLr0AuemotknSjjjOy8c+1lTCd2t44Mh0vmwNg4fDck2YdmTMBR516xJt4/
uQ/
LJQlni2kwqlm7scDv1l5k232EvvvVtCK0AYa4eWd6fQOpIESCO9CC9aYU1X51JuU+EBZmi3AmcqE
9U1LxEOWopaGyGOh3VyhKgi6JaVtQZt87PiJINKW8XQj3B9Qqe3VgYxWCQNa335YCNdsenASeBx
uMIEaBCYd111fVEodJZOGwXwfAde0MhcbD0kj7LVlzcS TYk2TZYTccnZ75TuTjj13qvYs=
<SRTP-Private Key>
b/DWc96X4YQraCnYzl5en1CIUhVQQqrvcR6Qd/8R52IEvJjOw/
e+Klm4XiIFEPaKmU8UbooxKG36SEdKusp0AQ==
```

Konfigurieren von Spracheinstellungen

Auf den Seiten **Voice** (Sprache) können Sie die Spracheinstellungen für Ihre SRP einsehen und konfigurieren. Diese Seiten sind in den folgenden Abschnitten beschrieben:

- **Seite Info (Infos)**
- **Seite System (System)**
- **Seite SIP (SIP)**
- **Seite Provisioning (Bereitstellung)**
- **Seite Regional (Regional)**
- **Seiten Line (1–2) (Leitung 1-2)**
- **Benutzerseiten (1–2)**

HINWEIS Um auf die Spracheinstellungen zuzugreifen, klicken Sie auf der Registerkarte auf **Voice** (Sprache) und danach auf die entsprechende Seite im Navigationsbereich.

Seite Info (Infos)

Auf dieser Seite erhalten Sie Informationen über die SRP-Sprachanwendung. Diese Seite enthält die folgenden Abschnitte:

- **Product Information (Produktinformationen)**
- **System Status (Systemstatus)**
- **Line Status (Status der Leitung)**

Product Information (Produktinformationen)

Voice > Info > Product Information (Sprache > Infos > Produktinformationen)

Product Name (Produktname)	Modellnummer/Modellname
Software Version (Softwareversion)	Versionsnummer der Software

Voice Module Version (Version des Sprachmoduls)	Versionsnummer des Sprachmoduls
Client Certificate (Client-Zertifikat)	Status des Client-Zertifikats, der anzeigt, ob die SRP von Ihrem ITSP autorisiert wurde.
Serial Number (Seriennummer)	Seriennummer des Produkts
Hardware Version (Hardwareversion)	Versionsnummer der Hardware
MAC Address (MAC-Adresse)	MAC-Adresse; zum Beispiel: 8843E1657936
Customization (Individuelle Optionen)	Diese Funktion wird nicht verwendet.

System Status (Systemstatus)

Voice > Info > System Status (Sprache > Infos > Systemstatus)

Current Time (Aktuelle Zeit)	Aktuelles Datum und aktuelle Zeit des Systems; zum Beispiel 10/3/2003 16:43:00 Sie können die Systemzeit auf der Seite Administration > Time Setup (Verwaltung > Zeiteinrichtung) ändern.
RTP Packets Sent (Gesendete RTP-Pakete)	Gesamtanzahl der gesendeten RTP-Pakete (einschließlich redundanter Pakete).
RTP Packets Recv (Empfangene RTP-Pakete)	Gesamtanzahl der empfangenen RTP-Pakete (einschließlich redundanter Pakete).
SIP Messages Sent (Gesendete SIP-Nachrichten)	Gesamtanzahl der gesendeten SIP-Nachrichten (einschließlich Neuübertragungen).
SIP Messages Recv (Empfangene SIP-Nachrichten)	Gesamtanzahl der empfangenen SIP-Nachrichten (einschließlich Neuübertragungen).
External IP (Externe IP)	Externe IP-Adresse, mit der die NAT-Zuordnung erfolgt.

Elapsed Time (Verstrichene Zeit)	Seit dem letzten Neustart des Systems verstrichene Gesamtzeit; zum Beispiel 25 Tage und 18:12:36
RTP Bytes Sent (Gesendete RTP-Bytes)	Gesamtanzahl der gesendeten RTP-Bytes
RTP Bytes Recv (Empfangene RTP-Bytes)	Gesamtanzahl der empfangenen RTP-Bytes
SIP Bytes Sent (Gesendete SIP-Bytes)	Gesamtanzahl der Bytes der gesendeten SIP-Nachrichten (einschließlich Neuübertragungen)
SIP Bytes Recv (Empfangene SIP-Bytes)	Gesamtanzahl der Bytes der empfangenen SIP-Nachrichten (einschließlich Neuübertragungen)

Line Status (Status der Leitung)

Voice > Info > Line 1 Status (Sprache > Infos > Status Leitung 1) (ähnliche Informationen werden für Leitung 2 bereitgestellt)

Hook State (Hook-Status)	Hook-Status des FXO-Ports. Leitungen sind entweder an oder aus.
Last Registration At (Zuletzt registriert am)	Datum und Zeitpunkt der letzten Registrierung der Leitung
Message Waiting (Neue Nachrichten)	Entweder Yes (Ja) oder No (Nein). Der Wert wird automatisch auf Ja gesetzt, wenn eine Nachricht erhalten wurde. Sie können die Markierung im Benutzermenü auch manuell löschen oder einstellen.
Last Called Number (Zuletzt gewählte Nummer)	Zuletzt über die FXO-Leitung gewählte Nummer
Registration State (Registrierungsstatus)	Zeigt an, ob die Leitung mit dem SIP-Proxy registriert wurde
Next Registration In (Nächste Registrierung in)	Anzahl der Sekunden bis zur nächsten Registrierungserneuerung Zeigt an, ob Sie eine neue Sprachnachricht haben.
Call Back Active (Aktiver Rückruf)	Zeigt an, ob gerade eine Rückrufanfrage verarbeitet wird. Entweder Yes (Ja) oder No (Nein).

Last Caller Number (Nummer des letzten Anrufers)	Nummer des letzten Anrufers
Mapped SIP Port (Zugeordneter SIP-Port)	Portnummer des von NAT zugeordneten SIP-Ports
Call 1 and 2 State (Status Anruf 1 und 2)	Die folgenden Werte sind möglich: ▪ Idle (Inaktiv) ▪ Collecting PSTN Pin (PSTN-PIN wird eingeholt) ▪ Invalid PSTN PIN (Ungültige PSTN-PIN) ▪ PSTN Caller Accepted (PSTN-Anrufer akzeptiert) ▪ Connected to PSTN (Mit PSTN verbunden)
Call 1 and 2 Tone (Ton Anruf 1 und 2)	Für den Anruf verwendeter Ton
Call 1 and 2 Encoder (Encoder Anruf 1 und 2)	Für das Kodieren verwendeter Codec
Call 1 and 2 Decoder (Decoder Anruf 1 und 2)	Für das Dekodieren verwendeter Codec
Call 1 and 2 FAX (FAX Anruf 1 und 2)	Status des Fax-Passthrough-Modus

Call 1 and 2 Type (Typ Anruf 1 und 2)	Richtung des Anrufs. Die folgenden Werte sind möglich: ▪ PSTN Gateway Call = VoIP-an-PSTN-Anruf ▪ VoIP Gateway Call = PSTN-an-VoIP-Anruf ▪ PSTN To Line 1 = PSTN-Anruf wird durchgestellt und von Leitung 1 beantwortet ▪ Line 1 Forward to PSTN Gateway = VoIP-Anrufe auf Leitung 1, die danach an den PSTN-GW weitergeleitet werden ▪ Line 1 Forward to PSTN Number = VoIP-Anrufe auf Leitung 1, die dann an die PSTN-Nummer weitergeleitet werden ▪ Line 1 To PSTN Gateway (Leitung 1 an PSTN-Gateway) ▪ Line 1 Fallback To PSTN Gateway (Leitung-1-Fallback an PSTN-Gateway)
Call 1 and 2 Remote Hold (Warteschleife Anruf 1 und 2)	Zeigt an, ob die Gegenstelle den Anruf in die Warteschleife gesetzt hat
Call 1 and 2 Callback (Rückruf Anruf 1 und 2)	Zeigt an, ob der Anruf über eine Rückrufanfrage initiiert wurde
Call 1 and 2 Peer Name (Peer-Name Anruf 1 und 2)	Name des Peer-Telefons
Call 1 and 2 Peer Phone (Peer-Telefon Anruf 1 und 2)	Telefonnummer des Peer-Telefons
Call 1 and 2 Call Duration (Dauer Anruf 1 und 2)	Dauer des Anrufs
Call 1 and 2 Packets Sent (Gesendete Pakete Anruf 1 und 2)	Anzahl der gesendeten Pakete
Call 1 and 2 Packets Recv (Empfangene Pakete Anruf 1 und 2)	Anzahl der empfangenen Pakete

Call 1 and 2 Packets Bytes Sent (Bytes der gesendeten Pakete Anruf 1 und 2)	Anzahl der gesendeten Bytes
Call 1 and 2 Packets Bytes Recv (Bytes der empfangenen Pakete Anruf 1 und 2)	Anzahl der empfangenen Bytes
Call 1 and 2 Decode Latency (Dekodierlatenz Anruf 1 und 2)	Anzahl der Millisekunden für die Decoder-Latenz
Call 1 and 2 Jitter (Jitter Anruf 1 und 2)	Anzahl der Millisekunden für Empfänger-Jitter
Call 1 and 2 Round Trip Delay (Round-Trip-Verzögerung Anruf 1 und 2)	Anzahl der Millisekunden für die Verzögerung
Call 1 and 2 Packets Lost (Verlorene Pakete Anruf 1 und 2)	Anzahl der verlorenen Pakete
Call 1 and 2 Packet Error (Paketfehler Anruf 1 und 2)	Anzahl der ungültigen empfangenen Pakete
Call 1 and 2 Mapped RTP Port (Zugeordneter RTP-Port Anruf 1 und 2)	Der Port, der Anruf 1 bzw. 2 für den Verkehr über das Real Time Protokoll zugeordnet wurde
Call 1 and 2 Media Loopback (Medien-Loopback Anruf 1 und 2)	Mit dem Medien-Loopback wird die Sprachqualität, die dem Endbenutzer geboten wird, sowohl quantitativ als auch qualitativ gemessen.

Seite System (System)

Auf der Seite **System** (System) können Sie die Einstellungen für Ihr System und Netzwerk konfigurieren. Diese Seite enthält die folgenden Abschnitte:

- **Systemkonfiguration**
- **Weitere Einstellungen**

Systemkonfiguration

Voice > System > System Configuration (Sprache > System > Systemkonfiguration)

Restricted Access Domains (Domänen mit eingeschränktem Zugriff)	Diese Funktion wird von der SRP derzeit nicht unterstützt.
IVR Admin Password (IVR-Administratorpasswort)	Administratorpasswort zur Verwaltung der SRP mithilfe des integrierten IVR über ein angeschlossenes Telefon. Der Standardwert ist 1234 .
IVR User Password (IVR-Benutzerpasswort)	Passwort für den Telefonbenutzer, mit dem dieser die Leitung mithilfe des integrierten IVR über ein Telefon verwalten kann. Die Standardeinstellung ist no password (Kein Passwort).

Weitere Einstellungen

Voice > System > Miscellaneous Settings (Sprache > System > Weitere Einstellungen)

Syslog Server (Syslog-Server)	Geben Sie die IP-Adresse des Syslog-Servers ein, an den Systemnachrichten gesendet werden.
Debug Server (Debug-Server)	Geben Sie die IP-Adresse des Syslog-Servers ein, an den Debugnachrichten gesendet werden.

Debug Level (Debug-Umfang)	Bestimmt den Umfang an Debug-Informationen, die erzeugt werden. Wählen Sie aus der Dropdown-Liste 0, 1, 2, 3 oder 3+Router aus. Je höher der Debug-Umfang, desto mehr Debug-Informationen werden erzeugt. Der Standardwert ist 0. Dies zeigt an, dass keine Debug-Informationen erzeugt werden. Beim Umfang 1, 2 & 3 werden Nachrichten erzeugt, die sich ausschließlich auf Sprachports beziehen. Bei 3+Router wird Debug-Inhalt sowohl für Sprach- als auch für Routerkomponenten erzeugt. Sie können die Protokollierungsoptionen auf den Seiten Administration > Log (Verwaltung > Protokoll) konfigurieren.
----------------------------	--

Seite SIP (SIP)

Auf der Seite **SIP** (SIP) können Sie zahlreiche SIP-Parameter und -Werte konfigurieren. Diese Seite enthält die folgenden Abschnitte:

- **SIP-Parameter**
- **SIP-Timer-Werte**
- **Behandlung von Antwortstatuscodes**
- **RTP Parameters (RTP-Parameter)**
- **SDP-Payload-Typen**
- **NSE Dynamic Payload (Dynamische NSE-Payload)**

SIP-Parameter

Voice > SIP > SIP Parameters (Sprache > SIP > SIP-Parameter)

Max Forward (Maximale Weiterleitung)	Wert für die maximale Weiterleitung, die zwischen 1 und 255 liegen kann. Der Standardwert ist 70.
Max Redirection (Maximale Umleitung)	Maximale Anzahl der Male, die eine INVITE-Nachricht umgeleitet werden kann, um eine Endlosschleife zu vermeiden Der Standardwert ist 5.

Max Auth (Maximale Authentifizierung)	Maximale Anzahl der Male (zwischen 0 und 255), die eine Authentifizierungsanfrage angefordert werden kann Der Standardwert ist 2.
SIP User Agent Name (Name des SIP-Benutzeragenten)	Header des Benutzeragenten, der bei ausgehenden Anfragen verwendet wird. Wenn leer, ist der Header nicht inbegriffen. Eine Makroerweiterung von \$A auf \$D ist entsprechend GPP_A auf GPP_D möglich. Die Standardeinstellung ist \$VERSION.
SIP Server Name (SIP-Servername)	Serverheader, der bei Antworten auf eingehende Antworten verwendet wird. Die Standardeinstellung ist \$VERSION.
SIP Reg User Agent Name (Name des SIP-Benutzeragenten bei Registrierung)	Name des Benutzeragenten, der bei einer Registrierungsanfrage verwendet wird. Wenn dieser Wert nicht festgelegt ist, wird der Parameter „Name des SIP-Benutzeragenten“ auch für die Registrierungsanfrage herangezogen. Die Standardeinstellung ist leer.
SIP Accept-Language (SIP-Accept-Language)	Accept-Language-Header, der verwendet wird. Es liegt hier keine Standardeinstellung vor (d. h., dass die SRP diesen Header nicht enthält). Wenn leer, ist der Header nicht inbegriffen.
DTMF Relay MIME Type (MIME-Typ für DTMF-Relay)	MIME-Typ, der in einer SIP-INFO-Nachricht zum Signalisieren eines DTMF-Ereignisses verwendet wird. Die Standardeinstellung ist application/dtmf-relay.
Remove Last Reg (Letzte Registrierung entfernen)	Mit dieser Funktion können Sie die letzte Registrierung entfernen, bevor Sie eine neue Registrierung mit einem unterschiedlichen Wert durchführen. Wählen Sie in der Dropdown-Liste Yes (Ja) oder No (Nein). Die Standardeinstellung ist No (Nein).

Use Compact Header (Compact-Header verwenden)	Mit dieser Funktion können Sie SIP-Compact-Header in ausgehenden SIP-Nachrichten verwenden. Wählen Sie in der Dropdown-Liste Yes (Ja) oder No (Nein). Wenn die Funktion aktiviert ist, verwendet die SRP bei ausgehenden SIP-Nachrichten SIP-Compact-Headers. Ist sie deaktiviert, verwendet die SRP normale SIP-Header. Bei eingehenden SIP-Anfragen, die Compact-Header enthalten, verwendet die SRP bei der Erzeugung der Antwort die gleichen Compact-Header erneut, und zwar unabhängig von den Einstellungen des Parameters Use Compact Header (Compact-Header verwenden). Wenn der Parameter Use Compact Header (Compact-Header verwenden) aktiviert ist und eingehende SIP-Anfragen normale Header enthalten, werden diese Header von der SRP durch Compact-Header ersetzt (wenn von RFC 261 festgelegt). Die Standardeinstellung ist No (Nein).
Escape Display Name (Anzeigenamen schützen)	Mit dieser Funktion können Sie den Anzeigenamen privat halten. Wählen Sie Yes (Ja) aus, wenn Sie möchten, dass die SRP die unter Display Name (Anzeigename) konfigurierte Zeichenfolge bei ausgehenden SIP-Nachrichten in Anführungszeichen setzt. Wenn der Anzeigename die Zeichen " oder \ enthält, werden diese durch \" und \\ in den Anführungszeichen geschützt. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
RFC 2543 Call Hold (RFC 2543-Warteschleife)	Mit dieser Funktion wird der Typ der Warteschleife für einen Anruf konfiguriert: a:sendonly oder 0.0.0.0. Die Standardeinstellung ist No (Nein); verwenden Sie die 0.0.0.0-Syntax bei einer HOLD-SDP nicht; verwenden Sie hingegen die a:sendonly-Syntax. Mark All AVT Packets (Alle AVT-Pakete markieren) Wenn diese Funktion aktiviert ist, weisen alle ATV-Tonpakete (für Redundanz kodiert) den Marker-Bit-Satz auf. Ist diese Funktion deaktiviert, weist nur das erste Paket den Marker-Bit-Satz für jedes DTMF-Ereignis auf. Die Standardeinstellung ist Yes (Ja).

Mark All AVT Packets (Alle AVT-Pakete markieren)	Wenn diese Funktion aktiviert ist, weisen alle AVT-Tonpakete (für Redundanz kodiert) den Marker-Bit-Satz auf. Ist diese Funktion deaktiviert, weist nur das erste Paket den Marker-Bit-Satz für jedes DTMF-Ereignis auf. Die Standardeinstellung ist Yes (Ja).
SIP TCP Port Min (SIP-TCP-Mindestportnummer)	Diese Funktion legt die niedrigste TCP-Portnummer fest, die für SIP-Sitzungen verwendet werden kann. Der Standardwert ist 5060.
SIP TCP Port Max (Maximale SIP-TCP-Portnummer)	Diese Funktion legt die höchste TCP-Portnummer fest, die für SIP-Sitzungen verwendet werden kann. Der Standardwert ist 5080.

SIP-Timer-Werte

Voice > SIP > SIP Timer Values (Sprache > SIP > SIP-Timer-Werte)

SIP T1	RFC 3261-T1-Wert (RTT-Schätzwert), der zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 0,5.
SIP T2	RFC 3261-T2-Wert (maximales Intervall bei Neuübertragungen für non-INVITE-Anfragen und INVITE-Antworten), der zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 4.
SIP T4	RFC 3261-T4-Wert (maximale Zeitspanne, die eine Nachricht im Netzwerk bleibt), der zwischen 0 und 64 Sekunden betragen kann Der Standardwert ist 5.
SIP Timer B (SIP-Timer B)	INVITE-Zeitüberschreitungswert, der zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 32.
SIP Timer F (SIP-Timer F)	Non-INVITE-Zeitüberschreitungswert, der zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 32.

SIP Timer H (SIP-Timer H)	Endgültige H-INVITE-Antwort, Zeitüberschreitungswert, der zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 32.
SIP Timer D (SIP-Timer D)	Anerkannte Verweilzeit, die zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 32.
SIP Timer J (SIP-Timer J)	Verweilzeit bei Non-INVITE-Antworten, die zwischen 0 und 64 Sekunden liegen kann Der Standardwert ist 32.
INVITE Expires (INVITE läuft ab)	Header-Wert Expires (Läuft ab) für INVITE-Anfragen. Wenn Sie 0 eingeben, enthält die Anfrage keinen „Expires“-Header. Der Standardwert ist 240. Bereich: 0–(2³¹-1).
ReINVITE Expires (ReINVITE läuft ab)	Header-Wert Expires (Läuft ab) für ReINVITE-Anfragen. Wenn Sie 0 eingeben, enthält die Anfrage keinen „Expires“-Header. Der Standardwert ist 30. Bereich: 0–(2³¹-1).
Reg Min Expires (Mindestzeit für Registrierung läuft ab)	Die vom Proxy zugelassene Mindestablaufzeit für Registrierungen im „Expires“-Header oder als Contact-Header-Parameter. Wenn der Proxy einen Wert zurückgibt, der unter dieser Einstellung liegt, wird der Mindestwert verwendet. Der Standardwert ist 1.
Reg Max Expires (Maximale Zeit für Registrierung läuft ab)	Die vom Proxy zugelassene maximale Ablaufzeit für Registrierungen im Header Min-Expires (Mindestzeit läuft ab). Wenn der Wert über dieser Einstellung liegt, wird der maximale Wert verwendet. Der Standardwert ist 7200.
Reg Retry Intvl (Intervall für erneuten Registrierungsversuch)	Intervall zwischen der letzten fehlgeschlagenen Registrierung und dem erneutem Registrierungsversuch der SRP. Der Standardwert ist 30.

Reg Retry Long Intvl (Langes Intervall für erneuten Registrierungsversuch)	Wenn die Registrierung aufgrund eines SIP-Antwortcodes, der nicht mit dem Retry-Reg-RSC übereinstimmt, fehlschlägt, wartet die SRP vor einem erneuten Versuch die festgelegte Zeitspanne ab. Wenn dieses Intervall auf 0 eingestellt ist, stellt die SRP keine weiteren Versuche mehr an. Dieser Wert sollte um einiges größer als der Reg-Retry-Intvl-Wert sein, der nicht 0 sein sollte. Der Standardwert ist 1200.
---	---

Behandlung von Antwortstatuscodes

Voice > SIP > Response Status Code Handling (Sprache > SIP > Verarbeitung von Antwortstatuscodes)

SIT1 RSC	SIP-Antwortstatuscode für das entsprechende Signal für Sonderinformationen (Special Information Tone, SIT). Wenn Sie beispielsweise SIT1-RSC auf 404 festlegen, dann ertönt das SIT1-Signal, wenn der Benutzer einen Anruf durchführen möchte und ein Fehlercode 404 zurückgegeben wird. Für SIT-1-RSC bis SIT-4-RSC ertönen bei allen nicht erfolgreichen Antwortstatuscodes standardmäßig der Reorder-Ton und das Besetztzeichen .
SIT2 RSC	SIP-Antwortstatuscode auf INVITE, bei dem das SIT2-Signal ertönt.
SIT3 RSC	SIP-Antwortstatuscode auf INVITE, bei dem das SIT3-Signal ertönt
SIT4 RSC	SIP-Antwortstatuscode auf INVITE, bei dem das SIT4-Signal ertönt
Try Backup RSC (RSC für versuchtes Backup)	SIP-Antwortcode, der die aktuelle Anfrage erneut an einen Backup-Server zu senden versucht
Retry Reg RSC (RSC für wiederholte Registrierung)	Intervall zwischen der letzten fehlgeschlagenen Registrierung und dem erneutem Registrierungsversuch der SRP

RTP Parameters (RTP-Parameter)

Voice > SIP > RTP Parameters (Sprache > SIP > RTP-Parameter)

RTP Port Min (RTP-Mindestportnummer)	Mindestportnummer für RTP-Übertragung und -Empfang Die Parameter RTP Port Min (RTP-Mindestportnummer) und RTP Port Max (Maximale RTP-Portnummer) sollten einen Bereich definieren, der mindestens 4 Ports aus geraden Ziffern enthält, beispielsweise 100-106. Der Standardwert ist 16384.
RTP Port Max (Maximale RTP-Portnummer)	Maximale Portnummer für RTP-Übertragung und -Empfang Der Standardwert ist 16482.
RTP Packet Size (RTP-Paketgröße)	Paketgröße in Sekunden, die zwischen 0,01 und 0,16 liegen kann Gültige Werte müssen ein Vielfaches von 0,01 Sekunden sein. Der Standardwert ist 0,030.
Max RTP ICMP Err (Maximale Anzahl von RTP-ICMP-Fehlern)	Anzahl von aufeinanderfolgenden ICMP-Fehlern, die bei der Übertragung von RTP-Paketen an den Peer zulässig ist, bevor die SRP den Anruf beendet. Wenn der Wert auf 0 eingestellt ist, ignoriert die SRP das Limit für ICMP-Fehler. Der Standardwert ist 0.

RTCP Tx Interval (RTCP-Übertragungsintervall)	Intervall zum Aussenden von RTCP-Senderberichten über eine aktive Verbindung. Es kann zwischen 0 und 255 Sekunden liegen. Die SRP kann bei aktiver Verbindung programmiert werden, um auf der Verbindung kombinierte RTCP-Pakete auszusenden. Mit Ausnahme des letzten enthält jedes kombinierte RTP-Paket einen SR (Senderbericht) und eine SDES (Quellenbeschreibung). Das letzte RTCP-Paket umfasst zusätzlich ein BYE-Paket. Jeder SR enthält genau 1 RR (Empfängerbericht), der letzte Senderbericht jedoch enthält keinen. Die SDES umfasst CNAME-, NAME- und TOOL-Identifikatoren. Der Wert „CNAME“ ist auf <Benutzer-ID>@<Proxy> eingestellt, „NAME“ auf <Anzeigenname> (oder „Anonym“, wenn der Benutzer die Anrufer-ID blockiert) und „TOOL“ auf die Softwareversion der Anbieter-/Hardware-Plattform (beispielsweise Cisco/srp5201.0.31(b)). Der im SR verwendete NTP-Zeitstempel ist ein Snapshot der lokalen Zeit auf der SRP und nicht der vom NTP-Server berichteten Zeit. Wenn die SRP vom Peer einen RR erhält, versucht sie, die Round-Trip-Verzögerung zu berechnen und sie auf der Seite Voice > Infos (Sprache > Infos) als Wert Call Round Trip Delay (Round-Trip-Anrufverzögerung) (ms) darzustellen. Der Standardwert ist 0.
No UDP Checksum (Keine UDP-Prüfsumme)	Aktivieren Sie diese Funktion, wenn Sie möchten, dass die SRP die UDP-Header-Prüfsumme für SIP-Nachrichten berechnet. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).

Stats In BYE (Statistiken in BYE-Nachrichten)	Mit dieser Funktion können Sie festlegen, ob die SRP P-RTP-Stat-Header oder -Antwort in eine BYE-Nachricht aufnimmt. Der Header umfasst die RTP-Statistiken zum aktuellen Anruf. Wählen Sie in der Dropdown-Liste Yes (Ja) oder No (Nein). Der R-RTP-Stat-Header weist folgendes Format auf: P-RTP-State: PS=<gesendete Pakete>,OS=<gesendete Oktetten>,PR=<empfangene Pakete>,OR=<empfangene Oktetten>,PL=<verlorene Pakete>,Jl=<Jitter in ms>,LA=<Verzögerung in ms>,DU=<Anrufdauer in Sek.>,EN=<Encoder>,DE=<Decoder>. Die Standardeinstellung ist Yes (Ja).
---	---

SDP-Payload-Typen

Voice > SIP > SDP Payload Types (Sprache > SIP > SDP-Payload-Typen)

NSE Dynamic Payload (Dynamische NSE-Payload)	Dynamischer NSE-Payload-Typ. Der gültige Bereich liegt zwischen 96 und 127. Der Standardwert ist 100.
AVT Dynamic Payload (Dynamische AVT-Payload)	Dynamischer AVT-Payload-Typ. Der gültige Bereich liegt zwischen 96 und 127. Der Standardwert ist 101.
INFOREQ Dynamic Payload (Dynamische INFOREQ-Payload)	Dynamischer INFOREQ-Payload-Typ Es gibt keine Standardeinstellung.
G726r32 Dynamic Payload (Dynamischer G726r32-Payload)	Dynamischer G726r32-Payload-Typ Der Standardwert ist 2.
G729b Dynamic Payload (Dynamischer G729b-Payload)	Dynamischer G729b-Payload-Typ. Der gültige Bereich liegt zwischen 96 und 127. Der Standardwert ist 99.
EncapRTP Dynamic Payload (Dynamische EncapRTP-Payload)	Dynamischer EncapRTP-Payload-Typ Der Standardwert ist 112.

RTP-Start-Loopback Dynamic Payload (Dynamische RTP-Start-Loopback-Payload)	Dynamischer RTP-Start-Loopback-Payload-Typ Der Standardwert ist 113.
RTP-Start-Loopback Codec (RTP-Start-Loopback-Codec)	RTP-Start-Loopback-Codec. Wählen Sie eine der folgenden Optionen aus: G711u, G711a, G726-32, G729a. Die Standardeinstellung ist G711u.
NSE Codec Name (NSE-Codec-Name)	Bei SDP verwendeter NSE-Codec-Name Die Standardeinstellung ist NSE.
AVT Codec Name (AVT-Codec-Name)	Bei SDP verwendeter AVT-Codec-Name Die Standardeinstellung ist telephone-event .
G711u Codec Name (G711u-Codec-Name)	Bei SDP verwendeter G.711u-Codec-Name Die Standardeinstellung ist PCMU.
G711a Codec Name (G711a-Codec-Name)	Bei SDP verwendeter G.711a-Codec-Name Die Standardeinstellung ist PCMA.
G726r32 Codec Name (G726r32-Codec-Name)	Bei SDP verwendeter G726r32-Codec-Name Die Standardeinstellung ist G726-32.
G729a Codec Name (G729a-Codec-Name)	Bei SDP verwendeter G.729a-Codec-Name Die Standardeinstellung ist G729a.
G729b Codec Name (G729b-Codec-Name)	Bei SDP verwendeter G.729b-Codec-Name Die Standardeinstellung ist G729ab.
EncapRTP Codec Name (EncapRTP-Codec-Name)	Bei SDP verwendeter EncapRTP-Codec-Name Die Standardeinstellung ist EncapRTP.

Parameter NAT-Unterstützung

Voice > SIP > NAT Support Parameters (Sprache > SIP > Parameter NAT-Unterstützung)

Handle VIA received (Empfangenen VIA verarbeiten)	Wenn Sie Yes (Ja) auswählen, verarbeitet die SRP den empfangenen Parameter im VIA-Header (dieser Wert wird vom Server in Reaktion auf eine beliebige Anfrage an diesen eingefügt). Wenn Sie No (Nein) auswählen, wird der Parameter ignoriert. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
Handle VIA rport (VIA-rport verarbeiten)	Wenn Sie Yes (Ja) auswählen, verarbeitet die SRP den rport-Parameter im VIA-Header (dieser Wert wird vom Server in Reaktion auf eine beliebige Anfrage an diesen eingefügt). Wenn Sie No (Nein) auswählen, wird der Parameter ignoriert. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
Insert VIA received (Empfangenen VIA einfügen)	Wenn sich die received-from-IP- und VIA-sent-by-IP-Werte unterscheiden, wird der empfangene Parameter mit dieser Funktion in den VIA-Header der SIP-Antworten eingefügt. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
Insert VIA rport (VIA-rport einfügen)	Wenn sich die received-from-IP- und VIA-sent-by-IP-Werte unterscheiden, wird der Parameter mit dieser Funktion in den VIA-Header der SIP-Antworten eingefügt. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
Substitute VIA Addr (VIA-Adresse ersetzen)	Mit dieser Funktion können Sie NAT-zugeordnete IP:port-Werte im VIA-Header verwenden. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).

Send Resp To Src Port (Antworten an Quellport senden)	Die Funktion sendet Antworten nicht an den VIA-sent-by-Port, sondern an den anfragenden Quellport. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
STUN Enable (STUN aktivieren)	Mit dieser Funktion können Sie die Verwendung von STUN zum Erkennen der NAT-Zuordnung aktivieren. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein) aus. Die Standardeinstellung ist No (Nein).
STUN Test Enable (STUN-Test aktivieren)	Wenn die Funktion STUN Enable (STUN aktivieren) aktiviert und ein gültiger STUN-Server verfügbar ist, kann die SRP beim Hochfahren einen NAT-Typ-Erkennungsvorgang durchführen. Sie kontaktiert den konfigurierten STUN-Server, und das Ergebnis des Erkennungsvorgangs wird in allen darauffolgenden REGISTER-Anfragen in einem Warnungsheader berichtet. Wenn die SRP ein symmetrisches NAT oder eine symmetrische Firewall erkennt, wird die NAT-Zuordnung deaktiviert. Die Standardeinstellung ist No (Nein).
STUN Server (STUN- Server)	IP-Adresse oder vollständig qualifizierter Domänenname des STUN-Servers, über die bzw. den Kontakt zur NAT-Zuordnungserkennung aufgenommen wird.

EXT IP (Externe IP)	Externe IP-Adresse, mit der die tatsächliche IP-Adresse der SRP bei allen ausgehenden SIP-Nachrichten substituiert wird. Wenn für diesen Parameter 0.0.0.0 festgelegt ist, erfolgt keine IP-Adressensubstitution. Wenn dieser Parameter anderweitig festgelegt ist, verwendet die SRP bei der Erzeugung von SIP-Nachrichten und SDP diese IP-Adresse (wenn die NAT-Zuordnung für diese Leitung aktiviert ist). Die Ergebnisse der Verarbeitung empfangener STUN- und VIA-Parameter, sofern vorhanden, ersetzen jedoch diesen statistisch konfigurierten Wert. BEMERKUNG: Für diese Option müssen Sie zwei Voraussetzungen erfüllen: einerseits müssen Sie über eine statische IP-Adresse von Ihrem Internet Service Provider verfügen und andererseits über ein Edge-Gerät mit einem symmetrischen NAT-Mechanismus. Wenn die SRP das Edge-Gerät darstellt, ist die zweite Voraussetzung erfüllt. Der Standardwert ist 0.0.0.0.
EXT RTP Port Min (EXT-RTP-Mindestportnummer)	Externe Portzuordnungsnummer der RTP-Mindestportnummer . Wenn dieser Wert nicht auf null festgelegt ist, wird die RTP-Portnummer bei allen ausgehenden SIP-Nachrichten durch den entsprechenden Portwert innerhalb des Bereichs für externe RTP-Portnummern substituiert. Es liegt hier kein Standardwert vor.
NAT Keep Alive Intvl (NAT-Keep-Alive-Intervall)	Intervall zwischen NAT-Zuordnungs-Keep Alive-Nachrichten. Der Standardwert ist 15.

Seite Provisioning (Bereitstellung)

Auf dieser Seite können Sie diverse Profile und Parameter konfigurieren. Diese Seite enthält die folgenden Abschnitte:

- **Konfigurationsprofil**
- **Firmware Upgrade (Firmware-Upgrade)**
- **Allgemeine Parameter**

Konfigurationsprofil

Voice > Provisioning > Configuration Profile (Sprache > Bereitstellung > Konfigurationsprofil)

Provision Enable (Bereitstellung aktivieren)	Diese Funktion steuert alle Resynchronisierungsaktionen unabhängig von Firmware-Upgrade-Aktionen. Wählen Sie Yes (Ja) aus, um die Remote-Bereitstellung zu aktivieren. Die Standardeinstellung ist Yes (Ja).
Resync On Reset (Resynchronisierung nach Neustart)	Diese Funktion löst nach jedem Neustart eine Resynchronisierung aus, wobei dies nicht für Neustarts gilt, die durch Parameteraktualisierungen oder Firmware-Upgrades bedingt sind. Die Standardeinstellung ist Yes (Ja).
Resync Random Delay (Zufällige Resynchronisierungsverzögerung)	Maximalwert für ein zufälliges Zeitintervall, das das Gerät abwartet, bevor es mit dem Bereitstellungsserver in Erstkontakt tritt. Diese Verzögerung kommt nur beim Versuch der Erstkonfiguration nach dem Einschalten oder einem Neustart des Geräts zum Tragen. Die Verzögerung ist eine Pseudozufallszahl zwischen null und diesem Wert. Dieser Parameter liegt in 20-Sekunden-Einheiten vor; der Standardwert von 2 steht für 40 Sekunden. Wenn dieser Parameter auf null festgelegt ist, ist diese Funktion deaktiviert. Mit dieser Funktion können Sie eine Überlastung des Bereitstellungsservers bei vielen gleichzeitig eingeschalteten Geräten verhindern. Der Standardwert ist 2 (40 Sekunden).

Resync Periodic (Periodische Resynchronisierung)	Zeitintervall zwischen periodischen Resynchronisierungen mit dem Bereitstellungsserver. Der zugehörige Resynchronisierungs-Timer ist erst nach der ersten erfolgreichen Synchronisierung mit dem Server aktiv. Wenn Sie periodische Resynchronisierungen deaktivieren möchten, legen Sie diesen Parameter auf null fest. Der Standardwert ist 3600 Sekunden.
Resync Error Retry Delay (Wiederholungsverzögerung bei fehlgeschlagener Resynchronisierung)	Im Fall einer fehlgeschlagenen Resynchronisierung kommt das Wiederholungsintervall für Resynchronisierungen (in Sekunden) zur Anwendung. Das Gerät verfügt über einen Wiederholungs-Timer für Fehlerfälle. Dieser wird aktiv, wenn der letzte Synchronisierungsversuch mit dem Bereitstellungsserver fehlgeschlagen ist. Das Gerät kontaktiert den Server erst dann erneut, wenn der Timer auf 0 heruntergezählt hat. Dieser Parameter ist der Wert, der zu Beginn in den Wiederholungs-Timer für Fehlerfälle geladen wird. Wenn dieser Parameter auf null festgelegt ist, startet das Gerät die Resynchronisierung mit dem Bereitstellungsserver sofort nach einem fehlgeschlagenen Versuch. Der Standardwert ist 3600 Sekunden.

Forced Resync Delay (Erzwungene Resynchronisierungsverzögerung)	Maximale Verzögerung (in Sekunden), die der SPA abwartet, bevor er eine Resynchronisierung durchführt. Das Gerät resynchronisiert sich nicht, solange eine seiner Telefonleitungen aktiv ist. Da eine Resynchronisierung einen Moment dauern kann, empfehlen wir Ihnen, mit der Resynchronisierung zu warten, bis das Gerät für einen längeren Zeitraum inaktiv war. Dadurch kann ein Benutzer mehrere Anrufe hintereinander ohne Unterbrechung führen. Das Gerät verfügt über einen Timer, der mit dem Herunterzählen beginnt, sobald sämtliche seiner Leitungen inaktiv sind. Dieser Parameter ist der Anfangswert des Zählers. Resynchronisierungsereignisse werden verzögert, bis dieser Zähler bei 0 angelangt ist. Der Standardwert ist 14.400 Sekunden.
Resync From SIP (Resynchronisierung über SIP)	Diese Funktion ermöglicht, dass eine Resynchronisierung über eine SIP-NOTIFY-Nachricht initialisiert werden kann. Die Standardeinstellung ist Yes (Ja).
Resync After Upgrade Attempt (Resynchronisierung nach versuchtem Upgrade)	Diese Funktion initialisiert eine Resynchronisierung nach jedem versuchten Firmware-Upgrade. Die Standardeinstellung ist Yes (Ja).
Resync Trigger 1 (Resynchronisierungs-Trigger 1)	Konfigurierbare Einstellungen für Resynchronisierungs-Trigger. Eine Resynchronisierung wird initialisiert, wenn die logische Gleichung in diesen Parametern als TRUE (Wahr) bewertet wird.
Resync Trigger 2 (Resynchronisierungs-Trigger 2)	Die Standeinstellung ist (leer).
Resync Fails On FNF (Fehlgeschlagene Resynchronisierung aufgrund von FNF)	Diese Funktion bestimmt, ob eine Datei-nicht-gefunden-Antwort (FNF) des Bereitstellungsservers eine erfolgreiche oder eine fehlgeschlagene Resynchronisierung darstellt. Durch eine fehlgeschlagene Resynchronisierung wird der Timer für fehlgeschlagene Resynchronisierungen aktiviert. Die Standardeinstellung ist Yes (Ja).

Profile Rule (Profilregel)	Dieser Parameter ist ein Profilskript, das sich aus dem Befehl einer Resynchronisierungsbereitstellung ergibt. Bei diesem Befehl handelt es sich um einen TCP/IP-Vorgang und eine zugehörige URL. Bei diesem TCP/IP-Vorgang kann es sich um TFTP, HTTP oder HTTPS handeln. Wenn der Befehl nicht festgelegt ist, wird TFTP übernommen und die Adresse des TFTP-Servers über die DHCP-Option 66 erhalten. In der URL kann entweder die IP-Adresse oder der FQDN des Servers definiert werden. Der Dateiname kann Makros aufweisen, beispielsweise \$MA, die sich dann auf die Geräte-MAC erstrecken. Die Standardeinstellung ist /srp\$PSN.cfg.
Profile Rule B (Profilregel B): Profile Rule C (Profilregel C): Profile Rule D (Profilregel D):	Diese Regeln definieren zweite, dritte und vierte Resynchronisierungsbefehle und zugehörige Profil-URLs. Diese Profilskripte werden nach Abschluss des Resynchronisierungsvorgangs der ersten Profilregel der Reihe nach ausgeführt. Wenn eine Resynchronisierung initialisiert wird und die Profilregel leer ist, werden die Profilregeln B, C und D weiterhin evaluiert und ausgeführt. Die Standeinstellung ist (leer).
Profile Name and Profile Region (Profilname und Profilregion)	Ein Bereitstellungsserver kann in diesem Parameter Zeichenfolgendaten speichern und diese Daten dann im Rahmen einer Anfrage an das Gerät abrufen. Er erfüllt sonst keine weitere interne Funktion.
Log Resync Request Msg (Protokollmel- dung über Resynchroni- sierungsanfrage)	Dieser Parameter enthält die Meldung, die zu Beginn einer versuchten Resynchronisierung an den Syslog-Server gesendet wird. Die Standardeinstellung ist \$PN \$MAC – Requesting resync \$SCHEME://\$SERVIP:\$PORT\$PATH.
Log Resync Success Msg (Protokollmeldung über erfolgreiche Resynchronisierung)	Nach einem erfolgreich abgeschlossenem Resynchronisierungsversuch gesendete Syslog-Meldung Die Standardeinstellung ist \$PN \$MAC – Successful resync \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR.

Log Resync Failure Msg (Protokollmeldung über fehlgeschlagene Resynchronisierung)	Nach einem fehlgeschlagenen Resynchronisierungsversuch gesendete Syslog-Meldung Die Standardeinstellung ist \$PN \$MAC – Resync failed: \$ERR.
Report Rule (Berichtsregel)	Ziel-URL, an die Konfigurationsberichte gesendet werden. Dieser Parameter weist die gleiche Syntax wie der Parameter Profile_Rule (Profilregel) auf und wird in einen TCP/IP-Befehl mit zugehöriger URL aufgelöst. Ein Konfigurationsbericht wird in Reaktion auf eine authentifizierte SIP-NOTIFY-Nachricht mit einem „Event:“-Bericht (Ereignis:-Bericht) erstellt. Der Bericht ist eine XML-Datei, die den Namen und den Wert aller Geräteparameter enthält. Dieser Parameter kann optional einen Verschlüsselungsschlüssel umfassen. Beispiel: [--key \$K] tftp://ps.callhome.net/\$MA/rep.xml.enc Die Standardeinstellung ist (leer).

Firmware Upgrade (Firmware-Upgrade)

Voice > Provisioning > Firmware Upgrade (Sprache > Bereitstellung > Firmware-Upgrade)

Upgrade Enable (Upgrade aktivieren)	Mit dieser Funktion können Sie Firmware-Upgrade-Vorgänge unabhängig von Resynchronisierungsaktionen aktivieren. Die Standardeinstellung ist Yes (Ja).
Upgrade Error Retry Delay (Wiederholungsverzögerung bei fehlgeschlagenem Upgrade)	Im Fall eines fehlgeschlagenen Upgrade kommt das Wiederholungsintervall für Upgrades (in Sekunden) zur Anwendung. Das Gerät verfügt über einen Timer für fehlgeschlagene Firmware-Updates. Dieser wird nach einem fehlgeschlagenen Firmware-Upgrade-Versuch aktiviert. Der Timer wird mit dem Wert in diesem Parameter initialisiert. Der nächste Firmware-Upgrade-Versuch erfolgt, nachdem dieser Timer auf null heruntergezählt hat. Der Standardwert ist 3600 Sekunden.

Downgrade Rev Limit (Rev-Limit-Downgrade)	Diese Funktion bietet einen unteren Grenzwert für akzeptable Versionsnummern während eines Firmware-Upgrades oder Downgrades. Das Gerät schließt keinen Firmware-Upgrade-Vorgang ab, bis die Firmware-Version größer oder gleich diesem Parameter ist. Die Standeinstellung ist (leer).
Upgrade Rule (Upgrade-Regel)	Dieser Parameter ist ein Firmware-Upgrade-Skript mit der gleichen Syntax wie Profile_Rule (Profilregel). Er definiert die Upgrade-Bedingungen und die zugehörigen Firmware-URLs. Die Standeinstellung ist (leer).
Log Upgrade Request Msg (Protokollmeldung über Upgrade-Anfrage)	Zu Beginn eines Firmware-Upgrade-Versuchs gesendete Syslog-Meldung Die Standardeinstellung ist \$PN \$MAC -- Requesting upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH.
Log Upgrade Success Msg (Protokollmeldung über erfolgreiches Upgrade)	Nach einem erfolgreich abgeschlossenen Firmware-Upgrade-Versuch gesendete Syslog-Meldung Die Standardeinstellung ist \$PN \$MAC -- Successful upgrade \$SCHEME://\$SERVIP:\$PORT\$PATH -- \$ERR.
Log Upgrade Failure Msg (Protokollmeldung über fehlgeschlagenes Upgrade)	Nach einem fehlgeschlagenen Firmware-Upgrade-Versuch gesendete Syslog-Meldung. Die Standardeinstellung ist \$PN \$MAC -- Upgrade failed: \$ERR.
License Keys (Lizenzschlüssel)	Dieses Feld findet bei der SRP500 derzeit keine Anwendung.

Allgemeine Parameter

Voice > Provisioning > General Purpose Parameters (Sprache > Bereitstellung > Allgemeine Parameter)

GPP A to GPP P (GPP A an GPP P)	Allgemeine Bereitstellungsparameter. Diese Parameter können bei der Bereitstellung und bei Upgrade-Regeln als Variablen herangezogen werden. Zur Erkennung dieser wird dem Namen der Variable ein \$-Zeichen vorangestellt, beispielsweise \$GPP_A. Die Standeinstellung ist (leer).
---------------------------------	--

Seite Regional (Regional)

Auf dieser Seite können Sie Ihr System mit den entsprechenden regionalen Einstellungen lokalisieren. Auf der Seite **Regional** (Regional) finden Sie die folgenden Abschnitte.

- **Anruffortschrittstöne**
- **Unterschiedliche Klingeltöne**
- **Unterschiedliche Anklopftöne**
- **Namen für unterschiedliche Klingel-/CWT-Töne**
- **Spezifikationen für Klingel- und Anklopftöne**
- **Kontrolltimerwerte (Sek.)**
- **Vertikale Dienstaktivierungscode**
- **Vertikale Dienstankündigungscode**
- **Codec-Auswahlcode für ausgehende Anrufe**
- **Weitere Bestimmungen**

Festlegen von Rufton-, Kadenz- und Tonskripten

Die SRP verwendet zum Festlegen von Rufton- und Tonmustern das Skrit-Konzept. Mit den folgenden Parametern wird definiert, wie Kadenzskripte (CadScripts), Frequenzskripte (FreqScripts) und Tonskripte (ToneScripts) erstellt werden.

CadScript

Mini-Skript aus maximal 127 Zeichen, das die Kadenzparameter eines Signals festlegt

Syntax: $S_1[S_2]$, wobei:

$S_i = D_i(\text{on}_{i,1}/\text{off}_{i,1}[\text{on}_{i,2}/\text{off}_{i,2}[\text{on}_{i,3}/\text{off}_{i,3}[\text{on}_{i,4}/\text{off}_{i,4}[\text{on}_{i,5}/\text{off}_{i,5}, \text{on}_{i,6}/\text{off}_{i,6}]]]])$ und als Abschnitt bezeichnet wird, $\text{on}_{i,j}$ und $\text{off}_{i,j}$ die Ein-/Aus-Dauer eines Segments in Sekunden ist und $i = 1$ oder 2 und $j = 1$ bis 6 . D_i ist die Gesamtdauer des Abschnitts in Sekunden. Alle Zeitintervalle dürfen für eine 1 ms-Auflösung maximal drei Dezimalstellen aufweisen. Der Platzhalter „*“ steht für Endlosdauer. Die Segmente innerhalb eines Abschnitts werden entsprechend der Reihenfolge abgespielt und wiederholt, bis die Gesamtdauer erreicht wurde.

Beispiel 1: 60 (2/4)

```
Anzahl von Kadenzfolgen = 1
Kadenzabschnitt 1: Abschnittslänge = 60 s
Anzahl von Segmenten = 1
Segment 1: An = 2 s, Aus = 4 s
Ruftongesamtlänge = 60 s
```

Beispiel 2 – Spezieller Rufton (kurz,kurz,kurz,lang): 60 (0,2/0,2, 0,2/0,2, 0,2/0,2, 1/4)

Anzahl von Kadenzabschnitten = 1
 Kadenzabschnitt 1: Abschnittslänge = 60s
 Anzahl von Segmenten = 4
 Segment 1: An = 0,2 s, Aus = 0,2 s
 Segment 2: An = 0,2 s, Aus = 0,2 s
 Segment 3: An = 0,2 s, Aus = 0,2 s
 Segment 4: An = 1,0 s, Aus = 4,0 s
 Ruftongesamtlänge = 60 s

FreqScript

Mini-Skript aus maximal 127 Zeichen, das die Frequenz- und Pegelparameter eines Tons festlegt

Syntax: $F_1@L_1[,F_2@L_2[,F_3@L_3[,F_4@L_4[,F_5@L_5[,F_6@L_6]]]]]$

Wobei F_1 – F_6 Frequenzen in Hz (nur unsignierte ganze Zahlen) und L_1 – L_6 entsprechende Pegel in dBm (mit bis zu 1 Dezimalstelle) sind. Leerzeichen vor und nach dem Komma sind zwar zulässig, allerdings nicht empfehlenswert.

Beispiel 1 – Anklopfton: 440@-10

Anzahl von Frequenzen = 1
 Frequenz 1 = 440 Hz bei -10 dBm

Beispiel 2 – Wählton: 350@-19,440@-19

Anzahl von Frequenzen = 2
 Frequenz 1 = 350 Hz bei -19 dBm
 Frequenz 2 = 440 Hz bei -19 dBm

ToneScript

Mini-Skript aus maximal 127 Zeichen, das Frequenz-, Pegel- und Kadenzparameter eines Anrufortschrittsstons festlegt. Es darf maximal 127 Zeichen enthalten.

Syntax: $\text{FreqScript}; Z_1[:Z_2]$.

Der Abschnitt Z_1 ähnelt dem Abschnitt S_1 in einem CadScript, mit der Ausnahme, dass auf jedes An/Aus-Segment ein Frequenzkomponentenparameter folgt: $Z_1 = D_1(\text{on}_{i,1}/\text{off}_{i,1}/f_{i,1}[, \text{on}_{i,2}/\text{off}_{i,2}/f_{i,2}[, \text{on}_{i,3}/\text{off}_{i,3}/f_{i,3}[, \text{on}_{i,4}/\text{off}_{i,4}/f_{i,4}[, \text{on}_{i,5}/\text{off}_{i,5}/f_{i,5}[, \text{on}_{i,6}/\text{off}_{i,6}/f_{i,6}]]]]])$, wobei $f_{i,j} = n_1[+n_2]+n_3[+n_4[+n_5[+n_6]]]]]$ und $1 < n_k < 6$ anzeigt, welche der Frequenzkomponenten aus dem FreqScript in diesem Segment verwendet werden; wenn mehr als eine Frequenzkomponente in diesem Segment verwendet wird, werden die Komponenten zusammengezählt.

Beispiel 1 – Wählton: 350@-19,440@-19;10(*0/1+2)

Anzahl von Frequenzen = 2
 Frequenz 1 = 350 Hz bei -19 dBm
 Frequenz 2 = 440 Hz bei -19 dBm
 Anzahl der Kadenzabschnitte = 1
 Kadenzabschnitt 1: Abschnittslänge = 10 s
 Anzahl von Segmenten = 1
 Segment 1: An = für immer, mit Frequenzen 1 und 2
 Ruftongesamtlänge = 10 s

Beispiel 2 – Stotternder Wählton: 350@-19,440@-19;2(0,1/0,1/1+2);10(*0/1+2)

Anzahl von Frequenzen = 2
 Frequenz 1 = 350 Hz bei -19 dBm
 Frequenz 2 = 440 Hz bei -19 dBm
 Anzahl der Kadenzabschnitte = 2
 Kadenzabschnitt 1: Abschnittslänge = 2 s
 Anzahl von Segmenten = 1
 Segment 1: Aus = 0,1 s, Aus = 0,1 s, mit Frequenzen 1 und 2
 Kadenzabschnitt 2: Abschnittslänge = 10 s
 Anzahl von Segmenten = 1
 Segment 1: An = für immer, mit Frequenzen 1 und 2
 Tongesamtlänge = 12 s

Anruffortschrittstöne

Voice > Regional > Call Progress Tones (Sprache > Regional > Anrufverarbeitungstöne

Wählton	Dieses Signal fordert den Benutzer zur Eingabe einer Telefonnummer auf. Wenn bei einem Wählton oder dessen Alternativen eine Zeitüberschreitung auftritt ertönt automatisch ein Reorder-Ton. Die Standardeinstellung ist 350@-19,440@-19;10(*0/1+2).
Second Dial Tone (Zweiter Wählton)	Alternative zum Wählton, wenn der Benutzer ein Dreiergespräch führen möchte Die Standardeinstellung ist 420@-19.520@-19;10(*0/1+2).
Outside Dial Tone (Externer Wählton)	Alternative zum Wählton. Dieses Signal fordert den Benutzer im Gegensatz zu einer internen Durchwahl zur Eingabe einer externen Telefonnummer auf. Dieser Wählton wird initialisiert, wenn im Wählplan ein „," (Komma) enthalten ist. Die Standardeinstellung ist 420@-19;10(*0/1).

Prompt Tone (Eingabeton)	Dieses Signal fordert den Benutzer zur Eingabe einer Telefonnummer zur Anrufweiterleitung auf. Die Standardeinstellung ist 520@-19,620@-19;10(*0/1+2).
Busy Tone (Besetztzeichen)	Dieses Signal ertönt, wenn ein 486 RSC für einen ausgehenden Anruf eingeht. Die Standardeinstellung ist 480@-19,620@-19;10(0,5/0,5/1+2).
Reorder Tone (Reorder-Ton)	Dieses Signal ertönt, wenn ein ausgehender Anruf fehlgeschlagen ist oder nachdem der Teilnehmer am anderen Ende bei aufrechter Verbindung aufgelegt hat. Wenn bei einem Wählton oder dessen Alternativen eine Zeitüberschreitung auftritt ertönt automatisch ein Reorder-Ton. Die Standardeinstellung ist 480@-19,620@-19;10(0,25/0,25/1+2).
Off Hook Warning Tone (Off-Hook- Warnsignal)	Dieses Signal ertönt, wenn der Anrufer das Telefon nicht richtig aufgelegt hat. Das Off-Hook-Warnsignal ertönt bei einer Zeitüberschreitung des Reorder-Tons. Die Standardeinstellung ist 480@10,620@0;10(0,125/0,125/1+2).
Ring Back Tone (Freizeichenton)	Dieses Signal ertönt während eines ausgehenden Anrufs, wenn es beim Teilnehmer am anderen Ende klingelt. Die Standardeinstellung ist 440@-19,480@-19;*(04,02,01+2).
Ring Back 2 Tone (Freizeichenton 2)	Ihre SRP spielt statt des Rückruftons diesen Rückrufton 2 ab, wenn die angerufene Partei eine SIP 182-Antwort ohne SDP auf die ausgehende INVITE-Anfrage zurückgibt. Die Standardeinstellung ist bei beiden Rückruftönen gleich, mit der Ausnahme, dass die Kadenz beim Rückrufton 2 1 s an und 1 s aus ist. Die Standardeinstellung ist 440@-19,480@-19;*(1,1,1+2).
Confirm Tone (Bestätigungston)	Kurzer Ton, mit dem der Benutzer darüber informiert wird, dass der letzte Eingabewert akzeptiert wurde. Die Standardeinstellung ist 600@-16; 1(0,25/0,25/1).

SIT1 Tone (SIT1-Ton)	Alternative zum Reorder-Ton, der ertönt, wenn bei der Durchführung eines ausgehenden Anrufs ein Fehler auftritt. Sie können den RSC, mit dem dieser Ton initialisiert wird, auf dem SIP-Bildschirm konfigurieren. Die Standardeinstellung ist 985@-16,1428@-16,1777@16;20(0,380/0/1,0,380/0/2,0,380/0/3,0/4/0).
SIT2 Tone (SIT2-Ton)	Alternative zum Reorder-Ton, der ertönt, wenn bei der Durchführung eines ausgehenden Anrufs ein Fehler auftritt. Sie können den RSC, mit dem dieser Ton initialisiert wird, auf dem SIP-Bildschirm konfigurieren. Die Standardeinstellung ist 914@-16,1371@-16,1777@16;20(274/0/1,0,274/0/2,0,380/0/3,0/4/0).
SIT3 Tone (SIT3-Ton)	Alternative zum Reorder-Ton, der ertönt, wenn bei der Durchführung eines ausgehenden Anrufs ein Fehler auftritt. Sie können den RSC, mit dem dieser Ton initialisiert wird, auf dem SIP-Bildschirm konfigurieren. Die Standardeinstellung ist 914@-16,1371@-16,1777@-16;20(380/0/1,0,380/0/2,0,380/0/3,0/4/0).
SIT4 Tone (SIT4-Ton)	Alternative zum Reorder-Ton, der ertönt, wenn bei der Durchführung eines ausgehenden Anrufs ein Fehler auftritt. Sie können den RSC, mit dem dieser Ton initialisiert wird, auf dem SIP-Bildschirm konfigurieren. Die Standardeinstellung ist 985@-16,1371@-16,1777@-16;20(0,380/0/1,0,274/0/2,0,380/0/3,0/4/0).
MWI Dial Tone (MWI-Wählton)	Dieses Signal ertönt statt des Wähltons, wenn sich in der Mailbox des Anrufers noch nicht abgehornte Nachrichten befinden. Die Standardeinstellung ist 350@-19,440@-19;2(0,1/0,1/1+2);10(* /0 1+2).
Cfwd Dial Tone (Cfwd-Wählton)	Dieses Signal ertönt, wenn Anrufe weitergeleitet werden. Die Standardeinstellung ist 350@-19,440@-19;2(0,2/0,2/1+2);10(* /0/1+2).

Holding Tone (Haltton)	Mit diesem Signal wird der lokale Anrufer darüber informiert, dass er vom Teilnehmer am anderen Ende in die Warteschleife gesetzt wurde. Die Standardeinstellung ist 600@-19* (0,1/0,1/1,0,1/0,1/1,0,1/9,5/1).
Conference Tone (Konferenzton)	Dieses Signal ertönt bei allen Parteien, wenn eine Dreierkonferenz aufgebaut wird. Die Standardeinstellung ist 350@-19;20(0,1/0,1/1,0,1/9,7/1).
Secure Call Indication Tone (Hinweiston für sichere Anrufe)	Dieses Signal ertönt, wenn ein Anruf erfolgreich in den sicheren Modus geschaltet wurde. Es sollte nur kurz (für weniger als 30 Sekunden) und bei verringertem Pegel (weniger als -19 dBm) ertönen, sodass das Gespräch nicht gestört wird. Die Standardeinstellung ist 397@-19,507@-19;15(0/2/0,0,2/0,1/1,0,1/2,1/2).
Feature Invocation Tone (Funktions- aktivierungston)	Dieses Signal ertönt, wenn eine Funktion umgesetzt wird. Die Standardeinstellung ist 350@-16;* (0,1/0,1/1).

Unterschiedliche Klingeltöne

Voice > Regional > Distinctive Ring Patterns (Sprache > Regional > Unterschiedliche Klingeltöne)

Ring1 Cadence (Kadenz Klingelton 1)	Kadenzskript für den unterschiedlichen Klingelton 1 Die Standardeinstellung ist 60 (2/4).
Ring2 Cadence (Kadenz Klingelton 2)	Kadenzskript für den unterschiedlichen Klingelton 2 Die Standardeinstellung ist 60 (0,8/0,4, 0,8/4).
Ring3 Cadence (Kadenz Klingelton 3)	Kadenzskript für den unterschiedlichen Klingelton 3 Die Standardeinstellung ist 60 (0,4/0,2, 0,4/0,2, 0,8/4).
Ring4 Cadence (Kadenz Klingelton 4)	Kadenzskript für den unterschiedlichen Klingelton 4 Die Standardeinstellung ist 60 (0,3/0,2, 0,1/0,2, 0,3/4).
Ring5 Cadence (Kadenz Klingelton 5)	Kadenzskript für den unterschiedlichen Klingelton 5 Die Standardeinstellung ist 1 (0,5/0,5).

Ring6 Cadence (Kadenz Klingelton 6)	Kadenzskript für den unterschiedlichen Klingelton 6 Die Standardeinstellung ist 60 (0,2/0,4, 0,2/0,4, 0,2/4).
Ring7 Cadence (Kadenz Klingelton 7)	Kadenzskript für den unterschiedlichen Klingelton 7 Die Standardeinstellung ist 60 (0,4/0,2, 0,4/0,2, 0,4/4).
Ring8 Cadence (Kadenz Klingelton 8)	Kadenzskript für den unterschiedlichen Klingelton 8 Die Standardeinstellung ist 60 (0,25/9,75).

Unterschiedliche Anklopftöne

Voice > Regional > Distinctive Call Waiting Tone Patterns (Sprache > Regional > Unterschiedliche Anklopftöne)

CWT1 Cadence (Kadenz CWT1)	Kadenzskript für den speziellen CWT 1 Die Standardeinstellung ist 30 (0,3/9,7).
CWT2 Cadence (Kadenz CWT2)	Kadenzskript für den speziellen CWT 2 Die Standardeinstellung ist 30 (0,1/0,1, 0,1/9,7).
CWT3 Cadence (Kadenz CWT3)	Kadenzskript für den speziellen CWT 3 Die Standardeinstellung ist 30 (0,1/0,1, 0,1/0,1, 0,1/9,7).
CWT4 Cadence (Kadenz CWT4)	Kadenzskript für den speziellen CWT 4 Die Standardeinstellung ist 30 (0,1/0,1, 0,3/0,1, 0,1/9,3).
CWT5 Cadence (Kadenz CWT5)	Kadenzskript für den speziellen CWT 5 Die Standardeinstellung ist 1 (0,5/0,5).
CWT6 Cadence (Kadenz CWT6)	Kadenzskript für den speziellen CWT 6 Die Standardeinstellung ist 30 (0,3/0,1, 0,3/0,1, 0,1/9,1).
CWT7 Cadence (Kadenz CWT7)	Kadenzskript für den speziellen CWT 7 Die Standardeinstellung ist 30 (0,3/0,1, 0,3/0,1, 0,1/9,3).
CWT8 Cadence (Kadenz CWT8)	Kadenzskript für den speziellen CWT 8 Die Standardeinstellung ist 2,3 (0,3/2).

Namen für unterschiedliche Klingel-/CWT-Töne

Voice > Regional > Distinctive Ring/CWT Pattern Names (Sprache > Regional > Namen für unterschiedliche Klingel-/CWT-Töne)

Ring1 Name (Name Klingelton 1)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 1 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r1.
Ring2 Name (Name Klingelton 2)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 2 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r2.
Ring3 Name (Name Klingelton 3)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 3 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r3.
Ring4 Name (Name Klingelton 4)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 4 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r4.
Ring5 Name (Name Klingelton 5)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 5 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r5.
Ring6 Name (Name Klingelton 6)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 6 für den eingehenden Anruf ausgewählt werden kann. Die Standardeinstellung ist Bellcore-r6.
Ring7 Name (Name Klingelton 7)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 7 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r7.
Ring8 Name (Name Klingelton 8)	Name in einem Warnungs-Informationen-Header einer INVITE-Anfrage, damit der spezielle Klingelton/CWT 8 für den eingehenden Anruf ausgewählt werden kann Die Standardeinstellung ist Bellcore-r8.

Spezifikationen für Klingel- und Anklopftöne

WICHTIG: Klingel- und Anklopftöne funktionieren nicht auf allen Telefonen gleich. Beachten Sie daher beim Einstellen Ihrer Klingeltöne folgende Empfehlungen:

- Beginnen Sie mit der standardmäßigen Klingeltonwellenform, Klingeltonfrequenz und Klingeltonspannung.
- Wenn sich die Kadenz Ihres Ruftons falsch anhört oder Ihr Telefon nicht läutet, ändern Sie die Klingeltonwellenform, Klingeltonfrequenz und Klingeltonspannung wie folgt:
 - Klingeltonwellenform: Sinusoid
 - Klingeltonfrequenz: 25
 - Klingeltonspannung: 80 Vc

Ring Waveform (Ruftonwellenform)	Wellenform des Klingeltons. Sie können zwischen Sinusoid (Sinusoid) oder Trapezoid (Trapezoid) auswählen. Die Standardeinstellung ist Trapezoid (Trapezoid).
Ring Frequency (Klingeltonfrequenz)	Frequenz des Klingeltons Gültige Werte liegen zwischen 10 und 100 (Hz). Der Standardwert ist 20.
Ring Voltage (Klingeltonspannung)	Klingeltonspannung. Sie können aus 60–90 (V) wählen. Der Standardwert ist 85.
CWT Frequency (CWT-Frequenz)	Frequenzskript des Anklopftons. Alle speziellen CWTs basieren auf diesem Ton. Die Standardeinstellung ist 440@-10.
Synchronized Ring (Synchronisierter Klingelton)	Wenn dieser Parameter auf Yes (Ja) eingestellt ist, klingeln alle Leitungen gleichzeitig, wenn die SRP angerufen wird (ähnlich einer gewöhnlichen PSTN-Leitung). Sobald eine Leitung antwortet, hören die anderen zu klingeln auf. Die Standardeinstellung ist No (Nein).

Kontrolltimerwerte (Sek.)

Voice > Regional > Control Timer Values (sec) (Sprache > Regional > Kontrolltimerwerte (Sek.))

Hook Flash Timer Min (Minestdauer für Hook-Flash-Timer)	On-Hook-Mindestdauer, bevor das Off-Hook als Hook-Flash bewertet wird. Wird diese Dauer unterschritten, wird das On-Hook-Ereignis ignoriert. Bereiche: 0,1–0,4 Sekunden Der Standardwert ist 0,1.
Hook Flash Timer Max (Maximale Dauer für Hook-Flash-Timer)	Maximale On-Hook-Dauer, bevor das Off-Hook als Hook-Flash bewertet wird. Wird diese Dauer überschritten, wird das On-Hook-Ereignis als On-Hook behandelt (kein Hook-Flash-Ereignis). Bereich: 0,4–1,6 Sekunden Der Standardwert ist 0,9.
Callee On Hook Delay (Callee-On-Hook-Verzögerung)	Telefon muss für diese Zeit in Sekunden aufgelegt sein, bevor die SRP den aktuellen eingehenden Anruf beendet. Dies gilt nicht für ausgehende Anrufe. Bereich: 0–255 Sekunden Der Standardwert ist 0.
Reorder Delay (Reorder-Verzögerung)	Verzögerung, die auftritt, nachdem der Teilnehmer am anderen Ende aufgelegt hat und bevor der Reorder-Ton ertönt. 0 = ertönt sofort, inf = ertönt niemals Bereich: 0–255 Sekunden Der Standardwert ist 5.
Call Back Expires (Rückrufzeit läuft ab)	Ablaufzeit für eine Rückrufaktivierung in Sekunden. Bereich: 0–65535 Sekunden Der Standardwert ist 1800.
Call Back Retry Intvl (Intervall für Rückrufwiederholung)	Intervall für Rückrufwiederholung in Sekunden. Bereich: 0–255 Sekunden Der Standardwert ist 30.

Call Back Delay (Rückrufverzögerung)	Verzögerung, die auftritt, nachdem die erste SIP 18x-Antwort empfangen wurde und bevor bekannt gegeben wird, dass es beim Teilnehmer am anderen Ende klingelt. Wenn in diesem Zeitraum eine Besetzt-Antwort eingeht, wird dieser Anruf von der SRP als fehlgeschlagen eingestuft und weiterhin versucht, den anderen Teilnehmer zu erreichen. Der Standardwert ist 0,5.
VMWI Refresh Intvl (Intervall für VMWI-Aktualisierung)	Intervall zwischen VMWI-Aktualisierungen auf CPE. Der Standardwert ist 0.
Interdigit Long Timer (Langer Inter-Digit-Timer)	Langer Zeitüberschreitungswert zwischen der Eingabe von Ziffern beim Wählvorgang. Die Werte für den Inter-Digit-Timer werden beim Wählvorgang als Standardwerte herangezogen. Der Interdigit_Long_Timer wird nach jeder beliebigen Ziffer verwendet, wenn noch nicht alle gültigen übereinstimmenden Folgen im Wählplan eingegeben wurden. Bereich: 0–64 Sekunden Der Standardwert ist 10.
Interdigit Short Timer (Kurzer Inter-Digit-Timer)	Kurzer Zeitüberschreitungswert zwischen der Eingabe von Ziffern beim Wählvorgang. Der Interdigit_Short_Timer wird nach jeder beliebigen Ziffer verwendet, wenn zumindest eine übereinstimmende Folge im Wählplan gewählt wurde, jedoch weitere eingegebene Ziffern auch mit anderen, noch nicht vollständigen Folgen übereinstimmen würden. Bereich: 0–64 Sekunden Der Standardwert ist 3.

CPC Delay (CPC-Verzögerung)	Verzögerung in Sekunden, die auftritt, nachdem der Anrufer aufgelegt hat und wenn die SRP beginnt, die a- und b-Aderspannung vom zugehörigen Gerät der angerufenen Partei zu entfernen. Bereich: 0–255 Sekunden Diese Funktion wird im Allgemeinen zur Antwortüberwachung auf Anruferseite verwendet, um dem zugehörigen Gerät zu signalisieren, wenn die Verbindung erfolgreich aufgebaut (Teilnehmer am anderen Ende hat geantwortet) oder unterbrochen (Teilnehmer am anderen Ende hat aufgelegt) wurde. Sie sollten diese Funktion für die angerufene Partei deaktivieren (anders ausgedrückt, Sie sollten für verbundenen und nicht-verbundenen Zustand die gleiche Polarität festlegen) und stattdessen die CPC-Funktion verwenden. Wenn Sie die CPC nicht aktivieren, ertönt nach einer konfigurierbaren Verzögerung ein Reorder-Ton. Wenn Sie die CPC aktivieren, ertönt ein Wählton, wenn die b-zu-a-Aderspannung wiederhergestellt ist. Die Auflösung beträgt 1 Sekunde. Der Standardbereich ist 2.
CPC Duration (CPC-Dauer)	Dauer in Sekunden, im Rahmen welcher die a-zu-b-Aderspannung entfernt wird, nachdem der Anrufer aufgelegt hat. Danach wird die a-zu-b-Aderspannung wiederhergestellt und es ertönt ein Wählton, wenn das zugehörige Gerät weiterhin abgehoben ist. Wenn Sie diesen Wert auf 0 festlegen, wird die CPC deaktiviert. Bereich: 0-1.000 Sekunden. Die Auflösung beträgt 0,001 Sekunden. Der Standardwert ist 0 (CPC deaktiviert).

Vertikale Dienstaktivierungscodes

Vertikale Dienstaktivierungscodes werden automatisch dem Wählplan hinzugefügt. Sie müssen diese Codes nicht in den Wählplan aufnehmen. Es verursacht allerdings auch keine Probleme, wenn Sie sie aufnehmen.

Voice > Regional > Vertical Service Activation Codes (Sprache > Regional > Vertikale Dienstaktivierungscodes

Call Return Code (Rückrufcode)	Mit diesem Code wird der letzte Anrufer angerufen. Die Standardeinstellung ist *69.
Call Redial Code (Wahlwiederholungscode)	Mit diesem Code wird die zuletzt gewählte Nummer angerufen. Die Standardeinstellung ist *07.
Blind Transfer Code (Code für Weiterleitung ohne Rückfrage)	Dieser Code initiiert eine Weiterleitung des aktuellen Anrufs an die nach dem Aktivierungscode festgelegte Durchwahl ohne Rückfrage. Die Standardeinstellung ist *98.
Call Back Act Code (Rückrufaktivierungscode)	Dieser Code beginnt mit einem Rückruf, wenn der letzte ausgehende Anruf nicht besetzt ist. Die Standardeinstellung ist *66.
Call Back Deact Code (Rückrufdeaktivierungscode)	Dieser Code deaktiviert einen Rückruf. Die Standardeinstellung ist *86.
Call Back Busy Act Code (Aktivierungscode für Rückruf bei Besetztzeichen)	Dieser Code beginnt mit einem Rückruf, wenn der letzte ausgehende Anruf besetzt ist. Die Standardeinstellung ist *05.
Cfwd All Act Code (Aktivierungscode für Rufumleitung Alle Anrufe)	Dieser Code leitet alle Anrufe an die Durchwahl weiter, die nach dem Aktivierungscode festgelegt ist. Die Standardeinstellung ist *72.
Cfwd All Deact Code (Deaktivierungscode für Rufumleitung Alle Anrufe)	Dieser Code deaktiviert die Weiterleitung aller Anrufe. Die Standardeinstellung ist *73.

Cfwd Busy Act Code (Aktivierungscode für Rufumleitung bei Besetzt)	Dieser Code leitet alle besetzten Anrufe an die Durchwahl weiter, die nach dem Aktivierungscode festgelegt ist. Die Standardeinstellung ist *90.
Cfwd Busy Deact Code (Deaktivierungscode für Rufumleitung bei Besetzt)	Dieser Code deaktiviert die Weiterleitung für besetzte Anrufe. Die Standardeinstellung ist *91.
Cfwd No Ans Act Code (Aktivierungscode für Rufumleitung falls keine Antwort)	Dieser Code leitet alle nicht beantworteten Anrufe an die Durchwahl weiter, die nach dem Aktivierungscode festgelegt ist. Die Standardeinstellung ist *92.
Cfwd No Ans Deact Code (Deaktivierungscode für Rufumleitung falls keine Antwort)	Dieser Code deaktiviert die Weiterleitung für nicht beantwortete Anrufe. Die Standardeinstellung ist *93.
Cfwd Last Act Code (Aktivierungscode für Rufumleitung für letzte Anrufe)	Dieser Code leitet die letzten eingehenden oder ausgehenden Anrufe an die Durchwahl weiter, die nach dem Aktivierungscode festgelegt ist. Die Standardeinstellung ist *63.
Cfwd Last Deact Code (Deaktivierungscode für Rufumleitung für letzte Anrufe)	Dieser Code deaktiviert die Weiterleitung für die letzten eingehenden oder ausgehenden Anrufe. Die Standardeinstellung ist *83.
Block Last Act Code (Aktivierungscode für Blockieren des letzten Anrufs)	Dieser Code blockiert den letzten eingehenden Anruf. Die Standardeinstellung ist *60.
Block Last Deact Code (Deaktivierungscode für Blockieren des letzten Anrufs)	Mit diesem Code wird das Blockieren des letzten eingehenden Anrufs deaktiviert. Die Standardeinstellung ist *80.

Accept Last Act Code (Aktivierungscode für Annehmen des letzten Anrufs)	Dieser Code nimmt den letzten ausgehenden Anruf an. Mit diesem Code wird der Anruf durchgestellt, wenn Sie die Funktionen Do not disturb (Bitte nicht stören) oder Call forwarding of all calls (Alle Anrufe umleiten) aktiviert haben. Die Standardeinstellung ist *64.
Accept Last Deact Code (Deaktivierungscode für Annehmen des letzten Anrufs)	Mit diesem Code wird die Annahme des letzten ausgehenden Anrufs deaktiviert. Die Standardeinstellung ist *84.
CW Act Code (Aktivierungscode für Anklopfen)	Mit diesem Code wird die Anklopffunktion für alle Anrufe aktiviert. Die Standardeinstellung ist *56.
CW Deact Code (Deaktivierungscode für Anklopfen)	Mit diesem Code wird die Anklopffunktion für alle Anrufe deaktiviert. Die Standardeinstellung ist *57.
CW Per Call Deact Code (Aktivierungscode Anklopfen für nächsten Anruf)	Mit diesem Code wird die Anklopffunktion für den nächsten Anruf aktiviert. Die Standardeinstellung ist *71.
CW Per Call Act Code (Deaktivierungscode Anklopfen für nächsten Anruf)	Mit diesem Code wird die Anklopffunktion für den nächsten Anruf deaktiviert. Die Standardeinstellung ist *70.
Block CID Act Code (Aktivierungscode für Blockieren der CID)	Mit diesem Code wird die Anrufer-ID bei allen ausgehenden Anrufen blockiert. Die Standardeinstellung ist *67.
Block CID Deact Code (Deaktivierungscode für Blockieren der CID)	Mit diesem Code wird das Blockieren der Anrufer-ID bei allen ausgehenden Anrufen deaktiviert. Die Standardeinstellung ist *68.

CID Per Call Act Code (Aktivierungscode für Blockieren der CID beim nächsten Anruf)	Mit diesen Code wird die Anrufer-ID beim nächsten ausgehenden Anruf blockiert. Die Standardeinstellung ist *81.
CID Per Call Deact Code (Deaktivierungscode für Blockieren der CID beim nächsten Anruf)	Mit diesem Code wird das Blockieren der Anrufer-ID beim nächsten eingehenden Anruf deaktiviert. Die Standardeinstellung ist *82.
Block ANC Act Code (Aktivierungscode für Blockieren anonymer Anrufe)	Mit diesem Code werden alle anonymen Anrufe blockiert. Die Standardeinstellung ist *77.
Block ANC Deact Code (Deaktivierungscode für Blockieren anonymer Anrufe)	Mit diesem Code wird das Blockieren aller anonymen Anrufe deaktiviert. Die Standardeinstellung ist *87.
DND Act Code (DND-Aktivierungscode)	Mit diesem Code wird die Funktion Do not Disturb (Bitte nicht stören) aktiviert. Die Standardeinstellung ist *78.
DND Deact Code (DND-Deaktivierungscode)	Mit diesem Code wird die Funktion Do not Disturb (Bitte nicht stören) deaktiviert. Die Standardeinstellung ist *79.
CID Act Code (CID-Aktivierungscode)	Mit diesem Code wird die Generierung von Anrufer-IDs aktiviert. Die Standardeinstellung ist *65.
CID Deact Code (CID-Deaktivierungscode)	Mit diesem Code wird die Generierung von Anrufer-IDs deaktiviert. Die Standardeinstellung ist *85.

CWCID Act Code (CWCID-Aktivierungscode)	Mit diesem Code werden Anrufweiterleitung und Generierung von Anrufer-IDs aktiviert. Die Standardeinstellung ist *25.
CWCID Deact Code (CWCID-Deaktivierungscode)	Mit diesem Code werden Anrufweiterleitung und Generierung von Anrufer-IDs deaktiviert. Die Standardeinstellung ist *45.
Dist Ring Act Code (Aktivierungscode für unterschiedliche Klingeltöne)	Mit diesem Code wird die Funktion für unterschiedliche Klingeltöne aktiviert. Die Standardeinstellung ist *26.
Dist Ring Deact Code (Deaktivierungscode für unterschiedliche Klingeltöne)	Mit diesem Code wird die Funktion für unterschiedliche Klingeltöne deaktiviert. Die Standardeinstellung ist *46.
Speed Dial Act Code (Kurzwahl-Aktivierungscode)	Mit diesem Code wird eine Kurzwahl zugewiesen. Die Standardeinstellung ist *74.
Paging Code (Paging-Code)	Dieser Code wird zum Paging anderer Clients in der Gruppe verwendet. Die Standardeinstellung ist *96.
Secure All Call Act Code (Aktivierungscode für Sichern aller Anrufe)	Mit diesem Code werden alle ausgehenden Gespräche gesichert. Die Standardeinstellung ist *16.
Secure No Call Act Code (Code für kein Sichern der Anrufe)	Mit diesem Code werden keine ausgehenden Gespräche gesichert. Die Standardeinstellung ist *17.
Secure One Call Act Code (Aktivierungscode für Sichern des nächsten Anrufs)	Mit diesem Code wird der nächste ausgehende Anruf gesichert. (Dieser ist redundant, wenn alle ausgehenden Anrufe standardmäßig gesichert werden) Die Standardeinstellung ist *18.

Secure One Call Deact Code (Deaktivierungscode für Sichern des nächsten Anrufs)	Mit diesem Code wird der nächste ausgehende Anruf nicht gesichert. (Dieser ist redundant, wenn alle ausgehenden Anrufe standardmäßig nicht gesichert werden) Die Standardeinstellung ist *19.
Conference Act Code (Konferenzaktivierungscode)	Ist dieser Code aktiviert, so muss der Benutzer diesen eingeben, bevor er die Nummer der dritten Partei für ein Konferenzgespräch wählt. Geben Sie den Code für ein Konferenzgespräch ein.
Attn-Xfer Act Code (Aktivierungscode für Rufübergabe nach Ankündigung)	Ist dieser Code aktiviert, so muss der Benutzer diesen eingeben, bevor er die Nummer der dritten Partei für eine Rufübergabe wählt. Geben Sie den Code für eine Rufübergabe ein.
Modem Line Toggle Code (Code für Umschalten einer Leitung auf ein Modem)	Mit diesem Code wird die Leitung auf ein Modem umgeschaltet. Die Standardeinstellung ist *99. Der Modem-Passthrough-Modus kann nur durch Vorwahl dieses Codes initialisiert werden.
FAX Line Toggle Code (Code für Umschalten einer Leitung auf ein Faxgerät)	Mit diesem Code wird die Leitung auf ein Faxgerät umgeschaltet. Die Standardeinstellung ist #99.
Media Loopback Code (Code für Medien-Loopback)	Dieser Code wird für ein Medien-Loopback verwendet. Die Standardeinstellung ist *03.

Referral Services Codes (Weiterleitungsdienstcodes)	Diesen Codes kann die SRP entnehmen, was zu tun ist, wenn der Benutzer den aktuellen Anruf in die Warteschleife setzt und den zweiten Wählton hört. Ein oder mehrere *-Codes können in diesem Parameter konfiguriert werden, beispielsweise *98 oder *97*98*123 etc. Die Länge darf 79 Zeichen nicht überschreiten. Dieser Parameter kommt zur Anwendung, wenn der Benutzer den aktuellen Anruf in die Warteschleife setzt (über Hook-Flash) und den zweiten Wählton hört. Jeder *-Code (und die darauffolgende gültige Zielnummer gemäß aktuellem Wählplan), der während des zweiten Wähltons eingegeben wird, veranlasst die SRP dazu, eine Weiterleitung ohne Rückfrage an eine Zielnummer mit vorangestelltem Dienst-*-Code durchzuführen. Wenn der Benutzer beispielsweise *98 wählt, spielt die SRP einen speziellen Freiton, Eingabeton genannt, ab und wartet darauf, dass der Benutzer eine Zielnummer eingibt (die wie bei normalen Anrufen mit dem Wählplan übereinstimmen muss). Wenn der Benutzer eine vollständige Nummer eingegeben hat, sendet die SRP eine REFER-Nachricht ohne Rückfrage an die Partei in der Warteschleife, wobei das Refer-to Target (Ziel der Weiterleitung) *98 target_number (*98 Zielnummer) entspricht. Mit dieser Funktion kann die SRP einen Anruf an einen Anwendungsserver für die weitere Verarbeitung, beispielsweise das Parken von Anrufen, leiten. Die *-Codes sollten mit keinem der anderen vertikalen Dienstcodes, die von der SRP intern verarbeitet werden, in Konflikt stehen. Sie können den entsprechenden *-Code, deren Verarbeitung nicht durch die SRP erfolgen soll, leer lassen.
--	---

Feature Dial Services Codes (Dienstcodes für Funktionswähltöne)	Diesen Codes kann die SRP entnehmen, was zu tun ist, wenn der Benutzer den ersten oder zweiten Wählton hört. Ein oder mehrere *-Codes können in diesem Parameter konfiguriert werden, beispielsweise *72 oder *72*74*67*82 etc. Die Länge darf 79 Zeichen nicht überschreiten. Dieser Parameter kommt zur Anwendung, wenn der Benutzer einen Wählton (erster oder zweiter Ton) hört. Der *-Code (und die darauffolgende gültige Zielnummer gemäß aktuellem Wahlplan), der während des Wähltons eingegeben wird, veranlasst die SRP dazu, die Zielnummer, der der *-Code vorangestellt ist, anzurufen. Wenn der Benutzer beispielsweise *72 wählt, spielt die SRP einen speziellen Ton, Eingabeton genannt, ab und wartet darauf, dass der Benutzer eine gültige Zielnummer eingibt. Wenn der Benutzer eine vollständige Nummer eingegeben hat, sendet die SRP eine INVITE-Anfrage an *72 target_number (*72 Zielnummer), wie bei einem normalen Anruf. Mit dieser Funktion kann der Proxy Funktionen wie Rufumleitung (*72) oder Anrufer-ID blockieren (*67) verarbeiten. Die *-Codes sollten mit keinem der anderen vertikalen Dienstcodes, die von der SRP intern verarbeitet werden, in Konflikt stehen. Sie können den entsprechenden *-Code, deren Verarbeitung nicht durch die SRP erfolgen soll, leer lassen. Sie können jedem *-Code in den Dienstcodes für Funktionswähltöne einen Parameter hinzufügen, um anzuzeigen, welcher Ton nach Eingabe des *-Codes ertönt, beispielsweise *72'c'*67'p'. Im Folgenden finden Sie eine Liste der zulässigen Tonparameter (achten Sie auf die einfachen Anführungszeichen, unter die der Parameter mit oder ohne Leerzeichen gesetzt ist). 'c' = <Cfwd-Wählton> 'd' = <Wählton> 'm' = <MWI-Wählton> 'o' = <Externer Wählton> 'p' = <Eingabe-Wählton> 's' = <Zweiter Wählton> 'x' = Kein Ton festgelegt; x steht für eine oben nicht genannte Ziffer Wenn kein Tonparameter festgelegt ist, spielt die SRP standardmäßig den Eingabeton ab. Wenn auf den *-Code keine Telefonnummer folgen soll, beispielsweise *73 zum Deaktivieren der Rufumleitung, nehmen Sie den Code nicht in diesen Parameter auf. Fügen Sie den *-Code in diesem Fall einfach dem Wahlplan hinzu, und die SRP sendet wie gewöhnlich INVITE *73@....., wenn ein Benutzer *73 wählt.
---	---

Vertikale Dienstankündigungscodes

Voice > Regional > Vertical Service Announcement Codes (Sprache > Regional > Vertikale Dienstankündigungscodes)

Service Annc Base Number (Basisnummer für Dienstankündigungen)	Basisnummer für Dienstankündigungen Die Standardeinstellung ist leer.
Service Annc Extension Codes (Durchwahlcodes für Dienstankündigungen)	Durchwahlcodes für Dienstankündigungen Die Standardeinstellung ist leer.

Codec-Auswahlcodes für ausgehende Anrufe

Voice > Regional > Outbound Call Codec Selection Codes (Sprache > Regional > Codec-Auswahlcodes für ausgehende Anrufe)

Prefer G711u Code (G711u-Code bevorzugen)	Vorwahl, mit der G.711u zum bevorzugten Codec für den Anruf wird Die Standardeinstellung ist *017110.
Force G711u Code (G711u-Code erzwingen)	Vorwahl, mit der G711u zum einzigen Codec wird, der für diesen Anruf verwendet werden kann Die Standardeinstellung ist *027110.
Prefer G711a Code (G711a-Code bevorzugen)	Vorwahl, mit der G.711a zum bevorzugten Codec für den Anruf wird Die Standardeinstellung ist *017111.
Force G711a Code (G711a-Code erzwingen)	Vorwahl, mit der G711a zum einzigen Codec wird, der für diesen Anruf verwendet werden kann Die Standardeinstellung ist *027111.
Prefer G726r32 Code (G726r32-Code bevorzugen)	Vorwahl, mit der G726r32 zum bevorzugten Codec für den Anruf wird Die Standardeinstellung ist *0172632.
Force G726r32 Code (G726r32-Code erzwingen)	Vorwahl, mit der G726r32 zum einzigen Codec wird, der für diesen Anruf verwendet werden kann Die Standardeinstellung ist *0272632.

Prefer G729a Code (G729a-Code bevorzugen)	Vorwahl, mit der G.729a zum bevorzugten Codec für den Anruf wird. Die Standardeinstellung ist *01729.
Force G729a Code (G729a-Code erzwingen)	Vorwahl, mit der G729a zum einzigen Codec wird, der für diesen Anruf verwendet werden kann Die Standardeinstellung ist *02729.

Weitere Bestimmungen

Voice > Regional > Miscellaneous (Sprache > Regional > Weitere Bestimmungen)

Set Local Date (mm/dd) (Lokales Datum einstellen) (MM/TT)	Mit dieser Funktion können Sie das lokale Datum einstellen (MM steht für Monate und TT für Tage). Das Jahr kann optional und im 2- oder 4-Stellenformat festgelegt werden.
Set Local Time (HH/mm) (Lokale Uhrzeit einstellen) (hh/mm)	Mit dieser Funktion können Sie die lokale Uhrzeit einstellen (hh steht für Stunden und mm für Minuten). Sekunden können optional festgelegt werden.
FXS Port Impedance (FXS-Port-Impedanz)	Mit dieser Funktion können Sie die elektrische Impedanz des FXS-Ports festlegen. Sie können aus den folgenden Werten wählen: 600, 900, 600+2.16uF, 900+2.16uF, 270+750 150nF, 220+850 120nF, 220+820 115nF oder 200+600 100nF. Der Standardwert ist 600. BEMERKUNG Verwenden Sie für die Impedanz in Neuseeland (370+620 310nF) 270+750 150nF.
FXS Port Input Gain (FXS-Port-Eingangsverstärkung)	Eingangsverstärkung in dB mit maximal drei Dezimalstellen. Bereich: 6.000 bis -12.000 Der Standardwert ist -3.
FXS Port Output Gain (FXS-Port-Ausgangsverstärkung)	Ausgangsverstärkung in dB mit maximal drei Dezimalstellen. Bereich: 6.000 bis -12.000 Die Anruf fortschrittstöne und der DTMF-Wiedergabepegel werden von der FXS-Port-Ausgangsverstärkung nicht beeinflusst. Der Standardwert ist -3.

DTMF Playback Level (DTMF-Wiedergabepegel)	Lokaler DTMF-Wiedergabepegel in dBm mit maximal einer Dezimalstelle. Der Standardwert ist -16,0.
DTMF Playback Length (DTMF-Wiedergabelänge)	Lokale Dauer der DTMF-Wiedergabe in Millisekunden Der Standardwert ist 0,1.
Detect ABCD (ABCD erkennen)	Wählen Sie Yes (Ja), wenn Sie die lokale Erkennung von DTMF-ABCD aktivieren möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist Yes (Ja). Diese Einstellung kommt nicht zum Tragen, wenn das DTMF-Übertragungsverfahren INFO ist; ABCD wird unabhängig von dieser Einstellung stets OOB gesendet.
Playback ABCD (ABCD-Wiedergabe)	Wählen Sie Yes (Ja), wenn Sie die lokale Wiedergabe von OOB-DTMF-ABCD aktivieren möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist Yes (Ja).

Anrufer-ID-Verfahren	Sie können aus den folgenden Optionen wählen: ▪ Belcore (Nordamerika, China): CID, CIDCW und VMWI. FSK wird nach erstem Klingelton gesendet (entspricht der ETSI FSK nach dem ersten Klingelton) (keine Polaritätsumkehr oder DTAS). ▪ DTMF (Finnland, Schweden): nur CID. DTMF wird nach der Polaritätsumkehr (ohne DTAS) sowie vor dem ersten Klingelton gesendet. ▪ DTMF (Dänemark): nur CID. DTMF wird vor dem ersten Klingelton ohne Polaritätsumkehr und DTAS gesendet. ▪ ETSI DTMF: nur CID. DTMF wird nach DTAS (und ohne Polaritätsumkehr) und vor dem ersten Klingelton gesendet. ▪ ETSI DTMF mit PR: nur CID. DTMF wird nach der Polaritätsumkehr und DTAS sowie vor dem ersten Klingelton gesendet. ▪ ETSI DTMF nach Rufton: nur CID. DTMF wird nach dem ersten Klingelton gesendet (ohne Polaritätsumkehr oder DTAS). ▪ ETSI FSK: CID, CIDCW und VMWI. FSK wird nach DTAS (aber ohne Polaritätsumkehr) und vor dem ersten Klingelton gesendet. Wartet auf Bestätigung von CPE nach DTAS für CIDCW. ▪ ETSI FSK mit PR (GB): CID, CIDCW und VMWI. FSK wird nach der Polaritätsumkehr und DTAS sowie vor dem ersten Klingelton gesendet. Wartet auf Bestätigung von CPE nach DTAS für CIDCW. Polaritätsumkehr erfolgt nur, wenn das Gerät aufgelegt ist. Die Standardeinstellung ist Belcore (Nordamerika, China).
FXS Port Power Limit (FXS-Port-Leistungsgrenze)	Sie können aus 1 bis 8 wählen. Der Standardwert ist 3.
Anrufer-ID-FSK-Standard	Die SRP unterstützt Bell 202- und v.23-Standards für die Generierung von Anrufer-IDs. Die Standardeinstellung ist Bell 202.
Feature Invocation Method (Funktionsaktivierungsverfahren)	Wählen Sie als gewünschtes Verfahren entweder Default (Standard) oder Sweden (Schweden) aus. Die Standardeinstellung ist Default (Standard).

Seiten Line (1–2) (Leitung 1-2)

Auf diesen Seiten können Sie die Leitungen für Sprachdienste konfigurieren. Diese Seiten enthalten die folgenden Abschnitte:

- **Leitung aktivieren**
- **Streaming-Audio-Server (SAS)**
- **NAT-Einstellungen**
- **Netzwerkeinstellungen**
- **SIP-Einstellungen**
- **Anruffunktionseinstellungen**
- **Proxy und Registrierung**
- **Outbound Proxy SIP (Ausgehender Proxy-SIP)**
- **Supplementary Service Subscription (Abonnement für ergänzende Dienste)**
- **Audiokonfiguration**
- **Wählplan**
- **Konfiguration der FXS-Portpolarität**

In einem Konfigurationsprofil muss an die Leitungsparameter die entsprechende Nummer angehängt sein (beispielsweise [1] oder [2]), damit die der Einstellung zugehörige Leitung identifiziert werden kann.

Leitung aktivieren

Voice > Line 1–2 > Line Enable (Sprache > Leitung 1-2 > Leitung aktivieren)

Leitung aktivieren	Wählen Sie yes (Ja), wenn Sie die Leitung für diesen Dienst aktivieren möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist Yes (Ja).
--------------------	--

Streaming-Audio-Server (SAS)

Voice > Line 1–2 > Streaming Audio Server (SAS) (Sprache > Leitung 1-2 > Streaming-Audio-Server (SAS))

SAS Enable (SAS aktivieren)	Wählen Sie Yes (Ja), wenn Sie die Leitung als Streaming-Audio-Quelle nutzen möchten. Andernfalls wählen Sie No (Nein) aus. Wenn diese Funktion aktiviert ist, kann die Leitung für ausgehende Anrufe nicht verwendet werden. Stattdessen beantwortet sie eingehende Anrufe und streamt RTP-Audiopakete an den Anrufer. Die Standardeinstellung ist No (Nein).
SAS DLG Refresh Intvl (Intervall für SAS-DLG-Aktualisierung)	Wenn dieser Wert nicht null ist, sendet der Streaming-Audio-Server Nachrichten zur Sitzungsaktualisierung (SIP re-INVITE-Nachrichten) in diesem Intervall aus, um zu bestimmen, ob die Verbindung mit dem Anrufer noch aktiv ist. Wenn der Anrufer nicht auf die Aktualisierungsnachricht reagiert, beendet die SRP den Anruf mit einer SIP-BYE-Nachricht. Der Bereich liegt zwischen 0 und 255 Sekunden (0 bedeutet, dass die Sitzungsaktualisierung deaktiviert wurde). Der Standardwert ist 30.

SAS Inbound RTP Sink (Eingehende RTP-Senke des SAS)	Diese Einstellung umgeht Geräte, die kein eingehendes RTP abspielen, wenn sich die SAS-Leitung selbst als Send-only-Gerät deklariert und den Client anweist, keine Audiodateien zu streamen. Geben Sie den vollständig qualifizierten Domännennamen (fully qualified domain name, FQDN) oder die IP-Adresse einer RTP-Senke ein. Dieser Wert wird von der SAS-Leitung im SDP ihrer 200 Antworten auf eine von einem Client eingehende INVITE-Nachricht herangezogen. Dieser Parameter dient dazu, Geräte zu umgehen, die kein eingehendes RTP abspielen, wenn sich die SAS-Leitung selbst als Send-only-Gerät deklariert und den Client anweist, keine Audiodateien zu streamen. Dieser Parameter ist ein FQDN oder eine IP-Adresse einer RTP-Senke, die von der SAS-Leitung im SDP ihrer 200 Antworten auf eingehende INVITE-Anfragen eines Client verwendet wird. Er wird in c = line und der Portnummer und, falls festgelegt, in m = line des SDP angezeigt. Wenn dieser Wert nicht auf 0 oder gleich 0 festgelegt ist, dann ist c = 0.0.0.0 und a=sendonly wird im SDP verwendet, um den SAS-Client anzuweisen, kein RTP an diese SAS-Leitung zu senden. Wenn der Wert nicht auf 0 festgelegt ist, dann ist a=sendrecv und der SAS-Client streamt Audiodateien an die entsprechende Adresse. Sonderfall: Wenn der Wert \$IP ist, dann wird die eigene IP-Adresse der SAS-Leitung in c=line und a=sendrecv verwendet. In diesem Fall streamt der SAS-Client RTP-Pakete an die SAS-Leitung. Der Standardwert ist leer.
--	---

NAT-Einstellungen

Voice > Line 1-2 > NAT Settings (Sprache > Leitung 1-2 > NAT-Einstellungen)

NAT Mapping Enable (NAT-Zuordnung aktivieren)	Wählen Sie Yes (Ja) aus, wenn Sie extern zugeordnete IP-Adressen und SIP/RTP-Ports in SIP-Nachrichten verwenden möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
NAT Keep Alive Enable (NAT-Keep-Alive aktivieren)	Wählen Sie Yes (Ja) aus, wenn Sie die konfigurierte NAT-Keep-Alive-Nachricht periodisch senden möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
NAT Keep Alive Msg (NAT-Keep-Alive-Nachricht)	Geben Sie die Keep Alive-Nachricht ein, die periodisch gesendet werden sollte, damit die aktuelle NAT-Zuordnung aufrechterhalten wird. Wenn der Wert \$NOTIFY ist, wird eine NOTIFY-Nachricht gesendet. Wenn der Wert \$REGISTER ist, wird eine REGISTER-Nachricht ohne Kontakt gesendet. Die Standardeinstellung ist \$NOTIFY.
NAT Keep Alive Dest (NAT-Keep-Alive-Ziel)	Ziel, an das NAT-Keep-Alive-Nachrichten gesendet werden sollten. Wenn der Wert \$PROXY ist, werden die Nachrichten an den aktuellen ausgehenden Proxyserver gesendet. Die Standardeinstellung ist \$PROXY.

Netzwerkeinstellungen

Voice > Line 1-2 > Network Settings (Sprache > Leitung 1-2 > Netzwerkeinstellungen)

SIP ToS/DiffServ Value (SIP ToS/DiffServ-Wert)	TOS/DiffServ-Feldwert in UDP-IP-Paketen, die eine SIP-Nachricht enthalten Der Standardwert ist 0x68.
SIP CoS Value [0-7] (SIP CoS-Wert) [0-7]	CoS-Wert für SIP-Nachrichten. Der Standardwert ist 3.

RTP ToS/DiffServ Value (RTP ToS/DiffServ-Wert)	ToS/DiffServ-Feldwert in UDP-IP-Paketen, die RTP-Daten enthalten Der Standardwert ist 0xb8.
RTP CoS Value [0-7] (RTP CoS-Wert) [0-7]	CoS-Wert für RTP-Daten Der Standardwert ist 6.
Network Jitter Level (Stärke des Jitters im Netzwerk)	Dieser Parameter bestimmt, wie die Größe des Jitter-Puffers von der SRP angepasst wird. Die Größe des Jitter-Puffers kann dynamisch angepasst werden. Die Mindestgröße des Jitter-Puffers beträgt für alle Jitter-Stärke-Einstellungen 30 Millisekunden oder (10 Millisekunden plus aktuelle RTP-Frame-Größe), je nachdem, welcher Wert größer ist. Der Ausgangswert für die Größe des Jitter-Puffers ist allerdings bei stärkerem Jitter höher. Diese Einstellung bestimmt die Rate, mit der die Größe des Jitter-Puffers angepasst wird, um den Mindestwert zu erreichen. Wählen Sie die entsprechende Einstellung: low (niedrig), medium (mittel), high (hoch), very high (sehr hoch), extremely high (äußerst hoch). Die Standardeinstellung ist high (hoch).
Jitter Buffer Adjustment (Anpassung des Jitter-Puffers)	Mit diesem Parameter wird die gewünschte Anpassung des Jitter-Puffers gesteuert. Wählen Sie die entsprechende Einstellung: up and down (nach oben und unten), up only (nur nach oben), down only (nur nach unten) oder disable (deaktivieren). Die Standardeinstellung ist up and down (nach oben und unten).

SIP-Einstellungen

Voice > Line 1-2 > SIP Settings (Sprache > Leitung 1-2 > SIP-Einstellungen)

SIP Transport (SIP-Transport)	Die TCP-Auswahl bietet eine „garantierte Zustellung“. Dadurch wird sichergestellt, dass alle verlorenen Pakete erneut übertragen werden. TCP gewährleistet ferner, dass die SIP-Pakete in der gleichen Reihenfolge empfangen werden, in der sie gesendet wurden. Folglich überwindet TCP die größten Nachteile des UDP. Darüber hinaus werden UDP-Ports von den Firewalls der meisten Unternehmen aus Sicherheitsgründen blockiert. Bei TCP müssen weder neue Ports geöffnet werden noch gehen Pakete verloren, da TCP bereits für grundlegende Aktivitäten wie Internet-Browsing oder e-Commerce verwendet wird. Wählen Sie aus den folgenden Optionen: UDP, TCP, TLS. Die Standardeinstellung ist UDP.
SIP Port (SIP-Port)	Portnummer des Überwachungs- und Übertragungsports für SIP-Nachrichten. Der Standardwert ist 5060.
SIP 100REL Enable (SIP 100REL aktivieren)	Wählen Sie yes (Ja), um die Unterstützung der 100REL SIP-Erweiterung für eine zuverlässige Übertragung von vorläufigen Antworten (18x) und die Verwendung von PRACK-Anfragen zu aktivieren. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
EXT SIP Port (EXT-SIP-Port)	Nummer des externen SIP-Ports
Auth Resync-Reboot (Resynchronisierung/ Neustart authentifizieren)	Wenn diese Funktion aktiviert ist, authentifiziert die SRP den Sender bei Erhalt der Meldung „NOTIFY resynch reboot“ (RFC 2617). Wählen Sie yes (Ja), wenn Sie diese Funktion nutzen möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist Yes (Ja).

SIP Proxy-Require (SIP Proxy-Require)	Wenn der Benutzeragent diesen Header aufweist, kann der SIP-Proxy eine spezielle Erweiterung oder ein spezielles Verhalten unterstützen. Wenn dieses Feld konfiguriert ist und der Proxy es nicht unterstützt, antwortet er mit der Nachricht „unsupported“ (wird nicht unterstützt). Geben Sie den gewünschten Header in das entsprechende Feld ein.
SIP Remote-Party-ID (SIP-ID der Gegenstelle)	Wählen Sie yes (Ja), wenn Sie den Header „Remote-Party-ID“ (ID der Gegenstelle) statt des Headers „From“ (Von) verwenden möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist Yes (Ja).
SIP GUID (SIP-GUID)	Die global eindeutige ID (GUID) wird für jede Leitung und für jedes Gerät generiert. Ist dieser Parameter aktiviert, fügt die SRP in der SIP-Anfrage einen GUID-Header hinzu. Die GUID wird generiert, wenn das Gerät das erste Mal hochfährt. Das Gerät behält diese GUID bei einem Neustart und sogar bei einer Zurücksetzung auf die Werkseinstellungen. Diese Funktion wurde von Bell Canada (Nortel) angefordert, um die Registrierung von SIP-Konten einzuschränken. Die Standardeinstellung ist No (Nein).

SIP Debug Option (SIP-Debug-Option)	SIP-Nachrichten werden von einem Proxy-Überwachungsport empfangen oder von diesem gesendet. Mit dieser Funktion können Sie steuern, welche SIP-Nachrichten Sie protokollieren möchten. Wählen Sie aus den folgenden Optionen aus: ▪ none: Keine Protokollierung. ▪ 1-line: Protokolliert nur die Startleitung für alle Nachrichten ▪ 1-line excl. OPT: Protokolliert nur die Startleitung für alle Nachrichten mit Ausnahme von OPTIONS-Anfragen/Antworten ▪ 1-line excl. NTFY: Protokolliert nur die Startleitung für alle Nachrichten mit Ausnahme von NOTIFY-Anfragen/Antworten ▪ 1-line excl. REG: Protokolliert nur die Startleitung für alle Nachrichten mit Ausnahme von REGISTER-Anfragen/Antworten ▪ 1-line excl. OPTINTFYIREG: Protokolliert nur die Startleitung für alle Nachrichten mit Ausnahme von OPTIONS-, NOTIFY- und REGISTER-Anfragen/Antworten ▪ full: Protokolliert alle SIP-Nachrichten im Volltext ▪ full excl. OPT: Protokolliert alle SIP-Nachrichten mit Ausnahme von OPTIONS-Anfragen/Antworten ▪ full excl. NTFY: Protokolliert alle SIP-Nachrichten mit Ausnahme von NOTIFY-Anfragen/Antworten ▪ full excl. REG: Protokolliert alle SIP-Nachrichten mit Ausnahme von REG-Anfragen/Antworten ▪ full excl. OPTINTFYIREG: Protokolliert alle SIP-Nachrichten im Volltext mit Ausnahme von OPTIONS-, NOTIFY- und REGISTER-Anfragen/Antworten Die Standardeinstellung ist None (Keine).
-------------------------------------	---

RTP Log Intvl (RTP-Protokollierungsintervall)	Intervall für die RTP-Protokollierung Der Standardwert ist 0.
Restrict Source IP (Quell-IP beschränken)	Wenn Leitung 1 und 2 den gleichen SIP-Port-Wert verwenden und die Funktion Restrict Source IP (Quell-IP beschränken) aktiviert ist, dann wird die Proxy-IP-Adresse für Leitung 1 und 2 als akzeptable IP-Adresse für beide Leitungen behandelt. Wählen Sie Yes (Ja), wenn Sie diese Funktion aktivieren möchten. Andernfalls wählen Sie No (Nein) aus. Wenn dieser Parameter konfiguriert ist, gehen auf der SRP alle Pakete, die von einer nicht vertrauenswürdigen IP-Adresse an den SIP-Port gesendet wurden, verloren. Eine IP-Adresse ist dann nicht vertrauenswürdig, wenn sie mit keiner der IP-Adressen übereinstimmt, die vom konfigurierten Proxy (oder ausgehenden Proxy, wenn die Funktion Use Outbound Proxy (Ausgehenden Proxy verwenden) aktiviert ist) aufgelöst wurden. Die Standardeinstellung ist No (Nein).
Referor Bye Delay (Bye-Verzögerung der weiterleitenden Partei)	Mit dieser Funktion können Sie steuern, wann die SRP eine BYE-Nachricht sendet, um veraltete Abschnitte eines Anrufs beim Abschluss von Anrufweiterleitungen zu beenden. Auf diesem Bildschirm können Sie mehrere Verzögerungseinstellungen konfigurieren: Referor (Weiterleitende Partei), Refer Target (Weiterleitungsziel), Referee (Empfänger der Weiterleitung), Refer-To Target (Ziel der Weiterleitung). Geben Sie für die Bye-Verzögerung bei der weiterleitenden Partei die entsprechende Zeitspanne in Sekunden ein. Der Standardwert ist 4.
Refer Target Bye Delay (Bye-Verzögerung des Weiterleitungsziels)	Geben Sie für die Bye-Verzögerung des Weiterleitungsziels die entsprechende Zeitspanne in Sekunden ein. Der Standardwert ist 0.

Referee Bye Delay (Bye-Verzögerung des Empfängers der Weiterleitung)	Geben Sie für die Bye-Verzögerung des Empfängers der Weiterleitung die entsprechende Zeitspanne in Sekunden ein. Der Standardwert ist 0.
Refer-To Target Contact (Ziel der Weiterleitung kontaktieren)	Wählen Sie Yes (Ja) aus, um das Refer-to Target (Ziel der Weiterleitung) zu kontaktieren. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
Sticky 183 (Sticky 183)	Wenn diese Funktion aktiviert ist, ignoriert die SRP nach Erhalt der ersten 183 SIP-Antworten für eine ausgehende INVITE-Nachricht weitere 180 SIP-Antworten. Wählen Sie Yes (Ja), wenn Sie diese Funktion aktivieren möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
Use Anonymous With RPID (Anonym mit RPID verwenden)	Wenn Sie diese Funktion auf Yes (Ja) festlegen, wird in der SIP-Nachricht anonymous (Anonym) verwendet. Die Standardeinstellung ist Yes (Ja).
Use Local Addr In From (Bei FROM-Nachrichten lokale Adresse verwenden)	Mit dieser Funktion wird die lokale SRP-IP-Adresse in der SIP-FRO-Nachricht verwendet. Die Standardeinstellung ist No (Nein).
Auth INVITE (INVITE-Anfragen authentifizieren)	Wenn diese Funktion aktiviert ist, wird für die ersten vom SIP-Proxy eingehenden INVITE-Anfragen eine Autorisierung verlangt.
Reply 182 On Call Waiting (Bei Anklopmodus mit 182 antworten)	Wenn diese Funktion aktiviert ist, sendet die SRP dem Anrufer eine SIP182-Antwort, wenn dieser bereits einen Anruf führt und die Leitung besetzt ist. Wählen Sie yes (Ja), wenn Sie diese Funktion aktivieren möchten. Die Standardeinstellung ist No (Nein).

Anruffunktionseinstellungen

Voice > Line 1-2 > Call Feature Settings (Sprache > Leitung 1-2 > Anruffunktionseinstellungen)

Blind Attn-Xfer Enable (Gesteuerte Anrufweiterleitung ohne Rückfrage aktivieren)	Mit dieser Funktion kann die SRP eine gesteuerte Anrufweiterleitung durchführen, indem sie den aktuellen Anrufabschnitt beendet und eine Weiterleitung ohne Rückfrage eines anderen Anrufabschnitts ausführt. Wenn diese Funktion deaktiviert ist, führt die SRP eine gesteuerte Anrufweiterleitung durch, indem sie den anderen Anrufabschnitt an den aktuellen Anrufabschnitt weiterleitet und dabei beide Anrufabschnitte aufrechterhält. Wählen Sie yes (Ja), wenn Sie diese Funktion nutzen möchten. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).
MOH Server (MOH- Server)	Benutzer-ID oder URL des automatisch antwortenden Streaming-Audio-Servers. Wenn nur die Benutzer-ID festgelegt ist, wird der aktuelle oder ausgehende Proxy kontaktiert. Warteschleifenmusik ist deaktiviert, wenn der MOH-Server nicht festgelegt ist.
Xfer When Hangup Conf (Weiterleitung nach beendeter Konferenz)	Diese Funktion veranlasst die SRP zu einer Weiterleitung, nachdem ein Konferenzgespräch beendet wurde. Wählen Sie aus dem Dropdown-Menü Yes (Ja) oder No (Nein). Die Standardeinstellung ist Yes (Ja).
Conference Bridge URL (URL der Konferenz- Bridge)	Diese Funktion unterstützt externes Konferenz-Bridging für n-Wege-Konferenzgespräche (n>2), anstatt die Audiodateien lokal zu mischen. Wenn Sie diese Funktion verwenden möchten, legen Sie diesen Parameter auf den Servernamen fest. Beispiel: conf@mysefver.com:12345 oder conf (die den Proxy-Wert als Domäne verwendet).
Conference Bridge Ports (Konferenz-Bridge-Ports)	Wählen Sie die maximale Teilnehmeranzahl für Konferenzgespräche. Bereich: 3 bis 10 Der Standardwert ist 3.

Proxy und Registrierung***Voice > Line 1–2 > Proxy and Registration (Sprache > Leitung 1-2 > Proxy und Registrierung)***

Proxy (Proxy)	SIP-Proxyserver für alle ausgehenden Anfragen
Outbound Proxy SIP (Ausgehender Proxy-SIP)	Ausgehender SIP-Proxyserver, wobei alle ausgehenden Anfragen als First Hop gesendet werden
Use Outbound Proxy (Ausgehenden Proxy verwenden)	Mit dieser Funktion wird die Verwendung eines ausgehenden Proxy aktiviert. Wenn dieser Parameter auf No (Nein) festgelegt ist, werden die Parameter Outbound Proxy (Ausgehender Proxy) und Use OB Proxy in Dialog (Ausgehenden Proxy im Dialog verwenden) ignoriert. Die Standardeinstellung ist No (Nein).
Use OB Proxy In Dialog (Ausgehenden Proxy im Dialog verwenden)	Mit dieser Funktion wird bestimmt, ob SIP-Anfragen innerhalb eines Dialogs an den ausgehenden Proxy gesendet werden müssen. Wird ignoriert, wenn dieser Parameter Use Outbound Proxy (Ausgehenden Proxy verwenden) auf No (Nein) festgelegt oder der Parameter Outbound Proxy (Ausgehender Proxy) leer ist. Die Standardeinstellung ist Yes (Ja).
Register (Registrieren)	Mit dieser Funktion können Sie die periodische Registrierung mit dem Proxy-Parameter aktivieren. Dieser Parameter wird ignoriert, wenn der Proxy nicht festgelegt ist. Die Standardeinstellung ist Yes (Ja).
Make Call Without Reg (Anrufe ohne Registrierung führen)	Mit dieser Funktion können vom Gerät ohne erfolgreiche (dynamische) Registrierung ausgehende Anrufe geführt werden. Wenn diese Funktion deaktiviert ist, ertönt kein Wählton, solange die Registrierung nicht erfolgreich war. Die Standardeinstellung ist No (Nein).
Register Expires (Registrierung läuft ab)	Ablaufwert in Sekunden bei einer REGISTER-Anfrage. Die SRP erneuert die Registrierung periodisch, kurz bevor die aktuelle Registrierung abläuft. Dieser Parameter wird ignoriert, wenn der Parameter Register (Registrieren) deaktiviert ist. Bereich: 0 – (2 ³¹ – 1) Sekunden Der Standardwert ist 3600.

Ans Call Without Reg (Anrufe ohne Registrierung beantworten)	Mit dieser Funktion können eingehende Anrufe ohne erfolgreiche (dynamische) Registrierung vom Gerät beantwortet werden. Die Standardeinstellung ist No (Nein).
Use DNS SRV (DNS-SRV verwenden)	Mit dieser Funktion wird festgelegt, ob eine DNS-SRV-Suche für Proxy und ausgehenden Proxy verwendet wird. Die Standardeinstellung ist No (Nein).
DNS SRV Auto Prefix (Automatische DNS-SRV-Vorwahl)	Ist diese Funktion aktiviert, stellt die SRP dem Namen des Proxy oder ausgehenden Proxy bei einer DNS-SRV-Suche nach diesem Namen automatisch "_sip._udp" voran. Die Standardeinstellung ist No (Nein).
Proxy Fallback Intvl (Intervall für Proxy-Fallback)	Mit diesem Parameter wird die Verzögerung (Sekunden) festgelegt, nach der die SRP einen neuen Versuch über die Proxyserver mit der höchsten Priorität (oder ausgehende Proxyserver) nach einem Failover mit einem Server niedrigerer Priorität startet. Dieser Parameter ist nur dann nützlich, wenn der SRP die Liste mit primären und Backup-Proxyservern über eine DNS-SRV-Datensatzsuche nach dem Servernamen bereitgestellt wurde. (Wenn mehrere DNS-A-Datensätze pro Servername verwendet werden, ist der Prioritätsbegriff nicht zulässig, und somit werden alle Hosts mit der gleichen Priorität behandelt, und die SRP versucht nach einem Failover keinen Fallback.) Der Standardwert ist 3600.

Proxy Redundancy Method (Proxy-Redundanz-Verfahren)	Wählen Sie Normal (Normal) oder Based on SRV Port (Auf Basis des SRV-Ports). Die SRP erstellt eine interne Liste von Proxys, die in den DNS-SRV-Datensätzen zurückgegeben werden. Wenn Sie Normal (Normal) auswählen, enthält die Liste die Proxys, geordnet nach Bedeutung und Priorität. Wenn Sie Based on SRV Port (Auf Basis des SRV-Ports) auswählen, verwendet die SRP die Portnummer auf Basis des erstgelisteten Proxyports. Die Standardeinstellung ist Normal (Normal).
Voice Mail Server (Voicemail-Server)	Geben Sie die URL oder IP-Adresse des Servers ein.
Mailbox Subscribe Expires (Mailbox-Abonnement läuft ab)	Mit dieser Funktion können Sie das Intervall für Hinweise auf noch nicht abgehornte Voicemail-Nachrichten festlegen.

Teilnehmerinformationen

Voice > Line 1-2 > Subscriber Information (Sprache > Leitung 1-2 > Teilnehmerinformationen)

Display Name (Anzeigename)	Anzeigename für die Anrufer-ID
User ID (Benutzer-ID)	Benutzer-ID für diese Leitung
Password (Passwort)	Passwort für diese Leitung
Use Auth ID (Authentifizierungs-ID verwenden)	Wählen Sie Yes (Ja), wenn Sie Authentifizierungs-ID und Passwort für die SIP-Authentifizierung verwenden möchten. Ansonsten wählen Sie No (Nein), um Benutzer-ID und Passwort zu verwenden. Die Standardeinstellung ist No (Nein).
Auth ID (Authentifizierungs-ID)	Authentifizierungs-ID für die SIP-Authentifizierung
Directory Number (Verzeichnisnummer)	Geben Sie die Nummer für diese Leitung ein.

Mini Certificate (Mini-Zertifikat)	Base64-kodiert vom Mini-Zertifikat, konkateniert mit dem öffentlichen 1024-Bit-Schlüssel der Zertifizierungsstelle, die das MC aller Teilnehmer in der Gruppe signiert. Der Standardwert ist leer.
SRTP Private Key (Privater SRTP-Schlüssel)	Base64-kodiert vom privaten 512-Bit-Schlüssel pro Teilnehmer für den Aufbau eines sicheren Anrufs. Der Standardwert ist leer.

Supplementary Service Subscription (Abonnement für ergänzende Dienste)

Die SRP bietet eine native Unterstützung für eine Vielzahl von erweiterten oder ergänzenden Diensten. Diese Dienste sind allesamt optional. Mit den in der folgende Liste angeführten Parametern können Sie einen speziellen ergänzenden Dienst aktivieren oder deaktivieren. Ein ergänzender Dienst sollte deaktiviert werden, wenn a) der Benutzer diesen nicht abonniert hat oder b) der Service Provider beabsichtigt, einen ähnlichen, nicht auf SRP-Basis laufenden Dienst zu unterstützen.

Voice > Line 1-2 > Supplementary Service Subscription (Sprache > Leitung 1-2 > Abonnement für ergänzende Dienste

Call Waiting Serv (Anklopfdienst)	Mit dieser Funktion können Sie den Anklopfdienst aktivieren. Die Standardeinstellung ist Yes (Ja).
Block CID Serv (Dienst zum Blockieren der CID)	Mit dieser Funktion können Sie den Dienst zum Blockieren der CID aktivieren. Die Standardeinstellung ist Yes (Ja).
Block ANC Serv (Dienst zum Blockieren anonymer Anrufe)	Mit dieser Funktion können Sie den Dienst zum Blockieren anonymer Anrufe aktivieren. Die Standardeinstellung ist Yes (Ja).
Dist Ring Serv (Dienst für unterschiedliche Klingeltöne)	Mit dieser Funktion können Sie den Dienst für unterschiedliche Klingeltöne aktivieren. Die Standardeinstellung ist Yes (Ja).

Cfwd All Serv (Dienst für Rufumleitung Alle Anrufe)	Mit dieser Funktion können Sie den Dienst für die Weiterleitung aller Anrufe aktivieren. Die Standardeinstellung ist Yes (Ja).
Cfwd Busy Serv (Dienst für Rufumleitung bei Besetzt)	Mit dieser Funktion können Sie den Dienst zur Anrufweiterleitung bei Besetztzeichen aktivieren. Die Standardeinstellung ist Yes (Ja).
Cfwd No Ans Serv (Dienst für Rufumleitung falls keine Antwort)	Mit dieser Funktion können Sie den Dienst zur Weiterleitung unbeantworteter Anrufe aktivieren. Die Standardeinstellung ist Yes (Ja).
Cfwd Sel Serv (Dienst für Rufumleitung ausgewählter Anrufe)	Mit dieser Funktion können Sie den Dienst zur Weiterleitung ausgewählter Anrufe aktivieren. Die Standardeinstellung ist Yes (Ja).
Cfwd Last Serv (Dienst für Rufumleitung des letzten Anrufs)	Mit dieser Funktion können Sie den Dienst zur Weiterleitung des letzten Anrufs aktivieren. Die Standardeinstellung ist Yes (Ja).
Block Last Serv (Dienst für Blockieren des letzten Anrufs)	Mit dieser Funktion können Sie den Dienst zum Blockieren des letzten Anrufs aktivieren. Die Standardeinstellung ist Yes (Ja).
Accept Last Serv (Dienst für Annahme des letzten Anrufs)	Mit dieser Funktion können Sie den Dienst zur Annahme des letzten Anrufs aktivieren. Die Standardeinstellung ist Yes (Ja).
DND Serv (DND-Dienst)	Mit dieser Funktion können Sie den Bitte-nicht-stören-Dienst aktivieren. Die Standardeinstellung ist Yes (Ja).
CID-Serv (CID-Dienst)	Mit dieser Funktion können Sie den Anrufer-ID-Dienst aktivieren. Die Standardeinstellung ist Yes (Ja).
CWCID Serv (CWCID-Dienst)	Mit dieser Funktion können Sie den Anklopf-Anrufer-ID-Dienst aktivieren. Die Standardeinstellung ist Yes (Ja).

Call Return Serv (Rückruf-Dienst)	Mit dieser Funktion können Sie den Rückrufdienst aktivieren. Die Standardeinstellung ist Yes (Ja).
Call Redial Serv (Wahlwiederholungsdienst)	Mit dieser Funktion können Sie den Wahlwiederholungsdienst aktivieren.
Call Back Serv (Rückrufdienst)	Mit dieser Funktion können Sie den Rückrufdienst aktivieren.
Three Way Call Serv (Dienst für Dreiergespräche)	Mit dieser Funktion können Sie den Dienst für Dreiergespräche aktivieren. Die Funktion Dreiergespräche ist für Dreierkonferenzen und die Anrufweiterleitung nach Ankündigung erforderlich. Die Standardeinstellung ist Yes (Ja).
Three Way Conf Serv (Dienst für Dreierkonferenzen)	Mit dieser Funktion können Sie den Dienst für Dreierkonferenzen aktivieren. Die Funktion Dreierkonferenzen ist für die Anrufweiterleitung nach Ankündigung notwendig. Die Standardeinstellung ist Yes (Ja).
Attn Transfer Serv (Dienst für die Anrufweiterleitung nach Ankündigung)	Mit dieser Funktion können Sie den Dienst für die Anrufweiterleitung nach Ankündigung aktivieren. Die Funktion Dreierkonferenzen ist für die Anrufweiterleitung nach Ankündigung notwendig. Die Standardeinstellung ist Yes (Ja).
Unattn Transfer Serv (Dienst für die Anrufweiterleitung ohne Ankündigung)	Mit dieser Funktion können Sie den Dienst für die Anrufweiterleitung ohne Ankündigung aktivieren. Die Standardeinstellung ist yes (Ja).
MWI Serv (MWI-Dienst)	Mit dieser Funktion können Sie den Dienst für Hinweise auf wartende Nachrichten aktivieren. Die Anzeige (Message Waiting Indicator, MWI) ist nur dann verfügbar, wenn die Bereitstellung einen Voicemail-Dienst umfasst. Die Standardeinstellung ist Yes (Ja).

VMWI Serv (VMWI-Dienst)	Mit dieser Funktion können Sie den VMWI-Dienst (FSK) aktivieren. Die Standardeinstellung ist Yes (Ja).
Speed Dial Serv (Kurzwahldienst)	Mit dieser Funktion können Sie den Kurzwahldienst aktivieren. Die Standardeinstellung ist Yes (Ja).
Secure Call Serv (Dienst für sichere Anrufe)	Mit dieser Funktion können Sie den Dienst für sichere Anrufe aktivieren. Die Standardeinstellung ist Yes (Ja).
Referral Serv (Weiterleitungsdienst)	Mit dieser Funktion können Sie den Weiterleitungsdienst aktivieren. Weitere Informationen finden Sie unter dem Parameter Referral Services Codes (Weiterleitungsdienstcodes). Die Standardeinstellung ist Yes (Ja).
Feature Dial Serv (Dienst für Funktionswähltöne)	Mit dieser Funktion können Sie den Dienst für Funktionswähltöne aktivieren. Weitere Informationen finden Sie unter dem Parameter Feature Dial Services Codes (Dienstcodes für Funktionsfreitöne). Die Standardeinstellung ist Yes (Ja).
Service Announcement Serv (Dienst für Dienstankündigung)	Mit dieser Funktion können Sie den Dienst für die Dienstankündigung aktivieren. Die Standardeinstellung ist Yes (Ja).

Audiokonfiguration

Voice > Line 1-2 > Audio Configuration (Sprache > Leitung 1-2 > Audiokonfiguration)

Preferred Codec (Bevorzugter Codec)	Bevorzugter Codec für alle Anrufe. (Der bei einem Anruf tatsächlich verwendete Codec hängt weiterhin vom Ergebnis des Codec-Aushandlungsprotokolls ab.) Wählen Sie aus den folgenden Optionen: G711u, G711a, G726-32 oder G729a. Die Standardeinstellung ist G711u.
Second Preferred Codec (Zweiter bevorzugter Codec)	Zweiter bevorzugter Codec für alle Anrufe. (Der bei einem Anruf tatsächlich verwendete Codec hängt weiterhin vom Ergebnis des Codec-Aushandlungsprotokolls ab.) Wählen Sie aus den folgenden Optionen: Unspecified (Nicht festgelegt), G711u, G711a, G726-32 oder G729a. Die Standardeinstellung ist Unspecified (Nicht festgelegt).
Third Preferred Codec (Dritter bevorzugter Codec)	Dritter bevorzugter Codec für alle Anrufe. (Der bei einem Anruf tatsächlich verwendete Codec hängt weiterhin vom Ergebnis des Codec-Aushandlungsprotokolls ab.) Wählen Sie aus den folgenden Optionen: Unspecified (Nicht festgelegt), G711u, G711a, G726-16, G726-24, G726-32, G726-40, G729a oder G723. Die Standardeinstellung ist Unspecified (Nicht festgelegt).
Use Pref Codec Only (Nur bevorzugten Codec verwenden)	Wählen Sie yes (Ja) aus, wenn Sie für alle Anrufe nur den bevorzugten Codec verwenden möchten. (Der Anruf schlägt fehl, wenn die Gegenseite diesen Codec nicht unterstützt.) Wählen Sie ansonsten no (Nein). Die Standardeinstellung ist No (Nein).
Silence Supp Enable (Pausenunterdrückung aktivieren)	Wählen Sie yes (Ja), wenn Sie die Pausenunterdrückung aktivieren möchten, sodass stille Audioframes nicht übertragen werden. Andernfalls wählen Sie No (Nein) aus. Die Standardeinstellung ist No (Nein).

Silence Threshold (Pausengrenzwert)	Stellen Sie den Grenzwert entsprechend ein: high (hoch), medium (mittel) oder low (niedrig). Die Standardeinstellung ist medium (mittel).
G729a Enable (G729a aktivieren)	Wählen Sie Yes (Ja), um die Verwendung des G.729a-Codec bei 8 Kbit/s zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
Echo Canc Enable (Echounterdrücker aktivieren)	Wählen Sie yes (Ja), um den Echounterdrücker zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
Echo Canc Adapt Enable (Anpassung des Echounterdrückers aktivieren)	Wählen Sie yes (Ja), um die Anpassung des Echounterdrückers zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
Echo Supp Enable (Echosperre aktivieren)	Wählen Sie yes (Ja), um die Echosperre zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX V21 Detect Enable (FAX-V21-Erkennung aktivieren)	Wählen Sie yes (Ja), um die Erkennung von V21-Faxtönen zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
G726-32 Enable (G726-32 aktivieren)	Wählen Sie yes (Ja), um die Verwendung des G726-32-Codec bei 32 Kbit/s zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX CNG Detect Enable (FAX-CNG-Erkennung aktivieren)	Wählen Sie yes (Ja), um die Erkennung von Faxruftönen (CNG) zu aktivieren. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX Passthru Codec (Fax-Passthrough-Codec)	Wählen Sie für den Fax-Passthrough-Codec entweder G711u oder G711a aus. Die Standardeinstellung ist G711u.

DTMF Process INFO (DTMF-Verarbeitungs- informationen)	Wählen Sie Yes (Ja), um die Funktion der DTMF-Verarbeitungsinformationen zu verwenden. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX Codec Symmetric (Symmetrischer FAX-Codec)	Wenn Sie möchten, dass die SRP während des Fax-Passthrough zwingend einen symmetrischen Codec verwendet, wählen Sie yes (Ja). Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
DTMF Process AVT (DTMF-Verarbeitungs-AVT)	Wählen Sie yes (Ja), um die Funktion der DTMF-Verarbeitungs-AVT zu verwenden. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX Passthru Method (FAX-Passthrough-Verfahren)	Wählen Sie das gewünschte Fax-Passthrough-Verfahren: None (Keine), NSE oder ReINVITE . Die Standardeinstellung ist NSE.
DTMF Tx Method (DTMF-Übertragungsverfahren)	Wählen Sie das Verfahren, mit dem Sie DTMF-Signale an die Gegenstelle senden möchten: InBand , AVT , INFO oder Auto . InBand sendet DTMF über den Audioweg. AVT sendet DTMF als AVT-Ereignisse. INFO verwendet das SIP-INFO-Verfahren. Auto nutzt InBand oder AVT je nach Ergebnis der Codec-Aushandlung. Die Standardeinstellung ist Auto .

DTMF Tx Mode (DTMF-Übertragungsmodus)	Der Übertragungsmodus für die DTMF-Erkennung steht für SIP-Informationen und AVT zur Verfügung. Sie können aus den folgenden Optionen wählen: Strict (Streng) oder Normal (Normal). Die Standardeinstellung ist Strict (Streng). Für diese Option gilt Folgendes: ▪ Für eine DTMF-Ziffer ist nach deren Erkennung eine extra lange Haltezeit erforderlich. ▪ Der DTMF-Pegelgrenzwert wird auf -20 dBm erhöht. Die untersten und obersten Grenzwerte für die Dauer sind wie folgt: ▪ Strenger Modus für AVT: 70 ms ▪ Normaler Modus für AVT: 40 ms ▪ Strenger Modus für SIP: 90 ms ▪ Normaler Modus für SIP-Info: 50 ms
FAX Process NSE (FAX-Verarbeitungs-NSE)	Wählen Sie yes (Ja), um die Funktion FAX-Verarbeitungs-NSE zu verwenden. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
Hook Flash Tx Method (Hook-Flash-Übertragungsverfahren)	Wählen Sie das Verfahren für die Signalisierung von Hook-Flash-Ereignissen: None (Keine), AVT oder INFO. Bei None (Keine) werden keine Hook-Flash-Ereignisse signalisiert. AVT verwendet RFC2833-AVT (Ereignis = 16). INFO verwendet SIP INFO mit dem das Signal einer einzelnen Leitung = hf im Nachrichtentext. Der MIME-Typ für diesen Nachrichtentext wird der Einstellung Hook Flash MIME Type (Hook-Flash-MIME-Typ) entnommen. Die Standardeinstellung ist None (Keine).
FAX Disable ECAN (ECAN für FAX deaktivieren)	Wenn diese Funktion aktiviert ist, wird der Echounterdrücker automatisch deaktiviert, wenn ein Fax-Ton erkannt wird. Wählen Sie yes (Ja), wenn Sie diese Funktion nutzen möchten. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist No (Nein).

Release Unused Codec (Nicht verwendeten Codec freigeben)	Mit dieser Funktion können Codecs, die nach der Codec-Aushandlung für den ersten Anruf nicht verwendet wurden, freigegeben werden, sodass andere Codecs für die zweite Leitung verwendet werden können. Wählen Sie yes (Ja), wenn Sie diese Funktion nutzen möchten. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX Enable T38 (T38 für Fax aktivieren)	Wählen Sie yes (Ja), wenn Sie die Verwendung des ITU-T T.38-Standards für FAX-Relay aktivieren möchten. Andernfalls wählen Sie no (Nein) aus. Die Standardeinstellung ist Yes (Ja).
FAX T38 Redundancy (FAX-T38-Redundanz)	Wählen Sie die entsprechende Zahl aus, um die Zahl der bisherigen Paketzustände festzulegen, die bei jedem Paket wiederholt werden. Wählen Sie 0, wenn Sie keine Zustandsredundanz festlegen möchten. Je höher die Zahl, desto größer die Paketgröße und desto mehr Bandbreite wird benötigt. Der Standardwert ist 1.
FAX T38 ECM Enable (FAX-T38-ECM aktivieren)	Wählen Sie yes (Ja), um den T.38-Fehlerkorrekturmodus zu aktivieren. Andernfalls wählen Sie no (Nein) aus.
FAX Tone Detect Mode (FAX-Ton-Erkennungsmodus)	Sie können bei diesem Parameter aus drei Werten wählen: ▪ caller or callee (Anrufer oder angerufene Partei): Die SRP erkennt den FAX-Ton sowohl beim Anrufer als auch bei der anrufenden Partei. ▪ caller only (Nur Anrufer): Die SRP erkennt den FAX-Ton nur beim Anrufer. ▪ callee only (Nur angerufene Partei): Die SRP erkennt den FAX-Ton nur bei der angerufenen Partei. Der Standardwert ist Caller (Anrufer) oder Callee (angerufene Partei).

Wählplan

Das standardmäßige Wählplanskript für jede Leitung lautet wie folgt: (*xxl[3469]1 1l0l00l[2- 9]xxxxxxl1xxx[2-9]xxxxxxlxxxxxxxxxxxx.). Die Syntax für einen Wählplanausdruck ist in der folgenden Tabelle beschrieben.

Voice > Line 1-2 > Dial Plan (Sprache > Leitung 1-2 > Wählplan)

Wählplaneintrag	Funktionen
*xx	Ermöglicht einen willkürlichen 2-stelligen Sternchencode
[3469]11	Ermöglicht x1 1-Folgen
0	Vermittlung
00	Internationale Vermittlung
[2-9]xxxxxx	Lokale US-Nummer
1xxx[2-9]xxxxxx	US 1 + 10-stellige Nummer für Ferngespräche
xxxxxxxxxxxx.	Alles Weitere (Internationales Ferngespräch, FWD ...)

Dial Plan (Wählplan)	Wählplanskript für diese Leitung Der Standardwert ist (*xxl[3469]1 1l0l00l[2- 9]xxxxxxl1xxx[2- 9]xxxxxxS0lxxxxxxxxxxxx.). Die Parameter sind jeweils durch ein Semikolon (;) voneinander getrennt. Beispiel 1: <pre>*1xxxxxxxxxx<:@fwdnat.pulver.com:5082;uid=jsmith;pwd=xy z</pre> Beispiel 2: <pre>*1xxxxxxxxxx<:@fwd.pulver.com;nat;uid=jsmith;pwd=xyz</pre> Beispiel 3: <pre>[39]11<:@gw0></pre>
PSTN Fallback Dial Plan (PSTN-Ausweichwählplan)	Wählplanskript zum Weiterleiten von Anrufen zum FXO-Port, wenn der IP-Dienst nicht verfügbar ist. Das Standardskript ist (S0<:@gw0>).

Enable IP Dialing (Wählen über IP aktivieren)	Mit dieser Funktion können Sie das Wählen über IP aktivieren oder deaktivieren. Wenn das Wählen über IP aktiviert ist, kann ein Benutzer [user-id@]a.b.c.d[:port] wählen, wobei '@', '.' ':' durch Eingabe von * gewählt werden, die Benutzer-ID numerisch sein muss (wie eine Telefonnummer), a, b, c, d zwischen 0 und 255 liegen müssen und der Port größer als 255 sein muss. Wenn der Port nicht festgelegt ist, wird 5060 verwendet. Port und Benutzer-ID sind optional. Wenn der Benutzer-ID-Abschnitt mit einem Muster im Wählplan übereinstimmt, dann wird er gemäß dem Wählplan als reguläre Telefonnummer interpretiert. Die INVITE-Nachricht wird allerdings weiterhin an den ausgehenden Proxy gesendet, wenn diese Funktion aktiviert ist. Die Standardeinstellung ist No (Nein).
Emergency Number (Notrufnummer)	Mit Kommas getrennte Liste von Notrufnummernmustern. Wenn ein ausgehender Anruf mit einem der Muster übereinstimmt, deaktiviert die SRP die Behandlung von Hook-Flash-Ereignissen. Die Bedingung wird nach Anrufende wieder auf normal zurückgesetzt. Ein leeres Feld bedeutet, dass keine Notrufnummer vorhanden ist. Die Nummer darf maximal 63 Zeichen lang sein. Die Standardeinstellung ist leer.

Konfiguration der FXS-Portpolarität

Voice > Line 1-2 > FXS Port Polarity Configuration (Sprache > Leitung 1-2 > Konfiguration der FXS-Portpolarität)

Idle Polarity (Polarität im inaktiven Zustand)	Polarität, bevor ein Anruf verbunden wird: Forward (Vorwärts) oder Reverse (Rückwärts) Die Standardeinstellung ist Forward (Vorwärts).
Caller Conn Polarity (Polarität der Anruferverbindung)	Polarität, nachdem ein ausgehender Anruf verbunden wurde: Forward (Vorwärts) oder Reverse (Rückwärts) Die Standardeinstellung ist Forward (Vorwärts).
Callee Conn Polarity (Polarität der Verbindung der angerufenen Partei)	Polarität, nachdem ein eingehender Anruf verbunden wurde: Forward (Vorwärts) oder Reverse (Rückwärts) Die Standardeinstellung ist Forward (Vorwärts).

Benutzerseiten (1–2)

Auf diesen Seiten können Sie die Benutzereinstellungen konfigurieren. Diese Seiten enthalten die folgenden Abschnitte:

- **Einstellungen Anrufweiterleitung**
- **Einstellungen zur Weiterleitung ausgewählter Anrufe**
- **Kurzwahleinstellungen**
- **Einstellungen für ergänzende Dienste**
- **Einstellungen für unterschiedliche Klingeltöne**
- **Einstellungen für den Klingelton**

Wenn ein Anruf über Leitung 1 oder 2 erfolgt, verwendet die SRP die Benutzer- und Leitungseinstellungen für diese Leitung; eine Benutzeranmeldung wird nicht unterstützt. Parameter-Tags für jeden Benutzer müssen im Konfigurationsprofil [1] oder [2] (entsprechend Leitung 1 oder 2) angehängt werden. Darauf wird der besseren Lesbarkeit wegen verzichtet.

Einstellungen Anrufweiterleitung

Voice > User 1–2 > Call Forward Settings (Sprache > Benutzer 1-2 > Einstellungen Anrufweiterleitung

Cfwd All Dest (Weiterleitungsziel für Rufumleitung Alle Anrufe)	Weiterleitungsnummer für den Dienst zur Weiterleitung aller Anrufe Die Standardeinstellung ist leer.
Cfwd Busy Dest (Weiterleitungsziel für Rufumleitung bei Besetzt)	Weiterleitungsnummer für den Dienst zur Anrufweiterleitung bei Besetztzeichen Die Standardeinstellung ist leer.
Cfwd No Ans Dest (Weiterleitungsziel für Rufumleitung falls keine Antwort)	Weiterleitungsnummer für den Dienst zur Weiterleitung unbeantworteter Anrufe Die Standardeinstellung ist leer.
Cfwd No Ans Delay (Weiterleitungsverzögerung für Rufumleitung falls keine Antwort)	Verzögerung in Sekunden, bevor der Dienst zur Weiterleitung unbeantworteter Anrufe initialisiert wird. Der Standardwert ist 20.

Einstellungen zur Weiterleitung ausgewählter Anrufe

Voice > User 1–2 > Selective Call Forward Settings (Sprache > Benutzer 1-2 > Einstellungen zur Weiterleitung ausgewählter Anrufe)

Cfwd Sel1- 8 Caller (Rufumleitung Sel1-8-Anrufer)	Muster der Anrufernummer, um den Dienst zur Weiterleitung ausgewählter Anrufe 1, 2, 3, 4, 5, 6, 7 oder 8 zu aktivieren Die Standardeinstellung ist leer.
Cfwd Sel1 - 8 Dest (Rufumleitungsziel Sel1-8-Anrufer)	Weiterleitungsnummer für den Dienst zur Weiterleitung ausgewählter Anrufe 1, 2, 3, 4, 5, 6, 7 oder 8 Die Standardeinstellung ist leer.
Cfwd Last Caller (Rufumleitung letzter Anrufer)	Anrufernummer, die aktiv an das Weiterleitungsziel des letzten Anrufs weitergeleitet wird. Zu diesem Zweck wird der Aktivierungscode für Weiterleitung des letzten Anrufs verwendet. Die Standardeinstellung ist leer.
Cfwd Last Dest (Rufumleitungsziel des letzten Anrufs)	Weiterleitungsnummer für die Weiterleitung letzter Anrufer Die Standardeinstellung ist leer.
Block Last Caller (Letzten Anrufer blockieren)	Anrufer-ID, die über den Dienst zum Blockieren des letzten Anrufers blockiert wird Die Standardeinstellung ist leer.
Accept Last Caller (Letzten Anrufer annehmen)	Anrufer-ID, die über den Dienst zur Annahme des letzten Anrufers akzeptiert wird Die Standardeinstellung ist leer.

Kurzwahleinstellungen

Voice > User 1–2 > Speed Dial Settings (Sprache > Benutzer 1-2 > Kurzwahleinstellungen)

Speed Dial 2-9 (Kurzwahl 2-9)	Zieltelefonnummer (oder URL), die den Kurzwahlen 2, 3, 4, 5, 6, 7, 8 oder 9 zugewiesen ist Die Standardeinstellung ist leer.
----------------------------------	---

Einstellungen für ergänzende Dienste

Die SRP bietet eine native Unterstützung für eine Vielzahl von erweiterten oder ergänzenden Diensten. Diese Dienste sind allesamt optional. Mit den in der folgende Liste angeführten Parametern können Sie einen speziellen ergänzenden Dienst aktivieren oder deaktivieren. Ein ergänzender Dienst sollte deaktiviert werden, wenn a) der Benutzer diesen nicht abonniert hat oder b) der Service Provider beabsichtigt, einen ähnlichen, nicht auf SRP-Basis laufenden Dienst zu unterstützen.

Voice > User 1-2 > Supplementary Service Settings (Sprache > Benutzer 1-2 > Einstellungen ergänzende Dienste)

CW Setting (Einstellung Anklopfen)	Mit dieser Einstellung können Sie das Anklopfen für alle Anrufe aktivieren oder deaktivieren. Die Standardeinstellung ist Yes (Ja).
Block CID Setting (Einstellung CID blockieren)	Mit dieser Einstellung können Sie das Blockieren der Anrufer-ID für alle Anrufe aktivieren oder deaktivieren. Die Standardeinstellung ist No (Nein).
Block ANC Setting (Einstellung ANC blockieren)	Mit dieser Einstellung können Sie das Blockieren anonymer Anrufe aktivieren oder deaktivieren. Die Standardeinstellung ist No (Nein).
DND Setting (Einstellung Bitte nicht stören)	Mit dieser Einstellung können Sie die Funktion Bitte nicht stören (DND) aktivieren oder deaktivieren. Die Standardeinstellung ist No (Nein).
CID Setting (Einstellung CID)	Mit dieser Einstellung können Sie das Erzeugen von Anrufer-IDs für alle Anrufe aktivieren oder deaktivieren. Die Standardeinstellung ist Yes (Ja).
CWCID Setting (Einstellung CWCID)	Mit dieser Einstellung können Sie das Erzeugen von Anrufer-IDs beim Anklopfen aktivieren oder deaktivieren. Die Standardeinstellung ist Yes (Ja).
Dist Ring Setting (Einstellung unterschiedliche Klingeltöne)	Mit dieser Einstellung können Sie unterschiedliche Klingeltöne aktivieren oder deaktivieren. Die Standardeinstellung ist Yes (Ja).
Secure Call Setting (Einstellung sichere Anrufe)	Wenn diese Funktion aktiviert ist, sind alle ausgehenden Anrufe standardmäßig sicher. Die Standardeinstellung ist No (Nein).

Message Waiting (Nachricht wartet)	Der Benutzer kann auch manuell Änderungen vornehmen, um die Markierung zu löschen oder festzulegen. Wenn Sie diesen Wert auf Yes (Ja) einstellen, können Sie den stotternden Wählton und das Signal für die Nachrichtenanzeige (VMWI) aktivieren. Dieser Parameter wird im Langzeitspeicher gespeichert und bleibt nach einem Neustart oder Ein- und Ausschalten erhalten. Die Standardeinstellung ist No (Nein).
Accept Media Loopback Request (Medien-Loopback-Anfrage annehmen).	Mit dieser Funktion können Sie steuern, wie eingehende Anfragen für eine Schleifenschaltung behandelt werden. Sie können aus den folgenden Optionen wählen: Never (Nie), Automatic (Automatisch) und Manual (Manuell), wobei: ▪ never (nie): Loopback-Anrufe werden nie angenommen; dem Anrufer wird mit 486 geantwortet. ▪ automatic (automatisch): Anruf wird automatisch ohne Klingeln angenommen ▪ manual (manuell): Zuerst klingelt das Telefon, und der Anruf muss vor Beginn des Loopback manuell angenommen werden. Die Standardeinstellung ist Automatic (Automatisch).
Media Loopback Mode (Medien-Loopback-Modus)	Schleifenschaltungsmodus, der lokal angewendet wird, wenn ein Anruf für eine Medien-Loopback-Anfrage geführt wird. Sie können aus den folgenden Optionen wählen: Source (Quelle) und Mirror (Spiegel). Die Standardeinstellung ist Source (Quelle). BEMERKUNG Wenn die SRP den Anruf beantwortet, wird der Modus vom Anrufer bestimmt.
Media Loopback Type (Typ des Medien-Loopback)	Typ der Schleifenschaltung, der verwendet wird, wenn ein Anruf für eine Anfrage für einen Medien-Loopback-Vorgang geführt wird. Sie können aus Media (Medien) und Packet (Paket) wählen. Die Standardeinstellung ist Media (Medien). Hinweis: Wenn die SRP den Anruf beantwortet, dann wird der Typ des Loopbacks vom Anrufer bestimmt (wenn mehrere Typen vorhanden sind, beantwortet die SRP stets den ersten angebotenen Typ des Loopbacks, wenn mehrere Typen enthalten sind).

Einstellungen für unterschiedliche Klingeltöne

Die Anrufernummernmuster werden mit Rufton 1 bis Rufton 8 in Übereinstimmung gebracht. Die erste Übereinstimmung (und nicht die größte) wird herangezogen, um den Teilnehmer zu warnen.

Voice > User 1–2 > Distinctive Ring Settings (Sprache > Benutzer 1-2 > Einstellungen für unterschiedliche Klingeltöne)

Ring1-8 Caller (Klingelton1-8-Anrufer)	Anrufnummernmuster, um den speziellen Klingelton bzw. CWT 1, 2, 3, 4, 5, 6, 7 oder 8 abzuspielen. Die Standardeinstellung ist leer.
---	--

Einstellungen für den Klingelton

Voice > User 1–2 > Ring Settings (Sprache > Benutzer 1-2 > Ruftoneinstellungen)

Default Ring (Standardklingelton)	Standardklingeltonmuster, 1–8, für alle Anrufer Der Standardwert ist 1.
Default CWT (Standard-CWT)	Standard-CWT-Muster, 1–8, für alle Anrufer Der Standardwert ist 1.
Hold Reminder Ring (Klingelton zur Erinnerung an die Warteschleife)	Klingeltonmuster, mit dem an einen Anruf in der Warteschleife erinnert wird, wenn das Telefon aufgelegt ist Der Standardwert ist 8.
Call Back Ring (Rückrufklingelton)	Klingeltonmuster für eine Rückrufbenachrichtigung Der Standardwert ist 7.

VPN-Konfiguration

In diesem Kapitel wird die Konfiguration von VPN-Richtlinien und -Einstellungen für die SRP beschrieben. Folgende Abschnitte sind enthalten:

- **IKE-Richtlinie**
- **IPSec-Richtlinie**
- **GRE-Tunnel**
- **VPN-Passthrough**
- **Cisco VPN Server**

Sie können in der Menüleiste **Configuration Utility** (Konfigurationsprogramm) über **VPN** auf diese Seiten zugreifen.

IKE-Richtlinie

Auf der Seite **IKE Policy** (IKE-Richtlinie) können Sie eine VPN-IKE-Richtlinie konfigurieren. Jede IKE-Richtlinie enthält die Parameter, die notwendig sind, um IKE-Authentifizierungsregeln festzulegen. Diese IKE-Richtlinien werden in verschiedenen VPN-Richtlinien verwendet.

SCHRITT 1 Klicken Sie auf **VPN > Site to Site IPSec VPN > IKE Policy** (VPN > standortübergreifende IP-Sec-VPN > IKE-Richtlinie). Das Fenster *IKE Policies* (IKE-Richtlinien) wird geöffnet.

In diesem Fenster können Sie die bestehenden IKE-Richtlinien aus der Liste der IKE-Richtlinien einsehen, Richtlinien bearbeiten, Richtliniendetails anzeigen und IKE-Richtlinien hinzufügen.

SCHRITT 2 Um eine IKE-Richtlinie hinzuzufügen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Konfigurationsfenster *IKE Policy* (IKE-Richtlinien) für die neue Richtlinie wird geöffnet.

- SCHRITT 3** Geben Sie im Feld **Policy Name** (Name der Richtlinie) einen eindeutigen Namen für die VPN-Richtlinie ein.
- SCHRITT 4** Wählen Sie aus der Dropdown-Liste einen Austauschmodus aus. Sie können zwischen **Main** (Hauptmodus) oder **Aggressive** (Aggressiver Modus) wählen.
- Wählen Sie den Hauptmodus, wenn Sie eine höhere Sicherheit bei langsamerer Verbindung wünschen. Wählen Sie den aggressiven Modus, wenn Sie eine schnellere Verbindung bei niedrigerer Sicherheit wünschen.
- SCHRITT 5** Legen Sie die IKE-SA-Parameter je nach Bedarf wie in der Tabelle **IKE-Richtlinieneinstellungen** definiert fest.
- SCHRITT 6** Wenn Sie mit einem XAUTH-Server verbunden sind, geben Sie Benutzernamen und Passwort ein. Wenn diese Funktion aktiviert ist, kann die SRP Benutzer eines externen Authentifizierungsservers, beispielsweise eines RADIUS-Servers, authentifizieren.
- SCHRITT 7** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

IKE-Richtlinieneinstellungen	
Feld	Beschreibung
Allgemein	
Policy Name (Name der Richtlinie)	Geben Sie einen eindeutigen Namen für die VPN-Richtlinie ein.

IKE-Richtlinieneinstellungen	
Feld	Beschreibung
Exchange Mode (Austauschmodus)	Wählen Sie den Exchange-Modus entsprechend Ihren Sicherheits- und Geschwindigkeitsanforderungen aus. ▪ Main (Hauptmodus): Wählen Sie diesen Modus, wenn Sie eine höhere Sicherheit bei langsamerer Verbindung wünschen. Der Hauptmodus basiert auf beidseitigem Schlüsselaustausch zwischen Initiator und Empfänger. Durch den Schlüsselaustauschprozess wird zwar die Verbindung verlangsamt, dafür jedoch die Sicherheit erhöht. ▪ Aggressive (Aggressiver Modus): Wählen Sie den aggressiven Modus, wenn Sie eine schnellere Verbindung bei niedrigerer Sicherheit wünschen. Im aggressiven Modus werden zwischen Initiator und Empfänger weniger Schlüssel ausgetauscht. Auf beiden Seiten erfolgt ein Informationsaustausch, noch bevor ein sicherer Kanal vorliegt.
IKE-SA-Parameter	
Encryption Algorithm (Verschlüsselungsalgorithmus)	Wählen Sie aus den folgenden Verschlüsselungsmodi aus: DES , 3DES , AES128 , AES192 und AES256 .
Authentication Algorithm (Authentifizierungsalgorithmus)	Wählen Sie aus den Folgenden einen Authentifizierungsalgorithmus für IKA SA aus: MD5 und SHA1 .
Pre Shared Key (Vorinstallierter Schlüssel)	Geben Sie einen alphanumerischen Schlüssel ein, den Sie mit dem IKE-Peer gemeinsam nutzen möchten.
Diffie-Hellman (DH) Group (Diffie-Hellman-(DH)-Gruppe)	Wählen Sie eine der folgenden DH-Gruppen aus, um die Stärke des Algorithmus in Bits festzulegen: Group 1 (768 Bits) (Gruppe 1 (768 Bits)) und Group 2 (1024 bits) (Gruppe 2 (1024 Bits)).

IKE-Richtlinieneinstellungen	
Feld	Beschreibung
Enable Dead Peer (DPD) Detection (Dead Peer Detection (DPD) aktivieren)	Wählen Sie Enable (Aktivieren), wenn Sie die DPD aktivieren möchten. Die Standardeinstellung ist Disabled (Deaktiviert). BEMERKUNG Die DPD ist für eine IKE-Regel nicht erforderlich. Ist sie jedoch aktiviert, erleichtert sie die Aufrechterhaltung der Verbindung in Zeiten ohne Datenverkehr.
DPD Interval (DPD-Intervall)	Geben Sie ein gültiges Intervall für DPD ein. Dieses Paket wird in Zeiten ohne Datenverkehr in einem Intervall (in Sekunden) periodisch gesendet.
DPD Timeout (DPD-Timeout)	Geben Sie ein Timeout (in Sekunden) für die Dead Peer Detection (DPD) ein.
Erweiterte Authentifizierung	
XAUTH Client Enable (XAUTH-Client aktivieren)	Aktivieren Sie diese Funktion, wenn der VPN-Peer Zugangsdaten für die erweiterte Authentifizierung benötigt. Die Standardeinstellung ist Disabled (Deaktiviert).
Username/ Password (Benutzername/ Passwort)	Geben Sie die Zugangsdaten ein, die die SRP verwendet, um mit dem Remote-Peer eine Verbindung herzustellen.

IPSec-Richtlinie

Auf der Seite **IPSec Policy** (IPSec-Richtlinie) können Sie eine VPN-IPSec-Richtlinie konfigurieren. Die IPSec-VPN-Richtlinie enthält die Parameter der **IPSec Security Association** (IPSec-Sicherheitszuordnungen), mit denen Verbindungs- und Schlüsseltyp festgelegt werden.

- SCHRITT 1** Klicken Sie auf **VPN > Site to Site IPSec VPN > IPSec Policy** (VPN > standortübergreifende IP-Sec-VPN > IPSec-Richtlinie). Das Fenster *IPSec Policy* (IPSec-Richtlinie) wird geöffnet.
- Auf dieser Seite können Sie die bestehenden IPSec-Richtlinien einsehen, IPSec-Richtlinien bearbeiten und hinzufügen. Sie können auch die Details zu jeder Richtlinie aus der Liste **IPSec Details** (IPSec-Details) anzeigen.
- SCHRITT 2** Um eine IPSec-Richtlinie hinzuzufügen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster *IPSec Policy* (IPSec-Richtlinie) wird geöffnet.
- SCHRITT 3** Wählen Sie **Enable** (Aktivieren), um die neue Richtlinie zu aktivieren.
- SCHRITT 4** Wählen Sie aus der Dropdown-Liste eine Richtlinien-Identifizierungsnummer aus.
- SCHRITT 5** Geben Sie im Feld **Policy Name** (Name der Richtlinie) einen eindeutigen Namen für die IPSec-Richtlinie ein.
- SCHRITT 6** Wählen Sie aus der Dropdown-Liste einen Richtlinientyp aus. Sie können zwischen **Auto** (Automatisch) oder **Manual** (Manuell) wählen.
- SCHRITT 7** Geben Sie die IPSec-Richtlinieneinstellungen unter Verwendung der Tabelle **IPSec-Richtlinieneinstellungen** ein.
- SCHRITT 8** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
- Die VPN-Richtlinie wird auf der Seite **IKE Policy Add Entry** (IKE-Richtlinieneintrag hinzufügen) in der Liste der IKE-Richtlinien angezeigt.

IPSec-Richtlinieneinstellungen	
Allgemeine Einstellungen	
Policy Name (Name der Richtlinie)	Geben Sie einen eindeutigen Namen für die VPN-Richtlinie ein.

IPSec-Richtlinieneinstellungen	
Policy Type (Richtlinientyp)	Legen Sie den Richtlinientyp fest. Sie können zwischen Auto Policy (Automatische Richtlinie) und Manual Policy (Manuelle Richtlinie) wählen. Die automatische Richtlinie setzt bei der Aushandlung der zufälligen Schlüssel das IKE-Protokoll ein, um eine erhöhte Sicherheit zu erzielen. Wenn Sie diese Option wählen, müssen Sie eine IKE-Richtlinie auch auf der Seite Site to Site IPSec VPN > IKE Policy (Standortübergreifende IPSec-VPN > IKE-Richtlinie) festlegen. Die manuelle Richtlinie verwendet IKE nicht, wodurch die Richtlinie zwar einfacher, dafür aber weniger sicher wird.
Remote Endpoint (Remote-Endgerät)	Wählen Sie, wie Sie das Remote-Gateway für diesen standortübergreifenden VPN-Tunnel identifizieren möchten. Geben Sie im Feld IP Address (IP-Adresse) eine IP-Adresse ein, geben Sie im Feld FQDN (FQDN) einen vollständig qualifizierten Domännennamen (fully qualified domain Name, FQDN) oder wählen Sie Any (Beliebig) (nur bei automatischer Richtlinie verfügbar) aus. Beachten Sie, dass die SRP für einen FQDN eine Verbindung mit einem DNS-Server herstellen können muss, um die Adresse vor Aufbau des VPN-Tunnels aufzulösen.
Encryption Algorithm (Verschlüsselungs- algorithmus)	Wählen Sie einen der folgenden Verschlüsselungsalgorithmen aus: DES (8 Zeichen), 3DES (24 Zeichen), AES-128 (16 Zeichen) AES192 (24 Zeichen) und AES256 (32 Zeichen).
Integrity Algorithm (Integritätsalgorithmus)	Wählen Sie einen der folgenden Integritätsalgorithmen aus: MD5 (16 Zeichen) oder SHA-1 (20 Zeichen).
Parameter für die automatische Richtlinie (Optionen werden nur angezeigt, wenn die automatische Richtlinie aktiviert ist)	
PFS (PFS)	Wählen Sie Enable (Aktivieren), um Perfect Forward Secrecy (PFS) zu aktivieren. Die Standardeinstellung ist Disabled (Deaktiviert). Bei dieser Funktion ist für jede Phase-2-Aushandlung ein neuer Diffie-Hellman-Austausch erforderlich. Dieser Prozess ist zwar langsamer, gewährleistet aber, dass keine Schlüssel von zuvor verwendeten Schlüsseln abhängig sind.

IPSec-Richtlinieneinstellungen	
SA Lifetime (SA-Gültigkeitsdauer)	Geben Sie die IPSec-SA-Gültigkeitsdauer in Sekunden ein. Der Standardwert ist 7800 (130 Minuten).
Parameter für die manuelle Richtlinie (Optionen werden nur angezeigt, wenn die manuelle Richtlinie aktiviert ist)	
SPI Incoming (Eingehender SPI)	Geben Sie für den eingehenden Sicherheitsparameterindex einen Hexadezimalwert zwischen 0x100 und 0xffffffff ein.
SPI Outgoing (Ausgehender SPI)	Geben Sie für den ausgehenden Sicherheitsparameterindex einen Hexadezimalwert zwischen 0x100 und 0xffffffff ein.
Encryption Algorithm Key (Verschlüsselungsalgorithmusschlüssel)	Geben Sie einen Hexadezimalwert für den Verschlüsselungsalgorithmusschlüssel ein. Die Länge des Schlüssels hängt von dem von Ihnen gewählten Verschlüsselungsalgorithmus ab. Die Schlüssellänge für 3DES beträgt beispielsweise 48 Hexadezimalziffern.
Integrity Algorithm Key (Integritätsalgorithmusschlüssel)	Geben Sie einen Hexadezimalwert für den Integritätsalgorithmusschlüssel ein. Die Länge des Schlüssels hängt von dem von Ihnen gewählten Integritätsalgorithmus ab. MD5 umfasst beispielsweise 32 Hexadezimalziffern und SHA-1 40 Hexadezimalziffern.
Lokale Datenverkehrsauswahl	
Local IP/IP Address/Subnet Mask (Lokale IP/IP-Adresse/Subnetzmaske)	Mit dieser Funktion können Sie festlegen, welche lokalen Hosts das VPN verwenden dürfen. Wählen Sie im Feld Single IP-Address (einzelne IP-Adresse) eine IP-Adresse oder im Feld Subnet Mask (Subnetzmaske) eine Subnetzmaske aus.
Remote Traffic Selection (Auswahl Remote-Datenverkehr)	
Remote IP/IP Address/Subnet Mask (Remote-IP/IP-Adresse/Subnetzmaske)	Datenverkehr von zugelassenen lokalen Hosts an die Remote-IP-Adresse oder das Subnetz wird über den VPN-Tunnel geleitet. Wählen Sie eine einzelne IP-Adresse oder Subnetzmaske aus.
Select IKE Policy (IKE-Richtlinie auswählen)	Wählen Sie eine IKE-Richtlinie, die Sie dieser IPSec-Richtlinie zuordnen möchten. Klicken Sie auf View IKE Table (IKE-Tabelle anzeigen), um alle IKE-Richtlinien anzuzeigen.

GRE-Tunnel

Auf der Seite **GRE Tunnel** (GRE-Tunnel) können Sie die Generic Routing Encapsulation (GRE) konfigurieren. Bei der GRE handelt es sich um ein von Cisco entwickeltes Tunneling-Protokoll, das eine Vielzahl an Pakettypen für Netzwerkschichtprotokolle in IP-Tunneln umfasst und an entfernten Punkten über ein IP-Internetwerk eine virtuelle Point-to-Point-Verknüpfung mit der SRP erstellen kann.

SCHRITT 1 Klicken Sie im Navigationsbereich auf **VPN > GRE Tunnel** (VPN > GRE-Tunnel). Das Fenster *GRE Tunnel* (GRE-Tunnel) wird geöffnet.

Auf dieser Seite können Sie die bestehenden GRE-Tunnel einsehen, GRE-Tunnel bearbeiten und neue GRE-Tunnel hinzufügen. Sie können auch die Details zu jedem Tunnel aus der Liste **GRE Details** (GRE-Details) anzeigen.

SCHRITT 2 Klicken Sie auf **Add Entry** (Eintrag hinzufügen), um einen GRE-Tunnel hinzuzufügen. Das Fenster für den neuen GRE-Tunnel wird geöffnet.

SCHRITT 3 Wählen Sie einen Identifizierungsnamen für den Tunnel, und geben Sie einen Namen für den Tunnel ein.

SCHRITT 4 Klicken Sie auf das Kontrollkästchen **Enable** (Aktivieren), um den Tunnel zu aktivieren.

SCHRITT 5 Legen Sie die Parameter für **Checksum** (Prüfsumme), **Sequence** (Folge) und **Key** (Schlüssel) in den entsprechenden Dropdown-Listen fest. Wenn Sie einen Schlüsselwert auswählen möchten, geben Sie dessen Wert in das Feld **Key Value** (Schlüsselwert) ein. Sie können einen Wert zwischen 0 und 4294967295 festlegen.

SCHRITT 6 Wählen Sie die WAN-Schnittstelle aus, über die der Tunnel verbunden werden soll. Beispiel: WAN1 oder WAN2. Die Standardeinstellung ist **System Default Route** (Systemstandardrate).

SCHRITT 7 Geben Sie die Ziel-IP-Adresse des Remote-Geräts ein, das den neuen Tunnel terminiert.

SCHRITT 8 Geben Sie die IP-Adresse und die Subnetzmaske des Remote-Hosts ein. Klicken Sie auf die Schaltfläche **Add** (Hinzufügen), um weitere IP-Adressen hinzuzufügen, oder klicken Sie auf **Delete** (Löschen), um eine IP-Adresse zu entfernen.

SCHRITT 9 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

GRE-Tunneleinstellungen	
Feld	Beschreibung
Tunnel Number (Tunnelnummer)	Wählen Sie eine Identifizierungsnummer für diesen Tunnel. Sie können maximal 10 Tunnel erstellen.
Tunnel Name (Name des Tunnels)	Geben Sie einen Namen als Beschreibung dieses Tunnels ein.
Enable (Aktivieren)	Klicken Sie auf das Kontrollkästchen, um den Tunnel zu aktivieren, oder entfernen Sie das Häkchen, um den Tunnel zu deaktivieren.
Checksum (Prüfsumme)	Wählen Sie Input (Eingang), Output (Ausgang), Both (Beides) oder None (Keine). Die Standardeinstellung ist None (Keine). Beim Parameter Input (Eingang) müssen alle eingehenden Pakete die korrekte Prüfsumme aufweisen. Beim Parameter Output (Ausgang) müssen die ausgehenden Pakete Prüfsummen aufweisen. Beim Parameter Both (Beide) müssen alle eingehenden und ausgehenden Pakete die Prüfsumme aufweisen.
Sequence (Folge)	Wählen Sie None (Keine), Both (Beide), Input (Eingang) oder Output (Ausgang). Die Standardeinstellung ist None (Keine). Beim Parameter Output (Ausgang) müssen ausgehende Pakete eine Folgenummer aufweisen. Beim Parameter Input (Eingang) müssen eingehende Pakete eine Folgenummer aufweisen. Beim Parameter Both (Beide) müssen eingehende und ausgehende Pakete eine Folgenummer aufweisen.
Key (Schlüssel)	Wählen Sie None (Kein), Both (Beide), Input (Eingang) und Output (Ausgang). Die Standardeinstellung ist None (Kein). Beim Parameter Input (Eingang) wird der Schlüssel für Eingänge festgelegt. Beim Parameter Output (Ausgang) wird der Schlüssel für Ausgänge festgelegt. Beim Parameter Both (Beide) wird der Schlüssel für beide Richtungen festgelegt.
Key value (Schlüsselwert)	Wenn Sie einen Schlüssel ausgewählt haben, geben Sie einen Schlüsselwert zwischen 0 und 4294967295 ein.

GRE-Tunneleinstellungen	
Feld	Beschreibung
WAN Interface Name (WAN-Schnittstellename)	Wählen Sie den WAN-Schnittstellennamen, der verwendet wird, um den GRE-Tunnel mit dem Remote-Host zu erstellen.
Destination IP or HostName (Ziel-IP oder Hostname)	IP-Adresse oder FQDN des Remote-Geräts, das den Tunnel terminiert.
Remote IP Address/Subnet Mask (Remote-IP-Adresse/Subnetzmaske)	Hier sind die Remote-Hosts und Netzwerke aufgelistet, die im Tunnel verfügbar sind.
Modify Remote IP Address/Subnet Mask (Remote-IP-Adresse/Subnetzmaske ändern)	Um einen Host oder ein Netzwerk festzulegen, der bzw. das über den Tunnel erreichbar ist, geben Sie die Adresse und Subnetzmaske ein. Klicken Sie danach auf Add (Hinzufügen). Um die Adresse zu entfernen, wählen Sie diese in der Liste Remote IP Address (Remote-IP-Adressen) aus, und klicken Sie auf Delete (Löschen).

VPN-Passthrough

Auf der Seite **VPN Passthrough** (VPN-Passthrough) können Sie das VPN-Passthrough für IPSec-, PPTP- und L2TP-Protokolle konfigurieren. Verwenden Sie diese Funktion bei Geräten, die über die SRP laufen und bei denen die IPSec-Tunnel unabhängig eingerichtet werden müssen, beispielsweise beim Verbinden dieser mit einem anderen Router im WAN.

-
- SCHRITT 1** Klicken Sie auf **VPN > Site to Site IPSec VPN > VPN Passthrough** (VPN > standortübergreifende IP-Sec-VPN > VPN-Passthrough). Das Fenster *VPN Passthrough* (VPN-Passthrough) wird geöffnet.
- SCHRITT 2** IPSec-, PPTP- und L2TP-Passthrough sind standardmäßig aktiviert. Klicken Sie auf **Disabled** (Deaktiviert), um eine dieser Passthrough-Optionen zu deaktivieren.
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

VPN-Passthrough-Einstellungen	
Feld	Beschreibung
IPSec Passthrough (IPSec-Passthrough)	Die Internetprotokollsicherheit (IPSec) ist eine Protokollsuite, über die der sichere Austausch von Paketen auf IP-Layer-Ebene erfolgt. IPSec-Passthrough ist standardmäßig aktiviert. Um IPSec-Passthrough zu deaktivieren, wählen Sie Disabled (Deaktiviert).
PPTP Passthrough (PPTP-Passthrough)	Das Point-to-Point Tunneling-Protokoll (PPTP) ermöglicht, dass das Point-to-Point-Protokoll (PPP) über ein IP-Netzwerk getunnelt werden kann. PPTP-Passthrough ist standardmäßig aktiviert. Um PPTP-Passthrough zu deaktivieren, wählen Sie Disabled (Deaktiviert).
L2TP Passthrough (L2TP-Passthrough)	Das Layer-2-Tunneling-Protokoll ist das Verfahren, mit dem Point-to-Point-Sitzungen über das Internet auf Layer-2-Ebene aktiviert werden. L2TP-Passthrough ist standardmäßig aktiviert. Um L2TP-Passthrough zu deaktivieren, wählen Sie Disabled (Deaktiviert).

Cisco VPN Server

In diesem Abschnitt wird beschrieben, wie Sie die Serverrichtlinien, Einstellungen und Benutzer für Cisco VPN Server konfigurieren. Mit Cisco VPN Server können Remote-Benutzer mithilfe von Cisco VPN Client über einen verschlüsselten IPSec-VPN-Tunnel auf Intranetressourcen zugreifen. Siehe www.cisco.com/go/vpnclient.

HINWEIS Sie können auf der SRP immer nur eine Option, VPN Server oder standortübergreifendes VPN, verwenden. Wenn Sie VPN Server aktivieren, wird das standortübergreifende VPN deaktiviert.

Konfigurieren von Gruppen

Auf der Seite „Group“ (Gruppe) können Sie die Einstellungen zum Steuern von Cisco VPN Server und die IPSec-Richtlinien für den Datenaustausch mit Remote-Benutzern konfigurieren.

- SCHRITT 1** Klicken Sie auf **VPN > Cisco VPN Server > Group** (VPN > Cisco VPN Server > Gruppe). Das Fenster *Group* (Gruppe) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Enable** (Aktivieren), um den VPN-Server zu aktivieren. Die Standardeinstellung lautet Deaktivieren.
- SCHRITT 3** Geben Sie unter „Identity“ (Identität) den **Group Name** (Gruppennamen) und das **Password** (Passwort) an.
- SCHRITT 4** Ändern Sie bei Bedarf die Einstellungen für **IKE Phase 1** (IKE-Phase 1) und **IKE Phase 2** (IKE-Phase 2), um sie den gewünschten IPSec-Richtlinien anzupassen.
- SCHRITT 5** Legen Sie die Einstellungen für die Moduskonfiguration fest.
- HINWEIS** Die SRP520-Modelle unterstützen bis zu 5 gleichzeitige Verbindungen/IP-Adresszuweisungen, die SRP540W-Modelle unterstützen bis zu 10.
- a. Legen Sie für das Feld **DNS1** die primäre DNS-Serveradresse fest. Im Feld **DNS2** können Sie optional einen Sicherungs-DNS-Server angeben.
 - b. Geben Sie ggf. die WINS-Server an, die verwendet werden sollen.
 - c. (Optional) Geben Sie eine Begrüßung in das Feld „Banner“ ein, falls gewünscht. Diese Nachricht wird dem VPN Client-Benutzer angezeigt, wenn die VPN-Sitzung herstellt wurde.
- SCHRITT 6** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Cisco VPN Server–Einstellungen

Gruppe	
Enable (Aktivieren)	Klicken Sie auf Enable (Aktivieren), um den VPN-Server zu aktivieren. Die Standardeinstellung lautet „Disable“ Deaktivieren. HINWEIS Alle definierten standortübergreifenden VPN-Tunnel werden durch die Aktivierung von VPN Server deaktiviert.
Identität	

Cisco VPN Server–Einstellungen

Group Name (Gruppenname)	Geben Sie den Namen für die „Cisco VPN Group“ (Cisco VPN-Gruppe) ein. Er dient als Kennung für den VPN-Server. Dieser Name muss mit dem im Profil von VPN Client angegebenen Gruppennamen übereinstimmen. Der Name kann bis zu 32 Zeichen lang sein, und es ist die Groß-/Kleinschreibung zu beachten.
Password (Passwort)	Geben Sie das Passwort für die „Cisco VPN Group“ (Cisco VPN-Gruppe) ein. Das Passwort muss mit dem im Profil von VPN Client angegebenen Passwort für die Gruppe übereinstimmen. Das Passwort kann bis zu 32 Zeichen lang sein, wobei die Groß-/Kleinschreibung zu beachten ist.
IKE Phase 1 (IKE-Phase 1)	
Aggressive Mode (Aggressiver Modus)	Der aggressive Modus wird standardmäßig angewendet und kann nicht geändert werden. Dieser Modus wird bei Verwendung von vorinstallierten Schlüsseln zur Authentifizierung für die Aushandlung von ISAKMP-SAs der ersten Phase (Internet Security Association and Key Management Protocol) genutzt.
ESP Algorithm (ESP-Algorithmus)	Geben Sie einen Verschlüsselungsalgorithmus für die ISAKMP-SAs ein. Zur Auswahl stehen AES, DES und 3DES. Die Standardeinstellung ist AES.
AH Algorithm (AH-Algorithmus)	Der für die ISAKMP-SAs verwendete Hash-Algorithmus. Sie können zwischen MD5 und SHA1 wählen. Die Standardeinstellung ist MD5.
Auth Method (Authentifizierungsmethode)	Die Methode zur Authentifizierung von Remote-Benutzern. Sie können zwischen PSK oder PSK+XAUTH wählen. Ist PSK (Pre-Shared Keys, vorinstallierte Schlüssel) ausgewählt, wird der Client authentifiziert, wenn er den Gruppennamen und das Passwort korrekt angibt. Wenn Sie PSK+XAUTH auswählen, sind ein zusätzlicher Benutzername und ein Passwort erforderlich.
DH Group (DH-Gruppe)	Die ausgewählte DH-Gruppe (Diffie-Hellman) bestimmt die Stärke des Algorithmus in Bits. Sie können nur die Option 2 (MODP 1024) auswählen.
IKE Phase 2P (IKE-Phase 2P)	

Cisco VPN Server–Einstellungen

PFS Group (PFS-Gruppe)	Wählen Sie eine DH-Gruppe für PFS in Phase 2 aus. Zur Auswahl stehen: 1 (MODP 768), 2 (MODP 1024), 5 (MODP 1536), 14 (MODP 2048) oder 15 (MODP 3072).
SA Lifetime (SA-Gültigkeitsdauer)	Definiert, wie lange eine IPSec-SA verwendet wird. Die Standardeinstellung ist 30 Minuten.
Mode Configuration (Moduskonfiguration)	
IP Pool (IP-Pool)	Starting IP Address (Start-IP-Adresse): Die erste IP-Adresse des Bereichs von Adressen, die dem Remote-Client zugewiesen sind. Dieser Bereich darf sich nicht im selben Subnetz wie ein VLAN befinden. Subnetzmaske: Maske für den Adressbereich, der den Remote-Clients zugewiesen ist. Die definierte Maske muss groß genug sein, um die maximale Anzahl an Verbindungen aufzunehmen, die von der SRP unterstützt werden.
DNS1	Primärer DNS-Server, der von den Remote-Clients verwendet wird.
DNS2	Sekundärer DNS-Server, der von den Remote-Clients verwendet wird.
WINS1	Primärer WINS-Server, der von den Remote-Clients verwendet wird.
WINS2	Sekundärer WINS-Server, der von den Remote-Clients verwendet wird.
Banner	Die Nachricht, die den Benutzern nach ihrer Anmeldung angezeigt wird. Das Banner kann bis zu 500 druckbare ASCII-Zeichen in 1 Zeile enthalten.

Konfigurieren von Benutzern

Die Seite „Users“ (Benutzer) enthält eine Liste der Benutzernamen, die für die Anmeldung am VPN-Server der SRP verwendet werden können. Sie können bis zu 15 eindeutige Benutzer definieren.

SCHRITT 1 Klicken Sie auf **VPN > Cisco VPN Server > Users** (VPN > Cisco VPN Server > Benutzer). Das Fenster *Users* (Benutzer) wird geöffnet.

Auf dieser Seite können Sie ein Benutzerkonto hinzufügen, bearbeiten oder löschen.

SCHRITT 2 Um einen neuen Benutzer hinzuzufügen, klicken Sie auf **Add Entry** (Eintrag hinzufügen). Das Fenster *User Account* (Benutzerkonto) wird geöffnet.

SCHRITT 3 Geben Sie einen **Username** (Benutzernamen) für den neuen Benutzer ein.

SCHRITT 4 Geben Sie ein **Password** (Passwort) ein, und geben Sie es im Feld **Confirm Password** (Passwort bestätigen) erneut ein.

SCHRITT 5 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Der Benutzer wird auf der Seite „Users“ (Benutzer) der Tabelle „List of VPN Server Users“ (Liste der VPN Server-Benutzer) hinzugefügt.

SCHRITT 6 Wiederholen Sie die Schritte 2 bis 5 für jeden Benutzer, der einen VPN-Zugang benötigt.

Einstellungen für Benutzerkonten

Username (Benutzername)	Der Benutzername, den der VPN-Client bei Verwendung von PSK+XAUTH als Authentifizierungsverfahren bereitstellen muss.
Password (Passwort)	Das Passwort, das der VPN-Client bei Verwendung von PSK+XAUTH als Authentifizierungsverfahren bereitstellen muss.
Confirm Password (Passwort bestätigen)	Der Inhalt dieses Felds muss mit dem des Felds „Password“ (Passwort) übereinstimmen.

Verwaltungseinstellungen

In diesem Kapitel werden die Verwaltungseinstellungen für die Services Ready-Plattformen erläutert. Folgende Themen sind enthalten:

- **Web Access Management (Webzugangsverwaltung)**
- **Remote-Management**
- **Time Setup (Zeiteinrichtung)**
- **Benutzerliste**
- **User Privilege Control (Benutzerberechtigungssteuerung)**
- **Protokollierung**
- **Factory Defaults (Werkseitige Einstellungen)**
- **Firmware Upgrade (Firmware-Upgrade)**
- **Datensicherung und -wiederherstellung**
- **Reboot (Neu starten)**
- **Status**
- **Switch Setting (Switch-Einstellung)**

Um auf diese Seiten zuzugreifen, klicken Sie in der Menüleiste des Konfigurationsprogramms auf **Administration** (Verwaltung).

Web Access Management (Webzugangsverwaltung)

Über die Seite für die Webzugangsverwaltung können Sie die Webzugangseinstellungen und die Remote-Zugangsregelungen für die SRP konfigurieren.

- SCHRITT 1** Klicken Sie auf **Administration > Web Access Management** (Verwaltung > Webzugangsverwaltung). Das Fenster *Web Access Management* (Webzugangsverwaltung) wird geöffnet.
- SCHRITT 2** Konfigurieren Sie die Remote-Zugangseinstellungen wie in der Tabelle **Einstellungen für die Webzugangsverwaltung** definiert.
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Einstellungen für die Webzugangsverwaltung	
Feld	Beschreibung
Web Access (Webzugang)	
Web Utility Access (Webprogrammzugang)	Wählen Sie HTTP und/oder HTTPS aus. Wählen Sie für einen sicheren Internetzugang HTTPS aus. Wenn Sie HTTPS auswählen, müssen Sie bei der Verbindung zum Dienstprogramm in die URL die Zeichenfolge „https“ einfügen. Beispiel: https://xxx.xxx.xxx.xxx, wobei die x für die IP-Adresse des Gateways stehen.
Web Utility Access via Wireless (Webprogrammzugang über Wireless)	Gibt dem Administrator die Möglichkeit, über einen lokalen Wireless-Client auf das Webdienstprogramm zuzugreifen.

Einstellungen für die Webzugangsverwaltung	
Feld	Beschreibung
Remote Access (Remote-Zugang)	
Remote-Management	Ermöglicht die Verwaltung der SRP über das Internet von einem Remote-Standort aus.
Web Utility Access (Webprogramm-zugang)	Wählen Sie HTTP oder HTTPS aus. Wählen Sie für einen sicheren Internetzugang HTTPS aus. Geben Sie für HTTPS in die Adresszeile Ihres Webbrowsers die Zeichenfolge <code>https://xxx.xxx.xxx.xxx</code> ein, wobei die x für die IP-Adresse des Gateways stehen.
Remote Upgrade (Remote-Aktualisierung)	Wenn diese Option aktiviert ist, kann die Firmware der SRP über das Internet aktualisiert werden. BEMERKUNG Sie können diese Einstellung nur ändern, wenn Sie die Verbindung zur Webschnittstelle über das LAN herstellen.
Allowed Remote IP Address (Zulässige externe IP-Adresse)	Um über eine externe IP-Adresse auf die SRP zugreifen zu können, wählen Sie Any IP Address (Beliebige IP-Adresse) aus. Um eine externe IP-Adresse oder einen externen IP-Adressbereich festzulegen, wählen Sie die zweite Optionsschaltfläche aus, und geben Sie die gewünschten IP-Adressen ein.
Remote Management Port (Remote-Management-Port)	Geben Sie die Nummer des Remote-Management-Ports ein. Die Standardportnummer lautet 8080.

Remote-Management

Auf den Remote-Management-Seiten können Sie die Einstellung für die folgenden Elemente konfigurieren:

- **TR069**
- **SNMP**
- **Local TFTP (Lokales TFTP)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Administration > Remote Management** (Verwaltung > Remote-Management).

TR069

Einige Service Provider können die Geräte am Standort Ihrer Kunden automatisch über einen zentralen Server verwalten. Auf der Seite für TR-069 können Sie die Kommunikation mit einem Auto-Configuration Server (ACS) einrichten.

SCHRITT 1 Klicken Sie auf **Administration > Remote Management > TR-069** (Verwaltung > Remote-Management > TR-069). Das Fenster *TR-069* wird geöffnet.

SCHRITT 2 Klicken Sie auf **Enabled** (Aktiviert), um die automatische Konfiguration der SRP über einen zentralen Server zu ermöglichen. Standardmäßig ist diese Option deaktiviert.

SCHRITT 3 Konfigurieren Sie die TR-069-Einstellungen wie in der Tabelle **TR-069-Einstellungen** definiert.

Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

TR-069-Einstellungen	
Feld	Beschreibung
Status	Klicken Sie auf Enabled (Aktiviert), um die automatische Konfiguration des Routers über einen zentralen Server zu ermöglichen. Standardmäßig ist diese Option deaktiviert.
ACS URL (ACS-URL)	Geben Sie die von Ihrem Service Provider bereitgestellte ACS-URL ein. Die ACS-URL nutzt das folgende Format: Protokoll://host:port/pfad - Als Protokoll sind http und https zulässig. - Der Host kann ein vollständig qualifizierter Domänenname oder eine IP-Adresse sein. - Der Port ist optional. - Der Pfad wird vom ACS festgelegt.
ACS Username (ACS-Benutzername)	Der Benutzername für den ACS. Der Standardbenutzername ist die OUI-Seriennummer. Dieser Benutzername muss mit dem ACS-Benutzernamen übereinstimmen.
ACS Password (ACS-Passwort)	Das Passwort für den ACS. Dieses Passwort muss mit dem ACS-Benutzernamen übereinstimmen.
Connection Request URL (URL für die Verbindungsanforderung)	Dieses Feld wird automatisch ausgefüllt. Das Format ist http://xxx.xxx.xxx.xxx:port. Die x stehen dabei für die WAN-IP-Adresse der SRP.
Connection Request Username (Benutzername für die Verbindungsanforderung)	Dieser Benutzername muss mit dem ACS-Benutzernamen übereinstimmen.
Connection Request Password (Passwort für die Verbindungsanforderung)	Dieses Passwort muss mit dem ACS-Benutzernamen übereinstimmen.

TR-069-Einstellungen	
Feld	Beschreibung
Periodic Inform Interval (Regelmäßiges Informationsintervall)	Gibt das Intervall (in Sekunden) an, in dem die SRP Verbindungen zum ACS initiiert. Der Standardwert ist 86400 Sekunden (24 Stunden).
Periodic Inform Enable (Regelmäßige Information aktivieren)	Wählen Sie Enabled (Aktiviert) aus, damit der Router regelmäßige Verbindungen zum ACS initiieren kann. Wählen Sie andernfalls Disabled (Deaktiviert) aus.
Request Download (Download anfordern)	Klicken Sie auf Apply (Anwenden), wenn sofort eine Verbindung zum ACS initiiert werden soll. Der ACS ruft den Download-RPC auf, wenn er die Anforderung empfängt.

SNMP

SNMP ist ein Protokoll für die Netzwerküberwachung und -verwaltung, mit dem Sie Ihr Netzwerk über einen SNMP-Manager überwachen und verwalten können. SNMP gibt Ihnen die Möglichkeit, Netzwerkgeräte zu überwachen und zu steuern und Konfigurationen, Statistikerfassungen, Leistung und Sicherheit zu verwalten. Die SRP unterstützt SNMPv2.

- SCHRITT 1** Klicken Sie auf **Administration > Remote Management > SNMP** (Verwaltung > Remote-Management > SNMP). Das Fenster *SNMP* wird geöffnet.
- SCHRITT 2** Um SNMP zu aktivieren, klicken Sie auf **Enabled** (Aktiviert).
- SCHRITT 3** Wählen Sie eine vertrauenswürdige IP-Einstellung aus. Sie können **Any** (Beliebig), **Address** (Adresse) oder **Netmask** (Netzmaske) auswählen. **Any** (Beliebig) wird nicht empfohlen.
- SCHRITT 4** Geben Sie die Get- und Set-Community-Passwörter ein.
- Das Get-Community-Passwort ermöglicht nur den Schreibzugriff auf die SNMP-Informationen des Gateways. Das Set-Community-Passwort ermöglicht den Lese- und Schreibzugriff.
- SCHRITT 5** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

SNMP-Einstellungen	
Feld	Beschreibung
Enable/Disable (Aktivieren/ Deaktivieren)	Um die SNMP-Identifizierung zu aktivieren, klicken Sie auf Enabled (Aktiviert). Standardmäßig ist diese Option deaktiviert.
Trusted IP (Vertrauenswürdige IP)	Wählen Sie Any (Beliebig) aus, um den Zugriff von jeder IP-Adresse aus zu erlauben (nicht empfehlenswert). Oder geben Sie die IP-Adresse und die Subnetzmaske eines einzelnen SNMP-Managers oder Trap Agent ein, der über SNMP auf die SRP zugreifen darf.
Get Community (Get-Community)	Geben Sie das Passwort ein, das nur den Schreibzugriff auf die SNMP-Informationen des Gateways erlaubt.
Set Community (Set-Community)	Geben Sie das Passwort ein, das den Lese- und Schreibzugriff auf die SNMP-Informationen des Gateways erlaubt.

SNMP-Portbeschreibungen

In den folgenden Tabellen werden die internen Linux-Schnittstellenbezeichnungen aufgeführt, die SNMP für das Anzeigen von Schnittstellen verwendet.

IP-Schnittstellen des SRP500	
br0	WAN Ethernet 1
br <i>n</i>	LAN VLAN <i>n</i> , wobei <i>n</i> = 1 bis 4079
br4080 bis br4083	ADSL PVC1 bis 4
lo	Loopback-Schnittstelle. Hostverwaltungsadressen, die im Konfigurationsprogramm und dem internen Loopback konfiguriert wurden (127.0.0.1).
ppp10	3G Modem PPP-Schnittstelle
gre0 bis gre9	GRE-Tunnelschnittstelle 1 bis 10
ipsec0 bis ipsec4	IPSec-Tunnelschnittstelle 1 bis 5
ath0 bis ath3	Wireless SSID 1 bis 4

Interne SRP500-Schnittstellen	
eth0	WAN-Ethernet-Schnittstelle
eth1	Interne Verbindung zum LAN-Switch
eth1 <i>n</i>	Interne Subschnittstellenverbindung zu LAN-VLANs (wobei <i>n</i> für die VLAN-Nummer 1 bis 4079 steht)
eth0.4080 bis eth0.4083	Interne überbrückte Verbindungen zu ADSL PVC 1 bis 4
eth0.4093	Interne Verbindung zum ADSL-Modem
wifi0	Interne Verbindung zum Wireless Access Point
ifb0	Derzeit nicht in Verwendung
fb1	Derzeit nicht in Verwendung
mast0	Derzeit nicht in Verwendung

Local TFTP (Lokales TFTP)

Auf der Seite für das lokale TFTP können Sie die SRP als TFTP-Server aktivieren. Wenn Sie TFTP aktivieren, können Sie über Remote-Zugriff Dateien auf die SRP herunterladen und sie anschließend als lokalen TFTP-Server einsetzen, um Hosts im LAN (z. B. IP-Telefonen) Dateien bereitzustellen.

- SCHRITT 1** Klicken Sie auf **Administration > Remote Management > Local TFTP** (Verwaltung > Remote-Management > Lokales TFTP). Das Fenster *Local TFTP Control* (Lokale TFTP-Steuerung) wird geöffnet.
- SCHRITT 2** Um TFTP zu aktivieren, klicken Sie auf **Enabled** (Aktiviert).
- SCHRITT 3** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
- SCHRITT 4** Konfigurieren Sie die Einstellungen für die Remote-Datei wie in der Tabelle **Lokale TFTP-Einstellungen** definiert.

Lokale TFTP-Einstellungen	
Feld	Beschreibung
TFTP	Wählen Sie Enabled (Aktiviert) aus, um TFTP zu aktivieren. Standardmäßig ist diese Option deaktiviert.
Abrufen von Einstellungen für die Remote-Datei	
Schnittstelle	Die Schnittstelle, über die die Remote-Dateien abgerufen werden.
URL	Geben Sie die URL ein, unter der die Remote-Dateien gespeichert sind. Beispiel: http://www.IhreWebsite.com:port/pfad/dateiname ftp://benutzername:passwort@IhreWebsite:port/pfad/dateiname.
Datei	Geben Sie den Namen der Remote-Datei ein.
Speichern unter	Geben Sie den Namen für die Datei ein, die Sie speichern möchten.
Benutzername	Geben Sie einen Benutzernamen für den Zugriff auf die Remote-Datei ein.
User Password (Benutzerpasswort)	Geben Sie ein Passwort für den Zugriff auf die Remote-Datei ein.

Lokale TFTP-Einstellungen	
Feld	Beschreibung
Timeout (Zeitüberschreitung)	Geben Sie den Wert für die Zeitüberschreitung (in Sekunden) an. Dies ist die maximal erlaubte Dauer für eine Verbindungssitzung. Die Verbindungszeitüberschreitung für HTTP- und FTP-Sitzungen beträgt 3 Sekunden. Die Verbindungszeitüberschreitung für TFTP beträgt 1 Sekunde. Bei HTTP und FTP wird eine Sitzung durch eine TCP-Antwortnachricht zum Zurücksetzen beendet.
Retry (Erneut versuchen)	Geben Sie an, wie oft erneut versucht werden soll, eine Verbindung herzustellen, wenn während einer Sitzung ein vorübergehender Fehler auftritt.
Status	Der Status der verarbeiteten Remote-Datei.
File List table (Dateilistentabelle)	Zeigt den Namen und die Größe der Remote-Datei an.

Time Setup (Zeiteinrichtung)

Auf der Seite für die Zeiteinrichtung können Sie die Zeitonenparameter für Ihr Netzwerk festlegen. Sie können das System manuell oder aber über den NTP-Server (Network Time Protocol) konfigurieren.

-
- SCHRITT 1** Klicken Sie auf **Administration > Time Setup** (Verwaltung > Zeiteinrichtung). Das Fenster *Time Setup* (Zeiteinrichtung) wird geöffnet.
- SCHRITT 2** Geben Sie die Einstellungen für Ihre Zeitzone ein. Die Zeitzone ist üblicherweise die lokale Zeit.
- SCHRITT 3** Um die Systemuhr manuell einzustellen, wählen Sie **User Manual** (Manuell durch Benutzer) aus, und geben Sie das Datum und die Zeitzone ein. Geben Sie das Datumsformat als „Jahr/Monat/Tag“ und das Zeitformat als „Stunde:Minute:Sekunde“ ein.
- SCHRITT 4** Um die Zeit automatisch festzulegen, konfigurieren Sie die Zeitzoneneinstellungen wie in der Tabelle **Einstellungen für die Zeiteinrichtung** definiert.
- SCHRITT 5** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.
-

Einstellungen für die Zeiteinrichtung	
Feld	Beschreibung
User Manual (Manuell durch Benutzer)	Um die Systemuhr manuell einzustellen, wählen Sie User Manual (Manuell durch Benutzer) aus, und geben Sie das Datum und die Zeitzone ein. Geben Sie das Datumsformat als „Jahr/Monat/Tag“ und das Zeitformat als „Stunde:Minute:Sekunde“ ein.
Zeitzone	
Regions (Regionen)	Wählen Sie die Zeitzone Ihrer Region aus der Dropdown-Liste aus. Beispiel: (GMT-8:00) Pacific Time (USA & Kanada)
Adjust Clock for Daylight Saving Changes (Auf Sommerzeit ändern)	Wählen Sie diese Option aus, damit die SRP automatisch die Sommerzeit berücksichtigt.
Time Server Address (Zeitserveradresse)	Wenn Sie den standardmäßigen NTP-Server (Network Time Protocol) der SRP verwenden möchten, wählen Sie aus der Dropdown-Liste die Option Auto (Automatisch) aus. Dies ist der Standard. Wenn Sie den NTP-Server selbst festlegen möchten, wählen Sie Manual (Manuell) aus, und geben Sie die URL oder IP-Adresse des gewünschten NTP-Servers ein.
Resync Timer (Timer für die Neusynchronisierung)	Geben Sie das Intervall für den Timer für die Neusynchronisierung (in Sekunden) an. Dieser Timer steuert, wie oft sich die SRP erneut mit dem NTP-Server synchronisiert. Die Voreinstellung ist 3600 Sekunden.

Setup Wizard (Installationsassistent)

Der Installationsassistent führt Sie durch die grundlegenden Schritte für die Konfiguration der SRP. Um den Installationsassistenten zu starten, klicken Sie auf der Registerkarte auf **Administration** (Verwaltung), und wählen Sie im Navigationsfenster die Option **Setup Wizard** (Installationsassistent) aus. Der Installationsassistent wird geöffnet. Folgen Sie den Anweisungen des Assistenten, um mit der Installation fortzufahren.

Benutzerliste

Auf der Seite für die Benutzerliste verwalten Sie die Benutzer, die Zugriff zum Konfigurationsprogramm haben.

Es gibt zwei Standardkonten, **admin** und **cisco**. Das Konto **admin** verfügt über Zugriff auf Administratorebene. Das Konto **cisco** verfügt über Zugriff auf Gastebene.

SCHRITT 1 Klicken Sie auf **Administration > User List** (Verwaltung > Benutzerliste). Das Fenster *User List* (Benutzerliste) wird geöffnet.

SCHRITT 2 Klicken Sie zum Bearbeiten auf das **Edit**-Symbol (Bleistift) für das Konto, das Sie ändern möchten.

Das Fenster *User Account* (Benutzerkonto) wird geöffnet.

SCHRITT 3 Geben Sie einen neuen Benutzernamen ein.

HINWEIS Die Standardbenutzernamen für **admin** und **cisco** können nicht geändert werden.

SCHRITT 4 Geben Sie das alte Passwort ein (nur für das Konto **admin**). Wenn Sie das Passwort ändern, werden Sie nach Ihrem alten Passwort gefragt.

SCHRITT 5 Geben Sie ein neues Passwort ein, und bestätigen Sie es. Maximal sind 32 Zeichen zulässig.

- Das Standardpasswort für den Administrator lautet **admin**.
- Das Standardpasswort für den Gast lautet **cisco**.

BEMERKUNG Beim Zugriff auf das Konfigurationsprogramm werden Sie auch nach Ihrem neuen Passwort gefragt. Aus Sicherheitsgründen wird nachdrücklich empfohlen, das Passwort zu ändern.

SCHRITT 6 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

User Privilege Control (Benutzerberechtigungssteuerung)

Auf der Seite für die Benutzerberechtigungssteuerung kann der Administrator die den Benutzern zugewiesenen Berechtigungen anpassen.

SCHRITT 1 Klicken Sie auf **Administration > User Privilege Control** (Verwaltung > Benutzerberechtigungssteuerung). Das Fenster *User Privilege Control* (Benutzerberechtigungssteuerung) wird geöffnet.

SCHRITT 2 Wählen Sie für die einzelnen Funktionen einen der folgenden Zugriffstypen.

- **Read/Write** (Lese-/Schreibzugriff) ermöglicht die Anzeige und Konfiguration der Webseite
- **Read Only** (Schreibzugriff) ermöglicht die Anzeige der Webseite
- **Hidden** (Ausgeblendet) blendet den Link zur Webseite aus

SCHRITT 3 Klicken Sie auf **Apply** (Anwenden), um die Einstellung zu speichern.

Protokollierung

Über die SRP können Sie Listen für eingehende, ausgehende und DHCP-Ereignisse aufzeichnen, die im Netzwerk auftreten. Unter **Incoming Log** (Eingehendes Protokoll) wird eine temporäre Liste der IP-Quelladressen und Zielportnummern für den eingehenden Internetverkehr angezeigt. Unter **Outgoing Log** (Ausgehendes Protokoll) wird eine temporäre Liste der lokalen IP-Adressen, Ziel-URLs/IP-Zieladressen und Service-/Portnummern für den ausgehenden Internetverkehr angezeigt.

SCHRITT 1 Klicken Sie auf **Administration > Log** (Verwaltung > Protokoll). Das Fenster *Log* (Protokoll) wird geöffnet.

SCHRITT 2 Klicken Sie auf **Enabled** (Aktiviert), um die Protokollierung zu aktivieren.

SCHRITT 3 Wählen Sie im Bereich **Log List** (Protokollliste) den Protokolltyp aus.

SCHRITT 4 Klicken Sie auf **Apply** (Anwenden), um die Einstellungen zu speichern.

Protokollierungseinstellungen

Feld	Beschreibung
Status	Um auf Aktivitätsprotokolle zuzugreifen, wählen Sie Enabled (Aktiviert) aus. Wenn die Protokollierung aktiviert ist, können Sie temporäre Protokolle anzeigen. Klicken Sie auf Disabled (Deaktiviert), um diese Funktion zu deaktivieren.
Log List (Protokollliste)	Der Protokolltyp. Legen Sie ihn als Incoming Log (Eingehendes Protokoll), Outgoing Log (Ausgehendes Protokoll) oder DHCP Client Log (DHCP-Client-Protokoll) fest.

Factory Defaults (Werkseitige Einstellungen)

Auf der Seite für die werkseitigen Einstellungen können Sie die SRP auf die Einstellungen zurücksetzen, mit denen sie beim Versand ab Werk konfiguriert war.

- SCHRITT 1** Klicken Sie auf **Administration > Factory Defaults** (Verwaltung > Werkseitige Einstellungen). Das Fenster *Factory Defaults* (Werkseitige Einstellungen) wird geöffnet.
- SCHRITT 2** Um die SRP auf die werkseitigen Einstellungen zurückzusetzen, klicken Sie auf **Yes** (Ja). Alle von Ihnen gespeicherten benutzerdefinierten Dateneinstellungen auf der SRP gehen durch das Zurücksetzen auf die werkseitigen Einstellungen verloren.
- SCHRITT 3** Um die Spracheinstellungen auf die werkseitigen Einstellungen zurückzusetzen, klicken Sie auf **Yes** (Ja). Alle von Ihnen gespeicherten benutzerdefinierten Spracheinstellungen auf der SRP gehen durch das Zurücksetzen auf die werkseitigen Einstellungen verloren.
- SCHRITT 4** Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Firmware Upgrade (Firmware-Upgrade)

Auf der Seite für die Firmware-Upgrades können Sie die SRP-Firmware aktualisieren. Ein Upgrade ist nur dann erforderlich, wenn Probleme mit dem Gerät auftreten oder wenn die neue Firmware über zusätzliche Funktionen verfügt, die Sie nutzen möchten. Bevor Sie die Firmware aktualisieren, müssen Sie die Upgrade-Datei für die SRP unter www.cisco.com/go/srp500 herunterladen. Klicken Sie auf den Link zum Herunterladen der Software, um die aktuelle Software herunterzuladen.

-
- SCHRITT 1** Klicken Sie auf **Administration > Firmware Upgrade** (Verwaltung > Firmware-Upgrade). Das Fenster *Firmware Upgrade* (Firmware-Upgrade) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie den Speicherort für die heruntergeladene Upgrade-Datei aus.
- SCHRITT 3** Klicken Sie auf **Upgrade**.
-



VORSICHT Der Upgrade-Vorgang für die Firmware kann einige Minuten in Anspruch nehmen. Vermeiden Sie es unbedingt, während des Vorgangs den Strom abzuschalten, die Hardware-Reset-Taste zu drücken oder im Browserfenster auf **Zurück** zu klicken.

Datensicherung und -wiederherstellung

In diesem Abschnitt wird beschrieben, wie Sie die Konfigurationseinstellungen für die SRP sichern und wiederherstellen. Folgende Themen sind enthalten:

- **Backup Configuration (Konfiguration sichern)**
- **Restore Configuration (Konfiguration wiederherstellen)**

Um auf diese Seiten zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Administration > Backup & Restore** (Verwaltung > Datensicherung und -wiederherstellung).

Backup Configuration (Konfiguration sichern)

Auf der Seite zum Sichern der Konfiguration können Sie die SRP-Konfigurationseinstellungen als Datei sichern. Später können Sie dieselben Einstellungen auf der SRP wiederherstellen.

-
- SCHRITT 1** Klicken Sie auf **Administration > Backup & Restore > Backup Configuration** (Verwaltung > Datensicherung und -wiederherstellung > Konfiguration sichern). Das Fenster *Backup Configuration* (Konfiguration sichern) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Backup** (Datensicherung), um die Konfigurationsdaten der SRP zu speichern.
-

Restore Configuration (Konfiguration wiederherstellen)

Auf der Seite zum Wiederherstellen der Konfiguration können Sie die SRP-Konfigurationseinstellungen aus einer vorherigen Datensicherung wiederherstellen. Stellen Sie sicher, dass Sie die Konfigurationseinstellungen gesichert haben, bevor Sie die Konfiguration wiederherstellen.

-
- SCHRITT 1** Klicken Sie auf **Administration > Backup & Restore > Restore Configuration** (Verwaltung > Datensicherung und -wiederherstellung > Konfiguration wiederherstellen). Das Fenster *Restore Configuration* (Konfiguration wiederherstellen) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Browse** (Durchsuchen), um die Sicherungsdatei zu suchen, und anschließend auf **Restore** (Wiederherstellen).
-

Reboot (Neu starten)

Über die Seite zum Neustarten können Sie die SRP bei Bedarf über das Konfigurationsprogramm neu starten.

-
- SCHRITT 1** Klicken Sie auf **Administration > Reboot** (Verwaltung > Neu starten). Das Fenster *Reboot* (Neu starten) wird geöffnet.
- SCHRITT 2** Klicken Sie auf **Reboot** (Neu starten), um die SRP herunterzufahren und neu zu starten.
-

Status

Auf der Statusseite können Sie den Status der CPU und des Speichers der SRP anzeigen. Die Statusinformationen werden in Echtzeit wiedergegeben.

Um auf diese Seite zuzugreifen, klicken Sie auf **Administration > Status** (Verwaltung > Status).

Auf dieser Seite können Sie Folgendes anzeigen:

- **CPU** (CPU) – MIPS, Ladezeit und Betriebszeit
- **Memory** (Speicher) – Gesamtgröße des Speichers (%), freier Speicher (%), verwendeter Speicher (%), Puffergröße (%), Cachegröße (%), aktiver und inaktiver Speicher (%)

Switch Setting (Switch-Einstellung)

Auf den DSL-Modellen SRP526W und SRP527W kann der Ethernet-Port 4 als WAN-Port konfiguriert werden. Außerdem können Sie über dieses Fenster die Jumbopaketgröße festlegen.

SCHRITT 1 Klicken Sie auf **Administration > Switch Setting** (Verwaltung > Switch-Einstellung).

Das Fenster *Switch Setting* (Switch-Einstellung) wird geöffnet.

SCHRITT 2 Wählen Sie **Disable** (Deaktivieren) aus, um den Ethernet-Port 4 als WAN-Port zu konfigurieren. Wählen Sie **Enable** (Aktivieren) aus, um den Ethernet-Port 4 als LAN-Port zu konfigurieren.

SCHRITT 3 Wählen Sie eine Jumbopaketgröße aus.

SCHRITT 4 Klicken Sie auf **Submit** (Senden), um die Einstellungen zu speichern.

Switch-Einstellungen

Feld	Beschreibung
DSL Interface (DSL-Schnittstelle)	Aktivieren oder deaktivieren Sie den DSL-Port. Wenn der DSL-Port aktiviert ist, funktioniert der Ethernet-Port 4 nur als LAN-Port. Wenn der DSL-Port deaktiviert ist, wechselt der Ethernet-Port 4 zwischen LAN- und WAN-Port.
Jumbo Mode (Jumbomodus)	Die Größe des Jumbopakets. Zur Auswahl stehen 1522 und 2048 Byte.

Verwenden der Diagnose für die Services Ready-Plattform

In diesem Kapitel wird die Verwendung der Diagnosefunktionen der Services Ready-Plattformen erläutert.

- **Ping Test (Ping-Test)**
- **Traceroute Test (Traceroute-Test)**
- **Detect Active LAN Clients (Aktive LAN-Clients erkennen)**

Klicken Sie in der Menüleiste des Konfigurationsprogramms auf die Registerkarte **Diagnostics** (Diagnose).

Ping Test (Ping-Test)

Über die Seite für den Ping-Test können Sie die Verbindung zwischen der SRP und einem verbundenen Gerät im Netzwerk testen.

-
- SCHRITT 1** Klicken Sie auf **Diagnostics > Ping Test** (Diagnose > Ping-Test). Das Fenster *Ping Test* (Ping-Test) wird geöffnet.
- SCHRITT 2** Geben Sie die IP- oder URL-Adresse ein, die Sie anpingen möchten.
- SCHRITT 3** Geben Sie eine Paketgröße in Byte ein. Der Bereich umfasst 32 bis 65500 Byte.
- SCHRITT 4** Wählen Sie aus der Dropdown-Liste aus, wie häufig ein Ping gesendet werden soll (5, 10 oder unbegrenzt).
- SCHRITT 5** Klicken Sie auf **Start to Ping** (Ping starten), um den Test zu starten. Nach Abschluss des Tests werden die Ergebnisse auf der Seite angezeigt.
- SCHRITT 6** Klicken Sie auf **Close** (Schließen), um die Testergebnisse zu schließen und das Formular anzuzeigen.
-

Traceroute Test (Traceroute-Test)

Über die Seite für die Traceroute können Sie den Weg zwischen der SRP und einem Ziel anzeigen.

-
- SCHRITT 1** Klicken Sie auf **Diagnostics > Traceroute Test** (Diagnose > Traceroute-Test). Das Fenster *Traceroute Test* (Traceroute-Test) wird geöffnet.
- SCHRITT 2** Geben Sie die IP- oder URL-Adresse ein, für die die Traceroute ausgeführt werden soll.
- SCHRITT 3** Klicken Sie auf **Start to Traceroute** (Traceroute starten), um den Test zu starten. Die Ergebnisse werden auf der Seite angezeigt und alle fünf Sekunden aktualisiert.
- SCHRITT 4** Klicken Sie auf **Close** (Schließen), um die Ergebnisse zu schließen und das Formular anzuzeigen.
-

Detect Active LAN Clients (Aktive LAN-Clients erkennen)

Auf der Seite zum Erkennen aktiver LAN-Clients können Sie nach aktiven LAN-Clients auf der SRP suchen.

-
- SCHRITT 1** Klicken Sie auf **Diagnostics > Detect Active LAN Client(s)** (Diagnose > Aktive LAN-Clients erkennen). Das Fenster *Detect Active LAN Client(s)* (Aktive LAN-Clients erkennen) wird geöffnet.
- SCHRITT 2** Wählen Sie aus der Dropdown-Liste die LAN-Schnittstelle aus, die Sie erkennen möchten. Beispiel: VLAN1.
- SCHRITT 3** Wählen Sie aus, wie lange diese Suche durchgeführt werden soll (5, 10 oder 15 Sekunden).
- SCHRITT 4** Klicken Sie auf **Start to Search** (Suche starten), um den Test zu starten. Die Testergebnisse werden in einem neuen Fenster angezeigt.
-

Anzeigen des Status der Services Ready-Plattformen

In diesem Kapitel wird erläutert, wie Sie den Status der Services Ready-Plattformen anzeigen.

- Router-Einstellungen
- Firewall Status (Firewall-Status)
- Interface Information (Schnittstelleninformationen)
- Wireless Network Status (Wireless-Netzwerk-Status)
- Wireless Client Information (Informationen zum Wireless-Client)
- Mobile Network Status (Mobilnetzstatus)
- DHCP Server Information (DHCP-Serverinformationen)
- QoS Status (QoS-Status)
- Routing Table (Routing-Tabelle)
- ARP Table (ARP-Tabelle)
- RIP Status (RIP-Status)
- IGMP Status (IGMP-Status)
- VPN Status (VPN-Status)
- CDP Neighbor Information (CDP-Nachbarinformationen)

Klicken Sie in der Menüleiste des Konfigurationsprogramms auf die Registerkarte **Status** (Status).

Router-Einstellungen

Auf der Seite für den Router werden Informationen zur SRP und ihren aktuellen Einstellungen angezeigt.

Status > Router (Status > Router)

Feld	Beschreibung
Modell	Produktname und -funktionen
Hardware Version (Hardware-Version)	Versionsnummer der Hardware
Boot Version (Startversion)	Versionsnummer der Start-Firmware
Firmware Version (Firmware-Version)	Aktuelle Firmware-Version
Recovery Firmware (Wiederherstellungs-Firmware)	Versionsnummer der Wiederherstellungs-Firmware
Setup Wizard Version (Version des Installationsassistenten)	Versionsnummer des Installationsassistenten
WAN MAC Address (WAN-MAC-Adresse)	MAC-Adresse der WAN-Schnittstelle
Current Time (Aktuelle Uhrzeit)	Auf der SRP eingestellte Uhrzeit
WAN	Typ und Ebene der WAN-Schnittstelle
LAN	LAN-Schnittstelle und Ebene
Wireless	Anzahl der aktivierten Wireless-SSIDs

Firewall Status (Firewall-Status)

Auf der Seite für den Firewall-Status können Sie die Informationen zur SRP-Firewall anzeigen.

Status > Firewall (Status > Firewall)

Firewall Status (Firewall-Status)	
Feld	Beschreibung
Internet Access Policy (Internet-Zugangsrichtlinie)	
Nein	Anzahl der Listen für die Internet-Zugangsrichtlinie
Policy Name (Richtliniennamen)	Numerische ID der Internet-Zugangsrichtlinie
Status	Zeigt den Status der Internet-Zugangsrichtlinie an. Klicken Sie auf den Link, um auf die Richtlinienkonfiguration zuzugreifen.
Passed (pkts) (Weitergeleitet (Pakete))	Anzahl der von dieser Regel weitergeleiteten Pakete
Passed (bytes) (Weitergeleitet (Byte))	Von dieser Regel weitergeleitetes Datenverkehrsvolumen in Byte
Blocked (pkts) (Blockiert (Pakete))	Anzahl der von dieser Regel blockierten Pakete
Blocked (bytes) (Blockiert (Byte))	Von dieser Regel weitergeleitetes Datenverkehrsvolumen in Byte
Port Forwarding (Portweiterleitung)	Zeigt den Status der derzeit aktiven Regeln für die Portweiterleitung an. Nicht aktivierte Regeln oder Regeln, die nicht verbundenen WAN-Schnittstellen zugewiesen sind, werden nicht angezeigt.
Typ	Gibt an, ob die Weiterleitung für einen einzelnen Port oder einen Portbereich gilt
Protokoll	Gibt an, an welchen Port die Daten weitergeleitet werden

Firewall Status (Firewall-Status)	
Feld	Beschreibung
Port	Gibt den vom Benutzer definierten Port für die Weiterleitung an
Host	IP-Adresse des LAN-Hosts, an den die Daten weitergeleitet werden
Packets (Pakete)	Anzahl der weitergeleiteten Pakete
Traffic (bytes) (Datenverkehr (Byte))	Weitergeleitetes Datenverkehrsvolumen in Byte
Statistik	Allgemeine Messungen des durch die Firewall geleiteten Datenverkehrs
Name	Mit der Firewall-Paketverarbeitung verbundener Name ▪ INPUT (Eingabe): Für die SRP vorgesehener Datenverkehr ▪ OUTPUT (Ausgabe): Von der SRP stammende Datenverkehr ▪ FORWARD (Weiterleiten): Zwischen dem öffentlichen/externen und privaten/internen Netzwerk übertragener Datenverkehr
Accept PKT (Akzeptierte Pakete)	Anzahl der über diesen Firewall-Pfad akzeptierten Pakete
Accept Volume (bytes) (Akzeptierte Pakete (Byte))	Über diesen Firewall-Pfad verarbeitetes Datenverkehrsvolumen in Byte
Drop PKT (Blockierte Pakete)	Anzahl der über diesen Firewall-Pfad blockierten Pakete
Drop Volume (bytes) (Blockiertes Volumen (Byte))	Über diesen Firewall-Pfad gefiltertes/blockiertes Datenverkehrsvolumen in Byte

Interface Information (Schnittstelleninformationen)

Auf der Seite mit den Schnittstelleninformationen können Sie Daten zu den verschiedenen Schnittstellen anzeigen lassen.

Status > Interface (Status > Schnittstelle)

Interface Information (Schnittstelleninformationen)	
Feld	Beschreibung
Interface List (Schnittstellenliste)	
Schnittstelle	Führt alle aktuell konfigurierten LAN- und WAN-Schnittstellen der dritten Ebene (IP) auf. Eine Ethernet-WAN-Schnittstelle wird als „WAN“ und eine ADSL-WAN-Schnittstelle als „PVC“ angezeigt. Es gilt folgende Nummerierung der Schnittstellen: ▪ Primary Interfaces (Primäre Schnittstellen): Die Nummerierung orientiert sich an der physischen Portbezeichnung (WAN1 und WAN2). ▪ Ethernet WAN Sub-interfaces (Ethernet-WAN-Unterschnittstellen): Die Nummerierung entspricht dem konfigurierten VLAN-Index. ▪ ADSL PVCs (ADSL-PVCs): Die Nummerierung erfolgt seriell von 0 bis 3. ▪ VLAN Interfaces (VLAN-Schnittstellen): Die Nummerierung entspricht dem konfigurierten VLAN-Index.
Connect Type (Verbindungstyp)	Von der Schnittstelle verwendetes Protokoll
IP-Adresse	IP-Adresse der Schnittstelle
Subnet Mask (Subnetzmaske)	Subnetzmaske der Schnittstelle
MAC-Adresse	MAC-Adresse der Schnittstelle

Interface Information (Schnittstelleninformationen)	
Feld	Beschreibung
Port List (Portliste)	
Schnittstelle	Führt alle aktuell konfigurierten LAN- und WAN-Schnittstellen der zweiten Ebene (Ethernet, Wi-Fi-SSID, DSL-PVC) auf
TX (pkts) (Übertragung (Pakete))	Anzahl der über diesen Port übertragenen Pakete
RX (pkts) (Übertragung (Pakete))	Anzahl der über diesen Port empfangenen Pakete
Status	Portverbindungsstatus
Clear TX & RX (Übertragung und Empfang löschen)	Klicken Sie auf diese Schaltfläche, um die Übertragungs- und Empfangspakete auf 0 zurückzusetzen.

Wireless Network Status (Wireless-Netzwerk-Status)

Auf der Seite für den Status des Wireless-Netzwerks können Sie Informationen zu den Wireless-Netzwerken anzeigen.

Status > Wireless (Status > Wireless)

Wireless Network (Wireless-Netzwerk)	
Feld	Beschreibung
Network Mode (Netzwerkmodus)	Für den integrierten Wireless Access Point konfigurierter Betriebsmodus. Weitere Informationen erhalten Sie unter Einrichten des Wireless LAN, Seite 49 .
Radio Band (Frequenzband)	Vom Wireless-Netzwerk verwendete Kanalbandbreite
Channel	Derzeit verwendeter Wireless-Kanal

Wireless Network (Wireless-Netzwerk)	
Feld	Beschreibung
Wireless List (Wireless-Liste)	Aktuelle SSID-Konfiguration Die Liste enthält die folgenden Spalten: ▪ SSID Name (SSID-Name): Konfigurierter SSID-Name ▪ Status (Status): SSID ist aktiviert oder deaktiviert ▪ Broadcast (Broadcast): SSID-Broadcast ist aktiviert oder deaktiviert ▪ Security (Sicherheit): Aktuelle Sicherheitseinstellungen ▪ WPS (WPS): WPS für diese SSID ist aktiviert oder deaktiviert

Wireless Client Information (Informationen zum Wireless-Client)

Auf der Seite mit den Informationen zum Wireless-Client können Sie Informationen zum Wireless-Client anzeigen.

Status > Wireless Client Information (Status > Informationen zum Wireless-Client)

Wireless Client Information (Informationen zum Wireless-Client)	
Feld	Beschreibung
MAC-Adresse	MAC-Adresse des Clients
Tx-Rate (Übertragungsrate)	Aktuelle Datenübertragungsrate des Clients
Rx-Rate (Empfangsrate)	Aktuelle Datenempfangsrate des Clients
RSSI (RSSI)	Signalstärke des zuletzt empfangenen Pakets
IDLE (Inaktiv)	Aktuelle Einstellung des Inaktivitäts-Timers der Station. Dies ist die Zeit in Millisekunden, nach der die Station in den Energiesparmodus wechselt, wenn auf der Verbindung keine Aktivität verzeichnet wird.

Mobile Network Status (Mobilnetzstatus)

Auf der Seite für den Mobilnetzstatus können Sie Informationen zu dem auf der SRP installierten USB-Breitbandmodem anzeigen.

HINWEIS Diese Seite ändert sich je nach Typ des installierten USB-Modems.

Status > Mobile Network (Status > Mobilnetz)

Einstellungen der USB-UMTS-Karte	
Feld	Beschreibung
IP-Adresse	Dem USB-Modem zugewiesene IP-Adresse
Connection Up Time (Verbindungszeit)	Dauer der aktuell verbundenen Sitzung
Current Session Usage (Aktuelle Auslastung der Sitzung)	Volumen der empfangenen und übertragenen Daten
Hersteller	Hersteller des angeschlossenen USB-Modems
Card Model (Kartenmodell)	Modellname des angeschlossenen USB-Modems
Card Firmware (Karten-Firmware)	Aktuell auf dem USB-Modem installierte Firmware-Version
SIM Status (SIM-Status)	Status der SIM-Karte (SIM ist bereit oder PIN-Code erforderlich)
IMSI (IMSI)	IMSI-Nummer des USB-Modems
Service Type (Servicetyp)	Servicetyp des USB-Modems
Signal Strength (Signalstärke)	Signalstärke
Card Status (Kartenstatus)	Status der Karte: Verbindung wird hergestellt, verbunden, Verbindung wird getrennt, nicht verbunden oder Karte nicht aktiviert. Wenn keine Karte angeschlossen ist, wird auf der Statusseite angezeigt, dass die SRP kein USB-Mobilmodem erkennen kann.

Einstellungen der USB-CDMA2000-EVDO-Karte	
Feld	Beschreibung
IP-Adresse	Dem USB-Modem zugewiesene IP-Adresse
Connection Up Time (Verbindungszeit)	Dauer der aktuell verbundenen Sitzung
Current Session Usage (Aktuelle Auslastung der Sitzung)	Volumen der empfangenen und übertragenen Daten
Hersteller	Hersteller des angeschlossenen USB-Modems
Card Model (Kartenmodell)	Modellname des angeschlossenen USB-Modems
Card Firmware (Karten-Firmware)	Aktuell auf dem USB-Modem installierte Firmware-Version
ESN (ESN)	ESN-Nummer des USB-Modems
PRL Version (PRL-Version)	PRL-Version des USB-Modems
Telefonnummer	Mit dem Konto des USB-Modems verbundene Telefonnummer
Transportunternehmen	Name des Betreibers des USB-Modemdienstes
Signal Strength (Signalstärke)	Signalstärke
Card Status (Kartenstatus)	Status der Karte: Verbindung wird hergestellt, verbunden, Verbindung wird getrennt, nicht verbunden oder Karte nicht aktiviert. Wenn keine Karte angeschlossen ist, wird auf der Statusseite angezeigt, dass die SRP kein USB-Mobilmodem erkennen kann.

DHCP Server Information (DHCP-Serverinformationen)

Auf der Seite für den DHCP-Serverstatus können Sie die Lease-Informationen des DHCP-Servers nach Regel anzeigen.

Status > DHCP Server Information (Status > DHCP-Serverinformationen)

DHCP-Serverstatus	
Feld	Beschreibung
Kundenname	Hostname des DHCP-Clients
IP-Adresse	An den Client geleaste IP-Adresse
MAC-Adresse	MAC-Adresse des DHCP-Clients
Expires Time (Ablaufzeit)	Ablaufzeit der aktuellen DHCP-Lease
Schnittstelle	Schnittstelle, über die der Client verbunden ist

QoS Status (QoS-Status)

Auf der Seite für den QoS-Status werden Statistiken zum Datenverkehr und zu den Warteschlangen angezeigt. Die SRP unterstützt fünf Warteschlangen: eine Warteschlange mit höchster Priorität und vier gewichtete Round-Robin-Warteschlangen.

Status > QoS (Status > QoS)

QoS Status (QoS-Status)	
Feld	Beschreibung
Queue Name (Name der Warteschlange)	Führt die fünf von der SRP verwendeten Warteschlangen auf
Config Rate (Konfigurationsrate)	Nominale Menge an Datenverkehr, die die einzelnen Warteschlangen unter balancierten und ausgelasteten Bedingungen verarbeiten können. Beachten Sie, dass die Bandbreite, die von einer Warteschlange nicht ausgenutzt wird, von einer anderen Warteschlange verwendet werden kann, d. h. dass die konfigurierte Bandbreite der einzelnen Warteschlangen überschritten werden kann.
Allow Maximum Rate (Maximal zulässige Rate)	Maximal zulässige Datenverkehrsrate in Kbit/s für die einzelnen Warteschlangen. Gewichtete Round-Robin-Warteschlangen können die gesamte konfigurierte Bandbreite nutzen, während der Verkehr über die Warteschlange höchster Priorität auf 70 % des Gesamtwerts beschränkt ist, um eine zuverlässige Verarbeitung von Echtzeitmedien sicherzustellen.
Send (bytes) (Gesendet (Byte))	Menge der über diese Warteschlange gesendeten Byte
Send (pkts) (Gesendet (Pakete))	Die Anzahl der über diese Warteschlange gesendeten Pakete.
Drop (Blockiert)	Anzahl der wegen Überschreitung der maximal zulässigen Gesamtverkehrsrate blockierten Pakete
Overlimits (Maximale Rate überschritten)	Anzahl der wegen Überschreitung der maximal zulässigen Datenverkehrsrate blockierten Pakete

QoS Status (QoS-Status)	
Feld	Beschreibung
Requeues (Wiedereinordnung)	Wenn ein Paket nicht gesendet werden kann, wird es erneut in die ursprüngliche Warteschlange eingeordnet, um das Senden erneut zu versuchen. Dieses Ereignis setzt den Zähler für die Wiedereinordnung nach oben.
Current Rate (bps) (Aktuelle Rate (Bit/s))	Aktuelle Durchsatzrate für diese Warteschlange in Bit pro Sekunde

Routing Table (Routing-Tabelle)

Auf der Statusseite für die Routing-Tabelle können Sie Routing-Informationen anzeigen.

Status > Routing Table (Status > Routing-Tabelle)

Status der Routing-Tabelle	
Feld	Beschreibung
Destination LAN IP (LAN-IP-Zieladresse)	Adresse des Netzwerks oder Hosts, dem die statische Route zugewiesen ist
Subnet Mask (Subnetzmaske)	Legt fest, bei welchem Teil einer IP-Adresse es sich um den Netzwerk- und den Host-Teil handelt
Gateway	IP-Adresse des Gateway-Geräts ein, das den Kontakt zwischen dem Gateway und dem gewünschten Netzwerk bzw. Host ermöglicht
Schnittstelle	Legt fest, ob sich die IP-Zieladresse im LAN- und Wireless-Netzwerk (internes verkabeltes und kabelloses Netzwerk) oder im Internet (WAN) befindet

ARP Table (ARP-Tabelle)

Auf der Statusseite für die ARP-Tabelle können Sie Informationen zu allen ARP-Einträgen (Address Resolution Protocol) anzeigen.

Status > ARP Table (Status > ARP-Tabelle)

Status der ARP-Tabelle	
Feld	Beschreibung
IP-Adresse	IP-Adresse des Geräts
HW Type (HW-Typ)	Hardware-Typ des Geräts
Markierungen	Markierungstyp des Geräts
HW Address (HW-Adresse)	MAC-Adresse des Geräts
Mask (Maske)	Maske des Geräts
Gerät	Schnittstellentyp des Geräts

RIP Status (RIP-Status)

Auf der Seite für den RIP-Status können Sie Informationen zu allen RIP-Aktivitäten (Routing Information Protocol) anzeigen. Um auf diese Seite zuzugreifen, klicken Sie im Konfigurationsprogramm auf **Status > RIP** (Status > RIP).

Auf dieser Seite werden alle auf RIP bezogenen Nachrichten für den zugehörigen RIP-Daemon gespeichert.

Für jede über RIP empfangene Route werden die Uhrzeit, zu der das Paket gesendet wurde, und die Markierungsinformationen angezeigt. Zudem wird der aktuelle RIP-Status wiedergegeben, also RIP-Timer, Filterung, Version, für RIP konfigurierte Schnittstellen und RIP-Peer-Informationen.

IGMP Status (IGMP-Status)

Auf der IGMP-Statusseite werden IGMP-Informationen angezeigt.

Status > IGMP (Status > IGMP)

Feld	Beschreibung
IP-Adresse	IP-Adresse des Geräts
Port	Port des Geräts

VPN Status (VPN-Status)

Auf der VPN-Statusseite können Sie VPN-Statusinformationen anzeigen.

Status > VPN Status (Status > VPN-Status)

VPN Status (VPN-Status)	
Feld	Beschreibung
Tunnel Name (Tunnelname)	Name des VPN-Tunnels
Remote Policy (Remote-Richtlinie)	Richtlinie für das Remote-Netzwerk
Local Policy (Lokale Richtlinie)	Richtlinie für das lokale Netzwerk
IKE Algorithm (IKE-Algorithmus)	Endergebnis des IKE-Algorithmus nach ISAKMP. Gilt nur für den Modus AUTO (Automatisch).
Upset Algorithm (Eingerichteter Algorithmus)	Vom Tunnel derzeit verwendeter IPSec-Algorithmus
TX Bytes (Übertragung in Byte)	Menge der über diesen Tunnel übertragenen Byte
RX Bytes (Empfang in Byte)	Menge der über diesen Tunnel empfangenen Byte
Connect Status (Verbindungsstatus)	Gilt nur für den Modus AUTO (Automatisch).

CDP Neighbor Information (CDP-Nachbarinformationen)

Auf der Seite mit den CDP-Nachbarinformationen können Sie über das Konfigurationsprogramm CDP-Nachbarinformationen anzeigen.

HINWEIS Um weitere Statusinformationen anzuzeigen, klicken Sie in der Liste mit den Nachbarinformationen auf das gewünschte Element. In der Tabelle mit den CDP-Details werden Informationen zum ausgewählten Gerät angezeigt.

Status > CDP Neighbor Information (Status > CDP-Nachbarinformationen)

CDP Neighbor Information (CDP-Nachbarinformationen)	
Feld	Beschreibung
Device ID (Geräte-ID)	Geräte-ID des Nachbarn
Local Interface (Lokale Schnittstelle)	Lokaler SRP-Name
Hold Time (Haltezeit)	Haltezeit, nach deren Ablauf CDP Pakete fallen lässt
Capability (Funktion)	Klasse des Nachbarn
Plattform	Hardware-System des Nachbarn
Port ID (Port-ID)	Portnummer des Nachbarn
IP-Adresse	IP-Adresse des Nachbarn

Technische Daten

In diesem Anhang werden die Spezifikationen für die SRP520-Modelle aufgeführt.

Funktion	SRP521W
WAN	Fast Ethernet
LAN	4 Fast Ethernet-Ports
Wireless	802.11b/g/n
Betriebstemperatur	0 °C bis 40 °C
Lagertemperatur	-20 °C bis 70 °C
Luftfeuchtigkeit bei Betrieb	10 bis 85 % (nicht kondensierend)
Luftfeuchtigkeit bei Lagerung	5 bis 90 % (nicht kondensierend)
Spannungsbereich	100 bis 240 V, 50/60 Hz Wechselstrom
Abmessungen	170 x 170 x 42 mm (B x T x H)
Gewicht	400 g

Funktion	SRP526W
WAN	ADSL2+ Annex B
LAN	4 Fast Ethernet-Ports
Wireless	802.11b/g/n
Betriebstemperatur	0 °C bis 40 °C
Lagertemperatur	-20 °C bis 70 °C

Funktion	SRP526W
Luftfeuchtigkeit bei Betrieb	10 bis 85 % (nicht kondensierend)
Luftfeuchtigkeit bei Lagerung	5 bis 90 % (nicht kondensierend)
Spannungsbereich	100 bis 240 V, 50/60 Hz Wechselstrom
Abmessungen	170 x 170 x 42 mm (B x T x H)
Gewicht	440 g

Funktion	SRP527W
WAN	ADSL2+ Annex A
LAN	4 Fast Ethernet-Ports
Wireless	802.11b/g/n
Betriebstemperatur	0 °C bis 40 °C
Lagertemperatur	-20 °C bis 70 °C
Luftfeuchtigkeit bei Betrieb	10 bis 85 % (nicht kondensierend)
Luftfeuchtigkeit bei Lagerung	5 bis 90 % (nicht kondensierend)
Spannungsbereich	100 bis 240 V, 50/60 Hz Wechselstrom
Abmessungen	170 x 170 x 42 mm (B x T x H)
Gewicht	440 g

Weiterführende Informationen

Cisco stellt eine Vielfalt von Ressourcen zur Verfügung, damit Sie und Ihre Kunden von allen Vorteilen der Services Ready-Plattformen profitieren können.

Produktressourcen

Support	
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport Informationen zur SRP finden Sie auf der Community-Seite unter dem Link für Router für kleine und mittlere Unternehmen.
Technischer Support und technische Dokumentation im Internet (Anmeldung erforderlich)	www.cisco.com/support
Support und Ressourcen für Cisco Small Business	www.cisco.com/go/smallbizhelp
Kontaktinformationen für telefonischen Support	www.cisco.com/go/sbsc
Software	
Software-Downloads (Anmeldung erforderlich)	www.cisco.com/go/srp500 Klicken Sie auf den Link zum Herunterladen der Software.
Open Source-Dokumentation	www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html
Produktdokumentation	
Cisco Services Ready Platform 500 Series for Small Business (Cisco Services Ready-Plattform der Serie 500 für kleine und mittlere Unternehmen)	www.cisco.com/go/srp500

Cisco Small Business	
Cisco Partner Central für kleine und mittlere Unternehmen (Partneranmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb
Marktplatz	www.cisco.com/go/marketplace