ADMINISTRATOR-HANDBUCH

Cisco RV215W Wireless N-VPN-Firewall

Überarbeitung: November 2013

78-20779-02

Inhalt

1

Einführung

In diesem Kapitel erhalten Sie Informationen, die Sie durch den Installationsprozess und die ersten Schritte mit dem browserbasierten Gerätemanager führen.

- **Überprüfen der Hardwareinstallation**
- **Verwenden des Setup-Assistenten**
- **Verwenden der Seite „Erste Schritte“**
- **Verbinden von Geräten mit dem WLAN**

Überprüfen der Hardwareinstallation

Konfigurieren Sie das Gerät für die Verbindung mit den drahtgebundenen oder drahtlosen Netzwerken mithilfe der Cisco RV215W Wireless-N VPN Firewall-Kurzanleitung.

VORSICHT Verwenden Sie das Netzteil (12V, 1.67a), das mit dem Gerät ausgeliefert wurde. Wenn Sie ein anderes Netzteil verwenden, kann dies die Leistung des Geräts beeinträchtigen oder zur Beschädigung des Geräts führen.

So überprüfen Sie die Hardwareinstallation und die Internetverbindung:

SCHRITT1 Überprüfen Sie den Status der LED. Weitere Informationen finden Sie in der Cisco RV215W Wireless-N VPN Firewall-Kurzanleitung, die mit dem Gerät bereitgestellt wird.

SCHRITT 2 Schließen Sie einen Computer an einen verfügbaren LAN-Anschluss an und vergewissern Sie sich, dass Sie eine Verbindung mit einer Website im Internet (beispielsweise www.cisco.com) herstellen können.

SCHRITT 3 Wenn Sie einen PC mit einer WLAN-Funktion verwenden, stellen Sie eine Verbindung mit dem Internet her (z. B. www.cisco.com) her. Die Konfiguration des Senders wird unter **Verbinden von Geräten mit dem WLAN** beschrieben.

Verwenden des Setup-Assistenten

Setup-Assistent und Gerätemanager werden unterstützt von Microsoft Internet Explorer 6.0 oder neuer, Mozilla Firefox 3.0 oder neuer und Apple Safari 3.0 oder neuer.

So verwenden Sie den Setup-Assistenten:

SCHRITT 1 Starten Sie den Computer, den Sie an einen LAN-Anschluss angeschlossen haben.

Der Computer wird zu einem DHCP-Client des Geräts und erhält eine IP-Adresse im Bereich 192.168.1.xxx.

SCHRITT 2 Starten Sie einen Webbrowser und geben Sie **192.168.1.1** in die Adressleiste ein. Dies ist die Standard-IP-Adresse der Gerät.

Daraufhin wird eine Meldung zum Sicherheitszertifikat der Site angezeigt. Die Gerät verwendet ein selbst signiertes Sicherheitszertifikat. Diese Meldung wird angezeigt, da der Computer die Gerät nicht kennt.

SCHRITT 3 Klicken Sie auf **Laden dieser Website fortsetzen** (bzw. auf die Option, die vom jeweils verwendeten Webbrowser angezeigt wird), um die Website aufzurufen. Das Fenster für die Anmeldung wird angezeigt.

SCHRITT 4 Geben Sie Benutzername und Kennwort ein.

Der Standardbenutzername lautet **cisco**. Das Standardkennwort lautet **cisco**. Bei Kennwörtern muss die Groß- und Kleinschreibung beachtet werden.

SCHRITT 5 Klicken Sie auf **Anmelden**. Der Setup-Assistent wird gestartet.

SCHRITT 6 Folgen Sie den auf dem Bildschirm angezeigten Anweisungen zum Einrichten der Gerät.

Der Setup-Assistent versucht, Ihre Verbindung automatisch zu erkennen und zu konfigurieren. Wenn dies nicht möglich ist, werden Sie möglicherweise vom Setup-Assistenten aufgefordert, Informationen zu Ihrer Internetverbindung anzugeben. Diese Informationen erhalten Sie von Ihrem ISP.

Wenn der Setup-Assistent die Gerät konfiguriert hat, müssen Sie das Standardkennwort ändern. Befolgen Sie die Anweisungen auf dem Bildschirm. Wenn Sie das Standardkennwort geändert haben, wird die Seite **Erste Schritte** angezeigt.

Konfiguration – Nächste Schritte

Obwohl der Setup-Assistent die Gerät automatisch konfiguriert, sollten Sie einige Einstellungen ändern, um die Sicherheit und Leistung zu verbessern.

- Wenn im Netzwerk bereits ein DHCP-Server vorhanden ist und Sie nicht möchten, dass die Gerät als DHCP-Server fungiert, deaktivieren Sie den Server. Weitere Informationen hierzu finden Sie unter **Konfigurieren der LAN-Einstellungen**.
- Konfigurieren Sie das VPN mithilfe von QuickVPN. QuickVPN ist auf der CD enthalten, die mit der Firewall ausgeliefert wurde. Weitere Informationen hierzu finden Sie unter **Anhang A, ?$paratext>?**.
- Die Gerät unterstützt bis zu vier WLANs. Wenn Sie den Setup-Assistenten verwenden, können Sie nur ein WLAN bzw. eine SSID einrichten. Wie Sie weitere WLANs mit dem Gerätemanager konfigurieren, erfahren Sie unter **Konfigurieren des WLANs**.

Verwenden der Seite „Erste Schritte“

Auf der Seite **Erste Schritte** werden die am häufigsten anfallenden Konfigurationsaufgaben für die Gerät angezeigt. Verwenden Sie die Links auf dieser Seite, um zur jeweiligen Konfigurationsseite zu wechseln.

Diese Seite wird bei jedem Start des Gerätemanagers angezeigt. Wenn Sie dies ändern möchten, aktivieren Sie **Nicht beim Start anzeigen**.

Anfangseinstellungen

Vorgegebenes Administratorkennwort ändern	Zeigt die Seite **Benutzer** an. Hier können Sie das Administratorkennwort ändern und ein Gastkonto einrichten. Weitere Informationen hierzu finden Sie unter **Konfigurieren von Benutzerkonten**.
Setup-Assistent starten	Startet den Setup-Assistenten. Befolgen Sie die Anweisungen auf dem Bildschirm.

WAN-Einstellungen konfigurieren	Öffnet die Seite **Interneteinrichtung**, auf der Sie Parameter wie den Hostnamen des Routers ändern können. Weitere Informationen hierzu finden Sie unter **Konfigurieren der WAN-Einstellungen**.
LAN-Einstellungen konfigurieren	Öffnet die Seite **LAN-Konfiguration**, auf der Sie die LAN-Parameter wie die Management-IP-Adresse ändern können. Weitere Informationen hierzu finden Sie unter **Konfigurieren der LAN-Einstellungen**.
WLAN-Einstellungen konfigurieren	Öffnet die Seite **Basiseinstellungen**, auf der Sie den Sender verwalten können. Weitere Informationen hierzu finden Sie unter **Konfigurieren des WLANs**.

Schnellzugriff

Firmware des Routers aktualisieren	Öffnet die Seite **Firmware-/Sprach-Upgrade**, auf der Sie die Firmware und das Sprachpaket für den Router aktualisieren können. Weitere Informationen hierzu finden Sie unter **Aktualisieren der Firmware oder Ändern der Sprache**.
VPN-Clients hinzufügen	Öffnet die Seite **VPN-Clients**, auf der Sie die virtuellen privaten Netzwerke verwalten können. Weitere Informationen hierzu finden Sie unter **VPN-Clients**.
Remoteverwaltungs-zugriff konfigurieren	Öffnet die Seite **Basiseinstellungen**, auf der Sie die Basisfunktionen des Routers aktivieren können. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

Gerätestatus

Systemzusammen-fassung	Zeigt die **Systemzusammenfassung** an, in der der Status des Routers aufgeführt ist. Weitere Informationen hierzu finden Sie unter **Anzeigen der Systemzusammenfassung**.
WLAN-Status	Zeigt die **WLAN-Statistiken** an, auf der der Funkstatus aufgeführt wird. Weitere Informationen hierzu finden Sie unter **Anzeigen von WLAN-Statistiken**.
VPN-Status	Zeigt die Seite **VPN-Status** mit der von diesem Router verwalteten VPN an. Weitere Informationen hierzu finden Sie unter **Anzeigen des VPN-Status**.

Andere Ressourcen

Support	Klicken Sie auf diese Option, um die Supportseite von Cisco zu öffnen.
Foren	Klicken Sie auf diese Option, um die Online-Supportforen von Cisco zu besuchen.

Speichern von Änderungen

Wenn Sie mit den Änderungen auf einer Konfigurationsseite fertig sind, klicken Sie auf **Speichern**, um die Änderungen im Flash-Speicher zu speichern, oder auf **Abbrechen**, um die Änderungen rückgängig zu machen.

Verbinden von Geräten mit dem WLAN

Um ein Client-Gerät (beispielsweise einen Computer) mit dem WLAN zu verbinden, müssen Sie die WLAN-Verbindung am Gerät mit den Informationen zur Wireless-Sicherheit konfigurieren, die Sie mithilfe des Setup-Assistenten für die Gerät konfiguriert haben.

Die folgenden Schritte dienen als Beispiel. Möglicherweise müssen Sie Ihr Client-Gerät anders konfigurieren. Speziell für Ihr Client-Gerät geltende Anleitungen finden Sie in der Dokumentation für das entsprechende Gerät.

SCHRITT1 Öffnen Sie für Ihr Gerät das Fenster oder das Programm mit den Einstellungen für die WLAN-Verbindung.

Möglicherweise ist auf Ihrem Computer eine spezielle Software zur Verwaltung von WLAN-Verbindungen installiert, oder Sie finden Angaben zu WLAN-Verbindungen in der Systemsteuerung unter **Netzwerkverbindungen** oder **Netzwerk und Internet**. (Der Zugriff auf diese Einstellungen hängt vom jeweiligen Betriebssystem ab.)

SCHRITT 2 Geben Sie den Netzwerknamen (SSID) ein, den Sie im Setup-Assistenten für das Netzwerk ausgewählt haben.

SCHRITT 3 Wählen Sie den Verschlüsselungstyp aus, und geben Sie den Sicherheitsschlüssel ein, den Sie im Setup-Assistenten angegeben haben.

Wenn Sie die Sicherheit nicht aktiviert haben (nicht empfohlen), lassen Sie die Felder für die Verschlüsselung der WLAN-Verbindung, die mit dem Sicherheitstyp und dem Kennwort konfiguriert wurden, leer.

SCHRITT 4 Überprüfen Sie Ihre WLAN-Verbindung und speichern Sie Ihre Einstellungen.

2

Anzeigen des Status des Geräts

In diesem Kapitel wird beschrieben, wie Sie Echtzeitstatistiken und andere Informationen zur Gerät anzeigen.

Anzeigen des Dashboards

Auf der Seite **Dashboard** werden wichtige Routerinformationen angezeigt.

Klicken Sie auf **Status** > **Dashboard**, um das Dashboard zu öffnen.

Zum Ändern der Aktualisierungsrate für die angezeigten Statistiken und Parameterwerte wählen Sie im Dropdown-Menü **Aktualisierungsrate** die Häufigkeit aus.

Zum Anzeigen einer interaktiven Ansicht der Rückseite des Routers klicken Sie auf **Bereichsansicht anzeigen**.

Auf der Rückseite sehen Sie die Anschlüsse, die mit einem Gerät verbunden sind. Diese leuchten grün.

- Zum Anzeigen der Verbindungsinformationen eines Anschlusses bewegen Sie die Maus über den Anschluss.
- Zum Aktualisieren der Anschlussinformationen klicken Sie auf **Aktualisieren**.

- Zum Schließen des Fensters mit den Anschlussinformationen klicken Sie auf **Schließen**.

Auf der Seite **Dashboard** wird Folgendes angezeigt:

Geräteinformationen

- **Systemname**: Der Name des Geräts.
- **Firmwareversion**: Die zurzeit im Gerät ausgeführte Firmwareversion.
- **Seriennummer**: Die Seriennummer des Geräts.

Ressourcenauslastung

- **CPU**: Die CPU-Auslastung.
- **Speicher**: Die Speicherauslastung.
- **Aktuelle Zeit**: Die Tageszeit.
- **Systembetriebszeit**: Gibt an, wie lange das System in Betrieb ist.

Syslog-Übersicht

Gibt an, ob die Protokollierung für diese Ereigniskategorien aktiviert ist:

- **Notfall**
- **Alarm**
- **Kritisch**
- **Fehler**
- **Warnung**

Zum Anzeigen der Protokolle klicken Sie auf **Details**. Weitere Informationen finden Sie unter **Anzeigen von Protokollen**.

Zum Verwalten der Protokolle klicken Sie auf **Protokollierung verwalten**. Weitere Informationen finden Sie unter **Konfigurieren von Protokollierungseinstellungen**.

LAN-Schnittstelle

- **MAC-Adresse**: Die MAC-Adresse des Geräts.
- **IPv4-Adresse**: Management-IP-Adresse des Geräts.
- **IPv6-Adresse**: Management-IP-Adresse des Geräts (wenn IPv6 aktiviert ist).

- **DHCP-Server**: Status des IPv4-DHCP-Servers des Geräts (aktiviert oder deaktiviert).
- **DHCPv6-Server**: Status des IPv6-DHCP-Servers des Routers (aktiviert oder deaktiviert).

Zum Anzeigen der LAN-Einstellungen klicken Sie auf **Details**. Weitere Informationen finden Sie unter **Konfigurieren der LAN-Einstellungen**.

WAN-Informationen (mobiles Netzwerk)

- **IPv4-Adresse**: IPv4-Adresse des USB-Anschlusses.
- **Status**: Status der mobilen WAN-Verbindung (aktiv oder inaktiv).

Zum Anzeigen der WAN-Einstellungen klicken Sie auf „Details“. Weitere Informationen finden Sie unter **Konfigurieren von drahtgebundenen WAN-Verbindungen**.

WAN-(Internet-)Informationen

- **IPv4-Adresse**: IPv4-Adresse des WAN-Anschlusses des Routers.
- **IPv6-Adresse**: IPv6-Adresse des WAN-Anschlusses des Routers, wenn IPv6 aktiviert ist.
- **Status**: Status der drahtgebundenen WAN-Verbindung (aktiv oder inaktiv).

Zum Anzeigen der WAN-Einstellungen klicken Sie auf **Details**. Weitere Informationen finden Sie unter **Konfigurieren von drahtgebundenen WAN-Verbindungen**.

WLANs

Listet den Status der vier WLAN-SSIDs auf.

Zum Anzeigen der WLAN-Einstellungen des Routers klicken Sie auf **Details**. Weitere Informationen finden Sie unter **Anzeigen von WLAN-Statistiken**.

VPN

QuickVPN-Benutzer: Anzahl der QuickVPN-Benutzer.

PPTP: Anzahl der PPTP-Benutzer (Point-to-Point Tunneling Protocol).

Anzeigen der Systemzusammenfassung

Auf der Seite **Systemzusammenfassung** wird eine Zusammenfassung der Gerätewerte wie die Firmwareversion und die Seriennummer angezeigt.

Zum Anzeigen einer Zusammenfassung der Systemeinstellungen wählen Sie **Status** > **Systemzusammenfassung** aus.

Klicken Sie auf den unterstrichenen Parameter, um zum entsprechenden Fenster zu wechseln. Wenn Sie z. B. die LAN-IP-Adresse ändern möchten, klicken Sie auf **LAN-IP**. Das Fenster „LAN-Konfiguration“ wird angezeigt.

Klicken Sie auf **Aktualisieren**, um die aktuellen Informationen abzurufen.

Auf der Seite **Systemzusammenfassung** werden folgende Informationen angezeigt:

Systeminformationen

- **Firmwareversion**: Die zurzeit im Gerät ausgeführte Softwareversion.
- **Firmware-MD5-Prüfsumme**: Der MD5-Algorithmus, der zum Überprüfen der Integrität von Dateien verwendet wird.
- **Gebietsschema**: Die im Router installierte Sprache.
- **Sprachversion**: Die Version des installierten Sprachpakets. Die Sprachpaketversion sollte mit der zurzeit installierten Firmware kompatibel sein. In manchen Fällen kann ein älteres Sprachpaket mit einem neueren Firmware-Image verwendet werden. Der Router überprüft, ob die Sprachpaketversion mit der aktuellen Firmwareversion kompatibel ist.
- **Sprach-MD5-Prüfsumme**: MD5-Prüfsumme des Sprachpakets.
- **CPU-Modell**: Der zurzeit verwendete CPU-Chipsatz.
- **Seriennummer**: Die Seriennummer des Geräts.
- **Systembetriebszeit**: Gibt an, wie lange das System in Betrieb ist.
- **Aktuelle Zeit**: Die Tageszeit.
- **PID VID**: Die Produkt-ID und Versions-ID des Geräts.

IPv4-Konfiguration

- **LAN-IP**: LAN-Adresse des Geräts.

- **WAN-IP**: WAN-IP-Adresse des Geräts. Sie können die aktuelle IP-Adresse freigeben und eine neue beziehen, indem Sie auf **Freigeben** oder **Erneuern** klicken.
- **Gateway**: IP-Adresse des Gateways, mit dem die Gerät verbunden ist (beispielsweise das Kabelmodem).
- **Modus**: Zeigt **Gateway** an, wenn NAT aktiviert ist, oder **Router**.
- **DNS 1**: Die IP-Adresse des primären DNS-Servers des WAN-Anschlusses.
- **DNS 2**: Die IP-Adresse des sekundären DNS-Servers des WAN-Anschlusses.
- **DDNS**: Gibt an, ob Dynamic DNS aktiviert oder deaktiviert ist.

IPv6-Konfiguration

- **LAN-IP**: LAN-Adresse des Geräts.
- **WAN-IP**: WAN-IP-Adresse des Geräts.
- **Gateway**: IP-Adresse des Gateways, mit dem die Gerät verbunden ist (beispielsweise das Kabelmodem).
- **NTP**: Network Time Protocol-Server (Hostname oder IPv6-Adresse).
- **Präfix-Delegation**: IPv6-Präfix, das vom Gerät des ISPs zurückgegeben und an IP-Adressen in der Gerät vergeben wird.
- **DNS 1**: IP-Adresse des primären DNS-Servers.
- **DNS 2**: IP-Adresse des sekundären DNS-Servers.

WLAN-Übersicht

- **SSID 1**: Öffentlicher Name des ersten WLANs.
  - **Sicherheit**: Sicherheitseinstellung für SSID 1.
- **SSID 2**: Öffentlicher Name des zweiten WLANs.
  - **Sicherheit**: Sicherheitseinstellung für SSID 2.
- **SSID 3**: Öffentlicher Name des dritten WLANs.
  - **Sicherheit**: Sicherheitseinstellung für SSID 3.
- **SSID 4**: Öffentlicher Name des vierten WLANs.
  - **Sicherheit**: Sicherheitseinstellung für SSID 4.

Firewall-Einstellungsstatus

- **DoS (Denial of Service)**: Gibt an, ob die DoS-Prävention aktiviert oder deaktiviert ist.
- **WAN-Anfrage sperren**: Gibt an, ob das Blockieren von WAN-Anfragen aktiviert oder deaktiviert ist.
- **Remote-Management**: Gibt an, ob ein Fernzugriff auf den Gerätemanager möglich ist.

VPN-Einstellungsstatus

- **QuickVPN-Verbindungen verfügbar**: Anzahl der verfügbaren QuickVPN-Verbindungen.
- **PPTP-VPN-Verbindungen verfügbar**: Anzahl der verfügbaren PPTP-VPN-Verbindungen.
- **Verbundene QuickVPN-Benutzer**: Anzahl der verbundenen QuickVPN-Benutzer.
- **Verbundene PPTP-VPN-Benutzer**: Anzahl der verbundenen PPTP-VPN-Benutzer.

Anzeigen von WLAN-Statistiken

Auf der Seite **WLAN-Statistik** werden WLAN-Statistiken für das Funkgerät angezeigt.

Zum Anzeigen der WLAN-Statistiken wählen Sie die Optionen **Status** > **WLAN-Statistiken** aus.

Zum Ändern der Aktualisierungsrate wählen Sie im Dropdown-Menü **Aktualisierungsrate** eine Aktualisierungsrate aus.

Zum Anzeigen der Bytes in Kilobytes (KB) und der numerischen Daten als gerundete Werte aktivieren Sie **Vereinfachte Statistik anzeigen** und klicken auf **Speichern**. Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt.

Zum Zurücksetzen der Zähler der WLAN-Statistik klicken Sie auf **Zähler zurücksetzen**. Außerdem werden die Zähler zurückgesetzt, wenn das Gerät neu gestartet wird.

Auf der Seite **WLAN-Statistik** werden folgende Informationen angezeigt:

SSID	Der Name des WLANs.
Paket	Anzahl der empfangenen und gesendeten WLAN-Pakete, die dem Sender für alle konfigurierten und aktiven SSIDs gemeldet wurden.
Byte	Anzahl der empfangenen und gesendeten Bytes mit Informationen, die dem Sender für alle konfigurierten SSIDs gemeldet wurden.
Fehler	Anzahl der empfangenen und gesendeten Paketfehler, die dem Sender für alle konfigurierten SSIDs gemeldet wurden.
Gelöscht	Anzahl der empfangenen und gesendeten Pakete, die vom Sender für alle konfigurierten SSIDs gelöscht wurden.
Multicast	Anzahl der über diesen Sender gesendeten Multicast-Pakete.
Kollisionen	Anzahl der Paketkollisionen, die dem Router gemeldet wurden.

Anzeigen des VPN-Status

Auf der Seite **VPN** wird der Status von VPN-Verbindungen angezeigt.

Zum Anzeigen des VPN-Benutzerverbindungsstatus wählen Sie **Status** > **VPN-Status** aus.

Auf der Seite **VPN** werden diese Informationen angezeigt:

Benutzername	Der Benutzername des VPN-Benutzers, der dem QuickVPN-PPTP-Tunnel zugeordnet ist.
Remote-IP	Zeigt die IP-Adresse des QuickVPN-Remoteclients an. Dabei kann es sich um eine mit NAT umgewandelte öffentliche IP-Adresse handeln, wenn sich der Client hinter dem NAT-Router befindet.

Status	Zeigt den aktuellen Status des QuickVPN-Clients an. OFFLINE bedeutet, dass der QuickVPN-Tunnel nicht vom VPN-Benutzer initiiert bzw. eingerichtet wurde. ONLINE bedeutet, dass der QuickVPN-Tunnel, der vom VPN-Benutzer initiiert bzw. eingerichtet wurde, aktiv ist.
Startzeit	Zeitpunkt, zu dem der VPN-Benutzer eine Verbindung hergestellt hat.
Endzeit	Zeitpunkt, zu dem der VPN-Benutzer eine Verbindung beendet hat.
Dauer (Sekunden)	Zeitspanne zwischen dem Herstellen und dem Beenden einer Verbindung durch den VPN-Benutzer.
Protokoll	Das vom Benutzer verwendete Protokoll.

Sie können den Status einer Verbindung ändern, um eine Verbindung mit dem konfigurierten VPN-Client herzustellen oder zu trennen.

Zum Beenden einer aktiven VPN-Verbindung klicken Sie auf **Trennen**.

Anzeigen des IPsec-Verbindungsstatus

Der IPsec-Verbindungsstatus zeigt den Status der aktiven VPN-Richtlinien in der Gerät an. (Diese Richtlinien werden auf der Seite **VPN** > **Erweiterte VPN-Einrichtung** konfiguriert.) So zeigen Sie den IPsec-Verbindungsstatus an:

SCHRITT 1 Wählen Sie **Status** > **IPsec-Verbindungsstatus** aus. Die Tabelle enthält die folgenden Informationen:

- **Aktualisierungsrate**: Wählen Sie aus, in welchen Abständen die Datenanzeige gelöscht und durch die neuesten Daten ersetzt werden soll.
- **Vereinfachte Statistik anzeigen**: Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt. Zum Anzeigen der Bytes in Kilobyte (KB) und der numerischen Daten im gerundeten Format aktivieren Sie **Vereinfachte Statistik anzeigen**.
- **Richtlinienname**: Name der VPN-Richtlinie, zu der die angezeigten Daten gehören.
- **Lokal oder Remote**: Zeigt die lokale bzw. Remote-IP-Adresse an.

- **Startzeit und Endzeit**: Zeigt die Start- und Endzeit der IPsec-Verbindungen an.
- **Dauer**: Dauer der aktiven Verbindung.
- **Paket**: Über die Verbindung empfangene (Rx) und übertragene (Tx) Pakete.
- **Byte**: Über die Verbindung empfangene (Rx) und übertragene (Tx) Byte.
- **Status**: Status der Verbindung (beispielsweise „Aktiv“ oder „Nicht verbunden“).
- **Aktion**: Aktionen, die Sie für die Verbindung durchführen können (beispielsweise „Verbindung trennen“).
- **Ext. Action**: Zeigt an, ob Sie zwischen der primären und der sekundären VPN-Verbindung umschalten können. Wenn das Kontrollkästchen **Rollback aktivieren** auf der Seite **Advanced VPN Parameters** (Erweiterte VPN-Parameter) aktiviert ist, ist die Schaltfläche **Switch** (Umschalten) ausgegraut.

SCHRITT 2 Falls Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**.

Anzeigen von Protokollen

Auf der Seite **Protokolle anzeigen** werden die Protokolle der Gerät angezeigt.

Zum Anzeigen der Protokolle wählen Sie **Status** > **Protokolle anzeigen** aus.

Klicken Sie auf **Protokolle aktualisieren**, um die neuesten Protokolleinträge anzuzeigen.

Zum Filtern der Protokolle oder zum Angeben des Schweregrads der anzuzeigenden Protokolle aktivieren Sie die Kontrollkästchen neben dem Protokolltyp und klicken auf **Los**. Beachten Sie, dass alle Protokolltypen über einem ausgewählten Protokolltyp automatisch enthalten sind und dass Sie diese Auswahl nicht aufheben können. Wenn Sie beispielsweise Fehlerprotokolle auswählen, sind zusätzlich zu den Fehlerprotokollen automatisch auch die Protokolle „Notfall“, „Alarm“ und „Kritisch“ enthalten.

Es stehen die folgenden Schweregrade für Ereignisse zur Verfügung, aufgelistet von der höchsten bis zur niedrigsten Gewichtung:

- **Notfall**: Das System kann nicht verwendet werden.
- **Alarm**: Es ist eine Aktion erforderlich.
- **Kritisch**: Das System befindet sich in einem kritischen Zustand.

- **Fehler**: Das System befindet sich im Fehlerzustand.
- **Warnung**: Es ist eine Systemwarnung aufgetreten.
- **Benachrichtigung**: Das System funktioniert ordnungsgemäß, es ist jedoch ein Systemhinweis aufgetreten.
- **Informationen**: Geräteinformationen.
- **Fehlerbehebung**: Bietet detaillierte Informationen zu einem Ereignis.

Wenn Sie alle Einträge im Protokollfenster löschen möchten, klicken Sie auf **Protokolle löschen**.

Wenn Sie alle Protokollmeldungen von der Firewall auf der lokalen Festplatte speichern möchten, klicken Sie auf **Protokolle speichern**.

Zum Speichern der Protokollmeldungen auf einem externen USB-Gerät klicken Sie auf **Save Log to USB** (Protokoll auf USB speichern).

Wenn Sie die Anzahl der Einträge angeben möchten, die pro Seite angezeigt werden sollen, wählen Sie im Dropdown-Menü eine Anzahl aus.

Verwenden Sie die Schaltflächen für die Seitennavigation, um zwischen den Protokollseiten zu wechseln.

Anzeigen von verbundenen Geräten

Auf der Seite **Verbundene Geräte** werden Informationen zu den mit der Gerät verbundenen aktiven Geräten angezeigt.

In der IPv4-ARP-Tabelle werden Informationen von Geräten angezeigt, die auf die ARP-Anforderung (Address Resolution Protocol) der Gerät geantwortet haben. Wenn ein Gerät auf die Anforderung nicht antwortet, wird es aus der Liste entfernt.

In der IPv6-NDP-Tabelle werden alle IPv6-NDP-Geräte (Neighbor Discovery Protocol) angezeigt, die mit dem lokalen Link der Gerät verbunden sind.

Zum Anzeigen von verbundenen Geräten wählen Sie die Optionen **Status** > **Verbundene Geräte** aus.

Um die Typen der anzuzeigenden Schnittstellen anzugeben, wählen Sie im Dropdown-Menü **Filter** einen Wert aus.

Alle: Alle mit dem Router verbundenen Geräte.

Drahtlos: Alle Geräte, die über die drahtlose Schnittstelle verbunden sind.

Drahtgebunden: Alle über die Ethernet-Anschlüsse am Router verbundenen Geräte.

WDS: Alle mit dem Router verbundenen WDS-Geräte (Wireless Distribution System).

Anzeigen von Anschlussstatistiken

Auf der Seite **Anschlussstatistik** werden die Anschlussaktivitäten detailliert angezeigt.

Zum Anzeigen der Anschlussstatistiken wählen Sie die Optionen **Status** > **Anschlussstatistiken** aus.

Wenn Sie erzwingen möchten, dass die Seite die Statistiken vom Router erneut liest und damit aktualisiert wird, wählen Sie im Dropdown-Menü **Aktualisierungsrate** eine Aktualisierungsrate aus.

Zum Anzeigen der Bytes in Kilobyte (KB) und der numerischen Daten im gerundeten Format aktivieren Sie **Vereinfachte Statistik anzeigen**, und klicken Sie auf **Speichern**. Standardmäßig werden Byte-Daten in Bytes und andere numerische Daten im Langformat angezeigt.

Zum Zurücksetzen der Zähler der Anschlussstatistik klicken Sie auf **Zähler zurücksetzen**.

Auf der Seite **Anschlussstatistik** werden folgende Informationen angezeigt:

Schnittstelle	Name der Netzwerkschnittstelle.
Paket	Anzahl der empfangenen und gesendeten Pakete.
Byte	Anzahl der pro Sekunde empfangenen und gesendeten Datenbytes.
Fehler	Anzahl der empfangenen und gesendeten Paketfehler.
Gelöscht	Anzahl der empfangenen und gesendeten Pakete, die gelöscht wurden.

Multicast	Anzahl der über diesen Sender gesendeten Multicast-Pakete.
Kollisionen	Anzahl der an diesem Anschluss aufgetretenen Signalkollisionen. Eine Kollision tritt auf, wenn der Anschluss zum gleichen Zeitpunkt wie ein Anschluss an einem anderen Router oder Computer, der mit diesem Anschluss verbunden ist, Daten zu senden versucht.

Anzeigen des Status des Gastnetzwerks

In der Statistik zum Gastnetzwerk werden Informationen über das in der Gerät konfigurierte Gastnetzwerk angezeigt.

Zum Anzeigen des Gastnetzwerkstatus wählen Sie **Status** > **Gastnetzstatus** aus. Die folgenden Informationen werden angezeigt:

- **Hostname**: Das mit dem Gastnetzwerk verbundene Gerät.
- **IP-Adresse**: Die dem verbundenen Gerät zugewiesene IP-Adresse.
- **MAC-Adresse**: Die MAC- oder Hardwareadresse des verbundenen Geräts.
- **Verbleibende Zeit**: Verbleibende Zeit, die noch für die Verbindung des Geräts zum Gastnetzwerk zur Verfügung steht. (Die Zeitbegrenzungen werden auf der Seite **WLAN** > **Basiseinstellungen** > **Gastnetzeinstellungen** konfiguriert.)
- **Aktion**: Aktionen, die Sie für das verbundene Gerät durchführen können (beispielsweise „Verbindung trennen“).

Anzeigen des Status des mobilen Netzwerks

Die Statistik des mobilen Netzwerks zum mobilen 3G/4G-Netzwerk und dem Kommunikationsgerät (Dongle), das in der Gerät konfiguriert ist.

Zum Anzeigen des Status des mobilen Netzwerks wählen Sie **Status** > **Mobiles Netzwerk** aus. Die folgenden Informationen werden angezeigt:

- **Verbindung**: Das mit dem Gastnetzwerk verbundene Gerät.
- **WAN-IP-Adresse**: Die dem USB-Gerät zugewiesene IP-Adresse.

- **Subnetzmaske**: Subnetzmaske des USB-Geräts.
- **Standardgateway**: IP-Adresse des Standardgateways.
- **Aktive Verbindungszeit**: Gibt an, wie lange die Verbindung aktiv ist.
- **Aktuelle Sitzungsverwendung**: Datenvolumen, das von der mobilen Verbindung empfangen (Rx) und dorthin übertragen (Tx) wurde.
- **Hersteller**: Name des Herstellers der Karte.
- **Kartenmodell**: Nummer des Kartenmodells.
- **Karten-Firmware**: Version der Karten-Firmware.
- **SIM-Status**: SIM-Status (Subscriber Identification Module).
- **IMS**: Die eindeutige Identifizierung, die den Benutzern von Mobiltelefonen im GSM-, UMTS- oder LTE-Netzwerk zugeordnet ist.
- **Träger**: Anbieter des mobilen Netzwerks.
- **Diensttyp**: Art des Dienstes, auf den zugegriffen wird.
- **Signalstärke**: Stärke des Signals des drahtlosen mobilen Netzwerks.

3

Konfigurieren der Netzwerkfunktionen

In diesem Kapitel wird beschrieben, wie Sie die Netzwerkeinstellungen der Gerät konfigurieren.

Konfigurieren der WAN-Einstellungen

Über den WAN-Anschluss oder ein drahtloses Modem, das am USB-Anschluss angeschlossen ist, kann eine Internetverbindung hergestellt werden. In diesem Abschnitt werden die Konfiguration des WAN, des mobilen Netzwerks sowie der Failover- und Wiederherstellungsfunktionen beschrieben.

Konfigurieren von drahtgebundenen WAN-Verbindungen

Auf welche Weise Sie die WAN-Eigenschaften für ein IPv4-Netzwerk konfigurieren, hängt vom Typ der Internetverbindung ab.

Konfigurieren von DHCP

Wenn Ihr Internet Service Provider(ISP) DHCP (Dynamic Host Control Protocol) verwendet, um Ihnen eine IP-Adresse zuzuweisen, erhalten Sie eine IP-Adresse, die bei jeder Anmeldung dynamisch generiert wird.

So konfigurieren Sie die DHCP-WAN-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **Automatische Konfiguration – DHCP** aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von statischen IP-Adressen

Wenn Ihnen der ISP eine permanente IP-Adresse zugewiesen hat, führen Sie die folgenden Schritte aus, um die WAN-Einstellungen zu konfigurieren:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **Statische IP-Adresse** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	IP-Adresse des Firewall-WAN-Anschlusses.
Subnetzmaske	Subnetzmaske des Firewall-WAN-Anschlusses.
Standardgateway	IP-Adresse des Standardgateways.
Statisches DNS 1	IP-Adresse des primären DNS-Servers.
Statisches DNS 2	IP-Adresse des sekundären DNS-Servers.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von PPPoE

So konfigurieren Sie die PPPoE-Einstellungen (Point-to-Point Protocol over Ethernet):

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **PPPoE** aus.

SCHRITT 3 Geben Sie die folgenden Informationen ein (möglicherweise müssen Sie den ISP nach den PPPoE-Anmeldeinformationen fragen):

Benutzername	Der vom ISP zugewiesene Benutzername.
Kennwort	Das vom ISP zugewiesene Kennwort.
Verbindung bei Bedarf	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten die Verbindung getrennt wird.

Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.
Authentifizierungstyp	**Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Die Gerät sendet die Anmeldeinformationen mit dem vom Server gesendeten Sicherheitstyp zurück. **PAP**: Password Authentication Protocol (PAP), wird von PPP (Point-to-Point Protocol) verwendet, um eine Verbindung zum ISP herzustellen. **CHAP**: Das Challenge Handshake Authentication Protocol (CHAP) erfordert, dass sowohl der Client als auch der Server den geheimen Schlüssel zur Verwendung der Dienste des ISPs kennen. **MS-CHAP oder MS-CHAPv2**: Die Microsoft-Version von CHAP, die für den Zugriff auf die Dienste des ISPs verwendet wird.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von PPTP

So konfigurieren Sie die PPTP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **PPTP** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	IP-Adresse des WAN-Anschlusses.
Subnetzmaske	Subnetzmaske des WAN-Anschlusses.

Standardgateway	IP-Adresse des Standardgateways.
PPTP-Server	IP-Adresse des PPTP-Servers (Point-to-Point Tunneling Protocol).
Benutzername	Der Ihnen vom ISP zugewiesene Benutzername.
Kennwort	Das Ihnen vom ISP zugewiesene Kennwort.
Verbindung bei Bedarf	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten die Verbindung getrennt wird.
Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.
Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus: **Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Die Gerät sendet die Anmeldeinformationen mit dem vom Server zuvor gesendeten Sicherheitstyp zurück. **PAP**: Die Gerät verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Die Gerät verwendet zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol). **MS-CHAP oder MS-CHAPv2**: Die Gerät verwendet das Microsoft Challenge Handshake Authentication-Protokoll zum Herstellen der Verbindung mit dem ISP.

SCHRITT 4 (Optional) Informationen zum Konfigurieren der optionalen Einstellungen finden Sie unter **Konfigurieren der optionalen Einstellungen**.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von L2TP

So konfigurieren Sie die L2TP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Internetverbindungstyp** die Option **L2TP** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

WAN-IP-Adresse	Geben Sie die IP-Adresse des WAN-Anschlusses ein.
Subnetzmaske	Geben Sie die Subnetzmaske des WAN-Anschlusses ein.
Standardgateway	Geben Sie die IP-Adresse des Standardgateways ein.
L2TP-Server	Geben Sie die IP-Adresse des L2TP-Servers ein.
Benutzername	Geben Sie den Benutzernamen ein, der Ihnen vom ISP zugewiesen wurde.
Kennwort	Geben Sie das Kennwort ein, das Ihnen vom ISP zugewiesen wurde.
Verbindung bei Bedarf	Wählen Sie diese Option aus, wenn Ihnen der ISP die Dauer der Verbindung in Rechnung stellt. Wenn Sie diese Option auswählen, ist die Internetverbindung nur aktiv, wenn Daten übertragen werden. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Wenn Sie auf **Verbindung bei Bedarf** klicken, geben Sie in das Feld **Max. Leerlaufzeit** ein, nach wie vielen Minuten die Verbindung getrennt wird.

Keep-Alive	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.
Authentifizierungstyp	**Automatisch aushandeln**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Die Gerät sendet die Anmeldeinformationen mit dem vom Server gesendeten Sicherheitstyp zurück. **PAP**: Password Authentication Protocol (PAP), wird verwendet, um eine Verbindung zum ISP herzustellen. **CHAP**: Das CHAP (Challenge Handshake Authentication Protocol) wird verwendet, um eine Verbindung zum ISP herzustellen. **MS-CHAP oder MS-CHAPv2**: Das Microsoft Challenge Handshake Authentication-Protokoll wird verwendet, um eine Verbindung mit dem ISP herzustellen.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der optionalen Einstellungen

So konfigurieren Sie die optionalen Einstellungen:

SCHRITT 1 Konfigurieren Sie im Abschnitt **Optionale Einstellungen** die folgenden Einstellungen:

Hostname	Hostname des Gerät.
Domänenname	Domänenname für Ihr Netzwerk.

MTU	Bei der MTU (Maximum Transmission Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Der MTU-Standardwert für Ethernet-Netzwerke beträgt in der Regel 1.500 Byte. Bei PPPoE-Verbindungen beträgt der Wert 1.492 Byte. Wenn vom ISP nichts anderes verlangt wird, sollten Sie **Automatisch** auswählen. Die MTU-Standardgröße beträgt 1.500 Byte. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, wählen Sie **Manuell** aus und geben Sie die MTU-Größe ein.
Größe	MTU-Größe.

SCHRITT 2 Klicken Sie auf **Speichern**.

Konfigurieren eines mobilen Netzwerkes

Auf der Seite „Mobiles Netzwerk“ können Sie die Gerät konfigurieren, um eine Verbindung mit einem mobilen USB-Breitbandmodem herzustellen, das an die USB-Schnittstelle angeschlossen ist.

Zur Anzeige des Fensters **Mobiles Netzwerk** klicken Sie auf **Netzwerk** > **WAN** > **Mobiles Netzwerk**.

Globale Einstellungen

So installieren Sie ein USB-Modem:

SCHRITT 1 Schließen Sie das USB-Modem an. Wenn das Modem unterstützt wird, wird es automatisch erkannt und auf der Seite „Mobiles Netzwerk“ angezeigt.

SCHRITT 2 Wählen Sie den Verbindungsmodus **Automatisch** oder **Manuell**. Die Ethernet-Wiederherstellung funktioniert nur, wenn der Verbindungsmodus auf „Automatisch“ gesetzt ist.

- Wählen Sie den Modus **Automatisch**, um das Modem für den automatischen Aufbau einer Verbindung zu aktivieren. Wenn Sie „Automatisch“ auswählen, müssen Sie entweder eine Zeit für „Verbindung bei Bedarf herstellen“ festlegen oder „Immer aufrechterhalten“ auswählen. Ist „Verbindung bei Bedarf herstellen“ ausgewählt, wird die Internetverbindung getrennt, wenn Sie eine bestimmte Zeit lang inaktiv ist (Leerlaufzeit).

  Wenn die Internetverbindung aufgrund von Inaktivität getrennt wird, stellt das Modem automatisch eine Verbindung her, wenn der Benutzer versucht, auf das Internet zuzugreifen. Geben Sie in das Feld **Max. Leerlaufzeit** die Anzahl der Minuten für die Leerlaufzeit an, die vor dem Trennen der Internetverbindung vergehen soll. Wenn Sie **Immer aufrechterhalten** auswählen, bleibt die Internetverbindung immer bestehen.

- Wenn Sie die Modemverbindung manuell herstellen oder trennen möchten, wählen Sie den Modus **Manuell** aus.

Das Gerät zeigt den aktuellen Modemverbindungsstatus an: „Initialisierung …“ SIM beschäftigt, „Wird verbunden“, „Wird getrennt“ oder „Getrennt“.

SCHRITT 3 Prüfen Sie, ob im Feld **Datenkartenstatus** angezeigt wird, dass Ihre mobile Datenkarte **Verbunden** ist.

Es können auch folgende Nachrichten angezeigt werden:

- Please set APN manually (because the device is unable to determine the access point name) (APN bitte manuell festlegen) (da das Gerät den Namen des Zugriffspunkts nicht ermitteln kann))
- Service wird gesucht …
- Keine SIM-Karte
- SIM gesperrt
- SIM besetzt
- SIM bereit
- PIN-Code erforderlich
- PIN-Code-Fehler
- Karte ist gesperrt
- Card is not activated (Karte ist nicht aktiviert)
- Card initialized error (Fehler bei der Initialisierung der Karte)
- Fehler

Setup für Mobiles Netzwerk

Wenn Parameter für das mobile Netzwerk im Bereich **Setup für Mobiles Netzwerk** geändert werden müssen, klicken Sie im Feld „Konfigurationsmodus“ auf die Optionsschaltfläche **Manuell**. Das Gerät erkennt automatisch unterstützte Modems und führt die entsprechenden Konfigurationsparameter auf. Die SIM-PIN kann entweder im Modus „Automatisch“ oder im Modus „Manuell“ geändert werden.

Das Kartenmodell zeigt das Modell des Modems am USB-Anschluss an. Nicht unterstützte Karten werden als **unbekannt** gekennzeichnet.

Zum Überschreiben der Parameter wählen Sie **Manuell** aus, und füllen Sie folgende Felder aus:

Feld	Beschreibung
Name des Zugriffpunkts (APN)	Internetnetzwerk, mit dem das mobile Geräte eine Verbindung herstellt. Geben Sie den Namen des Zugriffspunktes ein, den Sie von Ihrem Dienstanbieter für mobiles Netzwerk erhalten haben. Wenn Sie den Namen des Zugriffspunktes nicht kennen, wenden Sie sich an den Dienstanbieter.
Einwählnummer	Die Einwählnummer, die Sie von Ihrem Dienstanbieter für mobiles Netzwerk für die Internetverbindung erhalten haben.
Benutzername Kennwort	Benutzername und Kennwort, die Sie von Ihrem Dienstanbieter für mobiles Netzwerk erhalten haben.
SIM Check (SIM-Prüfung)	Prüfung der SIM-Karte aktivieren oder deaktivieren.
SIM-PIN	PIN-Code für die SIM-Karte. Dieses Feld wird nur für GSM-SIM-Karten angezeigt.
Servername	Name des Servers für die Internetverbindung (falls vom Dienstanbieter erhalten).

Feld	Beschreibung
Authentifizierung	Authentifizierung, die vom Dienstanbieter verwendet wird. Der Wert kann durch Auswählen des Typs „Automatisch“ aus der Dropdownliste geändert werden. Der Standardwert lautet „Automatisch“. Wenn Sie nicht wissen, welcher Authentifizierungstyp verwendet werden soll, wählen Sie „Automatisch“ aus.
Diensttyp	Der am häufigsten verwendete Typ einer mobiler Datenserviceverbindung, der auf dem lokalen Servicesignal des Bereichs basiert. Wenn an Ihrem Standort nur ein mobiler Datendienst unterstützt wird, können Sie Ihre bevorzugte Option einschränken, indem Sie die Häufigkeit der Verbindungseinrichtungen reduzieren. Die erste Auswahl sucht immer nach dem HSPDA/3G/UMTS-Dienst und schaltet automatisch auf GPRS um, wenn dieser Dienst verfügbar ist.
LTE-Dienst	Einstellung für „Long-term Evolution (LTE) Service“. Wählen Sie **Automatisch** für ein auf dem lokalen Servicesignal des Bereichs basierendes Signal. Wählen Sie **Nur 4G** wenn nur 4G-Signale verwendet werden sollen. Wählen Sie **Nur 3G** wenn nur 3G-Signale verwendet werden sollen.

SCHRITT 4 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Bandbreitenobergrenze

Das Gerät überwacht die Datenaktivität in der mobile Netzwerkverbindung und sendet eine Benachrichtigung, sobald es einen spezifischen Schwellenwert erreicht hat.

So aktivieren bzw. deaktivieren Sie die Option „Nachverfolgung Bandbreitenobergrenze“ und legen Grenzen fest:

SCHRITT 1 Klicken Sie auf **Aktivieren** oder **Deaktivieren**.

SCHRITT 2 Wählen Sie in der Dropdown-Liste den Eintrag **Datum für monatliche Verlängerung**, um anzugeben, an welchem Tag des Monats die Bandbreitenobergrenze zurückgesetzt werden soll.

SCHRITT 3 Geben Sie im Feld **Monatliche Bandbreitenobergrenze** den Höchstbetrag an Daten in Megabyte ein, der übertragen werden darf, bevor das Gerät eine Aktion (z. B. Senden einer E-Mail an den Administrator) ausführt.

E-Mail-Einstellung

Wenn die Bandbreitengrenze erreicht ist, kann eine E-Mail-Benachrichtigung an den Administrator gesendet werden. Aktivieren Sie das Kontrollkästchen **Email to** (E-Mail an), und klicken Sie auf **E-Mail-Adresse**, um die-E-Mail-Adresse des Empfängers einzurichten. Weitere Informationen finden Sie unter **Konfigurieren von E-Mail-Einstellungen**.

Wenn die Option aktiviert ist, wird unter folgenden Bedingungen eine E-Mail versendet:

- Die Nutzung des mobilen Netzwerk hat einen angegebenen Prozentwert überschritten.
- Das Gerät bricht beim Sicherungspfad ab und wird wiederhergestellt.
- In jedem während einer aktiven mobile Netzwerkverbindung angegebenen Intervall.

Einrichten von Failover und Wiederherstellung

Obwohl sowohl eine Ethernet- als auch eine mobile Netzwerkverbindung verfügbar sein können, kann immer nur eine Verbindung zum Aufbau einer WAN-Verbindung verwendet werden. Immer wenn eine WAN-Verbindung getrennt wird, versucht das Gerät, eine Verbindung an einer anderen Schnittstelle herzustellen. Diese Funktion wird Failover genannt. Wenn die primäre WAN-Verbindung wiederhergestellt ist, wird die Sicherungsverbindung verworfen. Diese Funktion wird Wiederherstellung genannt.

SCHRITT 1 Wählen Sie **Netzwerk** > **WAN** > **Failover & Wiederherstellung** aus.

SCHRITT 2 Legen Sie fest, ob es sich bei Ihrer primären Netzwerkverbindung um eine Ethernet-WAN-Verbindung oder eine mobile Netzwerkverbindung mit einem 3G-USB-Dongle handelt.

SCHRITT 3 Klicken Sie auf das Optionsfeld **Failover to Secondary Enable** (Bei Failover sekundäre Verbindung aktivieren), um bei einem Failover des Geräts mit der primären Netzwerkverbindung die Wiederherstellung der Verbindung mit der sekundären Verbindung zu aktivieren.

Bei der primären Verbindung handelt es sich z. B. um eine Ethernet-WAN-Verbindung und die WAN-Verbindung fällt aus. Das Gerät versucht dann, die Verbindung mit einer 3G-mobile Netzwerkverbindung an der USB-Schnittstelle wiederherzustellen. Wird **Failover to Secondary Enable** (Bei Failover sekundäre Verbindung aktivieren) nicht aktiviert, ist auch die sekundäre Verbindung deaktiviert.

SCHRITT 4 Klicken Sie auf das Optionsfeld **Recovery back to Primary aktivieren** (Wiederherstellung primärer Verbindung aktivieren), um die automatische Wiederherstellung der primären Verbindung durch das Gerät zu aktivieren und die sekundäre Verbindung dabei zu ignorieren. Der Verbindungsmodus **WAN** > **Mobiles Netzwerk** muss auf „Automatisch“ gesetzt werden, damit die primäre Verbindung automatisch wiederhergestellt werden kann.

SCHRITT 5 Geben Sie in das Feld **Wiederherstellungs-Prüfintervall** die Dauer (in Sekunden) ein, nach der das Gerät versuchen soll, Datenverkehr über die zweite Verbindung zu erkennen.

SCHRITT 6 Geben Sie in das Feld **Wiederherstellungs-Prüfintervall** die Dauer (in Sekunden) ein, nach der das Gerät versuchen muss, Datenverkehr über die zweite Verbindung zu erkennen. Wenn die Verbindung im Leerlauf ist, sendet das Gerät in diesem Intervall einen Ping an ein vorgegebenes Ziel. Wenn eine Antwort auf das Ping-Paket erhalten wird, geht das Gerät davon aus, dass die Verbindung funktioniert, und versucht, die primäre Netzwerkverbindung wiederherzustellen.

SCHRITT 7 Klicken Sie auf das Optionsfeld **Wenn Ethernet verfügbar ist, sofort zu Ethernet umschalten**, oder legen Sie für **Innerhalb eines bestimmten Zeitrahmens zu Ethernet umschalten** einen Zeitraum fest. Wenn Sie einen bestimmten Zeitraum auswählen, geben Sie die Start- und Endzeit ein.

SCHRITT 8 Geben Sie in das Feld **Wiederherstellungs-Ping** ein, wie oft das Gerät nach der Wiederherstellung einen Ping an die Site für Verbindungsvalidierung senden soll. Sie können bis zu 5 Pings vorgeben, die bezüglich der Wiederherstellung gesendet werden. Standardmäßig sendet das Gerät einen Ping an die Site für Verbindungsvalidierung.

SCHRITT 9 Wählen Sie im Feld **Site für Verbindungsvalidierung** den Speicherort aus, an den der Ping bei der Failover- und Wiederherstellungsvalidierung gesendet werden soll. Als Validierungssite können Sie den Gateway des Geräts, ein DNS oder eine benutzerdefinierte IP-Adresse auswählen. Geben Sie bei der Auswahl einer benutzerdefinierten Site die IPv4- oder IPv6-Adresse ein. Standardmäßig sendet das Gerät zur Failover-Validierung einen Ping an den Standardgateway.

SCHRITT 10 Klicken Sie zur Behebung von Problemen mit der mobilen 3G-Netzwerkverbindung auf das Optionsfeld **3G Diagnostic Enable** (3G-Diagnose aktivieren). Legen Sie eine Uhrzeit fest, zu der das Gerät die 3G-Verbindung täglich testen muss.

SCHRITT 11 Klicken Sie auf **Speichern**.

In der Tabelle „WAN-Schnittstelle“ wird der Status der Ethernet-WAN- und der mobile Netzwerkverbindung mit dem Internet angezeigt. Klicken Sie auf den Hyperlink **Status**, um die Anschlussdetails anzuzeigen.

WAN/USB-Geräteaktualisierung

Über diese Seite können Sie die USB-Modul-Dateien für die Unterstützung von USB-Dongles laden. Wenden Sie sich an Cisco Support, um USB-Moduldateien zu erhalten. Die Liste der USB-Modems mit dynamischer Last enthält die Moduldateien für den 3G- und 4G-USB-Dongle, die auf dem Gerät unterstützt werden.

Zum Löschen einer Modul-Datei wählen Sie das Modul in der Liste der USB-Modems mit dynamischer Last aus und klicken auf **Löschen**.

So laden Sie USB-Geräte-Firmware (ein Modul) vom PC hoch:

SCHRITT 1 Achten Sie darauf, dass der USB-Dongle nicht an das Gerät angeschlossen ist.

SCHRITT 2 Suchen Sie die Modul-Datei des USB-Dongles und wählen Sie sie aus.

SCHRITT 3 Klicken Sie auf **Importieren**.

SCHRITT 4 Schließen Sie den USB-Dongle an das Gerät an.

Konfigurieren der LAN-Einstellungen

Die Standardeinstellungen für DHCP und TCP/IP sind für die meisten Anwendungen geeignet. Wenn Sie einen anderen PC im Netzwerk als DHCP-Server verwenden möchten oder die Netzwerkeinstellungen aller Geräte manuell konfigurieren möchten, deaktivieren Sie DHCP.

Außerdem können Sie anstelle eines DNS-Servers, der Internetdomänennamen (beispielsweise www.cisco.com) IP-Adressen zuordnet, einen WINS-Server (Windows Internet Naming Service) verwenden. Ein WINS-Server ist das Äquivalent eines DNS-Servers, verwendet jedoch zum Auflösen von Hostnamen das NetBIOS-Protokoll. Die Gerät schließt die IP-Adresse des WINS-Servers in die DHCP-Konfiguration ein, die von der Gerät an DHCP-Clients gesendet wird.

Wenn die Gerät mit einem Modem oder Gerät verbunden ist, für das ein Netzwerk im gleichen Subnetz (192.168.1.x) konfiguriert ist, ändert die Gerät automatisch das LAN-Subnetz in ein zufällig ausgewähltes Subnetz nach dem Schema 10.x.x.x, sodass kein Konflikt mit dem Subnetz auf der WAN-Seite der Gerät entsteht.

Ändern der IP-Adresse für die Geräteverwaltung

Die IP-Adresse für die Verwaltung lokaler Geräte des Gerät ist statisch und lautet standardmäßig 192.168.1.1.

So ändern Sie die IP-Adresse für die Verwaltung lokaler Geräte:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **LAN-Konfiguration** aus.

SCHRITT 2 Geben Sie im Bereich **IPv4** diese Informationen ein:

VLAN	Die VLAN-Nummer.
Lokale IP-Adresse	Die IP-Adresse des lokalen LAN der Gerät. Stellen Sie sicher, dass diese IP-Adresse nicht von einem anderen Gerät verwendet wird.
Subnetzmaske	Subnetzmaske für die lokale IP-Adresse. Das Standardsubnetzmaske lautet 255.255.255.0.

SCHRITT 3 Klicken Sie auf **Speichern**.

Wenn Sie die IP-Adresse des Gerät geändert haben, kann der PC den Gerätemanager nicht mehr anzeigen.

Gehen Sie folgendermaßen vor, um den Gerätemanager anzuzeigen:

- Wenn DHCP in der Gerät konfiguriert ist, geben Sie die IP-Adresse des PCs frei, und erneuern Sie sie.
- Weisen Sie dem PC manuell eine IP-Adresse zu. Die Adresse muss sich im gleichen Subnetzwerk befinden wie der Gerät. Wenn Sie beispielsweise die IP-Adresse der Gerät in 10.0.0.1 ändern, weisen Sie dem PC eine IP-Adresse im Bereich von 10.0.0.2 bis 10.0.0.255 zu.

Öffnen Sie ein neues Browserfenster, und geben Sie die neue IP-Adresse der Gerät ein, um die Verbindung wiederherzustellen.

Konfigurieren eines DHCP-Servers

Standardmäßig funktioniert der Gerät als DHCP-Server zu den Hosts im WLAN (Wireless LAN) oder im drahtgebundenen LAN. Er weist IP-Adressen zu und stellt DNS-Serveradressen bereit.

Bei aktiviertem DHCP weist die Gerät den Netzwerkgeräten im LAN IP-Adressen aus einem Pool von IPv4-Adressen zu. Die Gerät testet jede Adresse vor der Zuweisung, um doppelte Adressen im LAN zu vermeiden.

Der Standard-IP-Adresspool lautet 192.168.1.100 bis 192.168.1.149. Wenn Sie eine statische IP-Adresse auf einem Netzwerkgerät festlegen möchten, verwenden Sie eine IP-Adresse außerhalb des Pools. Wenn z. B. der DHCP-Pool auf die Standardparameter gesetzt ist, können statische IP-Adressen aus dem IP-Adresspool 192.168.1.2 bis 192.168.1.99 verwendet werden. Dadurch vermeiden Sie Konflikte mit dem DHCP-IP-Adressenpool.

So konfigurieren Sie die DHCP-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **LAN-Konfiguration** aus.

SCHRITT 2 (Optional) Wählen Sie in der Dropdownliste ein zu bearbeitendes VLAN aus.

SCHRITT 3 Wählen Sie im Feld **DHCP-Server** eine der folgenden Optionen aus:

Aktivieren	Der Gerät kann als DHCP-Server im Netzwerk agieren.
Deaktivieren	Deaktiviert das DHCP im Gerät, wenn Sie die IP-Adressen aller Netzwerkgeräte manuell konfigurieren möchten.
DHCP-Relais	Leitet die IP Adressen weiter, die den Netzwerkgeräten von einem anderen DHCP-Server zugewiesen wurden.

Wenn Sie den DHCP-Server des Gerät aktiviert haben, geben Sie folgenden Informationen ein:

IP-Startadresse	Die erste Adresse aus dem IP-Adressenpool. Jedem DHCP-Client, der dem LAN beitritt, wird eine IP-Adresse in diesem Bereich zugewiesen.
Maximale Anzahl an DHCP-Benutzern	Die maximale Anzahl der DHCP-Clients.

IP-Adressbereich	(Schreibgeschützt) Der Bereich der IP-Adressen, die für die DHCP-Clients zur Verfügung stehen.
Leasedauer	Dauer (in Stunden), für die IP-Adressen an Clients vergeben werden.
Statisches DNS 1	IP-Adresse des primären DNS-Servers.
Statisches DNS 2	IP-Adresse des sekundären DNS-Servers.
Statisches DNS 3	IP-Adresse des tertiären DNS-Servers.
WINS	IP-Adresse des primären WINS-Servers.

SCHRITT 4 Wenn Sie **DHCP-Relais** ausgewählt haben, geben Sie die Adresse des Relais-Gateways in das Feld **Remote-DHCP-Server** ein. Das Relay-Gateway überträgt DHCP-Nachrichten an die Netzwerkgeräte, auch an solche anderer Subnetzwerke.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von VLANs

Bei einem virtuellen LAN (VLAN) handelt es sich um eine Gruppe von Endpunkten in einem Netzwerk, die einander aufgrund ihrer Funktion oder anderer gemeinsamer Merkmale zugeordnet werden. Im Gegensatz zu LANs, die normalerweise auf dem geografischen Standort basieren, können in VLANs Endpunkte ungeachtet des physischen Standorts der Geräte oder Benutzer gruppiert werden.

Der Gerät hat ein Standard-VLAN (VLAN 1), das nicht gelöscht werden kann. Sie können im Gerät bis zu vier weitere VLANs erstellen.

So erstellen Sie ein VLAN:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **VLAN-Mitgliedschaft** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

VLAN-ID	Numerische VLAN-ID, die Endpunkten in der VLAN-Mitgliedschaft zugewiesen werden soll. Sie müssen eine Zahl zwischen 3 und 4094 eingeben. VLAN-ID1 ist für das Standard-VLAN reserviert, das für an der Schnittstelle empfangene Frames ohne Tag verwendet wird.
Beschreibung	Eine Beschreibung des VLAN.
Inter-VLAN-Routing	Ermöglicht, dass eine Endstation in einem VLAN mit einer Endstation in einem anderen VLAN kommuniziert.
Anschluss 1 **Anschluss 2** **Anschluss 3** **Anschluss 4**	Sie können VLANs in der Gerät den LAN-Anschlüssen am Gerät zuordnen. Standardmäßig gehören alle Anschlüsse zu VLAN1. Sie können diese Anschlüsse bearbeiten, um sie anderen VLANs zuzuordnen. Wählen Sie für jeden Anschluss den Typ der ausgehenden Frames aus: **Ungetaggt**: Die Schnittstelle gehört dem VLAN als Mitglied ohne Tag an. Frames des VLANs werden ohne Tag an das Anschluss-VLAN gesendet. **Getaggt**: Der Anschluss gehört dem VLAN als Mitglied mit Tag an. Frames des VLANs werden mit Tag an das Anschluss-VLAN gesendet. **Ausgeschlossen**: Der Anschluss ist zurzeit kein Mitglied des VLANs. Dies ist bei der anfänglichen Erstellung des VLANs die Standardeinstellung für alle Anschlüsse.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines VLANs wählen Sie das VLAN aus und klicken Sie auf **Bearbeiten**. Zum Löschen eines ausgewählten VLANs klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von statischem DHCP

Sie können die Gerät so konfigurieren, dass einem Gerät mit einer bestimmten MAC-Adresse eine bestimmte IP-Adresse zugewiesen wird.

So konfigurieren Sie statisches DHCP:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **Statisches DHCP** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **VLAN** eine VLAN-Nummer aus.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Geben Sie folgende Informationen ein:

Beschreibung	Beschreibung des Client.
IP-Adresse	IP-Adresse des Geräts. Die zugewiesene IP-Adresse sollte nicht zum Pool der DHCP-Adressen gehören. Bei der statischen DHCP-Zuweisung weist der DHCP-Server einer definierten MAC-Adresse bei jeder Verbindung des Geräts mit dem Netzwerk die gleiche IP-Adresse zu. Der DHCP-Server weist die reservierte IP-Adresse zu, wenn das Gerät mit der entsprechenden MAC-Adresse eine IP-Adresse anfordert.
MAC-Adresse	MAC-Adresse des Geräts. Das Format einer MAC-Adresse lautet XX:XX:XX:XX:XX:XX. Dabei ist „X“ eine Zahl zwischen 0 und 9 (einschließlich) oder ein Buchstabe zwischen A und F (einschließlich).

Zum Bearbeiten der Einstellungen eines statischen DHCP-Clients wählen Sie den Client aus und klicken Sie auf **Bearbeiten**. Zum Löschen eines ausgewählten DHCP-Clients klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Anzeigen von DHCP-Lease-Clients

Sie können eine Liste der Endpunkte im Netzwerk aufrufen (identifiziert durch Hostname, IP-Adresse oder MAC-Adresse) und die IP-Adressen anzeigen, die den Endpunkten vom DHCP-Server zugewiesen wurden. Das VLAN der Endpunkte wird ebenfalls angezeigt.

Zum Anzeigen der DHCP-Clients wählen Sie **Netzwerk** > **LAN** > **DHCP-Lease-Clients** aus.

Für jedes in der Gerät definierte VLAN wird in einer Tabelle eine Liste der jeweils zugeordneten Clients angezeigt.

So weisen Sie einem der verbundenen Geräte eine statische IP-Adresse zu:

SCHRITT 1 Aktivieren Sie in der Zeile des verbundenen Geräts das Kontrollkästchen **Zu statischem DHCP hinzufügen**.

SCHRITT 2 Klicken Sie auf **Speichern**.

Der DHCP-Server im Gerät weist dann immer die angezeigte IP-Adresse zu, wenn das Gerät eine IP-Adresse anfordert.

Konfigurieren eines DMZ-Hosts

Die Gerät unterstützt demilitarisierte Zonen (DMZs). Bei einer DMZ handelt es sich um ein Subnetzwerk, das öffentlich verfügbar ist, sich aber hinter der Firewall befindet. Mithilfe einer DMZ können Sie an die IP-Adresse des WAN-Anschlusses gerichtete Pakete an eine bestimmte IP-Adresse im LAN umleiten.

Wir empfehlen, Hosts, die für das WAN verfügbar gemacht werden müssen (beispielsweise Webserver oder E-Mail-Server) im DMZ-Netzwerk zu platzieren. Sie können Firewallregeln konfigurieren, um den Zugriff auf bestimmte Services und Anschlüsse in der DMZ über das LAN oder das WAN zuzulassen. Im Fall eines Angriffs auf einen der DMZ-Knoten ist das LAN nicht zwangsläufig verwundbar.

Sie müssen eine feste (statische) IP-Adresse für den Endpunkt konfigurieren, den Sie als DMZ-Host festlegen. Sie sollten dem DMZ-Host eine IP-Adresse zuweisen, die sich im gleichen Subnetz befindet wie die LAN-IP-Adresse der Gerät. Die IP-Adresse kann jedoch nicht mit der IP-Adresse identisch sein, die für die LAN-Schnittstelle dieses Gateways vergeben wird.

So konfigurieren Sie die DMZ:

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **DMZ-Host** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die DMZ im Netzwerk zu aktivieren.

SCHRITT 3 Wählen Sie im VLAN-Dropdown-Menü die ID des VLANs aus, in dem die DMZ aktiviert ist.

SCHRITT 4 Geben Sie in das Feld **Host-IP-Adresse** die IP-Adresse des DMZ-Hosts ein. Der DMZ-Host ist der Endpunkt, der die umgeleiteten Pakete empfängt.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von RSTP

RSTP (Rapid Spanning Tree Protocol) ist ein Netzwerkprotokoll, das Schleifen im Netzwerk verhindert und dynamisch neu konfiguriert, welche physischen Verbindungen Frames weiterleiten sollen. So konfigurieren Sie RTSP (Rapid Spanning Tree Protocol):

SCHRITT 1 Wählen Sie **Netzwerk** > **LAN** > **RSTP** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

Systempriorität	Wählen Sie im Dropdown-Menü die Systempriorität aus: Sie können eine Systempriorität von 0 bis 61440 in Schritten von 4096 auswählen. Gültige Werte: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 40960, 45056, 49152, 53248, 57344 und 61440. Je niedriger die Systempriorität, umso größer ist die Wahrscheinlichkeit, dass die Gerät zum Stamm des Spanning Tree wird. Der Standardwert lautet **327688**.

Hello-Zeit	Die Hello-Zeit ist der Zeitraum, in dem der Stamm des Spanning Tree wartet, bis Hello-Nachrichten gesendet werden. Geben Sie eine Zahl von 1 bis 10 ein. Der Standardwert lautet **2**.
Maximales Alter	Das maximale Alter ist der Zeitraum, während dessen der Router auf den Empfang einer Hello-Nachricht wartet. Wenn das maximale Alter erreicht ist, versucht der Router, den Spanning Tree zu ändern. Geben Sie eine Zahl von 6 bis 40 ein. Der Standardwert lautet **20**.
Weiterleitungsverzögerung	Die Weiterleitungsverzögerung ist das Intervall, nach dem eine Schnittstelle vom Status „Blockieren“ zum Status „Weiterleiten“ wechselt. Geben Sie eine Zahl von 4 bis 30 ein. Der Standardwert lautet **15**.
Version erzwingen	Wählen Sie die Protokollversion aus, die standardmäßig verwendet werden soll. Wählen Sie **Normal** (RSTP verwenden) oder **Kompatibel** (kompatibel mit dem alten STP) aus. Der Standardwert lautet **Normal**.

SCHRITT 3 Konfigurieren Sie in der **Einstellungstabelle** die folgenden Einstellungen:

Protokoll aktiviert	Aktivieren Sie dieses Kontrollkästchen, um RSTP für den zugeordneten Anschluss zu aktivieren. RSTP ist standardmäßig deaktiviert.
Edge	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass der zugeordnete Anschluss ein Edge-Anschluss ist (Endstation). Deaktivieren Sie das Kontrollkästchen, um anzugeben, dass der zugeordnete Anschluss ein Link (Bridge) zu einem anderen STP-Gerät ist. Der Edge-Anschluss ist standardmäßig aktiviert.
Pfadkosten	Geben Sie die RSTP-Pfadkosten für die festgelegten Anschlüsse ein. Verwenden Sie „0“ als Standardwert (die Gerät bestimmt den Pfadwert automatisch). Sie können auch eine Zahl von 2 bis 200000000 eingeben.

SCHRITT 4 Klicken Sie auf **Speichern**.

Anschlussverwaltung

Sie können die Einstellungen für die Geschwindigkeit und die Flusskontrolle der vier LAN-Anschlüsse der Gerät konfigurieren.

So konfigurieren Sie die Anschlussgeschwindigkeit und die Flusskontrolle:

SCHRITT 1 Wählen Sie **Netzwerk** > **Anschlussverwaltung** aus.

SCHRITT 2 Konfigurieren Sie diese Informationen:

Port	Port-Nummer.
Leitung	Port-Geschwindigkeit. Wenn kein Gerät mit dem Anschluss verbunden ist, wird in diesem Feld **Ausgefallen** angezeigt.
Modus	Wählen Sie im Dropdown-Menü eine der folgenden Anschlussgeschwindigkeiten aus: • **Automatisch aushandeln**: Die Gerät und das verbundene Gerät wählen eine gemeinsame Geschwindigkeit aus. • **10 MBit/s Halbduplex**: 10 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. • **10 MBit/s Vollduplex**: 10 MBit/s in beide Richtungen gleichzeitig. • **100 MBit/s Halbduplex**: 100 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. • **100 MBit/s Vollduplex**: 100 MBit/s in beide Richtungen gleichzeitig.

Flusskontrolle	Aktivieren Sie dieses Kontrollkästchen, um die Flusskontrolle für diesen Anschluss zu aktivieren. Flusskontrolle ist ein Vorgang, bei dem die Datenübertragungsrate zwischen zwei Knoten verwaltet wird, um zu verhindern, dass ein Sender mit höherer Geschwindigkeit einen Empfänger mit niedrigerer Geschwindigkeit „überholt“. Es wird ein Mechanismus bereitgestellt, mit dem der Empfänger die Übertragungsgeschwindigkeit steuern kann, damit der empfangende Knoten nicht mit Daten vom sendenden Knoten überflutet wird.

SCHRITT 3 Klicken Sie auf **Speichern**.

Klonen der MAC-Adresse

Manchmal müssen Sie möglicherweise die MAC-Adresse des WAN-Anschlusses der Gerät so festlegen, dass sie mit der MAC-Adresse des PCs oder einer anderen MAC-Adresse identisch ist. Dies wird als Klonen der MAC-Adresse bezeichnet.

Beispielsweise registrieren manche ISP bei der anfänglichen Installation des Service die MAC-Adresse der Netzwerkkarte des Computers. Wenn Sie einen Router hinter dem Kabel- oder DSL-Modem platzieren, wird die MAC-Adresse des WAN-Anschlusses der Gerät vom ISP nicht erkannt.

In diesem Fall können Sie die Gerät so konfigurieren, dass sie vom ISP erkannt wird, indem Sie die MAC-Adresse des WAN-Anschlusses klonen, sodass sie mit der MAC-Adresse des Computers identisch ist.

So konfigurieren Sie eine geklonte MAC-Adresse:

SCHRITT 1 Wählen Sie **Netzwerk** > **MAC-Adresse klonen** aus.

SCHRITT 2 Aktivieren Sie im Feld **MAC-Adresse klonen** das Kontrollkästchen **Aktivieren**, um das Klonen der MAC-Adresse zu aktivieren.

SCHRITT 3 Führen Sie einen der folgenden Schritte aus, um die MAC-Adresse des WAN-Anschlusses der Gerät festzulegen:

- Wenn Sie die MAC-Adresse des WAN-Anschlusses auf die MAC-Adresse des PCs festlegen möchten, klicken Sie auf **MAC-Adresse des PCs klonen**.
- Wenn Sie eine andere MAC-Adresse angeben möchten, geben Sie diese in das Feld **MAC-Adresse** ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Routing

Nachfolgend wird beschrieben, wie Sie die Routing-Optionen konfigurieren.

Konfigurieren des Betriebsmodus

So konfigurieren Sie den Betriebsmodus der Gerät:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Wählen Sie im Feld **Betriebsmodus** eine der folgenden Optionen aus:

Gateway	(Empfohlen) Klicken Sie auf diese Schaltfläche, um festzulegen, dass die Gerät als Gateway dient. Behalten Sie diese Standardeinstellung bei, wenn die Gerät zum Hosten der Verbindung zwischen Ihrem Netzwerk und dem Internet verwendet wird und die Routing-Funktionen ausführt.
Router	(Nur für fortgeschrittene Benutzer) Klicken Sie auf diese Schaltfläche, um festzulegen, dass die Gerät als Router dient. Wählen Sie diese Option aus, wenn sich die Gerät in einem Netzwerk mit anderen Routern befindet. Durch das Aktivieren des Routermodus wird NAT (Network Address Translation) in der Gerät deaktiviert.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von dynamischem Routing

Das RIP-Protokoll (Routing Information Protocol) ist ein IGP-Protokoll (Interior Gateway Protocol), das allgemein in internen Netzwerken verwendet wird. Es ermöglicht dem Router den automatischen Austausch von Routing-Informationen mit anderen Routern sowie die dynamische Anpassung der Routing-Tabellen und die Anpassung an Änderungen im Netzwerk.

Mithilfe von dynamischem Routing (RIP) kann sich die Gerät automatisch an physische Änderungen im Layout des Netzwerks anpassen und Routing-Tabellen mit den anderen Routern austauschen.

Der Router bestimmt die Route der Netzwerkpakete basierend auf der kleinsten Anzahl von Hops zwischen Quelle und Ziel. RIP ist standardmäßig deaktiviert.

HINWEIS RIP ist im Gerät standardmäßig deaktiviert.

So konfigurieren Sie dynamisches Routing:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Einstellungen:

RIP	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um RIP zu aktivieren. Damit ermöglichen Sie der Gerät die Weiterleitung von Verkehr mithilfe von RIP.
Version des RIP Send-Pakets	Wählen Sie die Version des RIP Send-Pakets (**RIPv1** oder **RIPv2**) aus. Die zum Senden von Routing-Aktualisierungen an andere Router im Netzwerk verwendete RIP-Version hängt von den Konfigurationseinstellungen der anderen Router ab. RIPv2 ist abwärtskompatibel mit RIPv1.
Version des RIP Recv-Pakets	Wählen Sie die Version des RIP Recv-Pakets aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von statischem Routing

Sie können statische Routen konfigurieren, um Pakete an das Zielnetzwerk zu leiten. Eine statische Route ist ein zuvor festgelegter Pfad, den ein Paket zurücklegen muss, um einen bestimmten Host oder ein bestimmtes Netzwerk zu erreichen.

Manche ISP erfordern für die Erstellung der Routing-Tabelle statische Routen anstelle dynamischer Routing-Protokolle. Bei statischen Routen ist es nicht erforderlich, dass CPU-Ressourcen Routing-Informationen mit einem Peer-Router austauschen.

Sie können statische Routen auch verwenden, um Peer-Router zu erreichen, die keine dynamischen Routing-Protokolle unterstützen. Statische Routen können zusammen mit dynamischen Routen verwendet werden. Die Gerät unterstützt bis zu 30 statische Routen.

Achten Sie darauf, dass im Netzwerk keine Routing-Schleifen entstehen.

So konfigurieren Sie statisches Routing:

SCHRITT 1 Wählen Sie **Netzwerk** > **Routing** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Routeneinträge** einen Routeneintrag aus.

Zum Löschen des Routeneintrags klicken Sie auf **Diesen Eintrag löschen**.

SCHRITT 3 Konfigurieren Sie die folgenden Einstellungen für den ausgewählten Routeneintrag:

Routennamen eingeben	Geben Sie den Namen der Route ein.
Ziel-LAN-IP	Geben Sie die IP-Adresse des Ziel-LANs ein.
Subnetzmaske	Geben Sie die Subnetzmaske des Zielnetzwerks ein.
Gateway	Geben Sie die IP-Adresse des für diese Route verwendeten Gateways ein.

Schnittstelle	Wählen Sie die Schnittstelle aus, an die Pakete für diese Route gesendet werden: • **LAN und WLAN**: Klicken Sie auf diese Schaltfläche, um Pakete an das LAN und das WLAN zu leiten. • **WAN (Internet)**: Klicken Sie auf diese Schaltfläche, um Pakete an das Internet (WAN) zu leiten.

SCHRITT 4 Klicken Sie auf **Speichern**.

Anzeigen der Routing-Tabelle

Die Routing-Tabelle enthält Informationen zur Topologie des sie unmittelbar umgebenden Netzwerks.

Zum Anzeigen der Routing-Informationen im Netzwerk klicken Sie auf **Netzwerk** > **Routing-Tabelle**, und wählen Sie eine der folgenden Optionen aus:

- **IPv4-Routing-Tabelle anzeigen**: Die Routing-Tabelle wird mit den auf den Seiten **Netzwerk** > **Routing** konfigurierten Feldern angezeigt.
- **IPv6-Routing-Tabelle anzeigen**: Die Routing-Tabelle wird mit den auf den Seiten **Netzwerk** > **IPv6** konfigurierten Feldern angezeigt.

Konfigurieren von dynamischem DNS

Dynamic DNS (DDNS) ist ein Internetservice, der das Auffinden von Routern mit variierenden öffentlichen IP-Adressen anhand von Internetdomänennamen ermöglicht. Um DDNS zu verwenden, müssen Sie ein Konto bei einem DDNS-Anbieter einrichten (beispielsweise DynDNS.com, TZO.com, 3322.org oder noip.com).

Der Router benachrichtigt Dynamic DNS-Server über Änderungen an der WAN-IP-Adresse, sodass der Zugriff auf öffentliche Services in Ihrem Netzwerk anhand des Domänennamens möglich ist.

So konfigurieren Sie DDNS:

SCHRITT 1 Wählen Sie **Netzwerk** > **Dynamisches DNS** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **DDNS-Service** die Option **Deaktivieren** aus, um diesen Service zu deaktivieren, oder wählen Sie den DDNS-Service aus, der verwendet werden soll.

SCHRITT 3 Wenn Sie kein DDNS-Konto haben, klicken Sie auf die URL des Service, um die Website des ausgewählten DDNS-Service aufzurufen und ein Konto zu erstellen.

SCHRITT 4 Konfigurieren Sie diese Informationen:

E-Mail-Adresse	(TZO.com und noip.com) Geben Sie die E-Mail-Adresse ein, die Sie zum Erstellen des DDNS-Kontos verwendet haben.
Benutzername	(DynDNS.com und 3322.org) Geben Sie den Benutzernamen des DDNS-Kontos ein.
Kennwort	Kennwort für das DDNS-Konto
Kennwort bestätigen	(TZO.com, DynDNS.com und noip.com) Bestätigung für das Kennwort des DDNS-Kontos.
Hostname	(DynDNS.com, 3322.org und noip.com) Hostname des DDNS-Servers.
Domänenname	(TZO.com) Name der Domäne, die für den Zugriff auf das Netzwerk verwendet wird.

Aktualisierungsintervall	Wählen Sie eine der folgenden Optionen, um vorzugeben, wie oft die IP-Adresse und der Domänenname auf dem DDNS-Server aktualisiert werden sollen: **Nie**: Niemals aktualisieren. **Wöchentlich**: Wöchentlich am Montag um 00:MM Uhr aktualisieren. „MM“ entspricht dabei einer zufällig gewählten Zahl zwischen 0 und 59. Die Option „Wöchentlich“ ist standardmäßig ausgewählt. **Zweimal im Monat**: Die Aktualisierung erfolgt am ersten und fünfzehnten Tag des Monats um 00:MM Uhr. „MM“ entspricht dabei einer zufällig gewählten Zahl zwischen 0 und 59. **Monatlich**: Die Aktualisierung erfolgt am ersten Tag des Monats um 00:MM Uhr. „MM“ entspricht dabei einer zufällig gewählten Zahl zwischen 0 und 59.
WAN-IP-Adresse	(Schreibgeschützt) Die WAN-IP-Adresse des Gerät.
Status	(Schreibgeschützt) Zeigt an, dass die DDNS-Aktualisierung erfolgreich abgeschlossen wurde oder dass beim Senden der Kontoaktualisierungsinformationen an den DDNS-Server ein Fehler aufgetreten ist.

SCHRITT 5 Zum Testen der DDNS-Konfiguration klicken Sie auf **Konfiguration testen**.

SCHRITT 6 Klicken Sie auf **Speichern**.

Konfigurieren des IP-Modus

Die Eigenschaften der WAN-Konfiguration können für IPv4-Netzwerke und für IPv6-Netzwerke konfiguriert werden. Sie können auf diesen Seiten Informationen zum Internetverbindungstyp und andere Parameter eingeben.

So wählen Sie einen IP-Modus aus:

SCHRITT 1 Wählen Sie **Netzwerk** > **IP-Modus** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **IP-Modus** eine der folgenden Optionen aus:

LAN: IPv4, WAN: IPv4	Verwenden Sie IPv4 für die LAN- und WAN-Anschlüsse.
LAN: IPv6, WAN: IPv4	Verwenden Sie IPv6 für die LAN-Anschlüsse und IPv4 für die WAN-Anschlüsse.
LAN: IPv6, WAN: IPv6	Verwenden Sie IPv6 für die LAN- und WAN-Anschlüsse.
LAN: IPv4 + IPv6, WAN: IPv4	Verwenden Sie IPv4 und IPv6 für die LAN-Anschlüsse und IPv4 für die WAN-Anschlüsse.
LAN: IPv4 + IPv6, WAN: IPv4 + IPv6	Verwenden Sie IPv4 und IPv6 für die LAN- und WAN-Anschlüsse.
LAN: IPv4, WAN: IPv6	Verwenden Sie IPv4 für die LAN-Anschlüsse und IPv6 für die WAN-Anschlüsse.

SCHRITT 3 (Optional) Wenn Sie 6to4-Tunneling verwenden, das die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk ermöglicht, führen Sie die folgenden Schritte aus:

a. Klicken Sie auf **Statischen 6to4-DNS-Eintrag anzeigen**.

b. Geben Sie in die Felder **Domäne** und **IP** bis zu fünf Zuordnungen zwischen Domäne und IP-Adresse ein.

Die Funktion für 6to4-Tunneling wird normalerweise verwendet, wenn eine Site oder ein Endbenutzer über das vorhandene IPv4-Netzwerk eine Verbindung mit dem IPv6-Internet herstellen möchte.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von IPv6

Internetprotokoll Version 6 (IPv6) ist als Nachfolger von Internetprotokoll Version 4 (IPv4) vorgesehen. Die Konfiguration der WAN-Eigenschaften für ein IPv6-Netzwerk richtet sich nach dem Typ Ihrer Internetverbindung.

Konfigurieren von IPv6-WAN-Verbindungen

Sie können die Gerät als DHCPv6-Client des ISPs für dieses WAN konfigurieren oder eine vom ISP bereitgestellte statische IPv6-Adresse verwenden.

Zum Konfigurieren der IPv6-WAN-Einstellungen im Gerät müssen Sie zuerst den IP-Modus auf einen der folgenden Modi festlegen:

- LAN: IPv6, WAN: IPv6
- LAN: IPv4 + IPv6, WAN: IPv4
- LAN: IPv4 + IPv6, WAN: IPv4 + IPv6

Eine Anleitung zum Festlegen des IP-Modus finden Sie unter **Konfigurieren des IP-Modus**.

Konfigurieren von DHCPv6

Wenn Ihnen der ISP eine dynamisch zugewiesene Adresse bereitstellt, konfigurieren Sie die Gerät für die Verwendung als DHCPv6-Client.

So konfigurieren Sie die Gerät als DHCPv6-Client:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **Automatische Konfiguration (DHCPv6)** aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren einer statischen IPv6-WAN-Adresse

Wenn Ihnen der ISP eine feste Adresse für den Zugriff auf das WAN zuweist, konfigurieren Sie die Gerät für die Verwendung einer statischen IPv6-Adresse.

So konfigurieren Sie eine statische IPv6-WAN-Adresse

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **Statisches IPv6** aus.

SCHRITT 3 Geben Sie folgende Informationen ein:

IPv6-Adresse	IPv6-Adresse des WAN-Anschlusses.
IPv6-Präfixlänge	Geben Sie die normalerweise vom ISP definierte IPv6-Präfixlänge ein. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Alle Hosts im Subnetzwerk haben ein identisches Präfix. So ist beispielsweise in der IPv6-Adresse `2001:0DB8:AC10:FE01::` das Präfix `2001`.
Standard-IPv6-Gateway	IPv6-Adresse des Standardgateways. Dies ist normalerweise die IP-Adresse des Servers beim ISP.
Statisches DNS 1	IP-Adresse des primären IPv6-DNS-Servers.
Statisches DNS 2	IP-Adresse des sekundären IPv6-DNS-Servers.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der PPPoE IPv6-Einstellungen

Sie können IPv4 PPPoE, IPv6 PPPoE oder beide ausführen. Wenn Sie sich für beide entscheiden, müssen die IPv6 WAN PPPoE-Einstellungen mit den IPv4 WAN PPPoE-Einstellungen übereinstimmen. Wenn Sie nicht übereinstimmen, wird eine Nachricht mit der Frage angezeigt, ob Sie das IPv6-Protokoll so einstellen möchten, dass es mit dem IPv4-Protokoll übereinstimmt. Weitere Informationen finden Sie unter **Konfigurieren von PPPoE**.

So konfigurieren Sie die PPPoE IPv6-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-WAN-Konfiguration** aus.

SCHRITT 2 Wählen Sie im Feld **WAN-Verbindungstyp** die Option **PPPoE IPv6** aus.

SCHRITT 3 Geben Sie die folgenden Informationen ein (möglicherweise müssen Sie den ISP nach den PPPoE-Anmeldeinformationen fragen):

Benutzername	Der Ihnen vom ISP zugewiesene Benutzername.
Kennwort	Das Ihnen vom ISP zugewiesene Kennwort.
Verbindung bei Bedarf	Wenn beim ISP Kosten auf der Grundlage der Verbindungszeit entstehen, aktivieren Sie das Optionsfeld. Wenn diese Option aktiviert ist, ist die Internetverbindung nur aktiv, wenn Verkehr vorhanden ist. Wenn sich die Verbindung im Leerlauf befindet (das heißt, wenn kein Verkehr fließt), wird die Verbindung getrennt. Geben Sie im Feld **Max. Leerlaufzeit** an, wie lange (in Minuten) kein Verkehr auf der Verbindung erkannt worden sein muss, damit die Verbindung getrennt wird.
Keep-Alive	Hält die WAN-Verbindung aufrecht, indem eine „Aufrechterhalten“-Nachricht über den Anschluss gesendet wird. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Gerät versuchen soll, eine getrennte Verbindung wiederherzustellen.
Authentifizierungstyp	Authentifizierungstypen: **Automatisch aushandeln**: Ein Server sendet eine Konfigurationsanforderung, in der der auf dem Server festgelegte Sicherheitsalgorithmus angegeben ist. Der Gerät antwortet mit den Anmeldeinformationen einschließlich dem vom Server gesendeten Sicherheitstyp. **PAP**: PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP verwenden. **CHAP**: zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol) verwenden. **MS-CHAP oder MS-CHAPv2**: Das Microsoft Challenge Handshake Authentication-Protokoll wird verwendet, um eine Verbindung mit dem ISP herzustellen.

Servicename	Name, den der ISP für eine Anmeldung auf dem PPPoE-Server anfordern kann.
MTU	Bei der MTU (Maximum Transmission Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Wenn vom ISP nichts anderes verlangt wird, sollten Sie **Automatisch** auswählen. Der MTU-Standardwert für Ethernet-Netzwerke beträgt 1.500Byte. Bei PPPoE-Verbindungen beträgt der Wert 1.492 Byte. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, wählen Sie **Manuell** aus.
Größe	MTU-Größe. Wenn der ISP eine benutzerdefinierte MTU-Einstellung verwendet, geben Sie die MTU-Größe ein.
Adressmodus	Modus für dynamische Adresse oder Modus für statische Adressen. Wenn Sie „Statisch“ auswählen, geben Sie im nachfolgenden Feld die IPv6-Adresse ein.
IPv6-Präfixlänge	IPv6-Präfixlänge.
Standard-IPv6-Gateway	IP-Adresse des Standard-IPv6-Gateways.
Statisches DNS 1	IP-Adresse des primären DNS-Servers.
Statisches DNS 2	IP-Adresse des sekundären DNS-Servers.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von IPv6-LAN-Verbindungen

Im IPv6-Modus ist der LAN-DHCP-Server standardmäßig aktiviert (ähnlich wie im IPv4-Modus). Der DHCPv6-Server weist IPv6-Adressen aus konfigurierten Adressenpools zu, die die dem LAN zugewiesene IPv6-Präfixlänge verwenden.

Zum Konfigurieren der IPv6-LAN-Einstellungen in der Gerät müssen Sie zuerst den IP-Modus auf einen der folgenden Modi festlegen:

- LAN: IPv6, WAN: IPv4
- LAN: IPv6, WAN: IPv6
- LAN: IPv4 + IPv6, WAN: IPv4
- LAN: IPv4 + IPv6, WAN: IPv4 + IPv6

Eine Informationen zum Festlegen des IP-Modus finden Sie unter **Konfigurieren des IP-Modus**.

So konfigurieren Sie IPv6-LAN-Einstellungen:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-LAN-Konfiguration** aus.

SCHRITT 2 Geben Sie die folgenden Informationen ein, um die IPv6-LAN-Adresse zu konfigurieren:

IPv6-Adresse	Geben Sie die IPv6-Adresse der Gerät ein. Die standardmäßige IPv6-Adresse für das Gateway lautet „fec0::1“ (oder „FEC0:0000:0000:0000:0000:0000:0000:0001“). Sie können diese 128-Bit-IPv6-Adresse je nach Netzwerkanforderungen ändern.
IPv6-Präfixlänge	Geben Sie die IPv6-Präfixlänge ein. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. Standardmäßig hat das Präfix eine Länge von 64 Bits. Die Anfangs-Bits der IPv6-Adressen aller Hosts im Netzwerk sind identisch. In diesem Feld legen Sie die Anzahl der gemeinsamen Anfangs-Bits in den Netzwerkadressen fest.

SCHRITT 3 Klicken Sie auf **Speichern**, oder fahren Sie mit der Konfiguration der IPv6-DHCP-LAN-Einstellungen fort.

SCHRITT 4 Geben Sie die folgenden Informationen ein, um die DHCPv6-Einstellungen zu konfigurieren:

DHCP-Status	Aktivieren Sie dieses Kontrollkästchen, um den DHCPv6-Server zu aktivieren. Wenn diese Funktion aktiviert ist, weist der Gerät jedem LAN-Endpunkt, der über DHCP bereitgestellte Adressen anfordert, eine IP-Adresse innerhalb des angegebenen Bereichs zu und stellt zusätzliche Informationen bereit.
Domänenname	(Optional) Domänenname des DHCPv6-Servers.
Serverpriorität	Serverprioritätsstufe diese DHCP-Servers. DHCP-Ankündigungsnachrichten mit dem höchsten Servervoreinstellungswert an einen LAN-Host werden gegenüber anderen DHCP-Serverankündigungsnachrichten bevorzugt. Der Standardwert lautet „255“.
Statisches DNS 1	IPv6-Adresse des primären DNS-Servers im IPv6-Netzwerk des ISPs.
Statisches DNS 2	IPv6-Adresse des sekundären DNS-Servers im IPv6-Netzwerk des ISPs.
Leasedauer	Dauer der Leasedauer (in Stunden), während der IPv6-Adressen an Endpunkte im LAN vergeben werden.

SCHRITT 5 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-LAN-Konfiguration** aus.

SCHRITT 6 Klicken Sie in der **Tabelle für IPv6-Adressenpools** auf **Hinzufügen**.

SCHRITT 7 Geben Sie folgende Informationen ein:

Startadresse	Start-IPv6-Adresse im Pool.
Endadresse	End-IPv6-Adresse im Pool.
IPv6-Präfixlänge	Präfixlänge, die die Anzahl der gemeinsamen Anfangs-Bits in den Netzwerkadressen bestimmt.

SCHRITT 8 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines Pools wählen Sie den Pool aus und klicken Sie auf **Bearbeiten**. Zum Löschen eines ausgewählten Pools klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von statischem IPv6-Routing

Sie können statische Routen konfigurieren, um Pakete an das Zielnetzwerk zu leiten. Eine statische Route ist ein zuvor festgelegter Pfad, den ein Paket zurücklegen muss, um einen bestimmten Host oder ein bestimmtes Netzwerk zu erreichen.

Manche ISP verwenden für die Erstellung einer Routing-Tabelle statische Routen anstelle dynamischer Routing-Protokolle. Bei statischen Routen ist es nicht erforderlich, dass CPU-Ressourcen Routing-Informationen mit einem Peer-Router austauschen.

Sie können statische Routen auch verwenden, um Peer-Router zu erreichen, die keine dynamischen Routing-Protokolle unterstützen. Statische Routen können zusammen mit dynamischen Routen verwendet werden. Achten Sie darauf, dass im Netzwerk keine Routing-Schleifen entstehen.

So erstellen Sie eine statische Route:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Statisches IPv6-Routing** aus.

SCHRITT 2 Klicken Sie in der Liste der statischen Routen auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

Name	Routenname.
Ziel	IPv6-Adresse des Zielhosts oder -netzwerks für diese Route.
Präfixlänge	Anzahl der Präfix-Bits in der IPv6-Adresse, die das Zielsubnetz definieren.
Gateway	IPv6-Adresse des Gateways, über das der Zielhost bzw. das Zielnetzwerk erreicht werden kann.
Schnittstelle	Schnittstelle für die Route: **LAN**, **WAN** oder **6to4**.

Metrik	Priorität der Route. Wählen Sie einen Wert zwischen 2 und 15 aus. Wenn mehrere Routen mit demselben Ziel vorhanden sind, wird die Route mit der niedrigsten Metrik verwendet.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Route zu aktivieren. Wenn Sie eine inaktive Route hinzufügen, wird diese in der Routing-Tabelle aufgelistet, aber nicht vom Gerät verwendet. Wenn Sie die Route hinzufügen, und die Route ist nicht verfügbar, ist es hilfreich eine inaktive Route einzugeben. Sobald das Netzwerk verfügbar ist, können Sie die Route aktivieren.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen einer Route wählen Sie die Route aus und klicken Sie auf **Bearbeiten**. Zum Löschen einer ausgewählten Route klicken Sie auf **Löschen**. Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Konfigurieren von Routing (RIPng)

RIP Next Generation (RIPng) ist ein Routing-Protokoll, das auf dem Distanzvektoralgorithmus (D-V) basiert. RIPng verwendet UDP-Pakete, um über Anschluss 521 Routing-Informationen auszutauschen.

RIPng verwendet zum Messen der Distanz zu einem Ziel die Hop-Anzahl. Die Hop-Anzahl wird als Metrik bzw. Kosten bezeichnet. Die Hop-Anzahl von einem Router zu einem direkt verbundenen Netzwerk beträgt 0. Die Hop-Anzahl zwischen zwei direkt verbundenen Routern beträgt 1. Wenn die Hop-Anzahl größer oder gleich 16 ist, ist das Zielnetzwerk bzw. der Zielhost nicht erreichbar.

Standardmäßig wird die Routing-Aktualisierung alle 30 Sekunden gesendet. Wenn der Router nach 180 Sekunden keine Routing-Aktualisierungen von einem Nachbarn empfangen hat, werden die vom Nachbarn gelernten Routen als nicht erreichbar betrachtet. Wenn nach weiteren 240 Sekunden keine Routing-Aktualisierung empfangen wurde, entfernt der Router diese Routen aus der Routing-Tabelle.

In der Gerät ist RIPng standardmäßig deaktiviert.

So konfigurieren Sie RIPng:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Routing (RIPng)** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von Tunneling

IPv6-to-IPv4-Tunneling (6to4-Tunneling) ermöglicht die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk. IPv4-to-IPv6-Tunneling (4to6-Tunneling) ermöglicht die Übertragung von IPv4-Paketen über ein IPv6-Netzwerk.

6to4-Tunneling

6to4-Tunneling wird normalerweise verwendet, wenn eine Site oder ein Endbenutzer über das vorhandene IPv4-Netzwerk eine Verbindung mit dem IPv6-Internet herstellen möchte.

So konfigurieren Sie 6to4-Tunneling:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Tunneling** aus.

SCHRITT 2 Aktivieren Sie im Feld **6to4-Tunneling** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Wählen Sie den Tunneling-Typ aus (**6to4** oder **6RD** [Rapid Deployment]).

SCHRITT 4 Wählen Sie bei 6RD-Tunneling zwischen **Automatisch** und **Manuell**.

SCHRITT 5 Geben Sie folgende Informationen ein:

- **IPv6-Präfix**
- **IPv6-Präfixlänge**
- **Border-Relais**
- **IPv4-Maskenlänge**

SCHRITT 6 Klicken Sie auf **Speichern**.

4to6-Tunneling

So konfigurieren Sie 4to6-Tunneling:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Tunneling** aus.

SCHRITT 2 Aktivieren Sie im Feld **4to6-Tunneling** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Geben Sie die lokale WAN-IPv6-Adresse in der Gerät ein.

SCHRITT 4 Geben Sie die Remote IPv6-Adresse oder die IP-Adresse des Remoteendpunkts ein.

SCHRITT 5 Klicken Sie auf **Speichern**.

Anzeigen des IPv6-Tunnelstatus

So zeigen Sie den IPv6-Tunnelstatus an:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **IPv6-Tunnelstatus** aus.

SCHRITT 2 Klicken Sie auf **Aktualisieren**, um die aktuellen Informationen anzuzeigen.

Auf dieser Seite werden Informationen zum automatischen Tunnel angezeigt, der über die dedizierte WAN-Schnittstelle eingerichtet wurde. Sie sehen in der Tabelle den Namen des Tunnels und die im Gerät erstellte IPv6-Adresse.

Routerankündigung

Der Router Advertisement Daemon (RADVD) im Gerät hört Router-Anfragen im IPv6-LAN mit und antwortet nach Bedarf mit Router-Anzeigen. Dabei handelt es sich um eine statuslose automatische IPv6-Konfiguration. Der Gerät verteilt IPv6-Präfixe an alle Knoten im Netzwerk.

So konfigurieren Sie RADVD:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Router-Anzeige** aus.

SCHRITT 2 Geben Sie folgende Informationen ein:

RADVD-Status	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um RADVD zu aktivieren.
Anzeigemodus	Wählen Sie einen der folgenden Modi aus: **Unaufgefordertes Multicast**: Routerankündigungen (Router Advertisements, RAs) an alle Schnittstellen senden, die zur Multicast-Gruppe gehören. **Nur Unicast**: Beschränkt Ankündigungen auf allgemein bekannte IPv6-Adressen (RAs werden nur an die Schnittstelle gesendet, die zur bekannten Adresse gehört).
Anzeigeintervall	Anzeigeintervall (4–1800) für **Unaufgefordertes Multicast**. Der Standardwert lautet 30. Das Anzeigeintervall ist ein zufälliger Wert zwischen dem Mindestintervall für die Router-Anzeige (Minimum Router Advertisement Interval, MinRtrAdvInterval) und dem Maximalintervall für die Router-Anzeige (Maximum Router Advertisement Interval, MaxRtrAdvInterval). MinRtrAdvInterval = 0,33 * MaxRtrAdvInterval
RA-Flags	Aktivieren Sie **Verwaltet**, um das verwaltete/ statusbehaftete Protokoll für die automatische Adressenkonfiguration zu verwenden. Aktivieren Sie **Andere**, um das verwaltete/ statusbehaftete Protokoll für die automatische Konfiguration anderer Informationen, bei denen es sich nicht um Adressen handelt, zu verwenden.

Router-Priorität	Wählen Sie im Dropdown-Menü **Niedrig**, **Mittel** oder **Hoch** aus. Der Standardwert lautet Mittel. Die Router-Voreinstellung stellt eine Voreinstellungsmetrik für Standardrouter bereit. Die Werte „Niedrig“, „Mittel“ und „Hoch“ werden in nicht verwendeten Bits in RA-Nachrichten signalisiert. Diese Erweiterung ist sowohl für Router (Festlegen des Router-Voreinstellungswerts) als auch für Hosts (Interpretieren des Router-Voreinstellungswerts) abwärtskompatibel. Diese Werte werden von Hosts ignoriert, die keine Router-Priorität implementieren. Die Funktion ist hilfreich, wenn im LAN andere RADVD-fähige Geräte vorhanden sind.
MTU	MTU-Größe (0 oder 1.280 bis 1.500). Der Standardwert beträgt 1.500 Bytes. Bei der MTU (Maximum Transmit Unit) handelt es sich um die Größe des größten Pakets, das über das Netzwerk gesendet werden kann. Die MTU-Größe wird in RAs verwendet, um sicherzustellen, dass alle Knoten im Netzwerk den gleichen MTU-Wert verwenden, wenn die LAN-MTU-Größe nicht allgemein bekannt ist.
Router-Gültigkeitsdauer	Router-Lebensdauerwert oder die Zeit in Sekunden, während der die Anzeigenachrichten in der Route vorhanden sind. Der Standardwert beträgt 3.600 Sekunden.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von Anzeigepräfixen

So konfigurieren Sie die verfügbaren RADVD-Präfixe:

SCHRITT 1 Wählen Sie **Netzwerk** > **IPv6** > **Anzeigepräfixe** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

IPv6-Präfixtyp	Wählen Sie eine der folgenden Typen aus: **6to4**: Ermöglicht die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk. Es wird verwendet, wenn ein Endbenutzer über eine vorhandene IPv4-Verbindung eine Verbindung zum IPv6-Internet herstellen möchte. **Global/Lokal**: Eine lokal eindeutige IPv6-Adresse, die Sie in privaten IPv6-Netzwerken verwenden können, oder eine global eindeutige IPv6-Internetadresse.
SLA-ID	Wenn Sie **6to4** als IPv6-Präfixtyp auswählen, geben Sie die SLA-ID (Site-Level Aggregation Identifier) ein. Die SLA-ID im 6to4-Adresspräfix ist auf die Schnittstellen-ID der Schnittstelle festgelegt, über die die Anzeigen gesendet werden.
IPv6-Präfix	Wenn Sie **Global/Lokal** als IPv6-Präfixtyp auswählen, geben Sie das IPv6-Präfix ein. Das IPv6-Präfix gibt die IPv6-Netzwerkadresse an.
IPv6-Präfixlänge	Wenn Sie **Global/Lokal** als IPv6-Präfixtyp auswählen, geben Sie die Präfixlänge ein. Die Präfixlänge ist ein Dezimalwert, der die Anzahl der zusammenhängenden höherwertigen Bits der Adresse angibt, die den Netzwerkteil der Adresse bilden.
Präfixgültigkeitsdauer	Präfixgültigkeitsdauer oder der Zeitraum, in dem der anfordernde Router das Präfix verwenden darf.

SCHRITT 4 Klicken Sie auf **Speichern**.

4

Konfigurieren des WLANs

In diesem Kapitel wird beschrieben, wie Sie das Wireless-Netzwerk der Gerät konfigurieren.

- **Sicherheitsfunktionen bei der WLAN-Datenübermittlung**
- **Cisco RV215W Wireless-Netzwerke**
- **Konfigurieren der Basis-WLAN-Einstellungen**
- **Konfigurieren der erweiterten WLAN-Einstellungen**
- **Konfigurieren von WDS**
- **Konfigurieren von WPS**

Sicherheitsfunktionen bei der WLAN-Datenübermittlung

WLANs sind praktisch und einfach zu installieren und breiten sich daher in kleinen Unternehmen und in Privathaushalten mit Hochgeschwindigkeits-Internetzugriff rapide aus.

Da in WLANs Informationen über Funkwellen gesendet werden, sind diese Netzwerke anfälliger für Eindringlinge als herkömmliche Kabelnetzwerke.

Tipps zur Sicherheit bei der WLAN-Datenübermittlung

Sie können nicht physisch verhindern, dass jemand eine Verbindung mit Ihrem WLAN herstellt, aber Sie können das Netzwerk mit den folgenden Schritten schützen:

- Ändern Sie den Standardnamen des WLANs (die SSID).

  WLAN-Geräte haben im WLAN einen Standardnamen bzw. eine Standard-SSID. Dies ist der Name des WLANs, der aus maximal 32 Zeichen bestehen kann.

Ändern Sie zum Schutz des Netzwerks den Standardnamen für das WLAN in einen eindeutigen Namen, um das WLAN von anderen WLANs in der Umgebung zu unterscheiden.

Verwenden Sie bei der Auswahl des Namens keine persönlichen Informationen (beispielsweise Ihre Sozialversicherungsnummer), da diese Informationen für jeden sichtbar sind, der nach WLANs sucht.

- Ändern Sie das Standardkennwort.

  Bei WLAN-Produkten wie Zugriffspunkten, Routern und Gateways werden Sie nach einem Kennwort gefragt, wenn Sie die Einstellungen ändern möchten. Diese Geräte haben ein Standardkennwort. Das Standardkennwort lautet oft **cisco**.

  Hacker kennen diese Standardwerte und versuchen möglicherweise, mit diesen Standardwerten auf Ihr WLAN-Gerät zuzugreifen und die Netzwerkeinstellungen zu ändern. Vereiteln Sie nicht autorisierte Zugriffe, indem Sie für das Gerät ein schwer zu erratendes Kennwort wählen.

- Aktivieren Sie die MAC-Adressenfilterung.

  Bei Routern und Gateways von Cisco haben Sie die Möglichkeit, die MAC-Adressenfilterung zu aktivieren. Die MAC-Adresse ist eine eindeutige Folge von Ziffern und Buchstaben, die jedem Netzwerkgerät zugewiesen wird.

  Wenn die MAC-Adressenfilterung aktiviert ist, können nur WLAN-Geräte mit bestimmten MAC-Adressen auf das WLAN zugreifen. Sie können beispielsweise die MAC-Adressen der einzelnen Computer im Netzwerk angeben, sodass nur diese Computer auf das WLAN zugreifen können.

- Aktivieren Sie die Verschlüsselung.

  Verschlüsselung schützt Daten, die über ein WLAN übertragen werden. WPA/WPA2 (Wi-Fi Protected Access) und WEP (Wired Equivalent Privacy) bieten unterschiedliche Sicherheitsstufen für WLAN-Kommunikation. Zurzeit müssen Wi-Fi-zertifizierte Geräte WPA2 unterstützen, WEP jedoch nicht.

  Ein mit WPA/WPA2 verschlüsseltes Netzwerk ist sicherer als ein mit WEP verschlüsseltes Netzwerk, da bei WPA/WPA2 eine Verschlüsselung mit dynamischen Schlüsseln verwendet wird.

  Aktivieren Sie zum Schutz der Informationen bei der Funkübertragung die höchste Verschlüsselungsstufe, die von den Netzwerkgeräten unterstützt wird.

WEP ist ein älterer Verschlüsselungsstandard und ist möglicherweise bei einigen älteren Geräten ohne WPA-Unterstützung die einzige verfügbare Option.

- Stellen Sie WLAN-Router, Zugriffspunkte oder Gateways nicht in der Nähe von Außenwänden und Fenstern auf.
- Schalten Sie WLAN-Router, Zugriffspunkte oder Gateways aus, wenn sie nicht verwendet werden (beispielsweise nachts oder wenn Sie im Urlaub sind).
- Verwenden Sie sichere Kennwörter bzw. Schlüssel mit mindestens acht Zeichen. Kombinieren Sie Buchstaben und Ziffern, um die Verwendung von Standardwörtern zu vermeiden, die in einem Wörterbuch gefunden werden können.

Allgemeine Richtlinien für die Netzwerksicherheit

Die Sicherheit in einem WLAN ist wirkungslos, wenn das zugrunde liegende Netzwerk nicht sicher ist. Cisco empfiehlt, die folgenden Vorsichtsmaßnahmen zu treffen:

- Schützen Sie alle Computer im Netzwerk mit einem Kennwort, und schützen Sie vertrauliche Dateien individuell mit Kennwörtern.
- Ändern Sie die Kennwörter regelmäßig.
- Installieren Sie Antivirensoftware und Personal Firewall-Software.
- Deaktivieren Sie Dateifreigaben (Peer-to-Peer), um zu verhindern, dass Anwendungen ohne Ihre Einwilligung Dateifreigaben verwenden.

Cisco RV215W Wireless-Netzwerke

Die Gerät stellt vier virtuelle WLANs bzw. vier SSIDs (Service Set Identifiers) bereit: „ciscosb1“, „ciscosb2“, „ciscosb3“ und „ciscosb4“. Dabei handelt es sich um die Standardnamen oder SSIDs dieser Netzwerke, die Sie jedoch in aussagekräftigere Namen ändern können. In dieser Tabelle werden die Standardeinstellungen für die Netzwerke beschrieben.

SSID	ciscosb1	ciscosb2	ciscosb3	ciscosb4
Aktiviert	Ja	Nein	Nein	Nein
SSID-Übertragung	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert
Sicherheits-modus	Deaktiviert[1]	Deaktiviert	Deaktiviert	Deaktiviert
MAC-Filter	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
VLAN	1	1	1	1
WLAN-Isolation mit SSID	Deaktiviert	Deaktiviert	Deaktiviert	Deaktiviert
WMM	Aktiviert	Aktiviert	Aktiviert	Aktiviert
WPS-Hardware-taste	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert

1. Wählen Sie beim Verwenden des Setup-Assistenten die Option „Beste Sicherheit“ oder „Bessere Sicherheit“ aus, um die Gerät vor nicht autorisierten Zugriffen zu schützen.

Konfigurieren der Basis-WLAN-Einstellungen

Auf der Seite **Basiseinstellungen** (**WLAN** > **Basiseinstellungen**) können Sie grundlegende WLAN-Einstellungen konfigurieren.

So konfigurieren Sie grundlegende WLAN-Einstellungen:

SCHRITT 1 Wählen Sie **WLAN** > **Basiseinstellungen** aus.

SCHRITT 2 Aktivieren Sie im Feld **Funk** das Kontrollkästchen **Aktivieren**, um den WLAN-Sender zu aktivieren. Standardmäßig ist nur ein WLAN aktiviert (**ciscosb1**).

SCHRITT 3 Wählen Sie im Feld **WLAN-Modus** im Dropdown-Menü eine dieser Optionen aus:

B/G/N gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-N-, Wireless-B- und Wireless-G-Geräte vorhanden sind. Dies ist die Standardeinstellung (empfohlen).
Nur B	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-B-Geräte vorhanden sind.
Nur G	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-G-Geräte vorhanden sind.
Nur N	Wählen Sie diese Option aus, wenn im Netzwerk nur Wireless-N-Geräte vorhanden sind.
B/G gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-B- und Wireless-G-Geräte vorhanden sind.
G/N gemischt	Wählen Sie diese Option aus, wenn im Netzwerk Wireless-G- und Wireless-N-Geräte vorhanden sind.

SCHRITT 4 Wenn Sie **B/G/N gemischt**, **Nur N** oder **G/N gemischt** ausgewählt haben, wählen Sie im Feld **Wireless-Band-Auswahl** die WLAN-Bandbreite des Netzwerks aus (**20 MHz** oder **20/40 MHz**). Wenn Sie „Nur N“ auswählen, müssen Sie im Netzwerk WPA2-Sicherheit verwenden. Weitere Informationen hierzu finden Sie unter **Konfigurieren des Sicherheitsmodus**.

SCHRITT 5 Wählen Sie im Feld **WLAN-Kanal** im Dropdown-Menü den WLAN-Kanal aus.

SCHRITT 6 Wählen Sie im Feld **AP-Verwaltungs-VLAN** die Option **VLAN 1** aus, wenn Sie die Standardeinstellungen verwenden.

Wenn Sie zusätzliche VLANs erstellen, wählen Sie einen Wert aus, der dem VLAN entspricht, das in anderen Switches im Netzwerk konfiguriert ist. Dies dient zu Sicherheitszwecken. Möglicherweise müssen Sie das Verwaltungs-VLAN ändern, um den Zugriff auf den Gerätemanager der Gerät einzuschränken.

SCHRITT 7 (Optional) Aktivieren Sie im Feld **U-APSD (WMM-Energieeinsparung)** das Kontrollkästchen **Aktivieren**, um die U-APSD-Funktion (Unscheduled Automatic Power Save Delivery) zu aktivieren, die auch als WMM Power Save (WMM-Energieeinsparung) bezeichnet wird und Energieeinsparungen am Sender ermöglicht.

U-APSD ist eine Energiesparfunktion, die für Echtzeitanwendungen wie beispielsweise VoIP optimiert wurde, bei denen Vollduplexdaten über ein WLAN übertragen werden. Durch die Klassifizierung des ausgehenden IP-Verkehrs als Voice-Daten ermöglichen diese Anwendungsarten eine Verlängerung der Akkulaufzeit um ca. 25 % und minimieren Übertragungsverzögerungen.

SCHRITT 8 (Optional) Konfigurieren Sie die Einstellungen der vier WLANs (siehe **Bearbeiten der WLAN-Einstellungen**).

SCHRITT 9 Klicken Sie auf **Speichern**.

Bearbeiten der WLAN-Einstellungen

In der **WLAN-Tabelle** auf der Seite **Basiseinstellungen** (**WLAN** > **Basiseinstellungen**) werden die Einstellungen der vier von der Gerät unterstützten WLANs aufgelistet.

So konfigurieren Sie die Einstellungen für WLANs:

SCHRITT 1 Aktivieren Sie die Kontrollkästchen der Netzwerke, die Sie konfigurieren möchten.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Bearbeiten**.

SCHRITT 3 Konfigurieren Sie diese Einstellungen:

SSID aktivieren	Klicken Sie auf **Ein**, um das Netzwerk zu aktivieren.
SSID	Geben Sie den Namen des Netzwerks ein.
SSID-Broadcast	Aktivieren Sie dieses Kontrollkästchen, um die Übertragung der SSID zu aktivieren. Wenn die SSID-Broadcast aktiviert ist, kündigt der WLAN-Router WLAN-fähigen Geräten in seiner Reichweite seine Verfügbarkeit an.
VLAN	Wählen Sie das dem Netzwerk zugeordnete VLAN aus.
WLAN-Isolation mit SSID	Aktivieren Sie dieses Kontrollkästchen, um die WLAN-Isolation innerhalb der SSID zu aktivieren.

WMM (Wi-Fi Multimedia)	Aktivieren Sie dieses Kontrollkästchen, um WMM zu aktivieren.
WPS-Hardwaretaste	Aktivieren Sie dieses Kontrollkästchen, um die WPS-Taste an der Vorderseite der Gerät diesem Netzwerk zuzuordnen.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren des Sicherheitsmodus

Sie können einen der folgenden Sicherheitsmodi für WLANs konfigurieren.

Konfigurieren von WEP

Der WEP-Sicherheitsmodus bietet ein niedriges Sicherheitsniveau mit einer einfachen Verschlüsselungsmethode, die nicht so sicher ist wie WPA. Möglicherweise müssen Sie WEP verwenden, wenn die Netzwerkgeräte nicht für WPA geeignet sind.

HINWEIS Wenn Sie WEP nicht verwenden müssen, empfehlen wir die Verwendung von WPA2. Wenn Sie den WLAN-Modus „Nur N“ verwenden, müssen Sie WPA2 verwenden.

So konfigurieren Sie den WEP-Sicherheitsmodus:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**.

Die Seite **Sicherheitseinstellungen** wird angezeigt.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** die Option **WEP** aus.

SCHRITT 5 Wählen Sie im Feld **Authentifizierungstyp** eine der folgenden Optionen aus:

- **Offenes System**: Dies ist die Standardoption.
- **Gemeinsamer Schlüssel**: Wählen Sie diese Option aus, wenn der Netzwerkadministrator diese Einstellung empfiehlt. Wenn Sie nicht sicher sind, wählen Sie die Standardoption aus.

In beiden Fällen muss der WLAN-Client den richtigen gemeinsamen Schlüssel (Kennwort) angeben, um Zugriff auf das WLAN zu erhalten.

SCHRITT 6 Wählen Sie im Feld **Verschlüsselung** den Verschlüsselungstyp aus:

- **10/64-Bit (10 HEX-Zeichen):** Stellt einen 40-Bit-Schlüssel bereit.
- **26/128-Bit (26 HEX-Zeichen)**: Stellt einen 104-Bit-Schlüssel bereit, der stärkere Verschlüsselung bietet und daher schwerer zu dekodieren ist. Wir empfehlen 128-Bit-Verschlüsselung.

SCHRITT 7 (Optional) Geben Sie in das Feld **Kennsatz** einen alphanumerischen Begriff ein (optimale Sicherheit erreichen Sie mit mehr als acht Zeichen), und klicken Sie auf **Schlüssel generieren**, um in den WEP-Schlüsselfeldern vier eindeutige WEP-Schlüssel zu generieren.

Wenn Sie einen eigenen Schlüssel angeben möchten, geben Sie diesen direkt in das Feld **Schlüssel 1** ein (empfohlen). Die Länge des Schlüssels sollte 5 ASCII-Zeichen (oder 10 Hexadezimalzeichen) für 64-Bit-WEP und 13 ASCII-Zeichen (oder 26 Hexadezimalzeichen) für 128-Bit WEP betragen. Gültige Hexadezimalzeichen sind 0 bis 9 und A bis F.

SCHRITT 8 Wählen Sie im Feld **TX-Schlüssel** aus, welcher Schlüssel als gemeinsamer Schlüssel verwendet werden soll, den Geräte verwenden müssen, um auf das WLAN zuzugreifen.

SCHRITT 9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 10 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren von WPA-Personal, WPA2-Personal und WPA2-Personal Mixed

Die Sicherheitsmodi WPA-Personal, WPA2-Personal und WPA2-Personal Mixed können als Ersatz für WEP genutzt werden und bieten hohe Sicherheit.

- **WPA-Personal**: WPA ist ein Bestandteil des Wireless-Sicherheitsstandards (802.11i) der Wi-Fi Alliance und sollte als Übergangslösung WEP ersetzen, während der 802.11i-Standard erarbeitet wurde. WPA-Personal unterstützt TKIP (Temporal Key Integrity Protocol) und AES-Verschlüsselung (Advanced Encryption Standard).
- **WPA2-Personal**: (Empfohlen) WPA2 ist die Implementierung des im endgültigen 802.11i-Standard vorgegebenen Sicherheitsstandards. WPA2 unterstützt AES-Verschlüsselung und Authentifizierung über PSK (Preshared Key).

- **WPA2-Personal Mixed**: Ermöglicht WPA- sowie WPA2-Clients gleichzeitige Verbindungen mit PSK-Authentifizierung.

Bei der persönlichen Authentifizierung wird der PSK verwendet, bei dem es sich um einen alphanumerischen Kennsatz handelt, der mit dem WLAN-Peer ausgetauscht wird.

So konfigurieren Sie den Sicherheitsmodus WPA-Personal:

SCHRITT 1 Aktivieren Sie unter **WLANs** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**. Die Seite **Sicherheitseinstellungen** wird angezeigt.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** eine der drei Optionen für WPA-Personal aus.

SCHRITT 5 (Nur WPA-Personal) Wählen Sie im Feld **Verschlüsselung** eine der folgenden Optionen aus:

- **TKIP/AES**: Wählen Sie **TKIP/AES** aus, um die Kompatibilität mit älteren WLAN-Geräten sicherzustellen, die AES möglicherweise nicht unterstützen.
- **AES**: Dies ist die sicherere Option.

SCHRITT 6 Geben Sie in das Feld **Sicherheitsschlüssel** eine alphanumerische Zeichenfolge (8 – 63 ASCII-Zeichen oder 64 hexadezimale Ziffern) ein. Die Kennwortsicherheitsmessung zeigt die Sicherheit des Schlüssels an: „Unter Minimum“, „Schwach“, „Stark“, „Sehr stark“ oder „Sicher“. Wir empfehlen, einen Sicherheitsschlüssel zu verwenden, der in der Sicherheitsmessung als „Sicher“ eingestuft wird.

SCHRITT 7 Zum Anzeigen des Sicherheitsschlüssels bei der Eingabe aktivieren Sie das Kontrollkästchen **Kennwortmaskierung aufheben**.

SCHRITT 8 Geben Sie in das Feld **Schlüsselerneuerung** die Zeit (600-7.200 Sekunden) ein, die zwischen Schlüsselerneuerungen verstreichen soll. Der Standardwert lautet „3.600“.

SCHRITT 9 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 10 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren von WPA-Enterprise, WPA2-Enterprise und WPA2-Enterprise Mixed

Die Sicherheitsmodi WPA-Enterprise, WPA2-Enterprise und WPA2-Enterprise Mixed ermöglichen die Verwendung von RADIUS-Serverauthentifizierung.

- **WPA-Enterprise**: Ermöglicht die Verwendung von WPA mit RADIUS-Serverauthentifizierung.
- **WPA2-Enterprise**: Ermöglicht die Verwendung von WPA2 mit RADIUS-Serverauthentifizierung.
- **WPA2-Enterprise Mixed**: Ermöglicht WPA- sowie WPA2-Clients gleichzeitige Verbindungen mit RADIUS-Authentifizierung.

So konfigurieren Sie den Sicherheitsmodus WPA-Enterprise:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Sicherheitsmodus bearbeiten**.

SCHRITT 3 Wählen Sie im Feld **SSID auswählen** die SSID aus, für die Sie die Sicherheitseinstellungen konfigurieren möchten.

SCHRITT 4 Wählen Sie im Menü **Sicherheitsmodus** eine der drei Optionen für WPA-Enterprise aus.

SCHRITT 5 (Nur WPA-Enterprise) Wählen Sie im Feld **Verschlüsselung** eine der folgenden Optionen aus:

- **TKIP/AES**: Wählen Sie **TKIP/AES** aus, um die Kompatibilität mit älteren WLAN-Geräten sicherzustellen, die AES möglicherweise nicht unterstützen.
- **AES**: Dies ist die sicherere Option.

SCHRITT 6 Geben Sie in das Feld **RADIUS-Server** die IP-Adresse des RADIUS-Servers ein.

SCHRITT 7 Geben Sie in das Feld **RADIUS-Anschluss** den Anschluss ein, der für den Zugriff auf den RADIUS-Server verwendet wird.

SCHRITT 8 Geben Sie eine alphanumerische Zeichenfolge in das Feld **Gemeinsamer Schlüssel** ein.

SCHRITT 9 Geben Sie in das Feld **Schlüsselerneuerung** die Zeit (600-7.200 Sekunden) ein, die zwischen Schlüsselerneuerungen verstreichen soll. Der Standardwert lautet „3.600“.

SCHRITT 10 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 11 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren der MAC-Filterung

Sie können die MAC-Filterung verwenden, um den Zugriff auf das WLAN basierend auf der MAC-Adresse (Hardwareadresse) des anfordernden Geräts zuzulassen oder zu verweigern. Sie können beispielsweise die MAC-Adressen einer Gruppe von Computern eingeben und nur für diese Computer den Zugriff auf das Netzwerk zulassen. Sie können die MAC-Filterung für jedes Netzwerk bzw. jede SSID konfigurieren.

So konfigurieren Sie die MAC-Filterung:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **MAC-Filter bearbeiten**. Die Seite **WLAN-MAC-Filter** wird angezeigt.

SCHRITT 3 Aktivieren Sie im Feld **MAC-Filter bearbeiten** das Kontrollkästchen **Aktivieren**, um die MAC-Filterung für diese SSID zu aktivieren.

SCHRITT 4 Wählen Sie im Feld **Verbindungssteuerung** die Art des Zugriffs auf das WLAN aus:

- **Verhindern**: Wählen Sie diese Option aus, um zu verhindern, dass Geräte mit den in der **MAC-Adresstabelle** aufgelisteten Adressen auf das WLAN zugreifen. Diese Option ist standardmäßig ausgewählt.
- **Zulassen**: Wählen Sie diese Option aus, um zuzulassen, dass Geräte mit den in der **MAC-Adresstabelle** aufgelisteten Adressen auf das WLAN zugreifen.

SCHRITT 5 Zum Anzeigen der Computer und anderen Geräte im WLAN klicken Sie auf **Clientliste anzeigen**.

SCHRITT 6 Aktivieren Sie im Feld **In MAC-Adressfilterliste speichern** das Kontrollkästchen, um das Gerät der Liste der Geräte hinzuzufügen, die der **MAC-Adresstabelle** hinzugefügt werden sollen.

SCHRITT 7 Klicken Sie auf **Zu MAC hinzufügen**, um die ausgewählten Geräte in der **Clientlistentabelle** der **MAC-Adresstabelle** hinzuzufügen.

SCHRITT 8 Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SCHRITT 9 Klicken Sie auf **Zurück**, um zur Seite **Basiseinstellungen** zurückzukehren.

Konfigurieren des Tageszeitzugriffs

Sie können das Netzwerk weiter schützen, indem Sie den Zugriff auf bestimmte Zeiten beschränken, zu denen die Benutzer auf das Netzwerk zugreifen können.

So konfigurieren Sie den Tageszeitzugriff:

SCHRITT 1 Aktivieren Sie in der **WLAN-Tabelle** (**WLAN** > **Basiseinstellungen**) das Kontrollkästchen des zu konfigurierenden Netzwerks.

SCHRITT 2 Klicken Sie auf **Tageszeitzugriff**. Die Seite **Tageszeitzugriff** wird angezeigt.

SCHRITT 3 Aktivieren Sie im Feld **Aktive Zeit** das Kontrollkästchen **Aktivieren**, um den Tageszeitzugriff zu aktivieren.

SCHRITT 4 Geben Sie in den Feldern **Startzeit** und **Stoppzeit** den Zeitraum an, in dem der Zugriff auf das Netzwerk zulässig ist.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren des Wireless-Gastnetzwerks

Die Gerät unterstützt ein Wireless-Gastnetzwerk, das im Router von den anderen Wireless-SSIDs bzw. Netzwerken getrennt ist. Der Router ermöglicht einen sicheren Gastzugriff, der vom Rest des Netzwerks isoliert ist und für den eine begrenzte Zugriffsdauer und Bandbreitennutzung konfiguriert werden können. Folgende Einschränkungen und Konfigurationsrichtlinien sind dabei zu beachten:

- Für jede Gerät kann ein Gastnetzwerk konfiguriert werden.
- Das Gastnetzwerk wird als eine der vier verfügbaren SSIDs in der Gerät konfiguriert.
- Das Gastnetzwerk kann nicht im AP-Verwaltungs-VLAN (VLAN-ID 1) konfiguriert werden.

So konfigurieren Sie das Gastnetzwerk:

Erstellen eines neuen VLAN

SCHRITT 1 Klicken Sie in der Verwaltungsschnittstelle auf **Netzwerk** > **LAN** > **VLAN-Mitgliedschaft**.

SCHRITT 2 Fügen Sie in der Tabelle für VLAN-Einstellungen ein neues VLAN für das Gastnetzwerk hinzu. Klicken Sie beispielsweise auf **Hinzufügen**, und geben Sie Folgendes ein:

- **VLAN-ID**: Geben Sie eine Nummer für das VLAN ein (beispielsweise **4**).
- **Beschreibung**: Geben Sie einen Namen für das VLAN ein (beispielsweise **gast-netz**).

SCHRITT 3 Behalten Sie die Einstellung **Getaggt** für die Anschlüsse bei, und klicken Sie auf **Speichern**.

Einrichten des Gastnetzwerks

SCHRITT 1 Klicken Sie in der Verwaltungsschnittstelle auf **WLAN** > **Basiseinstellungen**.

SCHRITT 2 Wählen Sie in der WLAN-Tabelle die SSID bzw. das Netzwerk aus, die bzw. das als Gastnetzwerk fungieren soll.

SCHRITT 3 Klicken Sie auf **Bearbeiten**. Ändern Sie den SSID-Namen, um die Gastrolle kenntlich zu machen (zum Beispiel „*gast-netz*“).

SCHRITT 4 Aktivieren Sie das Kontrollkästchen **SSID-Broadcast**, damit das Netzwerk für Clients, die nach Netzwerken suchen, als verfügbare WLAN-Verbindung angezeigt wird.

SCHRITT 5 Aktivieren Sie das Kontrollkästchen **Gastnetzwerk**, um diese SSID als Gastnetzwerk zu konfigurieren.

SCHRITT 6 Wählen Sie das VLAN aus, das Sie für das Gastnetzwerk erstellt haben (falls Sie noch kein Netzwerk erstellt haben, wählen Sie **Neues VLAN hinzufügen** aus).

SCHRITT 7 Klicken Sie auf **Speichern**. Sie werden darüber benachrichtigt, dass die physischen Ethernet-Anschlüsse der Gerät von dem VLAN ausgeschlossen sind, das Sie dem Gastnetzwerk zugewiesen haben. Zusätzlich wird die WLAN-Isolation mit SSID und WMM automatisch aktiviert.

Konfigurieren des Kennworts und anderer Optionen

SCHRITT 1 Klicken Sie in der Verwaltungsschnittstelle auf **WLAN** > **Basiseinstellungen**.

SCHRITT 2 Klicken Sie in der WLAN-Tabelle auf **Gastnetz bearbeiten**.

SCHRITT 3 Geben Sie ein Kennwort ein, das für den Zugriff auf das Gastnetzwerk erforderlich sein soll.

SCHRITT 4 Geben Sie das Kennwort zur Bestätigung erneut ein.

SCHRITT 5 Geben Sie die Zeitdauer (in Minuten) ein, für die die Gastnetzwerkverbindung Benutzern zur Verfügung stehen soll.

SCHRITT 6 (Optional) Um die Bandbreitennutzung des Gastnetzwerks zu begrenzen, aktivieren Sie das Kontrollkästchen **Gast-Bandbreiteneinschränkung aktivieren**. (Hierzu muss QoS aktiviert sein. Wenn Sie QoS noch nicht konfiguriert haben, klicken Sie auf den Link zur Seite „Bandbreitenmanagement“.) Geben Sie im Feld **Verfügbare Bandbreite** ein, wie viel Prozent der Bandbreite dem Gastnetzwerk zugewiesen werden sollen.

SCHRITT 7 Klicken Sie auf **Speichern**.

Konfigurieren der erweiterten WLAN-Einstellungen

Die erweiterten WLAN-Einstellungen sollten nur von einem erfahrenen Administrator angepasst werden; falsche Einstellungen können die WLAN-Leistung beeinträchtigen.

So konfigurieren Sie die erweiterten WLAN-Einstellungen:

SCHRITT 1 Wählen Sie **WLAN** > **Erweiterte Einstellungen** aus. Die Seite „Erweiterte Einstellungen“ wird angezeigt.

SCHRITT 2 Konfigurieren Sie diese Einstellungen:

Frame Burst	Aktivieren Sie diese Option, um die Leistung der WLANs abhängig vom Hersteller der WLAN-Produkte zu verbessern. Wenn Sie nicht sicher sind, wie diese Option verwendet wird, behalten Sie die Standardeinstellung bei (aktiviert).
Keine WMM-Bestätigung	Klicken Sie, um diese Funktion zu aktivieren. Durch Aktivieren der Option „Keine WMM-Bestätigung“ können Sie einen effizienteren Durchsatz erzielen. In einer Hochfrequenzumgebung (HF) mit starkem Rauschen kann dies jedoch zu höheren Fehlerraten führen. Standardmäßig ist diese Einstellung deaktiviert.

Basisrate	Die Einstellung „Basisrate“ bezieht sich nicht auf die Übertragungsrate, sondern auf eine Reihe von Raten, die von der Services Ready-Plattform übertragen werden können. Die Gerät kündigt ihre Basisrate den anderen WLAN-Geräten im Netzwerk an, sodass diese wissen, welche Raten verwendet werden. Die Services Ready-Plattform kündigt außerdem an, dass automatisch die beste Rate für die Übertragung ausgewählt wird. Die Standardeinstellung ist „Standard“, wenn die Gerät alle standardmäßigen WLAN-Raten unterstützt (1 MBit/s, 2 MBit/s, 5,5 MBit/s, 11 MBit/s, 18 MBit/s, 24 MBit/s, 36 MBit/s, 48 MBit/s und 54 MBit/s). Neben den B- und G-Geschwindigkeiten unterstützt die Gerät auch N-Geschwindigkeiten. Als weitere Optionen stehen 1-2 MBit/s für die Verwendung mit älteren WLAN-Technologien zur Verfügung sowie „Alle“, wenn die Gerät mit allen WLAN-Raten übertragen kann. Die Basisrate entspricht nicht der Rate, mit der Daten tatsächlich übertragen werden. Wenn Sie die Datenübertragungsrate der Gerät angeben möchten, konfigurieren Sie die Einstellung „Übertragungsrate“.
Übertragungsrate	Die Datenübertragungsrate sollte abhängig von der Geschwindigkeit des WLANs festgelegt werden. Neben verschiedenen Übertragungsgeschwindigkeiten steht zudem die Option **Automatisch** zur Verfügung, mit der die Gerät automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen der Gerät und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.

N-Übertragungsrate	Die Datenübertragungsrate sollte abhängig von der Geschwindigkeit des Wireless-N-Netzwerks festgelegt werden. Neben verschiedenen Übertragungsgeschwindigkeiten steht zudem die Option **Automatisch** zur Verfügung, mit der die Gerät automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen der Gerät und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.
CTS-Schutzmodus	Die Gerät verwendet automatisch den CTS-Schutz (Clear To Send), wenn bei den Wireless-N- und Wireless-G-Geräten schwerwiegende Probleme auftreten und die Geräte in einer Umgebung mit hohem 802.11b-Verkehrsaufkommen keine Daten an die Gerät übertragen können. Diese Funktion optimiert Wireless-N- und Wireless-G-Übertragungen über die Gerät, führt jedoch zu einer spürbaren Beeinträchtigung der Leistung. Der Standardwert lautet „Automatisch“.
Beacon-Intervall	Der Wert für das Beacon-Intervall gibt das Häufigkeitsintervall des Beacons an. Ein Beacon ist ein Paket, das von der Gerät gesendet wird, um das WLAN zu synchronisieren. Geben Sie einen Wert zwischen 40 und 3.500 Millisekunden ein. Der Standardwert lautet „100“.
DTIM-Intervall	Dieser Wert (zwischen 1 und 255) gibt das Intervall für DTIM (Delivery Traffic Indication Message) an. Ein DTIM-Feld ist ein Countdownfeld, das Clients über das nächste Fenster zum Mithören von Broadcast- und Multicast-Nachrichten informiert. Wenn die Gerät Broadcast- oder Multicast-Nachrichten für zugeordnete Clients zwischengespeichert hat, sendet sie die nächste DTIM mit einem DTIM-Intervallwert. Die Clients empfangen die Beacons und werden aktiviert, sodass sie die Broadcast- und Multicast-Nachrichten empfangen. Der Standardwert lautet „1“.

Fragmentierungsschwellenwert	Dieser Wert gibt die maximal mögliche Paketgröße an, bevor Daten in mehrere Pakete aufgeteilt werden. Wenn Sie eine hohe Paketfehlerrate beobachten, können Sie den Fragmentierungsschwellenwert etwas erhöhen. Wenn Sie einen zu niedrigen Fragmentierungsschwellenwert festlegen, kann dies die Netzwerkleistung beeinträchtigen. Es wird empfohlen, den Wert nur geringfügig zu verringern. In den meisten Fällen sollten Sie den Standardwert „2.346“ beibehalten.
RTS-Schwellenwert	Wenn Sie einen uneinheitlichen Datenfluss beobachten, geben Sie nur einen geringfügig niedrigeren Wert ein. Empfohlen wird der Standardwert „2.347“. Wenn die Größe eines Netzwerkpakets den vorgegebenen RTS-Schwellenwert (Request to Send) unterschreitet, wird der RTS/CTS-Mechanismus (Clear to Send) nicht aktiviert. Die Services Ready-Plattform sendet RTS-Frames an eine bestimmte Empfängerstation und handelt das Senden eines Daten-Frames aus. Nach Empfang eines RTS antwortet die WLAN-Station mit einem CTS-Frame, um zu bestätigen, dass die Übertragung beginnen kann.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren von WDS

Ein Wireless Distribution System (WDS) ist ein System, das WLAN-Verbindungen zwischen Zugriffspunkten in einem Netzwerk ermöglicht. So kann ein WLAN mit mehreren Zugriffspunkten erweitert werden, ohne dass diese über einen drahtgebundenen Backbone verbunden sein müssen.

Zum Einrichten eines WDS-Links müssen Sie die Gerät und sonstige WDS-Remote-Peers mit dem gleichen WLAN-Modus, dem gleichen WLAN-Kanal, der gleichen WLAN-Band-Auswahl und den gleichen Verschlüsselungstypen („Keine“ oder „WEP“) konfigurieren.

WDS wird nur für eine SSID unterstützt.

So konfigurieren Sie WDS:

SCHRITT 1 Wählen Sie **WLAN** > **WDS** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Wi-Fi-Signal darf durch einen Repeater wiederholt werden**, um WDS zu aktivieren.

SCHRITT 3 Zum manuellen Eingeben der MAC-Adresse eines Repeaters klicken Sie auf **Manuell** oder wählen **Automatisch** aus, damit der Router Remotezugriffspunkte automatisch erkennt.

Wenn Sie Repeater aus der Tabelle der verfügbaren Netzwerke auswählen möchten, können Sie auch auf **Standortübersicht anzeigen** klicken, um die **Tabelle verfügbarer Netzwerke** anzuzeigen.

a. Aktivieren Sie die Kontrollkästchen, um maximal drei Zugriffspunkte auszuwählen, die als Repeater verwendet werden sollen.

b. Klicken Sie auf **Verbinden**, um die MAC-Adressen der ausgewählten Zugriffspunkte im Feld „MAC“ hinzuzufügen.

Sie können die MAC-Adressen von maximal drei Zugriffspunkten aus in die Felder **MAC 1**, **MAC 2** und **MAC 3** eingeben, um diese als Repeater zu verwenden.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von WPS

Konfigurieren Sie WPS so, dass WPS-fähige Geräte einfach und sicher mit dem WLAN verbunden werden können. Weitere Anweisungen zum Einrichten von WPS auf Ihrem Clientgerät finden Sie in der Dokumentation zum jeweiligen Clientgerät.

So konfigurieren Sie WPS:

SCHRITT 1 Wählen Sie **WLAN** > **WPS** aus. Die Seite „Wi-Fi Protected Setup“ wird angezeigt.

SCHRITT 2 Wählen Sie im Dropdown-Menü **SSID** das WLAN aus, für das Sie WPS aktivieren möchten.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **WPS aktivieren**, um WPS zu aktivieren. Zum Deaktivieren von WPS deaktivieren Sie das Kontrollkästchen.

SCHRITT 4 Konfigurieren Sie WPS für Clientgeräte mit einer der drei folgenden Methoden:

a. Klicken Sie auf den WPS-Knopf am Client-Gerät (oder drücken Sie darauf), und klicken Sie dann auf das WPS-Symbol auf dieser Seite.

b. Geben Sie die WPS-PIN-Nummer des Client ein, und klicken Sie auf **Registrieren**.

c. Geben Sie eine PIN-Nummer für den Router ein. Verwenden Sie die angegebene PIN-Nummer des Routers.

Geräte-PIN-Status: PIN-Status des WPA-Geräts.

Geräte-PIN: Gibt die PIN des Gerätes an, das versucht eine Verbindung herzustellen.

PIN-Gültigkeitsdauer: Die Gültigkeitsdauer des Schlüssels. Wenn die Gültigkeit abläuft, wird ein neuer Schlüssel ausgehandelt.

Wenn Sie WPS konfiguriert haben, werden unten auf der Seite **WPS** die folgenden Informationen angezeigt: Wi-Fi Protected Setup-Status, Netzwerkname (SSID) und Sicherheit.

5

Konfigurieren der Firewall

In diesem Kapitel wird beschrieben, wie Sie die Firewalleigenschaften der Gerät konfigurieren.

- **Firewallfunktionen des Cisco RV215W**
- **Konfigurieren der grundlegenden Firewalleinstellungen**
- **Verwalten von Firewallzeitplänen**
- **Konfigurieren der Serviceverwaltung**
- **Konfigurieren von Zugriffsregeln**
- **Erstellen einer Internetzugriffsrichtlinie**
- **Konfigurieren der Anschlussweiterleitung**

Firewallfunktionen des Cisco RV215W

Sie können Ihr Netzwerk schützen, indem Sie Regeln erstellen und anwenden, die von dem Gerät verwendet werden, um ein- und ausgehenden Internetverkehr selektiv zu blockieren bzw. zuzulassen. Dann geben Sie an, auf welche Weise und für welche Geräte die Regeln angewendet werden sollen. Hierzu müssen Sie Folgendes definieren:

- Services oder Verkehrstypen (Beispiele: Webbrowsing, VoIP, andere Standardservices sowie von Ihnen definierte benutzerdefinierte Services), die der Router zulassen oder blockieren soll.
- Die Verkehrsrichtung, indem Sie Quelle und Ziel des Verkehrs angeben; hierzu geben Sie die „Von“-Zone (LAN/WAN/DMZ) und die „An“-Zone (LAN/WAN/DMZ) an.
- Zeitpläne, nach denen der Router Regeln anwenden soll.

- Schlüsselwörter (in einem Domänennamen oder in der URL einer Webseite), die der Router zulassen oder blockieren soll.
- Regeln für das Blockieren des ein- und ausgehenden Internetverkehrs für bestimmte Services nach vorgegebenen Zeitplänen.
- MAC-Adressen von Geräten, bei denen der Router den eingehenden Zugriff auf das Netzwerk blockieren soll.
- Anschlussauslöser, die dem Router signalisieren, dass der Zugriff auf bestimmte durch die Anschlussnummer definierte Services zugelassen oder blockiert werden soll.
- Berichte und Warnungen, die der Router an Sie senden soll.

Sie können beispielsweise Regeln für eingeschränkten Zugriff festlegen, die auf der Tageszeit, auf Webadressen und auf Schlüsselwörtern in Webadressen basieren. Sie können den Internetzugriff durch Anwendungen und Services im LAN blockieren, beispielsweise für Chaträume oder Spiele. Sie können den Zugriff nur auf bestimmte PC-Gruppen im Netzwerk durch das WAN oder das öffentliche DMZ-Netzwerk blockieren.

Eingangsregeln (von WAN zu LAN/DMZ) schränken den Zugriff für im Netzwerk eingehenden Verkehr ein, sodass nur bestimmte Benutzer von außen auf bestimmte lokale Ressourcen zugreifen können. Standardmäßig wird der gesamte Zugriff von der nicht sicheren WAN-Seite auf das sichere LAN blockiert, sofern es sich nicht um Antworten auf Anforderungen aus dem LAN oder der DMZ handelt. Wenn Sie externen Geräten den Zugriff auf Services im sicheren LAN ermöglichen möchten, müssen Sie für jeden Service eine Firewallregel erstellen.

Wenn Sie eingehenden Verkehr zulassen möchten, müssen Sie die IP-Adresse des WAN-Anschlusses des Routers öffentlich bekannt machen. Dies wird als „Exponierung des Hosts“ bezeichnet, der nun bekannt und von außen zugänglich, aber auch angreifbar ist. Wie Sie die Adresse bekannt geben, hängt von der Konfiguration der WAN-Anschlüsse ab. Für Ihr Gerät können Sie die IP-Adresse verwenden, wenn dem WAN-Anschluss eine statische Adresse zugewiesen ist. Bei einer dynamischen WAN-Adresse kann ein dynamischer DNS-Name (DDNS) verwendet werden.

Ausgangsregeln (von LAN/DMZ zu WAN) schränken den Zugriff für Verkehr ein, der das Netzwerk verlässt. Dabei können nur bestimmte lokale Benutzer auf bestimmte externe Ressourcen zugreifen. Die Standardausgangsregel lässt den Zugriff aus der sicheren Zone (LAN) auf die öffentliche DMZ oder das nicht sichere WAN zu. Um den Zugriff von Hosts im sicheren LAN auf Services im externen (nicht sicheren) WAN zu blockieren, müssen Sie für jeden Service eine Firewallregel erstellen.

Konfigurieren der grundlegenden Firewalleinstellungen

So konfigurieren Sie grundlegende Firewalleinstellungen:

SCHRITT 1 Wählen Sie **Firewall** > **Basiseinstellungen** aus.

SCHRITT 2 Konfigurieren Sie die folgenden Firewalleinstellungen:

Firewall	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Firewalleinstellungen zu konfigurieren.
DoS-Schutz	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um den Denial of Service-Schutz zu aktivieren.
WAN-Anfrage „sperren“ Konfigurieren durch Benutzer zulassen	Blockiert über das WAN gesendete Ping-Anforderungen an das Gerät.
Webzugriff	Wählen Sie den Typ des Webzugriffs aus, der für Verbindungen mit der Firewall verwendet werden kann: HTTP oder HTTPS (sicheres HTTP).
Remoteverwaltung Remote-Zugriff Remote-Upgrade Zulässige Remote-IP-Adresse Remoteverwaltungs-anschluss	Weitere Informationen hierzu finden Sie unter **Konfigurieren der Remoteverwaltung**.
IPv4-Multicast-Passthrough (IGMP-Proxy)	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Multicast-Passthrough für IPv4 zu aktivieren.
IPv6-Multicast-Passthrough (IGMP-Proxy)	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Multicast-Passthrough für IPv6 zu aktivieren.
UPnP Konfiguration durch Benutzer zulassen Benutzer darf Internetzugriff deaktivieren	Weitere Informationen hierzu finden Sie unter **Konfigurieren von Universal Plug and Play**.

Java blockieren	Aktivieren Sie dieses Kontrollkästchen, um Java-Applets zu blockieren. Java-Applets sind kleine Programme, die in Webseiten eingebettet sind und dynamische Funktionen auf der Seite aktivieren. Ein bösartiges Applet kann verwendet werden, um Computer zu gefährden oder zu infizieren. Durch Aktivieren dieser Einstellung blockieren Sie das Herunterladen von Java-Applets. Klicken Sie auf **Automatisch**, um Java automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Anschluss ein, an dem Java blockiert werden soll.
Cookies blockieren	Aktivieren Sie dieses Kontrollkästchen, um Cookies zu blockieren. Cookies werden verwendet, um Sitzungsinformationen von Websites zu speichern, für die in der Regel eine Anmeldung erforderlich ist. Verschiedene Websites verwenden Cookies jedoch zum Speichern von Nachverfolgungsinformationen und Informationen zum Surfverhalten. Wenn Sie diese Option aktivieren, wird die Erstellung von Cookies durch Websites verhindert. Bei vielen Websites müssen Cookies akzeptiert werden, damit der ordnungsgemäße Zugriff auf die Website möglich ist. Das Blockieren von Cookies kann bei vielen Websites dazu führen, dass bestimmte Funktionen nicht zur Verfügung stehen. Klicken Sie auf **Automatisch**, um Cookies automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Anschluss ein, an dem Cookies blockiert werden sollen.

ActiveX blockieren	Aktivieren Sie dieses Kontrollkästchen, um ActiveX-Inhalte zu blockieren. ActiveX-Steuerelemente werden ähnlich wie Java-Applets beim Ausführen von Internet Explorer auf einem Computer unter Windows installiert. Ein bösartiges ActiveX-Steuerelement kann verwendet werden, um Computer zu gefährden oder zu infizieren. Durch Aktivieren dieser Einstellung blockieren Sie das Herunterladen von ActiveX-Steuerelementen. Klicken Sie auf **Automatisch**, um ActiveX automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Anschluss ein, an dem ActiveX blockiert werden soll.
Proxy blockieren	Aktivieren Sie dieses Kontrollkästchen, um Proxyserver zu blockieren. Ein Proxyserver (oder Proxy) ermöglicht Computern das Weiterleiten von Verbindungen an andere Computer durch den Proxy, sodass bestimmte Firewallregeln umgangen werden. Wenn beispielsweise Verbindungen mit einer bestimmten IP-Adresse durch eine Firewallregel blockiert werden, können die Anforderungen durch einen Proxy geleitet werden, der nicht durch die Regel blockiert wird. Dadurch wird die Einschränkung unwirksam. Wenn Sie diese Funktion aktivieren, werden Proxyserver blockiert. Klicken Sie auf **Automatisch**, um Proxyserver automatisch zu blockieren, oder klicken Sie auf **Manuell** und geben Sie einen bestimmten Anschluss ein, an dem Proxyserver blockiert werden sollen.
FTP ALG	Klicken Sie auf **Automatisch**, um den Standard-FTP-Port 21 zu verwenden. Klicken Sie auf **Manuell**, wenn Sie die Nummer des Ports eingeben möchten, über den der FTP-Verkehr auf dem Gerät geleitet werden soll.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren der Remoteverwaltung

Sie können das Remote-Management aktivieren, damit Sie über ein Remote-WAN auf das Gerät zugreifen können.

Zum Konfigurieren der Remoteverwaltung konfigurieren Sie auf der Seite **Basiseinstellungen** diese Einstellungen:

Remoteverwaltung	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Remoteverwaltung zu aktivieren.
Remotezugriff	Wählen Sie den Typ des Webzugriffs aus, der für Verbindungen mit der Firewall verwendet werden kann: HTTP oder HTTPS (sicheres HTTP).
Remote-Upgrade	Wenn Sie Remote-Upgrades des Geräts zulassen möchten, aktivieren Sie das Kontrollkästchen **Aktivieren**.
Zulässige Remote-IP-Adresse	Klicken Sie auf die Schaltfläche **Beliebige IP-Adresse**, um die Remoteverwaltung über beliebige IP-Adressen zuzulassen, oder geben Sie eine bestimmte IP-Adresse in das Adressfeld ein.
Remoteverwaltungs-anschluss	Geben Sie den Anschluss ein, an dem der Remotezugriff zulässig ist. Standardmäßig wird der Anschluss 443 verwendet. Wenn Sie remote auf den Router zugreifen, müssen Sie den Remoteverwaltungsanschluss als Teil der IP-Adresse eingeben. Beispiel: **https://<remote-ip>:<remote-port>** oder **https://168.10.1.11:443**

VORSICHT Wenn die Remoteverwaltung aktiviert ist, kann jeder, der die IP-Adresse kennt, auf den Router zugreifen. Da ein böswilliger WAN-Benutzer das Gerät umkonfigurieren und missbrauchen könnte, wird empfohlen, das Administratorkennwort und alle Gastkennwörter zu ändern, bevor Sie fortfahren.

Konfigurieren von Universal Plug and Play

Universal Plug and Play (UPnP) ermöglicht die automatische Erkennung von Geräten, die mit dem Gerät kommunizieren können.

Zum Konfigurieren von UPnP konfigurieren Sie auf der Seite **Basiseinstellungen** diese Einstellungen:

UPnP	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um UPnP zu aktivieren.
Benutzer darf konfigurieren	Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass Benutzer, auf deren Computern oder anderen UPnP-fähigen Geräten die UPnP-Unterstützung aktiviert ist, UPnP-Anschlusszuordnungsregeln festlegen. Wenn das Kontrollkästchen deaktiviert ist, lässt das Gerät nicht zu, dass die Weiterleitungsregel von Anwendungen hinzugefügt wird.
Benutzer darf Internetzugriff deaktivieren	Aktivieren Sie dieses Kontrollkästchen, um zuzulassen, dass Benutzer den Internetzugriff deaktivieren.

Verwalten von Firewallzeitplänen

Sie können Firewallzeitpläne erstellen, um Firewallregeln an bestimmten Tagen oder zu bestimmten Tageszeiten anzuwenden.

Hinzufügen oder Bearbeiten eines Firewallzeitplans

So erstellen oder bearbeiten Sie einen Zeitplan:

SCHRITT 1 Wählen Sie **Firewall** > **Zeitplanverwaltung** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie in das Feld **Name** einen eindeutigen Namen zum Identifizieren des Zeitplans ein. Dieser Name steht auf der Seite „Firewallregelkonfiguration“ in der Liste **Zeitplan auswählen** zur Verfügung. (Weitere Informationen hierzu finden Sie unter **Konfigurieren von Zugriffsregeln**.)

SCHRITT 4 Wählen Sie unter **Geplante Tage** aus, ob der Zeitplan an allen Tagen oder an bestimmten Tagen angewendet werden soll. Wenn Sie **Bestimmte Tage** auswählen, aktivieren Sie das Kontrollkästchen neben den Tagen, die Sie in den Zeitplan aufnehmen möchten.

SCHRITT 5 Wählen Sie unter **Geplante Tageszeit** die Tageszeit aus, zu der der Zeitplan angewendet werden soll. Sie können **Alle Zeiten** oder **Bestimmte Zeit** auswählen. Wenn Sie **Bestimmte Zeit** auswählen, geben Sie die Start- und Endzeit ein.

SCHRITT 6 Klicken Sie auf **Speichern**.

Konfigurieren der Serviceverwaltung

Wenn Sie eine Firewallregel erstellen, können Sie einen Service angeben, der durch die Regel gesteuert wird. Es stehen allgemeine Servicetypen zur Auswahl und Sie können auch eigene benutzerdefinierte Services erstellen.

Auf der Seite **Serviceverwaltung** können Sie benutzerdefinierte Services erstellen, für die Firewallregeln definiert werden können. Wenn Sie die Regeln definiert haben, wird der neue Service in der **Tabelle Verfügbare benutzerdefinierte Services** angezeigt.

So erstellen Sie einen benutzerdefinierten Service:

SCHRITT 1 Wählen Sie **Firewall** > **Serviceverwaltung** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie in das Feld **Servicename** zu Identifizierungs- und Verwaltungszwecken den Servicenamen ein.

SCHRITT 4 Wählen Sie im Dropdown-Menü im Feld **Protokoll** das vom Service verwendete Schicht-4-Protokoll aus:

- **TCP**
- **UDP**
- **TCP & UDP**
- **ICMP**

SCHRITT 5 Geben Sie in das Feld **Anfangsport** den ersten TCP- oder UDP-Anschluss des vom Service verwendeten Bereichs ein.

SCHRITT 6 Geben Sie in das Feld **Endport** den letzten TCP- oder UDP-Anschluss des vom Service verwendeten Bereichs ein.

SCHRITT 7 Klicken Sie auf **Speichern**.

Zum Bearbeiten eines Eintrags wählen Sie den Eintrag aus und klicken auf **Bearbeiten**. Nehmen Sie die Änderungen vor, und klicken Sie dann auf **Speichern**.

Konfigurieren von Zugriffsregeln

Konfigurieren der Standardausgangsrichtlinie

Auf der Seite **Zugriffsregeln** können Sie die Standardausgangsrichtlinie für den Verkehr konfigurieren, der vom sicheren Netzwerk (LAN) zum nicht sicheren Netzwerk (dediziertes WAN/optional) geleitet wird.

Die Standardeingangsrichtlinie für Verkehr, der aus der nicht sicheren Zone in die sichere Zone fließt, blockiert den Verkehr immer und kann nicht geändert werden.

So konfigurieren Sie die Standardausgangsrichtlinie:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Wählen Sie **Zulassen** oder **Verweigern** aus.

Hinweis: Stellen Sie sicher, dass die IPv6-Unterstützung im Gerät konfiguriert ist, wenn Sie eine IPv6-Firewall konfigurieren möchten. Weitere Informationen hierzu finden Sie unter **Konfigurieren von IPv6**.

SCHRITT 3 Klicken Sie auf **Speichern**.

Ändern der Reihenfolge der Zugriffsregeln

Die Reihenfolge, in der die Zugriffsregeln in der Zugriffsregeltabelle angezeigt werden, entspricht der Reihenfolge, in der die Regeln angewendet werden. Wenn die Regeln in einer bestimmten Reihenfolge angewendet werden sollen, müssen Sie ggf. die Reihenfolge in der Tabelle ändern. So können Sie beispielsweise festlegen, dass eine Regel zum Zulassen bestimmter Verkehrstypen vor der Blockierung anderer Verkehrstypen angewendet wird.

So ändern Sie die Reihenfolge der Zugriffsregeln:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Klicken Sie auf **Neu ordnen**.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen in der Zeile mit der zu verschiebenden Regel, und klicken Sie auf die Pfeile, um die Regel um eine Zeile nach oben oder unten zu verschieben. Sie können auch die gewünschte Position der Regel aus der Dropdown-Liste auswählen und dann auf **Verschieben nach** klicken.

SCHRITT 4 Klicken Sie auf **Speichern**.

Hinzufügen von Zugriffsregeln

Alle im Gerät konfigurierten Firewallregeln werden in der **Zugriffsregeltabelle** angezeigt. Aus dieser Liste geht außerdem hervor, ob die Regel aktiviert (aktiv) ist. Des Weiteren sehen Sie eine Zusammenfassung der „Von“-/„An“-Zone sowie der von der Regel betroffenen Services und Benutzer.

So erstellen Sie eine Zugriffsregel:

SCHRITT 1 Wählen Sie **Firewall** > **Zugriffsregeln** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Wählen Sie im Feld **Verbindungstyp** die Quelle des Verkehrs aus:

- **Ausgehend (LAN > WAN)**: Wählen Sie diese Option aus, um eine Ausgangsregel zu erstellen.
- **Eingehend (WAN > LAN)**: Wählen Sie diese Option aus, um eine Eingangsregel zu erstellen.
- **Eingehend (WAN > DMZ)**: Wählen Sie diese Option aus, um eine Eingangsregel zu erstellen.

SCHRITT 4 Wählen Sie im Dropdown-Menü **Aktion** die Aktion aus:

- **Immer blockieren**: Der ausgewählte Verkehrstyp wird immer blockiert.
- **Immer zulassen**: Der ausgewählte Verkehrstyp wird nie blockiert.
- **Gemäß Zeitplan blockieren, sonst zulassen**: Der ausgewählte Verkehrstyp wird nach einem Zeitplan blockiert.
- **Gemäß Zeitplan zulassen, sonst blockieren**: Der ausgewählte Verkehrstyp wird nach einem Zeitplan zugelassen.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Services** den Service aus, der für diese Regel zugelassen oder blockiert werden soll. Wählen Sie **Gesamter Datenverkehr** aus, um zuzulassen, dass die Regel auf alle Anwendungen und Services angewendet wird, oder wählen Sie eine einzelne Anwendung aus, die blockiert werden soll:

- Domain Name System (DNS), UDP oder TCP
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)

- Trivial File Transfer Protocol (TFTP)
- Internet Message Access Protocol (IMAP)
- Network News Transport Protocol (NNTP)
- Post Office Protocol (POP3)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Telnet
- STRMWORKS
- Terminal Access Controller Access-Control System (TACACS)
- Telnet (Befehl)
- Telnet (sekundär)
- Telnet SSL
- Voice (SIP)

SCHRITT 6 (Optional) Klicken Sie auf **Services konfigurieren**, um zur Seite **Serviceverwaltung** zu wechseln und die Services zu konfigurieren, bevor Sie Zugriffsregeln darauf anwenden.

Weitere Informationen finden Sie unter **Konfigurieren der Serviceverwaltung**.

SCHRITT 7 Wählen Sie im Feld **Quell-IP** die Benutzer aus, auf die die Firewallregel angewendet werden soll:

- **Beliebig**: Die Regel gilt für Verkehr, der von einem beliebigen Host im lokalen Netzwerk ausgeht.
- **Einzelne Adresse**: Die Regel gilt für Verkehr, der von einer einzelnen IP-Adresse im lokalen Netzwerk ausgeht. Geben Sie die Adresse in das Feld **Start** ein.
- **Adressbereich**: Die Regel gilt für Verkehr, der von einer IP-Adresse in einem Adressbereich ausgeht. Geben Sie in das Feld **Start** die IP-Startadresse und in das Feld **Ende** die IP-Endadresse ein.

SCHRITT 8 Geben Sie im Feld **Protokollieren** an, ob die Pakete für diese Regel protokolliert werden sollen.

Wenn Sie Details für alle dieser Regel entsprechenden Pakete protokollieren möchten, wählen Sie im Dropdown-Menü **Immer** aus. Wenn beispielsweise für einen Zeitplan die Ausgangsregel **Immer blockieren** ausgewählt ist, wird für jedes Paket, das eine ausgehende Verbindung für diesen Service herzustellen versucht, im Protokoll eine Meldung mit der Quell- und Zieladresse des Pakets (und weiteren Informationen) aufgezeichnet.

Das Aktivieren der Protokollierung kann zu einer großen Menge von Protokollmeldungen führen und wird nur zu Fehlerbehebungszwecken empfohlen.

Wählen Sie **Nie** aus, um die Protokollierung zu deaktivieren.

HINWEIS Wenn Verkehr vom LAN oder von der DMZ zum WAN fließt, setzt das System voraus, dass die Quell- oder Ziel-IP-Adresse eingehender IP-Pakete beim Passieren der Firewall neu geschrieben wird.

SCHRITT 9 Weisen Sie im Feld **QoS-Priorität** den IP-Paketen dieses Service eine Priorität zu. Die Prioritäten werden anhand von QoS-Stufen definiert: (**1 (niedrigste Stufe)**, **2**, **3**, **4 (höchste Stufe)**).

SCHRITT 10 Aktivieren Sie im Feld **Regelstatus** das Kontrollkästchen, um die neue Zugriffsregel zu aktivieren.

SCHRITT 11 Klicken Sie auf **Speichern**.

Erstellen einer Internetzugriffsrichtlinie

Das Gerät unterstützt verschiedene Optionen zum Blockieren des Internetzugriffs. Sie können den gesamten Internetverkehr blockieren, den Internetverkehr zu bestimmten PCs oder Endpunkten blockieren oder den Zugriff auf Internetsites blockieren, indem Sie Schlüsselwörter angeben, die blockiert werden sollen. Wenn diese Schlüsselwörter im Namen der Website gefunden werden (beispielsweise in einer Website-URL oder in einem Newsgroupnamen), wird die Website blockiert.

Hinzufügen oder Bearbeiten einer Internetzugriffsrichtlinie

So erstellen Sie eine Internetzugriffsrichtlinie:

SCHRITT 1 Wählen Sie **Firewall** > **Internetzugriffsrichtlinie** aus.

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Aktivieren Sie im Feld **Status** das Kontrollkästchen **Aktivieren**.

SCHRITT 4 Geben Sie zu Identifizierungs- und Verwaltungszwecken einen Richtliniennamen ein.

SCHRITT 5 Wählen Sie im Dropdown-Menü **Aktion** den Typ der gewünschten Zugriffseinschränkung aus:

- **Immer blockieren**: Internetverkehr wird immer blockiert. Damit blockieren Sie den Internetverkehr zu und von allen Endpunkten. Wenn Sie den gesamten Verkehr blockieren möchten, aber bestimmten Endpunkten den Empfang von Internetverkehr ermöglichen möchten, finden Sie weitere Informationen in Schritt 7.
- **Immer zulassen**: Internetverkehr ist immer zulässig. Sie können diese Einstellung optimieren, um Internetverkehr für bestimmte Endpunkte zu blockieren (siehe Schritt 7). Sie können auch sämtlichen Internetverkehr mit Ausnahme bestimmter Websites zulassen (siehe Schritt 8).
- **Gemäß Zeitplan blockieren**: Blockiert Internetverkehr gemäß einem Zeitplan (beispielsweise wenn Sie Internetverkehr an Wochentagen während der Geschäftszeiten blockieren, außerhalb der Geschäftszeiten und an Wochenenden jedoch zulassen möchten).
- **Gemäß Zeitplan zulassen**: Internetverkehr wird nach einem Zeitplan zugelassen.

Wenn Sie **Gemäß Zeitplan blockieren** oder **Gemäß Zeitplan zulassen** ausgewählt haben, klicken Sie auf **Zeitpläne konfigurieren**, um einen Zeitplan zu erstellen. Weitere Informationen hierzu finden Sie unter **Verwalten von Firewallzeitplänen**.

SCHRITT 6 Wählen Sie im Dropdown-Menü einen Zeitplan aus.

SCHRITT 7 (Optional) Wenden Sie die Zugriffsrichtlinie auf bestimmte PCs an, um Verkehr von bestimmten Geräten zuzulassen oder zu blockieren:

a. Klicken Sie in der Tabelle **Zugriffsrichtlinie auf die folgenden PCs anwenden** auf **Hinzufügen**.

b. Wählen Sie im Dropdown-Menü **Typ** aus, wie der PC identifiziert werden soll (anhand der MAC-Adresse, anhand der IP-Adresse oder anhand eines IP-Adressbereichs).

c. Geben Sie in das Feld **Wert** abhängig von Ihrer Auswahl im vorherigen Schritt einen der folgenden Werte ein:

- Die MAC-Adresse (xx:xx:xx:xx:xx:xx) des PCs, für den die Richtlinie gilt.
- Die IP-Adresse des PCs, für den die Richtlinie gilt.
- Die erste und letzte IP-Adresse des zu blockierenden Adressbereichs (beispielsweise 192.168.1.2 – 192.168.1.253).

SCHRITT 8 So blockieren Sie Verkehr von bestimmten Websites:

a. Klicken Sie in der Tabelle **Website-Blockierung** auf **Hinzufügen**.

b. Wählen Sie im Dropdown-Menü **Typ** aus, wie eine Website blockiert werden soll (durch Angeben der URL oder durch Angeben eines in der URL enthaltenen Schlüsselworts).

c. Geben Sie in das Feld **Wert** die URL oder das Schlüsselwort ein, die bzw. das zum Blockieren der Website verwendet werden soll.

Wenn Sie beispielsweise die URL Beispiel.com blockieren möchten, wählen Sie im Dropdown-Menü die Option **URL-Adresse** aus und geben **Beispiel.com** in das Feld **Wert** ein. Wenn Sie eine URL blockieren möchten, die das Schlüsselwort „Beispiel“ enthält, wählen Sie im Dropdown-Menü die Option **Schlüsselwort** aus, und geben Sie in das Feld **Wert** den Begriff **Beispiel** ein.

SCHRITT 9 Klicken Sie auf **Speichern**.

Konfigurieren der Anschlussweiterleitung

Die Anschlussweiterleitung wird verwendet, um Verkehr aus dem Internet von einem Anschluss im WAN an einen anderen Anschluss im LAN umzuleiten. Häufig verwendete Services sind bereits vordefiniert. Alternativ können Sie einen benutzerdefinierten Service und zugeordnete Anschlüsse für die Weiterleitung definieren.

Auf den Seiten **Regeln für die Einzelportweiterleitung** und **Regeln für die Portbereichsweiterleitung** werden alle verfügbaren Anschlussweiterleitungsregeln für das Gerät aufgeführt und Sie können Anschlussweiterleitungsregeln konfigurieren.

HINWEIS Für Server im LAN ist die Anschlussweiterleitung nicht geeignet, da die eingehenden Anschlüsse erst geöffnet werden, wenn das LAN-Gerät eine ausgehende Verbindung hergestellt hat.

Manche Anwendungen funktionieren beim Herstellen einer Verbindung durch externe Geräte nur dann ordnungsgemäß, wenn sie Daten an einem bestimmten Anschluss oder Portbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur am erforderlichen Anschluss oder Portbereich senden.

Das Gateway verfügt über eine Liste gängiger Anwendungen und Spiele sowie der ausgehenden und eingehenden Anschlüsse, die jeweils geöffnet werden müssen. Sie können auch eine Anschlussweiterleitungsregel angeben, indem Sie den Verkehrstyp (TCP oder UDP) und den Bereich der eingehenden und ausgehenden Anschlüsse definieren, die geöffnet werden sollen, wenn die Regel aktiviert ist.

Konfigurieren der Einzelportweiterleitung

So fügen Sie eine Regel für die Einzelportweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Einzelportweiterleitung** aus. Eine bereits vorhandene Liste mit Anwendungen wird angezeigt.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Anschlussweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie in das Feld **Externer Port** die Anschlussnummer ein, die diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird.

SCHRITT 4 Geben Sie in das Feld **Interner Port** die Anschlussnummer ein, die vom Remotesystem verwendet wird, um auf die empfangene Anforderung zu antworten.

SCHRITT 5 Wählen Sie im Menü „Schnittstelle“ **Beides (Ethernet & 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 6 Wählen Sie im Dropdown-Menü **Protokoll** ein Protokoll aus (**TCP**, **UDP** oder **TCP** & **UDP**).

SCHRITT 7 Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts auf der LAN-Seite ein, an den der jeweilige IP-Verkehr weitergeleitet werden soll. Sie können beispielsweise HTTP-Verkehr an Anschluss 80 der IP-Adresse eines Webservers auf der LAN-Seite weiterleiten.

SCHRITT 8 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 9 Klicken Sie auf **Speichern**.

Konfigurieren der Portbereichsweiterleitung

So fügen Sie eine Regel für die Portbereichsweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Portbereichsweiterleitung** aus.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Anschlussweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie im Feld **Externer Port** die Anschlussnummer an, die diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird.

SCHRITT 4 Geben Sie im Feld **Start** die Anschlussnummer an, mit der der Bereich der weiterzuleitenden Anschlüsse beginnt.

SCHRITT 5 Geben Sie im Feld **Ende** die Anschlussnummer an, mit der der Bereich der weiterzuleitenden Anschlüsse endet.

SCHRITT 6 Wählen Sie im Menü „Schnittstelle“ **Beides (Ethernet & 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 7 Wählen Sie im Dropdown-Menü **Protokoll** ein Protokoll aus (**TCP**, **UDP** oder **TCP** & **UDP**).

SCHRITT 8 Geben Sie in das Feld **IP-Adresse** die IP-Adresse des Hosts auf der LAN-Seite ein, an den der jeweilige IP-Verkehr weitergeleitet werden soll.

SCHRITT 9 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 10 Klicken Sie auf **Speichern**.

Konfigurieren der Auslösung des Portbereichs

Mithilfe der Anschlussauslösung können Geräte im LAN oder in der DMZ anfordern, dass einer oder mehrere Anschlüsse an sie weitergeleitet werden. Die Anschlussauslösung wartet auf ausgehende Anforderungen vom LAN bzw. von der DMZ an einem der definierten ausgehenden Anschlüsse und öffnet dann einen eingehenden Anschluss für den angegebenen Verkehrstyp.

Die Anschlussauslösung ist eine Form der dynamischen Anschlussweiterleitung, während eine Anwendung Daten über die geöffneten ausgehenden oder eingehenden Anschlüsse überträgt. Die Anschlussauslösung öffnet einen eingehenden Anschluss für einen bestimmten Verkehrstyp an einem definierten ausgehenden Anschluss. Die Anschlussauslösung ist flexibler als die (beim Konfigurieren von Firewallregeln verfügbare) statische Anschlussweiterleitung, da eine Regel nicht auf eine bestimmte IP-Adresse oder einen bestimmten IP-Adressbereich im LAN verweisen muss. Außerdem werden die Anschlüsse bei Nichtverwendung nicht offen gelassen, wodurch die Sicherheit gegenüber der Anschlussweiterleitung erhöht wird.

HINWEIS Für Server im LAN ist die Anschlussauslösung nicht geeignet, da die eingehenden Anschlüsse erst geöffnet werden, wenn das LAN-Gerät eine ausgehende Verbindung hergestellt hat.

Manche Anwendungen funktionieren beim Herstellen einer Verbindung durch externe Geräte nur dann ordnungsgemäß, wenn sie Daten an einem bestimmten Anschluss oder Portbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur am erforderlichen Anschluss oder Portbereich senden. Das Gateway verfügt über eine Liste gängiger Anwendungen und Spiele sowie der ausgehenden und eingehenden Anschlüsse, die jeweils geöffnet werden müssen. Sie können auch eine Anschlussauslösungsregel angeben, indem Sie den Verkehrstyp (TCP oder UDP) und den Bereich der eingehenden und ausgehenden Anschlüsse definieren, die geöffnet werden sollen, wenn die Regel aktiviert ist.

So fügen Sie eine Anschlussauslösungsregel hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Ausgelöste Portbereiche** aus.

SCHRITT 2 Geben Sie in das Feld **Anwendung** den Namen der Anwendung ein, für die Sie die Anschlussweiterleitung konfigurieren möchten.

SCHRITT 3 Geben Sie in die Felder unter **Ausgelöster Bereich** die Anschlussnummer bzw. den Anschlussnummernbereich ein, die bzw. der diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird. Wenn die ausgehende Verbindung nur einen Anschluss verwendet, geben Sie in beide Felder die gleiche Anschlussnummer ein.

SCHRITT 4 Geben Sie in die Felder unter **Weitergeleiteter Bereich** die Anschlussnummer bzw. den Anschlussnummernbereich ein, die bzw. der vom Remotesystem verwendet wird, um auf die empfangene Anforderung zu antworten. Wenn die eingehende Verbindung nur einen Anschluss verwendet, geben Sie in beiden Feldern die gleiche Anschlussnummer an.

SCHRITT 5 Wählen Sie im Menü „Schnittstelle“ **Beides (Ethernet & 3G)**, **Ethernet** oder **3G** aus.

SCHRITT 6 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 7 Klicken Sie auf **Speichern**.

6

Konfigurieren von VPN

In diesem Kapitel wird beschrieben, wie Sie das VPN und die Sicherheit für das Gerät konfigurieren.

VPN-Tunneltypen

Ein VPN stellt einen sicheren Kommunikationskanal (Tunnel) zwischen zwei Gateway-Routern oder einem Remote-Mitarbeiter und einem Gateway-Router bereit. Sie können abhängig von den Geschäftsanforderungen verschiedene Arten von VPN-Tunneln erstellen. Nachstehend werden verschiedene Szenarien beschrieben. Lesen Sie diese Beschreibungen, um sich mit den Optionen und den erforderlichen Schritten zum Einrichten eines VPNs vertraut zu machen.

Remotezugriff über PPTP

In diesem Szenario stellt ein Remotebenutzer mit einem Computer mit einem Microsoft-Betriebssystem eine Verbindung mit einem PPTP-Server an Ihrem Standort her, um auf Netzwerkressourcen zuzugreifen. Verwenden Sie diese Option, um die VPN-Einrichtung zu vereinfachen. Sie brauchen keine VPN-Richtlinien konfigurieren, denn Remotebenutzer können über den PPTP-Client von einem Computer mit einem Microsoft-Betriebssystem aus eine Verbindung herstellen. Es ist nicht notwendig, einen VPN-Client zu installieren. Beachten Sie jedoch, dass in diesem Protokoll Sicherheitsschwachstellen gefunden wurden.

Remotezugriff mit Cisco QuickVPN

Verteilen Sie zur Beschleunigung der Einrichtung mit grundlegenden VPN-Sicherheitseinstellungen die Cisco QuickVPN-Software an die Benutzer, die dann sicher auf die Netzwerkressourcen zugreifen können. Verwenden Sie diese Option, wenn Sie die VPN-Einrichtung vereinfachen möchten. Sie brauchen keine VPN-Richtlinien konfigurieren, denn Remotebenutzer können mit dem Cisco QuickVPN-Client und einer Internetverbindung eine sichere Verbindung herstellen.

Site-to-Site-VPN

Das Gerät unterstützt standortübergreifendes VPN für einen einzigen Gateway-to-Gateway-VPN-Tunnel. Sie können beispielsweise das Gerät in einer Filiale so konfigurieren, dass eine Verbindung zum Router am Hauptstandort hergestellt wird und ein sicherer Zugriff auf das Unternehmensnetzwerk möglich ist. Site-to-Site-VPN wird auf der Seite **VPN** > **Grundlegende VPN-Einrichtung** konfiguriert.

VPN-Clients

Zum Einrichten eines VPN-Tunnels zwischen dem Router und dem Remoteendpunkt wird VPN-Clientsoftware benötigt. Ihr Gerät unterstützt Cisco QuickVPN- und PPTP-VPN-Clients.

Konfigurieren von PPTP

PPTP (Point to Point Tunneling Protocol) ist ein Netzwerkprotokoll, das die sichere Übertragung von Daten von einem Remoteclient an ein Unternehmensnetzwerk ermöglicht, indem eine sichere VPN-Verbindung über öffentliche Netzwerke wie beispielsweise das Internet erstellt wird.

HINWEIS Wenn Sie das VPN in des Geräts aktivieren, wird das LAN-Subnetz im Gerät automatisch geändert, um IP-Adressenkonflikte zwischen dem Remotenetzwerk und dem lokalen Netzwerk zu vermeiden.

So konfigurieren Sie den PPTP-VPN-Service:

SCHRITT 1 Wählen Sie **VPN** > **VPN-Clients** aus.

SCHRITT 2 Geben Sie folgende Informationen ein:

PPTP-Server	Aktivieren Sie dieses Kontrollkästchen, um den PPTP-Server zu aktivieren.
IP-Adresse für PPTP-Server	Geben Sie die IP-Adresse des PPTP-Servers ein.
IP-Adresse für PPTP-Clients	Geben Sie den IP-Adressbereich für PPTP-Clients ein.
MPPE-Verschlüsselung	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die MPPE-Verschlüsselung zu aktivieren. MPPE (Microsoft Point-to-Point Encryption) wird verwendet, wenn Benutzer einen PPTP-VPN-Client für Verbindungen mit dem Gerät einrichten und verwenden.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren eines QuickVPN

SCHRITT 1 Fügen Sie die QuickVPN-Benutzer auf der Seite **VPN > VPN-Clients** hinzu. Weitere Informationen hierzu finden Sie unter **Importieren von VPN-Clienteinstellungen** und **Erstellen und Verwalten von QuickVPN-Benutzern**.

SCHRITT 2 Weisen Sie die Benutzer an, die kostenlose Cisco QuickVPN-Software von Cisco.com herunterzuladen und auf ihren Computern zu installieren. Weitere Informationen hierzu finden Sie unter **Verwenden der Cisco QuickVPN-Software**.

SCHRITT 3 Zum Aktivieren des Zugriffs mit Cisco QuickVPN auf Ihrem Gerät müssen Sie das Remote-Management aktivieren, um Anschluss 443 für SSL zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

Konfigurieren von NetBIOS über VPN

So aktivieren Sie NetBIOS über VPN:

SCHRITT 1 Aktivieren Sie im Feld **NetBIOS über VPN** das Kontrollkästchen, um die Übertragung von NetBIOS-Broadcasts durch den VPN-Tunnel zuzulassen. Für Clientrichtlinien ist die NetBIOS-Funktion standardmäßig verfügbar.

SCHRITT 2 Klicken Sie auf **Speichern**.

Erstellen und Verwalten von PPTP-Benutzern

So erstellen Sie PPTP-Benutzer:

SCHRITT 1 Klicken Sie in der **Tabelle der VPN-Clienteinstellungen** auf **Hinzufügen**.

SCHRITT 2 Geben Sie folgende Informationen ein:

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um den Benutzer zu aktivieren.
Benutzername	Geben Sie den Benutzernamen des PPTP-Benutzers ein (4 bis 32 Zeichen).
Kennwort	Geben Sie das Kennwort ein (4 bis 32 Zeichen).
Protokoll	Wählen Sie im Dropdown-Menü die Option **PPTP-Benutzer** aus.

SCHRITT 3 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines PPTP-Benutzers aktivieren Sie das entsprechende Kontrollkästchen und klicken auf „Bearbeiten“. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Zum Löschen eines PPTP-Benutzers aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie auf **Löschen**.

Erstellen und Verwalten von QuickVPN-Benutzern

So erstellen Sie QuickVPN-Benutzer:

SCHRITT 1 Klicken Sie in der **Tabelle der VPN-Clienteinstellungen** auf **Hinzufügen**.

SCHRITT 2 Geben Sie folgende Informationen ein:

SCHRITT 3 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines QuickVPN-Benutzers aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie auf **Bearbeiten**. Nehmen Sie Änderungen vor, und klicken Sie auf **Speichern**.

Zum Löschen eines QuickVPN-Benutzers aktivieren Sie das entsprechende Kontrollkästchen, klicken Sie auf **Löschen** und anschließend auf **Speichern**.

Weitere Informationen zu QuickVPN finden Sie unter **Anhang A, ?$paratext>?**.

Importieren von VPN-Clienteinstellungen

Sie können VPN-Clienteinstellungsdateien importieren, die Benutzernamen und Kennwörter von Clients in einer CSV-Textdatei (Comma Separated Values, durch Kommas getrennte Werte) enthalten.

Zum Erstellen einer CSV-Datei mit den VPN-Clienteinstellungen können Sie ein Programm wie beispielsweise Microsoft Excel verwenden. Die Datei sollte eine Zeile für die Überschrift und eine oder mehrere Zeilen für die VPN-Clients enthalten.

Im Folgenden finden Sie z. B. die Einstellungen für zwei zu importierende Benutzer:

PROTOCOL	USERNAME	PASSWORD
PPTP	pptp-user-1	12345678
QuickVPN	qv-user-1	12345678

VORSICHT Beim Importieren von VPN-Clienteinstellungen werden vorhandene Einstellungen gelöscht.

So importieren Sie VPN-Clienteinstellungen:

SCHRITT 1 Klicken Sie auf **Durchsuchen**, um die Datei zu suchen.

SCHRITT 2 Klicken Sie auf **Importieren**, um die Datei zu laden.

SCHRITT 3 Wenn Sie gefragt werden, ob die vorhandenen VPN-Benutzereinstellungen gelöscht und die Einstellungen aus der CSV-Datei importiert werden sollen, klicken Sie auf **Ja**.

Konfigurieren grundlegender Einstellungen für ein standortübergreifendes VPN-IPsec

Das Gerät unterstützt Site-to-Site-VPN für einen einzigen Gateway-to-Gateway-VPN-Tunnel. In dieser Konfiguration stellt das Geräte eine sichere Verbindung zu einem anderen VPN-fähigen Router her. Sie können beispielsweise das Gerät in einer Filiale so konfigurieren, dass eine Verbindung zum Router am Hauptstandort hergestellt wird und ein sicherer Zugriff auf das Unternehmensnetzwerk möglich ist.

So konfigurieren Sie die grundlegenden VPN-Einstellungen für eine Site-to-Site-Verbindung:

SCHRITT 1 Klicken Sie auf **VPN** > **Grundlegende VPN-Einrichtung**.

SCHRITT 2 Geben Sie im Feld **Verbindungsname** einen Namen für den VPN-Tunnel ein.

SCHRITT 3 Geben Sie im Feld **Vorinstallierter Schlüssel** den vorinstallierten Schlüssel bzw. das Kennwort ein, den bzw. das die beiden Router austauschen sollen. Der Schlüssel muss zwischen 8 und 49 Zeichen lang sein.

SCHRITT 4 Geben Sie in den Feldern unter **Endpunktinformationen** die folgenden Informationen ein:

- **Remoteendpunkt**: Wählen Sie aus, auf welche Weise der Remoteendpunkt oder der Router, mit dem das Gerät verbunden wird, identifiziert werden soll. Beispielsweise anhand einer IP-Adresse wie 192.168.1.1 oder anhand eines vollständigen Domänennamens wie „cisco.com“.
- **IP-Adresse des Remote-WAN**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des Remoteendpunkts ein.

- **Redundancy Endpoint** (Redundanzendpunkt): Zur Aktivierung der Umschaltung des Geräts auf einen alternativen Gateway beim Ausfall der primäre VPN-Verbindung aktivieren Sie das Kontrollkästchen **Aktivieren**. Geben Sie die WAN-IP-Adresse oder die FQDN für den Redundanzendpunkt ein.
- **IP-Adresse des lokalen WAN**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des lokalen Endpunkts (Gerät) ein.

SCHRITT 5 Geben Sie in den Feldern unter **Remotezugriff über sichere Verbindung** die folgenden Informationen ein:

- **Remote-LAN-IP-Adresse**: Geben Sie die Adresse des Remoteendpunkts im privaten Netzwerk (LAN) ein. Dies ist die IP-Adresse aus dem internen Netzwerk am Remotestandort.
- **Remote-LAN-Subnetzmaske**: Geben Sie die Subnetzmaske des Remoteendpunkts im privaten Netzwerk (LAN) ein.
- **Lokale LAN-IP-Adresse**: Geben Sie die Adresse des lokalen Netzwerks im privaten Netzwerk (LAN) ein. Dies ist die IP-Adresse aus dem internen Netzwerk in der Gerät.
- **Lokale LAN-Subnetzmaske**: Geben Sie die Subnetzmaske des privaten Netzwerks im privaten Netzwerk (LAN) ein (Gerät).

Hinweis: Die Remote-WAN- und die Remote-LAN-IP-Adresse dürfen nicht zum selben Subnetz gehören. Wenn beispielsweise die Remote-LAN-IP-Adresse 192.168.1.100 und die lokale LAN-IP-Adresse 192.168.1.115 lauten würden, würden beim Routing von Datenverkehr über das VPN Konflikte entstehen. Das dritte Oktett muss unterschiedlich sein, damit die IP-Adressen zu verschiedenen Subnetzen gehören. Eine Kombination aus der Remote-LAN-IP-Adresse 192.168.1.100 und der lokalen LAN-IP-Adresse 192.168.2.100 wäre beispielsweise zulässig.

SCHRITT 6 Klicken Sie auf **Speichern**.

Anzeigen von Standardwerten

Die in den grundlegenden VPN-Einstellungen verwendeten Standardwerte entsprechen den vom VPN Consortium (VPNC) empfohlenen Standardwerten. Es wird davon ausgegangen, dass Sie einen vorher vereinbarten Schlüssel bzw. ein Kennwort verwenden, der bzw. das sowohl dem Gerät als auch dem Router am anderen Ende (beispielsweise einem Cisco RV220W) bekannt ist. So zeigen Sie die Standardwerte an:

SCHRITT 1 Klicken Sie auf **VPN** > **Grundlegende VPN-Einrichtung**.

SCHRITT 2 Klicken Sie auf **Standardeinstellungen anzeigen**, um die Standardwerte anzuzeigen.

Weitere Informationen zu diesen Werten finden Sie unter **Konfigurieren erweiterter VPN-Parameter**.

Konfigurieren erweiterter VPN-Parameter

Auf der Seite Erweiterte VPN-Einrichtung können Sie erweiterte VPN-Parameter konfigurieren, beispielsweise IKE-Richtlinien und andere VPN-Richtlinien. Mit diesen Richtlinien steuern Sie, wie das Gerät VPN-Verbindungen mit anderen Endpunkten initiiert und empfängt.

Verwalten von IKE-Richtlinien

Mit dem IKE-Protokoll (Internet Key Exchange) werden dynamisch Schlüssel zwischen zwei IPsec-Hosts ausgetauscht. Sie können IKE-Richtlinien erstellen, um die Sicherheitsparameter zu definieren (beispielsweise die Authentifizierung des Peers und die bei diesem Vorgang verwendeten Verschlüsselungsalgorithmen). Achten Sie darauf, für die VPN-Richtlinie kompatible Verschlüsselungs-, Authentifizierungs- und Schlüsselgruppenparameter zu verwenden.

SCHRITT 1 Klicken Sie auf **VPN** > **IPsec** > **Erweiterte VPN-Einrichtung**.

SCHRITT 2 Wenn Sie in der **VPN-Richtlinientabelle** das Kontrollkästchen in der Zeile für die VPN-Verbindung aktivieren, stehen folgende Optionen zur Verfügung:

- **Hinzufügen** oder **Bearbeiten**: Bearbeiten der Eigenschaften der IKE-Richtlinie. Weitere Informationen hierzu finden Sie unter **Hinzufügen oder Bearbeiten von IKE-Richtlinien**.
- **Aktivieren**: Aktivieren der Richtlinie.
- **Deaktivieren**: Deaktivieren der Richtlinie.
- **Löschen**: Löschen der Richtlinie.

HINWEIS Sie können eine IKE-Richtlinie nicht löschen, wenn diese in einer VPN-Richtlinie verwendet wird. Um die IKE-Richtlinie löschen zu können, müssen Sie zunächst die VPN-Richtlinie in der **VPN-Richtlinientabelle** deaktivieren und löschen.

- **Hinzufügen**: Hinzufügen einer IKE-Richtlinie. Weitere Informationen hierzu finden Sie unter **Hinzufügen oder Bearbeiten von IKE-Richtlinien**.

HINWEIS Wenn bereits eine VPN-Verbindung konfiguriert ist, müssen Sie diese zunächst löschen, um eine neue hinzufügen zu können.

SCHRITT 3 Klicken Sie auf **Speichern**.

Hinzufügen oder Bearbeiten von IKE-Richtlinien

SCHRITT 1 Konfigurieren Sie beim Hinzufügen oder Bearbeiten von IKE-Richtlinien folgende Einstellungen:

- **Richtlinienname**: Geben Sie zu Identifizierungs- und Verwaltungszwecken einen eindeutigen Namen für die Richtlinie ein.
- **Austauschmodus**: Wählen Sie eine der folgenden Optionen aus:
  - **Haupt**: Aushandlung des Tunnels mit höherer Sicherheit, die Geschwindigkeit ist jedoch geringer.
  - **Aggressiv**: Herstellung einer schnelleren Verbindung, die Sicherheit ist jedoch geringer.
- **Local Identifier** (Lokale Kennung): Lokale IKE-Kennung.
- **Remote Identifier** (Remote-Kennung): Remote-IKE-Kennung.
- **Redundancy Identifier** (Redundanzkennung): Eindeutige Kennung des alternativen Backupendpunkts, der beim Ausfall der originalen VPN-Verbindung zur Wiederherstellung der Verbindung verwendet wird.

SCHRITT 2 Im Abschnitt **IKE-SA-Parameter** definieren die SA-Parameter (Security Association, Sicherheitsvereinbarung) die Stärke und den Modus für die Sicherheitsvereinbarung. Sie können folgende Einstellungen konfigurieren:

- **Verschlüsselungsalgorithmus**: Wählen Sie den für die Aushandlung der Sicherheitsvereinbarung verwendeten Algorithmus aus:
  - **DES**
  - **3DES**
  - **AES-128**
  - **AES-192**
  - **AES-256**
- **Authentifizierungsalgorithmus**: Geben Sie den Authentifizierungsalgorithmus für den VPN-Header an:
  - **MD5**
  - **SHA-1**
  - **SHA2-256**

  Der Authentifizierungsalgorithmus muss auf beiden Seiten des VPN-Tunnels gleich konfiguriert sein (beispielsweise für den Gerät und den Router, mit dem es die Verbindung herstellt).
- **Vorinstallierter Schlüssel**: Geben Sie den Schlüssel in das entsprechende Feld ein. Beachten Sie, dass doppelte Anführungszeichen (") im vorinstallierten Schlüssel nicht unterstützt werden.
- **Diffie-Hellman-Gruppe (DH)**: Geben Sie den Algorithmus „Diffie-Hellman-Gruppe (DH)“ an, der beim Austausch von Schlüsseln verwendet wird. Die DH-Gruppe legt die Stärke des Algorithmus in Bit fest. Stellen Sie sicher, dass die DH-Gruppe auf beiden Seiten der IKE-Richtlinie gleich konfiguriert ist.
- **SA-Gültigkeitsdauer**: Geben Sie das Intervall (in Sekunden) ein, nach dem die Sicherheitsvereinbarung ungültig wird.

- **Dead-Peer-Detection**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um die Funktion zu aktivieren, oder deaktivieren Sie das Kontrollkästchen, um die Funktion zu deaktivieren. Mit der Dead-Peer-Detection (DPD) wird erkannt, ob der Peer aktiv ist. Wenn erkannt wird, dass der Peer nicht aktiv ist, löscht der Router die IPsec- und IKE-Sicherheitsvereinbarung. Wenn Sie diese Funktion aktivieren, müssen Sie auch diese Einstellungen eingeben:
  - **DPD-Verzögerung**: Geben Sie das Intervall (in Sekunden) zwischen zwei aufeinanderfolgenden DPD R-U-THERE-Nachrichten ein. DPD R-U-THERE-Nachrichten werden nur gesendet, wenn sich der IPsec-Verkehr im Leerlauf befindet.
  - **DPD-Zeitüberschreitung**: Geben Sie ein, wie lange das Gerät höchstens auf eine Antwort auf die DPD-Nachricht warten soll, bevor der Peer für inaktiv erklärt wird.

SCHRITT 3 Aktivieren Sie das Kontrollkästchen **XAUTH Type Enable** (XAUTH-Typ aktivieren), um die erweiterte Authentifizierung für Ihre VPN-IPsec-Richtlinie zu konfigurieren. Geben Sie den Benutzernamen und das Kennwort für die Authentifizierung ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Verwalten von VPN-Richtlinien

So verwalten Sie VPN-Richtlinien:

SCHRITT 1 Klicken Sie auf **VPN** > **IPsec** > **Erweiterte VPN-Einrichtung**.

SCHRITT 2 Wenn Sie in der **VPN-Richtlinientabelle** das Kontrollkästchen in der Zeile für die VPN-Verbindung aktivieren, stehen folgende Optionen zur Verfügung:

- **Hinzufügen** oder **Bearbeiten**: Bearbeiten der Eigenschaften der VPN-Richtlinie. Weitere Informationen hierzu finden Sie unter **Hinzufügen oder Bearbeiten von VPN-Richtlinien**.
- **Aktivieren**: Aktivieren der Richtlinie.
- **Deaktivieren**: Deaktivieren der Richtlinie.
- **Löschen**: Löschen der Richtlinie.
- **Hinzufügen**: Hinzufügen einer VPN-Richtlinie. Weitere Informationen hierzu finden Sie unter **Hinzufügen oder Bearbeiten von VPN-Richtlinien**.

HINWEIS Wenn bereits eine VPN-Verbindung konfiguriert ist, müssen Sie diese zunächst löschen, um eine neue hinzufügen zu können.

SCHRITT 3 Klicken Sie auf **Speichern**.

Hinzufügen oder Bearbeiten von VPN-Richtlinien

Um eine automatische VPN-Richtlinie zu erstellen, müssen Sie zuerst eine IKE-Richtlinie erstellen und dann die entsprechende automatische Richtlinie für diese IKE-Richtlinie hinzufügen.

Beim Hinzufügen oder Bearbeiten von VPN-Richtlinien können Sie folgende Einstellungen konfigurieren:

- **Richtlinienname**: Geben Sie einen eindeutigen Namen ein, um die Richtlinie zu identifizieren.
- **Richtlinientyp**: Wählen Sie eine der folgenden Optionen aus:
  - **Automatische Richtlinie**: Einige Parameter für den VPN-Tunnel werden automatisch generiert. Hierzu müssen die Parameter zwischen den beiden VPN-Endpunkten unter Verwendung des IKE-Protokolls (Internet Key Exchange) ausgehandelt werden.
  - **Manuelle Richtlinie**: Alle Einstellungen (einschließlich der Schlüssel) für den VPN-Tunnel werden für jeden Endpunkt manuell eingegeben. Es wird weder ein außenstehender Server noch eine außenstehende Organisation benötigt.
- **Remoteendpunkt**: Wählen Sie den Typ der Kennung aus, die Sie für das Gateway am Remoteendpunkt bereitstellen möchten: **IP-Adresse** oder **FQDN** (voll qualifizierter Domänenname). Geben Sie die Kennung in das entsprechende Feld ein.
- **Redundancy Endpoint** (Redundanzendpunkt): Zur Aktivierung der Umschaltung des Geräts auf einen alternativen Gateway beim Ausfall der primären VPN-Verbindung aktivieren Sie das Kontrollkästchen **Aktivieren**. Geben Sie die WAN-IP-Adresse oder die FQDN für den Redundanzendpunkt ein.

  Zur automatischen Wiederherstellung des primären VPN bei der Wiederherstellung der Verbindung aktivieren Sie das Kontrollkästchen **Rollback aktivieren**.

Geben Sie unter **Lokale Datenverkehrauswahl** und **Remotedatenverkehrauswahl** diese Einstellungen ein:

- **Lokale IP/Remote-IP**: Wählen Sie den Typ der Kennung aus, die Sie für den Endpunkt bereitstellen möchten:

- **Einzeln**: Begrenzt die Richtlinie auf einen Host. Geben Sie in das Feld „Start-IP-Adresse“ die IP-Adresse des Hosts ein, der Mitglied des VPNs sein soll. Geben Sie in das Feld **Startadresse** die IP-Adresse ein.
- **Subnetz**: Lässt Verbindungen eines gesamten Subnetzes mit dem VPN zu. Geben Sie in das Feld „Start-IP-Adresse“ die Netzwerkadresse und in das Feld „Subnetzmaske“ die Subnetzmaske ein. Geben Sie in das Feld **Startadresse** die IP-Adresse des Subnetzes ein. Geben Sie in das Feld **Subnetzmaske** die Subnetzmaske ein, beispielsweise 255.255.255.0. Im Feld wird automatisch eine auf der IP-Adresse basierende Standardsubnetzadresse angezeigt.

  WICHTIG: Vergewissern Sie sich, dass Sie für die Remotedatenverkehrauswahl oder die lokale Datenverkehrauswahl keine überlappenden Subnetze verwenden. Für die Verwendung dieser Subnetze müssten Sie statische Routen im Router und die zu verwendenden Hosts hinzufügen. Vermeiden Sie beispielsweise diese Kombination:

  Lokale Datenverkehrauswahl: 192.168.1.0/24

  Remotedatenverkehrauswahl: 192.168.0.0/16

Geben Sie beim Richtlinientyp **Manuell** die Einstellungen im Abschnitt **Parameter für manuelle Richtlinien** ein:

- **SPI eingehend, SPI ausgehend**: Geben Sie einen hexadezimalen Wert aus 3 bis 8 Zeichen ein, beispielsweise 0x1234.
- **Verschlüsselungsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Verschlüsseln der Daten verwendet wird:
  - DES
  - 3DES
  - AES-128
  - AES-192
  - AES-256
- **Schlüsseleingabe**: Geben Sie den Verschlüsselungsschlüssel der Eingangsrichtlinie ein. Die Länge des Schlüssels hängt vom ausgewählten Verschlüsselungsalgorithmus ab:
  - DES: 8 Zeichen
  - 3DES: 24 Zeichen

- AES-128: 16 Zeichen
- AES-192: 24 Zeichen
- AES-256: 32 Zeichen

- **Schlüsselausgabe**: Geben Sie den Verschlüsselungsschlüssel der Ausgangsrichtlinie ein. Die Länge des Schlüssels hängt wie oben erläutert vom ausgewählten Verschlüsselungsalgorithmus ab.
- **Integritätsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Überprüfen der Integrität der Daten verwendet wird:
  - MD5
  - SHA-1
  - SHA2-256
- **Schlüsseleingabe**: Geben Sie den Integritätsschlüssel (für ESP mit Integritätsmodus) für die Eingangsrichtlinie ein. Die Länge des Schlüssels hängt vom ausgewählten Algorithmus ab:
  - MD5: 16 Zeichen
  - SHA-1: 20 Zeichen
  - SHA2-256: 32 Zeichen
- **Schlüsselausgabe**: Geben Sie den Integritätsschlüssel (für ESP mit Integritätsmodus) für die Ausgangsrichtlinie ein. Die Länge des Schlüssels hängt wie oben gezeigt vom ausgewählten Algorithmus ab.

Geben Sie beim Richtlinientyp **Automatisch** die Einstellungen im Abschnitt **Parameter für automatische Richtlinien** ein:

- **SA-Gültigkeitsdauer**: Geben Sie die Dauer der Sicherheitsvereinbarung (in Sekunden) ein. Wenn die angegebene Zahl von Sekunden verstrichen ist, wird die Sicherheitsvereinbarung erneut ausgehandelt. Der Standardwert beträgt 3.600 Sekunden. Der Mindestwert beträgt 300 Sekunden.
- **Verschlüsselungsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Verschlüsseln der Daten verwendet wird.
- **Integritätsalgorithmus**: Wählen Sie den Algorithmus aus, der zum Überprüfen der Integrität der Daten verwendet wird.

- **PFS-Schlüsselgruppe**: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um mithilfe von PFS (Perfect Forward Secrecy) die Sicherheit zu verbessern. Dieses Protokoll ist zwar langsamer, kann jedoch Abhören verhindern, da es sicherstellt, dass für alle Phase-2-Aushandlungen ein Diffie-Hellman-Schlüsselaustausch stattfindet.
- **IKE-Richtlinie auswählen**: Wählen Sie die IKE-Richtlinie aus, die die Merkmale von Phase 1 der Aushandlung definieren soll. Klicken Sie auf **Anzeigen**, um die im Gerät konfigurierte vorhandene IKE-Richtlinie anzuzeigen oder zu bearbeiten.

Konfigurieren der Zertifikatverwaltung

Das Gerät verwendet digitale Zertifikate für die VPN-IPsec-Authentifizierung und SSL-Überprüfung (für HTTPS). Sie können mithilfe der im Gerät verfügbaren Funktion eigene Zertifikate generieren und signieren.

Generieren eines neuen Zertifikats

Sie können ein neues Zertifikat generieren, um das vorhandene Zertifikat im Gerät zu ersetzen.

So generieren Sie ein Zertifikat:

SCHRITT 1 Wählen Sie **VPN** > **Zertifikatverwaltung** aus.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Neues Zertifikat generieren**.

SCHRITT 3 Klicken Sie auf **Zertifikat generieren**.

Importieren von Zertifikaten

Über die Schaltfläche **Für Administrator exportieren** können Sie in einer Datei gespeicherte Zertifikate importieren.

So importieren Sie ein Zertifikat:

SCHRITT 1 Wählen Sie **VPN** > **Zertifikatverwaltung** aus.

SCHRITT 2 Klicken Sie auf die Schaltfläche **Zertifikat aus Datei importieren**.

SCHRITT 3 Klicken Sie auf **Durchsuchen** und suchen Sie die Zertifikatdatei.

SCHRITT 4 Klicken Sie auf **Zertifikat installieren**.

Exportieren von Zertifikaten für den Administrator

Sie können das Zertifikat für den Administrator in einen Ordner auf Ihrem Computer oder an einen externen Speicherort auf einem USB-Laufwerk exportieren. Das Zertifikat für den Administrator enthält den privaten Schlüssel und sollte als Backup an einem sicheren Ort gespeichert werden. Wenn die Konfiguration des Geräts auf die Werkseinstellungen zurückgesetzt wird, kann dieses Zertifikat importiert und im Router wiederhergestellt werden.

So exportieren Sie ein Zertifikat für den Administrator:

SCHRITT 1 Wählen Sie **VPN** > **Zertifikatverwaltung** aus.

SCHRITT 2 Zum Exportieren des Zertifikats auf Ihren Computer klicken Sie auf **Für Administrator exportieren**. Der Gerätemanager speichert die Datei „admin.pem“ unter „C:\Dokumente und Einstellungen\Benutzername\Eigene Dokumente\Downloads“.

Zum Exportieren des Zertifikats auf ein externes USB-Laufwerk klicken Sie auf **Für Administrator auf USB exportieren**.

Exportieren von Zertifikaten für den Client

Zertifikate für Clients können Sie auf Ihren Computer oder an einen externen Speicherort auf einem USB-Laufwerk exportieren. Das Zertifikat für den Client ermöglicht QuickVPN-Benutzern das Herstellen sicherer Verbindungen mit der Cisco RV215W. QuickVPN-Benutzer müssen das Zertifikat im Installationsverzeichnis des QuickVPN-Clients speichern.

So exportieren Sie ein Zertifikat für den Client:

SCHRITT 1 Wählen Sie **VPN** > **Zertifikatverwaltung** aus.

SCHRITT 2 Zum Exportieren des Zertifikats auf Ihren Computer klicken Sie auf **Für Client exportieren**. Auf einem PC speichert der Gerätemanager die Datei „client.pem“ unter „C:\Dokumente und Einstellungen\Benutzername\Eigene Dokumente\Downloads“.

Zum Exportieren des Zertifikats auf ein externes USB-Laufwerk klicken Sie auf **Für Client auf USB exportieren**.

Konfigurieren von VPN-Passthrough

Mithilfe von VPN-Passthrough kann VPN-Verkehr von VPN-Clients das Gerät passieren.

So konfigurieren Sie VPN-Passthrough:

SCHRITT 1 Wählen Sie **VPN** > **VPN-Passthrough** aus.

SCHRITT 2 Wählen Sie den Verkehrstyp aus, der die Firewall passieren können soll:

IPsec	Aktivieren Sie die Option **Aktivieren**, damit IPsec-Tunnel das Gerät passieren können.
PPTP	Aktivieren Sie die Option **Aktivieren**, damit PPTP-Tunnel das Gerät passieren können.
L2TP	Aktivieren Sie die Option **Aktivieren**, damit L2TP-Tunnel (Layer 2 Tunneling Protocol) das Gerät passieren können.

SCHRITT 3 Klicken Sie auf **Speichern**.

7

Konfigurieren der Servicequalität (Quality of Service, QoS)

Für die Cisco RV215W können Sie die folgenden QoS-Funktionen (Quality of Service) konfigurieren:

- **Konfigurieren des Bandbreitenmanagements auf Seite 127**
- **Konfigurieren der anschlussbasierten QoS-Einstellungen auf Seite 130**
- **Konfigurieren der CoS-Einstellungen auf Seite 132**
- **Konfigurieren der DSCP-Einstellungen auf Seite 132**

Die Servicequalität (Quality of service, QoS) weist den verschiedenen Anwendungen, Benutzern oder Datenflüssen Prioritäten zu oder garantiert einem Datenfluss eine bestimmte Leistungsstufe. Diese Zusagen sind wichtig bei unzureichender Netzwerkkapazität. Dies gilt besonders für das Streaming von Multimedia-Anwendungen in Echtzeit wie VoIP, Online-Spielen und IP-TV, da diese Anwendungen häufig feste Bitraten benötigen und anfällig für Verzögerungen sind. Außerdem sind die Zusagen in Netzwerken wichtig, in denen die Kapazität eine eingeschränkte Ressource ist, wie z. B. bei der mobilen Datenübertragung.

Konfigurieren des Bandbreitenmanagements

Mit dem Bandbreitenmanagement des Geräts können Sie die Bandbreite des Verkehrs verwalten, der vom sicheren Netzwerk (LAN) zum nicht sicheren Netzwerk (WAN) fließt.

Konfigurieren der Bandbreite

Sie können die Bandbreite begrenzen, um die Datenübertragungsrate des Geräts zu reduzieren. Außerdem können Sie mithilfe eines Bandbreitenprofils den ausgehenden Verkehr begrenzen und so verhindern, dass die LAN-Benutzer die gesamte Bandbreite der Internetverbindung verwenden.

So legen Sie die Upstream- und Downstream-Bandbreite fest:

SCHRITT 1 Wählen Sie **QoS** > **Bandbreitenmanagement** aus.

SCHRITT 2 Aktivieren Sie im Feld **Bandbreitenmanagement** das Kontrollkästchen **Aktivieren**. Im Abschnitt **Bandbreite** wird die vom ISP bereitgestellte maximale Bandbreite angezeigt.

SCHRITT 3 Geben Sie in die **Bandbreiten** die folgenden Informationen für die WAN-Schnittstelle ein:

Upstream	Die Bandbreite (KBit/s), die zum Senden von Daten an das Internet verwendet wird.
Downstream	Die Bandbreite (KBit/s), die zum Empfangen von Daten aus dem Internet verwendet wird.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der Bandbreitenpriorität

Unter **Bandbreitenprioritäten** können Sie die Verwendung der Bandbreite verwalten, indem Sie Services Prioritäten zuweisen.

So konfigurieren Sie die Bandbreitenpriorität:

SCHRITT 1 Wählen Sie **QoS** > **Bandbreitenmanagement** aus.

SCHRITT 2 Aktivieren Sie im Feld **Bandbreitenmanagement** das Kontrollkästchen **Aktivieren**. Im Abschnitt **Bandbreite** wird die vom ISP bereitgestellte maximale Bandbreite angezeigt.

SCHRITT 3 Klicken Sie unter **Bandbreitenprioritäten** auf **Hinzufügen**.

SCHRITT 4 Geben Sie folgende Informationen ein:

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Bandbreitenmanagement für diesen Service zu aktivieren.
Service	Wählen Sie den Service aus, der priorisiert werden soll.
Richtung	Wählen Sie die Richtung des Verkehrs aus, den Sie priorisieren möchten (**Downstream** oder **Upstream**).
Priorität	Wählen Sie die Priorität des Services aus (**Niedrig**, **Normal**, **Mittel** oder **Hoch**).

SCHRITT 5 Klicken Sie auf **Speichern**.

Zum Bearbeiten der Einstellungen eines Eintrags in der Tabelle aktivieren Sie das entsprechende Kontrollkästchen, und klicken Sie auf **Bearbeiten**. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Zum Löschen eines Eintrags aus der Tabelle aktivieren Sie das entsprechende Kontrollkästchen, klicken auf **Löschen** und anschließend auf **Speichern**.

Zum Hinzufügen eines neuen Serviceziels klicken Sie auf die Schaltfläche **Serviceverwaltung**. Sie können einen neuen Service definieren, der für alle Firewalldefinitionen und QoS-Definitionen verwendet werden soll. Weitere Informationen hierzu finden Sie unter **Konfigurieren der Serviceverwaltung**.

Konfigurieren der anschlussbasierten QoS-Einstellungen

Sie können QoS-Einstellungen für jeden LAN-Anschluss der Cisco RV215W konfigurieren. Das Gerät unterstützt vier Prioritätswarteschlangen, die die Verkehrspriorisierung pro physischem Switch-Port ermöglichen.

So konfigurieren Sie QoS-Einstellungen für die LAN-Anschlüsse des Geräts:

SCHRITT 1 Wählen Sie **QoS** > **Anschlussbasierte QoS-Einstellungen** aus.

SCHRITT 2 Geben Sie für jeden Anschluss in der **Tabelle für anschlussbasierte Ethernet-QoS-Einstellungen** diese Informationen ein:

Vertrauensmodus	Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus: • **Anschluss**: Mit dieser Einstellung wird anschlussbasiertes QoS aktiviert. Anschließend können Sie die Verkehrspriorität für einen bestimmten Anschluss festlegen. Die Priorität der Verkehrswarteschlange beginnt mit der niedrigsten Priorität 1 und endet mit der höchsten Priorität 4. • **DSCP**: Differentiated Services Code Point (DSCP). Wenn Sie diese Funktion aktivieren, wird der Netzwerkverkehr durch das LAN basierend auf den DSCP-Warteschlangenzuordnungen auf der Seite **DSCP-Einstellungen** priorisiert. • **CoS**: Class of Service (CoS).
Standardmäßige Datenverkehrweiterleitungswarteschlange für nicht vertrauenswürdige Geräte	Wählen Sie eine Prioritätsstufe für ausgehenden Verkehr aus (1 bis 4).

SCHRITT 3 Geben Sie für jeden Anschluss in der **Tabelle für anschlussbasierte 3G-QoS-Einstellungen** diese Informationen ein:

Vertrauensmodus	Wählen Sie im Dropdown-Menü eine der folgenden Optionen aus: • **Anschluss**: Mit dieser Einstellung wird anschlussbasiertes QoS aktiviert. Anschließend können Sie die Verkehrspriorität für einen bestimmten Anschluss festlegen. Die Priorität der Verkehrswarteschlange beginnt mit der niedrigsten Priorität 1 und endet mit der höchsten Priorität 4. • **DSCP**: Differentiated Services Code Point (DSCP). Wenn Sie diese Funktion aktivieren, wird der Netzwerkverkehr durch das LAN basierend auf den DSCP-Warteschlangenzuordnungen auf der Seite **DSCP-Einstellungen** priorisiert. • **CoS**: Class of Service (CoS).
Standardmäßige Datenverkehrweiterleitungswarteschlange für nicht vertrauenswürdige Geräte	Wählen Sie eine Prioritätsstufe für ausgehenden Verkehr aus (1 bis 4).

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Wiederherstellen der Standardeinstellungen für anschlussbasiertes QoS klicken Sie auf **Standard wiederherstellen** und anschließend auf **Speichern**.

Konfigurieren der CoS-Einstellungen

Verwenden Sie den Link zur Seite „Anschlussbasierte QoS-Einstellungen“, um die CoS-Prioritätseinstellungen der QoS-Warteschlange zuzuordnen.

So ordnen Sie CoS-Prioritätseinstellungen der Warteschlange für die Datenverkehrweiterleitung zu:

SCHRITT 1 Wählen Sie **QoS** > **CoS-Einstellungen** aus.

SCHRITT 2 Aktivieren Sie das Optionsfeld **Ethernet** oder **3G**.

SCHRITT 3 Wählen Sie für jede CoS-Prioritätsstufe unter **CoS-Einstellungen** einen Prioritätswert im Dropdown-Menü **Datenverkehrweiterleitungswarteschlange** aus.

Diese Werte kennzeichnen Verkehrstypen mit je nach Verkehrstyp höherer oder niedrigerer Verkehrspriorität.

SCHRITT 4 Klicken Sie auf **Speichern**.

Zum Wiederherstellen der Standardeinstellungen für anschlussbasiertes QoS klicken Sie auf **Standard wiederherstellen** und anschließend auf **Speichern**.

Konfigurieren der DSCP-Einstellungen

Auf der Seite **DSCP-Einstellungen** können Sie die Zuordnung von DSCP-Warteschlangen zu QoS-Warteschlangen konfigurieren.

So konfigurieren Sie die Zuordnung von DSCP-Warteschlangen zu QoS-Warteschlangen:

SCHRITT 1 Wählen Sie **QoS** > **DSCP-Einstellungen** aus.

SCHRITT 2 Aktivieren Sie das Optionsfeld **Ethernet** oder **3G**.

SCHRITT 3 Wählen Sie aus, ob nur RFC-Werte oder alle DSCP-Werte in der **DSCP-Einstellungstabelle** aufgelistet werden sollen, indem Sie auf die entsprechende Schaltfläche klicken.

SCHRITT 4 Wählen Sie für jeden DSCP-Wert in der **DSCP-Einstellungstabelle** im Dropdown-Menü **Warteschlange** eine Prioritätsstufe aus.

Damit wird der DSCP-Wert der ausgewählten QoS-Warteschlange zugeordnet.

SCHRITT 5 Klicken Sie auf **Speichern**.

Zum Wiederherstellen der DSCP-Standardeinstellungen klicken Sie auf **Standard wiederherstellen** und anschließend auf **Speichern**.

8

Verwalten des Routers

In diesem Kapitel werden die Verwaltungsfunktionen des Geräts beschrieben. Dazu gehören das Erstellen von Benutzern, die Netzwerkverwaltung, Systemdiagnose und -protokolle, Datum und Uhrzeit sowie weitere Einstellungen.

Festlegen der Kennwortkomplexität

Das Gerät kann bei Kennwortänderungen Mindestanforderungen für die Kennwortkomplexität erzwingen.

So konfigurieren Sie die Einstellungen für die Kennwortkomplexität:

SCHRITT 1 Wählen Sie **Administration** > **Kennwortsicherheit** aus.

SCHRITT 2 Aktivieren Sie im Feld **Einstellungen für Kennwortkomplexität** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Konfigurieren Sie die Einstellungen für die Kennwortkomplexität:

Kennwortmindestlänge	Geben Sie die Kennwortmindestlänge ein (0 bis 64 Zeichen).
Mindestanzahl an Zeichenklassen	Geben Sie eine Zahl ein, die eine der folgenden Zeichenklassen darstellt: • Großbuchstaben • Kleinbuchstaben • Ziffern • Auf einer Standardtastatur verfügbare Sonderzeichen Kennwörter müssen standardmäßig Zeichen aus mindestens drei dieser Klassen enthalten.
Das neue Kennwort darf nicht mit dem aktuellen identisch sein.	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um festzulegen, dass neue Kennwörter nicht mit dem aktuellen Kennwort identisch sein dürfen.
Kennwortfälligkeit	Aktivieren Sie das Kontrollkästchen **Aktivieren**, damit Kennwörter nach einem angegebenen Zeitraum ablaufen.
Kennwortfälligkeitszeit	Geben Sie ein, nach wie vielen Tagen das Kennwort abläuft (1-365). Der Standardwert beträgt 180 Tage.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Benutzerkonten

Das Gerät unterstützt zwei Benutzerkonten zum Verwalten und Anzeigen von Einstellungen: Einen administrativen Benutzer (Standardbenutzername und -kennwort: „cisco“) und einen Gastbenutzer (Standardbenutzername: „guest“).

Das Gastkonto verfügt nur über Lesezugriff. Sie können den Benutzernamen und das Kennwort für das Administratorkonto und für das Gastkonto festlegen und ändern.

So konfigurieren Sie die Benutzerkonten:

SCHRITT 1 Wählen Sie **Administration** > **Benutzer** aus.

SCHRITT 2 Aktivieren Sie im Feld **Kontoaktivierung** die Kontrollkästchen für die Konten, die Sie aktivieren möchten. Das Administratorkonto muss aktiv sein.

SCHRITT 3 (Optional) Um das Administratorkonto zu bearbeiten, aktivieren Sie unter **Administratorkonto-Einstellungen** das Kontrollkästchen **Administratoreinstellungen bearbeiten**. Um das Gastkonto zu bearbeiten, aktivieren Sie unter **Gasteinstellungen** das Kontrollkästchen **Gasteinstellungen bearbeiten**. Geben Sie folgende Informationen ein:

Neuer Benutzername	Geben Sie einen neuen Benutzernamen ein.
Altes Kennwort	Geben Sie das aktuelle Kennwort ein.
Neues Kennwort	Geben Sie das neue Kennwort ein. Achten Sie darauf, dass das Kennwort keine Wörter aus einem Wörterbuch einer beliebigen Sprache enthält und aus einer Mischung aus Buchstaben (Groß- und Kleinbuchstaben), Ziffern und Symbolen besteht. Das Kennwort darf maximal 64 Zeichen enthalten.
Neues Kennwort erneut eingeben	Geben Sie das neue Kennwort erneut ein.

SCHRITT 4 So importieren Sie Benutzernamen und Kennwörter aus einer CSV-Datei:

a. Klicken Sie im Feld **Benutzername und Kennwort importieren** auf **Durchsuchen**.

b. Suchen Sie die Datei und klicken Sie auf **Öffnen**.

c. Klicken Sie auf **Importieren**.

SCHRITT 5 Geben Sie das alte Kennwort ein.

SCHRITT 6 Klicken Sie auf **Speichern**.

Festlegen des Sitzungs-Timeout-Werts

Der Timeout-Wert gibt an, wie lange (in Minuten) der Gerätemanager im inaktiven Zustand verbleiben kann, bis die Gerätemanagersitzung beendet wird. Sie können ein Timeout für das Administratorkonto und das Gastkonto konfigurieren.

So konfigurieren Sie ein Sitzungs-Timeout:

SCHRITT 1 Wählen Sie **Administration** > **Sitzungs-Timeout** aus.

SCHRITT 2 Geben Sie in das Feld **Administratorinaktivitäts-Timeout** ein, nach wie vielen Minuten ein Sitzungs-Timeout aufgrund von Inaktivität auftritt. Wählen Sie **Nie** aus, um zuzulassen, dass der Administrator dauerhaft angemeldet bleibt.

SCHRITT 3 Geben Sie in das Feld **Gastinaktivitäts-Timeout** ein, nach wie vielen Minuten ein Sitzungs-Timeout aufgrund von Inaktivität auftritt. Wählen Sie **Nie** aus, um zuzulassen, dass der Gast dauerhaft angemeldet bleibt.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von SNMP (Simple Network Management)

Mit dem SNMP (Simple Network Management Protocol) können Sie den Router über einen SNMP-Manager überwachen und verwalten. SNMP ermöglicht die Remoteüberwachung und -steuerung von Netzwerkgeräten sowie die Verwaltung von Konfigurationen, Statistiken, Leistung und Sicherheit.

Konfigurieren von SNMP-Systeminformationen

Auf der Seite **SNMP** können Sie SNMP im Abschnitt **SNMP-Systeminformationen** aktivieren.

Zum Verwenden von SNMP müssen Sie zuerst SNMP-Software auf dem Computer installieren. Das Gerät unterstützt nur SNMPv3 für die SNMP-Verwaltung und SNNPv1/2/3 für SNMP-Trap-Nachrichten.

So aktivieren Sie SNMP:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um SNMP zu aktivieren.

SCHRITT 3 Geben Sie folgende Informationen ein:

SysContact	Geben Sie den Namen der Kontaktperson für diese Firewall ein (beispielsweise **Admin** oder **Monika Mustermann**).
SysLocation	Geben Sie den physischen Standort der Firewall ein (beispielsweise **Rack 2, 4. Stock**).
SysName	Geben Sie einen Namen ein, der die einfache Identifizierung der Firewall ermöglicht.

SCHRITT 4 Klicken Sie auf **Speichern**.

Bearbeiten von SNMPv3-Benutzern

Sie können SNMPv3-Parameter für die beiden Standardbenutzerkonten des Geräts (Administrator und Gast) konfigurieren.

So konfigurieren Sie SNMPv3-Einstellungen:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Konfigurieren Sie unter **SNMPv3-Benutzerkonfiguration** die folgenden Einstellungen:

Benutzername	Wählen Sie das zu konfigurierende Konto aus (**Administrator** oder **Gast**).
Zugriffsrecht	Zeigt die Zugriffsrechte des ausgewählten Benutzerkontos an.
Sicherheitsstufe	Wählen Sie die SNMPv3-Sicherheitsstufe aus: **Keine Authentifizierung und keine Berechtigung**: Erfordert keine Authentifizierung und keinen Datenschutz. **Authentifizierung und keine Berechtigung**: Es werden nur der Authentifizierungsalgorithmus und das Kennwort übermittelt. **Authentifizierung und Berechtigung**: Es werden der Authentifizierungs-/Datenschutzalgorithmus und das Kennwort übermittelt.
Authentifizierungsalgo-rithmusserver	Wählen Sie den Typ des Authentifizierungsalgorithmus aus (**MD5** oder **SHA**).
Authentifizierungskenn-wort	Geben Sie das Authentifizierungskennwort ein.
Datenschutzalgorithmus	Wählen Sie den Typ des Datenschutzalgorithmus aus (**DES** oder **AES**).
Datenschutzkennwort	Geben Sie das Datenschutzkennwort ein.

SCHRITT 3 Klicken Sie auf **Speichern**.

Konfigurieren der SNMP-Traps

In den Feldern im Abschnitt **SNMP-Trap-Konfiguration** können Sie einen SNMP-Agent konfigurieren, an den die Firewall Trap-Nachrichten (Benachrichtigungen) sendet.

So konfigurieren Sie die Traps:

SCHRITT 1 Wählen Sie **Administration** > **SNMP** aus.

SCHRITT 2 Nehmen Sie unter **Trap-Konfiguration** die folgenden Einstellungen vor:

IP-Adresse	Geben Sie die IP-Adresse des SNMP-Managers oder Trap-Agents ein.
Port	Geben Sie den SNMP-Trap-Anschluss der IP-Adresse ein, an die Trap-Nachrichten gesendet werden sollen.
Community	Geben Sie die Community-Zeichenfolge für den Agent ein. Die meisten Agents sind so konfiguriert, dass Traps in der öffentlichen Community abgehört werden.
SNMP-Version	Wählen Sie die SNMP-Version aus: **v1**, **v2c** oder **v3**.

SCHRITT 3 Klicken Sie auf **Speichern**.

Verwenden von Diagnosetools

Das Gerät stellt verschiedene Diagnosetools bereit, die die Behebung von Netzwerkproblemen erleichtern sollen.

- **Netzwerktools**
- **Konfigurieren der Anschlussspiegelung**

Netzwerktools

Mit Netzwerktools können Sie Probleme im Netzwerk behandeln.

Verwenden von Ping

Mit dem Ping-Dienstprogramm können Sie die Konnektivität zwischen diesem Router und einem anderen Gerät im Netzwerk testen. Außerdem können Sie mit dem Ping-Tool die Konnektivität mit dem Internet testen, indem Sie einen Ping an einen voll qualifizierten Domänennamen (beispielsweise www.cisco.com) senden.

So verwenden Sie Ping:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **IP-Adresse/Domänenname** die IP-Adresse des Geräts oder einen voll qualifizierten Domänennamen wie beispielsweise „www.cisco.com“ ein, um einen Ping zu senden.

SCHRITT 3 Klicken Sie auf **Ping**. Die Ping-Ergebnisse werden angezeigt. Diesen Ergebnissen können Sie entnehmen, ob das Gerät erreichbar ist.

SCHRITT 4 Klicken Sie auf **Schließen**, wenn Sie fertig sind.

Verwenden der Routenverfolgung

Mit dem Dienstprogramm für die Routenverfolgung können Sie alle Router anzeigen, die sich zwischen der Ziel-IP-Adresse und diesem Router befinden. Der Router zeigt maximal 30 Hops (zwischengeschaltete Router) zwischen diesem Router und dem Ziel an.

So verwenden Sie die Routenverfolgung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **IP-Adresse/Domänenname** die IP-Adresse ein, die Sie verfolgen möchten.

SCHRITT 3 Klicken Sie auf **Routenverfolgung**. Die Ergebnisse der Routenverfolgung werden angezeigt.

SCHRITT 4 Klicken Sie auf **Schließen**, wenn Sie fertig sind.

Ausführen einer DNS-Suche

Sie können das Suchtool verwenden, um die IP-Adresse des Hosts (beispielsweise eines Webservers, FTP-Servers oder Mailservers) im Internet zu ermitteln.

Zum Abrufen der IP-Adresse eines Webservers, FTP-Servers, Mailservers oder eines beliebigen anderen Servers im Internet geben Sie den Internetnamen in das Textfeld ein, und klicken Sie auf **Abfrage**. Wenn der Host- oder Domäneneintrag vorhanden ist, wird eine Antwort mit der IP-Adresse angezeigt. Wenn die Meldung „Unbekannter Host“ angezeigt wird, ist der angegebene Internetname nicht vorhanden.

So verwenden Sie das Suchtool:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Netzwerktools** aus.

SCHRITT 2 Geben Sie in das Feld **Internetname** den Internetnamen des Hosts ein.

SCHRITT 3 Klicken Sie auf **Suche**. Die nslookup-Ergebnisse werden angezeigt.

SCHRITT 4 Klicken Sie auf **Schließen**, wenn Sie fertig sind.

Konfigurieren der Anschlussspiegelung

Bei der Anschlussspiegelung wird der Netzwerkverkehr überwacht, indem Kopien aller ein- und ausgehenden Pakete von einem Anschluss an einen Überwachungsanschluss gesendet werden. Sie können die Anschlussspiegelung als Diagnose- und Fehlerbehebungstool verwenden, insbesondere wenn Sie einen Angriff abwehren oder den Benutzerverkehr vom LAN zum WAN anzeigen möchten, um herauszufinden, ob Benutzer auf Informationen oder Websites zugreifen, auf die sie nicht zugreifen sollen.

Der LAN-Host (PC) sollte eine statische IP-Adresse verwenden, um Probleme bei der Anschlussspiegelung zu vermeiden. DHCP-Leases für einen LAN-Host können ablaufen und zu Fehlern bei der Anschlussspiegelung Gespiegelter Port führen, wenn für den LAN-Host keine statische IP-Adresse konfiguriert ist.

So konfigurieren Sie die Anschlussspiegelung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Anschlussspiegelung** aus.

SCHRITT 2 Wählen Sie im Feld **Spiegelquelle** die zu spiegelnden Anschlüsse aus.

SCHRITT 3 Wählen Sie im Dropdown-Menü **Spiegelanschluss** einen gespiegelten Anschluss aus. Wenn Sie einen Anschluss für die Spiegelung verwenden, sollten Sie ihn nicht für anderen Verkehr verwenden.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren der Protokollierung

Sie können für die Cisco RV215W Protokollierungsoptionen konfigurieren.

Konfigurieren von Protokollierungseinstellungen

So konfigurieren Sie die Protokollierung:

SCHRITT 1 Wählen Sie **Administration** > **Protokollierung** > **Protokolleinstellungen** aus.

SCHRITT 2 Aktivieren Sie im Feld **Protokollmodus** das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Klicken Sie auf **Hinzufügen**.

SCHRITT 4 Konfigurieren Sie die folgenden Einstellungen:

Remoteprotokollserver	Geben Sie die IP-Adresse des Protokollservers ein, auf dem die Protokolle gesammelt werden sollen.
Schweregrad für lokales und per E-Mail versendetes Protokoll	Wählen Sie durch Klicken den Schweregrad der zu konfigurierenden Protokolle aus. Beachten Sie, dass alle Protokolltypen über einem ausgewählten Protokolltyp automatisch enthalten sind und dass Sie diese Auswahl nicht aufheben können. Wenn Sie beispielsweise Fehlerprotokolle auswählen, sind zusätzlich zu den Fehlerprotokollen automatisch auch die Protokolle „Notfall“, „Alarm“ und „Kritisch“ enthalten. Es stehen die folgenden Schweregrade für Ereignisse zur Verfügung, aufgelistet von der höchsten bis zur niedrigsten Gewichtung: • **Notfall**: Das System kann nicht verwendet werden. • **Alarm**: Es ist eine Aktion erforderlich. • **Kritisch**: Das System befindet sich in einem kritischen Zustand. • **Fehler**: Das System befindet sich im Fehlerzustand. • **Warnung**: Es ist eine Systemwarnung aufgetreten. • **Benachrichtigung**: Das System funktioniert ordnungsgemäß, es ist jedoch ein Systemhinweis aufgetreten. • **Informationen**: Geräteinformationen. • **Fehlerbehebung**: Bietet detaillierte Informationen zu einem Ereignis. Wenn Sie diesen Schweregrad auswählen, werden umfangreiche Protokolle generiert. Dies wird bei normalem Betrieb des Routers nicht empfohlen.

Aktivieren	Zum Aktivieren dieser Protokollierungseinstellungen aktivieren Sie dieses Kontrollkästchen.

SCHRITT 5 Klicken Sie auf **Speichern**.

Zum Bearbeiten eines Eintrags in der **Tabelle für Protokollierungseinstellungen** wählen Sie den Eintrag aus, und klicken Sie auf **Bearbeiten**. Nehmen Sie die Änderungen vor, und klicken Sie dann auf **Speichern**.

Konfigurieren von E-Mail-Einstellungen

Sie können die Cisco RV215W so konfigurieren, dass Ereignisprotokolle, Warnungen zu neuer Firmware und 3G-Warnungen per E-Mail versendet werden. Wir empfehlen, zum Senden und Empfangen von E-Mail-Warnungen ein separates E-Mail-Konto einzurichten.

So konfigurieren Sie die E-Mail-Einstellungen:

SCHRITT 1 Wählen Sie **Administration** > **Protokollierung** > **E-Mail-Einstellungen** aus.

SCHRITT 2 Im Abschnitt **E-Mail-Benachrichtigungskonfiguration**:

- Aktivieren Sie das Kontrollkästchen **3G E-mail Alert Enable**, (E-Mail-Warnung zu 3G aktivieren) um 3G-Warnungen per E-Mail zu versenden.
- Aktivieren Sie das Kontrollkästchen **Protokolle per E-Mail versenden aktivieren**, um Protokolle per E-Mail zu versenden**.** Achten Sie darauf, den Schweregrad für die Ereignisse festzulegen, die Sie protokollieren möchten. Weitere Informationen finden Sie unter **Konfigurieren von Protokollierungseinstellungen**. Im Feld **Minimum E-mail Log Severity** (Minimaler Schweregrad des E-Mail-Protokolls) wird der Schweregrad der Protokolle angezeigt, die Sie erfassen möchten. Zum Ändern des Protokollschweregrads klicken Sie auf **Schweregrad konfigurieren**.

  Wählen Sie im Abschnitt **E-Mail-Protokolle nach Zeitplan senden** aus, ob die E-Mail **Stündlich**, **Täglich** oder **Wöchentlich** gesendet werden soll. Wenn Sie **Nie** auswählen, werden keine Protokolle gesendet. Wenn Sie einen wöchentlichen Zeitplan ausgewählt haben, wählen Sie den Wochentag aus, an dem die Protokolle per E-Mail gesendet werden sollen. Wenn Sie einen täglichen oder wöchentlichen Zeitplan ausgewählt haben, wählen Sie die Uhrzeit aus, zu der das Gerät die Protokolle per E-Mail senden soll.

SCHRITT 3 Geben Sie im Abschnitt **E-Mail-Einstellungen** die folgenden Informationen ein, um die Einstellungen für die per E-Mail gesendeten Warnungen zu konfigurieren:

Adresse des Mailservers	Geben Sie die IP-Adresse des SMTP-Servers ein. Dabei handelt es sich um den Mailserver, der dem von Ihnen eingerichteten E-Mail-Konto zugeordnet ist (beispielsweise mail.Firmenname.com).
Port des Mailservers	Geben Sie den SMTP-Serveranschluss ein. Wenn für den E-Mail-Anbieter ein spezieller Anschluss für E-Mail erforderlich ist, geben Sie diesen hier ein. Verwenden Sie anderenfalls den Standardwert (25).
Antwort-E-Mail-Adresse	Geben Sie die Antwort-E-Mail-Adresse ein, an die die Cisco RV215W Nachrichten sendet, wenn Warnungen vom Router nicht an die unter „An E-Mail-Adresse senden“ angegebene E-Mail-Adresse übermittelt werden.
An E-Mail-Adresse (1) senden	Geben Sie eine E-Mail-Adresse ein, an die Warnungen gesendet werden sollen (beispielsweise Protokollierung@Firmenname.com).
An E-Mail-Adresse (2) senden (optional)	Geben Sie eine zusätzliche E-Mail-Adresse ein, an die Warnungen gesendet werden.
An E-Mail-Adresse (3) senden (optional)	Geben Sie eine zusätzliche E-Mail-Adresse ein, an die Warnungen gesendet werden.
E-Mail-Verschlüsselung (SSL)	Zum Aktivieren der E-Mail-Verschlüsselung aktivieren Sie das Kontrollkästchen **Aktivieren**.
Authentifizierung an SMTP-Server	Wenn der SMTP-Server (Mailserver) Verbindungen nur nach Authentifizierung akzeptiert, wählen Sie im Dropdown-Menü den Authentifizierungstyp aus: **Keine**, **ANMELDUNG**, **NORMAL** oder **CRAM-MD5**.
E-Mail-Authentifizierungsbenutzername	Geben Sie den Benutzernamen für die E-Mail-Authentifizierung ein (beispielsweise Protokollierung@Firmenname.com).

E-Mail-Authentifizierungskennwort	Geben Sie das E-Mail-Authentifizierungskennwort ein (beispielsweise das Kennwort für den Zugriff auf das von Ihnen eingerichtete E-Mail-Konto, an das Warnungen gesendet werden sollen).
E-Mail-Authentifizierungstest	Klicken Sie auf **Testen**, um die E-Mail-Authentifizierung zu testen.

SCHRITT 4 Konfigurieren Sie im Abschnitt **E-Mail-Protokolle nach Zeitplan senden** die folgenden Einstellungen:

Einheit	Wählen Sie die Zeiteinheit für die Protokolle aus (**Nie**, **Stündlich**, **Täglich** oder **Wöchentlich**). Wenn Sie **Nie** auswählen, werden keine Protokolle gesendet.
Tag	Wenn Sie für das Senden von Protokollen einen wöchentlichen Zeitplan ausgewählt haben, wählen Sie den Wochentag aus, an dem die Protokolle gesendet werden sollen.
Uhrzeit	Wenn Sie für das Senden von Protokollen einen täglichen oder wöchentlichen Zeitplan ausgewählt haben, wählen Sie die Tageszeit aus, zu der die Protokolle gesendet werden sollen.

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von Bonjour

Bei Bonjour handelt es sich um ein Protokoll für die Ankündigung und Erkennung von Services. Die in der Cisco RV215W konfigurierten Standardservices werden nur dann von Bonjour angekündigt, wenn Bonjour aktiviert ist.

So aktivieren Sie Bonjour:

SCHRITT 1 Wählen Sie **Administration** > **Bonjour** aus.

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Aktivieren**, um Bonjour zu aktivieren.

SCHRITT 3 Zum Aktivieren von Bonjour für ein in den **Bonjour-Schnittstellensteuerungseinträgen** aufgeführtes VLAN aktivieren Sie das entsprechende Kontrollkästchen **Bonjour aktivieren**.

Sie können Bonjour für bestimmte VLANs aktivieren. Wenn Sie Bonjour für ein VLAN aktivieren, können im VLAN vorhandene Geräte die im Router verfügbaren Bonjour-Services erkennen (beispielsweise HTTP/HTTPS).

Wenn beispielsweise ein VLAN mit der ID 2 konfiguriert ist, können Geräte und Hosts in VLAN 2 nur dann im Router ausgeführte Bonjour-Services erkennen, wenn Bonjour für VLAN 2 aktiviert ist.

SCHRITT 4 Klicken Sie auf **Speichern**.

Konfigurieren von Datums- und Zeiteinstellungen

Sie können die Zeitzone konfigurieren, ob die Zeit an die Sommerzeit angepasst werden soll und mit welchem NTP-Server (Network Time Protocol) Datum und Uhrzeit synchronisiert werden sollen. Der Router erhält dann die Datums- und Zeitinformationen vom NTP-Server.

So konfigurieren Sie NTP und Zeiteinstellungen:

SCHRITT 1 Wählen Sie **Administration** > **Zeiteinstellungen** aus. Hier wird die aktuelle Zeit angezeigt.

SCHRITT 2 Konfigurieren Sie diese Informationen:

Zeitzone	Wählen Sie die Zeitzone relativ zur Greenwich Mean Time (GMT) aus.
Automatisch auf Sommer-/Winterzeit umstellen	Aktivieren Sie das Kontrollkästchen **Automatisch auf Sommer-/Winterzeit umstellen**, wenn dies für Ihre Region unterstützt wird. Das Kontrollkästchen wird aktiviert, wenn Sie unten im Feld **Datum und Uhrzeit festlegen** auf **Automatisch** klicken.

Sommerzeit-Modus	Sie haben die Wahl zwischen **Nach Datum** (Sie geben das Datum für die Umstellung auf den Sommerzeitmodus ein) und **Wiederkehrend** (Sie geben den Monat, die Woche, den Wochentag und die Uhrzeit für die Umstellung auf den Sommerzeitmodus ein). Geben Sie die entsprechenden Informationen in die Felder „von“ und „bis“ ein.
Sommerzeitdifferenz	Wählen Sie im Dropdown-Menü die Differenz zur Coordinated Universal Time (UTC) aus.
Datum und Uhrzeit festlegen	Wählen Sie aus, wie Datum und Uhrzeit festgelegt werden sollen.
NTP-Server	Wenn Sie die Standard-NTP-Server verwenden möchten, klicken Sie auf die Schaltfläche **Standard verwenden**. Wenn Sie einen bestimmten NTP-Server verwenden möchten, klicken Sie auf **Benutzerdefinierter NTP-Server** und geben Sie den voll qualifizierten Domänennamen oder die IP-Adresse des NTP-Servers in die beiden verfügbaren Felder ein.
Datum und Uhrzeit eingeben	Geben Sie das Datum und die Uhrzeit ein.

SCHRITT 3 Klicken Sie auf **Speichern**.

Sichern und Wiederherstellen des Systems

Auf der Seite **Administration** > **Einstellungen sichern/wiederherstellen** können Sie benutzerdefinierte Konfigurationseinstellungen zur späteren Wiederherstellung sichern oder Einstellungen aus einer zuvor erstellten Sicherung wiederherstellen.

Wenn die Firewall mit den konfigurierten Einstellungen funktioniert, können Sie die Konfiguration sichern, damit Sie sie später wiederherstellen können. Bei der Sicherung werden die Einstellungen als Datei auf dem PC gespeichert. Aus dieser Datei können Sie die Einstellungen der Firewall wiederherstellen.

VORSICHT Versuchen Sie bei einer Wiederherstellung erst nach Abschluss des Vorgangs, eine Onlineverbindung herzustellen, die Firewall auszuschalten, den PC herunterzufahren oder die Firewall zu verwenden. Dies sollte ungefähr eine Minute dauern. Warten Sie nach dem Erlöschen der Test-LED noch ein paar Sekunden, bevor Sie die Firewall verwenden.

Sichern der Konfigurationseinstellungen

So sichern Sie die Konfiguration oder stellen sie wieder her:

SCHRITT 1 Wählen Sie **Administration** > **Einstellungen sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie die Konfiguration aus, die Sie sichern oder löschen möchten:

Startkonfiguration	Wählen Sie diese Option aus, um die Startkonfiguration herunterzuladen. Die Startkonfiguration ist die aktuelle ausgeführte Konfiguration, die vom Gerät verwendet wird. Wenn die Startkonfiguration des Routers verloren gegangen ist, verwenden Sie diese Seite, um die Sicherungskonfiguration in die Startkonfiguration zu kopieren. Dabei bleiben alle vorherigen Konfigurationsinformationen erhalten. Sie können die Startkonfiguration herunterladen, um sie einfach auf anderen Cisco RV215W-Geräten bereitzustellen.
Spiegelkonfiguration	Wählen Sie diese Option aus, um das Gerät anzuweisen, die Startkonfiguration nach 24 Betriebsstunden ohne Änderung an der Startkonfiguration zu sichern.
Konfiguration sichern	Wählen Sie diese Option aus, um die aktuellen Konfigurationseinstellungen zu sichern.

SCHRITT 3 Klicken Sie auf **Download**, um die Backupdatei auf Ihren Computer herunterzuladen.

Standardmäßig wird die Datei („startup.cfg“, „mirror.cfg“ oder „backup.cfg“) in den Standardordner für Downloads heruntergeladen, beispielsweise C:\Dokumente und Einstellungen\admin\Eigene Dokumente\Downloads\.

Wenn Sie die Backup-Datei auf einem USB-Laufwerk speichern möchten, klicken Sie auf **Save to USB** (Auf USB speichern).

SCHRITT 4 Zum Löschen der ausgewählten Konfiguration klicken Sie auf **Löschen**.

Wiederherstellen der Konfigurationseinstellungen

Sie können eine zuvor gespeicherte Konfigurationsdatei wiederherstellen:

SCHRITT 1 Wählen Sie **Administration** > **Konfiguration sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie im Feld zum Hochladen der Konfiguration die hochzuladende Konfiguration aus (**Startkonfiguration** oder **Konfiguration sichern**).

SCHRITT 3 Sie können die Konfigurationsdatei von Ihrem PC oder von einem externen USB-Gerät hochladen.

Zum Upload von Ihrem Computer klicken Sie auf das Optionsfeld **PC**. Klicken Sie auf **Durchsuchen**, um die Datei zu suchen. Suchen Sie die Datei und klicken Sie auf **Öffnen**.

Zum Hochladen von einem USB-Laufwerk klicken Sie auf das Optionsfeld **USB**. Klicken Sie auf **Show USB** (USB anzeigen), um alle angeschlossenen USB-Geräte anzuzeigen. Suchen Sie die Datei auf dem USB-Laufwerk und klicken Sie auf **Öffnen**.

HINWEIS Auf USB-Geräten unterstützt Ihr Gerät NTFS im schreibgeschützten Modus und die Dateiformate FAT und FAT32 im Modus mit Lese- und Schreibzugriff.

SCHRITT 4 Klicken Sie auf **Jetzt hochladen**.

Das Gerät lädt die Konfigurationsdatei hoch und verwendet die darin enthaltenen Einstellungen zum Aktualisieren der Startkonfiguration. Anschließend wird das Gerät neu gestartet und verwendet die neue Konfiguration.

Kopieren der Konfigurationseinstellungen

Kopieren Sie die Startkonfiguration in die Sicherungskonfiguration, um sicherzustellen, dass Sie über eine Sicherungskopie verfügen, falls Sie Ihren Benutzernamen und Ihr Kennwort vergessen und dann nicht auf den Gerätemanager zugreifen können. In diesem Fall können Sie den Gerätemanager erst dann wieder verwenden, wenn Sie das Gerät auf die Werkseinstellungen zurückgesetzt haben.

Die Sicherungskonfigurationsdatei bleibt im Arbeitsspeicher, und Sie können die gesicherten Konfigurationsinformationen in die Startkonfiguration kopieren, wobei alle Einstellungen wiederhergestellt werden.

So kopieren Sie eine Konfiguration (um beispielsweise eine Startkonfiguration in die Sicherungskonfiguration zu kopieren):

SCHRITT 1 Wählen Sie **Administration** > **Konfiguration sichern/wiederherstellen** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü im Feld **Kopieren** die Quell- und Zielkonfiguration aus.

SCHRITT 3 Klicken Sie auf **Jetzt kopieren**.

Generieren eines Verschlüsselungsschlüssels

Sie können auf dem Router einen Verschlüsselungsschlüssel generieren, um die Sicherungsdateien zu schützen.

So generieren Sie einen Verschlüsselungsschlüssel:

SCHRITT 1 Wählen Sie **Administration** > **Konfiguration sichern/wiederherstellen** aus.

SCHRITT 2 Klicken Sie auf **Erweiterte Einstellungen anzeigen**.

SCHRITT 3 Geben Sie in das Feld den zum Generieren des Schlüssels verwendeten Seed-Wert ein.

SCHRITT 4 Klicken Sie auf **Speichern**.

Aktualisieren der Firmware oder Ändern der Sprache

Auf der Seite **Administration** > **Firmware-/Sprach-Upgrade** können Sie die Router-Firmware auf eine neuere Version aktualisieren oder auf dem Router die Sprache ändern.

VORSICHT Versuchen Sie bei einem Firmware-Upgrade nicht, vor Abschluss des Vorgangs eine Onlineverbindung herzustellen, das Gerät auszuschalten, den PC herunterzufahren oder den Vorgang auf irgendeine Weise zu unterbrechen. Der Vorgang dauert einschließlich des Neustarts ungefähr eine Minute. Wenn Sie den Upgrade-Vorgang an bestimmten Stellen unterbrechen, während Daten in den Flash-Speicher geschrieben werden, werden die Daten möglicherweise beschädigt und der Router kann nicht mehr verwendet werden.

Automatisches Aktualisieren der Firmware

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 Wählen Sie im Abschnitt **Automatic Firmware Upgrade** (Automatisches Firmware-Upgrade) im Feld **Intervall - Überprüfung alle** (Prüfungsintervall) aus, wie oft das Gerät nach aktualisierter Firmware suchen soll.

SCHRITT 3 Wählen Sie im Feld **Upgrade automatisch durchführen** aus, ob das Upgrade auf die aktuellste Firmware zu einem bestimmten Zeitpunkt oder direkt durchgeführt werden soll, nachdem eine neue Version ermittelt wurde.

SCHRITT 4 Aktivieren Sie eines der folgenden Kontrollkästchen, um bei Verfügbarkeit neuer Firmware oder nach dem Upgrade mit aktuellster Firmware benachrichtigt zu werden:

- **Notify via Admin GUI** (Über Admin-GUI benachrichtigen): Sie werden über die Administrations-GUI der RV215W benachrichtigt, wenn Sie sich das nächste Mal anmelden.
- **Email to** (E-Mail an): Sie werden über E-Mail-Warnungen benachrichtigt. Klicken Sie auf **E-Mail-Adresse**, um die E-Mail-Einstellungen zu konfigurieren. Dieses Kontrollfeld ist ausgegraut, wenn **E-Mail-Benachrichtigung zu neuer Firmware** nicht aktiviert wurde. Weitere Informationen finden Sie unter **Konfigurieren von E-Mail-Einstellungen**.

SCHRITT 5 Klicken Sie auf **Speichern**.

Automatisches Upgrade der Firmware/Konfiguration von einem USB-Gerät

So führen Sie ein automatisches Upgrade der Firmware und Konfiguration von einem USB-Gerät durch:

SCHRITT 1 Wählen Sie im Feld **Beim Einschalten des Geräts Upgrade vom USB-Laufwerk ausführen** die Option **Aktivieren** aus.

Bei dieser Einstellung für die Bereitstellung ohne Benutzereingriff geschieht Folgendes, wenn das USB-Gerät angeschlossen wird:

- Die Firmware auf Ihrem Gerät wird automatisch aktualisiert, sobald das Gerät eingeschaltet wird.
- Die Konfigurationsdatei wird automatisch hochgeladen, wenn das Gerät eingeschaltet und auf die werkseitigen Standardeinstellungen zurückgesetzt wird.

SCHRITT 2 Klicken Sie auf **Speichern**.

Manuelles Aktualisieren der Firmware

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 Klicken Sie im Abschnitt **Manuelles Firmware-/Sprach-Upgrade** im Feld **Dateityp** auf das Optionsfeld **Firmware-Image**.

SCHRITT 3 Laden Sie die aktuellste Firmware auf Ihren PC oder ein USB-Gerät herunter. Zum Download der aktuellsten Firmware von cisco.com auf ein USB-Gerät klicken Sie im Feld **Save to USB from cisco.com** (Von cisco.com auf USB speichern) auf **Download starten**.

SCHRITT 4 Wählen Sie eine der folgenden Optionen für die Quelle des Upgrades, um das Upgrade auf die aktuellste Firmwareversion durchzuführen:

- **cisco.com**: Laden Sie die Firmware von der Website cisco.com herunter.
- **PC**: Klicken Sie auf **Durchsuchen**, um die auf den Computer heruntergeladene Firmware zu suchen und auszuwählen.
- **USB**: Klicken Sie auf **Show USB** (USB anzeigen), um alle Dateien auf dem USB-Gerät in der **USB Content Table** (Tabelle der Inhalte auf USB) anzuzeigen. Suchen Sie die Firmware-Datei und wählen Sie sie aus.

HINWEIS Auf USB-Geräten unterstützt Ihr Gerät NTFS im schreibgeschützten Modus und die Dateiformate FAT und FAT32 im Modus mit Lese- und Schreibzugriff.

VORSICHT Beim Zurücksetzen des Geräts auf die werkseitigen Einstellungen werden alle Konfigurationseinstellungen gelöscht.

SCHRITT 5 Klicken Sie auf **Upgrade starten**.

Nach der Überprüfung des neuen Firmware-Images wird das Image in den Flash-Speicher des Geräts geschrieben und der Router wird automatisch mit der neuen Firmware neu gestartet. Im Abschnitt **Systeminformationen** wird die aktuellste Firmware angezeigt.

Ändern der Sprache

So ändern Sie die Sprache:

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 Klicken Sie im Feld **Dateityp** auf die Schaltfläche **Sprachdatei**.

SCHRITT 3 Klicken Sie auf **Durchsuchen**, um die heruntergeladene Sprachdatei zu suchen und auszuwählen.

SCHRITT 4 Wenn Sie die Parameter der Gerätekonfiguration auf die werkseitigen Standardeinstellungen zurücksetzen möchten, wählen Sie **Alle Konfigurationen/ Einstellungen auf Werkseinstellungen zurücksetzen** aus.

SCHRITT 5 Klicken Sie auf **Upgrade starten**.

Neustarten der Cisco RV215W

So starten Sie den Router neu:

SCHRITT 1 Wählen Sie **Administration** > **Neu starten** aus.

SCHRITT 2 Klicken Sie auf **Neu starten**.

Wiederherstellen der Werkseinstellungen

VORSICHT Versuchen Sie bei einer Wiederherstellung erst nach Abschluss des Vorgangs, eine Onlineverbindung herzustellen, den Router auszuschalten, den PC herunterzufahren oder den Router zu verwenden. Der Vorgang sollte ungefähr eine Minute dauern. Warten Sie nach dem Erlöschen der Test-LED noch ein paar Sekunden, bevor Sie den Router verwenden.

So stellen Sie die Werkseinstellungen des Routers wieder her:

SCHRITT 1 Wählen Sie **Administration** > **Werkseinstellungen wiederherstellen** aus.

SCHRITT 2 Klicken Sie auf **Standard**.

Ausführen des Setup-Assistenten

So führen Sie den Setup-Assistenten aus:

SCHRITT 1 Wählen Sie **Administration** > **Setup-Assistent** aus.

SCHRITT 2 Folgen Sie den auf dem Bildschirm angezeigten Anweisungen.

A

Verwenden von Cisco QuickVPN

Übersicht

In diesem Anhang wird die Installation und Verwendung der Cisco QuickVPN-Software erläutert, die Sie von Cisco.com herunterladen können. QuickVPN kann auf Computern unter Windows 7, Windows XP, Windows Vista oder Windows 2000 verwendet werden. (Auf Computern unter anderen Betriebssystemen müssen Sie VPN-Software eines Drittanbieters verwenden.)

Dieser Anhang enthält die folgenden Abschnitte:

- **Vorbereitung**
- **Installieren der Cisco QuickVPN-Software**
- **Verwenden der Cisco QuickVPN-Software**

Vorbereitung

Das QuickVPN-Programm kann nur verwendet werden, wenn der Router so konfiguriert ist, dass er QuickVPN-Verbindungen unterstützt. Führen Sie die folgenden Schritte aus:

SCHRITT 1 Aktivieren Sie die Remoteverwaltung. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

SCHRITT 2 Erstellen Sie QuickVPN-Benutzerkonten. Weitere Informationen hierzu finden Sie unter **Konfigurieren von PPTP**. Wenn Sie ein Benutzerkonto erstellt haben, können die Anmeldeinformationen vom QuickVPN-Client verwendet werden.

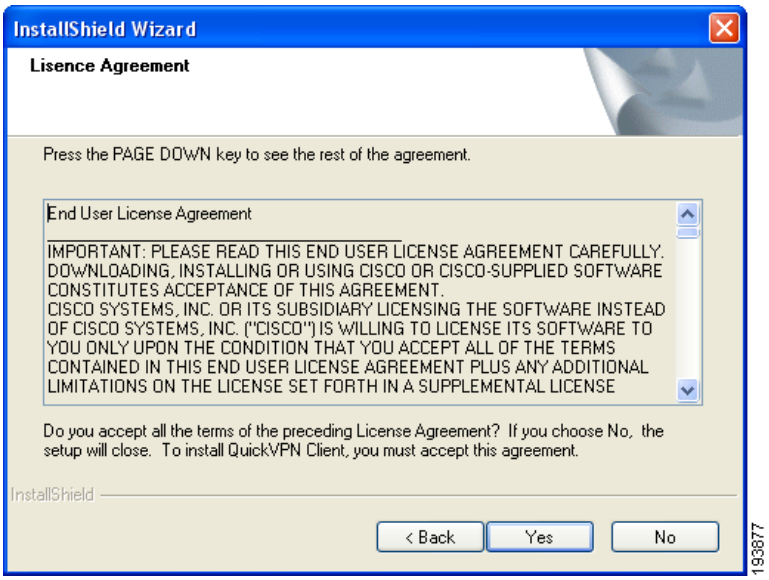
Installieren der Cisco QuickVPN-Software

Installieren von der CD-ROM

SCHRITT 1 Legen Sie die CD-ROM für die Cisco RV215W in das CD-ROM-Laufwerk ein. Klicken Sie nach dem Start des Setup-Assistenten auf den Link **Install QuickVPN** (QuickVPN installieren).

Das Fenster mit der Lizenzvereinbarung wird angezeigt.

Lizenzvereinbarung



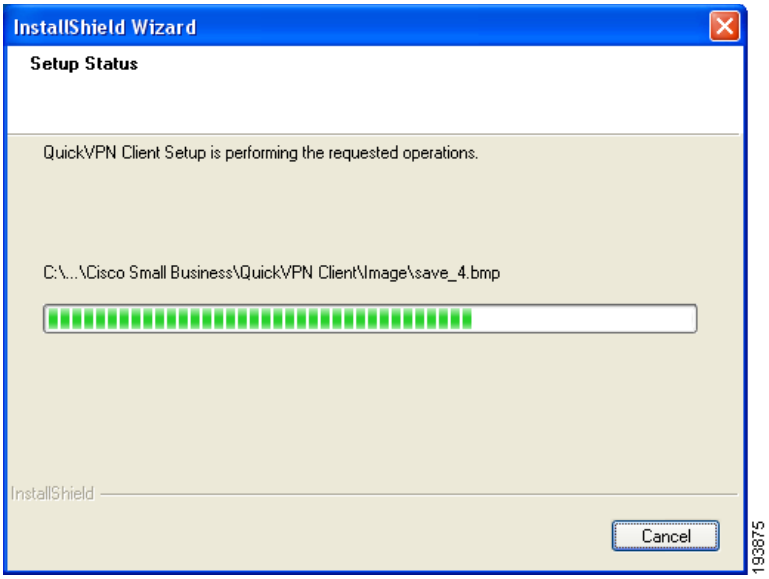
SCHRITT 2 Klicken Sie auf **Ja**, um die Vereinbarung zu akzeptieren.

SCHRITT 3 Klicken Sie auf **Durchsuchen**, und wählen Sie aus, wohin die Dateien kopiert werden sollen (beispielsweise „C:\Cisco Small Business\QuickVPN Client“).

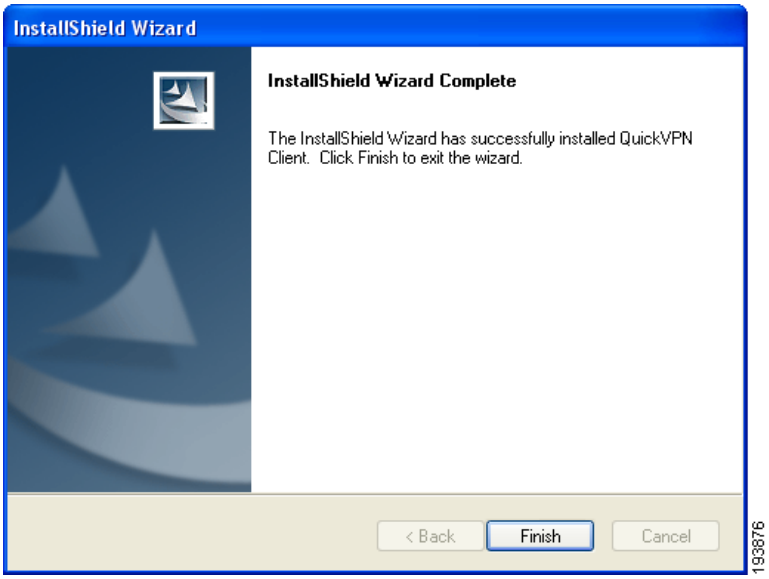
SCHRITT 4 Klicken Sie auf **Weiter**.

Der Setup-Assistent kopiert die Dateien an den ausgewählten Speicherort.

Copying Files (Dateien werden kopiert)



Finished Installing Files (Installieren der Dateien beendet)



SCHRITT 5 Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen. Fahren Sie mit **?$paratext>? auf Seite 161** fort.

Herunterladen und Installieren aus dem Internet

SCHRITT 1 Gehen Sie in **Anhang B, ?$paratext>?** zum Link „Herunterladen von Software“.

SCHRITT 2 Geben Sie in das Suchfeld „Cisco RV215W“ ein, und suchen Sie die **QuickVPN**-Software.

SCHRITT 3 Speichern Sie die ZIP-Datei auf Ihrem PC und extrahieren Sie die EXE-Datei.

SCHRITT 4 Doppelklicken Sie auf die EXE-Datei und folgen Sie den Anweisungen auf dem Bildschirm.

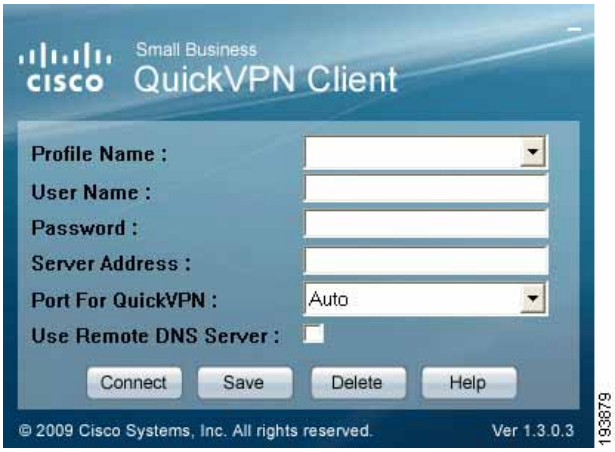
Verwenden der Cisco QuickVPN-Software

SCHRITT 1 Doppelklicken Sie auf dem Desktop oder in der Taskleiste auf das Cisco QuickVPN-Symbol.

QuickVPN Desktop Icon

QuickVPN Tray Icon—
No Connection

Das Fenster für die QuickVPN-Anmeldung wird angezeigt.



SCHRITT 2 Geben Sie in das Feld **Profile Name** (Profilname) einen Namen für Ihr Profil ein.

SCHRITT 3 Geben Sie in die Felder **User Name** (Benutzername) und **Kennwort** den Benutzernamen bzw. das Kennwort ein.

SCHRITT 4 Geben Sie in das Feld **Server Address** (Serveradresse) die IP-Adresse oder den Domänennamen der Cisco RV215W ein.

SCHRITT 5 Geben Sie in das Feld **Port For QuickVPN** (Anschluss für QuickVPN) die Anschlussnummer ein, die der QuickVPN-Client für die Kommunikation mit dem VPN-Remoterouter verwendet, oder behalten Sie die Standardeinstellung **Auto** bei.

SCHRITT 6 Zum Speichern des Profils klicken Sie auf **Speichern**.

Zum Löschen des Profils klicken Sie auf **Löschen**. Weitere Informationen erhalten Sie, wenn Sie auf **Hilfe** klicken.

HINWEIS Wenn Sie Tunnel für mehrere Sites erstellen müssen, können Sie mehrere Profile anlegen. Es kann jedoch nur jeweils ein Tunnel aktiv sein.

SCHRITT 7 Zum Starten der QuickVPN-Verbindung klicken Sie auf **Verbinden**.

Der Verbindungsfortschritt wird angezeigt: Wird verbunden, Provisioning (Bereitstellen), Activating Policy (Richtlinie aktivieren) und Verifying Network (Netzwerk überprüfen).

SCHRITT 8 Wenn die QuickVPN-Verbindung hergestellt ist, wird das QuickVPN-Symbol in der Taskleiste grün dargestellt und das Fenster mit dem QuickVPN-Status wird angezeigt.

In diesem Fenster werden die IP-Adresse der Remoteseite des VPN-Tunnels sowie Uhrzeit und Datum des Beginns des VPN-Tunnels und die Gesamtdauer der Aktivität des VPN-Tunnels angezeigt.

Zum Beenden des VPN-Tunnels klicken Sie auf **Trennen**. Zum Ändern Ihres Kennworts klicken Sie auf **Kennwort ändern**. Weitere Informationen erhalten Sie, wenn Sie auf **Hilfe** klicken.

SCHRITT 9 Wenn Sie auf **Kennwort ändern** geklickt haben und über die Berechtigung zum Ändern Ihres eigenen Kennworts verfügen, wird das Fenster **Connect Virtual Private Connection** (Virtuelle private Verbindung herstellen) angezeigt.

SCHRITT 10 Geben Sie Ihr Kennwort in das Feld **Altes Kennwort** ein. Geben Sie Ihr neues Kennwort in das Feld **Neues Kennwort** ein. Geben Sie dann in das Feld **Confirm New Password** (Neues Kennwort bestätigen) das neue Kennwort erneut ein.

SCHRITT 11 Klicken Sie auf **OK**, um das neue Kennwort zu speichern.

HINWEIS Sie können Ihr Kennwort nur ändern, wenn das Kontrollkästchen **Kennwortänderung durch Benutzer zulassen** für den jeweiligen Benutzernamen aktiviert ist.

B

Weitere Informationen

Support	
Cisco Support-Community	www.cisco.com/go/smallbizsupport
Technischer Online-Support und Dokumentation (Anmeldung erforderlich)	www.cisco.com/support
Telefonischer Kundensupport	www.cisco.com/en/US/support/tsd_cisco_small_ business_support_ center_contacts.html
Herunterladen von Software (Anmeldung erforderlich)	Gehen Sie zu tools.cisco.com/support/downloads und geben Sie die Modellnummer in das Software-Suchfeld ein.

Produktdokumentation	
Wireless N-VPN-Firewall	www.cisco.com/en/US/products/ps9923/tsd_products_support_series_home.html
Cisco Partner Central (Partner-Anmeldung erforderlich)	www.cisco.com/web/partners/sell/smb
Marktplatz	www.cisco.com/go/marketplace