ADMINISTRATOR-HANDBUCH

Cisco RV 110W Wireless N-VPN-Firewall

Überarbeitung: September 2014

78-20157-04

Inhalt

1

Einführung

Dieses Kapitel enthält Informationen, die Sie mit den Produktfunktionen vertraut machen, Sie durch den Installationsvorgang führen und Ihnen die ersten Schritte bei der Verwendung des browserbasierten Gerätemanagers erleichtern sollen.

Produktübersicht

Vielen Dank, dass Sie sich für die Cisco Wireless-N VPN Firewall RV110W entschieden haben.

Bei der Cisco RV110W handelt es sich um eine fortschrittliche Lösung für die gemeinsame Nutzung des Internets für die Anforderungen kleinerer Unternehmen. Sie ermöglicht mehreren Computern in Ihrem Unternehmen die gemeinsame Nutzung einer Internetverbindung. Die Computer können dabei sowohl über Kabel als auch per WLAN verbunden werden.

Die Cisco RV110W bietet einen Wireless-N-Zugriffspunkt sowie Unterstützung für VPN-Clients (Virtual Private Network, virtuelles privates Netzwerk), um die Sicherheit beim Remotezugriff auf Ihr Netzwerk zu erhöhen.

Die 10/100-Fast Ethernet-WAN-Schnittstelle des Routers wird direkt an Ihr Breitbandmodem (DSL oder Kabel) angeschlossen.

LAN-Ethernet-Schnittstellen

Die Cisco RV110W verfügt über vier 10/100 Fast Ethernet-LAN-Schnittstellen mit Unterstützung für Vollduplex, über die bis zu vier Geräte angeschlossen werden können. Sie können einen Switch von Cisco an einen der verfügbaren Anschlüsse anschließen, um das Netzwerk nach Bedarf zu erweitern.

WLAN-Zugriffspunkt

Der WLAN-Zugriffspunkt der Cisco RV110W unterstützt den 802.11n-Standard mit MIMO-Technologie, sodass die effektive Datenrate vervielfacht wird. Diese Technologie verbessert den Durchsatz und die Reichweite im Vergleich zu 802.11g-Netzwerken.

Firewall und VPN-Clientzugriff

Das Cisco RV110W enthält eine SPI-basierte (Stateful Packet Inspection) Firewall mit DoS-Schutz (Denial of Service) und ein VPN-Modul (Virtual Private Network, virtuelles privates Netzwerk) für die sichere Kommunikation zwischen mobilen Mitarbeitern bzw. Remote-Mitarbeitern und Außenstellen.

Die Cisco RV110W unterstützt bis zu fünf Client-zu-Gateway-VPN-Tunnel, um Verbindungen zwischen Zweigstellen über verschlüsselte virtuelle Links zu ermöglichen. Benutzer, die eine Verbindung durch einen VPN-Tunnel herstellen, werden mit dem Netzwerk Ihres Unternehmens verbunden und können genauso sicher auf Dateien, E-Mails und das Intranet zugreifen, als würden sie sich im gleichen Gebäude befinden.

Security

Die Cisco RV110W implementiert die Sicherheitsstandards WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise und WEP sowie weitere Sicherheitsfunktionen wie beispielsweise Deaktivieren von SSID-Broadcasts, MAC-basierte Filterung und Zulassen bzw. Verweigern des tageszeitabhängigen Zugriffs basierend auf der SSID.

Quality of Service

Die Cisco RV110W unterstützt Wi-Fi Multimedia (WMM) und Wi-Fi Multimedia Power Save (WMM-PS) für Quality of Service (QoS).

Außerdem unterstützt die Cisco RV110W 802.1p, Differentiated Services Code Point (DSCP) und Type of Service (ToS) für drahtgebundenes QoS. Dadurch kann die Qualität Ihres Netzwerks verbessert werden, wenn Sie verzögerungsempfindliche VoIP-Anwendungen (Voice over IP) und bandbreitenintensive Videostreaming-Anwendungen verwenden.

Wireless Distribution System

Der WLAN-Zugriffspunkt der Cisco RV110W unterstützt Wireless Distribution System (WDS), sodass die WLAN-Reichweite ohne Kabel erweitert werden kann.

Virtuelle Netzwerke

Die Cisco RV110W unterstützt außerdem mehrere SSIDs (Service Set Identifiers) für die Verwendung in virtuellen Netzwerken (bis zu vier separate virtuelle Netzwerke) mit 802.1Q-basierter VLAN-Unterstützung für die Trennung des Datenverkehrs.

Konfiguration und Verwaltung

Dank des eingebetteten Webservers der Cisco RV110W können Sie die Einstellungen der Cisco RV110W über den browserbasierten Gerätemanager konfigurieren. Der Cisco RV110W unterstützt die Webbrowser Internet Explorer, Firefox und Safari.

Des Weiteren bietet die Cisco RV110W einen Setup-Assistenten, mit dem Sie die Basiseinstellungen der Cisco RV110W einfach und schnell konfigurieren können.

Machen Sie sich vertraut mit der Cisco RV110W

Vorderseite

	**Stromver-sorgung**	Die Betriebs-LED (Netz-LED) leuchtet grün, wenn das Gerät eingeschaltet wird. Beim Einschalten blinkt sie grün.
	**WPS**	Mit der WPS-Taste (Wi-Fi Protected Setup) konfigurieren Sie den WLAN-Zugriff für WPS-fähige Geräte in Ihrem Netzwerk. Weitere Informationen finden Sie unter **Konfigurieren von WPS**.
	**WAN**	Die WAN-LED leuchtet grün, wenn die Cisco RV110W über ein Kabelmodem oder DSL-Modem mit dem Internet verbunden ist. Die LED leuchtet nicht, wenn die Cisco RV110W nicht mit dem Internet verbunden ist. Die LED blinkt grün, wenn Daten gesendet oder empfangen werden.
	**WLAN**	Die Wireless-LED leuchtet grün, wenn das WLAN-Modul aktiviert ist. Wenn die LED nicht leuchtet, ist das WLAN-Modul deaktiviert. Die LED blinkt grün, wenn die Firewall Daten über das WLAN-Modul sendet oder empfängt.
	**LAN-Anschlüsse**	Die nummerierten LEDs entsprechen den LAN-Anschlüssen der Cisco RV110W. Wenn eine LED ununterbrochen grün leuchtet, ist die Cisco RV110W über den entsprechenden Anschluss (1, 2, 3 oder 4) mit einem Gerät verbunden. Die LED eines Anschlusses blinkt grün, wenn die Firewall gerade Daten über diesen Anschluss sendet oder empfängt.

Rückseite

RESET	Wenn Probleme mit der Internetverbindung über die Cisco RV110W bestehen, drücken Sie mit einer Büroklammer oder einem anderen spitzen Gegenstand die **RESET**-Taste mindestens drei, aber maximal zehn Sekunden lang. Die Funktionsweise ist ähnlich wie bei der RESET-Taste am PC, mit der dieser neu gestartet wird. Wenn schwerwiegende Probleme bei der Cisco RV110W vorliegen, obwohl Sie alle Maßnahmen zur Problembehandlung ergriffen haben, halten Sie die **RESET**-Taste länger als 10 Sekunden gedrückt. Dadurch wird das Gerät neu gestartet und auf die Werkseinstellungen zurückgesetzt. Änderungen, die Sie vorher an den Einstellungen der Cisco RV110W vorgenommen haben, gehen dabei verloren.
LAN (1 - 4)	Anschlüsse für LAN-Verbindungen mit Netzwerkgeräten wie PCs, Druckservern oder Switches.
WAN	Der WAN-Anschluss (Internet) ist mit Ihrem Internetgerät verbunden, beispielsweise mit einem Kabelmodem oder DSL-Modem.
POWER	Mit dieser Taste schalten Sie die Cisco RV110W ein und aus.
12VDC	Am 12-V-DC-Anschluss stecken Sie das im Lieferumfang enthaltene 12-V-AC-Netzteil ein.

Installieren des Cisco RV110W

Hinweise zum Aufstellort

- **Umgebungstemperatur**: Damit sich die Firewall nicht überhitzt, betreiben Sie sie nicht in einer Umgebung, in der die Temperatur 40 °C überschreitet.
- **Luftzirkulation**: Achten Sie darauf, dass um den Router herum die Luft ungehindert zirkulieren kann.
- **Mechanische Belastung**: Stellen Sie sicher, dass der Router eben und stabil positioniert ist, um gefährliche Situationen zu vermeiden.

Stellen Sie die Cisco RV110W horizontal auf einer ebenen Oberfläche auf, sodass sie sicher auf ihren Gummifüßen ruht.

Anschließen von Geräten

Für die Konfiguration bei der Inbetriebnahme müssen Sie einen PC über ein Ethernet-Kabel anschließen. Nachdem die anfängliche Konfiguration abgeschlossen ist, können administrative Aufgaben über eine WLAN-Verbindung ausgeführt werden.

SCHRITT 1 Schalten Sie alle Geräte aus, einschließlich des Kabel- oder DSL-Modems, des PCs und des Cisco RV110W.

SCHRITT 2 Ihr PC ist wahrscheinlich bereits mit einem Ethernet-Kabel an das aktuelle Kabelmodem oder DSL-Modem angeschlossen. Ziehen Sie das eine Ende des Kabels vom PC ab, und stecken Sie es in den mit „WAN“ markierten Anschluss des Geräts ein.

SCHRITT 3 Schließen Sie ein Ende eines anderen Ethernet-Kabels an einen der LAN-Anschlüsse auf der Rückseite des Geräts an. (In diesem Beispiel wird der LAN-Anschluss 1 verwendet.) Schließen Sie das andere Ende an einen Ethernet-Anschluss des PCs an, mit dem Sie den webbasierten Setup-Assistenten und den Gerätemanager ausführen möchten.

SCHRITT 4 Schalten Sie das Kabelmodem oder DSL-Modem ein und warten Sie, bis die Verbindung aktiv ist.

SCHRITT 5 Schließen Sie das Netzteil an den Netzanschluss (12VDC) der Cisco RV110W an.

VORSICHT Verwenden Sie ausschließlich das mit dem Gerät gelieferte Netzteil. Das Verwenden eines anderen Netzteils kann zur Beschädigung des Geräts führen.

SCHRITT 6 Stecken Sie den Stecker des Netzteils in eine Steckdose. Unter Umständen benötigen Sie für Ihr Land einen speziellen Stecker (im Lieferumfang enthalten).

SCHRITT 7 Drücken Sie an der Cisco RV110W die **POWER**-Taste, um die Firewall einzuschalten.

Die POWER-LED auf der Vorderseite leuchtet grün, wenn das Netzteil korrekt angeschlossen ist und das Gerät eingeschaltet wird.

Verwenden des Setup-Assistenten

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

So verwenden Sie den Setup-Assistenten:

SCHRITT 1 Starten Sie den Computer, den Sie in Abschnitt **Anschließen von Geräten** unter Schritt 2 an den Anschluss LAN 1 angeschlossen haben.

Der Computer wird zu einem DHCP-Client der Cisco RV110W 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 Cisco RV110W.

Daraufhin wird eine Meldung zum Sicherheitszertifikat der Site angezeigt. Die Cisco RV110W verwendet ein selbst signiertes Sicherheitszertifikat. Diese Meldung wird angezeigt, da der Computer die Cisco RV110W 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.

SCHRITT 4 Wenn die Anmeldeseite angezeigt wird, geben Sie den Benutzernamen und das 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 Cisco RV110W.

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

HINWEIS: Wenn Sie den Setup-Assistenten verwenden, können Sie nur ein WLAN bzw. eine SSID einrichten. Die Cisco RV110W unterstützt bis zu vier WLANs. Wenn Sie zusätzliche WLANs konfigurieren möchten, verwenden Sie den webbasierten Gerätemanager. Weitere Informationen hierzu finden Sie unter **Konfigurieren des WLANs**.

Wenn der Setup-Assistent die Cisco RV110W konfiguriert hat, müssen Sie das Standardkennwort ändern. Wir empfehlen, Kennwortkomplexität zu verwenden (siehe **Festlegen der Kennwortkomplexität**).

Wenn Sie das Standardkennwort geändert haben, wird die Seite **Erste Schritte** angezeigt. Weitere Informationen finden Sie unter **Verwenden der Seite „Erste Schritte“**.

Verwenden der Seite „Erste Schritte“

Auf der Seite **Erste Schritte** werden die am häufigsten anfallenden Konfigurationsaufgaben für die Cisco RV110W angezeigt. Verwenden Sie die Links auf dieser Seite, um zur jeweiligen Konfigurationsseite zu wechseln.

Diese Seite wird standardmäßig angezeigt, wenn Sie den Gerätemanager starten. Sie können dieses Verhalten jedoch ändern, indem Sie unten auf der Seite das Kontrollkästchen **Nicht beim Start anzeigen** aktivieren.

Anfangseinstellungen

Standardmäßiges Administratorkennwort ändern	Klicken Sie auf diese Option, um die Seite **Benutzer** zu öffnen, auf der Sie das Administratorkennwort ändern können. Weitere Informationen hierzu finden Sie unter **Konfigurieren von Benutzerkonten**.
Einrichtungsassistent starten	Klicken Sie auf diese Option, um den Setup-Assistenten zu starten.
WAN-Einstellungen konfigurieren	Klicken Sie auf diese Option, um die Seite **Interneteinrichtung** zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der WAN-Einstellungen**.
Configure LAN Settings	Klicken Sie auf diesen Link, um die Seite **LAN-Konfiguration** zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der LAN-Einstellungen**.

Einstellungen konfigurieren	Klicken Sie auf diese Option, um die Seite **Basiseinstellungen** zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der Basis-WLAN-Einstellungen**.

Schnellzugriff

Router-Firmware-Upgrade durchführen	Klicken Sie auf diese Option, um die Seite **Firmware-/Sprach-Upgrade** zu öffnen. Weitere Informationen hierzu finden Sie unter **Aktualisieren der Firmware oder Ändern der Sprache**.
VPN-Clients hinzufügen	Klicken Sie auf diese Option, um die Seite **VPN-Clients** zu öffnen. Weitere Informationen hierzu finden Sie unter **VPN-Clients**.
Remoteverwaltungszu-griff konfigurieren	Klicken Sie auf diese Option, um die Seite **Basiseinstellungen** zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

Gerätestatus

System Summary	Klicken Sie auf diese Option, um die Seite **Systemübersicht** zu öffnen. Weitere Informationen hierzu finden Sie unter **Anzeigen der Systemzusammenfassung**.
WLAN-Status	Klicken Sie auf diese Option, um die Seite **WLAN-Statistik** zu öffnen. Weitere Informationen hierzu finden Sie unter **Anzeigen der Wireless-Statistik**.
VPN-Status	Klicken Sie auf diese Option, um die Seite **VPN-Status** zu öffnen. 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.

Navigieren durch die Seiten

Verwenden Sie den Navigationsbaum im linken Bereich, um die Konfigurationsseiten zu öffnen.

Klicken Sie im linken Bereich auf ein Menüelement, um dieses zu erweitern. Klicken Sie darunter auf einen Menünamen, um eine Aktion auszuführen oder ein Untermenü anzuzeigen.

Speichern von Änderungen

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

Anzeigen der Hilfedateien

Wenn Sie weitere Informationen zu einer Konfigurationsseite anzeigen möchten, klicken Sie in der rechten oberen Ecke der Seite auf den Link **Hilfe**.

Konfiguration – Nächste Schritte

Obwohl der Setup-Assistent die Cisco RV110W automatisch konfiguriert, sollten Sie einige der Standardeinstellungen ändern, um die Sicherheit und Leistung zu verbessern.

Außerdem müssen Sie möglicherweise einige Einstellungen manuell konfigurieren. Vorgeschlagene Schritte:

1. Ändern Sie den Leerlauf-Timeout-Wert. Standardmäßig werden Sie vom Gerätemanager nach zehn Minuten ohne Aktivität automatisch abgemeldet. Dies kann beim Konfigurieren des Geräts lästig sein. Weitere Informationen hierzu finden Sie unter **Festlegen des Sitzungs-Timeout-Werts**.
2. (Optional) Wenn im Netzwerk bereits ein DHCP-Server vorhanden ist und Sie nicht möchten, dass die Cisco RV110W als DHCP-Server fungiert, lesen Sie **Konfigurieren der LAN-Einstellungen**.
3. Konfigurieren Sie das WLAN, insbesondere die Sicherheitsfunktionen für die WLAN-Datenübermittlung. Weitere Informationen hierzu finden Sie unter **Konfigurieren des WLANs**.
4. Konfigurieren Sie das VPN mithilfe von QuickVPN. Die QuickVPN-Software finden Sie auf der Dokumentations- und Software-CD, die im Lieferumfang der Firewall enthalten ist. Weitere Informationen hierzu finden Sie unter **Verwenden von Cisco QuickVPN**.

Überprüfen der Hardwareinstallation

Gehen Sie wie folgt vor, um die Hardwareinstallation zu überprüfen:

- Überprüfen Sie den Status der LED. Diese werden in **Machen Sie sich vertraut mit der Cisco RV110W** beschrieben.
- 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.
- Konfigurieren Sie ein Gerät für die Verbindung mit dem WLAN und vergewissern Sie sich, dass das WLAN funktionsfähig ist. Weitere Informationen hierzu finden Sie unter **Verbinden von Geräten mit dem WLAN**.

Verbinden von Geräten mit dem WLAN

Um ein Gerät (beispielsweise einen Computer) mit dem WLAN zu verbinden, müssen Sie die WLAN-Verbindung am Gerät mit den Informationen zur WLAN-Sicherheit konfigurieren, die Sie mithilfe des Setup-Assistenten für die Cisco RV110W konfiguriert haben.

Die folgenden Schritte sollen als Beispiel dienen. Möglicherweise müssen Sie Ihr Gerät anders konfigurieren. Anleitungen, die speziell für Ihr Gerät gelten, finden Sie in der Dokumentation für das entsprechende Gerät.

SCHRITT 1 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**. (Die Position 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

Konfigurieren der Netzwerkfunktionen

In diesem Kapitel wird beschrieben, wie Sie die Netzwerkeinstellungen der Cisco RV110W konfigurieren.

- Konfigurieren der WAN-Einstellungen
- Konfigurieren der LAN-Einstellungen
- Klonen der MAC-Adresse
- Konfigurieren von Routing
- Portverwaltung
- Konfigurieren von dynamischem DNS
- Konfigurieren des IP-Modus
- Konfigurieren von IPv6

Konfigurieren der WAN-Einstellungen

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

Konfigurieren der automatischen Konfiguration (DHCP)

Wenn Ihr Internetdienstanbieter DHCP (Dynamic Host Control Protocol) verwendet, um Ihnen eine IP-Adresse zuzuweisen, erhalten Sie eine dynamische IP-Adresse, die bei jeder Anmeldung neu 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 (Optional) Informationen zum Konfigurieren der optionalen Einstellungen finden Sie unter **Konfigurieren der optionalen Einstellungen**.

SCHRITT 4 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	Geben Sie die IP-Adresse des WAN-Anschlusses ein.
Subnetzmaske	Geben Sie die Subnetzmaske des WAN-Anschlusses ein.
Standard-Gateway	Geben Sie die IP-Adresse des Standard-Gateways ein.
Statisches DNS 1	Geben Sie die IP-Adresse des primären DNS-Servers ein.
Statisches DNS 2	Geben Sie die IP-Adresse des sekundären DNS-Servers ein.

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

SCHRITT 5 Klicken Sie auf **Speichern**.

Konfigurieren von PPPoE

So konfigurieren Sie die PPPoE-Einstellungen:

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 Internetdienstanbieter nach den PPPoE-Anmeldeinformationen fragen):

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.
Aufrechterhalten	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Cisco RV110W versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus: **Automatisch Aushandlung**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Dann sendet die Cisco RV110W Anmeldeinformationen mit dem vorher vom Server gesendeten Sicherheitstyp zurück. **PAP**: Die Cisco RV110W verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Die Cisco RV110W verwendet zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol). **MS-CHAP oder MS-CHAPv2**: Die Cisco RV110W 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 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	Geben Sie die IP-Adresse des WAN-Anschlusses ein.
Subnetzmaske	Geben Sie die Subnetzmaske des WAN-Anschlusses ein.

Standard-Gateway	Geben Sie die IP-Adresse des Standard-Gateways ein.
PPTP-Server	Geben Sie die IP-Adresse des PPTP-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.
Aufrechterhalten	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Cisco RV110W versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus: **Automatisch Aushandlung**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Dann sendet die Cisco RV110W Anmeldeinformationen mit dem vorher vom Server gesendeten Sicherheitstyp zurück. **PAP**: Die Cisco RV110W verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Die Cisco RV110W verwendet zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol). **MS-CHAP oder MS-CHAPv2**: Die Cisco RV110W 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.

Standard-Gateway	Geben Sie die IP-Adresse des Standard-Gateways 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.
Aufrechterhalten	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Cisco RV110W versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungstyp	Wählen Sie den Authentifizierungstyp aus: **Automatisch Aushandlung**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Dann sendet die Cisco RV110W Anmeldeinformationen mit dem vorher vom Server gesendeten Sicherheitstyp zurück. **PAP**: Die Cisco RV110W verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Die Cisco RV110W verwendet zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol). **MS-CHAP oder MS-CHAPv2**: Die Cisco RV110W 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 der optionalen Einstellungen

So konfigurieren Sie die optionalen Einstellungen:

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

Hostname	Geben Sie den Hostnamen der Cisco RV110W ein.
Domänenname	Geben Sie den Domänennamen für Ihr Netzwerk ein.

MTU	Bei der MTU (Maximum Transmit 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 Internetdienstanbieter nichts anderes verlangt wird, sollten Sie **Autom.** 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	Geben Sie die MTU-Größe ein.

SCHRITT 2 Klicken Sie auf **„Speichern“**.

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 PCs 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 Cisco RV110W schließt die IP-Adresse des WINS-Servers in die DHCP-Konfiguration ein, die von der Cisco RV110W an DHCP-Clients gesendet wird.

HINWEIS Wenn die Cisco RV110W mit einem Modem oder Gerät verbunden ist, für das ein Netzwerk im gleichen Subnetz (192.168.1.x) konfiguriert ist, ändert die Cisco RV110W 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 Cisco RV110W entsteht.

Sie können jedem Subnetz der Cisco RV110W eine IP-Adresse zuweisen.

Ändern der Standard-IP-Adresse der Cisco RV110W

So konfigurieren Sie die Standard-LAN-IP-Adresse der Cisco RV110W:

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

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

VLAN	Wählen Sie im Dropdown-Menü die VLAN-Nummer aus.
Lokale IP-Adresse	Geben Sie die LAN-IP-Adresse der Cisco RV110W ein. Stellen Sie sicher, dass die Adresse nicht von einem anderen Gerät verwendet wird.
Subnetzmaske	Wählen Sie im Dropdown-Menü die Subnetzmaske für die neue IP-Adresse aus. Das Standardsubnetz lautet 255.255.255.0.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Wenn Sie die LAN-IP-Adresse der Cisco RV110W geändert haben, ist der PC nicht mehr mit der Cisco RV110W verbunden.

SCHRITT 4 Führen Sie einen der folgenden Schritte aus, um den PC wieder mit der Cisco RV110W zu verbinden:

- Wenn DHCP in der Cisco RV110W 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 Subnetz befinden wie der Cisco RV110W. Wenn Sie beispielsweise die IP-Adresse der Cisco RV110W 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.

SCHRITT 5 Öffnen Sie ein neues Browserfenster, und geben Sie die neue IP-Adresse der Cisco RV110W ein, um die Verbindung wiederherzustellen.

Konfigurieren von DHCP

Die Cisco RV110W fungiert standardmäßig als DHCP-Server für die Hosts im WLAN (Wireless LAN) oder LAN, weist IP-Adressen zu und stellt DNS-Serveradressen bereit.

Wenn DHCP aktiviert ist, dient die IP-Adresse der Cisco RV110W als Gateway-Adresse für Ihr LAN. Die Cisco RV110W weist den Netzwerkgeräten im LAN IP-Adressen aus einem Adressenpool zu. Die Cisco RV110W testet jede Adresse vor der Zuweisung, um doppelte Adressen im LAN zu vermeiden.

Standardmäßig weist die Cisco RV110W jedem Host im LAN eine IP-Adresse aus dem standardmäßigen IP-Adressenpool zu (192.168.1.100 bis 192.168.1.149). Wenn Sie für einen Host eine statische IP-Adresse festlegen müssen, verwenden Sie eine IP-Adresse aus dem Adressenpool 192.168.1.2 bis 192.168.1.99. Dadurch vermeiden Sie Konflikte mit dem standardmäßigen IP-Adressenpool.

So konfigurieren Sie die DHCP-Einstellungen:

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

SCHRITT 2 (Optional) Wählen Sie in der Dropdown-Liste das zu bearbeitende VLAN aus.

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

Aktivieren	Klicken Sie auf diese Schaltfläche, um zuzulassen, dass die Cisco RV110W im Netzwerk als DHCP-Server fungiert.
Deaktivieren	Klicken Sie auf diese Schaltfläche, um DHCP in der Cisco RV110W zu deaktivieren. Wenn Sie ein anderes Gerät im Netzwerk als DHCP-Server verwenden möchten oder die Netzwerkeinstellungen aller PCs manuell konfigurieren möchten, deaktivieren Sie DHCP.
DHCP-Relais	Klicken Sie auf diese Schaltfläche, um das **DHCP-Relais** auszuwählen und die Cisco RV110W so zu konfigurieren, dass sie als Relais für IP-Adressen eines anderen DHCP-Servers fungiert.

SCHRITT 4 Wenn Sie **Aktivieren** ausgewählt haben, geben Sie diese Informationen ein:

IP-Startadresse	Geben Sie die erste Adresse aus dem IP-Adressenpool ein. Jedem neuen DHCP-Client, der dem LAN beitritt, wird eine IP-Adresse in diesem Bereich zugewiesen (die letzte IP-Adresse im Pool wird durch den Wert bestimmt, den Sie in das Feld **Maximale Anzahl an DHCP-Benutzern** eingeben).
Maximale Anzahl an DHCP-Benutzern	Geben Sie die maximale Anzahl an DHCP-Clients ein.
IP-Adressbereich	(Schreibgeschützt) Zeigt den Bereich der IP-Adressen an, die für die DHCP-Clients zur Verfügung stehen.
Client-Lease-Zeit	Geben Sie die Dauer (in Stunden) ein, während der IP-Adressen an Clients vergeben werden.
Statisches DNS 1	Geben Sie die IP-Adresse des primären DNS-Servers ein.
Statisches DNS 2	Geben Sie die IP-Adresse des sekundären DNS-Servers ein.
Statisches DNS 3	Geben Sie die IP-Adresse des tertiären DNS-Servers ein.
WINS	Geben Sie die IP-Adresse des primären WINS-Servers ein.

SCHRITT 5 Wenn Sie **DHCP-Relais** ausgewählt haben, geben Sie die Adresse des Relais-Gateways in das Feld **Remote-DHCP-Server** ein. Das Relais-Gateway überträgt DHCP-Nachrichten zwischen mehreren Subnetzen.

SCHRITT 6 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.

Die Cisco RV110W hat ein Standard-VLAN (VLAN 1), das Sie nicht bearbeiten oder ändern können. Sie können in der Cisco RV110W 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	Geben Sie die numerische VLAN-ID ein, die Endpunkten in der VLAN-Mitgliedschaft zugewiesen werden soll. Sie müssen eine Zahl zwischen 3 und 4094 eingeben. VLAN-ID 1 ist für das Standard-VLAN reserviert, das für an der Schnittstelle empfangene Frames ohne Tag verwendet wird. Die VLAN-IDs 1 und 2 sind reserviert und können nicht verwendet werden.
Beschreibung	Geben Sie eine Beschreibung ein, um das VLAN zu identifizieren.

Anschluss 1 **Anschluss 2** **Anschluss 3** **Anschluss 4**	Sie können VLANs in der Cisco RV110W den LAN-Anschlüssen am Gerät zuordnen. Standardmäßig gehören alle vier Anschlüsse zu VLAN 1. Sie können diese Anschlüsse bearbeiten, um sie anderen VANS zuzuordnen. Wählen Sie für jeden Anschluss den Typ der ausgehenden Frames aus: **Ohne Tag**: Die Schnittstelle gehört dem VLAN als Mitglied ohne Tag an. Frames des VLANs werden ohne Tag an das Anschluss-VLAN gesendet. **Mit Tag**: 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 Cisco RV110W 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	Geben Sie eine Beschreibung des Clients ein.
IP-Adresse	Geben Sie die IP-Adresse des Geräts ein. Die zugewiesene IP-Adresse sollte nicht zum Pool der konfigurierten DHCP-Adressen gehören. Da der DHCP-Pool als allgemeiner Pool behandelt wird, sollte keine reservierte IP-Adresse zu diesem Pool gehören. Bei der statischen DHCP-Zuweisung weist der DHCP-Server der definierten MAC-Adresse bei jeder Verbindung des Geräts mit dem Netzwerk die gleiche IP-Adresse zu. Der DHCP-Server stellt die reservierte IP-Adresse bereit, wenn das Gerät mit der entsprechenden MAC-Adresse eine IP-Adresse anfordert.
MAC-Adresse	Geben Sie die MAC-Adresse des Geräts ein. Das Format der MAC-Adresse lautet XX:XX:XX:XX:XX:XX. Dabei ist „X“ eine Zahl zwischen 0 und 9 (einschließlich) oder ein Buchstabe des Alphabets 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 Cisco RV110W 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 in der Cisco RV110W weist dann immer die angezeigte IP-Adresse zu, wenn das Gerät eine IP-Adresse anfordert.

Konfigurieren eines DMZ-Hosts

Die Cisco RV110W 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 ebenfalls 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 Cisco RV110W. 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 Cisco RV110W 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 Cisco RV110W bestimmt den Pfadwert automatisch). Sie können auch eine Zahl von 2 bis 200000000 eingeben.

SCHRITT 4 Klicken Sie auf **„Speichern“**.

Portverwaltung

Sie können die Einstellungen für die Geschwindigkeit und die Flusssteuerung der vier LAN-Anschlüsse der Cisco RV110W konfigurieren.

So konfigurieren Sie die Anschlussgeschwindigkeit und die Flusssteuerung::

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

SCHRITT 2 Konfigurieren Sie diese Informationen:

Anschluss	Port-Nummer.
Leitung	Port-Geschwindigkeit. Wenn kein Gerät mit dem Anschluss verbunden ist, wird in diesem Feld **Nicht genutzt** angezeigt.
Mode	Wählen Sie im Dropdown-Menü eine der folgenden Anschlussgeschwindigkeiten aus: ▪ **Autom. Aushandlung**: Die Cisco RV110W und das verbundene Gerät wählen eine gemeinsame Geschwindigkeit aus. ▪ **10 MBit/s Halb**: 10 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. ▪ **10 MBit/s Voll**: 10 MBit/s in beide Richtungen gleichzeitig. ▪ **100 MBit/s Halb**: 100 MBit/s in beide Richtungen, aber nur jeweils eine Richtung. ▪ **100 MBit/s Voll**: 100 MBit/s in beide Richtungen gleichzeitig.

Flusssteuerung	Aktivieren Sie dieses Kontrollkästchen, um die Flusssteuerung für diesen Anschluss zu aktivieren. Flusssteuerung 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 Cisco RV110W 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 Cisco RV110W vom ISP nicht erkannt.

In diesem Fall können Sie die Cisco RV110W so konfigurieren, dass sie vom Internetdienstanbieter 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 Cisco RV110W 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 Cisco RV110W:

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 Cisco RV110W als Gateway dient. Behalten Sie diese Standardeinstellung bei, wenn die Cisco RV110W 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 Cisco RV110W als Router dient. Wählen Sie diese Option aus, wenn sich die Cisco RV110W in einem Netzwerk mit anderen Routern befindet. Durch das Aktivieren des Routermodus wird NAT (Network Address Translation) in der Cisco RV110W 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 Cisco RV110W 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 Cisco RV110W 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 Cisco RV110W die Weiterleitung von Verkehr mithilfe von RIP.
Version der RIP Send-Pakete	Wählen Sie die Version für RIP Send-Pakete (**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 der RIP Recv-Pakete	Wählen Sie die Version für RIP Recv-Pakete 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 vorgegebener Pfad, den ein Paket verwenden 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 werden keine CPU-Ressourcen benötigt, um Routing-Informationen mit einem Peer-Router auszutauschen.

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 Cisco RV110W 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**: Klicken Sie auf diese Schaltfläche, um Pakete an das Internet (WAN) zu leiten.

SCHRITT 4 Klicken Sie auf **„Speichern“**.

Konfigurieren von Inter-VLAN-Routing

Aktivieren Sie das Kontrollkästchen „Inter-VLAN-Routing“, um das Routing zwischen den verschiedenen VLANs in der Cisco RV110W zu aktivieren.

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** > **Dynamic 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	Geben Sie das Kennwort des DDNS-Kontos ein.
Kennwort bestätigen	(TZO.com, DynDNS.com und noip.com) Geben Sie erneut das Kennwort des DDNS-Kontos ein.
Hostname	(DynDNS.com, 3322.org und noip.com) Geben Sie den Hostnamen des DDNS-Servers ein.
Domänenname	(TZO.com) Geben Sie den Namen der Domäne ein, die für den Zugriff auf das Netzwerk verwendet wird.
WAN-IP-Adresse	(Schreibgeschützt) Die Internet-IP-Adresse der Cisco RV110W.
Status	(Schreibgeschützt) Der Status wird angezeigt, wenn die DDNS-Aktualisierung erfolgreich abgeschlossen wurde oder wenn 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	Wählen Sie diese Option aus, um IPv4 an den LAN- und WAN-Anschlüssen zu verwenden.
LAN: IPv6, WAN: IPv4	Wählen Sie diese Option aus, um IPv6 an den LAN-Anschlüssen und IPv4 an den WAN-Anschlüssen zu verwenden.
LAN: IPv6, WAN: IPv6	Wählen Sie diese Option aus, um IPv6 an den LAN- und WAN-Anschlüssen zu verwenden.
LAN: IPv4 + IPv6, WAN: IPv4	Wählen Sie diese Option aus, um IPv4 und IPv6 an den LAN-Anschlüssen und IPv4 an den WAN-Anschlüssen zu verwenden.
LAN: IPv4 + IPv6, WAN: IPv4 + IPv6	Wählen Sie diese Option aus, um IPv4 und IPv6 an den LAN- und WAN-Anschlüssen zu verwenden.
LAN: IPv4, WAN: IPv6	Wählen Sie diese Option aus, um IPv4 an den LAN-Anschlüssen und IPv6 an den WAN-Anschlüssen zu verwenden.

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 des WANs für ein IPv6-Netzwerk

Sie können die Cisco RV110W als DHCPv6-Client des ISPs für dieses WAN konfigurieren oder eine vom ISP bereitgestellte statische IPv6-Adresse verwenden.

Festlegen des IP-Modus

Zum Konfigurieren der IPv6-WAN-Einstellungen der Cisco RV110W müssen Sie zuerst den IP-Modus auf „LAN: IPv6, WAN: IPv6“ oder „LAN: IPv4 + IPv6, WAN: IPv4 + IPv6“ festlegen.

Weitere Informationen finden Sie unter **Konfigurieren des IP-Modus**.

Konfigurieren von DHCPv6

Wenn Ihnen der Internetdienstanbieter eine dynamisch zugewiesene Adresse bereitstellt, konfigurieren Sie die Cisco RV110W für die Verwendung als DHCPv6-Client.

So konfigurieren Sie die Cisco RV110W 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 WAN-IP-Adresse

Wenn Ihnen der Internetdienstanbieter eine feste Adresse für den Zugriff auf das Internet zuweist, konfigurieren Sie die Cisco RV110W für die Verwendung einer statischen IPv6-Adresse.

So konfigurieren Sie die Cisco RV110W für die Verwendung einer statischen IPv6-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 Address	Geben Sie die IPv6-Adresse des WAN-Anschlusses ein.
IPv6-Präfix-Länge	Geben Sie die vom Internetdienstanbieter definierte IPv6-Präfixlänge ein. Das IPv6-Netzwerk (Subnetz) wird anhand der ersten Bits der Adresse identifiziert, die als Präfix bezeichnet werden. So ist beispielsweise in der IP-Adresse 2001:0DB8:AC10:FE01:: 2001 das Präfix. 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.
Standard-IPv6-Gateway	Geben Sie die IPv6-Adresse des Standard-Gateways ein. Dies ist die IP-Adresse des Servers beim Internetdienstanbieter, mit dem der Router eine Verbindung herstellt, um auf das Internet zuzugreifen.
Statisches DNS 1	Geben Sie die IP-Adresse des primären DNS-Servers im IPv6-Netzwerk des Internetdienstanbieters ein.
Statisches DNS 2	Geben Sie die IP-Adresse des sekundären DNS-Servers im IPv6-Netzwerk des Internetdienstanbieters ein.

SCHRITT 4 Klicken Sie auf **„Speichern“**.

Konfigurieren der PPPoE-Einstellungen unter IPv6

Wenn Sie sich für diese Option entscheiden, müssen die IPv6 WAN PPPoE-Einstellungen mit den IPv4 WAN PPPoE-Einstellungen übereinstimmen. Weitere Informationen hierzu finden Sie unter **Konfigurieren von PPPoE**.

So konfigurieren Sie die PPPoE IPv6-Einstellungen der Cisco RV110W:

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 Internetdienstanbieter nach den PPPoE-Anmeldeinformationen fragen):

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.
Aufrechterhalten	Wenn Sie diese Option auswählen, ist die Internetverbindung immer aktiv. Geben Sie in das Feld „Zeit bis Neueinwahl“ ein, nach wie vielen Sekunden die Cisco RV110W versuchen soll, eine getrennte Verbindung wiederherzustellen.

Authentifizierungs-typ	Wählen Sie den Authentifizierungstyp aus: **Automatisch Aushandlung**: Der Server sendet eine Konfigurationsanforderung, in der der festgelegte Sicherheitsalgorithmus angegeben ist. Dann sendet die Cisco RV110W Anmeldeinformationen mit dem vorher vom Server gesendeten Sicherheitstyp zurück. **PAP**: Die Cisco RV110W verwendet PAP (Password Authentication Protocol) zum Herstellen der Verbindung mit dem ISP. **CHAP**: Die Cisco RV110W verwendet zum Herstellen der Verbindung mit dem ISP CHAP (Challenge Handshake Authentication Protocol). **MS-CHAP oder MS-CHAPv2**: Die Cisco RV110W verwendet das Microsoft Challenge Handshake Authentication-Protokoll zum Herstellen der Verbindung mit dem ISP.
Dienstname	Möglicherweise hat Ihr Internetdienstanbieter einen Servicenamen konfiguriert, der zum Anmelden beim PPPoE-Server erforderlich ist. Wenn dies der Fall ist, geben Sie den Servicenamen hier ein.
MTU	Bei der MTU (Maximum Transmit 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 Internetdienstanbieter nichts anderes verlangt wird, sollten Sie **Autom.** 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	Geben Sie die MTU-Größe ein.

Adressmodus	Wählen Sie aus, ob der Modus für dynamische Adressen oder der Modus für statische Adressen verwendet werden soll. Wenn Sie *Dynamisch* auswählen, geben Sie im nachfolgenden Feld die IPv6-Adresse ein.
IPv6-Präfix-Länge	Wenn Sie als Adressmodus *Statisch* ausgewählt haben, geben Sie in diesem Feld die Länge des IPv6-Präfixes ein.
Standard-IPv6-Gateway	Geben Sie die IP-Adresse des Standard-IPv6-Gateways ein.
Statisches DNS 1	Wenn Sie als Adressmodus *Statisch* ausgewählt haben, geben Sie in diesem Feld die IP-Adresse des primären DNS-Servers ein.
Statisches DNS 2	Wenn Sie als Adressmodus *Statisch* ausgewählt haben, geben Sie in diesem Feld die IP-Adresse des sekundären DNS-Servers ein.

SCHRITT 4 Klicken Sie auf **„Speichern“**.

Konfigurieren der IPv6-LAN-Einstellungen

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.

Festlegen des IP-Modus

Zum Konfigurieren der IPv6-LAN-Einstellungen in der Cisco RV110W 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

Weitere Informationen finden Sie unter **Konfigurieren des IP-Modus**.

Konfigurieren einer statischen LAN-IP-Adresse

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 Address	Geben Sie die IPv6-Adresse der Cisco RV110W 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-Präfix-Länge	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“**.

Konfigurieren der DHCPv6-Einstellungen

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 DHCPv6-Einstellungen zu konfigurieren:

DHCP-Status	Aktivieren Sie dieses Kontrollkästchen, um den DHCPv6-Server zu aktivieren. Wenn diese Funktion aktiviert ist, weist der Cisco RV110W jedem LAN-Endpunkt, der über DHCP bereitgestellte Adressen anfordert, eine IP-Adresse innerhalb des angegebenen Bereichs sowie zusätzliche angegebene Informationen zu.
Domänenname	(Optional) Geben Sie den Domänennamen des DHCPv6-Servers ein.
Serverpriorität	Geben Sie die Servervoreinstellungsebene dieses DHCP-Servers ein. DHCP-Ankündigungsnachrichten mit dem höchsten Servervoreinstellungswert an einen LAN-Host werden gegenüber anderen DHCP-Serverankündigungsnachrichten bevorzugt. Der Standardwert lautet „255“.
Statisches DNS 1	Geben Sie die IPv6-Adresse des primären DNS-Servers im IPv6-Netzwerk des Internetdienstanbieters ein.
Statisches DNS 2	Geben Sie die IPv6-Adresse des sekundären DNS-Servers im IPv6-Netzwerk des Internetdienstanbieters ein.
Client-Lease-Dauer	Geben Sie die Client-Lease-Zeit ein. Geben Sie die Dauer (in Stunden) ein, während der IPv6-Adressen an Endpunkte im LAN vergeben werden.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Konfigurieren von IPv6-Adressenpools

Sie können das IPv6-Delegationspräfix für einen Bereich von IPv6-Adressen definieren, die vom DHCPv6-Server der Cisco RV110W bereitgestellt werden sollen.

Mithilfe eines Delegationspräfixes können Sie den Vorgang automatisieren, mit dem andere Netzwerkgeräte im LAN spezifische DHCP-Informationen für das zugewiesene Präfix erhalten.

So konfigurieren Sie IPv6-Adressenpools:

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

SCHRITT 2 Klicken Sie in der **Tabelle für IPv6-Adressenpools** auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

Startadresse	Geben Sie die erste IPv6-Adresse des Pools ein.
Endadresse	Geben Sie die letzte IPv6-Adresse des Pools ein.
IPv6-Präfix-Länge	Geben Sie die Präfixlänge ein. Dieses Feld bestimmt die Anzahl der gemeinsamen Anfangs-Bits in den Netzwerkadressen.

SCHRITT 4 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 erfordern für die Erstellung der Routing-Tabelle statische Routen anstelle dynamischer Routing-Protokolle. Bei statischen Routen werden keine CPU-Ressourcen benötigt, um Routing-Informationen mit einem Peer-Router auszutauschen.

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	Geben Sie den Namen der Route ein.
Ziel	Geben Sie die IPv6-Adresse des Zielhosts oder -netzwerks für diese Route ein.
Präfixlänge	Geben Sie die Anzahl der Präfix-Bits in der IPv6-Adresse ein, die das Zielsubnetz definieren.
Gateway	Geben Sie die IPv6-Adresse des Gateways ein, über das der Zielhost bzw. das Zielnetzwerk erreicht werden kann.
Schnittstelle	Wählen Sie im Dropdown-Menü die Schnittstelle für die Route aus: **LAN**, **WAN** oder **6to4**.
Metrik	Geben Sie die Priorität der Route ein, indem Sie einen Wert zwischen 2 und 15 auswählen. Wenn mehrere Routen zum gleichen 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 von der Cisco RV110W verwendet. Sie können die Route jederzeit später aktivieren. Diese Funktion ist hilfreich, wenn das Netzwerk, mit dem die Route eine Verbindung herstellt, beim Hinzufügen der Route nicht verfügbar ist. 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 Cisco RV110W 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

6to4-Tunneling

IPv6-to-IPv4-Tunneling (6to4-Tunneling) ermöglicht die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk. 6-to-4-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 6-to-4-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-Präfix-Länge**
- **Border Relay**
- **IPv4-Maskenlänge**

SCHRITT 6 Klicken Sie auf **„Speichern“**.

4to6-Tunneling

IPv4-to-IPv6-Tunneling (4to6-Tunneling) ermöglicht die Übertragung von IPv4-Paketen über ein IPv6-Netzwerk. 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 Cisco RV110W 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 Cisco RV110W 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 Cisco RV110W 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**: Wählen Sie diesen Modus aus, um Router-Anzeigen (Router Advertisements, RAs) an alle Schnittstellen zu senden, die zur Multicast-Gruppe gehören. **Nur Unicast**: Wählen Sie diesen Modus aus, um Anzeigen auf allgemein bekannte IPv6-Adressen zu beschränken (RAs werden nur an die Schnittstelle gesendet, die zur bekannten Adresse gehört).
Anzeigeintervall	Wenn Sie **Unaufgefordertes Multicast** als Anzeigemodus ausgewählt haben, geben Sie das Anzeigeintervall ein (4–1800). Der Standardwert beträgt **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-Kennzeichen	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 Routerpriorität implementieren. Die Funktion ist hilfreich, wenn im LAN andere RADVD-fähige Geräte vorhanden sind.
MTU	Geben Sie die MTU-Größe ein (0 oder 1280 bis 1500). Der Standardwert lautet **1500** Byte. Bei der MTU-Größe 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-Lebensdauer	Geben Sie den Router-Lebensdauerwert ein oder die Zeit in Sekunden, während der die Anzeigenachrichten in der Route vorhanden sind. Der Standardwert beträgt **3600** Sekunden.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Konfigurieren von Ankündigungspräfixen

So konfigurieren Sie die verfügbaren RADVD-Präfixe:

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

SCHRITT 2 Klicken Sie auf **Hinzufügen**.

SCHRITT 3 Geben Sie folgende Informationen ein:

IPv6-Präfixtyp	Wählen Sie eine der folgenden Typen aus: Schnittstelle für die Route aus: **6to4**: 6to4 ist ein System, das die Übertragung von IPv6-Paketen über ein IPv4-Netzwerk ermöglicht. 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-Präfix-Länge	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	Geben Sie die Präfixgültigkeitsdauer ein oder den Zeitraum, in dem der anfordernde Router das Präfix verwenden darf.

SCHRITT 4 Klicken Sie auf **„Speichern“**.

3

Konfigurieren des WLANs

In diesem Kapitel wird beschrieben, wie Sie das Wireless-Netzwerk der Cisco RV110W konfigurieren.

- **Sicherheitsfunktionen bei der WLAN-Datenübermittlung**
- **WLANs der Cisco RV110W**
- **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.

WLANs der Cisco RV110W

Die Cisco RV110W 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
Sicherheitsmodus	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-Hardwaretaste	Aktiviert	Deaktiviert	Deaktiviert	Deaktiviert

1. Wählen Sie beim Verwenden des Setup-Assistenten die Option **Beste Sicherheit** oder **Bessere Sicherheit** aus, um die Cisco RV110W 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 **Frequenzband** 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 **Kanal** im Dropdown-Menü den Kanal aus.

SCHRITT 6 Wählen Sie im Feld **VLAN für die Zugriffspunktverwaltung** 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 Cisco RV110W 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 Cisco RV110W 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-Übertragung	Aktivieren Sie dieses Kontrollkästchen, um die Übertragung der SSID zu aktivieren. Wenn die SSID-Übertragung 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 Cisco RV110W 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 knacken ist. Wir empfehlen 128-Bit-Verschlüsselung.

SCHRITT 7 (Optional) Geben Sie in das Feld **Passphrase** einen alphanumerischen Begriff ein (optimale Sicherheit erreichen Sie mit mehr als acht Zeichen) und klicken Sie auf **Schlüssel generieren**, um in den WEP-Schlüsselfeldern darunter 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 eine alphanumerische Passphrase handelt, die mit dem WLAN-Peer ausgetauscht wird.

So konfigurieren Sie den Sicherheitsmodus WPA-Personal:

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** 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 in das Feld **Gemeinsamer Schlüssel** einen alphanumerischen Begriff (8 bis 63 ASCII-Zeichen oder 64 hexadezimale Ziffern) 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** in 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 Cisco RV110W 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 Cisco RV110W kann ein Gastnetzwerk konfiguriert werden.
- Das Gastnetzwerk wird als eine der vier verfügbaren SSIDs in der Cisco RV110W 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 **Mit Tag** 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-Übertragung*, 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 Cisco RV110W 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 „Bandbreitenverwaltung“.) 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 Cisco RV110W 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 Cisco RV110W 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 Cisco RV110W auch N-Geschwindigkeiten. Als weitere Optionen stehen 1-2 MBit/s für die Verwendung mit älteren WLAN-Technologien zur Verfügung sowie „Alle“, wenn die Cisco RV110W mit allen WLAN-Raten übertragen kann. Die Basisrate entspricht nicht der Rate, mit der Daten tatsächlich übertragen werden. Wenn Sie die Datenübertragungsrate der Cisco RV110W 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 Cisco RV110W automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen der Cisco RV110W und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.

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 Cisco RV110W 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 Cisco RV110W 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 Cisco RV110W auch N-Geschwindigkeiten. Als weitere Optionen stehen 1-2 MBit/s für die Verwendung mit älteren WLAN-Technologien zur Verfügung sowie „Alle“, wenn die Cisco RV110W mit allen WLAN-Raten übertragen kann. Die Basisrate entspricht nicht der Rate, mit der Daten tatsächlich übertragen werden. Wenn Sie die Datenübertragungsrate der Cisco RV110W 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 Cisco RV110W automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen der Cisco RV110W 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 Cisco RV110W automatisch die schnellstmögliche Datenrate verwendet und die Funktion für automatisches Fallback aktiviert. Beim automatischen Fallback wird die höchstmögliche Verbindungsgeschwindigkeit zwischen der Cisco RV110W und einem WLAN-Client ausgehandelt. Der Standardwert lautet „Automatisch“.
CTS-Schutzmodus	Die Cisco RV110W 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 Cisco RV110W übertragen können. Diese Funktion optimiert Wireless-N- und Wireless-G-Übertragungen über die Cisco RV110W, führt jedoch zu einer spürbaren Beeinträchtigung der Leistung. Der Standardwert lautet „Automatisch“.
Beacon Interval	Der Wert für das Beacon-Intervall gibt das Häufigkeitsintervall des Beacons an. Ein Beacon ist ein Paket, das von der Cisco RV110W 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 Cisco RV110W 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“.

Fragmentation Threshold	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 Threshold	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 Cisco RV110W und sonstige WDS-Remote-Peers mit dem gleichen WLAN-Modus, dem gleichen WLAN-Kanal, der gleichen WLAN-Band-Auswahl und den gleichen Verschlüsselungstypen („Keine“ und „WEP“) konfigurieren.

HINWEIS WDS wird nur für eine SSID unterstützt.

So konfigurieren Sie WDS:

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

SCHRITT 2 Aktivieren Sie das Kontrollkästchen **Wiederholung des Wireless-Signals durch einen Repeater zulassen**, um WDS zu aktivieren.

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

SCHRITT 4 (Optional) Klicken Sie auf die Schaltfläche **Standortbefragung anzeigen**.

In der daraufhin angezeigten **Tabelle verfügbarer Netzwerke** werden die verfügbaren WLAN-Zugriffspunkte aufgelistet.

a. (Optional) Klicken Sie auf die Schaltfläche **Aktualisieren**, um die Einträge in der Tabelle zu aktualisieren.

b. Wählen Sie in der **Tabelle verfügbarer Netzwerke** maximal drei Zugriffspunkte aus, um diese als Repeater zu verwenden.

c. Klicken Sie auf **Verbinden**, um die MAC-Adressen der ausgewählten Zugriffspunkte den MAC-Feldern unter der Tabelle hinzuzufügen.

SCHRITT 5 Wenn Sie auf die Schaltfläche **Manuell** geklickt haben, geben Sie in die Felder **MAC 1**, **MAC 2** und **MAC 3** die MAC-Adressen von maximal drei Zugriffspunkten ein, um diese als Repeater zu verwenden.

SCHRITT 6 Klicken Sie auf **„Speichern“**.

Konfigurieren von WPS

Sie können in der Cisco RV110W WPS konfigurieren, damit WPS-fähige Geräte leichter Verbindungen mit dem WLAN herstellen können.

So konfigurieren Sie WPS für Clientgeräte:

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 im Feld **WPS** das Kontrollkästchen **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:

- WPS-Methode 1
- WPS-Methode 2
- WPS-Methode 3

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

WPS-Methode 1

Verwenden Sie diese Methode, wenn das Clientgerät eine WPS-Taste hat.

SCHRITT 1 Drücken Sie die WPS-Taste am Clientgerät.

SCHRITT 2 Klicken Sie auf der Seite **WPS** auf die Schaltfläche **WPS**. Nach Abschluss der WPS-Konfiguration wird ein Dialogfeld angezeigt.

SCHRITT 3 Klicken Sie auf **„OK“**.

Weitere Anweisungen zum Einrichten Ihres Clientgeräts finden Sie in der Dokumentation zum jeweiligen Clientgerät.

WPS-Methode 2

Verwenden Sie diese Methode, wenn das Clientgerät eine WPS-PIN hat.

SCHRITT 1 Geben Sie auf der Seite **WPS** die PIN in das entsprechende Feld ein.

SCHRITT 2 Klicken Sie auf **Registrieren**.

SCHRITT 3 Klicken Sie nach Abschluss der Konfiguration auf **OK**.

Weitere Anweisungen zum Einrichten Ihres Clientgeräts finden Sie in der Dokumentation zum jeweiligen Clientgerät.

WPS-Methode 3

Wenn für das Clientgerät eine PIN vom Router erforderlich ist, verwenden Sie die unter Punkt 3 auf der Seite **WPS** genannte Nummer.

4

Konfigurieren der Firewall

In diesem Kapitel wird beschrieben, wie Sie die Firewalleigenschaften der RV110W konfigurieren.

- **Firewallfunktionen Cisco RV110W**
- **Konfigurieren der grundlegenden Firewalleinstellungen**
- **Verwalten von Firewallzeitplänen**
- **Konfigurieren der Serviceverwaltung**
- **Konfigurieren von Zugriffsregeln**
- **Erstellen einer Internetzugriffsrichtlinie**
- **Konfigurieren der Anschlussweiterleitung**

Firewallfunktionen Cisco RV110W

Sie können Ihr Netzwerk schützen, indem Sie Regeln erstellen und anwenden, die von der Cisco RV110W 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 die Cisco RV110W können Sie die IP-Adresse verwenden, wenn dem WAN-Anschluss eine statische Adresse zugewiesen ist. Bei einer dynamischen WAN-Adresse kann ein DDNS-Name (Dynamic DNS) 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	Blockiert Ping-Anforderungen an die Cisco RV110W über das WAN.
Webzugriff	Wählen Sie den Typ des Webzugriffs aus, der für Verbindungen mit der Firewall verwendet werden kann: HTTP oder HTTPS (sicheres HTTP).
Remoteverwaltung **Remotezugriff** **Remote-Upgrade** **Zulässige Remote-IP-Adresse** **Remoteverwaltungsan-schluss**	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 **Konfigurieren durch Benutzer zulassen** **Deaktivierung des Internetzugriffs durch Benutzer zulassen**	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.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Konfigurieren der Remoteverwaltung

Sie können die Remoteverwaltung aktivieren, damit Sie über ein Remote-WAN auf die Cisco RV110W 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 der Cisco RV110W 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.
Remoteverwaltungsanschluss	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*>:<*Remoteanschluss*> 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 die Cisco RV110W umkonfigurieren und missbrauchen könnte, wird dringend 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 der Cisco RV110W kommunizieren können.

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

UPnP	Aktivieren Sie das Kontrollkästchen **Aktivieren**, um UPnP zu aktivieren.
Konfigurieren durch Benutzer zulassen	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 die Cisco RV110W nicht zu, dass die Weiterleitungsregel von Anwendungen hinzugefügt wird.
Deaktivierung des Internetzugriffs durch Benutzer zulassen	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 **Dienstname** zu Identifizierungs- und Verwaltungszwecken den Dienstnamen 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 **Startanschluss** den ersten TCP- oder UDP-Anschluss des vom Service verwendeten Bereichs ein.

SCHRITT 6 Geben Sie in das Feld **Endanschluss** 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 IPv6-Unterstützung in der Cisco RV110W 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 in der Cisco RV110W 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

Die Cisco RV110W 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 Einzelanschlussweiterleitung** und **Regeln für die Anschlussbereichsweiterleitung** 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 Anschlussbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur am erforderlichen Anschluss oder Anschlussbereich 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 Einzelanschlussweiterleitung

So fügen Sie eine Regel für die Einzelanschlussweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Einzelanschlussweiterleitung** 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 Anschluss** die Anschlussnummer ein, die diese Regel auslöst, wenn eine Verbindungsanforderung von ausgehendem Verkehr gestellt wird.

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

SCHRITT 5 Wählen Sie im Dropdown-Menü **Protokoll** ein Protokoll aus (**TCP**, **UDP** oder **TCP** & **UDP**).

SCHRITT 6 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 7 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 8 Klicken Sie auf **„Speichern“**.

Konfigurieren der Anschlussbereichsweiterleitung

So fügen Sie eine Regel für die Anschlussbereichsweiterleitung hinzu:

SCHRITT 1 Wählen Sie **Firewall** > **Anschlussbereichsweiterleitung** 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 Anschluss** 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 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.

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

SCHRITT 9 Klicken Sie auf **„Speichern“**.

Konfigurieren der Auslösung des Anschlussbereichs

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 Anschlussbereich empfangen. Der Router darf alle eingehenden Daten für diese Anwendung nur am erforderlichen Anschluss oder Anschlussbereich 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 Anschlussbereiche** 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 Aktivieren Sie im Feld **Aktivieren** das Kontrollkästchen **Aktivieren**, um die Regel zu aktivieren.

SCHRITT 6 Klicken Sie auf **„Speichern“**.

5

Konfigurieren von VPN

In diesem Kapitel wird beschrieben, wie Sie das VPN und die Sicherheit für die Cisco RV110W 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.

Geben Sie auf der Seite *VPN > VPN-Clients* in der Tabelle für VPN-Clienteinstellung die PPTP-Servereinstellungen ein und fügen Sie die Benutzer hinzu. Wählen Sie **PPTP** als Benutzerprotokoll aus. Weitere Informationen hierzu finden Sie unter **Erstellen und Verwalten von PPTP-Benutzern**.

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.

1. Fügen Sie auf der Seite *VPN > VPN-Clients* in der Tabelle für VPN-Clienteinstellung die Benutzer hinzu. Wählen Sie **QuickVPN** als Benutzerprotokoll aus. Weitere Informationen hierzu finden Sie unter **Importieren von VPN-Clienteinstellungen**.
2. Weisen Sie die Benutzer an, die kostenlose Cisco QuickVPN-Software von Cisco.com herunterzuladen und auf ihren Computern zu installieren. Weitere Informationen finden Sie unter **Verwenden von Cisco QuickVPN**

Zum Aktivieren des Zugriffs auf diesen Router über Cisco QuickVPN müssen Sie die Remoteverwaltung aktivieren, um Anschluss 443 für SSL zu öffnen. Weitere Informationen hierzu finden Sie unter **Konfigurieren der grundlegenden Firewalleinstellungen**.

Site-to-Site-VPN

Die Cisco RV110W unterstützt Site-to-Site-VPN für einen einzigen Gateway-to-Gateway-VPN-Tunnel. Sie können beispielsweise die Cisco RV110W 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** > **Basis-VPN-Einrichtung** konfiguriert.

VPN-Clients

Zum Einrichten eines VPN-Tunnels zwischen dem Router und dem Remoteendpunkt wird VPN-Clientsoftware benötigt. Open Source-Software (beispielsweise OpenVPN oder Openswan) sowie IPsec-VPN-Software von Microsoft kann konfiguriert werden, um einen IPsec-VPN-Tunnel einzurichten. Ausführliche Anweisungen zur Einrichtung finden Sie im Handbuch für die Clientsoftware sowie in der Onlinehilfe des Routers.

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 der Cisco RV110W aktivieren, wird das LAN-Subnetz in der Cisco RV110W 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 Führen Sie die folgenden Schritte aus:

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 die IP-Adresse 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 der Cisco RV110W einrichten und verwenden.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

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** aus.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Zum Bearbeiten der Einstellungen eines PPTP-Benutzers aktivieren Sie das entsprechende Kontrollkästchen und klicken Sie 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:

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um den Benutzer zu aktivieren.
Benutzername	Geben Sie den Benutzernamen des QuickVPN-Benutzers ein (4 bis 32 Zeichen).
Kennwort	Geben Sie das Kennwort ein (4 bis 32 Zeichen).
Kennwortänderung durch Benutzer zulassen	Aktivieren Sie dieses Kontrollkästchen, damit der Benutzer das Kennwort ändern kann.
Protokoll	Wählen Sie im Dropdown-Menü die Option **QuickVPN** aus.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

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

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

Weitere Informationen zu QuickVPN finden Sie unter **Verwenden von Cisco QuickVPN**

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 Beispiel werden die Einstellungen für zwei Benutzer angegeben (ein PPTP-Benutzer und ein QuickVPN-Benutzer), die importiert werden sollen:

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 VPN-Einstellungen (Site-to-Site-VPN)

Die Cisco RV110W unterstützt Site-to-Site-VPN für einen einzigen Gateway-to-Gateway-VPN-Tunnel. In dieser Konfiguration stellt die Cisco RV110W eine sichere Verbindung zu einem anderen VPN-fähigen Router her. Sie können beispielsweise die Cisco RV110W in einer Filiale so konfigurieren, dass eine Verbindung zum Router am Hauptstandort hergestellt wird und ein sicherer Zugriff auf das Unternehmensnetzwerk möglich ist. So können Sie zum Beispiel einen Router wie den Cisco RV220W implementieren, der zehn Site-to-Site-VPN-Tunnel unterstützt, und für sichere Verbindungen an jedem Remotestandort eine Cisco RV110W betreiben.

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

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

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

SCHRITT 3 Geben Sie im Feld *Pre-Shared Key* den Pre-Shared Key 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 die Cisco RV110W verbunden wird, identifiziert werden soll (nach IP-Adresse, beispielsweise *192.168.1.1*, oder vollständig qualifiziertem Domänennamen, beispielsweise *cisco.com*).
- **IP-Adresse des Remote-WAN**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des Remoteendpunkts ein.
- **IP-Adresse des lokalen WAN**: Geben Sie die öffentliche IP-Adresse oder den Domänennamen des lokalen Endpunkts ein (Cisco RV110W).

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 Cisco RV110W.
- **Lokale LAN-Subnetzmaske**: Geben Sie die Subnetzmaske des lokalen Netzwerks im privaten Netzwerk (LAN) ein (Cisco RV110W).

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 vorinstallierten Schlüssel bzw. ein Kennwort verwenden, der bzw. das sowohl der Cisco RV110W 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** > **Basis-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 die Cisco RV110W 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 usw.). Achten Sie darauf, für die VPN-Richtlinie kompatible Verschlüsselungs-, Authentifizierungs- und Schlüsselgruppenparameter zu verwenden.

So verwalten Sie IKE-Richtlinien:

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

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

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

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:

- **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 IKE-Richtlinien

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:
  - **Hauptmodus**: In diesem Modus wird der Tunnel mit höherer Sicherheit ausgehandelt, die Geschwindigkeit ist jedoch niedriger.
  - **Aggressiv**: In diesem Modus wird eine schnellere Verbindung hergestellt, die Sicherheit ist jedoch niedriger.

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 die Cisco RV110W und den Router, mit dem sie 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 die Cisco RV110W höchstens auf eine Antwort auf die DPD-Nachricht warten soll, bevor der Peer für inaktiv erklärt wird.

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 dann die Kennung in das entsprechende Feld ein.

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 dann 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

- **Schlüsseleingang**: 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
- **Schlüsselausgang**: 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
- **Schlüsseleingang**: 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
- **Schlüsselausgang**: Geben Sie den Integritätsschlüssel (für ESP mit Integritätsmodus) für die Ausgangsrichtlinie ein. Die Länge des Schlüssels hängt wie oben gezeigt vom ausgewählten Algorithmus ab.

Legen Sie beim Richtlinientyp **Automatisch** die Einstellungen unter **Parameter für automatische Richtlinien** fest.

- **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 in der Cisco RV110W konfigurierte vorhandene IKE-Richtlinie anzuzeigen oder zu bearbeiten.

Konfigurieren der Zertifikatverwaltung

Die Cisco RV110W verwendet digitale Zertifikate für die IPsec-VPN-Authentifizierung und SSL-Überprüfung (für HTTPS). Sie können mithilfe der in der Cisco RV110W verfügbaren Funktionalität eigene Zertifikate generieren und signieren.

Generieren eines neuen Zertifikats

Sie können ein neues Zertifikat generieren, um das vorhandene Zertifikat in der Cisco RV110W 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

Das Zertifikat für den Administrator enthält den privaten Schlüssel und sollte als Backup an einem sicheren Ort gespeichert werden. Wenn die Konfiguration der Cisco RV110W 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 Klicken Sie auf **Für Administrator exportieren**.

Auf einem PC speichert der Gerätemanager die Datei „admin.pem“ unter „C:\Dokumente und Einstellungen*Benutzername*\Eigene Dokumente\Downloads“.

Exportieren von Zertifikaten für den Client

Das Zertifikat für den Client ermöglicht QuickVPN-Benutzern das Herstellen sicherer Verbindungen mit der Cisco RV110W. 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 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“.

Konfigurieren von VPN-Passthrough

Mithilfe von VPN-Passthrough kann VPN-Verkehr von VPN-Clients die Cisco RV110W 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 die Cisco RV110W passieren können.
PPTP	Aktivieren Sie die Option **Aktivieren**, damit PPTP-Tunnel die Cisco RV110W passieren können.
L2TP	Aktivieren Sie die Option **Aktivieren**, damit L2TP-Tunnel (Layer 2 Tunneling Protocol) die Cisco RV110W passieren können.

SCHRITT 3 Klicken Sie auf **„Speichern“**.

6

Konfigurieren der Servicequalität (Quality of Service, QoS)

Sie können für die Cisco RV110W die folgenden QoS-Funktionen (Quality of Service) konfigurieren:

Konfigurieren der Bandbreitenverwaltung

Sie können die Bandbreitenverwaltung der Cisco RV110W verwenden, um die Bandbreite des Verkehrs zu verwalten, der vom sicheren Netzwerk (LAN) zum nicht sicheren Netzwerk (WAN) fließt.

Konfigurieren der Bandbreite

Sie können die Bandbreite begrenzen, um die Datenübertragungsrate der Cisco RV110W zu reduzieren. Außerdem können Sie mithilfe eines Bandbreiteprofils den ausgehenden Verkehr begrenzen und so verhindern, dass die LAN-Benutzer die gesamte Bandbreite der Internetverbindung verbrauchen.

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

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

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

SCHRITT 3 Geben Sie in die **Bandbreitentabelle** 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

In der **Bandbreitenprioritätstabelle** können Sie die Verwendung der Bandbreite verwalten, indem Sie Services Prioritäten zuweisen.

So konfigurieren Sie die Bandbreitenpriorität:

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

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

SCHRITT 3 Klicken Sie in der **Bandbreitenprioritätstabelle** auf **Hinzufügen**.

SCHRITT 4 Geben Sie folgende Informationen ein:

Aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Bandbreitenverwaltung 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 und klicken Sie auf **Löschen**. Klicken Sie dann 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 RV110W konfigurieren. Die Cisco RV110W unterstützt vier Prioritätswarteschlangen, die die Verkehrspriorisierung pro physischer Switch-Anschluss ermöglichen.

So konfigurieren Sie QoS-Einstellungen für die LAN-Anschlüsse der Cisco RV110W:

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

SCHRITT 2 Geben Sie für jeden Anschluss in der **Tabelle für anschlussbasierte 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 Datenverkehrweiter-leitungswarte-schlange für nicht vertrauenswürdige Geräte	Wählen Sie eine Prioritätsstufe für ausgehenden Verkehr aus (1 bis 4).

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Zum Wiederherstellen der Standardeinstellungen für anschlussbasiertes QoS klicken Sie auf **Standard wiederherstellen**. Klicken Sie dann auf **Speichern**.

Konfigurieren der CoS-Einstellungen

Sie können der Datenverkehrweiterleitungswarteschlange des Cisco RV110W CoS-Prioritätseinstellungen zuordnen.

Sie können den Link zur Seite „Anschlussbasierte QoS-Einstellungen“ verwenden, 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 Wählen Sie für jede CoS-Prioritätsstufe in der **CoS-Einstellungstabelle** einen Prioritätswert im Dropdown-Menü **Datenverkehrweiterleitungswarteschlange** aus.

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

SCHRITT 3 Klicken Sie auf **„Speichern“**.

Zum Wiederherstellen der Standardeinstellungen für anschlussbasiertes QoS klicken Sie auf **Standard wiederherstellen**. Klicken Sie dann 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 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 3 Wählen Sie für jeden DSCP-Wert in der **DSCP-Einstellungstabelle** im Dropdown-Menü **Queue Warteschlange** eine Prioritätsstufe aus.

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

SCHRITT 4 Klicken Sie auf **„Speichern“**.

Zum Wiederherstellen der DSCP-Standardeinstellungen klicken Sie auf **Standard wiederherstellen**. Klicken Sie dann auf **Speichern**.

7

Verwalten des Cisco RV110W

In diesem Kapitel werden die Verwaltungsfunktionen der Cisco RV110W beschrieben. Dazu gehören die Erstellung von Benutzern, die Netzwerkverwaltung, Systemdiagnose und -protokolle und weitere Einstellungen.

Festlegen der Kennwortkomplexität

Die Cisco RV110W 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 - 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

Die Cisco RV110W unterstützt zwei Benutzerkonten zum Verwalten und Anzeigen von Einstellungen: Einen administrativen Benutzer (Standardbenutzername und -kennwort: „cisco“) und einen Gastbenutzer (Standardbenutzername und Kennwort: „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 *Administratoreinstellungen* 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 Gast 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. Die Cisco RV110W unterstützt nur SNMPv3 für die SNMP-Verwaltung. Die Cisco RV110W unterstützt SNMP-Trap-Nachrichten mit SNMPv1/2/3.

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 der Cisco RV110W (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.
Authentifizierungsalgorithmusserver	Wählen Sie den Typ des Authentifizierungsalgorithmus aus (**MD5** oder **SHA**).
Authentifizierungskennwort	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.
Anschluss	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

Für die Cisco RV110W werden verschiedene Diagnosetools bereitgestellt, die Ihnen die Behandlung 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 führen, wenn für den LAN-Host keine statische IP-Adresse konfiguriert ist.

So konfigurieren Sie die Port-Siegelung:

SCHRITT 1 Wählen Sie **Administration** > **Diagnose** > **Port-Spiegelung** aus.

SCHRITT 2 Wählen Sie im Feld **Spiegelquelle** die zu spiegelnden Ports aus.

SCHRITT 3 Wählen Sie im Dropdown-Menü **Gespiegelter Port** einen gespiegelten Port aus. Wenn Sie einen Port 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 RV110W 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 den Protokolltyp „Fehler“ auswählen, sind zusätzlich zu den Fehlerprotokollen automatisch 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 des E-Mail-Versands für Protokolle

Sie können die Cisco RV110W so konfigurieren, dass Protokolle per E-Mail gesendet werden. Wir empfehlen, zum Senden und Empfangen von Protokollen ein separates E-Mail-Konto einzurichten.

Zuerst müssen Sie den Schweregrad der zu erfassenden Protokolle einrichten (siehe **Konfigurieren von Protokollierungseinstellungen**).

So konfigurieren Sie den E-Mail-Versand für Protokolle:

SCHRITT 1 Wählen Sie **Administration** > **Protokollierung** > **E-Mail-Einstellungen** aus.

SCHRITT 2 Zum Aktivieren des E-Mail-Versands für Protokollereignisse aktivieren Sie das Kontrollkästchen **Aktivieren**.

SCHRITT 3 Der Mindest-Schweregrad für die E-Mail-Protokollierung der zu erfassenden Protokolle wird angezeigt. Zum Ändern des Schweregrads klicken Sie auf **Schweregrad konfigurieren**.

SCHRITT 4 Konfigurieren Sie die folgenden Einstellungen:

Mailserveradresse	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*).
E-Mail-Serveranschluss	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 RV110W Nachrichten sendet, wenn Protokolle vom Router nicht an die unter „An E-Mail-Adresse senden“ angegebene E-Mail-Adresse übermittelt werden können.

E-Mail-Adresse für Benachrichtigungen Adresse (1)	Geben Sie eine E-Mail-Adresse ein, an die Protokolle gesendet werden sollen (beispielsweise *Protokollierung@Firmenname.com*).
E-Mail-Adresse für Benachrichtigungen Adresse (2) (Optional)	Geben Sie eine zusätzliche E-Mail-Adresse ein, an die Protokolle gesendet werden sollen.
E-Mail-Adresse für Benachrichtigungen Adresse (3) (Optional)	Geben Sie eine zusätzliche E-Mail-Adresse ein, an die Protokolle gesendet werden sollen.
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**, **Anmelden**, **Unverschlüsselt** 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, das für den Zugriff auf das von Ihnen eingerichtete E-Mail-Konto verwendet wird, an das Protokolle gesendet werden sollen).
E-Mail-Authentifizierungstest	Klicken Sie auf **Testen**, um die E-Mail-Authentifizierung zu testen.

SCHRITT 5 Konfigurieren Sie im Abschnitt **Protokolle nach Zeitplan per E-Mail versenden** 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 6 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 RV110W 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 der **Tabelle für Bonjour-Schnittstellensteuerung** 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 **An Sommerzeit anpassen**, 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 den Feldern „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** > **Konfiguration 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. Der Vorgang 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** > **Konfiguration 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 von der Cisco RV110W 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 RV110W-Systemen bereitzustellen.
Spiegelkonfiguration	Wählen Sie diese Option aus, um die Cisco RV110W anzuweisen, dass die Startkonfiguration nach 24 Betriebsstunden ohne Änderung an der Startkonfiguration gesichert werden soll.
Sicherungskonfiguration	Wählen Sie diese Option aus, um die aktuellen Konfigurationseinstellungen zu sichern.

SCHRITT 3 Zum Herunterladen einer auf der ausgewählten Konfigurationsoption basierenden Sicherungsdatei klicken Sie auf **Herunterladen**.

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*\.

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 **Sicherungskonfiguration**).

SCHRITT 3 Klicken Sie auf **Durchsuchen**, um die Datei zu suchen.

SCHRITT 4 Suchen Sie die Datei und klicken Sie auf **Öffnen**.

SCHRITT 5 Klicken Sie auf **Jetzt hochladen**.

Die Cisco RV110W lädt die Konfigurationsdatei hoch und verwendet die darin enthaltenen Einstellungen zum Aktualisieren der Startkonfiguration. Anschließend wird die Cisco RV110W neu gestartet und verwendet die neue Konfiguration.

Kopieren der Konfigurationseinstellungen

Sie kopieren die Startkonfiguration in die Sicherungskonfiguration, um sicherzustellen, dass Sie eine Sicherungskopie haben, falls Sie Ihren Benutzernamen und Ihr Kennwort vergessen und daher der Gerätemanager für Sie gesperrt ist. In diesem Fall können Sie den Gerätemanager erst dann wieder verwenden, wenn Sie die Cisco RV110W auf die Werkseinstellungen zurückgesetzt haben.

Die Sicherungskonfigurationsdatei bleibt im Speicher 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 **Kopieren starten**.

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.

Aktualisieren der Firmware

So aktualisieren Sie den Router auf eine neuere Version der Firmware:

SCHRITT 1 Wählen Sie **Administration** > **Firmware-/Sprach-Upgrade** aus.

SCHRITT 2 (Optional) Klicken Sie auf **Herunterladen**, um die aktuelle Version der Firmware herunterzuladen.

SCHRITT 3 Klicken Sie im Feld **Dateityp** auf die Schaltfläche **Firmware-Image**.

SCHRITT 4 Klicken Sie auf **Durchsuchen**, um die heruntergeladene Firmware zu suchen und auszuwählen.

SCHRITT 5 (Optional) Um die Cisco RV110W nach der Aktualisierung der Firmware auf die Werkseinstellungen zurückzusetzen, aktivieren Sie das Kontrollkästchen **Alle Konfigurationen/Einstellungen auf Werkseinstellungen zurücksetzen**.

VORSICHT Beim Zurücksetzen der Cisco RV110W auf die Werkseinstellungen werden alle benutzerdefinierten Einstellungen gelöscht.

SCHRITT 6 Klicken Sie auf **Upgrade starten**.

Nach der Überprüfung des neuen Firmware-Images wird das Image in den Flash-Speicher geschrieben und der Router wird automatisch mit der neuen Firmware neu gestartet.

SCHRITT 7 Wählen Sie **Status** > **Systemübersicht** aus, um sich zu vergewissern, dass die neue Firmwareversion im Router installiert wurde.

Ändern der Sprache

So ändern Sie Sie 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 Klicken Sie auf **Upgrade starten**.

Neustarten der Cisco RV110W

So starten Sie den Router neu:

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

SCHRITT 2 Klicken Sie auf **Neustart**.

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.

8

Anzeigen des Status der Cisco RV110W

In diesem Kapitel wird beschrieben, wie Sie Echtzeitstatistiken und andere Informationen zur Cisco RV110W anzeigen.

Anzeigen des Dashboards

Auf der Seite **Dashboard** erhalten Sie eine allgemeine Übersicht über wichtige Informationen zum Router.

So zeigen Sie das Dashboard an:

SCHRITT 1 Wählen Sie **Status** > **Dashboard** aus.

SCHRITT 2 Zum Anzeigen einer interaktiven Ansicht der Rückseite des Routers klicken Sie auf **Panelansicht anzeigen**.

In der Ansicht der Rückseite sehen Sie, welche Anschlüsse verwendet werden (grün dargestellt), und können auf einen Anschluss klicken, um Informationen zur Verbindung zu erhalten.

- Zum Anzeigen der Verbindungsinformationen eines Anschlusses klicken Sie auf den Anschluss.

- Zum Aktualisieren der Anschlussinformationen klicken Sie auf **Aktualisieren**.
- Zum Schließen der Seite 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 Softwareversion.
- **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 (Lokales Netzwerk)-Schnittstelle

- **MAC-Adresse**: Die MAC-Adresse des Routers.
- **IPv4-Adresse**: Die lokale IP-Adresse des Routers.

- **IPv6-Adresse**: Die lokale IP-Adresse des Routers (wenn IPv6 aktiviert ist).
- **DHCP-Server**: Der Status des IPv4-DHCP-Servers des Routers (aktiviert oder deaktiviert).
- **DHCPv6-Server**: Der 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-(Internet-)Informationen

- **IPv4-Adresse**: Die IP-Adresse des WAN-Anschlusses des Routers.
- **IPv6-Adresse**: Die IP-Adresse des WAN-Anschlusses des Routers, wenn IPv6 aktiviert ist.
- **Status**: Der Status der Internetverbindung (aktiv oder inaktiv).

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

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 der Wireless-Statistik**.

VPN

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

Anzeigen der Systemzusammenfassung

Auf der Seite **Systemübersicht** wird eine Übersicht über die Einstellungen des Routers angezeigt.

So zeigen Sie eine Übersicht über die Systemeinstellungen an:

SCHRITT 1 Wählen Sie **Status** > **Systemübersicht** aus.

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

Auf der Seite **Systemübersicht** 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**: Die LAN-Adresse des Geräts.
- **WAN-IP**: Die WAN-Adresse des Geräts. Sie können die aktuelle IP-Adresse freigeben und eine neue beziehen, indem Sie auf **Freigeben** oder **Erneuern** klicken.

- **Gateway**: Die IP-Adresse des Gateways, mit dem die Cisco RV110W 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** Die LAN-Adresse des Geräts.
- **WAN-IP**: Die WAN-Adresse des Geräts.
- **Gateway**: Die IP-Adresse des Gateways, mit dem die Cisco RV110W verbunden ist (beispielsweise das Kabelmodem).
- **NTP**: Network Time Protocol-Server (Hostname oder IPv6-Adresse).
- **Präfix-Delegation**: IPv6-Präfix, das vom Gerät des Internetdienstanbieters zurückgegeben und an IP-Adressen in der Cisco RV110W vergeben wird.
- **DNS 1**: Die IP-Adresse des primären DNS-Servers.
- **DNS 2**: Die IP-Adresse des sekundären DNS-Servers.

WLAN-Übersicht

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

Firewall-Einstellungsstatus

- **DoS (Denial of Service)**: Gibt an, ob die DoS-Prävention aktiviert oder deaktiviert ist.

- **WAN-Anfrage blockieren**: Gibt an, ob das Blockieren von WAN-Anfragen aktiviert oder deaktiviert ist.
- **Remoteverwaltung**: Gibt an, ob die Remoteverwaltung aktiviert oder deaktiviert ist (beispielsweise wenn remote auf den Gerätemanger der Cisco RV110W zugegriffen werden kann).

VPN-Einstellungsstatus

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

Anzeigen der Wireless-Statistik

Auf der Seite **WLAN-Statistik** werden die kumulierten relevanten WLAN-Statistiken für den Sender des Geräts angezeigt.

So zeigen Sie die WLAN-Statistik an:

SCHRITT 1 Wählen Sie **Status** > **WLAN-Statistik** aus.

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

SCHRITT 3 (Optional) 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 statistische Daten anzeigen** und klicken Sie auf **Speichern**.

SCHRITT 4 Zum Zurücksetzen der Zähler der WLAN-Statistik klicken Sie auf **Zähler löschen**.

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

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

HINWEIS Die Zähler werden zurückgesetzt, wenn das Gerät neu gestartet wird.

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- oder 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	der Zeitpunkt, zu dem der VPN-Benutzer eine Verbindung hergestellt hat
Endzeit	der Zeitpunkt, zu dem der VPN-Benutzer eine Verbindung beendet hat
Dauer (Sekunden)	die Zeitspanne zwischen dem Herstellen und dem Beenden einer Verbindung durch den VPN-Benutzer
Protokoll	das vom Benutzer verwendete Protokoll (QuickVPN oder PPTP)

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 Cisco RV110W. (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.

SCHRITT 2 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 statistische Daten 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 statistische Daten 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“).

SCHRITT 3 Falls Sie Änderungen vorgenommen haben, klicken Sie auf **Speichern**.

Anzeigen von Protokollen

Auf der Seite **Protokolle anzeigen** können Sie die Protokolle des Cisco RV110W anzeigen.

So zeigen Sie die Protokolle an:

SCHRITT 1 Wählen Sie **Status** > **Protokolle anzeigen** aus.

SCHRITT 2 Klicken Sie auf **Protokolle aktualisieren**, um die neuesten Protokolleinträge anzuzeigen.

SCHRITT 3 Zum Filtern der Protokolle oder zum Angeben des Schweregrads der anzuzeigenden Protokolle aktivieren Sie die Kontrollkästchen neben dem Protokolltyp und klicken Sie 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 den Protokolltyp „Fehler“ auswählen, sind zusätzlich zu den Fehlerprotokollen automatisch 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**.

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 Cisco RV110W verbundenen aktiven Geräten angezeigt.

In der IPv4-ARP-Tabelle werden Informationen von Geräten angezeigt, die auf die ARP-Anforderung (Address Resolution Protocol) der Cisco RV110W 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 Cisco RV110W verbunden sind.

So zeigen Sie verbundene Geräte an:

SCHRITT 1 Wählen Sie **Status** > **Verbundene Geräte** aus.

SCHRITT 2 In der *IPv4-ARP-Tabelle* können Sie die Typen der anzuzeigenden Schnittstellen angeben, indem Sie eine Option aus dem Dropdown-Menü **Filter** auswählen. Sie können eine der folgenden Optionen auswählen:

Alle	Zeigt eine Liste aller mit dem Router verbundenen Geräte an.
WLAN	Zeigt eine Liste aller über die WLAN-Schnittstelle verbundenen Geräte an.
Kabel	Zeigt eine Liste aller über die Ethernet-Anschlüsse am Router verbundenen Geräte an.
WDS	Zeigt eine Liste aller mit dem Router verbundenen WDS-Geräte (Wireless Distribution System) an.

Anzeigen von Anschlussstatistiken

Auf der Seite **Anschlussstatistik** werden Anschlussstatistiken angezeigt.

So zeigen Sie Anschlussstatistiken an:

SCHRITT 1 Wählen Sie **Status** > **Anschlussstatistik** aus.

SCHRITT 2 Wählen Sie im Dropdown-Menü **Aktualisierungsrate** eine Aktualisierungsrate aus. Daraufhin werden die Statistiken erneut vom Router eingelesen und die Seite wird aktualisiert.

SCHRITT 3 (Optional) 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 statistische Daten anzeigen** und klicken Sie auf **Speichern**.

SCHRITT 4 Zum Zurücksetzen der Zähler der Anschlussstatistik klicken Sie auf **Zähler löschen**.

In dieser Tabelle werden die Datenübertragungsstatistiken für die dedizierten WAN-, LAN- und VLAN-Anschlüsse einschließlich der Dauer ihrer Aktivierung angezeigt.

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

Schnittstelle	Der Name der Netzwerkschnittstelle.
Paket	Die Anzahl der empfangenen und gesendeten Pakete.
Byte	die Anzahl der pro Sekunde empfangenen und gesendeten Datenbytes
Fehler	Die Anzahl der empfangenen und gesendeten Paketfehler.
Gelöscht	Die Anzahl der empfangenen und gesendeten Pakete, die gelöscht wurden.
Multicast	die Anzahl der über diesen Sender gesendeten Multicast-Pakete

Kollisionen	Die 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 Gastnetzstatus

In der Statistik zum Gastnetzwerk werden Informationen über das in der Cisco RV110W 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 Zeitdauer, 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“).

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.

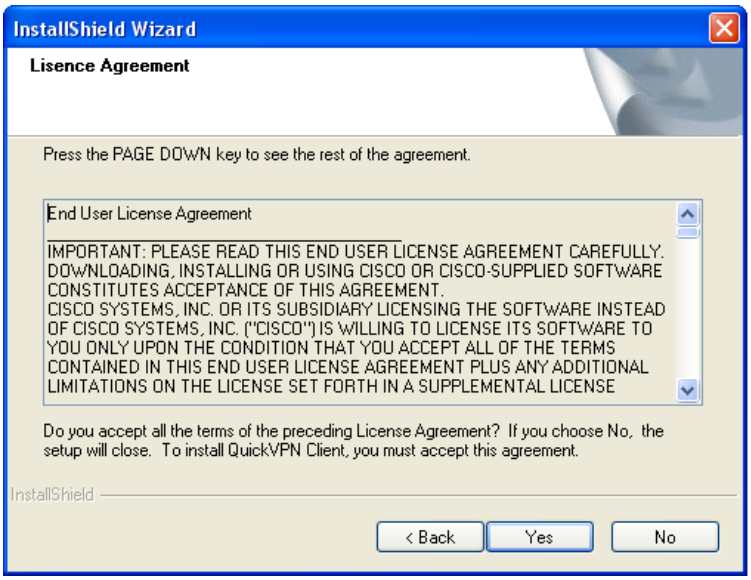
Installieren der Cisco QuickVPN-Software

Installieren von der CD-ROM

SCHRITT 1 Legen Sie die CD-ROM für die Cisco RV110W 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



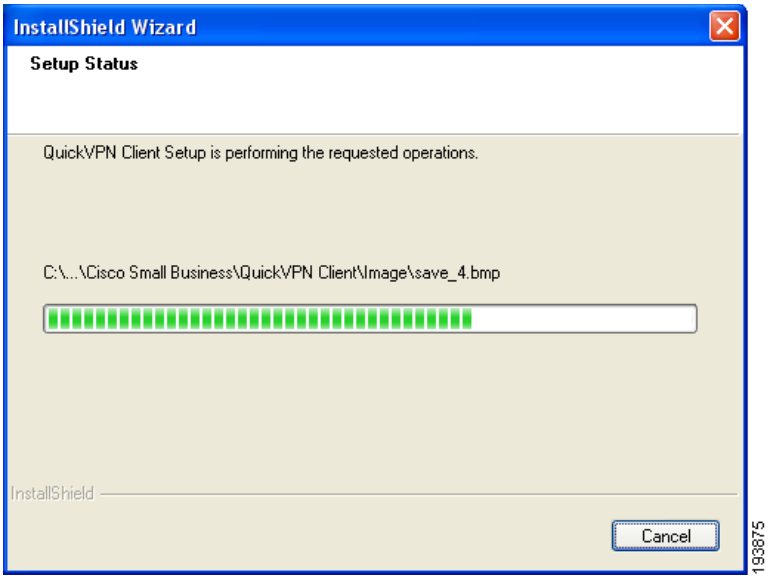
SCHRITT 2 Klicken Sie auf **Ja**, um die Vereinbarung zu akzeptieren.

SCHRITT 3 Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie aus, wohin die Dateien kopiert werden sollen (beispielsweise „C:\Cisco\QuickVPN Client“).

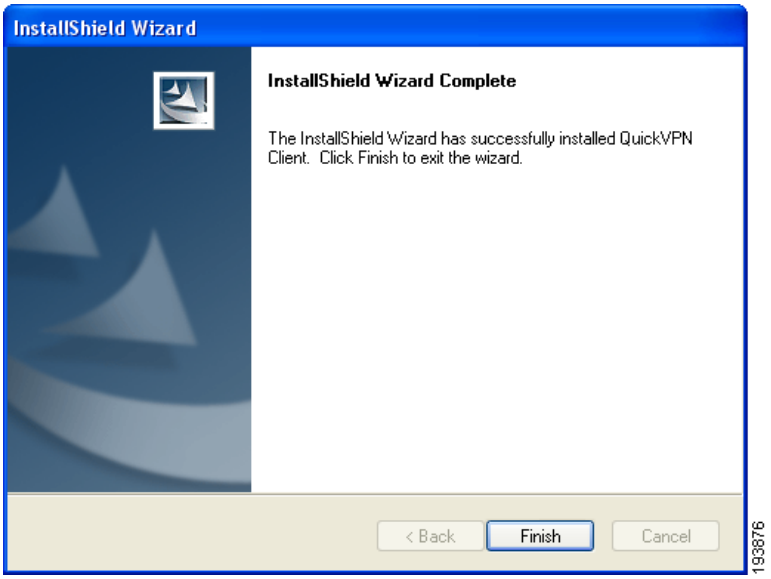
SCHRITT 4 Klicken Sie auf **„Weiter“**.

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 **Ende**, um die Installation abzuschließen. Fahren Sie mit **Verwenden der Cisco QuickVPN-Software** fort.

Herunterladen und Installieren aus dem Internet

SCHRITT 1 Gehen Sie in **Weitere Informationen** zum Link „Herunterladen von Software“.

SCHRITT 2 Geben Sie in das Suchfeld „Cisco RV110W“ 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 **Password** (Kennwort) den Benutzernamen und das Kennwort ein, die Sie in **Erstellen und Verwalten von QuickVPN-Benutzern** erstellt haben.

SCHRITT 4 Geben Sie in das Feld **Server Address** (Serveradresse) die IP-Adresse oder den Domänennamen der Cisco RV110W 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 **Ändern des Kennworts**. Weitere Informationen erhalten Sie, wenn Sie auf **Hilfe** klicken.

SCHRITT 9 Wenn Sie auf **Ändern des Kennworts** 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 **Allow User to Change Password** (Kennwortänderung durch Benutzer zulassen) für den jeweiligen Benutzernamen aktiviert ist. Weitere Informationen hierzu finden Sie unter **Erstellen und Verwalten von QuickVPN-Benutzern**.

B

Weitere Informationen

Cisco bietet eine breite Palette von Ressourcen an, die Ihnen helfen sollen, in vollem Umfang von den Vorteilen des Cisco RV110W zu profitieren.

Produktressourcen

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	
Cisco RV110W	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