

# ARP-Schutz vor Angriffen auf den RV315W VPN-Router

## Ziel

ARP (Address Resolution Protocol) dient der Verfolgung aller Geräte, die direkt mit der RV315W verbunden sind. Der ARP-Schutz dient zum Schutz eines Netzwerks vor ARP-Angriffen. Wenn ein Paket an einer Schnittstelle (Port/LAG) ankommt, die als nicht vertrauenswürdig definiert ist, vergleicht ein ARP-Schutzangriff die IP-Adresse und die MAC-Adresse des Pakets mit den IP-Adressen und MAC-Adressen, die zuvor in den ARP-Zugriffskontrollregeln definiert wurden. Wenn die Adressen übereinstimmen, gilt das Paket als gültig und wird anderweitig weitergeleitet, da das Paket verworfen wird. In diesem Artikel wird erläutert, wie Sie den ARP-Schutz auf dem RV315W VPN-Router konfigurieren.

## Anwendbares Gerät

RV315W

## Softwareversion

·1.01.03

## Schutz vor ARP-Angriffen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > ARP Attack Protection (Sicherheit > ARP-Schutz für Angriffe) aus**. Die Seite *ARP Attack Protection* wird geöffnet:

The screenshot shows the configuration page for ARP Attack Protection. It is divided into two main sections: ARP Attack Protection and IP&MAC Binding.

**ARP Attack Protection**

- ARP Attack Protection:  Enable  Disable
- Enable Auto Learning:  Enable  Disable
- ARP Flooding Threshold: 50 (30-1000)
- ARP Broadcast Interval: 15 (0-65535, 0 means disabled)

Buttons: Save, Cancel

**IP&MAC Binding (Status: Disabled)**

IP Address	MAC Address	Action
<input type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	<input type="checkbox"/> <input type="checkbox"/>

Buttons: Add, Delete

Schritt 2: Klicken Sie im Feld "Attack Protection" auf das Optionsfeld **Enable**, um den ARP-Schutz auf dem RV315W zu aktivieren.

Schritt 3: (Optional) Um die automatische Lernfunktion für die RV315W zu aktivieren, klicken Sie im Feld Automatische Lernfunktion aktivieren **auf** Aktivieren. Mithilfe dieser Funktion

kann die RV315W erkennen, welche IP-Adressen und MAC-Adressen im Netzwerk gültig sind.

Schritt 4: Geben Sie die maximale Anzahl an ARP-Paketen ein, die die RV315W pro Sekunde empfangen kann. Wenn das Gerät mehr als den festgelegten Wert erhält, wird der ARP-Schutz auf den RV315W angewendet.

Schritt 5: Geben Sie das Intervall für den ARP-Broadcast im Feld ARP Broadcast Interval (ARP-Broadcast-Intervall) ein. Dieses Intervall bestimmt die Anzahl der ausgesendeten ARP-Broadcasts.

## IP&MAC-Bindung

In diesem Bereich kann der Administrator eine IP-Adresse und eine MAC-Adresse zuordnen, um die Sicherheit zu erhöhen. Ein Host darf nur dann auf das Netzwerk zugreifen, wenn die IP-Adresse und die MAC-Adresse des Hosts mit der im Bereich für die IP&MAC-Bindung konfigurierten Adresse übereinstimmen.

### Hinzufügen einer IP&MAC-Bindung

**Add IP&MAC Binding Rule**

IP Address:  For example: 192.168.1.22

MAC Address:  For example: 60:eb:69:78:7c:cc

Schritt 1: Klicken Sie auf **Hinzufügen**, um eine neue IP&MAC-Bindungsregel hinzuzufügen. Diese Seite "IP&MAC-Bindungsregel hinzufügen" wird geöffnet:



Schritt 2: Geben Sie die IP-Adresse ein, die der MAC-Adresse im Feld IP Address (IP-Adresse) zugeordnet ist.

Schritt 3: Geben Sie die MAC-Adresse ein, die der IP-Adresse im Feld MAC Address (MAC-Adresse) zugeordnet ist.

Schritt 4: Klicken Sie auf **Speichern**. Diese Regel wird in der IP&MAC-Bindungsliste angezeigt.

### Bearbeiten einer IP&MAC-Bindungsregel

**IP&MAC Binding (Status: Disabled)**

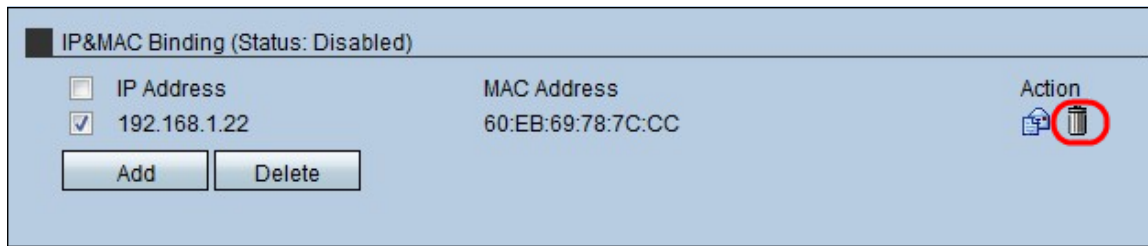
IP Address	MAC Address	Action
<input checked="" type="checkbox"/> 192.168.1.22	60:EB:69:78:7C:CC	 

Schritt 1: Aktivieren Sie das Kontrollkästchen der IP&MAC-Bindungsregel, die bearbeitet werden soll.

Schritt 2: Klicken Sie auf das **Umschlagsymbol**, um die IP&MAC-Bindungsregel zu

bearbeiten.

## IP&MAC-Bindungsregel löschen



Schritt 1: Aktivieren Sie das Kontrollkästchen der zu löschenden IP&MAC-Bindungsregel.

Schritt 2: Klicken Sie auf das **Trashcan**-Symbol, um die IP&MAC-Bindungsregel zu löschen.