

# Konfiguration der ARP-Inspektionseigenschaften (Address Resolution Protocol) auf Stackable Switches der Serie Sx500

## Ziel

Das Address Resolution Protocol (ARP) wird auf Layer 2, der Datenverbindungsschicht, des OSI-Modells ausgeführt und ermöglicht die Zuordnung der IP-Adresse zur MAC-Adresse des Ziel-Hosts mithilfe einer Nachschlagetabelle, die auch als ARP-Cache bezeichnet wird.

ARP Inspection wurde eingerichtet, um eine Vergiftung des ARP-Cache zu verhindern, die böswilligen Dritten die Abfangen und Kontrolle des Netzwerkverkehrs ermöglichen kann. Ziel dieses Dokuments ist die Einrichtung von ARP-Inspektionseigenschaften für stapelbare Switches der Serie Sx500.

Damit die ARP-Inspektion ordnungsgemäß funktioniert, müssen die folgenden Konfigurationen in der unten angegebenen Reihenfolge durchgeführt werden:

1. ARP-Inspektionseigenschaften, die in diesem Artikel behandelt werden.
2. Konfigurieren Sie die Schnittstelleneinstellungen. Weitere Informationen zu dieser Konfiguration finden Sie im Artikel *Address Resolution Protocol (ARP) Inspection Interface Settings (ARP)-Schnittstelleneinstellungen auf stapelbaren Switches der Serie Sx500*.
3. Konfigurieren von Zugriffskontroll- und Zugriffskontrollregeln finden Sie in folgendem Artikel: *Konfiguration der ARP-Zugriffskontrolle und Zugriffskontrollregeln auf stapelbaren Switches der Serie Sx500* für diese Konfiguration.
4. Konfigurieren der VLAN-Einstellungen. Weitere Informationen zu dieser Konfiguration finden Sie im Artikel *Address Resolution Protocol (ARP) Inspection VLAN Settings Configuration auf Stackable Switches der Serie Sx500*.

## Anwendbare Geräte

- Stackable Switches der Serie Sx500

## Softwareversion

- 1,3 0,62

## ARP-Inspektionseigenschaften

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Security > ARP Inspection > Properties** aus. Die Seite *Eigenschaften* wird geöffnet:

**Properties**

ARP Inspection also uses the [DHCP Snooping Binding database](#) if it is available.

ARP Inspection Status:  Enable

ARP Packet Validation:  Enable

Log Buffer Interval:  Retry Frequency  sec. (Range: 0 - 86400, Default: 5)  
 Never

Apply Cancel

Schritt 2: Aktivieren Sie im Feld ARP Inspection Status (ARP-Inspektionsstatus) die Option **Enable (Aktivieren)**, um die ARP-Inspektionsfunktion zu aktivieren. Diese Funktion ist standardmäßig deaktiviert.

**Hinweis:** Die ARP-Prüfung wird nur an nicht vertrauenswürdigen Schnittstellen durchgeführt. Pakete von vertrauenswürdigen Schnittstellen werden weitergeleitet. Sie können vertrauenswürdige Schnittstellen auf der Seite *Schnittstelleneinstellungen* konfigurieren.

**Properties**

ARP Inspection also uses the [DHCP Snooping Binding database](#) if it is available.

ARP Inspection Status:  Enable

ARP Packet Validation:  Enable

Log Buffer Interval:  Retry Frequency  sec. (Range: 0 - 86400, Default: 5)  
 Never

Apply Cancel

Schritt 3: Aktivieren Sie im Feld ARP Packet Validation (ARP-Paketvalidierung) die Option **Enable (Aktivieren)**, um die Paketvalidierung in ARP zu aktivieren. Diese Funktion ist standardmäßig deaktiviert. Wenn dieses Feld markiert ist, werden die folgenden Werte mit den vorhandenen Datenbanken verglichen, um externe Angriffe zu verhindern:

- Quell-MAC - Die Quell-MAC-Adresse des Pakets im Ethernet-Header wird mit der MAC-Adresse des Absenders in der ARP-Anfrage verglichen. Diese Prüfung wird sowohl für ARP-Anfragen als auch für Antworten durchgeführt.
- Ziel-MAC - Die Ziel-MAC-Adresse des Pakets im Ethernet-Header wird mit der MAC-Adresse der Zielschnittstelle verglichen. Diese Prüfung wird nur für ARP-Antworten durchgeführt.
- IP Addresses (IP-Adressen): Dieser Parameter vergleicht den ARP-Dateninhalt mit ungültigen und unerwarteten IP-Adressen. IP-Adressen umfassen 0.0.0.0, 255.255.255.255 und alle IP-Multicast-Adressen.

Darüber hinaus verwendet die ARP-Inspektion eine DHCP-Snooping-Binding-Datenbank, wenn DHCP-Snooping aktiviert ist, um neben den Zugriffskontrollregeln auch die IP-Adresse des Pakets zu überprüfen. Weitere Informationen zur Konfiguration der DHCP-Snooping-Binding-Datenbank finden Sie im Artikel *DHCP Snooping Binding Database Configuration on Sx500 Series Stackable Switches*. Sie können die Konfigurationsseite der DHCP Snooping

Binding-Datenbank aufrufen, indem Sie oben auf der Seite Eigenschaften auf den Link der **DHCP Snooping Binding-Datenbank** klicken.

**Properties**

ARP Inspection also uses the [DHCP Snooping Binding database](#) if it is available.

ARP Inspection Status:  Enable

ARP Packet Validation:  Enable

Log Buffer Interval:  Retry Frequency  sec. (Range: 0 - 86400, Default: 5)  Never

Schritt 4: Klicken Sie im Feld Log Buffer Interval (Protokollpuffer-Intervall) auf eines der folgenden Optionsfelder:

- Häufigkeit erneut versuchen - Aktiviert das Senden von SYSLOG-Nachrichten für verworfene Pakete. Geben Sie die Häufigkeit ein, mit der die Nachrichten gesendet werden. Die Standardfrequenz beträgt 5 Sekunden. Der Bereich liegt zwischen 0 und 86.400 Sekunden.
- Never (Niemals): Deaktiviert verlorene SYSLOG-Paketmeldungen.

**Properties**

Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

ARP Inspection also uses the [DHCP Snooping Binding database](#) if it is available.

ARP Inspection Status:  Enable

ARP Packet Validation:  Enable

Log Buffer Interval:  Retry Frequency  sec. (Range: 0 - 86400, Default: 5)  Never

Schritt 5: Klicken Sie auf **Apply**, um die Änderungen vorzunehmen. Die Einstellungen werden definiert, und die aktuelle Konfigurationsdatei wird aktualisiert.