

ACL-Regelkonfiguration auf dem WAP371

Ziel

Eine Zugriffskontrollliste (ACL) ist eine optionale Sicherheitsebene, die als Firewall zur Steuerung des ein- und ausgehenden Datenverkehrs eines Subnetzes fungiert. Zugriffslisten sind Zusammenstellungen von Genehmigungsbedingungen und Verweigerungsbedingungen oder -regeln, die aus verschiedenen Gründen für Sicherheit sorgen. Diese Regeln können z. B. nicht autorisierte Benutzer blockieren, autorisierten Benutzern den Zugriff auf bestimmte Ressourcen ermöglichen und alle ungerechtfertigten Versuche, Netzwerkressourcen zu erreichen, blockieren.

In diesem Dokument wird erläutert, wie Sie ACL-Regeln auf dem WAP 371 konfigurieren.

Anwendbare Geräte

WAP371

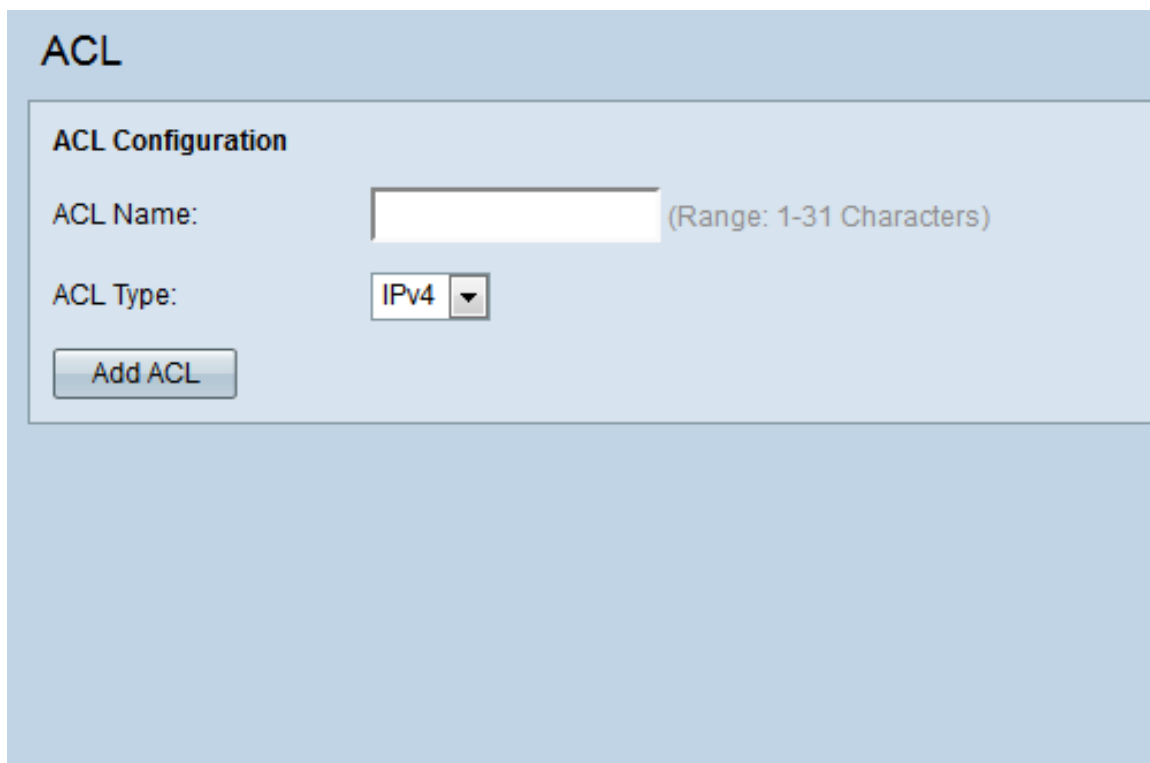
Softwareversion

·v1.2.0.2

ACL-Regelkonfiguration

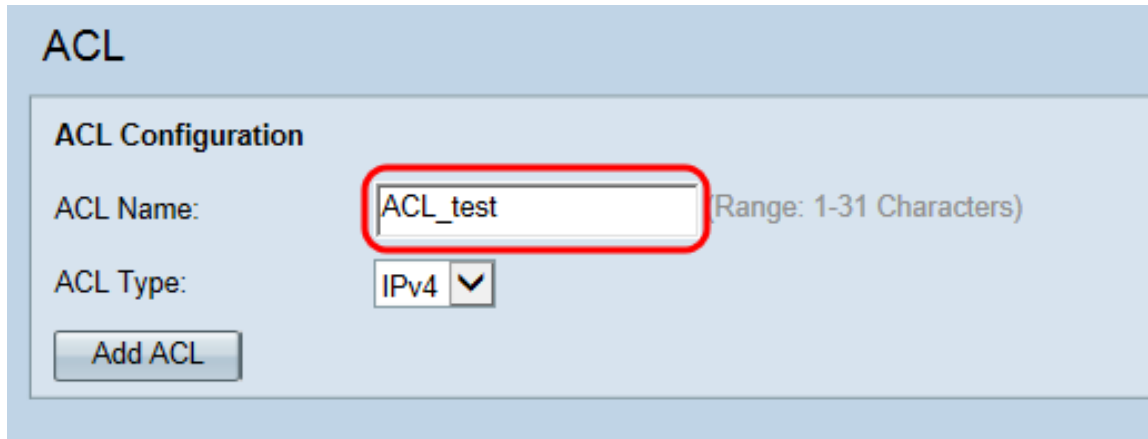
ACL-Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Client QoS** > **ACL** aus. Die Seite *ACL* wird geöffnet:



The screenshot shows the 'ACL' configuration page. At the top, the title 'ACL' is displayed. Below it, the section 'ACL Configuration' is visible. There are two main input fields: 'ACL Name:' with a text box and a note '(Range: 1-31 Characters)', and 'ACL Type:' with a dropdown menu currently set to 'IPv4'. At the bottom left of the configuration area, there is a button labeled 'Add ACL'.

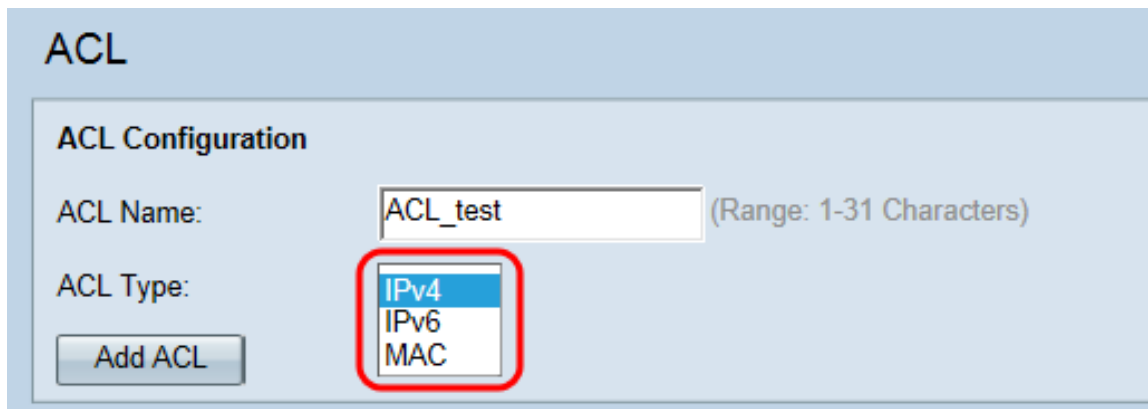
Schritt 2: Geben Sie den gewünschten ACL-Namen in das Feld *ACL Name ein*. Der Bereich liegt zwischen 1 und 31 Zeichen.



The screenshot shows the 'ACL Configuration' section of a network device's web interface. The 'ACL Name' field contains the text 'ACL_test' and is circled in red. To its right, a note indicates '(Range: 1-31 Characters)'. Below this, the 'ACL Type' dropdown menu is set to 'IPv4' and also has a red circle around it. An 'Add ACL' button is visible at the bottom left of the configuration area.

Hinweis: Der ACL-Name ist ein Bezeichner für die jeweilige ACL. sie hat keine Auswirkungen auf den Betrieb des Geräts.

Schritt 3: Wählen Sie in der Dropdown-Liste *ACL Type (ACL-Typ)* den ACL-Typ aus.



This screenshot shows the same 'ACL Configuration' interface as the previous one. The 'ACL Name' field still contains 'ACL_test'. The 'ACL Type' dropdown menu is now open, showing three options: 'IPv4', 'IPv6', and 'MAC'. The dropdown menu is circled in red. The 'Add ACL' button remains visible at the bottom left.

Folgende Optionen sind verfügbar:

- IPv4 - Eine 32-Bit-Adresse (vier Byte).
- IPv6 - Ein Nachfolger von IPv4 besteht aus einer 128-Bit-Adresse (8 Byte).
- MAC: Die MAC-Adresse ist die eindeutige Adresse, die einer Netzwerkschnittstelle zugewiesen ist.

Hinweis: IPv4- und IPv6-ACLs steuern den Zugriff auf Netzwerkressourcen anhand von Layer-3- und Layer-4-Kriterien. MAC-ACLs steuern den Zugriff auf der Grundlage von Layer-2-Kriterien.

Schritt 4: Klicken Sie auf **ACL hinzufügen**, um die neue ACL hinzuzufügen.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▼

ACL-Regelkonfiguration für IPv4 und IPv6

Hinweis: Die folgenden Screenshots beziehen sich auf IPv4-ACL-Regeln, sind aber mit IPv6-ACL-Regeln austauschbar.

Schritt 1: Wählen Sie eine Aktion für die Regel aus der Dropdown-Liste *Aktion* aus.

Action:

Match Every Packet:

Protocol: Select From List: ▼ Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port: Select From List: ▼ Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port: Select From List: ▼ Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: ▼ Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Die Optionen werden wie folgt beschrieben:

- Zulassen - Die Regel ermöglicht es dem gesamten Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteiern. Datenverkehr, der die Kriterien nicht erfüllt, wird verworfen.

- Verweigern: Die Regel verhindert, dass der gesamte Datenverkehr, der die Regelkriterien erfüllt, das WAP-Gerät betritt oder verlässt. Datenverkehr, der die Kriterien nicht erfüllt, wird an die nächste Regel weitergeleitet. Wenn es sich um die letzte Regel handelt, wird der nicht explizit zulässige Datenverkehr verworfen.

Schritt 2: Aktivieren oder deaktivieren Sie das Kontrollkästchen **Jedes Paket** zuordnen. Bei Auswahl dieser Regel, die entweder eine Zulassen- oder eine Ablehnungsaktion hat, wird der Frame oder das Paket unabhängig vom Inhalt zugeordnet.

The screenshot shows a configuration panel with the following settings:

- Action: Deny (dropdown)
- Match Every Packet: (highlighted with a red circle)
- Protocol: Select From List: ip (dropdown) | Match to Value: (text input) (Range: 0 - 255)
- Source IP Address: (text input) (xxx.xxx.xxx.xxx) | Wild Card Mask: (text input) (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")
- Source Port: Select From List: (dropdown) | Match to Port: (text input) (Range: 0 - 65535)
- Destination IP Address: (text input) (xxx.xxx.xxx.xxx) | Wild Card Mask: (text input) (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")
- Destination Port: Select From List: (dropdown) | Match to Port: (text input) (Range: 0 - 65535)
- Service Type
- IP DSCP: Select From List: (dropdown) | Match to Value: (text input) (Range: 0 - 63)
- IP Precedence: (text input) (Range: 0 - 7)
- IP TOS Bits: (text input) (Range: 00 - FF) | IP TOS Mask: (text input) (Range: 00 - FF)
- Delete ACL:

Hinweis: Wenn Sie dieses Feld auswählen, können Sie keine zusätzlichen Anpassungskriterien konfigurieren. Die Option **Jedes Paket** zuordnen ist für eine neue Regel standardmäßig ausgewählt. Sie müssen die Option zum Konfigurieren anderer Übereinstimmungsfelder deaktivieren.

Schritt 3: Aktivieren Sie das Kontrollkästchen **Protocol**, um eine L3- oder L4-Protokollabgleichbedingung basierend auf dem Wert des IP-Protokollfelds in IPv4-Paketen oder das Next Header-Feld in IPv6-Paketen zu verwenden. Wenn das Kontrollkästchen Protocol aktiviert ist, wählen Sie eine der folgenden Optionsfelder aus.

The close-up shows the 'Protocol' section with the following settings:

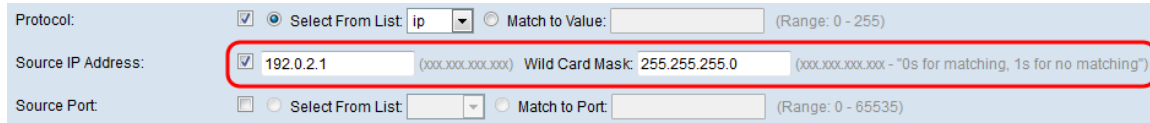
- Match Every Packet:
- Protocol: Select From List: ip (dropdown) | Match to Value: (text input) (Range: 0 - 255)
- Source IP Address: (text input) (xxx.xxx.xxx.xxx) | Wild Card Mask: (text input) (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Die Optionen werden wie folgt beschrieben:

- Select From List (Aus Liste auswählen): Wählen Sie ein Protokoll aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* aus. Folgende Optionen sind verfügbar:
 - IP - Das Internet Protocol (IP) ist das wichtigste Kommunikationsprotokoll in der Internet Protocol Suite für die netzwerkübergreifende Datenweitergabe.
 - ICMP - Das Internet Control Message Protocol (ICMP) ist ein Protokoll in der Internet Protocol Suite, das von Geräten wie Routern zum Senden von Fehlermeldungen verwendet wird.
 - IGMP - Das Internet Group Management Protocol (IGMP) ist ein Kommunikationsprotokoll, das vom Host verwendet wird, um Multicast-Gruppenmitgliedschaften in IPv4-Netzwerken herzustellen.
 - TCP - Das Transmission Control Protocol (TCP) ermöglicht es zwei Hosts, eine Verbindung herzustellen und Datenströme auszutauschen.
 - UDP - Das User Datagram Protocol ist ein Protokoll in der Internet Protocol Suite, das ein verbindungsloses Übertragungsmodell verwendet.

- "Match to Value" (Dem Wert zuordnen) - Geben Sie eine standardmäßige IANA-zugeordnete Protokoll-ID ein, die für alle nicht aufgelisteten Protokolle zwischen 0 und 255 liegt. Weitere Informationen zu IANA-zugewiesenen Protokoll-IDs finden Sie unter [Zugewiesene Internetprotokollnummern](#).

Schritt 4: Aktivieren Sie das Kontrollkästchen **Quell-IP-Adresse**, um eine IP-Adresse der Quelle in den Match-Zustand einzuschließen. Geben Sie die IP-Adresse und die Platzhaltermaske der Quelle in die entsprechenden Felder ein. Die Platzhaltermaske bestimmt, welche Bits der Quelladresse verwendet werden und welche ignoriert werden. Sie kann als invertierte Subnetzmaske betrachtet werden. Dies ist nützlich, um die Größe eines Netzwerks oder Subnetzes für einige Routing-Protokolle anzugeben oder einen Bereich von IP-Adressen zuzulassen oder zu verweigern.



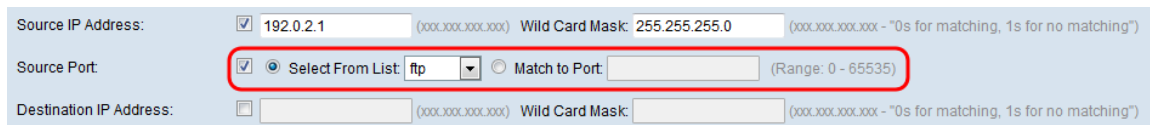
Protocol: Select From List: ip Match to Value: (Range: 0 - 255)

Source IP Address: 192.0.2.1 (xxx.xxx.xxx.xxx) Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Hinweis: Das Feld Platzhaltermaske ist erforderlich, wenn das Kontrollkästchen **Quell-IP-Adresse** aktiviert ist.

Schritt 5: Aktivieren Sie das Kontrollkästchen **Quellport**, um einen Quellport in die Übereinstimmung einzubeziehen. Wenn das Kontrollkästchen **Quellport** aktiviert ist, wählen Sie eine der folgenden Optionsschaltflächen aus.



Source IP Address: 192.0.2.1 (xxx.xxx.xxx.xxx) Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Die Optionen werden wie folgt beschrieben:

·Select From List (Aus Liste auswählen): Wählen Sie einen Quellport aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* aus. Folgende Optionen sind verfügbar:

- FTP - Das File Transfer Protocol (FTP) ist ein standardmäßiges Netzwerkprotokoll, das verwendet wird, um Dateien von einem Host zu einem anderen über ein TCP-basiertes Netzwerk wie das Internet zu übertragen.

- FTP-Daten - Ein Datenkanal, der von dem mit einem Client verbundenen Server initiiert wird, in der Regel über Port 20.

- HTTP - Das Hypertext Transfer Protocol (HTTP) ist ein Anwendungsprotokoll, das die Grundlage der Datenkommunikation für das World Wide Web bildet.

- SMTP - Das Simple Mail Transfer Protocol (SMTP) ist ein Internet-Standard für die Übertragung von E-Mails (E-Mail).

- SNMP - Das Simple Network Management Protocol (SNMP) ist ein Internetstandardprotokoll zur Verwaltung von Geräten in IP-Netzwerken.

- Telnet - Ein Sitzungsschichtprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um eine bidirektionale interaktive textorientierte Kommunikation bereitzustellen.

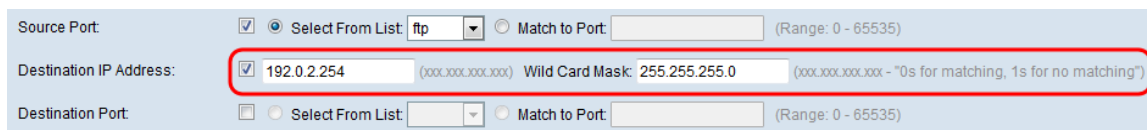
- TFTP - Das Trivial File Transfer Protocol (TFTP) ist ein Internet-Software-Dienstprogramm zur Übertragung von Dateien, das einfacher zu verwenden ist als FTP, aber weniger fähig ist.

- WWW - Das World Wide Web ist ein System von Internetservern, die HTTP-formatierte Dokumente unterstützen.

·Match to Port (Zuordnung zu Port) - Geben Sie im Feld *Übereinstimmung mit Port* die Portnummer zwischen 0 und 65535 für nicht aufgeführte Quellports ein. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

- 0 bis 1023 — Bekannte Ports.
- 1024 bis 49151 — Registrierte Ports
- 49152 bis 65535 — Dynamische und/oder private Ports

Schritt 6: Aktivieren Sie das Kontrollkästchen **Ziel-IP-Adresse**, um die IP-Adresse des Ziels in die Übereinstimmung einzubeziehen. Geben Sie die IP-Adresse und die Platzhaltermaske des Ziels in die entsprechenden Felder ein. Die Platzhaltermaske bestimmt, welche Bits der Quelladresse verwendet werden und welche ignoriert werden. Sie kann als invertierte Subnetzmaske betrachtet werden. Dies ist nützlich, um die Größe eines Netzwerks oder Subnetzes für einige Routing-Protokolle anzugeben oder einen Bereich von IP-Adressen zuzulassen oder zu verweigern.



Source Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

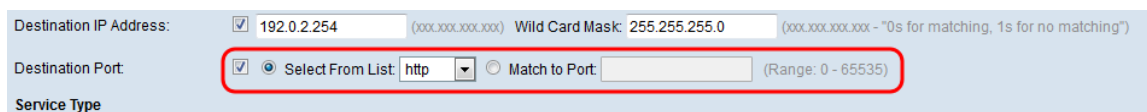
Destination IP Address: 192.0.2.254 (xxx.xxx.xxx.xxx) Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Hinweis: Das Kontrollkästchen *Wild Card Mask* (Platzhaltermaske) ist erforderlich, wenn das Kontrollkästchen **Destination IP Address (IP-Zieladresse)** aktiviert ist.

Hinweis: Wenn Sie nur eine einzige IP-Adresse zuordnen möchten, verwenden Sie die Platzhaltermaske 0.0.0.0.

Schritt 7: Aktivieren Sie das Kontrollkästchen **Destination Port (Zielport)**, um einen Zielport in die Übereinstimmung einzubeziehen. Wenn das Kontrollkästchen **Zielport** aktiviert ist, wählen Sie eine der folgenden Optionsfelder aus.



Destination IP Address: 192.0.2.254 (xxx.xxx.xxx.xxx) Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port: Select From List: http Match to Port: (Range: 0 - 65535)

Service Type

Die Optionen werden wie folgt beschrieben:

·Select From List (Aus Liste auswählen): Wählen Sie einen Zielport aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* aus. Folgende Dropdown-Listenoptionen sind verfügbar:

- FTP - Das File Transfer Protocol (FTP) ist ein standardmäßiges Netzwerkprotokoll, das verwendet wird, um Dateien von einem Host zu einem anderen über ein TCP-basiertes Netzwerk wie das Internet zu übertragen.
- FTP-Daten - Ein Datenkanal, der von dem mit einem Client verbundenen Server initiiert wird, in der Regel über Port 20.
- HTTP - Das Hypertext Transfer Protocol (HTTP) ist ein Anwendungsprotokoll, das die Grundlage der Datenkommunikation für das World Wide Web bildet.
- SMTP - Das Simple Mail Transfer Protocol (SMTP) ist ein Internet-Standard für die Übertragung von E-Mails (E-Mail).

- SNMP - Das Simple Network Management Protocol (SNMP) ist ein Internetstandardprotokoll zur Verwaltung von Geräten in IP-Netzwerken.

- Telnet - Ein Sitzungsschichtprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um eine bidirektionale interaktive textorientierte Kommunikation bereitzustellen.

- TFTP - Das Trivial File Transfer Protocol (TFTP) ist ein Internet-Software-Dienstprogramm zur Übertragung von Dateien, das einfacher zu verwenden ist als FTP, aber weniger fähig ist.

- WWW - Das World Wide Web ist ein System von Internetservern, die HTTP-formatierte Dokumente unterstützen.

·Match to Port (Zuordnung zu Port) - Geben Sie die Portnummer zwischen 0 und 65535 im Feld "*Übereinstimmung mit Port*" für nicht aufgeführte Zielports ein. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

- 0 bis 1023 — Bekannte Ports.

- 1024 bis 49151 — Registrierte Ports

- 49152 bis 65535 - Dynamische und/oder private Ports

Hinweis: Im Bereich "Service Type" (Servicetyp) kann nur einer der Services ausgewählt und für die Übereinstimmung hinzugefügt werden.

Konfiguration des ACL-Regelservicetyps für IPv4

Schritt 1: Aktivieren Sie das Kontrollkästchen **IP DSCP**, um die Pakete auf der Grundlage von IP-DSCP-Werten abzugleichen. DSCP wird verwendet, um die Verkehrsprioritäten über den IP-Header des Frames anzugeben. Dadurch werden alle Pakete für den zugehörigen Datenverkehrsstrom mit dem IP-DSCP-Wert kategorisiert, den Sie in der Liste auswählen. Wenn das Kontrollkästchen IP DSCP aktiviert ist, wählen Sie eine der folgenden Optionsfelder aus.

Service Type

IP DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

Die Optionen werden wie folgt beschrieben:

·Select From List (Aus Liste auswählen): Wählen Sie aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* einen IP-DSCP-Wert aus. Folgende Optionen sind verfügbar:

- DSCP Assured Forwarding (AS) - Ermöglicht dem Betreiber, die Zustellung sicherzustellen, solange der Datenverkehr die gezeichnete Rate nicht überschreitet.

- Class of Service (CS) - Ermöglicht Abwärtskompatibilität mit Netzwerkgeräten, die noch das Feld "Precedence" verwenden.

- Expedited Forwarding (EF) - Ermöglicht die Erstellung eines End-to-End-Service mit geringem Verlust, niedriger Latenz, niedrigem Jitter und zugesicherter Bandbreite durch

DS (DiffServ)-Domänen.

·Match to Value (Dem Wert zuordnen): Geben Sie den DSCP-Wert ein, der zwischen 0 und 63 im Feld *Match to Value (Zuordnung zum Wert) liegt*, um DSCP-Werte anzupassen.

Hinweis: Weitere Informationen zu DSCP finden Sie unter [DSCP und Precedence Values \(DSCP- und Prioritätswerte\)](#).

Schritt 2: Aktivieren Sie das Kontrollkästchen **IP Precedence** (IP-Rangfolge), um einen IP Precedence-Wert in die Übereinstimmung einzubeziehen. Dies ist ein Mechanismus für die Zuweisung einer Priorität für jedes IP-Paket, wobei 0 die niedrigste Priorität und 7 die höchste Priorität ist. Wenn das Kontrollkästchen **IP Precedence** (IP-Rangfolge) aktiviert ist, geben Sie einen IP-Rangfolgewert zwischen 0 und 7 ein.

IP DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Hinweis: Weitere Informationen zur IP-Rangfolge finden Sie unter [DSCP und Precedence Values \(DSCP- und Prioritätswerte\)](#).

Schritt 3: Aktivieren Sie das Kontrollkästchen **IP-TOS-Bits**, um die Type of Service (TOS)-Bits des Pakets im IP-Header als Entscheidungskriterien zu verwenden. Ein TOS-Feld wird verwendet, um die Priorität eines Datagramms anzugeben und es entsprechend zu routen. Wenn das Kontrollkästchen IP TOS Bits aktiviert ist, geben Sie die IP TOS-Bits ein, die zwischen 00-FF und der IP TOS-Maske liegen, die zwischen 00-FF in den entsprechenden Feldern liegt.

IP Precedence: 5 (Range: 0 - 7)

IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)

Delete ACL:

Schritt 4: (Optional) Wenn Sie die konfigurierte ACL löschen möchten, aktivieren Sie das Kontrollkästchen **ACL löschen**.

IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)

Delete ACL:

Schritt 5: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Action: Deny
 Match Every Packet:
 Protocol: Select From List: **ip** Match to Value: (Range: 0 - 255)
 Source IP Address: 192.0.2.1 Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")
 Source Port: Select From List: **ftp** Match to Port: (Range: 0 - 65535)
 Destination IP Address: 192.0.2.254 Wild Card Mask: 255.255.255.0 (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")
 Destination Port: Select From List: **http** Match to Port: (Range: 0 - 65535)
Service Type
 IP DSCP: Select From List: **af11** Match to Value: (Range: 0 - 63)
 IP Precedence: 5 (Range: 0 - 7)
 IP TOS Bits: 00 (Range: 00 - FF) IP TOS Mask: FF (Range: 00 - FF)
 Delete ACL:

ACL-Regelkonfiguration für IPv6

Schritt 1: Aktivieren Sie das Kontrollkästchen **IPv6 Flow Label**, um eine 20-Bit-Nummer festzulegen, die für ein IPv6-Paket eindeutig ist. Sie wird von Endstationen verwendet, um die QoS-Verarbeitung in Routern (Bereich 0 bis 1048575) anzugeben.

IPv6 Flow Label: **FFFFF** (Range: 00000 - FFFFF)
 IPv6 DSCP: Select From List: Match to Value: (Range: 0 - 63)
 Delete ACL:

Schritt 2: Aktivieren Sie das Kontrollkästchen **IPv6 DSCP**, um die Pakete auf der Grundlage von IP-DSCP-Werten abzugleichen. DSCP wird verwendet, um die Verkehrsprioritäten über den IP-Header des Frames anzugeben. Dadurch werden alle Pakete für den zugehörigen Datenverkehrsstrom mit dem IP-DSCP-Wert kategorisiert, den Sie in der Liste auswählen. Wenn das Kontrollkästchen **IPv6 DSCP** aktiviert ist, wählen Sie eine der folgenden Optionsfelder aus.

IPv6 Flow Label: (Range: 00000 - FFFFF)
 IPv6 DSCP: Select From List: **af11** Match to Value: (Range: 0 - 63)
 Delete ACL:

Die Optionen werden wie folgt beschrieben:

·Select From List (Aus Liste auswählen): Wählen Sie aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* einen IP-DSCP-Wert aus. Folgende Optionen sind verfügbar:

- DSCP Assured Forwarding (AS) - Ermöglicht dem Betreiber, die Zustellung sicherzustellen, solange der Datenverkehr die gezeichnete Rate nicht überschreitet.
- Class of Service (CS) - Ermöglicht Abwärtskompatibilität mit Netzwerkgeräten, die noch das Feld "Precedence" verwenden.
- Expedited Forwarding (EF) - Ermöglicht die Erstellung eines End-to-End-Service mit geringem Verlust, niedriger Latenz, geringem Jitter und garantierter Bandbreite durch DS

(DiffServ)-Domänen.

·Match to Value (Dem Wert zuordnen): Geben Sie den DSCP-Wert ein, der zwischen 0 und 63 im Feld *Match to Value (Zuordnung zum Wert)* liegt, um DSCP-Werte anzupassen.

Hinweis: Weitere Informationen zu DSCP finden Sie unter [DSCP und Precedence Values \(DSCP- und Prioritätswerte\)](#).

Schritt 3: (Optional) Wenn Sie die konfigurierte ACL löschen möchten, aktivieren Sie das Kontrollkästchen **ACL löschen**.

IPv6 Flow Label: FFFFF (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

Delete ACL:

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

Action: Deny

Match Every Packet:

Protocol: Select From List: ip Match to Value: (Range: 0 - 255)

Source IPv6 Address: 2001:DB8::1 Source IPv6 Prefix Length: 128 (Range: 1 - 128)

Source Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

Destination IPv6 Address: 2001:DB8:0:FFFF::FFF Destination IPv6 Prefix Length: 128 (Range: 1 - 128)

Destination Port: Select From List: ftp Match to Port: (Range: 0 - 65535)

IPv6 Flow Label: FFFFF (Range: 00000 - FFFFF)

IPv6 DSCP: Select From List: af11 Match to Value: (Range: 0 - 63)

Delete ACL:

Save

ACL-Regelkonfiguration für MAC

Schritt 1: Wählen Sie eine Aktion für die Regel aus der Dropdown-Liste *Aktion* aus.

Action: Deny Permit

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

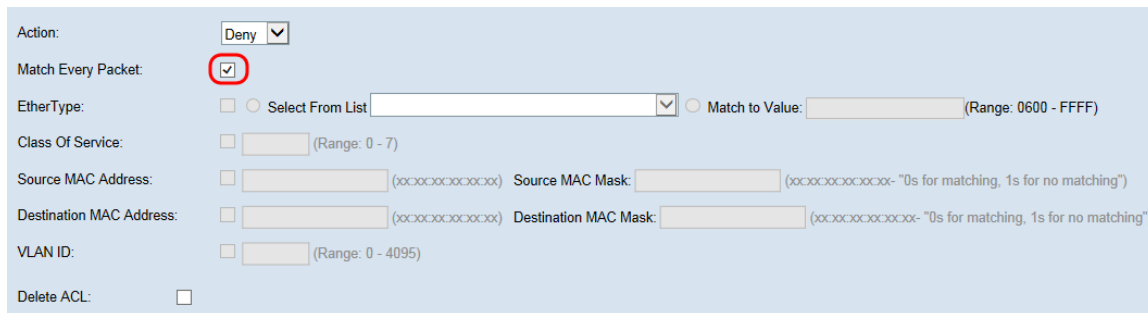
Delete ACL:

Die Optionen werden wie folgt beschrieben:

·Zulassen - Die Regel ermöglicht es dem gesamten Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteuern. Datenverkehr, der die Kriterien nicht erfüllt, wird verworfen.

·Verweigern: Die Regel verhindert, dass der gesamte Datenverkehr, der die Regelkriterien erfüllt, das WAP-Gerät betritt oder verlässt. Datenverkehr, der die Kriterien nicht erfüllt, wird an die nächste Regel weitergeleitet. Wenn es sich um die letzte Regel handelt, wird der nicht explizit zulässige Datenverkehr verworfen.

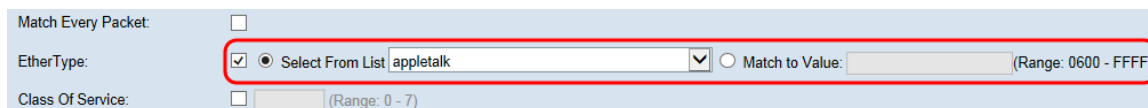
Schritt 2: Aktivieren oder deaktivieren Sie das Kontrollkästchen **Jedes Paket** zuordnen. Bei Auswahl dieser Regel, die entweder eine Zulassen- oder eine Ablehnungsaktion hat, wird der Frame oder das Paket unabhängig vom Inhalt zugeordnet.



The screenshot shows a configuration window for an ACL rule. The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is checked and circled in red. Below it are several fields for matching criteria, all of which are currently unchecked: 'EtherType', 'Class Of Service', 'Source MAC Address', 'Destination MAC Address', and 'VLAN ID'. The 'Delete ACL' checkbox is also unchecked.

Hinweis: Wenn Sie dieses Feld auswählen, können Sie keine zusätzlichen Anpassungskriterien konfigurieren. Die Option **Jedes Paket** zuordnen ist standardmäßig für eine neue Regel aktiviert. Sie müssen die Option zum Konfigurieren anderer Übereinstimmungsfelder deaktivieren.

Schritt 3: Aktivieren Sie das Kontrollkästchen **EtherType**, um die Anpassungskriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Wenn das Kontrollkästchen **EtherType** aktiviert ist, wählen Sie eine der folgenden Optionsfelder aus.



The screenshot shows the 'EtherType' section of the configuration window. The 'Match Every Packet' checkbox is unchecked. The 'EtherType' checkbox is checked and circled in red. The 'Select From List' radio button is selected, and the dropdown menu shows 'appletalk'. The 'Match to Value' radio button is unselected. The 'Class Of Service' checkbox is unchecked.

Die Optionen werden wie folgt beschrieben:

·Select from List (Aus Liste auswählen): Wählen Sie ein Protokoll aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* aus. Folgende Optionen sind verfügbar:

- AppleTalk - AppleTalk ist eine proprietäre Suite von Netzwerkprotokollen, die von Apple Inc. für ihre Macintosh-Computer entwickelt wurde. AppleTalk enthielt eine Reihe von Funktionen, mit denen lokale Netzwerke ohne vorherige Einrichtung verbunden werden konnten oder ein zentralisierter Router oder Server jeglicher Art erforderlich war.

- ARP - Das Address Resolution Protocol (ARP) ist ein Telekommunikationsprotokoll zur Auflösung von Netzwerkschichtadressen in Link Layer-Adressen, eine wichtige Funktion in Netzwerken mit mehreren Zugriffen.

- IPv4 - Internet Protocol Version 4 (IPv4) ist die vierte Version in der Entwicklung des Internet Protocol (IP). Es ist eines der Kernprotokolle standardbasierter Internetworking-Methoden im Internet.

- IPv6 - Internet Protocol Version 6 (IPv6) ist die neueste Version des Internetprotokolls (IP), dem Kommunikationsprotokoll, das ein Identifizierungs- und Standortsystem für Computer in Netzwerken bereitstellt und Datenverkehr über das Internet weiterleitet.

- IPX - Internetwork Packet Exchange (IPX) ist das Netzwerkschichtprotokoll in der IPX/SPX-Protokoll-Suite. IPX basiert auf dem IDP von Xerox Network Systems. Sie kann auch als Transportschichtprotokoll fungieren.

- NetBIOS - NetBIOS ist eine Abkürzung für Network Basic Input/Output System. Es stellt Dienste im Zusammenhang mit der Sitzungsschicht des OSI-Modells bereit, mit denen Anwendungen auf separaten Computern über ein LAN kommunizieren können. Als strikte API ist NetBIOS kein Netzwerkprotokoll.

- PPPOE - Das Point-to-Point Protocol over Ethernet (PPPoE) ist ein Netzwerkprotokoll zur Kapselung von PPP-Frames in Ethernet-Frames.

·Dem Wert zuordnen - Geben Sie eine benutzerdefinierte Protokollkennung ein, der Pakete zugeordnet werden. Der Wert ist eine vierstellige Hexadezimalzahl im Bereich von 0600 bis FFFF.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Class of Service**, um eine 802.1p-Benutzerpriorität für den Vergleich mit einem Ethernet-Frame einzugeben. Wie IP Precedence ist 0 die niedrigste Priorität und 7 die höchste. Der gültige Bereich liegt zwischen 0 und 7.

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)
Class Of Service: 5 (Range: 0 - 7)
Source MAC Address: Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Schritt 5: Aktivieren Sie das Kontrollkästchen **Quell-MAC-Adresse**, um eine Quell-MAC-Adresse einzugeben, die mit einem Ethernet-Frame verglichen werden soll. Wenn das Kontrollkästchen Quell-MAC-Adresse aktiviert ist, geben Sie die Quell-MAC-Adresse im Feld *Quell-MAC-Adresse* ein. Geben Sie dann die Quell-MAC-Adressenmaske in das Feld *Quell-MAC-Maske* ein. Dadurch wird festgelegt, welche Bits von der Quell-MAC-Adresse mit einem Ethernet-Frame verglichen werden.

Hinweis: Wenn nur eine MAC-Adresse zugeordnet werden soll, verwenden Sie die Maske der Platzhalterkarte 00:00:00:00:00:00.

Class Of Service: (Range: 0 - 7)
Source MAC Address: / Source MAC Mask: FF:FF:FF:FF:FF:FF (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
Destination MAC Address: Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Schritt 6: Aktivieren Sie das Kontrollkästchen **Ziel-MAC-Adresse**, um eine MAC-Zieladresse einzugeben, die mit einem Ethernet-Frame verglichen werden soll. Wenn das Kontrollkästchen Ziel-MAC-Adresse aktiviert ist, geben Sie die Ziel-MAC-Adresse im Feld *Ziel-MAC-Adresse* ein. Geben Sie dann die MAC-Adressmaske in das Feld *Ziel-MAC-Maske* ein. Dadurch wird festgelegt, welche Bits von der MAC-Zieladresse mit einem Ethernet-Frame verglichen werden.

Source MAC Address: Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
Destination MAC Address: / Destination MAC Mask: FF:FF:FF:FF:FF:FF (xxxxxxxxxxxx- "0s for matching, 1s for no matching")
VLAN ID: (Range: 0 - 4095)

Hinweis: Wenn nur eine MAC-Adresse zugeordnet werden soll, verwenden Sie die Maske der Platzhalterkarte 00:00:00:00:00:00.

Schritt 7: Aktivieren Sie das Kontrollkästchen **VLAN-ID**, um eine VLAN-ID einzugeben, die

mit einem Ethernet-Frame verglichen werden kann. Wenn das Kontrollkästchen **VLAN-ID** aktiviert ist, geben Sie die VLAN-ID in das *VLAN-ID*-Feld ein. Der Bereich der VLAN-ID liegt zwischen 0 und 4095.

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Schritt 8: (Optional) Wenn Sie die konfigurierte ACL löschen möchten, aktivieren Sie das Kontrollkästchen **ACL löschen**.

VLAN ID: (Range: 0 - 4095)

Delete ACL:

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

Action:

Match Every Packet:

EtherType: Select From List Match to Value: (Range: 0600 - FFFF)

Class Of Service: (Range: 0 - 7)

Source MAC Address: (xxxxxxxxxxxx) Source MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

Destination MAC Address: (xxxxxxxxxxxx) Destination MAC Mask: (xxxxxxxxxxxx- "0s for matching, 1s for no matching")

VLAN ID: (Range: 0 - 4095)

Delete ACL: