Konfigurieren der AP-Paketerfassung auf Catalyst 9800 Wireless Controllern

Inhalt

Einleitung

In diesem Dokument wird die Verwendung der Paketerfassungsfunktion von Access Points (AP) beschrieben.

Hintergrundinformationen

Diese Funktion steht nur Cisco IOS APs (wie AP 3702) zur Verfügung und ist daher nach Cisco IOS XE Version 17.3 veraltet.

Diese Lösung wird durch Intelligent Capture mit DNAC ersetzt oder alternativ durch Festlegen des Sniffer-Modus für den Access Point.

Mit der Funktion "AP Packet Capture" können Sie die Paketerfassung per Funk mit geringem Aufwand durchführen. Wenn die Funktion aktiviert ist, wird eine Kopie aller angegebenen Wireless-Pakete und Frames, die per Funk von/an APs gesendet und von/an eine bestimmte Wireless-MAC-Adresse empfangen werden, an einen FTP-Server (File Transfer Protocol) weitergeleitet, von dem Sie sie als .pcap-Datei herunterladen und mit Ihrem bevorzugten Paketanalyse-Tool öffnen können.

Nachdem die Paketerfassung gestartet wurde, erstellt der WAP, dem der Client zugeordnet ist, eine neue PCAP-Datei auf dem FTP-Server (stellen Sie sicher, dass der für die FTP-Anmeldung angegebene Benutzername über Schreibrechte verfügt). Wenn der Client Roaming durchläuft, erstellt der neue WAP eine neue .pcap-Datei auf dem FTP-Server. Wenn der Client zwischen SSIDs (Service Set Identifiers) wechselt, behält der WAP die Paketerfassung bei, sodass Sie alle Management-Frames sehen können, wenn der Client der neuen SSID zugeordnet wird.

Wenn Sie die Erfassung auf einer offenen SSID vornehmen (keine Sicherheit), können Sie den Inhalt der Datenpakete sehen, aber wenn der Client einer gesicherten SSID zugeordnet ist (eine kennwortgeschützte SSID oder 802.1x-Sicherheit), dann ist der Datenanteil der Datenpakete verschlüsselt und kann nicht im Klartext gesehen werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zugriff auf die Wireless-Controller über die Befehlszeilenschnittstelle (CLI) oder die grafische Benutzeroberfläche (GUI)
- FTP-Server
- .pcap-Dateien

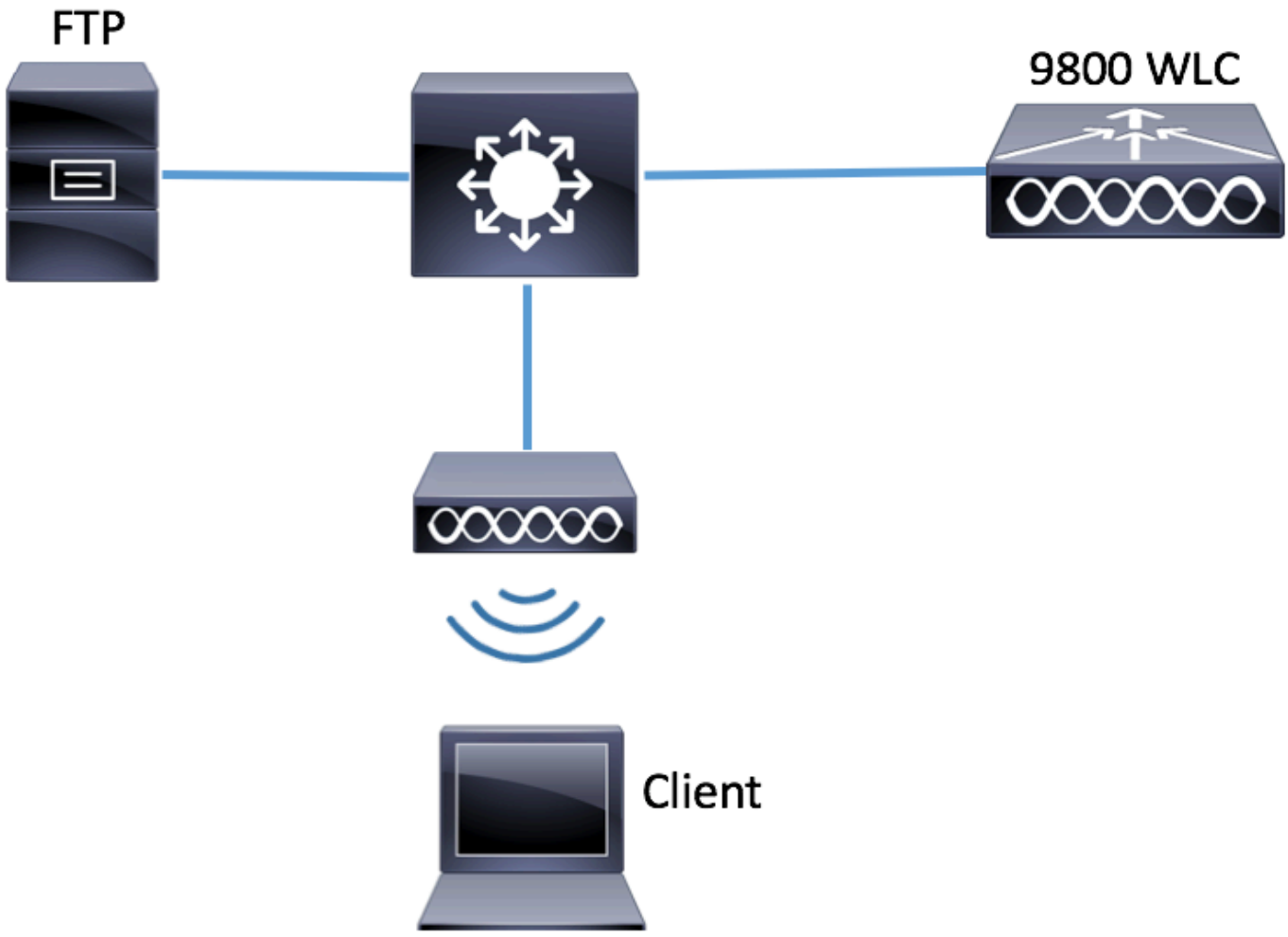
Verwendete Komponenten

- 9800 WLC v16.10
- AP 3700
- FTP-Server

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Konfiguration

Netzwerkdiagramm



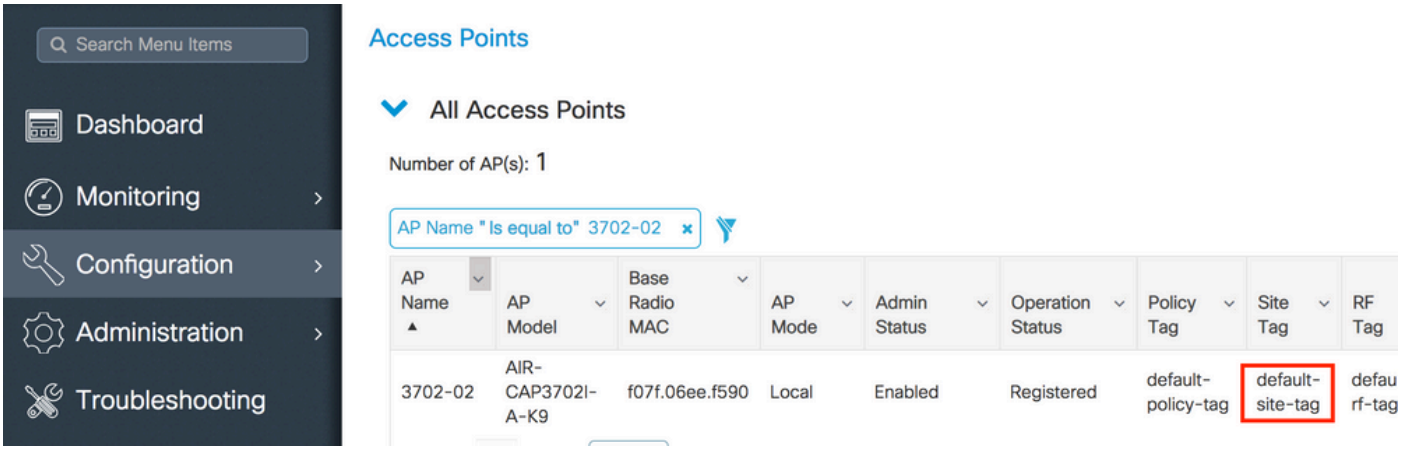
Konfigurationen

Überprüfen Sie vor der Konfiguration, welche APs vom Wireless-Client angeschlossen werden können.

Schritt 1: Überprüfen Sie die aktuelle Site-Tag-Nummer, die den APs zugeordnet ist, die der Wireless-Client für die Verbindung verwenden konnte.

GUI:

Navigieren Sie zu **Konfiguration > Wireless > Access Points.**



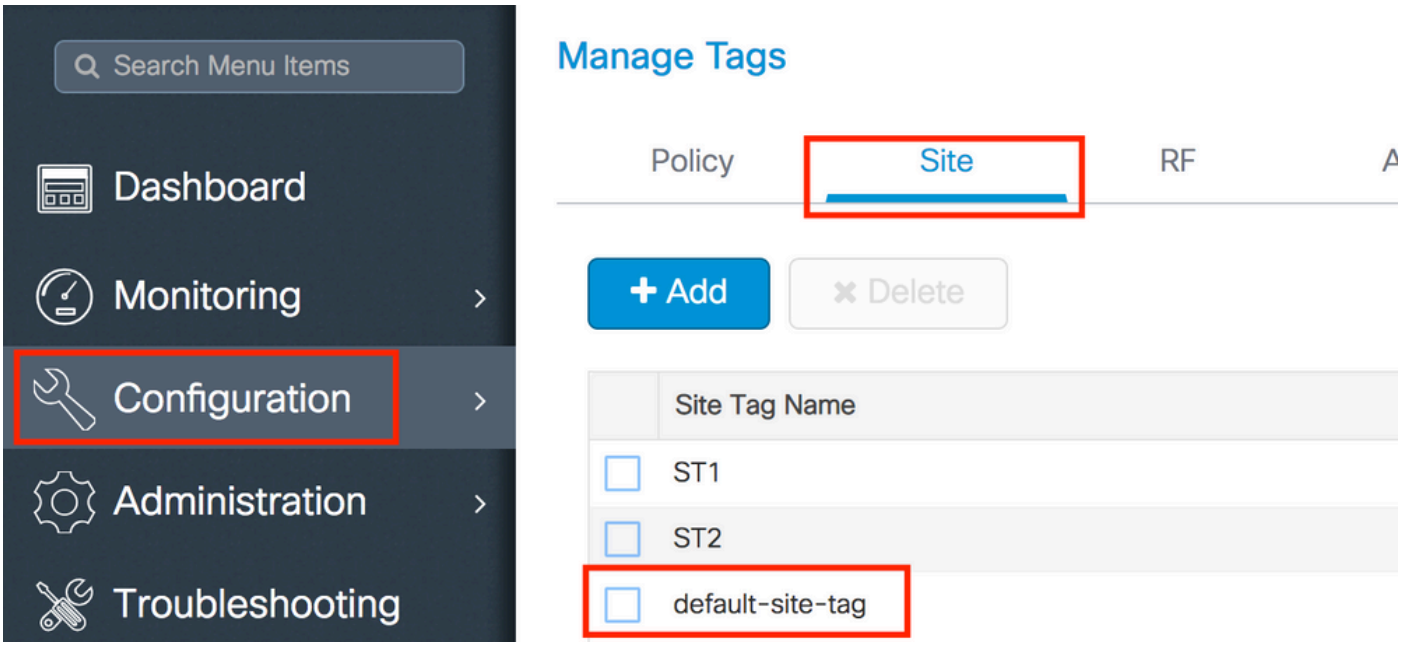
CLI:

```
# show ap tag summary | inc 3702-02

3702-02 f07f.06e1.9ea0 default-site-tag default-policy-tag default-rf-tag No Default
```

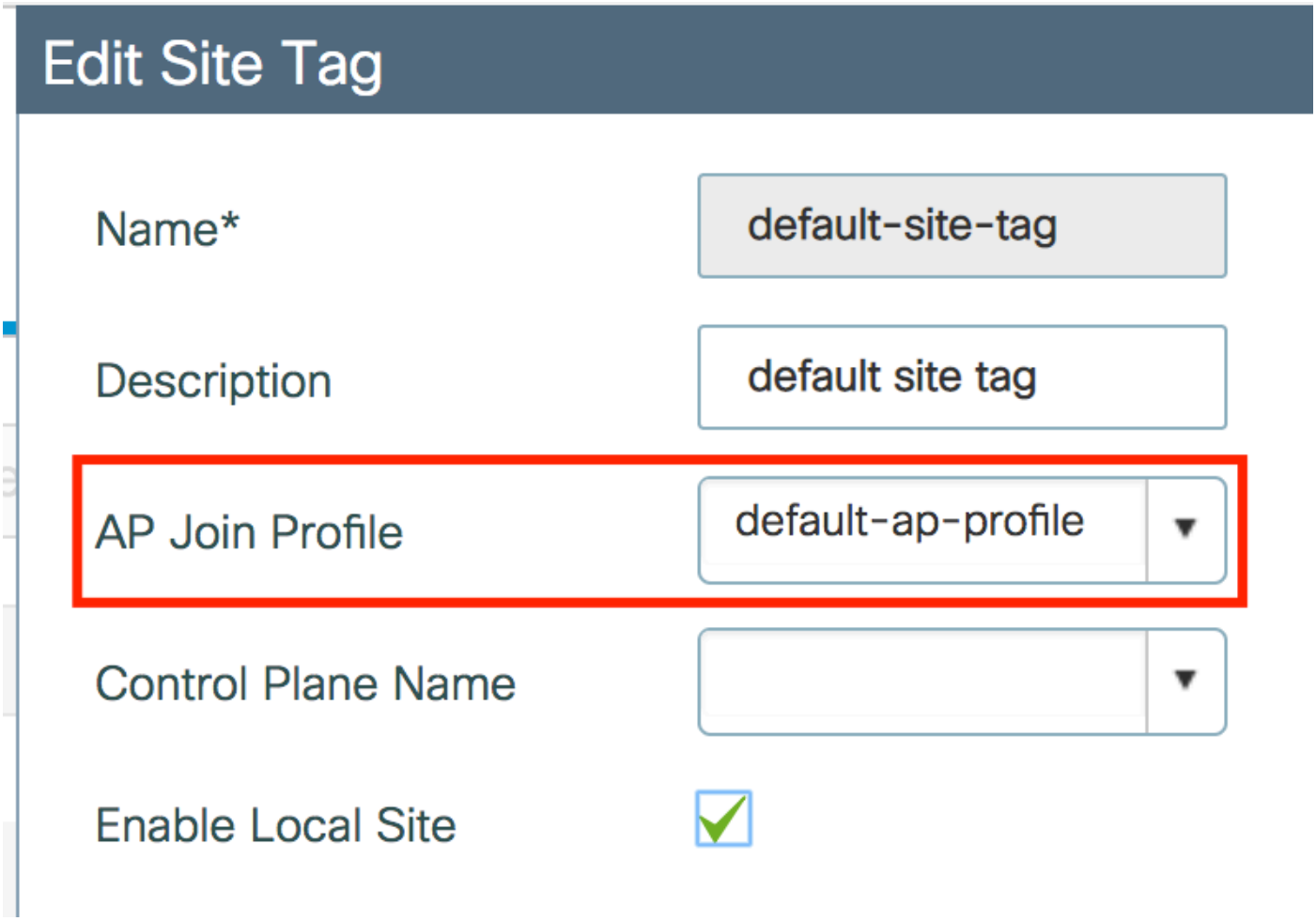
Schritt 2: Überprüfen Sie das mit dieser Site-Tag-Nummer verknüpfte AP-Teilnahmeprofil.

GUI:

Navigieren Sie zu **Konfiguration > Tags & Profile > Tags > Site > Site Tag Name**



Notieren Sie das zugeordnete Zugangsprofil für den Access Point.



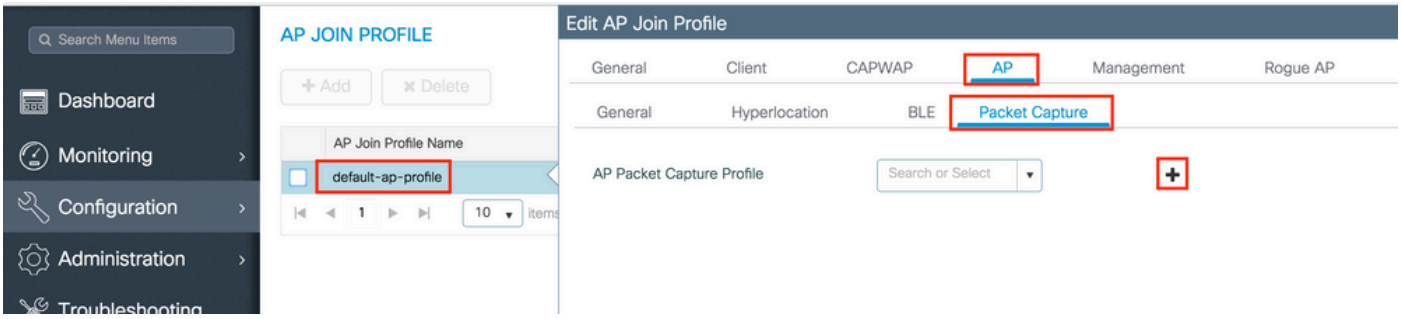
CLI:

```
# show wireless tag site detailed default-site-tag

Site Tag Name : default-site-tag
Description : default site tag
-------------------------------------
AP Profile : default-ap-profile
Local-site : Yes
Image Download Profile: default-me-image-download-profile
```

Schritt 3: Fügen Sie die Paketerfassungseinstellungen im AP-Join-Profil hinzu.

GUI:

Navigieren Sie zu **Configuration > Tags & Profiles > AP Join > AP Join Profile Name > AP > Packet Capture,** und fügen Sie ein neues **AP Packet Capture Profile hinzu.**

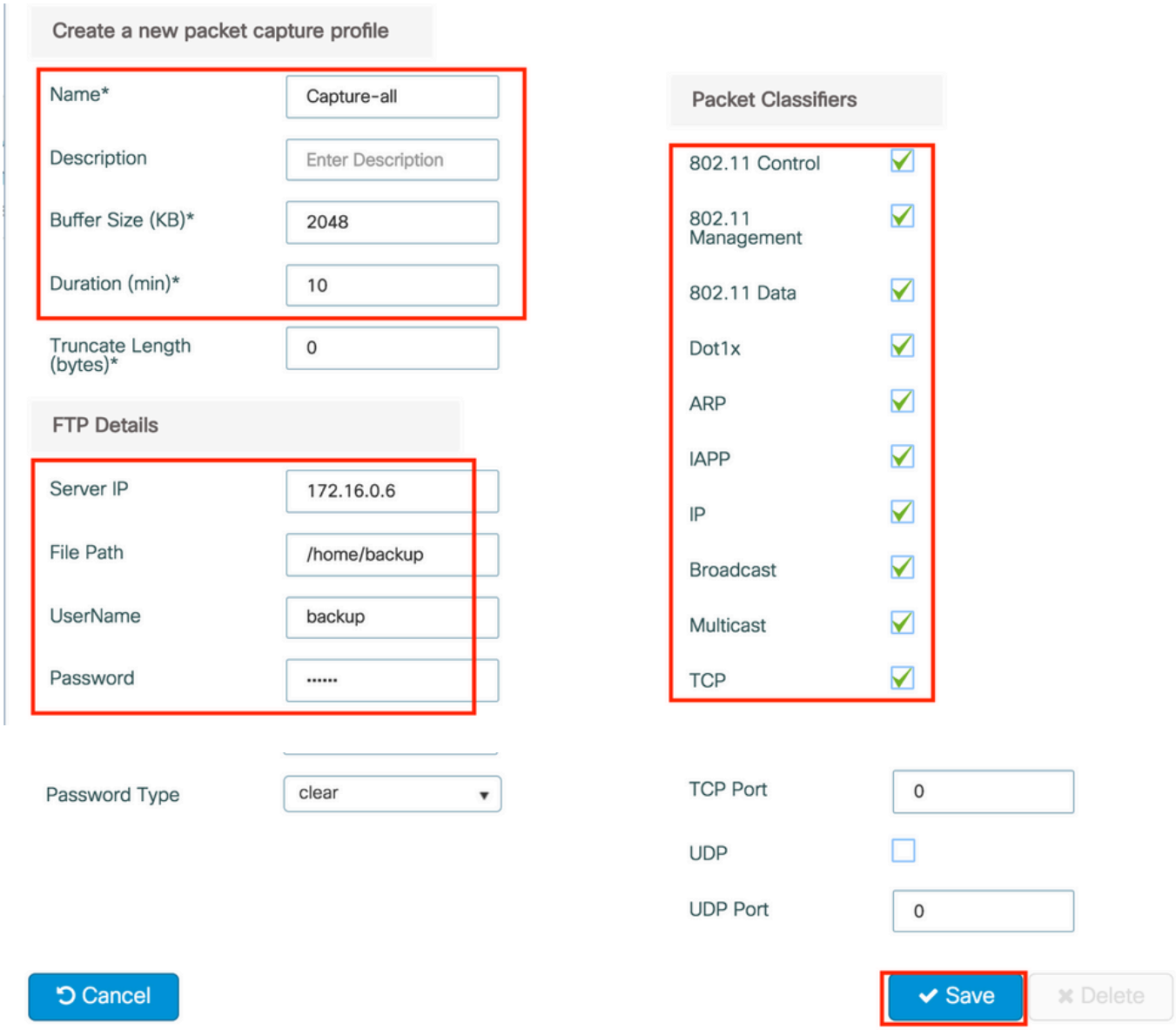


Wählen Sie einen Namen für das Paketerfassungsprofil aus, und geben Sie die FTP-Serverdetails

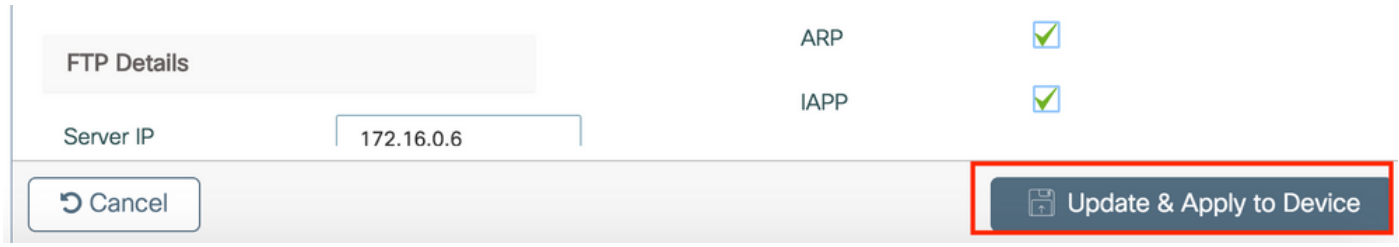
ein, an die die APs die Paketerfassung senden. Stellen Sie außerdem sicher, dass Sie die Art von Paketen auswählen, die überwacht werden sollen.

Puffergröße = 1024-4096

Dauer = 1-60



Klicken Sie nach dem Speichern des Erfassungsprofils auf **Aktualisieren und auf Gerät anwenden.**



CLI:

```
# config t
# wireless profile ap packet-capture Capture-all
```

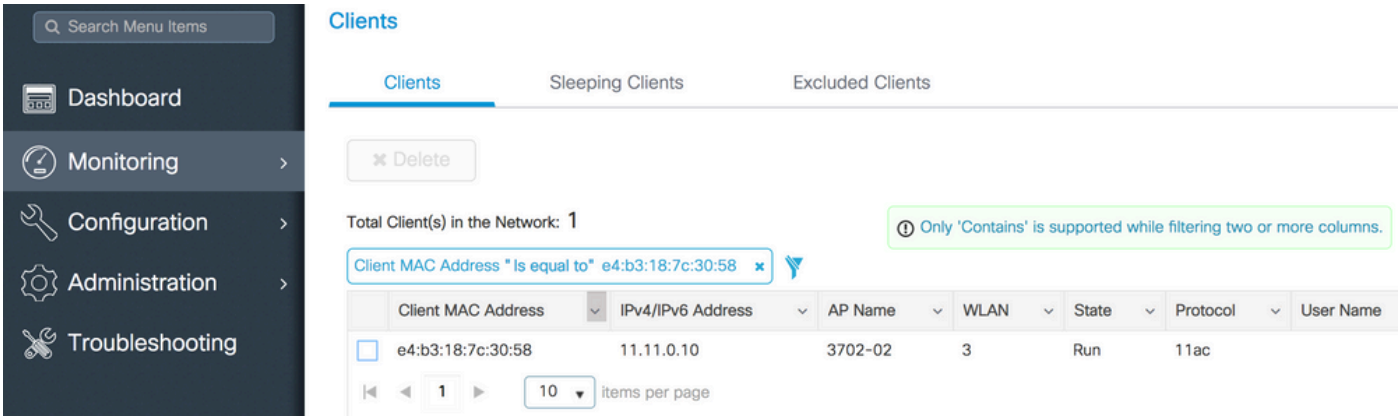
```
# classifier arp
# classifier broadcast
# classifier data
# classifier dot1x
# classifier iapp
# classifier ip
# classifier tcp
# ftp password 0 backup
# ftp path /home/backup
# ftp serverip 172.16.0.6
# ftp username backup
# exit

# ap profile default-ap-profile
# packet-capture Capture-all
# end

# show wireless profile ap packet-capture detailed Capture-all

Profile Name : Capture-all
Description  :
-------------------------------------------------
Buffer Size       : 2048 KB
Capture Duration  : 10 Minutes
Truncate Length   : packet length
FTP Server IP     : 172.16.0.6
FTP path          : /home/backup
FTP Username      : backup

Packet Classifiers
  802.11 Control  : Enabled
  802.11 Mgmt     : Enabled
  802.11 Data     : Enabled
  Dot1x           : Enabled
  ARP             : Enabled
  IAPP            : Enabled
  IP              : Enabled
  TCP             : Enabled
  TCP port        : all
  UDP             : Disabled
  UDP port        : all
  Broadcast       : Enabled
  Multicast       : Disabled
```

Schritt 4: Stellen Sie sicher, dass der zu überwachende Wireless-Client bereits mit einer der SSIDs und einem der APs verbunden ist, denen das Tag zugewiesen wurde, an dem das Zugangsprofil des AP mit den Paketerfassungseinstellungen zugewiesen wurde. Andernfalls kann die Erfassung nicht gestartet werden.

> **Tipp:** Wenn Sie eine Fehlerbehebung für den Grund durchführen möchten, aus dem ein Client keine Verbindung zu einer SSID herstellen kann, können Sie eine Verbindung zu einer SSID herstellen, die einwandfrei funktioniert, und dann zu der ausgefallenen SSID wechseln. Die Erfassung folgt dem Client und erfasst dessen gesamte Aktivität.

GUI:

Navigieren Sie zu **Überwachung > Wireless > Clients**



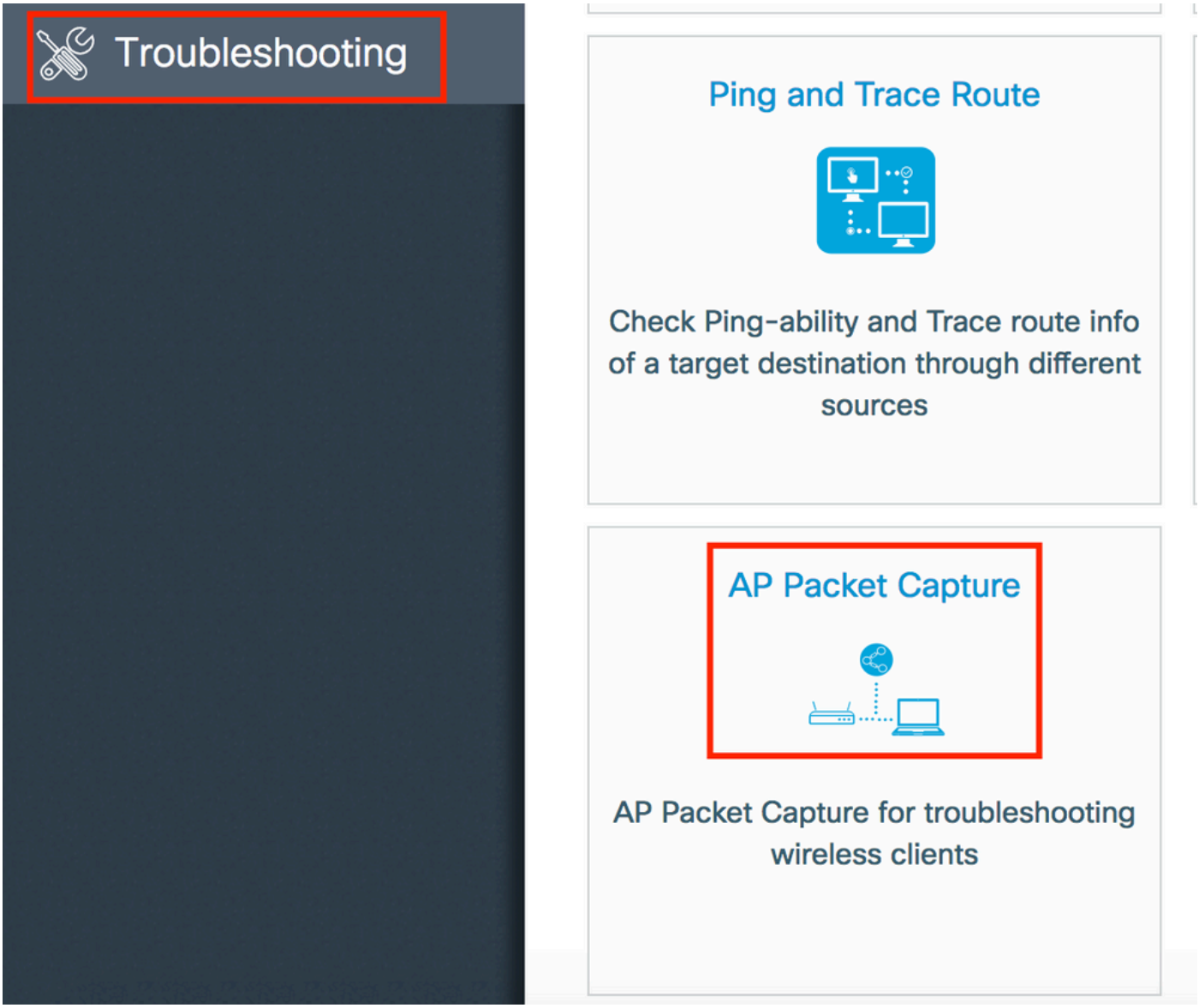
CLI:

```
# show wireless client summary | inc e4b3.187c.3058

e4b3.187c.3058 3702-02 3 Run 11ac
```

Schritt 5: Erfassung starten

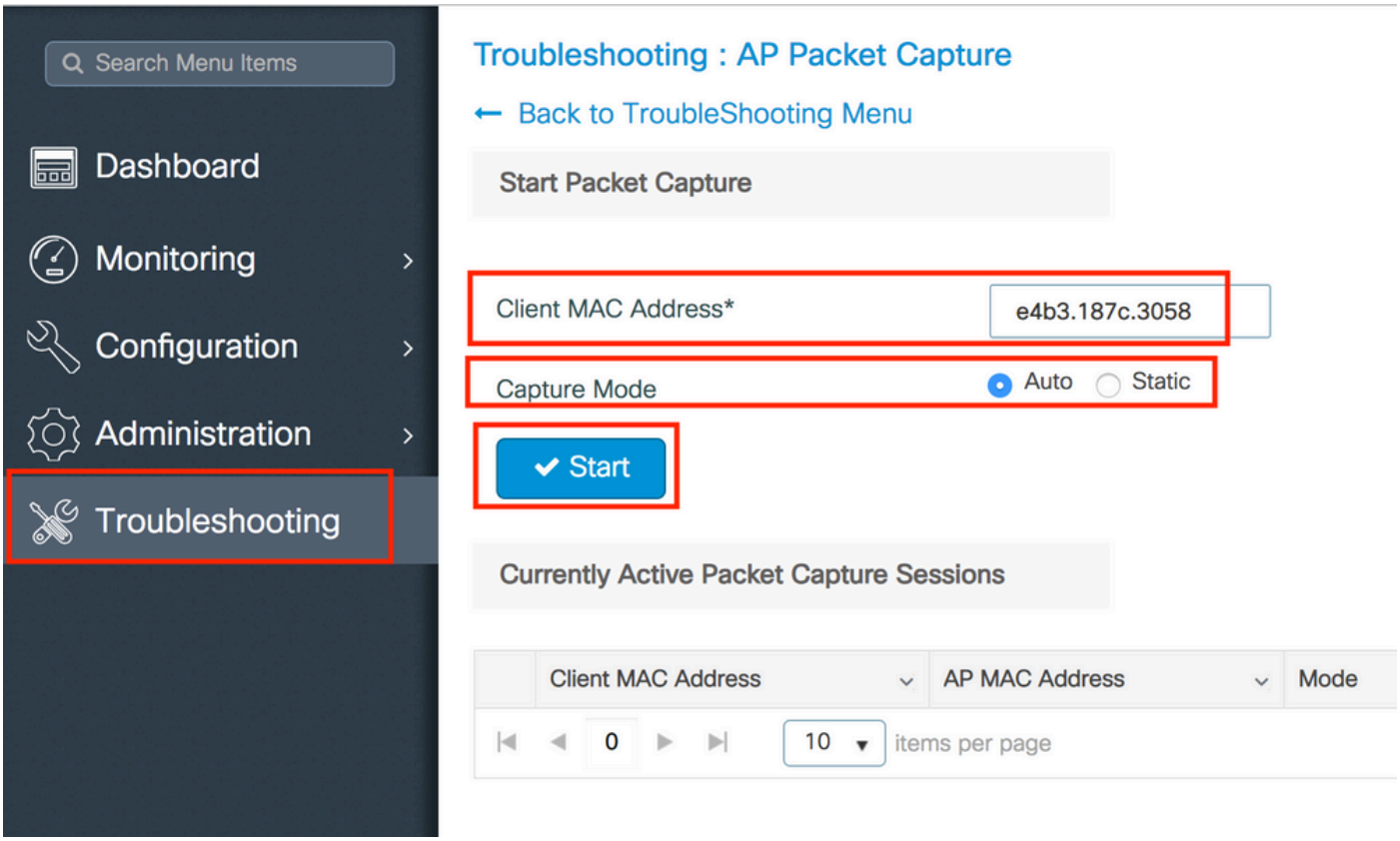
GUI:

Navigieren Sie zu **Fehlerbehebung > AP-Paketerfassung.**

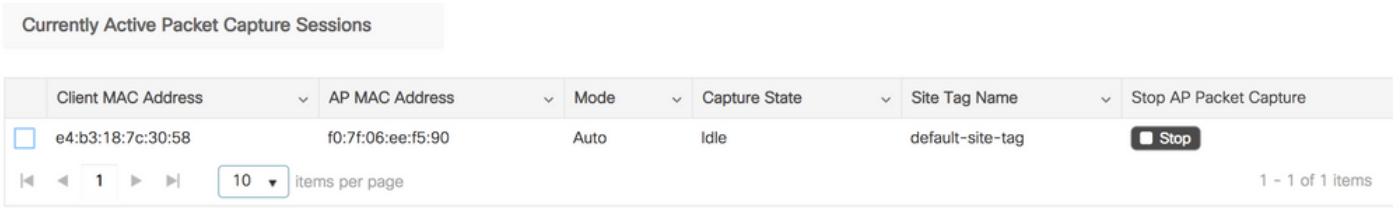


Geben Sie die MAC-Adresse des zu überwachenden Clients ein, und wählen Sie den **Erfassungsmodus aus. Auto** bedeutet, dass jeder WAP, mit dem der WLAN-Client verbunden ist, automatisch eine neue .pcap-Datei erstellt. **Statisch** ermöglicht die Auswahl eines bestimmten WAP zur Überwachung des Wireless-Clients.

Starten Sie die Erfassung mit **Start.**



Dann können Sie den aktuellen Zustand der Erfassung sehen:



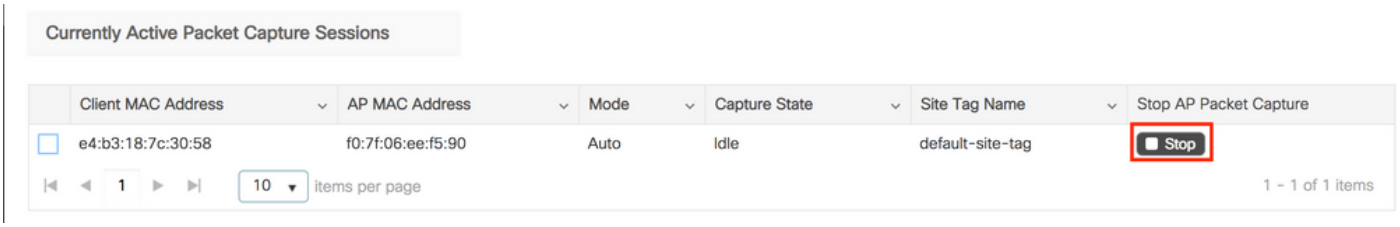
CLI:

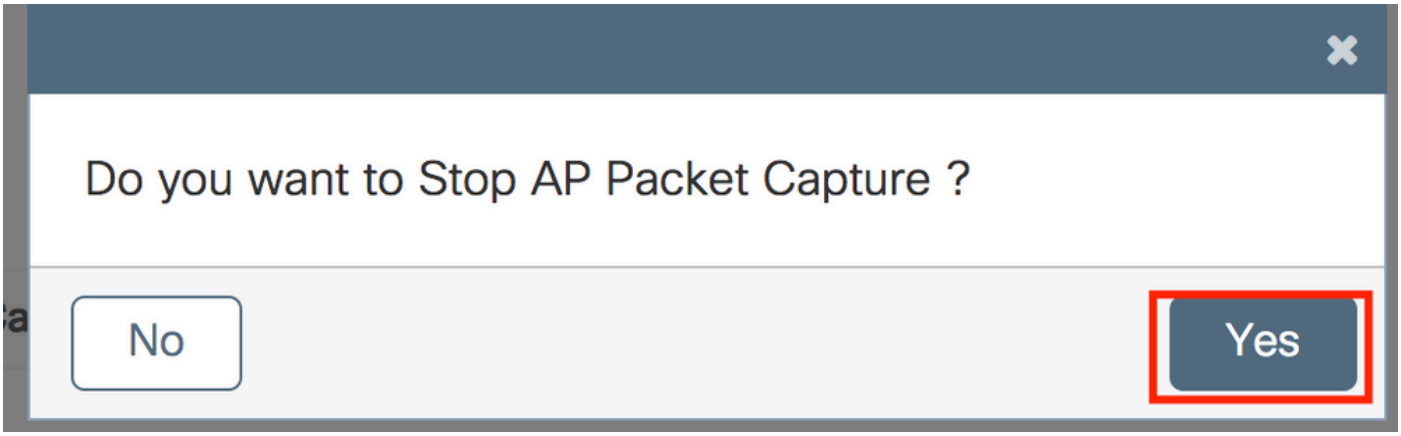
```
# ap packet-capture start <E4B3.187C.3058> auto
```

Schritt 6: Erfassung beenden

Sobald das gewünschte Verhalten erfasst wurde, beenden Sie die Erfassung entweder über die GUI oder die CLI:

GUI:



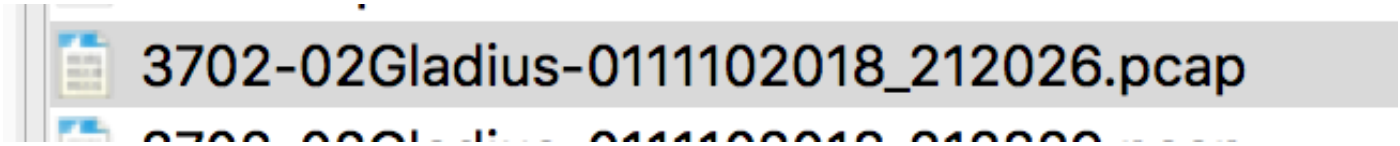


CLI:

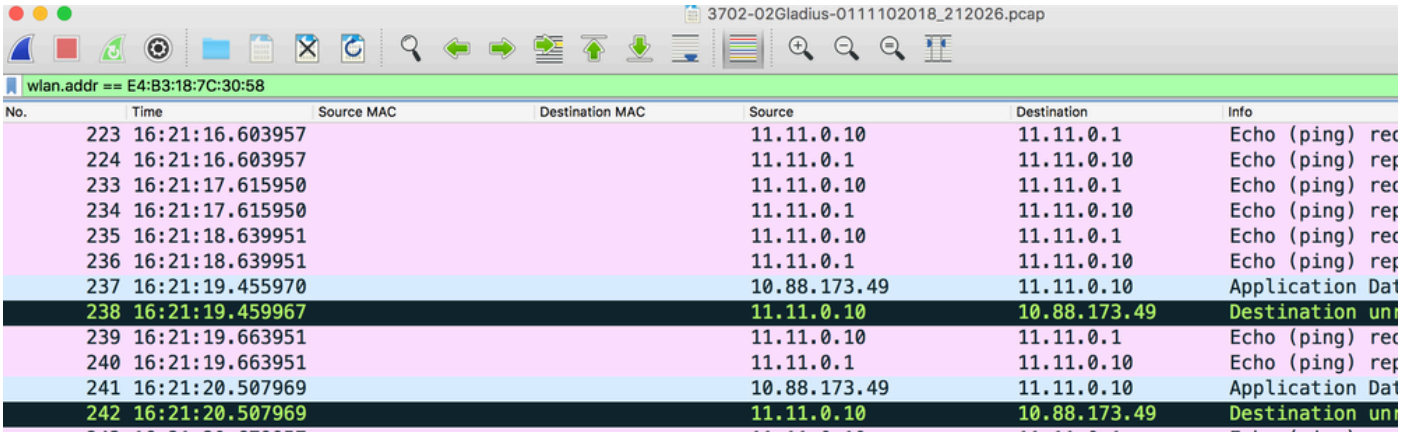
```
# ap packet-capture stop <E4B3.187C.3058> all
```

Schritt 7. Sammeln Sie die .pcap-Datei vom FTP-Server

Sie müssen eine Datei mit dem Namen <ap-name><9800-wlc-name>-<##-file><Tag><Monat><Jahr>_<Stunde><Minute><Sekunde>.pcap finden.



Schritt 8: Sie können die Datei mit Ihrem bevorzugten Paketanalyse-Tool öffnen.



Überprüfung

Sie können diese Befehle verwenden, um die Konfiguration der Paketerfassungsfunktion zu überprüfen.

```
# show ap status packet-capture

Number of Clients with packet capture started : 1

Client MAC      Duration(secs)   Site tag name            Capture Mode
-----------------------------------------------------------------------
e4b3.187c.3058  600              default-site-tag         auto
```

```
# show ap status packet-capture detailed e4b3.187c.3058

Client MAC Address    : e4b3.187c.3058
Packet Capture Mode   : auto
Capture Duration      : 600 seconds
Packet Capture Site   : default-site-tag

Access Points with status
AP Name                  AP MAC Addr     Status
-----------------------------------------------------
APf07f.06e1.9ea0         f07f.06ee.f590  Started
```

Fehlerbehebung

Sie können zur Fehlerbehebung für diese Funktion die folgenden Schritte durchführen:

Schritt 1: Debug-Bedingung aktivieren

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules debug
```

Schritt 2: Wiedergabe des Verhaltens

Schritt 3: Die aktuelle Uhrzeit des Controllers überprüfen, um die Anmeldezeiten nachverfolgen zu können

```
# show clock
```

Schritt 4: Protokolle sammeln

```
# show logging process wncmgrd internal | inc ap-packet-capture
```

Schritt 5: Setzen Sie die Protokollbedingung auf die Standardwerte zurück.

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules notice
```

> **Hinweis**: Es ist sehr wichtig, dass Sie nach einer Sitzung zur Fehlerbehebung die Protokollstufen zurücksetzen, um die Erstellung unnötiger Protokolle zu vermeiden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.