Versionsinfo:

Firmware für SG3218XP-M2(UN) 1.0. Diese Firmware ist vollständig an Omada Controller V5.14 angepasst.

Notiz:

Wenn Sie die Konfiguration vor einem Upgrade gespeichert und nur ACL-Zulassungseinträge für konfiguriert haben

Login-Zugriffskontrolle, nach dem Upgrade sind DHCP- und ARP-Pakete nicht in der ACL-Whitelist enthalten

wird gelöscht, was die Interaktion mit Uplink- und Downlink-Geräten verhindert und Benutzer verursacht

Es ist nicht möglich, dynamische IP-Adressen für den Internetzugang zu erhalten.

Die Lösung besteht darin, zwei Regeln zu konfigurieren:

1. Eine MAC/Combine-ACL-Zulassungsregel für Typ 0806, um ARP-Pakete zuzulassen.

2. Eine MAC/Combine-ACL-Zulassungsregel für Quell-MAC entspricht der MAC-Adresse des DHCP-Servers

um die vom DHCP-Server gesendeten Pakete zuzulassen

Neue Funktionen:

1. Fügen die Unterstützung für Cloud-Firmware-Überprüfung und -Upgrade bei eigenständiger Nutzung hinzu.

2. Fügen die Unterstützung für VLAN-spezifische Portisolation hinzu.

3. Fügen die Unterstützung für RSPAN hinzu.

4. Fügen die Unterstützung für DHCP Option 43 hinzu.

5. Fügen die Unterstützung für DHCP-Filter pro VLAN bei eigenständiger Nutzung hinzu.

6. Unterstützung für die Zuweisung von IP-Adressen mit 31-stelliger Subnetzmaske in VLAN-Schnittstellen hinzufügen.

7. Fügen die Unterstützung für die Verwendung von Domänennamen bei der Konfiguration des NTP-Servers hinzu.

8. Fügen die Unterstützung für statische IP-Bindung mit MAC-Adress-Platzhaltern hinzu.

9. Fügen die Unterstützung für das Aktivieren/Deaktivieren des Schalters hinzu, der Broadcasts im Zusammenhang mit dem Omada-Controller sendet

Pakete über CLI.

10. Unterstützung für den automatischen Import/Export von IMPB-Einträgen hinzufügen.

11. Wenn das Gerät vom Omada-Controller verwaltet wird, fügen Sie den SSH-Ein/Aus-Schalter auf der WebUI hinzu, falls dies der Fall ist

Der Gerätestatus auf dem Controller ist abnormal.

12. Unterstützung für die Konfiguration eines statischen DNS-Servers bei eigenständiger Nutzung hinzufügen.

13. Fügen die Unterstützung für die Übertragung von Portnamen hinzu, die auf dem Omada-Controller konfiguriert sind, an den Switch.

14. Fügen die Unterstützung für Befehle hinzu, die zwischen Blacklist und Whitelist für ACL bei eigenständiger Verwendung wechseln.

15. Fügen den Controller-Protokollen den Text „Erkannte Schleife“ hinzu, wenn Schleifen über die Loopback-Erkennung erkannt werden.

16. Fügen die Unterstützung für die Clusterbereitstellung hinzu.

Verbesserungen:

1. Legen die Loopback-Schnittstelle als globale Quellschnittstelle für die gesamte SNMP-Kommunikation zwischen fest

der SNMP-Client und -Server.

2. Standard-NTP-Server aktualisiert.

3. OpenSSL-Bibliothek aktualisiert.

4. Deaktivieren standardmäßig den HTTP-Zugriff bei Standalone-Nutzung.

5. Fügen eine Warnmeldung hinzu, wenn Sie PortFast an einem Port konfigurieren.

6. Vereinheitlichen Sie das von allen Omada-Switches gesendete DHCP-Vendor-Class-Identifier-Attribut.

7. Fügen das Feld „lldpRemTimeMark“ in der Antwort des Geräts auf „lldpRemTable“ in der öffentlichen SNMP-Bibliothek hinzu.

8. Unterstützung für die Bearbeitung von Standard-OUI-Vorlagen für Sprach-VLAN hinzufügen.

9. LLDP standardmäßig aktiviert.

Fehler behoben:

1. Das Kompatibilitätsproblem zwischen Remote Syslog und Visual Syslog Server wurde behoben.

2. Die abnormale Konvergenz von Spanning Tree bei hoher Clientanzahl wurde behoben.

3. Das Problem wurde behoben, bei dem die Konfiguration von sFlow ohne Beschreibung zu Konfigurationsfehlern führte

auf WebUI unter eigenständiger Nutzung.

4. Das Problem, das beim Hinzufügen von 5 illegalen SNMPv3-AuthPriv-Benutzern zu Fehlern auf Geräten führte, wurde behoben

gesamt.

5. Die RCE- und DOS-Schwachstellen in cloud-brd wurden behoben.

6. Die Schwachstellen der Broken Access Control wurden behoben.