Diese Firmware ist vollständig an Omada Controller V5.14 angepasst
Neue Funktionen/Fehler behoben:
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. Fügen die Unterstützung für die Zuweisung von IP-Adressen mit 31-stelliger Subnetzmaske in VLAN-Schnittstellen hinzu.
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 Omada-Controller-bezogen sendet
Broadcast-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. Legen die Loopback-Schnittstelle als globale Quellschnittstelle für die gesamte SNMP-Kommunikation fest
zwischen SNMP-Client und Server.
14. Fügen die Unterstützung für die Übertragung von Portnamen hinzu, die auf dem Omada-Controller konfiguriert sind, an den Switch.
15. Unterstützung für Befehle zum Umschalten zwischen Blacklist und Whitelist für ACL im Standalone-Modus hinzufügen
Verwendung.
16. Standard-NTP-Server aktualisiert.
17. OpenSSL-Bibliothek aktualisiert.
18. Deaktivieren die standardmäßig den HTTP-Zugriff bei Standalone-Nutzung.
19. Fügen eine Warnmeldung hinzu, wenn Sie PortFast an einem Port konfigurieren.
20. Beheben das Kompatibilitätsproblem zwischen Remote Syslog und Visual Syslog Server.
21. Vereinheitlichen Sie das von allen Omada-Switches gesendete DHCP-Vendor-Class-Identifier-Attribut.
22. Fügen das Feld „lldpRemTimeMark“ in der Antwort des Geräts auf „lldpRemTable“ im öffentlichen SNMP hinzu
Bibliothek.
23. Die abnormale Konvergenz von Spanning Tree bei hoher Clientanzahl wurde behoben.
24. Das Problem wurde behoben, zu dem die Konfiguration von sFlow ohne Beschreibung führte
Konfigurationsfehler auf der WebUI bei eigenständiger Nutzung.

25. Das Problem wurde behoben, das beim Hinzufügen von 5 illegalen SNMPv3-Geräten zu Fehlern führte
AuthPriv-Benutzer insgesamt.
26. Fügen den Text „Erkannte Schleife“ in Controller-Protokollen hinzu, wenn Schleifen über Loopback erkannt werden
Erkennung.
27. Unterstützung für die Bearbeitung von Standard-OUI-Vorlagen für Sprach-VLAN hinzugefügt.
28. Unterstützung für den Temperaturabruf über SNMP hinzufügen.
29. Unterstützung für IMPBv6 hinzufügen, um parallel zur IPv6-ACL zu arbeiten.
30. Beheben das Problem der ungewöhnlich hohen CPU-Auslastung, die durch den Datenverkehr verursacht wird
Weiterleitung, wenn die MAC-Adresstabelle den Grenzwert überschreitet.
31. Fügen unter „Standard“ oder „Standard“ Unterstützung für den Abgleich von IPv6-Verkehr mithilfe von MAC ACL und MAC VLAN hinzu
Enterprisev4-Vorlage.
32. Fügen die Unterstützung für Combine ACL/IP ACL hinzu, um parallel mit MAC ACL und MAC VLAN zu arbeiten
für den Abgleich und die Durchsetzung.
33. Das Problem wurde behoben, bei dem die Aktivierung des QinQ-Stacks auf einem UNI-Port zu doppelt markierten Pings führte
scheitern.
34. Das Problem wurde behoben, bei dem MAC ACL und MAC VLAN nicht mit DHCP- und ARP-Paketen übereinstimmen konnten.
35. Unterstützung für die Clusterbereitstellung hinzufügen.
36. LLDP standardmäßig aktiviert.
Hinweis: Wenn Sie die Konfiguration vor einem Upgrade gespeichert und nur die ACL-Zulassung konfiguriert haben
Einträge zur Login-Zugriffskontrolle, nach dem Upgrade keine DHCP- und ARP-Pakete mehr enthalten
in der ACL-Whitelist werden gelöscht, wodurch eine Interaktion mit Uplink und Downlink verhindert wird
Geräte und führen dazu, dass Benutzer keine dynamischen IP-Adressen für den Internetzugang erhalten können.
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 von DHCP
Server, um die vom DHCP-Server gesendeten Pakete zuzulassen.