Konfigurieren des BDRL-Durchsatzlimits (QoS) auf Catalyst Wireless Controllern der Serie 9800 mit AAA Override

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Beispiel: Gast- und Unternehmens-QoS-Richtlinien Konfigurieren AAA-Server und Methodenliste WLAN-Richtlinie, Site-Tag und AP-Tag OoS Überprüfung Auf dem WLC Auf dem AP Paketerfassung IO-Grafik-Analyse Fehlerbehebung Flexconnect Local Switching (oder Fabric/SDA) Konfiguration Fehlerbehebung: FlexConnect/Fabric **Referenzen**

Einleitung

Dieses Dokument beschreibt ein Konfigurationsbeispiel für Bi Directional Rate Limit (BDRL) für Catalyst Wireless Controller der Serie 9800

Voraussetzungen

Anforderungen

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

- Catalyst Wireless 9800-Konfigurationsmodell
- AAA mit Cisco Identity Service Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Wireless Controller 9800-CL (auf Version) 16.12.1s
- Identity Service Engine auf Version 2.2

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 kennen.

Hintergrundinformationen

QoS in der 9800 WLC-Plattform verwendet dieselben Konzepte und Komponenten wie die Catalyst 9000-Plattformen.

Dieser Abschnitt bietet einen globalen Überblick über die Funktionsweise dieser Komponenten und ihre Konfiguration zur Erzielung unterschiedlicher Ergebnisse.

Im Wesentlichen funktioniert die QoS-Rekursion wie folgt:

1. Class-Map: Identifiziert eine bestimmte Art von Datenverkehr. Klassenzuordnungen können die Application Visibility and Control (AVC)-Engine nutzen.

Außerdem kann der Benutzer benutzerdefinierte Klassenzuordnungen definieren, um Datenverkehr zu identifizieren, der mit einer Zugriffskontrollliste (ACL) oder einem Differentiated Services Code Point (DSCP) übereinstimmt.

2. Policy-Map: Dies sind Richtlinien, die für Class-Maps gelten. Diese Richtlinien können DSCP markieren, den Datenverkehr, der der Klassenzuordnung entspricht, verwerfen oder beschränken

4. Service-Policy: Policy-Maps können mit dem Service-Policy-Befehl auf das Richtlinienprofil einer SSID oder pro Client in einer bestimmten Richtung angewendet werden.

3. (Optional) Table-Map: Sie werden verwendet, um einen Markentyp in einen anderen umzuwandeln, z. B. CoS in DCSP.

Hinweis: Geben Sie in der Table-Map die zu ändernden Werte an (4 bis 32); in der Policy-Map wird die Technologie angegeben (COS zu DSCP).

class-map = MATCH

- · AVC (Application or Group)
- User defined
 - ACL
 - DSCP

policy-map = TAKE ACTION

- Mark DSCP
- Drop
- Police (rate-limit)

service-policy = WHERE and DIRECTION

- Client Ingress / Egress
- SSID Ingress / Egress

Hinweis: Falls zwei oder mehr Richtlinien pro Ziel anwendbar sind, wird die Richtlinienauflösung auf Basis dieser Prioritätsstufe ausgewählt:

ãf» AAA Override (höchste)
ãf» Native Profilerstellung (lokale Richtlinien)
ãf» Konfigurierte Richtlinie
ãf» Standardrichtlinie (niedrigste)

Weitere Einzelheiten finden Sie im offiziellen QoS-Konfigurationsleitfaden für 9800.

Weitere Informationen zur QoS-Theorie finden Sie im <u>QoS-Konfigurationsleitfaden für die Serie 9000.</u>

Beispiel: Gast- und Unternehmens-QoS-Richtlinien

In diesem Beispiel wird veranschaulicht, wie die erläuterten QoS-Komponenten in einem realen Szenario angewendet werden.

Ziel ist die Konfiguration einer QoS-Richtlinie für Gäste, die:

- Anmerkungen DSCP
- Drops Youtube- und Netflix-Video
- Übertragungsrate Begrenzt einen in einer ACL angegebenen Host auf 50 Kbit/s
- Rate Schränkt den gesamten anderen Datenverkehr auf 100 Kbit/s ein



POLICY MAP - Guest

Beispielsweise muss die QoS-Richtlinie pro SSID in beiden Richtungen auf den Eingang und den Ausgang des Richtlinienprofils angewendet werden, das mit dem Gast-WLAN verknüpft ist.

Konfigurieren

AAA-Server und Methodenliste

Schritt 1: Navigieren Sie zu **Configuration > Security > AAA > Authentication > Servers/Groups,** und wählen Sie +**Add.**

Geben Sie den AAA-Servernamen, die IP-Adresse und den Schlüssel ein, der mit dem gemeinsamen geheimen Schlüssel unter Administration > Network Resources > Network Devices on ISE (Verwaltung > Netzwerkressourcen > Netzwerkgeräte auf ISE) übereinstimmen muss.

Name*	ISE22
IPv4 / IPv6 Server Address*	172.16.13.6
PAC Key	
Key Type	0 •
Key*	
Confirm Key*	
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED

Schritt 2: Navigieren Sie zu **Configuration > Security > AAA > Authentication > AAA Method List,** und wählen Sie +**Add aus.** Wählen Sie die zugewiesenen Servergruppen aus den verfügbaren Servergruppen aus.

Method List Name*	ISE-Auth		
Type*	dot1x	Ŧ	
Group Type	group	Ŧ	
Fallback to local			
Available Server Groups	A	ssigned Server Group	ps
radius Idap tacacs+	* >	ISE22G	*
	÷		Ŧ

Schritt 3: Navigieren Sie zu **Konfiguration > Sicherheit > AAA > Autorisierung > AAA-Methodenliste,** und wählen Sie **Hinzufügen aus.** Wählen Sie als Typ die Standardmethode und "network" aus.

Quick Setup: AAA Authoriza	ation	
Method List Name*	default	
Type*	network	•
Group Type	group	•
Fallback to local		
Authenticated		
Available Server Groups		Assigned Serve
ldap tacacs+	>	radius

Dies ist erforderlich, damit der Controller die vom AAA-Server zurückgegebenen Autorisierungsattribute (z. B. hier die QoS-Richtlinie) anwenden kann. Andernfalls wird die vom RADIUS empfangene Richtlinie nicht angewendet.

WLAN-Richtlinie, Site-Tag und AP-Tag

Schritt 1: Navigieren Sie zu **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile,** und wählen Sie +**Add aus,** um ein neues WLAN zu erstellen. Konfigurieren Sie die SSID, den Profilnamen und die WLAN-ID, und legen Sie den Status auf "Aktiviert" fest.

Navigieren Sie anschließend zu **Security > Layer 2**, und konfigurieren Sie die Authentifizierungsparameter für Layer 2:

General	Security	Advanced			
Layer2	Layer3	AAA			
Layer 2 Securi MAC Filtering	ity Mode		WPA + WPA2	•	Fast Transition Over the DS
Protected Ma	anagement F	rame			Reassociation Timeout
PMF WPA Parame	aters		Disabled	•	
WPA Policy					
WPA2 Policy					
WPA2 Encrypt	tion		AES(CCMP128) CCMP256 GCMP128 GCMP256		
MPSK					
Auth Key Mgm	nt		802.1x PSK CCKM FT + 802.1x FT + PSK 802.1x-SHA256 PSK-SHA256		

Die SSID-Sicherheit muss nicht 802.1x als Voraussetzung für QoS sein. In diesem Konfigurationsbeispiel wird sie jedoch für die AAA-Überschreibung verwendet.

Schritt 2: Navigieren Sie zu **Security > AAA**, und wählen Sie den AAA-Server im Dropdown-Feld **Authentifizierungsliste**) aus.

General	General Security		nced	
Layer2	Layer3	AAA		
Authentication	List		ISE-Auth	•
Local EAP Aut	hentication			

Schritt 3: Wählen Sie **Richtlinienprofil** und anschließend +**Hinzufügen aus.** Konfigurieren Sie den Richtlinienprofilnamen.

Legen Sie den Status auf "Aktiviert" fest. Aktivieren Sie außerdem die Funktionen für zentrales Switching, Authentifizierung, DHCP und Zuordnung:

General	Access Policies	QOS and AVC	Mobility	Advanced	
	A Configuring	in enabled state will resul	t in loss of conn	ectivity for clients associated with t	nis profile.
Name*		QoS-PP		WLAN Switching Policy	
Descriptio	n	QoS-PP		Central Switching	ENABLED
Status		ENABLED		Central Authentication	ENABLED
Passive C	lient	DISABLED		Central DHCP	ENABLED
Encrypted	Traffic Analytics	DISABLED		Central Association	ENABLED
CTS Polic	су			Flex NAT/PAT	DISABLED
Inline Tag	ging				
SGACL En	forcement				
Default SG	ат	2-65519]		

Schritt 4: Navigieren Sie zu **Access Policies (Zugriffsrichtlinien**), und konfigurieren Sie das VLAN, dem der Wireless-Client zugewiesen ist, wenn der Client eine Verbindung mit der SSID herstellt:

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Prof	filing			
Local Subsc	riber Policy Name	Search or S	elect 🔻	
WLAN Loca	al Profiling			
Global State Classification	of Device	Disabled (i)		
HTTP TLV C	aching			
DHCP TLV C	Caching			
VLAN				
VLAN/VLAN	Group	VLAN2613	•	
Multicast VL	AN	Enter Multic	cast VLAN	

Schritt 5: Wählen Sie **Policy Tag (Richtlinientag)** und anschließend +**Hinzufügen aus.** Konfigurieren Sie den Namen des Policy Tags.

Wählen Sie unter **WLAN-Policy Maps (WLAN-Richtlinienzuordnungen)** unter +**Hinzufügen** aus den Dropdown-Menüs **WLAN Profile** und **Policy Profile (WLAN-Profil** und **Richtlinienprofil**) aus, und aktivieren Sie die Option Check for the map to be configured (Nach zu konfigurierender Zuordnung suchen).

Name*	QoS-PT		
Description	QoS-PT		
V WLAN-POLIC	Y Maps: 0		
WLAN Profile		 Policy Profile 	×
4 4 0 ⊨ ⊨	10 🔻 items per page		No items to display
Map WLAN and Pol	icy		
WLAN Profile*	QoSWLAN	Policy Profile*	QoS-PP v

Schritt 6: Wählen Sie **Site-Tag aus**, und wählen Sie +**Hinzufügen aus**. Aktivieren Sie das Kontrollkästchen **Enable Local Site** (Lokalen Standort aktivieren), damit die Access Points im lokalen Modus ausgeführt werden (oder lassen Sie es für FlexConnect deaktiviert):

Name*	QoS-ST
Description	Enter Description
AP Join Profile	default-ap-profile
Control Plane Name	•
Enable Local Site	2

Schritt 7. Wählen Sie die **Tag-APs aus**, wählen Sie die APs aus, und fügen Sie das Policy-, Site- und RF-Tag hinzu:

Tags		
Policy	QoS-PT	•
Site	QoS-ST	•
RF	default-rf-tag	•

Changing AP Tag(s) will cause associated AP(s) to reconnect

QoS

Schritt 1: Navigieren Sie zu **Configuration > Services > QoS,** und wählen Sie +**Add**, um eine QoS-Richtlinie zu erstellen.

Benennen Sie es (in diesem Beispiel: BWLimitAAAClients).

QoS												
Auto QOS		DISABLE	D									
Policy Name*	E	WLimitAA	AClients									
Description												
Match ~ Type	Match Value	< Mark Type	×	Mark Value	 Police Value (kbps) 	×	Drop	~	AVC/User Defined	~	Actions	~
Add Class-M	H C	IO ▼ ite	ms per p	oage						No ite	ms to displa	зу
Add Class-M	laps N	IO V ite	ms per p	⇒age ▼	Police(kbp	5)		8	8 - 1000000	No ite	ms to displ	ау
Add Class-M Class Default Mark Drag and Drop, do selected Profiles	laps N uble click o	10 v ite × Del one	ete	oage ▼ on to add/rel	Police(kbp: move Profiles from	s)	0	٤ ۲ Se	8 - 1000000 earch	No ite	ms to displa	ay
Add Class-M + Add Class-M Class Default Mark Drag and Drop, do selected Profiles Available (2)	laps N uble click o	IO V ite	ete	oage ▼ on to add/rea	Police(kbp: move Profiles from Selected	s) 1 (O)	C	E X Se	8 - 1000000 earch	No ite	ms to displa	зу

Schritt 2: Fügen Sie eine Klassenkarte, um Youtube und Netflix fallen. Klicken Sie auf Add Class-Maps (Klassenzuordnung hinzufügen). Wählen Sie AVC, eine beliebige Aktion löschen und beide Protokolle aus.

Match ~ Matc Type Value	h ~ Mark ~ e Type	Mark Value	Police Value (kbps)	~	Drop	×	AVC/User Defined	~
⊲ ⊲ 0 ⊳ ⊳	10 🔻 items per p	page						No ite
AVC/User Defined	AVC	•						
Match	• Any O All							
Drop	\checkmark							
Match Type	protocol	•						
	Available Protocol(s)		Selected Protocol(s))				
	netbios-ssn netblt netflow	> <	youtube netflix					
							්ට Can	cel

Drücken Sie Speich.

Schritt 3: Fügen Sie eine Klassenzuordnung mit den Hinweisen zu DSCP 46 bis 34 hinzu.

Klicken Sie auf Klassenzuordnungen hinzufügen.

- Übereinstimmung mit beliebigen, benutzerdefinierten
 Übereinstimmung mit Typ DSCP
 Übereinstimmender Wert 46

- Typ **DSCP** markieren
- Markenwert **34**

•

Match v Match Type Value	h ~ Mark ~ e Type	Mark v Value	Police Value ~ (kbps)	Drop 🗸	AVC/User ~ Defined
protocol youtu	ube,netflix None		8	Enabled	AVC
	10 🔻 items per pag	je			1 -
AVC/User Defined	User Defined	,			
Match	• Any O All				
Match Type	DSCP	,			
Match Value*	46				
Mark Type	DSCP	,	Mark Value	34	4
Drop					
Police(kbps)	8 - 10000000				
					Cancel

Drücken Sie Speich.

Schritt 4: Um eine Klassenzuordnung zu definieren, die den Datenverkehr zu einem bestimmten Host regelt, erstellen Sie eine entsprechende ACL.

Klicken Sie auf Klassenzuordnungen hinzufügen,

Wählen Sie Benutzerdefiniert, **Beliebige** zuordnen, Zuordnungsart **ACL**, wählen Sie Ihren ACL-Namen (hier **specifichostACL**), markieren Sie Typ **keine** und wählen Sie **den** Grenzwert für **die** Rate aus.

Klicken Sie auf Speichern.

	Match ~ Type	Match ~ Value	Mark v Type	Mark v Value	Police Value (kbps)	\sim	Drop 🗸	AVC/User Defined	×,
	protocol	youtube,netflix	None		8		Enabled	AVC	
	DSCP	46	DSCP	34			Disabled	User Defined	
-	⊲ 1 ⊳	▶ 10 •) items per pag	ge					1 -
AVC	/User Defined	User De	fined	•					
Mato	ch	 Any 							
Mato	ch Type	ACL	,	•					
Mato	ch Value*	specific	nostACL	•					
Mark	к Туре	None		•					
Drop)								
Polic	ce(kbps)	50							
								Cancel	

Nachfolgend finden Sie ein Beispiel für eine ACL, die zum Identifizieren eines bestimmten Host-Datenverkehrs verwendet wird:

	Sequence ~	Action ~	Source IP 🗸	Source v Wildcard	Destination ~ IP	Destination ~ Wildcard	Protocol ~	Source Port
	1	permit	any		192.168.1.59		ip	
	2	permit	192.168.1.59		any		ip	
14	≪ 1 ⊨ .	▶ 10	▼ items per pag	je				

Schritt 5: Verwenden Sie im Rahmen für die Klassenzuordnungen die Standardklasse, um die Durchsatzgrenze für den gesamten anderen Datenverkehr festzulegen.

Dadurch wird eine Durchsatzratenbegrenzung für den gesamten Client-Datenverkehr festgelegt, für den keine der oben genannten Regeln gilt.

Match	1	Marl	ĸ		N	one		•]		Police(kbps)		10	00	
Match ~ Match ~ Mark ~ Police Value ~ Drop AVC/User protocol youtube,netflix None 8 Enabled AVC DSCP 46 DSCP 34 Disabled User Defined ACL specifichostACL None 50 Disabled User Defined 1 1 10 items per page		CI	ass Defau	lt											
Match TypeMatch ValueMark TypeMark ValuePolice Value (kbps)DropAVC/User Definedprotocolyoutube,netflixNone8EnabledAVCDSCP46DSCP34DisabledUser DefinedACLspecifichostACLNone50DisabledUser DefinedIIIIIIII		+	Add Class	s-Ma	ips										
Match TypeMatch ValueMark TypeMark ValuePolice Value (kbps)DropAVC/User Definedprotocolyoutube,netflixNone8EnabledAVCDSCP46DSCP34DisabledUser DefinedACLspecifichostACLNone50DisabledUser Defined		[≪	∢ 1	Þ) 	10 🔻 i	items per	page	9						1
Match TypeMatch ValueMark TypeMark 			ACL		specifiche	ostACL	None				50		Disabled	User Defined	
Match Type Match Value Mark Type Mark Value Mark Value Police Value (kbps) Drop Value AVC/User Defined protocol youtube,netflix None 8 Enabled AVC			DSCP		46		DSCP		34				Disabled	User Defined	
Match v Match v Mark v Mark v Police Value v AVC/User Type Value Value v Drop v Defined			protocol		youtube,r	netflix	None				8		Enabled	AVC	
			Match Type	\sim	Match Value	~	Mark Type	\sim	Mark Value	×	Police Value (kbps)	\sim	Drop 🗸	AVC/User Defined	

Schritt 6: Klicken Sie unten auf Apply to Device (Auf Gerät anwenden).

Entsprechende CLI-Konfiguration:

```
policy-map BWLimitAAAclients
class BWLimitAAAclients1_AVC_UI_CLASS
 police cir 8000
  conform-action drop
  exceed-action drop
 class BWLimitAAAclients1_ADV_UI_CLASS
  set dscp af41
 class BWLimitAAAclients2_ADV_UI_CLASS
 police cir 50000
  conform-action transmit
   exceed-action drop
 class class-default
 police cir 100000
   conform-action transmit
   exceed-action drop
class-map match-all BWLimitAAAclients1_AVC_UI_CLASS
 description BWLimitAAAclients1_AVC_UI_CLASS UI_policy_D0_NOT_CHANGE
match protocol youtube
match protocol netflix
class-map match-any BWLimitAAAclients1_ADV_UI_CLASS
 description BWLimitAAAclients1_ADV_UI_CLASS UI_policy_D0_NOT_CHANGE
match dscp ef
class-map match-all BWLimitAAAclients2_ADV_UI_CLASS
 description BWLimitAAAclients2_ADV_UI_CLASS UI_policy_D0_NOT_CHANGE
match access-group name specifichostACL
```

Hinweis: In diesem Beispiel wurden unter der QoS-Richtlinie keine **Profile** ausgewählt, da sie durch AAA-Überschreibung angewendet werden. Um die QoS-Richtlinie jedoch manuell auf ein Richtlinienprofil anzuwenden, wählen Sie die gewünschten Profile aus.

Schritt 2: Navigieren Sie auf der ISE zu **Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierungsprofile,** und wählen Sie auf +**Hinzufügen aus**, um ein Autorisierungsprofil zu erstellen.

Um die QoS-Richtlinie anzuwenden, fügen Sie sie über Cisco AV-Paare als **erweiterte** Attributeinstellungen hinzu.

Es wird davon ausgegangen, dass die ISE-Authentifizierungs- und Autorisierungsrichtlinien so konfiguriert sind, dass sie mit den richtigen Regeln übereinstimmen und dieses Autorisierungsergebnis erhalten.

Die Attribute sind ip:sub-qos-policy-in=<Policy-Name> und ip:sub-qos-policy-out=<Policy-Name>

 Advanced Attributes Setti 	ngs
Cisco:cisco-av-pair	📀 = ip:sub-qos-policy-in=BWLimitA 📀 —
Cisco:cisco-av-pair	📀 = ip:sub-qos-policy-out=BWLimit 📀 — 🕂
 Attributes Details 	
Access Type = ACCESS_ACCEPT cisco-av-pair = ip:sub-qos-policy-i cisco-av-pair = ip:sub-qos-policy-	in=BWLimitAAAClients out=BWLimitAAAClients

Hinweis: Bei Richtliniennamen wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass das Gehäuse korrekt ist!

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

Auf dem WLC

show run wlan
show run aaa
show aaa servers
show aaa servers
show ap tag summary
show ap name <AP-name> tag detail
show wireless tag policy summary
show wireless tag policy detailed <policy-tag-name>
show wireless profile policy detailed <policy-profile-name>
show policy-map <policy-map name>
show policy-map interface wireless ssid/client profile-name <WLAN> radio type <2.4/5GHz> ap name <name>i
show interface wireless is the state of the s

```
# show wireless client mac
```

```
detail
# show wireless client
      service-policy input
# show wireless client
       service-policy output
To verify EDCS parameters :
sh controllers dot11Radio 1 | begin EDCA
<#root>
9800#show wireless client mac e836.171f.a162 det
Client MAC Address : e836.171f.a162
Client IPv4 Address : 192.168.1.11
Client IPv6 Addresses : fe80::c6e:2ca4:56ea:ffbf
                        2a02:a03f:42c2:8400:187c:4faf:c9f8:ac3c
                        2a02:a03f:42c2:8400:824:e15:6924:ed18
                        fd54:9008:227c:0:1853:9a4:77a2:32ae
                        fd54:9008:227c:0:1507:c911:50cd:2062
Client Username : Nico
AP MAC Address : 502f.a836.a3e0
AP Name: AP780C-F085-49E6
AP slot : 1
Client State : Associated
(...)
 Local Policies:
      Service Template : wlan_svc_QoS-PP (priority 254)
         VLAN
                          : 1
          Absolute-Timer : 1800
 Server Policies:
          Input QOS
                          : BWLimitAAAClients
          Output QOS
                          : BWLimitAAAClients
 Resultant Policies:
         VLAN Name
                          : default
          Input QOS
                          : BWLimitAAAClients
                          : BWLimitAAAClients
          Output QOS
          VLAN
                           : 1
          Absolute-Timer : 1800
```

Auf dem AP

Wenn sich der Access Point im lokalen Modus befindet oder sich der SSID im FlexConnect Central Switching-Modus befindet, ist keine Fehlerbehebung am Access Point erforderlich, da die QoS und die Servicerichtlinien vom WLC übernommen werden.

Paketerfassung IO-Grafik-Analyse



Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Ihrer Konfiguration.

Schritt 1: Löschen Sie alle bereits vorhandenen Debugbedingungen.

clear platform condition all

Schritt 2: Aktivieren Sie das Debugging für den betreffenden Wireless-Client.

debug wireless mac <client-MAC-address> {monitor-time <seconds>}

Schritt 3: Verbinden Sie den Wireless-Client mit der SSID, um das Problem zu reproduzieren. Schritt 4: Beenden Sie die Fehlersuche, sobald das Problem reproduziert wurde.

no debug wireless mac <client-MAC-address>

Die während des Tests erfassten Protokolle werden auf dem WLC in einer lokalen Datei mit dem Namen: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log Wenn diese Ablaufverfolgung über den GUI-Workflow generiert wird, lautet der gespeicherte Dateiname debugTrace_aaaa.bbb.cccc.txt.

Schritt 5: Um die zuvor generierte Datei zu sammeln, kopieren Sie entweder die Datei ra trace .log auf einen externen Server oder zeigen die Ausgabe direkt auf dem Bildschirm an.

Überprüfen Sie den Namen der RA Traces-Datei mit dem folgenden Befehl:

```
# dir bootflash: | inc ra_trace
```

Datei auf externen Server kopieren:

copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.d

Oder zeigen Sie den Inhalt an:

```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

Schritt 6: Entfernen Sie die Debug-Bedingungen.

```
# clear platform condition all
```

Flexconnect Local Switching (oder Fabric/SDA)

Im Fall von Flexconnect Local Switching (oder Fabric/SDA) wendet der Access Point alle QoS-Richtlinien an, die Sie auf dem WLC definiert haben.

Bei Wave2- und 11ax-Access Points erfolgt die Ratenbegrenzung auf Flow-Ebene (5 Tupel) und nicht pro Client oder SSID vor dem 17.6.

Dies gilt für APs in FlexConnect/Fabric-Bereitstellungen sowie in Embedded Wireless Controller on Access Point (EWc-AP)-Bereitstellungen.

Ab dem 17.5. kann AAA-Überschreibung verwendet werden, um die Attribute weiterzugeben und eine Durchsatzratenbeschränkung pro Client zu erreichen.

Ab Version 17.6 wird die bidirektionale Ratenbeschränkung pro Client auf 802.11ac Wave 2- und 11ax-APs in der Flex Local Switching-Konfiguration unterstützt.

Hinweis: Flex APs unterstützen nicht das Vorhandensein von ACLs in QoS-Richtlinien. Sie unterstützen auch kein BRR (Bandbreite bleibt erhalten) und keine Richtlinienpriorität, die über die

CLI konfigurierbar sind, aber in der Webbenutzeroberfläche des 9800 nicht verfügbar sind und von 9800 nicht unterstützt werden. Die Cisco Bug-ID <u>CSCvx81067</u> verfolgt die Unterstützung von ACLs in QoS-Richtlinien für flexible APs.

Konfiguration

Die Konfiguration entspricht exakt dem ersten Teil dieses Artikels, mit zwei Ausnahmen:

1. Das Richtlinienprofil ist auf "Lokales Switching" festgelegt. Für die Flex-Bereitstellung muss die Central Association bis zur Version Bengaluru 17.4 deaktiviert sein.

Ab 17.5 ist dieses Feld nicht mehr für die Benutzerkonfiguration verfügbar, da es fest codiert ist.



2. Die Sitebezeichnung ist so festgelegt, dass sie keine lokale Site ist.



Fehlerbehebung: FlexConnect/Fabric

Da der Access Point das Gerät ist, das die QoS-Richtlinien anwendet, können diese Befehle dazu beitragen, die angewendeten Aktionen einzugrenzen.

dot11 qos anzeigen Richtlinienplan anzeigen show rate-limit client show rate limit bssid Show Rate-Limit-WLAN Flexconnect-Client anzeigen <#root> AP780C-F085-49E6# show dot11 gos Qos Policy Maps (UPSTREAM) ratelimit targets: Client: A8:DB:03:6F:7A:46 platinum-up targets: VAP: 0 SSID:LAB-DNAS VAP: 1 SSID:VlanAssign VAP: 2 SSID:LAB-Qos Qos Stats (UPSTREAM) total packets: 29279 dropped packets: 0 marked packets: 0 shaped packets: 0 policed packets: 182 copied packets: 0 DSCP TO DOT1P (UPSTREAM) Default dscp2dot1p Table Value: [0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48 Active dscp2dot1p Table Value: [0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48 Trust DSCP Upstream : Disabled Qos Policy Maps (DOWNSTREAM) ratelimit targets: Client: A8:DB:03:6F:7A:46 Qos Stats (DOWNSTREAM) 25673 total packets: dropped packets: 0 marked packets: 0 shaped packets: 0 policed packets: 150 copied packets: 0 DSCP TO DOT1P (DOWNSTREAM) Default dscp2dot1p Table Value: [0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1 [8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1 [16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1 [24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1 [32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1 [40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1 [48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1 [56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1 Active dscp2dot1p Table Value: [0]->0 [1]->0 [2]->1 [3]->0 [4]->1 [5]->0 [6]->1 [7]->0

```
[8]->1 [9]->1 [10]->2 [11]->1 [12]->2 [13]->1 [14]->2 [15]->1
[16]->2 [17]->2 [18]->3 [19]->2 [20]->3 [21]->2 [22]->3 [23]->2
[24]->3 [25]->3 [26]->4 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3
[32]->4 [33]->4 [34]->5 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4
[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->6 [47]->5
[48]->7 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6
[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7
Profinet packet recieved from
wired port:
0
wireless port:
AP780C-F085-49E6#
show policy-map
2 policymaps
Policy Map BWLimitAAAClients
                                        type:qos client:default
    Class BWLimitAAAClients_AVC_UI_CLASS
      drop
    Class BWLimitAAAClients_ADV_UI_CLASS
      set dscp af41 (34)
    Class class-default
      police rate 5000000 bps (625000Bytes/s)
        conform-action
        exceed-action
Policy Map platinum-up
                                type:qos client:default
    Class cm-dscp-set1-for-up-4
      set dscp af41 (34)
    Class cm-dscp-set2-for-up-4
      set dscp af41 (34)
   Class cm-dscp-for-up-5
      set dscp af41 (34)
   Class cm-dscp-for-up-6
      set dscp ef (46)
   Class cm-dscp-for-up-7
      set dscp ef (46)
   Class class-default
      no actions
AP780C-F085-49E6#
```

```
show rate-limit client
```

Config: mac vap rt_rate_out rt_rate_in rt_burst_out rt_burst_in nrt_rate_out nrt_rate_in nrt_burst A8:DB:03:6F:7A:46 2 0 0 0 0 0 0 Statistics: name up down Unshaped 0 0 Client RT pass 0 0 Client NRT pass 0 0 Client RT drops 0 0 Client NRT drops 0 38621 9 54922 0 AP780C-F085-49E6# AP780C-F085-49E6# show flexconnect client Flexconnect Clients: mac radio vap aid state encr aaa-vlan aaa-acl aaa-ipv6-acl assoc auth switching | A8:DB:03:6F:7A:46 1 2 1 FWD AES_CCM128 none none none Local Central Local AP780C-F085-49E6#

Referenzen

Catalyst 9000 16.12 QoS-Leitfaden 9800 QoS-Konfigurationsleitfaden Catalyst 9800-Konfigurationsmodell Cisco IOS® XE 17.6 - Versionshinweise

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.