Configurar o limite de taxa de QoS (BDRL) nos controladores sem fio Catalyst 9800 com substituição de AAA

Contents

Introduction Prerequisites **Requirements** Componentes Utilizados Informações de Apoio Exemplo: políticas de QoS de convidado e corporativo Configurar Servidor AAA e lista de métodos Política de WLAN, Tag de Site e Tag de AP qos Verificar Na WLC No AP O pacote captura a análise do gráfico de E/S Troubleshoot Cenário de switching local Flexconnect (ou malha/SDA) Configuração Solução de problemas do Flexconnect/Fabric **Referências**

Introduction

Este documento descreve um exemplo de configuração para BDRL (Bi Directional Rate Limit, Limite de taxa bidirecional) nos controladores sem fio Catalyst 9800 Series.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Modelo de configuração Catalyst Wireless 9800
- AAA com Cisco Identity Service Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador sem fio Cisco Catalyst 9800-CL na versão 16.12.1s
- Identity Service Engine na versão 2.2

The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A QoS na plataforma 9800 WLC usa os mesmos conceitos e componentes que as plataformas Catalyst 9000.

Esta seção fornece uma visão geral global de como esses componentes funcionam e como podem ser configurados para alcançar resultados diferentes.

Em essência, a recursão de QoS funciona assim:

1. Mapa de Classes: Identifica um determinado tipo de tráfego. Os mapas de classe podem aproveitar o mecanismo Application Visibility and Control (AVC).

Além disso, o usuário pode definir mapas de classe personalizados para identificar o tráfego que corresponde a uma ACL (Access Control Lists, lista de controle de acesso) ou DSCP (Differentiated Services Code Point, ponto de código de serviços diferenciados)

2. Mapa de Políticas: São políticas que se aplicam a mapas de classes. Essas políticas podem marcar DSCP, descartar ou limitar a taxa do tráfego que corresponde ao mapa de classes

4. Política de Serviço: Os mapas de política podem ser aplicados no Perfil de Política de um SSID ou Por Cliente em uma determinada direção com o comando service-policy.

3. (Opcional) Mapa de Tabela: Eles são usados para converter um tipo de marca em outro, por exemplo, CoS para DCSP.

Nota: No mapa de tabela, especifique os valores a serem alterados (4 a 32); no mapa de política, a tecnologia é especificada (COS a 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

Observação: caso duas ou mais políticas sejam aplicáveis por destino, a resolução da política é escolhida com base nesta classificação de prioridade:

- · AAA Override (maior)
- · Criação nativa de perfis (políticas locais)
- · Política configurada
- · Política padrão (mais baixa)

Mais detalhes podem ser encontrados no guia oficial de configuração de QoS para o 9800

Informações adicionais sobre a teoria de QoS podem ser encontradas no <u>guia de configuração de QoS da</u> <u>série 9000</u>

Exemplo: políticas de QoS de convidado e corporativo

Este exemplo demonstra como os componentes de QoS explicados se aplicam em um cenário real.

A intenção é configurar uma Política de QoS para convidado que:

- Comentários DSCP
- Deixa cair o vídeo do Youtube e Netflix
- A taxa limita um host especificado em uma ACL a 50 Kbps
- A taxa limita todo o tráfego restante a 100 Kbps



Por exemplo, a Política de QoS deve ser aplicada por SSID em ambas as direções Ingress e Egress para o Perfil de Política que se vincula à WLAN Convidada.

Configurar

Servidor AAA e lista de métodos

Etapa 1. Navegue para Configuration > Security > AAA > Authentication > Servers/Groups e selecione

+Add.

Insira o nome do servidor AAA, o endereço IP e a chave, que devem corresponder ao segredo compartilhado em **Administration > Network Resources > Network Devices** no ISE.

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

Etapa 2. Navegue para **Configuration > Security > AAA > Authentication > AAA Method List** e selecione +**Add.** Selecione os Grupos de servidores atribuídos nos Grupos de servidores disponíveis.

Method List Name*	ISE-Auth	
Type*	dot1x 🔻	
Group Type	group v	
Fallback to local		
Available Server Groups	Assigned Sen	ver Groups
radius Idap tacacs+	> SE22G	*

Etapa 3. Navegue para **Configuration > Security > AAA > Authorization > AAA method List** e selecione **Add.** Escolha o método padrão e "rede" como o tipo.

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

Isso é necessário para que o controlador aplique os atributos de autorização (por exemplo, a política de QoS aqui) retornados pelo servidor AAA. Caso contrário, a política recebida do RADIUS não será aplicada.

Política de WLAN, Tag de Site e Tag de AP

Etapa 1. Navegue para **Configuration > Wireless Setup > Advanced > Start Now > WLAN Profile** e selecione +**Add** para criar uma nova WLAN. Configure o SSID, o nome do perfil, a ID da WLAN e defina o status como habilitado.

Em seguida, navegue até **Security > Layer 2** e configure os parâmetros de autenticação da Camada 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		

A segurança SSID não precisa ser 802.1x como um requisito para QoS, mas é usada neste exemplo de configuração para substituição de AAA.

Etapa 2. Navegue para **Security > AAA** e selecione o servidor AAA na caixa suspensa **Authentication List**.

General	Security	Adva	nced	
Layer2	Layer3	AAA		
Authenticatio	on List		ISE-Auth	•
Local EAP Au	uthentication			

Etapa 3. Selecione **Policy Profile** e selecione +**Add.** Configure o nome do Perfil de Diretiva.

Defina o Status como Enabled (Habilitado); habilite também Central Switching (Comutação central), Authentication (Autenticação), DHCP e association (Associação):

General	Access Policies	QOS and AVC	Mobility	Advanced	
	Configuring	in enabled state will resu	It in loss of conr	nectivity for clients associated with t	his 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 Er	nforcement				
Default SC	ат	2-65519			

Etapa 4. Navegue até **Access Policies** e configure a VLAN à qual o cliente sem fio está atribuído quando o cliente se conecta ao SSID:

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Pro	filing			
Local Subsc	riber Policy Name	Search or S	elect 🔻	
WLAN Loca	al Profiling			
Global State Classificatio	of Device n	Disabled (1)		
HTTP TLV C	aching			
DHCP TLV C	Caching			
VLAN				
VLAN/VLAN	Group	VLAN2613	•	
Multicast VL	AN	Enter Multic	cast VLAN	

Etapa 5. Selecione **Policy Tag** e +**Add.** Configure o nome da tag de política.

Em WLAN-Policy Maps, em +Add, selecione o Perfil da WLAN e o Perfil da política nos menus suspensos, selecione a verificação para o mapa a ser configurado.

Name*	QoS-PT			
Description	QoS-PT			
VIAN-POLICY	' Maps: 0			
+ Add × Delete				
WLAN Profile		 Policy Profile 		~
	10 🔻 items per page		No ite	ms to display
Map WLAN and Pol	icy			
WLAN Profile*	QoSWLAN V	Policy Profile*	QoS-PP	•

Etapa 6. Selecione **Marca do site** e +**Adicionar.** Marque a caixa **Enable Local** Site para que os APs operem no Modo Local (ou deixe-a desmarcada para FlexConnect):

Name*	QoS-ST	
Description	Enter Description	
AP Join Profile	default-ap-profile	٠
Control Plane Name		•
Enable Local Site		

Passo 7. Selecione Tag APs, escolha os APs e adicione a tag Policy, Site e RF:

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

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

qos

Etapa 1. Navegue até **Configuration > Services > QoS** e selecione +**Add** para criar uma política de QoS.

Nomeie-o (neste exemplo: BWLimitAAClients).

QoS															
Auto QOS		Di:	SABLED												
Policy Name*	[BWLi	mitAAAClie	ents											
Description															
Match ~ Type	Match Value	~	Mark Type	~	Mark Value	~	Police Value (kbps)	~	Drop	~	AVC/Us Defined	er	~	Actions	,
Add Class-N	►I laps	10	▼ items < Delete	per pa	ige							N	No iten	ns to displ	зy
Add Class-N Class Default Mark	Maps	10 None	items	per pa	▲		Police(kbps)			8	3 - 10000	0000	No iten	ns to displa	ау
Add Class-M Class Default Mark	Naps	10 None	items tems Celete	per pa		ramou	Police(kbps)			8	3 - 10000	0000	No iten	ns to displa	ay
Add Class-N Class Default Mark Trag and Drop, do elected Profiles	► Itaps	None	items Celete ck on the l	per pa	rge ▼ n to add/r	remov	Police(kbps) ve Profiles from		0	E Se	3 - 10000 earch	0000	Vo iten	ns to displa	ay
Add Class-N Class Default Class Default Mark Trag and Drop, do elected Profiles Available (2)	Naps	None	items A Delete ck on the I	per pa	rge ▼	remov	Police(kbps) ve Profiles from Selected (0)	0	E X Se	3 - 10000 earch	000	No iten	ns to displa	ay

Etapa 2. Adicione um mapa de aula para soltar Youtube e Netflix. Clique em Add Class-Maps. Selecione a ação AVC, match any, drop e escolha os dois protocolos.

Match v Match Type Value	✓ Mark ✓ Type	Mark Value	 Police Value (kbps) 	\sim	Drop	~	AVC/User Defined	~
	10 🔻 items per p	oage						No ite
AVC/User Defined	AVC	•						
Match	⊙ Any ◯ All							
Drop								
Match Type	protocol	•						
	Available Protocol(s)		Selected Protocol(s)				
	netbios-ssn netblt netflow	>	youtube netflix					
							່ວ Can	cel

Pressione Salvar.

Etapa 3. Adicione um mapa de classe que comente DSCP 46 a 34.

Clique em Add Class-Maps.

- Corresponder a qualquer, Definido pelo usuário
 Corresponder tipo DSCP
- Corresponder valor 46
- Marcar tipo **DSCP**
- Valor da marca 34

•

Match v M Type V	latch v alue	Mark ~ Type	Mark v Value	Police Value ~ (kbps)	Drop 🗸	AVC/User Defined	~
protocol y	outube,netflix	None		8	Enabled	AVC	
	10 🔻) items per pag	ge				1 - 1
AVC/User Defined	User Def	fined	•				
Match	 Any 						
Match Type	DSCP		•				
Match Value*	46						
Mark Type	DSCP		•	Mark Value	3	4	•
Drop							
Police(kbps)	8 - 100	00000					
						Cancel	

Pressione Salvar.

Etapa 4. Para definir um mapa de classe que reguie o tráfego para um host específico, crie uma ACL para ele.

Clique em Add Class-Maps,

Escolha Definido pelo usuário, corresponder a **qualquer**, corresponder ao tipo ACL, escolha o nome da ACL (aqui specifichostACL), marque o tipo nenhum e escolha o valor de limite de taxa.

Click Save.

Match ✓ Match ✓ Mark ✓ Police Value ✓ Drop ✓ AVC/User ✓ □ protocol youtube,netflix None 8 Enabled AVC □ DSCP 46 DSCP 34 Disabled User Defined ■ 1 ■ 10 • items per page 1 ▲ 1 ■ ■ 10 • items per page 1 ▲ ACL ● ACL ● ACL ● Match Value* specifichostACL ● ● ● ● Police(kbps) 50 50 50 ●								
protocol youtube,netflix None 8 Enabled AVC DSCP 46 DSCP 34 Disabled User Defined I I I I I I I + Add Class-Maps × Delete AVC/User Defined User Defined User Defined - Match Image: Anny Image: All image:	Match ~ Type	Match ~ Value	Mark v Type	Mark v Value	Police Value v (kbps)	Drop 🗸	AVC/User Defined	\sim
DSCP 46 DSCP 34 Disabled User Defined I I I I I I I + Add Class-Maps × Delete AVC/User Defined User Defined • Match Image: Any Image: All Match Type ACL Match Value* specifichostACL Mark Type None Police(kbps) 50	protocol	youtube,netflix	None		8	Enabled	AVC	
Image: Second system Image:	DSCP	46	DSCP	34		Disabled	User Defined	
+ Add Class-Maps × Delete AVC/User Defined User Defined Match • Any Match Type ACL Match Value* specifichostACL Mark Type None Drop □ Police(kbps) 50		⊨ 10 ▼) items per pag	ge				1 -
AVC/User Defined Match Match Type ACL Match Value* specifichostACL Mark Type None Drop Police(kbps) 50								
Match ● Any All Match Type ACL ▼ Match Value* specifichostACL ▼ Mark Type None ▼ Drop □ Police(kbps) 50	AVC/User Defined	User De	fined	•				
Match Type ACL Match Value* specifichostACL Mark Type None Drop	Match	 Any 						
Match Value* specifichostACL Mark Type None Drop	Match Type	ACL	,	•				
Mark Type None Drop	Match Value*	specific	nostACL	•				
Drop Drop 50 Sol	Mark Type	None	,	•				
Police(kbps) 50	Drop							
D Cancel	Police(kbps)	50						
							່ ວ Cancel	

Aqui está um exemplo de ACL que usamos para identificar um tráfego de host específico :

	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 	ge				

Etapa 5. No quadro mapas de classe, use a classe padrão para definir o limite de taxa para todo o tráfego restante.

Isso define um limite de taxa em todo o tráfego de cliente que não é alvo de uma das regras acima.

Marl	k		ſ	None		•]		Police(kbps)		[10	0	
CI	ass Default	:												
+	Add Class-	-Map	ps	×	Delete									
4	∢ 1	Þ	▶ (10 🗸	items pe	er page	9							1
	ACL		specific	hostAC	L None				50		Disable	ed	User Defined	i
	DSCP		46		DSCP		34				Disable	ed	User Defined	1
	protocol		youtube	e,netflix	None				8		Enable	d	AVC	
	Match Type	\sim	Match Value	`	Mark Type	×.	Mark Value	~	Police Value (kbps)	¥,	Drop	~	AVC/User Defined	,

Etapa 6. Clique em Apply to Device na parte inferior.

Configuração equivalente de CLI:

```
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
```

Observação: neste exemplo, nenhum **perfil** foi selecionado na política de QoS, pois é aplicado pela substituição de AAA. No entanto, para aplicar a política de QoS a um perfil de política manualmente, selecione os perfis desejados.

Etapa 2. No ISE, navegue para **Política > Elementos de política > Resultados > Perfis de autorização** e selecione +**Adicionar** para criar um perfil de autorização.

Para aplicar a política de QoS, adicione-as como Advanced Attributes Settings através de Cisco AV Pairs.

Supõe-se que as políticas de Autenticação e Autorização do ISE estejam configuradas para corresponder à regra correta e obter esse resultado de autorização.

Os atributos são ip:sub-qos-policy-in=<policy name> e ip:sub-qos-policy-out=<policyname>

Cisco:cisco-av-pair	ip:sub-qos-policy-in=BWLimitA 📀 —
Cisco:cisco-av-pair	📀 = ip:sub-qos-policy-out=BWLimit 📀 — 🕂
 Attributes Details 	

Observação: os nomes de política diferenciam maiúsculas de minúsculas. Verifique se o gabinete está correto!

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente:

Na WLC

```
# show run wlan
# show run aaa
# 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>:
```

```
# show wireless client mac
```

```
# 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:
```

detail

Input QOS : BWLimitAAAClients Output QOS : BWLimitAAAClients Resultant Policies: VLAN Name : default Input QOS : BWLimitAAAClients Output QOS : BWLimitAAAClients

```
VLAN : 1
Absolute-Timer : 1800
```

No AP

Nenhuma solução de problemas é necessária no AP quando o AP está no modo local ou o SSID no modo de switching central do Flexconnect, pois as políticas de QoS e de serviço são feitas pela WLC.

O pacote captura a análise do gráfico de E/S



Troubleshoot

Esta seção fornece informações para solucionar problemas da sua configuração.

Etapa 1. Limpe todas as condições de depuração preexistentes.

clear platform condition all

Etapa 2. Ative a depuração para o cliente sem fio em questão.

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

Etapa 3. Conecte o cliente sem fio ao SSID para reproduzir o problema.

Etapa 4. Pare as depurações depois que o problema for reproduzido.

no debug wireless mac <client-MAC-address>

Os registros capturados durante o teste são armazenados no WLC em um arquivo local com o nome:

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Se o fluxo de trabalho da GUI for usado para gerar esse rastreamento, o nome do arquivo salvo será debugTrace_aaaa.bbbb.cccc.txt.

Etapa 5. Para coletar o arquivo gerado anteriormente, copie o arquivo .log do ratrace para um servidor externo ou exiba a saída diretamente na tela.

Verifique o nome do arquivo de rastreamentos do RA com este comando:

dir bootflash: | inc ra_trace

Copie o arquivo para um servidor externo:

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

Como alternativa, exiba o conteúdo:

more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

Etapa 6. Remova as condições de depuração.

```
# clear platform condition all
```

Cenário de switching local Flexconnect (ou malha/SDA)

No caso do switching local flexconnect (ou malha / SDA), é o AP que aplica qualquer política de QoS que você definiu na WLC.

Nos pontos de acesso wave2 e 11ax, o limite de taxa ocorre em um nível por fluxo (5 tuplas) e não por cliente ou por SSID antes de 17,6.

Isso se aplica ao AP em implantações Flexconnect/Fabric, Embedded Wireless Controller on Access Point (EWc-AP).

A partir da versão 17.5, a substituição de AAA pode ser aproveitada para enviar os atributos para atingir o limite de taxa por cliente.

A partir da versão 17.6, o limite de taxa bidirecional por cliente é suportado nos APs 802.11ac Wave 2 e 11ax na configuração de switching local flexível.

Observação: os APs flexíveis não suportam a presença de ACLs nas políticas de QoS. Eles também não suportam o BRR (largura de banda restante) e a prioridade de política que são configuráveis através da CLI, mas não estão disponíveis na interface do usuário da Web do 9800 e não são suportados no 9800. O bug da Cisco ID <u>CSCvx81067</u> rastreia o suporte de ACLs em políticas de QoS para APs flex.

Configuração

A configuração é exatamente a mesma da primeira parte deste artigo, com duas exceções:

1. O perfil de diretiva está definido como switching local. A implantação do Flex exige que a Central Association esteja desabilitada até a versão Bengaluru 17.4.

A partir da versão 17.5, esse campo não está disponível para a configuração do usuário, pois é codificado.



2. A marca de site está definida como site não local



Solução de problemas do Flexconnect/Fabric

Como o AP é o dispositivo que aplica as políticas de QoS, esses comandos podem ajudar a restringir o que é aplicado.

show dot11 qos

show policy-map

show rate-limit client

show rate-limit bssid

show rate-limit wlan

show flexconnect client

<#root>

AP780C-F085-49E6#

```
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
                 0
shaped packets:
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)
total packets:
                 25673
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:

A8:DB:03:6F:7A:46 2 0 0 0 0 0 0 Statistics: up down name 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#

Referências

Guia de QoS do Catalyst 9000 16.12

Guia de configuração de QoS 9800

Modelo de configuração do Catalyst 9800

Notas da versão do Cisco IOS® XE 17.6

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.