v1.14_Setting 'Rate limit' (DHCP traffic) on AP and ESR

To configure DHCP shaper via EMS on an access point:

- 1. Select Configuration
- 2. Select Client.QoS Class Map tab
- Add a required class
 Protocol = 17 (UDP), Source/Destination Port = 67

Description Wi-Fi clients C	Competitive AP monitoring Monitoring Configuration Access				
Network					
Wireless settings	Row filter:				
Access	📰 🗊 Change fields 🧟 Reload 🔹 Add 🙆 Delete 🗳 Export				
Radio interfaces	Match layer 3 proto	Class map name	Match criteria configuration		
Virtual access points	IPv4	SSDP	Match Every : Off, Protocol : 17; Destination Port : 1900		
Key holder data	IPv4	mDNS	Match Every: Off: Protocol : 17: Destination Port : 5353		
GIODAI RADIUS	IDv/	nethios_dam_tcn	Nath Even : Off Protocol : 6: Destination Port : 139		
QoS EDCA parameters	10.4	netblos-ugniticp	Math Care Of Detroit of Destination for 130		
Client QoS, Global	IPV4	netbios-agm-uap	Match Every: Un; Protocol: 17; Destination Port: 138		
Client QoS. Class Map	IPv4	netbios-ns-tcp	Match Every: Off; Protocol : 6; Destination Port : 137		
Client QoS. Policy Map	IPv4	netbios-ns-udp	Match Every: Off, Protocol : 17; Destination Port : 137		
WDS	IPv4	vrrp	Match Every: Off, Protocol : 255; Destination IP Address : 224.0.0.18; Destination IP Mask : 255.255.255.255.255		
Captive Portal. Global	Matab aritaria an	efermation for ID-4	· · · · · · · · · · · · · · · · · · ·		
Captive Portal. Instance	iviateri criteria co	niguration for IPV4			
Cluster. Main	Class map name	DHCP SHAPER			
AirTune service					
System time	Match Every	* 011 💌			
System events	Protocol	17			
SNMP tran					
CLI/telnet	Source IP Address				
CLI/ssh	Source IP Mask				
	Destination ID Addre	ee 🗆			
	Destinution in Addre				
	Destination IP Mask				
	Source Port	67			
	Destination Port	67			
	EtherType				
	Charles Of Frendra				
	Class Of Service				
	Source MAC Addres	s 🗌			
	Source MAC Mask				
	✓ Accept ¥ Cancel				

When the class is created, select Client.QoS Policy.Map and add a policy ("Add Policy" button).

Description Wi-Fi clients	Competitive AP monitoring Monitoring Configuration Access		
Network			
Wireless settings	Row filter:		Linewrap
Access	🛛 😂 Reload 🛟 Add Policy 🄇	길 Delete Policy 🛟 Add Class 🍳	Delete Class
Radio interfaces			
Virtual access points		(port	
Key holder data	Policy map name	Class map name	Policy class definition
Global RADIUS	ChattyDrop	SSDP	Police Simple : Off, Send : Off, Drop : On
QoS. Main	ChattyDrop	mDNS	Police Simple : Off, Send : Off, Drop : On
QoS. EDCA parameters	ChattyDrop	netbios-dgm-tcp	Police Simple : Off, Send : Off, Drop : On
Client QoS. Global	Chath@rop	nethios-dam-udn	Police Simple - Off Send - Off Dron - On
Client QoS. Class Map	Chattybrop	netbios-agin-aup	
Client QoS. Policy Map	ChattyDrop	netbios-ns-tcp	Police Simple : Off, Send : Off, Drop : On
WDS	ChattyDrop	netbios-ns-udp	Police Simple : Off; Send : Off; Drop : On
Captive Portal. Global	ChattyDrop	vrrp	Police Simple : Off, Send : Off, Drop : On
Captive Portal. Instance		1	
Cluster. Main	_		
AirTune service	_	[*	
System time	_	Add Policy Map	×
System events	_	Input Policy Map name.	
SNMP	_	May contain values not more	than 31 characters long and without spaces
SNMP trap	_	Policy map name DHCF	P A A A A A A A A A A A A A A A A A A A
CLI/teinet			
- Lussii			Accept Cancel

Then add the class to the policy.

To do that, select the class and click "Add Class" button.

63 Host is up (0.00056s latency). PORT STATE SERVICE

DHCP_SHAPER	: IPv4	
SSDP	: IPv4	
mDNS	: IPv4	
netbios-dgm-tcp	: IPv4	
netbios-dam-udp	: IPv4	
netbios-ns-tcp	: IPv4	
netbios-ns-udp	: TPv4	
vrrp	: TPv4	
	✓ Accept X Cancel	

After that, specify limits and action in the opened window.

Policy Simple	Off 🔽
Committed Rate	
Committed Burst	
Action types	
Send	Off 💌
Drop	Off 💌
Mark Class Of Service	
Mark IP DSCP	NONE 🔻
Mark IP Precedence	
	Accept 🔀 Cancel

Policy Simple is a simplified setting where two parameters are defined:

- Committed Rate the bandwidth guaranteed for matching traffic.
 Committed Burst the maximum packet size in bytes that conforms the amount of traffic sent. It should ideally be 1.5 times higher than Committed Burst in bytes to work correctly.

The action performed on the traffic should be selected in Action types. Send — if set to On, all packets of corresponding traffic flow will be transmitted; Drop — if set to On, all packets of corresponding traffic will be dropped.

Only the traffic with certain speed should be transmitted, the rest of the packets should go to Drop. Consequently, enter the values and set Send to On.

Policy Simple	0n 🔻
Committed Rate	100
Committed Burst	12500
Action types	
Send	On v
Drop	Off v
Mark Class Of Service	
Mark IP DSCP	NONE V
Mark IP Precedence	
	✓ Accept 🔀 Cancel

The result will be a rule limiting DHCP traffic to 100 kbps.

Description Wi-Hickents Competitive AP monitoring Monitoring Configuration Access			
Network	Row filter:		
Wireless settings	C Dalaad Add Daliau	Delete Delieur	
Access	Veload Veload Veload	Delete Policy 🤯 Add Class	Telete Class
Virtual accors points	🔚 🖸 Change fields 🚿 Exp	ort	
Key holder data	Policy map name	Class map name	Policy class definition
Global RADIUS	ChattyDrop	SSDP	Police Simple : Off, Send : Off, Drop : On
QoS. Main	ChattyDrop	mDNS	Police Simple : Off: Send : Off: Drop : On
QoS. EDCA parameters	ChattyDrop	nethios-dam-tcn	Palice Simple : Off Send : Off Dron : On
Client QoS. Global	ChattyDrop	nothios dam ude	Palies Cimple - Off Control - Off Decord On
Client QoS. Class Map	Спацуртор	netolos-ugin-uup	Fonce simple cont, send cont, on the context of the sender s
Client QoS. Policy Map	ChattyDrop	netbios-ns-tcp	Police Simple : Off; Send : Off; Drop : On
WDS	ChattyDrop	netbios-ns-udp	Police Simple : Off, Send : Off, Drop : On
Captive Portal. Global	ChattyDrop	vrrp	Police Simple : Off; Send : Off; Drop : On
Captive Portal. Instance	DHCP	DHCP SHNAPER	Police Simple : On; Committed Rate : 100; Committed Burst : 12500; Send : On; Drop : Off
		-	
System time			
System events			
SNMP			
SNMP trap			
CLI/telnet			
CLI/ssh			

When configuring a shaper on ESR, either Discover (from client to server) or Offer (from server to client) transmitting may be limited.

1. Limiting DHCP Discover transmitting from client to server

```
security zone-pair any self
rule 999
action permit
rate-limit pps 2
match not fragment
match protocol udp
match destination-port DHCP
enable
exit
exit
```

2. Limiting DHCP Offer transmitting from server to client

```
security zone-pair apuser any
rule 999
    action permit
    rate-limit pps 2
    match not fragment
    match protocol udp
    match destination-port DHCP
    enable
    exit
exitt
```