Fair Usage Policy Implementation - Part II

We have provided a basic policy implementation for fair usage. In this example we will provide detailed configuration for PEAP in Mikrotik devices. In this example users have daily 500 MB quota and TekRADIUS will disconnect user session when the user consumes all assigned quota. User will be able to login after midnight when TekRADIUS will update user's daily quota. Session termination is done by sending a RADIUS disconnect request.

Network Topology



Mikrotik Configuration

Click IP / Addresses in Mikrotik WinBox menu and set an available IP address in your LAN for the bridge interface. You connection to the wireless device may be lost after this procedure. Try to reconnect if your connection is lost.



Set wireless interface parameters. Click Wireless in Mikrotik WinBox menu. Create a security profile first. Click + at Security Profiles tab.

Wireless Tal	bles									
Interfaces	Nstreme Dual	Access List	Registration	Connect List	Security P	rofiles Ch	annels			
+ -	T					Security P	rofile <tekr< th=""><th>ADIUS></th><th>,</th><th></th></tekr<>	ADIUS>	,	
	∧ Mode	Authen	ticatio Unio	cast Ciphers G	iroup Ciphers	General	RADIUS	EAP S	Static Keys	ОК
* default	dynamic k	eys WPA E	AP W aes	ccm a	es com			Name:	TekRADIUS	Cancel
								Mode:	dynamic keys	Apply
						A	uthenticatior	n Types:	WPA PSK WPA2 PS WPA EAP WPA2 EA	K P Copy
							Unicast	Ciphers:	🖌 aes ccm 📃 tkip	Remove
							Group	Ciphers:	✓ aes ccm 🗌 tkip	
						W	/PA Pre-Sha	red Key:		
0.7 (1	1					WF	A2 Pre-Sha	red Key:		
Z items (1 se	elected)						Supplicant	Identity:		
							Group Key	Update:	00:00:30	
						Man	agement Pro	otection:	allowed	F
						Manager	ment Protect	ion Key:		

Enter recommended values as shown above for General parameters. Set EAP Accounting at RADIUS tab.

Interfaces Name Access List Registration Connect List Security Profiles Channels Image: A construction Authenticatio Unicast Ciphers General RADIUS Image: Authentication OK TekRADIUS dynamic keys WPA EAP aes com aes com MAC Authentication OK * default dynamic keys WPA EAP www.aes com aes com MAC Accounting Apply Interim Update: 00:05:00 Copy MAC Format: XX:XX:XX:XX:XX Temove MAC Mode: as username Time: disabled Time: disabled Time:
Image: Security Profile < Tek RADIUS Name Mode Authenticatio Unicast Ciphers Tek RADIUS General RADIUS EAP Static Keys OK Image: Comparison of the state of the
Name Mode Authenticatio Unicast Ciphers General RADIUS EAP Static Keys OK Tek RADIUS dynamic keys WPA EAP aes ccm aes ccm MAC MAC Authentication Cancel Image: default dynamic keys WPA EAP www.aes ccm aes ccm MAC Accounting Apply Interim Update: 00:05:00 Copy MAC Format: XX:XX:XX:XX:XX Temove MAC Mode: as usemame Image: disabled

Set EAP Methods = passtrough at EAP parameters tab.

interfaces No	Imme Dual Acc	eas List Registr	ation Connect L	HE Security P	Channels	Tek RADUU	50		6
Name TekRADAUS defaut	Mode dynamic keya dynamic keya	Adherocatio WPA2 EAP WPA EAP W	Unicast Ophers aes con ees con	Group Opher ses cont wes cont	General RADI EAP Methods TLS Mode TLS Cettricate	dont verf	Static Keys y cetticate	¥ 0 ¥ ¥	OK Cancel Apply Copy Remove
2 Itema (1 select	ed)								

Double click wlan1 interface at Interfaces tab. Set "ap bridge" as Mode, set a name for SSID, set Bridge Mode = enabled, select previously set security profile, select Default Authentication option at the bottom.

	Interface <wlan1></wlan1>				
	General Wireless	HT HT MCS	WDS Nstreme	NV2 Status	ОК
	Mod	e: ap bridge		₹	Cancel
Wireless Tables	Ban	d: 2GHz-B/G/N		₹	Apply
Interfaces Nstreme Dual Access List Registration	Channel Widt	h: 20/40MHz C	e		Disable
+ ▼ -	Frequenc	y: auto		▼ MHz	Comment
Name 🛆 Type	SSI	D: Internet		^	
S 🔅 wlan1 Wireless (Atheros AR9	Scan Lis	st: default		= +	Advanced Mode
	Wireless Protoco	ol: any		Ŧ	Torch
	Security Profil	e: TekRADIUS		Ŧ	Scan
	Bridge Mod	e: enabled		₹	Freq. Usage
	VLAN Mod	e: no tag		Ŧ	Align
	VLAN II	D: 1			Sniff
					Snooper
•	Default AP Tx Rat	e:		▼ bps	Reset Configuration
1 item out of 3 (1 selected)	Default Client Tx Rate	e:		▼ bps	
		Default Au	thenticate		
		Default Fo	rward		
		Hide SSID			
	enabled	running	slave	running ap	

Create a RADIUS server profile for wireless service next. Click Radius menu option in Mikrotik WinBox menu. Select only "wireless" as Service option, enter IP adddress of TekRADIUS installed machine, shared secret for RADIUS communications, 1812 for the authentication, 1813 for the accounting port. 5000 ms is recommended for the Timeout parameter. Click OK to accept settings.

Radius					
+ - * x	Reset State	us Inco	ming	Fin	d
# Service	Called ID [Domain	Address	Secret	•
0 wireless			192.168.88.3		
	Radius Server <1	92.168.88.	3>		
	General Status	3			OK
	Serv	ice: pp	p 🔤 🗌 login		Cancel
		dh	cp	55	Apply
	Called	ID:		•	Disable
	Dom	ain:			Comment
	Addr	ess: 192.1	68.88.3		Сору
1 item (1 selected)	Sec	cret:			Remove
	Authentication F	Port: 1812			Reset Status
	Accounting F	Port: 1813			
	Time	out: 5000		ms	
		Ac	counting Backu	0	
	Re	alm:			
	Src. Addr	ess: 0.0.0	0	▲	
	enabled				

Click Incoming button, click Accept option and set 3799 as Port.

Radiu	2L					
÷		Reset Sta	atus Inc	coming	Find	
#	Service	Called ID	Domain	Address	Secret	-
0	wireless			192.168.88.3		
			[Radius Incoming		
				Port:	Accept	OK Cancel
				Requests:	0	Apply
				Bad Requests:	0	Reset Status
				Acks:	0	
				Naks:	0	
1 iten	n					

TekRADIUS Configuration

Create a RADIUS client entry for the wireless access device first. the 'Interim Update Period' may be set to force TekRADIUS to clear any associated active sessions and simultaneous session entries

if an update is not received in the period specified. The minimum allowed value for interim update period is 60 seconds. 300 seconds (*5 minutes*) is set as interim update period in this example. You need to set Mikrotik as vendor.

🥃 TekR	ADIUS Ma	nager LT 5 Help	.4 [SP]									-		×
Users	Groups	Clients	Settings	Application Lo	g Active Se	ssions	Diction	nary Editor	Reportin	ig Count	ers S	QL I	Proxy	
NAS			Secre	t '	Vendor	Enable	ed	Interim Up	date					
192.1	68.88.21		test		mikrotik	Yes		300						
RADI	US Client	: Propertie	s											
NAS			S	ecret	Username Part	t		Vendor		Enabled	Inter	im Upda	te Period	
192.1	68.88.21		t	est				mikrotik	~	Yes N	<u> </u>	00 -	seconds	
	mmand												+	×
Selected	client rer	moved								TekRAD	DIUS LT	Servio	e is runnir	1g 😺 .:

User and Group Profiles

Here are typical group and user profiles created for this scenario;

sers Groups Clients Settings Application Log	Active Sessions	Dictionary	Editor	Reporting	Counters	SQL	Proxy	r	
Browse Groups	Group myfupg	group (Enab	led)						
Group-Na V like V V Group Name 1h 3h Blank Default myfupgroup RAS-RDP-Access RAS-RDP-Access RAS-RDP-Access-2FA RAS-RDP-Access-2FA-GA settimanale Teachers Wired	Attribute Credit-Period Credit-Per-Pe Credit-Expiry TLS-Server-(Credit-Unit	eriod Action Certificate	Type Check Check Check Check Check	Value Daily 500 Send- office. MByte	PoD kaplansoft. s-sum	.com			
									_

Group profile

🥃 TekRADIUS Manager LT 5.4 [SP]			- 0	×
<u>File Service H</u> elp				
Users Groups Clients Settings Application Log Active	essions Dictionary Editor	Reporting Counters	SQL Proxy	
Browse Users User of	rsun (Enabled)			
All Ver-Name Ver like Ver Attrib	te Type	Value		
Username Group User-	assword Check	****		
dursun myfupgroup	redit Check	500		
		10.07.0010.1	0.00	
Enter username mytupgi 🖌 📴 🛉 📝 🗙 Check	V First-Logon	10.07.2018 1	.0:23: 🔨 🖓 🕂 7	~
User 'dursun' selected		TekRADIUS I	LT Service is running	7

Sample user profile

User profile has Credit-Period = Daily and Credit-Per-Period = 5000 attributes. These attributes grant user to have 500 MB data usage. User's data quota will be reset daily. You can also set User-Credit manually when needed.

TLS-Server-Certificate is required for PEAP authentication you can create a server certificate using TekCERT.

TekRADIUS will disconnect user session(s) when all the the credit is consumed. You can disconnect active user sessions manually through Active Sessions tab by selecting active user sessions and clicking **PoD** button.