

Application notes



version 1.1 3/2/2018

RACOM s.r.o. • Mirova 1283 • 592 31 Nove Mesto na Morave • Czech Republic Tel.: +420 565 659 511 • Fax: +420 565 659 512 • E-mail: racom@racom.eu

Table of Contents

ntroduction	5
I. Basic Backup Example	6
1.1. MIDGE Configuration	6
1.2. Practical Test	0
2. Mobile IP together with VPN tunnels	2
2.1. MIDGE Configuration	2
2.2. MG102i Configuration	8
2.3. Practical Test	7
A. Revision History	9

Introduction

Under typical circumstances, VPN tunnels between central M!DGE and other routers are established over the WAN network. When the WAN fails, traffic to/from the respective remote router is automatically redirected to the cellular network.

1. Basic Backup Example



Fig. 1.1: Basic Backup Example

1.1. M!DGE Configuration

MIDGE



		S ROUTING FIREWALL VPN S	
Status Summary	Summary		
WAN	Description	Administrative Status	Operational Status
WWAN Ethernet	Hotlink		LAN2
LAN	LAN2	enabled	ир
DHCP IPsec System	WWAN1	enabled	down
	IPsec1	enabled	ир

Fig. 1.2: Central M!DGE HOME menu

MIDGE is connected via the WAN network using its LAN2 interface. The WWAN1 link (cellular network) is down and the IPsec VPN connection is already established. To achieve this, several steps must be performed.

1.1.1. Ethernet Ports

In the example, the first port (LAN1) is used for the local subnet 192.168.1.0/24 and the WAN port (LAN2) is configured with an IP address 192.168.131.239/24. See the following pictures for the details.

N!DGE		
		ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
WAN Link Management Supervision Settings	LAN1 LAN2	
Ethernet Port Assignment VLAN Management IP Settings	Mode:	● LAN ● WAN
Mahila	Static Configuration	
SIMs	IP address:	192.168.1.1
USB	Subnet mask:	255.255.255.0
Serial	Alias IP address:	
Digital I/O	Alias subnet mask:	

Apply Continue

Fig. 1.3: Central MIDGE LAN1 configuration

M!DGE



HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Management		
unervision		
Settings	IP Settings LAN2	
hernet	Mode:	
ort Assignment		
LAN Management		• WAN
P Settings		
obile	WAN mode:	DHCP client
SIMs		static IP
Interraces		DDDoF
SB		⊖ FFF6E
erial	Static Configuration	
igital I/O	IP address:	192.168.131.239
	Subnet mask:	255.255.255.0
	Default gateway:	192.168.131.253
	Primary DNS server:	192.168.0.2
	Secondary DNS server:	192.168.0.29
	MTU:	

Fig. 1.4: Central M!DGE WAN configuration

1.1.2. Cellular Network

For the backup link, you need to configure your SIM card and APN accordingly. The configuration is made in the INTERFACES – Mobile menu. Configure it to meet your APN configuration.

N!DGE		
	HOME INTERFACES ROUTING FIRE	WALL VPN SERVICES SYSTEM LOGOUT
WAN Link Management Supervision Settings	Edit WWAN Interface WWAN1 Mobile Connection Advanced	
Ethernet Port Assignment VLAN Management IP Settings	Connection settings:	id from database ecify
Mobile	Phone number: *99***1#	
Interfaces	Access point name:	
USB	Authentication: PAP	v
Serial		
Digital I/O	Username:	
	Password:	
	Apply	

Fig. 1.5: Mobile interface configuration

Use manual for more details about the mobile interface configuration¹.

1.1.3. VPN Tunnel

Configure and enable the IPsec (or OpenVPN) tunnel to the remote peer. In the example, the local network is 192.168.1.0/24 and remote network is 192.168.20.0/24.

N!DGE								
	HOME I	NTERFA	CES ROUTING	G FIREWALL	VPN SEF	RVICES SYSTE	M LOGOUT	
OpenVPN Administration	IPsec Tunn	el Configu	ration					
Tunnel Configuration	Name	Туре	Peer	IKE	IPsec	Local Network	Remote Network	
IPsec	Tunnel 1	psk	10.203.3.33	3des-md5	3des-md5	192.168.1.0/24	192.168.20.0/24	
Administration Tunnel Configuration								•

Fig. 1.6: IPsec configuration

Keep in mind that you need to configure Peer IP address to be reachable via both connections (WAN and WWAN) so it may establish IPsec connection.

¹ http://www.racom.eu/eng/products/m/midge1/web_conf.html#interfaces

See the VPN examples in VPN Configuration² application note or the manual³ for more details.

1.1.4. WAN Link Management

In the Link Management menu, configure the LAN2 interface as the permanent and primary option. Set the WWAN interface as its backup. The Establishment mode can be either set to "on switchover" (to be connected only when the permanent link is not active) or "permanent" (to be connected all the time – it is used for the faster link switching).

M!DGE



	HOME	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT			
WAN Link Management		k Management			
Supervision Settings	In case a establishe multiple li	In case a WAN link goes down, the system will automatically switch over to the next link in order of priority. A link can be either established when the switch occurs or permanently to minimize link downtime. Outgoing traffic can also be distributed over multiple links on a per IP session basis.			
Ethernet	Priority	Interface	Operation Mode		
VLAN Management	1st	LAN2	permanent 🗸	1	I E
IP Settings	2nd	WWAN1	on switchover 🗸	0	ľ
Mobile SIMs Interfaces	Apply				

Fig. 1.7: WAN Link Management

Another step is configuring the Supervision feature.

² http://www.racom.eu/eng/products/m/midge/app/vpn/index.html

³ http://www.racom.eu/eng/products/m/midge1/web_conf.html#VPN

MIDGE

	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT				
WAN	Link Supervision				
Supervision Settings	Network outage detection can be pe declared as down in case all trials fa	rformed by sending pings on each WAN link to authoritative hosts. The link will be illed. You may further specify an emergency action if a certain downtime is reached.			
Ethernet	Link:	ANY V			
Port Assignment VLAN Management IP Settings	Mode:	also validate when link comes up			
		only validate if link is up			
Mobile	Primary host:	10.203.0.1			
Interfaces	Secondary host:	(optional)			
USB	Ping timeout:	5000 milliseconds			
Serial	Ping interval:	60 seconds			
Digital I/O	Retry interval (if ping failed):	30 seconds			
	Max. number of failed trials:	5			
	Emergency action:	none			
		restart link services			
		💽 reboot system			
		after 30 minutes being down			

Apply

Fig. 1.8: Supervision

The Supervision enables MIDGE to control the link switching procedure. In our example, MIDGE checks the connection by executing the ping packets to the host on the IP address 10.203.0.1. If five consecutive ping packets are unsuccessful, the link is considered down and is switched. If there is no connectivity for 30 minutes, the unit is rebooted as a result of the Emergency action.

Both links are checked when they are up (Link – ANY), otherwise you could choose just one link to be checked or create two different Supervision for each link (e.g. lower timeouts and more frequent checks on the WAN link).

1.2. Practical Test

Now you should be connected via the primary WAN link (LAN2). The easiest way to test the switching is to unplug the ETH cable from the LAN2 interface. MIDGE almost immediately recognizes the unplugged cable and it switches to the cellular network. The VPN tunnel should also be reestablished.



MIDGE

Status

RACOM

HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
 Summary

Summary	,		
WAN	Description	Administrative Status	Operational Status
WWAN	Li - Hi- I-		1404/4 NI1
Ethernet	Houink		WWWAINT
LAN	LAN2	enabled	down
IPsec	WWAN1	enabled	up
System	IPsec1	enabled	up

Fig. 1.9: WWAN link is UP



Note

You can test the connectivity by issuing a ping to any desired IP address (e.g. behind the VPN tunnel) in the SYSTEM – Troubleshooting – Network debugging menu.

Plug the cable back into the LAN2 interface and wait a moment for the MIDGE to reestablish the primary connection again.

You can also check the correct functioning of the Supervision feature.

Fill in both host IP addresses in the Supervision menu. One needs to be reachable only via the cellular network and the other one only via the WAN network. Turn off the server with an IP address reachable via the WAN network. The active connection should be changed to the cellular network. Turn on the server again and see the link switch back to the primary one.

2. Mobile IP together with VPN tunnels

If the primary link fails in the previous example, our MIDGE has to dial up the mobile connection and reestablish the VPN tunnel which can take more time than your application can handle. With Mobile IP and permanent backup link availability, we can shorten this time to several seconds...



Fig. 2.1: MobileIP with VPN tunnel example topology

The diagram depicts an example in which the M!DGE unit is the VPN and MobileIP server. The server has just one connection option and it needs to communicate with the device behind the remote MG102i unit.

The remote MG102i unit has two possible connection types. The primary link is via faster leased line to the provider's network and the cellular connection is the backup option. Both will be "up" permanently.



Note

The remote connection types can be various, e.g. using WLAN or dualSIM unit with two cellular providers.

On both units, we configure the Mobile IP feature so the VPN tunnel can resist switching the links.

2.1. MIDGE Configuration

On the central M!DGE unit, we need to configure Ethernet IP addresses, mobile connection, VPN tunnel, correct time and of course Mobile IP.

2.1.1. Ethernet

The Ethernet IP address of the server is 192.168.1.1 with 255.255.255.0 mask.

MIDGE



AN	LAN1 LAN2	
.ink Management 3upervision		
Settings	IP Settings LAN1	
thernet Port Assignment	Mode:	
IP Settings		
	Static Configuration	
SIMs Interfaces	IP address:	192.168.1.1
ISB	Subnet mask:	255.255.255.0
50		
erial	Alias IP address:	
igital I/O	Alias subnet mask:	

Apply Continue

Fig. 2.2: Server's Ethernet configuration

The server is utilizing only the first port so you do not need change the LAN2 IP address. Another step is to define the mobile connection. Configure the SIM card, APN and username/password in the INTER-FACES - Mobile menu and check whether it is enabled afterwards.

MIDGE				
	HOME		I ROUTING FIREWALL VPN SERVIC	ES SYSTEM LOGOUT
WAN Link Management Supervision Settings	WAN Lin In case a establish multiple I	Ik Management WAN link goes o hed when the swit links on a per IP s	own, the system will automatically switch over to the ch occurs or permanently to minimize link downtime ession basis.	next link in order of priority. A link can be either . Outgoing traffic can also be distributed over
Ethernet Port Assignment	Priority	Interface	Operation Mode	
VLAN Management IP Settings	1st	WWAN1	permanent v	ß
Mobile SIMs Interfaces	Apply	0		

Fig. 2.3: Server mobile connection is activated

In case you will use OpenVPN tunnel, it's necessary to have a correct time in the unit. This can be achieved by setting the NTP server to synchronize the internal time. Go to the SYSTEM – Time & Region menu and fill in the reachable NTP server of your choice. Also set the correct time zone and Daylight saving option.



Note

If using IPsec tunnel, it is not necessary to have a correct time our routers, but it is still useful for troubleshooting.

MIDGE



RACOM

System Settings	 System Time	
Time & Region Reboot	Current system time:	2015-06-03 12:54:51 Set time
Authentication	Time Synchronisation	
User Accounts	NTP server 1:	10.203.0.1
Remote Authentication	NTP server 2 (optional):	
Software Update Software Update Firmware Update	Time zone	
Software Profiles	Time zone:	UTC+01:00 Belgrade, Bratislava, Budapest, Prague 🗸
Configuration File Configuration	Daylight saving changes:	
Troubleshooting	Apply Sync	

Fig. 2.4: NTP Configuration

2.1.2. Mobile IP

Now we need to configure the MobileIP functionality. With Mobile IP, the client (mobile node) can be connected to the network anywhere and if the server's (home agent) cellular IP address is reachable from the client, you can always communicate via new pair of IP addresses. See the details in the example.

MIDG6	
-------	--

Stat

HOME INTERFACES ROL	JTING FIREWALL VPN SERVICES SYSTEM LOGOUT
– Mobile IP	
Mobile IP can be used to move from	m one network to another while maintaining a permanent IP address and thus avoiding that
running IP sessions (including VP	N tunnels) must be reconnected.
Administrative status:	 mobile node home agent
	disabled
Home network address:	192.168.36.1
Home network mask:	255.255.255.0
-	HOME INTERFACES ROU Mobile IP Mobile IP can be used to move fro running IP sessions (including VPI Administrative status: Home network address: Home network mask:

Fig. 2.5: Mobile IP Home agent configuration

The configuration itself is very easy. Just choose the "home agent" status and fill in the agent's IP address and mask - in our example it is 192.168.36.1/24.

The Mobile IP is automatically enabled afterwards.

Another step is to configure the clients (mobile nodes). For each client, define a specific SPI (36 in our example), authentication type (prefix-suffix-md5) and shared secret (ASCII password).

M!DGE		
		UTING FIREWALL VPN SERVICES SYSTEM LOGOUT
Static Routes	SPI:	36
Extended Routes	Authentication type:	prefix-suffix-md5 🗸
Multipath Routes	Shared secret:	ASCII 🗸
Mobile IP Administration Mobile Nodes	Apply Cancel	

Fig. 2.6: Mobile nodes

The last step is to configure the VPN tunnel. It can either be OpenVPN or IPsec, the functionality is the same in this example.

2.1.3. OpenVPN

Configure the OpenVPN server in routed mode.

|--|--|

penVPN	Tunnel 1 Tunnel 2	Tunnel 3 Tunnel 4
Administration Tunnel Configuration	OpenVPN Tunnel 1 Configura	tion
Client Management	Operation mode:	disabled
Sec Administration		client
Tunnel Configuration		• server • expert
PTP Administration	Server port:	1194
Tunnel Configuration	Туре:	TUN 🗸
RE Administration	Protocol:	UDP V
Tunnel Configuration	Network mode:	• routed MTU:
ial-in Server	_	bridged
	Cipher:	AES-128-CBC 🗸
	Authentication:	certificate-based V
		HMAC digest: SHA512 V
	Options:	✓ use compression
		✓ use keepalive

Apply Erase

Fig. 2.7: OpenVPN server, Mobile IP

Configure one client (MG102i). Configure the correct IP subnets.

MIDGE

Оре

IPse Ad

PPT Ad

GRE

Dial-in Server

)penVPN	Clients	Networking	Routes	Download	
Administration Tunnel Configuration	Transport Netw	ork			
Client Management	Network:		10.8.0.0		
^o sec Administration	Netmask:		255.255.2	55.0]
Tunnel Configuration					
PTP Administration	Client Networks This menu can b	e used to configure	a fixed tunnel en	dpoint address fo	r each client. You may also specify a network whose
I unnel Configuration	puono to ono dia g	got routou tomardo a	io onorit.		
RE Administration	Select client:		midgeWA	NV	
Tunnel Configuration					

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT

Tunnel address: dynamic fixed Client network: Onone specify Network: 192.168.10.0 Netmask: 255.255.255.0

Apply

Fig. 2.8: OpenVPN server - Networking

MIDGE

HOME | INTERFACES | ROUTING | FIREWALL | VPN | SERVICES | SYSTEM | LOGOUT Routes Clients Networking Download OpenVPN Administration **Client Routes** Tunnel Configuration Client Management This list of network routes will be pushed to each client, so that matching packets will be routed back to the server. Network Netmask IPsec Administration 192.168.1.0 255.255.255.0 Tunnel Configuration PPTP Administration Tunnel Configuration GRE Administration Tunnel Configuration Dial-in Server Enable routing between clients: ~ Apply

Fig. 2.9: OpenVPN server - Routes

The only difference to the basic VPN configuration is when downloading the Expert file for the client. You must configure the Mobile IP address (192.168.36.1 in our example) so the remote unit connects via Mobile IP network.







M!DGE		٩
	HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT	
OpenVPN Administration Tunnel Configuration	Clients Networking Routes Download Download Expert Mode Files	
Client Management	Server address/hostname: 192.168.36.1	
IPsec Administration Tunnel Configuration	Download	

Fig. 2.10: OpenVPN server - Downloading expert file

Enable OpenVPN server and **uncheck** the box for "**Restart on link change**". This is very important step, do not forget to uncheck this box. If the box is checked, everytime any link changes the status, the tunnel is restarted and we do not want this. This is mainly important on the client's side.

MIDGE		
	Home Interfaces Routing Firewall VPN Ser	VICES SYSTEM LOGOUT
OpenVPN Administration Tunnel Configuration	OpenVPN Administration OpenVPN administrative status:	
Client Management	Glabled disabled	
Administration Tunnel Configuration PPTP	Apply Restart	

Fig. 2.11: Enabling OpenVPN server

When we finish all configuration steps, we should see the following state in the HOME menu.

N!DGE			
		S ROUTING FIREWALL VPN S	SERVICES SYSTEM LOGOUT
Status Summary	Summary		
WAN	Description	Administrative Status	Operational Status
WWAN Ethernet	Hotlink		WWAN1
LAN	WWAN1	enabled	up
OpenVPN	OpenVPN1	enabled, server	up
IPsec MobileIP	MobileIP	enabled	up
System			

Fig. 2.12: OpenVPN server and Mobile IP are running

2.1.4. IPsec

If you want to use IPsec, the situation is very similar. Just configure the correct IP subnets, set Peer IP address to the Mobile IP address (192.168.36.2) and uncheck the "Restart on link change" box as with OpenVPN.

M!DGE									
	HOME II	NTERFA	CES ROUTING	i FIREWALL	VPN SEF	RVICES SYSTEI	M I LOGOUT		
OpenVPN Administration	IPsec Tunn	el Configu	ration						
Tunnel Configuration	Name	Туре	Peer	IKE	IPsec	Local Network	Remote Network		
Client Management	Tunnel 1	psk	192.168.36.2	3des-md5	3des-md5	192.168.1.0/24	192.168.10.0/24	ľ	
IPsec									•
Fig. 2.13: IPsec – M	1!DGE config	uratio	n						
	HOME II	NTERFAC	ces _I routing	i FIREWALL	VPN SEF	RVICES SYSTEI	M I LOGOUT		
OpenVPN Administration	IPsec Admi	inistration							
Tunnel Configuration Client Management	IPsec admi	nistrative s	status:	• enabled					
IPsec				U disabled					
Administration	Propose N/	AT traversa	al:	✓					

Apply
Apply

Restart on link change:

Fig. 2.14: Enabling IPsec – M!DGE

Tunnel Configuration

PPTP Administration Tunnel Configuration

2.2. MG102i Configuration

The client's configuration is more complex due to two connectivity options. The unit needs to be connected to both options simultaneously (permanently).

2.2.1. WAN Configuration

MG102



	LANI	
VAN	LAINT	
Link Management		
Settings	IP Settings LAN5	
thernet	Mode:	LAN
Port Assignment		
VLAN Management		WAN
IP Settings		
Nobile	WAN mode:	OHCP client
SIMs		• static IP
Interfaces		DDDoE
VLAN		€ PPP0E
Administration	Static Configuration	
Configuration	g	
IP Settings	IP address:	192.168.131.239
JSB	Subnet mask:	255.255.255.0
erial		
)igital I/O	Default gateway:	192.168.131.253
INSS	Primary DNS server:	192.168.0.2
	Secondary DNS server:	192.168.0.29
	MTU:	

Fig. 2.15: MG102i WAN configuration

The LAN5 interface is configured as the primary WAN link. LAN1 subnet should be set to 192.168.10.1/24.

MG102i

		OUTING FIREWALL VPN SERVICES SYSTEM LOGOUT
WAN	LAN1 LAN5	
Link Management		
Supervision		
Settings	IP Settings LAN1	
Ethernet	Mode:	
Port Assignment		
VLAN Management		WAN
IP Settings		
Mobile	Static Configuration	
SIMs	IP address:	192 168 10 1
Interfaces		152.100.10.1
	Subnet mask:	255.255.255.0
WLAN		
Administration		
Configuration	Alias IP address:	
IP Settings		
JSB	Allas subnet mask.	
Serial		
Digital I/O	Apply Continue	

Fig. 2.16: MG102i LAN configuration

Configure the mobile connection and set both links to be permanently "up".

//G102 i				
	HOME	INTERFACE	S ROUTING FIREWALL VPN SERVICES S	SYSTEM LOGOUT
WAN Link Management Supervision Settings	WAN Lini In case a establish multiple l	k Management WAN link goes ed when the swi inks on a per IP	down, the system will automatically switch over to the next l tch occurs or permanently to minimize link downtime. Outg session basis.	link in order of priority. A link can be either oing traffic can also be distributed over
Ethernet Port Assignment	Priority	Interface	Operation Mode	
VLAN Management	1st	LAN5	permanent 🗸	
IP Settings	2nd	WWAN1	permanent 🗸	1
Mobile SIMs Interfaces	Apply)		

Fig. 2.17: MG102i Link Management

We need to recognize that LAN5 is not available for us and switch to WWAN interface. This is recognized if the Ethernet cable is disconnected, but with Supervision feature, we can check the IP host reachability with ping probes and if this host is not reachable, switch to the backup profile.

In our example, we configure this for each link separately.



MG102

VAN Link Management	Link Supervision			
Supervision Settings	Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reache			
hernet	Link:	LAN5 V		
Port Assignment VLAN Management IP Settings	Mode:	 also validate when link comes up only validate if link is up 		
obile SIMs	Primary host:	192.168.131.102		
Interfaces	Secondary host:	(optional)		
LAN Administration	Ping timeout:	1000 milliseconds		
Configuration	Ping interval:	10 seconds		
P Settings	Retry interval (if ping failed):	5 seconds		
SB	Max. number of failed trials:	5		
erial	Emergency action:			
igital I/O		onne		
NSS		restart link services		

Fig. 2.18: LAN5 Supervision

The primary link is checked every 10 seconds by pinging the 192.168.131.102 host. If the ping is lost 5 times, the link is considered down and the mechanism switches to the WWAN option.

MG102i



HOME INTERFACES ROUT	TING FIREWAI	L VPN SERVICES	SYSTEM LOGOUT
Link Supervision			
Network outage detection can be performed by sending pings on each WAN link to authoritative hosts. The link will be declared as down in case all trials failed. You may further specify an emergency action if a certain downtime is reached.			
Link: WWAN1 V			
Mode:	 also val only val 	lidate when link comes up lidate if link is up	
Primary host:	10.203.0.1		
Secondary host:			(optional)
Ping timeout:	5000	milliseconds	
Ping interval:	60	seconds	
Retry interval (if ping failed):	30	seconds	
Max. number of failed trials:	5		
Emergency action:	• none		
	restart I	ink services	
	HOME INTERFACES ROUT Link Supervision Network outage detection can be pedeclared as down in case all trials fate in the second sec	HOME INTERFACES ROUTING FIREWAL Link Supervision Metwork outage detection can be performed by sending declared as down in case all trials failed. You may furth Link: WWAN1 ~ Mode: • also va • only va Primary host: 10.203.0.1 Secondary host: Ping timeout: 5000 Ping interval: 60 Retry interval (if ping failed): 30 Max. number of failed trials: 5 Emergency action: • none restart I	HOME INTERFACES ROUTING FIREWALL VPN SERVICES Link Supervision Network outage detection can be performed by sending pings on each WAN link to a declared as down in case all trials failed. You may further specify an emergency action Link: WWAN1 ~ Mode: • also validate when link comes up • only validate if link is up Primary host: 10.203.0.1 Secondary host: 10.203.0.1 Ping timeout: 5000 Ping timeout: 60 seconds Retry interval (if ping failed): 30 seconds Max. number of failed trials: 5 Emergency action: • none • restart link services • reboot system

Apply

Fig. 2.19: WWAN1 Supervision

The WWAN1 interface is also checked, but we increased the ping timeout (mobile latency can be high) and we check the reachability (of IP 10.203.0.1) less frequently.



Note

In this example, if we switch off the host 192.168.131.102, the Supervision feature will switch the active link to WWAN. It is good to have a similar option for your own testing.

Configure the NTP server in the SYSTEM – Time & Region menu so we have the correct time.

MG102		
	HOME INTERFACES RO	UTING FIREWALL VPN SERVICES SYSTEM LOGOUT
System Settings	– System Time	
Time & Region Reboot	Current system time:	2015-06-02 21:15:13 Set time
Authentication	Time Synchronisation	
Authentication User Accounts	NTP server 1:	10.203.0.1
Remote Authentication	NTP server 2 (optional):	1.pool.ntp.org
Software Update Software Update Firmware Update	Sync time from GNSS:	
Software Profiles	Time zone	
Configuration File Configuration	Time zone:	UTC+01:00 Belgrade, Bratislava, Budapest, Prague 🗸
Factory Configuration	Daylight saving changes:	
Troubleshooting Network Debugging	Apply Sync	

Fig. 2.20: MG102i NTP configuration

2.2.2. Mobile IP

Our MG102i unit needs to be configured as a mobile node for the Mobile IP functionality. Go to the Routing – Mobile IP menu.

Mobile IP together w	vith VPN tunnels
----------------------	------------------

MG102i

Static Routes	- Mahila ID			
Extended Routes	Mobile IP can be used to move from o	ne network to another while maintaining a nermanent ID address and thus avoiding		
Multipath Routes	that running IP sessions (including VF	woone IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.		
Mobile IP Administration	Administrative status:	• mobile node		
		home agent		
Administration		disabled		
Classification				
	Primary home agent address:	10.203.3.28		
	Secondary home agent address:	(optional)		
	Home address:	192.168.36.2		
	SPI:	36		
	Authentication type:	prefix-suffix-md5 🗸		
	Shared secret:	ASCII 🗸		
	Life time:	3600		
	MTU:	1468		
	UDP encapsulation:	enabled disabled		
	Mobile network address:	(optional)		
	Mobile network mask:	(optional)		

Fig. 2.21: MG102i Mobile IP – Mobile node

Set the Primary home agent address to the cellular IP address of the M!DGE (server) unit, 10.203.3.28 in our example. The home address must fall into the 192.168.36.0/24 subnet. Set the correct SPI which was configured on the server and fill in the correct secret. Keep the rest in the defaults.

Another step is to define the server's Mobile IP address (192.168.36.1/32 via MobileIP1 interface) in the Routing menu.



RACOM

		CES ROUTING FIRE	EWALL I VPN I SERVIO	CES SYSTEM	LOGOUT	_	
Static Routes	Static Routes	- Static Routes					
Extended Routes	This menu shows all	routing entries of the system	, they can consist of active a	and configured ones	h.,		
Multipath Routes	The flags are as follows: (A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route (Netmasks can be specified in CIDR notation)						
Mobile IP	Destination	Netmask	Gateway	Interface	Metric	Flags	
Administration	0.0.0.0	0.0.0.0	192.168.131.253	LAN5	0	AD	
QoS Administration	10.64.64.64	255.255.255.255	0.0.0.0	WWAN1	0	АН	
Classification	192.168.10.0	255.255.255.0	0.0.0.0	LAN1	0	AN	
	192.168.131.0	255.255.255.0	0.0.0.0	LAN5	0	AN	
	192.168.36.1	255.255.255.255	0.0.0.0	MOBILEIP1 ~	0	АРН 🔽	∕]×
							-

Fig. 2.22: MG102i Routing menu

Without this option, MG102i unit would not know the server's Mobile IP address which is essential for the proper functionality of Mobile IP.

2.2.3. OpenVPN

MG102i is a client in the OpenVPN configuration so just upload the Expert file and set the mode to "Routed".

MG102[°]

	Tuppel 1 Tuppel 2	Tuppel 2 Tuppel 4	
OpenVPN Administration Tunnel Configuration	OpenVPN Tunnel 2 Configura	ation	
Psec	Operation mode:	disabled	
Administration		•	standard
Tunnel Configuration			• expert
PPTP		U server	
Administration			
Tunnel Configuration	Network mode:	routed	
GRE		bridged	
Administration			
Tunnel Configuration	Expert mode file:	installed	
Dial-in Server			

Fig. 2.23: MG102i OpenVPN - Expert file

Enable the tunnel and **uncheck** the **"Restart on link change"**. This is essential for fast switching of active link, do not forget to uncheck this option.

MG102i			
	HOME INTERFACES ROUTIN	IG FIREWALL VPN SERVICES SYSTEM	LOGOUT
OpenVPN Administration Tunnel Configuration	- OpenVPN Administration OpenVPN administrative status:		
IPsec Administration		or enabled disabled	
Tunnel Configuration PPTP Administration	Apply Restart		

Fig. 2.24: Enabling OpenVPN – MG102i

The tunnel should be established quickly and the HOME menu should be similar to the following example.

MG102			
		S ROUTING FIREWALL VPN S	Services System Logout
Status Summary	Summary		
WAN	Description	Administrative Status	Operational Status
WWAN Ethernet	Hotlink		LAN5
LAN	LAN5	enabled	up
OpenVPN	WWAN1	enabled	up
IPsec MobileIR	OpenVPN2	enabled, client	up
System	MobileIP	enabled	up

Fig. 2.25: OpenVPN and Mobile IP running - MG102i

2.2.4. IPsec

If you choose IPsec, configure the tunnel as on the server (credentials, IDs switched, networks switched, ...) and set the Peer IP to 192.168.36.1 (Mobile IP address of MIDGE unit).



Fig. 2.26: IPsec configuration - MG102i

Enable the tunnel and uncheck the "Restart on link change" box again.

MG102		
	HOME INTERFACES ROU	ITING FIREWALL VPN SERVICES SYSTEM LOGOUT
OpenVPN Administration	IPsec Administration	
Tunnel Configuration	IPsec administrative status:	• enabled
IPsec		O disabled
Administration Tunnel Configuration	Propose NAT traversal:	×
PPTP Administration	Restart on link change:	
Tunnel Configuration	Apply Restart	

Fig. 2.27: Enabling IPsec - MG102i

If configured correctly, check the HOME menu.

MG102					
		۲ ROUTING FIREWALL VPN ۲	ERVICES SYSTEM LOGOUT		
Status Summary	Summary				
WAN WWAN Ethernet	Description	Administrative Status	Operational Status		
	Hotlink		LAN5		
LAN	LAN5	enabled	up		
IPsec	WWAN1	enabled	up		
MobileIP	IPsec1	enabled	up		
oyatom					

enabled

up

Fig. 2.28: Ipsec and Mobile IP running – MG102i

MobileIP

2.3. Practical Test

After all required configuration steps are done, the reachability of devices in the M!DGE and MG102i subnets should be achieved. The encrypted data should pass through the LAN5 (WAN) interface on MG102i unit. If you do not have any attached devices, you can check the reachability from the CLI menu of either M!DGE or MG102i.



Fig. 2.29: Ping probe from MG102i to M!DGE

If you are using Windows to access the unit, run Putty for accessing the unit via SSH. Set the user to "root" and use the same password as for the admin account for the web interface. Running the command "ping" must be defined with "-I" parameter so the source address would fall into the VPN routed subnet.

To force the link of MG102i to switch to backup option, you can either unplug the Ethernet cable or switch off the host set in the Supervision menu. The result will be that the WWAN interface will be used.



		HOME INTERFACES ROUTING FIREWALL VPN SERVICES SYSTEM LOGOUT			
Status Summary	Summary				
WAN	Description	Administrative Status	Operational Status		
Ethernet	Hotlink		WWAN1		
LAN	LAN5	enabled	down		
OpenVPN	WWAN1	enabled	up		
IPsec MobileIP	OpenVPN2	enabled, client	up		
System	MobileIP	enabled	up		

Fig. 2.30: Using the backup interface

During the switchover, run the ping command continuously from the Server to the Client (pinging 192.168.10.1 IP address with a source address within 192.168.1.0/24 subnet). You will see that several packets are lost, but the time needed for the switchover is within seconds. You can compare it without using Mobile IP functionality.

You can also run your target application and see what happens during switching the links.



MG102[®]

Note

Using the web interface's Network debugging tool would not work, because the source IP address/interface cannot be set and the reply would not be forwarded to the VPN tunnel.

See the *manual*¹ for more details.

¹ http://www.racom.eu/eng/products/m/midge1/index.html

Appendix A. Revision History

Revision 1.0 First issue 2017-12-07

Revision 1.1 2018-02-28 Termination of M!DGE UMTS routers manufacturing