



Универсальность оборудования MikroTik для решения любых задач корпоративной сети.
Единая корпоративная сеть на базе MikroTik



MikroTik User Meeting, Moldova 2013

About Presenter

БОДЕНКОВ ДМИТРИЙ

Сертифицированный специалист МТСНА, МТСРЕ.

Системный администратор с 10 летним стажем и т.д. и

т.п.😊

Опыт работы с Mikrotik с 2008 года.

About Tetis INTERNATIONAL CO.



Национальный фармацевтический дистрибутор на рынке Республики Молдова с 1994 г. и в настоящее время является одной из самых крупных компаний, специализирующихся на импорте и оптовых продажах лекарств и изделий медицинского назначения.

Темы:

- Спектр устройств которые используются в сети.
- Разделение каналов от двух ISP для разных потребностей (WEB, VPN).
- Пропорциональное разделение скорости WEB пользователям.
- SMS оповещения о падении одного из ISP и переключение основного GW.
- VPN сеть по республике.
- Оборудование на стороне удаленной точки.
- Реализация backup канала по 3G, мониторинг, оповещения.
- MESH WIFI сеть складских помещений.

Спектр устройств которые используются в сети.

RB-150

RB-133

RB-411

RB-411AR

RB-433UAH

RB-750

RB-751U-2HnD

RB-1100AHx2

Общее количество устройств Routerboard в работе – 103шт.

Разделение каналов от двух ISP для разных потребностей (WEB, VPN).

Настраиваем основные маршруты

Route <0.0.0.0/0>

General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	192.168.1.1
Check Gateway:	ping
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

Route <0.0.0.0/0>

General	Attributes
Dst. Address:	0.0.0.0/0
Gateway:	192.168.1.93
Check Gateway:	
Type:	unicast
Distance:	1
Scope:	30
Target Scope:	10
Routing Mark:	
Pref. Source:	

ISP1 используется как основной GW и как VPN канал
ISP2 используется как WEB канал и как BACKUP канал для
VPN в случае падения ISP1

Разделение каналов от двух ISP для разных потребностей (WEB, VPN).

Для того чтобы пользователи выходили в Интернет через ISP2 маркируем и добавляем маршрут :

;;; WEB_traffic_Route

chain=prerouting action=mark-routing new-routing-mark=WEB_traffic

*passthrough=yes protocol=tcp src-address=192.168.0.0/24
in-interface=LAN dst-port=80,8080,443*

В итоге у нас 3 маршрута:

	Dst. Address	Gateway	Distance	Routing Mark
AS	► 0.0.0.0/0	► 192.168.1.1 reachable	1	
AS	► 0.0.0.0/0	► 192.168.93 reachable	1	WEB_traffic
S	► 0.0.0.0/0	► 192.168.93 reachable	1	

Пропорциональное разделение скорости WEB пользователям.

Маркируем соединения и пакеты на основании уже промаркированного маршрута:

; ; WEB_traffic_Conn

chain=prerouting action=mark-connection

*new-connection-mark=WEB_traffic_Conn passthrough=no
connection-state=new*

routing-mark=WEB_traffic

; ; Web_traffic_Packet

*chain=prerouting action=mark-packet new-packet-
mark=Web_traffic_Packet*

passthrough=no connection-mark=WEB_traffic_Conn

Пропорциональное разделение скорости WEB пользователям.

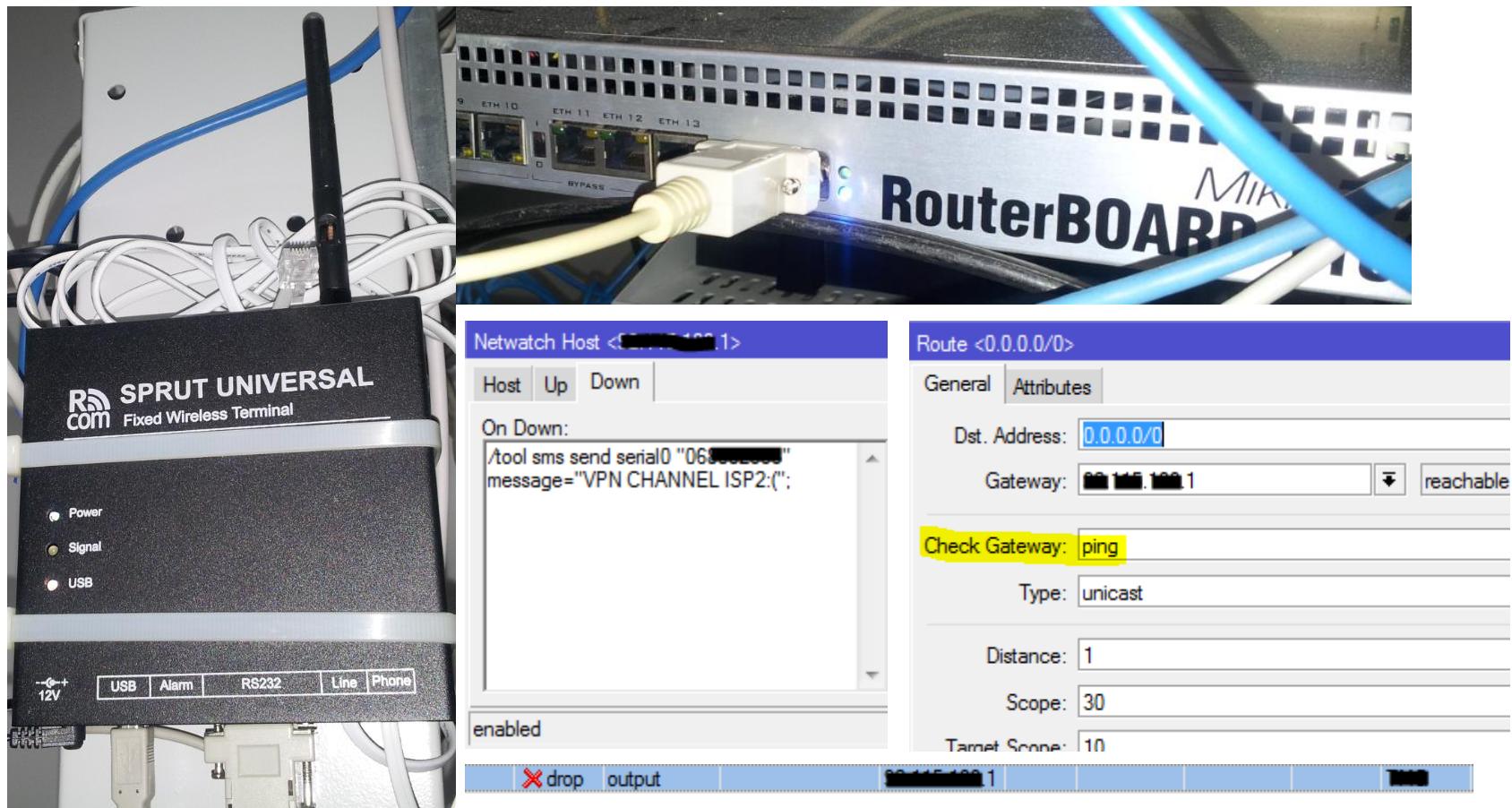
Создаем очередь:

```
name="WEB" target-addresses=192.168.0.0/24 interface=all  
parent=none packet-marks=Web_traffic_Packet  
direction=both priority=8  
queue=pcq-up/pcq-down limit-at=0/0 max-limit=20M/20M  
burst-limit=0/0  
burst-threshold=0/0 burst-time=0s/0s total-queue=default-  
small  
time=9h-18h,mon,tue,wed,thu,fri
```

В итоге 20 Мбит будут делиться на кол-во пользователей пропорционально

SMS оповещения о падении одного из ISP и переключение основного GW.

Для использования SMS оповещений используется подключенный по COM порту GSM шлюз и Netwatch:



VPN сеть по республике.

Time: 12:50:37 Date: Aug/06/2013 CPU: 19% Memory: 1305.4 MB Uptime: 174d 11:35:37 Hide Passwords

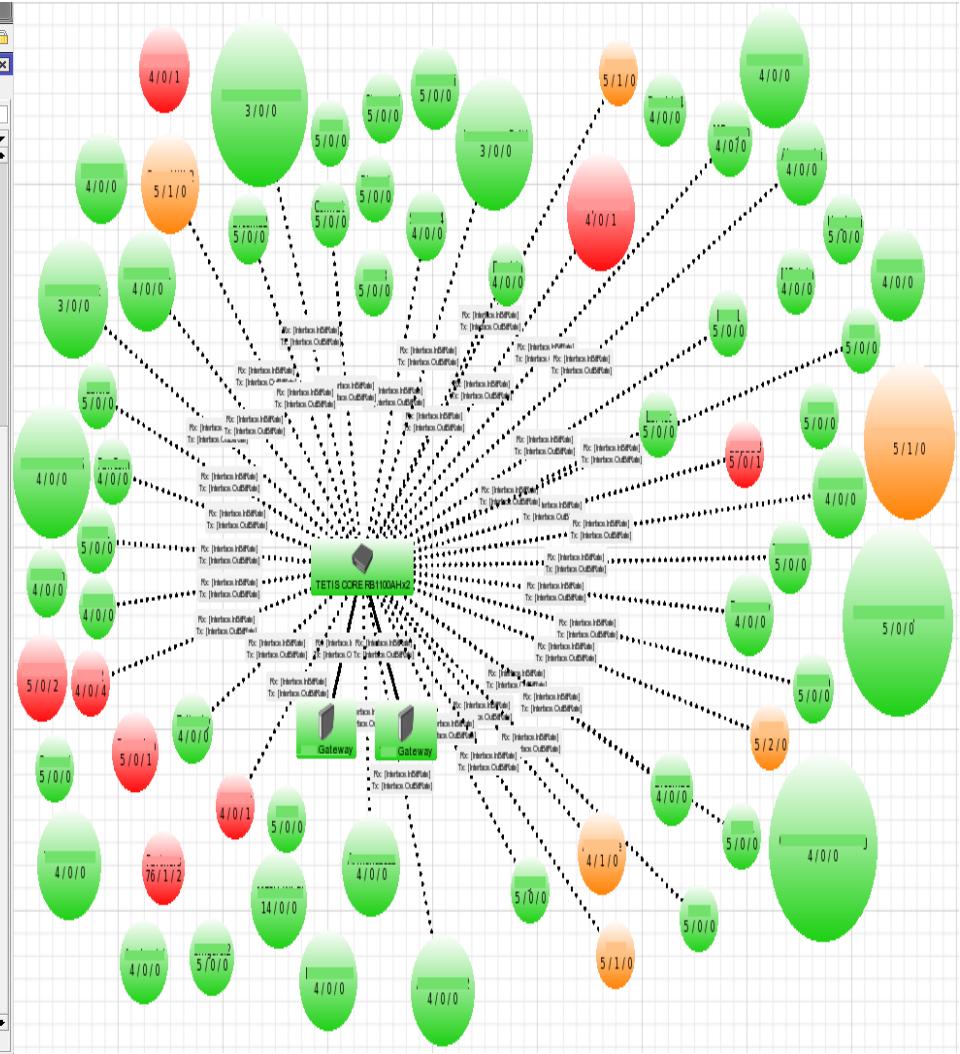
PPP

Interface PPPoE Servers Secrets Profiles Active Connections

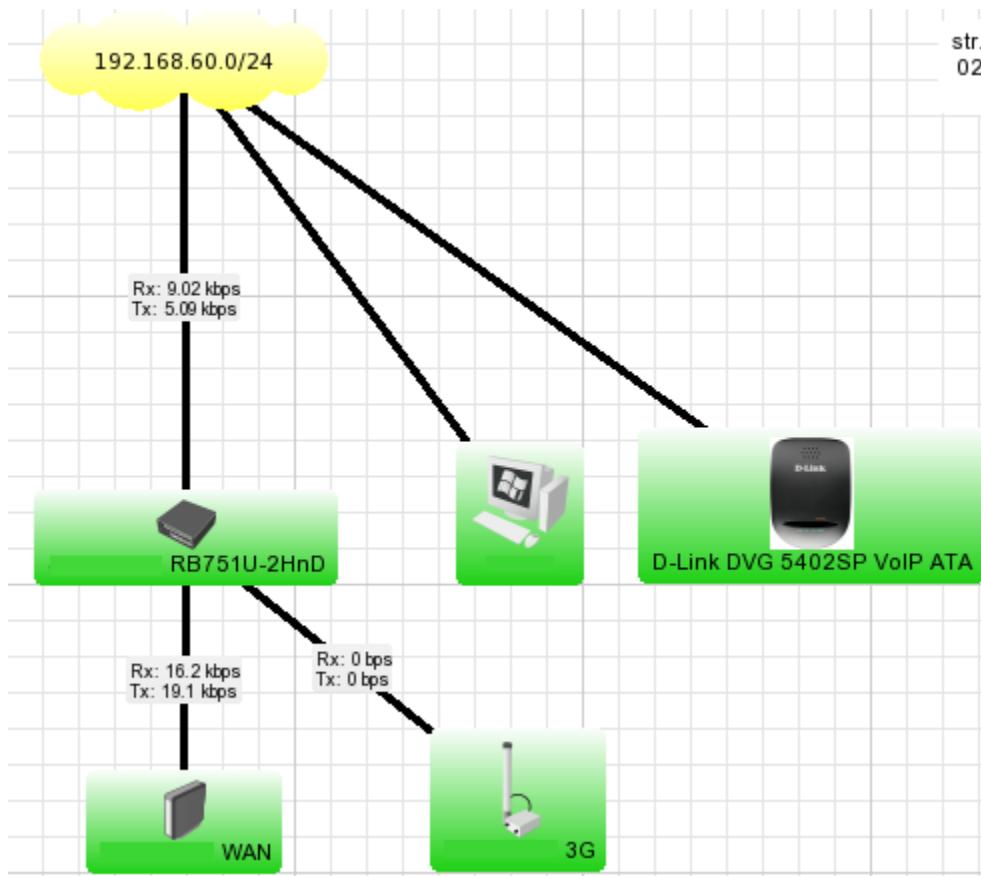
Find

Name	Service	Caller ID	Encoding	Address	Uptime
L	ppp		MPPE128 stateless	34d 20:36:46	
L	ppp		MPPE128 stateless	37d 18:16:51	
L	ppp		MPPE128 stateless	70d 21:30:50	
L	ppp		MPPE128 stateless	19d 20:39:49	
L	ppp		MPPE128 stateless	73d 12:16:23	
L	ppp		MPPE128 stateless	39d 11:17:08	
L	ppp		MPPE128 stateless	19d 10:47:24	
L	ppp		MPPE128 stateless	12d 01:19:34	
L	ppp		MPPE128 stateless	15d 00:49:58	
L	ppp		MPPE128 stateless	44d 11:57:13	
L	ppp		MPPE128 stateless	9d 11:49:11	
L	ppp		MPPE128 stateless	59d 08:28:45	
L	ppp		MPPE128 stateless	9d 21:04:57	
L	ppp		MPPE128 stateless	19d 19:55:21	
L	ppp		MPPE128 stateless	6d 04:45:14	
L	ppp		MPPE128 stateless	22:55:40	
L	ppp		MPPE128 stateless	22d 20:48:07	
L	ppp		MPPE128 stateless	17d 22:19:32	
L	ppp		MPPE128 stateless	25d 18:32:25	
L	ppp		MPPE128 stateless	3d 08:30:03	
L	ppp		MPPE128 stateless	17d 21:42:40	
L	ppp		MPPE128 stateless	18d 22:10:37	
L	ppp		MPPE128 stateless	22d 18:54:58	
L	ppp		MPPE128 stateless	59d 12:09:52	
L	ppp		MPPE128 stateless	6d 00:04:34	
L	ppp		MPPE128 stateless	75d 10:26:53	
L	ppp		MPPE128 stateless	17d 21:29:55	
L	ppp		MPPE128 stateless	4d 15:22:34	
L	ppp		MPPE128 stateless	7d 20:47:40	
L	ppp		MPPE128 stateless	41d 02:45:57	
L	ppp		MPPE128 stateless	30d 23:38:52	
L	ppp		MPPE128 stateless	7d 21:32:34	
L	ppp		MPPE128 stateless	3d 21:57:12	
L	ppp		MPPE128 stateless	00:37:33	
L	ppp		MPPE128 stateless	02:44:59	
L	ppp		MPPE128 stateless	1d 10:43:12	
L	ppp		MPPE128 stateless	6d 06:07:11	
L	ppp		MPPE128 stateless	16d 21:00:07	
L	ppp		MPPE128 stateless	2d 00:32:07	
L	ppp		MPPE128 stateless	04:44:37	
L	ppp		MPPE128 stateless	04:54:21	
L	ppp		MPPE128 stateless	19d 22:10:56	
L	ppp		MPPE128 stateless	4d 07:36:23	
L	ppp		MPPE128 stateless	04:43:57	
L	ppp		MPPE128 stateless	41d 18:15:40	
L	ppp		MPPE128 stateless	47d 18:53:58	
L	ppp		MPPE128 stateless	04:03:46	
L	ppp		MPPE128 stateless	04:53:11	
L	ppp		MPPE128 stateless	18d 04:03:53	
L	ppp		MPPE128 stateless	02:31:46	
L	ppp		MPPE128 stateless	05:20:45	
L	ppp		MPPE128 stateless	53d 19:00:20	
L	ppp		MPPE128 stateless	4d 07:34:56	
L	ppp		MPPE128 stateless	39d 03:21:34	
L	ppp		MPPE128 stateless	53d 07:33:32	
L	ppp		MPPE128 stateless	35d 23:24:51	
L	ovpoe		AES-128-CBC/SHA1	4d 07:34:59	
L	ppp		MPPE128 stateless	3d 02:37:37	

84 items (1 selected)



VPN сеть по республике. Оборудование на стороне удаленной точки.



RB-751U-2HnD

Реализация backup канала по 3G, мониторинг, оповещения.

Активным шлюзом по умолчанию является основной ISP с опцией «Check Gateway=Ping» и метрикой=1

Второй шлюз по умолчанию через 3G не активен и имеет метрику=2.

При падении основного шлюза backup шлюз станет активным автоматически.

Реализация backup канала по 3G, мониторинг, оповещения.

Таблица маршрутов:

The screenshot displays a network management interface with three main windows:

- Route List Window:** Shows a table of routes. The table has columns: Dst. Address, Gateway, Distance, and Routing Mark. The routes listed are:
 - AS ▶ 0.0.0.0/0 [REDACTED].1 reachable WAN
 - S ▶ 0.0.0.0/0 Unite3G reachable
 - AS ▶ 0.0.0.0/0 Unite3G reachable
 - AS ▶ [REDACTED] reachable [REDACTED]
 - AS ▶ 212.0.212.212 Unite3G reachable
- Route <0.0.0.0/0> Configuration Dialog (Left):** A modal dialog for a specific route entry. It has tabs for General and Attributes. The General tab shows:
 - Dst. Address: 0.0.0.0/0
 - Gateway: [REDACTED].1 reachable WAN
 - Check Gateway: ping
 - Type: unicast
 - Distance: 1
 - Scope: 30
 - Target Scope: 10
 - Routing Mark:
 - Pref. Source:
- Route <0.0.0.0/0> Configuration Dialog (Right):** Another modal dialog for a route entry. It has tabs for General and Attributes. The General tab shows:
 - Dst. Address: 0.0.0.0/0
 - Gateway: Unite3G reachable
 - Check Gateway:
 - Type: unicast
 - Distance: 2
 - Scope: 30
 - Target Scope: 10
 - Routing Mark:
 - Pref. Source:

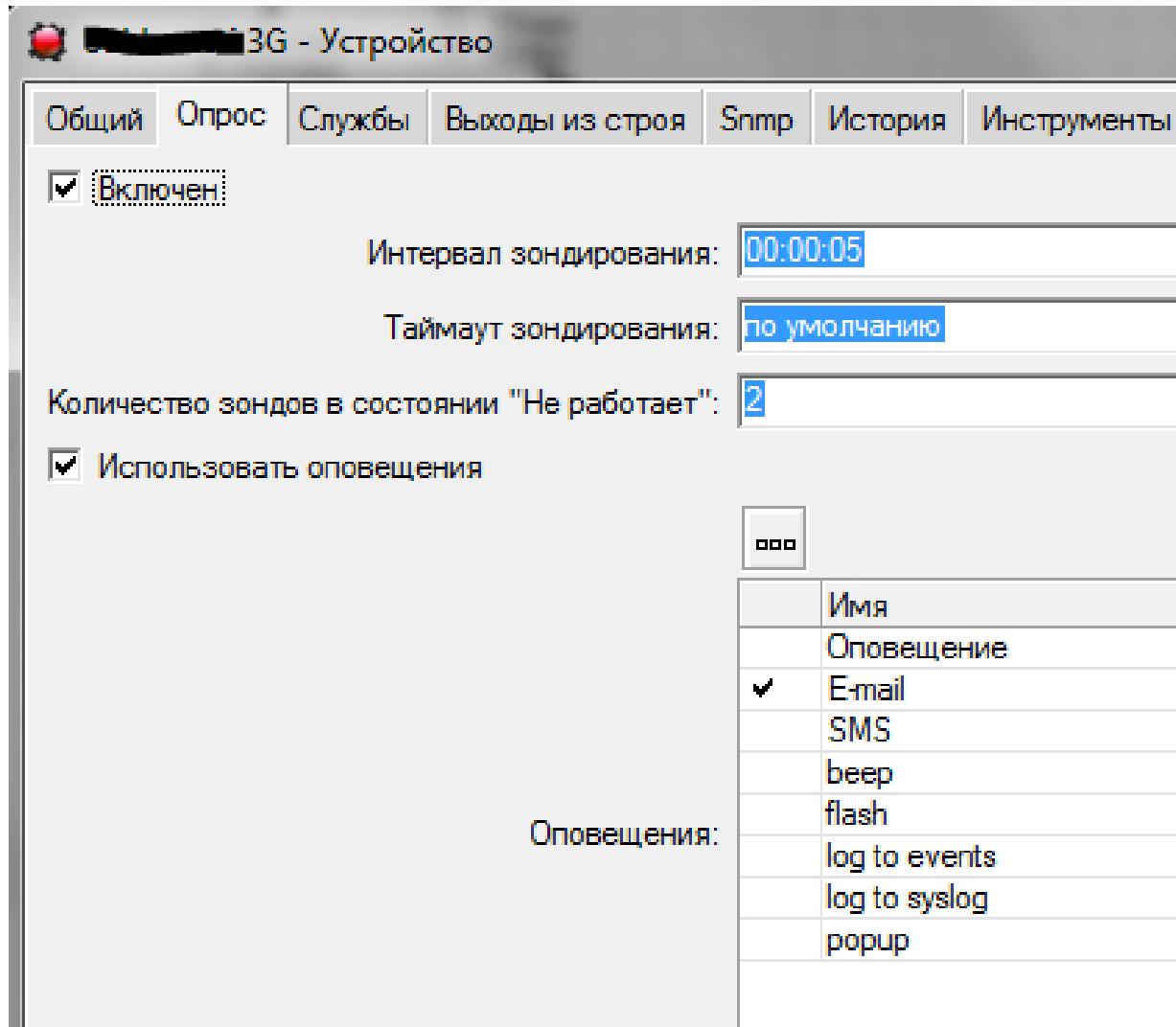
Реализация backup канала по 3G, мониторинг, оповещения.

Для того чтобы мониторить живучесть backup канала маркируем маршрут исходящий от роутера с протоколом ICMP через 3G интерфейс и с IP адреса 3G модема:

```
chain=output action=mark-routing new-routing-mark=3G  
passthrough=no protocol=icmp src-address=109.185.178.125
```

Сам мониторинг осуществляется сервером Dude который установлен на основной роутер в Центральном Офисе и рассыпает E-mail сообщения администраторам о падении устройств.

Реализация backup канала по 3G, мониторинг, оповещения.



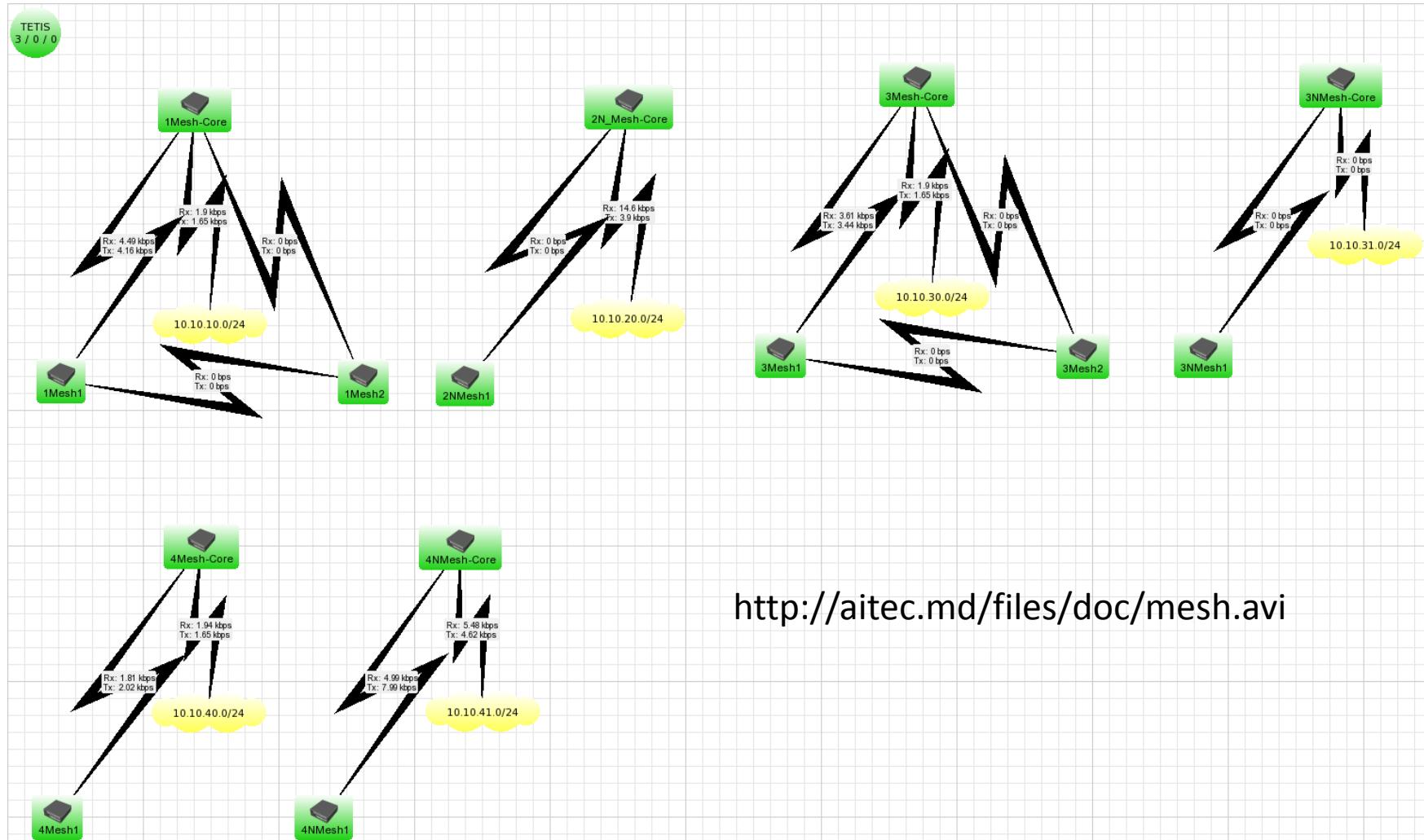
Реализация backup канала по 3G, мониторинг, оповещения.

В случае падения ISP1 в Центральном Офисе и переходе на ISP2 удаленные точки также переподключаются к VPN но уже на адрес второго ISP. Реализовано это с помощью того же Netwatch-а который мониторит IP адрес ISP1:

	Name	Type	L2 MTU	Tx	Rx
X	↔ Backup	PPTP Client		0 bps	0 bps
R	↔ Tetis	PPTP Client		5.4 kbps	4.2 kbps
R	↔ Unite3G	PPP Client	1500	880 bps	752 bps

down-script=
/in pptp-cl dis Tetis;
:delay 5;
/in pptp-cl en Backup;
up-script=
/in pptp-cl dis Backup;
:delay 5;
/in pptp-cl en Tetis;

MESH WIFI сеть складских помещений.



MESH WIFI сеть складских помещений.



MESH WIFI сеть складских помещений.



Powered by



Спасибо за внимание!
Any questions?

