



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 MTCNA, MTCRE.

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 дистрибьютор 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-433UАН

RB-750

RB-751U-2HnD

RB-1100АНx2

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 reachable

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: 172.16.1.93 reachable

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 чтоб 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 192.168.1.1	1	
AS	▶ 0.0.0.0/0	192.168.1.93 reachable 192.168.1.93	1	WEB_traffic
S	▶ 0.0.0.0/0	192.168.1.93 reachable 192.168.1.93	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.

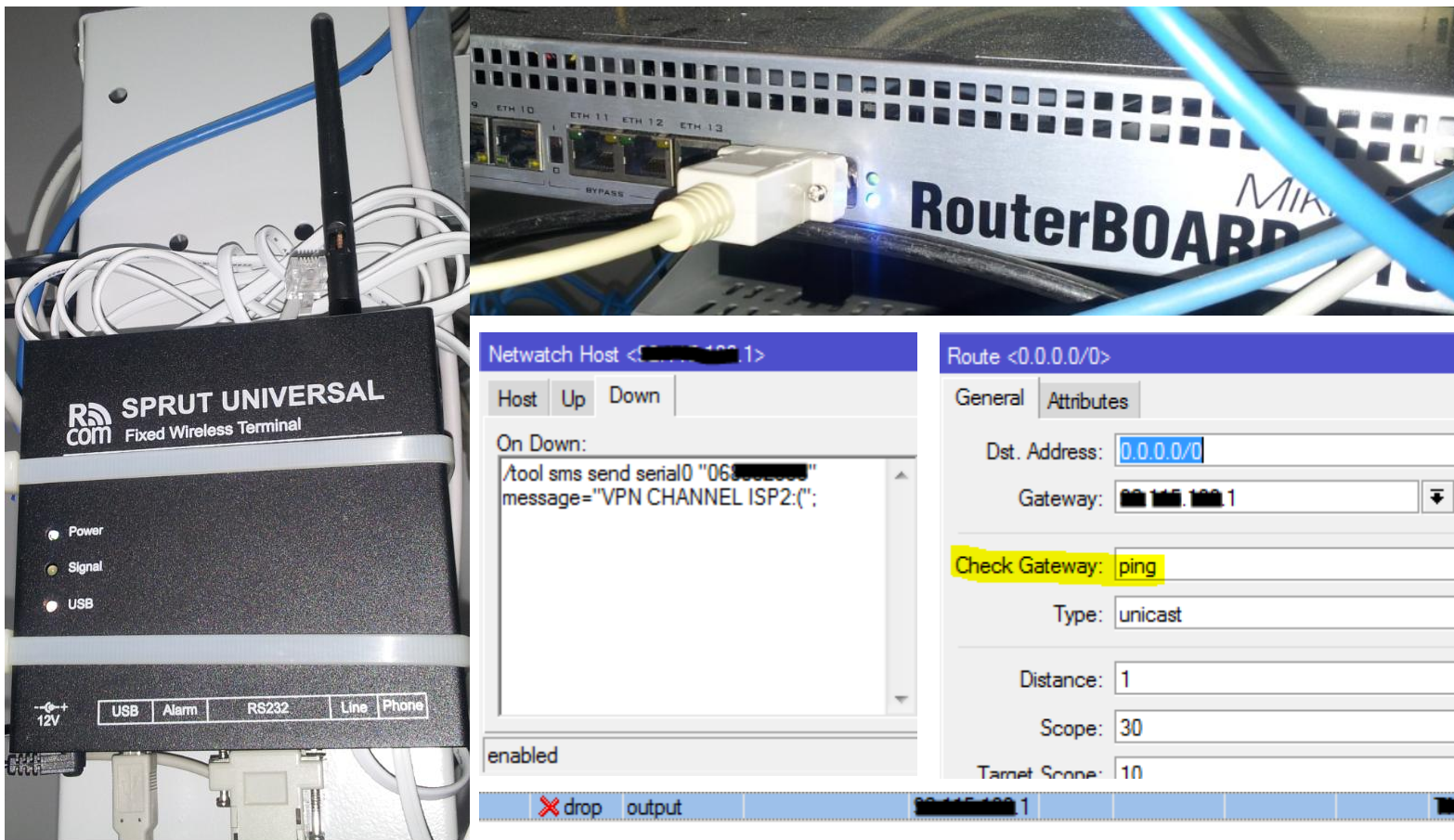
Создаем очередь:

```
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  

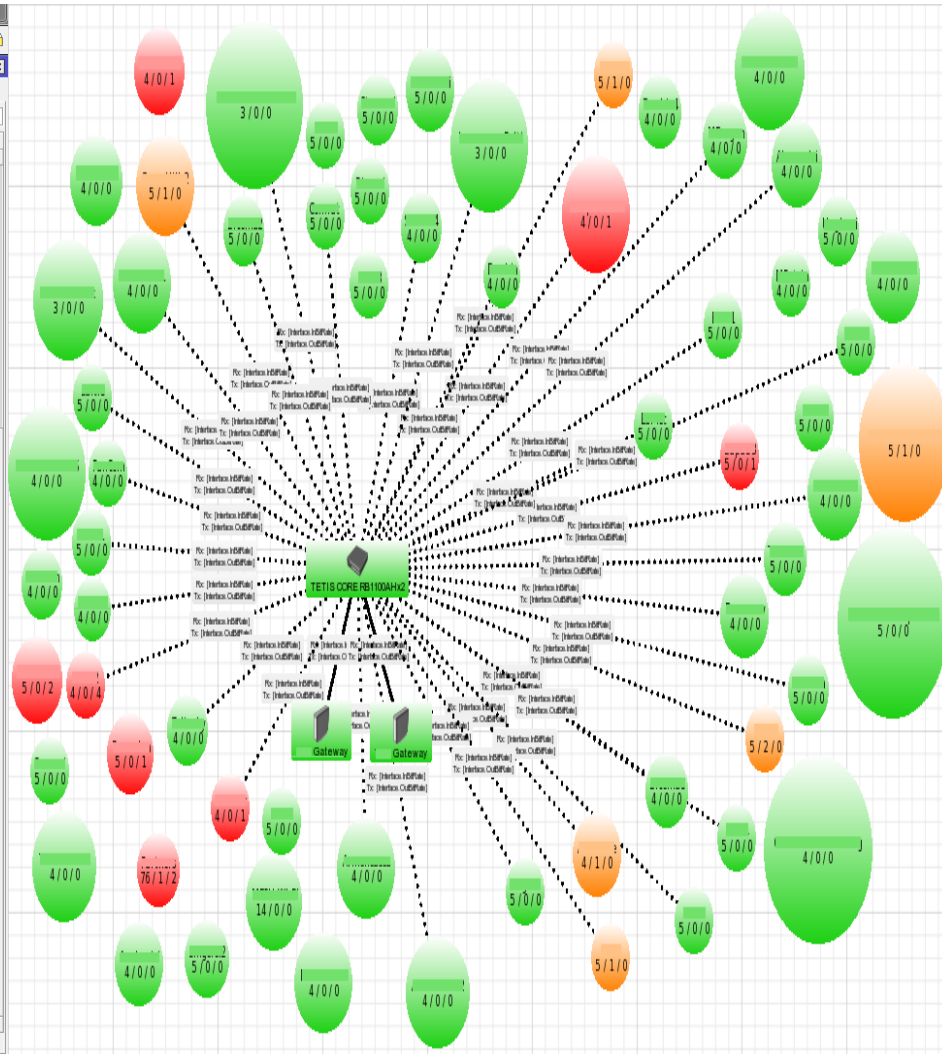
PPP

Interface PPPoE Servers Secrets Profiles Active Connections

  Find

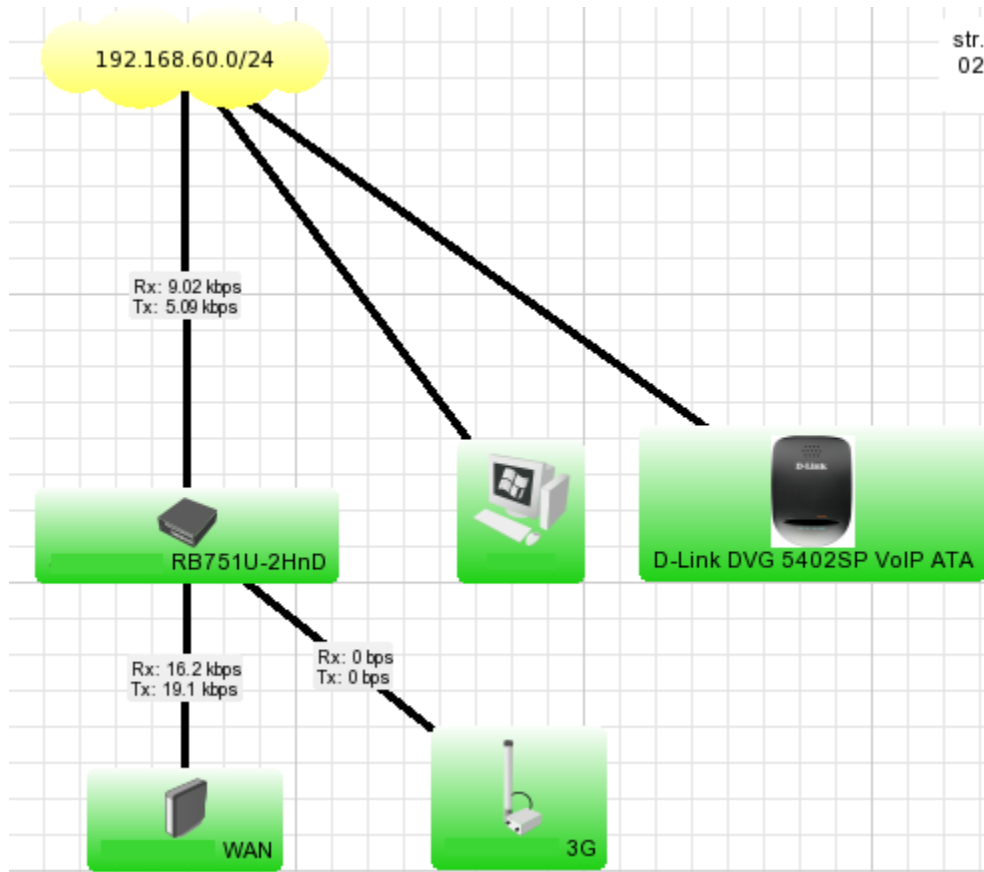
Name	Service	Caller ID	Encoding	Address	Uptime
L	ppptp		MPPE128 stateless	34d 20:36:46	
L	ppptp		MPPE128 stateless	37d 18:16:51	
L	ppptp		MPPE128 stateless	70d 21:30:50	
L	ppptp		MPPE128 stateless	19d 20:39:49	
L	ppptp		MPPE128 stateless	73d 12:16:23	
L	ppptp		MPPE128 stateless	39d 11:17:08	
L	ppptp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

94 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 configuration interface. At the top, a 'Route List' window shows a table of routes. Below it, two configuration windows for static routes are shown side-by-side.

**Route List Table:**

	Dst. Address	/	Gateway	Distance	Routing Mark
AS	0.0.0.0/0		[redacted] 1 reachable WAN	1	
S	0.0.0.0/0		Unite3G reachable	2	
AS	0.0.0.0/0		Unite3G reachable	1	3G
AS	[redacted]		[redacted] reachable [redacted]	1	
AS	212.0.212.212		Unite3G reachable	1	

**Left Configuration Window (Route <0.0.0.0/0>):**

- General tab selected.
- Dst. Address: 0.0.0.0/0
- Gateway: [redacted] 9.1 reachable WAN
- Check Gateway: ping
- Type: unicast
- Distance: 1
- Scope: 30
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled, active, static

**Right Configuration Window (Route <0.0.0.0/0>):**

- General tab selected.
- Dst. Address: 0.0.0.0/0
- Gateway: Unite3G reachable
- Check Gateway: (empty)
- Type: unicast
- Distance: 2
- Scope: 30
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)
- Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove
- Status: enabled, active, static


# Реализация backup канала по 3G, мониторинг, оповещения.

Для того чтоб 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 рассылает E-mail сообщения администраторам о падении устройств.

# Реализация backup канала по 3G, мониторинг, оповещения.

 **3G - Устройство**

Общий | **Опрос** | Службы | Выходы из строя | Snmp | История | Инструменты

☒ Включен

Интервал зондирования: 00:00:05

Таймаут зондирования: по умолчанию

Количество зондов в состоянии "Не работает": 2

☒ Использовать оповещения

Оповещения:

...

	Имя
	Оповещение
✓	E-mail
	SMS
	beep
	flash
	log to events
	log to syslog
	popup



# Реализация backup канала по 3G, мониторинг, оповещения.

В случае падения ISP1 в Центральном Офисе и переходе на ISP2 удаленные точки также переподключатся 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=*

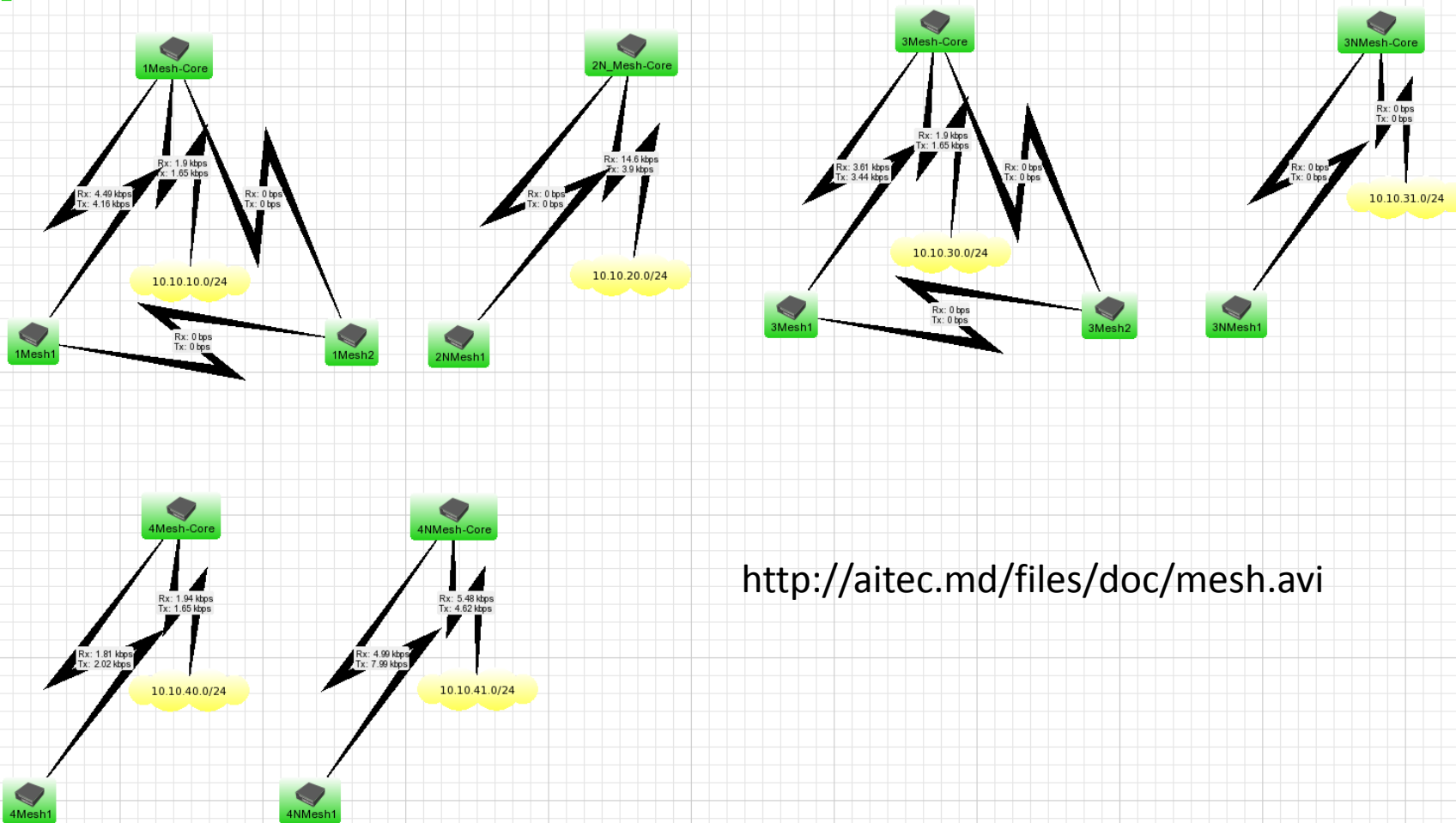
*/in pptp-cl dis Backup;*

*:delay 5;*

*/in pptp-cl en Tetis;*

# MESH WIFI сеть складских помещений.

TETIS  
3 / 0 / 0



<http://aitec.md/files/doc/mesh.avi>

# MESH WIFI сеть складских помещений.



# MESH WIFI сеть складских помещений.





Спасибо за внимание!  
Any questions?

