

Универсальный конфиг для малого и среднего офиса

MikroTik



Приветствую, коллеги!

Антон Мороз

Генеральный директор ООО «Реал»

www.realsd.ru

14 лет в ИТ области, 6 лет на рынке ИТ аутсорсинга.

Сертификаты Mikrotik: MTCNA, MTCWE, MTCTCE, MTCRE, MTCIPv6E



О чем поговорим?



Цели, которые мы преследуем

1. Получить универсальный конфиг, который можно легко и быстро развернуть в любой среднестатистической компании
2. Не забывать настроить мелочи, которые на первый взгляд не видно, но нужны
3. Иметь возможность быстрого развертывания при массовых поставках оборудования или глобальных сбоях
4. Иметь структурированную и понятную базу для ежедневной и рутинной настройки, гибко изменяемую под индивидуальные требования клиента
5. Минимизировать возможные ошибки и опечатки при конфигурировании



О чем поговорим?



Из чего же состоит универсальный конфиг?

1. Заводская конфигурация от компании Mikrotik
2. Небольшой тюнинг системных параметров
3. Расширенная настройка Firewall и безопасности сети
4. Подготовка инфраструктуры для себя
5. Универсальная минимальная настройка QoS
6. Шаблоны для быстрого запуска сервисов VPN, CAPsMAN, TFTP

1. Default config by Mikrotik

*Mikro***Tik**



1. Default config by Mikrotik



Почему бы не остановиться на заводском конфиге?

1. Его достаточно для первоначального запуска
2. У него не плохая безопасность
3. С него можно начинать практическое любое внедрение
4. Подходит для новичков и знакомства с оборудованием

Но...

Нам нужно большее!

2. Тюнинг «Default config by Mikrotik»

*Mikro***Tik**



2. Тюнинг «Default config by Mikrotik»



1. TCP established timeout длительностью 24 часа

Не всегда соединения корректно закрываются. Короткие сессии долго висят занимая оперативную память.

`/ip firewall connection tracking print`

max-entries: Максимальное количество записей в Connection tracking. Может быть увеличено при необходимости если есть свободная оперативная память

total-entries: Текущее количество соединений в Connection tracking

Решение

Установить менее длительное время жизни соединения

`/ip firewall connection tracking set tcp-established-timeout=1h`



2. Тюнинг «Default config by Mikrotik»

moroz@10.10.1.1 (Cloud_GW) - WinBox v6.43.13 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 10.10.1.1

RouterOS WinBox

Quick Set
Interfaces
Bridge
PPP
Mesh
IP
IPv6
Routing
System
Queues
Files
Log
RADIUS
Tools
New Terminal
Make Spout.rtf
Manual
New WinBox
Exit

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Tracking

Connection Tracking

Enabled: auto

TCP Syn Sent Timeout: 00:00:05

TCP Syn Received Timeout: 00:00:05

TCP Established Timeout: 01:00:00

TCP Fin Wait Timeout: 00:00:10

TCP Close Wait Timeout: 00:00:10

TCP Last Ack Timeout: 00:00:10

TCP Time Wait: 00:00:10

TCP Close: 00:00:10

TCP Max Retransmit Timeout: 00:05:00

TCP Unacked Timeout: 00:05:00

UDP Timeout: 00:00:10

UDP Stream Timeout: 00:03:00

ICMP Timeout: 00:00:10

Generic Timeout: 00:10:00

	Src. Address	Dest. Address
SCF	5.9.24.135	82.198.171.162
SC	5.9.24.135	82.198.171.162
SC	5.9.24.135	178.218.112.55
SCF	5.9.24.135	178.218.112.55
SC	5.9.24.135	178.57.84.86
SCF	5.9.24.135	79.135.239.246
SCF	5.9.24.135	178.57.84.86
SCF	5.9.24.135	91.77.168.56
SCF	5.9.24.135	213.85.9.229
SCF	5.9.24.135	217.76.37.200
SCF	5.9.24.135	178.209.123.114
SCF	5.9.24.135	94.159.34.86
SC	5.9.24.135	213.85.9.229
SC	5.9.24.135	91.77.168.56
SAC	5.9.24.135.500	217.76.37.200:500
SAC	5.9.24.135.500	91.77.168.56:500
SAC	5.9.24.135.500	94.159.34.86:500
SAC	5.9.24.135.500	178.57.84.86:500
SAC	5.9.24.135.500	178.209.123.114:500
SAC	5.9.24.135.500	213.85.9.229:500
SAC	5.9.24.135.500	82.198.171.162:500
SC	5.9.24.135.40648	213.133.98.98:53
SC	5.9.24.135.51498	213.133.98.98:53
SACFd	5.9.24.188.42952	5.9.24.135.10051
SACFd	5.9.24.188.42962	5.9.24.135.10051

215 items Max Entries: 934904



2. Тюнинг «Default config by Mikrotik»

2. DHCP Lease Time всего 10 минут

В редких случаях бывают проблемы при обновлении арендованного IP у некоторых специфичных устройств. Часто встречается у продукции Apple.

Решение

Установить более длительное время аренды

```
/ip dhcp-server set [find name="defconf"] lease-time=3d
```

Name	Interface	Relay	Lease Time	Address Pool	Add AR...
Default	bridge novlan		3d 00:00:00	default-dhcp	no

DHCP Server <Default>

Name: Default

Interface: bridge novlan

Relay: [dropdown]

Lease Time: 3d 00:00:00

Bootp Lease Time: forever

Address Pool: default-dhcp

DHCP Option Set: [dropdown]

Buttons: OK, Cancel, Apply, Disable, Copy, Remove



2. Тюнинг «Default config by Mikrotik»



3. MAC на Bridge копируется с первого участника этого Bridge.
Но, иногда, при использовании VLAN MAC-таблица должна быть уникальна.

Решение

Устанавливать Admin MAC отличный от других MAC адресов на устройстве.

Создание нового бриджа:

```
/interface bridge {  
    add name=bridge1  
    set bridge1 auto-mac=no admin-mac=[get bridge1 mac-address]  
}
```



2. Тюнинг «Default config by MikroTik»

New Interface

General STP VLAN Status Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

Admin. MAC Address:

Ageing Time:

IGMP Snooping

DHCP Snooping

Fast Forward

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave

Interface <bridge1>

General STP VLAN Status Traffic

Name:

Type:

MTU:

Actual MTU:

L2 MTU:

MAC Address:

ARP:

ARP Timeout:

Admin. MAC Address:

Ageing Time:

IGMP Snooping

DHCP Snooping

Fast Forward

OK Cancel Apply Disable Comment Copy Remove Torch

enabled running slave



2. Тюнинг «Default config by Mikrotik»

4. Отключаем не используемые службы

Решение

```
/ip service {  
set telnet disabled=yes  
set ftp disabled=yes  
set www disabled=yes  
set api disabled=yes  
set api-ssl disabled=yes  
}
```



2. Тюнинг «Default config by Mikrotik»

5. Отключаем не используемые helper`ы (ALG или service port)

Решение

```
/ip firewall service-port  
set ftp disabled=yes  
set tftp disabled=yes  
set irc disabled=yes  
set h323 disabled=yes  
set sip disabled=yes  
set pptp disabled=yes  
set dccp disabled=yes  
set sctp disabled=yes
```



2. Тюнинг «Default config by Mikrotik»



6. Дефолтный пользователь admin без пароля.
Оставить нельзя исправить.

Решение

Переименовываем пользователя admin, меняем пароль.

```
/user add name=newadmin password=adminpass group=full
```

```
/user remove admin
```



2. Тюнинг «Default config by Mikrotik»



7. По умолчанию правила NAT не работают из локальной сети.

Wiki Mikrotik предлагает решение Hairpin NAT (https://wiki.mikrotik.com/wiki/Hairpin_NAT).

Но необходимо создавать Source NAT правило под каждое правило «проброса портов». Это не совсем удобно громоздко.

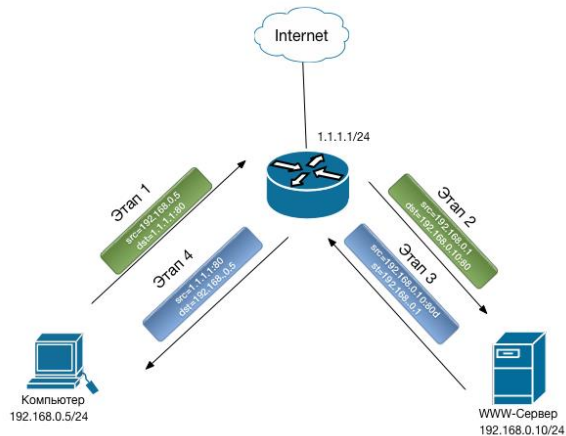
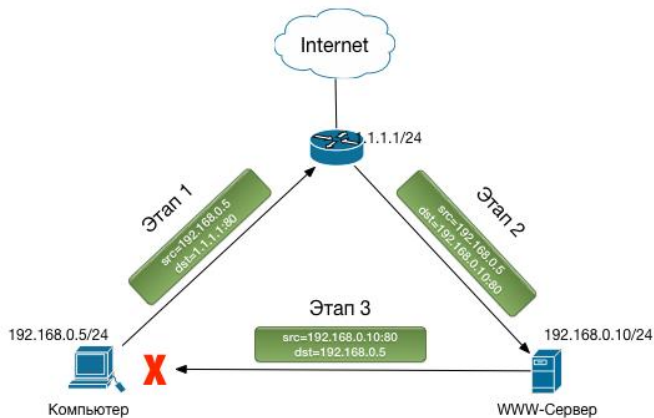
Решение

Сделать «финт ушами» - одно глобальное правило.

```
/ip firewall nat add chain=srcnat action=masquerade out-interface-list=LAN src-address-list=LocalNet comment="NAT loopback masquerade for LAN"
```




2. Тюнинг «Default config by Mikrotik»





2. Тюнинг «Default config by Mikrotik»



Как ЭТИМ пользоваться?

В Address List LocalNet добавляем наши локальные подсети

```
/ip firewall address-list add address=192.168.0.0/24 list=LocalNet
```

В Address List WAN_ISP1_IP1 добавляем наш внешний IP адрес

```
/ip firewall address-list add address=1.1.1.1 list= WAN_ISP1_IP1
```

Правило «проброса порта» выглядит так

```
/add action=dst-nat chain=dstnat dst-address-list= WAN_ISP1_IP1 dst-port=80  
protocol=tcp to-addresses=192.168.0.10 comment="Example of port forwarding"
```



2. Тюнинг «Default config by Mikrotik»



7. NTP клиент резолвит доменные имена серверов только один раз.

Решение

Использовать скрипт с wiki.mikrotik.ru, немного упростив его

```
/system script add name=NTPServerUpdate policy=read,write,test source="
:local ntpcura [/system ntp client get primary-ntp];
:local ntpcurb [/system ntp client get secondary-ntp];
:local ntpipa [:resolve 0.ru.pool.ntp.org];
:local ntpipb [:resolve 1.ru.pool.ntp.org];
:if ($ntpipa != $ntpcura) do={"/system ntp client set primary-ntp="$ntpipa";}
:if ($ntpipb != $ntpcurb) do={"/system ntp client set secondary-ntp="$ntpipb};"
```



2. Тюнинг «Default config by Mikrotik»

И создаем расписание для запуска резервного копирования

```
/system scheduler add \  
comment="Check and set NTP servers" \  
disabled=no \  
interval=12h \  
name=CheckNTPServers \  
on-event="/system script run NTPServerUpdate" \  
policy=read,write,test \  
start-date=jan/01/1970 \  
start-time=07:00:00
```

3. Firewall и безопасность сети

MikroTik



3. Firewall и безопасность сети



1. Наличие ответа на PING с WAN портов в разы повышает шансы попасть под прицел злоумышленников

Решение

Запретить ICMP ответы с WAN портов в цепочке INPUT и отключить MAC Ping

```
/ip firewall filter add chain=input action=drop protocol=icmp icmp-options=8:0 in-interface-list=WAN src-address-list="!AllowIPRemoteManagement" comment="Drop IN echo request"
```

```
/tool mac-server ping set enabled=no
```



3. Firewall и безопасность сети



2. Находясь в открытой сети мы постоянно подвергаемся попыткам подключиться к стандартным портам распространенных служб и протоколов

Решение

Отловить и заблокировать тех, кто пытается это сделать

```
/ip firewall filter add chain=input action=add-src-to-address-list in-interface-list=WAN src-address-list="!NotTrapsIP" protocol=tcp dst-port=5060,5061,4569,3389,8291,22,23,389,445,53 connection-nat-state=!dstnat address-list=TrapAddress address-list-timeout=3d comment="Trap for TCP traffic"
```



3. Firewall и безопасность сети



UDP трафик не исключение

Решение

Такое же правило для UDP трафика

```
/ip firewall filter add chain=input action=add-src-to-address-list in-interface-list=WAN src-address-list="!NotTrapsIP" protocol=tcp dst-port=5060,4569,389,53,161 connection-nat-state=!dstnat address-list=TrapAddress address-list-timeout=3d comment="Trap for UDP traffic"
```




3. Firewall и безопасность сети



Как ЭТИМ пользоваться?

Блокируем все собранные IP адреса в Firewall Raw

```
/ip firewall raw add action=drop chain=prerouting src-address-list=TrapAddress  
comment="Drop Address from Trap"
```

Не забудьте добавить в Address List NotTrapsIP адреса из «Белого списка»

```
/ip firewall address-list add address=192.168.0.0/24 list=NotTrapsIP
```

При создании правила NAT, которое совпадает с Traps правилами, такое соединение не попадать в «Черный список» и блокироваться не будет.



3. Firewall и безопасность сети



3. Достаточно часто мы подвергаемся массовому сканированию портов со стороны злоумышленников

Решение

Детектировать сканирование и блокировать источники

```
/ip firewall filter add chain=input action=add-src-to-address-list in-interface-list=WAN src-address-list="!NotTrapsIP" protocol=tcp psd=10,10s,3,1 address-list=TrapAddress address-list-timeout=7d comment="Trap for port scanning"
```



3. Firewall и безопасность сети

--▲-- PSD

Weight Threshold:

Delay Threshold:

Low Port Weight:

High Port Weight:



3. Firewall и безопасность сети



1	Real_defconf: Trap for port scanning	6 (tcp)		1724.8	40 861
2	Real_defconf: DoS attack detected from single IP			0 B	0
3	Real_defconf: DoS attack detected from 24 subnet			0 B	0
4	Trap for UDP SIP port	17 (u...)	5060	1175.1	2 725
5	Trap for RDP port	6 (tcp)	3389	84.3	1 944
6	Trap for WinBox port	6 (tcp)	8291	8.1	174
7	Trap for SSH port	6 (tcp)	22	785.4	14 470
8	Trap for Telnet port	6 (tcp)	23	981.1	24 437
9	Trap for SMB port	6 (tcp)	445	776.1	18 402
10	Trap for LDAP port	6 (tcp)	389	10.4	229
11	Trap for DNS port	17 (u...)	53	60.3	1 036 317
12	Trap for SNMP port	17 (u...)	161	20.1	273
13	Trap for TCP SIP port	6 (tcp)	5060,5061	13.8	316

Resources [Close] [Maximize]

Uptime: 15d 01:27:05 OK

Free Memory: 958.6 MB PCI

Total Memory: 1024.0 MB USB

CPU: ARMv7 CPU

CPU Count: 4 IRQ

CPU Frequency: 1400 MHz

CPU Load: 1 %

Free HDD Space: 85.3 MB

Total HDD Size: 128.3 MB

Architecture Name: arm

Board Name: RB1100AHx4

Version: 6.43.12 (stable)

Build Time: Feb/08/2019 11:46:26



3. Firewall и безопасность сети



::: Drop Address from Trap					
0	✘ drop	prerouting		595.6 GiB	429 405 895
::: Drop Address from ScanPort Trap					
1	✘ drop	prerouting		1480.8 KiB	37 375
::: Drop Address from DoS Attack					
2	✘ drop	prerouting		0 B	0

Resources [Close] [X]

Uptime: OK

Free Memory: PCI

Total Memory: USB



3. Firewall и безопасность сети



4. Угроза иногда исходит не только из вне и не только для нас.

Наша сеть тоже может быть источником опасности для внешнего мира.

Решение

Отлавливать и блокировать вирусную активность из внутренней сети

```
/ip firewall filter add action=drop chain=forward protocol=tcp dst-port=25,587,465  
connection-state=new out-interface-list=WAN dst-address-  
list=!SMTP_External_Servers src-address-list=!SMTP_Internal_Servers/Clients  
log=yes log-prefix="SMTP Spam" comment="Drop out SMTP not allow hosts"
```

```
/ip firewall filter add action=drop chain=forward protocol=tcp dst-port=445  
connection-state=new out-interface-list=WAN log=yes log-prefix="SMB Scan"  
comment="Drop out SMB not allow hosts"
```



3. Firewall и безопасность сети



Как ЭТИМ пользоваться?

В Address List SMTP_External_Servers мы добавляем адреса внешних SMTP серверов, через которые отправляем письма.

```
/ip firewall address-list add address=smtp.gmail.com list=SMTP_External_Servers
```

В Address List SMTP_Internal_Servers/Clients мы добавляем адреса наших внутренних SMTP сервер или привилегированных клиентов, которым разрешено отправлять письма в мир.

```
/ip firewall address-list add address=192.168.0.4 list=SMTP_Internal_Servers/Clients
```



3. Firewall и безопасность сети



5. Защита опубликованных сервисов от DoS Attack.

Решение

Ловить и блокировать IP адреса, генерирующие большое количество соединений

```
/ip firewall filter add action=add-src-to-address-list address-list=DoS_Attack_Address  
address-list-timeout=1d chain=forward comment="DoS attack detected from single  
IP" connection-limit=20,32 connection-nat-state=dstnat in-interface-list=WAN
```

```
/ip firewall filter add action=add-src-to-address-list address-list=DoS_Attack_Address  
address-list-timeout=1d chain=forward comment="DoS attack detected from 24  
subnet" connection-limit=100,24 connection-nat-state=dstnat in-interface-list=WAN
```




3. Firewall и безопасность сети



6. Не красиво загрязнять чужие сети мусорным трафиком, а так же полезно отлавливать и блокировать аномальную активность из внутренней сети

Решение

Не пускать через внешние интерфейсы трафик предназначенный для не маршрутизируемых сетей

```
/ip firewall rule add action= drop chain=forward comment="Reject BOGONS routing over WAN" dst-address-list=BOGONS out-interface-list=WAN log=yes log-prefix="BOGONS over WAN"
```



3. Firewall и безопасность сети



```
/ip firewall address-list  
add address=0.0.0.0/8 list=BOGONS  
add address=10.0.0.0/8 list=BOGONS  
add address=100.64.0.0/10 list=BOGONS  
add address=127.0.0.0/8 list=BOGONS  
add address=169.254.0.0/16 list=BOGONS  
add address=172.16.0.0/12 list=BOGONS  
add address=192.0.0.0/24 list=BOGONS  
add address=192.0.2.0/24 list=BOGONS  
add address=192.168.0.0/16 list=BOGONS  
add address=198.18.0.0/15 list=BOGONS  
add address=198.51.100.0/24 list=BOGONS  
add address=203.0.113.0/24 list=BOGONS
```

Подробности на <https://www.securitylab.ru/blog/personal/aodugin/305208.php>

4. ГОТОВИМ КОНФИГ ДЛЯ СВОИХ НУЖД

MikroTik



4. ГОТОВИМ КОНФИГ ДЛЯ СВОИХ НУЖД



1. Нам нужен удаленный доступ к маршрутизатору «на всякий пожарный»

Решение

Использовать разрешенные IP для управления

```
/ip firewall filter add action=accept chain=forward dst-port=8291,22 in-interface-list=WAN protocol=tcp src-address-list=AllowIPRemoteManagement place-before=0
```

Как ЭТИМ ПОЛЬЗОВАТЬСЯ?

В Address List AllowIPRemoteManagement мы добавляем внешнее DNS имя

```
/ip firewall address-list add list=AllowIPRemoteManagement address=AllowIP.company.com
```



4. ГОТОВИМ КОНФИГ ДЛЯ СВОИХ НУЖД



2. Всегда необходимо иметь резервные копии конфига

Решение

Не забываем настроить автоматический бекап устройства, к примеру на почту. Используем скрипт с wiki.mikrotik.com, но немного изменив.

```
/system script add name=Backup_to_email policy=read,write,policy,sensitive,test  
source="/system backup save name=email_backup;  
:delay 5; /tool e-mail send file="email_backup.backup"  
to="backup.mikrotik@realsd.ru" from=mikrotik@company.com body="See attached  
file" subject="$[/system identity get name] $[/system clock get time] $[/system clock  
get date] Backup";  
:delay 5; /file remove [find name="email_backup.backup"];"
```



4. ГОТОВИМ КОНФИГ ДЛЯ СВОИХ НУЖД



Как ЭТИМ пользоваться?

Для отправки писем необходимо настроить учетную запись.

Пример для mail.ru

```
/tool e-mail set address=smtp.mail.ru from="Mikrotik Backup"  
password=$EmailPassword port=465 start-tls=tls-only user=$EmailUserName
```

И создаем расписание для запуска резервного копирования

```
/system scheduler add interval=1d name=Backup on-event="/system script run  
Backup_to_email" policy=read,write,policy,sensitive,test start-date=jan/01/1970  
start-time=00:00:00
```



4. ГОТОВИМ КОНФИГ ДЛЯ СВОИХ НУЖД



3. Сетевое оборудование необходимо мониторить. Обычно для этого используется SNMP.

Решение

Подготовим параметры SNMP для своей системы мониторинга:

```
/snmp community set [find default=yes] name=$CommunityName security=private  
authentication-password=$AuthPass authentication-protocol=SHA1 encryption-  
password=$EncrPass encryption-protocol=AES
```

```
/snmp set enabled=yes trap-community=$CommunityName trap-version=3 engine-  
id=[/interface ethernet get number=0 mac-address]
```

5. Минимальная настройка QoS

MikroTik



5. Минимальная настройка QoS



В малых инсталляциях необходимо не столько ограничить скорость, сколько приоритизировать важный трафик и минимизировать воздействие на него менее важного.

Решение

Выделить наиболее важный трафик и промаркировать его. Начнем с управляющего трафика

```
/ip firewall mangle
```

```
add action=mark-connection chain=prerouting connection-state=new dst-port=8291,22 new-connection-mark=ManTraff_conn passthrough=yes protocol=tcp
```

```
add action=mark-packet chain=prerouting connection-mark=ManTraff_conn new-packet-mark=ManTraff_Packets passthrough=no
```



5. Минимальная настройка QoS



SIP

```
add action=mark-connection chain=prerouting connection-state=new dst-address-list=SIP_External_Servers new-connection-mark=SIP_Conn passthrough=yes src-address-list=SIP_Internal_Servers/Clients
```

```
add action=mark-connection chain=prerouting connection-state=new dst-address-list=SIP_Internal_Servers/Clients new-connection-mark=SIP_Conn passthrough=yes src-address-list=SIP_External_Servers
```

```
add action=mark-packet chain=prerouting connection-mark=SIP_Conn new-packet-mark=SIP_Packets passthrough=no
```



5. Минимальная настройка QoS



DNS

```
add action=mark-connection chain=prerouting connection-state=new dst-port=53  
new-connection-mark=DNS_conn passthrough=yes protocol=tcp
```

```
add action=mark-connection chain=prerouting connection-state=new dst-port=53  
new-connection-mark=DNS_conn passthrough=yes protocol=udp
```

```
add action=mark-packet chain=prerouting connection-mark=DNS_conn new-packet-  
mark=DNS_Packets passthrough=no
```

HTTP

```
add action=mark-connection chain=prerouting connection-state=new dst-  
port=80,443 new-connection-mark=HTTP_Conn passthrough=yes protocol=tcp
```

```
add action=mark-packet chain=prerouting connection-mark=HTTP_Conn new-packet-  
mark=HTTP_Packets passthrough=no
```



5. Минимальная настройка QoS



RDP

```
add action=mark-connection chain=prerouting connection-state=new dst-port=3389  
new-connection-mark=RDP_Conn passthrough=yes protocol=tcp
```

```
add action=mark-packet chain=prerouting connection-mark=RDP_Conn new-packet-  
mark=RDP_Packets passthrough=no
```

Весь остальной трафик

```
add action=mark-connection chain=prerouting connection-state=new connection-  
mark=no-mark new-connection-mark=Other_traff_conn passthrough=yes
```

```
add action=mark-packet chain=prerouting connection-mark=Other_traff_conn new-  
packet-mark=Other_traff_packets passthrough=no
```



5. Минимальная настройка QoS



Для SIP трафика создаем отдельный тип очередей

```
/queue type add kind=pcq name=SIP pcq-classifier=src-address,dst-address,src-port,dst-port pcq-dst-address6-mask=128 pcq-rate=160k pcq-src-address6-mask=128 pcq-limit=10KiB
```

Создаем простейшую очередь с приоритетами

```
/queue simple
```

```
add dst=ether1 name=ISP1 target=bridge1 total-max-limit="$InetSpeed"
```

```
add dst=ether1 name=SIP target=bridge1 packet-marks=SIP_Packets parent=ISP1 priority=1/1 total-queue=SIP total-max-limit=10M
```

```
add dst=ether1 name=ManTraff target=bridge1 packet-marks=ManTraff_Packets parent=ISP1 priority=2/2 total-max-limit=10M
```



5. Минимальная настройка QoS



```
add dst=ether1 name=DNS target=bridge1 packet-marks=DNS_Packets parent=ISP1  
priority=3/3 total-max-limit=10M
```

```
add dst=ether1 name=RDP target=bridge1 packet-marks=RDP_Packets parent=ISP1  
priority=4/4 total-queue=pcq-download-default total-max-limit=10M
```

```
add dst=ether1 name=HTTP target=bridge1 packet-marks=HTTP_Packets  
parent=ISP1 priority=6/6 total-queue=pcq-download-default total-max-limit=10M
```

```
add dst=ether1 name=Other target=bridge1 packet-marks=Other_traff_packets  
parent=ISP1 priority=7/7 total-queue=pcq-download-default total-max-limit=10M
```

Как этим пользоваться?

Во всех очередях изменить параметр **total-max-limit** параметр на значение вашей скорости канала. По умолчанию 10 мбит/с. Работает на симметричных каналах.

6. Шаблоны для быстрого запуска

*Mikro***Tik**



6. Шаблоны для быстрого запуска



1. Трудно представить современный офис без удаленного доступа, а значит без VPN.

Решение

Настроить VPN сервер. Самый простой и универсальный протокол для запуска L2TP over IPSec. Начнем с подготовки:

```
/interface list add name=VPN_L2TP_Users comment="Real_DefConf";  
/ip pool add name="VPN_Users" ranges=10.255.255.0/24 comment="Real_DefConf";  
/ppp profile add name=L2TP_Profiles local-address=10.255.255.1 remote-  
address=VPN_Users address-list=VPN_L2TP_Users interface-list=VPN_L2TP_Users  
change-tcp-mss=yes use-compression=no use-encryption=no only-one=yes;
```




6. Шаблоны для быстрого запуска



Запускаем сам сервер:

```
/interface l2tp-server server set enabled=yes default-profile=L2TP_Profiles  
authentication=mschap2 use-ipsec=required ipsec-secret="$VPNPSK" caller-id-  
type=number;
```

Firewall, настраиваем разрешающие правила:

```
/ip firewall filter{  
    add chain=input action=accept protocol=udp port=1701,500,4500 place-  
before=[find where comment="drop all not coming from LAN"] comment="Allow port  
for L2TP server"  
    add chain=input action=accept protocol=ipsec-esp place-before=[find where  
comment="drop all not coming from LAN"] comment="Allow esp protocol for  
L2TP/Ipsec server"  
};
```



6. Шаблоны для быстрого запуска

Создание VPN пользователя:

```
/ppp secret add name=user1 password=passuser1 profile=L2TP_Profiles  
service=l2tp
```

PPP Secret <user1>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

Limit Bytes In:

Limit Bytes Out:

Last Logged Out:

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove



6. Шаблоны для быстрого запуска



2. У каждого пользователя офиса имеется от 1 до 3 мобильных устройств, работающих с WiFi. Нам нужна WiFi сеть на всей территории компании.

Решение

Настроить CAPsMAN и использовать несколько WiFi точек. Начнем с частот:

```
/caps-man channel {
```

```
    add band=2ghz-g/n control-channel-width=20mhz extension-  
channel=disabled frequency=2412,2437,2462 name=2.4Channels reselect-  
interval=1d tx-power=20
```

```
    add band=5ghz-n/ac control-channel-width=20mhz extension-  
channel=Ce frequency=5180,5220,5260,5300,5680,5745,5785 name=5Channels  
reselect-interval=1d tx-power=20 skip-dfs-channels=yes
```

```
}
```



6. Шаблоны для быстрого запуска



Настроим модуляции:

```
/caps-man rates add name=StandartDataRates basic=1Mbps,6Mbps ht-basic-  
mcs=mcs-0,mcs-1,mcs-2,mcs-3,mcs-4,mcs-5,mcs-6,mcs-7 ht-supported-mcs="  
0,mcs-1,mcs-2,mcs-3,mcs-4,mcs-5,mcs-6,mcs-7,mcs-8,mcs-9,mcs-10,mcs-11,mcs-  
12,mcs-13,mcs-14,mcs-15"  
supported="1Mbps,2Mbps,5.5Mbps,11Mbps,6Mbps,9Mbps,12Mbps,18Mbps,24Mbps,  
36Mbps,48Mbps,54Mbps" vht-basic-mcs=mcs0-7 vht-supported-mcs=mcs0-9
```

Настроим профиль безопасности:

```
/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm group-  
encryption=aes-ccm disable-pmkid=yes name=OfficeNetPass  
passphrase="$PassOffice"
```



6. Шаблоны для быстрого запуска



Настроим access list для переключения между точками:

```
/caps-man access-list {  
    add action=accept allow-signal-out-of-range=5s disabled=no  
interface=any mac-address=00:00:00:00:00:00 signal-range=-75..0 ssid-regexp=""  
    add action=reject allow-signal-out-of-range=always disabled=no  
interface=any mac-address=00:00:00:00:00:00 signal-range=-120..120 ssid-regexp=""  
}
```

Настроим правила потока трафика:

```
/caps-man datapath add client-to-client-forwarding=yes local-forwarding=yes  
name=OfficeNet
```



6. Шаблоны для быстрого запуска



Создадим сами конфигурации для применения на WiFi точках:

```
/caps-man configuration {  
    add channel=2.4Channels country=russia3 datapath=OfficeNet  
    distance=indoors guard-interval=long max-sta-count=32 mode=ap multicast-  
    helper=default name=OfficeNet2 rates=StandartDataRates rx-chains=0,1  
    security=OfficeNetPass ssid="$SSIDOffice-2.4Ghz" tx-chains=0,1  
  
    add channel=5Channels country=russia3 datapath=OfficeNet  
    distance=indoors guard-interval=long max-sta-count=32 mode=ap multicast-  
    helper=default name=OfficeNet5 rates=StandartDataRates rx-chains=0,1  
    security=OfficeNetPass ssid="$SSIDOffice-5Ghz" tx-chains=0,1  
}
```



6. Шаблоны для быстрого запуска



Настраиваем автоконфигурацию в сети:

```
/caps-man provisioning {  
    add action=create-disabled hw-supported-modes=gn master-  
configuration= OfficeNet2 name-format=prefix-identity name-prefix=2Ghz  
    add action=create-disabled hw-supported-modes=ac master-  
configuration= OfficeNet5 name-format=prefix-identity name-prefix=5Ghz  
}
```

И наконец включаем CAPsMAN:

```
/caps-man manager set enabled=yes
```



6. Шаблоны для быстрого запуска



Настойка CAP:

```
/system reset-configuration caps-mode=yes
```

После перезагрузки оборудования устанавливаем понятное имя:

```
/system identity set name="CAP1"
```

Для безопасности устанавливаем логин и пароль и отключаем все лишнее.

Остается только включить созданные при автоконфигурации интерфейсы на контроллере.



6. Шаблоны для быстрого запуска



Осталось доработать напильником



6. Шаблоны для быстрого запуска



3. Не всем WiFi пользователям необходим доступ в корпоративную сеть, многим достаточно простого наличия сети Интернет.

Решение

Настроить на уже созданном CAPsMAN гостевую WiFi сеть с доступом только в Интернет.

Создадим отдельный bridge для гостей:

```
/interface bridge add name=bridge10;
```

```
/ip address add address="$GuestSubnet.1/24" interface=bridge10;
```



6. Шаблоны для быстрого запуска



Нам нужен отдельный DHCP сервер на гостевом bridge:

```
/ip pool add name="wifi-guest-dhcp" ranges="$GuestSubnet.20-$GuestSubnet.254"  
comment="Real_DefConf";
```

```
/ip dhcp-server add name=Real_DefConf address-pool="wifi-guest-dhcp"  
interface=bridge10 lease-time=3h disabled=no;
```

```
/ip dhcp-server network add address="$GuestSubnet.0/24"  
gateway="$GuestSubnet.1" comment="Real_DefConf";
```



6. Шаблоны для быстрого запуска



Направим всех гостей в отдельную таблицу маршрутизации и создадим минимальный набор маршрутов:

```
/ip route rule add action=lookup-only-in-table interface=bridge10 table=WiFi_Guest;  
/ip route {  
add dst-address="$GuestSubnet.0/24" gateway=bridge10 routing-mark=WiFi_Guest;  
add dst-address="$WANIP/$WANIPprefix" gateway=ether1 routing-mark=WiFi_Guest;  
add dst-address=0.0.0.0/0 gateway="$WANGW" routing-mark=WiFi_Guest;  
}
```



6. Шаблоны для быстрого запуска



Приступим к настройкам CAPsMAN:

Настройки каналов, модуляций и листы доступа у нас уже есть.

Нам нужны настройки потока данных:

```
/caps-man datapath add bridge=bridge10 client-to-client-forwarding=no local-forwarding=no name=GuestNe
```

Профиль безопасности:

```
/caps-man security add authentication-types=wpa2-psk encryption=aes-ccm group-encryption=aes-ccm disable-pmkid=yes name=GuestNetPass  
passphrase="$PassGuest"
```



6. Шаблоны для быстрого запуска



И конфигурации:

```
/caps-man configuration {
```

```
    add channel=2.4Channels country=russia3 datapath=GuestNet  
    distance=indoors guard-interval=long max-sta-count=32 mode=ap multicast-  
    helper=default name=GuestNet2 rates=StandartDataRates rx-chains=0,1  
    security=GuestNetPass ssid="$SSIDOffice-Guest" tx-chains=0,1
```

```
    add channel=5Channels country=russia3 datapath=GuestNet  
    distance=indoors guard-interval=long max-sta-count=32 mode=ap multicast-  
    helper=default name=GuestNet5 rates=StandartDataRates rx-chains=0,1  
    security=GuestNetPass ssid="$SSIDOffice-Guest" tx-chains=0,1
```

```
}
```



6. Шаблоны для быстрого запуска



Добавляем конфигурации к нашей автонастройке:

```
/caps-man provisioning {  
    set [find master-configuration=OfficeNet2] slave-  
configurations=GuestNet2  
    set [find master-configuration=OfficeNet5] slave-  
configurations=GuestNet5  
};
```

Гостевая Wifi сеть готова



6. Шаблоны для быстрого запуска



3. С ростом популярности и доступности IP телефонии современные офисы все чаще оборудованы именно IP телефонами, при этом необходимо настраивать каждый аппарат для работы с офисной или виртуальной АТС.

Решение

Практически любой IP телефон умеет получать необходимые настройки по сети, самый универсальный способ через TFTP. Нам нужен TFTP сервер.

```
/ip tftp add ip-addresses="$SubnetAccess.0/24" real-filename=/TFTPFolder req-filename=.*
```




6. Шаблоны для быстрого запуска



Создание папки для хранения конфигурационных файлов

```
:local Folder TFTPFolder;
```

```
/ip service set ftp disabled=no;
```

```
/user group add name=onlyftp policy=ftp,read,write;
```

```
/user add name=ftp password=ftp group=onlyftp;
```

```
/ip firewall filter add action=accept chain=input src-address=127.0.0.1 place-  
before=[find comment=\"Real_DefConf: drop all not coming from LAN\"]  
comment=\"For folder created\";
```

```
/file print file=temp;
```



6. Шаблоны для быстрого запуска



```
/tool fetch address=127.0.0.1 mode=ftp user=ftp password=ftp src-path=temp.txt  
dst-path=($Folder."/temp.txt");  
:delay 2;  
/file remove temp.txt;  
/file remove ($Folder."/temp.txt");  
/ip firewall filter remove [find comment="For folder created"];  
/user remove ftp;  
/user group remove onlyftp;  
/ip service set ftp disabled=yes;
```



6. Шаблоны для быстрого запуска



Через DHCP опции сообщим телефонам, что в сети имеется TFTP сервер и к какому ip необходимо подключиться для поиска конфигурационных файлов

```
/ip dhcp-server option add code=66 name=66_TFTP_Server value="s'192.168.203.1"
```

```
/ip dhcp-server option add code=150 name=150_TFTP_Server  
value="s'192.168.203.1"
```

```
/ip dhcp-server network set [find address="$SubnetAccess.0/24"] dhcp-  
option=66_TFTP_Server,150_TFTP_Server
```

Генерируем и копируем конфиги в папку TFTPFolder, перезагружаем телефоны



6. Шаблоны для быстрого запуска

File List

[-] [Filter] [New Folder] [Backup] [Restore] [Upload...] [Find]

File Name	Type	Size	Creation Time
flash	disk		Jan/01/1970 03:00:05
flash/TFTPRoot	directory		Dec/11/2018 12:16:36
flash/TFTPRoot/805ec00ab85...	.cfg file	172 B	Dec/11/2018 19:46:39
flash/TFTPRoot/805ec00ab85f...	.cfg file	174 B	Dec/11/2018 19:47:01
flash/TFTPRoot/805ec00ab86...	.cfg file	164 B	Dec/11/2018 19:47:17
flash/TFTPRoot/805ec00ab87...	.cfg file	164 B	Dec/11/2018 19:47:39
flash/TFTPRoot/805ec00ab88...	.cfg file	166 B	Dec/11/2018 19:47:57
flash/TFTPRoot/805ec00ab89...	.cfg file	168 B	Dec/11/2018 19:48:11
flash/TFTPRoot/805ec00ab8af...	.cfg file	162 B	Dec/11/2018 19:48:26
flash/TFTPRoot/805ec00ab90...	.cfg file	164 B	Jan/11/2019 12:28:56
flash/TFTPRoot/805ec00ab94...	.cfg file	168 B	Dec/11/2018 19:48:42
flash/TFTPRoot/y0000000000...	.cfg file	490 B	Dec/11/2018 19:36:54
flash/skins	directory		Jan/01/1970 03:00:01

13 items 11.7 MiB of 16.0 MiB used 26% free

7. Что со всем ЭТИМ делать?

MikroTik



7. Что со всем этим делать?



«Копипастить» каждый раз не удобно и долго.

При ручном переносе настроек возможны опечатки и ошибки.

Решение





7. Что со всем этим делать?



#Installation script variables

#General settings

```
:local localSubnet "10.0.0";  
:local SystemIdentity "RealMikrotik_GW";  
:local AdminUser "newadmin";  
:local AdminPass "adminpass";  
:local AllowIPRemoteManagement "allowip.company.com";
```

#WAN

#WAN IP type (static or dynamic)

```
:local WANConnect "static";  
#Static IP  
:local WANIP "1.1.1.2";  
:local WANIPprefix "29";  
:local WANGW "1.1.1.1";  
:local WANDNS "8.8.8.8,8.8.4.4";
```



7. Что со всем этим делать?



#Queues

#QoS customize? (1 yes, 0 no)

:local QueuesInstall 1;

#Internet access rate for queues. Specify in bytes

:local InetSpeed "50000000";

#Backup

#Backup to email service customize? (1 yes, 0 no)

:local BackupSend 1;

#SMTP settings. SMTP-TLS = yes, no, tls-only.

:local SMTPServer "smtp.mail.ru";

:local SMTPPort "465";

:local SMTPUser "mikrotik@company.com";

:local SMTPPass "mailpass";

:local SMTPTLS "tls-only";

:local SMTPFrom "Mikrotik Backup";

:local BackupToEmail "backup.mikrotik@company.com";



7. Что со всем этим делать?



#NTP

```
#NTP client customize? (1 yes, 0 no)
:local NTPUpdate 1;

#NTP settings. DNS name
:local ntpsrv1 "0.ru.pool.ntp.org";
:local ntpsrv2 "1.ru.pool.ntp.org";
```

#VPN

```
#L2TP VPN service customize? (1 yes, 0 no)
:local VPNInstall 1;

#L2TP VPN settings
:local VPNPoolSubnet "10.1.0";
:local VPNPSK "hyvZmRoFoXBzXcBqhdh6hdP66S7LKbaw";
```



7. Что со всем этим делать?



#CAPsMAN

#CAPsMAN service customize? (1 yes, 0 no)

:local CAPsMANInstall 1;

#CAPsMAN settings

:local SSIDOffice "OfficeNet";

:local PassOffice "wifiofficepass";

#CAPsMAN guest service customize? (1 yes, 0 no)

:local CAPsMANGuestNetInstall 1;

#CAPsMAN guest settings

:local SSIDGuest "GuestNet";

:local PassGuest "wifiguestpass";

:local GuestSubnet "10.2.0";



7. Что со всем этим делать?



#TFTP

```
#TFTP service customize? (1 yes, 0 no)
:local TFTPInstall 1;

    #Настройки для TFTP
    :local Folder "TFTPRoot";
    :local SubnetAccess "10.0.0";
```

#SNMP

```
#SNMP service customize? (1 yes, 0 no)
:local SNMPInstall 1;

    #Setting for SNMP service
    :local CommunityName "NotDefault"
    :local EncrPass "EncrPass"
    :local AuthPass "AuthPass"
```

Создание Bridge, установка Admin MAC и добавление в него портов

```
:log info "Start Bridge created";
:do {#Создаем бридж и добавляем в него интерфейсы
/interface bridge {
  add name=bridge1 priority=0x1000 comment="Real_DefConf"
  :local adminmac;
  :local etherlmac "$[/interface ethernet get number=0 mac-address]";
  :if ([:pick $etherlmac 16 17]=0) do={
    :if ([:pick $etherlmac 15 16]~"[A-F]") do={
      :set adminmac "$[:pick $etherlmac 0 15]9";
    } else={
      :set adminmac "$[:pick $etherlmac 0 15]$([:tonum [:pick $etherlmac 15 16]] - 1)";
    }
    :set adminmac ("$adminmac"."F");
  } else {
    :if ([:pick $etherlmac 16 17]~"[A-F]") do={
      :set adminmac "$[:pick $etherlmac 0 16]9";
    } else={
      :set adminmac "$[:pick $etherlmac 0 16]$([:tonum [:pick $etherlmac 16 17]] - 1)";
    }
  }
  set bridge1 auto-mac=no admin-mac=$adminmac;
};
:foreach k in=[/interface find where !(slave=yes || name="ether1" || name~"bridge1")] do={
  :local tmpPortName [/interface get $k name];
  :log info "port: $tmpPortName";
  /interface bridge port add bridge=bridge1 interface=$tmpPortName comment="Real_DefConf";
};
} on-error={:log warning "Error create bridge"};
```

Установка локальных сетевых настроек

```
:do {
/ip address add address="$localSubnet.1/24" interface=bridgel comment="$CommentPref";
/ip pool add name="default-dhcp" ranges="$localSubnet.20-$localSubnet.254" comment="$CommentPref";
/ip dhcp-server add name=Real_DefConf address-pool="default-dhcp" interface=bridgel lease-time=72h disabled=no;
/ip dhcp-server network add address="$localSubnet.0/24" gateway="$localSubnet.1" comment="$CommentPref";
:if ($WANConnect != "static" and $WANConnect != "dynamic") do {
:log error message="Error WAN connections type. WAN IP not installed";
} else {
:if ($WANConnect = "static") do {
:do {
/ip address add address="$WANIP/$WANIPprefix" interface=ether1l comment="$CommentPref: WAN ISPI IP1";
/ip firewall address-list add list="WAN_ISPI_IP1" address="$WANIP" comment="$CommentPref: WAN IP1 on ether1l";
/ip route add dst-address=0.0.0.0/0 gateway="$WANGW";
/ip dns set servers="$WANDNS";
} on-error={:log error "Error Static WAN IP installed";
} else {
:do {
/ip dhcp-client add interface=ether1l disabled=no comment="$CommentPref" script="\r
\n:local count [/ip firewall address-list print count-only where list=\\"WAN_ISPI_IP1\"]\r
\n:if (\$bound=1) do{\r
\n :if (\$count = 0) do{\r
\n /ip firewall address-list add list=\\"WAN_ISPI_IP1\" address=\$\"lease-address\" comment=\\"RealDefConf: WAN IP from DHCP clinet on ether1\"\\r
\n } else{\r
\n :if (\$count = 1) do{\r
\n :local test [/ip firewall address-list find where comment=\\"RealDefConf: WAN IP from DHCP clinet on ether1\"\\r
\n :if ([/ip firewall address-list get \$test address] != \$\"lease-address\") do{\r
\n /ip firewall address-list set \$test address=\$\"lease-address\"\\r
\n }\\r
\n } else{\r
\n :error \\"Multiple address found\"\\r
\n }\\r
\n }\\r
\n } else{\r
\n /ip firewall address-list remove [find where comment=\\"RealDefConf: WAN IP from DHCP clinet on ether1\"\\r
\n];\r
\n}
:log info "DHCP WAN IP installed";
} on-error={:log error "Error DHCP WAN IP installed";
};
};
} on-error={:log error "Error Local or WAN IP configured";
```

Настройка отдельной таблицы маршрутизации для гостевой WiFi сети при использовании DHCP на WAN порту

```
:local script [/ip dhcp-client get value-name=script [/ip dhcp-client find where comment="$CommentPref"]];
/ip dhcp-client set [/ip dhcp-client find where comment="$CommentPref"] script=$script\r\
\n:local remark \"WiFi_Guest\";\r\
\n:local WanNet [/ip address get value-name=network [/ip address find where interface=ether1 dynamic=yes]];\r\
\n:local count [/ip route print count-only where comment=\"$WANGW\" routing-mark=$remark];\r\
\n:local countnet [/ip route print count-only where comment=\"$WANNET\" routing-mark=$remark];\r\
\n:if ($bound=1) do{\r\
\n  :if ($countnet = 0) do{\r\
\n    \n  /ip route add dst-address=\"$WanNet\" gateway=ether1 comment=\"$WANNET\" routing-mark=$remark;\r\
\n  } else{\r\
\n    :if ($countnet = 1) do{\r\
\n      :local test [/ip route find where comment=\"$WANNET\" routing-mark=$remark];\r\
\n      :if ([/ip route get $test dst-address] != \"$WanNet\") do{\r\
\n        \n      /ip route set $test dst-address=\"$WanNet\";\r\
\n        \n      };\r\
\n      } else{\r\
\n        :error \"Multiple routes found\";\r\
\n      };\r\
\n    };\r\
\n  :if ($count = 0) do{\r\
\n    \n  /ip route add gateway=$\"gateway-address\" comment=\"$WANGW\" routing-mark=$remark; \r\
\n  } else {\r\
\n    :if ($count = 1) do{\r\
\n      :local test [/ip route find where comment=\"$WANGW\" routing-mark=$remark];\r\
\n      :if ([/ip route get $test gateway] != \"$gateway-address\") do{\r\
\n        \n      /ip route set $test gateway=$\"gateway-address\";\r\
\n        \n      };\r\
\n      } else{\r\
\n        :error \"Multiple routes found\";\r\
\n      };\r\
\n    };\r\
\n  };\r\
\n} else{\r\
\n  /ip route remove [find where comment=\"$WANGW\" routing-mark=$remark];\r\
\n  /ip route remove [find where comment=\"$WANNET\" routing-mark=$remark];\r\
\n};
```



Спасибо за внимание!

Вопросы?

Полная версия скрипта

<https://nc.realclouds.ru/index.php/s/RT5ykgZd54anCDo>

Презентация

<https://nc.realclouds.ru/index.php/s/wbgTeNLAdEZzZw5>

Контакты

E-mail moroz@llcreal.ru

Telegram @AntonMoroz_LLCCReal