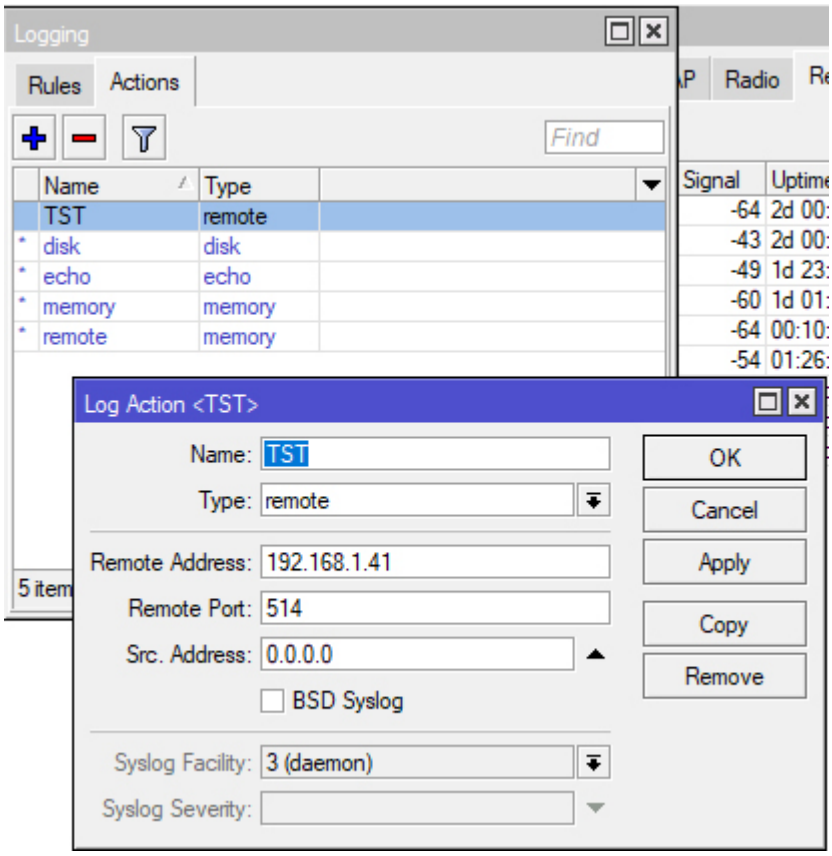
Логирование событий на удаленный сервер rsyslog

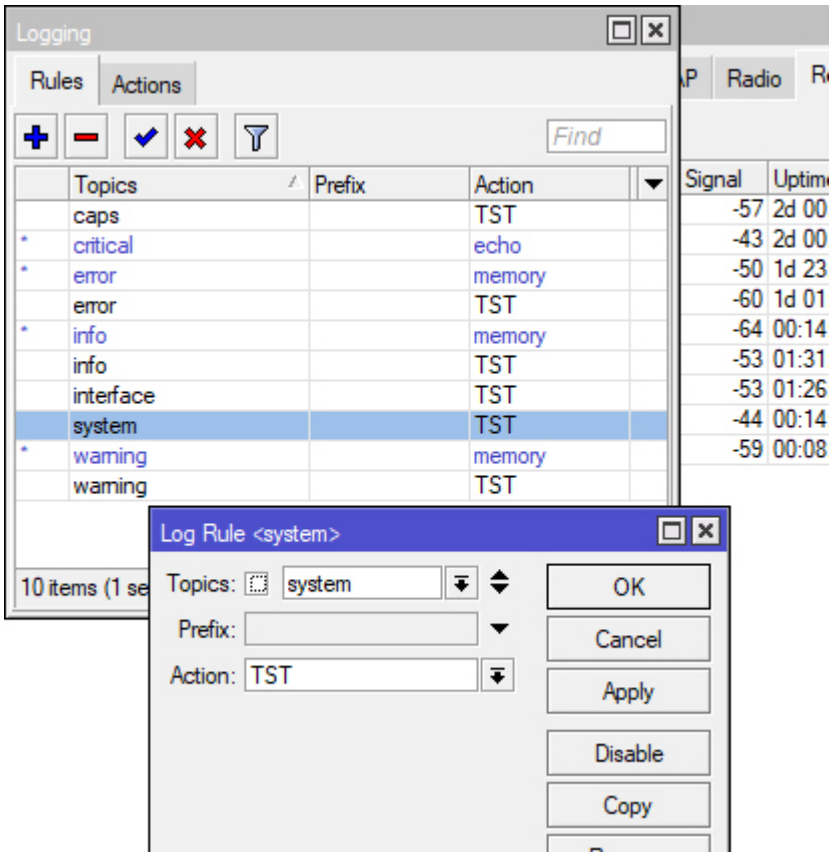
System–>Logging–>Actions–>New Action



Type – remote

Remote Address – IP сервера syslog

Потом делаем новый Rules



В поле Topics выбираем события какие мы хотим логировать, в поле Action выбираем наш созданный action.

На стороне сервера нужно отредактировать rsyslog.conf, раскоментировав следующие строки:

```
# vi /etc/rsyslog.conf

# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

и создать конфигурационный файл, в котором пропишем путь для отдельного файла лога, что бы события не писались или дублировались в /var/log/messages:

```
# vi /etc/rsyslog.d/mikrotik.conf

$template      FILENAME,"/var/log/mikrotik/%fromhost-ip%/syslog.log"
if $fromhost-ip != '127.0.0.1' then ?FILENAME
& stop
```

Проверить firewall на предмет открытия 514 udp порта.

После этого

```
# systemctl restart rsyslog
```

И можно наблюдать события

```
# less /var/log/mikrotik/192.168.1.1/syslog.log
```

Настроим ротацию логов:

```
# cat /etc/logrotate.d/mikrotik
/var/log/mikrotik/*/*.log {
        weekly
        rotate 12
        compress
        olddir /var/log/mikrotik/old
        missingok
        notifempty
        create 0644 root root
}
```

Проверим

```
#  /usr/sbin/logrotate  -d  /etc/logrotate.conf  2> /tmp/logrotate.debug
```

Ротация логов будет осуществляться еженедельно, во всех директориях, хранится будет хранится 12 сжатых архивов, директория для хранения /var/log/mikrotik/old.