

Some Networking Problems in Bangladesh, Solutions & Expectations from MikroTik

PRESENTED BY:

Syed Abu Saleh



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



About Me

- ❑ Syed Abu Saleh
- ❑ 20+ Years in Networking
- ❑ All MikroTik Certification
- ❑ MikroTik Consultant
- ❑ MikroTik Certified Trainer
- ❑ Facebook Group Admin (MikroTik User Group, Bangladesh)
- ❑ Managing Director, SASTECH LIMITED



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Congratulations BANGLADESH for successfully launch Bangabandhu-1 the country's first commercial satellite



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



About SASTECH LIMITED



sales@sastechbd.com

+8801976123401



SASTECH LIMITED



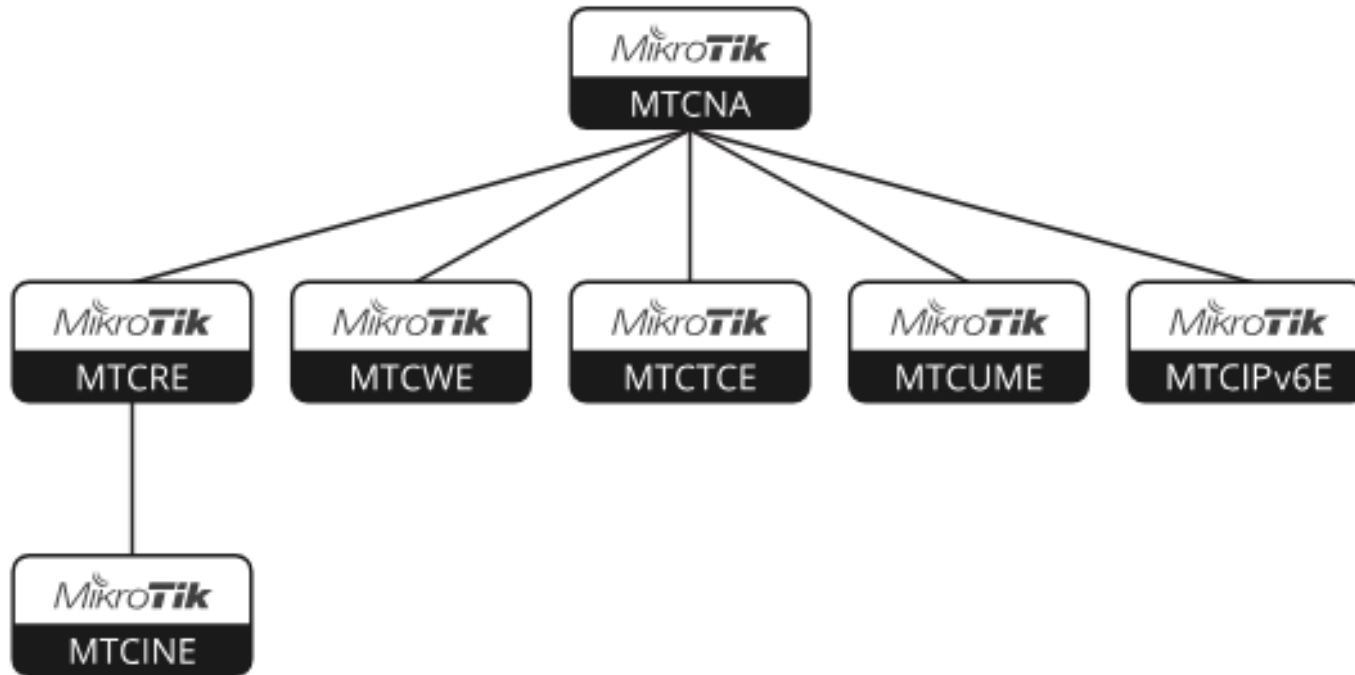
www.sastechbd.com



facebook.com/sastechbd



MikroTik Training & Certification



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



How much bandwidth Router can handle?



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Problems



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load



SAShTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High Layer7 load

```
/ip firewall layer7-protocol
```

```
add name=youtube regexp="^(youtube).*\$"
```

```
add name=facebook regexp="^(facebook).*\$"
```

```
/ip firewall filter
```

```
add action=drop chain=forward layer7 protocol=facebook
```

```
Add action=drop chain=forward layer7- protocol=youtube
```



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



“High Layer7 load”

```
/ip firewall layer7-protocol
```

```
add name=youtube regexp="^(youtube).*\$"
```

```
add name=facebook regexp="^(facebook).*\$"
```

```
/ip firewall filter
```

```
add action=drop chain=forward layer7 protocol=facebook
```

```
Add action=drop chain=forward layer7- protocol=youtube
```

WRONG!!!



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Analysis of the problem

- Problem:

- High CPU load, increased latency, packet loss, jitter, youtube and facebook is not blocked

- Diagnosis:

- “/tool profile” high layer7 load

- Reason:

- Each connection is rechecked over and over again
- Layer7 is checked in the wrong place and against all traffic



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Layer7

- Layer7-protocol is a method of searching for patterns in **ICMP/TCP/UDP** streams
- On trigger Layer7 collects next 10 packets or 2KB of a connection and searches for the pattern in the collected data
- All Layer7 patterns available on the Internet are designed to work only for the first 10 packets or 2KB of a connection.



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Correct implementation

- /ip firewall mangle

```
add action=mark-connection chain=prerouting protocol=udp  
dst-port=53 connection-mark=no-mark layer7-protocol=youtube  
new-connection-mark=youtube_conn passthrough=yes
```

```
add action=mark-packet chain=prerouting connectionmark=  
youtube_conn new-packet-mark=youtube_packet
```

- /ip firewall filter

```
add action=drop chain=forward packet-mark=youtube_packet  
add action=drop chain=input packet-mark=youtube_packet
```

(and same set for facebook)



SAS TECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load on PPPoE server



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load on PPPoE server

- 3000 pppoe-clients in 10.0.0.0/20 network
- Connected via 172.16.x.0/24 networks to other PPPoE servers with 10.x.0.0/20 PPPoE client network.
- All PPPoE servers and gateway in the same backbone area with redistribute connected routes

```
/routing ospf network
```

```
add network=172.16.1.0/24 area=backbone
```

```
add network=10.0.0.0/20 area=backbone
```



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load on PPPoE server

- 3000 pppoe-clients in 10.0.0.0/20 network
- Connected via 172.16.x.0/24 networks to other PPPoE servers with 10.x.0.0/20 PPPoE client network.
- All PPPoE servers and gateway in the same backbone area with redistribute connected routes

```
/routing ospf network
```

```
add network=172.16.1.0/24 area=backbone
```

```
add network=10.0.0.0/20 area=backbone
```

WRONG!!!



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Analysis of the problem

- Problem:

- CPU overloaded, PPPoE clients disconnect, clients can't reach target speeds, sometimes can't connect to the device

- Diagnosis:

- /tool profile shows “routing” process holding one CPU core 100% all the time, all other cores sometimes can also reach 100% with “ppp” and “networking” processes

- Reason:

- OSPF is spammed with PPPoE client /32 route updates



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



OSPF and PPPoE

- All dynamic routing protocols (more precisely - routing table updates and protocol calculations) are limited to a single core
- Every time a pppoe-client connects or disconnects it creates or deletes a /32 route. If that route is a part of an OSPF network, OSPF update is initiated
- Every time a pppoe-client connects or disconnects pppoe-interface is added to or removed from OSPF interfaces, that also initiates OSPF update



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Correct implementation

- /routing ospf area
add area-id=0.0.0.1 authentication=none
name=pppoe1 type=stub
- /routing ospf network
add area=pppoe1 network=10.0.0.0/20
- /routing ospf area range
add advertise=yes area=pppoe1
range=10.0.0.0/20
- /routing ospf interface
add interface=all passive=yes



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load on PPPoE server

- 3000 pppoe-clients in 10.0.0.0/20 network
- Static public IP address on public interface
- Masquerade rule
- No other firewall



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



High CPU load on PPPoE server

- 3000 pppoe-clients in 10.0.0.0/20 network
- Static public IP address on public interface
- Masquerade rule
- No other firewall

WRONG!!!



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Analysis of the Problem

- Problem:
 - CPU overloaded, PPPoE clients disconnect, clients can't reach target speeds, sometimes can't connect to boards.
- Diagnosis:
 - /tool profile shows “firewall” process dominating CPU load
- Reason:
 - Improper use of masquerade



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Masquerade

- Firewall NAT action=masquerade is unique subversion of action=srcnat, it was designed for specific use in situations when public IP can randomly change - when public IP is dynamic.
- Every time an interface disconnects and/or its IP address changes, router will search and purges connection tracking from connections related to that interface, to improve recovery time



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Correct implementation

- /ip firewall nat

```
add action=src-nat chain=srcnat outinterface=<Public> to-addresses=<Public_IP>
```



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Expectations from MikroTik

?



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd



Thank You



SASTECH LIMITED



www.sastechbd.com



facebook.com/sastechbd

