sciendo

Ensuring Equal Bandwidth for Remote Connections to the Local Company Server

doi:10.2478/mape-2020-0025
Date of submission to the Editor: 03/2020
Date of acceptance by the Editor: 06/2020
MAPE 2020, volume 3, issue 1, pp. 285-295

Adam Muc
ORCID ID: 0000-0002-9495-087X

Tomasz Muchowski
ORCID ID: 0000-0002-0200-7041
Gdynia Maritime University, **Poland**

Marcin Kluczyk
ORCID ID: 0000-0001-7357-6762
Polish Naval Academy of the Heroes of Westerplatte, **Poland**

Adam Szeleziński
ORCID ID: 0000-0003-2842-0683
Gdynia Maritime University, **Poland**

INTRODUCTION

Providing equal bandwidth is a popular problem not only for remote connections, but also for local connections. The scale of the problem with remote VPN tunnel connections is increasing as available bandwidth depends on the actual download and upload speeds of the router's WAN interface. For local connections, bandwidth is typically high because most business-class routers are equipped with Gigabit interfaces. This means that with a single LAN interface, the router is able to deliver bandwidth equal to 1 Gb/s and if multiple local interfaces are used, the bandwidth is multiplied. Of course, when connecting local devices to a local server, the bandwidth can be limited by not only the local server interface, but also by the backbone of the local network. However, this bandwidth in small and medium enterprises is high enough not to cause noticeable problems with access to server resources. In case of VPN tunneling over the Internet jamming the link is a popular issue. Usually business-class routers are equipped with a single WAN interface, and actual bandwidth also depends on the ISP (Internet Service Provider). It may be worth considering transferring data and server services (i.e. web applications, websites, databases) to the cloud, but this entails costs and the necessity to entrust the cloud provider with company data (Jain and Mahajan, 2017). The costs increase and security decrease may be too great for a company to afford to use cloud services.

A solution to the unequal distribution of the bandwidth between employees' devices may be the use of QOS (Quality of Service). It is a mechanism that

Contact address: a.szelezinski@wm.umg.edu.pl

allows to force an equal division of the bandwidth, as well as to prioritize a particular type of network traffic (Szigeti, et all, 2013; Burakowski and Dąbrowski, 2002).

TEST BECH

Test router

The authors used Mikrotik router with RouterOS 6.47 software flashed. The configured router (RB951G-2HnD model) has been reset to factory settings. The initial configuration has been done – IP address of LAN interface has been set, DHCP service has been configured, the required IP address pools have been created and OpenVPN service has been enabled. The configuration did not use manufacturer's proprietary solutions, so the configuration of other brands routers providing the same functionality should be similar. Table 1 provides information on router configuration.

Table 1 Router's configuration

Interface	Addressing
WAN interface IP address	192.168.100.247
LAN address	192.168.200.0/24
Router's LAN interface address	192.168.200.1
DHCP address pool	192.168.200.100-192.168.200.254
VPN address pool	192.168.200.10-192.168.200.99

Source: authors' own work

As it can be seen in the table above, the local network has been divided into two pools. The local and remote devices are therefore in the same subnet. Figure 1 shows a diagram of the network created for testing

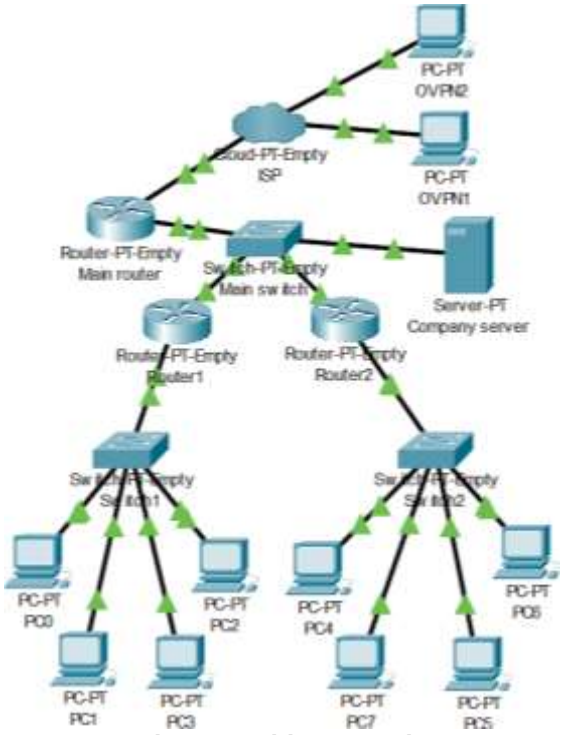


Fig. 1 IP address pools

As it can be seen in the picture above, the network consists of the main router with the main switch to which the company's server is connected, as well as two other routers (also Mikrotik routers), whose purpose is to create separate subnets for company departments. The WAN interfaces of these routers have been connected to the main switch providing access to the enterprise server to the devices of all company departments. The main router (also acting as a VPN server) and OpenVPN client devices are connected to another router simulating ISP. Table 2 shows the address of the devices in the network.

Table 2 Router's configuration

Interface	Addressing
Main router WAN interface IP address	192.168.100.247
Main router LAN interface IP address	192.168.200.1
First department's router WAN interface IP address	192.168.200.254
First department's LAN network address	10.1.0.0/16
Second department's router WAN interface IP address	192.168.200.253
Second department's LAN network address	10.2.0.0/16
Company server IP address	192.168.200.252

Source: authors' own work

As it can be seen in the table above, both the company server and routers of all departments of the company are connected to the LAN of the main router. Remote devices using VPN will also be connected to this LAN.

Test client devices

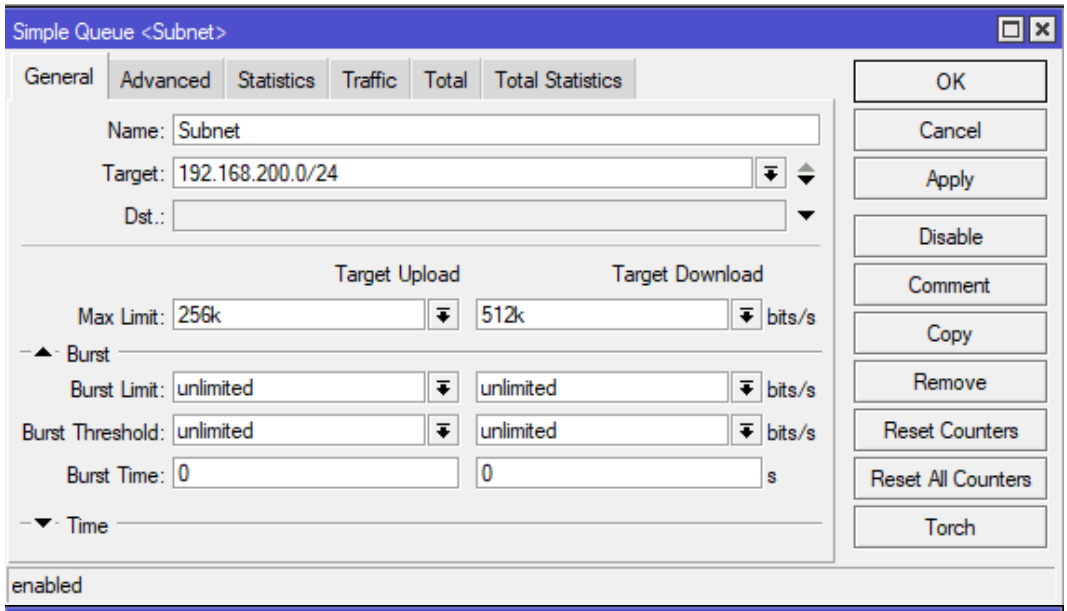
As client devices, the authors used several computers with Windows 10 operating system installed. Operating systems on all devices were freshly installed for testing purposes. On the remote devices there was installed software (OpenVPN Website, 2020) allowing to create a tunnel to OpenVPN server.

ENABLING VPN SERVICE

Router configuration

Created queues are designed to ensure equal distribution of WAN bandwidth among local network users and remote users using VPN. The purpose of the created configuration is to ensure that a single local network user or a single remote user cannot take over the whole bandwidth. As both remote devices and routers separating departments of the company are located in the local subnet of the main router, QOS (Queues -> Simple Queues) has been superimposed on this subnet. First, a queue was created to cover the entire local subnet of the main router, where PCQ (Per Connection Queueing) was enabled. The task of PCQ is to provide equal access (Mikrotik Manual, 2020) to download and upload bandwidth of WAN interface to all devices connected to the subnet. The operation of creating a queue is shown in Figure 2.

a)



b)

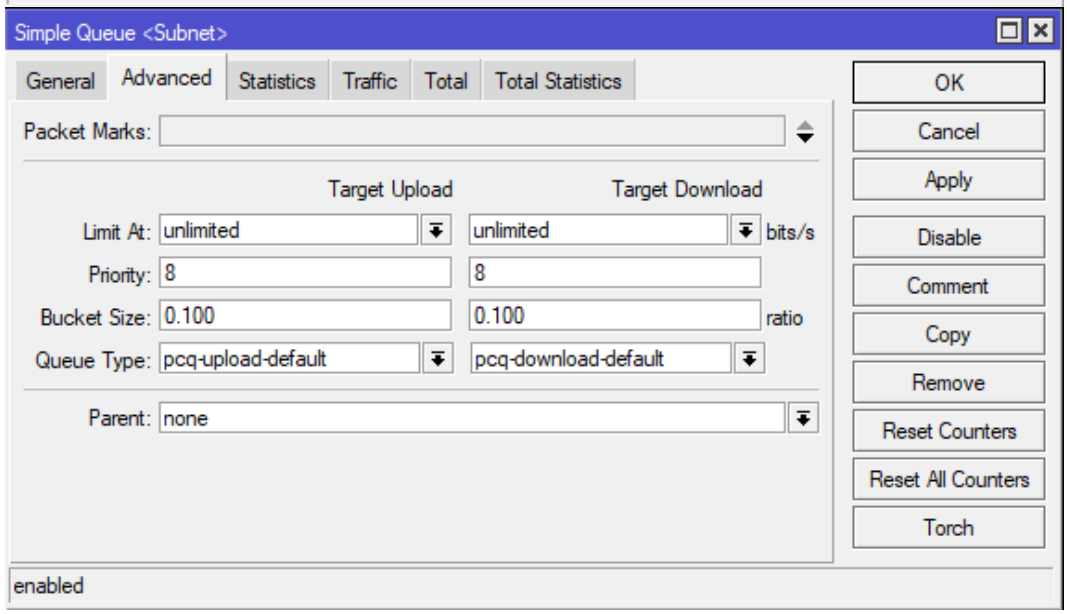
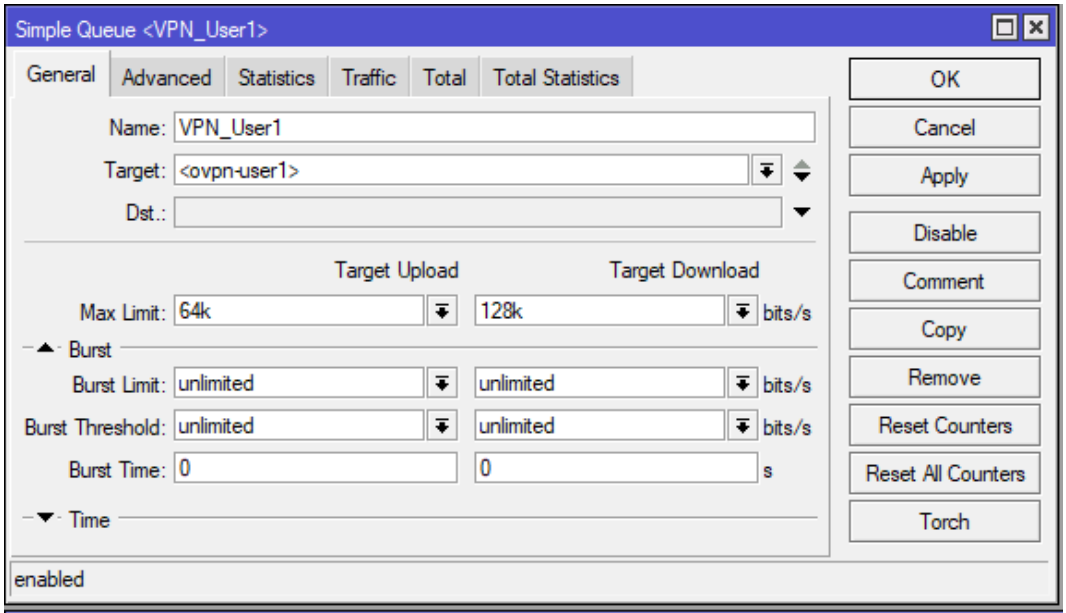


Fig. 2 Creating a queue covering the LAN subnet

As can be seen in the picture above, the overall bandwidth of the WAN interface is limited to 256k UP/512k DOWN. These are test values that allow to present PCQ operation in a more transparent way. In real application the limit should be equal to the real limits for download and upload on the WAN interface according to the limitation of the interface itself, but also to the bandwidth limit of the ISP. The value of the limit therefore depends on the bandwidth provided by the ISP. Setting the upper limit of bandwidth is necessary for the PCQ mechanism to have a reference value allowing to determine the guaranteed bandwidth for each user (Vassisa, et all, 2013). The creation of this single queue is sufficient to ensure an equal distribution of access to the Internet connection. However, it is worth creating sub queues to gain more control over the distribution of bandwidth. Figure 3 shows the process of creating a sub queue for one of the VPN users to guarantee a certain amount of bandwidth.

a)



b)

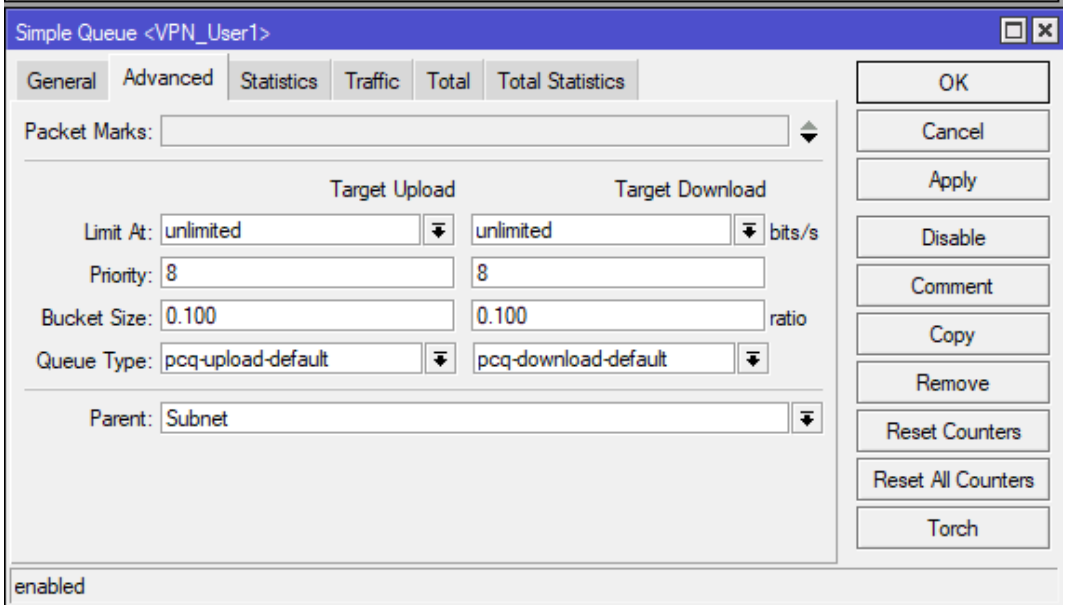


Fig. 3 Creating a queue for remote device

As it can be seen in the picture above, the created queue is a subqueue of the *Subnet* queue. It is necessary to create queues for all remote users as well as for local devices. As segmenting routers are connected to the local subnet of the main router, subqueues have been created for them. Creating more subqueues is similar to the process in Figure 3, but the *Target* needs to be changed. In the case of routers segmenting enterprise subnets, the *Target* field's content should be the IP address of the WAN port of the segmenting router, and in the case of remote devices, next user profiles should be selected. The *Burst* option, which allows to temporarily exceed the limits (Mikrotik Manual, 2020; Cisco, 2020), has not been configured because during testing, it turned out that the negative impact of local device burst on remote devices is too great and causes OpenVPN transmission disconnections. Although not configured, burst may occur, but for very short periods of time and should not affect the

guaranteed speed of other devices. Figure 4 shows the list of queues created for test configuration.

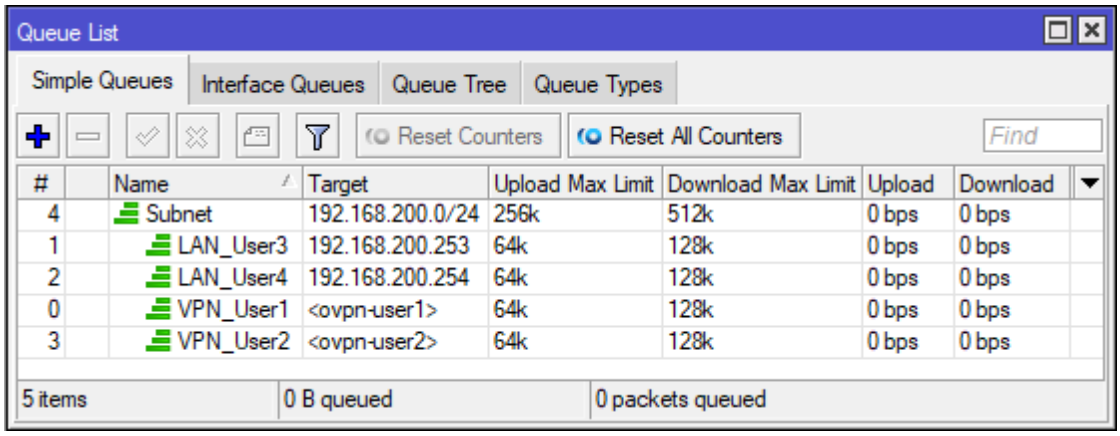


Fig. 4 View of created queues

As can be seen in the picture above, each queue has been allocated an equal share of the available bandwidth. This means that this bandwidth is guaranteed for each department of the company and each remote device.

The created configuration does not take into account the equal distribution of bandwidth between devices connected to the segmenting router (router of one of the departments). QOS control may not be necessary for local devices to local server connections, but as Internet access is controlled, the bandwidth of WAN connections is equally distributed between all departments and remote devices. Depending on the number of devices in the network segment, an even bandwidth distribution may be necessary. In this case, however, the upper limit for Internet connections will be the guaranteed bandwidth allocated to the segment. The upper limit for server connections will be the WAN interface bandwidth of the segmenting router (usually for business class routers it's 1Gb/s) used to connect to the local network, as the only limit is the bandwidth of the local network backbone. Therefore, it is necessary to create two separate queues and to mark the network traffic so that it is managed by the appropriate queues. Firewall Mangle rules can be used to mark network traffic. Figures 5 and 6 show the connection and packet marking process.

Creating outgoing traffic markings is similar to the process shown in Figure 5. However, it is necessary to change the direction of packet flow and input interface. In the case of incoming traffic, the input interface (In. Interface) is the WAN interface (in this case ether1) of the segmenting router, because it is this interface that is the source of incoming traffic. The local subnet of the segmenting router is in this case the destination of packets flow (Dst. Address) of packets. For outgoing traffic, the situation will be reversed. The input interface (In. Interface) will be the local interfaces of the segmenting router (in this case the bridge1 containing all local ports of the router), because these interfaces are the source of outgoing traffic.

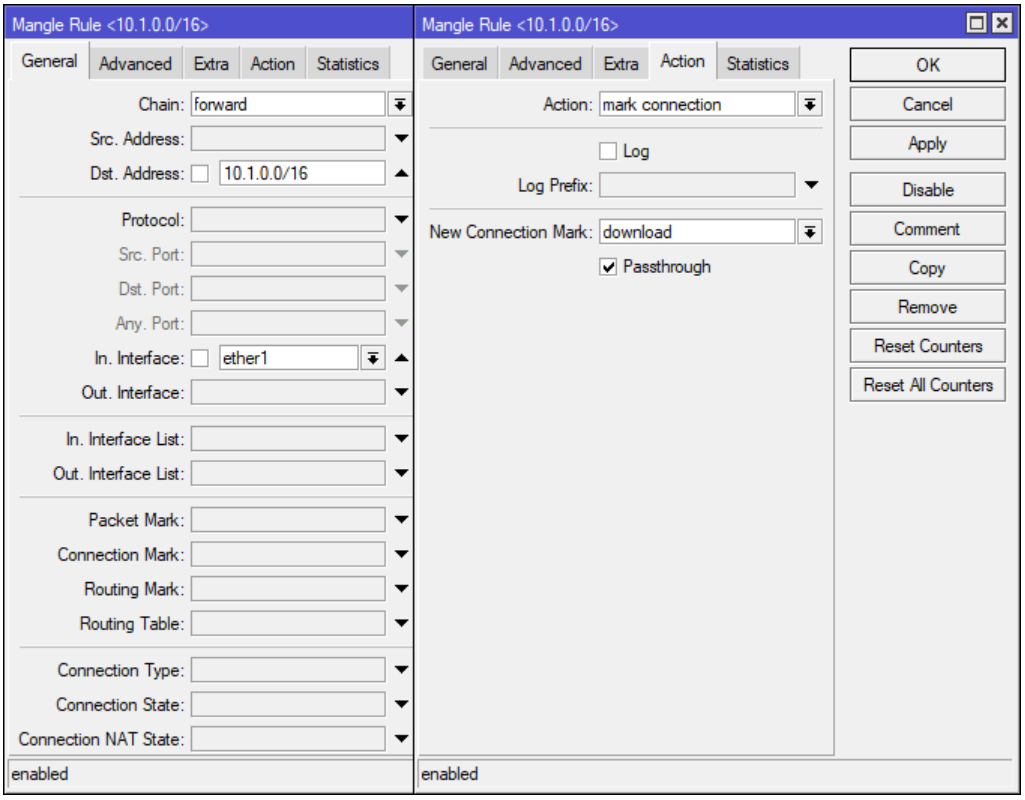


Fig. 5 Marking the incoming connections

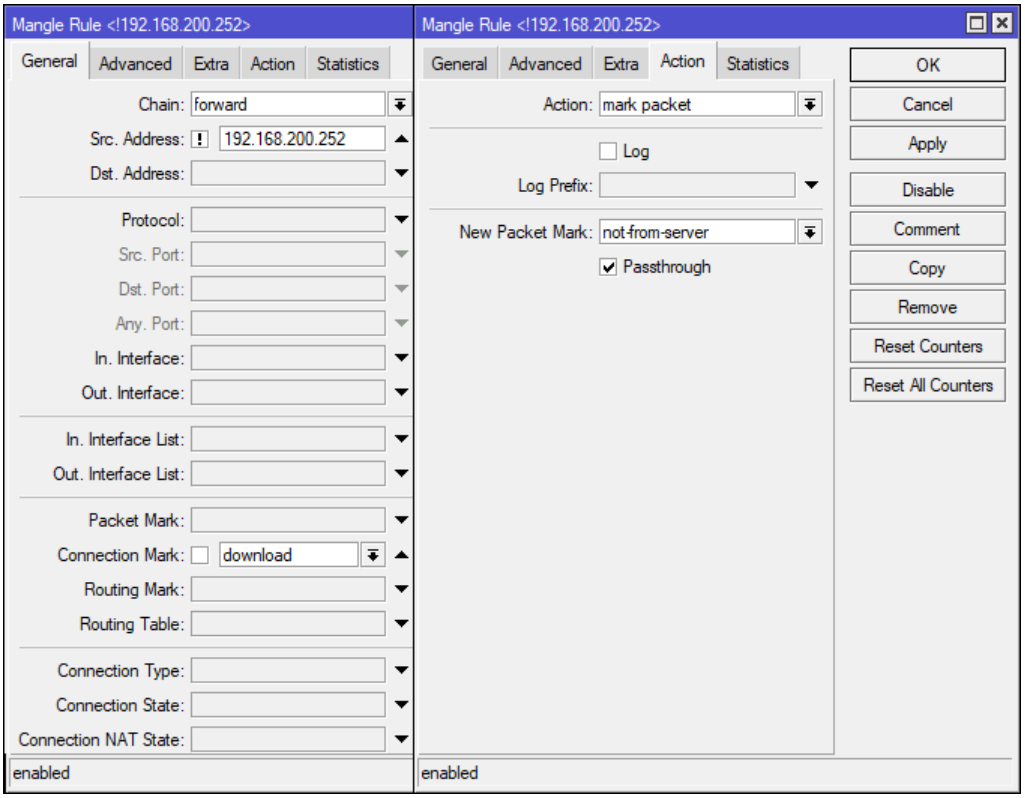


Fig. 6 Marking the incoming packets from the local server

The local subnet of the segmenting router is in this case the source of packet flow (Src. Address). Incoming traffic is marked as download, and outgoing traffic is marked as upload.

The creation of outgoing packet markings is similar to the process shown in Figure 6. However, it is necessary to change the direction of packet flow and the marked connection. In case of incoming packets, their source is determined and the connection is marked as incoming traffic. In the case of outgoing packets, their destination direction is determined, and the connection is marked as outgoing traffic. In the test example, two types of markings were created – outgoing and incoming server traffic (*to-server* and *from-server*) and outgoing and incoming traffic not flowing to or from the server (*not-to-server* and *not-from-server*). Created markings allow to determine which transmissions should be subjected to the queue covering local server traffic and which transmissions should be subjected to the queue covering main router's WAN interface traffic. Figure 7 shows created firewall Mangle rules.

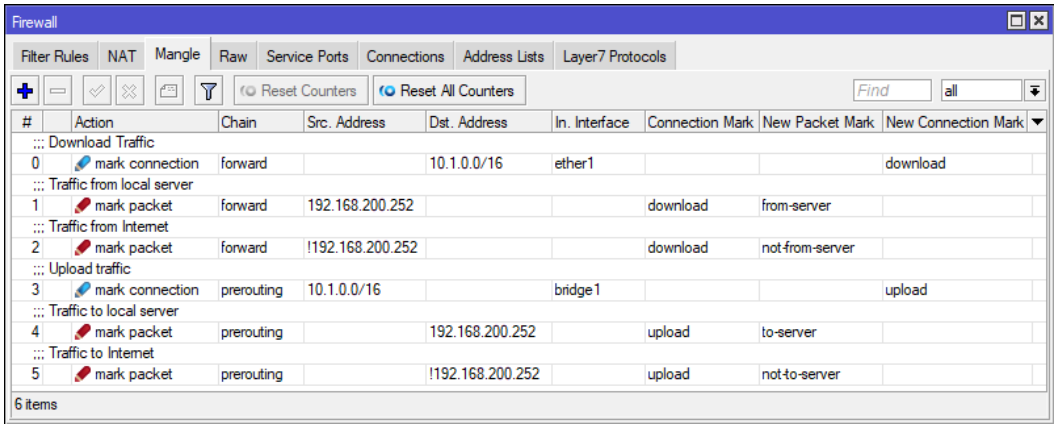


Fig. 7 Firewall Mangle rule list

The next step is to create the required queues. Queue Tree mechanism (Queues -> Queue Tree) was used. Figure 8 shows the process of creating one of the queues, and Figure 9 shows a list of created queues.

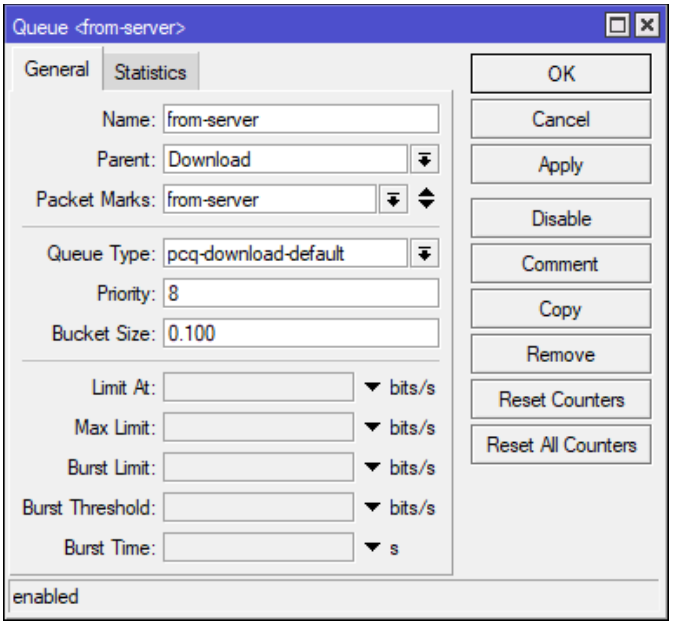


Fig. 8 Creating a queue for marked packets

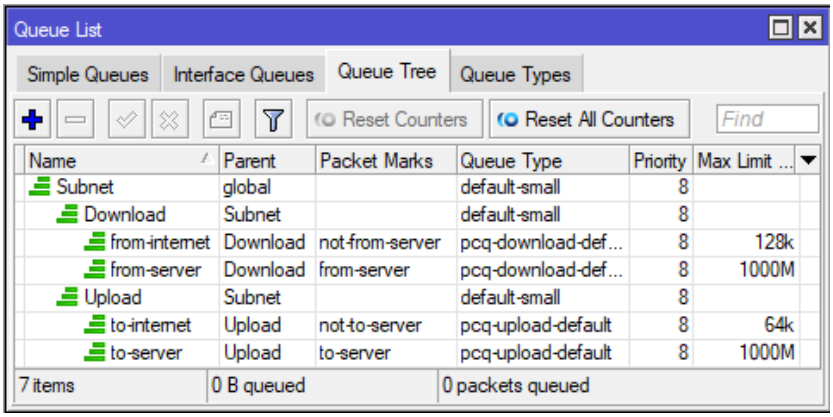


Fig. 9 View of created queue tree

As can be seen in the picture above, the network traffic of a local subnet of one of the company's departments is now fairly distributed. The QOS of the traffic to the local server is done according to different rules than other traffic. In this case, only server connections were treated as local traffic to the main router's subnet, while the remaining connections were treated as Internet traffic. In real life use, the main router's network could have more servers or other network devices (e.g. network printers). For these devices, queues would have to be created similar to the queue created for server related traffic.

Connections testing

A typical scenario was considered during testing. Local devices connected to the segregating routers (separating departments of the company) were generating traffic related to local server, but also were downloading files from the Internet. Two remote devices were connected to the network and downloaded files from the server. As the network traffic of the devices connected via VPN goes through the main router's WAN interface, it was controlled by QOS. Files were transferred from the server using SMB protocol.

During the operation of all devices, the QOS with PCQ mechanism equally divides the bandwidth and ensures guaranteed bandwidth. Burst, despite the not being configured, still occurs, but in very short periods of time that do not affecting the stability of VPN connections, as it does not affect the allocated bandwidth guarantee. The operation of QOS with PCQ is shown in Figure 10.

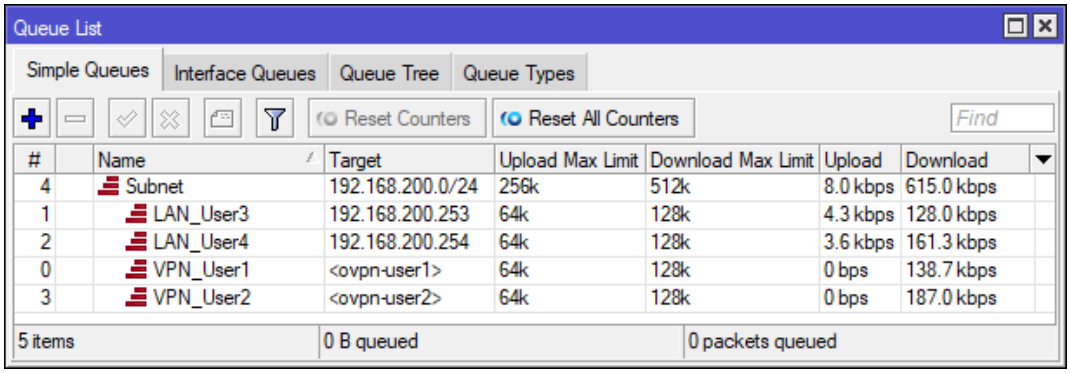


Fig. 10 QoS operation test

As it can be seen in the picture above, the burst occurred but did not violate the guaranteed speed. The possibility of a burst will only appear if the WAN bandwidth is higher than the set limit.

CONCLUSION

The QOS mechanism allows for prioritization of the selected type of traffic, but can also be used to guarantee specific bandwidth to devices. PCQ, on the other hand, allows for fair sharing of the bandwidth between all devices. The use of these mechanisms in an enterprise providing remote access to a local server via VPN enables fair sharing of the bandwidth between local devices and remote devices. This is important because taking over entire bandwidth by a local device may prevent remote operation. Significant slowdowns may occur or the connection may suddenly end due to insufficient bandwidth speed. Providing fair access to server resources to all employees is necessary for them to do their job properly. Significant delays will result in a loss of employee productivity, as an employee is unable to affect the performance of the IT infrastructure. The presented test configuration solves the problem of unequal access to the server. Each department of the company and remote employees have equal access.
QOS technology is not only used in enterprises. It can be used in any network where there is a problem with taking over the whole bandwidth by a single device.

REFERENCES

Burakowski, W. and Dąbrowski, M. (2002) Multi-service IP QoS network: architecture and practical experiments. Warsaw: Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, Tom 5.

Cisco. QoS: Policing and Shaping Configuration Guide [online]. Available at: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_plcshp/configuration/xe-3s/qos-plcshp-xe-3s-book/qos-plcshp-pct-shp.html [Accessed 1 June 2020]

Jain, A. and Mahajan, N. (2017) The Cloud DBA-Oracle: Managing Oracle Database in the Cloud. New York: Apress.

Mikrotik Manual. Queues: Burst [online]. Available at: https://wiki.mikrotik.com/wiki/Manual:Queues_-_Burst [Accessed 1 June 2020]

Mikrotik Manual. Queues: PCQ [online]. Available at: https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ [Accessed 1 June 2020]

OpenVPN Website. Community download section [online] Available at: https://openvpn.net/community-downloads/ [Accessed 1 June 2020].

Shaik, B. and Vallarapu, A. (2018) Beginning PostgreSQL on the Cloud: Simplifying Database as a Service on Cloud Platforms. New York: Apress.

Szigeti, T. and Hattingh, C. amd Barton, R. and Briley K. (2013) End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition. London: Cisco Press.

Vassisa, D. and Kampourakia, A. and Belsisb, P. and Skourlasa C. (2013) A Resource Reservation and Traffic Categorization Agent for QoS in Medical Ad Hoc Networks. Budapest: Elsevier Procedia - Social and Behavioral Sciences Vol 73.

Abstract: Creating the required IT infrastructure to enable the ability for comfortable remote working is not an easy task. Improper configuration can create the possibility of taking over the whole bandwidth of the link by one device. Increasing bandwidth introduces extra costs and does not completely eliminate the problem – it will be more difficult to take over the whole bandwidth, but it is still possible. The solution to the problem may be the use of clouds and VPS, but it is associated with high costs and the need to entrust company data to providers of these services. Due to security and too high costs, this may not be an optimal solution. An alternative solution may be to use QoS along with PCQ. This mechanism allows to ensure equal division of the bandwidth between the devices under its control. With an appropriate configuration, QoS can eliminate the problem of taking over the whole bandwidth and ensure equal access to resources.

Keywords: QOS, PCQ, bandwidth sharing, remote working, VPN