ІНСТИТУТ СПЕЦІАЛЬНОГО ЗВ’ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Cпеціальна кафедра №1

Звіт

З навчальної дисципліни «Засоби і комплекси криптографічного захисту інформації»

Практична робота №3.7: "Налаштування QOS"

**Виконав:**

Командир С-04 групи

Іван ФЕСЕНКО

**Перевірив:**

Капітан Володимир КУБРАК

**Київ 2023**

**Алгоритми конфігурації QoS**

**Для телефонії:**

1. Розпізнайте, який трафік у вашій мережі відноситься до голосового зв'язку, такого як трафік від IP-телефонів, програм VoIP або інших голосових служб.
2. Створіть групи для різних видів трафіку, використовуючи протоколи або порти, які використовуються голосовими програмами. Наприклад, часто використовуються протоколи SIP або RTP для VoIP-трафіку.
3. Встановіть пріоритет для класифікованого голосового трафіку. QoS може використовувати різні механізми пріоритету, такі як черги з пріоритетами, управління пропускною здатністю або обмеження затримки.
4. Налаштуйте обмеження швидкості передачі даних для певних класів трафіку. Це допоможе уникнути перевантаження мережі та забезпечити стабільний голосовий зв'язок.
5. Більшість мережних пристроїв підтримують функціональність QoS. Знайдіть відповідні налаштування на маршрутизаторі або комутаторі та активуйте їх.
6. Після внесення змін проведіть тестування, щоб переконатися, що голосовий зв'язок працює належним чином. Якщо виникають проблеми, може знадобитися коригування налаштувань QoS та повторне тестування, поки не будуть досягнуті бажані результати.

**Для відео:**

1. Встановіть, який трафік у вашій мережі є відеоконтентом. Це може бути потокове відео, що використовує протоколи, такі як HTTP, RTSP (Real-Time Streaming Protocol) або інші відеопрограми.
2. Створіть категорії для різних видів відеотрафіку, використовуючи протоколи або порти, які використовуються відеододатками. Наприклад, потокове відео може використовувати порти 80 (HTTP) або 554 (RTSP).
3. Встановіть пріоритет для класифікованого відеотрафіку, щоб надати йому перевагу перед іншими типами трафіку. Використовуйте механізми QoS, такі як черги з пріоритетами або керування пропускною здатністю, для забезпечення достатньої пропускної здатності для відео.
4. Використовуйте обмежувачі трафіку, щоб обмежити швидкість передачі відеотрафіку. Це може бути корисним для запобігання перевантаження мережі та забезпечення стабільного відтворення відео.
5. Переконайтеся, що функціональність QoS активована на вашому мережевому обладнанні. Знайдіть налаштування QoS на маршрутизаторі або комутаторі та ввімкніть їх.
6. Після налаштування виконайте тестування, щоб переконатися, що відео передається з високим пріоритетом та стабільністю. Якщо виникають проблеми, може знадобитися коригування налаштувань QoS та повторне тестування, поки не будуть досягнуті бажані результати.

**Linux QoS:**

Налаштування параметрів QoS здійснюється за допомогою команди tc, яка входить до пакету iproute. Оскільки ця команда має складний інтерфейс, рекомендується використовувати високорівневі інструменти для зручності роботи з нею.

Для зниження затримок можна використовувати команду wondershaper, яка обмежує трафік до значення, незначно нижчого за максимальну пропускну здатність каналу. Після налаштування мережевого інтерфейсу, обмеження трафіку встановлюється за допомогою команди wondershaper interface download\_rate upload\_rate. Назва інтерфейсу може бути, наприклад, enp1s0, eth0 або ppp0, а значення вказуються в кілобітах за секунду. Ця команда перенаправляє функцію керування трафіком на окрему сторінку.

У випадку підключення через Ethernet мережу, зазвичай слід викликати скрипт wondershaper після налаштування функції. Це означає, що команда wondershaper повинна бути додана до файлу /etc/network/interfaces після налаштування і перед його скасуванням. Для підключення через PPP можна створити скрипт, який викликає wondershaper у /etc/ppp/ip-up.d/ для керування трафіком під час встановлення з'єднання. Нижче наведений приклад, використовуючи перший метод:

Зміни у файлі /etc/network/interfaces:

iface eth0 inet dhcp

up /sbin/wondershaper eth0 500 100

down /sbin/wondershaper remove eth0

Оптимальна конфігурація:

Файл /usr/share/doc/wondershaper/README.Debian.gz містить опис рекомендованого розробниками пакета методу налаштування з деякими деталями.

Стандартна конфігурація:

При виборі конкретної конфігурації QoS, ядро Linux використовує планувальник черги pfifo\_fast, який має декілька цікавих функцій. Пріоритет кожного IP-пакету базується на полі DSCP (Differentiated Services Code Point) в цьому пакеті. Зміна цього 6-бітного поля може бути корисною для використання різних функцій планування.

Поле DSCP можна встановити при генерації IP-пакетів або динамічно за допомогою netfilter. Наступні правила є достатніми для забезпечення пріоритету для SSH-сервера, незалежно від значення DSCP, яке необхідно встановити в шістнадцятковому форматі

nft add table ip mangle

nft add rule ip mangle PREROUTING tcp sport 22 counter ip dscp set 0x04

nft add rule ip mangle PREROUTING tcp dport 22 counter ip dscp set 0x04

**Cisco QoS:**

Класифікація трафіку:

Для ідентифікації відеотрафіку розподілимо його за протоколом HTTP та портом 80.

Класифікуємо IP-телефонію з використанням протоколу SIP та портів голосового зв'язку, наприклад, 5060 та 5061.

Встановлення пріоритетів:

Надамо IP-телефонії вищий пріоритет, щоб забезпечити пріоритетну передачу голосового трафіку.

Знизимо пріоритет відеотрафіку, надаючи меншу важливість для передачі цього типу даних.

Черги з пріоритетами:

Створимо дві черги з пріоритетами: "Високий" та "Низький".

Призначимо чергу з високим пріоритетом для IP-телефонії та чергу з низьким пріоритетом для відеотрафіку.

Управління пропускною здатністю:

Виділимо достатню пропускну здатність для IP-телефонії, наприклад, 30% від загальної пропускної здатності мережі.

Обмежимо пропускну здатність для відеотрафіку, наприклад, до 70% від загальної пропускної здатності мережі.

Конфігурація QoS для маршрутизатора Cisco (за допомогою CLI):class-map match-any VIDEO\_TRAFFIC

match protocol http

match access-group 101

class-map match-any VOIP\_TRAFFIC

match protocol sip

match access-group 102

policy-map QOS\_POLICY

class VIDEO\_TRAFFIC

bandwidth percent 70

queue-limit 100 packets

random-detect dscp-based

random-detect dscp 10 20 30

class VOIP\_TRAFFIC

bandwidth percent 30

queue-limit 50 packets

priority

random-detect dscp-based

random-detect dscp 40 50

interface GigabitEthernet0/0

service-policy output QOS\_POLICY

**QoS Mikrotic:**

У MikroTik RouterOS існує два підходи до реалізації QoS:

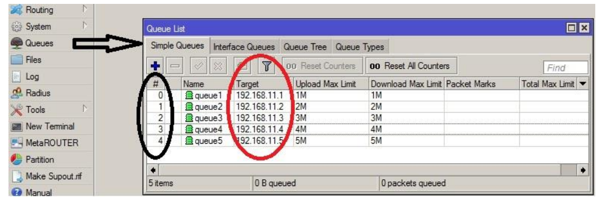
Simple queues (прості черги).

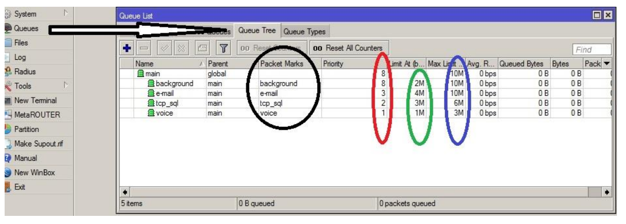
* Обробка даних у порядку їх надходження.
* Легкість налаштування.
* Можливість управління трафіком без використання позначення пакетів (цільових міток).
* Ефективна робота з багатоядерними процесорами, зокрема з родиною маршрутизаторів CCR.
* Звичайне використання: обмеження швидкості для окремих користувачів на основі їх IP-адреси.

Queue tree (дерево черг).

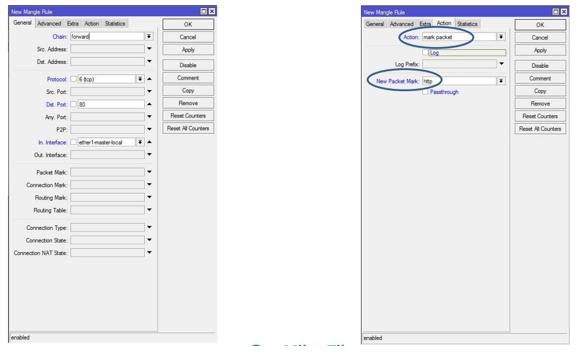
Класифікація та маркування:

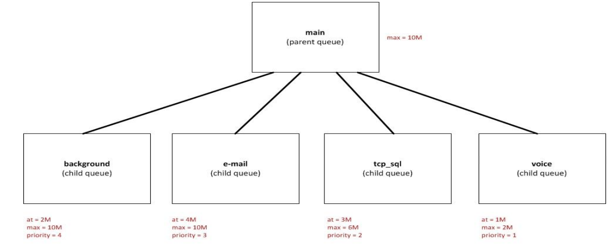
* Для того, щоб направити трафік до черги, необхідно відокремити його і надати віртуальну мітку.
* В RouterOS доступні три типи віртуальних міток, які діють в межах операційної системи, не виходячи за межі маршрутизатора:
* Мітка з'єднання (mark connection)
* Мітка маршрутизації (політика маршрутизації)
* Мітка пакету (QoS)
* Для маркування трафіку використовується таблиця Mangle:

/ip firewall mangle.



**Проведення класифікації та маркування:**





**Fasttrack:**

