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»

Практика №11: "QOS"

**Виконав:**

Курсант С-04 групи

Клячко А.О.

**Перевірив:**

Капітан Володимир Кубрак

**Київ 2023**

**QoS для телефонії:**

* Ідентифікуйте трафік голосового зв'язку: Визначте, який трафік у вашій мережі належить до голосового зв'язку. Це може бути трафік від IP-телефонів, VoIP-програм або інших голосових служб.
* Визначте класифікацію трафіку: Створіть класифікацію трафіку на основі протоколів або портів, які використовуються голосовими програмами. Наприклад, VoIP-трафік зазвичай використовує протоколи SIP або RTP
* Налаштуйте пріоритети: Встановіть пріоритети для класифікованого голосового трафіку. QoS може використовувати різні механізми пріоритету, такі як черги з пріоритетами, управління пропускною здатністю або обмеження затримки.
* Налаштуйте шейпери трафіку: Шейпери трафіку дають змогу обмежувати швидкість передачі даних для певних класів трафіку. Це може допомогти запобігти перевантаженню мережі та гарантувати стабільність голосового зв'язку.
* Увімкніть QoS на маршрутизаторі або комутаторі: У більшості мережних пристроїв є функціональність QoS. Знайдіть відповідні налаштування на маршрутизаторі або комутаторі та увімкніть їх.
* Тестування та налаштування: Після внесення змін проведіть тестування, щоб переконатися, що голосовий зв'язок функціонує належним чином. Якщо виникають проблеми, вам може знадобитися відрегулювати налаштування QoS і повторити тестування до досягнення бажаного результату.

**QoS для вiдео:**

* Ідентифікуйте відеотрафік: Визначте, який трафік у вашій мережі відноситься до відео. Це може бути потокове відео з використанням протоколів, таких як HTTP, RTSP (Real-Time Streaming Protocol) або інші відеопрограми.
* Класифікуйте відеотрафік: Створіть класифікацію відеотрафіку на основі протоколів або портів, що використовуються відео додатками. Наприклад, потокове відео може використовувати порти 80 (HTTP) або 554 (RTSP).
* Налаштуйте пріоритети: Встановіть пріоритети для класифікованого відеотрафіку. Це дозволить пріоритезувати передачу відео перед іншими типами трафіку. Ви можете використовувати механізми QoS, такі як черги з пріоритетами або керування пропускною здатністю, щоб надати достатню пропускну здатність відео.
* Налаштуйте шейпери трафіку: Використовуйте шейпери трафіку для обмеження швидкості передачі відеотрафіку. Це може бути корисним, щоб запобігти перевантаженню мережі та забезпечити стабільне відтворення відео.
* Увімкніть QoS на маршрутизаторі або комутаторі: Переконайтеся, що функціональність QoS увімкнена на вашому мережному обладнанні. Зверніться до документації обладнання для отримання вказівок щодо увімкнення та налаштування QoS.
* Тестування та налаштування: Після налаштування проведіть тестування, щоб переконатися, що відео передається з пріоритетом та стабільністю. Якщо виникають проблеми, ви можете коригувати налаштування QoS і повторювати тестування, доки не досягнете бажаного результату.

**Настройка QoS с использованием маршрутизатора Cisco:**

Класифікація трафіку:

Класифікуємо відеотрафік на основі протоколу HTTP та порту 80.

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

Встановлення пріоритетів:

Встановимо вищий пріоритет для IP-телефонії.

Встановимо нижчий пріоритет відеотрафіку.

Черги з пріоритетами:

Створимо дві черги з пріоритетами: High (високий) та Low (низький).

Призначимо чергу High для IP-телефонії та чергу Low для відеотрафіку.

Управління пропускною спроможністю:

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

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

Приклад конфігурації QoS для маршрутизатора Cisco (на основі 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

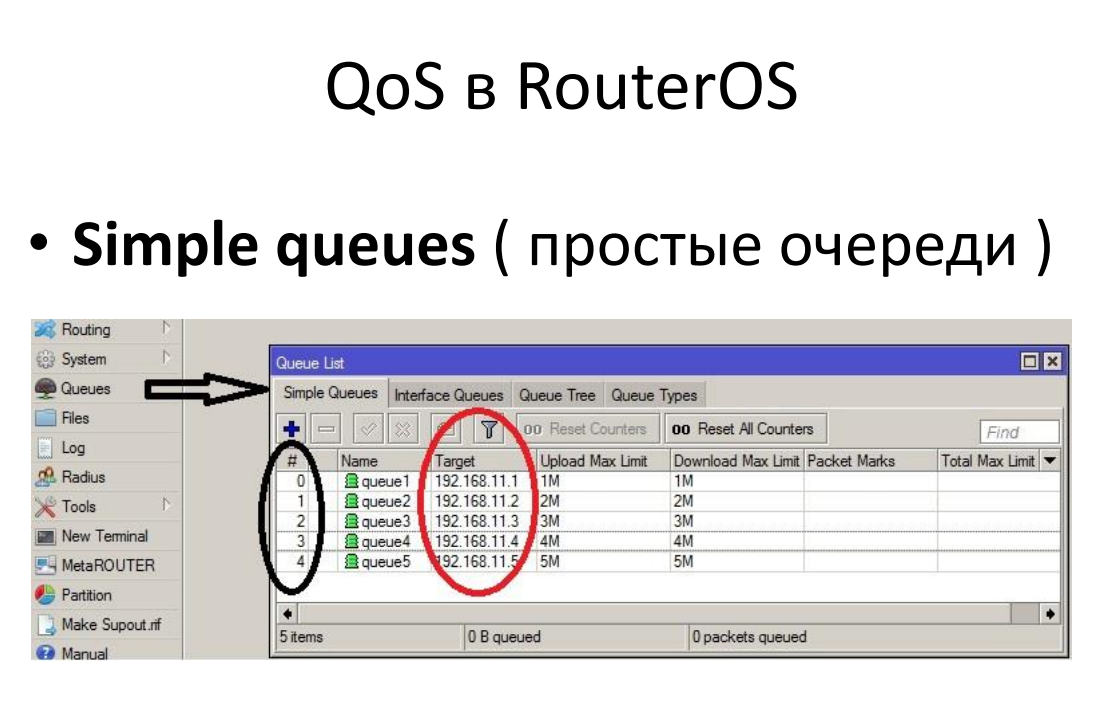
**QoS у RouterOS**

• У MikroTik RouterOS існує 2

підходи до реалізації QoS:

• Simple queues (прості черги)

• Queue tree (дерево черг)



QoS у RouterOS

• Simple queues (прості черги):

• Обробка в порядку прямування

• Простота, зручність конфігурування

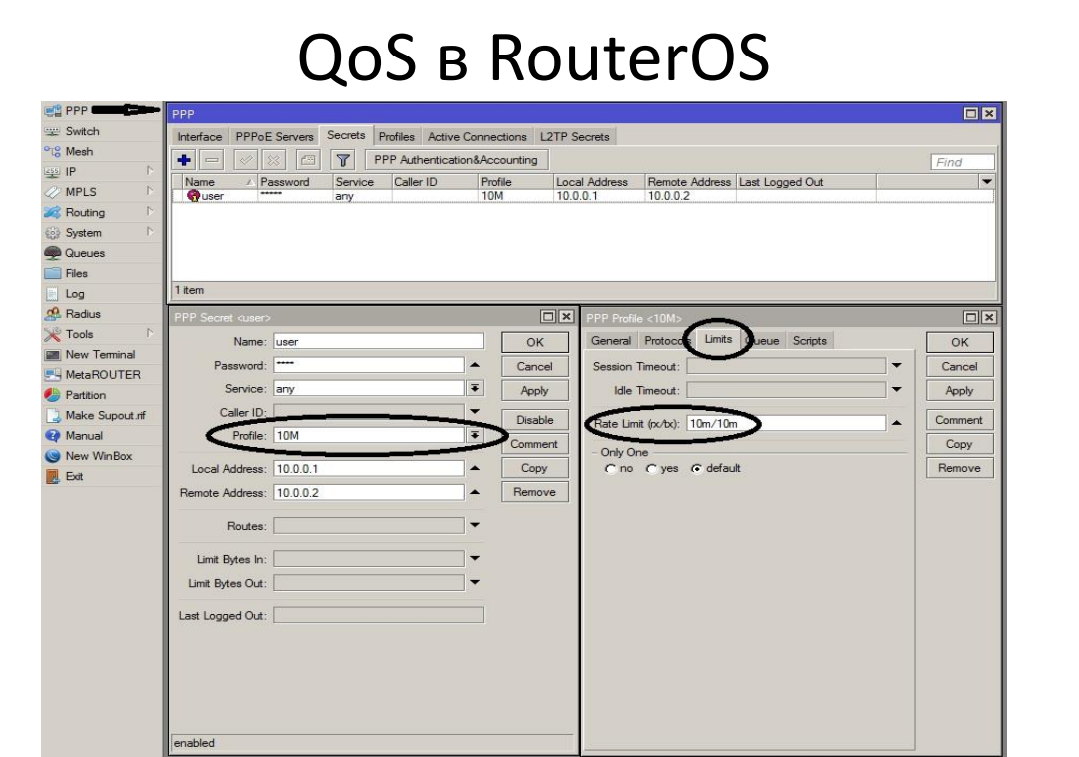
• Можливість обійтися без packet mark (target)

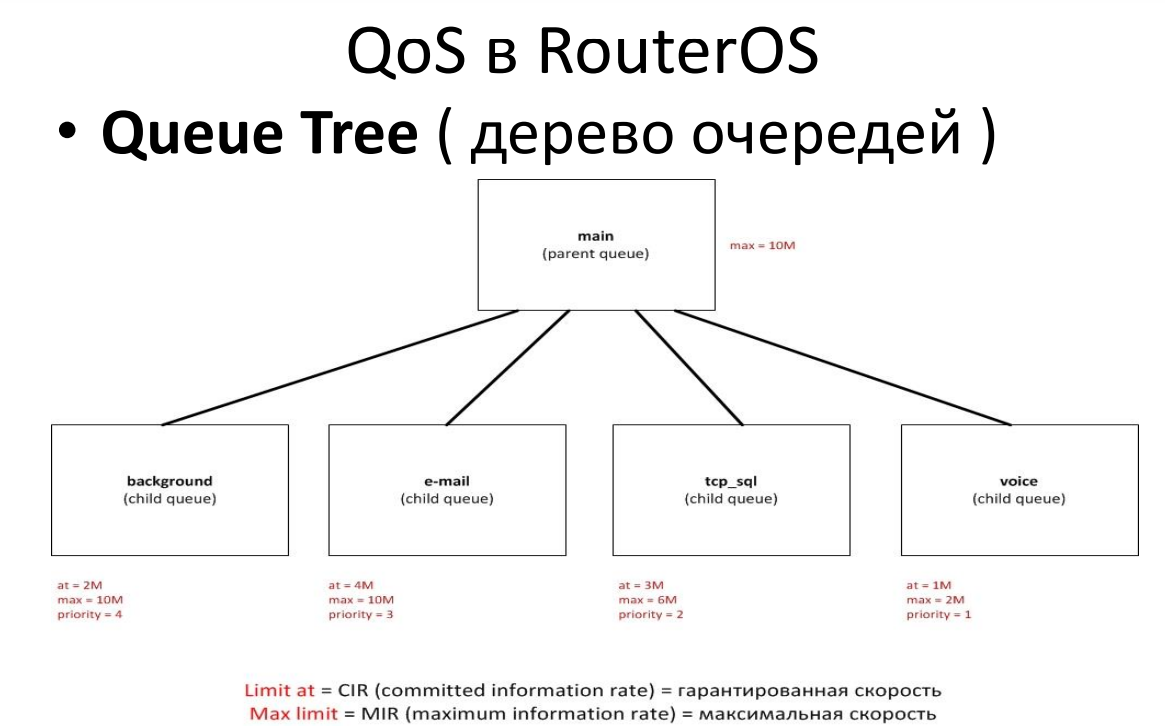
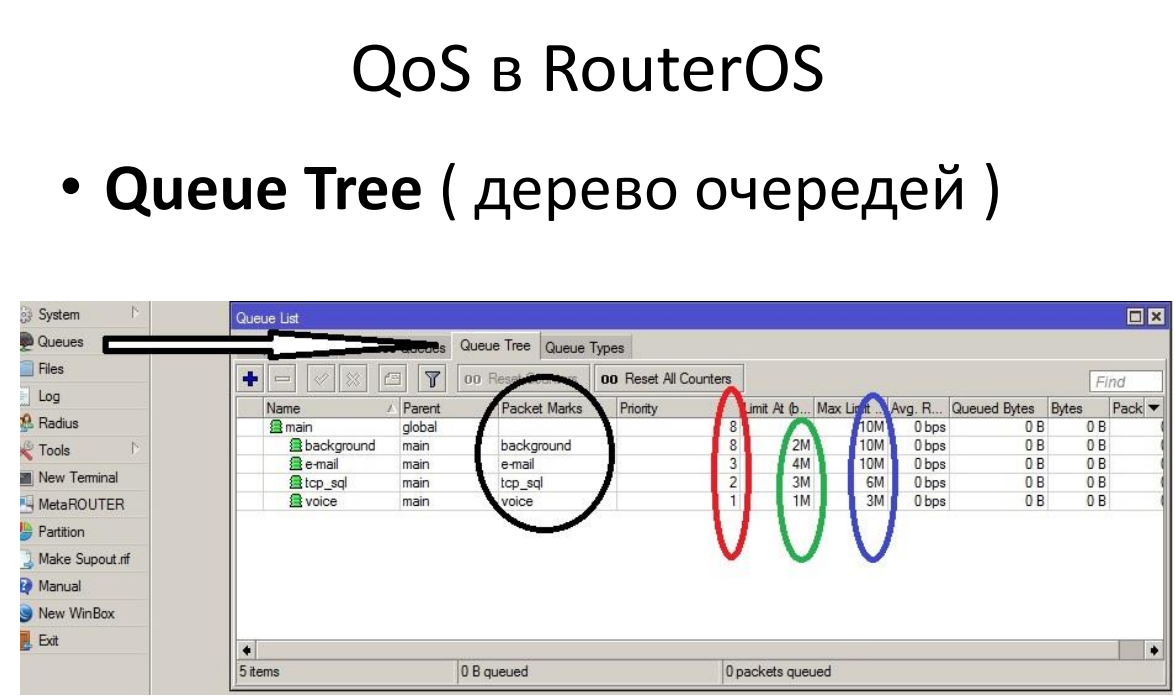
• Добре обробляються багатоядерними

процесорами (родина роутерів CCR)

• Типове застосування: обмеження швидкості

для конкретних користувачів за їх IP-адресою





Класифікація та маркування

• Для того, щоб трафік потрапив у чергу, потрібно

його виділити та промаркувати спеціальною

міткою

• У RouterOS є 3 типи віртуальних міток,

які існують тільки всередині ОС, не виходячи

за межі роутера:

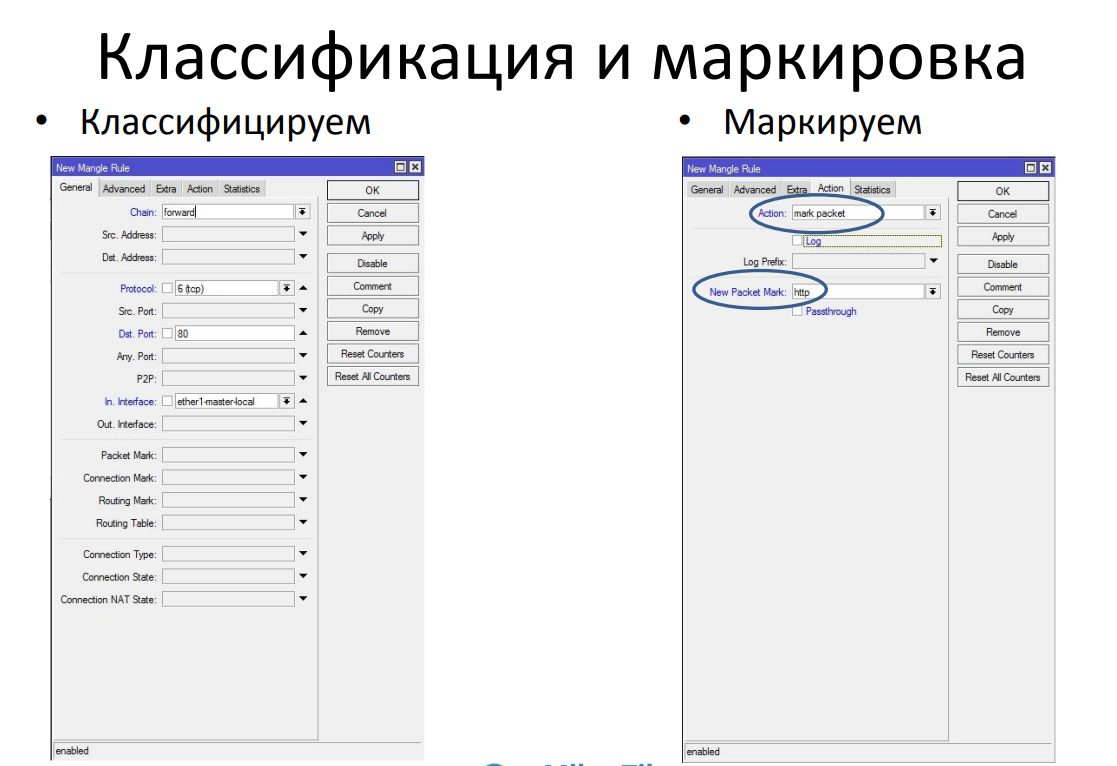
- mark connection

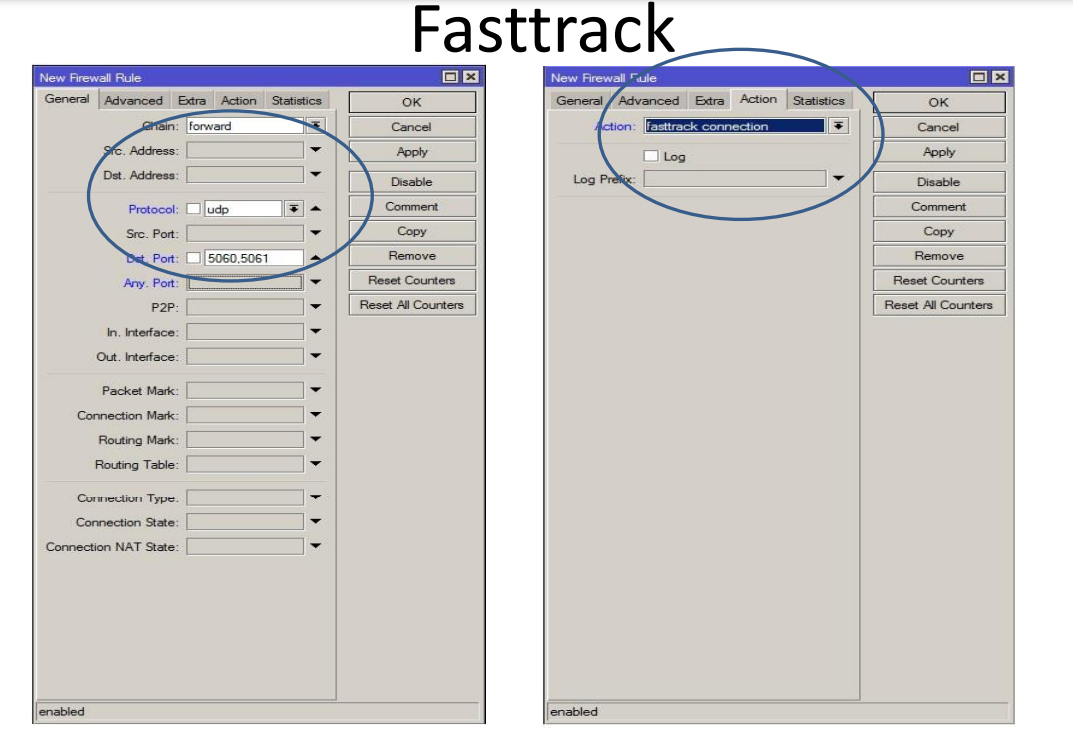
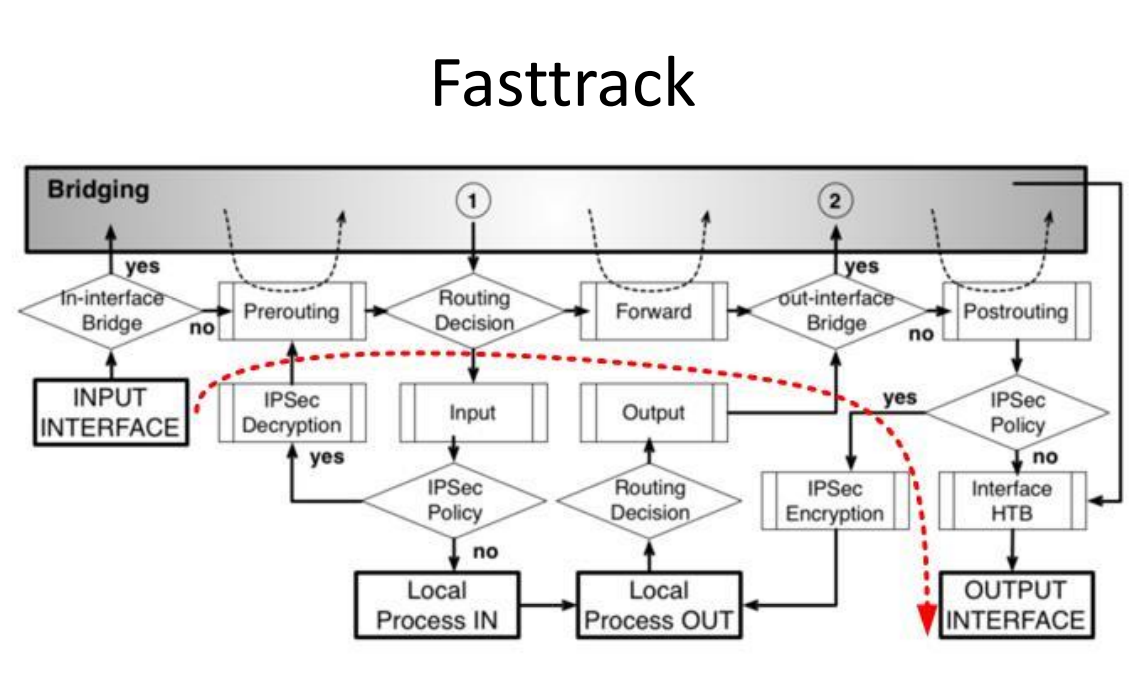
- mark routing (policy routing)

- mark packet (QoS)

• Маркуємо трафік ми у таблиці Mangle:

/ip firewall mangle





**QoS у linux**

**Налаштування та виконання**

Параметри QoS налаштовуються через команду tc (включена у пакет iproute). Оскільки інтерфейс цієї команди досить складним до сприйняття рекомендується використовувати до роботи з нею високорівневі інструменти.

**Зменшення затримок: wondershaper**

Основне завдання команди wondershaper (у пакеті зі схожим ім'ям) - зменшення затримок переміщення пакетів по мережі. Це досягається обмеженням всього трафіку до величини трохи нижче лінії повного насичення каналу. Після того, як мережевий interface is configured, setting up this traffic limitation is achieved by running wondershaper interface download\_rate upload\_rate. Interface може бути enp1s0, eth0 або ppp0 для прикладу, і що слів є expressed в kilobits per second. Пристрій переміщує функцію зв'язку, що відповідає розподільчому управлінню транспортним засобом на особливу сторінку.

Для підключення до мережі Ethernet, historically this script не слід називати правою після того, як функція configured. Це означає, що адреса вниз і вниз напрямки до /etc/network/interfaces файлу, за допомогою встановлених кнопок, щоб скористатися, по-своєму, після того, як interface configured and before it is deconfigured. Або в PPP випадку, створюючи script, що розмовляє wondershaper в /etc/ppp/ip-up.d/ буде можливий транспортний контроль як один як зв'язок. Below is an example using this first method:

Зміни у файлі /etc/network/interfaces:

iface eth0 inet dhcp

up /sbin/wondershaper eth0 500 100

down /sbin/wondershaper remove eth0

**Оптимальна настройка**

Файл /usr/share/doc/wondershaper/README.Debian.gz содержит описание, с некоторыми деталями, метода настройки, который рекомендуется разработчиками пакета.

#### Стандатна настройка

Вибираючи специфічний QoS configuration, Linux kernel використовує pfifo\_fast queue scheduler, який забезпечує багато цікавих особливостей до нього. Пріоритет всіх процесів IP-пакету базується на розділі DSCP (Differentiated Services Code Point) з цього пакета; Модифікація цього 6-бітного поля є приємною для того, щоб розглянути пов'язані з scheduling features. Refer to https://en.wikipedia.org/wiki/Differentiated\_services#Class\_Selector for more information.

DSCP field може бути встановлений при застосуванні, що генерується IP пакетів, або встановлений на ходу netfilter. Наступні правила є достатнім для збільшення відповідності для серверів SSH-сервісу, не дивлячись на те, що в DSCP філії необхідно встановити в hexadecimal:

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