

Н. М. Коваль¹, Е. А. Гимпель¹

¹ ФГАОУ ВО «Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия

ЛАБОРАТОРНЫЙ РАЗБОР TCP-ACL И ИНТЕРФЕЙСНЫХ ПОКАЗАТЕЛЕЙ СЕТЕВОГО СТЕНДА

Аннотация. В статье представлен учебный разбор фрагментов сетевой конфигурации и авторской сводки интерфейсных показателей лабораторного стенда. Рассматриваются Cisco Catalyst 2960, Eltex MES1428 и MikroTik CRS326. Цель работы — сопоставить содержание показанных команд с границами интерпретации агрегированных счётчиков, не выдавая их изменение за проверенную фильтрацию определённого потока. В конфигурациях Cisco и Eltex приведены запреты TCP между двумя заданными узлами и последующее разрешение остального IP-трафика. Это не общий запрет IP-пакетов. Для MikroTik показаны создание моста и добавление интерфейсов; правило ACL и его назначение в этих листингах не представлены. Авторы описывают мониторинг SNMP в Zabbix с интервалом опроса 60 секунд. Получаемые показатели усредняются за интервал и не позволяют установить протокольный состав трафика или кратковременные пики. В работе сохранены авторские значения нагрузки до и после описанных изменений, а производные отношения пересчитаны по их округлённым центральным значениям. Эти вычисления характеризуют сводные числа, а не долю фактически пропущенных пакетов. Исходные временные ряды и расчёт авторских величин после знака «±» не представлены, поэтому их статистический смысл не подтверждается. Практическое значение материала состоит в разборе TCP-правил, назначении фильтра интерфейсу и разграничении конфигурации, агрегированного наблюдения и доказательства эффекта. Сопоставление производителей, состава остаточной нагрузки и аппаратных причин различий по данным статьи не проводится.

Ключевые слова: TCP; ACL; коммутатор; SNMP; интерфейсный счётчик; лабораторный стенд.

Введение

Списки контроля доступа (Access Control Lists) представляют собой один из базовых инструментов управления потоком пакетов в сети. Их основная задача — отбирать проходящие через устройство пакеты по заданным критериям и регулировать доступ к сетевым сервисам. ACL применимы не только на традиционных маршрутизаторах и межсетевых экранах, но и на современных L2+ коммутаторах, сочетающих коммутацию на канальном уровне с некоторыми возможностями сетевого уровня.

Важно учитывать, что на L2+ платформах обработка пакетов бывает разнородной. Часть трафика проходит полностью через аппаратные механизмы коммутации, тогда как другие типы пакетов отправляются на программную обработку — в контроллерную плоскость или CPU. От архитектуры устройства зависят поддерживаемые поля заголовков, порядок и место применения фильтров и вообще перечень трафика, на который распространяются ACL.

В своей классической форме ACL — это упорядоченная последовательность правил, которые проверяют параметры пакета: MAC-адреса, VLAN-теги, IP-адреса, номера портов, протоколы и т. п. На практике возможности платформы ограничены: аппаратные таблицы (например, TCAM) имеют фиксированный объём и нередко не поддерживают все необходимые поля и операции. В результате сложные проверки выносятся в программную плоскость, а часть сопоставлений выполняется аппаратно, только при наличии соответствующих возможностей.

Коммутаторы уровня L2+ фактически занимают промежуточное положение между «чистыми» L2-устройствами и полноценными L3-коммутаторами. За счёт этого пользовательский поток в большинстве случаев обрабатывается аппаратно, тогда как служебные протоколы (ARP, STP, LLDP, DHCP и др.) и специфические пакеты могут отправляться по отдельным, программным путям. Следствие — одно и то же правило ACL может по-разному сработать для разных типов пакетов или вовсе не примениться к некоторым из них.

Поэтому проверка работоспособности и полноты ACL должна сочетать формальный разбор конфигурации с реальными нагрузочными испытаниями. Эксперименты позволяют определить, какие классы трафика действительно блокируются аппаратно, а какие проходят

через устройство, создавая «остаточную» нагрузку на контроллер и CPU. Практическую ценность представляют тест-сценарии с инкапсуляцией, модификацией VLAN-тегов, передачей служебного трафика и моделированием пиковых нагрузок с переключениями между аппаратной и программной обработкой.

Наблюдение и воспроизведение подобных сценариев важно для понимания реальной эффективности базовых ACL на L2+ платформах.

Объект работы — показанные сетевые конфигурации и сводные интерфейсные показатели лабораторного стенда.

Предмет работы — содержание TCP-правил, их назначение интерфейсам и ограничения интерпретации агрегированных показателей нагрузки.

Цель работы — разобрать приведённые команды и сводные значения, разграничив настройку, наблюдение общего счётчика и подтверждение фильтрации заданного потока.

Для достижения цели поставлены следующие задачи:

- Разобрать показанные TCP-ACL и их назначение на Cisco Catalyst 2960 и Eltex MES1428; для MikroTik отдельно описать имеющийся фрагмент настройки bridge;
- Описать указанный авторами способ наблюдения агрегированной нагрузки через SNMP без установления её протокольного состава;
- Сохранить авторские сводные значения T0 и T1, явно указав отсутствие исходных временных рядов и подтверждённого расчёта величин после знака «±»;
- Пересчитать отношения и разности округлённых центральных значений, не трактуя эти вычисления как пакетный эффект фильтрации;
- Указать ограничения сопоставления сценариев и границы использования общего интерфейсного счётчика.

Теоретические предпосылки

Эффективность ACL на L2+ устройствах определяется тем, какие типы кадров и на каком уровне обработки доступны механизму фильтрации.

В документации Cisco подчёркивается разграничение фильтрации IP и non-IP трафика: IP access list применимы только к IP-пакетам, тогда как non-IP трафик (включая ARP) относится к области MAC-фильтрации и требует иных механизмов [1].

Существенным ограничением аппаратной фильтрации является конечный объём аппаратных ресурсов для правил (таблицы ACL/память аппаратной классификации). Для коммутаторов серии Eltex MES в руководстве приведены количественные лимиты ACL-правил для конкретных моделей, включая MES1428 [2].

Для ряда платформ Cisco указывается, что при превышении возможностей аппаратной ACL-фильтрации может использоваться программная фильтрация (software filtering), что сопровождается ростом нагрузки на CPU и потенциальным снижением производительности [3].

Передача пакетов на обработку CPU в терминах Cisco описывается как punt (передача в CPU/slow path) и применяется при невозможности аппаратной обработки отдельных классов трафика [4].

В устройствах MikroTik с аппаратным offload поведение зависит от конфигурации bridge: трафик, проходящий через bridge, по умолчанию может обходить IP firewall, а для принудительной обработки используются отдельные настройки; также описаны правила ACL с перенаправлением трафика в CPU (redirect-to-cpu) [5, 6].

Таким образом, при интерпретации результатов нагрузочного тестирования необходимо разделять: эффект IP-фильтрации, долю non-IP/L2 кадров (например, ARP, RFC 826) и влияние аппаратных лимитов и возможного перехода части обработки в CPU/программную плоскость [7].

Материалы и методы

Техническое оснащение эксперимента

- Три различных коммутатора: Cisco Catalyst 2960, Eltex MES 1428 и MikroTik CRS326-24G-2S+RM;

- Два персональных компьютера: первый формирует сетевой трафик, второй принимает его;
- По описанию авторов, на первом компьютере развёрнут Zabbix [8], регистрирующий интерфейсные счётчики SNMP с интервалом 60 с. Эти показатели усредняются между опросами и не устанавливают кратковременные пики или протокольный состав нагрузки. Расчёт величин после знака «±» в авторской сводке не приложен; интервал опроса сам по себе не подтверждает эти величины.

Порядок работы:

- Базовая настройка оборудования (IP-адресация, проверка связности);
- Генерация интенсивного трафика и фиксация нагрузки на интерфейсах;
- Разбор и применение показанных TCP-правил Cisco и Eltex; фрагмент MikroTik рассматривается как настройка bridge;
- Регистрация показателей на этапе, который авторы описывают как повторную генерацию нагрузки после изменения настроек.

Арифметические соотношения сводных значений

Обозначения: T_0 и T_1 — авторские сводные показатели интерфейсной нагрузки до и после описанных изменений (Мбит/с). При опросе SNMP раз в 60 с это интервальные показатели, а не доказанные кратковременные пики.

- Отношение T_1/T_0 , выраженное в процентах, показывает величину второго сводного показателя относительно первого;
- Разность $T_0 - T_1$ характеризует изменение сводного показателя, Мбит/с;
- Относительное изменение рассчитывается как доля разности $T_0 - T_1$ по отношению к T_0 , выраженная в процентах.

Указанные отношения задают арифметические отношения сводных значений. Производные центральные значения в таблице пересчитаны редакторски по округлённым T_0 и T_1 ; это не новые измерения. Значения после «±» в исходных T_0/T_1 сохранены как авторские, без подтверждения их статистического смысла.

Результаты и обсуждение

Cisco Catalyst 2960

Настройка и применение ACL

Листинги 1 и 2 показывают создание TCP-ACL и его назначение на входящий трафик интерфейса Cisco Catalyst 2960.

Показанные правила запрещают TCP между двумя заданными хостами, затем разрешают остальной IP-трафик. Наличие этих команд само по себе не подтверждает отбрасывание целевых пакетов; агрегированный интерфейсный показатель также не даёт такой проверки.

Листинг 1 – Создание списка ACL на Cisco Catalyst 2960

```
Switch(config)#access-list 105 deny tcp host 192.168.88.3 host 192.168.88.1
Switch(config)#access-list 105 deny tcp host 192.168.88.1 host 192.168.88.3
Switch(config)#access-list 105 permit ip any any
```

Листинг 2 – Назначение ACL на интерфейс Cisco Catalyst 2960

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#ip access-group 105 in
Switch(config-if)#ex
```

Интерфейсная нагрузка Cisco Catalyst 2960

На рисунке 1 приведена авторская диаграмма интерфейсной нагрузки Cisco Catalyst 2960 для этапов, описанных как до и после изменения ACL. Она показывает изменение общего показателя, но не устанавливает, какие пакеты были пропущены или отброшены и чем вызвано изменение.

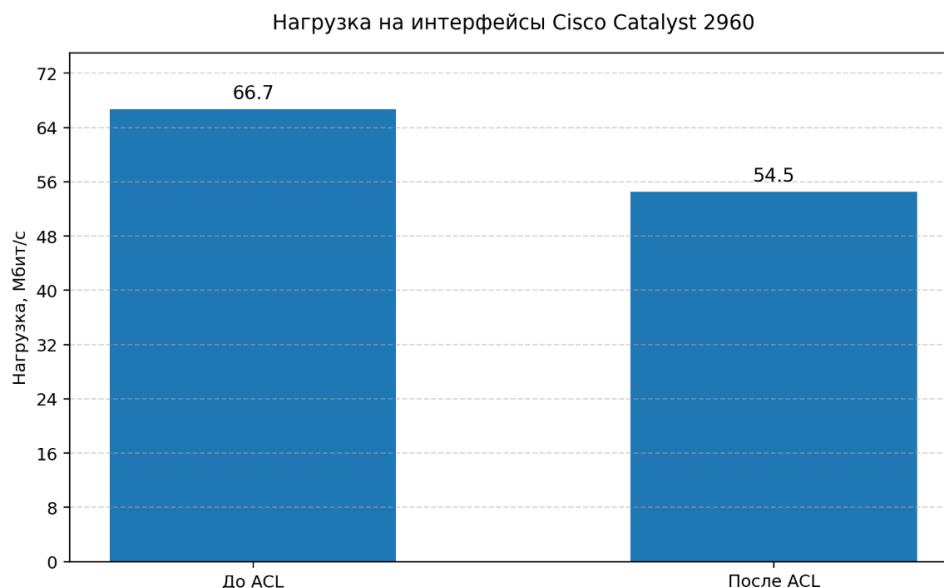


Рис. 1. Интерфейсная нагрузка Cisco Catalyst 2960 до и после изменения конфигурации

Eltex MES1428

Настройка и применение ACL

Листинги 3 и 4 показывают TCP-запреты между двумя хостами, последующее permit ip any any и назначение списка интерфейсу Eltex MES1428. Разрешения отдельных ICMP/TCP-потоков после общего permit ip избыточны для уже разрешённого трафика. Команды сохранены как в исходном примере; пакетная проверка результата не показана.

Листинг 3 – Создание ACL на Eltex MES1428

```
console(config)#ip access-list extended 1001
console(config-ext-nacl)#deny tcp host 192.168.88.1 host 192.168.88.3
console(config-ext-nacl)#deny tcp host 192.168.88.3 host 192.168.88.1
console(config-ext-nacl)#permit ip any any
console(config-ext-nacl)#permit tcp any any
console(config-ext-nacl)#permit icmp any any
```

Листинг 4 – Назначение ACL на интерфейс Eltex MES1428

```
console(config)#interface fastethernet 0/1
console(config-if)#ip access-group 1001 in
console(config-if)#ex
```

Интерфейсная нагрузка Eltex MES1428

Рисунок 2 содержит авторскую диаграмму интерфейсной нагрузки Eltex MES1428 для двух описанных этапов. Раздельных IP/поп-IP-счётчиков и захвата целевого потока нет, поэтому диаграмма не подтверждает уменьшение именно IP-трафика либо сохранение определённого L2-трафика.

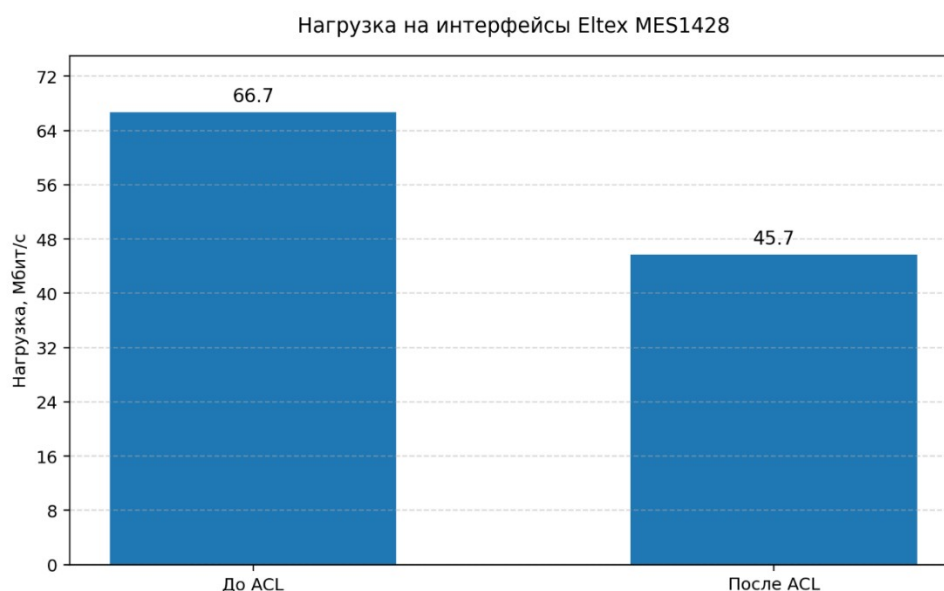


Рис. 2. Интерфейсная нагрузка Eltex MES1428 до и после изменения конфигурации

MikroTik CRS326-24G-2S+RM

Настройка bridge и интерфейсов MikroTik

Листинги 5 и 6 показывают создание bridge и добавление интерфейсов MikroTik. Они не содержат правила ACL или команды его назначения. По этому фрагменту нельзя утверждать, что на MikroTik был выполнен такой же тест ACL, как описан для двух других устройств.

Листинг 5 – Создание bridge и добавление первого интерфейса MikroTik

```
[admin@MikroTik] /interface ethernet switch rule> /interface bridge
[admin@MikroTik] /interface bridge> add name=bridge2
[admin@MikroTik] /interface bridge> /interface bridge port
[admin@MikroTik] /interface bridge port> add bridge=bridge2 interface=ether1
hw=yes learn=no unknown-flood=no
```

Листинг 6 – Добавление второго интерфейса в bridge на MikroTik CRS326

```
[admin@MikroTik] /interface bridge port> add bridge=bridge2 interface=ether2
hw=yes
```

Сводные показатели нагрузки MikroTik

На рисунке 3 сохранены авторские сводные показатели MikroTik для двух этапов. Представленная конфигурация не подтверждает применение ACL, поэтому эти показатели не интерпретируются как результат фильтрации. Исходные ряды и метод расчёта неопределённости отсутствуют; роль bridge или аппаратной обработки по ним не устанавливается.

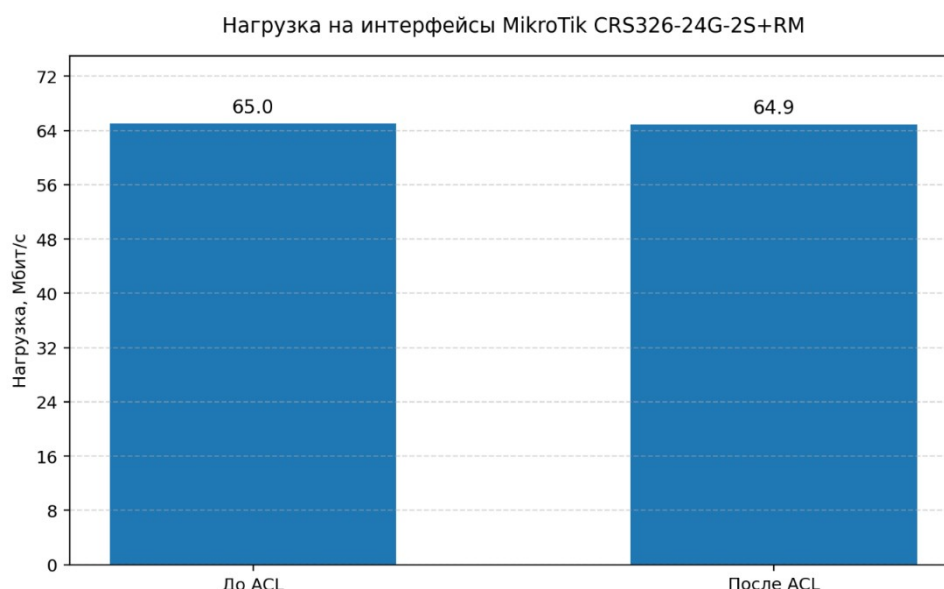


Рис. 3. Авторские сводные показатели интерфейсной нагрузки MikroTik CRS326

Таблица 1 объединяет авторские сводные значения нагрузки и редакторские арифметические расчёты по их округлённым центральным значениям. Это не сопоставимый эксперимент по эффективности фильтрации трёх платформ.

Таблица 1 – Сводные интерфейсные показатели до и после изменения конфигурации

Устройство	T_0 , Мбит/с	T_1 , Мбит/с	T_1/T_0 , %	$T_0 - T_1$, Мбит/с	Изменение, %
Cisco Catalyst 2960	66.7 ± 2.2	54.5 ± 1.8	81.7	12.2	18.3
Eltex MES1428	66.7 ± 2.2	45.7 ± 1.5	68.5	21.0	31.5
MikroTik CRS326-24G-2S+RM	65.0 ± 2.2	64.9 ± 2.2	99.8	0.1	0.2

Границы интерпретации таблицы 1

Cisco Catalyst 2960. Показаны TCP-правила. Изменение общего счётчика не подтверждает эффект фильтрации. Авторские $\pm$ не проверены.

Eltex MES1428. Показаны TCP-правила. Протокольный состав нагрузки не установлен; причинный эффект ACL не подтверждён. Авторские $\pm$ не проверены.

MikroTik CRS326. Показана настройка bridge, без правила ACL. Значения не интерпретируются как эффект фильтрации. Авторские $\pm$ не проверены.

Заключение

Приведённые команды Cisco и Eltex задают запрет определённых TCP-поток и разрешение остального IP-трафика. Показанные фрагменты MikroTik задают bridge и его интерфейсы, но не ACL.

Авторские диаграммы и T_0/T_1 фиксируют сводное описание двух этапов каждого сценария. Исходные ряды счётчиков не приложены; расчёт величин после « $\pm$ » не подтверждён. Поэтому они сохранены как авторские сведения без статистической интерпретации.

Редакторские отношения T_1/T_0 и разности $T_0 - T_1$ вычислены только по округлённым центральным значениям. Они не равны измеренной доле пропущенных пакетов и не доказывают причинный эффект ACL.

Общий интерфейсный счётчик не разделяет IP, ARP и другие протоколы. Ненулевое значение нельзя назвать остаточным L2-трафиком без отдельных счётчиков или захвата.

Сценарии не дают основания ранжировать производителей: одинаковая конфигурация фильтрации для трёх платформ и контроль состава нагрузки не представлены.

Практическая проверка TCP-правила должна отдельно фиксировать прохождение разрешённых и запрещённых целевых пакетов. Здесь этот шаг обозначен как граница материала, а не выполненный результат.

Материал пригоден для учебного разбора команд и ограничений мониторинга. Выводы об аппаратных причинах различий, общей устойчивости ACL и количественной эффективности фильтрации по представленным материалам не делаются.

Библиографический список

1. Cisco. Configuring IPv4 ACLs (разграничение IP ACL и MAC ACL) [Электронный ресурс]. – URL: https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b_ie3500_1718-cg/configuring_ipv4_acls.html (дата обращения: 12.10.2026).
2. Eltex. MES Series User Manual 10.4.2.1 (лимиты ACL для MES1428) [Электронный ресурс]. – URL: https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf (дата обращения: 12.10.2026).
3. Cisco. Configuring IPv4 Access Control Lists на Catalyst 2960L (software filtering при ограничениях аппаратных ресурсов) [Электронный ресурс]. – URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_7_e/configuration_guide/sec/b_1527e_security_2960l_cg/configuring_ipv4_access_control_lists.html (дата обращения: 12.10.2026).
4. Cisco. Configure Punt/Inject and FED Packet Capture (определение punt в CPU) [Электронный ресурс]. – URL: <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-gibraltar-16121/216746-configure-punt-inject-fed-packet-capture.html> (дата обращения: 12.10.2026).
5. MikroTik. L3 Hardware Offloading (ACL redirect-to-cpu и особенности offload) [Электронный ресурс]. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/62390319/L3%2BHardware%2BOffloading> (дата обращения: 12.10.2026).
6. MikroTik. Bridging and Switching (bridge traffic bypass firewall, use-ip-firewall) [Электронный ресурс]. – URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging%2Band%2BSwitching> (дата обращения: 12.10.2026).
7. IETF. RFC 826: An Ethernet Address Resolution Protocol [Электронный ресурс]. – URL: <https://datatracker.ietf.org/doc/html/rfc826> (дата обращения: 12.10.2026).
8. ALT Linux Wiki Установка и первоначальная настройка ZABBIX [Электронный ресурс]. – URL: https://www.altlinux.org/Установка_и_первоначальная_настройка_ZABBIX (дата обращения: 12.10.2026).

References

1. Cisco. (n.d.). *Configuring IPv4 ACLs (distinction between IP ACL and MAC ACL)*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/IOT/switches/ie35xx/sw-config-guide/17-18/b_ie3500_1718-cg/configuring_ipv4_acls.html
2. Eltex. (n.d.). *MES series user manual 10.4.2.1*. Retrieved October 12, 2026, from https://api.prod.eltex-co.ru/storage/upload_center/files/54/MES_Series_user_manual_10.4.2.1_en.pdf
3. Cisco. (n.d.). *Configuring IPv4 access control lists on Catalyst 2960L (software filtering under hardware resource limitations)*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960l/software/15-2_7_e/configuration_guide/sec/b_1527e_security_2960l_cg/configuring_ipv4_access_control_lists.html
4. Cisco. (n.d.). *Configure punt/inject and FED packet capture*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-xe-gibraltar-16121/216746-configure-punt-inject-fed-packet-capture.html>
5. MikroTik. (n.d.). *L3 hardware offloading*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/62390319/L3%2BHardware%2BOffloading>
6. MikroTik. (n.d.). *Bridging and switching*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging%2Band%2BSwitching>
7. Plummer, D. C. (1982). *An Ethernet address resolution protocol (RFC 826)*. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/html/rfc826>
8. ALT Linux Wiki. (n.d.). *Installation and initial configuration of Zabbix*. Retrieved October 12, 2026, from https://www.altlinux.org/Установка_и_первоначальная_настройка_ZABBIX

Информация об авторах

Коваль Николай Михайлович — студент факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; e-mail: nik.koval_10@mail.ru.

Гимпель Евгений Анатольевич — студент факультета комплексной безопасности топливно-энергетического комплекса ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И. М. Губкина», Москва, Россия; для переписки — через соавтора Н. М. Ковалья: nik.koval_10@mail.ru.

LABORATORY ANALYSIS OF TCP ACLS AND INTERFACE METRICS IN A NETWORK TESTBED

Koval N. M.¹, Gimpel E. A.¹

¹ Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia

Abstract. This paper presents a teaching-oriented analysis of network configuration fragments and the authors' summary of interface measurements from a laboratory testbed. It considers Cisco Catalyst 2960, Eltex MES1428, and MikroTik CRS326. The objective is to relate the commands actually shown to the limits of aggregate-counter interpretation, without treating a counter change as verified filtering of a particular traffic flow. The Cisco and Eltex configurations deny TCP between two specified hosts and then permit other IP traffic; they do not impose a general IP-packet ban. The MikroTik fragments create a bridge and add interfaces, but show neither an ACL rule nor its attachment. The authors describe SNMP monitoring in Zabbix with a sixty-second polling interval. These measurements average traffic over the interval and cannot identify protocol composition or brief peaks. The reported before-and-after load values are retained, while derived ratios are recalculated from their rounded central values. These calculations characterize summary numbers rather than the proportion of packets actually forwarded. Raw time series and the calculation of the authors' plus-or-minus quantities are unavailable, so their statistical interpretation is not established. The material supports discussion of TCP rules, interface attachment, and the distinction between configuration, aggregate observation, and evidence of a filtering effect. It does not compare vendors or establish the composition of residual load or hardware causes of differences.

Keywords: TCP; ACL; switch; SNMP; interface counter; laboratory testbed.

Information about the authors

Nikolai Mikhailovich Koval — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: nik.koval_10@mail.ru.

Evgeny Anatolyevich Gimpel — student, Faculty of Integrated Security of the Fuel and Energy Complex, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence via co-author N. M. Koval: nik.koval_10@mail.ru.