

Аристархова А. А., Чеков М. В.

Российский государственный университет нефти и газа (национальный исследовательский университет)
имени И. М. Губкина, Москва, Россия

ЛАБОРАТОРНЫЙ РАЗБОР SWITCH SPOOFING И DOUBLE TAGGING В КОНФИГУРАЦИИ ROUTER-ON-A-STICK НА CISCO

Аннотация. В статье описана настройка Router-on-a-Stick с маршрутизатором Cisco 1941 и коммутатором Cisco Catalyst 2960, а также два лабораторных эпизода с Yersinia: Switch Spoofing и Double Tagging. Текст фиксирует конфигурацию VLAN и транкового соединения, подключение атакующего узла и показанные в рукописи кадры и состояния портов. Эксперименты относятся к указанному стенду Cisco; таблица с конфигурациями Eltex и MikroTik содержит справочные настройки, но не результаты атак на этих устройствах. Работа не представляет контролируемого сравнения производителей, не сообщает повторность опытов и не измеряет общий уровень защищенности архитектуры Router-on-a-Stick. Практические рекомендации по Cisco ограничены ручной настройкой trunk/access-портов, отключением DTP там, где оно не требуется, контролем разрешенных VLAN и выбором выделенной native VLAN с учетом совместимости устройств. Double Tagging связан с условиями обработки тегов и native VLAN, поэтому его нельзя считать неизбежным следствием самого Router-on-a-Stick. Результаты иллюстрируют конкретный случай и не подтверждают поведение иных моделей или прошивок. В работе не сравниваются разные версии ПО, не приводятся повторные контрольные серии и не оцениваются эксплуатационные риски для иной топологии. Снимки фиксируют отдельные моменты настройки и передачи пакетов; их недостаточно для оценки вероятности успешного повторения атаки, влияния нагрузки или устойчивости конфигурации после перезапуска оборудования. Настройки сопоставлялись с IEEE 802.1Q и документацией производителей коммутаторов и маршрутизатора.

Ключевые слова: Router-on-a-Stick, Cisco Catalyst, VLAN, DTP, Switch Spoofing, Double Tagging.

Введение

Крупные организации используют VLAN для логической сегментации сети. Межвлановая маршрутизация позволяет организовать обмен между сегментами согласно заданной политике; один из вариантов — Router-on-a-Stick с субинтерфейсами маршрутизатора на trunk-соединении.

В работе описывается конфигурация Router-on-a-Stick на оборудовании Cisco и два сценария, показанных авторами на этом стенде. Возможность атак зависит от настроек конкретного порта, протоколов согласования и обработки тегов; она не является неизбежным свойством архитектуры.

Ошибочная настройка VLAN и trunk-портов может создавать условия для атак канального уровня. Такая возможность зависит от конкретной конфигурации, используемых протоколов и топологии; архитектура Router-on-a-Stick сама по себе не означает автоматической уязвимости.

Актуальность работы — в описании конкретного Cisco-стенда и двух показанных сценариев. Полученные наблюдения не переносятся на все реализации межвлановой маршрутизации.

Объект исследования: конфигурация Router-on-a-Stick на указанном лабораторном стенде Cisco.

Предмет исследования: условия выполнения Switch Spoofing и Double Tagging в данной конфигурации и настройки trunk/VLAN, показанные в материалах опыта.

Цель работы: описать конфигурацию Router-on-a-Stick на Cisco и зафиксировать результаты двух лабораторных проверок, ограничив выводы наблюдениями конкретного стенда.

Материалы и методы

Router-on-a-Stick использует один физический интерфейс маршрутизатора и логические субинтерфейсы, сопоставленные с VLAN. Безопасность зависит от настроек маршрутизатора и коммутатора. В исходных материалах приводилось процентное утверждение о влиянии

Рубрика 2. Методы и системы защиты информации, информационная безопасность

коммутатора, однако экспериментальных данных для его проверки нет; здесь оно не используется.

Работа рассматривает два отдельных Cisco-сценария без универсальных выводов о защищённости архитектуры.

Исследовательские методы включали анализ конфигурации лабораторного стенда Cisco, выполнение двух учебных сценариев и изучение представленных захватов Wireshark. Единого сравнительного протокола для разных производителей, повторных измерений и оценки статистической значимости в исходных данных нет.

Эмпирическая часть охватывала маршрутизатор Cisco 1941, коммутатор Cisco Catalyst 2960 и рабочие станции Linux. Таблица 1 дополнительно содержит конфигурационные фрагменты Eltex и MikroTik, но атаки и защитные меры на этих платформах не представлены как результаты. Настройки сопоставлялись с IEEE 802.1Q и документацией производителей коммутаторов и маршрутизатора [1–7].

Испытания охватывали два сценария на Cisco: Switch Spoofing и Double Tagging. Изменение подключений и отсутствие общего контрольного протокола не позволяют трактовать их как сравнение производителей.

Практическая часть

Практическая часть описывает маршрутизатор Cisco 1941 и коммутатор Cisco Catalyst 2960. Испытания двух сценариев проводились на оборудовании Cisco. Примеры конфигураций других производителей приведены справочно и не считаются результатами тестирования.

Схема лабораторной сети Router-on-a-Stick представлена на рис. 1.

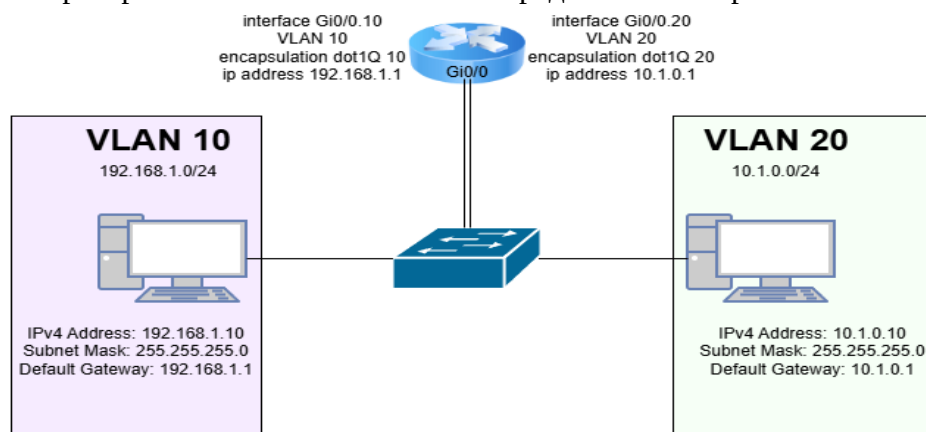


Рис. 1. Схема маршрутизации между VLAN 10 и VLAN 20 по технологии Router-on-a-Stick

Оборудование лабораторного стенда:

- коммутаторы Cisco Catalyst 2960, Eltex MES1428 и MikroTik;
- Маршрутизатор Cisco 1941;
- Рабочие станции под управлением операционной системы Linux;
- Ethernet-кабели.

Последовательность настройки:

В эксперименте использовали маршрутизатор Cisco 1941 и коммутатор Cisco Catalyst 2960. Примеры для других производителей в таблице 1 носят справочный характер. Для анализа архитектуры использованы материалы IEEE 802.1Q и документация производителей [1–7].

Конфигурация маршрутизатора Cisco 1941 приведена в листинге 1.

Листинг 1 – Пример конфигурации субинтерфейсов маршрутизатора Cisco 1941

```
Router> enable
Router# config t
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/0.10
Router(config-if)# encapsulation dot1Q 10
```

```
Router(config-if)# ip address 192.168.1.1 255.255.255.0
Router(config-if)# exit
Router(config)# interface gigabitEthernet 0/0.20
Router(config-if)# encapsulation dot1Q 20
Router(config-if)# ip address 10.1.0.1 255.255.255.0
Router(config-if)# exit
```

Таблица 1 содержит конфигурационные фрагменты для Cisco Catalyst 2960, Eltex MES1428 и MikroTik. Эти примеры иллюстрируют настройки VLAN и не означают, что описанные далее атаки были испытаны на Eltex или MikroTik.

Таблица 1 – Примеры настройки VLAN на Cisco, Eltex и MikroTik

Cisco 2960	Eltex mes1428	Mikrotik
enable config t vlan 10 name A vlan 20 name M exit interface range Fa0/1-4 description CLI switchport mode access switchport access vlan 10 exit interface range Fa0/15-18 description SERV switchport mode access switchport access vlan 20 exit interface Fa0/9 description LINK switchport mode trunk exit	enable configure terminal vlan 10 name A exit vlan 20 name M exit interface range fastEthernet 1/0/1-4 description CLI switchport mode access switchport access vlan 10 exit interface range fastEthernet 1/0/15-18 description SERV switchport mode access switchport access vlan 20 exit interface fastEthernet 1/0/9 description LINK switchport mode trunk exit	/interface bridge add name=bridge1 vlan-filtering=yes /interface bridge port add bridge=bridge1 interface=ether1 add bridge=bridge1 interface=ether2 add bridge=bridge1 interface=ether3 add bridge=bridge1 interface=ether4 add bridge=bridge1 interface=ether15 add bridge=bridge1 interface=ether16 add bridge=bridge1 interface=ether17 add bridge=bridge1 interface=ether18 add bridge=bridge1 interface=ether9 /interface bridge vlan add bridge=bridge1 tagged=ether9 untagged=ether1,ether2,ether3,ether4 vlan-ids=10 add bridge=bridge1 tagged=ether9 untagged=ether15,ether16,ether17,ether18 vlan-ids=20

Далее рассматриваются только два сценария, выполненные на Cisco: Switch Spoofing и Double Tagging. Анализ ограничен представленными результатами работы Yersinia и Wireshark.

В первом сценарии тестовый узел Kali Linux был подключён к Cisco, после чего с помощью Yersinia передавались DTP-кадры. На рис. 2 представлена изменённая топология, на рис. 3 — выполнение сценария, а в листинге 2 — состояние портов. Автоматическое согласование trunk зависит от режима DTP конкретного интерфейса.

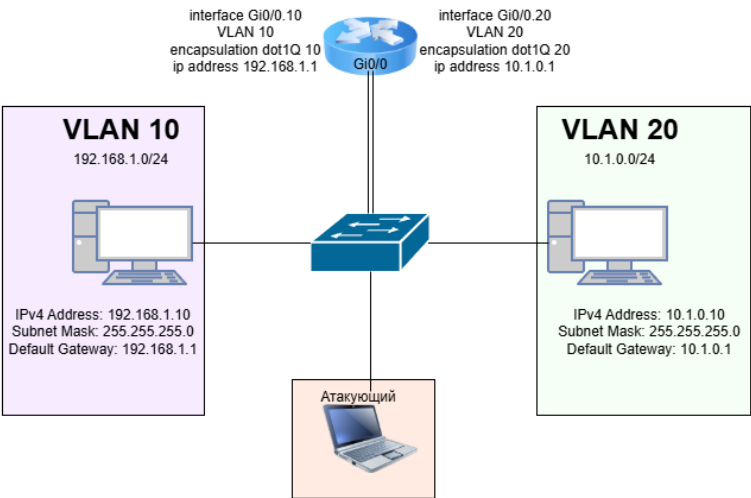


Рис. 2. Подключение тестового узла к коммутатору Cisco в лабораторной топологии

Рубрика 2. Методы и системы защиты информации, информационная безопасность

В листинге 2 интерфейс Fa0/11 отображается в режиме trunk. Возможность Switch Spoofing зависит от динамической настройки соединения. На пользовательских портах Cisco её следует отключать, если она не требуется; в работе этот сценарий на Eltex и MikroTik не испытывался.

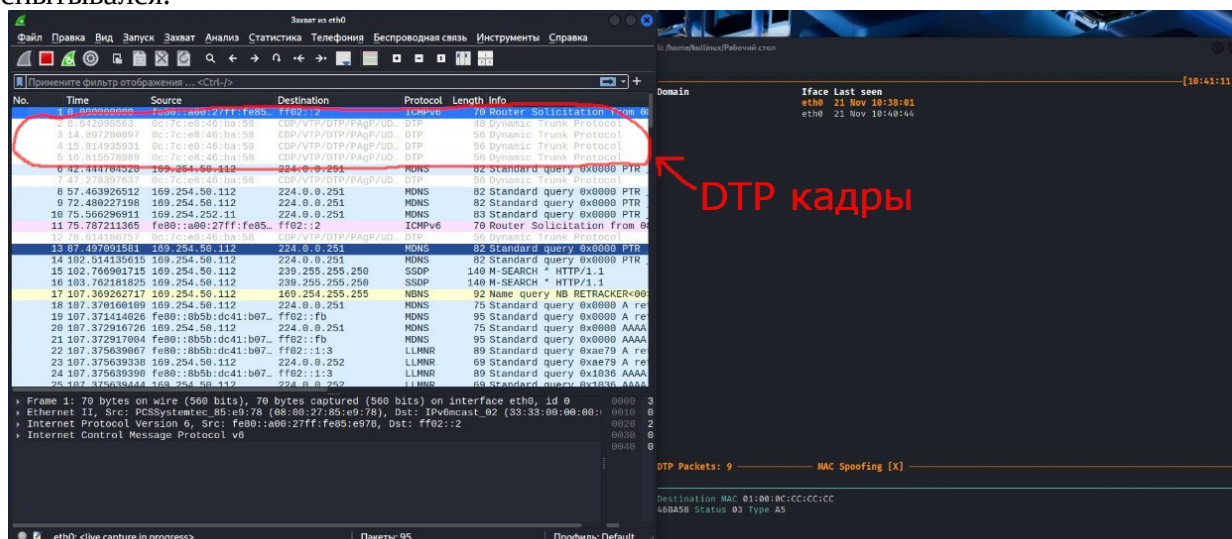


Рис. 3. Выполнение сценария Switch Spoofing и наблюдение DTP-кадров

DTP относится к представленному сценарию Cisco. Это наблюдение не устанавливает отсутствие других вариантов VLAN hopping на иных платформах и не является сравнительным испытанием производителей.

Листинг 2 – Вывод show interfaces status на Cisco Catalyst 2960

Switch>show int status

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1	ANNA	connected	10	auto	auto	10/100BaseTX
Fa0/2	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/3	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/4	ANNA	notconnect	10	auto	auto	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9	LINK	connected	trunk	a-full	a-100	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX
Fa0/11		connected	trunk	a-full	a-100	10/100BaseTX
Fa0/12		notconnect	1	auto	auto	10/100BaseTX
Fa0/13		notconnect	1	auto	auto	10/100BaseTX
Fa0/14		notconnect	1	auto	auto	10/100BaseTX
Fa0/15	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/16	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/17	MAX	connected	20	a-full	a-100	10/100BaseTX
Fa0/18	MAX	notconnect	20	auto	auto	10/100BaseTX
Fa0/19		notconnect	1	auto	auto	10/100BaseTX
Fa0/20		notconnect	1	auto	auto	10/100BaseTX
Fa0/21		notconnect	1	auto	auto	10/100BaseTX
Fa0/22		notconnect	1	auto	auto	10/100BaseTX
Fa0/23		notconnect	1	auto	auto	10/100BaseTX
Fa0/24		notconnect	1	auto	auto	10/100BaseTX
Gi0/1		notconnect	1	auto	auto	10/100/1000BaseTX
Gi0/2		notconnect	1	auto	auto	10/100/1000BaseTX

Во втором сценарии на Cisco проверяли Double Tagging с использованием двух тегов VLAN. Условия прохождения кадров зависят от VLAN атакующего, native VLAN, параметров trunk и обработки тегов; сама архитектура Router-on-a-Stick недостаточна для вывода об успешности атаки.

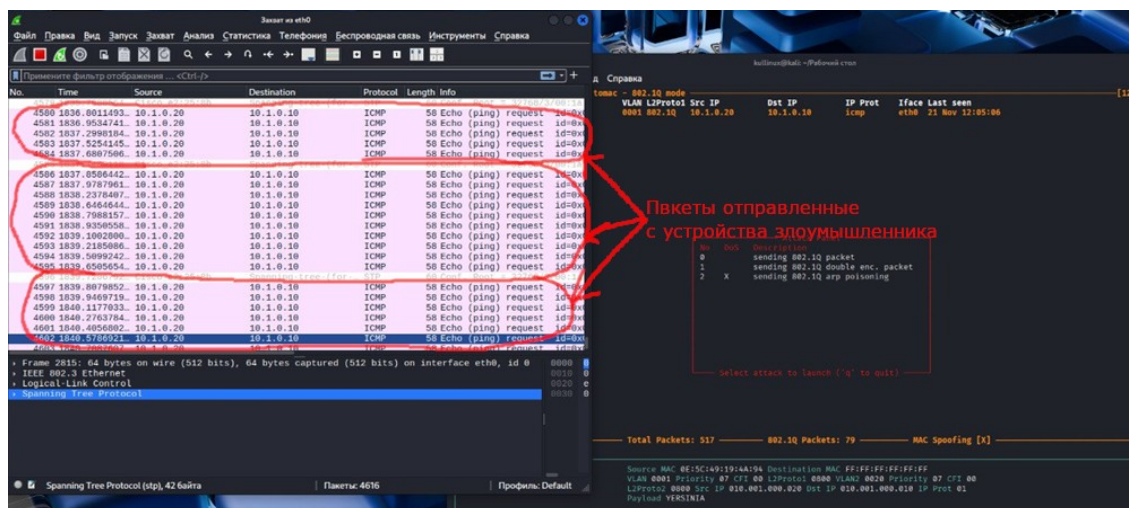


Рис. 4. Выполнение сценария Double Tagging

В описанном эпизоде кадр передавался через trunk-соединение. Дальнейшая обработка зависит от параметров native VLAN и конфигурации маршрутизатора и коммутатора. Представленные данные относятся к указанному стенду.

На рис. 5 представлен захват Wireshark, который авторы интерпретируют как доставку тестового пакета в VLAN 20. Повторные измерения и полный сетевой путь пакета в материалах не представлены.

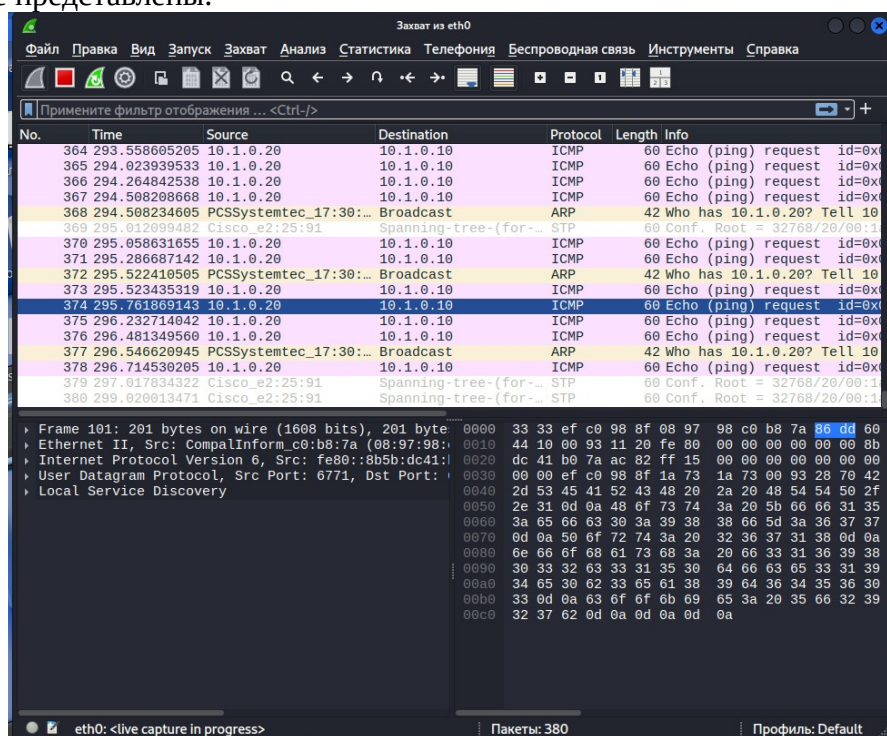


Рис. 5. Захват тестовых сетевых пакетов в Wireshark

Представленный захват авторы интерпретируют как успешную передачу в целевой сегмент в одном запуске. Он не позволяет оценить частоту успеха или перенести результат на другие модели и конфигурации.

В таблице 2 собраны рекомендации по настройке с указанием границ применимости. В работе непосредственно проверялись только конфигурация и сценарии Cisco; сведения по другим платформам не являются экспериментально подтверждёнными результатами.

Рубрика 2. Методы и системы защиты информации, информационная безопасность

Таблица 2 – Меры снижения рисков Switch Spoofing и Double Tagging

	Cisco Catalyst 2960	Eltex MES1428	MikroTik
Switch Spoofing	На пользовательских портах явно задать access. Для статического trunk применять switchport mode trunk и при отсутствии необходимости в DTP — switchport nonegotiate; соседний порт настроить вручную [2, 3].	В работе не проверены поведение DTP и эффективность противодействия на Eltex. Требуется руководство для конкретной модели и версии ПО [6].	Сценарий Switch Spoofing на MikroTik не испытывался; отсутствие Cisco DTP не подтверждает отсутствие иных атак VLAN hopping [5].
Double Tagging	Явно настроить native VLAN, исключить пользовательские access-порты из неё и ограничить разрешённые VLAN. Возможность тегирования native VLAN зависит от платформы [2, 4].	Double Tagging на Eltex не проверялся. Меры следует выбирать по документации модели и подтверждать испытанием trunk-конфигурации [6].	Double Tagging на MikroTik не проверялся. Вывод об отсутствии уязвимостей по этим материалам не делается [5].

Для MikroTik приведены справочные параметры bridge/VLAN. Отсутствие DTP Cisco не доказывает отсутствия иных атак VLAN hopping или полной защищённости платформы. В данной работе атаки на MikroTik не проводились.

Заключение

На лабораторном стенде Cisco представлены конфигурация Router-on-a-Stick и два сценария исследования VLAN hopping. Работа не является сравнительной оценкой производителей или исчерпывающим исследованием архитектуры.

Доступные наблюдения показывают переход указанного интерфейса Cisco в trunk и захват тестового трафика, интерпретированный авторами как Double Tagging. Эти фрагменты не подтверждают универсальную уязвимость технологии или свойства других платформ.

Рекомендации ниже относятся к конфигурации Cisco и требуют проверки на конкретной модели, версии ПО и топологии.

Основные рекомендации:

- На пользовательских портах следует явно задавать режим access и отключать динамическое согласование trunk там, где оно не требуется [3];
- Для статически настроенного Cisco trunk документация указывает возможность отключить DTP командой switchport nonegotiate; соседний интерфейс также настраивают вручную [2];
- Native VLAN и список разрешённых VLAN следует задавать явно; не следует без необходимости размещать пользовательские устройства в native VLAN. Меры против Double Tagging зависят от платформы и топологии; Cisco описывает отдельные варианты снижения риска [4, 5].

Возможные направления дальнейших исследований:

- Исследование устойчивости архитектуры Router-on-a-stick к комбинированным атакам;
- Анализ безопасности альтернативных методов межвлановой маршрутизации;
- Разработка автоматизированных сценариев защиты и обнаружения атак на уровне управления сетью.

Библиографический список

1. IEEE. IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks (IEEE 802.1Q-2022) [Электронный ресурс]. URL: <https://standards.ieee.org/ieee/802.1Q/10323/> (дата обращения: 12.10.2026).
2. Cisco. Configure VLAN Trunking, Cisco IOS XE 17 [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/lyr2-fwd/vlan/vlan-configuration-guide/configure-vlan-trunks.html> (дата обращения: 12.10.2026).

3. Cisco. Catalyst 2960 configuration guide: Configuring VLAN Trunks [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_3_e/consolidated_guide/b_1523e_2960p_2960c_cg/b_1522e_2960_2960c_2960s_2960sf_2960p_cg_chapter_01101.html (дата обращения: 12.10.2026).
4. Cisco. Campus Network for High Availability Design Guide: Preventing Double 802.1Q Encapsulated VLAN Hopping [Электронный ресурс]. URL: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html (дата обращения: 12.10.2026).
5. MikroTik. Bridge VLAN Table: RouterOS Documentation [Электронный ресурс]. URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/28606465/Bridge%20VLAN%20Table> (дата обращения: 12.10.2026).
6. Eltex. MES: настройка порта коммутатора в режиме Trunk [Электронный ресурс]. URL: <https://docs.eltex-co.ru/pages/viewpage.action?pageId=619644036> (дата обращения: 12.10.2026).
7. Cisco. Configure Inter-VLAN Routing with the Use of an External Router [Электронный ресурс]. URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html> (дата обращения: 12.10.2026).

References

1. IEEE. (2022). *IEEE Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks* (IEEE 802.1Q-2022). Retrieved October 12, 2026, from <https://standards.ieee.org/ieee/802.1Q/10323/>.
2. Cisco. (n.d.). *Configure VLAN Trunking, Cisco IOS XE 17*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/td/docs/switches/lan/c9000/lyr2-fwd/vlan/vlan-configuration-guide/configure-vlan-trunks.html>.
3. Cisco. (n.d.). *Catalyst 2960 configuration guide: Configuring VLAN Trunks*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/15-2_3_e/consolidated_guide/b_1523e_2960p_2960c_cg/b_1522e_2960_2960c_2960s_2960sf_2960p_cg_chapter_01101.html.
4. Cisco. (n.d.). *Campus Network for High Availability Design Guide: Preventing Double 802.1Q Encapsulated VLAN Hopping*. Retrieved October 12, 2026, from https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html.
5. MikroTik. (n.d.). *Bridge VLAN Table: RouterOS Documentation*. Retrieved October 12, 2026, from <https://help.mikrotik.com/docs/spaces/ROS/pages/28606465/Bridge%20VLAN%20Table>.
6. Eltex. (n.d.). *MES: Configuring a switch port in Trunk mode*. Retrieved October 12, 2026, from <https://docs.eltex-co.ru/pages/viewpage.action?pageId=619644036>.
7. Cisco. (n.d.). *Configure Inter-VLAN Routing with the Use of an External Router*. Retrieved October 12, 2026, from <https://www.cisco.com/c/en/us/support/docs/lan-switching/inter-vlan-routing/14976-50.html>.

Информация об авторах

Аристархова А. А. — студентка 3 курса факультета комплексной безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; e-mail: anya_aristarkhova906@mail.ru.

Чеков М. В. — студент 3 курса факультета комплексной безопасности топливно-энергетического комплекса Российского государственного университета нефти и газа (НИУ) имени И. М. Губкина, Москва, Россия; для корреспонденции через соавтора А. А. Аристархову: anya_aristarkhova906@mail.ru.

SWITCH SPOOFING AND DOUBLE TAGGING IN A CISCO ROUTER-ON-A-STICK LABORATORY CASE

Aristarkhova A. A., Chekov M. V.

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

Abstract. *This article describes a Router-on-a-Stick configuration using a Cisco 1941 router and Cisco Catalyst 2960 switch, together with two laboratory episodes using Yersinia: Switch Spoofing and Double Tagging. It records the*

Рубрика 2. Методы и системы защиты информации, информационная безопасность

VLAN and trunk configuration, connection of the attacker host, and packet and port states shown in the manuscript. The experiments concern the stated Cisco setup; a table containing Eltex and MikroTik configurations provides setup examples, not attack results for those devices. The work is not a controlled vendor comparison, reports no repeated trials, and does not measure the overall security of the Router-on-a-Stick architecture. Cisco-focused recommendations are limited to explicit trunk and access port configuration, disabling DTP where it is unnecessary, controlling allowed VLANs, and choosing a dedicated native VLAN subject to device compatibility. Double Tagging depends on tag processing and native-VLAN conditions and should not be treated as an inevitable consequence of Router-on-a-Stick itself. The results illustrate one case and do not establish behavior on other models or software versions. The study does not compare software releases, provide repeated control trials, or assess operational risk in other topologies. Configuration examples were checked against IEEE 802.1Q and the switch and router vendors' documentation [1–7].

Keywords: Router-on-a-Stick, Cisco Catalyst, VLAN, DTP, Switch Spoofing, Double Tagging.

Information about the authors

Aristarkhova A. A. — third-year 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: anya_aristarkhova906@mail.ru.

Chekov M. V. — third-year 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 A. A. Aristarkhova: anya_aristarkhova906@mail.ru.