

Ляхова М. В., Сеникова Н. Г.

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

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ RSTP С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА ROOT GUARD НА L2+ УСТРОЙСТВАХ

Аннотация. В статье рассматривается учебный сценарий изменения корневого моста в коммутируемой сети и применение Root Guard для ограничения такого изменения. Цель работы состоит в разборе наблюдений лабораторного стенда и формулировании проверяемого порядка настройки защиты, а не в сравнении производительности оборудования. Исходный стенд включает рабочие станции, коммутаторы Cisco 2960 SI, Eltex MES1428 и устройство MikroTik; для генерации управляющих кадров используется Yersinia. В работе сохранены схемы трех подключений, адресные части идентификаторов корня до и после воздействия, отдельные ответы ring и фрагменты служебного вывода. Эти материалы показывают состояния конкретных узлов и позволяют обсудить изменение выбора корня, но не устанавливают единую временную последовательность всех событий. Авторы также приводят таблицу наблюдений при включенной защите, в которой адресные части идентификаторов остаются неизменными. Такой результат рассматривается как ограниченное наблюдение стенда, поскольку полный журнал настроек и переходов портов не представлен. Документированное поведение Root Guard отделено от наблюдаемых результатов; приведены примеры настройки и диагностики для Cisco IOS и RouterOS с явными условиями применимости. Время восстановления, загрузка процессора, длительность разрыва связи и потери во время защитного блокирования не измерялись и не используются в выводах. Практическая ценность материала заключается в последовательном разделении исходного состояния, воздействия, проверки идентификатора корня и проверки состояния защищенного порта. Полученные выводы относятся к учебному сценарию и не подтверждают универсальную защиту от всех атак канального уровня.

Ключевые слова: RSTP; Root Guard; корневой мост; BPDU; коммутируемая сеть; учебный стенд.

Введение

Протоколы семейства Spanning Tree формируют беспетлевую активную топологию сети Ethernet. RSTP возник как расширение с ускоренной реконфигурацией дерева; назначение стандарта описано IEEE [1]. Базовые состояния порта — discarding, learning и forwarding; выбор корня зависит от сравнения идентификаторов мостов и параметров пути [2]. Возможность передачи более предпочтительного BPDU делает выбор корня зависимым от доверия к подключенному сегменту. Само получение роли корня не доказывает перехват всего пользовательского трафика: путь передачи определяется топологией и ролями портов.

Root Guard позволяет задать административную границу, через которую не должен появляться более предпочтительный корень. В реализации Cisco прием superior BPDU на защищенном порту вызывает root-inconsistent и блокирование передачи через этот порт; после прекращения таких BPDU восстановление происходит автоматически [3]. Поэтому сохранение положения корня и непрерывная доступность всех узлов — разные свойства. Цель статьи — разобрать имеющийся учебный пример и показать, какие наблюдения необходимы для корректной интерпретации защиты.

Материалы и методы

Использованный лабораторный стенд включает рабочие станции PC1, PC2 и PCA и коммутаторы Cisco 2960 SI, Eltex MES1428 и MikroTik. Модель MikroTik и версии программного обеспечения не указаны. Схемы стенда приведены на рис. 1–4. На отдельных схемах для рабочей станции используются обозначения PC3 и PCA; далее PCA означает атакующий узел, однако тождество этих обозначений во всех конфигурациях не подтверждено. Показанные IP-адреса 192.168.1.1–192.168.1.3 относятся к одному диапазону адресации; исходное описание отдельных подсетей не подтверждено приведёнными настройками.

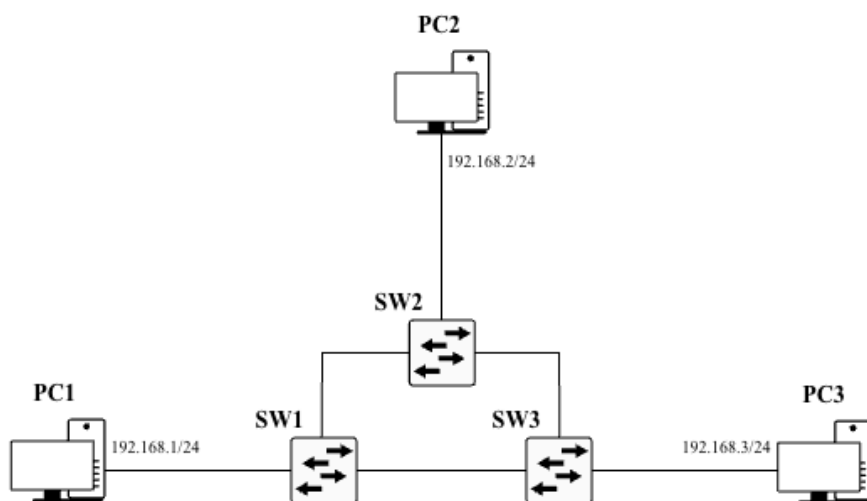


Рис. 1. Общая схема стенда: рабочие станции PC1–PC3 и коммутаторы SW1–SW3

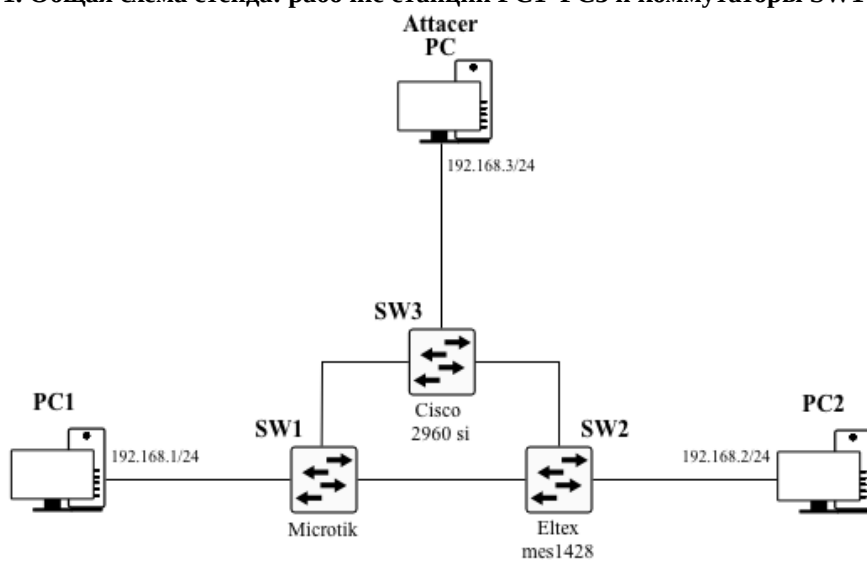


Рис. 2. Первый вариант соединения коммутаторов MikroTik, Eltex и Cisco

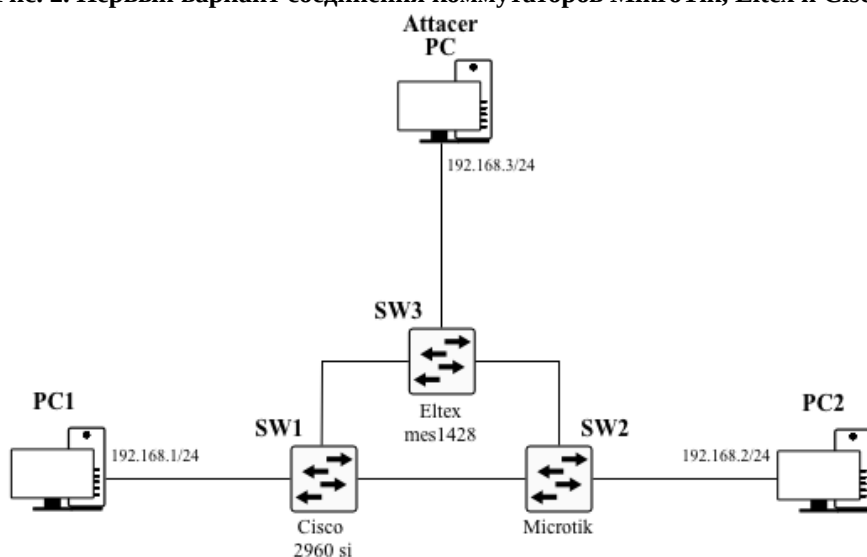


Рис. 3. Второй вариант соединения коммутаторов Cisco, MikroTik и Eltex

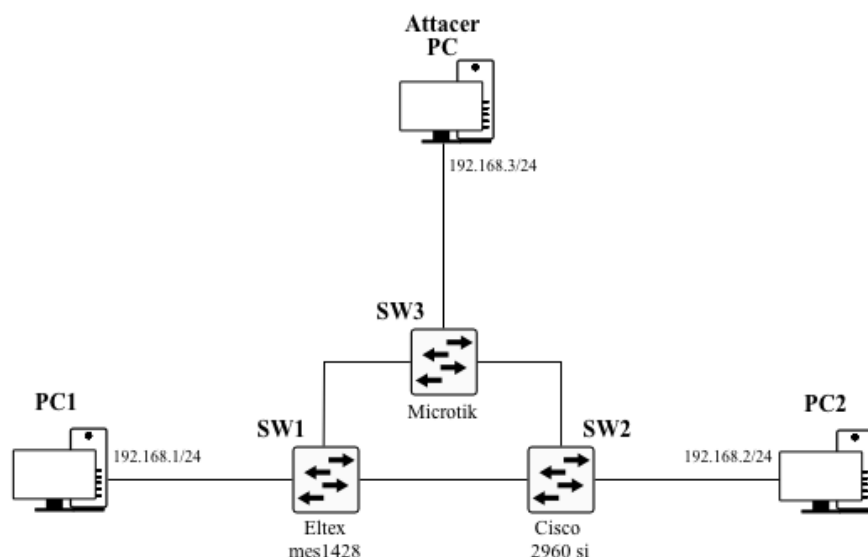


Рис. 4. Третий вариант соединения коммутаторов Eltex, Cisco и MikroTik

Для формирования управляющего трафика применялась утилита Yersinia. Реализованные в ней протокольные сценарии описаны в репозитории разработчиков [4], а способ запуска и перечень поддерживаемых протоколов — в справочнике Kali Linux [5]. Версия программы, параметры генерируемых BPDU и данные о повторных запусках не приведены. Поэтому ниже сопоставляются только наблюдаемые состояния устройств и сообщённые значения; причинное сравнение производителей и статистическая оценка эффективности не выполняются.

Перед воздействием были выполнены короткие проверки ping. В листингах 1–3 сохранены количество пакетов и время ответа. Один или два ответа не позволяют оценить долговременную доступность сети и не отражают потери во время воздействия.

Листинг 1 – Исходная проверка адреса 192.168.1.1

```

ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.843 ms
^C
--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.843/0.843/0.843/0.000 ms
  
```

Листинг 2 – Исходная проверка адреса 192.168.1.2

```

ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.052 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.046 ms
^C
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1028ms
rtt min/avg/max/mdev = 0.046/0.049/0.052/0.003 ms
  
```

Листинг 3 – Исходная проверка адреса 192.168.1.3

```

ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=2.97 ms
^C
--- 192.168.1.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.974/2.974/2.974/0.000 ms
  
```

Результаты

В таблице 1 представлены адресные части Root ID до и после воздействия при отключённой защите. Приоритет моста не приведён, поэтому полный Bridge ID по этим значениям восстановить нельзя. Три наблюдения не следует трактовать как синхронные состояния одной инстанции дерева: в отдельных выводах устройства независимо показывают

себя корнем. Без временных меток и полного протокольного журнала можно установить лишь сообщённое изменение адресной части идентификатора, но нельзя однозначно связать его с определённым поддельным BPDU.

Таблица 1 – Адресные части идентификатора корня до и после воздействия без защиты

Наблюдение	До воздействия	После воздействия
1	2401.c735.5780	e4:5a:d4:9a:40:40
2	e4:5a:d4:9a:40:40	C4:AD:34:03:6F:2A
3	C4:AD:34:03:6F:2A	2401.c735.5780

В листингах 4–6 приведены фрагменты консольного вывода коммутаторов. Сообщения This bridge is the root и root-bridge: yes характеризуют состояние соответствующего устройства, но не подтверждают получение атакующей станцией роли корня. В выводе Eltex указан MSTP, что дополнительно ограничивает трактовку всех эпизодов как работы в едином режиме RSTP.

Листинг 4 – Фрагмент состояния дерева STP на Cisco

```
Spanning tree enabled protocol rstp
Root ID      Priority      32868
             Address      2401.c735.5780
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
Bridge ID    Priority      32868 (priority 32768 sys-id-ext 100)
             Address      2401.c735.5780
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300 sec
Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/7        Desg FWD 19         128.7    P2p
Fa0/13       Desg FWD 19         128.13   P2p
Fa0/17       Desg FWD 19         128.17   P2p
```

Листинг 5 – Фрагмент состояния дерева STP на Eltex

```
console#show spanning-tree
Root Id      Priority      32768
             Address      e4:5a:d4:9a:40:40
             Cost          0
             Port          0 [0]
             This bridge is the root
             Max age 0 sec Forward delay 0 sec Hello time 0 sec
             Hello Time 2 sec 0 cs

MST00
MST00 is executing the mstp compatible Multiple Spanning Tree Protocol
Bridge Id    Priority      32768
             Address      e4:5a:d4:9a:40:40
             Max age 0 sec Forward delay 0 sec Hello time 0 sec
             Hello Time 2 sec 0 cs
```

Листинг 6 – Фрагмент состояния моста на MikroTik

```
[admin@MikroTik] /interface bridge port> /interface bridge monitor bridge
;;; defconf
state: enabled
current-mac-address: C4:AD:34:03:6F:2A
root-bridge: yes
root-bridge-id: 0x8000.C4:AD:34:03:6F:2A
root-path-cost: 0
root-port: none
port-count: 26
designated-port-count: 1
fast-forward: no
```

В листинге 7 представлены сообщения Destination Host Unreachable. Они фиксируют недоступность узла в отдельный момент времени, однако продолжительность и непосредственная причина отказа на основании этого фрагмента не устанавливаются.

Листинг 7 – Фрагмент сообщений о недоступности узла

```
From 192.168.1.2 icmp_seq=1 Destination Host Unreachable
From 192.168.1.2 icmp_seq=2 Destination Host Unreachable
```

From 192.168.1.2 icmp_seq=3 Destination Host Unreachable

В таблице 2 приведены значения идентификатора корня при включённой защите: адресная часть остаётся неизменной. Для этих наблюдений отсутствуют полные команды настройки Root Guard и журнал переходов защищённых портов. Поэтому неизменность идентификатора не доказывает переход всех устройств в root-inconsistent и не подтверждает непрерывность пользовательского обмена.

Таблица 2 – Адресные части идентификатора корня до и после воздействия при защите

Наблюдение	До воздействия	После воздействия
1	2401.c735.5780	2401.c735.5780
2	e4:5a:d4:9a:40:40	e4:5a:d4:9a:40:40
3	C4:AD:34:03:6F:2A	C4:AD:34:03:6F:2A

Обсуждение и порядок настройки

Дальнейшие команды приведены по документации производителей как примеры для повторной проверки, а не как журнал команд, выполненных в описанном эксперименте. В Cisco IOS Root Guard задаётся на интерфейсе, за которым согласно проекту не должен появляться корневой мост [3]. Порт должен выбираться по фактической схеме: включение Root Guard на ожидаемом восходящем root port способно нарушить связность. Root Guard отличается от BPDU Guard: первая функция ограничивает выбор корня, тогда как вторая может отключать граничный порт при получении BPDU [6].

Листинг 8 – Пример включения Root Guard и проверки портов Cisco IOS

```
configure terminal
interface fastethernet 0/8
spanning-tree guard root
end
show spanning-tree inconsistentports
```

Синтаксис зависит от версии Cisco IOS. Для отдельных старых платформ в документации приведена команда spanning-tree rootguard [3]. Без версии ПО исследованного коммутатора нельзя считать листинг 8 дословной записью настроек стенда.

В RouterOS ограничение возможной роли корня на порту задаётся параметром restricted-role. Для STP/RSTP документация указывает поддержку начиная с RouterOS 7.14: при приёме superior BPDU порт переходит в роль alternate-port и состояние discarding, а не обязательно получает диагностическую метку Cisco root-inconsistent [7]. Листинг 9 применим к уже созданному мосту и интерфейсу на поддерживаемой версии RouterOS; его выполнение на использованном стенде не подтверждено.

Листинг 9 – Пример ограничения роли порта в RouterOS

```
/interface bridge port
set [find where interface=ether1] restricted-role=yes
/interface bridge port monitor [find where interface=ether1] once
```

Для Eltex показано состояние дерева, но не указаны версия ПО и применённая команда защиты. Поэтому команды других моделей Eltex не выдаются за проведённую настройку. Для воспроизводимой проверки следует фиксировать модель и версию, конфигурацию порта, режим и инстанцию STP, затем — исходный Root ID, параметры полученного BPDU, роль и состояние защищённого порта и восстановление после прекращения воздействия. Эти данные позволяют отличить ограничение выбора корня от случайного изменения связности.

Представленные материалы не содержат временных рядов загрузки процессора, скорости передачи, длительности восстановления либо серии контролируемых испытаний с одинаковой топологией. Эти показатели не оценивались. Неизменный Root ID не подтверждает непрерывную передачу через блокируемый порт. Root Guard не аутентифицирует отправителя BPDU и не заменяет остальные меры защиты сети: его применение зависит от допустимого направления появления более предпочтительного корневого моста.

Заключение

Учебные наблюдения демонстрируют необходимость контролировать выбор корня и корректно интерпретировать вывод команд Spanning Tree. В таблицах приведены адресные

части идентификаторов корня до и после воздействия, а в листингах — состояния устройств и отдельные ответы ring. Материалы не доказывают универсальную эффективность Root Guard на всех моделях, перехват пользовательского трафика или рост производительности. Документированная функция Root Guard ограничивает появление superior BPDU со стороны выбранного порта и может блокировать передачу через него. Следовательно, такое поведение следует учитывать при проектировании. Для сравнительного экспериментального исследования потребовались бы одинаковые протокольные настройки, версии ПО, параметры кадров и полные журналы, которые в данном опыте отсутствуют.

Благодарности. Научный руководитель — Павловский В. В., старший преподаватель кафедры безопасности информационных технологий РГУ нефти и газа (НИУ) имени И. М. Губкина.

Библиографический список

64. IEEE 802.1 Working Group. 802.1w — Rapid Reconfiguration of Spanning Tree [Электронный ресурс]. — URL: <https://www.ieee802.org/1/pages/802.1w.html>. — Текст : электронный.
65. Cisco Systems. Understand Rapid Spanning Tree Protocol (802.1w) [Электронный ресурс]. — 2023. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>. — Текст : электронный.
66. Cisco Systems. Enhance STP with Root Guard [Электронный ресурс]. — 2026. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>. — Текст : электронный.
67. Yersinia developers. Yersinia: A framework for layer 2 attacks [Электронный ресурс]. — URL: <https://github.com/tomac/yersinia>. — Текст : электронный.
68. Kali Linux. Yersinia [Электронный ресурс]. — URL: <https://www.kali.org/tools/yersinia/>. — Текст : электронный.
69. Cisco Systems. Understand STP Loop Guard and UDLD Features [Электронный ресурс]. — 2022. — URL: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol-stp-8021d/218321-configure-stp-with-loop-guard-and-bpdu-s.html>. — Текст : электронный.
70. MikroTik. Bridging and Switching [Электронный ресурс]. — URL: <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>. — Текст : электронный.

References

71. IEEE 802.1 Working Group. (n.d.). 802.1w — *Rapid Reconfiguration of Spanning Tree*. <https://www.ieee802.org/1/pages/802.1w.html>
72. Cisco Systems. (2023). *Understand Rapid Spanning Tree Protocol (802.1w)*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>
73. Cisco Systems. (2026). *Enhance STP with Root Guard*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>
74. Yersinia developers. (n.d.). *Yersinia: A framework for layer 2 attacks*. <https://github.com/tomac/yersinia>
75. Kali Linux. (n.d.). *Yersinia*. <https://www.kali.org/tools/yersinia/>
76. Cisco Systems. (2022). *Understand STP Loop Guard and UDLD Features*. <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol-stp-8021d/218321-configure-stp-with-loop-guard-and-bpdu-s.html>
77. MikroTik. (n.d.). *Bridging and Switching*. <https://help.mikrotik.com/docs/spaces/ROS/pages/328068/Bridging+and+Switching>

Информация об авторах

Ляхова Мария Владимировна — студентка Российского государственного университета нефти и газа (национального исследовательского университета) имени И. М. Губкина, Москва, Россия; e-mail: mariahlyahova@yandex.ru.

Сеникова Наталья Григорьевна — студентка Российского государственного университета нефти и газа (национального исследовательского университета) имени И. М. Губкина, Москва, Россия; адрес для корреспонденции через соавтора М. В. Ляхову: mariahlyahova@yandex.ru.

Lyakhova M. V., Senikova N. G.

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

Abstract. The article examines an educational scenario involving a change of the root bridge in a switched network and the use of Root Guard to restrict that change. The aim is to interpret the available laboratory observations and describe a verifiable configuration procedure rather than compare equipment performance. The test setup includes workstations, Cisco 2960 SI and Eltex MES1428 switches, and a MikroTik device. Yersinia is used to generate control traffic. The paper preserves connection diagrams, address components of root identifiers before and after the reported intervention, individual ping responses, and console fragments. These materials describe particular node states, but do not establish a synchronized sequence for all events. A second table reports unchanged root addresses when protection was enabled. This is treated as a limited observation because the available evidence does not include complete configuration logs or protected port state transitions. Documented Root Guard behavior is distinguished from experimental observations. Cisco IOS and RouterOS configuration examples are accompanied by explicit applicability conditions and are not presented as commands executed in the reported trial. Recovery time, processor utilization, interruption duration, and packet loss during protective blocking were not measured. The practical contribution is a structured distinction between the baseline state, intervention, root identifier check, and protected port state check. The conclusions apply to the educational case and do not establish universal protection against Layer 2 attacks.

Keywords: RSTP; Root Guard; root bridge; BPDU; switched network; educational setup.

Information about the authors

Maria V. Lyakhova — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; e-mail: mariahyahova@yandex.ru.

Natalia G. Senikova — student, Gubkin Russian State University of Oil and Gas (National Research University), Moscow, Russia; correspondence through co-author M. V. Lyakhova: mariahyahova@yandex.ru.