ПРОФЕССИОНАЛИТЕТ, 2025, № 2 (006)

***УДК** 004.056*

М. А. Руфин [1], М. В. Васильев [1]

[1]ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, Российская Федерация

ВОПРОСЫ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ОТ АТАКИ STP С ИСПОЛЬЗОВАНИЕМ МЕХАНИЗМА ROOT GUARD НА КОММУТАТОРАХ УРОВНЯ ДОСТУПА/РАСПРЕДЕЛЕНИЯ

Аннотация: *В статье рассматривается проблема защиты канального уровня корпоративной сети от атак, связанных с подменой корневого моста в протоколах STP и RSTP. Актуальность исследования обусловлена тем, что при отсутствии механизмов контроля злоумышленник, получивший доступ к сетевому порту, может отправить поддельные BPDU-пакеты с более высоким приоритетом и инициировать изменение топологии сети. Это приводит к перерасчету дерева, временной потере связности и создает условия для перехвата или нарушения передачи трафика. Цель работы заключается в экспериментальной оценке эффективности механизма Root Guard в смешанной сетевой инфраструктуре, построенной на оборудовании Cisco Catalyst 2960, MikroTik и Eltex MES1428. В ходе исследования была смоделирована атака с использованием утилиты Yersinia, выполнено сравнение поведения сети при отключенной и включенной защите, а также проанализированы различия в настройке и диагностике Root Guard у разных производителей. Полученные результаты показали, что без защиты атакующий узел во всех сценариях успешно становился корневым мостом, вызывая нарушение стабильности сети. После активации Root Guard поддельные superior BPDU блокировались, а защищенные порты переводились в состояние блокировки, не допуская изменения Root Bridge. Сделан вывод, что Root Guard является эффективным средством защиты L2-топологии, однако его применение требует учета особенностей конкретного оборудования и организации мониторинга событий безопасности.*

Ключевые слова: *протокол STP, Root Guard, корневой мост, BPDU-пакет, сетевая безопасность, топология сети, коммутатор.*

Введение

Надёжность и защищённость сетевой инфраструктуры имеют ключевое значение для организаций, активно использующих цифровые сервисы и распределённые информационные системы. Одним из базовых механизмов обеспечения устойчивости сетей канального уровня является протокол Spanning Tree Protocol (STP), а также его более современные модификации — RSTP и MSTP. Эти протоколы предназначены для предотвращения образования петель в L2-сегментах и поддержания работоспособности сети при изменении её топологии. Корректность функционирования STP и RSTP зависит от ряда параметров, включая выбор корневого моста, передачу BPDU-сообщений, значения приоритетов устройств и настройки таймеров, определяющих скорость реакции сети на топологические изменения [1].

Вместе с тем протоколы семейства STP имеют существенное ограничение с точки зрения безопасности: BPDU-сообщения не предусматривают встроенного механизма аутентификации. Из-за этого устройство, подключённое к порту коммутатора, может отправить superior BPDU и повлиять на процесс выбора корневого моста. При успешной реализации такого сценария возможна нежелательная перестройка сетевой топологии, временное нарушение связности, а в отдельных случаях — создание условий для перехвата сетевого трафика [2]. Согласно принципам, заложенным в IEEE 802.1D, выбор root bridge выполняется на основании сравнения приоритетов и MAC-адресов сетевых устройств, поэтому получение более «предпочтительного» BPDU может привести к изменению текущей роли коммутаторов в топологии [3].

Для снижения риска несанкционированной смены корневого моста применяется механизм Root Guard. Его задача заключается в защите портов, на которых не должны появляться superior BPDU. Если такой пакет всё же поступает на защищённый интерфейс, порт переводится в состояние root-inconsistent, что блокирует возможность изменения root bridge через данный участок сети. Тем самым Root Guard помогает сохранить предсказуемую L2-топологию и повысить устойчивость сети к атакам на STP [6]. При этом реализация и особенности поведения данного механизма могут различаться в зависимости от производителя сетевого

оборудования, например Cisco, MikroTik или Eltex. Это обстоятельство особенно важно учитывать при построении смешанных инфраструктур, где используются устройства разных вендоров [7].

Цель работы состоит в сравнительной оценке применения Root Guard в гетерогенной сетевой инфраструктуре с последующим определением его влияния на устойчивость L2-топологии и способность противодействовать атакам на STP. Практическая значимость результатов связана с задачами сетевых инженеров, администраторов и архитекторов инфраструктуры, обеспечивающих защиту корпоративных сетей от топологических атак и отказов на канальном уровне.

Методика исследования

Для воспроизведения атакующего сценария и проверки защитного механизма была развернута экспериментальная сетевая схема, представленная на рис. 1. Стенд включал три коммутатора уровня доступа/распределения: Cisco Catalyst 2960 SI с поддержкой PVST+, MikroTik с реализацией стандартных режимов RSTP/MSTP и Eltex MES1428 с поддержкой RSTP. Топология строилась как связанная группа коммутаторов, при этом к каждому устройству был подключен оконечный узел — персональный компьютер. Один из ПК выполнял роль атакующей станции (PCA). Для генерации поддельных BPDU-пакетов использовалась утилита Yersinia, эмулирующая атаку с объявлением ложного корневого моста, имеющего наивысший приоритет.

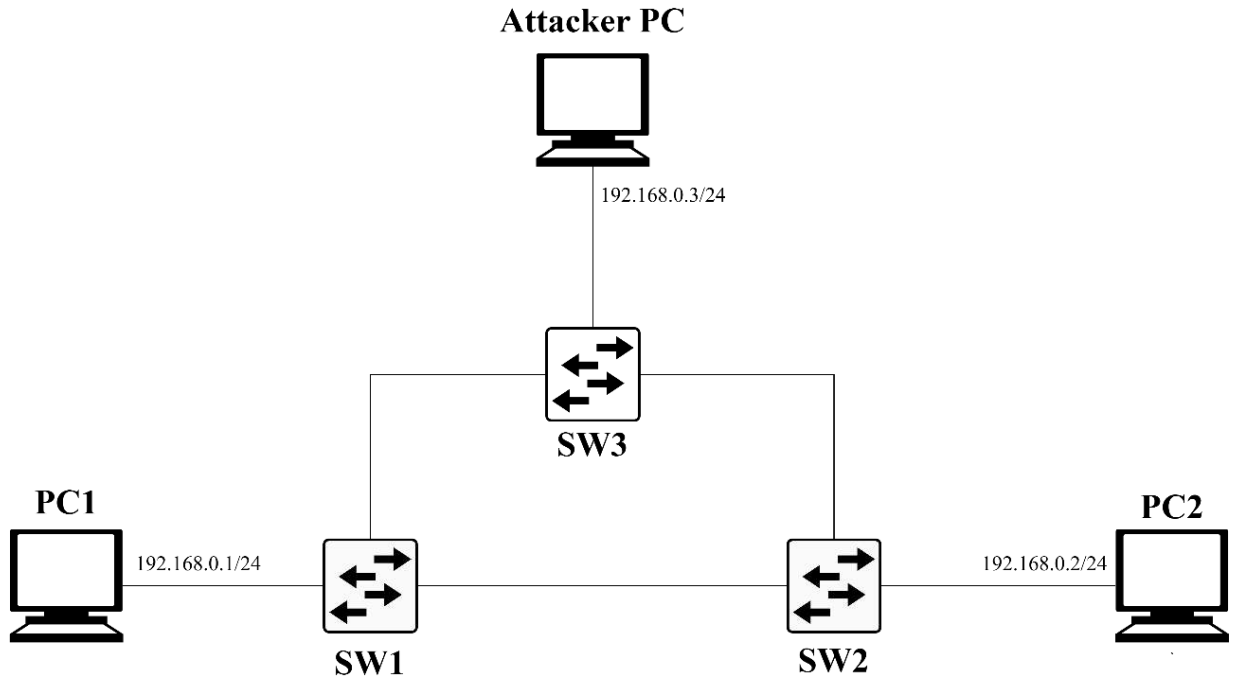

Рис. 1 Топология сети для моделирования атаки на STP с использованием коммутаторов Cisco, MikroTik и Eltex

Методика исследования включала следующие этапы:

1. **Начальное тестирование уязвимости:** при отключенных механизмах защиты на всех коммутаторах проводилась серия атак с целью подтверждения возможности перехвата роли корневого моста.
2. **Тестирование Root Guard:** на всех портах, подключенных к непроверенным сегментам (включая порты, соединяющие коммутаторы между собой и ведущие к PCA), активировался механизм Root Guard. Атаки повторялись, фиксировалось состояние портов и стабильность топологии.
3. **Сравнительный анализ:** анализировались различия в синтаксисе команд активации Root Guard, в выводе диагностических команд (show spanning-tree, show spanning-tree inconsistentports), а также во времени перехода порта в состояние root-inconsistent после получения superior BPDU.

Таблица 1 – Топология сети для каждой атаки

Номер атаки	Компьютер	Подключенный коммутатор
1	PC1	Microtik
	PC2	Eltex mes1428
	PCA	CISCO 2960 si
2	PC1	Eltex mes1428
	PC2	CISCO 2960 si
	PCA	Microtik
3	PC1	Microtik
	PC2	CISCO 2960 si
	PCA	Eltex mes1428

Проведение исследования

В ходе серии последовательных экспериментов была выполнена комплексная практическая проверка устойчивости протокола STP к попыткам навязывания ложного корневого моста с последующей оценкой эффективности механизма Root Guard на коммутаторах уровня доступа/распределения. Основной задачей выступило тестирование работоспособности системы защиты при воздействии внешнего узла, инициирующего передачу поддельных BPDU-кадров.

Для моделирования атаки использовалось специализированное программное средство Yersinia, предустановленное на атакующей рабочей станции (PCA). Данный инструмент, предназначенный для тестирования уязвимостей протоколов канального уровня (L2), применялся для генерации и передачи поддельных BPDU-пакетов с минимальным значением Root ID и подмененным MAC-адресом, что соответствует классическому сценарию атаки по перехвату роли корневого моста. До проведения основного эксперимента была выполнена проверка сетевой доступности между всеми задействованными узлами стенда. Полученные результаты отражены на рисунке 2.

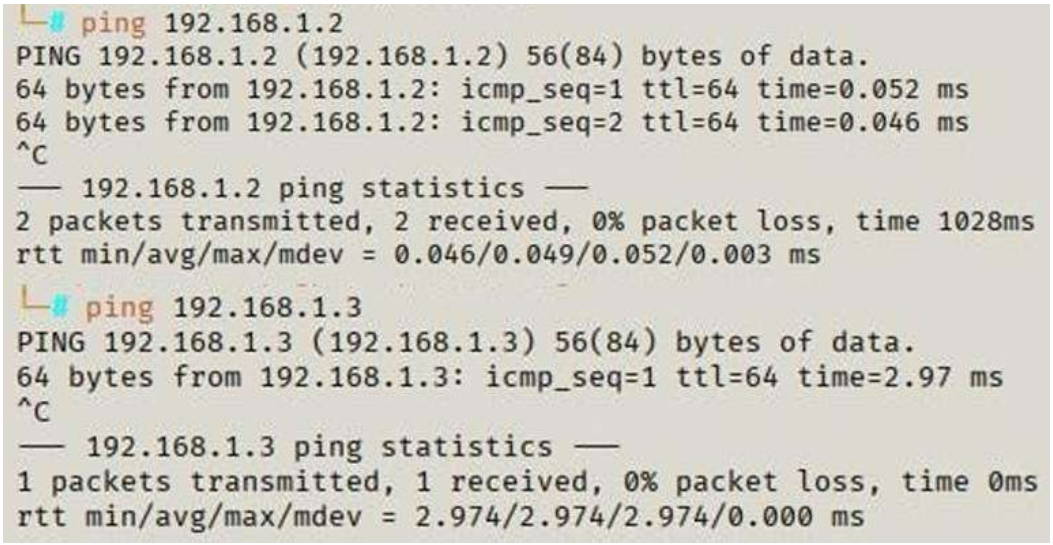

Рис. 2 Проверка сетевой связности между узлами до проведения атак на STP

Для более корректной интерпретации итогов исследования на предварительном этапе были зафиксированы исходные значения идентификаторов корневых мостов — Root ID. Это позволило в дальнейшем сопоставить состояние сети до и после воздействия и определить, привела ли каждая попытка атаки к изменению корневого моста. Эксперимент проводился с атакующей рабочей станции PCA, что имитировало типовой сценарий, при котором злоумышленник получает физический доступ к порту коммутатора.

На этапе проверки уязвимости защитные механизмы были отключены. В таких условиях коммутаторы принимали и обрабатывали поддельные BPDU-кадры без должной фильтрации,

вследствие чего атакующий узел смог быть выбран в качестве корневого моста. Данный результат подтвердил практическую уязвимость STP к воздействию через внедрение BPDU-сообщений с более приоритетными параметрами, то есть superior BPDU. Изменения в состоянии протокола фиксировались с помощью служебных команд на коммутаторах. Полученные данные продемонстрировали смену идентификатора корневого моста и последующую реконфигурацию spanning-tree. Переназначение Root Bridge спровоцировало перерасчет ролей всех портов (корневой, назначенный, альтернативный) и привело к временному нарушению сетевой связности.

При отключенных механизмах защиты коммутаторы корректно обрабатывали и принимали, поступающие поддельные BPDU, вследствие чего атакующее устройство назначалось корневым мостом. Это подтвердило практическую уязвимость протокола STP к внешнему воздействию, основанному на передаче superior BPDU. В ходе эксперимента данный эффект был зафиксирован с помощью служебных команд коммутатора, которые отображают текущее состояние протокола STP. Полученные выводы продемонстрировали смену идентификатора корневого моста и последующее перестроение дерева. Изменение Root Bridge вызвало перерасчет ролей портов (root port, designated port, alternate port) и привело к временной потере связности. Результаты исследования представлены на рисунках 3, 4, 5, 6.

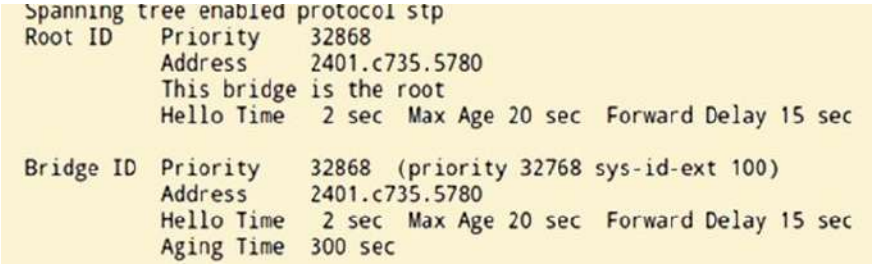

Рис. 3 Результат первой атаки с фиксацией изменения корневого моста после отправки поддельных BPDU-пакетов

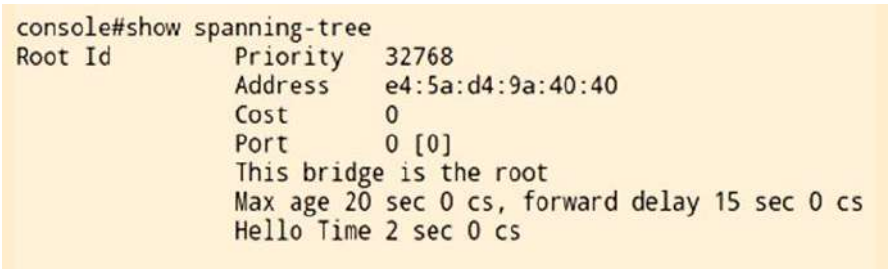

Рис. 4 Результат второй атаки с фиксацией назначения атакующего узла корневым мостом

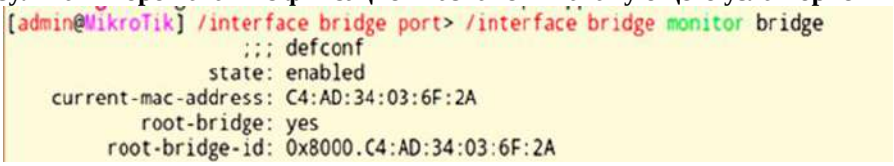

Рис. 5 Результат третьей атаки с подтверждением успешной подмены корневого моста

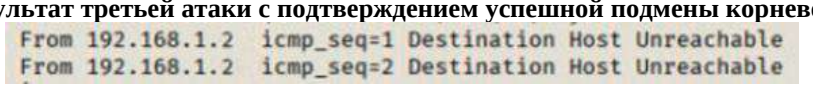

Рис. 6 Нарушение сетевой связности после изменения топологии STP в результате атаки

В итоге таблица сравнения Root ID до атаки и после на всех коммутаторах уровня доступа/распределения выглядит следующим образом:

Таблица 2 – Сравнение Root ID до атаки и после

№ атаки	Root ID до атаки	Root ID после атаки
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

С этого момента злоумышленник получает возможность перехватывать любой незашифрованный трафик, модифицировать данные в потоке, нарушить работу сети, а также стать

центральным узлом, через который проходит всё, что позволяет развернуть любые последующие атаки.

Во избежание атаки появляется необходимость в включении функции Root Guard. После включения функции Root Guard на ключевых портах коммутаторов последующие попытки навязать ложный корневой мост оказались безуспешными и не привели к изменению топологии сети. При поступлении с атакующего сегмента более приоритетных BPDU-сообщений protected-порты автоматически переводились в состояние root-inconsistent. Такой режим работы исключал возможность выбора неавторизованного устройства в роли корневого моста и тем самым блокировал воздействие на механизм построения STP-топологии [4].

Активация Root Guard позволила остановить дальнейшее распространение поддельных BPDU и сохранить исходный Root Bridge без изменений. В результате топология сети осталась стабильной: роли портов не были пересчитаны, маршруты передачи кадров не изменились, а обмен трафиком продолжался без нарушения связности. Это подтверждает практическую эффективность Root Guard как средства защиты STP от несанкционированного влияния со стороны внешних или неконтролируемых устройств.

Таблица 3 – Изменение Root ID после атаки поддельными BPDU с включенным Root Guard

№ атаки	Root ID до атаки	Root ID после атаки
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

Результаты эксперимента фиксируют, что включение Root Guard исключает назначение стороннего узла корневым мостом и повышает устойчивость L2-инфраструктуры к атакам, основанным на передаче superior BPDU. Блокировка таких BPDU на защищённых портах не допускает изменения топологии, сокращает необходимость перерасчёта ролей портов и уменьшает риск потери связности, возникающий при некорректном выборе Root Bridge. В условиях активной генерации ложных BPDU сеть сохраняла стабильное состояние, что соответствует логике работы применяемого защитного механизма.

Сравнительный анализ

Основные различия между платформами проявились в синтаксисе конфигурационных команд, полноте диагностических данных, времени реакции на атаку и доступности средств мониторинга инцидентов. Для объективной оценки эффективности механизма Root Guard в гетерогенной среде эксперимент был расширен за счет сбора временных метрик и анализа журналов событий [5].

Методика сбора метрик

Для измерения времени нарушения связности (convergence time) использовался непрерывный ICMP-трафик (ping) между легитимными узлами PC1 и PC2 (см. Рис. 1), проходящий через корневой мост. Момент начала атаки (инжекции superior BPDU) фиксировался по системному времени на атакующей станции (PCA). Момент восстановления связности фиксировался по получению первого успешного ICMP-ответа после серии потерь. Длительность нарушения связности (failover time) рассчитывалась как разница между временем первого потерянного и первого успешного пакета после восстановления. Дополнительно фиксировалось время реакции механизма Root Guard — интервал от начала атаки до перевода порта в состояние root-inconsistent (получено из логов коммутатора).

Таблица 4 – Сравнительный анализ конфигурации, диагностики и производительности Root Guard

Коммутатор	**Режим STP**	**Способ реализации защиты**	**Состояние порта при срабатывании**	**Особенности диагностики**
Cisco Catalyst 2960	PVST+ / Rapid-PVST+	Включение Root Guard на выбранном интерфейсе	Root Inconsistent	Поддерживается подробная диагностика по порту и VLAN, событие фиксируется в syslog

MikroTik	RSTP / MSTP	Включение параметра restricted-role на bridge-порту	Discarding	Отдельный статус Root Guard не отображается, требуется анализ состояния порта и STP-логов
Eltex MES1428	RSTP	Включение Root Guard на выбранном интерфейсе	Root Inconsistent	Диагностика близка к Cisco, поддерживается проверка состояния порта и фиксация события в журнале

Основные команды настройки и проверки Root Guard приведены ниже. Они вынесены отдельно от таблицы, так как содержат технические строки конфигурации и при размещении внутри таблицы ухудшают читаемость материала.

Список команд для настройки и проверки Root Guard Cisco Catalyst 2960

Включение Root Guard на интерфейсе:

```
configure terminal
interface FastEthernet0/1
spanning-tree guard root
end
```

Проверка состояния STP и заблокированных портов:

```
show spanning-tree inconsistentports
show spanning-tree interface FastEthernet0/1 detail
```

Проверка журналов событий:

```
show logging
```

При срабатывании защиты в журнале может отображаться сообщение вида:

SPANTREE-2-ROOTGUARDBLOCK

MikroTik

Включение защиты на bridge-порту:

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

Или при добавлении нового порта в bridge:

```
/interface bridge port
add bridge=bridge1 interface=ether1 restricted-role=yes
```

Проверка состояния bridge-порта:

```
/interface bridge port print detail
/interface bridge monitor bridge1
```

Включение логирования STP-событий:

```
/system logging add topics=stp action=memory
/log print
```

При срабатывании защиты порт может перейти в состояние:

discarding

Eltex MES1428

Включение Root Guard на интерфейсе:

```
configure terminal
interface fastethernet 0/1
spanning-tree guard root
exit
```

Проверка состояния STP на интерфейсе:

```
show spanning-tree interface fastethernet 0/1
```

Проверка портов в состоянии блокировки:

```
show spanning-tree inconsistentports
```

Проверка журналов событий:

```
show logging
```

Таким образом, сравнительный анализ показал, что на оборудовании Cisco и Eltex механизм Root Guard имеет более наглядную диагностику, так как порт переводится в состояние Root Inconsistent, а событие может фиксироваться в системном журнале. На устройствах MikroTik схожий защитный механизм настраивается с помощью параметра restricted-role. При этом в

интерфейсе управления не выводится отдельное состояние, явно указывающее на срабатывание Root Guard. В связи с этим для обнаружения подобного события требуется дополнительно проверять состояние bridge-порта и анализировать журналы, связанные с работой STP. Данная особенность особенно важна при проектировании гетерогенных сетей, в которых одновременно применяются коммутаторы разных производителей.

Реализация Root Guard на оборудовании MikroTik

Результаты исследования показали, что при успешной реализации атаки перестроение сетевой топологии сопровождалось временной потерей связности продолжительностью примерно от 30 до 45 секунд вне зависимости от используемого оборудования. Такой интервал соответствует базовым таймерам STP, включая Max Age и Forward Delay, а также согласуется с принципами сходимости, описанными в стандарте IEEE 802.1D. При этом скорость реакции механизма Root Guard на получение superior BPDU отличалась в зависимости от платформы. Наибольшая задержка была зафиксирована на MikroTik и достигала 7 секунд. Вероятно, это связано не с особенностями самого протокола, а с механизмом обновления и отображения состояния bridge-портов в RouterOS. Оборудование Cisco и Eltex реагировало быстрее — в пределах 2–5 секунд, фактически сразу после обработки первого поддельного BPDU.

Особенности обработки BPDU и диагностики на разных платформах

Исследование зафиксировало различия не только на уровне команд активации Root Guard, но и в механизмах обработки BPDU-сообщений, регистрации событий безопасности и последующей диагностики. Эти параметры имеют прикладное значение для эксплуатации смешанных L2-инфраструктур: они определяют трудоёмкость администрирования, скорость выявления инцидента и фактическую результативность защиты топологии.

Cisco Catalyst 2960 (PVST+ / Rapid-PVST+)

Оборудование Cisco характеризуется более развитой реализацией защитных функций, что связано с применением проприетарного механизма PVST+. В соответствии с технической документацией Cisco [6], PVST+ передаёт сведения об исходной VLAN (PVID) внутри BPDU-пакета. За счёт этого коммутатор способен контролировать не только попытки несанкционированной смены корневого моста, но и отдельные ошибки конфигурации, возникающие на уровне конкретных VLAN. Для работы Root Guard такая модель обработки BPDU формирует следующие преимущества:

- **Детекция инцидентов на уровне VLAN.** При получении superior BPDU на порту, защищенном Root Guard, коммутатор Cisco анализирует не только приоритет корневого моста, но и соответствие VLAN. Если BPDU несет информацию о VLAN, отличной от настроенной на порту, порт также может быть заблокирован, что предотвращает атаки, направленные на конкретный VLAN (VLAN hopping через STP);
- **Диагностическая полнота.** Статус Root Inconsistent отображается отдельно для каждой VLAN в выводе команды show spanning-tree inconsistentports, что позволяет точно локализовать проблемный сегмент. Генерация syslog-сообщения «SPANTREE-2-ROOTGUARD-BLOCK» с указанием VLAN и порта обеспечивает немедленное оповещение администратора о попытке атаки.

MikroTik RouterOS. На устройствах MikroTik функциональный аналог Root Guard реализован через параметр restricted-role. Данный механизм основан на стандартной логике IEEE 802.1w, то есть RSTP, и не содержит дополнительных вендорских средств, направленных на упрощение диагностики срабатываний. Это приводит к ряду эксплуатационных ограничений.

Во-первых, для MikroTik характерно отсутствие VLAN-ориентированной детализации работы механизма. Стандартный RSTP оперирует не отдельными VLAN, а экземплярами дерева, поэтому при получении superior BPDU порт может быть заблокирован независимо от конкретного VLAN-контекста. В результате устройство не позволяет явно выделить атаки, направленные на отдельную VLAN в гибридной сетевой инфраструктуре.

Во-вторых, ограничены возможности диагностики. Согласно особенностям реализации MikroTik, параметр restricted-role не сопровождается отдельным состоянием, однозначно указывающим на срабатывание Root Guard. Порт переводится в состояние discarding, однако такое

состояние может возникать не только при защитной блокировке, но и в штатной работе RSTP, например для резервного Alternate-порта. Поэтому для точного определения причины изменения состояния администратору необходимо дополнительно анализировать роли портов и журналы STP. Отсутствие специализированного syslog-уведомления о срабатывании защиты усложняет оперативное выявление атаки и требует внедрения дополнительных средств мониторинга, например периодического опроса состояния bridge-портов и сравнения их ролей.

Eltex MES1428 RSTP. Коммутаторы Eltex MES1428 также используют стандартный RSTP, однако с точки зрения диагностики событий безопасности их поведение ближе к оборудованию Cisco.

Особенностью Eltex является комбинированный подход к реализации защиты. Устройство поддерживает команду spanning-tree guard root, аналогичную применяемой на Cisco, а также позволяет просматривать состояние Root Inconsistent через вывод команды show spanning-tree inconsistentports. Вместе с тем, в отличие от Cisco, данный механизм не обладает VLAN-специфичностью, поскольку функционирует в рамках стандартной реализации RSTP.

Дополнительным преимуществом Eltex является наличие системного логирования событий блокировки порта. Коммутатор формирует syslog-сообщения при срабатывании Root Guard, что упрощает интеграцию оборудования в централизованные системы мониторинга и анализа событий безопасности, включая SIEM. По этому параметру Eltex имеет преимущество перед MikroTik в инфраструктурах, где важны оперативное обнаружение инцидентов и централизованный аудит сетевой безопасности.

Логирование инцидентов. Одним из наиболее значимых различий между рассмотренными платформами является способ фиксации событий, связанных со срабатыванием защитного механизма.

На оборудовании Cisco и Eltex при блокировке порта Root Guard формируется явное системное сообщение. Для Cisco характерна явная регистрация события Root Guard в виде системного сообщения SPANTREE-2-ROOTGUARDBLOCK. Такое уведомление фиксирует попытку изменения роли конкретного порта и его перевод в состояние root-inconsistent. Наличие отдельного диагностического события сокращает время выявления воздействия на STP-топологию и позволяет оперативно передать информацию администратору.

На оборудовании MikroTik специализированное уведомление о срабатывании restricted-role по умолчанию отсутствует. Для обнаружения аналогичного события требуется предварительно включить логирование по STP-связанным темам и затем анализировать журнал на предмет нетипичных изменений ролей и состояний портов. Особое значение имеют переходы в состояния Designated и Discarding, поскольку они могут указывать на попытку вмешательства в построение топологии. Такая модель диагностики повышает требования к анализу журналов и затрудняет автоматизированное выявление попыток компрометации L2-инфраструктуры.

Отдельным методическим условием стала проверка совместимости режимов STP до начала тестирования защитных механизмов. Совместное использование PVST+ на Cisco и стандартного RSTP на MikroTik и Eltex потребовало дополнительной настройки, включая приведение магистральных портов Cisco к режиму rapid-pvst для корректного формирования единого spanning-tree-домена. При отсутствии данного этапа коммутаторы могли формировать изолированные экземпляры дерева, что искажало бы результаты последующих испытаний безопасности.

Заключение

Проведённое исследование подтвердило, что Root Guard выступает обязательным и результативным элементом защиты STP/RSTP-инфраструктуры от атак, связанных с подменой корневого моста. В экспериментальных условиях активация механизма приводила к блокированию всех попыток навязать ложный Root Bridge, при этом топология сети сохраняла устойчивое состояние.

Сравнительный анализ выявил различия в синтаксисе команд и эксплуатационных характеристиках, влияющих на итоговый уровень защищённости гетерогенной сети:

– Различия во времени реакции защиты. На оборудовании Cisco и Eltex реакция на атаку составляла 2–4 секунды, на MikroTik — 5–7 секунд. Такая задержка может иметь критическое значение для сред с жёсткими требованиями к детерминированному поведению сети и быстрому восстановлению после инцидентов.

– Критичность мониторинга. На MikroTik не формируются детализированные syslog-события, однозначно указывающие на срабатывание защиты, поэтому администраторам необходимо внедрять дополнительные процедуры обнаружения атак. Cisco и Eltex, напротив, предоставляют развёрнутую диагностику, достаточную для немедленного реагирования на инцидент.

– Влияние на связность. При активированном Root Guard атака не приводит к смене корневого моста и, соответственно, не вызывает длительной потери связности, характерной для штатного пересчёта STP продолжительностью 30–45 секунд. Этот результат подтверждает эффективность Root Guard как средства обеспечения непрерывности сервиса.

– Глубина обработки BPDU. На Cisco реализация Root Guard в связке с PVST+ обеспечивает VLAN-специфичную защиту и позволяет выявлять более широкий спектр атак, тогда как MikroTik и Eltex, работающие в рамках стандартного RSTP, реализуют защиту на уровне экземпляра дерева.

Полученные количественные данные и выявленные особенности имеют высокую прикладную значимость для специалистов, проектирующих и эксплуатирующих отказоустойчивые гетерогенные сети. Корректное применение Root Guard невозможно без учета выявленных вендор-специфичных особенностей конфигурации, диагностики и мониторинга инцидентов. При построении смешанных инфраструктур рекомендуется унифицировать режимы STP (например, переход на стандартный MSTP, поддерживаемый всеми тремя вендорами) и разрабатывать дополнительные сценарии мониторинга для платформ с ограниченной диагностикой (MikroTik) с целью обеспечения паритета в обнаружении атак.

Библиографический список

1. Малыгин, В. С. Исследование работы технологий STP, RSTP при различных показателях их характеристик / В. С. Малыгин, В. И. Фрейман // Инновационные технологии: теория, инструменты, практика. – 2022. – Т. 1. – С. 327–333. – EDN EAUKDH.
2. Чайка, Е. Ю., Шкуренков, Е. С. Атака на протокол STP: Man in the Middle. Методики тестирования и защиты / Е. Ю. Чайка, Е. С. Шкуренков // Актуальные исследования. – 2025. – № 27 (262). – С. 37–48 – URL: https://apni.ru/article/12611-ataka-na-protokol-stp-man-in-the-middle-metodiki-testirovaniya-i-zashity.
3. IEEE Std 802.1D-2004. *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*. — IEEE, 2004. — 281 p.
4. IEEE Std 802.1w-2001. *IEEE Standard for Local and Metropolitan Area Networks — Common Specifications: Rapid Reconfiguration of Spanning Tree*. — IEEE, 2001. — 54 p.
5. Seaman, M. An Overview of IEEE 802.1 Spanning Tree Protocols / M. Seaman // *IEEE 802.1 Working Group Documents*. – 2009. – 38 p. – URL: https://www.ieee802.org/1/files/public/docs2009/aq-seaman-merged-spanning-tree-protocols-0509.pdf.
6. Cisco Systems. Understanding and Configuring Spanning Tree Root Guard and BPDU Guard // Cisco Documentation. – 2019. – URL: https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html.
7. Уймин, А. Г. Компьютерные сети. L2-технологии: практикум для СПО / А. Г. Уймин. – Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2024. – 105 с.

References

1. Malygin, V. S., & Freiman, V. I. (2022). Study of the operation of STP and RSTP technologies under various performance characteristics. *Innovative Technologies: Theory, Tools, Practice, 1*, 327–333. EDN EAUKDH.
2. Chaika, E. Yu., & Shkurenkov, E. S. (2025). Attack on the STP protocol: Man-in-the-Middle. Testing and protection techniques. *Current Research, 27*(262), 37–48. Retrieved from https://apni.ru/article/12611-ataka-na-protokol-stp-man-in-the-middle-metodiki-testirovaniya-i-zashity

3. IEEE. (2004). *IEEE Std 802.1D-2004: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*. IEEE. https://doi.org/10.1109/IEEESTD.2004.94569
4. IEEE. (2001). *IEEE Std 802.1w-2001: IEEE Standard for Local and Metropolitan Area Networks — Common Specifications: Rapid Reconfiguration of Spanning Tree*. IEEE. https://doi.org/10.1109/IEEESTD.2001.93365
5. Seaman, M. (2009). *An overview of IEEE 802.1 spanning tree protocols* [Paper presentation]. IEEE 802.1 Working Group Documents. Retrieved from https://www.ieee802.org/1/files/public/docs2009/aq-seaman-merged-spanning-tree-protocols-0509.pdf
6. Cisco Systems. (2019). *Understanding and configuring Spanning Tree Root Guard and BPDU guard* [Technical documentation]. Cisco Documentation. Retrieved from https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html
7. Uymin, A. G. (2024). *Computer networks. Layer 2 technologies: Practical workbook for secondary vocational education*. Profobrazovanie, IPR Media.

Информация об авторах

Руфин Матвей Алексеевич — студент кафедры «Комплексная безопасность критически важных объектов», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: rufin.m@mail.ru

Васильев Матвей Валерьевич — студент кафедры «Комплексная безопасность критически важных объектов», ФГАОУ ВО «РГУ нефти и газа (НИУ) имени И.М. Губкина», г. Москва, e-mail: matveyv2005@gmail.com

ISSUES OF PROTECTING STP AGAINST ATTACKS USING THE ROOT GUARD MECHANISM ON ACCESS/DISTRIBUTION LAYER SWITCHES

Rufin M. A.[1], Vasiliev M. V.[1]

[1]National University of Oil and Gas «Gubkin University»

Abstract. *The article examines the problem of protecting the data link layer of a corporate network against attacks aimed at spoofing the root bridge in STP and RSTP protocols. The relevance of the study is determined by the fact that, without additional protection mechanisms, an attacker with access to a switch port can send forged BPDU packets with a higher priority and trigger an unauthorized topology change. This may lead to spanning tree recalculation, temporary loss of connectivity, and conditions for traffic interception or disruption. The purpose of the study is to experimentally evaluate the effectiveness of the Root Guard mechanism in a heterogeneous network infrastructure based on Cisco Catalyst 2960, MikroTik, and Eltex MES1428 switches. During the experiment, an attack was simulated using the Yersinia tool, the network behavior with disabled and enabled protection was compared, and vendor-specific differences in Root Guard configuration and diagnostics were analyzed. The results showed that, without protection, the attacking host successfully became the root bridge in all tested scenarios, causing instability in the network topology. After Root Guard was enabled, forged superior BPDU packets were blocked, and protected ports were placed into a blocking state, preventing unauthorized Root Bridge changes. The study concludes that Root Guard is an effective mechanism for protecting L2 topology, but its correct use requires consideration of vendor-specific implementation features and proper security event monitoring.*

Keywords: *STP protocol, Root Guard, root bridge, BPDU packet, network security, network topology, switch.*

Information about the authors

Rufin Matvey Alekseevich — Student of the Department of «Comprehensive Security of Critical Facilities», National University of Oil and Gas «Gubkin University», Russia, Moscow, e-mail: rufin.m@mail.ru

Vasiliev Matvey Valeryevich — Student of the Department of «Comprehensive Security of Critical F

acilities», National University of Oil and Gas «Gubkin University», Russia, Moscow, e-mail: matveyv2005@gmail.com