OSNOVO

cable transmission

РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ

Настройка протокола MSTP с помощью интерфейса командной строки (CLI)

Прежде чем приступать к эксплуатации изделия,
внимательно прочтите настоящее руководство

www.osnovo.ru

Оглавление

ВВЕДЕНИЕ

В настоящее время протоколы группы STP (Spanning Tree Protocol) доступны практически в каждом управляемом промышленном, и просто управляемом коммутаторе уровня L2+, L3. Протокол MSTP (Multiple Spanning Tree Protocol) является дальнейшим развитием протокола RSTP (Rapid Spanning Tree), основное отличие – это возможность работы с несколькими VLAN (виртуальная локальная сеть).

Основным преимуществом MSTP является возможность создавать несколько инстансов (inst) протокола STP, в зависимости от количества логических топологий сети и распределять по ним VLANы. Это позволяет предотвращать образование петлевых соединений и обеспечивает безопасную и устойчивую работу сети. Протокол MSTP также дает возможность более эффективно использовать ресурсы сети, балансировать трафик и обеспечивать быстрое восстановление работы сети в случае сбоев.

На управляемых коммутаторах протокол MSTP можно запускать и настраивать с помощью команд через командную строку (CLI), или через WEB-интерфейс. Настройка параметров через командную строку позволяет делать более глубокие настройки протокола в части распределения трафика и оптимизации работы сети. Управление настройками протокола через WEB-интерфейс предоставляет более скромные возможности.

В данном руководстве представлено оба способа настройки параметров протокола MSTP. В большинстве случаев для предотвращения образования петлевых соединений и обеспечения устойчивой работы сети достаточно запустить протокол MSTP на коммутаторах, что проще сделать через соответствующие разделы меню WEB-интерфейса. Если требуется произвести более глубокие настройки протокола для распределения трафика и оптимизации маршрутов в сети, то следует обратиться к разделу управления с помощью командной строки.

1. Конфигурация MSTP через WEB-интерфейс

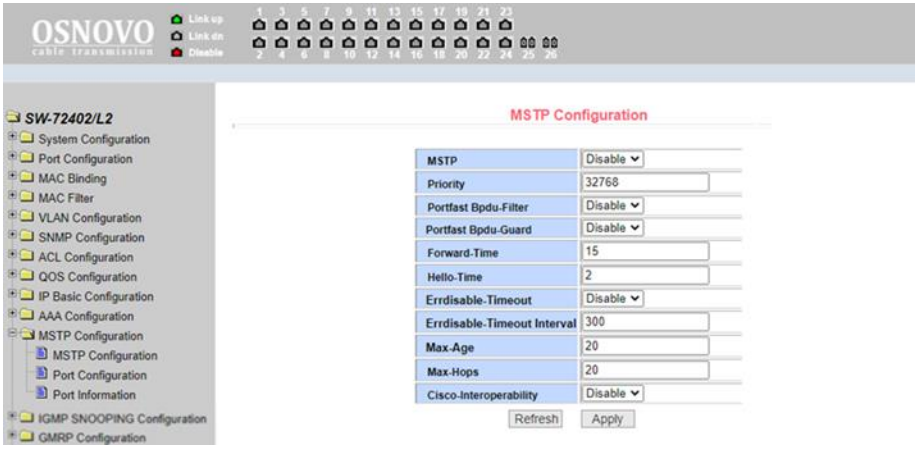
1.1 Вход в WEB интерфейс

Для входа в WEB интерфейс введите в адресную строку браузера IP адрес коммутатора (192.168.0.1 по умолчанию), откроется всплывающее окно для идентификации.

После того, как будут введены корректные данные для входа (имя пользователя: ***admin***, пароль: ***admin*** по умолчанию) отобразится главная страница WEB-интерфейса управления коммутатором, далее следует в левой части окна выбрать **MSTP configuration**.

1.2 MSTP Configuration (Настройка работы протокола STP)

1.2.1 MSTP Configuration (Основные настройки MSTP)

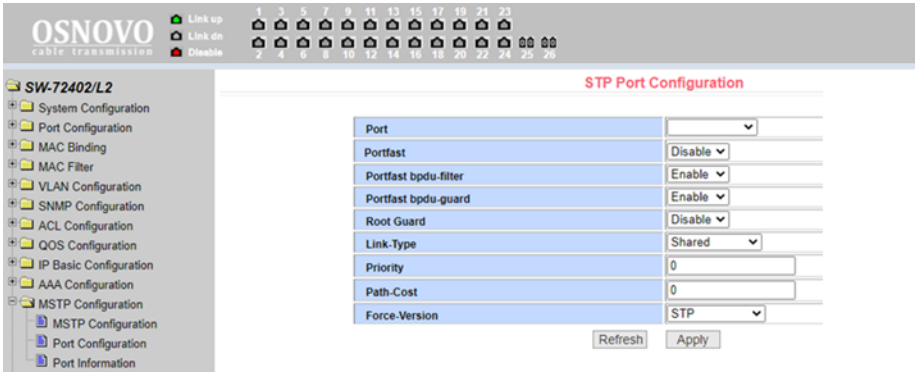


На данной странице WEB интерфейса представлены глобальные настройки протокола MSTP (*Multiple Spanning Tree Protocol*):

- *MSTP (Disable/Enable)* – вкл/выкл поддержку протокола MSTP;
- *Priority* – настройка приоритезации. Устройства с более низким приоритетом подходят больше для роли корневого моста(root bridge);
- *Portfast BPDU Filter (Disable/Enable)* – вкл/выкл фильтрацию BPDU пакетов на порте;
- *Portfast BPDU Guard (Disable/Enable)* – вкл/выкл функцию защиты BPDU пакетов;
- *Forward Time* – настройка задержки пересылки пакетов;
- *Hello Time* – настройка интервала отправки MSTP HELLO пакетов;
- *Errdisable Timeout (Enable/Disable)* – вкл/выкл функции *Errdisable.* Если порт с включенным BPDU Guard получает пакеты BPDU запускается *Errdisable* таймер. По истечении заданного времени *(Errdisable timeout)* порт будет перезапущен;
- *Errdisable timeout* – время после которого будет перезапущен порт получивший пакет BPDU;
- *Max Age* – время в секундах в течение которого коммутатор ожидает информацию о конфигурации ST(spanning tree) прежде чем запустить процесс конфигурации заново;
- *Max Hops* – количество переходов (хопов) до отбрасывания BPDU пакетов в домене;
- *CISCO Interoperability (Enable/Disable)* – вкл/выкл совместимость с настройками STP CISCO.

После внесения изменений в настройки, нажмите кнопку *Apply* (принять).

1.2.2 MSTP Port Configuration (настройка MSTP на портах)

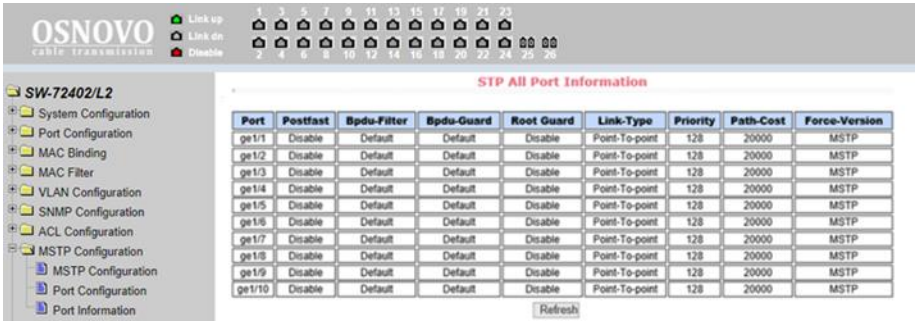


На данной странице WEB интерфейса представлены настройки MSTP (*Multiple Spanning Tree* Protocol) для портов.

- *Port* – выбор порта для настройки;
- *Portfast (Enable/Disable)* – вкл/выкл состояния Portfast для выбранного ранее порта. В состоянии Portfast порт переходит из состояния блокировки в состояние пересылки(forward) пакетов минуя состояние обучения(learning) и прослушивания (listening);
- *Portfast BPDU filter (Enable/Disable)* – вкл/выкл фильтрацию BPDU пакетов на выбранном порте;
- *Portfast BPDU GUARD (Enable/Disable)* – вкл/выкл функцию защиты BPDU пакетов на выбранном порте;
- *Root Guard (Enable/Disable)* – вкл/выкл функции защиты корневого моста (root bridge) от приема BPDU пакетов от устройств с более высоким приоритетом, чем мост;
- *Link Type* – настройка типа подключения. Point to Point (точка-точка) позволяет быстро менять состояние порта. Shared подключение не позволяет быстро менять состояние порта. Необходимо пройти 802.1D процедуры, чтобы определить статус порта;
- *Priority* – настройка CIST приоритета, значение может быть только кратным 16 в диапазоне от 0-240. По умолчанию значение равно 128;
- *Path Cost* – от 0 – 200 000 000. Более низкие значения обычно соответствуют root'ам;
- *Force Version* – тип отправляемых пакетов.

После внесения изменений в настройки, нажмите кнопку *Apply* (принять).

1.2.3 MSTP information (Общая информация о конфигурации MSTP)



Port	Postfast	Bpdu-Filter	Bpdu-Guard	Root Guard	Link-Type	Priority	Path-Cost	Force-Version
ge1/1	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/2	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/3	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/4	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/5	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/6	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/7	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/8	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/9	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP
ge1/10	Disable	Default	Default	Disable	Point-To-point	128	20000	MSTP

На данной странице WEB интерфейса представлена сводная информация о конфигурации MSTP (только для чтения).

2. CLI Command line interface (Введение)

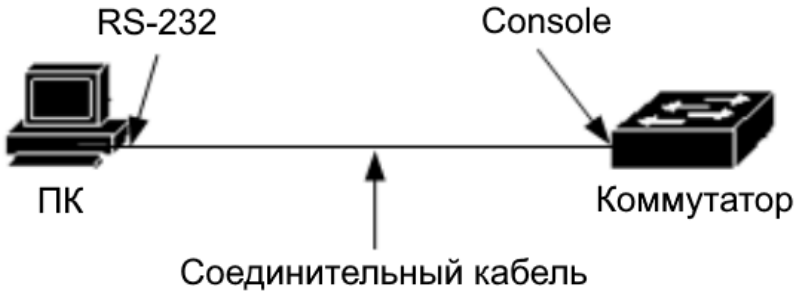
Управление коммутатором через COM-порт (RS-232) с помощью командной строки (CLI) предоставляет пользователю широкие возможности по настройке и управлению режимами работы коммутатора, или в случае, если по каким-либо причинам управление через WEB-интерфейс недоступно.

2.1 Accessing CLI (Доступ к CLI)

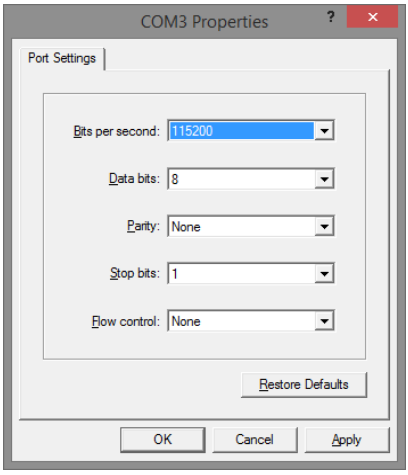
Процедура подготовки к управлению с помощью командной строки описана в руководстве по эксплуатации коммутатором (п.8).

2.1.1 Users access CLI via Console port (Подключение через порт Console)

- Соедините порт Console коммутатора с COM-портом компьютера с помощью кабеля (см. рис. ниже);



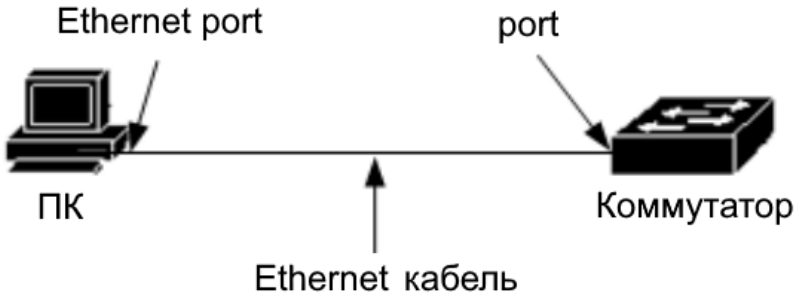
- Запустите HyperTerminal на ПК;
- Задайте имя для нового консольного подключения;
- Выберите COM-порт, к которому подключен коммутатор;
- Настройте COM-порт следующим образом:
  - ✓ Скорость передачи данных (Baud Rate) – 115200;
  - ✓ Биты данных (Data bits) – 8;
  - ✓ Четность (Parity) – нет (no);
  - ✓ Стоп биты (Stop bits) – 1;
  - ✓ Управление потоком (flow control) – нет (no).



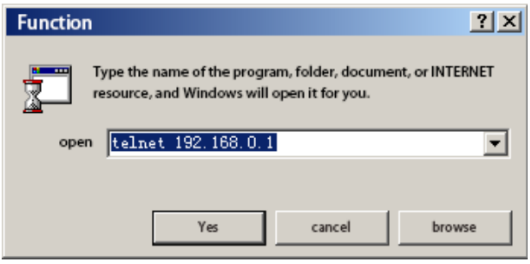
- Включите коммутатор, система предложит войти в интерфейс CLI (управление через командную строку).

2.1.2 Users access CLI via TELNET (Подключение через TELNET)

- Соедините порт коммутатора с Ethernet портом компьютера с помощью кабеля (см. рис. ниже);



- Чтобы получить доступ к CLI коммутатора через Telnet, ПК и коммутатор должны находиться в одной сети. Установите IP адрес сетевого адаптера ПК (например 192.168.0.3) IP адрес коммутатора ***192.168.0.1*** (по умолчанию);
- Если ПК соединен с коммутатором откроется Telnet интерфейс (встроен в командную строку CMD семейства операционных систем Microsoft Windows см. рис. ниже);



- Если пароль не установлен, то Telnet интерфейс предоставит доступ к к CLI коммутатора. В противном случае потребуется аутентификация (по умолчанию: Login: **admin** Password: **admin**).

Внимание !

- IP адрес порта коммутатора зависит от VLAN layer 3 интерфейса. Перед тем как подключиться к коммутатору, должен быть установлен IP адрес VLAN интерфейса. По умолчанию IP адрес vlan1 192.168.0.1. Иной IP адрес VLAN интерфейса может быть установлен через порт console.

- Подключить ПК к коммутатору можно через один из портов непосредственно кабелем Ethernet, или через локальную сеть (если имеется возможность соединения ПК и VLAN коммутатора).

2.2 CLI Mode introduction (CLI режимы)

2.2.1 CLI Role of mode (CLI роли режимов)

Основные функции режимов CLI:

- Упрощение классификации пользователей и предотвращение неавторизованного использования командной строки.
Пользователи разделяются на два уровня: обычный и привилегированный. Обычные пользователи могут только просматривать статусы некоторых операций коммутатора с использованием команд просмотра.
Привилегированные пользователи (в дополнение к перечисленным выше) имеют возможность конфигурировать настройки коммутатора.

- Упрощение управлением коммутатора.

Т.к. коммутатор имеет множество конфигураций, то для пользователей удобно объединять их в различные режимы для использования. Сходные по функциональному назначению команды объединены в режимы. Например связанные с управлением VLAN команды и команды управления интерфейсом объединены в соответствующие режимы.

2.2.2 Identification of CLI mode (Идентификация CLI режимов)

При использовании командной строки пользователь может узнать текущий режим CLI, который указан в CLI prompt. CLI prompt состоит из двух частей, одна идентифицирует хост, а другая идентифицирует режим.

CLI prompt хост использует имя хоста системы. Имя хоста системы (по умолчанию *switch*) может быть изменено. Таким образом, CLI prompt начинает работу с именем хоста «switch».

Изменения части CLI prompt, касающейся режима CLI не предусмотрены. Каждый режим привязан к соответствующей данному режиму строке. Существуют фиксированные строки и изменяемые строки. Например строка режима VLAN конфигурации фиксированная, а строка режима интерфейса конфигурации изменяемая.

Пример:

- CLI prompt switch # определяет привилегированный режим (switch определяет хост, # определяет режим).
- CLI prompt switch (config-ge1 / 1) # определяет режим интерфейса конфигурации и конфигурирует GE1 / 1 порт (switch определяет хост, (config-ge1 / 1), # определяет режим).
- CLI prompt switch (config-vlan2) # определяет режим интерфейса конфигурации vlan2 (switch определяет хост, (config-vlan2), # определяет режим).

2.2.3 Classification of CLI modes (Классификация CLI режимов)

Режимы CLI разделены на четыре группы: обычный (normal mode), привилегированный (privileged mode), глобальной конфигурации (global configuration mode) и конфигурационный (configuration sub mode, включает несколько cli подрежимов).

Простым пользователям доступен только обычный режим, привилегированным пользователям доступны все cli режимы.

При подключении через console и telnet сначала доступен только нормальный режим. После ввода соответствующей команды возможен переход в привилегированный режим при условии успешной аутентификации, *(простой пользователь не имеет возможности перехода в другие режимы*). После входа в привилегированный режим возможно перейти в режим глобальной конфигурации. Для перехода из режима глобальной конфигурации в другие подрежимы (sub mode) следует ввести соответствующие команды.

Таблица основных cli режимов коммутатора.

Режим	**Описание**	**Prompt**	**Команда входа**	**Команда выхода**
Normal mode	Просмотр текущей информации о коммутаторе.	Switch>	Режим доступен автоматически при первичном входе.	exit или quit для выхода из telnet terminal.
Privileged mode	Просмотр текущей информации о коммутаторе. Команды debugging, version upgrade, configuration maintenance.	Switch#	**enable** в режиме normal mode.	**disable** возврат в normal mode. exit или quit для выхода из telnet terminal.
whole situation mode of configuration	Основные команды недоступные в режимах configuration sub mode, такие как configuration static routing.	Switch(config)#	Перейти в режим команд из privileged mode.	**exit**, **quit**, или **end** возврат в privileged mode.
Interface configuration mode	Команды для конфигурации интерфейса портов и VLAN.	Port: Switch(config-ge1/1)# VLAN port: Switch(config-vlan1)#	< **if name** > в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.
VLAN mode of	Команды для конфигурации VLAN, такие как	Switch(config-vlan)#	vlan database order	**exit** или **quit** для выхода из global configuration mode.

config uration	создать и удалить VLAN.		в режиме global configuration mode.	**end** для выхода из privileged mode.
MSTP config uration mode	Команды для конфигурации MSTP, такие как создать и удалить MSTP интерфейсы.	Switch(config-mst)#	Войти в spaning tree MST в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.
Termin al config uration mode	Команды для конфигурации console и telnet, такие как timeout интерфейса.	Switch(config-line)#	Войти в строку команд vty в режиме global configuration mode.	**exit** или **quit** для выхода из global configuration mode. **end** для выхода из privileged mode.

2.3 Introduction to command syntax (Синтаксис команд)

2.3.1 Command composition (Композиция команд)

CLI команды состоят из ключевых слов объединенных с параметрами. Сначала располагается ключевое слово, далее следующее ключевое слово или параметр. Ключевые слова и параметры могут чередоваться. Команда может содержать только ключевое слово (без параметра).

Пример:

- Команда < write > состоит только из ключевого слова;
- Команда < show version > состоит из двух ключевых слов;
- Команда VLAN < VLAN ID > состоит из ключевого слова и параметра;
- Команда instance < instance ID > VLAN < VLAN ID > состоит из двух ключевых слов и двух параметров, которые чередуются.

2.3.2 Parameter type (Типы параметров)

Параметры CLI команд разделяются на два типа: обязательные и опциональные. При вводе команды обязательные параметры должны быть тоже введены, ввод опциональных параметров не является необходимым.

Пример:

- Для команды VLAN < VLAN ID > параметр является обязательным;
- Для команды < show interface [if name] > параметр является опциональным.

2.3.3 Command syntax rules (Правила синтаксиса)

При описании команд в тексте данной инструкции используются следующие правила:

1) Ключевые слова описываются словами, совпадающими по смыслу.
2) Параметры заключаются в символы < >
   Пример: VLAN < VLAN ID >
3) Опциональный параметр заключается в прямоугольные скобки [ ]
   Пример: VLAN [< VLAN ID >] в этом же случае символы < > могут быть опущены: VLAN [VLAN ID] соответственно параметр VLAN ID может не вводиться. Если параметр обязательный, то в скобки он не заключается.
4) Если необходимо выбрать одно из нескольких ключевых слов или параметров, то для выделения используются фигурные скобки { }. Для разделения ключевых слов и параметров используется символ | с обязательными пробелами до и после |
   Пример: spanning-tree mst link-type {point-to-point | shared}
   Выбор одного из параметров no arp {<ip-address> | <ip-prefix>}
   Ключевые слова и параметры Show spanning-tree mst {none | instance <0-15>}ng
5) Если необходимо выбрать одно ключевое слово или параметр, то для выделения используются прямоугольные скобки [ ]. Для разделения ключевых слов и параметров используется символ | с обязательными пробелами до и после |

Пример: debug ip tcp [recv | send]
Ключевые слова recv и send могут быть выбраны или не выбраны
show ip route [<ip-address> | <ip-prefix>] show interface [<if-name> | switchport]

6) Если необходимо выбрать группу из нескольких ключевых слов или параметров, следует добавить символ «*» после группы (Group) ключевых слов или параметров.
Пример: ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*
-j <count> <ip-address>* --- Несколько IP адресов могут быть добавлены последовательно
-k <count> <ip-address>* --- Несколько IP адресов могут быть добавлены последовательно
7) Если параметр представлен одним и более словами, следует разделить слова символом «-» и использовать строчные буквы
Пример (правильно): <vlan-id>, <if-name>, <router-id>, <count>
Пример (не правильно): <1-255>, <A.B.C.D>, <WORD>, <IFNAME>

2.3.4 Command abbreviation (Сокращения)

При вводе команд в CLI интерфейс, допустимо использование сокращенной записи ключевых слов. CLI поддерживает использование префиксов, соответствующих ключевым словам. В зависимости от уникальности префикса, CLI определяет соответствующую ключевому слову команду. Эта функция создает дополнительное удобство для пользователей CLI, т.к. сокращает число вводимых символов необходимых для завершения команды.

Пример: команда show version ---- sh ver

2.3.5 Grammar help (Помощь)

Интерфейс CLI поддерживает функцию помощи (по синтаксису) для команд и параметров на каждом уровне.

1) При вводе в cli символа ? будет показано первое ключевое слово и описание всех связанных с ним команд.
   Пример: switch (config) #?
2) Введите первую часть команды, далее пробел и ?. Будут выведены все ключевые слова или параметры с описаниями.
   Пример: switch #show ?
3) Введите часть ключевого слова и символ ? Будут выведены все ключевые слова с описаниями относящиеся к введенному префиксу.
   Пример: switch #show ver?
4) Введите первую часть команды, далее пробел и tab. Будут выведены все ключевые слова для следующего уровня (кроме параметров, в этом случае информация не выводится).
5) Введите часть ключевого слова, далее tab. Если только одно ключевое слово соответствует префиксу, то он будет дополнен. Если префиксу соответствует несколько ключевых слов, то они все будут выведены.

2.3.6 Command line error message (Сообщения об ошибках)

Сообщение об ошибке появляется при вводе команд с неверным синтаксисом. Типовые сообщения об ошибках приведены в таблице ниже:

Таблица типовых сообщений об ошибках.

Сообщение	Причина ошибки
Invalid input or Unrecognized command	Не найдено ключевое слово. Введен некорректный параметр. Введено слишком много ключевых слов или параметров.
Incomplete command	Неполная команда, не введено ключевое слово или параметр.
Ambiguous command	Неполная команда, несколько ключевых слов соответствует префиксу.

3. System management (Конфигурация управление системой)

Перед переходом к изучению дальнейших возможностей по конфигурированию коммутатора следует провести настройку некоторых основных параметров управления системой. В этом разделе описываются основные настройки системы управления коммутатором:

- System security configuration (Конфигурация системы безопасности)
- System maintenance and commissioning (Обслуживание и эксплуатация)
- Monitoring system (Мониторинг системы)
- Profile management (Управление профилем)

3.1 System security (Конфигурация системы безопасности)

Для предотвращения допуска неавторизованных лиц к управлению коммутатором предусмотрен ряд настроек которые включают следующие:

- Multi user management control (Управление многопользовательским режимом)
- Enable Password control (Защита паролем)
- TELNET service control (Управление TELNET)
- SNMP service control (Управление SNMP)
- HTTP service control (Управление HTTP)

3.1.1 Multi user management control (Многопользовательский режим)

Многопользовательский режим повышает безопасность системы и обеспечивает возможность управления и обслуживания коммутатора несколькими пользователями одновременно. Многопользовательский режим обеспечивает безопасность путем индивидуальной аутентификации пользователей (присвоение каждому пользователю своего имени и пароля для входа в систему). При настройке

многопользовательского режима устанавливаются определенные права для каждого пользователя.

Многопользовательский режим предусматривает два уровня прав для пользователей: обычный и привилегированный. Обычные пользователи могут использовать только обычный режим командной строки CLI, команды display для просмотра информации о коммутаторе. Привилегированные пользователи могут использовать все режимы командной строки CLI, все команды управления коммутатором.

Многопользовательский режим применяется только для управления через telnet и недоступен для управления через console. При управлении через console для входа в систему не требуется аутентификация, пользователь может непосредственно войти в командную строку CLI. При входе в систему через telnet требуется ввести имя пользователя и пароль. Доступ к командной строке CLI возможен только после успешной аутентификации.

По умолчанию *имя пользователя и пароль* **admin**. Пользователь admin является администратором (привилегированным пользователем), его настройки не могут быть изменены на обычного пользователя, и он не может быть удален.

Таблица команд многопользовательского режима.

Команда	**Описание**	**CLI ржим**
username <user-name> password <key> {normal | privilege}	Добавление пользователя, изменение пароля, прав пользователя (если пользователь уже существует). 1й параметр - user name, 2й параметр - пароль, опционально - права пользователя (normal – обычный, privilege – привилегированный).	Global configuration mode
no username [user-name]	Удалить пользователя.	Global configuration mode

show running-config	Просмотр текущей конфигурации системы, конфигурации многопользовательского режима.	Privileged mode

3.1.2 Enable password control (Управление аутентификацией)

Управление аутентификацией применяется для перевода управления коммутатора из обычного режима в привилегированный режим. Перед включением аутентификации пользователю доступна для просмотра только информация о коммутаторе. После включения и прохождения аутентификации пользователь получает доступ к настройкам коммутатора.

Возможность включения аутентификации не имеет привязки к конкретному пользователю. Любой пользователь, который входит через console или telnet в привилегированный режим управления должен ввести корректный пароль. После успешной аутентификации пользователь также может оставаться в обычном режиме управления.

При вводе команды в обычном режиме пользователю необходимо ввести пароль. После успешной аутентификации система перейдет в привилегированный режим управления. В противном случае система останется в обычном режиме управления.

При включенной аутентификации система по умолчанию не будет требовать ввод пароля для входа в обычный режим.

Таблица команд управления режимом аутентификаци.

Команда	Описание	CLI режим
enable password <key>	Установка пароля для входа в систему.	Global configuration mode
no enable password	Удаление пароля, «пустой» пароль.	Global configuration mode
show running-config	Просмотр текущей конфигурации, в т.ч. пароля.	Global configuration mode
enable	Включение режима аутентификации. Переход	Global configuration

	в привилегированный режим.	mode

Для обеспечения безопасности системы администратору следует включить режим аутентификации и установить пароль.

3.1.3 TELNET service control (Управление TELNET сервисом)

В случаях когда отсутствует необходимость дистанционного управления коммутатором и управление осуществляется локально через console, для обеспечения безопасности системы и предотвращения неавторизованного дистанционного управления, администратор может отключить управление по telnet (включено по умолчанию). Команды приведены в таблице ниже:

Таблица команд управления telnet сервисом

Команда	Описание	CLI ржим
security-manage telnet enable	Включить telnet	Global configuration mode
security-manage telnet disable	Отключить telnet	Global configuration mode
security-manage telnet number <1-100>	Диапазон параметра от1 до 100, по умолчанию 5.	Global configuration mode
security-manage telnet access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage telnet access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

3.1.4 SNMP Service control (Управление SNMP сервисом)

Управление сервисом SNMP и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off). Команды приведены в таблице ниже:

Таблица команд управления SNMP сервисом

Команда	Описание	CLI ржим
security-manage snmp enable	Включить SNMP	Global configuration mode
security-manage snmp disable	Отключить SNMP	Global configuration mode
security-manage snmp access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage snmp access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

3.1.5 HTTP Service control (Управление HTTP сервисом)

Управление сервисом HTTP и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off). Команды приведены в таблице ниже:

Таблица команд управления HTTP сервисом:

Команда	Описание	CLI ржим
security-manage http enable	Включить HTTP	Global configuration mode

security-manage http disable	Отключить HTTP	Global configuration mode
security-manage http access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage http access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

3.1.6 HTTPS Service control (Управление HTTPS сервисом)

Управление сервисом HTTPS и IP адресом доступа к коммутатору через ACL может быть включено или отключено (on / off). Команды приведены в таблице ниже:

Таблица команд управления HTTPS сервисом

Команда	Описание	CLI ржим
security-manage https enable	Включить HTTPS	Global configuration mode
security-manage https disable	Отключить HTTP	Global configuration mode
security-manage https access-group <1-99> (Note: subject to the actual product)	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage https access-group	Отключить управление IP адресом.	Global configuration mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

3.1.7 SSH Service control (Управление SSH сервисом)

Многие программы сетевого сервиса такие как FTP, pop и Telnet не являются безопасными т.к. передают данные и пароли открытым текстом, что делает возможным их перехват злоумышленниками. Методы обеспечения безопасности этих сервисов имеют ряд уязвимостей для атак типа «middleman» (ретрансляция данных через промежуточный сервер). При использовании сервиса SSH производится шифрование передаваемых данных, что делает атаки типа «middleman» не эффективными, кроме того предотвращается DNS spoofing и IP spoofing. Еще одним преимуществом сервиса SSH является сжатие передаваемых данных и повышение скорости передачи.

Сервис SSH не заменяет Telnet, но обеспечивает безопасный канал передачи данных для FTP, pop и PPP. Команды приведены в таблице ниже:

Таблица команд управления SSH сервисом

Команда	Описание	CLI ржим
security-manage ssh enable	Включить ssh	Global configuration mode
security-manage ssh disable	Отключить ssh	Global configuration mode
security-manage ssh access-group <1-99>	Выбор группы ACL, вкл управление IP адресом. Если группа ACL нестандартная или отсутствует, управление IP адресом будет невозможно.	Global configuration mode
no security-manage ssh access-group	Отключить управление IP адресом.	Global configuration mode
ip sshd auth-retries <times>	Установить количество попыток аутентификации.	Global configuration mode
ip sshd silence-period <seconds>	Установить время ожидания после исчерпания всех попыток аутентификации.	Global configuration mode
show ip sshd	Просмотр конфигурации настроек sshd	Privileged mode
show security-manage	Просмотр конфигурации управления сервисом.	Privileged mode

3.2 System maintenance and commissioning (Обслуживание системы)

Подготовка к эксплуатации и дальнейшее обслуживание коммутатора включает в себя следующие пункты:

- Configure the system clock (Настройка системных часов)
- Configure terminal timeout attribute (Настройка времени бездействия)
- System reset (Сброс системы)
- View system information (Просмотр системной информации)
- Network connectivity debugging (Устранение сетевых неполадок)
- Traceroute debugging (Устранение неполадок маршрутизации)

3.2.1 Configure the system clock (Настройка системных часов)

В коммутаторе предусмотрены системные часы, которые синхронизированы с реальным временем. С помощью команд можно устанавливать и просматривать текущее время. Для удобства эксплуатации коммутатора системные часы обеспечены встроенным питанием, которое делает не нужной установку времени после длительного отключения коммутатора от энергоснабжения. После первого включения коммутатора следует проверить точность установки системных часов и при необходимости откорректировать.

Таблица команд управления системными часами

Команда	Описание	CLI ржим
set date-time <year> <month> <day> <hour> <minute> <second>	Установка текущего времени и даты в последовательности: год, месяц, день, час, минуты, секунды (вводятся значения параметров).	Privileged mode
show date-time	Просмотр текущей даты и времени системных часов.	Normal mode. privileged mode

3.2.2 Configure terminal timeout attribute (Настройка времени бездействия)

Для обеспечения безопасности в коммутаторе предусмотрена функция автоматического выхода из режима управления при бездействии, по истечении определенного интервала времени, который может быть изменен пользователем.

Процессы выхода из режима управления через console и telnet различаются. При управлении через console по истечении временного интервала, командная строка CLI переходит в обычный режим. При управлении через telnet по истечении временного интервала, соединение telnet прерывается, коммутатор выходит из режима управления. По умолчанию временной интервал бездействия составляет 10 мин, пользователь может изменить его или отключить эту функцию.

Таблица команд настройки времени бездействия

Команда	Описание	CLI ржим
exec-timeout <minutes> [seconds]	Установка времени бездействия. При выборе значения параметра 0, функция будет отключена.	Global configuration mode
no exec-timeout	Установка времени бездействия 10 мин (заводская установка, по умолчаню).	Global configuration mode
show running-config	Просмотр текущей конфигурации системы, в т.ч. установленного времени бездействия.	Privileged mode

3.2.3 System reset (Сброс системы)

Таблица команды сброса системы

Команда	Описание	CLI ржим
reset	Сброс системы	Privileged mode

3.3 Profile management (Управление профилем)

Существует два типа конфигурации: текущая (current configuration) и стартовая (initial configuration). Текущая конфигурация создается с учетом требований эксплуатации коммутатора и хранится в памяти системы. Стартовая конфигурация используется при первичном включении коммутатора и хранится на внутренней flash памяти коммутатора (configuration file). При использовании соответствующих команд стартовая конфигурация может быть изменена. Команда Save (сохранить) позволяет сохранить внесенные изменения и при последующем запуске будет загружена уже измененная (текущая) конфигурация.

Файлы конфигурации имеют тот же формат что и текст командной строки (прост и интуитивно понятен). Формат файла конфигурации имеет следующий вид:

- Файл состоит из текстовых команд.
- Может быть сохранена только измененная конфигурация, неизмененная конфигурация не сохраняется
- Формат команд аналогичен применяемому в командной строке. Команды объединены в сегменты, сегменты разделяются знаком "!". В режиме global configuration команды со сходными значениями объединены в секции, разделяются знаком "!".
- В режиме configuration sub mode, перед командой должен стоять пробел, в режиме global configuration mode пробел перед командой должен отсутствовать.
- Файл конфигурации заканчивается командой "end".

Команды управления файлом конфигурации включают следующие:

- View configuration information (Просмотр конфигурации)
- Save configuration (Сохранение конфигурации)
- Delete configuration profile (Удаление конфигурации)
- Download from configuration file (Загрузка конфигурации)

3.3.1 View configuration information (Просмотр конфигурации)

Пользователь имеет возможность просмотра текущей (current configuration) и стартовой (initial configuration) конфигурации системы. Файл конфигурации хранится на внутренней flash памяти коммутатора, если файл конфигурации отсутствует, то при включении коммутатора загружаются заводские настройки (по умолчанию). В этом случае при вводе команды для просмотра стартовой конфигурации, система выдаст сообщение об отсутствии файла.

Таблица команд просмотра конфигурации

Команда	Описание	CLI ржим
show running-config	Просмотр текущей конфигурации системы.	Privileged mode
show startup-config	Просмотр стартовой конфигурации системы.	Privileged mode

3.3.2 Save configuration (Сохранение конфигурации)

После внесения изменений в текущую конфигурацию системы пользователь имеет возможность сохранить эти изменения для того чтобы при последующем включении коммутатора загрузилась последняя сохраненная версия конфигурации. В противном случае при включении коммутатора будет загружена конфигурация без учета внесенных изменений.

Таблица команд сохранения конфигурации

Команда	Описание	CLI ржим
write	Сохранить текущую конфигурацию	Privileged mode

Внимание *!* Если пользователь не сохранит последние внесенные в текущую конфигурацию изменения, то при выключении коммутатора изменения настроек будут потеряны. При последующем включении коммутатора будет загружена последняя сохраненная конфигурация.

3.3.3 Delete configuration file (Удаление файла конфигурации)

Если пользователю необходимо чтобы при включении были загружены заводские настройки системы (настройки по умолчанию), то следует удалить файл конфигурации. Удаление файла конфигурации не приводит к изменениям в текущей конфигурации до выключения коммутатора. Для возвращения к заводским настройкам после удаления файла следует перезагрузить коммутатор.

Таблица команд удаления файла конфигурации

Команда	Описание	CLI ржим
delete startup-config	Удаление файла конфигурации	Privileged mode

Внимание *!*
Будьте внимательны, удаление файла конфигурации приведет к потере текущей конфигурации после перезагрузки коммутатора.

3.3.4 Download configuration file (Загрузка файла конфигурации)

В случае повреждения или удаления файла конфигурации или необходимости вернуться к заводской конфигурации коммутатора предусмотрена возможность загрузки заводского файла с ПК в память коммутатора.

Загрузка заводского файла конфигурации не приводит к изменениям в текущей конфигурации до выключения коммутатора. Для возвращения к заводским настройкам после загрузки файла следует перезагрузить коммутатор.

Загрузка и скачивание файла конфигурации также доступна через web, подробно процедура описана в полной инструкции по эксплуатации коммутатора.

Таблица команд загрузки файла конфигурации

Команда	Описание	CLI ржим
upload configure <ip-address> <file-name>	Скачивание файла конфигурации на ПК.	Privileged mode

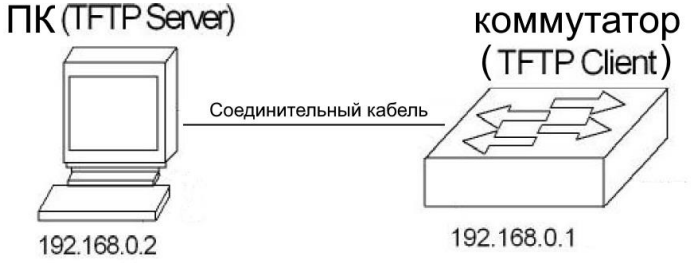
	1й параметр IP адрес ПК 2й параметр имя файла.	
download configure <ip-address> <file-name>	Загрузка файла конфигурации в коммутатор. 1й параметр IP адрес ПК 2й параметр имя файла.	Privileged mode

Загрузите файл конфигурации в коммутатор, используйте протокол TFTP. Запустите TFTP client на коммутаторе и TFTP на ПК. Далее действуйте по пунктам ниже:

Шаг 1: Сформируйте сетевое окружение.
Шаг 2: Сохраните файл конфигурации TFTP software на ПК.
Шаг 3: Сохраните файл конфигурации на коммутаторе.
Шаг 4: Запустите команду configuration file upload на коммутаторе для скачивания файла конфигурации на ПК.
Шаг 5: При необходимости запустите команду configuration file download command на коммутаторе для загрузки файла конфигурации в коммутатор.
Шаг 6: Перезагрузите коммутатор для обновления конфигурации.

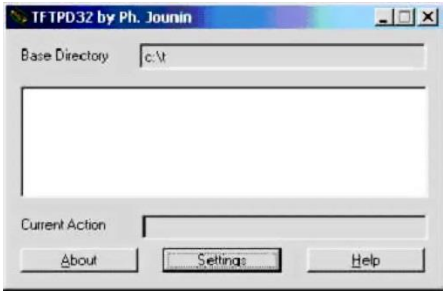
Пример: Загрузка и скачивание файла конфигурации на коммутатор с VLAN и IP адресом.

Шаг 1: Сетевое окружение.

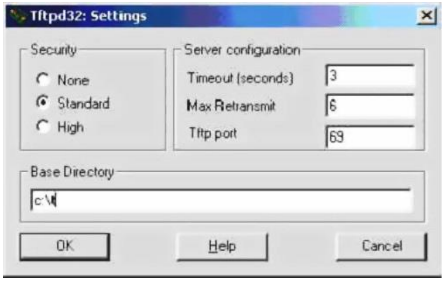


Соединить ПК с конфигурационным портом коммутатора сетевым кабелем. Установить TFTP server на ПК и установить IP адрес сетевого адаптера (например 192 168.0.2) в одной подсети с IP адресом коммутатора (по умолчанию 192.168.0.1), проверить наличие соединения.

Шаг 2: Запустите TFTP сервер на ПК и сконфигурируйте его параметры.



Откройте директорию с файлом конфигурации, далее нажмите [settings].



Введите путь в base directory и нажмите [OK] для завершения.

Шаг 3: Введите команду write на коммутаторе для Сохранения файла текущей конфигурации.

Шаг 4: Запустите команду configuration file upload на коммутаторе для скачивания файла конфигурации на ПК (192 168.0.2).

Шаг 5: Для загрузки файла конфигурации с ПК (192 168.0.2) в коммутатор запустите команду configuration file download command на коммутаторе.

Шаг 6: Для обновления конфигурации вводом команды switch#reset перезагрузите коммутатор.

4. MSTP Configure (Конфигурация MSTP)

4.1 MSTP introduction (Введение)

Протокол MSTP (Multiple Spanning Tree Protocol) является расширением протокола RSTP и позволяет настраивать отдельное связующее *дерево* для любой *VLAN* или группы *VLAN*, создавая множество маршрутов передачи трафика. Таким образом, множество VLAN агрегируются в разветвленную сеть с независимой топологией. Такая архитектура обеспечивает множественную маршрутизацию потоков данных, распределяет нагрузку, снижает зацикливание и поддерживает большое количество VLAN в сети. Протокол MSTP обратно совместим с протоколами STP и RSTP.

Коммутатор поддерживает IEEE802.1d, IEEE802.1w, IEEE802.1s STP стандарты и протоколы.

4.1.1 Multi spanning tree domain (MST домен)

Для корректной работы протокола multi spanning tree (MST) должны быть последовательно проведены соответствующие MST настройки коммутатора. Настройки коммутатора связанные с MST являются MST доменом.

Конфигурация MST определяет домен к которому относится каждый коммутатор. Конфигурация включает имя домена, номер revision number, MST instance и VLAN assignment mapping. На основе этой информации генерируется уникальный элемент (digest) конфигурации MST, соответствующий элементу summaries домена (эти элементы должны быть одинаковыми). Информация о настройках MST выводится по команде show spanning tree MST config.

Домен может иметь один или несколько членов с одной и той же конфигурацией MST. Каждый член должен обладать возможностью поддерживать RSTP BPDU. Количество MST доменов в сети не ограничено, но каждый домен поддерживает до 16и instances. Каждому spanning tree instance может соответствовать один VLAN.

4.1.2 IST, CIST, CST

Internal spanning tree (IST) специальная копия связующего дерева, которая по умолчанию существует в каждом MST домене. Она может отправлять и получать кадры BPDU и служит для управления топологией внутри домена. В каждом MST домене MSTP обслуживает множество создаваемых instances. Instance 0 – специальный instance домена, который называется ist. Все остальные MST instances имеют номера от 1 до 15.

Для отправления и получения BPDU используется ist. Вся другая информация о spanning tree instance в сжатом виде содержится в MSTI BPDU. Т.к. MSTI BPDU содержит информацию о всех instances, то она должна быть обработана коммутатором поддерживающим multiple spanning tree instances. Номера BPDU означают упрощение.

Все MST instances в домене используют один таймер протокола, но каждый MST instance имеет свои собственные технологические параметры, такие как ID маршрутного коммутатора, root path cost и т.д. По умолчанию все VLAN относятся к ist.

Common и internal spanning tree (CIST) являются сборником всех ist в каждом MST домене и общим spanning tree (соединяют MST домен и single spanning tree).

Spanning tree вычисляемая внутри домена, является subtree относящейся к CST, которая содержит все домены коммутатора. CIST формируется по результатам вычислений spanning tree протоколами 802.1w и 802.1d. CIST в MST домене такая же как CST вне домена.

Common spanning tree (CST) это spanning tree разворачиваемая между MST доменами.

4.1.3 Intra domain operation (Операции в домене)

Ist соединяет все MSTP коммутаторы в домене. Когда ist создает маршрут, то ist становится ist master (мастером), коммутатором с низшим мостом ID и высшим соединением с маршрутом CST в домене. Если в сети только один домен, ist master является CST маршрутом.

Если CST маршрут проходит вне домена, MSTP коммутатор находящийся на границе домена выбирается как ist master.

При запуске MSTP коммутатора, он отправляет запрос BPDU на назначение его как маршрут CST и ist master и path cost к маршруту CST, ist master устанавливается на 0. Одновременно коммутатор инициализирует все MST instances и запрашивает возможность быть их маршрутизатором. Если коммутатор получает информацию MST маршрутизации, то он становится главенствующим по данным хранящимся в текущем порту (low bridge ID, low path cost и т.д.), требование стать ist master отменяется.

В процессе инициализации, домен может получить несколько суб-доменов, каждый со своим собственным ist master. Когда коммутатор получает более высокоприоритетное ist сообщение, он покидает старый суб-домен и вступает в новый суб-домен, который может содержать реальный ist master. Таким образом, все суб-домены сокращаются, кроме тех которые содержат реальные ist master.

Для корректного функционирования все коммутаторы MST домена должны опознавать один и тот же ist master. Коммутаторы в любых двух доменах синхронизируют роли порта одного из их MST instances только в том случае если они сходятся в публичном ist master.

4.1.4 Inter domain operation (Операции между доменами)

Если в сети присутствует несколько доменов или коммутаторов ранних моделей с поддержкой протокола 802.1d, MSTP создает и обслуживает CST, которые включают MST домены и коммутаторы ранних моделей с STP во всех сетях. MST instances включаются в ist на границе домена чтобы стать CST.

Ist соединяет все коммутаторы в MSTP домене и имеет вид subtree в CST (охватывая все коммутаторы и домены). Маршрутизатор subtree становится ist master. MST домен принимает вид виртуального коммутатора, примыкающего к коммутатору STP и MST домену.

Только CST instances отправляют и получают BPDU, MST instances добавляют информацию о своем spanning tree в BPDU, взаимодействуют с соседними коммутаторами и рассчитывают

финальную топологию spanning tree. По этому параметры spanning tree относятся к передаче BPDU (hello time, forward time, Max age and Max hops) и конфигурируются только в CST instances, но не оказывают влияния на все MST instances. Параметры относящиеся к топологии spanning tree (switch priority, port VLAN cost, port VLAN priority) могут быть сконфигурированы в CST instances и MST instances.

Коммутаторы MSTP используют версию 3 RSTP BPDU или 802.1d BPDU для коммуникации с коммутаторами поддерживающими протокол 802.1d. Коммутаторы MSTP используют MSTP BPDU для коммуникации с коммутаторами MSTP.

4.1.5 Skip count (Пропуск счета)

В BPDU конфигурирующим расчет топологии spanning tree, ist и MST instances не используют сообщения age и maximum age information. Вместо этого используется path cost маршрута и механизм hop count эквивалентный IP TTL.

Можно установить наибольшее число hops в домене и применить его для ist и всех MST instances в этом домене. Имплементация расчета hop count такая же как для message age (определяется после triggering a reconfiguration). Instance root коммутатор всегда отправляет BPDU (or-m-record) с cost 0 и hop count максимального размера. Когда коммутатор получает BPDU, он вычитает оставшиеся hops по одному и возвращает оставшиеся hops их сгенерировавшему BPDU. Когда счет достигает 0, коммутатор отбрасывает BPDU и обновляет информацию порта.

В домене сообщения message age и maximum age information в части RSTP BPDU остаются такими же, оставшаяся часть такая же, и то же значение передается на специальный порт на границе домена.

4.1.6 Boundary port (Граничный порт)

Граничный порт – это домен spanning tree, который соединяет MST домен с отдельным RSTP running spanning tree доменом, или

отдельным 801.1d spanning tree доменом, или другим MST доменом с отличающейся конфигурацией. Граничный порт соединен с LAN. Назначенный коммутатор LAN это любой отдельный spanning tree коммутатор или коммутатор с другой конфигурацией MST домена.

В граничном порту роль MST порта не важна, и их статус устанавливается таким же, как и у ist порта (когда ist port отправляет данные, MST порт на границе тоже отправляет данные). Ist порт на границе может иметь роль отличную от backup port.

При граничном соединении (shared boundary), MST порт ожидает истечения времени задержки отправки данных в заблокированном статусе в режиме learning state. MST порт ожидает истечение другой временной задержки для перехода в режим отправки данных.

Если граничный порт подключен в режиме точка-точка и является ist root port (маршрутным), MST порт переключится в режим отправки данных, как только ist port изменит свой режим на отправление.

Если граничный порт переходит в режим отправления в instance, то он отправляет все instances и топология изменяется. Если граничный порт с маршрутом ist root или выделенный порт получит уведомление об изменении топологии, то ist instance и все MST instances на активном порту MSTP коммутатора получат изменение топологии.

4.1.7 Interoperability MSTP and 802.1d STP (Совместимость)

Коммутатор MSTP поддерживает встроенный протокол механизма миграции, который используется координации взаимодействия с 802.1d. Если коммутатор получает 802.1d конфигурированный BPDU от порта, то он отправляет 802.1d BPDU на этот порт. Когда граничный порт домена получает 802.1d BPDU, MSTP BPDU или RSTP BPDU от другого домена, MSTP коммутатор может принять его.

Если коммутатор перестает получать 802.1d BPDU, то он не возвращается в режим MSTP автоматически, потому что он не может определить находится ли передающий коммутатор в соединении пока не определен его статус (назначение). Когда подключенный (к первому)

коммутатор становится членом домена, первый коммутатор может продолжить определять назначение роли порта и начать процесс миграции протокола (force negotiation with the neighbor switch).

Если все коммутаторы поддерживают RSTP, то они все могут поддерживать MSTP BPDU и RSTP BPDU. Таким образом, MSTP коммутаторы могут отправлять любую версию конфигурации (version 0), TCN BPDU или версию 3 MSTP BPDU на граничный порт. Для граничного порта соединенного с LAN, назначенный коммутатор может иметь отдельное spanning tree или это может быть коммутатор с другой MST конфигурацией.

4.1.8 Port role (Роль порта)

MSTP использует быстрый алгоритм конвергации RSTP. Ниже описываются основные моменты взаимодействия MSTP port roles и быстрой конвергенции в сочетании с RSTP.

RSTP обеспечивает быструю конвергенцию ролей порта (port roles) и определения активной топологии. RSTP основывается на протоколе IEEE802 1D STP, выбирает высокий приоритет для коммутатора, как маршрутного. Когда RSTP определяет роль для порта:

Root port (маршрутный порт) – обеспечивает оптимальный путь (path cost) когда коммутатор отправляет данные на маршрутный коммутатор.

Designated port (назначенный порт) – связан и соединен с назначенным коммутатором. Когда LAN отправляет пакеты данных маршрутному коммутатору, создается lowest path cost (путь низшего порядка). Указанный порт (specified port) связан с указанным коммутатором, который соединяется с LAN.

Alternate port (альтернативный порт) - обеспечивает альтернативный путь к порту маршрутного коммутатора.

Backup port (резервный порт) – обеспечивает запасной путь от выделенного порта к spanning tree. Резервный порт существует только когда два порта соединены вместе (точка-точка), или когда два или более коммутаторов объединены в сегмент LAN (shared).

Disable port (отключенный порт) – роль порта в работе spanning tree отсутствует.

Master port (мастер порт) – находится в маршруте домена или

кратчайший путь в общем маршрутет, т.е. порт соединяет домен с общим маршрутом.

Роль маршрутного порта или определенного порта участвует в работе активной топологии. Роль замещающего или резервного порта не участвует в работе активной топологии.

В масштабе всей сети со стабильной топологией и фиксированными ролями портов, RSTP обеспечивает немедленный переход маршрутных и определенных портов в статус отправления данных, когда все замещенные и резервные порты находятся в статусе сброса. Статус порта (Port status) определяет состояние отправки или обучения (learning) порта.

Быстрая конвергенция.

RSTP обеспечивает быстрое восстановление работоспособности в следующих случаях: сбой работы коммутатора, сбой работы порта или сбой работы LAN. Обеспечивается быстрое восстановление крайних портов (edge ports), новых маршрутных портов и соединений точка-точка.

Edge Ports (крайние порты) – при данной конфигурации порта, крайний порт немедленно переходит в статус отправки (forwarding state). Порт может быть открыт как связанный порт (boundary port) только в случае если порт соединен с отдельным терминалом или с коммутатором который не участвует в расчете spanning tree.

Root Ports (маршрутные порты) – Если протокол RSTP выбирает новый маршрутный порт, то старый маршрутный порт блокируется а новый немедленно изменяет свой статус на отправление (forwarding state).

Point to point links (соединение точка-точка) – когда порты соединяются как точка-точка локальный порт становится назначенным (designated port), происходит соединение со связанным с ним портом посредством proposal agreement handshake для определения быстрой конвергенции по петлевой технологии (fast convergence loop free topology).

Изменение топологии. Ниже описываются различия между протоколами RSTP и 802.1d при развертывании технологии spaning tree topology.

Detection (детектирование) – в протоколе 802.1d любые изменения статусов заблокировано (blocking) и отправление (forwarding)

вызывают изменение топологии. В протоколе RSTP только изменение статуса от блокировки к передаче вызывает изменение топологии (увеличение количества соединений). Изменение статуса крайнего порта не вызывает изменения топологии. Когда RSTP коммутатор обнаруживает изменение топологии, он передает информацию всем не крайним портам, кроме порта принимающего TC информацию.

В отличие от протокола 802.1d, который использует TCN BPDU, протокол RSTP эту информацию не использует. Для взаимодействия с протоколом 802.1d RSTP коммутатор генерирует и обрабатывает TCP BPDU.

Когда RSTP коммутатор получает сообщение с TCN от 802.1d коммутатора на определенный порт, он откликается на BPDU с 802.1d и устанавливает флаговый TCA бит. Если TC во время отсчета таймера (того же что и таймер смены топологии в 802.1d) активен, соединен с маршрутным портом 802.1d коммутатора и получает конфигурацию BPDU с TCA, TC будет перезапущен (restart \ reset). Это действие требуется для поддержки 802.1d коммутаторов. RSTP BPDU не имеет флагового TCA бита.

Propagation (распространение) – когда RSTP коммутатор получает TC сообщение от других коммутаторов через определенный или маршрутный порт, то он передает всем не крайним портам, определенным портам и маршрутным портам (кроме принимающего порта receiving port). Все такие порты коммутатора запускают TC во время отсчета таймера и передают полученную (learned) информацию.

Protocol migration (миграция протокола) – для обеспечения обратной совместимости с 802.1d коммутаторами, RSTP выборочно отправляет 802.1d BPDU конфигурацию и TCN BPDU основанную на каждом порту. При инициализации запускается таймер задержки (минимум определяется в течение периода когда отправляется RSTP BPDU), и отправляется RSTP. Во время отсчета таймера, коммутатор обрабатывает все BPDU полученные от порта и игнорирует тип протокола.

После прерывания таймера миграции, если коммутатор получает 802.1d BPDU, он предполагает что он соединен с 802.1d коммутатором и начинает использовать 802.1d протокол BPDU. Если RSTP коммутатор использует 802.1d BPDU на порту и получает RSTP BPDU после прерывания таймера, порт перезапустит таймер и начнет использовать RSTP BPDU.

4.1.9 802.1D spanning tree Introduction (Введение)

Протокол spanning tree основывается на следующих пунктах:

- Уникальный групповой адрес (group address) (01-80-c2-00-00-00) определяет все коммутаторы принадлежащие LAN. Этот адрес может быть опознан всеми коммутаторами.
- Каждый коммутатор имеет уникальную идентификацию.
- Каждый порт каждого коммутатора имеет уникальный идентификатор. Для управления конфигурацией spanning tree необходима координация относительного приоритета каждого коммутатора, приоритета каждого порта каждого коммутатора и учета значимости пути каждого порта.

Маршрутный коммутатор имеет наивысший приоритет. Каждый порт коммутатора имеет значимость пути (root path cost), которая является суммой значимостей путей каждого сегмента сети от коммутатора к маршрутному коммутатору. Порт с минимальной значимостью пути называется маршрутным (root port). Если несколько портов имеют одинаковую значимость пути (root path cost), порт с наивысшим приоритетом становится маршрутным портом.

В каждом LAN существует назначенный коммутатор (designated switch), который принадлежит коммутатору с наименьшей значимостью пути в LAN. Порт соединяющий LAN и назначенный коммутатор называется назначенным портом LAN. Если более двух портов определенного коммутатора соединены с LAN, то порт с наивысшим приоритетом выбирается назначенным.

Необходимые элементы решений spanning tree:

- Определение маршрутного коммутатора. Сначала все коммутаторы считаются маршрутными. Коммутатор отправляет конфигурацию BPDU в LAN, свой root_ ID, Bridge_ ID (одинаковые значения). Когда коммутатор получает конфигурацию BPDU от другого коммутатора и если он находит путь в принятой конфигурации BPDU_ поле ID превышает число маршрутов коммутатора, значение ID параметра, то кадр будет сброшен. В противном случае маршрут коммутатора будет обновлен (ID, root path cost root_ path_ Cost и пр.), коммутатор продолжит отправлять конфигурацию BPDU с обновленными данными.

- Определение маршрутного порта. Порт с минимальным значением root path cost в коммутаторе назначается маршрутным. Если несколько портов имеют одинаковое минимальное значение root path cost, то порт с наивысшим приоритетом назначается маршрутным. Если два и более порта имеют одинаковое минимальное значение и одинаковый приоритет, то порт с меньшим номером назначается маршрутным.

- Назначенный коммутатор LAN. Сначала все коммутаторы считаются назначенными в LAN. Когда коммутатор получает BPDU от другого коммутатора (из того же LAN) с меньшим значением root path cost, коммутатор перестает считать себя назначенным. Если два и более коммутаторов в LAN имеют одинаковое значение root path cost, коммутатор с наивысшим приоритетом становится назначенным.

- Если назначенный коммутатор получает конфигурацию BPDU от другого коммутатора LAN который считает себя назначенным, первый назначенный коммутатор отправляет в ответ конфигурацию BPDU для подтверждения своего назначения.

- Определение определенного порта (specified port). Порт определенного коммутатора соединенный с LAN называется определенным. Если определенный коммутатор имеет два и более портов соединенных с LAN, порт с наименьшей идентификацией назначается определенным. Кроме маршрутного и определенного портов, все остальные порты будут переведены в статус блокированных.
Т.о. после определения маршрутного коммутатора, маршрутного порта коммутатора, назначенного коммутатора, назначенного порта каждого LAN определяется топология spanning tree.

4.2 MSTP configuration (Конфигурация MSTP)

4.2.1 Default configuration (Конфигурация по умолчанию)

Таблица значений параметров настроек MSTP по умолчанию

Параметр команды	Значение
spanning-tree mst enable(start mstp) включение-отключение MSTP	Off (отключено)

Spanning-tree mst priority(Switch CIST priority) Приоритет коммутатора	32768
spanning-tree mst hello-time(Switch cist hello-time) Время отклика коммутатора cist hello-time	2 сек.
spanning-tree mst forward-time(Switch cist forward-time) Время отправки cist forward-time	15 сек.
spanning-tree mst max-age(Switch cist max-age) Максимальное время cist max-age	20 сек.
spanning-tree mst max-hops(Switch cist max-hops) Максимальное время cist max-hops	20 сек.
instance 1 priority (Priority instance) Приоритет instance 1	32768
spanning-tree mst instance 1 priority(Port instance priority) Приоритет порта instance 1	128
spanning-tree mst instance 1 path-cost(Port instance path-cost) Значение path-cost instance 1 порта	20000000
spanning-tree mst priority (Port cist priority) Приоритет порта	128
spanning-tree mst path-cost (Port cist path-cost) Значение path-cost порта	20000000

4.2.2 General configuration (Команды основной конфигурации)

Включить MSTP (при запуске коммутатора отключен по умолчанию).
Команды запуска MSTP:

Switch#configure terminal
Switch(config)#spanning-tree mst enable

Команды отключения MSTP:
Switch#configure terminal
Switch(config)#no spanning-tree mst

Установка параметра Max age.
Max age это конфигурация всех instances. Max age это время (в секундах), в которое коммутатор ожидает получения информации о конфигурации spanning tree, перед началом распознавания. Пределы

диапазона от 6 до 40 сек, значение по умолчанию 20 сек.
Команды конфигурации:

Switch#configure terminal

Switch(config)#spanning-tree mst max-age <seconds>

Установка Max hops

Max hops это количество отсчетов в установленных в домене до сброса BPDU. Пределы изменения параметра от 1 до 40, значение по умолчанию 20.

Команды конфигурации:

Switch#configure terminal

Switch(config)#spanning-tree mst max-hops <hop-count>

Установка времени отправки (forward time)

Конфигурация forward time для всех instances. Forward time это время (в секундах), которое порт ожидает от момента сброса до получения и от получения до отправления данных. Пределы диапазона от 4 до 30 сек, значение по умолчанию 15 сек. Согласно сгенерированному протоколом числу forward time должно соответствовать следующему условию: 2 * (forward time – 1) > = max age.

Команды конфигурации:

Switch#configure terminal

Switch(config)#spanning-tree mst forward-time <seconds>

Установка времени Hello time

Hello time является конфигурацией всех instances. Hello time это временной интервал (в секундах) генерации информации о конфигурации маршрутным коммутатором. Пределы диапазона от 1 до 10 сек, значение по умолчанию 2 сек. Согласно сгенерированному протоколом числу forward time должно соответствовать следующему условию: 2 *(Hello time + 1) = max age.

Команды конфигурации:

Switch#configure terminal

Switch(config)# spanning-tree mst hello-time <seconds>

Установка приоритета моста CIST Bridge

Значение параметра по умолчанию 32768, диапазон значений параметра < 0-61440 >, приоритет CIST является множественным значением 4096.

Команды конфигурации:

Switch#configure terminal
Switch(config)#spanning-tree mst priority <priority>

Установка конфигурации совместимой с Cisco

Сетевой коммутатор поддерживает протокол MSTP основанный на 802.1s, длина каждого MSTI сообщения составляет 16 бит. Длина каждого MSTI сообщения BPDU Cisco составляет 26 бит. Для обеспечения совместимости с коммутаторами Cisco, совместимый коммутатор должен быть запущен во время конфигурирования настроек сети.

При запуске конфигурации совместимой с Cisco, при определении домена имя домена, номер версии должны совпадать. По умолчанию функция отключена.

Команды включения функции совместимости Cisco:

Switch#configure terminal
Switch(config)#spanning-tree mst cisco-interoperability enable

Команды отключения функции совместимости Cisco:

Switch#configure terminal
Switch(config)#spanning-tree mst cisco-interoperability disable

Сброс протокола проверки задачи (Reset protocol check task)

Для обеспечения совместимости протоколов 802.1d и STP, система может автоматически определять протокол другой системы. Протокол исполняемый портом определяется согласно протоколу исполняемому на другой стороне.

В некоторых случаях требуется произвести сброс протокола. Например, после установления соединения система исполняет протокол STP на одном порту, через некоторое время устройство на другой стороне исполняющее протокол STP заменяется хостом. В этот момент требуется изменить конфигурацию порта на fast port, но данный порт исполняет STP протокол, и выполнение задачи согласования протоколов останавливается. Требуется сбросить задачу согласования протоколов и позволить начать согласование протокола с хостом.

Команды сброса задачи определения протокола (Reset protocol reconnaissance task для устройства в целом):

Switch#clear spanning-tree detected protocols

Команды сброса задачи определения протокола (Reset protocol reconnaissance task для порта):

Switch#clear spanning-tree detected protocols interface <if-name>

4.2.3 Domain configuration (Конфигурация домена)

Если два и более устройства входят в один домен, то для взаимодействия они должны иметь единый VLAN instance mapping relationship, одной версии и одно имя домена.

Домен включает в себя один или несколько членов с одной конфигурацией MST и каждый член поддерживает возможности RSTP BPDU. Отсутствует ограничение по числу членов в сети, но каждый домен может поддерживать до 16 instances.

Конфигурация instances описана в соответствующем разделе. Ниже представлена конфигурация имени домена и версии конфигурации.
Команды конфигурации имени домена (domain name)

Switch#configure terminal:
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region <region-name>

Команды конфигурации номера версии (revision number)

Switch#configure terminal:
Switch(config)#spanning-tree mst configuration
Switch(config-mst)# revision <revision-num>

4.2.4 Instance configuration (Конфигурация Instance)

Система поддерживает 16 instances, диапазон номеров (instance ID) от 0 до 15. VLAN может относиться только к одному spanning tree instance. По умолчанию существует только один instance 0, и все VLAN принадлежат этому instance.
Команды конфигурации instance:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Конфигурация приоритета MSTI Bridge
По умолчанию значение параметра 32768, диапазон значений параметра < 0-61440 >, приоритет MSTI является множественным значением 4096.

Команды конфигурации приоритета MSTI Bridge:

Switch#configure terminal

Switch(config)#spanning-tree mst configuration

Switch(config-mst)#instance <instance-id> priority <priority>

4.2.5 Port configuration (Конфигурация порта)

Ниже описывается информация о конфигурации порта относящаяся к MSTP (представлена простая конфигурация).

Команды конфигурации порта для включения в instance:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id>

Конфигурация приоритета порта CIST. Диапазон значений параметра от 0 до 240, по умолчанию значение 128, значение приоритета порта CIST может быть множественным до 16.

Команды конфигурации:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst priority <priority>

Конфигурация приоритета порта MSTI. Диапазон значений параметра от 0 до 240, по умолчанию значение 128, значение приоритета порта MSTI может быть множественным до 16.

Команды конфигурации:

Switch#configure terminal

Switch(config)#interface <if-name>

Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Конфигурация path cost порта CIST

По умолчанию значение параметра 20000000, диапазон значений параметра 1-200000000.

Таблица зависимости значений path cost mapping от пропускной (bandwidth)

bandwidth (bps)	Path cost
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Команды конфигурации path-cost:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst path <path-cost>

Конфигурация path cost порта MSTI

По умолчанию значение параметра 20000000, диапазон значений параметра 1-200000000. Взаимосвязь пропускной способности (bandwidth) и значения представлены в таблице выше.

Команды конфигурации path-cost порта MSTI:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>

Конфигурация номера версии отправляемого пакета протокола

Отправить пакет протокола MSTP с конфигурацией по умолчанию. Диапазон значений параметра конфигурации 0-3, mapping relationship 0-stp, 2-rstp, 3-mstp.

Команды конфигурации:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)# spanning-tree mst force-version <version-id>

Конфигурация типа соединения

Если порт соединен с другим портом в режиме точка-точка, локальный порт становится назначенным, RSTP устанавливает взаимосвязь

методом быстрой миграции по соглашению (proposal agreement process), соединенный порт становится маршрутным, определяется ациклична топология. Ниже описывается установление взаимосвязи путем процесса предложение-согласие (proposal agreement).
Когда порт коммутатора получает proposal сообщение и порт выбирается как новый маршрутный, RSTP заставляет остальные порты синхронизироваться с информацией нового маршрутного порта.
Если все остальные порты синхронизированы с первостепенной маршрутной информацией полученной от маршрутного порта, коммутатор считается синхронизированным.
Когда протокол RSTP заставляет синхронизироваться с новой маршрутной информацией, определенный порт в статусе отправки и не сконфигурирован как крайний порт, то он изменит свой статус на заблокированный. В основном, когда RSTP заставляет порт синхронизироваться с новыми маршрутными сообщениями, порт переходит в заблокированный статус.
Когда соглашение отправляется на соответствующий порт коммутатора, требуется подтверждение, что вся информация была отправлена. Когда коммутаторы соединены как точка-точка по соглашению с ролями портов, RSTP незамедлительно переводит порт в статус отправления.
В случае shared соединения, статус порта должен быть определен путем вычислительного процесса протокола 802.1d. По умолчанию установлен тип соединения точка-точка.
Команды установки соединения точка-точка (point-to-point):

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst link-type point-to-point
```

Команды установки соединения shared:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config-ge1/2)#spanning-tree mst link-type shared
```

4.2.6 PORTFAST Related configuration (Конфигурация PORTFAST)

Port Fast
Функция Port fast моментально изменяет статус access или trunk портов с заблокированного на передающий (forwarding), минуя статусы listening

и learning. Функция port fast может быть использована для соединения удаленной рабочей станции с сервером, который позволяет устройствам соединяться с сетью немедленно без ожидания развертывания spaning tree.
Команды установки fast port:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast

BPDU Filtering

Функция фильтрации BPDU filtering может быть включена на коммутаторе (global) или на каждом порту коммутатора, но некоторые параметры будут отличаться.
В режиме global layer, можно использовать spaning tree MST portfast BPDU команду для включения BPDU фильтрации на порту portfast BPDU filter.
В режиме port layer, можно использовать spaning tree MST portfast BPDU фильтр для открытия BPDU фильтра на каждом порту.
Эта функция закрывает port fast порт от получения или отправления BPDU.
Команды конфигурации BPDU фильтрации (global configuration mode):

Switch#configure terminal
Switch(config)# spanning-tree mst portfast bpdu-filter

Команды конфигурации BPDU фильтрации (interface configuration mode):

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast bpdu-filter enable

BPDU Guard

Защита BPDU может быть включена на коммутаторе (globally) или на каждом порту коммутатора, но некоторые параметры будут отличаться.
В режиме global layer, можно использовать spaning tree MST portfast BPDU для включения функции BPDU guard на порту portfast BPDU.
В режиме port layer, можно включить функцию BPDU guard на любом порту.
Когда порт с включенной функцией BPDU gurad получает BPDU, spaning tree отключает порт. В действующей конфигурации, port fast порт не получает BPDU. Получение BPDU port fast портом указывает на неправильную конфигурацию, как подключение неавторизованного

оборудования, BPDU guard переходит в статус отключения ошибки (error disabled state).
Статус отключения ошибки (Error disabled) означает что когда порт с включенной функцией BPDU gurad получает BPDU, система запускает таймер отключения ошибки. Функция Error disable перезапустит порт после истечения установленного времени.
Команды конфигурации (global configuration mode):

Switch#configure terminal
Switch(config)# spanning-tree mst portfast bpdu-guard

Команды конфигурации (interface configuration mode):

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast bpdu-guard enable

Команды включения error-disable:

Start the error disable mechanism
Switch#configure terminal
Switch(config)#spanning-tree mst errdisable-timeout enable

Команды конфигурации error disable timeout:

Switch#configure terminal
Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>

4.2.7 Root Guard Related configuration (Конфигурация Root Guard)

Современные сети уровня layer 2 могут содержать множество соединенных и связанных коммутаторов. В случае такой топологии, spanning tree может проводить собственную реконфигурацию и выбирать customer коммутатор как маршрутный (root). Для обхода этого следует сконфигурировать порт с помощью root guard SP коммутатора соединенного с коммутатором в customer сети. Если вычисления spanning tree приводят к тому, что порт customer сети выбирается маршрутным, функция root guard переводит порт в статус root inconsistent (blocked) для предотвращения назначения customer коммутатора маршрутным или путем маршрута.
Если коммутатор не принадлежащий SP сети становится маршрутным, порт блокируется (root inconsistent STAT) и spanning tree выбирает новый маршрутный коммутатор. Соответственно коммутатор не становится маршрутным и маршрутный путь будет отсутствовать.

Если коммутатор работает в режиме MST, функция root guard заставляет порт стать определенным (specified port). Если граничный порт (boundary port) заблокирован в ist instance функцией root guard, то этот порт блокируется и во всех MST instances. Граничный порт соединен с LAN. Определенный коммутатор должен поддерживать 802.1d или быть сконфигурированным в разных MST доменах.
Когда порт открыт, функция root guard применяется ко всем VLAN, которым принадлежит порт. VLANы могут быть агрегированы в MST instance.
Команды включения root guard:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst guard root
```

4.2.8 MSTP Configuration example (Пример конфигурации MSTP)

Конфигурация:
Три коммутатора соединены в по схеме кольцо. Требуется включить протокол spanning tree на каждом коммутаторе для предотвращения нарушения кольца. Конфигурация каждого коммутатора представлена отдельно.

Конфигурация коммутатора 1:

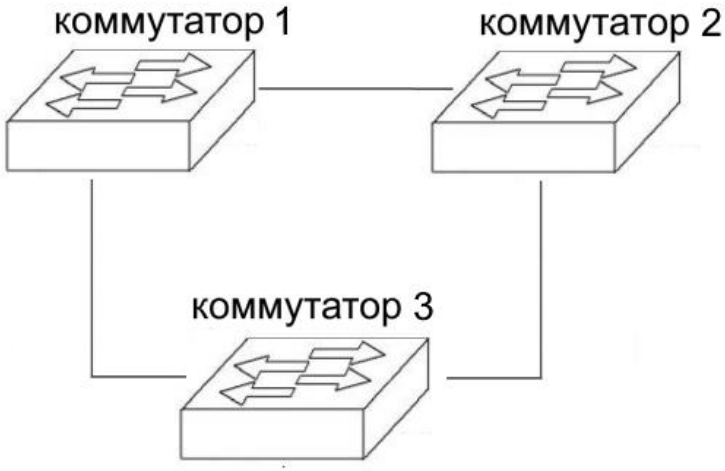
```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```

Конфигурация коммутатора 2:

```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```

Конфигурация коммутатора 3:

```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```



Внимание:

Проверьте какой коммутатор выбран как маршрутный (root bridge): Выполните просмотр spanning tree MST, убедитесь, что значение параметра cistroot соответствует наименьшему MAC адресу из трех, что результат выбора пути корректный.

Switch#show spanning-tree mst

Для просмотра статуса порта коммутатора в spanning tree выполните команду show spanning tree MST interface GE1/1 и убедитесь что значение параметра порта GE1/1 в instance 0.

Switch#show spanning-tree mst interface ge1/1