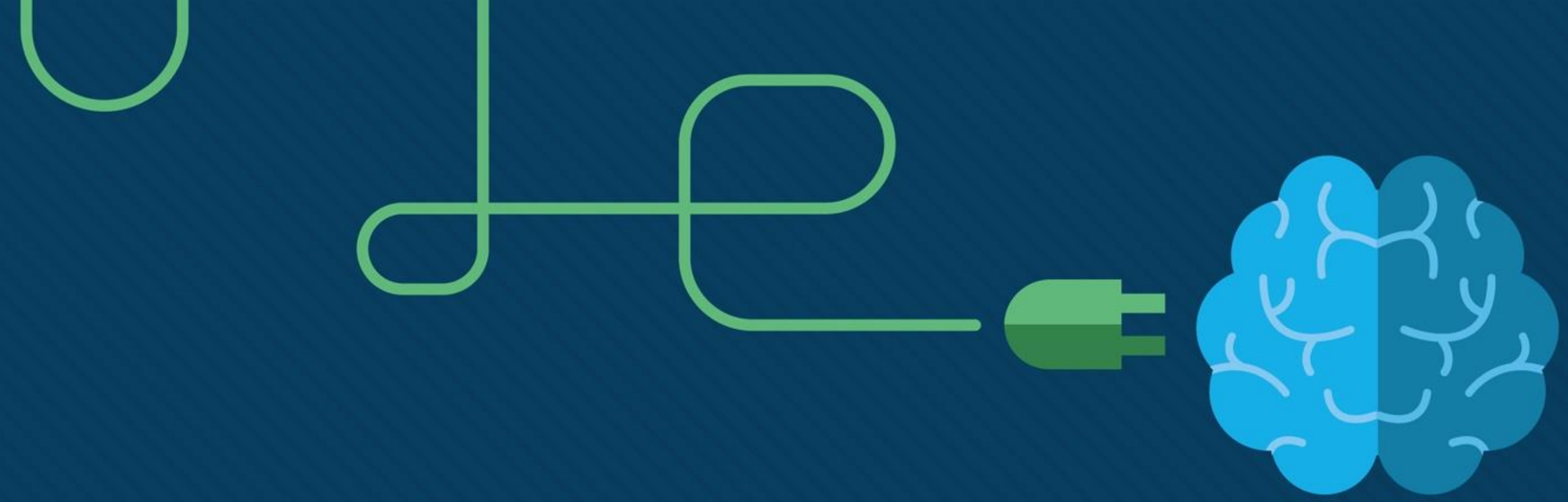


Модуль 5: Основные понятия STP

Switching, Routing and Wireless Essentials v7.0 (SRWE)

Module Objectives

Module Title: STP Concepts

Module Objective: Explain how STP enables redundancy in a Layer 2 network.

Topic Title	Topic Objective
Purpose of STP	Explain common problems in a redundant, L2 switched network.
STP Operations	Explain how STP operates in a simple switched network.
Evolution of STP	Explain how Rapid PVST+ operates.

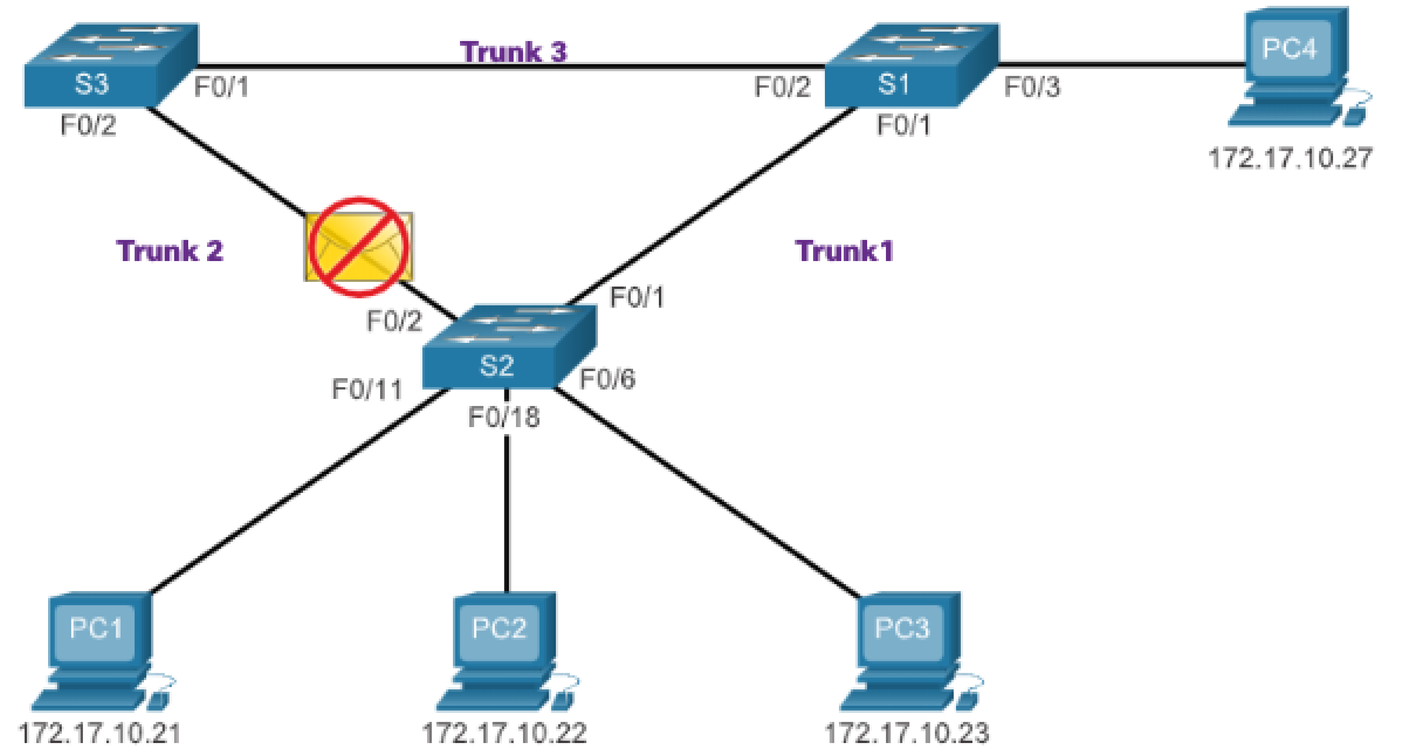
5.1 Назначение протокола STP

Избыточность в коммутируемых сетях уровня 2

- В этом разделе рассматриваются причины возникновения петель в коммутируемых сетях и кратко описывается, как работает протокол связующего дерева. Резервирование является важной частью иерархической модели, предотвращающей перебои в оказании сетевых сервисов пользователям. Для сетей с резервированием требуется добавление физических путей, но необходимо также предусмотреть и логическое резервирование. Наличие альтернативных физических каналов для передачи данных по сети позволяет пользователям получить доступ к сетевым ресурсам даже в случае сбоя одного из каналов. Тем не менее избыточные маршруты в коммутируемой сети Ethernet могут привести к возникновению физических и логических петель 2-го уровня.
- Для локальных сетей Ethernet требуется топология без петель с одним путем между любыми двумя устройствами. Петля в локальной сети Ethernet может вызывать постоянное распространения кадров Ethernet до тех пор, пока соединение не будет разорвано и это не ликвидирует петлю.

Назначение протокола STP
Spanning Tree Protocol

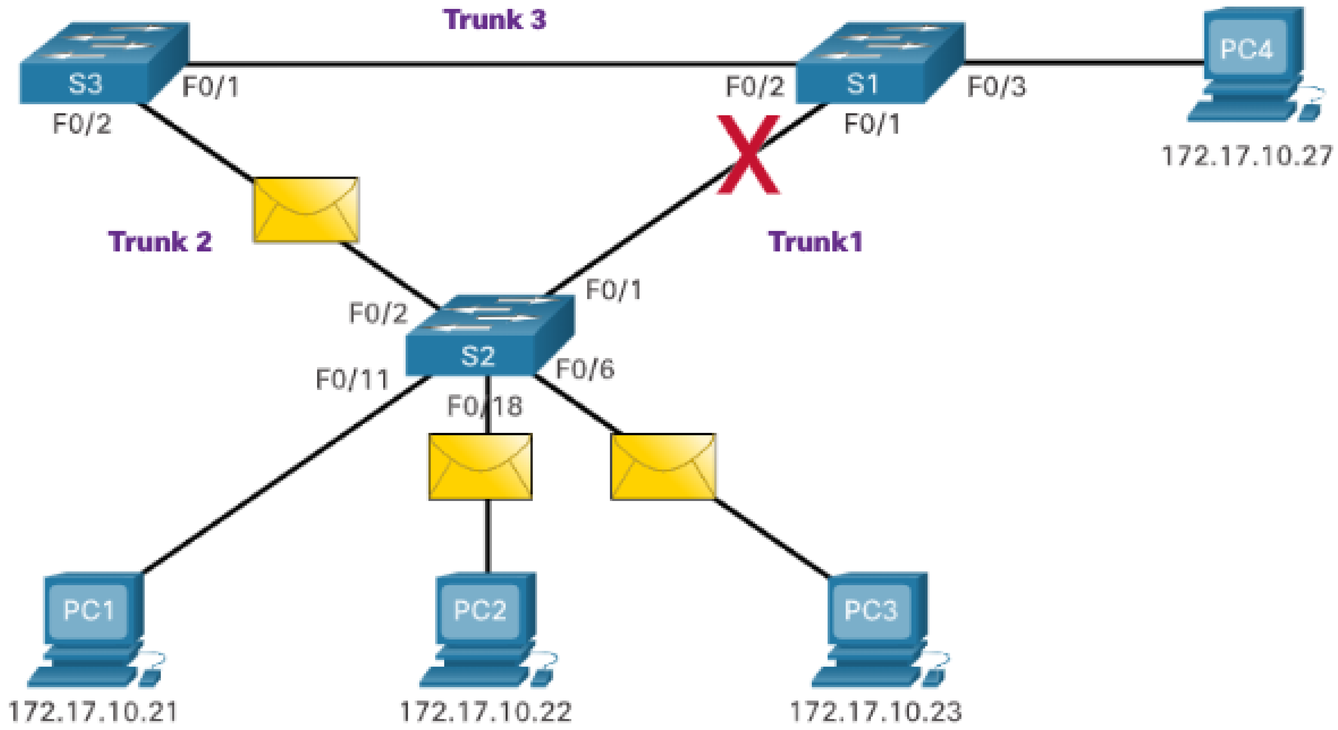
- Протокол связующего дерева (STP) – это сетевой протокол предотвращения петель, который обеспечивает избыточность при создании топологии уровня 2 без петель.
- STP логически блокирует физические петли в сети уровня 2, предотвращая бесконечное хождение кадров в сети.



S2 drops the frame because it received it on a blocked port.

Назначение протокола STP
Пересчет STP

STP компенсирует сбои в сети путем перерасчета и открытия ранее заблокированных портов.



Проблемы с избыточными каналами коммутатора

- Резервирование путей обеспечивает необходимую доступность множества сетевых сервисов, устраняя вероятность перебоев в работе всех сетевых служб в случае отказа в отдельной точке. При наличии нескольких путей между двумя устройствами и отсутствии реализации протокола spanning-tree возникает петля 2-го уровня. Петли уровня 2 могут привести к нестабильности таблицы MAC-адресов, перегрузке каналов и высокой загрузке ЦП на коммутаторах и конечных устройствах, в результате чего сеть становится непригодной для использования.
- Уровень 2 Ethernet не включает в себя механизм распознавания и устранения бесконечно зацикливающихся кадров. Некоторые протоколы 3-го уровня используют механизмы времени жизни (TTL), которые ограничивают количество попыток повторной передачи пакетов сетевыми устройствами 3-го уровня. Маршрутизатор уменьшит TTL (Time to Live) в каждом пакете IPv4 и поле Hop Limit в каждом пакете IPv6. Когда эти поля уменьшатся до 0, маршрутизатор отбрасывает пакет. Коммутаторы Ethernet и Ethernet не имеют сопоставимого механизма ограничения числа раз, когда коммутатор передает кадр уровня 2. STP был разработан специально в качестве механизма предотвращения петли для Ethernet уровня 2.

Петли уровня 2

- Без включения STP петли уровня 2 могут формироваться, что приводит к бесконечному циклу широковещательных, многоадресных и неизвестных одноадресных кадров. Это может быстро разрушить сеть.
- При появлении петли возникает возможность постоянного изменения таблицы MAC-адресов на коммутаторе обновлениями из кадров широковещательной рассылки, что приводит к нестабильности базы данных MAC-адресов. Это может привести к высокой загрузке ЦП, что приводит коммутатор вне рабочее состояние.
- Неизвестный одноадресный кадр с коммутатора формируется, когда у коммутатора нет MAC-адреса назначения в таблице MAC-адресов, и он должен переслать этот кадр со всех своих портов, за исключением входного порта.

Широковещательный шторм

- Широковещательный шторм – это ненормально большое количество широковещательных передач, подавляющих сеть в течение определенного периода времени. Широковещательные штормы могут отключить сеть за считанные секунды, перегружая коммутаторы и конечные устройства. Широковещательные штормы могут быть вызваны аппаратными проблемами, такими как неисправный сетевой адаптер или петля 2-го уровня в сети.
- Широковещательные рассылки уровня 2 в сети, такие как ARP-запросы, очень распространены. Многоадресные рассылки второго уровня обычно пересылаются так же, как и широковещательные рассылки коммутатором. Пакеты IPv6 никогда не пересылаются как широковещательная передача уровня 2, ICMPv6 Neighbor Discovery использует многоадресную рассылку уровня 2.
- Узел, участвующий в сетевой петле, недоступен для других узлов в сети. Кроме того, вследствие постоянных изменений в таблице MAC-адресов коммутатор не знает, из какого порта следует пересылать кадры одноадресной рассылки.
- Во избежание подобных проблем в сети с избыточностью, на коммутаторах должны быть включены определенные типы протокола spanning-tree. Протокол spanning-tree по умолчанию включено на коммутаторах Cisco, предотвращая, таким образом, возникновение петель 2-го уровня.

Алгоритм STP

- Протокол STP основан на алгоритме, изобретенном Радией Перлман (Radia Perlman) во время ее работы в Digital Equipment Corporation и опубликованном в статье 1985 г. “Алгоритм распределенного вычисления протокола связующего дерева в расширенной сети LAN” (An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN). Ее алгоритм связующего дерева (STA) создаст топологию без петли, выбрав один корневой мост, где все остальные коммутаторы определяют один путь с наименьшей стоимостью.
- Протокол STP предотвращает возникновение петель за счет настройки беспетлевого пути в сети с использованием портов, стратегически настроенных на заблокированное состояние. Коммутаторы, использующие протокол STP, могут компенсировать сбои за счет динамической разблокировки ранее блокированных портов и разрешения передачи трафика по альтернативным путям.

Алгоритм STP (Продолжение)

Как STA создает топологию без петли?

- Выбор корневого моста: этот мост (коммутатор) является опорной точкой для всей сети для построения STP.
- Блокирование резервных путей: Протокол STP обеспечивает наличие только одного логического пути между всеми узлами назначения в сети путем намеренного блокирования резервных путей, которые могли бы вызвать петлю. Порт считается заблокированным, когда заблокирована отправка и прием данных на этот порт.
- Создать топологию без петли: Заблокированный порт приводит к тому, что эта ссылка не пересылает между двумя коммутаторами. Это создает топологию, в которой каждый коммутатор имеет только один путь к корневому мосту, аналогично ветвям дерева, которые подключаются к корню дерева.
- Перерасчет в случае сбоя соединения: Физические пути по-прежнему используются для обеспечения избыточности, однако эти пути отключены в целях предотвращения петель. Если путь потребуется для компенсации неисправности сетевого кабеля или коммутатора, протокол STP повторно рассчитывает пути и снимает блокировку с требуемых портов, чтобы разрешить активацию избыточного пути. Перерасчет STP также могут происходить в любой момент, когда новый коммутатор или новый межкоммутационный канал добавляется в сеть.

Video – Observe STP Operation

This video demonstrates the use of STP in a network environment.

Packet Tracer – Investigate STP Loop Prevention

In this Packet Tracer activity, you will complete the following objectives:

- Create and configure a simple three switch network with STP.
- View STP operation.
- Disable STP and view operation again.

5.2 Принципы работы STP

Шаги к топологии без петель

Используя STA, STP строит топологию без петель в четырехэтапном процессе:

1. Выбор корневого моста.
2. Выбор корневых портов.
3. Избранные порты.
4. Выбор альтернативных (заблокированных) портов.

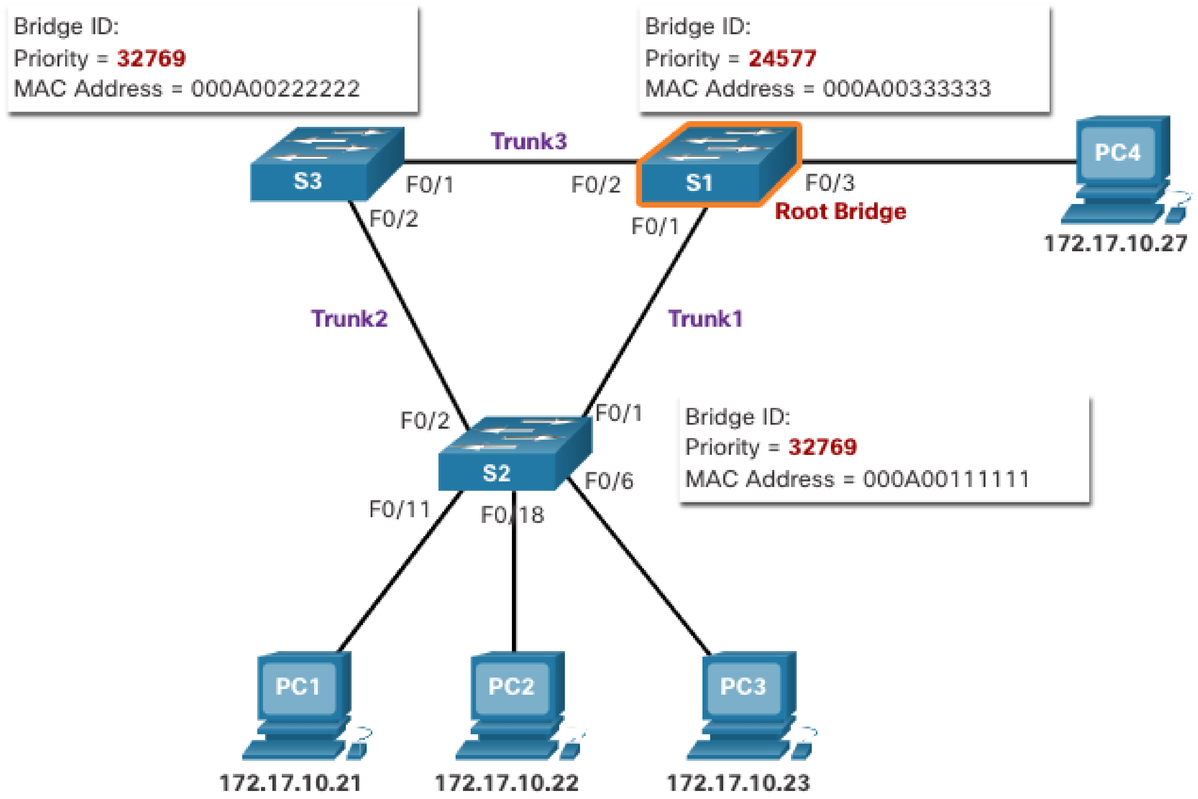
- При работе STA и STP коммутаторы используют блоки данных протокола моста (BPDU) для обмена информацией о себе и своих каналах. BPDU используются для выбора корневого моста, корневых портов, назначенных портов и альтернативных портов.
- Каждая BPDU содержит идентификацию BID, который определяет коммутатор, отправивший BPDU. BID участвует в принятии многих решений STA, включая роли корневого моста и портов.
- Идентификатор BID содержит значение приоритета, MAC-адрес отправляющего коммутатора и дополнительный расширенный идентификатор системы. Самое низкое значение BID определяется комбинацией значений в этих трех полях.

Шаги к топологии без петель

- **Приоритет моста:** Значение приоритета по умолчанию для всех коммутаторов Cisco равно десятичному значению 32768. Значения варьируются в диапазоне от 0 до 61440 с шагом в 4096. Предпочтительнее более низкий приоритет моста. Приоритет моста 0 имеет преимущество по сравнению со всеми остальными значениями приоритета моста.
- **Значение расширенного идентификатора системы:** Это десятичное значение, добавляемое к значению приоритета моста в BID для определения приоритета и сети VLAN кадра BPDU.
- **MAC-адрес:** Если два коммутатора настроены с одинаковым приоритетом, и у них одинаковый расширенный идентификатор системы, то коммутатор с наименьшим значением MAC-адреса, выраженным в шестнадцатеричном формате, получит меньший идентификатор BID.

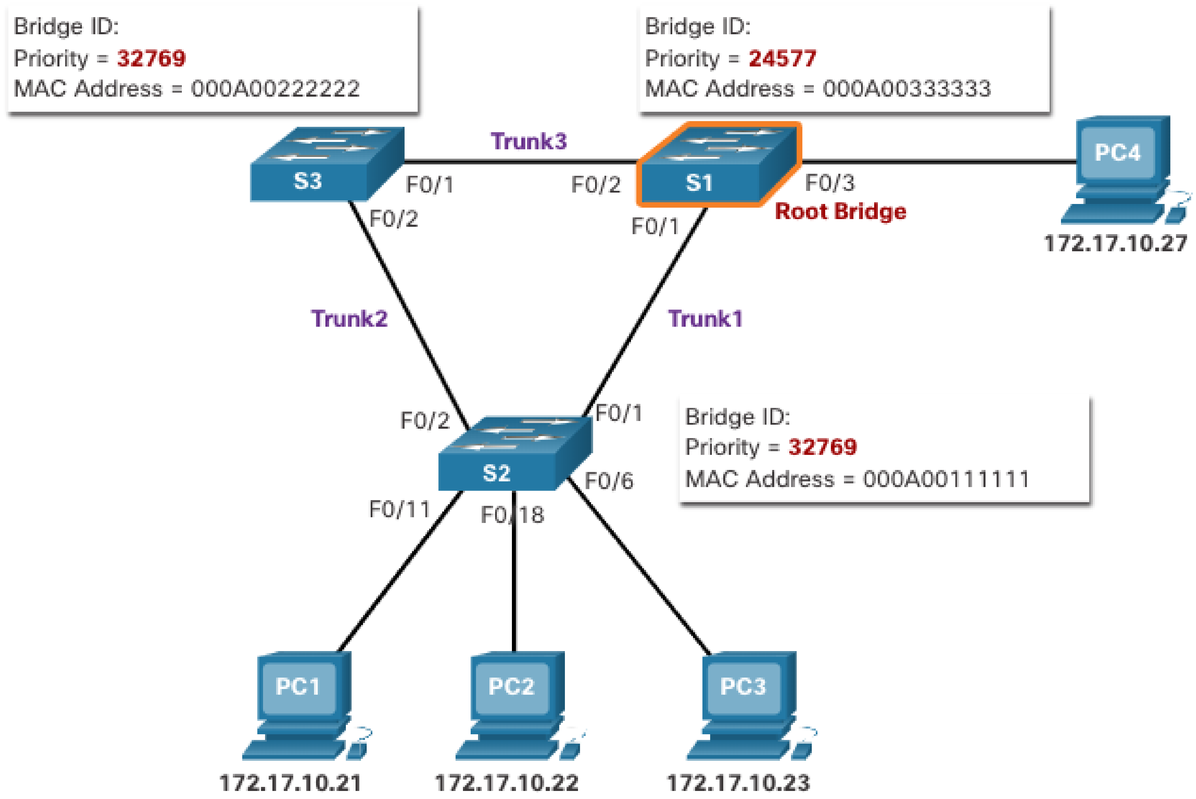
Принцип работы STP
1. Выбор корневого моста

- STA назначает один из коммутаторов в качестве корневого моста и использует его как точку привязки для расчета всех путей. Коммутаторы обмениваются BPDU для создания безпетельной топологии, начиная с выбора корневого моста.
- Все коммутаторы в домене широковещательной рассылки участвуют в процессе выбора. После загрузки коммутатора они начинают рассылать кадры BPDU с интервалом в две секунды. Эти кадры BPDU содержат BID передающего коммутатора и BID корневого моста, известный как Root ID.
- Коммутатор с самым низким значением идентификатора моста (BID) становится корневым мостом. Сначала все коммутаторы объявляют себя корневым мостом с собственным BID, установленным в качестве корневого идентификатора. В конце концов коммутаторы узнают через обмен BPDU, у которых коммутатор имеет самый низкий BID и будет согласовывать через корневой мост



Принципы работы STP
Влияние BID по умолчанию

- Поскольку значение BID по умолчанию равно 32768, два или более коммутаторов могут иметь одинаковый приоритет. В этом сценарии, где приоритеты одинаковы, коммутатор с самым низким MAC-адресом станет корневым мостом. Администратор должен настроить требуемый коммутатор корневого моста с более низким приоритетом.
- На рисунке все коммутаторы настроены с одинаковым приоритетом 32769. Здесь MAC-адрес становится решающим фактором в отношении того, какой коммутатор становится корневым мостом. MAC-адрес с самым низким шестнадцатеричным значением считается предпочтительным корневым мостом. В этом примере S2 имеет наименьшее значение MAC-адреса и, следовательно, назначается корневым мостом для этого экземпляра протокола spanning-tree.
- **Примечание**: Для всех коммутаторов используется значение 32769. Это значение основано на значении приоритета по умолчанию 32768 и назначением сети VLAN 1, связанном с каждым из коммутаторов (32768+1).



Принцип работы STP

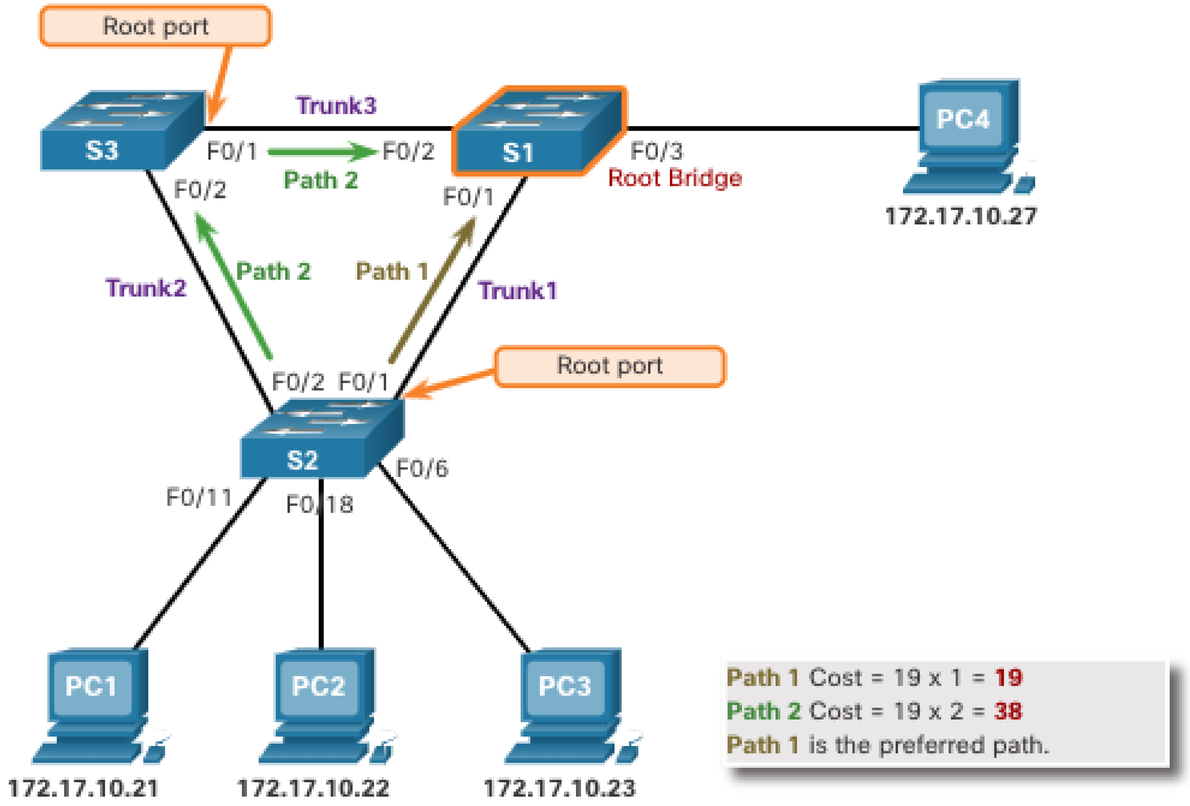
Определение стоимости корневого пути

- Если корневой мост выбран для экземпляра протокола spanning-tree, STA начинает процесс определения оптимальных путей к корневому мосту от всех некорневых коммутаторов в домене широковещательной рассылки. Информация о пути, известная как стоимость внутреннего корневого пути, равна сумме стоимости отдельных портов на пути от коммутатора к корневому мосту.
- Когда коммутатор получает блок BPDU, он добавляет стоимость входного порта сегмента для определения своей стоимости для внутреннего корневого пути.
- Стоимость портов по умолчанию определяется скоростью работы порта. В таблице показаны расходы на порты по умолчанию, предложенные IEEE. Коммутаторы Cisco по умолчанию используют значения, определенные стандартом IEEE 802.1D, также известные как стоимость короткого пути, как для STP, так и для RSTP.
- Хотя с портами коммутатора связано значение стоимости пути по умолчанию, значение стоимости порта можно настроить. Возможность настройки отдельных портов предоставляет администратору необходимую гибкость при контроле путей протокола spanning-tree к корневому мосту..

Скорость канала	Стоимость STP: IEEE 802.1D-1988	Стоимость RSTP: IEEE 802.1w-2004
10 Гбит/с	2	2,000
1 Гбит/с	4	20,000
100 Мбит/с	19	200,000
10 Мбит/с	100	2,000,000

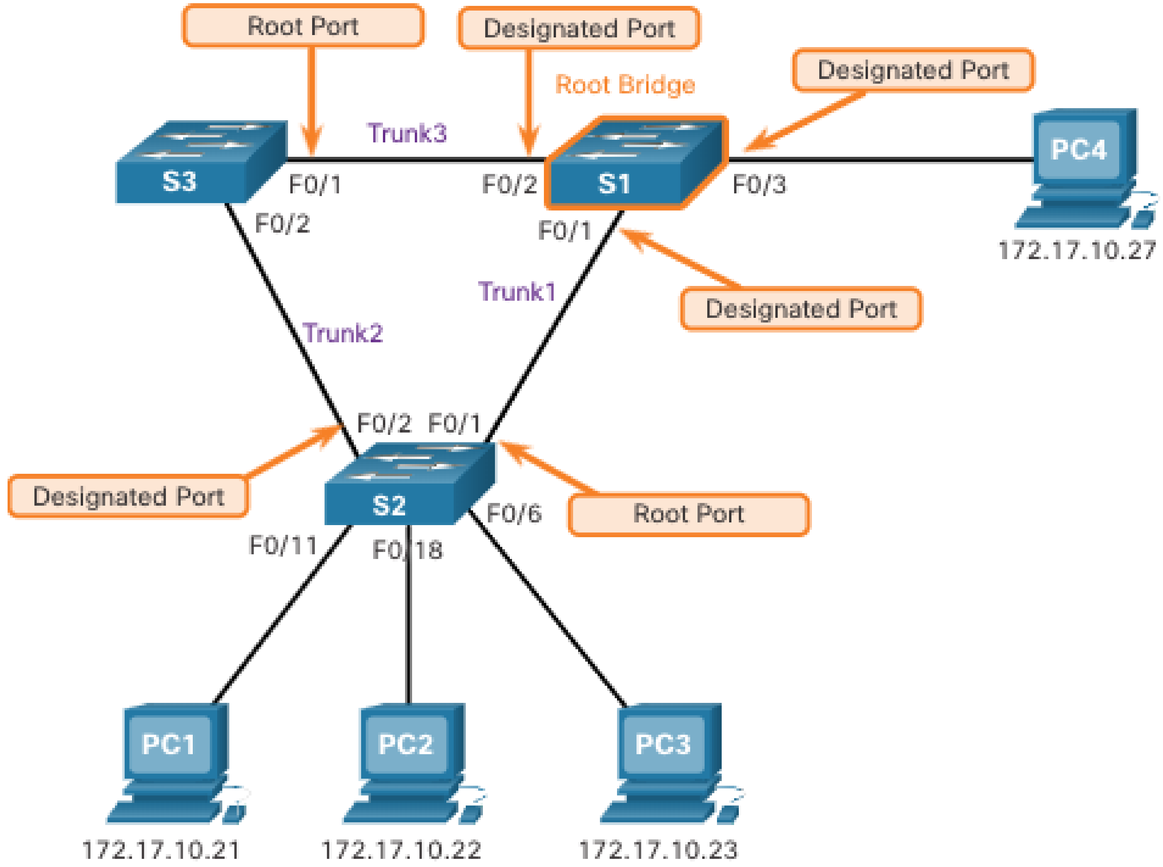
Принципы работы STP
2. Выбор корневых портов

- После определения корневого моста для выбора корневого порта используется алгоритм STA. Каждый некорневой коммутатор выбирает один корневой порт. Корневые порты – порты коммутатора, ближайшие к корневому мосту с точки зрения общей стоимости маршрута к нему. Эта общая стоимость известна как стоимость пути до корневого моста.
- Стоимость внутреннего корневого пути равна сумме стоимостей путей от всех портов к корневому мосту, как показано на рисунке. Пути с наименьшей стоимостью становятся предпочтительными, а все остальные избыточные пути блокируются. В этом примере стоимость внутреннего корневого пути от S2 до корневого моста S1 по пути 1 равна 19, а стоимость внутреннего корневого пути для пути 2 равна 38. Поскольку общая стоимость пути 1 к корневому мосту ниже, именно этот путь является предпочтительным.



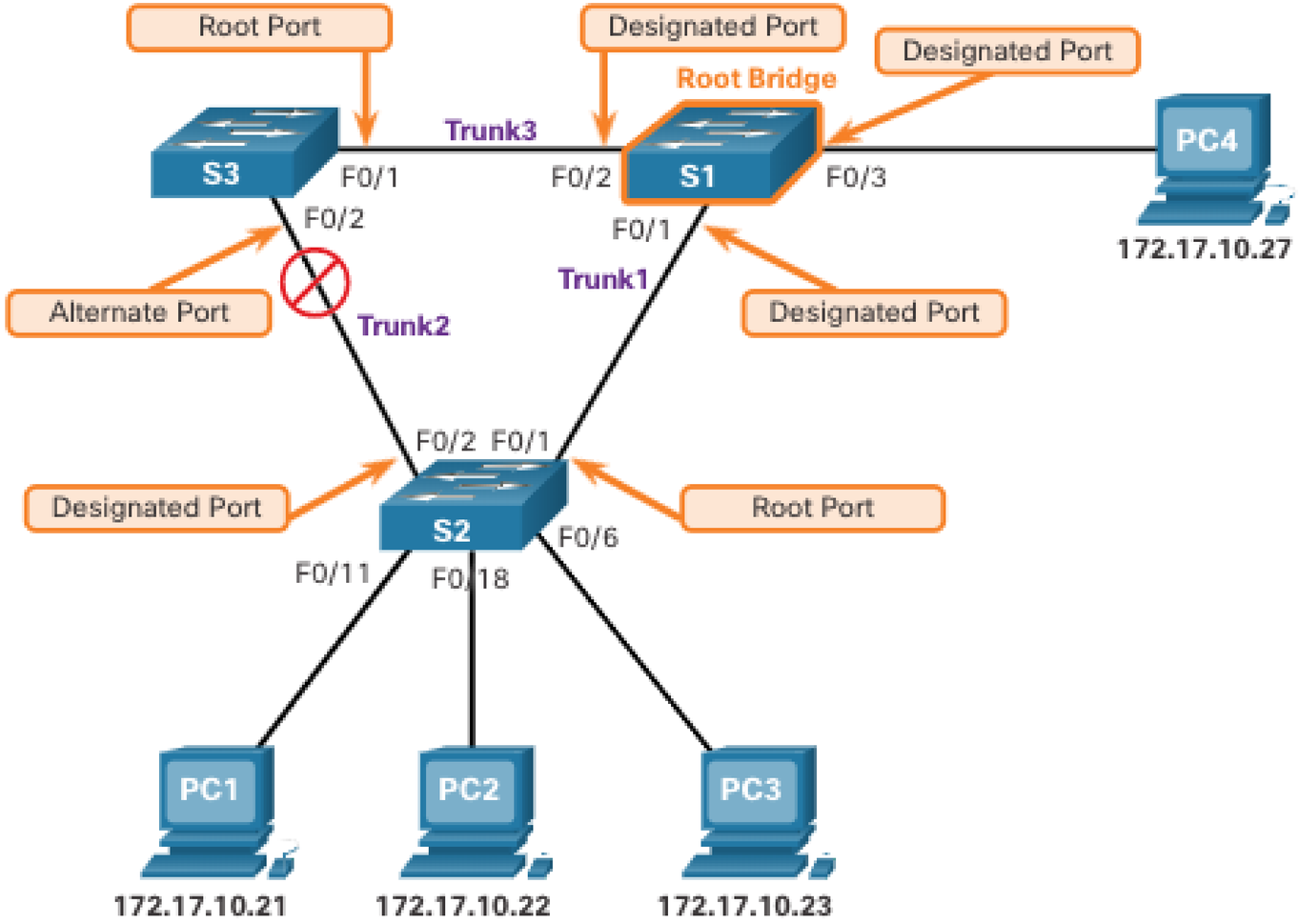
3. Выбор назначенных портов

- Каждый сегмент между двумя коммутаторами будет иметь один назначенный порт. Назначенный порт – это порт в сегменте, который имеет стоимость внутреннего корневого пути к корневому мосту. Другими словами, назначенный порт имеет наилучший путь для приема трафика, ведущего к корневому мосту.
- То, что не является корневым или назначенным портом, становится альтернативным или заблокированным портом.
- Все порты на корневом мосте являются назначенными портами.
- Если на одном конце сегмента находится корневой порт, на другом конце будет назначенный порт.
- Все порты, подключенные к конечным устройствам, являются назначенными портами.
- На сегментах, между двумя коммутаторами, где ни один из коммутаторов не является корневым мостом, порт коммутатора с наименьшей стоимостью пути к корневому мосту является назначенным портом.



4. Выбор альтернативных (заблокированных) портов

Если порт не является корневым или назначенным портом, он становится альтернативным (или резервным) портом.
Альтернативные порты – находятся в состоянии отклонения или блокирования для предотвращения петель. На рисунке STA настроил порт F0/2 на коммутаторе S3 в роли альтернативного порта. Порт F0/2 на S3 находится в блокирующем состоянии и не будет пересылать кадры Ethernet. Все остальные порты между коммутаторами находятся в состоянии пересылки. Он работает как часть STP для предотвращения образования петель.



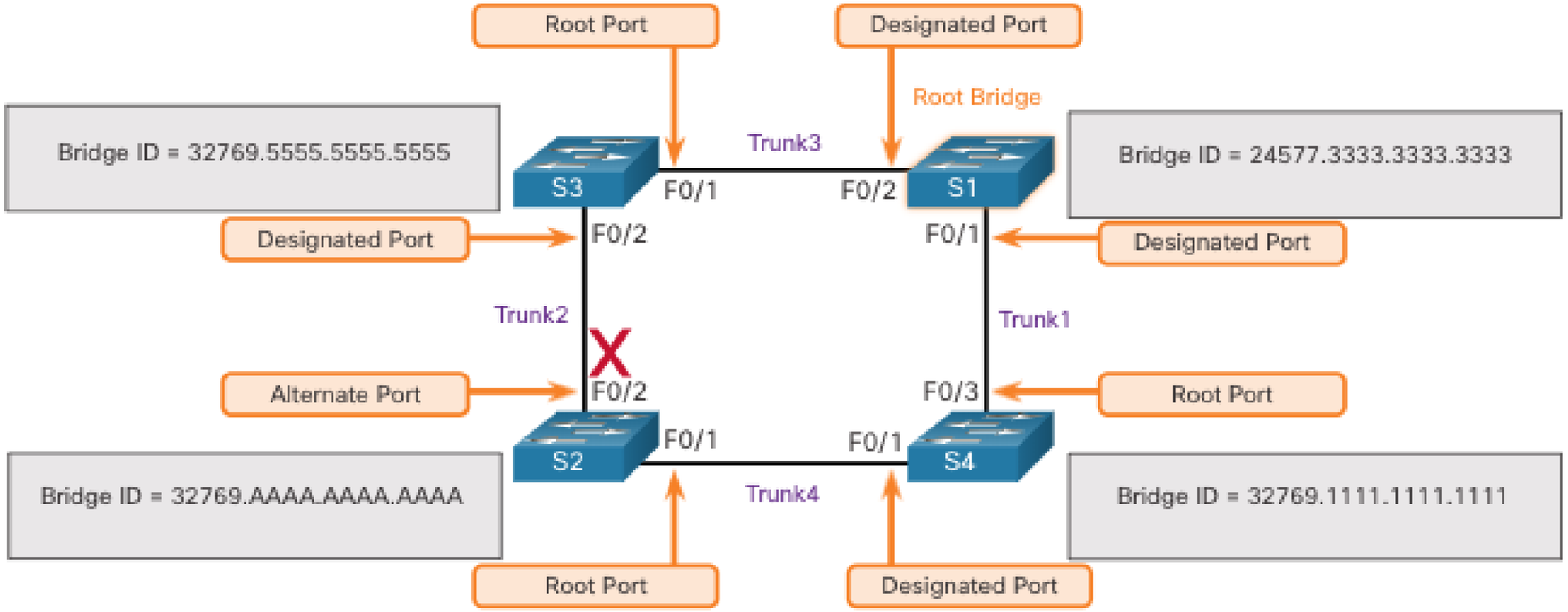
Выбор корневого порта из нескольких путей равной стоимости

Если коммутатор имеет несколько путей равной стоимости к корневому мосту, коммутатор определяет порт, используя следующие критерии:

- Самое низкое значение идентификатора моста отправителя BID
- Самое низкое значение идентификатора порта-отправителя
- Самое низкое значение идентификатора порта-отправителя

Выбор корневого порта из нескольких путей равной стоимости (Продолжение)

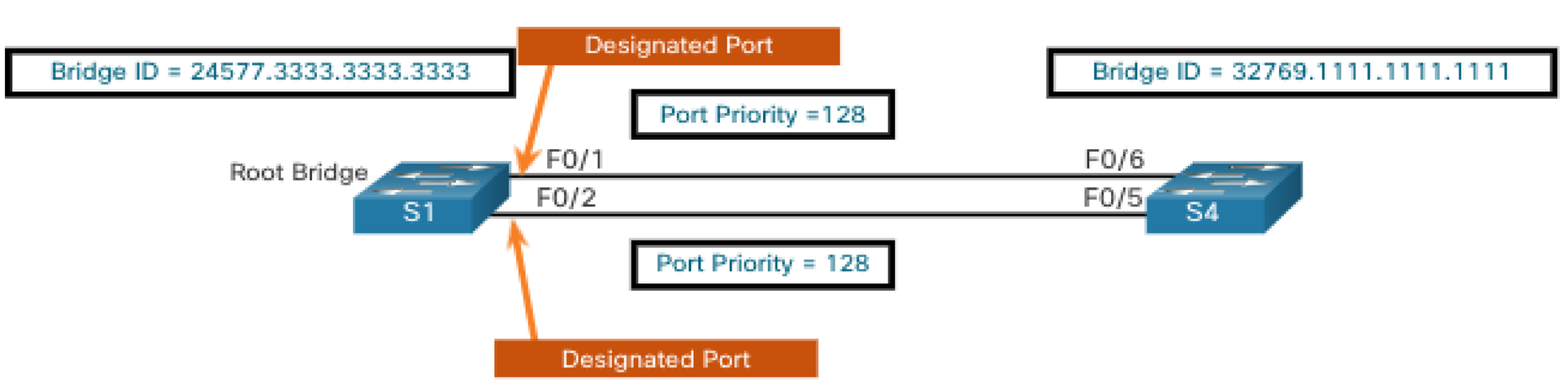
Самый низкий BID отправителя: Эта топология имеет четыре коммутатора с коммутатором S1 в качестве корневого моста. Порт F0/1 на коммутаторе S3 и порт F0/3 на коммутаторе S4 были выбраны в качестве корневых портов, поскольку они имеют стоимость корневого пути к корневому мосту для соответствующих коммутаторов. S2 содержит два порта – F0/1 и F0/2 – с путями равной стоимости к корневому мосту. Идентификаторы моста S3 и S4 будут использоваться для разрыва связи. Это называется BID отправителя. S3 имеет BID 32769.5555.5555.5555, а S4 имеет BID 32769.1111.1111.1111. Поскольку значение BID для S4 меньше, корневым портом будет порт коммутатора S2 F0/1, подключенный к S4.



Выбор корневого порта из нескольких путей равной стоимости (Продолжение)

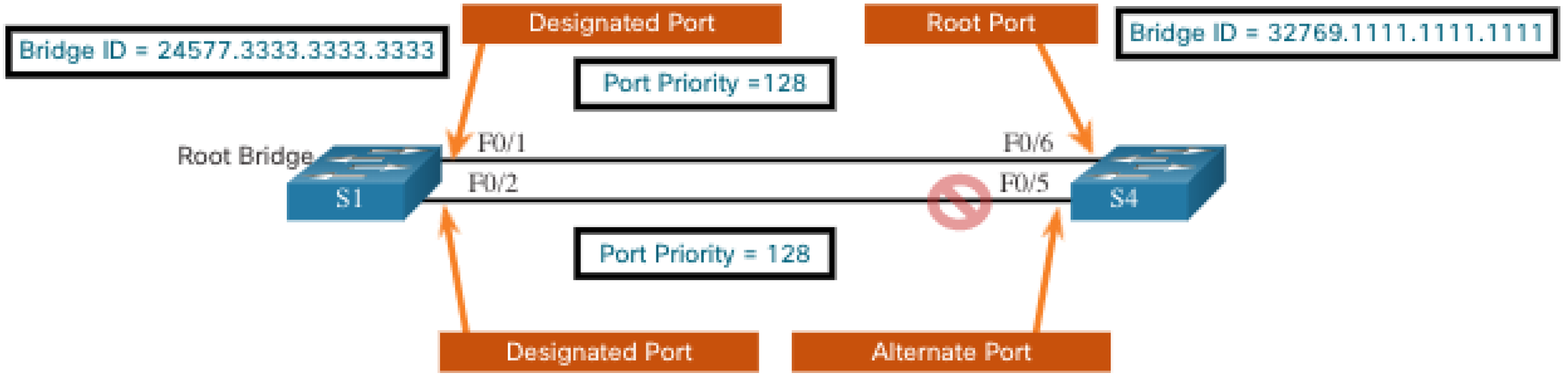
Самый низкий приоритет порта отправителя: Эта топология имеет два коммутатора, которые связаны между собой двумя равноправными путями. S1 является корневым мостом, поэтому оба его порта являются назначенными портами.

- S4 имеет два порта с равными по стоимости путями к корневому мосту. Поскольку оба порта подключены к одному коммутатору, BID отправителя (S1) равен. Итак, первый шаг – ничья.
- Далее – приоритет порта отправителя (S1). Приоритет порта по умолчанию равен 128, поэтому оба порта S1 имеют одинаковый приоритет порта. Это тоже ничья. Однако, если любой порт на S1 настроен с более низким приоритетом порта, S4 помещал бы свой смежный порт в состояние пересылки. Другой порт на S4 будет блокирующим состоянием.



Выбор корневого порта из нескольких путей равной стоимости (Продолжение)

- **Самый низкий идентификатор порта отправителя:** Последний определитель – является самым низким идентификатором порта отправителя. Коммутатор S4 получил BPDU от порта F0/1 и порта F0/2 на S1. Решение основано на идентификаторе порта отправителя, а не на идентификаторе порта получателя. Поскольку идентификатор порта F0/1 на S1 меньше, чем порт F0/2, порт F0/6 коммутатора S4 будет корневым портом. Это порт на S4, который подключен к порту F0/1 на S1.
- Порт F0/5 на S4 станет альтернативным портом и будет помещен в состояние блокировки.



Таймеры STP и состояния портов

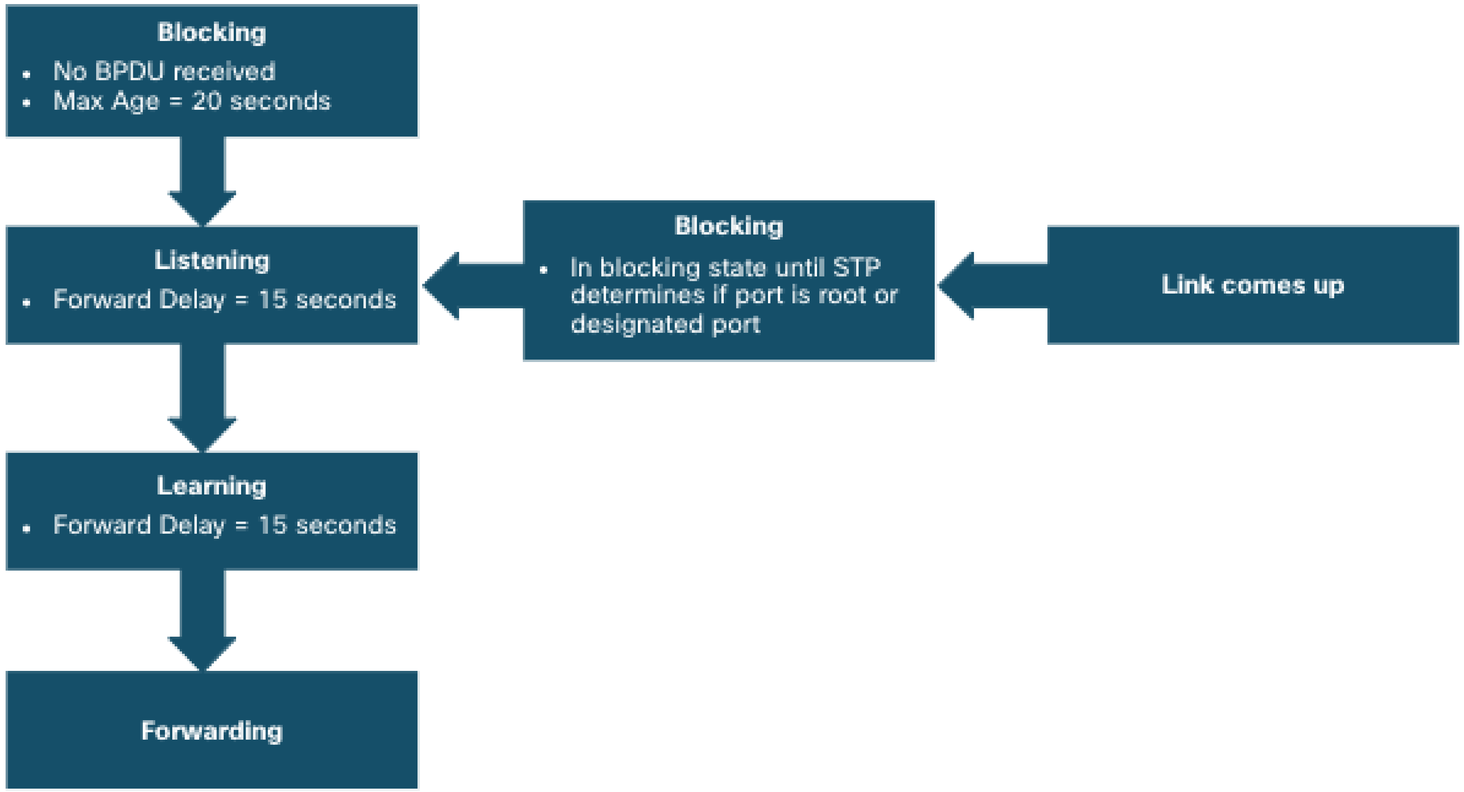
Для конвергенции STP требуется три таймера, а именно:

- **Hello Timer** – время приветствия – это интервал между BPDU. По умолчанию это значение равно 2 секундам, но его можно настроить в диапазоне от 1 до 10 секунд.
- **Forward Delay Timer** – Таймер задержки пересылки (Forward Delay Timer) (15 секунд) – время, проводимое в состояниях прослушивания и обучения. Значение по умолчанию составляет 15 секунд, но может быть изменено на 4-30 секунд.
- **Max Age Timer** – Это максимальное время ожидания коммутатора перед попыткой изменения топологии STP. По умолчанию это значение равно 20 секундам, но его можно настроить в диапазоне от 6 до 40 секунд.

Примечание: Время по умолчанию может быть изменено на корневом мосту, который определяет значение этих таймеров для домена STP.

Таймеры STP и состояния портов (Продолжение)

Протокол STP упрощает создание логического беспетлевого пути по домену широковещательной рассылки. Протокол spanning-tree определяется с помощью данных, полученных в процессе обмена кадрами BPDU между соединенными друг с другом коммутаторами. Если порт коммутатора переходит непосредственно из состояния блокирования в состояние пересылки, не получив информацию о полной топологии в процессе перехода, он может временно создать петлю данных. По этой причине STP имеет пять состояний портов, четыре из которых являются рабочими состояниями портов, как показано на рисунке. Отключенное состояние считается неработоспособным.



Эксплуатационные данные каждого состояния порта

В таблице приведены рабочие подробности каждого состояния порта.

Состояние порта	BPDU	Таблица MAC-адресов	Пересылка кадров данных
Блокирующий режим	Только получение	Без обновления	Нет
Режим прослушивания	Получение и отправка	Без обновления	Нет
Обучение	Получение и отправка	Обновление таблицы	Нет
Режим пересылки	Получение и отправка	Обновление таблицы	Да
Отключено	Не отправлено или получено	Без обновления	Нет

Протокол PerVLAN Spanning Tree Protocol

STP можно настроить для работы в среде с несколькими VLAN. В версиях STP для каждого VLAN Spanning Tree (PVST) существует корневой мост, выбранный для каждого экземпляра связующего дерева. Возможно наличие нескольких отдельных корневых мостов для различных наборов сетей VLAN. STP управляет отдельным экземпляром STP для каждой отдельной VLAN. Если все порты на всех коммутаторах являются участниками сети VLAN 1, значит, существует только один экземпляр протокола spanning-tree.

5.3 Эволюция STP

Различные версии STP

- Многие специалисты используют термин spanning tree и STP для обозначения различных реализаций протокола spanning-tree, например протокола Rapid Spanning Tree Protocol (RSTP) и протокола Multiple Spanning Tree Protocol (MSTP). Чтобы правильно объяснять принципы протокола spanning-tree, важно понимать, о какой конкретно реализации или стандарте идет речь в данном контексте.
- В новейшей документации IEEE по протоколу связующего дерева (IEEE-802-1D-2004) указано: “STP теперь заменен протоколом Rapid Spanning Tree Protocol (RSTP)”. IEEE использует “STP” для обозначения исходной реализации связующего дерева, а “RSTP” – для описания версии связующего дерева, указанной в IEEE-802.1D-2004.
- Так как в этих двух протоколах используется по большей части одинаковая терминология и методы обеспечения пути без петель, основной акцент будет сделан на текущем стандарте и собственных реализациях Cisco для протоколов STP и RSTP.
- Коммутаторы Cisco под управлением IOS 15.0 или более поздней версии по умолчанию запускают PVST+. Эта версия содержит множество спецификаций IEEE 802.1D-2004, таких как альтернативные порты вместо бывших неназначенных портов. Чтобы использовать протокол RSTP, коммутаторы должны быть явно настроены на быстрый режим связующего дерева.

Эволюция STP

Различные версии STP (Продолжение)

Варианты STP	Описание
STP	Это исходная версия IEEE 802.1D (802.1D-1995 и более ранняя), которая предотвращает формирование петель в топологии сети с резервными каналами. Общий протокол spanning-tree (CST) предполагает использование только одного экземпляра протокола spanning-tree для всей сети с мостовым соединением независимо от количества сетей VLAN.
PVST+	Per-VLAN Spanning Tree (PVST+) усовершенствованный корпорацией Cisco протокол STP, обеспечивающий отдельный экземпляр связующего дерева 802.1D для каждой сети VLAN, настроенной в сети. Рассматриваемый вариант протокола spanning-tree поддерживает PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard и loop guard.
802.1D-2004	Это обновленная версия стандарта STP, в которую входит IEEE 802.1w.
RSTP	Rapid Spanning Tree Protocol (RSTP) или IEEE 802.1w доработанный протокол STP, который обеспечивает более быстрое схождение, чем протокол STP.
Rapid PVST+	Это усовершенствованная технология RSTP Cisco, которая использует PVST+ и предоставляет отдельный экземпляр 802.1w на VLAN. Каждый отдельный экземпляр поддерживает функции PortFast, BPDU guard, BPDU filter, root guard и loop guard.
MSTP	Протокол MSTP (Multiple Spanning Tree Protocol) это стандарт IEEE на базе ранней реализации собственного протокола Cisco с несколькими экземплярами - Multiple Instance STP (MISTP). MSTP сопоставляет несколько сетей VLAN в пределах одного экземпляра протокола spanning-tree.
MST	Реализация Cisco протокола MSTP, которая обеспечивает до 16 экземпляров протокола RSTP и объединяет множество сетей VLAN с идентичной физической и логической топологией в один общий экземпляр RSTP. Каждая реализация поддерживает функции PortFast, BPDU guard, BPDU filter, root guard и loop guard.

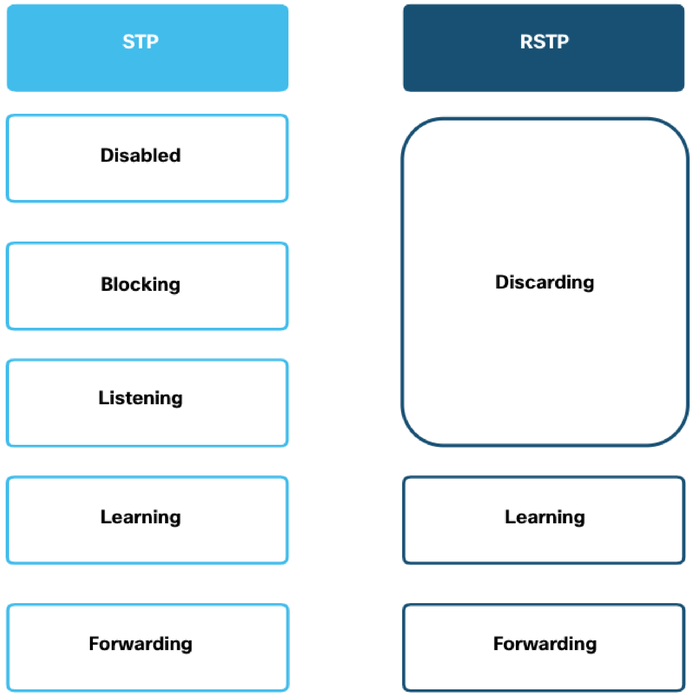
RSTP Concepts

- RSTP (IEEE 802.1w) supersedes the original 802.1D while retaining backward compatibility. The 802.1w STP terminology remains primarily the same as the original IEEE 802.1D STP terminology. Most parameters have been left unchanged. Users that are familiar with the original STP standard can easily configure RSTP. The same spanning tree algorithm is used for both STP and RSTP to determine port roles and topology.
- RSTP increases the speed of the recalculation of the spanning tree when the Layer 2 network topology changes. RSTP can achieve much faster convergence in a properly configured network, sometimes in as little as a few hundred milliseconds. If a port is configured to be an alternate port it can immediately change to a forwarding state without waiting for the network to converge.

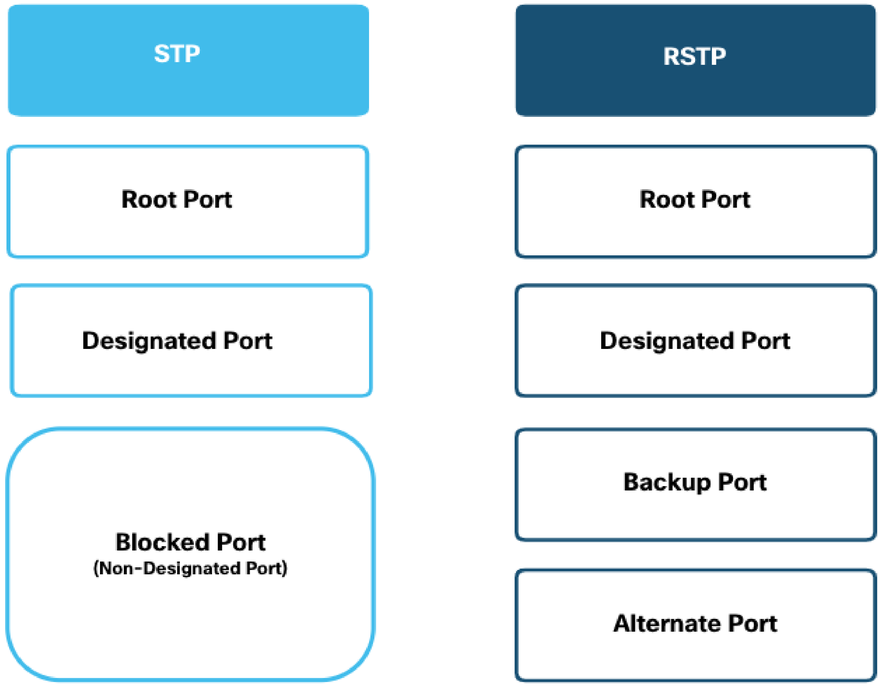
Note: Rapid PVST+ is the Cisco implementation of RSTP on a per-VLAN basis. With Rapid PVST+ an independent instance of RSTP runs for each VLAN.

RSTP Port States and Port Roles

There are only three port states in RSTP that correspond to the three possible operational states in STP. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

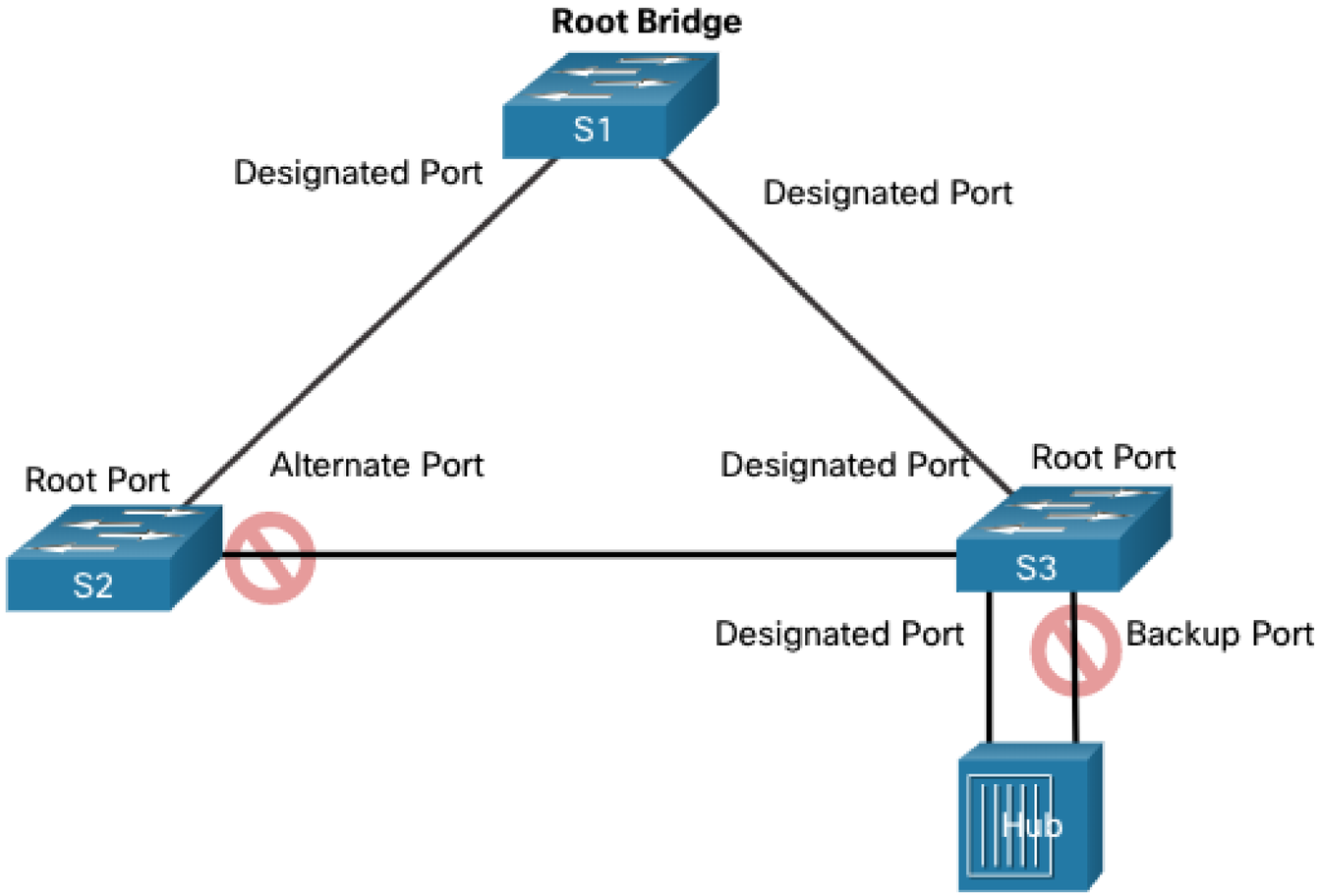


Root ports and designated ports are the same for both STP and RSTP. However, there are two RSTP port roles that correspond to the blocking state of STP. In STP, a blocked port is defined as not being the designated or root port. RSTP has two port roles for this purpose.



RSTP Port States and Port Roles (Cont.)

The alternate port has an alternate path to the root bridge. The backup port is a backup to a shared medium, such as a hub. A backup port is less common because hubs are now considered legacy devices.



PortFast and BPDU Guard

- When a device is connected to a switch port or when a switch powers up, the switch port goes through both the listening and learning states, each time waiting for the Forward Delay timer to expire. This delay is 15 seconds for each state for a total of 30 seconds. This can present a problem for DHCP clients trying to discover a DHCP server because the DHCP process may timeout. The result is that an IPv4 client will not receive a valid IPv4 address.
- When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, avoiding the 30 second delay. You can use PortFast on access ports to allow devices connected to these ports to access the network immediately. PortFast should only be used on access ports. If you enable PortFast on a port connecting to another switch, you risk creating a spanning tree loop.
- A PortFast-enabled switch port should never receive BPDUs because that would indicate that switch is connected to the port, potentially causing a spanning tree loop. Cisco switches support a feature called BPDU guard. When enabled, it immediately puts the switch port in an errdisabled (error-disabled) state upon receipt of any BPDU. This protects against potential loops by effectively shutting down the port. The administrator must manually put the interface back into service.

Alternatives to STP

- Over the years, organizations required greater resiliency and availability in the LAN. Ethernet LANs went from a few interconnected switches connected to a single router, to a sophisticated hierarchical network design including access, distribution and core layer switches.
- Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements, as part of RSTP and MSTP.
- An important aspect to network design is fast and predictable convergence when there is a failure or change in the topology. Spanning tree does not offer the same efficiencies and predictabilities provided by routing protocols at Layer 3.
- Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch. In other words, the connections between access layer switches and distribution switches would be Layer 3 instead of Layer 2.

5.4 Module Practice and Quiz

What Did I Learn In This Module?

- Redundant paths in a switched Ethernet network may cause both physical and logical Layer 2 loops.
- A Layer 2 loop can result in MAC address table instability, link saturation, and high CPU utilization on switches and end-devices. This results in the network becoming unusable.
- STP is a loop-prevention network protocol that allows for redundancy while creating a loop-free Layer 2 topology. Without STP, Layer 2 loops can form, causing broadcast, multicast and unknown unicast frames to loop endlessly, bringing down a network.
- Using the STA, STP builds a loop-free topology in a four-step process: elect the root bridge, elect the root ports, elect designated ports, and elect alternate (blocked) ports.
- During STA and STP functions, switches use BPDUs to share information about themselves and their connections. BPDUs are used to elect the root bridge, root ports, designated ports, and alternate ports.
- When the root bridge has been elected for a given spanning tree instance, the STA determines the best paths to the root bridge from all destinations in the broadcast domain. The path information, known as the internal root path cost, is determined by the sum of all the individual port costs along the path from the switch to the root bridge.
- After the root bridge has been determined the STA algorithm selects the root port. The root port is the port closest to the root bridge in terms of overall cost, which is called the internal root path cost.
- After each switch selects a root port, switches will select designated ports. The designated port is a port on the segment (with two switches) that has the internal root path cost to the root bridge.
- If a port is not a root port or a designated port, then it becomes an alternate (or backup) port. Alternate ports and backup ports are in discarding or blocking state to prevent loops.

What Did I Learn In This Module? (Cont.)

- When a switch has multiple equal-cost paths to the root bridge, the switch will determine a port using the following criteria: lowest sender BID, then the lowest sender port priority, and finally the lowest sender port ID.
- STP convergence requires three timers: the hello timer, the forward delay timer, and the max age timer.
- Port states are blocking, listening, learning, forwarding, and disabled.
- In PVST versions of STP, there is a root bridge elected for each spanning tree instance. This makes it possible to have different root bridges for different sets of VLANs.
- STP is often used to refer to the various implementations of spanning tree, such as RSTP and MSTP.
- RSTP is an evolution of STP that provides faster convergence than STP.
- RSTP port states are learning, forwarding and discarding.
- PVST+ is a Cisco enhancement of STP that provides a separate spanning tree instance for each VLAN configured in the network. PVST+ supports PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard, and loop guard.
- Cisco switches running IOS 15.0 or later, run PVST+ by default.
- Rapid PVST+ is a Cisco enhancement of RSTP that uses PVST+ and provides a separate instance of 802.1w per VLAN.
- When a switch port is configured with PortFast, that port transitions from blocking to forwarding state immediately, bypassing the STP listening and learning states and avoiding a 30 second delay.
- Use PortFast on access ports to allow devices connected to these ports, such as DHCP clients, to access the network immediately, rather than waiting for STP to converge on each VLAN.

What Did I Learn In This Module? (Cont.)

- Cisco switches support a feature called BPDU guard which immediately puts the switch port in an error-disabled state upon receipt of any BPDU to protect against potential loops.
- Over the years, Ethernet LANs went from a few interconnected switches that were connected to a single router, to a sophisticated hierarchical network design. Depending on the implementation, Layer 2 may include not only the access layer, but also the distribution or even the core layers. These designs may include hundreds of switches, with hundreds or even thousands of VLANs. STP has adapted to the added redundancy and complexity with enhancements as part of RSTP and MSTP.
- Layer 3 routing allows for redundant paths and loops in the topology, without blocking ports. For this reason, some environments are transitioning to Layer 3 everywhere except where devices connect to the access layer switch.


CISCO