

Упражнение 9. Spanning Tree Protocol (STP)

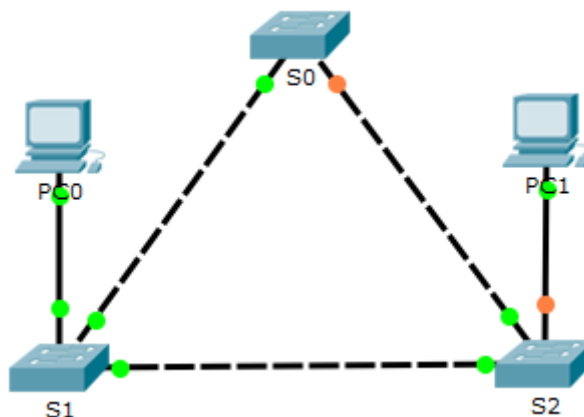
1. Цел на упражнението.

Целта на упражнението е да се получат практически знания и умения за конфигуриране и администриране на отказоустойчиви мрежови конфигурации, използвайки Spanning Tree Protocol (STP).

2. Теоретични сведения

2.1 Отказоустойчиви топологии с излишни трасета

За постигане на отказоустойчивост в локална мрежа е необходимо да има допълнителни (излишни) трасета, които да предават данните при отпадане на основните. Пример за отказоустойчива топология е показан на фигура 9.1.



Фиг. 9.1. Примерна отказоустойчива топология с излишни трасета

Тъй като комуникацията е изцяло на второ ниво от OSI модела и поведението на комутатора е да препраща broadcast пакетите на всички свои портове, без този, на който е получен пакета, тази топология няма да работи без специален протокол за блокиране на излишните трасета. При изпращане на broadcast пакет от някой компютър, например PC0, комутатор S1 ще го получи и ще го изпрати към комутатори S0 и S2. Така всеки от двата комутатора ще получи по две копия на broadcast пакета от всеки от своите съседи и ще ги препрати към другия си съсед. В резултат се получава непрекъснато препредаване на много копия на broadcast пакетите, които никога не се изхвърлят и мрежата спира да работи, защото е заета да предава broadcast пакети. Това е познато като Broadcast storm (буря от broadcast пакети).

Някои модели комутатори предотвратяват проблема, като ограничават броя broadcast пакети, които могат да се предават за единица време на всеки порт и по този начин мрежата не спира да работи, но продължава да се натоварва от излишното постоянно предаване на тези пакети.

2.2 Spanning Tree Protocol

Повечето съвременни устройства поддържат протокола Spanning Tree или новите му разновидности, които са предназначени да позволяват отказоустойчиви топологии, но да не позволяват зацикляне на информация в мрежата. Това става чрез блокиране на всички излишни трасета и конфигурирането на мрежата като дървовидна топология без затворени контури, които могат да предизвикат broadcast storm. Протоколът е описан в стандарт IEEE 802.1D.

2.2.1 Избор на корен (Root) на мрежата

Първоначално комутаторите (и мостовете, ако има такива) избират кой ще играе роля на корен (root) на дървовидната мрежова топология. Изборът става чрез предаването на специални пакети (Bridge Protocol Data Unit, BPDU), които съдържат идентификатора на всеки мост или комутатор. Идентификаторът се състои от две части: приоритет и MAC адрес на устройството. Примерен идентификатор е показан на фигура 9.2.

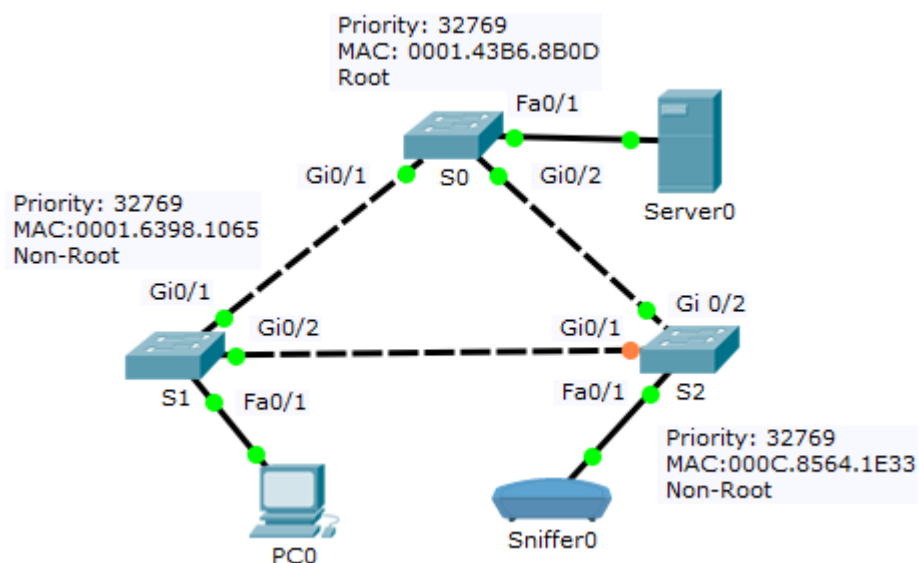
Приоритет	MAC адрес
0 - 65535	0001.1111.1111

Фиг. 9.2. Идентификатор на устройство (BridgeID)

Частта приоритет по подразбиране на всички устройства е 32768 + номера на VLAN. Базовият приоритет може да бъде настройван от администратора на стъпки по 4096, т.е. може да бъде 0, 4096, 8192, 12288 и т.н. до 61440.

Устройството с най-нисък приоритет се избира за корен (root) на мрежата. Ако приоритетите на всички устройства са еднакви се сравняват MAC адресите на устройствата и това с най-малък по стойност MAC адрес се избира за корен.

Примерна топология е показана на фиг. 9.3.



Фиг. 9.3. Избор на корен (root)

В примера и трите комутатора имат базов приоритет по подразбиране (32768) и е конфигуриран VLAN 1. Поради еднаквите приоритети се сравняват MAC адресите и S0, чиито MAC адрес е най-малък се избира за root.

2.2.2 Избор на порт за достигане до корена (Root port)

Следващата стъпка е всеки комутатор да избере свой порт, по който ще предава до корена (Root port). Това става, като на всеки порт се присвоява цена (cost) и всеки комутатор събира цените на всички връзки до корена, като връзката с най-малка обща цена се избира за root port. Цените могат да бъдат променяни от администратора, но по подразбиране имат стойности, които се определят от скоростта на връзката. Определените от IEEE цени са показани в таблица 9.1.

Табл. 9.1. Цени на връзките

	802.1D-1990	802.1D-1998	802.1t-2001, 802.1D-2004
Link Speed	Cost	Cost	Cost
10 Mb/s	100	99	2,000,000
100 Mb/s	10	19	200,000
1 Gb/s	1	4	20,000
2 Gb/s	1	4	10,000
5 Gb/s	1	3	4,000
10 Gb/s	1	2	2,000
50 Gb/s	1	1	400
100 Gb/s	1	1	200
1 Tb/s	1	1	20
10 Tb/s	1	1	2
20 Tb/s	1	1	1

Най-старата спецификация на стандарта IEEE 802.1D от 1990 г. определя цена 100 на връзка със скорост 10Mbit/s, цена 10 на връзка със скорост 100 Mbit/s и цена 1 на всички връзки със скорости 1 Gbit/s и по-високи. По този начин всички трасета със скорост 1 Gbit/s и по-висока се третират като еднакви. След излизането на стандарта за 10 Gbit/s, през 2008 беше направена ревизия на цените на връзките, при която цената на 100 Mbit/s е 19, на 1 Gbit/s – 4, на 10 Gbit/s – 2.

В момента има стандарти за Ethernet мрежи на 2.5, 5, 10, 40 и 100 Gbit/s. Те също не могат да бъдат различени правилно, използвайки спецификацията от 1998 г. Действащият в момента стандарт е версията от 2004 г. Той предлага цени на връзката, показани в последната колона, но тези стойности не се побират в 16 битово число, което се е използвало при старите стандарти, затова от гледна точка на съвместимост някои производители продължават да използват спецификацията от 2008 г. Тя се използва и в настоящото упражнение.

За примерната мрежа от фигура 9.3, комутатор S1 има два възможни пътя до корена – един директен на порт Gi0/1 с цена 4 и втори през комутатор S2, където до корена има две последователни връзки със скорост 1 Gbit/s, чиято цена се сумира и общата цена на този път до корена става 8. Следователно S1 избира за свой Root port Gi0/1.

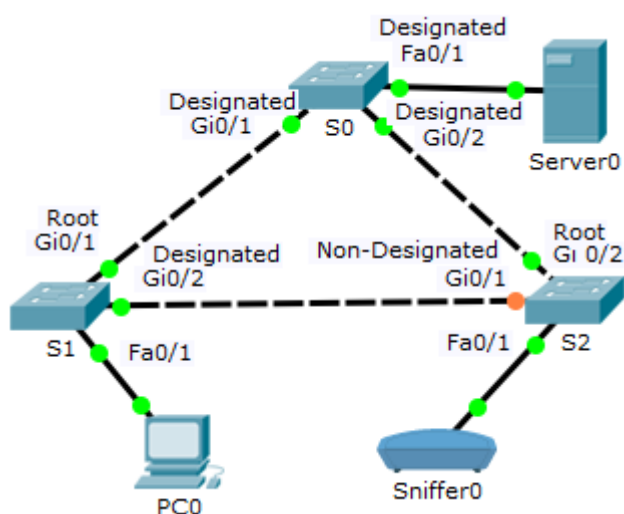
По същия начин комутатор S2 избира за свой Root порт Gi0/2 с цена 4.

2.2.3 Избор на включени (Designated) и блокирани (Non-designated) портове

Когато даден порт бъде избран за Root порт, той винаги е в състояние „включен“ (Designated). Всички портове на корена винаги са в такова състояние. За да се премахне възможността за зацикляне на информацията, комутаторите в мрежата трябва да поставят някои портове в блокирано (Non-designated) състояние, в което тези портове не предават и не приемат данни. В примера от фигура 9.3 единият от двата комутатора – S1 и S2 трябва да постави своя порт на връзката помежду им в блокирано състояние, за да премахне затворения контур.

За да се контролира този процес е предвидена стойност за приоритет на порт. Приоритетът е стойност от 1 до 255, като по подразбиране всички портове имат приоритет 128. Администраторът може да променя приоритета, но ако не го направи, двата комутатора сравняват своя идентификатор. Този, чиито идентификатор е по-малък (в примера – S1) оставя порта си във включено състояние, а другият с по-голям идентификатор (в примера - S2) блокира порта си. Ако включите един кабел в два порта на един и същ комутатор, портът с по-малък номер ще остане активен, а този с по-голям номер ще се блокира.

На фигура 8.4 е показана получената мрежова топология с описани типове на портовете.



Фиг. 9.3. Избор на видове портове

2.2.4. Състояния на портовете

Когато в даден порт на комутатора се включи устройство, комутаторът не разрешава веднага на този порт да се предават данни. Вместо това портът преминава последователно през следните състояния:

- Блокирано (Blocking) – комутаторът не предава на този порт и не приема данни, а само слуша за служебни пакети на протокола STP (наричани още BPDU – Bridge Protocol Data Unit). В това състояние портът остава 20 секунди;
- Слушане (listening) – Ако комутаторът е решил по време на предишното състояние, че портът ще бъде Root или Designated, той отива в състояние на слушане, където не приема и не предава данни, но приема и предава служебни кадри на STP (BPDU). В това състояние портът остава за около 15 секунди;
- Научаване (Learning) – в това състояние комутаторът научава MAC адресите на устройствата, включени към порта. Това продължава около 15 секунди.
- Препращане (Forwarding) – това е работното състояние на порта, в него той приема и предава данни.

Съществува и състояние „забранено“ (Disabled) в което портът е неработоспособен, не предава и не приема нито данни, нито служебни кадри.

Така след включване на устройство в даден порт то може да получава или предава данни едва след 50 секунди, което не винаги е удобно. Затова при устройствата на Cisco Systems даден порт може да се настрои в режим PortFast, при който след включване на устройство в порта той пропуска първите три състояния и се поставя директно в режим на препращане на данни, за бо-бързо включване на устройството към мрежата. Ако на този порт е включен друг комутатор и има излишн трасета, може да се получи зацикляне на broadcast пакетите.

2.3 Rapid Spanning Tree Protocol

За да се избегне забавянето при преконфигуриране на мрежовата топология от 30 – 50 секунди при стандартния STP е разработено разширение, наречено Rapid Spanning Tree Protocol (RSTP), което е стандартизирано в IEEE802.1w. При него преконфигурирането на мрежата обикновено е в рамките на няколко милисекунди до около 6 секунди, което е значително подобрение.

Типовете портове са:

- Root – Най-добрият порт, който се използва за изпращане към root;
- Designated – включен порт, който предава данни
- Alternate – алтернативен (резервен) път към root, който може да се използва незабавно, ако основният стане неактивен;

- Backup – Резервен път към мрежов сегмент, към който е свързан друг Designated порт на същото устройство и може да се използва веднага, ако основният отпадне.

Състоянията на портовете при RSTP са:

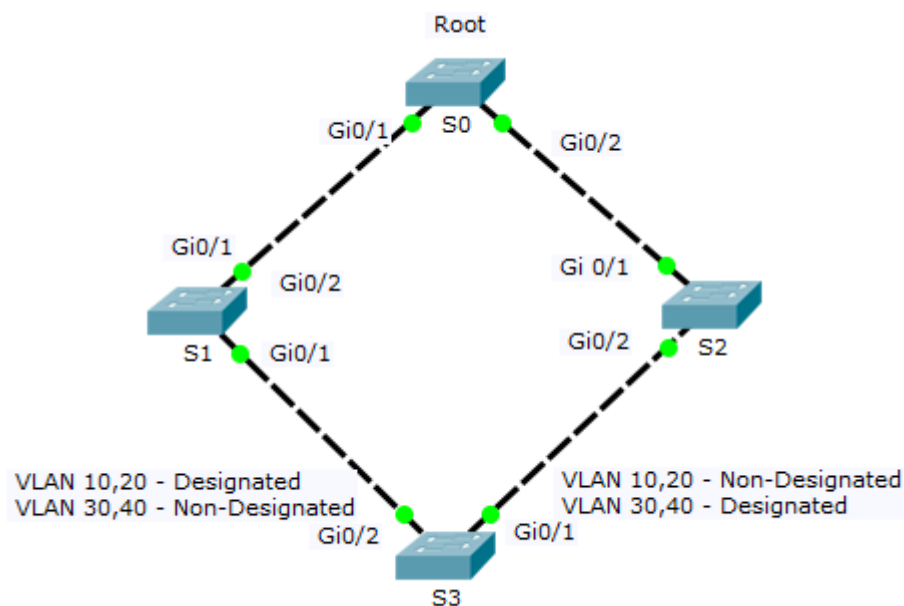
- Discarding – не се изпращат и приемат потребителски данни;
- Learning – портът още не изпраща данни, но научава MAC адреси;
- Forwarding – портът изпраща и приема данни.

Вместо режим PortFast (само при Cisco за STP), при RSTP портовете на комутатора, където са свързани крайни устройства (компютри, сървъри, принтери) могат да се поставят в режим Edge, като по този начин се пропуска състоянието Learning и портът започва веднага да предава данни.

2.4. Per-VLAN Spanning Tree (PVST) и Per-VLAN Spanning Tree Plus

Това подобрение на Spanning Tree протокола е разработено от Cisco Systems и работи главно на техните комутатори, но се поддържа и от други производители, между които Force10 Networks, Alcatel-Lucent, Extreme Networks, Avaya, Brocade Communications Systems and BLADE Network Technologies. Старият протокол PVST не е съвместим със стандарта за гръбнак на VLAN – IEEE802.1q, затова е разработен и по-често се използва PVST+.

При този протокол се изгражда отделно дърво за всеки VLAN, като може по-ефективно да се използва мрежовата топология – например да се препраща информацията за част от VLAN мрежите по единия порт, а да се блокира за другите VLAN, които да използват друг гръбначен порт. Пример за такава топология е показан на фиг. 9.4.



Фиг. 9.3. Избор на видове портове

В примера за VLAN 10 и 20 пътят от S3 през S1 към корена S0 се избира за основен и се поставя във включено положение (Designated), а пътят през S2 се избира за резервен и се блокира. За VLAN 30 и 40 – обратно, оставя се включен пътят през S2, а пътят през S1 се блокира. Така могат да се използват едновременно и двете трасета, но не се получава затворен контур, тъй като пакетите от отделните VLAN не се предават в друг VLAN.

2.5. Multiple Spanning Tree

Стандартът за няколко различни дървета в една мрежова топология на IEEE се нарича Multiple Spanning Tree (MST) и е описан в IEEE802.1s. Принципът е подобен на описания в точка 2.4, като разликата е, че за PVST+ се прави отделно дърво за всеки VLAN, независимо колко резервни трасета има, така се консумира повече памет и процесорно време на комутатора, както и се изпращат отделни служебни пакети (BPDU) за всеки VLAN. При MSTP се изграждат толкова дървета, колкото са необходими и се назначава кои VLAN кое дърво да използва. Така се пестят ресурси на комутаторите и мрежата.

2.6. VLAN Spanning Tree Protocol

Разработка на Juniper Networks за съвместимост с PVST+ на Cisco Systems. Изгражда отделно дърво за всеки VLAN. Работи само на някои модели комутатори на компанията и има известни ограничения.

2.7. Rapid Per-VLAN Spanning Tree + (RPVST+)

Този протокол е разработка на Cisco Systems и представлява комбинация от бързия RSTP, като се изгражда отделно дърво за всеки VLAN, като при PVST+, с което се използват по-ефективно резервираните трасета.

Забележка: Поради ограничения на използвания симулатор Cisco Packet Tracer се поддържат само протоколите PVST+ и RPVST+.

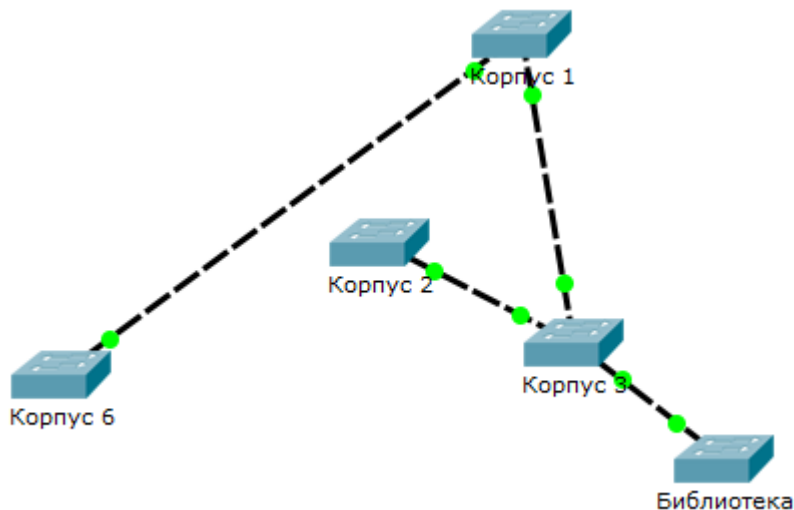
3. Задачи за изпълнение

1. Чрез програмата Cisco Packet Tracer заредете файла **no-spanningtree.pkt**. Проверете настройките на IP адреси на компютъра и сървъра. Чрез командата Ping изпратете ICMP пакет от компютъра до сървъра. Наблюдавайте преминаването на данните в режим на симулация. Проверете какви пакети

достигат до устройството за прихващане на данни (Sniffer). Как можете да спрете получения broadcast storm?

2. Заредете файла **STP.pkt**. Разгледайте топологията. Определете кой комутатор е root и какви са състоянията на портовете. Изпратете чрез ping пакети от компютъра до сървъра и наблюдавайте до къде достига ARP заявката в режим на симулация. Има ли зацикляне на информацията?
3. Симулирайте прекъсване на връзката на основното трасе между S1 и S0. Наблюдавайте преконфигурирането на мрежата. За колко време се възстановява предаването на пакети между компютъра и сървъра? Възстановете връзката.
4. Създайте нов компютър в топологията без да го включвате с кабел, назначете му IP адрес от мрежата. Пуснете ping -t към новия компютър от PC0. Включете новия компютър с кабел към интерфейс Fa0/2. Наблюдавайте след колко време ще стане достъпен.
5. Включете същия компютър към порт fa0/24, който е настроен в режим PortFast. Каква е разликата?
6. Свържете несвързания комутатор S3 с кабел към S1. Наблюдавайте промените в реално време. Колко време изисква преконфигурирането на мрежата? Определете кой комутатор е root и какви са състоянията на портовете. Повторете действията в режим на симулация, разгледайте пакетите, тяхната последователност и съдържание.
7. Свържете S3 и към S0. Наблюдавайте процеса на преконфигурация в реално време и в симулация. Каква е новата топология на мрежата?
8. Заредете файла **RSTP.pkt**. Разгледайте топологията. Определете кой комутатор е root и какви са състоянията на портовете. Изпратете чрез ping пакети от компютъра до сървъра и наблюдавайте до къде достига ARP заявката в режим на симулация. Има ли зацикляне на информацията? Изпълнете задачи 3 – 7 с новия протокол и вижте разликата.
9. Заредете файла **PVST.pkt**. Адресирайте компютрите според фигурата. Наблюдавайте откъде минават пакетите за различните VLAN. Проверете отказоустойчивостта, изключвайки един по един всеки от двата гръбначни сегмента, след което възстановете връзката.

10. Симулирайте топологията на университетската мрежа. Добавете отказоустойчивост чрез прекарване на нови трасета от корпус 6 до библиотека и от корпус 2 до корпус 1. Проверете отказоустойчивостта. Кой комутатор е коренът на дървото? Как можете да направите мрежата по-устойчива?



4. Контролни въпроси

1. Защо е необходим протоколът STP?
2. Как може да се постигне отказоустойчивост в локална мрежа без STP?
3. Важно ли е кой комутатор ще се избере за корен (root)?
4. Колко време се преконфигурира мрежата при STP? А при RSTP?
5. Защо е необходимо да се прави повече от едно дърво?
6. Как може да се ускори достъпността на ново включено устройство към мрежата при STP? Какво е положението при RSTP?
7. При спецификацията от 2008 година, ако имаме едно трасе, съставено от три последователни 10 Gbit/s мрежови сегмена и второ трасе, съставено от един 1 Gbit/s мрежов сегмент кое ще бъде предпочетено?

5. Допълнителни ресурси

1. IEEE, IEEE Standard for Local and Metropolitan Area Networks—Media access control (MAC) Bridges (Incorporates IEEE 802.1t™-2001 and IEEE 802.1w™), <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>, дата на използване 26.03.2017 г.
2. Cisco Systems, Per VLAN Spanning Tree Plus (PVST+), <http://www.cisco.com/c/en/us/tech/lan-switching/per-vlan-spanning-tree-plus-pvst/index.html>, дата на използване 26.03.2017 г.
3. IEEE, 802.1s - Multiple Spanning Trees, <http://www.ieee802.org/1/pages/802.1s.html>, дата на използване 26.03.2017 г.