Internet Technologies

Kamil NOWAK
Katedra Informatyki
Wydział Informatyki i Zarządzania Politechniki Wrocławskiej
kamil.nowak@pwr.edu.pl

Spanning Tree Protocol (STP)
- Creating redundant LAN topologies
- Protection against loops and broadcast storm in the switched network

Version 0.1-181025

Keywords
STP, RSTP, switching loop, broadcast storm, spanning tree, redundant topology, root bridge

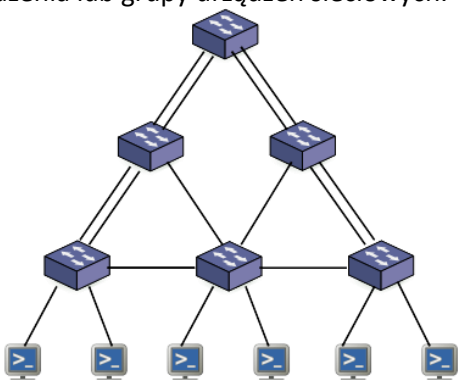
Wprowadzenie
Wprowadzenie nadmiarowych łączy do topologii sieci bazującej na przełącznikach sprawia, że sieć staje się bardziej niezawodna. Nadmiarowe łącza zwiększają odporność sieci na awarie i przeciążenia. Przypadkowo odpięty lub uszkodzone kabel, awaria zasilania w jednym z przełączników lub inne zdarzenia nie zakłócą całkowicie działania sieci. Nadmiarowe łącza sprawiają, że urządzenia posiadają alternatywne drogi do poprowadzenia ruchu i ominięcia uszkodzenia.
Wprowadzenie nadmiarowości łączy niesie z sobą jednak zagrożenia zapętlenia ruchu. Protokół Ethernet działający w drugiej warstwie sieciowej ISO-OSI nie posiada żadnych mechanizmów ochrony przed pętlami. Niekontrolowany, zapętlony ruch prowadzi do przeciążenia urządzeń. Szczególnie groźne są ramki broadcastowe, które propagowane są do wszystkich portów przełącznika (z wyjątkiem nadającego broadcast). Nadmierna ilość krążących broadcastów tworzy tzw. sztormy broadcastowe, które przeciążają przełącznik do tego stopnia, że nie jest w stanie przekazywać zwykłego ruchu.
Mechanizmem zabezpieczającym przed tworzeniem pętli komunikacyjnych w sieciach przełączanych jest protokół Spanning Tree (STP). Protokół ten jest obecnie dostępny w większości przełączników (tzw. zarządzalnych) i domyślnie uruchomiony. Protokół posiada różne odmiany (szybkie, wolne, otwarte, zamknięte) i różne możliwości parametryzacji. Źle działający protokół STP potrafi mocno spowolnić sieć, dlatego ważna jest jego zrozumienie i umiejętne dostosowanie do posiadanej topologii.

Spis treści

Protokół drzewa opinającego - STP (Spanning Tree Protocol)

Nadmiarowość fizycznych połączeń w sieci lokalnej.

W celu zwiększenia niezawodności sieci komputerowych projektuje się topologie zawierające nadmiarowe, dodatkowe fizyczne połączenia pomiędzy aktywnymi urządzeniami. Alternatywne łącza mogą wystąpić pomiędzy sąsiednimi urządzeniami lub pomiędzy grupą urządzeń, tworząc rodzaj sieci. Rozwiązanie to wprawdzie zmniejsza ilość użytecznych portów, ale zapewnia ciągłość pracy sieci w przypadku awarii kabla, urządzenia lub grupy urządzeń sieciowych.



Rysunek 1 Nadmiarowość połączeń w sieci bazującej na przełącznikach.

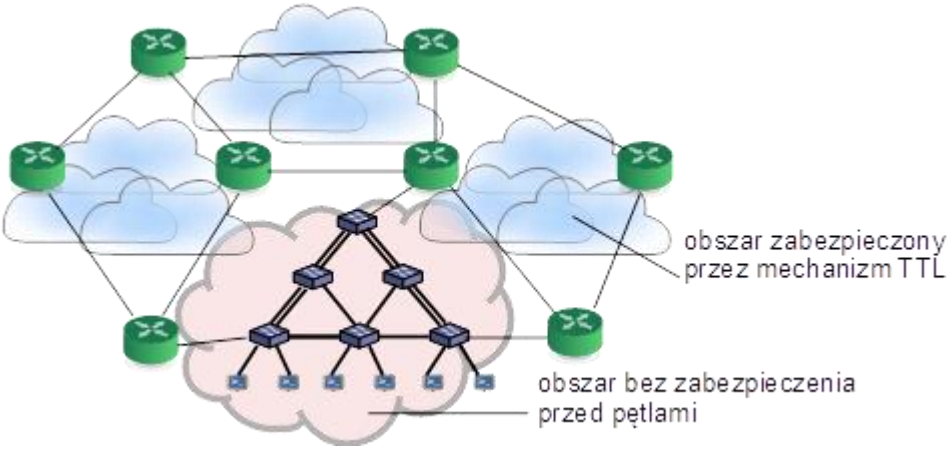
Nadmiarowe i niekontrolowane połączenia w sieci bazującej na przełącznikach niosą ze sobą duże zagrożenia. W sieci lokalnej zostają utworzone pętle komunikacyjne. Ramki z wiadomościami unicastowymi powielają się, a ramki broadcastowe krążą w pętlach zmniejszając w ten sposób dostępną przepustowość i wydajność sieci. Efekty powstałych pętli mogą być następujące:

- Niestabilność bazy danych MAC adresów na przełączniku – te same adresy mogą pojawiać się na różnych portach. Przełącznik w krótkim czasie zmienia przypisanie danego adresu MAC do różnych portów, przez co host docelowy może być nieosiągalny;
- Wielokrotne rozsyłanie tych samych ramek unicastowych – do odbiorcy mogą docierać wielokrotnie te same dane;
- Tworzenie sztormów broadcastowych – ramki typu broadcast krążą w pętli w nieskończoność.

Duża liczba krążących ramek zmniejsza wydajność sieci i ostatecznie może prowadzić do jej przeciążenia. Ramkami bardzo groźnymi dla wydajności sieci są ramki broadcastowe, przeznaczone do wszystkich odbiorców. W ich przypadku przełącznik nie będzie potrafił ograniczyć ich propagacji posługując się tablicą MAC adresów. Ramki te domyślnie są przesyłane do wszystkich portów, z wyjątkiem portu, z którego przyszły.

Protokół Spanning Tree

Protokół IP działający w warstwie trzeciej posiada mechanizm zabezpieczający przed nieskończonym przesyłaniem tego samego pakietu. W nagłówku sterującym protokołu IP występuje pole TTL (Time To Live), którego wartość jest obniżana po przejściu pakietu przez każdy router. Dlatego „zabłąkane” pakiety są usuwane z sieci, gdy wartość TTL w ich nagłówku IP osiągnie wartość 0. Mechanizm ten działa jedynie w sieci pomiędzy routerami i tylko pośrednio zabezpiecza przed pętlami.



Rysunek 2 - Protokół Ethernet nie posiada mechanizmu ochrony przed pętlami komunikacyjnymi.

Protokół Ethernet nie posiada mechanizmu zabezpieczającego przed ciągłym propagowaniem tych samych ramek w przypadku wystąpienia pętli w topologii sieci. Sposobem na „przecięcie" pętli komunikacyjnej w środowisku sieci bazującej na przełącznikach jest fizyczne albo programowe zablokowanie portu poprzez który tworzy się pętla. Fizyczne rozpięcie połączeń alternatywnych sprawi, że nasza sieć przestanie być odporna na uszkodzenia łączy i urządzeń. Rozwiązaniem umożliwiającym posiadanie topologii nadmiarowej jest programowe blokowanie portów. Programowy mechanizm blokowania wspierany jest przez protokół STP (Spanning Tree Protocol). Protokół ten jest domyślnie zaimplementowany i aktywowany w większości przełączników sieciowych. Protokół STP służy do przerywania pętli, powstałych przy połączeniach przełączników. Jest to protokół, który działa w warstwie drugiej modelu ISO-OSI. Protokół ten powinien być zaimplementowany na większości zarządzalnych przełączników.
Tworzenie nadmiarowych połączeń pomiędzy przełącznikami zapewnia bezpieczeństwo w przypadku awarii kabla lub przełącznika. Stworzone w ten sposób pętle powinny być rozcinane przez protokół STP. W przypadku awarii łącza głównego protokół STP uaktywnia połączenie zapasowe. Jeżeli połączenie główne zostanie przywrócone, połączenie zapasowe zostanie ponownie zablokowane. Sposób blokowania pętli przez przełącznik jest ścisłe określony poprzez algorytm spanning-tree (protokół drzewa rozpinającego).

Mechanizm powstawania zdublowanych ramek i sztormów broadcastowych

Występujące w topologii sieci pętle komunikacyjne umożliwiają tworzenie się tzw. sztormów broadcastowych. Przełącznik wysyła zapytania broadcast do wszystkich aktywnych portów w danej sieci VLAN oraz do wszystkich aktywnych połączeń typu trunk, w których dany VLAN jest przepuszczany. Jeżeli przełącznik X wyśle ramkę broadcastową do połączonego z nim przełącznika Y, to ten również roześle tę ramkę do wszystkich aktywnych portów. W przypadku gdy istnieje drugie (i dalsze) połączenie do przełącznika X, ramka typu broadcast trafi z powrotem do przełącznika X, który ją wysłał. Przełącznik X roześle ramkę ponownie do wszystkich aktywnych portów, co sprawi, że ramka będzie krążyć w pętli w nieskończoność. Pojawiające się kolejne zapytania broadcast dodają się do poprzednich i zaczynają krążyć razem w pętli. Duża ilość krążących broadcastów może przeciążyć przełącznik i sprawić, że stanie się on niestabilny. Przełącznik może ulec czasowej awarii.

Zasada działania algorytmu drzewa rozpinającego

Przełączniki spięte w sieć wymieniają między sobą informacje STP w postaci ramek BPDU (Bridge Protocol Data Unit). Przełącznik, który odebrał na którymś z portów ramkę BPDU uaktywnia protokół STP. Działanie protokołu STP zaburza czasowo pracę sieci (30-60s).Łączone porty nie są w stanie

przesyłać danych użytkowników do momentu zakończenia działania algorytmu. W trakcie działania algorytmu nowo połączony port może przyjmować różne stany:

- listening (port aktywny);
- learning (uczenie się adresów MAC);
- forwarding (przekazywanie ramek);
- blocking (port zablokowany);
- disabled (wyłączony administracyjnie).

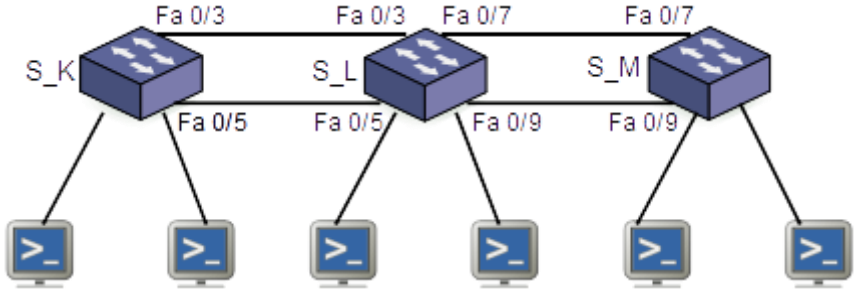
W ramkach BPDU zapisane są następujące informacje:

- Root BID (priorytet plus VLAN nr +MAC address)
- Patch cost (odległość do przełącznika root liczona jako suma kosztów portów na drodze do przełącznika root)
- Sender Bridge ID
- Port ID (identyfikator portu, z którego ramka BPDU została nadana: priorytet portu plus numer).

Domyślny priorytet nieskonfigurowanego przełącznika wynosi 32768. Jest on powiększany o numer VLANu. Domyślny priorytet portu to 8. Przełącznik jest jednoznacznie identyfikowany przez identyfikator powstały przez dodanie priorytetu STP, numeru VLANu i adresu MAC. Identyfikator ten określany jest jako *Bridges ID*. Przykładowo dla VLANu 10, *Bridges ID* wyniesie 32778 plus adres MAC. Priorytet można ustawiać w zakresie 0-61440. Im przełącznik ma niższą wartość Bridges id tym wyższy jest jego priorytet w procesie wyboru przełącznika głównego root. W przypadku ustawiania priorytetu można skonfigurować tylko jego określoną wartość będącą wielokrotnością wartości 4098 (0, 4096, 8192, 12288, 16384, ...).

Konfiguracja protokołu STP na przykładzie przełącznika firmy Cisco.

Konfiguracja fizycznego urządzenia



Rysunek 3 - Przykładowa topologia sieci przełączników z dodatkowymi łączami.

Sprawdzenie konfiguracji protokołu STP na przełączniku:

```
S_K#show spanning-tree
```

Sprawdzenie konfiguracji protokołu STP na przełączniku w konkretnej sieci VLAN:

```
S_K#show spanning-tree VLAN K
S_K#show spanning-tree VLAN K-M
```

Zmiana priorytetu przełącznika:

```
S_L(config)#spanning-tree vlan L priority 4096 (0-61440 increments of 4096)
S_L(config)#spanning-tree vlan K-L root primary
S_L(config)#spanning-tree vlan M root secondary
```

Przywrócenie domyślnego priorytetu przełącznika

```
S_L(config)#spanning-tree vlan M no root primary
```

Debugowanie protokołu STP

```
S_K#debug spanning-tree ?
S_K#debug spanning-tree events
```

Ustawienie szybkiej wersji protokołu STP

```
S_L(config)#spanning-tree mode rapid-pvst
```

Zmiana priorytetu portu:

```
S_L(config)#interface Fa 0/5
S_L(config-if)#spanning-tree cost 18
```

Powrót do domyślnej wartości kosztu portu na przełączniku

```
S_L(config-if)#no spanning-tree cost
```

Wyłączenie protokołu STP na portach typu access i ustawienie ochrony przed przypadkowym odbiorem ramek STP (BPDU) na tych portach:

```
S_K(config)#interface range Fa 0/3, Fa 0/5
S_K(config-if)#spanning-tree portfast
S_K(config-if)#spanning-tree bpduguard enable
```

Literatura

Materiały dydaktyczne Akademii Cisco CCNA 3

Laboratory tasks
- Spanning Tree Protocol (STP)

Basic information

Variables and symbols

- X - the variable X corresponds to the device number, as well as the laboratory group number.
- Y – universal variable correspond to device number of any other group.
- K, L, M, N, ... - variables used interchangeably with the variable X and Y. Correspond to the devices and groups numbers.
  The variables K, L, M, N, ... are used when the order of the connected devices is important. For example, when configuration on the R_K router differs from the R_L router configuration. The variable L should correspond to the number of the current device (current laboratory group number), variable K indicates the "left" device and M the "right" device.
- A, B, C, ... - variables corresponding to the addresses of the networks created in the labs.
- [1.2.3.4] – the number of the CCNA lab corresponding to the current exercise.
- {Variable} - designation of the required variable.
- [Variable] - designation of an alternative variable.
- 1 point - points indicate the degree of difficulty of a given task.
- COLORS - can be used to display some additional meaning:
  - **red - means extremely important things and obligatory tasks;**
  - orange - means additional/alternative tasks;
  - gray - means content that can be omitted in standard mode;
  - green – means additional information, explanations;
  - blue – means information to note to be checked by the instructor.
- FONT
  - **bold - highlighted information.**
  - `Courier New - means configuration commands.`

IP addressing and device names used in the exercise

PCs

Name:		PC_L1, PC_L2
Net:		LAN_L1 (Cisco)
	IP PC_L1:	192.168.0.L1 / 24
	IP PC_L2:	192.168.0.L2 / 24
Gateway:		192.168.0.L0

Switch

Name:		S_L
Net:		LAN_L1
	Interface:	VLAN 1
	IP:	192.168.0.L9 / 24
Native VLAN:		VLAN 1
Gateway:		192.168.0.L0

Router

Name: R_L
Net: LAN_L1
- Interface: Fa0/0 (Fa0/2/0, or another connected)
- IP: 192.168.0.L0 / 24

Net: WAN_L1
- Interface: Serial 0/0/0 DCE (Serial 0/3/0 or another connected)
- IP: 10.L.M.1/ 30
- clock rate: 128000

Net: WAN_L2
- Interface: Serial 0/0/1 DTE (Serial 0/1/0, 0/3/1 or another connected)
- IP: 10.K.L.2/ 30
- clock rate: brak

Net: WAN_L3 (if exist)
- Interface: Serial 0/3/0 DCE (Serial 0/3/0 lub inny podłączony)
- IP: 10.X.Y.1(2)/ 30
- clock rate: 128000 lub brak w zależności od topologii

Gateway: Serial 0/0/0 (“right” serial interface)

Base topology of a single laboratory group

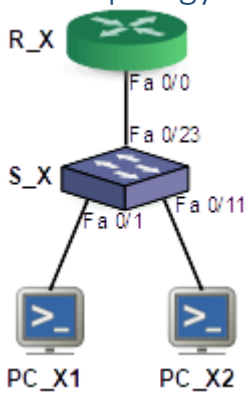


Figure 4 - Base topology of a single laboratory group.

PC_X1 connected with a straight cable to S_X port Fa 0/1.
PC_X2 connected with a straight cable to S_X port Fa 0/11.
R_X connected with a straight cable to S_X port Fa 0/23.

Base PC configuration

Configure the computer's IP addresses according to the data given in the manual. Add the addresses on the network card that leads to the lab set (Cisco).
Check if the second network card (Internet) receives the correct address from the DHCP server.

Base switch configuration

1. Erase the old configuration if exist and reload the switch.

```
S_X#erase startup-config .
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm] – confirm with ENTER
```

```
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

S_X#delete vlan.dat
Delete filename [vlan.dat]? – confirm with ENTER
Delete flash:vlan.dat? [confirm] – confirm with ENTER
S_X#reload .
Proceed with reload? [confirm] – confirm with ENTER
```

Do not save the configuration during the reload.

After restarting, do not enter the auto-configuration mode:

```
Would you like to enter the initial configuration dialog? [yes/no]:
no
Would you like to terminate autoinstall? [yes/no]: yes
```

2. Check if the configuration has definitely been deleted.

```
S_X#show startup-config
startup-config is not present
```

3. Set the device name according to the device number X: S_X, R_X, ...

```
Switch(config)#hostname S_X
```

4. Set the console password - **cisco**

```
S_X(config)#line console 0
S_X(config-line)#password cisco
S_X(config-line)#login
```

5. Set enable level password - **class**

```
S_X(config)#enable password class
```

6. Set the vty (telnet/ssh) password - **cisco**

```
S_X(config)#line vty 0 15
S_X(config-line)#password cisco
S_X(config-line)#login
```

7. Protect console and vty terminals against command breaks caused by the console messages.

```
S_X(config-line)#logging synchronous
```

8. Set the protection against the translation to the IP address of the incorrectly entered commands

```
S_X(config)#no ip domain-lookup
```

9. Set the motd message

```
S_X(config)#banner motd #Group X welcome. Unauthorized access to this
device is strongly prohibited!#
```

10. Configure the required IP addresses.

```
S_X(config)#interface vlan 1
S_X(config-if)#ip address 192.168.0.X9 255.255.255.0
```

11. Activate all used interfaces.

```
S_X(config-if)#no shutdown
```

12. Test connectivity between devices.

```
S_X#ping 192.168.0.X1 (PC1)
S_X#ping 192.168.0.X2 (PC2)
```

13. Check the possibility of remote login.

Connection PC_X1 – S_X

```
C:\Users\Adm>telnet 192.168.0.X9
…
```

Connection PC_X2 – S_X

```
C:\Users\Adm>telnet 192.168.0.X9
…
```

References to the CCNA R&S 3 v. 6.0 labs

[3.0.1.2] - Class Activity - Stormy Traffic Instructions
[3.1.2.12] - Building a Switched Network with Redundant Links
[3.3.2.3] - Configuring Rapid PVST, PortFast, and BPDU Guard
[3.4.1.1.] - Class Activity - Documentation Tree

References to the CCNA R&S 3 v. 6.0 Packet Tracer scripts

[3.1.1.5] - Packet Tracer - Examining a Redundant Design
[3.3.1.5] - Packet Tracer - Configuring PVST+
[3.3.2.2.] - Packet Tracer - Configuring Rapid PVST+

Task 1 – Creation of LAN network topology with redundant connections between switches

Points: 2

Exercise objectives:

→ Creation of LAN topology with redundant connections between switches. Two or more switches should be used.
→ Theoretical determination of the root bridge and ports that should be blocked in created topology.
→ Practical verification of previous calculation.
→ Study of the impact of changing the numbers of the connected ports, the priority of the switch and the cost of the port on the active topology of the network.
→ Checking the impact of changing the connected ports, the switch priority and the ports costs on the STP topology.

Practical task

The network administrator got the job of connecting the group of switches into a reliable network. The following problems, which occur in the company's network, should be solved:

- Overload of some switches preventing normal operation.
- Random failures of single switches cause the connectivity problems in entire network. Computers lose network and Internet access.

- Random switch failures prevent the entire network from operating. Computers lose connectivity and access to the Internet.
- The fast links are not fully used.

Network topology

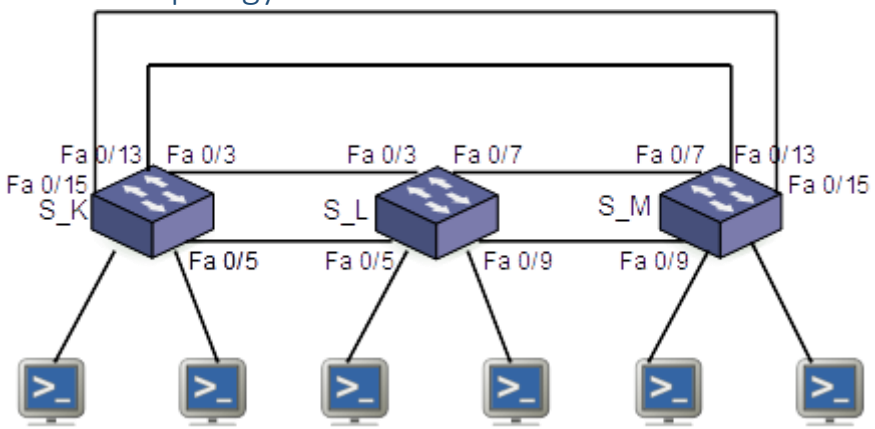


Figure 5 - The proposed laboratory network topology.

The task can be performed in several laboratory groups, each of which will configure one switch. Connect the cooperating switches using additional straight cables. The physical loops should be created between them. Proposed connections:

S_K port Fa 0/3 - S_L port Fa 0/3
S_K port Fa 0/5 - S_L port Fa 0/5

S_L port Fa 0/7 - S_M port Fa 0/7
S_L port Fa 0/9 - S_M port Fa 0/9

S_M port Fa 0/13 - S_K port Fa 0/13
S_M port Fa 0/15 - S_K port Fa 0/15

K, L, M – correspond to switches numbers.

Exercise scenario

Note: the person configuring the router should make a telnet connection to the S_X switch and write all the stages of the exercise in the notepad. In particular, save the results of commands marked in blue in the text.

1. Create a text document in the home directory and save the whole course of the exercise in it.
2. **Delete the previous switch and VLANs configuration and restart the device.**
3. Configure PCs to work in a laboratory network. Use the IP addresses provided in the instructions.
4. Create the basic configuration of the switch.
5. Check the correctness of connections in the underlying network topology. Add additional cable connections required in the exercise.
6. Establish parallel telnet connections to cooperating switches. It will allow monitoring their states during the exercise.

```
C:\Users\Adm>telnet 192.168.0.Y9
C:\Users\Adm>telnet …
```

7. Check and save the Bridge ID, VLAN priority values and port costs on each switch.
8. Figure out and note which switch should be selected as the root and which ports should be blocked by the STP protocol. Explain why.
9. Check if the switches have disabled the previously predicted ports. In the case of mistakes, correct and save your new calculations. Write in the notepad the states of all connected switch ports.
10. On the root switch swap the cables that create the loop. For example, if the switch S_K has been selected as the root switch and switch S_L as the slave switch change the cables as follows:

    S_K port Fa 0/**5** - S_L port Fa 0/3
    S_K port Fa 0/**3** - S_L port Fa 0/5
11. Figure out and save which ports should be blocked.
12. Check which ports have been really blocked. In case of difference, repeat calculations. Write in the notebook the states of all connected switch ports.
13. Restore the original cable connections.
14. Check precisely the default costs of the switch ports.

    ```
    S_L#show spanning-tree
    ```
15. On the slave switch, increase the priority of the blocked port.

    ```
    S_L(config)#interface f0/5
    S_L(config-if)#spanning-tree vlan 1 cost 18
    ```
16. Check and record which port is blocked. Write in the notepad the states of all switch ports.
17. Restore the original port settings.
18. If the switches have higher-speed ports, connect them together. For example, perform an additional connection of the following ports:

    S_K port Gi 0/1 - S_L port Gi 0/1
19. Figure out and save which ports should be blocked in new topology.
20. Check in practice which ports have been blocked. In the case of difference, repeat the calculation. Write in the notebook the states of all switch ports.
21. Swap the cable on the root switch (not blocking the ports) from the port with the higher speed to the lower one. For example:

    S_K port Fa 0/**7** - S_L port Gi 0/1
22. Check in practice which ports have been blocked. Write in the notepad the states of all switch ports.
23. Before proceeding to the next task, report the results stored in the text file to the instructor.
24. **If this is your last exercise, delete the device's startup configuration. Release and put back the extra cables used in the exercise.**

Task 2 – Controlling the selection of the Root bridge for individual VLANs

Points: 1

Exercise objectives:

→ Creation of LAN topology with redundant connections between switches. Two or more switches should be used.

→ Creation of new VLAN: VLAN K, VLAN L, VLAN M.

→ Balancing of switch traffic across all physical trunk links.

→ Changing the Bridge ID parameter for individual VLANs in the way the S_K, S_L, S_M switches will become the root bridge in the corresponding VLAN.

Practical task

The administrator in the company got the job of connecting the group of switches into a reliable network. After applying redundant connections and implementing the STP protocol, it turned out that the network is still not efficient. Communication between computers connected to distant switches is always done through the main switch overloading its links. Despite the physical connection and proximity, edge switches cannot communicate with each other because the links are blocked by STP protocol. The administrator has the task to spread traffic between all trunk links.

Network topology

The task can be performed in several laboratory groups, each of which will configure one switch. Connect the cooperating switches using additional straight cables. The physical loops should be created between them. Proposed connections:

S_K port Fa 0/3 - S_L port Fa 0/3
S_K port Fa 0/5 - S_L port Fa 0/5

S_L port Fa 0/7 - S_M port Fa 0/7
S_L port Fa 0/9 - S_M port Fa 0/9

S_M port Fa 0/13 - S_K port Fa 0/13
S_M port Fa 0/15 - S_K port Fa 0/15

K, L, M – means switches numbers.

Exercise scenario

Note: the person configuring the router should make a telnet connection to the S_X switch and write all the stages of the exercise in the notepad. In particular, save the results of commands marked in blue in the text.

1. Create a text document in the home directory and save the whole course of the exercise in it.
2. Create additional VLANs on each of the cooperating switches: VLAN K, VLAN L, VLAN M.
3. Ensure connectivity of all VLANs configured on the switches. All ports connecting the switches should be configured in trunk mode.
4. Establish parallel telnet connections to cooperating switches. It will allow monitoring their states during the exercise.
5. Change the priorities of the switches so that they are selected as the root bridges in the appropriate VLANs (VLAN number corresponding to the switch number).

   ```
   S_L(config)#spanning-tree vlan L priority ...
   ```

   or by automatic enforcement

   ```
   S_L(config)#spanning-tree vlan L root primary
   ```

   or

   ```
   S_M(config)#spanning-tree vlan L root secondary
   ```

6. Check and save how much priority increase/decrease with the second command (`... root primary/secondary`)?
7. Before proceeding to the next task, report the results stored in the text file to the instructor.
8. **If this is your last exercise, delete the device's startup configuration. Release and put back the extra cables used in the exercise.**

Task 3 – Configuration of the rapid STP protocol.

Points: 1

Exercise objectives:

→ Creation of LAN topology with redundant connections between switches. Two or more switches should be used for the exercise.

→ Creation of the VLAN networks: VLAN99, VLAN K, VLAN L, VLAN M.

→ Checking the convergence of the STP protocol.

→ Checking the response time of STP protocol to topology changes.

→ Acceleration of the STP protocol using PortFast and BPDU Guartd commands.

→ Configuration of RSTP protocol (Rapid PVST +).

→ Checking the convergence of the RSTP protocol (Rapid PVST +).

Practical task

There are frequent changes to the network topology in the company. Managers who coordinate the work of various teams should connect their laptops to different network segments. They complains about very long times the computers connect to the network. Additionally any changes in the network topology make the whole network stop working properly for quite long time. Employees are nervous about the long waiting time for access to resources.
The network administrator got the task to parametrize the switched network. The network should be resistant to topology changes and the computers should immediately connect to the network.

Network topology

The task can be performed in several laboratory groups, each of which will configure one single switch. Connect the cooperating switches using additional straight cables. The physical loops should be created between them. Proposed connections:

S_K port Fa 0/3 - S_L port Fa 0/3
S_K port Fa 0/5 - S_L port Fa 0/5

S_L port Fa 0/7 - S_M port Fa 0/7
S_L port Fa 0/9 - S_M port Fa 0/9

S_M port Fa 0/13 - S_K port Fa 0/13
S_M port Fa 0/15 - S_K port Fa 0/15

K, L, M – correspond to switches numbers.

Exercise scenario

Note: the person configuring the router should make a telnet connection to the S_X switch and write all the stages of the exercise in the notepad. In particular, save the results of commands marked in blue in the text.

1. Create a text document in the home directory and save the whole course of the exercise in it.
2. Create new VLANs on every switch: VLAN 99, VLAN K, VLAN L, VLAN M.
3. Configure the ports interconnecting the switches in the trunk mode.
4. Set VLAN 99 as management VLAN.
5. Configure the ports connected to PCs in VLAN 99.
6. Establish parallel telnet connections to cooperating switches. It will allow monitoring their states during the exercise.
7. Measure the approximate convergence time of the STP protocol on trunk ports. Unplug and plug any trunk link. Check the amount of time the STP protocol needs for activation of new trunk connection. Observe the behavior of the LED on the port. Test the connection to remote switch with the `ping -t` command. Note the convergence time and number of ping loss.
8. Measure the approximate convergence time of the STP protocol on access ports. Unplug and plug the cable connecting PC to switch. Note the convergence time and number of ping loss.
9. Configure the Rapid STP (Rapid PVST +) protocol. The computers ports set to PortFast mode and set the BPDU Guard protection.
10. Measure the approximate convergence time of the RSTP protocol on trunk ports. Disconnect and reconnect any active trunk link. Check the amount of time the RSTP protocol needs for activation of new trunk connection. Observe the behavior of the LED on the switch port. Test the connection to remote switch with the `ping -t` command. Note the convergence time and number of ping loss.
11. Measure the approximate convergence time of the RSTP protocol on access ports (PC ports). Unplug and plug the cable connecting PC to switch. Note the convergence time and number of ping loss.
12. Before proceeding to the next task, report the results stored in the text file to the instructor.
13. **If this is your last exercise, delete the device's startup configuration. Release and put back the extra cables used in the exercise.**

Alternative Task 4 – Triggering a broadcast storm on the switch

Points: 1

Exercise objectives:

→ Triggering a broadcast storm on the switch.

→ Testing the overloaded switch behavior.

Practical task

W jednym z departamentów firmy praca w sieci komputerowej staje się bardzo uciążliwa. Przełączniki wyglądają na przeciążone. W szafie rakowej słychać głośne działanie wentylatorów. Na urządzeniach widać ciągle migające diody LED. Pracownicy nie mogą dostać się do serwerów firmy. Problem chwilowo zanika po zresetowaniu urządzeń sieciowych.

Administrator dostał za zadanie zdiagnozować i rozwiązać problem. Podejrzewa, że system przeciążany jest przez burze broadcastową. Administrator dostał zgodę na czasowe odcięcie fragmentu sieci od reszty przedsiębiorstwa i zrobienie testów przeciążeniowych.

Network topology

Zadanie można wykonać wspólnie w kilku grupach laboratoryjnych, z których każda będzie odpowiedzialna za skonfigurowanie jednego z przełączników.
Używając dodatkowych kabli prostych połącz przełączniki w ten sposób, aby utworzyły się pomiędzy nimi fizyczne pętle. Można stworzyć również pętlę łącząc kablem porty tego samego przełącznika.
Proponowane połączenia:

S_K port Fa 0/3 - S_L port Fa 0/3
S_K port Fa 0/5 - S_L port Fa 0/5

S_**K** port Fa 0/7 - S_**K** port Fa 0/9
S_**L** port Fa 0/9 - S_**L** port Fa 0/9

K, L – oznaczają numery przełączników

Exercise scenario

Uwaga: osoba konfigurująca router powinna wykonać połączenie telnet do przełącznika S_X i zapisywać w notatniku wszystkie etapy ćwiczenia. W szczególności należy zapisać rezultaty poleceń zaznaczonych na niebiesko w tekście.

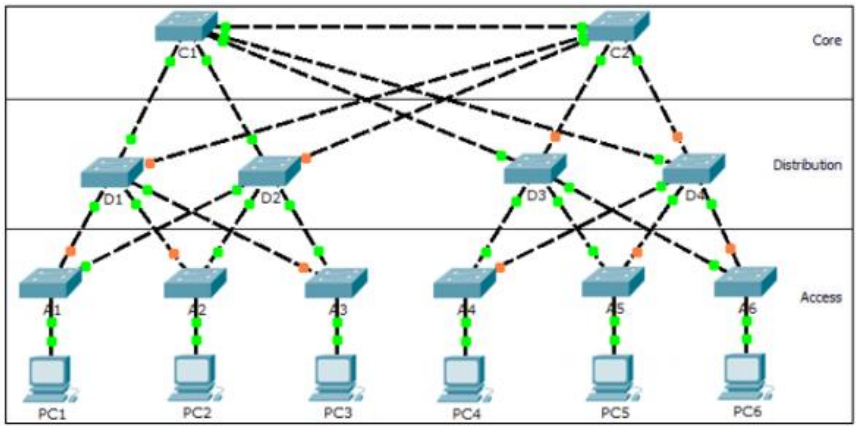
1. W katalogu domowym utwórz dokument tekstowy i zapisuj w nim cały przebieg ćwiczenia.
2. Wyłącz protokół STP na swoim przełączniku.
3. Wykonaj jedną lub więcej pętli używając dodatkowego kabla komputerowego. Pętla może obejmować tylko jeden lub więcej przełączników.
4. Do przełącznika podłącz dwa komputery PC.
5. Na pierwszym z komputerów staraj się wytworzyć ruch broadcastowy.
6. Na drugim z komputerów uruchom program Wireshark i spróbuj znaleźć powtarzające się ramki broadcastowe. Zapisz w notatniku i przedstaw w programie Wireshark zapętlone ramki.
7. Sprawdzaj obciążenie przełącznika.

```
S_K#show process ?
S_K#show process cpu
S_K#show process mem
```

8. Przed przejściem do kolejnego zadania zgłoś wyniki zapisane w pliku tekstowym do sprawdzenia instruktorowi.
9. **Jeżeli jest to twoje ostatnie ćwiczenie skasuj konfigurację startową urządzeń. Rozepnij i odłóż na miejsce dodatkowe kable użyte w ćwiczeniu**.

Zadania laboratoryjne w środowisku wirtualnym symulatora Packet Tracer
- Spanning Tree Protocol (STP)

Środowisko programu Packet Tracer umożliwia analizę działania protokołu STP w rozbudowanej sieci komputerowej. Symulator umożliwia realizowanie zadań dydaktycznych bez dostępu do fizycznego sprzętu. W symulatorze można również zaprojektować i przeprowadzić proste testy złożonej sieci komputerowej. Należy pamiętać, że w symulowanym środowisku użytkownik ma dostęp jedynie do wybranych modeli przełączników oraz wybranych wersji systemów operacyjnych. Nie wszystkie komendy CLI zostały zaimplementowane.



Rysunek 6 - Przykładowa topologia sieci stworzona w programie Packet Tracer. Źródło: materiały Akademii Cisco CCNA3