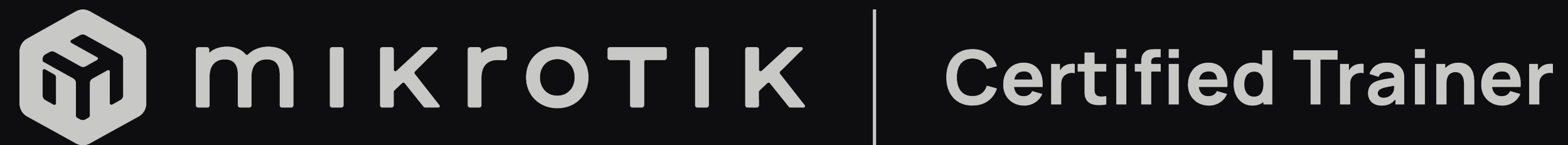


MBUM #9

RSTP w RouterOS 7

Warszawa - 2024

Ihor Hreskiv



1000+

kursantów w Polsce

5+

lat pracy trenerem

200+

szkoleń w Polsce

e-mail: ihor@hreskiv.pl



Wprowadzenie do RSTP **(Rapid Spanning Tree Protocol)**

Algorhyme

I think that I shall never see
A graph more lovely than a tree.

A tree whose crucial property
Is loop-free connectivity.

A tree which must be sure to span
So packets can reach every LAN.

First the root must be selected.
By ID it is elected.

Least cost paths from root are traced.
In the tree these paths are placed.

A mesh is made by folks like me
Then bridges find a spanning tree.

Radia Perlman, 1985

Czym jest RSTP?



Czym jest RSTP?

Protokół **Rapid Spanning Tree** - algorytm drzewa rozpinającego, znany również jako IEEE 802.1w

Czym jest RSTP? / Standardy

802.1D-1990 - MAC Bridges

802.1D-1998 - MAC Bridges (rollup of 802.1D-1990, 802.1j, 802.6k, P802.12e and P802.1p)

802.1w-2001 - Rapid Reconfiguration of Spanning Tree

802.1D-2004 - MAC Bridges (rollup of 802.1D-1998, 802.1t, 802.1w, P802.1y, and 802.11c)

Czym jest RSTP?

Protokół sieciowy zapobiegający pętlom w topologiach sieciowych:

- Następca klasycznego STP (Spanning Tree Protocol), skracający czas rekonfiguracji sieci.
- Znacznie szybsza konwergencja – od 1 do 6 sekund w porównaniu do 30-50 sekund w STP.

STP vs RSTP

Czas konwergencji: RSTP szybko reaguje na zmiany topologii (awarie), przełączając porty do stanu **Forwarding** niemal natychmiast.

Nowe stany portów:

Discarding: porty, które nie przekazują ruchu.

Learning: porty uczące się adresów MAC.

Forwarding: porty przekazujące ruch.

STP vs RSTP

Cechy	STP (Spanning Tree Protocol)	RSTP (Rapid Spanning Tree Protocol)
Standard	IEEE 802.1D	IEEE 802.1w
Czas konwergencji	30-50 sekund	1-6 sekund
Wysyłanie BPDU	Tylko root bridge	Każdy przełącznik
Częstotliwość wysyłania BPDU	Co 2 sekundy (domyślnie)	Co 2 sekundy
Porty w stanie Forwarding po uruchomieniu	Po fazach Listening i Learning	Natychmiast dla portów brzegowych (Edge)
Stany portów	Blocking, Listening, Learning, Forwarding, Disabled	Discarding, Learning, Forwarding
Maksymalny czas oczekiwania na BPDU	20 sekund	6 sekund
Mechanizm negocjacji	Brak (bazuje na stałych fazach)	Proposal i Agreement

Zasady działania RSTP

Podsumowanie kroków na każdym przełączniku:

1. Przełącznik wykrywa zmianę i wysyła **Proposal**.
2. Sąsiad analizuje propozycję i wysyła **Agreement**.
3. Porty natychmiast przechodzą do stanu **Forwarding**.

Korzyści z wykorzystania RSTP

Szybkie wykrywanie i eliminacja pętli sieciowych.

Minimalizacja przestojów w sieci w razie awarii.

Łatwa integracja z istniejącymi sieciami STP.

Mniejsze opóźnienia i większa wydajność sieci.

Łatwiejsza konfiguracja i zarządzanie

Konfiguracja RSTP

Konfiguracja bridge'a

STP

Protocol Mode ☐ MSTP ☐ none ☒ RSTP ☐ STP

Priority 8000

Port Cost Mode ☒ long ☐ short

Region Name

Region Revision 0

Max Message Age 00:00:20

Forward Delay 00:00:15

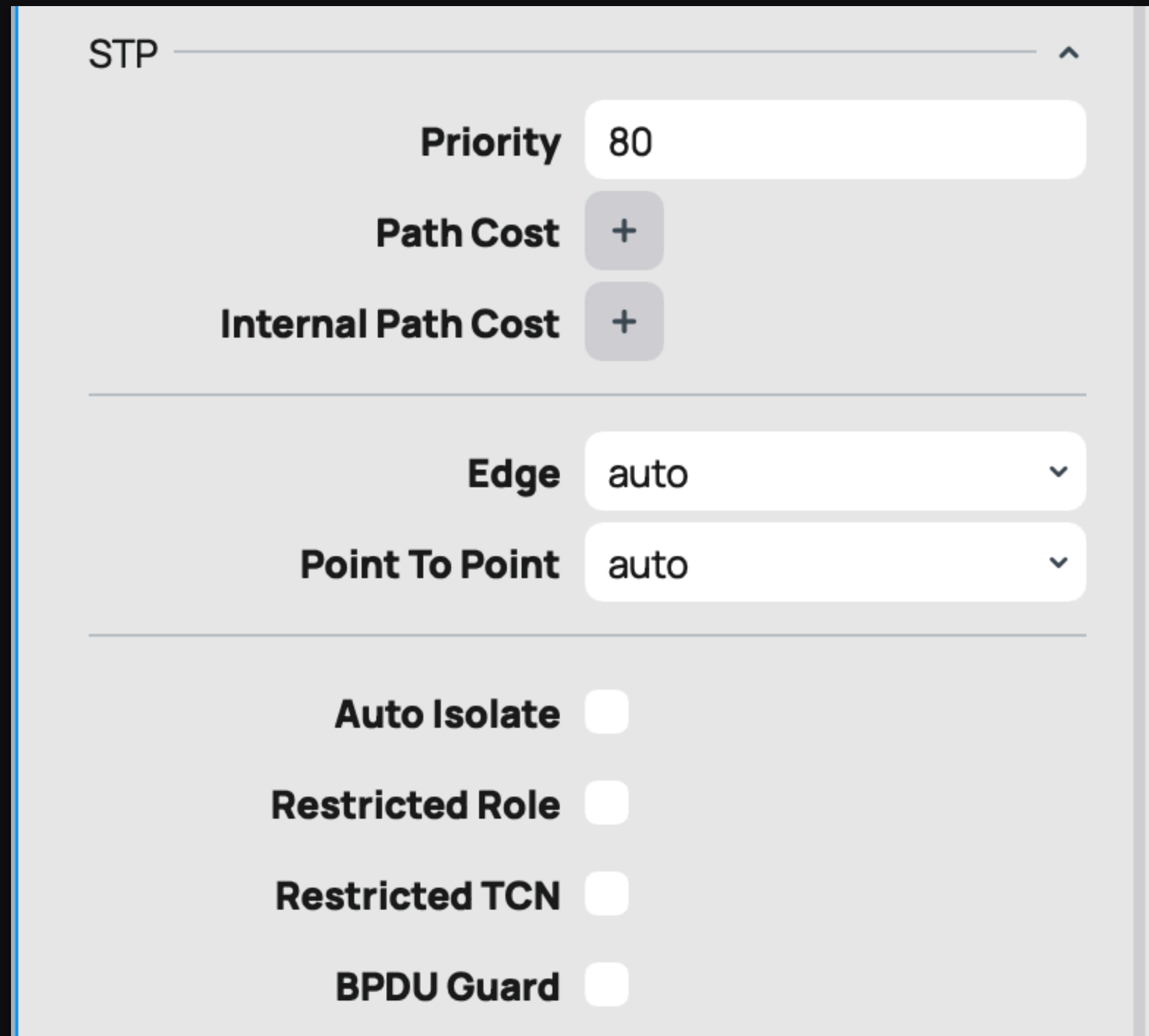
Transmit Hold Count 6

Max Hops 20

Domyślnie, na wszystkich interfejsach typu **bridge**, jest włączona obsługa protokołu RSTP

```
/interface/bridge/add name=bridge-local
```


Ustawienia portów



The screenshot shows a configuration panel for STP (Spanning Tree Protocol) on a network device. The panel is titled 'STP' with an expand/collapse arrow. It contains several settings:

- Priority:** A text input field containing the value '80'.
- Path Cost:** A button with a '+' sign.
- Internal Path Cost:** A button with a '+' sign.
- Edge:** A dropdown menu currently set to 'auto'.
- Point To Point:** A dropdown menu currently set to 'auto'.
- Auto Isolate:** An unchecked checkbox.
- Restricted Role:** An unchecked checkbox.
- Restricted TCN:** An unchecked checkbox.
- BPDU Guard:** An unchecked checkbox.

Wartość parametru Path cost nie jest podawana jawnie, a brana od parametru **Port cost mode** przy dodawaniu bridge-a (long lub short).

W “starszych” wersjach wartość była ustawiona na 10, bez uwzględnienia prędkości portu.

Ustawienia portów

What's new in 7.13 (2023-Dec-14 09:24):
*) bridge - added automatic "path-cost" values depending on interface rate;

Data rate	Long	Short
100 Mbps	200 000	19
1 Gbps	20 000	4
10 Gbps	2 000	2
25 Gbps	800	1
VLAN, EoIP, VXLAN, WIFI	20 000	10

Polecenie dla zmiany wszystkich kosztów na podstawie prędkości interfejsów:

```
/interface bridge port
:foreach i in=[find where bridge="bridge-local"] do={unset $i path-cost}
```

Ustawienia portów

STP

Priority

80

Path Cost

+

Internal Path Cost

+

Edge

auto

Point To Point

auto

Auto Isolate

☐

Restricted Role

☐

Restricted TCN

☐

BPDU Guard

☐

BPDU Guard wyłączy port, jeżeli na nim otrzyma ramkę BPDU.
Wymagane ręczne włączenie portu.

Bridge											
Bridge Ports											
New											
#	^	Interface	Bridge	Horiz...	Trust...	Priority	PVID	Actual P...	Role	Internal ...	Root Pa.
BPDU guard changed port role to disabled due to received BPDU frame, manual bridge port re-enable is required											
☐	0	I ether1	bridge1		no	80	1			0	20000

Ustawienia portów

STP ^

Priority

80

Path Cost

+

Internal Path Cost

+

Edge

auto

Point To Point

auto

Auto Isolate

☐

Restricted Role

☐

Restricted TCN

☐

BPDU Guard

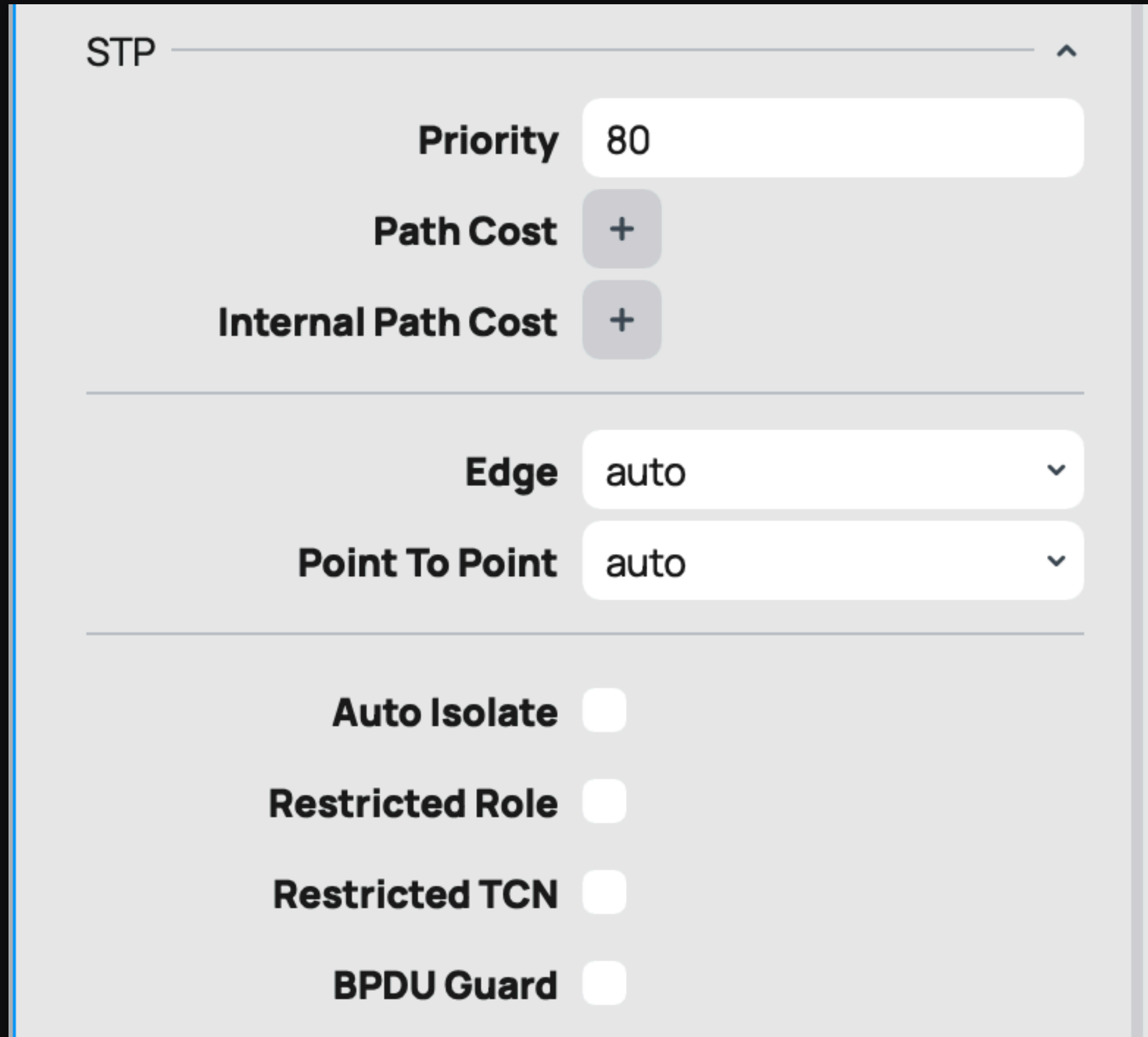
☐

Restricted Role zapobiega stanie się Root Bridge-m.

Inaczej możemy to nazwać **Root Guard**.

Przy ustawieniu **restricted-role=yes**, port nie będzie przyjmować rolę Root Port, mimo tego, że jest lepszy (z punktu widzenia RSTP) wektor priorytetu dla spanning tree.

Ustawienia portów



The screenshot shows a configuration window for STP (Spanning Tree Protocol) on a specific port. The window has a title bar 'STP' with a collapse icon. It contains several settings organized into sections separated by horizontal lines. The first section includes 'Priority' (a text input field with the value '80'), 'Path Cost' (a button with a '+' sign), and 'Internal Path Cost' (a button with a '+' sign). The second section includes 'Edge' (a dropdown menu with 'auto' selected) and 'Point To Point' (a dropdown menu with 'auto' selected). The third section includes four checkboxes: 'Auto Isolate', 'Restricted Role', 'Restricted TCN', and 'BPDU Guard', all of which are currently unchecked.

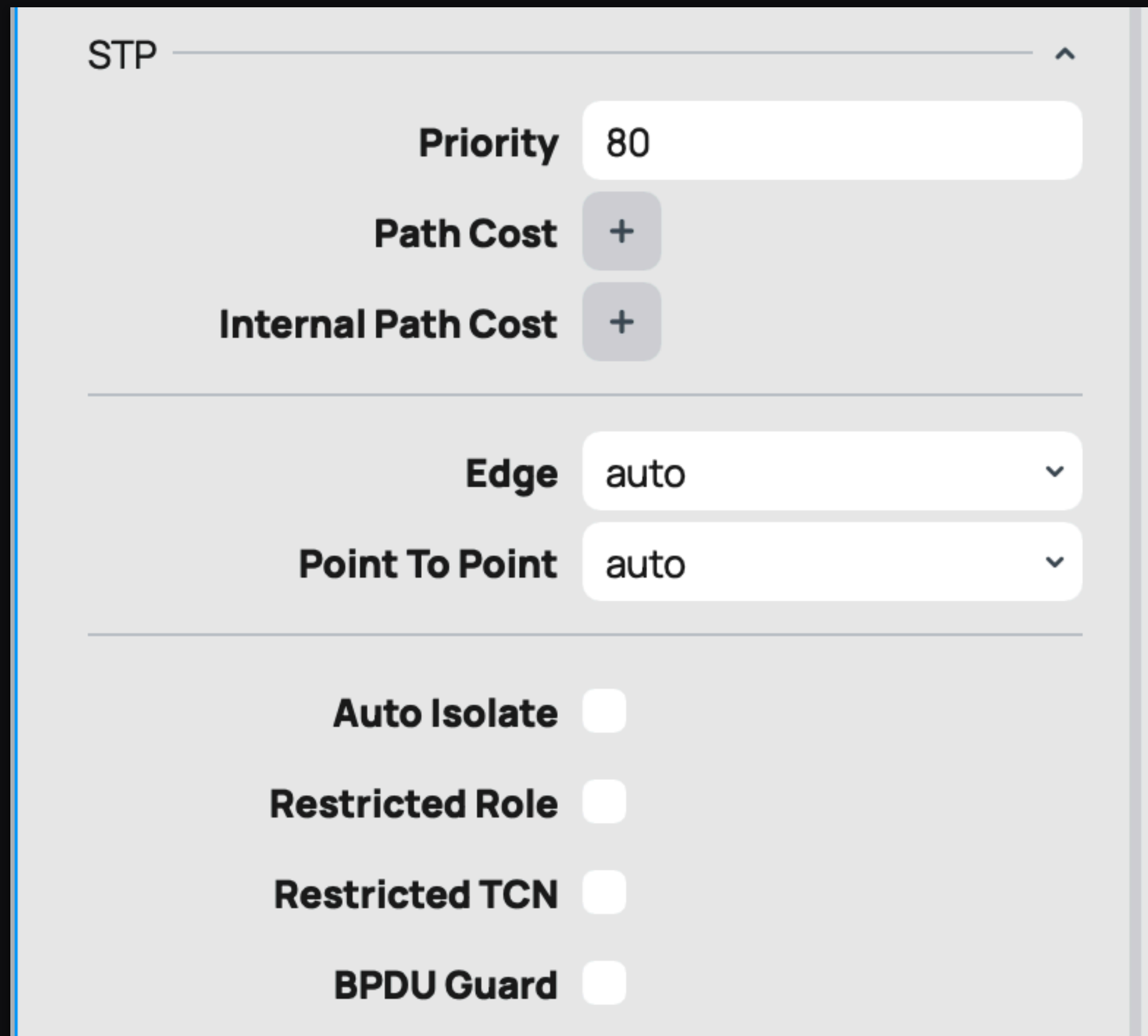
Setting	Value
Priority	80
Path Cost	+
Internal Path Cost	+
Edge	auto
Point To Point	auto
Auto Isolate	☐
Restricted Role	☐
Restricted TCN	☐
BPDU Guard	☐

Auto Isolate chroni port przed zmianą stanu z **Discarding** na **Forwarding**.

Ten mechanizm służy do tego, aby porty nie przechodziły do stanu **Forwarding**, dopóki nie ma pewności, że sąsiadujący przełącznik jest w pełni aktywny i wymienia ramki BPDU. Jest to dodatkowa ochrona przed nieprawidłowymi stanami topologii.

Działa tylko na portach, na których **edge=no**.

Ustawienia portów



The screenshot shows a configuration panel for STP (Spanning Tree Protocol) on a network device. The panel is titled 'STP' with a collapse/expand arrow. It contains several settings:

- Priority:** A text input field containing the value '80'.
- Path Cost:** A button with a '+' sign.
- Internal Path Cost:** A button with a '+' sign.
- Edge:** A dropdown menu currently set to 'auto'.
- Point To Point:** A dropdown menu currently set to 'auto'.
- Auto Isolate:** An unchecked checkbox.
- Restricted Role:** An unchecked checkbox.
- Restricted TCN:** An unchecked checkbox.
- BPDU Guard:** An unchecked checkbox.

Edge, inaczej port brzegowy.

Wymaga od administratora ustawienia na **yes**, dla portów klienckich.

Taki port od razu przechodzi do stanu **Forwarding**, omijając inne stany (**Discarding**, **Learning**).

Domyślnie ustawiony na **auto**, co jest to samo jak **no-discover**, czyli oczekujemy BPDU ramkę na porcie, jeżeli nie otrzymamy, to zmieni się na **edge**.

Sprawdzanie STP/RSTP/MSTP

```
interface/bridge/monitor bridge-local
    state: enabled
    current-mac-address: 2C:C8:1B:FF:69:B6
    root-bridge: yes
    root-bridge-id: 0x8000.2C:C8:1B:FF:69:B6
    root-path-cost: 0
    root-port: none
    port-count: 4
designated-port-count: 2
    fast-forward: no
```


Sprawdzanie STP/RSTP/MSTP

```
interface/bridge/port/monitor 0,1
    interface: ether1          ether2
    status: in-bridge         in-bridge
    port-number: 1            2
    role: root-port          designated-port
    edge-port: no             no
    edge-port-discovery: yes  yes
    point-to-point-port: yes  yes
    external-fdb: no          no
    sending-rstp: yes         yes
    learning: yes             yes
    forwarding: yes           yes
    actual-path-cost: 20000    20000
    root-path-cost: 20000
    designated-bridge: 0x8000.50:00:00:01:00:00
    designated-cost: 0
    designated-port-number: 2
```

Logowanie STP/RSTP/MSTP

What's new in 7.11 (2023-Aug-15 09:33):
*) bridge - added more STP-related logging;

Logging

Rules

Actions

New

0 (5)

	Topics	Prefix	Action
☐	* critical		echo
☐	* error		memory
☐	* info		memory
☐	stp	STP	memory
☐	* warning		memory

				contains	stp
		Buffer	Topics	Message	
	-10-15 08:48:01	memory	bridge, stp	ether2:0 discarding	
	-10-15 08:48:01	memory	bridge, stp	ether2:0 becomes Designated	
☐	50	2024-10-15 08:48:01	memory	bridge, stp	ether1:0 becomes Root
☐	48	2024-10-15 08:47:59	memory	bridge, stp	ether1:0 becomes Designated
☐	47	2024-10-15 08:47:03	memory	bridge, stp, warning	bpdu-guard disabling ether1 due to received bpdu
☐	46	2024-10-15 08:47:03	memory	bridge, stp	ether2:0 becomes Root
☐	44	2024-10-15 08:47:03	memory	bridge, stp	ether1:0 becomes Designated
☐	41	2024-10-15 08:29:22	memory	bridge, stp	ether2:0 TCHANGE over
☐	40	2024-10-15 08:29:19	memory	bridge, stp	ether2:0 TCHANGE start
☐	39	2024-10-15 08:29:19	memory	bridge, stp	ether2:0 TCHANGE over

SNMP dla STP/RSTP/MSTP

Można monitorować stan oraz rolę portów w bridge za pomocą protokołu SNMP.

Baza danych MIB dla bridge

https://mibbrowser.online/mibdb_search.php?mib=BRIDGE-MIB

Optymalizacja sieci

Redukcja opóźnień / Konwergencja

RSTP znacząco skraca czas konwergencji po awarii lub zmianie w topologii sieci z 30-50 sekund (w STP) do **1-6 sekund**.

W STP tylko Root Bridge wysyła BPDU i jest przekazywany przez innych, podczas gdy **w RSTP wszystkie bridge generują BPDU co 2 sekundy**, co jest podobne do mechanizmu “keepalive”.

Poprawa redundancji

Mechanizm **Proposal/Agreement** w RSTP znacząco poprawia redundancję w sieci, ponieważ umożliwia szybkie przełączanie ruchu na alternatywne ścieżki w przypadku awarii.

Kiedy przełącznik wykryje zmianę w topologii, natychmiast wysyła wiadomość **Proposal** do sąsiadujących urządzeń, które dynamicznie akceptują nową ścieżkę, wysyłając wiadomość **Agreement**.

Dzięki temu porty mogą niemal natychmiast przejść do stanu **Forwarding**, zapewniając ciągłość działania bez długich przestojów.

Zarządzanie przepustowością

RSTP dynamicznie wybiera najlepsze ścieżki przesyłu danych, preferując porty o niższym koszcie ścieżki (path cost).

Lepsze ścieżki mają niższe koszty, co zapewnia szybszy przesył danych w sieci i bardziej efektywne wykorzystanie łączy.

Szybka rekonfiguracja zapewnia ciągły przesył danych bez widocznych opóźnień dla użytkowników końcowych

Dobre praktyki

Wybór odpowiedniego przełącznika root bridge

Należy wybrać przełącznik o centralnej lokalizacji w sieci jako root bridge – taki, który ma najlepszy dostęp (jest “najmocniejszym”) do wszystkich innych urządzeń.

Ustawić priorytet tego przełącznika na najwyższy, domyślnie jest to **0x8000** (32768 w postaci dziesiętnej), więc np. warto ustawić **0x1000** (4096) dla root bridge-a. I **jest polecana zmiana z krokiem w 0x1000**.

Zapewnić redundancję na poziomie **root bridge**, konfigurując drugi przełącznik jako zapasowy (przy czym ustawić dla niego niższy priorytet niż dla głównego).

Ustawienie portów brzegowych (Edge Ports)

Porty brzegowe (znane również jako porty dostępu) są używane do połączenia przełączników bezpośrednio z urządzeniami końcowymi (komputerami, drukarkami i in.). Porty te nie powinny uczestniczyć w procesie negocjacji topologii, ponieważ nie mogą tworzyć pętli.

Należy skonfigurować porty brzegowe, aby natychmiast przechodziły do stanu Forwarding. W RouterOS za to odpowiada parameter **edge=yes**.

Ustawić **BPDU Guard** na portach brzegowych, aby chronić sieć przed przypadkowym podłączeniem urządzeń, które mogą wysłać BPDU. Jeśli przełącznik wykryje BPDU na porcie brzegowym, port zostanie natychmiast wyłączony, co zapobiega potencjalnym pętlom.

Konfiguracja priorytetów i kosztów portów

RSTP wybiera najlepsze ścieżki na podstawie priorytetów portów oraz kosztów ścieżki (path cost). Koszt portu zależy od szybkości połączenia, ale można ręcznie dostosować koszty dla różnych łączy, aby zoptymalizować przepływ ruchu.

Należy dostosować priorytety portów i koszty ścieżek w zależności od ich przeznaczenia. Na przykład, ustawić niższe koszty dla szybszych połączeń (np. porty 10Gbps), aby były preferowane jako główne ścieżki.

BPDU Filter i BPDU Guard

Zalecane włączanie **BPDU Guard** na wszystkich portach brzegowych, aby zapobiec przypadkowemu podłączeniu innych przełączników, co mogłoby wywołać pętle w sieci.

W RouterOS jest możliwość filtrowania otrzymanych ramek BPDU na poszczególnych portach przełącznika, za pomocą ACL. (Ta funkcjonalność nie jest możliwa na bridge filter lub reguły NAT, tak jak w inny sposób przetwarza się ramki BPDU).

Przykład dla CRS3xx lub 5xx:

```
/interface ethernet switch rule
add dst-mac-address=01:80:C2:00:00:00/FF:FF:FF:FF:FF:FF new-dst-ports="" \
    ports=ether1 switch=switch1
```

Dziękuję