

Securing network against rouge root bridge switches

To avoid problems with rouge switches which want to become root switches in our network or at least join to our stp topology we can implement “**spanguard**” feature.

Spanguard is disabled by default.

It secures our topology by locking port in case of receiving unexpected BPDU frames on port which is not a trunk port.

We enable spanguard globally on switch.

```
set spantree spanguard enable
```

```
show spantree spanguard
```

```
Spanguard is enabled
```

Next we set all non-trunk port(device ports) to adminedge ports,e.g. for ports from 1 to 48

```
set spantree adminedge fe.1.1-48 true
```

Since then each BPDU frames received by adminedge port will lock this port. Port can be unlock either manually by typing,e.g.for port fe.1.1

```
clear spantree spanguardlock fe.1.1
```

or automatically when time specified in “spanguardtimeout” has ended. Time is counted from last received BPDU frame,default is 300 seconds but we can change this value typing

```
set spantree spanguardtimeout 500
```

to see current spanguardtimeout value type

```
show spantree spanguardtimeout
```

```
Spanguard timeout: 500
```

To check spanguard status on ports we can use commands:

```
show spantree spanguardlock – for all ports
```

or

```
show spantree spanguardlock fe.1.1 – for one port
```

```
Port fe.1.1 is Unlocked
```