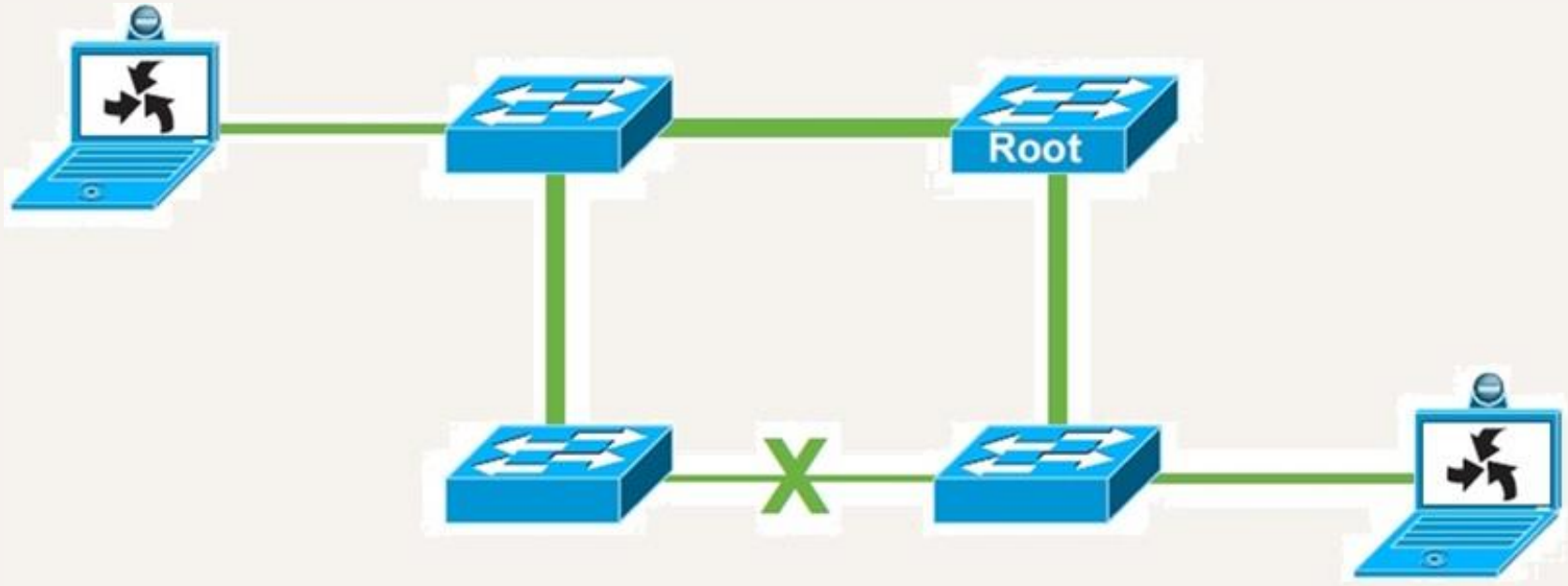
STP Security

CyberQuince

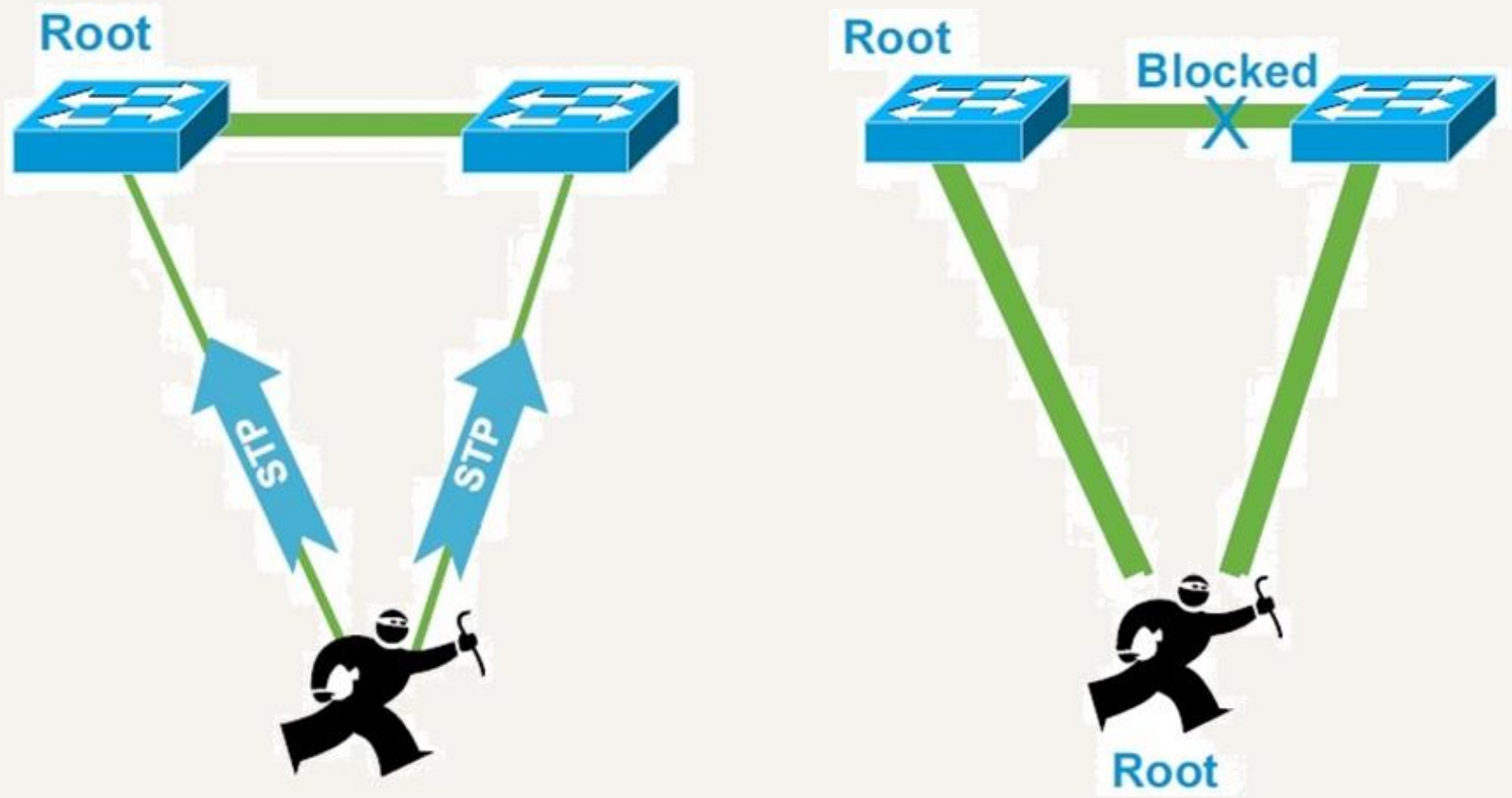
Spanning-Tree Protocol

STP (Spanning-Tree Protocol) maintains loop-free topologies in a redundant L2 network.

BPDU (Bridge Protocol Data Unit) messages are frames that switches distribute in between themselves. Switches choose the Root Bridge, Designated, and Root ports based on information from BPDUs.



STP Attack



STP Attack

The attacker sends BPDU messages to inform the switches that he is now Root (by giving himself the lowest priority).

If the two switches to which attacker connects are linked, STP will block the link between them, and they will only be able to communicate through the attacker – which is a school example of the *Man-in-the-Middle* attack.

STP Attack — Countermeasures

BPDU guard is an addition to STP, introduced to protect ports to which end users connect.

BPDU messages are exchanged ***only between switches***, which means they are not expected to be received on access ports.

If a *BPDU guard*-enabled port receives a BPDU packet, that port will automatically be disabled – it will go into the "`errdisable`" state.

STP Attack — Countermeasures

BPDU guard can be configured *globally* on a switch – it will be enabled on all *PortFast* ports:

```
Switch(config)# spanning-tree portfast bpduguard default
```

BPDU guard configuration per-port:

```
Switch(config-if)# spanning-tree bpduguard enable
Switch(config-if)# spanning-tree bpduguard disable
```

WARNING: A BPDU guard-enabled port will not take part in STP!

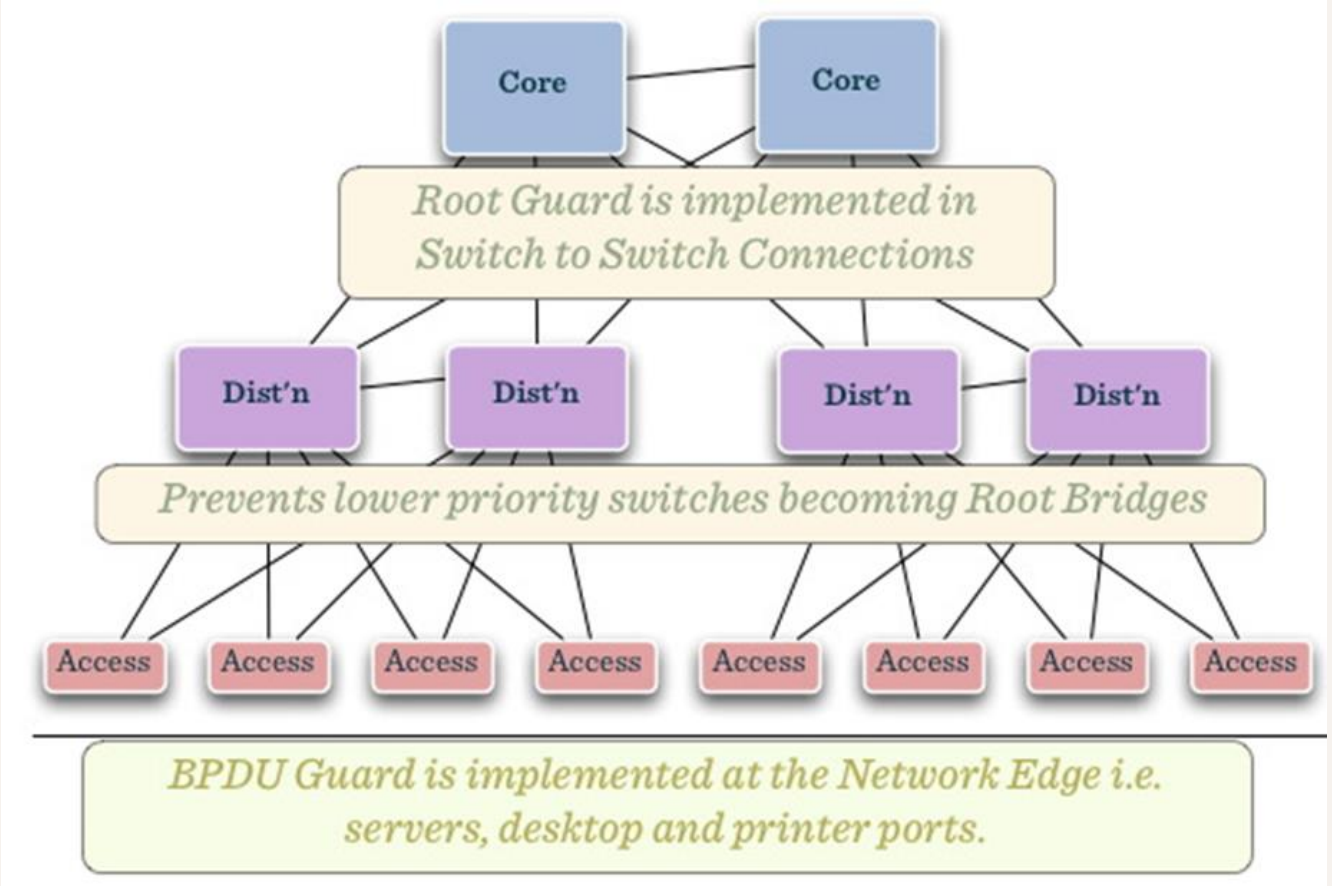
STP Attack — Countermeasures

Root guard is another STP addition, similar to BPDU guard – but intended to protect ports on root switches, not access switches.

Root guard-enabled ports can still receive and send BPDU messages, but will block those neighbors that try to become a Root bridge.

```
S(config-if)#spanning-tree guard root
```

STP Attack — Countermeasures



STP Security

CyberQuince