STP Attacks

Applied Network security (comp420 –001)

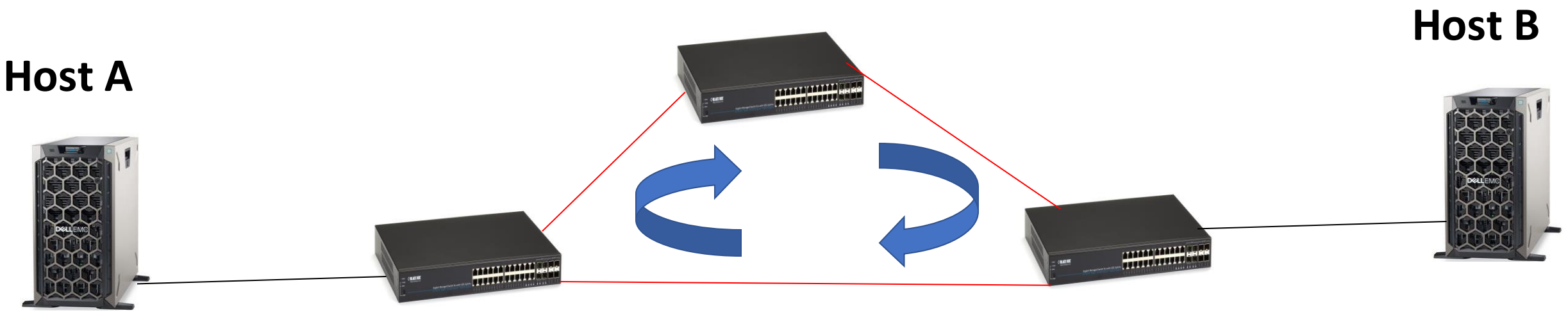
Department of Computer science

Fall 2020

Layer 2 Switching Loops

- A **redundant link** is an additional link that we create as the backup link of the primary link.
- If the primary link fails, the redundant link prevents the network from getting down due to the primary link failure.
- **Switching loop:** The redundant or backup link is helpful only when the primary link fails. While the primary link is functioning, the backup link should be disabled. If both the primary and backup links are active at the same time, they will create a switching loop.

Switched LAN With a Loop



Broadcast Storm

- If a switch sends a broadcast to the other two switches, they will receive and rebroadcast it by forwarding it through all ports because they couldn't find the address in their table. In fact, they will go for a repeating loop called a **broadcast storm.**
  - **Unstable MAC address table**
  - **Duplicate Frames**
- This is simply because **TTL** (Time To Live) field of a packet, which is found in Layer 3 header, does not exist in L2 fields.
- Broadcast storm can be a serious threat to your network **availability**.

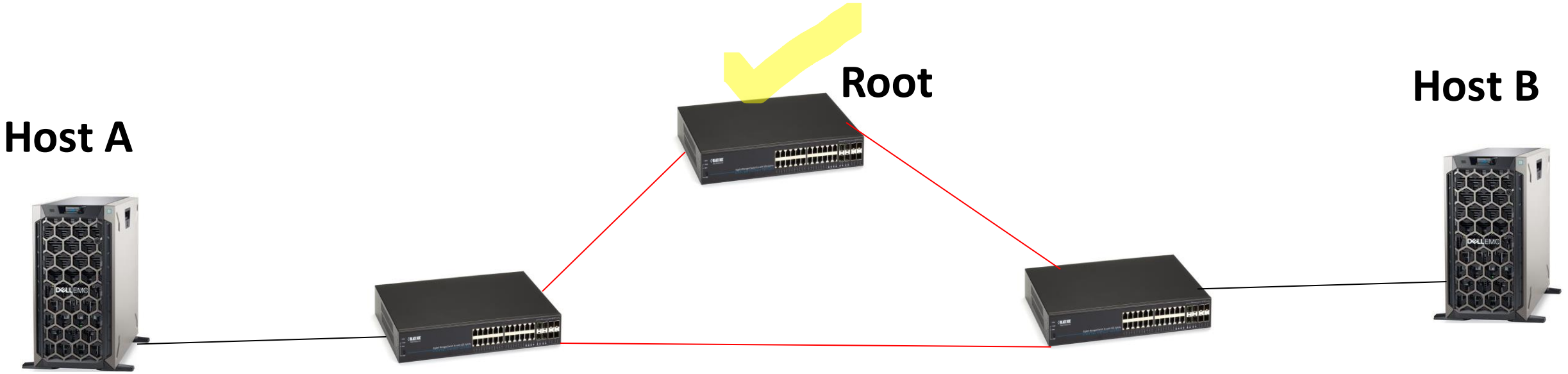
Remedy

- Block some ports and break the loop, but which ports???

- The **Spanning Tree Protocol** (**STP**) was developed by Radia Perlman in 1985 to solve the problem of Ethernet (switch) loops.
- STP appeared to solve this networking issue by blocking the redundant paths, thanks to the **Spanning Tree Algorithm** (**STA**) based on the IEEE 802.1d standard.
- Spanning Tree Protocol (STP) can allow you to have redundant links while having a loop-free topology, thus preventing the potential for a broadcast storm.

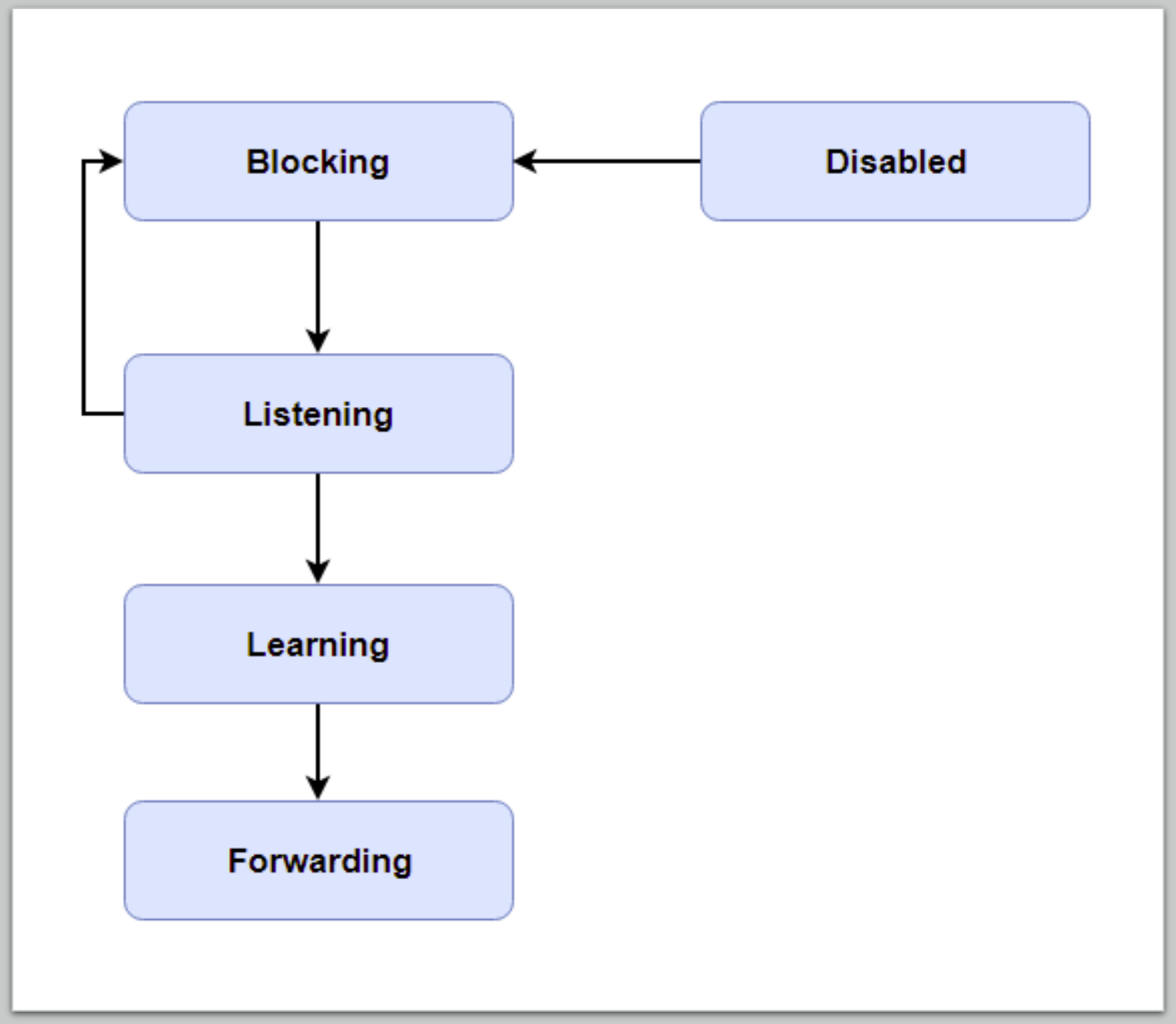
STP

- Step 1: The switches making arrangements for election of the root bridge through the exchange of **Bridge Protocol Data Units (BPDU)**.
  - **Root bridge election**: Switches are not very smart devices. By default, each switch in the network claims to be the root bridge, which is the main switch that controls the topology. To select a root bridge, all switches send their **bridge ID** (**BID**), which is 8 bytes combined between a bridge priority and a MAC address; by default, it is 32,768. The switch with the minimum BID gets selected as a root bridge.



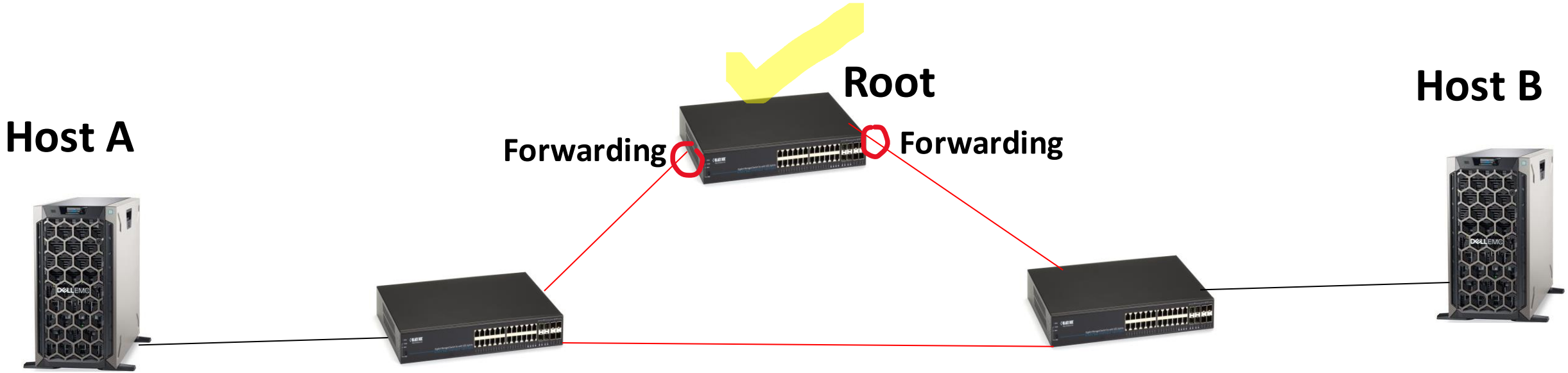
STP (Cont.)

- The following workflow describes the stages of ports in STP.
- **Disabled port**: This port idoes not work at all.
- **Blocked (Discarding) port**: This port doesn't forward data. It receives data but pretends nothing's received.
- **Listening port**: This port doesn't learn MAC addresses or forward them. Only a root or designated port will move to the listening state.
- **learning port**: This port learns the MAC addresses but does not forward the frames.
- **Forwarding port**: This port learns MAC addresses and forwards data



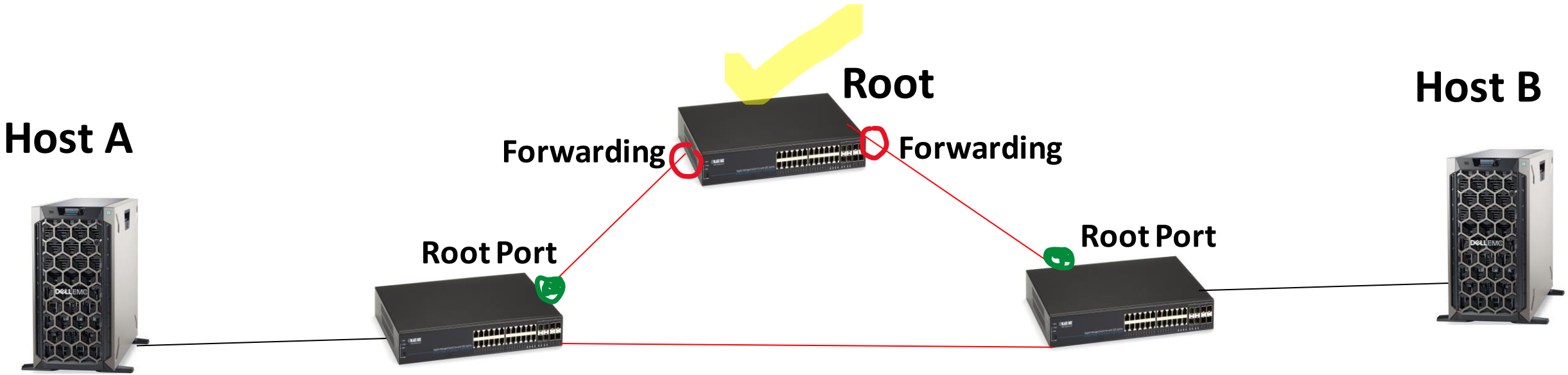
STP (Cont.)

- Step 2: Root interfaces goes into forwarding state.



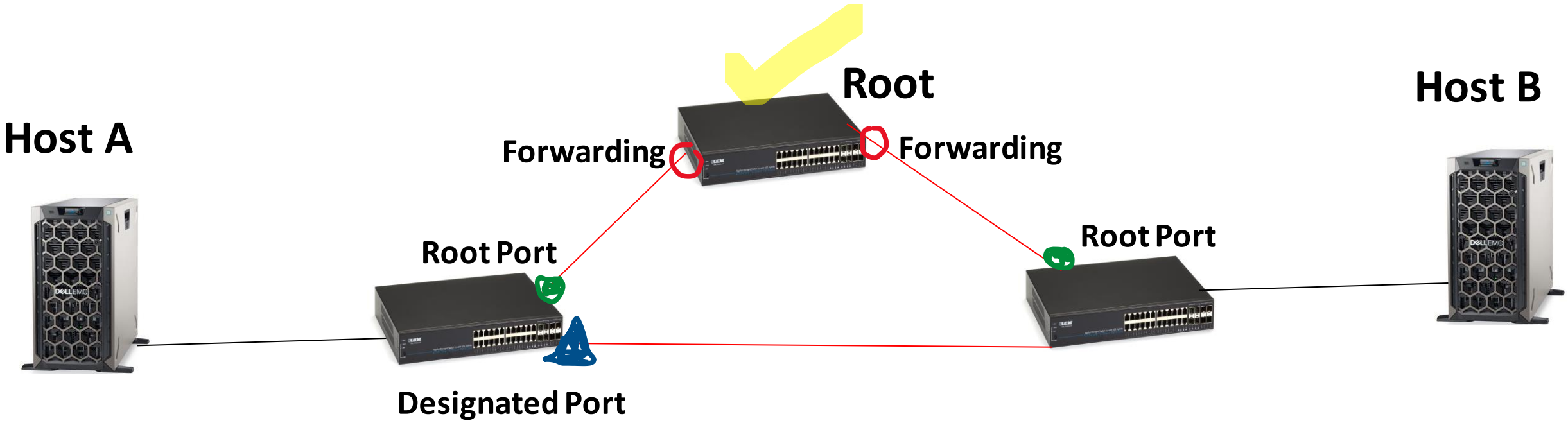
STP (Cont.)

- Step 3: Each non-root switch selects its root port, the port “closest” to the root bridge switch, in terms of “cost.”



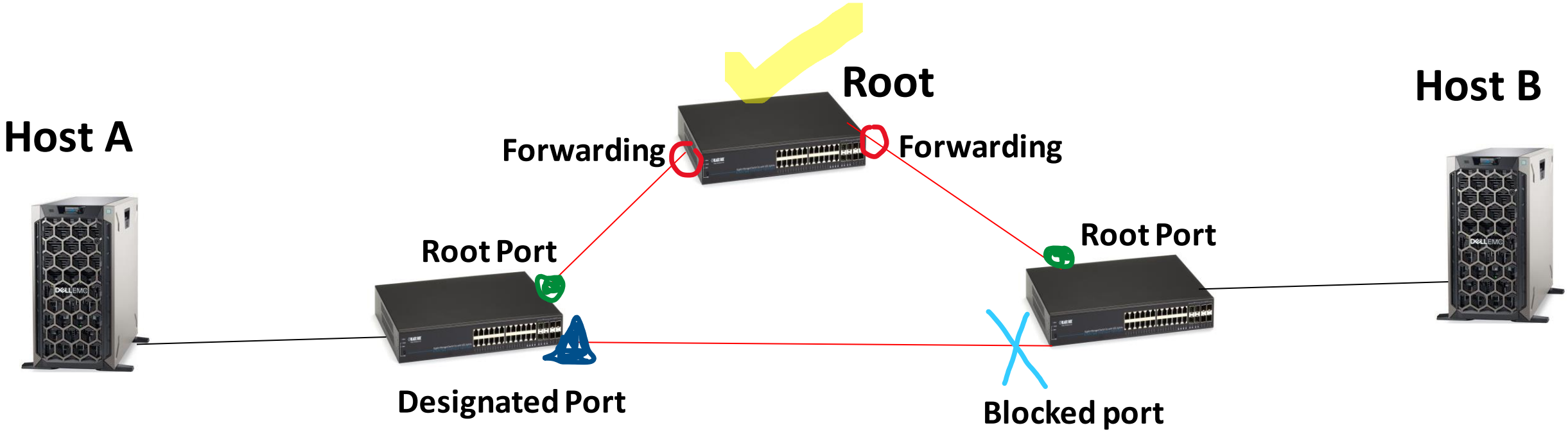
STP (Cont.)

- Step 4: Each Remaining Link choose a designated port.
  - A **designated port** is a non-root **port** that is permitted to forward traffic.



STP (Cont.)

- Step 5: All other ports are put into a blocking state.
  - When a port is not a designated or root port it will be in **blocking mode**.



Topology Change Notification (TCN) Attack

- TCN is a BPDU that is used to notify the root switch when there is a topology change.
- Any switch the receives the TCN will forward it to the root switch.
- The Root switch then asks all switches in the network to shorten their MAC address table againg time (usually from 300 sec to 15 sec for the first time). This helps evict the old entries related to the old network topology.
- Attackers can send fake TCN messages continously when there is no topology changes. This makes the switches to reduce againg even more. It then increase the chance of receiving a request and no MAC table entry matches.
- The switch then broadcast the received message and this will increse the traffic load on the network.
- The attacker can continue the attack and after a while the network perfoms very slow.

Root Role Attack

- If an attacker has access to switch ports that are able to become trunk ports, she can introduce a rogue switch into the network.
- If she configures her rogue switch to have priority less than any other switch in the netwok, most of the traffic will theoretically pass through that switch.
- Rogue switch with e.g priority 0 announces its BPDUs and the STP topology reconverts. The rouge switch will become root bridge and all the traffic will cross this switch. This gives the attacker the possibility to sniff all traffic in the network.