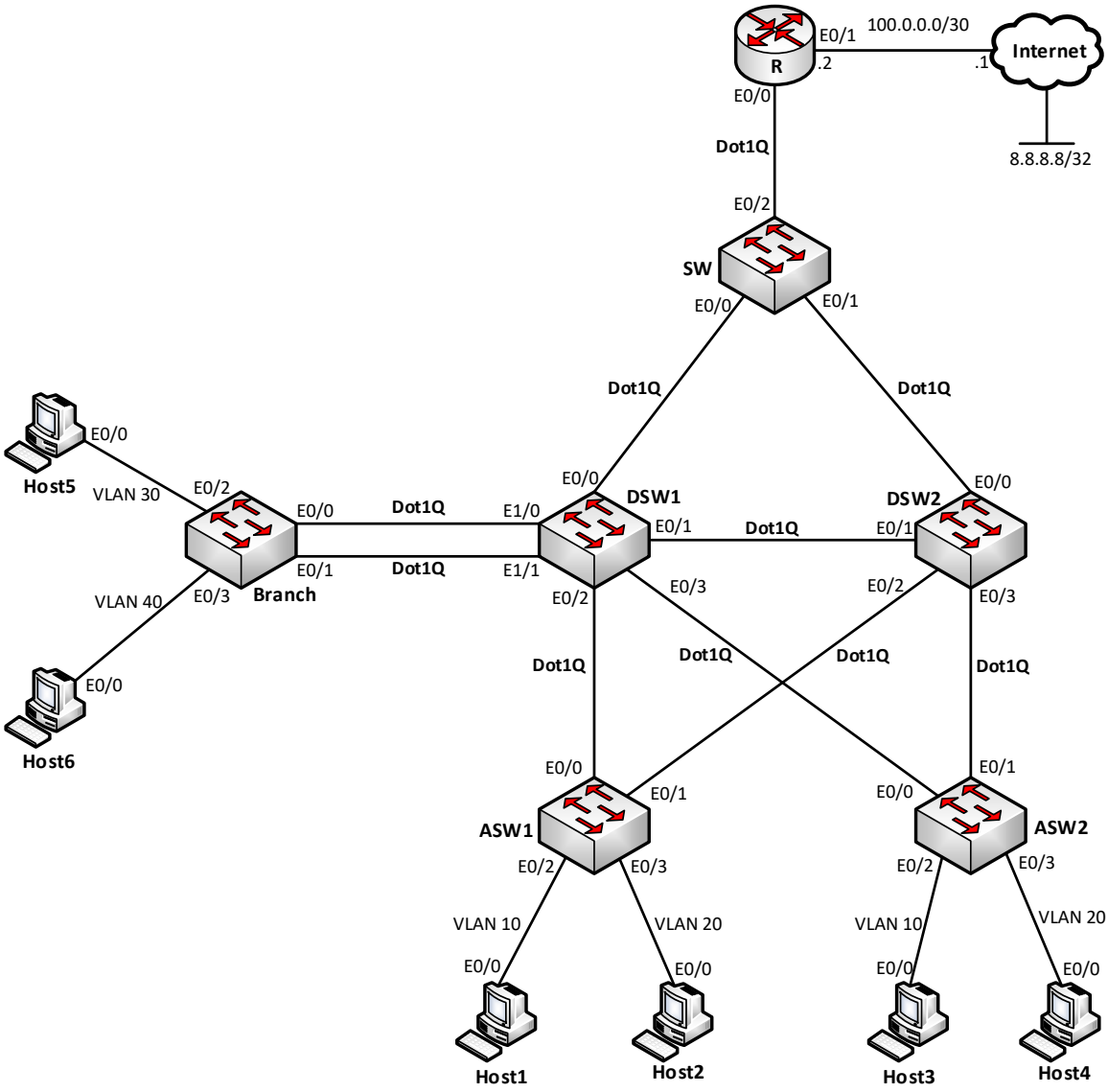
Lab 3 – STP – Bài số 2

Sơ đồ:



Hình 1 – Sơ đồ bài lab.

Mô tả:

- Sơ đồ bài lab gồm các thiết bị được kết nối với nhau như trên hình 1. Trên sơ đồ này, các bạn học viên sẽ thực hành các thao tác hiệu chỉnh STP trên một topo sử dụng mô hình 3 lớp.
- Các thiết bị đều đã được cấu hình thiết lập hostname thích hợp, các bạn không cần phải cấu hình lại thông số này.
- Các bạn học viên không can thiệp vào thiết bị giả lập Internet trong suốt quá trình thực hiện bài lab.

Yêu cầu:

1. Cấu hình Trunking, VLAN:

- Cấu hình tất cả các đường link kết nối các switch thành trunking Dot1Q.
- Cấu hình VLAN trên các switch theo yêu cầu sau:
  - DSW1, SW : VLAN 10, 20, 30, 40.
  - DSW2, ASW1, ASW2: VLAN 10, 20.
  - Branch: VLAN 30, 40.

2. Cấu hình STP – Branch và DSW1:

Thực hiện hiệu chỉnh STP trên DSW1 và Branch đảm bảo:

- Lưu lượng VLAN 30 đi từ Branch về DSW1 sẽ chọn link trên (nối giữa E0/0 của Branch và E1/0 của DSW1) làm đường chính và link dưới (nối giữa E0/1 của Branch và E1/1 của DSW1) làm đường dự phòng.
- Lưu lượng VLAN 40 đi từ Branch về DSW1 sẽ chọn link dưới làm đường chính và link trên làm đường dự phòng.

3. Dự phòng uplink cho các VLAN 10 và 20:

Bước này thực hiện cấu hình đường đi layer 2 uplink từ các switch access lên distribution của các VLAN người dùng 10 và 20. Yêu cầu đặt ra như sau:

- VLAN 10 chọn đường uplink lên DSW1 là đường chính, đường uplink lên VLAN 20 chỉ để dự phòng.
- Ngược lại, VLAN 20 lại chọn đường uplink lên DSW2 là đường chính, đường uplink lên VLAN 10 chỉ để dự phòng.

4. Yêu cầu thêm:

Thực hiện thêm một số yêu cầu thêm cho bài lab:

- Cấu hình router R định tuyến VLAN cho các VLAN 10, 20, 30, 40 theo quy hoạch IP như sau:
  - E0/0.10: 172.16.10.1/24, nối đến VLAN 10.
  - E0/0.20: 172.16.20.1/24, nối đến VLAN 20.
  - E0/0.30: 172.16.30.1/24, nối đến VLAN 30.
  - E0/0.40: 172.16.40.1/24, nối đến VLAN 40.
- Cấu hình router R đóng vai trò DHCP server cấp phát IP cho các user thuộc các VLAN và đảm bảo các user này truy nhập được Internet (các host kiểm tra bằng cách ping đến 8.8.8.8).

5. STP toolkit:

Hãy thực hiện cấu hình tính năng Portfast, Uplinkfast và BPDUguard tại các vị trí thích hợp trên sơ đồ.

Thực hiện:

1. Cấu hình Trunking, VLAN:

Cấu hình:

Cấu hình Trunking Dot1Q giữa các switch:

```
DSW1(config)#interface range e0/0 - 3,e1/0 - 1
DSW1(config-if-range)#switchport trunk encapsulation dot1q
DSW1(config-if-range)#switchport mode trunk

DSW2(config)#interface range e0/0 - 3
DSW2(config-if-range)#switchport trunk encapsulation dot1q
DSW2(config-if-range)#switchport mode trunk

SW(config)#interface range e0/0 - 1
SW(config-if-range)#switchport trunk encapsulation dot1q
SW(config-if-range)#switchport mode trunk

ASW1(config)#interface range e0/0 - 1
ASW1(config-if-range)#switchport trunk encapsulation dot1q
ASW1(config-if-range)#switchport mode trunk

ASW2(config)#interface range e0/0 - 1
ASW2(config-if-range)#switchport trunk encapsulation dot1q
ASW2(config-if-range)#switchport mode trunk

Branch(config)#interface range e0/0 - 1
Branch(config-if-range)#switchport trunk encapsulation dot1q
Branch(config-if-range)#switchport mode trunk
```

Cấu hình VLAN phù hợp trên các switch:

```
DSW1(config)#vlan 10,20,30,40
DSW1(config-vlan)#

SW(config)#vlan 10,20,30,40
SW(config-vlan)#

DSW2(config)#vlan 10,20
DSW2(config-vlan)#

ASW1(config)#vlan 10,20
ASW1(config-vlan)#

ASW2(config)#vlan 10,20
ASW2(config-vlan)#

Branch(config)#vlan 30,40
Branch(config-vlan)#
```

Về yêu cầu cấu hình VLAN, các bạn học viên có thể sử dụng phương pháp cấu hình trên từng switch như trên hoặc sử dụng VTP để đồng bộ.

Kiểm tra:

Kiểm tra rằng các đường trunk đã được thiết lập, ví dụ, trên DSW1:

```
DSW1#show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et0/0       on               802.1q         trunking      1
Et0/1       on               802.1q         trunking      1
Et0/2       on               802.1q         trunking      1
Et0/3       on               802.1q         trunking      1
Et1/0       on               802.1q         trunking      1
Et1/1       on               802.1q         trunking      1

Port        Vlans allowed on trunk
Et0/0       1-4094
Et0/1       1-4094
Et0/2       1-4094
Et0/3       1-4094
Et1/0       1-4094
Et1/1       1-4094

Port        Vlans allowed and active in management domain
Et0/0       1,10,20,30,40
Et0/1       1,10,20,30,40
Et0/2       1,10,20,30,40
Et0/3       1,10,20,30,40
Et1/0       1,10,20,30,40
Et1/1       1,10,20,30,40

Port        Vlans in spanning tree forwarding state and not pruned
Et0/0       1,10,20,30,40
Et0/1       1,10,20,30,40
Et0/2       1,10,20,30,40
Et0/3       1,10,20,30,40
Et1/0       1,10,20,30,40
Et1/1       1,10,20,30,40
```

Kiểm tra cấu hình VLAN trên các switch, ví dụ, DSW1:

```
DSW1#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Et1/2, Et1/3
10   VLAN0010                         active
20   VLAN0020                         active
30   VLAN0030                         active
40   VLAN0040                         active
(…)
```

2. Cấu hình STP – Branch và DSW1:

Cấu hình:

Cấu hình để DSW1 làm root switch trên hai VLAN 30 và 40:

```
DSW1(config)#spanning-tree vlan 30,40 root primary
```

Với cấu hình này, VLAN 30 đã đạt yêu cầu đặt ra vì cổng E1/0 của DSW1 có Port – ID tốt hơn Port – ID của cổng E1/1:

```
DSW1#show spanning-tree vlan 30

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     aabb.cc00.1000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24606  (priority 24576 sys-id-ext 30)
              Address     aabb.cc00.1000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100       128.6    Shr

Branch#show spanning-tree vlan 30

VLAN0030
  Spanning tree enabled protocol ieee
  Root ID     Priority    24606
              Address     aabb.cc00.1000
              Cost        100
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32798  (priority 32768 sys-id-ext 30)
              Address     aabb.cc00.5000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec
```

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Root FWD 100       128.1    Shr <- Link chính
Et0/1               Altn BLK 100       128.2    Shr <- Link dự phòng, bị khóa
```

Với VLAN 40, để Branch khóa cổng E0/0, mở cổng E0/1, trên DSW1, thực hiện chỉnh port – priority cho cổng E1/1 tốt hơn cổng E1/0:

```
DSW1(config)#interface e1/1
DSW1(config-if)#spanning-tree vlan 40 port-priority 0
```

Kiểm tra rằng kết quả trên VLAN 40 đã hội tụ đúng theo yêu cầu:

```
DSW1#show spanning-tree vlan 40

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID     Priority    24616
              Address     aabb.cc00.1000
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24616  (priority 24576 sys-id-ext 40)
              Address     aabb.cc00.1000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Desg FWD 100       128.1    Shr
Et0/1               Desg FWD 100       128.2    Shr
Et0/2               Desg FWD 100       128.3    Shr
Et0/3               Desg FWD 100       128.4    Shr
Et1/0               Desg FWD 100       128.5    Shr
Et1/1               Desg FWD 100         0.6    Shr
Branch#show spanning-tree vlan 40

VLAN0040
  Spanning tree enabled protocol ieee
  Root ID     Priority    24616
              Address     aabb.cc00.1000
              Cost        100
              Port        2 (Ethernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


  Bridge ID   Priority    32808  (priority 32768 sys-id-ext 40)
              Address     aabb.cc00.5000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec
```

```
Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Altn BLK 100       128.1    Shr <- Link dự phòng, bị khóa
Et0/1               Root FWD 100       128.2    Shr <- Link chính
```

3. Dự phòng uplink cho các VLAN 10 và 20:

Cấu hình:

Với sơ đồ lớp 2 kết nối các khu vực Distribution và Access như trên, để đạt được yêu cầu, ta thực hiện hiệu chỉnh STP như sau:

- Trên VLAN 10, DSW1 làm root switch, DSW2 làm secondary root switch.
- Trên VLAN 20, DSW2 làm root switch, DSW1 làm secondary root switch.

Trên VLAN 10:

```
DSW1(config)#spanning-tree vlan 10 root primary
DSW2(config)#spanning-tree vlan 10 root secondary
```

Trên VLAN 20:

```
DSW2(config)#spanning-tree vlan 20 root primary
DSW1(config)#spanning-tree vlan 20 root secondary
```

Kiểm tra:

Thực hiện kiểm tra trên các access switch để xác nhận rằng các đường uplink của các VLAN đã được mở và khóa theo đúng yêu cầu đặt ra.

Trên VLAN 10:

```
ASW1#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     aabb.cc00.1000
              Cost        100
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec


 Bridge ID  Priority    32778  (priority 32768 sys-id-ext 10)
              Address     aabb.cc00.3000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Root FWD 100       128.1    Shr
Et0/1               Altn BLK 100       128.2    Shr
```

```
ASW2#show spanning-tree vlan 10

VLAN0010
  Spanning tree enabled protocol ieee
  Root ID     Priority    24586
              Address     aabb.cc00.1000
              Cost        100
              Port        1 (Ethernet0/0)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     aabb.cc00.4000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Root FWD 100       128.1    Shr
Et0/1               Altn BLK 100       128.2    Shr
```

Kết quả show cho thấy cả hai switch access đều mở cổng uplink E0/0 nối đến DSW1 (vai trò là "Root" và trạng thái là "Forwarding" – "FWD") và khóa cổng uplink E0/1 nối đến DSW2 (vai trò "Alternative" – "Altn" và trạng thái là "Blocking" – "BLK"). Cổng E0/1 sẽ chỉ mở ra nếu cổng link Ethernet trên cổng E0/0 down. Như vậy, hoạt động dự phòng uplink trên VLAN 10 đã diễn ra đúng theo yêu cầu.

Ta có thể thực hiện kiểm tra tương tự trên VLAN 20:

```
ASW1#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     aabb.cc00.2000
              Cost        100
              Port        2 (Ethernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     aabb.cc00.3000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Altn BLK 100       128.1    Shr <- Uplink dự phòng
Et0/1               Root FWD 100       128.2    Shr <- Uplink chính
```

```
ASW2#show spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID     Priority    24596
              Address     aabb.cc00.2000
              Cost        100
              Port        2 (Ethernet0/1)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32788  (priority 32768 sys-id-ext 20)
              Address     aabb.cc00.4000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------------
Et0/0               Altn BLK 100       128.1    Shr <- Uplink dự phòng
Et0/1               Root FWD 100       128.2    Shr <- Uplink chính
```

Với cách hiệu chỉnh STP như trên, ta đã thực hiện chia tải trên các đường link theo VLAN (VLAN load – sharing), phần nào khắc phục được nhược điểm của STP là không hỗ trợ cân bằng tải qua nhiều đường đi.

4. Yêu cầu thêm:

Cấu hình:

Cấu hình định tuyến VLAN:

```
R(config)#interface e0/0
R(config-if)#no shutdown
R(config)#interface e0/0.10
R(config-subif)#encapsulation dot1Q 10
R(config-subif)#ip address 172.16.10.1 255.255.255.0
R(config-subif)#exit
R(config)#interface e0/0.20
R(config-subif)#encapsulation dot1Q 20
R(config-subif)#ip address 172.16.20.1 255.255.255.0
R(config-subif)#exit
R(config)#interface e0/0.30
R(config-subif)#encapsulation dot1Q 30
R(config-subif)#ip address 172.16.30.1 255.255.255.0
R(config-subif)#exit
R(config)#interface e0/0.40
R(config-subif)#encapsulation dot1Q 40
R(config-subif)#ip address 172.16.40.1 255.255.255.0
R(config-subif)#exit

SW(config)#interface e0/2
SW(config-if)#switchport trunk encapsulation dot1q
SW(config-if)#switchport mode trunk
SW(config-if)#exit
```

Cấu hình router R làm DHCP server cấp phát IP cho các VLAN:

```
R(config)#ip dhcp excluded-address 172.16.10.1
R(config)#ip dhcp excluded-address 172.16.20.1
R(config)#ip dhcp excluded-address 172.16.30.1
R(config)#ip dhcp excluded-address 172.16.40.1
R(config)#ip dhcp pool VLAN10
R(dhcp-config)#network 172.16.10.0 /24
R(dhcp-config)#default-router 172.16.10.1
R(dhcp-config)#exit
R(config)#ip dhcp pool VLAN20
R(dhcp-config)#network 172.16.20.0 /24
R(dhcp-config)#default-router 172.16.20.1
R(dhcp-config)#exit
R(config)#ip dhcp pool VLAN30
R(dhcp-config)#network 172.16.30.0 /24
R(dhcp-config)#default-router 172.16.30.1
R(dhcp-config)#exit
R(config)#ip dhcp pool VLAN40
R(dhcp-config)#network 172.16.40.0 /24
R(dhcp-config)#default-router 172.16.40.1
R(dhcp-config)#exit
```

Cấu hình truy nhập Internet:

```
R(config)#interface e0/1
R(config-if)#no shutdown
R(config-if)#ip address 100.0.0.2 255.255.255.252

R(config-if)#exit
R(config)#ip route 0.0.0.0 0.0.0.0 100.0.0.1

R(config)#access-list 1 permit 172.16.10.0 0.0.0.255
R(config)#access-list 1 permit 172.16.20.0 0.0.0.255
R(config)#access-list 1 permit 172.16.30.0 0.0.0.255
R(config)#access-list 1 permit 172.16.40.0 0.0.0.255
R(config)#ip nat inside source list 1 interface e0/1 overload

R(config)#interface e0/0.10
R(config-subif)#ip nat inside
R(config-subif)#exit
R(config)#interface e0/0.20
R(config-subif)#ip nat inside
R(config-subif)#exit
R(config)#interface e0/0.30
R(config-subif)#ip nat inside
R(config-subif)#exit
R(config)#interface e0/0.40
R(config-subif)#ip nat inside
R(config-subif)#exit
```

```
R(config)#interface e0/1
R(config-if)#ip nat outside
R(config-if)#exit
```

Trên các switch access và Branch, cấu hình đưa các test host vào các VLAN tương ứng như được chỉ ra trên sơ đồ:

```
ASW1-2(config)#interface e0/2
ASW1-2(config-if)#switchport mode access
ASW1-2(config-if)#switchport access vlan 10
ASW1-2(config-if)#exit
ASW1-2(config)#interface e0/3
ASW1-2(config-if)#switchport mode access
ASW1-2(config-if)#switchport access vlan 20
ASW1-2(config-if)#exit

Branch(config)#interface e0/2
Branch(config-if)#switchport mode access
Branch(config-if)#switchport access vlan 10
Branch(config-if)#exit
Branch(config)#interface e0/3
Branch(config-if)#switchport mode access
Branch(config-if)#switchport access vlan 20
Branch(config-if)#exit
```

Kiểm tra:

Kiểm tra rằng các host trên sơ đồ đã nhận được IP từ DHCP và đi được Internet, ví dụ, Host1:

```
Host1#
*Nov 22 08:12:37.692: %DHCP-6-ADDRESS_ASSIGN: Interface Ethernet0/0 assigned DHCP
address 172.16.10.2, mask 255.255.255.0, hostname Host1

Host1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

5. STP toolkit:

Cấu hình:

Cấu hình tính năng Portfast trên các cổng access nối đến end – user của các switch ASW1, ASW2 và Branch:

```
interface range e0/2 - 3
 spanning-tree portfast
```

Ngoài ra, trên cổng trunk của switch SW nối đến router R, ta cũng nên sử dụng portfast với tùy chọn "`trunk`":

```
SW(config)#interface e0/2
SW(config-if)#spanning-tree portfast trunk
```

Để hoạt động HA trên các đường uplink diễn ra nhanh, ta thực hiện cấu hình tính năng uplinkfast trên các switch ASW1, ASW2 và Branch:

```
spanning-tree uplinkfast
```

Cuối cùng, để chống tấn công vào cây STP từ phía người dùng, sử dụng tính năng BPDUguard trên các access – port của các switch ASW1, ASW2 và Branch:

```
interface range e0/2 - 3
 spanning-tree bpduguard enable
```