Lab Guide & Module

Cisco Certified Network Associate 200-301 V.1.1

3. Spanning Tree Protocol

Karakteristik utama dari jaringan komunikasi yang dibangun dengan baik adalah ketahanannya (resiliency). Network yang baik ketahanannya memerlukan perangkat atau koneksi redundant. Walaupun tujuannya ingin meningkatkan resiliency, namun redundancy di link layer-2 dapat menyebabkan looping di koneksi layer-2.

STP membantu mencegah terjadinya looping dalam jaringan switched yang redundant, dengan melakukan blocking-port ke salah satu switch. STP bekerja dengan cara mengirimkan BPDU message kepada setiap perangkat, yang berfungi untuk mendeteksi sekaligus membangun "gambaran" topologi switching yang digunakan.

STP Toolkit

PortFast

PortFast adalah fitur dalam Spanning Tree Protocol (STP) yang mempercepat proses konvergensi jaringan pada switch port yang terhubung ke perangkat endpoint seperti komputer atau printer. Ketika PortFast diaktifkan pada sebuah port, port tersebut akan segera beralih ke status forwarding tanpa harus melalui tahap listening dan learning yang biasanya memakan waktu beberapa detik. Hal ini sangat berguna untuk mempercepat proses pengaktifan port ketika perangkat endpoint baru terhubung. PortFast sebaiknya hanya diaktifkan pada port yang terhubung ke perangkat endpoint dan bukan pada port yang terhubung ke switch lain, karena dapat menyebabkan loop jaringan jika terjadi kesalahan konfigurasi.

Root Guard

Root Guard adalah fitur STP yang mencegah perangkat switch lain di jaringan menjadi root bridge selain switch yang sudah diinginkan. Root Guard digunakan untuk menjaga stabilitas topologi jaringan dengan memastikan bahwa port yang dilindungi oleh Root Guard tidak bisa menerima BPDU dengan priority yang lebih kecil dari root bridge yang digunakan. Jika ada BPDU yang mencoba menantang root bridge dari port yang dilindungi, maka port tersebut akan di-pindah ke status root-inconsistent, mencegah potensi perubahan root bridge yang tidak diinginkan. Root Guard biasanya diaktifkan pada switch port yang mengarah ke switch yang dianggap kurang terpercaya atau berada di luar kendali administratif.

Loop Guard

Unidirectional link failures dapat menyebabkan sebuah root port atau alternate ort menjadi designated port jika tidak menerima BPDU. Unidirectional Link Failures dapat disebabkan oleh isu hardware maupun software yang dapat menyebabkan temporary loop dalam jaringan switch. Fitur Loop Guard memeriksa apakah sebuah root port atau alternate port menerima BPDU atau tidak. Jika port tidak menerima BPDU, maka fitur Loop Guard akan menempatkan port tersebut dalam kondisi inconsistent hingga port tersebut kembali menerima BPDU.

BPDU Filter

BPDU Filter adalah fitur STP yang memungkinkan kita untuk memblokir pengiriman dan penerimaan BPDU pada port tertentu. Ketika BPDU Filter diaktifkan, port tersebut akan berhenti mengirim BPDU dan juga mengabaikan BPDU yang diterima. Hal ini dapat berguna pada port PortFast dimana BPDU tidak diharapkan, untuk mencegah pengiriman BPDU yang tidak perlu ke perangkat endpoint. Namun, penggunaan BPDU Filter harus hati-hati karena mematikan fungsi STP pada port tersebut dapat menyebabkan potensi loop jaringan jika port tersebut tiba-tiba terhubung ke switch lain.

BPDU Guard

BPDU Guard adalah fitur STP yang menonaktifkan port secara otomatis jika port tersebut menerima BPDU. BPDU Guard digunakan untuk melindungi port yang diaktifkan PortFast, memastikan bahwa hanya perangkat endpoint yang boleh terhubung dan bukan switch lain yang bisa mengirim BPDU. Jika sebuah port yang dilindungi oleh BPDU Guard menerima BPDU, port tersebut akan secara otomatis dinonaktifkan (err-disabled) untuk mencegah potensi loop atau perubahan topologi jaringan yang tidak diinginkan. BPDU Guard sangat penting untuk menjaga integritas dan stabilitas jaringan pada port yang hanya seharusnya terhubung ke perangkat endpoint.

Skenario LAB#1

Pada lab pertama ini, kita akan menggunakan Spanning-tree di VLAN 1. Perangkat CORE1 akan bertindak sebagai Root Bridge dan Perangkat CORE2 akan bertindak sebagai Backup- Root Bridge.

Langkah Pengerjaan:

Konfigurasikan CORE1 sebagai Root Bridge untuk VLAN 1

CORE1

```
Switch(config)#hostname CORE1

CORE1(config)#spanning-tree mode rapid-pvst

CORE1(config)#spanning-tree vlan 1 root primary

CORE1(config)#int range fa0/1-4

CORE1(config-if-range)#switchport trunk encapsulation dot1q

CORE1(config-if-range)#switchport mode trunk
```

Konfigurasikan CORE2 sebagai Backup Root Bridge untuk VLAN 1

CORE2

```
Switch(config)#hostname CORE2

CORE2(config)#spanning-tree mode rapid-pvst

CORE2(config)#spanning-tree vlan 1 root secondary

CORE2(config)#int range fa0/1-4

CORE2(config-if-range)#switchport trunk encapsulation dot1q

CORE2(config-if-range)#switchport mode trunk
```

Mari lakukan pengecekan di switch ACCESS1

ACCESS1

```
Switch(config)#hostname ACCESS1

ACCESS1#show spanning-tree vlan 1
```

Skenario LAB#2

Pada lab ini, kita akan menambahkan Spanning-tree di VLAN 2. Perangkat CORE2 akan bertindak sebagai Root Bridge dan Perangkat CORE1 akan bertindak sebagai Backup- Root Bridge.

Setelah pengerjaan skenario 2 ini, seharusnya semua link bisa dipakai sebagai forwarding port. Tidak seperti skenario sebelumnya, dimana dari total 2 link switch ACCESS hanya 1 link saja yang bisa digunakan menuju switch CORE.

Langkah Pengerjaan:

Konfigurasikan CORE2 sebagai Root Bridge untuk VLAN 2

CORE2

```
CORE2(config)#vlan 2

CORE2(config-vlan)#spanning-tree vlan 2 priority 0
```

Konfigurasikan CORE1 sebagai Backup Root Bridge untuk VLAN 2

CORE1

```
CORE1(config)#vlan 2

CORE1(config-vlan)#spanning-tree vlan 2 priority 4096
```

Enable VLAN 2 di Switch ACCESS1

ACCESS1

```
ACCESS1(config)#vlan 2
```

Enable VLAN 2 di Switch ACCESS2

ACCESS2

```
Switch(config)#hostname ACCESS2

ACCESS2(config)#vlan 2
```

```
ACCESS2(config)#end

ACCESS2#show spanning-tree int fa0/1
```

```
ACCESS2
```

```
ACCESS2#show spanning-tree
```