

Huawei Genel Notlar

Bu yazıda Huawei switchlerde STP, VBST ve RSTP protokollerinin konfigürasyon süreci açıklanacaktır.

STP Konfigürasyonu

- Varsayılanda cihazlarda STP protokolü devrede gelmeyebiliyor. Bunun için ilk olarak “**stp {enable | disable}**” komutuyla STP protokolünün cihaz genelinde devreye alınması gerekiyor.
 - o Devrede olup olmadığını “**display stp brief**” komutuyla kontrol edebilirsiniz.
 - o İsteğe bağlı olarak STP protokolünün çalışması istenmeyen portlarda ilgili portun arayüzüne giriş yapılarak “**stp {enable | disable}**” komutuyla STP protokolü devre dışı bırakılabilir veya devreye alınabilir.
- STP protokolü devreye alındıktan sonra “**stp mode {stp | mstp | vbst | rstp}**” komutuyla çalışması istenen STP versiyonu belirlenmelidir (varsayılanda MSTP protokolü devreye alınıyor).

```
[~CE6800-1]stp enable
[~CE6800-1]stp mode ?
  mstp  Multiple Spanning Tree Protocol (MSTP) mode
  rstp  Rapid Spanning Tree Protocol (RSTP) mode
  stp   Spanning Tree Protocol (STP) mode
  vbst  Vlan-based Spanning Tree (VBST) mode

[~CE6800-1]stp mode stp
[*CE6800-1]commi
```

- Cisco cihazlarda olduğu gibi burada da Root Bridge seçilmesi istenen switchler üzerinde “**stp root {primary | secondary}**” komutu kullanılarak öncelik verilmesi ve yedek olması sağlanabilir.
 - o İsteğe bağlı olarak “**stp priority <Priority>**” komutuyla Bridge Priority değeri de tanımlanabilir.

```
[~CE6800-1]stp priority ?
  INTEGER<0-61440> Bridge priority, in steps of 4096, the default is 32768
```

- STP protokolünde Path Cost değeri olarak kullanılacak aralık tanımını belirlemek için “**stp pathcost-standard {dot1d | dot1t | legacy}**” komutu kullanılıyor (<https://support.huawei.com/enterprise/en/doc/EDOC1100008296/a388a9d4/stp-pathcost-standard>) (varsayılanda Dot1T seçili olarak geliyor).
 - o Dot1D -> 1 – 65535 arasında değerlendiriliyor.
 - o Dot1T -> 1 – 200.000.000 arasında değerlendiriliyor.
 - o Legacy -> 1 – 200.000 arasında değerlendiriliyor.

```
[*CE6800-1]stp root ?
  primary    Primary root switch
  secondary   Secondary root switch

[*CE6800-1]stp root primary
[*CE6800-1]stp pathcost-standard ?
  dot1d-1998  IEEE 802.1D-1998
  dot1t       IEEE 802.1T
  legacy      Legacy

[*CE6800-1]stp pathcost-standard dot1t
[*CE6800-1]commit
```

- Portların Cost veya Priority değerleri üzerinde ayarlamalar yapabilmek için ilgili portun arayüzüne giriş yapılarak “**stp cost <Cost>**” veya “**stp port priority <Port Priority>**” komutları kullanılıyor.

- o Portlara Priority değeri 16’nın katları halinde tanımlanabiliyor.

```
[*CE6800-1]int ge 1/0/1
[*CE6800-1-GE1/0/1]stp cost 30
[*CE6800-1-GE1/0/1]stp port priority 32
[*CE6800-1-GE1/0/1]quit
```

- İstemci bağlı portlarda Loop oluşmayacağı bilindiği için bu portlar Cisco cihazlarda PortFast moduna alınıyordu. Huawei switchlerde ise portlar Edge Port olarak isimlendiriliyor. İstemci bağlı portları Edge Port moduna almak için ilgili arayüzüne giriş yapılarak “**stp edged-port {enable | disable}**” komutunun kullanılması gerekiyor.
- o System-view modunda “**stp edged-port default**” komutu kullanılarak bütün portların varsayılanda Edge Port moduna alınması sağlanabiliyor.
 - o Her ne kadar istemci bağlı portlar Edge-Port olarak tanımlansa da Loop oluşuma ihtimaline karşı “**stp bpdu-protection**” komutuyla da BPDU korumasının cihaz genelinde devreye alınması gerekiyor.

```
[*CE6800-1]int ge 1/0/5
[*CE6800-1-GE1/0/5]stp edged-port enable
[*CE6800-1-GE1/0/5]quit
[*CE6800-1]stp bpdu-protection
```

- İstemci bağlı portlarda BPDU-Guard koruması devreye alınmadığı sürece bir saldırgan cihazından TCN bitleri set edilmiş BPDU paketler gönderilerek STP ağacının manipüle edilmesi sağlanabilir. Bu nedenle isteğe bağlı olarak istemci bağlı portlarda TCN-Guard koruması açılarak bu portlardan gelen TCN bitlerinin set edildiği BPDU paketlerinin cihaz üzerinde herhangi bir etki oluşturamaması sağlanabiliyor (Switch üzerinde de herhangi bir değişime neden olmazken aynı zamanda bu bilgi diğer portlardan komşu switchlere de gönderiliyor). TCN-Guard korumasını cihaz genelinde devreye almak için System-view modunda “**stp tc-protection**” komutu kullanılıyor (isteğe bağlı olarak özelleştirilebiliyor).
- o Daha fazla koruma mekanizması için **CCNP - 02 – STP** notlarını inceleyebilirsiniz.

```
[*HUAWEI]stp tc-protection ?
interval    The time interval
threshold   Set the threshold value
<cr>
[*HUAWEI]stp tc-protection
```

- STP protokolünde kullanılan Timer süreleri “**stp timer {forward-delay <Forward Delay> | hello <Hello Timer> | max-age <Max Age>}**” komutları kullanılarak güncellenebiliyor.

```
[*CE6800-1]stp timer ?
forward-delay Specify forward delay
hello         Specify hello time interval
max-age       Specify max age
```

VBST (VLAN Based STP) Konfigürasyonu

Cisco Cihazlardaki PVST’ye karşılık gelen protokoldür. Bu protokolü devreye almak için;

- VBST konfigürasyonuna başlamadan önce cihaz üzerinde temel VLAN konfigürasyonunun yapılması gerekiyor.

- VLAN tanımları yapılmalıdır.
- Switch bağlı portlar Trunk moduna alınarak geçişine izin verilecek VLAN trafikler belirtilmelidir.
- Temel VLAN konfigürasyonu tamamlandıktan sonra cihaz üzerinde STP protokolünü devreye almak için “**stp enable**” komutunu kullanmak gerekiyor.
- VBST protokolünü devreye almak için “**stp mode vbst**” komutu kullanılmalıdır.
 - Huawei switchler arasında Proposal ve Agreement bayrak bitlerinin de kullanılarak daha hızlı anlaşabilmeleri için karşılıklı bağlı switch portların arayüzlerine girilerek “**stp no-agreement-check**” komutunun kullanılması gerekiyor (Cisco cihazlarda bulunun RPVST protokolünün dengi oluyor. Farklı olarak burada cihaz genelinde uygulanmak yerine port bazında uygulanıyor) (<https://support.huawei.com/enterprise/en/doc/EDOC1100064352/736edef8/stp-no-agreement-check>).

```
[*CE6800-1]stp enable
[*CE6800-1]stp mode vbst
[*CE6800-1]int ge 1/0/1
[*CE6800-1-GE1/0/1]stp no-agreement-check
[*CE6800-1-GE1/0/1]quit
[*CE6800-1]commit
```

- Bu kısımdan sonraki konfigürasyon yapısı STP protokolüyle aynıdır. Sadece kullanılan komutlar VLAN bazında tanımlanacağı için hangi VLAN’a uygulanacağını belirtmesi gerekiyor. Aşağıdaki görseller örnek olarak verilmiştir;
 - Hangi VLAN’ın hangi switch üzerinde Root Bridge seçileceğini belirlemek için “**stp vlan <VLAN Id> {primary | secondary}**” komutu kullanılıyor.

```
[~SwitchA] stp vlan 10 root primary
[*SwitchA] commit
[~SwitchA] stp vlan 20 root primary
[*SwitchA] commit

[~SwitchB] stp vlan 10 root secondary
[*SwitchB] commit
[~SwitchB] stp vlan 20 root secondary
[*SwitchB] commit
```

- Hangi VLAN’ın hangi switch portunda ne kadar Cost değerine sahip olacağını tanımlamak için “**stp vlan <VLAN Id> cost <Cost>**” komutu kullanılıyor.

```
[~SwitchA] interface ge 1/0/2
[~SwitchA-GE1/0/2] stp vlan 10 cost 2000000
[*SwitchA-GE1/0/2] stp vlan 20 cost 2000000
[*SwitchA-GE1/0/2] quit
[*SwitchA] commit
```

RSTP Konfigürasyonu

- RSTP konfigürasyonu için cihaz üzerinde “**stp enable**” komutuyla STP protokolü devreye alındıktan sonra “**stp mode rstp**” komutunu kullanmak yeterli oluyor. Bu kısımdan sonraki özelleştirmeler STP protokolüyle birebir aynıdır.

```
[*CE6800-1]stp enable
[*CE6800-1]stp mode rstp
[*CE6800-1]commit
```

NOTLAR

- Topolojide kullanılan STP mod seçiminin veya Timer sürelerinin her switch üzerinde aynı olması gerektiğini hatırlatmakta fayda var.

Kontrol Komutları

- display stp brief
- display stp interface <Interface Id> brief
- display stp vlan <VLAN Id>

Kaynaklar

- <https://support.huawei.com/enterprise/en/doc/EDOC1000141870/3dc65c52/example-for-configuring-stp>
- <https://support.huawei.com/enterprise/en/doc/EDOC1000178168/bd103455/example-for-configuring-vbst>
- <https://support.huawei.com/enterprise/en/doc/EDOC1100026507/7c984a5b/configuring-interworking-between-vbst-and-rapid-pvst>
- <https://support.huawei.com/enterprise/en/doc/EDOC1100279009/ae7adb14/stp-rstp-configuration>