

Aruba Genel Notlar

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

STP Kofigürasyonu

- İlk adımda cihaz üzerinde kullanılacak STP versiyonunu belirlemek için “**spanning-tree mode {rpvst | mstp}**” komutu kullanılmalıdır (Bu tanımlama cihaz üzerinde STP protokolü devre dışı durumdayken yapılmalıdır. STP protokolü devredeyse “**no spanning-tree**” komutuyla devre dışı bırakılabilir).
 - o Lab ortamında kullandığım Aruba CX model switch STP ve RSTP desteklemediği için uygulamasını yapamadım. Buradaki konfigürasyonlar Aruba markasının kendi dökümanları doğrultusunda hazırlanmıştır. Cisco cihazlarla bir bütün halde çalışabilmesi adına bazı modellerinde STP protokolü “**spanning-tree force-version {stp-compatible | rstp-operation | mstp-operation}**” komutuyla devreye alınabiliyor. Bu kısımdan sonraki uygulanan konfigürasyon komutları kullanılan STP versiyonu fark etmeksizin uygulanabilir.
- Aruba switchlerde varsayılanda STP protokolü devre dışı gelebiliyor. Kullanılacak STP versiyonu tanımlandıktan sonra STP protokolünü devreye almak için global konfigürasyon modunda “**spanning-tree**” komutunun kullanılması gerekiyor.
 - o Kapalı olup olmadığını “**do sh spaning-tree detail**” komutuyla kontrol edebilirsiniz.
 - o Bu komutla STP protokolü devreye alındığında varsayılanda MSTP protokolü devreye alınıyor.

```
ArubaCX-1(config)# spanning-tree mode
mstp Multiple spanning tree mode
rpvst Rapid PVST mode
ArubaCX-1(config)# spanning-tree mode rpvst
ArubaCX-1(config)# spanning-tree
```

- Cisco cihazlarda olduğu gibi burada da Root Bridge seçilmesi istenen switchler üzerinde “**spanning-tree priority <Priority>**” komutu kullanılarak Bridge Priority değerinin değiştirilmesi sağlanabiliyor.
- STP protokolünde Path Cost değeri olarak kullanılacak aralık tanımını belirlemek için “**spanning-tree pathcost-type {long | sort}**” komutu kullanılıyor.
 - o Long parametresi, 1 – 200.000.000 arasında değerlendiriliyor
 - o Sort parametresi, 1 – 65535 arasında değerlendiriliyor.

```
ArubaCX-1(config)# spanning-tree priority
<0-15> Enter an integer number (Default: 8)
ArubaCX-1(config)# spanning-tree priority 1
ArubaCX-1(config)# spanning-tree pathcost-type
long Configure the pathcost as long (Default)
short Configure the pathcost as short
ArubaCX-1(config)# spanning-tree pathcost-type long
```

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

- Kullandığınız modele göre varsayılanda cihaz portları L3’de gelebilir. STP komutları çalıştırılmadan önce “**no routing**” komutuyla portlar L2’ye alınmalıdır.

```
ArubaCX-1(config)# int 1/1/1
ArubaCX-1(config-if)# no routing
ArubaCX-1(config-if)# spanning-tree cost 1
ArubaCX-1(config-if)# spanning-tree port-priority
<0-15> Enter an integer number (Default: 8)
ArubaCX-1(config-if)# spanning-tree port-priority 0
ArubaCX-1(config-if)# exit
```

- İstemci bağlı portlarda Loop oluşmayacağı bilindiği için bu portlar Cisco cihazlarda PortFast moduna alınıyordu. Aruba switchlerde ise portlar Admin-Edge olarak isimlendiriliyor. İstemci bağlı portları Admin-Edge moduna almak için ilgili arayüzüne giriş yapılarak “**spanning-tree port-type {network-edge | admin-edge}**” komutunun kullanılması gerekiyor.
 - Her ne kadar istemci bağlı portlar Admin-Edge-Port olarak tanımlansa da Loop oluşuma ihtimaline karşı “**spanning-tree bpdu-guard**” komutuyla da BPDU korumasının ilgili port üzerinde devreye alınması gerekiyor.

```
ArubaCX-1(config)# int 1/1/1
ArubaCX-1(config-if)# spanning-tree port-type
admin-edge Set as administrative edge port
admin-network Set as administrative network port (Default)
ArubaCX-1(config-if)# spanning-tree port-type admin-edge
ArubaCX-1(config-if)# spanning-tree bpdu-guard
ArubaCX-1(config-if)# exit
```

- 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 oluşturmaması sağlanabiliyor (Switch üzerinde de herhangi bir değişime neden olmazken aynı zamanda bu bilgi diğer portlardan komşu switchlere de gönderiliyor). TCN-Guard korumasını devreye almak için ilgili portun arayüzüne giriş yapılarak “**spanning-tree tcn-guard**” komutu kullanılıyor.
 - Daha fazla koruma mekanizması için **CCNP - 02 – STP** notlarını inceleyebilirsiniz.

```
ArubaCX-1(config)# interface 1/1/1
ArubaCX-1(config-if)# spanning-tree tcn-guard
ArubaCX-1(config-if)# exit
```

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

```
ArubaCX-1(config)# spanning-tree max-age
<6-40> Enter an integer number (Default: 20 secs)
ArubaCX-1(config)# spanning-tree max-age 20
ArubaCX-1(config)# spanning-tree hello-time
<2-10> Enter an integer number (Default: 2 secs)
ArubaCX-1(config)# spanning-tree hello-time 2
ArubaCX-1(config)# spanning-tree forward-delay
<4-30> Enter an integer number (Default: 15 secs)
ArubaCX-1(config)# spanning-tree forward-delay 15
```

PVST+/RPVST+ Konfigürasyonu

- PVST/RPVST konfigürasyonuna başlamadan önce cihaz üzerindeki portların L2'ye çekilmesi ve temel VLAN konfigürasyonunun yapılması gerekiyor. Bu süreçte;
 - o L2'de kullanılacak portların arayüzlerine girilerek **"no routing"** komutunun kullanılması gerekiyor.
 - o VLAN tanımları yapılmalıdır.
 - o Switch bağlı portlar Trunk moduna alınarak geçişine izin verilecek VLAN trafikler belirtilmelidir.
- Temel VLAN konfigürasyonu tamamlandıktan sonra cihaz üzerinde RPVST protokolünü devreye almak için **"spanning-tree mode rpvst"** komutunu kullanmak gerekiyor.
 - o STP protokolünü devreye almak için **"spanning-tree"** komutu kullanıldığında devreye varsayılanda MSTP protokolü alınıyordu. Farklı bir STP versiyonunu devreye alabilmek için öncelikle **"no spanning-tree"** komutuyla STP protokolünün cihaz genelinde devre dışı bırakılması gerekiyor. Aksi takdirde istenilen STP versiyonuna geçiş yapılamayacaktır. STP protokolünün devre dışı olduğu görüldükten sonra **"spanning-tree mode {rpvst | mstp}"** komutuyla istenilen STP versiyonu ayarlanmalıdır. Ayarlama yapıldıktan sonra **"spanning-tree"** komutuyla STP protokolü tekrar devreye alınmalıdır.

```
ArubaCX-1(config)# spanning-tree
ArubaCX-1(config)# spanning-tree mode rpvst
Cannot configure the rpvst mode, disable spanning-tree to configure (or change)
the mode.
ArubaCX-1(config)# no spanning-tree
ArubaCX-1(config)# spanning-tree mode rpvst
ArubaCX-1(config)# spanning-tree
```

- RPVST protokolü devreye alındıktan sonra RPVST protokolünde kullanılacak/ağaç oluşturulacak her bir VLAN'ın **"spanning-tree vlan <VLAN IDs>"** komutuyla tanımlanması gerekiyor. Aksi takdirde RPVST üzerinde kullanılacak VLAN'lar üzerinde herhangi bir işlem yapılamıyor.

```
ArubaCX-1(config)# spanning-tree vlan 10 priority 10
Error : STP instance not present for one or more VLANs.
ArubaCX-1(config)# spanning-tree vlan 10-12,20,30
ArubaCX-1(config)# spanning-tree vlan 10 priority 10
```

- Kullanılacak VLAN'lar tanımlandıktan sonraki süreçte STP protokolünde kullanılan her komutlara ek olarak uygulanacağı VLAN tanımının yapılması gerekiyor. Aşağıdaki görseller örnek olarak verilmiştir;
 - o Hangi VLAN'ın hangi switch üzerinde Root Bridge seçileceğini belirlemek için **"spanning-tree vlan <VLAN Id> priority <Priority>"** komutu kullanılıyor.
 - o Hangi VLAN'ın hangi switch portunda ne kadar Cost değerine sahip olacağını veya port Priority değerini tanımlamak için **"spanning-tree vlan <VLAN Id> cost <Cost>"** ve **"spanning-tree vlan <VLAN Id> port-priority <Port Priority>"** komutları kullanılıyor.

```
ArubaCX-1(config)# spanning-tree vlan 20 priority 5
ArubaCX-1(config)# spanning-tree vlan 10 priority 1
ArubaCX-1(config)# int 1/1/1
ArubaCX-1(config-if)# spanning-tree vlan 10 cost 2
ArubaCX-1(config-if)# spanning-tree vlan 10 port-priority 1
ArubaCX-1(config-if)# spanning-tree vlan 20 cost 10
ArubaCX-1(config-if)# spanning-tree vlan 20 port-priority 5
ArubaCX-1(config-if)# exit
```

- Hangi VLAN için hangi Timer ayarlanmak isteniyorsa “**spanning-tree vlan <VLAN Id> {forward-delay <Forward Delay> | hello-time <Hello Time> | max-age <Max Age>}**” komutu kullanılıyor.

```
ArubaCX-1(config)# spanning-tree vlan 10 hello-time 2
ArubaCX-1(config)# spanning-tree vlan 10 max-age 20
```

NOT

- RPVS konfigürasyonunda komutlar VLAN belirtilmeden uygulandığında tanımlamalar bütün VLAN tanımlarına uygulanmıyor. Denemek için bir portun Priority değeri VLAN belirtilmeden değiştirildiğinde bu port bütün Priority değeri bütün VLAN tanımları için geçerli olmuyor. Eğer olsaydı, her ne kadar arka planda her VLAN için ayrı STP ağacı oluşturulsa da aslında bu şekilde kullanıldığında oluşan yapı RPVST yerine RSTP protokolü gibi görülebilirdi (Bu durumda olarak her VLAN için aynı STP ağacı oluşacaktı).

Kaynaklar

- https://www.arubanetworks.com/techdocs/AOS-CX/10.10/PDF/l2_bridging_83xx-9300-10000.pdf
- <https://www.arubanetworks.com/techdocs/CLI-Bank/Content/aos8/spanning-tree.htm>
- <https://higherlogicdownload.s3.amazonaws.com/HPE/MigratedAssets/STP%20Feature%20Interop%20Guide-%20ArubaOS%20and%20Cisco%20IOS%20.pdf>
- https://www.arubanetworks.com/techdocs/AOS-CX/10.09/HTML/security_4100i-6000-6100/Content/Chp_Port_acc/Port_acc_rol_cmds/stp-adm-edg-por-fl-ml-10.htm
- https://www.arubanetworks.com/techdocs/AOS-CX/10.07/HTML/5200-7868/Content/Chp_stp/mstp_cmds/spa-tre-tcn-gua-mst.htm#:~:text=Description,of%20disabled%20on%20the%20interface.