STP

STP protokolü networklerde döngü oluşumunu önlemek için kullanılan bir protokoldür. Zaman içerisinde ihtiyaçlara yönelik olarak farklı versiyonları çıkarılmıştır.

- **802.1D Standart/Original STP**
  - Karar verme süreci yavaştır. Yedek hatta geçiş uzun sürer.
  - Yedek hat bloklanır/kullanılmaz, yük dengeleme yapılmaz (Load-Balance özelliği yoktur).
- **PVSTP (Per-VLAN Spanning Tree)**
  - Encapsulation protokolü olarak sadece ISL (Cisco'ya özel protocol) destekliyor. ISL başlık boyutunun büyük olması gibi çeşitli nedenlerden dolayı artık günümüzde kullanılmadığı için PVSTP de kullanılmıyor.
  - Cisco'ya özel protokoldür.
  - Yedek hatlar arasında yük paylaşımı (Load Balancing) yapılabiliyor (Her VLAN için farklı root bridge seçilip farklı Spanning Tree'ler oluşturuluyordu. Bu sayede her VLAN için farklı portlar bloklanıyordu. Detayları CCNA notlarında).
- **PVSTP+ (Per-VLAN Spanning Tree Plus)**
  - Encapsulation protokolü olarak ISL protokolüne ek olarak 802.1q desteği de getirildi.
- **Rapid PVST (Rapid Per-VLAN Spanning Tree Protocol)**
  - Hızlandırılmış ve yük dengeleme özelliğini destekleyen protokoldür.
- **802.1W RSTP (Rapid Spanning Tree Protocol)**
  - IEEE tarafından oluşturulmuştur.
  - STP protokolünün karar verme süreci hızlandırılmıştır (yedek hatta geçiş süreci 50 sn'den 2 sn'ye kadar düşürülmüştür). Yedek hatlara çok daha hızlı geçiş yapılabilmektedir.
  - Path Cost değer aralığı genişletilmiştir (Bu sayede switchlerde ayrıca konfigürasyon yapmaya gerek kalmadan daha yüksek bant genişliklerine sahip networklerde bloklanacak portlara daha doğru karar verilebiliyor).
- **802.1S MST (Multiple Spanning Tree Protocols)**
  - IEEE tarafından oluşturulmuştur.
  - Yedek hatlar arasında yük dengeleme yapılabiliyor.

802.1D STP Protocol Port Durumları

Bir switch portuna yeni bir cihaz bağlandığında döngü kontrolü ve sonrası için STP protokolü çalışırken portun alabileceği birkaç durum vardır. Bu durumlar;

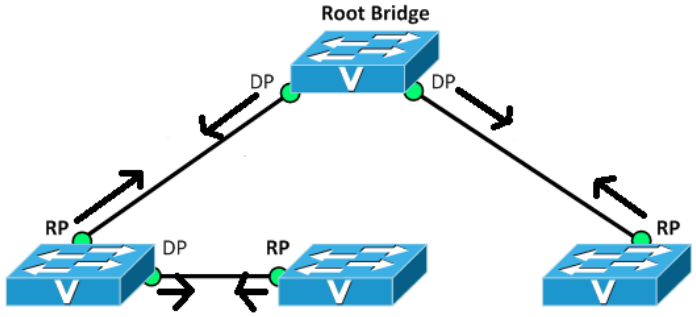
- **Disabled**, portun kapalı olduğu durumdur.
- **Blocking**, karar mekanizması çalıştıktan sonra döngü oluşturan portlardan trafik akışının engellendiği durumdur. Port kapanmaz. Sadece gelen paketler drop edilir. Bloklanan portlardan sadece BPDU paketleri gönderilmeye devam edilir.
- **Listening**, STP protokolünün devrede olduğu bir switche yeni bir kablo bağlandığında döngü oluşturup oluşturmadığını anlamak için portun dinlenmeye alındığı durumdur. Bu süreçte switch portlarından BPDU paketleri gönderir ve paketlerin geri gelip gelmediği kontrol edilir. Bu durum 15 saniye sürmektedir. Bu süreçte port üzerinden hiçbir trafiğe izin verilmez (MAC adresleri de öğrenilmiyor).

- **Learning**, Listening durumunda döngü oluşmadığı anlaşıırsa porta gelen paketlerin içerisinde bulunan MAC adresleri öğrenilmeye başlanır ama yine de trafik geçişine izin verilmez. Bu durum 15 saniye sürmektedir.
- **Forwarding**, döngü oluşturmayan portların trafik akışına izin verildiği durumdur.
- **Broken**, switch port üzerinde anomali algıladığı zamanlarda (bağlantılarda oluşan kopmalar gibi) portun aldığı durumdur.

Port Tipleri

STPprotokolünde Spanning Tree oluşturulurken portlara belirli roller atanıyordu. Bu rollere bakıldığında;

- Root Port (RP), Root Bridge'e doğru giden portlara verilen isimdir.
- Designated Port (DP), Root Bridge'den aşağı yöne giden/çıkan portlara verilen iisimdir.
- Blocking Port, döngü oluşturduğu için (karşılıklı her iki portunnda DP olma durumu) blok durumuna alınan portun alındığı moddur.



Root Bridge ve Cost Değerleri

Root Bridge seçiminde öncelikle her switch kendisini Root Bridge olarak ilan ediyordu ve komşu switchlerden BPDU paketleri geldikçe paket içerisindeki bilgiler değerlenidriliyor ve topolojideki Root Bridge'e karar veriliyordu. Root Bridge seçiminden sonra portlardan BPDU paketleri gönderilerek switch portları DG (Designated Port) ve RP (Root Port) olarak etiketleniyor, karşılıklı DP olan bağlantılarda döngü oluştuğu anlaşılarak bloklama işlemi yapılıyordu (Detaylar CCNA notlarında açıklanmıştı). Bloklama sürecinde ise switchlerde sırasıyla **portların Path Cost değerine, switchlerin Bridge ID değerine** veya **Port Id (kablolar aynı switche bağlıysa)** değerine bakılarak karar veriliyor.

STP Path Cost değeri için Short Mode ve Long Mode olarak iki mod kullanılabiliyor. Bu modlardan hangisinin kullanılacağına topolojide kullanılan bant genişliklerine bakılarak karar veriliyor. Bu seçimi değiştirmek için "**spanning tree method <long |short>**" komutu kullanılıyor.

Link Speed	Short-Mode STP Cost	Long-Mode STP Cost
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2,000
20 Gbps	1	1,000
100 Gbps	1	200
1 Tbps	1	20
10 Tbps	1	2

STP Protokolünde Root Bridge seçiminden sonra switchlerde her portundan Root Bridge'e ulaşmak için gereken Cost değeri hesaplanarak tablolarına kaydediyor. Bu sayede bloklanacak portlar belirlenebiliyor.

```
SW1#sh spanning-tree vlan 1
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID     Priority    32769
              Address     0002.16D5.2E03
              Cost        19
              Port        2(FastEthernet0/2)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0009.7C52.4658
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/2            Root FWD 19        128.2    P2p
Fa0/1            Desg FWD 19        128.1    P2p

SW1#
```

|→ Görsel Rapid-PVST konfigürasyonundan alınmıştır (yani her VLAN için farklı STP bilgsi görünebilir). Root Bridge bilgileri bulunuyor (DP'un Cost değeri, yani switchin Root switch'e olan total/toplam Cost değeri -> 19,. Bu bilgiler doğrultusunda Fa portu 100Mbit ve Root Bridge'e doğrudan bağlı denilebilir).

|→ Alt kısımda ise switch portlarının detayları gösteriliyor. Örneğin Fa 0/1 portunun Cost değeri->19.

|→ Görselde Type –> P2p görünmesinin anlamı, portun Full-Duplex çalıştığını gösteriyor . --> P2p Edge olsaydı, bu portun Full-Duplex çalıştığını ve Port-Fast özelliğinin açık olduğunu gösterirdi.

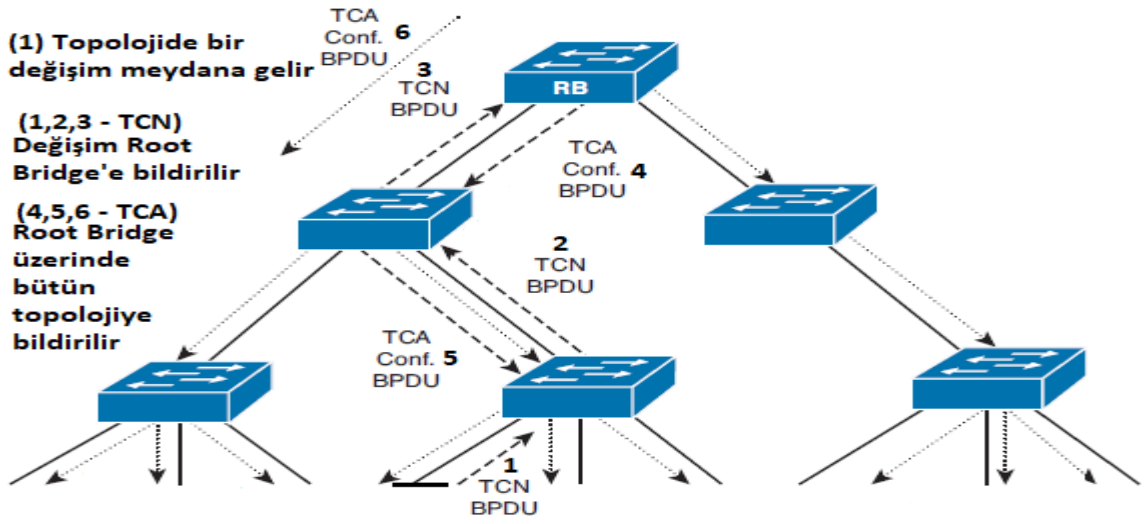
|→ Priority değerinin 32768 olduğu ve System ID Extension (VLAN Numarası -> 1) değeriyle beraber Bridge ID Priority değerinin 32769 olduğu görülüyor (**Terminolojiler kısmında System ID, Bridge ID tanımları açıklanmıştır -** Görselde portların Priority değerlerinin varsayılanda 128 olduğu görülüyor).

|→ Root Bridge'e giden portun (yani aktif seçilen port) Cost değerini değiştirmek için öncelikle Cost değeri değiştirilecek portun arayüze giriş yapılarak "**spanning-tree cost <Cost>**" veya "**spanning tree vlan <Vlan ID> cost <Cost>**" komutu kullanılıyor (Kullanılan komutlar STP türüne göre değişim gösteriyor).

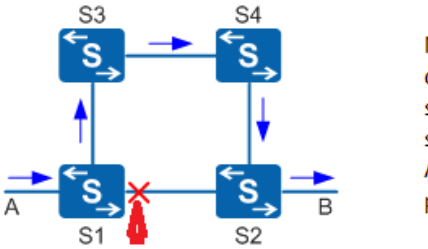
```
SW1(config)#int fa 0/1
SW1(config-if)#spanning-tree cost ?
  <1-200000000>  port path cost
SW1(config-if)#spanning-tree vlan ?
  WORD  vlan range, example: 1,3-5,7,9-11
SW1(config-if)#spanning-tree vlan 1 cost ?
  <1-200000000>  Change an interface's per VLAN spanning tree path cost
SW1(config-if)#
```

Topolojide Bir Değişim Olduğunda

Topolojide bir değişim meydana geldiğinde, değişimin meydana geldiği switch bunu Root Bridge'e BPDU paketi içerisindeki TCN bitini set ederek bildiriyor. Root Bridge bu değişimi öğrendikten sonra topolojideki diğer switchlere BPDU paketi içerisindeki TCA bitini set ederek bildiriyor. Bu bilgiyi alan switchler MAC Address tablosundaki kayıtların silinme sürelerini kısaltıyor. Yani varsayılanda 300 saniye içerisinde herhangi bir trafik oluşturulmadığında silinen MAC adresi TCA biti set edilmiş BPDU paketi aldığında 15 saniyeye düşüyor.



TCA biti set edilmiş BPDU paketi aldıklarında MAC Address tablosundan kayıt silme sürelerinin kısaltılmasının nedeni ise normalde topolojide bir switchin bağlantısı koptuğunda bunu doğrudan bağlı switch bilir ve bu bağlantı üzerinden öğrenilen MAC adreslerini MAC Address tablosundan siler. Her ne kadar kendisine doğrudan bağlı switch MAC Address tablosundaki kayıtları güncellese de kendisine farklı switchler üzerinden bağlanan switchler bu değişimi doğrudan algılayamadığı için MAC Address tablolarını güncelleyemiyorlar. Yani topolojiden kaldırılan switch üzerinde bulunan bir istemciye paket göndermek gerektiğinde paketi hedef istemciye gönderecek ara switche göndermeye devam edilecektir ama paket hedefine ulaşamayacaktır.



Loop oluşumunu önlemek için bloklanan port

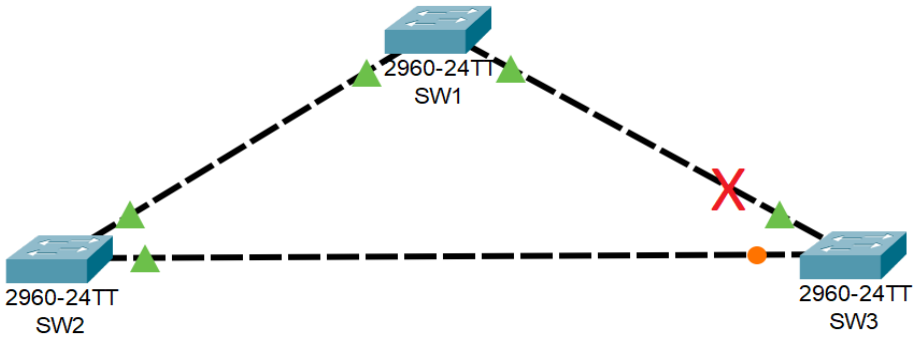
Normalde TCA biti set edilmiş BPDU paketi gönderilmediği durumda S3 ve S1 arasındaki bağlantı koptuğunda bunu S4 swtichi bilmemeyeceği için A istemcisine gidecek paketleri S3 switchine göndermete devam edecektir. S3 istemcisinin MAC Address tablosunda A istemcisine ait MAC adresi silineceği için paketler drop edilecekti.

|→ Bu durumu düzenlemek için Root Bridge üzerinde TCA biti set edilmiş BPDU paketi gönderildiğinde topolojideki bütün switchler MAC Address tablolarında trafik oluşturmayan kayıtları silme süresini 15 saniyeye düşürerek aslında topolojiden ayrılan switch üzerinden erişilemeyen MAC adreslerini MAC Address tablolarından kaldırmaları sağlanıyor. Bu sayede 15 saniye boyunca yanıt alınamayan MAC adresine tablodan kaldırıldıktan sonra hangi port üzerinden erişileceği yeniden belirleniyor (Bu süreçte döngü oluşturduğu için bloklanan portlar olabilir (aktif bağlantı koptuğu için bloklanan portlar devreye alınacaktır) veya farklı switchler üzerinden erişilebilecek alternatif seçenekler olabilir. Bu durumlar yeniden değerlendiriliyor).

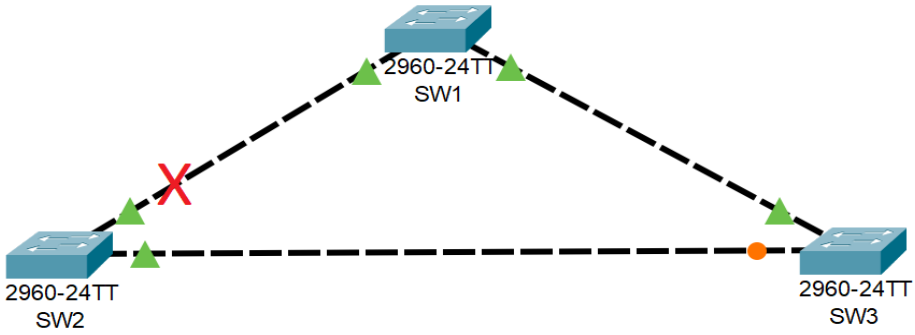
Bir bağlantı koptuğunda yaşanabilecek 3 durum vardır.

- İlk durumda aşağıdaki görselde olduğu gibi Root Bridge'e doğrudan bağlı bir switch bağlantısında kopma meydana geldiğinde (portlarından biri bloklanmış, diğerinin bağlantısı kompmuş) bağlantısı kopan switch Root Bridge'e herhangi bir TCN biti set edilmiş BPDU paketi gönderemeyecektir çünkü burada switch Root Bridge'e ulaştığı portun bağlantısını kaybediyor (Blok portundan sadece gelen BPDU paketlerini dinleyebiliyor). Bu durumda Root Bridge bu bağlantı kopukluğunu anlayıp topolojide bir değişiklik olduğunu TCA biti set edilmiş BPDU paketiyle bütün topolojiye bildirecektir.

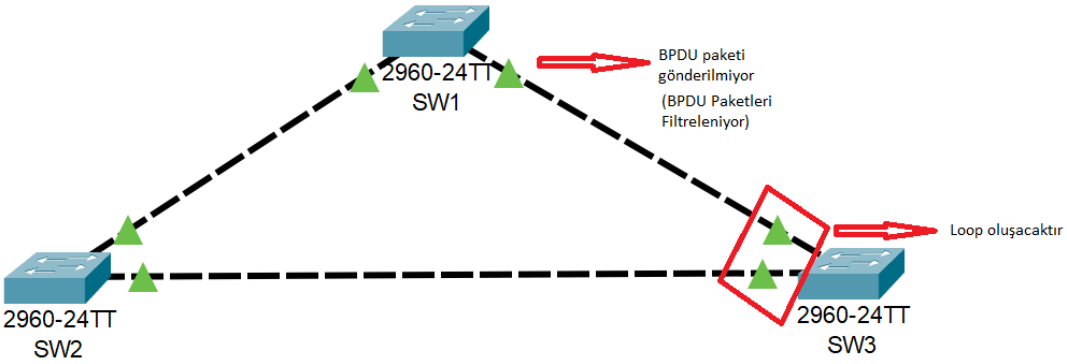
- Bu süreçte SW3 30 saniye (15 saniye Listening+15 saniye Learning) geçtikten sonra bloklanan portunu açacaktır.



- İkinci durumda aşağıdaki görselde olduğu gibi Root Bridge'e bağlı portlardan birinde kopma meydana geldiğinde SW2 Root Bridge'den BPDU paketi alamayacağı için kendisini Root Bridge ilan edecektir ve SW3'e bu doğrultuda BPDU paketigönderecektir. SW3 bu paketi aldığında SW2'nin Root Bridge'e bağlantısının koptuğunu anlıyor (SW3 bunu Root Bridge daha düşük değerler göndermeye devam etmesine rağmen SW2 Root Bridge olduğunu gösteren BPDU paketleri göndermeye devam etmesinden anlıyor) ve TCN biti set edilmiş BPDUpaketini Root Bridge'e bildiriyor. Root Bridge ise TCA bitini set ederek topolojide değişim olduğunu bütün switchlere bildiriyor ve SW3 bloklanan portunu devreye alıyor.



- Üçüncü durumda aşağıdaki görselde olduğu gibi Root Bridge'e bağlanan portta bağlantı olmasına rağmen BPDU paketi gönderilmiyor olabilir (BPDU paketleri filtrelenmiş olabilir). Bu durumda SW3 20 sn (Max Age) bekleyecektir. Bu süre sonunda SW3 Root Bridge'e olan bağlantısını kaybettiğini düşünerek kendisini Root Bridge ilan ederek SW2'ye kendisini Root Bridg gösteren BPDU paketleri gönderecektir. SW2, SW3'ün Root Bridge'e olan bağlantısını kaybettiğini düşünecek (Bağlantı devam etse de sadece Root Bridge tarafından BPDU paketi alamıyor) Root Bridge'e TCN biti set edilmiş BPDU paketleriyle topolojide değişim olduğunu bildirecektir. Bu durumda SW3 bloklanan portunu devreye alacaktır (20 sn Max Age + 15sn Listening + 15sn Learning = 50 sn) ve Root Bridge'e (SW1) bloğunu kaldırdığı port üzerinden ulaşacaktır. Ne yazık ki burada Root Bridge'den BPDU paketi alamadığı port da devrede kalacağı için bu durum LOOP oluşumuna neden olacaktır. Bu durum networkün çökmesine neden olacaktır.
    - BPDU Filter özelliği kullanılarak portlarda BPDU paketlerinin gönderilmesi de alınması da engellenebiliyor. Bu özellik son kısımlarda açıklanıyor.



NOT

- Topolojilerde her switchin Root switche ulaşması gerekiyor. Bu nedenle genelde topolojideki en büyük şaseye sahip switchin Root switch seçilmesi istenir. Bu seçim sürecini de Priority değerleri değiştirilerek sağlanıyor.

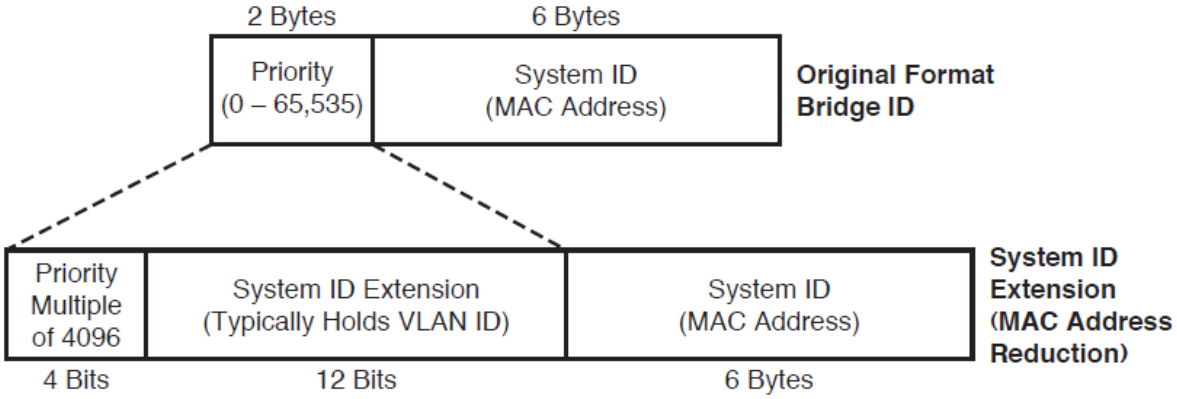
Terminolojiler

- Root Bridge, oluşturulan Spanning Tree'nin en baştında bulunan kök switche verilen isimdir.
- BPDU (Bridge Protocol Data Unit), tüm topolojinin tespit edilmesi, STP ile bloklanacak portların belirlenmesi gibi kararlar alınırken kullanılan pakettir. Her 2 sn'de bir STP çalışa bütün portlardan gönderilir.
- Configuration BPDU, root bridge değişimi veya bloklanan portlarda yaşanan değişim gibi topolojide oluşan değişmleri temsil eden BPDU paketleri için kullanılan bir terimdir.
- TCN (Topology Chance Notification), topolojide bir değişiklik yaşadığında bunu switchlerin Root Bridge'e bildirmek için kullanılan BPDU paketi içerisindeki 1 bitlik bir alandır.
- TCA (Topology Chance Acknowledgement), topolojide bir değişiklik yaşadığında bunu switchlerin Root Bridge'e TCN biti set edilerek bildiriliyordu. Root Bridge ise bu değişimi topolojideki diğer switchlere bildirmek için kullanılan BPDU paketi içerisindeki 1 bitlik bir alandır.
- Root Path Cost, STP protokolünde bloklanacak porta karar verilirken değerlendirilmede kullanılan ve portların bant genişlikleri göz önünde bulundurularak elde edilen bir değerdir. Bloklanacak portlar arasında en düşük Root Path Cost değerine sahip olan port en kaliteli port olur ve aktif port seçilir.
    - Root Path Cost değerinin nasl hesaplandığı CCNA notlarında açıklanmıştı.
- Bridge Identifier, switchin adı olarak tanımlanabilir. Bu değer öncelik numarası ve MAC adresinin birleşimiyle oluşturuluyor. Varsayılanda bu değer bütün switchlerde aynıdır. Yani bu durumda Root Bridge seçimini MAC adresi küçük olan switch kazanır (CCNA notarında bahsedilmişti).
- System Priority, STP protokolünde switchlerin Root Bridge olması için öncelik bilgisini gösterir. Bridge Priority değerinin sonuna System ID Extension (VLAN Numarası) değerini eklenmesiyle oluşur.

    - Difference between bridge ID and system priority -> https[:]//www.firewall.cx/networking-topics/protocols/spanning-tree-protocol/1054-spanning-tree-protocol-root-bridge-election.html
- System ID Extension, PVST ve türevi protokoller kullanılırken her VLAN için farklı Spanning Tree oluşturuluyordu. Her VLAN için her switchin de ayırt edilebilmesi gerekiyor ki oluşturulan Spanning Tree'lerde hangi VLAN için hangi switch portlarının bloklanacağı ayırt edilebilsin. Bu nedenle switchlerde her VLAN için oluşturulan Spanning Tree'lerde switchleri unique kılmak/ayırt edebilmek için Bridge Priority değerinin sonuna System ID Extension (VLAN Numarası) ekleniyor. Bu sayede başlık yapısı bozulmadan (IEEE tarafından çıkarılan protokollerle başlık bilgisi bölümünün sorun çıkarmaması adına önemli) her VLAN için oluşturulan Spanning Tree'lerde switchler ayırt edilebiliyor.

Bridge Prioirty (4 Bits)				System ID Extension (12 Bits) - VLAN											
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

1000 = 32768 000000000001 = 1



- Port Priority, portlara atanan öncelik değeridir. Priority değeri (0-255 arasında değr alır. Varsayılanda 128 gelmektedir) ve port numarasının birleşimiyle oluşmaktadır (Örnek 1. Port için Port Priorit değeri = 128.1 olacaktır).
    - Bir kablonun her iki ucu da aynı switch üzerine takıldığında hangi portun bloklanacağını ayırt edip karar verebilmek için kullanılıyor.
- Hello Time, STP protokolünde 2 saniye aralıklarla bütün portlardan BPDU gönderilmesidir.
- Forward Delay, switche yeni bir cihaz bağlandığı zaman döngü kontolü için Listening ve Learning modlarında geçirilen süredir (802.1D için varsayılanda Listen -> 15 sn – Learning –> 15 sn).

Kontrol Komutları

- sh spanning-tree root
- sh spanning-tree vlan <VLAN Number>
- sh spanning-tree