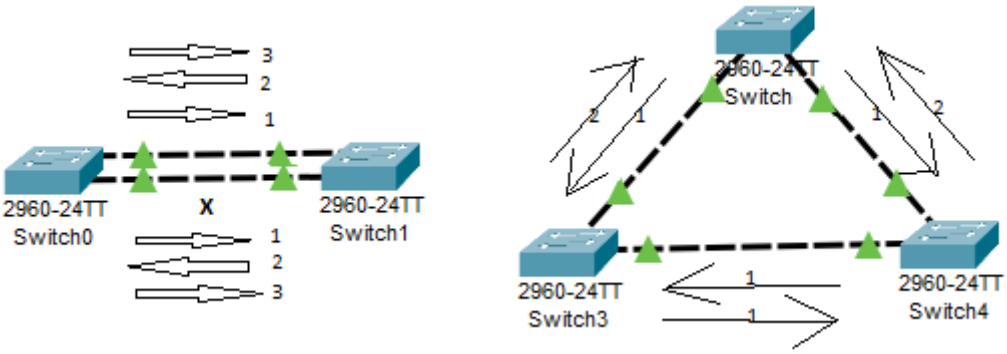
STP (802.1d)

Networklerde (özellikle de networkte hassas işlemler gerçekleştiren şirketler) oluşabilecek kesintilerin önüne geçilmek istenir. Bunun için switchler arasında yedeklemeler yapılmak istenir. Ne yazık ki switchler (L2) arasında birden fazla kablo bağlanarak yedekleme gerçekleştirilemiyor. Nedeni ise iki switch arasında birden fazla kablo bağlandığında **Loop/döngü** oluşmasıdır.

Loop, switchlerin kendisine gelen broadcast veya multicast paketleri geldiği port dışında bütün portlarına anahtarlamasıyla gerçekleşiyor. Switchler arasında aktif birden fazla bağlantı olduğunda broadcast paketleri her aktif bağlantıdan gönderildiği için networkte döngü oluşuyor ve paketler tekrar tekrar switchler arasında anahtarlanıp duruyor. Nedeni L2 başlık bilgisinde L3'de olduğu gibi paketin anahtarlanma sayısını kontrol eden bir bölüm olmamasıdır. Bu durum network haberleşmesini olumsuz etkilemekle kalmayıp iletişimin kesilmesine de neden olabiliyor. Buna **Broadcast Storm** deniyordu (CCNA - 2.02 - Passwrd Recovery Switch Concepts and Switch Leds – NOTES-2).



STP (Spanning Tree Protocol), networkte döngü oluşturacak bağlantıların tespit edilip bloklanmasını sağlayan protokoldür. STP protokolü ile iki switch arasında birden fazla bağlantı seçeneği olduğu tespit edilirse bu durumun döngü oluşturmaması için tespit edilen bağlantılardan biri dışındaki bütün portlar bloklanır. Bloklanmayan port üzerinde bir problem yaşandığında ise bloklanan portlardan biri devreye alınarak kesintinin önüne geçilmesi sağlanır. Yani STP protokolü sayesinde hem networkte yedeklilik sağlanıyor hem de loop oluşmasının önüne geçilerek networkte kaos oluşmasının/sistemin çökmesi engelliyor.

> |→ MAC adresi öğrenilirken de (ARP) kullanılan paketler broadcast yayın yapılarak networke bırakılıyordu. Bu yayın döngü olan bir networkte gerçekleştirildiğinde switch portlarına aynı MAC adresi farklı portlarından tekrar gelecektir ve CAM tablosunda aynı MAC adresi için birden fazla kayıt oluşturulacaktır (Nedeni switchin bir portundan gönderdiği paket diğer portlarından (yani bağlı olduğu switchler üzerinden) tekrar kendine anahtarlanmasıdır). Bu durumda CAM tablosuna kaydedilen MAC adresine bir paket gönderilmek istendiğinde switch bu paketi birden fazla portundan anahtarlayacaktır (Çünkü tek bir MAC adresi, MAC Address tablosunda birden fazla port için kaydedilmiş durumda olacaktır). Bu durumda yine döngü oluşacak ve bu durum zamanla network trafiğini yavaşlatacak hatta sistemin çökmesine neden olacaktır.

Spanning Tree Algoritmasında switchler aralarında haberleşebilmek için her 2 saniyede bir tüm portlarından birbirlerine **BPDU** (Bridge Protocol Data Unit) paketleri gönderiyorlar (Buna Hello Timer deniliyor).

Spanning Tree Algoritması (Standart);

- Switch portuna bir cihaz bağlandığında port **Listening** durumuna alınıyor. Bu modda switch 15 saniye boyunca port dinleyerek gönderdiği BPDU paketleriyle sistemi tanımaya, döngü oluşup oluşmadığını anlamaya çalışıyor. Bu süreye **Forward Delay** deniliyor. Bu süre boyunca bu bağlantı üzerinden hiçbir veri aktarımı gerçekleştirilmiyor (herhangi bir MAC adresi de öğrenilmiyor).
  |→ Döngü olduğu tespit edilirse port **Blocking** durumuna alınarak bloklanıyor. Blocking durumunda olan portlarda sadece BPDU paketlerine izin veriliyor.
  |→ Döngü olmadığı anlaşılırsa **Learning** durumuna geçiliyor. Bu durumda MAC adresleri öğrenilirken dahi veri aktarımına izin verilmiyor (Bu durum da 15 saniye sürmektedir). Bu durum sonrasında da döngü oluşmadığı anlaşılırsa **Forwarding** durumuna geçiliyor ve port veri aktarımına başlanıyor.

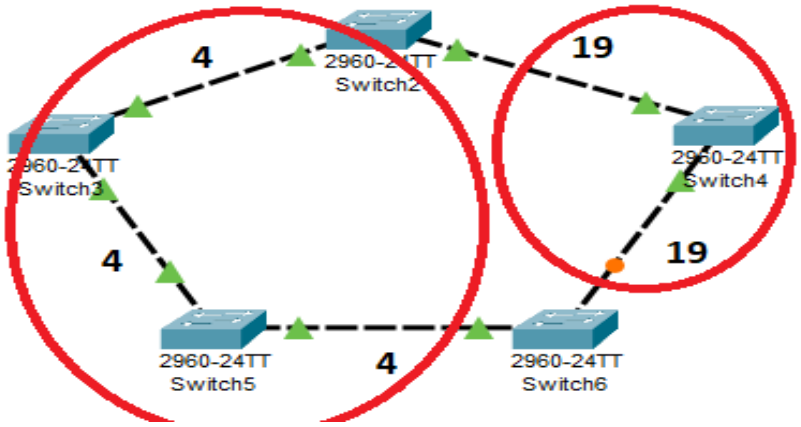
Spanning Tree Karar Verme Mekanizması

Döngü oluşturan iki port arasında karar verme sürecine bakıldığında;

- Bloklanacak portlar arasında **Path Cost** (Bant genişliği) değerlerine bakılarak hangi portun aktif olacağına karar veriliyor. **Path Cost değeri en düşük port kullanılmaya devam edilirken** döngü oluşturan diğer portlar bloklanıyor.

Data rate	STP cost (802.1D-1998)	RSTP cost (802.1W-2004, default value) [154]
100 Mbit/s	19	200,000
1 Gbit/s	4	20,000
2 Gbit/s	3	10,000
10 Gbit/s	2	2,000

|→ Bu değerler hedef cihaza ulaşmak için kullanılan rotalar üzerindeki bağlantılara veriliyor (bant genişliklerine göre). Hedef cihaza ulaşmak için **hangi rotanın toplamda daha düşük Path Cost değerine sahip olduğuna bakılarak** aktif kalacak porta karar verilir. Aktif seçilen portlar dışındaki (alternatif) portlar bloklanır.
|→ **RSTP** (Rapid Spanning Tree Protocol), STP ile tam olarak aynı çalışma mantığına dayanıyor. Sadece 10Gbit ve üzeri hızlarda Path Cost değerlerini doğru verilebilmesi için STP'nin genişletilmiş verisyonudur.



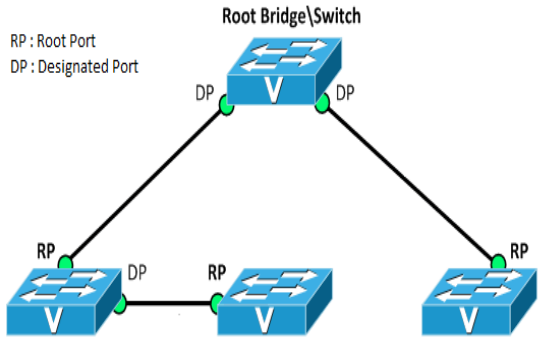
- Path Cost değerlerinin eşit olduğu durumlarda her routerun kendine tanımladığı **BID** (Bridge Id) değerine bakılarak karar verilir. **Küçük BID (Bridge Priority değeri + MAC adresi)** değerine sahip port seçilir.

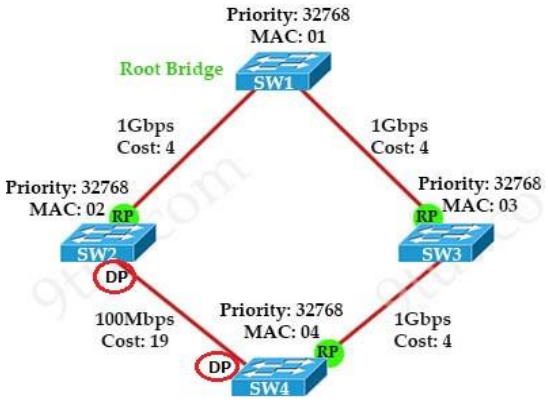
- Kablonun iki ucu de aynı switchin iki farklı portuna bağlanmadığı sürece MAC adreslerinin aynı olması beklenemez ama MAC adreslerinin aynı olduğu durumda (yönetici ayrıca Bridge Priority değerini değiştirmemişse) **Port Id** değerine bakılıyor. **Port Id değerleri küçük olan port** kullanılmaya devam edilirken diğer portlar bloklanıyor.
  |→ İki switch arasında birden fazla bağlantı yapıldığında eğer ki path cost değerleri de(bağlantı hızları) aynıysa kullanılmaya devam edecek portu belirlemek için Port Id değerlerine bakılıyor (**Burada BPDU paketini yollayan switchin Port Id değerine bakılır**).

Spanning Tree Protokolü çalışırken başlangıçta switchler birbirlerine BPDU paketleri gönderiyorlar. BPDU paketleri içerisinde BID değerleri var ve bu değere göre en küçük BID değerine sahip switch Root switch (**Root Bridge**) seçiliyor. Bu adımdan sonra bir ağaç yapısı oluşturularak her porta bir rol veriliyor. **Root switchden çıkan tüm portlara Destignated Port, Root Bridge'e gelen tüm portlara Root Port deniliyor**. Portlara bu roller atanırken switchler arasındaki bağlantılarda her iki portun da Designated port olduğu durumda döngü olduğu anlaşılıyor ve portlardan biri karar verme mekanizması göz önünde bulundurularak bloklanıyor.

|→ BID (Bridge Id) değeri en küçük olan Root Switch seçiliyor.

|→ Bloklanan portlara **Undesignated port** deniliyor.

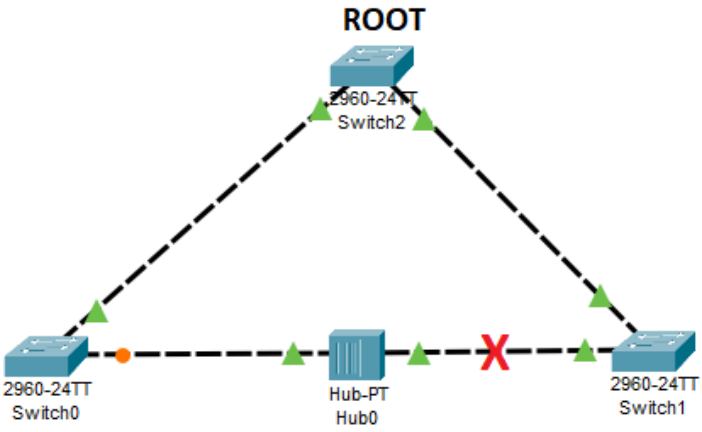




|→ Kullanılan/Aktif portun bağlantısı kesildiğinde portu bloklanan switche bağlı switcler bunu anlıyor (Detayı bilgi için CCNP - 02 – STP notlarını inceleyebilirsin) ve yeniden Spanning Tree Algoritmasını çalıştırarak 30 saniye Listening ve Learning modlarının ardından bloklanan portu devreye alıyor.

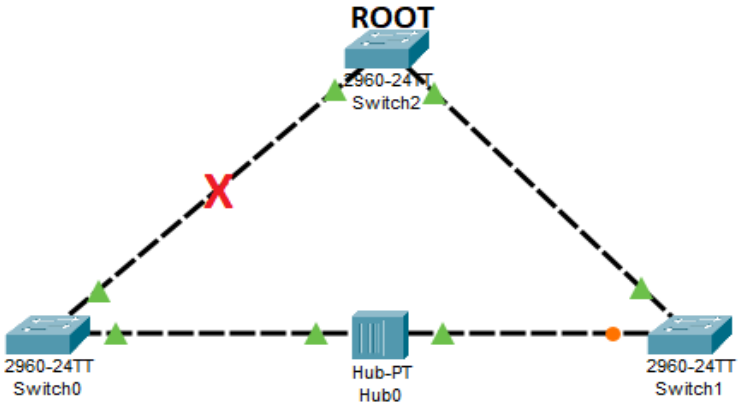
SORU : Aşağıdaki görselde de görüldüğü gibi iki switch arasına Unmanageable bir switch veya hub konumlandırıldığında STP protokolü döngü tespit ettiği portu bloklamaktadır. Peki Hub ve Switch1 arasındaki bağlantıda kesinti olursa Switch0 bunu nasıl anlayıp bloklanan portunu devreye alacaktır?

|→ Switch1 ile hub arasındaki bağlantı kesildiğinde Switch0'a gönderilen BPDU paketleri kesilecektir. Bu durumda Switch0 **20 saniye (Max Age)** bekledikten sonra BPDU paketleri gelmediğini görecek ve 15 saniye Listening + 15 saniye Learning sonrasında portu devreye alacaktır (Kafa karışıklığı olmaması için burada Hub Unmanageable olduğu için kendisi ayrıca BPDU paketleri gönderememektedir. Sadece switchlerden gelen BPDU paketlerini iletiyor).



SORU : Aşağıdaki görselde de belirtildiği gibi Root Bridge ile Switch0 arasındaki bağlantısı kesilirse Switch1'ın bloklanan portu nasıl devreye alınır?

|→ Bu durumda Switch0 kendisini Root Bridge ilan edecektir. Böylece portlarından BPDU paketleri içerisinde bu bilgiyi gönderdiğinde Switch1 aynı anda iki Root Bridge olduğunu görüp Switch0'ın Root Bridge ile bağlantısının kesildiğini anlayacaktır (Switch2'nin (Root Bridge) port hızı – BID veya Port ID değerlerinin Switch0'a göre daha yüksek olduğunu görecektir). Bu durumda bloklanan portunu 30 saniye (Listening + Learning) sonunda devreye alacaktır.



STP Protokolünün Zayıf Yönleri

- Yavaş olması, Bir cihaz bağlandığında toplamda 30 saniye boyunca döngü olup olmadığına karar verilirken portlardan veri geçişine izin verilmiyor.
  |→ STP protokolünün hızlanması için **RSTP** (Rapid Spanning Tree) protokolü çıkarılmıştır (RSTP protokolü üzerine **CCNA - 2.05 – STP** dizininde ayrıca yazı hazırlanmıştır).

- Yedek hattın/döngü oluşturan portun bloklaması, döngü oluşturan portu bloklamak yerine Load Balance/yük dengeleme yapılarak sahip olunan bant genişliği arttırılabilirdi.
  |→ Döngü oluşturan portta Load Balance yapabilmek için **PVST** (Per-VLAN Spanning Tree) protokolü geliştirilmiş. Bu protokol her switch için ayrıca STP ağacı oluşturulması sağlıyor. PVST protokolü aynı zamanda Portfast,UplinkFast, BackboneFast, BPDU Guard, BPDU Filter, Root Guard cve Loop Guard gibi özellikler de içermektedir (PVST protokolü üzerine **CCNA - 2.05 – STP** dizininde ayrıca yazı hazırlanmıştır).

|→ RSTP protokolü Load Balance yapmasa da oldukça hızlıdır. Zaman içerisinde hızlı olduğu kadar yük dengeleme yapabilmesi için de geliştirilerek **MSTP** (Multiple Spaning Tree) protokolü oluşturulmuştur. MSTP protokolü, RSTP protokolünü temel alırken aynı zamanda Load Balance da yapabilmektedir. IEEE tarafından geliştirilmiştir. Konfigürasyonu daha karmaşıktır (Detaylı bilgiyi **CCNP - 02 – STP** notlarında bulabilirsin).

STP Konfigürasyonu;

Cisco cihazlarda genelde STP protkolü varsayılanda açık geliyor. Sadece özelleştirilmek istendiği durumlarda konfigürasyon yapılmaya ihtiyaç duyuluyor.

- Bir swtichin her zaman Root Bridge seçilebilmesi için BID değerini oluşturan Priority değerini düşürebiliyoruz. Bunun için global konfigürasoyon modunda "**spanning-tree vlan 1 priority <Priority Number>**" komutu kullanılıyor (Burada **Per-Vlan Rapid Spanning Tree** kullanılıyor. Ek olarak Priority değeri için sadece belirli sayılar verilebiliyor.).

```
L3SW(config)#spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096
L3SW(config)#spanning-tree vlan 1 priority 20
% Bridge Priority must be in increments of 4096.
% Allowed values are:
  0     4096  8192  12288 16384 20480 24576 28672
  32768 36864 40960 45056 49152 53248 57344 61440
L3SW(config)#spanning-tree vlan 1 priority 4096
L3SW(config)#
```

- Networkte kullanılan Spanning-Tree protokolünün türü "**spanning-tree mode <STP Mode>**" komutuyla değiştirilebilir (Kullanılan modele değişiklik gösterebilir). Bunu networkteki her switchte tanımlamak gerekiyor (Burada kullanılan switch sadece PVST destekliyor).

```
L3SW(config)#spanning-tree mode ?
  pvst        Per-Vlan spanning tree mode
  rapid-pvst  Per-Vlan rapid spanning tree mode
L3SW(config)#
```

- **PortFast** özeliği açmak için ilgili arayüze girilip "**spanning-tree portfast**" komutu kullanılıyor. Bu porta BPDU paketleri gönderecek herhangi bir cihaz takılmasına karşı "**spanning-tree bpduguard enable**" komutuyla BPDU koruması açılıyor. Bu sayede porta switch gibi BPDU paketi gönderecek bir cihaz bağlandığında portun disable moduna alınması sağlanyor.
    - Cihaz genelinde PortFast özelliği devreye alınan bütün portlarda BPDU Guard özelliğinin de otomatik olarak devreye alınması için global konfigürasyon modunda "**spanning-tree bpduguard enable**" komutu da kullanılabilir.

```
SW1(config)#interface fastEthernet 0/10
SW1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/10 but will only
have effect when the interface is in a non-trunking mode.
SW1(config-if)#spanning-tree bpduguard enable
SW1(config-if)#exit
SW1(config)#
```

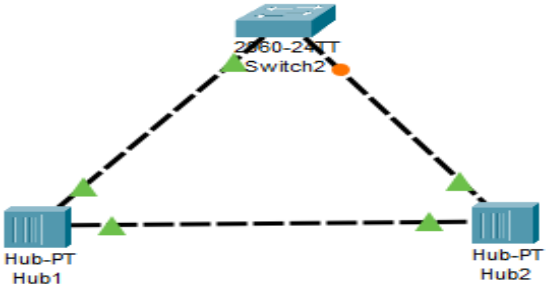
- İsteğe bağlı olarak port arayüzlerine giriş yapılarak "**spanning-tree {port-priority <Port Priority> | Cost <Cost>}**" komutuyla portların Priority ve Cost değerleri de özelleştirilebiliyor. Komutlar bu şekilde kullanıldığında (özel bir VLAN tanımı yapılmadığı sürece) bütün VLAN tanımları için geçerli oluyor.

NOTLAR:

- Routerlar arasında da döngüler oluşabiliyor ama 3. Katman başlığında TTL/HOP değeri bulunduğu için paketler sonsuza kadar yönlendirilmiyor. Bu değerler sıfırlandığında paketler drop ediliyor.
  |-> TTL/HOP değerleri paketin çıktığı bilgisayardaki işletim sistemine göre belirleniyor. Bu değerler göz önünde bulundurularak bir istemcinin kullandığı işletim sistemi tespit edilebiliyor.

Operating System	Time To Live
Linux (Kernel 2.4 and 2.6)	64
Google Linux	64
FreeBSD	64
Windows XP	128
Windows Vista and 7 (Server 2008)	128
iOS 12.4 (Cisco Routers)	255

- **Max Age**, STP protokolü için kullanılan üç zamanlayıcıdan (Hello, Forward Delay, Max Age) biridir. Switchlerde bloklanan portlarda 20 saniye boyunca BPDU paketleri gelmediği taktirde portu devreye almak için kullanılan zamanlamadır. Bloklanan porta 20 saniye boyunca BPDU paketi gelmezse 15 saniye Listening + 15 saniye Learning adımlarından sonra (toplamda 50 saniye sonrasında) portu devreye alıyor.
  - İsteğe bağlı olarak "**spanning-tree vlan <VLAN Id> {forward-time <Forward Tiime> | hello-time <Hello Time> | max-age <Max Age Time>}**" komutuyla Timer süreleri de ayarlanabiliyor.
-
- Portlarda (Buna bloklanan portlarda dahildir) ayrıca bir konfigürasyon yapılmadığı sürece (PortFast özelliği gibi) her porttan BPDU paketi yollanır.
- Networkte tek bir Manageable switch olması Loop oluşumunu engellemek için yeterlidir. Manageable switch tarafından gönderilen BPDU paketleri yine Swtich portuna geleceği için döngü oluşturan port bloklanacaktır.



- Özetle Root Switch seçiminde karar mekanizması için sırasıyla, **Bridge Priority – MAC adresi – Port Id** değerlerine bakılıyor (düşük olanlar seçiliyor).
- Kullanılacak port seçiminde karar mekanizması için sırasıyla, **Path Cost – Bridge Id – Port Id** değerlerine bakılıyor (düşük olanlar seçiliyor).
- PVST (Per-VLAN Spanning Tree Protocol) protokolü kullanılarak her VLAN için farklı portların kullanılması sağlanabiliyor. Yani her VLAN için farklı portların bloklanması sağlanarak portlar arasında yük dengeleme işlemi yapılabiliyor.

- Rapid PVST protokolü, RSTP protokolünün hızıyla ve PVST protokolünün özelliklerinin bütünleştirildiği STP protokolüdür. Cisco tarafından gerliştirilmiştir.
- RSTP protokolü switchler arasında Loop olup olmadığına karar verip portun durumuu belirlerken, istemci bağlı uçlarda bu süre yine 30 saniye sürmektedir. Nedeni Switchler arası BPDU paketleriyle switchler aralarında hızlıca senkronize olurken istemci bağlı uçlarda BPDU paketleri gönderilmediği için 30 saniye boyunca port açılamamaktadır.
- Porta istemci bağlanacağı kesin ise portta **PortFast** özelliği açılarak 30 saniye beklemeden istemcinin switche bağlandığı anda networke erişebilmesi sağlanabiliyor.
  |→ Bu özellik açılırken dikkat edilmesi gerekiyor çünkü bu port her ne kadar kendisine switch bağlandığında kendisini Listening durumuna alıp STP protokolün çalıştırmaya başlasa da, STP protokolü başlatılana kadarki sürede (RSTP protokolünde bu süre her ne kadar toplamda 2 saniye olsa da networkü çökertmek için yeterli olacaktır) loop oluşma ihtimali vardır. Bu durum bütün networkü etkilemekle kalmayıp çökmesine dahi neden olabilmektedir.
  |→ PortFast özelliği açılan portlarda döngü oluşmasını engellemek için BPDU Guard özelliği açılabiliyor. PortFast özelliği açılan bir porta yanlışlıkla bir switch bağlandığında swtich BPDU paketleri göndermeye başlayacaktır. PortFast açılan portta BPDU Guard özelliği de açılmışsa bu porta bir switch bağlandığı anlaşılacak ve port disable moda alınacaktır. Portu tekrar aktif hale getirebilmek için network yönteicisinin portun arayüzüne girerek manuel olarak "**shutdown**" komutuyla kapatıp "**no shutdown**" komutuyla tekrar açması gerekiyor.
- WoL (Wake ın Lan) özelliği, uyku modundaki bilgisayarları network üzerinden (uzaktan) uyandırabilmek için kullanılan bir protokoldur.
- VLAN ,bir tür ağ sanallaştırma tekniğidir.
- Bu konfigürasyonu mümkünse network kullanımının az olduğu saatlerde, yani mesai saatleri dışında yapmak gerekiyor.

Terminolojiler:

- Unknown Unicast Frames, hedef MAC adresi bilinmeyen paketlere verilen isimdir. Bu frameler switchlerde geldiği port dışında switchin bütün portlarına anahtarlanıyor.
- BID (Bridge Id), switchlerin kendilerine tanımladığı bir değerdir. Bu değer sayesinde switchler networkte birbirlerini ayırt edebiliyorlar. Bu değer, Bridge Priority değeri + MAC adresini birleşimiyle oluşuyor.
  |→ Bridge Priority değeri varsayılanda 32768'dir. Yönetici bu değeri manuel olarak verebiliyor/değiştirebiliyor. Bu sayede istenen switchin Root Bridge seçilmesi sağlanabiliyor.
- Port Id, Port Priority değeri + Port numarasının birleşiminden oluşuyor.
  |-> Port Priority değeri 0 - 255 arasında değer alabiliyor.

Kontrol Komutları

- Show spanning-tree