

## VLAN

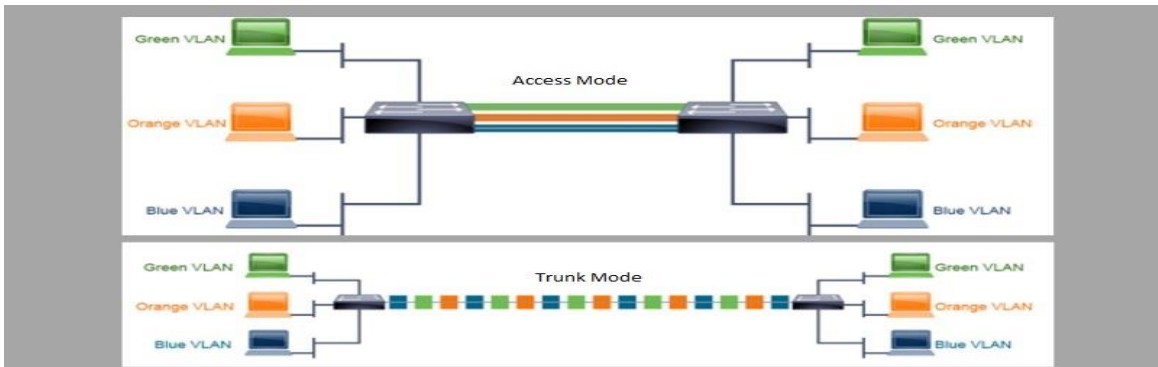
VLAN, bir networkü mantıksal daha küçük networklere bölmek için kullanılan teknolojidir. Aynı işi yapan istemcileri gruplamak olarak da tanımlanabilir. Bu sayede;

- Networkteki broadcast domainler küçülür ve trafik yükünü azaltır.
- Oluşan sanal networkler arası bir noktaya kadar güvenlik sağlar.
- Switchler üzerinde sanal networkler oluşturulur. Oluşturulan sanal networklerin port bazında gruplandırılarak kullanılması switch portlarının daha verimli kullanılmasını sağlar.
- VLAN kullanılmadan tasarlanan topolojiye kıyasla switch sayısı çok daha az olacaktır. Bu durum IT operasyonları kolaylaştırırken aynı zamanda network maliyetini de azaltacaktır.
- Fiziksel olarak farklı konumlarda bulunan cihazlar için uzun kablolar yapmak yerine o konuma yakın bir switch portuna bağlayarak cihaz istenilen sanal networke (VLAN'a) dahil edilebilmektedir. Bu kullanıma örnek olarak yazıcı türü ortak kullanılan cihazlar verilebilir.

VLAN teknolojisinde Access ve Trunk olmak üzere switch portlarına uygulanabilecek iki mod bulunmaktadır.

- **Access mod**, bilgisayar, laptop gibi istemcilerin bağlandığı portlarda kullanılan moddur. Access moduna alınan portlar tek bir VLAN için hizmet verir (Access moduna alınan portlarda framelere herhangi bir ek etiket bilgisi eklenmeden veri iletimi gerçekleştirilir).
- **Trunk modu**, farklı switchlerde oluşturulan aynı VLAN'lara atanmış portların aralarında haberleşebilmesi gerekiyor. Bu haberleşmeyi gerçekleştirebilmek için iki farklı yöntem kullanılabilmektedir.
  - o İlk yöntem, her VLAN için iki switch arasında access moduna alınmış portlardan birer kablo/bağlantı çekilerek aynı VLAN'a dahil cihazların aralarında haberleşebilmesi sağlanabilmektedir. Bu yöntem kullanıldığında çok fazla VLAN olması durumunda switch portlarının gereksiz kullanılmasına neden olacaktır.
  - o İkinci bir yöntem ise portların Trunk moduna alınmasıdır. Trunk moduna alınan portlar, üzerlerinden birden fazla VLAN trafiğinin taşınabilmesi sağlıyor. Bu sayede switch portları gereksiz yere meşgul edilmeden, aynı VLAN'a dahil cihazlar farklı switchler üzerinde olsalar dahi aralarında haberleşebilmesi sağlanabiliyor.

Trunk, switchler arasından farklı VLAN'lara ait framlarin iletimini, IEEE tarafından çıkarılan 802.1q protokolü kullanılarak gerçekleştiriyor (Bu haberleştirme ilk olarak Cisco tarafından çıkarılan ISL (Inter Switch Link – 29 bayt başlık bilgisi eklenir) teknolojisiyle gerçekleştirilmeye başlanmıştır.). Trunk yapılandırılan portlardan geçen ethernet framlarının içerisine VLAN bilgilerini tanımlayan 4 baytlık yeni bir başlık bilgisi ekliyor. Frame kaynak switchden çıkarken eklenen bu başlık bilgisi hedef switchte ulaştığında çıkarılıyor ve başlık bilgisine göre hedef switchdeki ilgili potlara iletilmesi sağlanıyor.



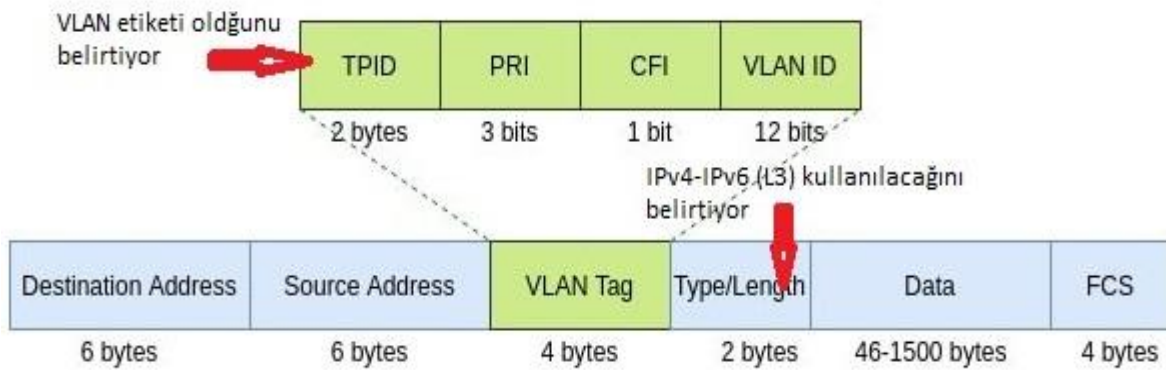
## 802.1Q Etiket Yapısı

|→ Type, VLAN etiketi olduğunu belirten alandır (EtherType değeri için <https://en.wikipedia.org/wiki/EtherType> → 0x8100 = VLAN, 0x0800 = IPv4 gibi).

|→ User Priority, öncelik numarasıdır. QoS için kullanılıyor (Örnek olarak ip telefon trafiği, dinamik yönlendirme protokollerinin trafiği gibi çeşitli trafiklere öncelik verilebiliyor). Bu özellik VLAN oluşturulduğunda varsayılanda gelmiyor. Ayrıca yapılandırılması gerekiyor (öncelik verilmek istenen VLAN için bu değerin 0 dan büyük olması bu VLAN trafiğine öncelik verilmesi için yeterlidir).

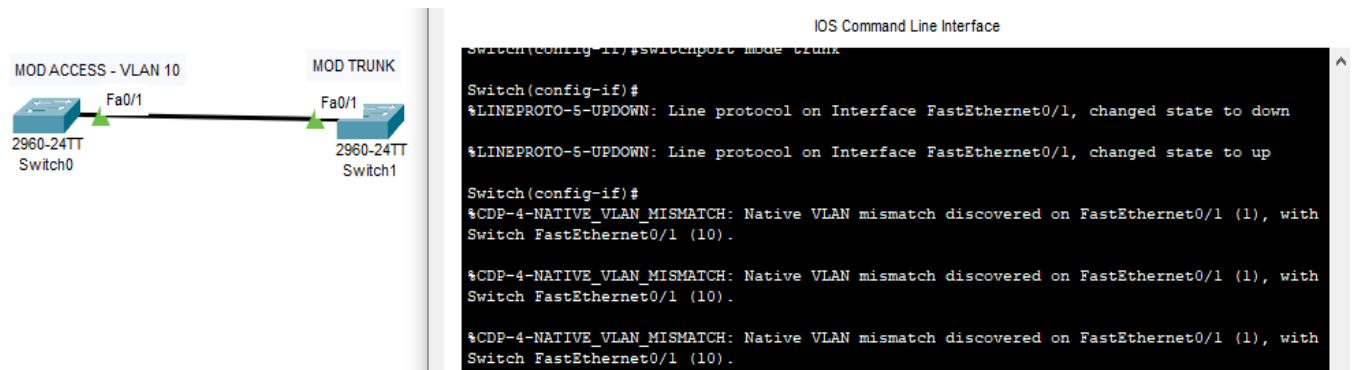
|→ CFI (Canonical Format Identifier), Token Ring için kullanılam alandır. Günümüzde kullanılmıyor.

|→ Vlan ID, VLAN'ın id numarasını bulunuyor. Bu alan 12 bit boyutundadır (Yani  $2^{12}$  bit = 4096 VLAN oluşturulabiliyor).



SORU: Farklı VLAN'lara atanmış portlar birbirine bağlanırsa ne olur?

Farklı VLAN'lara atanmış portlar birbirine bağlanırsa, bağlanılan portlardaki VLAN'ları birbirine geçirmiş olur. Özetle, Access modunda alınan portlarda paketler iletilirken paketlere ek başlık bilgisi eklenmiyordu. Bu nedenle Access moduna alınan portlardan çıkan framerlerde VLAN bilgisi bulunmayacaktır. Bu bilgiler doğrultusunda, Switch 1 de VLAN 2'ye atanmış bir port ile switch 2 de VLAN 99'a atanmış bir port birbirine bağlandığında, Switch1'deki VLAN 1 trafiği Switch2'de VLAN 2'ye atanmış portlarına gönderilecektir. Yani Switch 1'deki VLAN 2'ye atanmış istemciler ile Switch2'deki VLAN 99'a atanmış istemciler haberleştirilmiş oluyor. Aynı durum Native VLAN bilgisi aynı olmayan iki switch için de geçerlidir. Switchler bu durumu algılayıp CLI'a hata mesajı gönderecektir.



SORU: Portlarından biri Trunk moduna alınmış bir switch ile Portlarından biri access moduna alınmış başka bir switch birbirine bağlanırsa ne olur?

Access moda alınan port, trunk moduna alınan porta frame'leri 802.1q başlığı eklemeyen göndereceği için Trunk moduna alınan switch'de frame'leri Native VLAN'a atanmış portlarına anahtarlacaktır. Trunk moduna alınan switch'den ise her VLAN trafiği frame'lere 802.1q etiketi eklenerek gönderilecektir. Bu durumda ise sadece Native VLAN trafiği etiketsiz gönderileceği için sadece Native VLAN trafiği geçirilecektir. Özetle SW1 -> Access port (VLAN 2), SW2 -> Trunk porta sahip switchler olarak düşünüldüğünde SW1 üzerindeki VLAN2'ye atanan cihazlar ile SW2 üzerindeki Native VLAN'a atanan cihazlar birbirine geçirilmiş (birleştirilmiş) durumda olacaktır.

## VLAN Konfigürasyonu

- VLAN konfigürasyonu için öncelikle switchlerde global konfigürasyon modunda "**vlan <VLAN ID>**" komutuyla VLAN oluşturulmalı. Son olarak isteğe bağlı olarak "**name <VLAN Name>**" komutuyla oluşturulan VLAN'a isim de verilebilir (VLAN isimlendirilmediği takdirde varsayılanda "**VLAN<VlanNumber>**" şeklinde isim tanımı yapılmaktadır).

```
SW1(config)#vlan 11
SW1(config-vlan)#name Personel
SW1(config-vlan)#exit
SW1(config)#vlan 12
SW1(config-vlan)#name Misafir
SW1(config-vlan)#exit
SW1(config)#vlan 13
SW1(config-vlan)#name Test
SW1(config-vlan)#exit
```

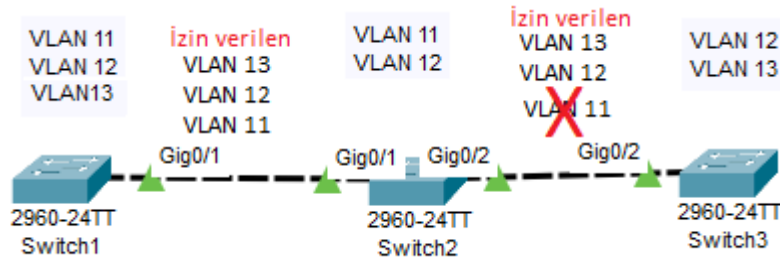
- VLAN oluşturulduktan sonra bu VLAN'a atamak istenen portların arayüzlerine giriş yapılarak, bağlanacak cihazın tipine göre Trunk veya Access moduna alınması gerekiyor.  
|→ İstemci bağlanacak portlar için "**switchport mode access**" komutuyla önce port access moduna alınıyor. Ardından "**switchport access vlan <VLAN ID>**" komutuyla port bir VLAN'a atanıyor.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 11
SW1(config-if)#exit
```

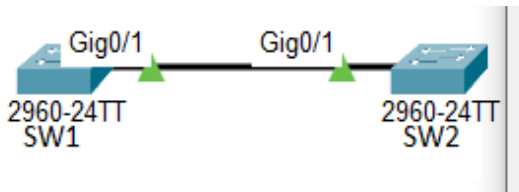
- |→ Switch veya access point gibi birçok VLAN trafiğini geçiren cihazlar için port Trunk moduna alınıyor. Trunk modu için ilgili portun arayüzüne giriş yapılarak sadece "**switchport mode trunk**" komutu kullanılıyor.

```
SW1(config)#interface fastEthernet 0/2
SW1(config-if)#switchport mode trunk
SW1(config-if)#exit
```

Cisco cihazlarda portlar trunk moduna alındığında varsayılanda bütün VLAN trafiğini geçirmektedir. Ne yazık ki bu durum istemci sayısının çok olduğu networkler için istenen bir durum değildir. Nedeni, bir VLAN içerisinde broadcast yayın yapıldığı zaman bu yayın her Trunk portundan iletilecektir. Yayının iletildiği switch üzerinde yayın yapılan VLAN'a ait port bulunmadığı zamanlarda gelen trafik sadece switchin portunu gereksiz yere meşgul edecektir. Yani Switch3 üzerinde broadcast yayın yapılan VLAN11'e ait port olmadığı için frame'in Switch2-Switch3 arasında kullanılan bağlantıda drop edilmesi gerekiyor. Bu nedenle Trunk yapılandırılan portlarda sadece belirli VLAN'lara ait trafiğe izin verilmesi için "**switchport trunk allowed vlan <VLAN IDs>**" komutu kullanılıyor. Bu kısıtlamalar her iki switch'de de (karşılıklı olarak) aynı tanımlanmalıdır.



Cisco dışındaki switchlerde ise port trunk moduna alındığında varsayılanda bütün VLAN'lara izin verilmediği için portlar trunk moduna alınırken geçirilmesi istenen VLAN trafikerinin ayrıca tanımlaması gerekiyor. Tanımlamalarda ard arda VLAN numaraları girebilmek için aralara “,” işareti, belirli aralık belirtilirken ise “-” sembolü kullanılıyor (Bu tanımlama birbirine bağlı her iki switch üzerinde de uygulanmalı).



```
SW1(config)#
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan 11,12-13
SW1(config-if)#exit
SW1(config)#
```

Trunk moduna alınan portta çok fazla VLAN için tanımlama yapıldığı durumlarda tanımlanan VLAN'lar arasında yeni VLAN eklemek veya çıkarmak için “**switchport trunk allowed vlan remove <VLAN IDs>**” veya “**switchport trunk allowed vlan add <VLAN IDs>**” komutları kullanılabilir. Ekleme yapılmak istendiğine sadece “**allowed vlan <VLAN IDs>**” komutu kullanılırsa daha önce tanımlanan VLAN'lar geçersiz sayılacaktır. Son durumda portta tanımlanan konfigürasyonlar için “**show running-config**” komutu çalıştırılarak konfigürasyonlar görülebilir.

```
SW1(config)#vlan 14
SW1(config-vlan)#vlan 15
SW1(config-vlan)#vlan 16
SW1(config-vlan)#exit
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport trunk allowed vlan remove 11
SW1(config-if)#switchport trunk allowed vlan remove 12
SW1(config-if)#switchport trunk allowed vlan add 14
SW1(config-if)#switchport trunk allowed vlan add 15
SW1(config-if)#switchport trunk allowed vlan add 16
SW1(config-if)#exit
```

```
interface GigabitEthernet0/1
  switchport trunk allowed vlan 11-13
  switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
```

Before

```
interface GigabitEthernet0/1
  switchport trunk allowed vlan 13-16
  switchport mode trunk
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  shutdown
```

After

SORU: Switch portlarına atanmış bir VLAN silindiğinde (“**no vlan <VLAN ID>**”) port nasıl davranır?

Kullanılan bir VLAN silinirse, portların konfigürasyonları silinmez. Potlardaki konfigürasyonlar duruyor olsa da switch üzerinde tanımlı bir VLAN olmadığı için portlara hiçbir trafik yönlendirilmez. Yani portlar, silinen VLAN yeniden oluşturulana kadar bloklanır.

**DTP (Dynamic Trunking Protocol)**, tanımlandığı portlarda karşısına bağlanan cihazın türünü tespit ederek kendi portundaki modu Access veya Trunk olarak otomatik seçilmesini sağlayan protokoldür. Bu protokol bir güvenlik zafiyeti olarak görülüyor. Nedeni bir saldırganın DTP moduna alınmış bir porta bağlanıp kendini bir switch gibi göstererek portun trunk moduna alınmasını sağlayabiliyor. Bu sayede bütün VLAN trafiğini kendi üzerine alarak dinleyebiliyor. Saldırgan networkteki bütün VLAN trafiğini dinlemekle kalmayıp ayrıca istediği türde paketler oluşturup içine VLAN bilgilerini ekleyerek bütün VLAN'lere erişim sağlayabiliyor.

Varsayılanda switchlerde bütün portlar DTP (dynamic auto) modundan gelmektedir. **Bu durumun güvenlik problemi oluşturmaması için VLAN yapılandırmalarında bütün portlar mutlaka Access moda alınmalıdır. Access moduna almak yerine doğrudan DTP protokolü kapatılmak isteniyorsa ilgili arayüze girilerek "switchport nonegotiable" komutu kullanılıyor.** DTP ptotolölü açılmak istendiğinde ise ilgili portun arayüzünde girilerek "**switchport mode dynamic auto**" komutu kullanılıyor.

```
SW1(config)#interface range fastEthernet 0/1-24
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#exit
```

DTP protolölünün Auto ve Desirable olma üzere iki modu bulunmaktadır.

- Auto modu çekinik/pasif (kendisini Trunk moda çekmek konusunda) mod olarak görülebilir. Yani karşısına Desirable modunda veya Trunk modunda bir port olmadığı sürece kendisini access moduna alan moddur.
- Desirable modu, dominant/aktif (kendisini Trunk moda çekmek konusunda) mod olarak görülebilir. Karşısına Access moduna alınmış bir port gelmediği sürece kendisini Trunk moduna alan moddur.

SORU: Neden iki VLAN'in aralarında haberleşmesi istenir?

Örnek olarak bir kurumda network yöneticileri farklı bir VLAN'da bulunurken, Management VLAN farklı bir VLAN'de bulunuyor. Yani network yöneticilerinin bulunduğu VLAN ile Management Vlan haberleştirilmediği sürece network yöneticileri cihazlara uzak erişim kurup konfigürasyon yapamazlar.

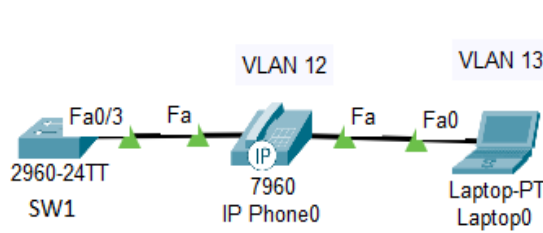
## NOT

- Varsayılanda switchlerde Native VLAN, VLAN 1'de geliyor. Aynı zamanda varsayılanda bütün portlar da VLAN 1'de geliyor. Bu sayede switchlerde herhangi bir konfigürasyon yapılmadan iki switch birbirine bağlandığında framelere başlık bilgisi eklenmeden switchler arasında iletilmesi sağlanıyor.
- VLAN 1 varsayılanda gelir, adı "default" 'tur ve silinemez.
- Switch portları varsayılanda VLAN 1 de geldiği için VLAN kullanımı 2'den başlanarak verilmesi ve Native VLAN'in farklı bir VLAN'a alınması tavsiye ediliyor. Nedeni, switchin boş portuna bağlanan bir istemci doğrudan VLAN 1 'deki cihazlara erişebilir hale geliyor.
- Normalde VLAN tanımlamalarında 1-40945 arasında VLAN numarası seçilebiliyor ama 1-1005 arası değerler (1002-1005 eski L2 teknolojileri için rezerve edilmiş ama kullanılmıyor) normal aralık olarak görülürken, 1006-4095 aralığı genişletilmiş aralık olarak görülüyor.

| -> Normal aralıkta tanımlanan VLAN konfigürasyonları flash hafızada "vlan.dat" ismiyle tutuluyor.

| -> VTP özelliği, normal aralıkta tanımlanan VLAN'larda kullanılabilirken, genişletilmiş aralıkta daha az özelliği destekliyor. Ayrıca genişletilmiş aralıkta VTP kullanabilmek için ek konfigürasyonlar yapılması gerekiyor.

- Kurumlarda kablolama işlemi duvar içlerinden yapılır. Kablolama işleminde kullanıcılara Voice VLAN ve Data VLAN için tek bir kablo da çekilebilirken iki ayrı kablo da çekilebiliyor. Tek kablo kullanıldığında, IP telefonların içinde gömülü gelen küçük bir switch yardımıyla IP telefon ve bilgisayar farklı VLAN'lara atanarak birbirinden izole kullanılabiliyor.



```
SW1(config)#interface fastEthernet 0/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 13
SW1(config-if)#switchport voice vlan 12
SW1(config-if)#exit
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
SW1(config)#
```

- Bir porta atanmış VLAN'ı kaldırmak için o portun arayüzüne girip portu VLAN'a atamak için kullanılan komutun başına "no" ekleyerek gerçekleştirilebiliyor.

```
SW1(config)#interface fastEthernet 0/1
SW1(config-if)#no switchport access vlan 11
SW1(config-if)#exit
```

- Oluşturulan bir VLAN'ı silmek için ise "no vlan" komutu kullanılıyor.

```
SW1(config)#no vlan 11
SW1(config)#do show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
12	Misafir	active	
13	Test	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

- Switch üzerindeki bütün VLAN konfigürasyonunu silmek için Privileged Exec modunda "delete vlan.dat" komutundan sonra "reload" komutuyla switch yeniden başlatılması gerekiyor.

```
SW1#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
SW1#reload
```

- VTP ve VTP Pruning özelliği aktive edilerek de hangi VLAN'ların hangi portlardan gönderileceğine otomatik karar verilmesi sağlanabiliyor. Bu sayede ihtiyaç duyulmayan VLAN trafikleri trunk portlarından bloklanıyor.
- Switchlerde tanımlanan VLAN yapılandırılmaları flash hafızada "vlan.dat" ismiyle tutuluyor. Bu nedenle "show running-config" veya "show startup-config" komutları kullanılarak oluşturulan VLAN'ler görüntülenemez (Sadece bir port VLAN'a atanırsa bu yapılandırma görünür). VLAN yapılandırmalarını görebilmek için "show vlan" komutu kullanılıyor. "vlan.dat" dosyası silindiğinde switch üzerinde tanımlanmış VLAN yapılandırmalarının tamamı silinir.



## Terminolojiler

- Management VLAN, switch yönetimi için kullanılan VLAN'e deniliyor. Yani switchlerde ip adresini atamak için seçilen VLAN'lere deniliyor.
- Data VLAN, veri haberleşmesinin gerçekleştiği her VLAN data VLAN'dir.
- Voice VLAN, ip telefonlar için kullanılan VLAN'lere deniliyor. Ip telefonlarda güvenlik ve minimum gecikme gibi nedenlerden dolayı farklı bir VLAN'e alınır ve bu VLAN trafiğine öncelik verilir. Konfigürasyonu için ip telefon bağlanan portun arayüzüne girilerek "**switchport voice vlan <VLAN ID>**" komutu kullanılır.
- Native VLAN, normalde VLAN'lar trunk portundan iletilirken kaynak switchlerde framelere 802.1q etiketi ekleniyordu. Native vlan ise trunk potundan etiket kullanmadan frame iletiminin sağlanmasıdır. Bu sadece tek bir VLAN için yapılabilir. Switch 802.1q etiketi olmayan bir frame geldiğinde switch bunu native VLAN olarak değerlendiriyor ve native VLAN için tanımlanmış portlarına iletiyor. Varsayılanda native VLAN, VLAN 1 de geliyor. İstenirse bu özellik trunk moduna alınan portun arayüzünde "**switchport trunk native vlan <VLAN ID>**" komutu kullanılarak değiştirilebilir. **Burada dikkat edilmesi gereken konulardan biri, native VLAN bilgisinin networkteki switchlerin birbirine bağlı portlarında aynı tanımlanması gerekiyor (Native VLAN bilgisi Trunk portlara özel tanımlanıyor. Yani aynı switch üzerindeki farklı Trunk portları farklı Native VLAN bilgilerine sahip olabilir. Önemli olan karşılıklı bağlanan portlar aynı Native VLAN bilgisine sahip olmalı).** Aksi taktirde iki VLAN trafiği birbirine girecektir.

```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 11
SW1(config-if)#exit
```

- VTP (Vlan Trunking Protocol), VLAN tanımlarının (oluşturma – silme – isim değiştirme) topolojideki diğer switchlere de otomatik tanımlanmasını sağlayan bir protokoldür. Örnek olarak bir switch'de VLAN oluşturulduğunda bu VLAN VTP protokolü devredeyse bütün switchlere öğretiliyor/oluşturuluyor. Benzer şekilde silme ve benzeri değişiklikler uygulandığında bunu bağlı switchlerde de otomatik olarak tanımlıyor. Yani her switchde ayrıca tanımlamaya gerek kalmıyor. Bu özellik kullanılarak büyük topolojilerde VLAN konfigürasyonlarının çok daha hızlı yapılmasını sağlıyor (Detaylar CCNP Encore notlarında ...).

## Kontrol Komutları

- show vlan
- show vlan brief
- show interface vlan
- show interface <Interface ID> switchport
- show vlan <VLAN ID>, vlan detaylarını verecektir.
- show interface trunk
- show dtp interface <Interface ID>