VLAN

Vlan, bir network'ü mantıksal daha küçük ağlara bölmek için kullanılan teknolojidir. Aynı işi yapan istemcileri gruplamak olarak da görülebilir. Bu sayede;

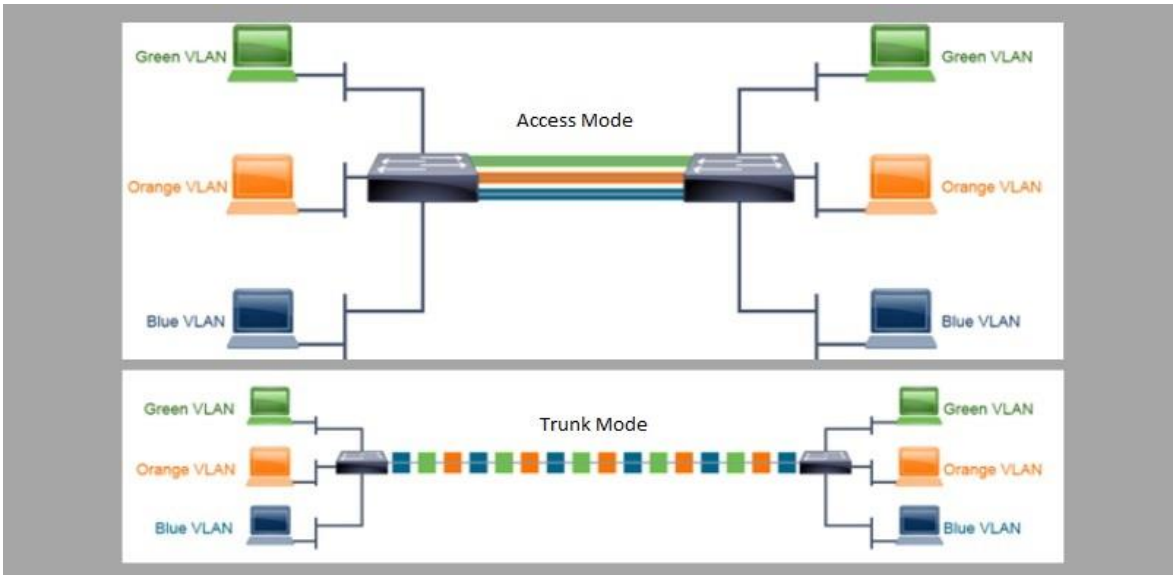
- Networkteki broadcast domainler küçülür ve trafik yükü azaltır.
- Oluşan sanal networkler arası bir noktaya kadar güvenlik sağlar.
- Switchler üzerinde sanal networkler oluşturulduğu ve oluşturulan sanal networkler port bazlı gruplandırılp kullanıldığı için VLAN kullanılmayan duruma kıyasla switch sayısı çok daha az olacaktır. Bu durum IT operasyonlarıı kolaylaştırırlem, network maliyetini de azaltmaktadır.
- Fiziksel olarak farklı konumlarda bulunan cihazlar için uzun kablolamalar yapmak yerine o konuma yakın bir switch portuna bağlayarak istenilen sanal networke dahil edilebilmektedir. Bu duruma örnek olarak yazıcı türü ortak kullanılan cihazlar verilebilir.

Vlan için switchlerde Access ve Trunk olmak üzere iki mod kullanılıyor.

Access mod, bilgisayar, laptop gibi istemcilerin bağlandığı portlarda tanımlanan moddur. Access moduna alınan portlar tek bir VLAN için hizmet verir. Access moduna alınan portlarda framelere herhangi bir etiket bilgisi eklenmeden veri iletimi sağlanıyor.

Trunk modu, farklı switchlerde oluşturulan aynı VLAN'ların aralarında haberleşebilmesi gerekiyor. Bu haberleşme her VLAN için iki switch arasında access moduna alınmış portlardan birer kablo çekilerek aynı VLAN'a dahil cihazların haberleşmesi sağlanabilir ama bu durum çok fazla VLAN olması durumunda switch'in portlarının gereksiz kullanılmasına neden olacaktır. Trunk , birden fazla VLAN trafiğini tek bir port üzerinden geçmesini sağlayan moddur. Bu sayede gereksiz port kullanılmadan aynı VLAN'a dahil cihazlar farklı switchler üzerinde de olsa aralarında haberleşebilmektedir.

|-> Trunk switchler arasından farklı VLAN'lara ait framlerin iletimini, IEEE tarafından çıkarılan 802.1q protokolü kullanarak gerçekleştiriyor (Bu haberleştirme ilk olarak Cisco tarafından çıkarılan ISL (Inter Switch Link – 29 bayt başlık bilgisi eklenir) teknolojisiyle gerçekleştirilmeye başlanmıştır.). Trunk yapılandırılan portu üzerinden geçen ethernet frame'lerinin içerisine VLAN bilgilerini içeren 4 baytlık yeni bir başlık bilgisi ekliyor. Kaynak switch'den çıkarken eklenen bu başlık bilgisi hedef switch'e ulaştığında çıkarılıyor ve başlık bilgisine göre switchdeki ilgili potlara iletilmesi sağlanıyor.



802.1Q Etiket İçeriği;

|->Type, VLAN etiketi olduğunu belirten alandır.

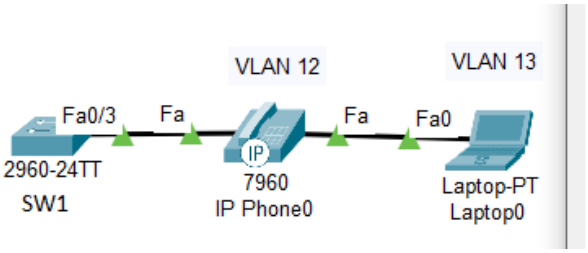
|->User Priority, öncelik numarası. QoS için kullanılıyor. Örnek olarak Ip telefon trafiği, yönlendirme protokollerinin trafiğine öncelik verilebiliyor. Bu özellik vlan oluşturulduğunda gelmiyor. Ayrıca yapılandırılması gerekiyor. (öncelik verilmek istenen VLAN için bu değerin 0 dan büyük olması, bu VLAN trafiğine öncelik veirlmesi için yeterli.)

|->CFI (Cannonical 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.

NOT

- Varsayılanda switchlede 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 varsyılanda VLAN 1 de geldiği için VLAN kullanımı 2'den başlanarka verilmesi ve ntive VLAN'in farklı bir VLAN'a alınması tavsiye ediliyor. Nedeni, switchin boş portuna bağlanan bir istemci doprudan 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 rzerve 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 özellikliği, normal aralıkta tanımlanan VLAN'larda kullanılabilirken, genişletilmiş aralıkta daha az özelliği destekliyor. Ayrıca genişletilmiş aralıkta VTP kullanabilmek için ek konfigürasyonlar yapılması gerekiyor.
- Switchlerde tanımlanan VLAN yapılandırmaları 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 yapılandırmaların tamamı silinir.
- Kurumlarda kablolama işelmi 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)#
```

Öğrenilen Terminolojiler

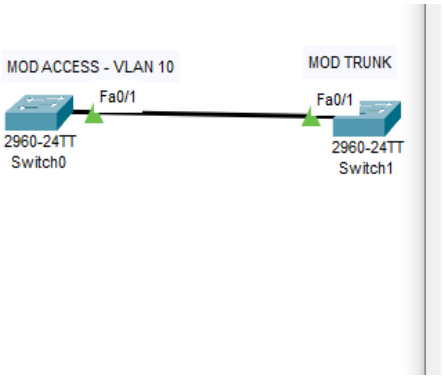
- Management VLAN, switch yönetimi için kullanılan VLAN'e deniliyor. Yani switchlerde ip adresini atamak için seçilen VLAN'lere deniliyor.
- Data VLAN, veri haberleşmesinin gerçekleştiği her VLAN data VLAN'dir.
- Voice VLAN, ip telefonlar için kullanılan VLAN'lere deniliyor. Ip telefonlarında güvenlik ve minimum gecikme gibi nedenlerden dolayı farklı bir VLAN'e alınır ve bu VLAN trafiğine öncelik verilir.
- 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 yapılabiliyor. Switche 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 " komutu kullanılarak değiştirilebiliyor. Burada dikkat edilmesi gereken konulardan biri, native VLAN bilgisinin networkteki switchlerin birbirine bağlı portlarında aynı tanımlanması gerekiyor. Aksi taktirde iki VLAN trafiği birbirine girecektir.

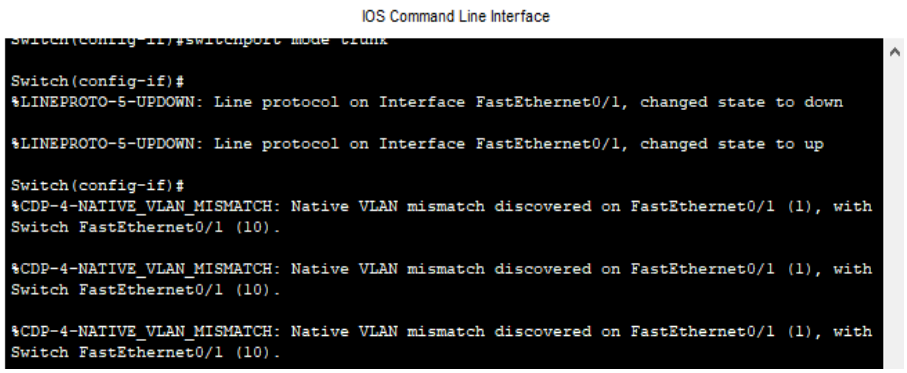
```
SW1(config)#interface gigabitEthernet 0/1
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport trunk native vlan 11
SW1(config-if)#exit
```

- VTP (Vlan Trunking Protocol), VLAN konfigürasyonlarının 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 sağlamaktadır.

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

Farklı vlanlara atanmış portlar birbirine bağlanırsa, bağlanılan portlardaki VLAN'lari birbirine geçirmiş oluruz. Yani portlar access modunda tanımlandığı için portlar arasında frameler iletilirken başlık bilgisi eklenmiyordu. Bu nedenle access moduna alınan portlardan çıkan framelerde VLAN bilgisi bulunmayacaktır. 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'te 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 frameleri 802.1q başlığı eklemeden göndereceği için trunk moduna alınan switchde framele native vlan'a atanmış portlarına anahtarlanacaktır. Trunk moduna alınan switchden ise bütün VLAN trafiği gönderilecektir ama sadece access mod tanımlanan switch'de portun atandığı vlan trafiğine izin verilecektir.

VLAN Konfigürasyonu

- VLAN konfigürasyonu için öncelikle switchlerde global konfigürasyon modunda “vlan” komutuyla VLAN oluşturulmalı. Ardından “name” komutuyla oluşturulan VLAN’a İsim de verilebilir.

```
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
```

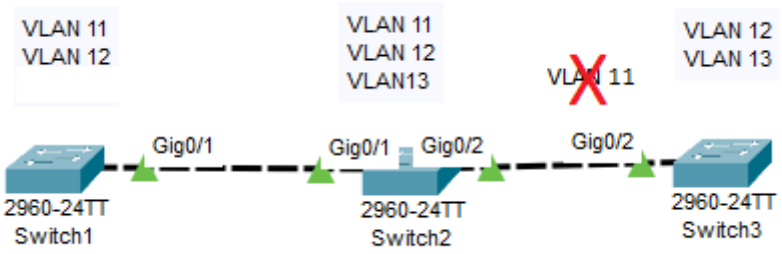
- VLAN oluşturuldutan sonra bu VLAN’a atamak istenen portların arayüzlerine giriş yapılarak, bağlanacak cihazın tipine göre trunk veya access moduna alınması gerekiyor.
  |-> İstemci bağlanacak portlar için “switchport mode access” komutuyla önce port access moduna alınıyor. Ardından “swtchport access vlan” 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
```

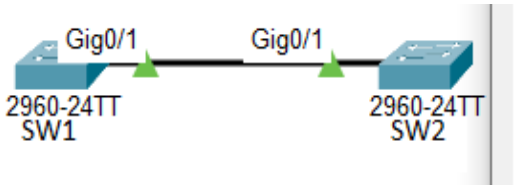
|-> Switch veya access point gibi birçok VLAN trafiğini geçiren cihazlar için port trunk moduna alınıyor. Trunk modu için ilgili portun arayüzüne giriş yapılarak sadece “switchport mode trunk” komutu kullanılıyor.

```
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 içinde 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 switch üzerinde yayın yapılan VLAN2’a ait port olmadığı için frame drop edilecektir. Bu nedenle trunk yapılandırılan portlarda sadece belirli VLAN’lara ait trafiğe izin verilmesi için "switchport trunk allowed vlan" komutu kullanılıyor. Bu tanımlamalar her iki switchde de karşılıklı olarak yapılandırılmalı.



Cisco dışındaki swtichlerde ise port trunk moduna alındığında varsayılanda bütün VLAN'lara izin verilmediği için portlar trunk moduna alınırken geçirilecek VLAN trafikleri ayrıca tanımlaması gerekiyor. Tanımlamalarda VLAN numaraları aralara "," işareti koyularak sıralanabilirken, "-" işareti kullanılarak bir aralık da belirtilebiliyor. Bu tanımlama birbirine bağlı iki switchde de yapılmalı.




```
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 veye çıkarmak için "switchport trunk allowed vlan remove" veya "switchport trunk allowed vlan add" komutları kullanılabiliyor. 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

NOT

- 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.
- 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 silemk 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 "delete vlan.dat" komutundan sonra "reload" komutuyla switch yeniden başlatılarak kullanılıyor.

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

SW1#reload
```

SORU: Swiitch portlarına atanmış bir VLAN silindiğinde (no vlan) port nasıl davranır?

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

DTP (Dynamic Trunking Protocol), tanımlandığı portlarda karşısına bağlanan cihazın tipini tespit ederek kendi portundaki modu "access" veya "trunk" olarak otomatik seçilmesini sağlayan protokoldür. Bu protokol bir güvenlik zafiyeti olarak görülüyor. Nedeni bir saldırganın kendini bir DTP moduna alınmış bir porta bağlanıp kendini bir switch gibi göstererek, portun trunk moduna alınmasını sağlaması ve bu sayede bütün VLAN trafiği monitör edebilmesini sağlayabilmesidir. Saldırgan netwotkteki bütün VLAN trafiğini izlemekle kalmayıp ayrıca bir paket oluşturup içine VLAN bilgilerini ekleyerek bütün VLAN'lere erişim sağlayabilir. Varsayılanda switchlerde bütün portlar DTP (dynamic auto) modundan gelmektedir. Bu durumun güvenlik problemi oluştutmaması için VLAN yapılandırmalarında bütün portlar mutlaka "access" moda alınmalıdır. Access moduna almak yerine doğrudan DTP protokolü kapatılmak isteniyorsa ilgili arayüze girilerek "switchport nonegotiable" komutu kullanılıyot. DTP ptotololü 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 protololünün 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.

Kontrol komutları

- show vlan
- show vlan brief
- show interface vlan
- show interface fa 0/1 switchport
- show vlan id, vlan detaylarını verecektir.
- show interface trunk
- show dtp interface fa 0/1

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.

Switchler arası iki trunk mod kullanılarak portlar yedeklendirilebiliyor mu?

Double tagging,

Vlan Hopping,