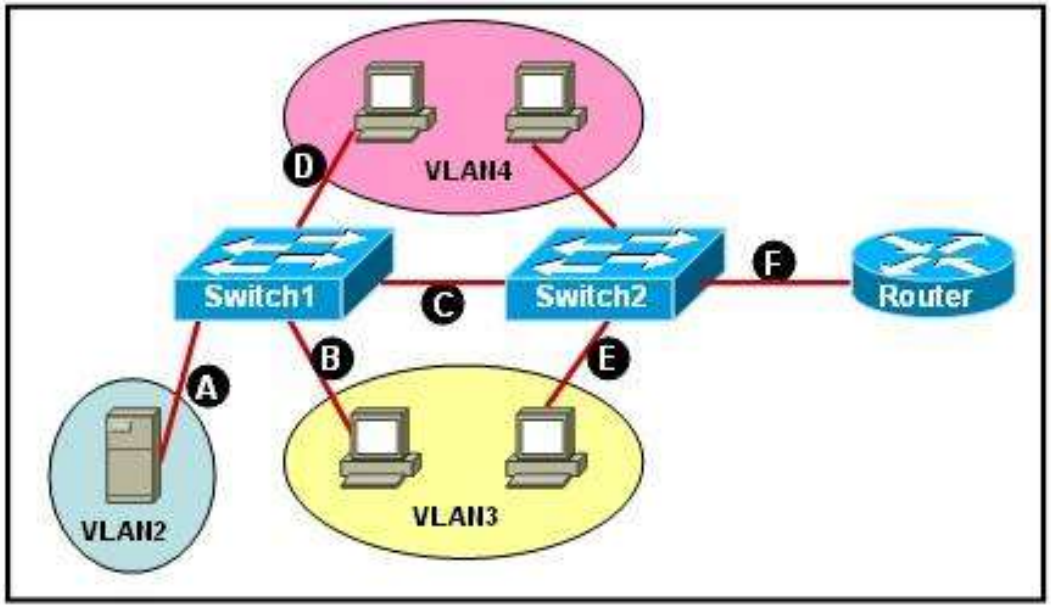
VLAN

Sanal LAN

Virtual Local Area Network (VLAN)

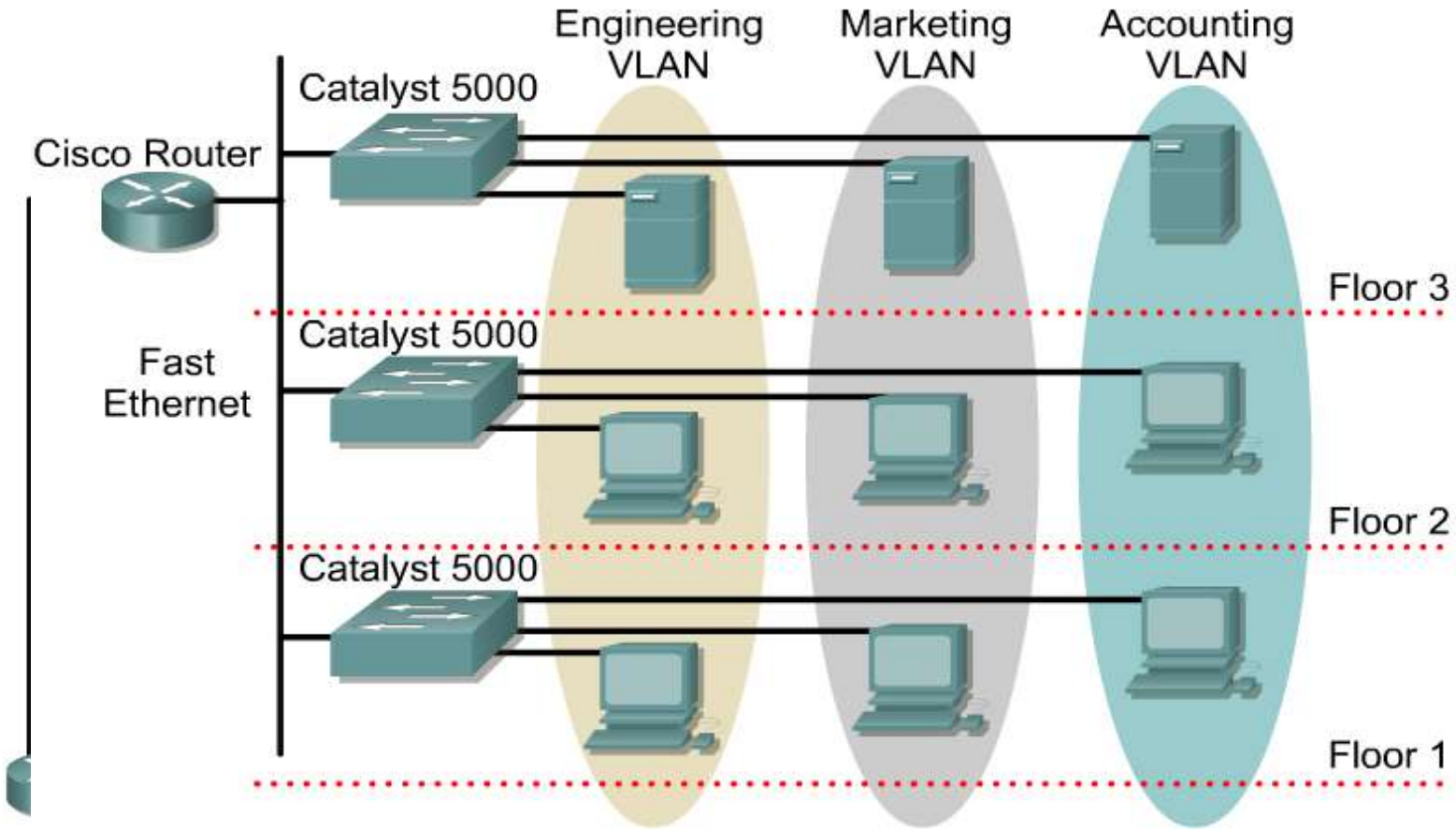
- VLAN'ın açılımı **«Virtual Local Area Network'tur».** Türkçesi ise Sanal Yerel Alan Ağları'dır. IEEE tarafından geliştirilmiştir.
- VLAN OSI 2. katmanda çalışır (Layer 2). VLAN, bu teknolojiyi destekleyen cihazlar üzerinde mantıksal ağlar oluşturma işlemidir.
- VLAN, yerel alan ağı üzerindeki ağ kullanıcılarının ve kaynaklarının mantıksal olarak gruplandırılması, farklı broadcast domainlere atanması ve ağ cihazları üzerinde farklı portlara atanması ile uygulanır.
- VLAN ölçeklenebilirlik, güvenlik ve ağ yönetimi için yapılandırılır.
- VLAN kullanılan bir ağda, bir VLAN'da bulunan kullanıcılar sadece kendi broadcast domain'ine sahip olacağından, birbirleri ile haberleşebilirler. Oluşturulmuş farklı bir VLAN'da bulunan kullanıcılar ile iletişim kuramazlar. Büyük ağlarda VLAN ihtiyacı işte bu sebepten dolayı ortaya çıkmış ve Network Mühendisleri'ni büyük bir zahmetten kurtarmıştır.

VLAN (Virtual LAN)

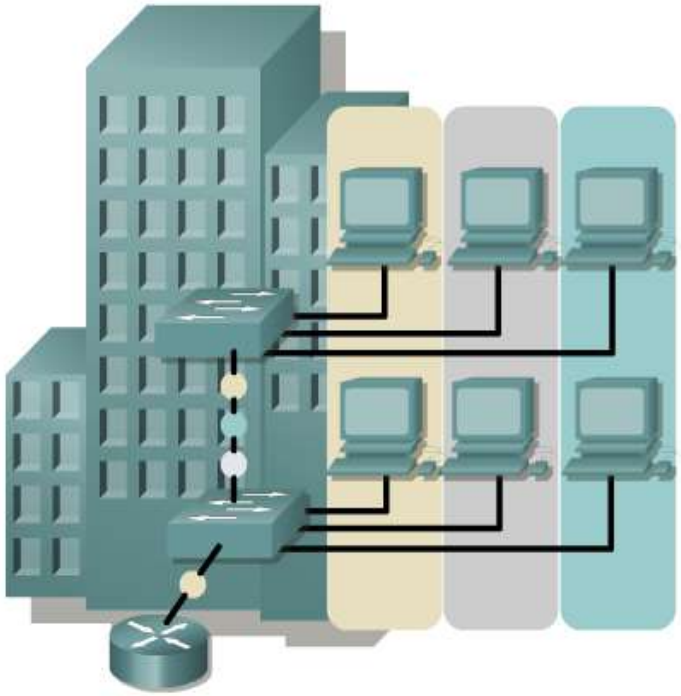


VLAN'lar Farklı veya aynı swithclerin (2.Katman) farklı portlarına bağlı hostlar ile bir broadcast domaini (farklı Subnet'te denebilir- veya mantıksal ağlar) oluşturmasına izin verir.

Farklı VLAN'lere üye olan bilgisayarlar ağ üzerinden birbirlerine erişemezler. Bir VLAN'in ARP isteği diğer VLAN'lere normalde hiçbir şekilde ulaşamaz. Çünkü herbir VLAN farklı bir "broadcast domain"idir.



- VLAN'lanlar Broadcast domainİ temelli segmentasyon sağlarlar.
- Fiziksel konum ve bağlantıdan bağımsız olarak; bir özel workgrup tarafından kullanılan workstationlar ve sunucular benzer VLAN'ın üyesidir. Bu LAN'ı paylaşırlar.

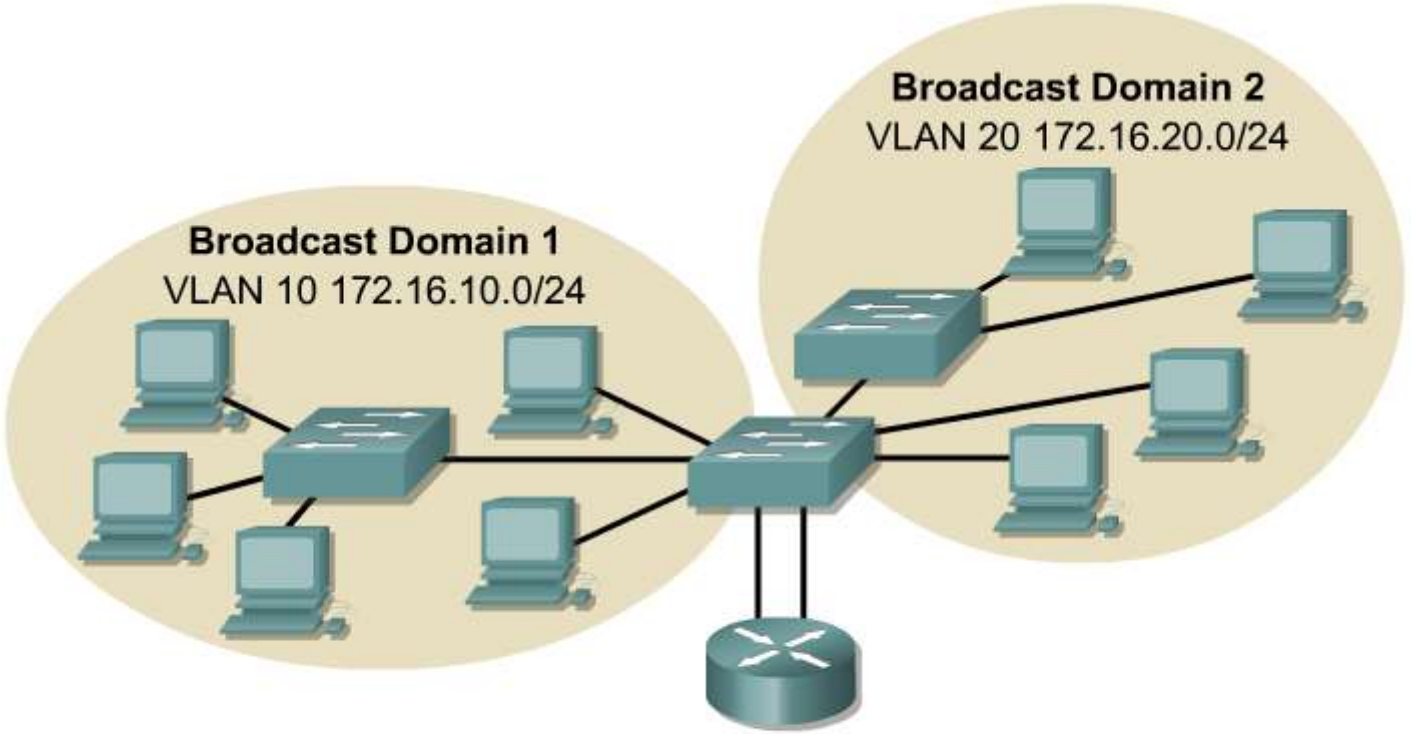


- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- VLAN geleneksel LAN yapılandırmalarında, fiziksel router tarafından sağlanan segmentasyon hizmetlerini sağlamak için oluşturulur.
- VLAN topolojilerinde ki RouterLar yayın filtreleme, güvenlik ve trafik akış yönetimi sağlar.
- Switchler, VLAN yayın alanı bütünlüğünü ihlal edecek şekilde, VLAN'lar arasında herhangi bir trafiğe köprü olmamaldır.

VLAN’ların kontrol broadcast sahaları

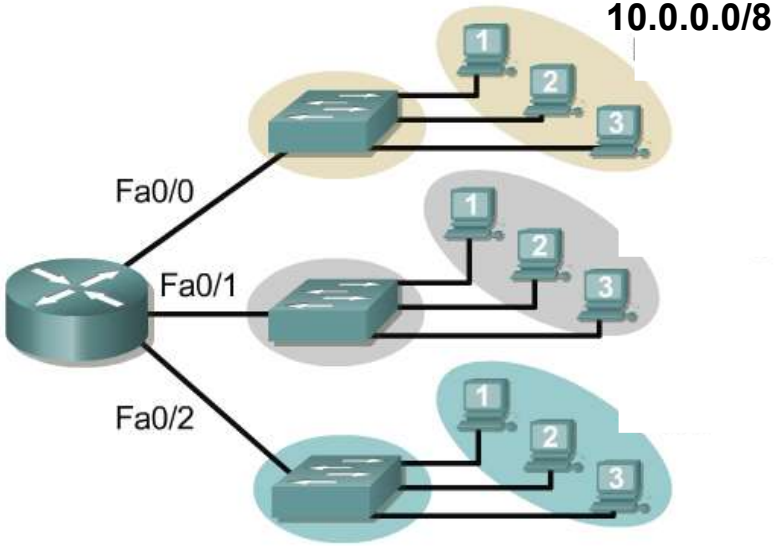
Trafik sadece VLAN’lar arasında Router’lar ile yönlendirilmelidir



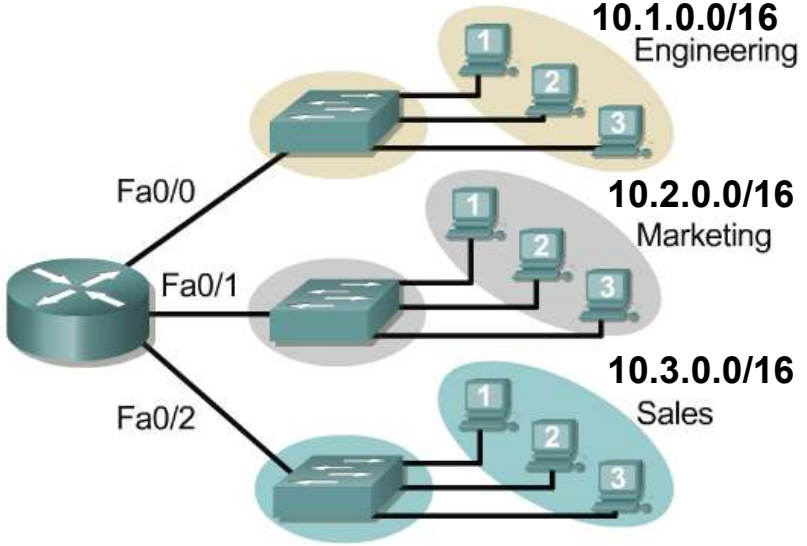
VLANs plus routers limit broadcasts to the domain or origin.

VLAN'lı ve Routerlı Broadcast Domain

1) VLAN'sız (Routerlar ile)



2)VLAN'lı veya VLAN'sız



1) VLAN yok.. Başka bir değişle bir adet VLAN. Tek IP network.

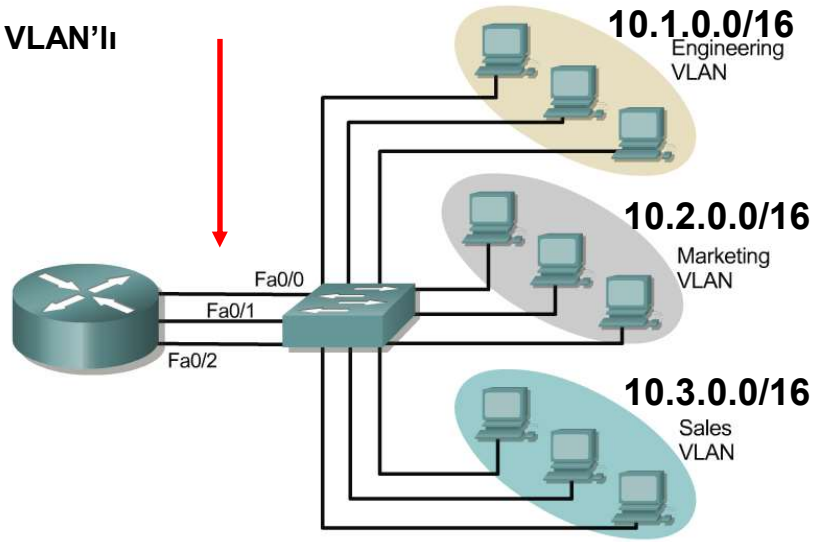
2) VLAN'lı veya VLAN'sız. Routerın farklı arayüzlerine bağlı Switchlerin herbiri için bi r VLAN denebilir.

3) VLAN'ların oluşturulması. Switch uygun VLAN'lar oluşturmak için konfigüre edilir.

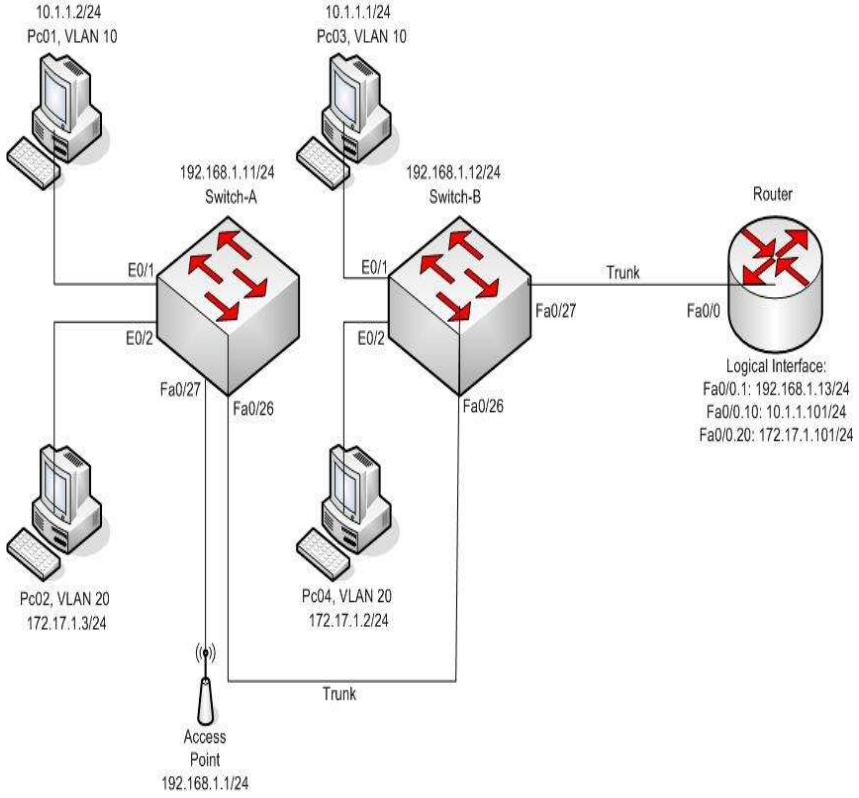
- Herbirinde kaç broadcast domain mevcuttur?

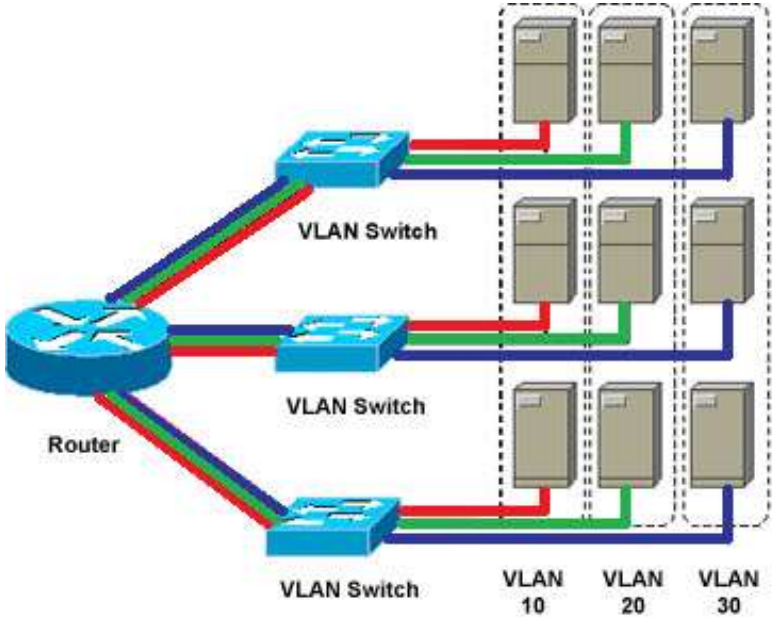
One link per VLAN or a single VLAN Trunk (later)

3) VLAN'lı

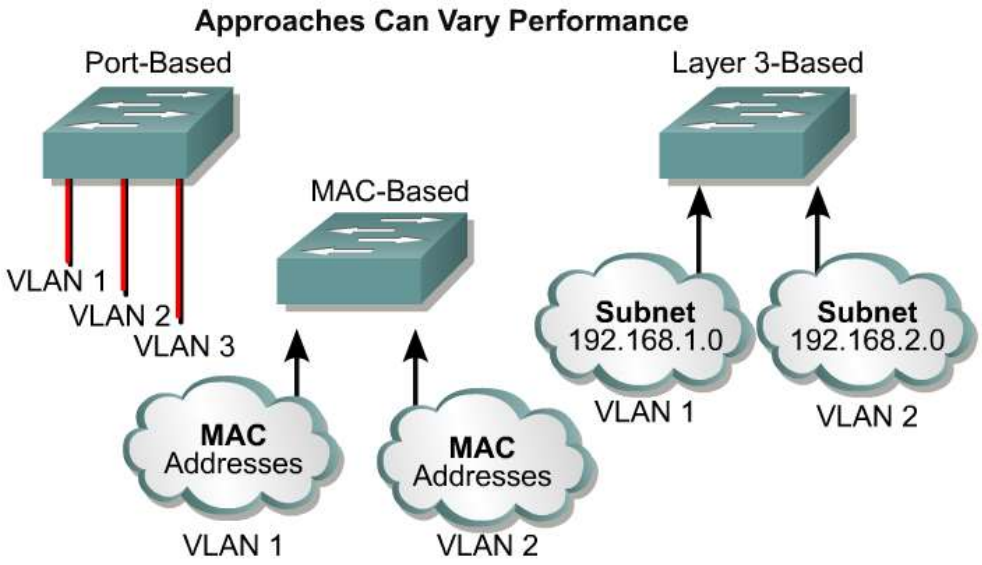


- VLAN’lerin birbirlerine erişebilmeleri için, VLAN arayüzleri oluşturmak, bu arayüzlere birer IP numarası vermek ve sonrasında da “Inter-VLAN routing (VLAN’ler arası yönlendirme)” yapmak gerekir.
- Bunun için de ya bir yönlendiriciye ya da yönlendirici özelliği bulunan bir anahtarlama (3.katman Switch) cihazına ihtiyaç vardır.





VLAN Tipleri



VLAN Types	Description
Port-based	- Yaygın bir konfigirasyon metodudur. - Portlar tek olarak , guruplar halinde veya satırlar halinde veya çaprazlama olarak VLAN 'lara atanır. - Bu yapıda, Portardaki hostlara DHCP protokolu ile IP atanır.
MAC address	-Günümüzde az gerçekleştirilir. -Herbir MAC adresi Switche girilip bireysel olarak konfigüre edilmelidir. - Hata onarımı ve yönetimi zordur.
Protocol Based	-MAC adresleme gibi configure edilir, fakat IP adresleme kullnılır. -DHCP'den dolayı yaygındır.

VLAN Oluşturma tipleri

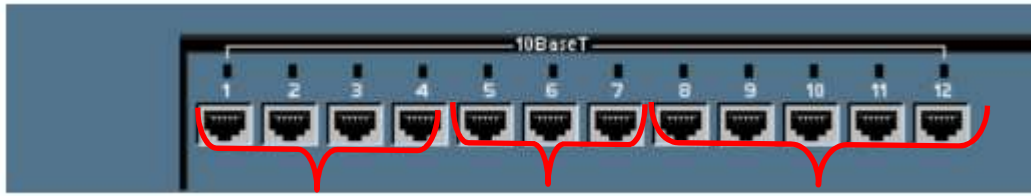
Configuring VLANs	Description
Statically	Network Yöneticisi portları kendisi konfigüre eder. Herbir port bir özel VLAN ile irtibatlandırılır. Network yöneticisi Vlan'lar ve portlar arası haritalamadan sorumludur.
Dynamically	Portlar, VLAN konfigirasyonu için dinamik rol oynar. VLAN haritalamasında MAC adresleriningyazılımsal veri tabanı kullanılır (Veri tabanını ağ yöneticisi ilk sefer oluşturur)

- Her bir switch portu farklı VLAN'a atanabilir.
- Benzer VLAN'lara atanan Portlar aynı Broadcast domain'ini kullanır.
- Farklı VLAN'lardaki portlar aynı Broadcast'i desteklemez.
- Dinamik VLAN oluşturma için yazılım: VLAN Management Policy Server VMPS

VLAN konfigirasyonu

```
Switch# show running-config
!
interface FastEthernet0/1
 switchport access vlan 50
!
interface FastEthernet0/2
 switchport access vlan 50
!
interface FastEthernet0/3
 switchport access vlan 50
!
interface FastEthernet0/4
 switchport access vlan 50
```

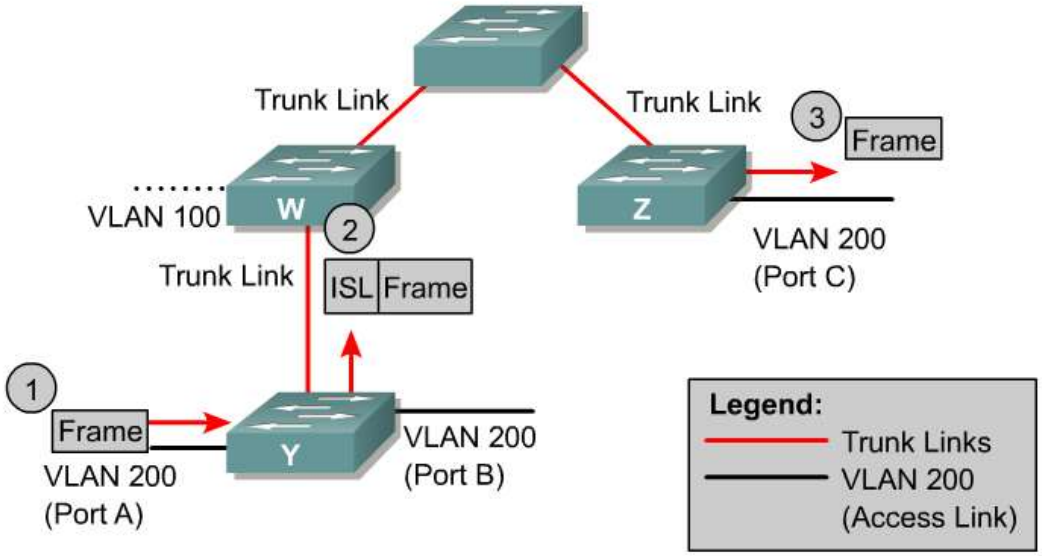
Statik VLAN Konfigirasyonu



vlan 1 default **vlan 2** **vlan 3**

```
SydneySwitch#show vlan

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------

VLAN Name                 Status    Ports
---- -------------------- ------- -------------------------------
1    default              active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
2    VLAN2                active    Fa0/5, Fa0/6, Fa0/7
3    VLAN3                active    Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                    Fa0/12
1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type SAID MTU  Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ---- ---- ---- ------ ------ -------- ---------- ------ -------
1    enet 100001 1500  -      -      -        -   -     1002   1003
2    enet 100002 1500  -      -      -        -   -     0      0
```

Access ve Trunk Bağlantıları (Links)



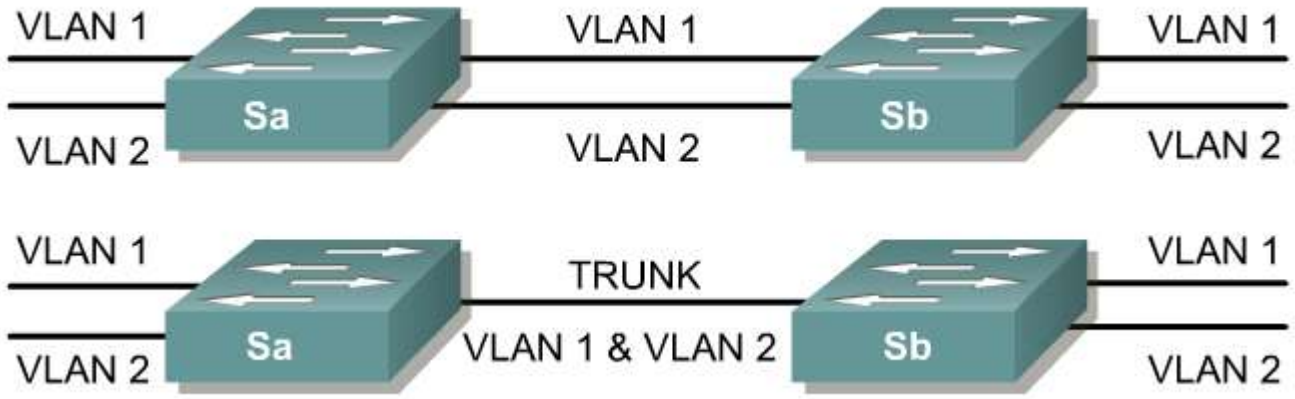
ISL maintains VLAN information as frames travel between switches on trunk links.

ISL: İnterSwitch Link.
ISL , switchler arasındaki trunk linklerinde seyahat eden çerçevelerin bilgilerini tutar.

Cisco switchlerin portları ya “access port” ya da “trunk port” olarak tanımlanabilirler. “access port”, bir adet VLAN’e (Native LAN) atanmış port olarak bilinir. “access port”ların, bağlı bulundukları VLAN haricindeki diğer VLAN portlarına erişimi yoktur.

Trunk Links

Without trunking



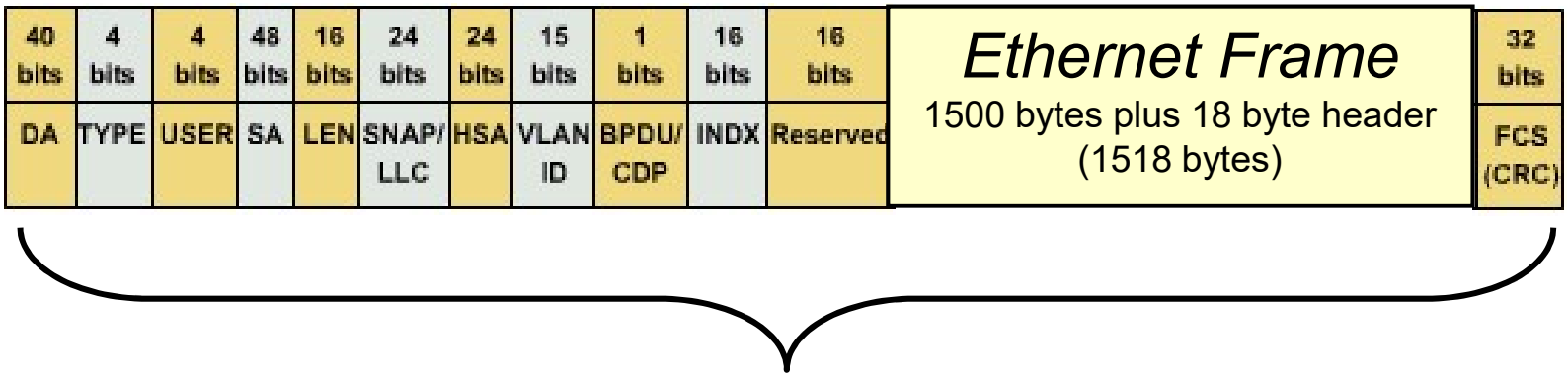
With trunking

“trunk port” ise Switch üzerinde yer alan tüm VLAN’lere üyedir ve farklı Switchler üzerinde tanımlı olan farklı VLAN’lere üye portların birbirleriyle iletişimini sağlar (Switchler arası veya Switch Router Arası)

ISL ve IEEE802.1Q

- Anahtarlar arasındaki trafiğin ayırt edilebilmesi için "trunk port", üzerinden geçen çerçevelere (frame) bir etiket eklenmelidir. Bu etiketleme mekanizması iki türlü yapılır. Bunlar;
- IEEE 802.1q etiketlemesi,
- ISL (InterSwitch Link) etiketlemesi : Sadece Cisco anahtarlarda çalışabilen etiketlemedir.
- Anahtarlar arası VLAN erişiminin sağlanması için anahtarları birbirine bağlayan "trunk port"ların aynı etiketleme türüne sahip olması gereklidir. (Karşılıklı bağlanmış olan "trunk port"ların ya IEEE 802.1q ya da ISL etiketli olması gereklidir.)

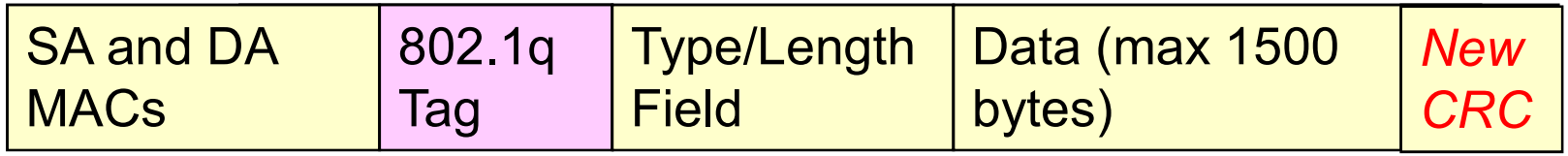
ISL (Frame Encapsulation)



Standart NIC kartları ve ağ cihazları bu büyük çerçeveyi tanımlayamaz. Bir Cisco switch bu çerçeveyi bir erişim Acces link portuna göndermeden önce bu kapsüllemeyi kaldırmalıdır.

802.1q

NIC kartları ve ağ cihazları bu çerçeveyi (1522 bayt) anlayabilir. Bununla birlikte, bir Cisco anahtarı, çerçeveyi bir erişim (acces) bağlantısına göndermeden önce bu kapsüllemeyi kaldırmalıdır.



2-byte TPID — Tag Protocol Identifier

2-byte TCI — Tag Control Info (includes VLAN ID)

Bir portu VLAN TRUNK olarak yapılandırmaya başlamadan önce, portun hangi kapsülleme protokollarını (IDL veya 802.1q) desteklediğini belirlemek gerekir:

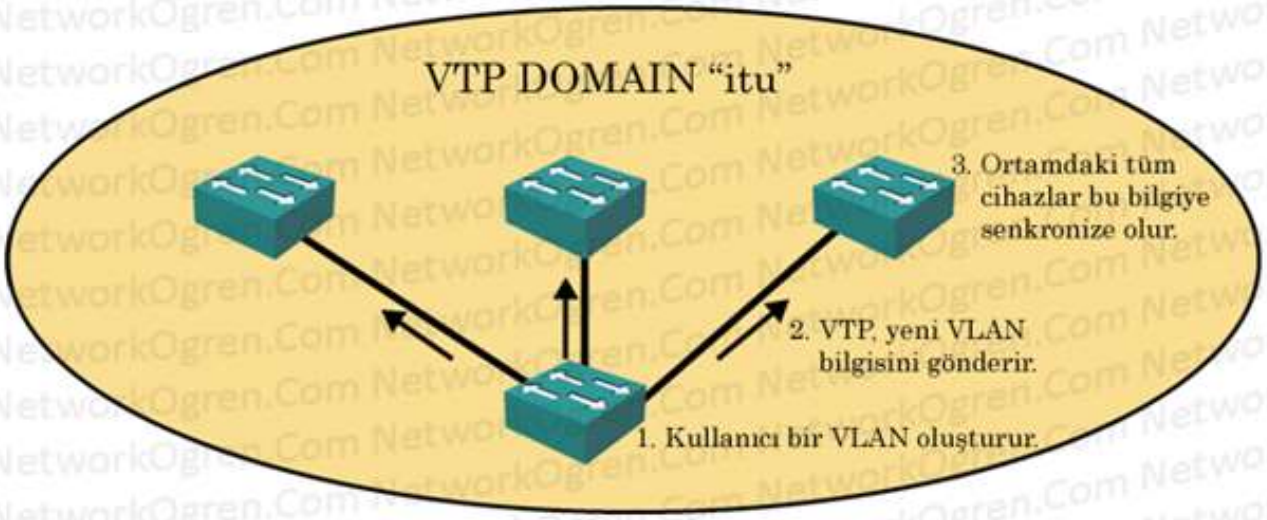
```
switch(config-if)# switchport trunk encapsulation ?
```

```
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode [access | multi | trunk]

Switch(config-if)# switchport trunk encapsulation
{isl|dot1q}

Switch(config-if)# switchport trunk allowed vlan remove
vlan-list
Switch(config-if)# switchport trunk allowed vlan add vlan-
list
```

By default, all VLANS, 1-1005 transported automatically

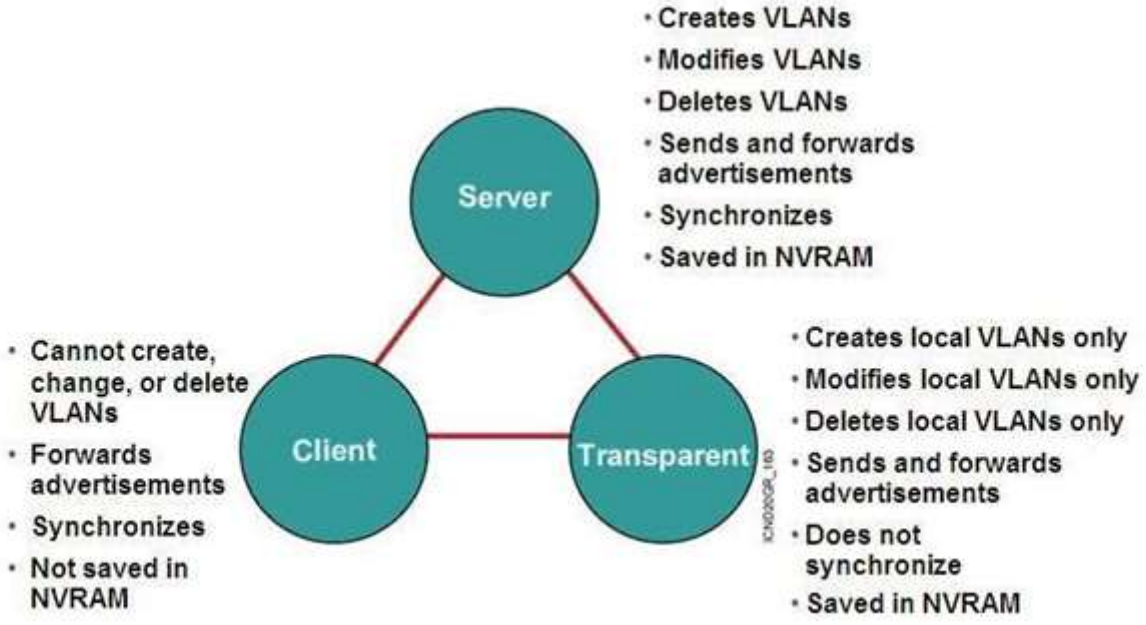
VTP - VLAN TRUNKING PROTOCOL

- VLAN bilgilerinin ağdaki diğer cihazlar ile paylaşılması amacı ile oluşturulan bir protokoldür.
- Böylece geniş bir ağ içerisindeki tüm cihazlar için aynı VLAN konfigürasyonunun yapılmasına gerek kalmaz.
- Her bir switch kendi üzerinde oluşturulmuş VLAN'ları diğer switchlere tanıtır. Böylece ağ içerisinde aynı VTP domain'inde yer alan her cihaz birbiri ile senkron olur.
- VTP, Server-Client yapısı ile çalışan bir sistemdir.
- VTP bilgileri yalnızca trunk portlar arasında taşınmaktadır.



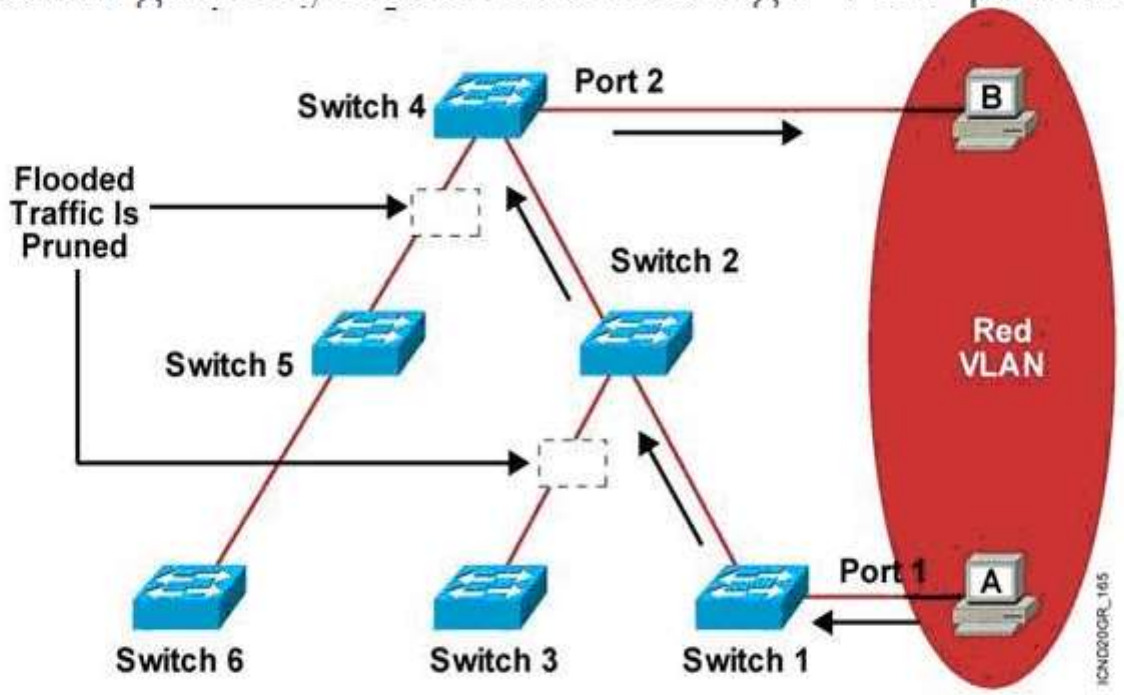
VTP MODLARI

- Server Mode: Bu modda çalışan switch üzerinde VLAN oluşturulur, değiştirilir ve silinebilir.
- Transparent Mode: Bu modda çalışan switch VTP'den VLAN bilgilerini alabildiği gibi, kendi üzerinde de VLAN oluşturulabilir. Ancak, kendi üzerinde üretilen VLAN bilgilerini diğer switchler ile paylaşmaz.
- Client Mode: Bu modda çalışan switch trunk portları üzerinden VLAN bilgisini alırlar ve VLAN bilgilerini diğer trunk portlara taşırlar. Ancak kendi üzerilerinde VLAN oluşturamaz va da silemezsiniz.



VTP PRUNING

- Networkde gönderilen broadcast paketleri varsayılan olarak trunk portlardan tüm cihazlara taşınacaktır. Çünkü o cihazlarda o VLAN'e üye bazı kullanıcılar bulunabilir.
- Fakat VLAN'a üye kullanıcı olmadığı sezimlenirse taşınmasına gerek yoktur. Bu özelliğe VTP pruning adı verilir.



VLAN Konfigürasyonu

- Switchler üzerinde VLAN'lar oluşturulur.

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 2
Switch(config-vlan)# name VLAN2
Switch(config-vlan)# exit
Switch(config)# vlan 3
Switch(config-vlan)# name VLAN3
Switch(config-vlan)# exit
Switch(config)# exit
Switch#
```

VLAN Konfigürasyonu

- İlgili portlar/cihazlar bu VLAN'lara üye yapılır.

```
Switch> enable
Switch# configure terminal
Switch(config)#i nt fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 2
Switch(config-if)# exit
Switch(config)# int fastEthernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 3
Switch(config-if)# exit
Switch(config)# int fastEthernet 0/4
Switch(config-if)# switchport mode trunk
Switch(config-if)# exit
Switch(config)#
```

VLAN Konfigürasyonu

- Eğer birden çok switch varsa VTP kullanılarak daha etkin PDU paylaşımı sağlanır.

```
Switch> enable
Switch# vlan database
Switch(vlan)# vtp domain MyCompanyArea
Changing VTP domain name from NULL to MyCompanyArea
Switch(vlan)# vtp client
Setting device to VTP CLIENT mode.
Switch(vlan)# exit
APPLY completed.
Exiting....
Switch#
```

VLAN atlama (Hopping) atağı

- Anahtarlar üzerinde bazı güvenlik önlemleri alınmadığı takdirde VLAN'ler arası geçiş sağlanıp, bir VLAN'e bağlı bir bilgisayar, kendi VLAN'inin haricinde farklı bir VLAN'de yer alan başka bir bilgisayara erişebilmektedir.

- Saldırganın, bağlı bulunduğu anahtardan farklı bir anahtar üzerinde kendi VLAN'i haricindeki, normalde erişememesi gereken bir VLAN'e erişmesine *VLAN atlama atağı* denmektedir.

- VLAN atlama atakları ikinci katmanda (Layer 2) gerçekleştirildiği için IP tabanlı (Layer 3) saldırı tespit ya da engelleme sistemleri tarafından yakalanmaları mümkün değildir.

VLAN Hopping Atakları

a) Anahtar Sahtekarlığı (Switch Spoofing)

- Bu atak türü, Cisco switchlere yönelik bir ataktır. Cisco anahtarlarının portları ya "access port" ya da "trunk port" olarak tanımlanabilirler.
- "access port", bir adet VLAN'e atanmış port olarak bilinir. "access port"ların, bağlı bulundukları VLAN haricindeki diğer VLAN portlarına erişimi yoktur.
- "trunk port" ise anahtar üzerinde yer alan tüm VLAN'lere üyedir ve switch-switch veya switch-Router bağlantısı ile birçok VLAN bilgisi taşınır.
- Bir portu Trunking mode olarak ayarlamanın ise elle ve otonom olarak Dynamic Trunking Protocol (DTP) olacak şekilde iki farklı konfigürasyon seçeneği mevcuttur.

- Buna göre anahtar kandırma atağının nasıl yapıldığını inceleyelim:

- Cisco switchlerin portları beş modda çalışırlar: “on”, “off”, “desirable”, auto” ve “nonegotiate”. Cisco anahtarların portları ön tanımlı (default) olarak “dynamic desirable” modundadırlar. Bu da şu anlama gelmektedir: Bu portun karşısındaki port “access port” ise port kendisini otomatik olarak “access port” olarak tanımlayacaktır. Karşısındaki portun modu “on”, “auto” ya da “dynamic desirable” ise port kendisini “trunk port” olarak tanımlayacaktır.

Saldırgan, kendi bağlı olduğu switch üzerinde kendisine bakan interface konfigürasyonunun "dynamic desirable", "dynamic auto" veya "trunk mode" olması durumunda, switch gibi davranıp kendi cihazından DTP (Dynamic Desirable Protocol) mesajları oluşturarak TRUNK bir bağlantı kurmuş olacaktır. Yani kendi bilgisayarınında bir switchin trunk portu olduğunu tanıtacak ve dolayısıyla hedeflediği VLAN'lar ile iletişim kurabilecektir..

FastEthernet0/12 için:

interface FastEthernet0/12
switchport mode dynamic auto

FastEthernet0/12 interface'i karşıdan gelecek olan paketler ile mode seçimine karar verecektir. Bu durumda saldırgan bunu kötüye kullanabilecektir. Saldırgan herhangibir saldırı aracıyla bu porta DTP mesajları göndererek karşıdaki switch ile trunk bağlantı kuracaktır.

b) Çift Etiketleme (Double Tagging)

- Bu saldırının anlaşılabilmesi için “native(yerel) VLAN” ve IEEE 802.1q kavramları önemlidir.
- **Yerel VLAN (Native VLAN):** "Trunk" bağlantı noktasına atanmış VLAN'dır. Bir "Trunk" bağlantı noktası; hem VLAN etiketi olmayan trafiği (untagged traffic) hem de, çok sayıda VLAN tarafından oluşturulan trafiği de (tagged traffic) destekler. "Trunk" bağlantı noktası herhangi bir VLAN'dan gelmeyen trafiği Yerel VLAN'a yönlendirir. Bir cihaz tarafından oluşturulan ve herhangi bir VLAN'dan gelmeyen trafik anahtarlayıcının Yerel VLAN olarak yapılandırılmış olan vlan üzerinden iletilir.

- Normalde anahtar üzerindeki her bir port sadece bir VLAN’e üye yapılabilir. Bir porttan birden fazla VLAN’e iletim için ilgili porta IEEE 802.1q tanımlamasının yapılması gereklidir. Yani TRUNK PORT. IEEE 802.1q tanımı yapılmış olan port, kendisine gelen çerçevenin “MAC adresi” ve “EtherType” alanlarının arasına 32-bitlik bir başka alan (tag-etiket) ekler. IEEE.802.1q portu, sadece etiketlenmiş çerçeveleri iletir. Etiketlenmemiş çerçeveler IEEE 802.1q portundan geçemezler.

- Bunun istisnası “native VLAN”e üye olan çerçevelerdir. IEEE 802.1q portuna gelen ve “native VLAN”e üye olan çerçeveler, herhangi bir etiketlenme yapılmaksızın IEEE 802.1q portu üzerinden karşıdaki anahtara iletilirler.

- Karşılıklı bağlanmış switchler arasında VLAN iletişiminin yapılabilmesi için karşılıklı bağlanmış bu anahtarların IEEE 802.1q portlarının “native VLAN” numaralarının aynı olması gereklidir.

- IEEE 802.1q portuna etiketlenmemiş çerçeve gelirse bu çerçeveler “native VLAN”e üye kabul edilirler. Özetle, IEEE 802.1q tanımı yapılmış olan portlar “native VLAN” için normal bir port gibi davranır.

“native VLAN” özelliği çift etiketlenmiş VLAN atlama saldırılarına açıktır. Şimdi çift etiketleme saldırısının nasıl yapıldığına bakalım:

Herhangi bir tanımlama yapılmadığı takdirde, bir IEEE 802.1q portunun “native VLAN” numarası “1”dir (VLAN 1). Saldırgan, oluşturmuş olduğu çift VLAN etiketli çerçevenin, dış VLAN etiket numarasına “native VLAN”in numarasını verir. İç VLAN etiket numarası olarak da hedef anahtarda yer alan hedef VLAN’in numarasını verir.
örnekle açıklayalım:

Saldırgan, kendisini “native VLAN”e üyeymiş gibi gösteren bir çerçeve oluşturur. Tabii ki bu saldırıyı yapabilmesi için saldırganın, bağlı olduğu anahtarın “native VLAN” numarasını bilmesi gereklidir. Yukarıda da belirtildiği gibi “native VLAN” için herhangi bir tanım yapılmamışsa, VLAN 1 “native VLAN”dir ki “native VLAN” numarası da anahtarlarda genellikle değiştirilmemektedir.

Bu durumda saldırgan kendisinin VLAN 1’de olduğunu belirten bir çerçeve oluşturur. Bu çerçeveye 32-bitlik bir etiket ekler (IEEE 802.1q etiketi). Bu ilk etiketin içindeki VLAN değerine de (VID) “1” verir.

Bundan sonra saldırgan, çerçeveye ikinci bir 32-bitlik etiket daha ekler. Bu etiketin içine de saldırıyı yapacağı VLAN’in numarasını yazar. Bu şekilde saldırgan çift etiketli bir çerçeve oluşturmuş olur. (Bu şekilde özel çerçevelerin (frame) oluşturulabildiği programlara internet üzerinden ulaşmak zor değildir.)

Aşağıdaki örnekte IEEE 802.1q portlarının “native VLAN” numarası “1” olarak kabul edilmiştir. Saldıracağımız VLAN’in numarasının da 61 dir. Bu durumda, çift VLAN etiketli çerçevenin dış VLAN etiketi ”1”, iç VLAN etiketi de “61” olarak belirlenir.

Saldırganın hedefindeki VLAN, “61” numaralı VLAN’e bağlı olan bilgisayarlardır. Saldırgan, göndermiş olduğu çerçeveye çift etiket eklemiştir. “1” numaralı anahtarın IEEE 802.1q portuna gelen çerçevedeki dış etiket “1” numaralı “native VLAN”e ait olduğundan anahtar “1” numaralı etiketi çıkarır ve çerçeveyi karşıdaki “2” numaralı anahtara gönderir. “2” numaralı anahtarın IEEE 802.1q portu da kendisine gelen bu çerçevenin “61” numaralı VLAN etiketini okuyarak çerçeveyi “61” numaralı VLAN’e ait olan portlara gönderir. Bu şekilde saldırgan “2” numaralı anahtarda yer alan “61” numaralı VLAN’e erişmiş olur. Saldırgan, “61” numarasını değiştirmek suretiyle “2” numaralı anahtarda tanımlanmış olan herhangi bir VLAN’e erişebilecektir. Saldırganın yapması gereken tek şey, iç VLAN etiket numarasının yerine erişmek istediği VLAN numarasını yazmaktır.

Önlem

- Anahtar kandırma (switch spoofing) atağını engellemek için anahtarın portlarından DTP (DynamicTrunking Port) özelliğini kaldırmak gerekir.
- IEEE 802.1q portuna ihtiyacımız olduğu takdirde bunun manuel olarak yapılması tavsiye edilir. Aşağıdaki komut satırı girilmek suretiyle anahtarın portlarından DTP kaldırılmış olur:

ANAHTAR(config)# interface range FastEthernet 0/1 – 24
ANAHTAR(config-if)# switchport mode access

- Çift etiketleme atağından korunmak için de aşağıdaki maddeler tavsiye edilir:

1. “native VLAN”i kullanıcılar için kullanmayın,
2. “default VLAN” numarasına “1”den farklı bir değer verin ve bu VLAN’i kullanıcılar için kullanmayın,
3. Kullanılmayan portları kapatın ve bu portları “default VLAN” haricinde başka bir VLAN’e dahil edin.