

# VLAN ve VLAN Durumları Simülasyonu

Şevval CANLI<sup>1</sup> ve Öznur KALAFAT<sup>2</sup>

<sup>1</sup>Bilgisayar Mühendisliği Bölümü, Mimarlık Mühendislik Fakültesi, Nişantaşı Üniversitesi, 34485 İstanbul  
(20182013053@std.nisantasi.edu.tr)

<sup>2</sup>Bilgisayar Mühendisliği Bölümü, Mimarlık Mühendislik Fakültesi, Nişantaşı Üniversitesi, 34485 İstanbul  
(20182013067@std.nisantasi.edu.tr)

## ÖZET

Teknolojinin gelişmesiyle birlikte ağ kullanımı yaygınlaşmaktadır. Giderek artan ağ kullanımı sonucunda yeni teknolojiler ortaya çıkmaktadır. Bu teknolojilerle beraber ağın performansı artırmak, güvenlik yönetimini kolaylaştırmak ve adres yönetimini sağlamak için kurumsal ağların tasarımında sıklıkla Sanal Yerel Alan Ağları (VLAN-Virtual Local Area Network) kullanılmaktadır. Sanal yerel ağ anlamına gelen VLAN, IEEE 802.11Q standardıdır. Yerel ağ içerisinde çalışma grupları oluşturmak ve yerel ağı mantıksal alt ağlara bölmek için kullanılmaktadır. Bu çalışmada, Sanal Yerel Alan Ağı olan VLAN konusuna değinilmiştir. LAN ve VLAN farklarından bahsedilmiş; VLAN'ın avantajlarına, VLAN'ın türlerine ve switch arayüz VLAN'ın durumlarına giriş yapılmıştır. Ayrıca VLAN hakkında yapılan çalışmalar incelenmiştir. Cisco Packet Tracer programı aracılığıyla; anahtar cihazlarda arayüz vlan erişim durumu, anahtar cihazlarda arayüz trunk durumu, trunk arayüzler için izin verilen vlan trafiği, trunk arayüzler için izin verilen vlan trafiği, anahtar cihazlarda arayüz dinamik durum güncellemesi, yönetim vlan'ları ve vlan arayüzleri, vtp (vlan trunking protocol), vlan veri tabanını silme ve vlan'lar arası yönlendirme konuları simülasyonlarla beraber işlenmiştir.

**Anahtar Kelimeler:** LAN, VLAN, Ağ, Switch, Cisco Packet Tracer, Trunk, Access, Desirable.

## ABSTRACT

With the development of technology, the use of networks is becoming widespread. As a result of increasing network usage, new technologies are emerging. Along with these technologies, Virtual Local Area Networks (VLANs) are often used in the design of corporate networks in order to increase the performance of the network, facilitate security management and provide address management. VLAN, which stands for virtual local area network, is the IEEE 802.11Q standard. It is used to create workgroups within the local network and to divide the local network into logical subnets. In this study, VLAN, which is a Virtual Local Area Network, is mentioned. LAN and VLAN differences are mentioned; The advantages of VLAN, types of VLAN, and states of switch interface VLAN are introduced. In addition, studies on VLAN were examined. Through the Cisco Packet Tracer program; interface vlan access status on switch devices, interface trunk status on switch devices, vlan traffic allowed for trunk interfaces, vlan traffic allowed for trunk interfaces, interface dynamic status update on switch devices, management vlans and vlan interfaces, vtp (vlan trunking protocol), deleting the vlan database and routing between vlans are covered with simulations.

**Keywords:** LAN, VLAN, Network, Switch, Cisco Packet Tracer, Trunk, Access, Desirable.

## I. GİRİŞ

Gelişen teknolojiyle birlikte hedeflere ve amaçlara ulaşmak için ağ, bir araç niteliği olarak karşımıza çıkmaktadır. Ağ, iki veya daha fazla cihazın bir araya getirildiği ve bu cihazlar arasında veri paylaşımının sağlandığı bir oluşumdur. Ağlar teknolojiye göre şekillenmektedir ve ihtiyaçlara göre de yapı olarak değişiklik göstermektedir. Bir kuruluş, birim veya yerleşke içerisinde bilgisayarların oluşturduğu bilgisayar ağları “Yerel Alan Ağı (LAN-Local Area Network)”

olarak adlandırılır. Günümüzde teknolojinin gelişmesi, ağ maliyetinin düşmesine ve ağ kullanımının artmasına sebep olmuştur. Geleneksel ağ altyapıları güncelliğini kaybetmiştir. Ağın yönetimi ve bağlantı sorunları ağ geniş bir alana yayıldıkça giderek zorlaşmaktadır. Ağ erişim ekipmanları ve ağ yapıları giderek daha karmaşık hale gelmektedir, bu sebeple ağ kullanıcılarının farklı ihtiyaçlarını karşılamak için VLAN teknolojisi ortaya çıkmıştır.

Bilgisayar ağları; Geniş Alan Ağları (WAN-Wide Area Network), LAN ve alt kümesi olan VLAN olmak üzere üçe ayrılır. WAN uzak lokasyonların birbirleri ile

iletiřim saęlaması iin, LAN ise aynı lokasyonda ve arada bir ynlendirici bulunmadan alıřabilecek řekilde tasarlanmıřtır. VLAN ise, sayısı artan aędaki cihazların internet eriřimini ve cihazların birbirleri ile olan iletiřimini daha kolay ynetilebilmeleri iin kullanılmaktadır. VLAN adından da anlařılacağı zere gerek bir LAN'ı mantıksal alt aęlara ayırıp daha kolay ynetmek iin sanal olarak alt aęlara ayırmak amacıyla kullanılır [1].

VLAN'lar, birden ok yerleřke ierisindeki aęlarda belirli toplama noktalarından ana merkeze fiber optik kablolar ile baęlantı saęlamaktadır. Bilgisayarlar, UTP (Unshielded Twisted Pair) kablolar aracılığıyla switch (anahtarlayıcı) ve router (ynlendirici) gibi aę cihazlarına baęlanarak LAN'a dahil olur. Bu aę cihazlarından oluřan LAN'ların da ana omurga cihazlarına (backbone) baęlanması neticesinde yerleřke aęı oluřmaktadır. Son kullanıcıların yerleřke aęına dahil olması iin kablolu baęlantının dıřında kablosuz baęlantı yntemi de kullanılır. ok sayıda bilgisayarların ve aę cihazlarının oluřturduęu bu yapının ynetimi olduka zordur. Yntemi kolaylařtırmak amacıyla yerleřke aęı, VLAN'lara blnr. Sanal Yerel Aę anlamına gelen VLAN, IEEE 802.11Q standardı olarak bilinir [2].

VLAN, yerel aę ierisinde alıřma grubu oluřturmak ve yerel aęı mantıksal alt aęlara blmek amacıyla kullanılır. Fiziksel olarak aynı aę ierisinde bulunsalar dahi farklı VLAN'larda bulunan cihazlar birbirleriyle ynlendirme olmadan doęrudan iletiřim kuramaz. Aęda bulunan cihazlar arttığı takdirde aęda yerel yayın (broadcast) sayısı da artmaktadır. Bir yerleřke aęında bulunan aę cihazlarının sayısı binlerce olabilmektedir. stelik aynı aę anahtarı (switch) zerinde ses, video ve veri trafięi yapılabilir. Video ve ses paketleri UDP protokol ile iletilmektedir. Bu servislerde yařanacak bir gecikmenin telafisi mmkn olmaz. Bu servisler aynı switch zerinden gerekleřse dahi farklı VLAN trafik nceliklendirmesi ile gecikmelerin nne geilebilir. Cihazlar ve kullanıcılar belirli VLAN'lar altında genellikle yerleřim yerine ve kaynakların iřlevine gre gruplanırlar [2].

VLAN kullanıcılara; gvenlik, performans, yayın alanı ve maliyet konusunda avantaj saęlamaktadır.

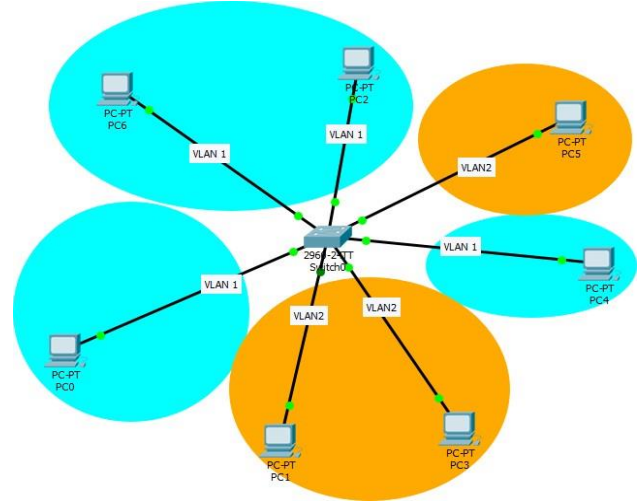
**Performans:** VLAN uygulanmamıř switchlerde gereksiz paket gnderimine yol aılabilir ve performans sorunlarına neden olabilir. Bu problemin nne gemek iin, bir aę VLAN'lar kullanarak blmlere ayrılır. VLAN'lar arasında ayrı trafik oluřtuęu iin bir VLAN'ın aę trafięi dięerini etkilemez. Gereksiz yayın trafięi oluřmaz. Her VLAN'da aę iletiřim performansı artar.

**Gvenlik:** VLAN'lar kullanılarak bir aęda birbirleriyle ilgisi olmayan grupların iletiřim halinde olması engellenir. Bu sayede dıř tehditlere karřı nlem alınmıř olunur. Aęlar mantıksal olarak blndę iin VLAN'lardaki cihazlar, dięer VLAN'lardaki aęlardan ayrılır. Switch zerindeki cihazlar VLAN'lara ayrıldığında aę zerinde herhangi bir uca baęlanıp tm

aęı dinleme ve aędaki bilgileri ele geirme ihtimali ortadan kalkacaktır. Kullanıcı sadece baęlanacağı VLAN zerinde iřlem yapabilir [3].

**Yayın Alanı (leklenebilirlik):** Her VLAN'ın ayrı mantıksal aęı olduęu iin ayrı bir yayın alanı oluřturulur. VLAN'larda oluřan yayın paketleri dięer VLAN'lara aktarılmaz [3].

**Maliyet:** Switch cihazı iinde ayrı VLAN'lar oluřturulur. Bylelikle yeni switch ihtiyaı ortadan kalkar. Bu sayede maliyet dřer.



**řekil 1:** VLAN'lar ile ayrı yayın alanlarına blnmř switch cihazı [3].

## II. İLGİLİ ALIřMALAR

Bahri A, Chamberland S, WLAN tasarlama problemini incelemiř ve her bir AP'nin konumu, gc ve kanalının seilmesi iin bir optimizasyon modeli nermiřtir. Bu tasarım probleminin matematiksel bir formlasyonunu sundular. Bařlangı zmlerini retmek iin bir buluřsal yntem ve bu bařlangı zmn geliřtirmek iin bir tabu arama algoritması nerilmiřtir [4].

Zhang Z, Huang X, Keune B, Cao Y, Li Y; standart veri akıřının nicel olarak analiz edildięini ve ıktının gerek zamanlı olarak VLAN'a dayalı bir alt istasyon iin deęerlendirilmesini nerdi. Uygun VLAN řemaları oluřturmanın, blme iindeki dngsel SAV'leri azaltarak veri akıřını nemli lde azaltacağı ve bylece aę baęlantılarının kullanımını ve SCN Ethernet gecikmesini en aza indireceęi sonucuna varılabilir [5].

Haiyan Y, ekirdek anahtarların, aę geidi artıklık yedeklemesini gerekleřtirmek ve yk dengeleme ve baęlantı yedekleme amacına ulařmak iin farklı VLAN verilerinin farklı baęlantılarla ulařmasını saęladığını zetlemiřtir [6].

### III. VLAN TÜRLERİ

Yerleşke ağlarında ağ içerisinde bulunan verinin türüne göre farklı VLAN grupları oluşturulmaktadır. Bu durum kolay yönetilmeyi sağlamaktadır. Ayrıca verinin tasnifi, izolasyonu, internete açık olup olmaması, servis kalitesi, kimlerin bu ağa ulaşım ulamayacağına kadar detaylandırılabilir [4].

**Varsayılan VLAN (Default VLAN):** Varsayılan VLAN yapılandırılmasında; switch'teki bütün portlar, switch başlatıldığında otomatik olarak varsayılan VLAN'a dahil olurlar. Varsayılan VLAN, switchte "VLAN 1" şeklinde adlandırılmıştır. VLAN 1 yeniden adlandırılmaz veya silinemez. Switch portlarının varsayılan VLAN'a bağlı olması durumunda bu portlar aynı broadcast domain'e dahil olur. Bu switchte bağlanan bütün cihazlar birbiriyle iletişim kurabilirler [4].

**Veri VLAN (Data VLAN, User VLAN):** Kullanıcı veri trafiğini taşımak için Veri VLAN'ı kullanılır. Aynı anda ses ya da video temelli trafik taşınabilir.

**Yerel VLAN (Native VLAN):** Farklı VLAN trafiğinin switchten çıkışı 802.1q protokolü ile sağlanır. VLAN 1 başlangıç için yerel olarak kabul edilir ancak etiketsiz olarak çıkış yapar. Burada 802.1q protokolü yerine Ethernet II protokolü kullanılır. Veri trafiğinin etiketsiz aktarımını önlemek için yerel VLAN'ın değiştirilmesi önerilmektedir [7].

**Yönetim VLAN (Management VLAN):** VLAN'lara IP adresi atanarak uzaktan Telnet ve SSH gibi uygulamalarla yönetilebilir. Uzaktan erişim ile cihazın yönetilmesini sağlayan VLAN'lar, Yönetim VLAN'ıdır.

**Ses VLAN (Voice VLAN):** Ağlardaki Ses VLAN'ı üzerinden sadece ses trafiğinin geçirilmesi ile yapılandırılan VLAN çeşididir. Ses iletimi için IP telefon kullanılır.

**Reserved VLAN:** Bu VLAN'lar da, Varsayılan VLAN gibi başlangıçta yapılandırılmıştır. Özel amaçlı protokollerin kullanılması amacıyla Reserved VLAN tercih edilir. Varsayılan VLAN'daki VLAN 1 gibi silinemez ve değiştirilemez [8].

### IV. ANAHTARLAMA CİHAZI ARAYÜZ (PORT) VLAN DURUMLARI

Anahtarlama cihazı arayüzleri, veri trafiği ve protokollere göre farklı durumlarda yapılandırılabilir. Dinamik Trunk Protokolü, sanal ağlara (VLAN) sahip katman 2 cihazlarının arasındaki bağlantı türlerini otomatik olarak belirleyen ağ protokolüdür. Katman 2 cihazlarının sahip olduğu arayüzler kullanım ihtiyacına göre ayarlanabilmektedir. DTP kısaca Cisco Switchler (anahtarlama cihazları) arasında çalışan ve iki

anahtarlama cihazının aralarında paylaştıkları DTP mesajı ile, bağlı oldukları portu Trunk portu (Gövde portu) yapmasını sağlayan bir protokoldür. Dinamik Trunk Protokolü aracılığıyla portlar arası "trunk" olma işlemi otomatik olarak yapılmaktadır. Dinamik Trunk Protokolü'nün gerçekleştirilmesi için uygulanabilecek 3 çeşit mod vardır [9]:

**Access Modu:** Genellikle istemci/sunucu makinelerle bağlantı aşamasında kullanılmaktadır. Access modu aktif olan arayüzlere yalnızca bir sanal ağ atanabilmektedir. Bu modda DTP protokolünün etkisi bulunmamaktadır.

**Trunk Modu:** Genellikle switch-switch veya switch-router bağlantılarında kullanılmaktadır. Trunk modu ayarlanmış arayüzlerde birden fazla sanal ağ bağlantı yapmak mümkün olmaktadır. Bu modda DTP anlaşması gerçekleşmesi mümkün olmaktadır.

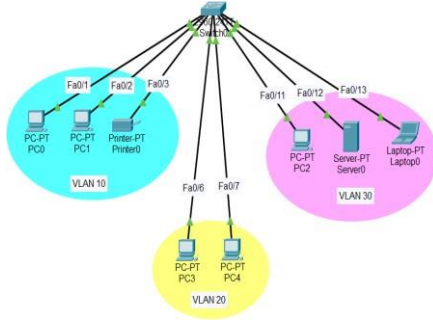
**Desirable Modu:** DTP protokolünün tam anlamıyla devreye girdiği diğer iki mod ise 'Dynamic Auto' ve 'Dynamic Desirable' modlarıdır. Bu modlar anahtar arayüzünün konumuna göre kendisini günceller [9].

DTP (Dinamik Trunk Protokolü), VTP (VLAN Trunk Protokol) den farklı bir yapıya sahiptir. VTP, aynı VTP etki alanında bulunan iki anahtarlama cihazının portunun VLAN bilgilerini paylaşmaya yönelik bir protokol iken, DTP ise iki anahtarlama cihazının birbirine bağlanan portlarının anlaşma ile otomatik olarak "trunk" yapılmasını belirleyen protokoldür. Varsayılan olarak anahtarlama cihazları Dynamic Desirable (Dinamik İstenen) moddadır [10].

Bu mod sürekli DTP paketleri gönderilmesine sebep olacağından fazladan bir yük bindirecek ve portların her an "trunk" moda geçip VLAN bilgisi gibi bazı bilgileri bu port üzerinden aktarılmaya olanak sağlayarak güvenlik açığı oluşturur. Bu durumu ortadan kaldırmak için "switchport nonegotiate" komutu işletilebilir. Belli bir portun yapılandırmaya bakıldığında DTP'nin etkin olup olmadığını ve etkinse hangi modunun etkin olduğunu görebiliriz. Bu komut yürütüldükten sonra DTP dinamik moddan çıkıp statik olarak "access" veya "trunk" durumuna gelmektedir.

### V. ANAHTAR CİHAZLARDA ARAYÜZ VLAN ERİŞİM DURUMU

Anahtar arayüzleri erişim durumundayken tek VLAN için atanabilir. Varsayılan olarak tüm arayüzler VLAN 1'e atanmış olarak yapılandırılmıştır. Yeni oluşturulan VLAN'lara atanarak sadece o VLAN'ın ağ trafiği yayın alanı içinde kalması sağlanabilir. Cisco Packet Tracer kullanarak Switch'ler üzerinde VLAN'lar oluşturulabilir.



Şekil 2: Uç Cihaz VLAN Topolojisi.

Bu çalışmada şekil 2’de gösterilen topolojiye göre arayüz bağlantıları oluşturularak VLAN topolojisi hazırlanmıştır. VLAN 10, 2 bilgisayar ve 1 yazıcıdan; VLAN 20, 2 bilgisayardan; VLAN 30 ise, 1 bilgisayar, 1 server ve 1 laptopdan oluşmaktadır. Bu cihazlar şekilde gösterilen kablo arayüz bağlantılarına göre switch’e bağlanmıştır.

```
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name Muhasebe
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Danisma
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Yonetim
Switch(config-vlan)#exit
```

Şekil 3: VLAN’lara isimlerini atama işlemi.

VLAN’lara, switch üzerinden isim atamaları yapılabilir.

```
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/5-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 30
Switch(config-if-range)#exit
```

Şekil 4: İlgili arayüzleri VLAN’lara atama işlemi.

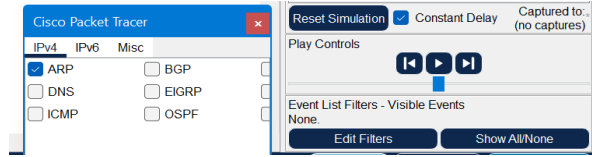
İlgili arayüzler VLAN’lar ile eşleştirilerek access modu aktif edilir.

```
Switch#show vlan
```

| VLAN Name   | Status | Ports  |
|-------------|--------|--|
| 1 default   | active | Fa0/16, Fa0/17, Fa0/18, Fa0/19<br>Fa0/20, Fa0/21, Fa0/22, Fa0/23<br>Fa0/24, Gig0/1, Gig0/2 |
| 10 Muhasebe | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4   |
| 20 Danisma  | active | Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10  |
| 30 Yonetim  | active | Fa0/11, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15   |

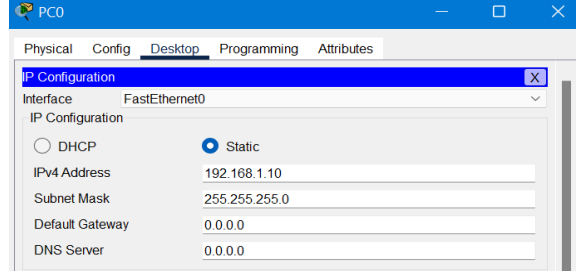
Şekil 5: VLAN tablosu.

İlgili arayüz ve VLAN eşleşmelerini kontrol etmek için “show vlan” komutu kullanılır ve VLAN’lar tablo halinde görselleştirilebilir.



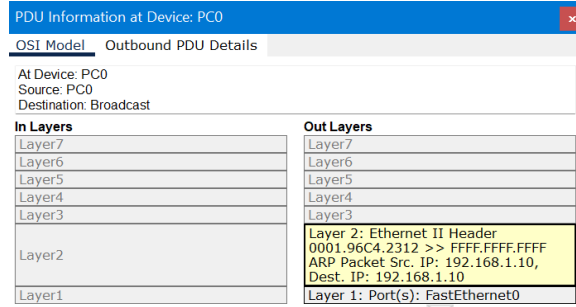
Şekil 6: Ağ simülasyonunda ARP paketi seçimi.

Ağ paketlerini gözlemlemek için Simulation, Show All/None ve Edit Filters düğmelerine tıklayarak ARP paketi seçilir.



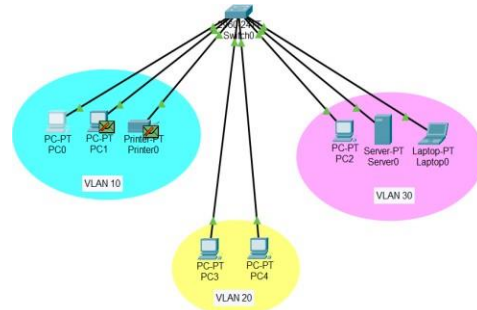
Şekil 7: PC0 için statik olarak IP adresi atama.

PC0 için statik olarak 192.168.1.10 IP adresi ve 255.255.255.0 alt ağ maskesi girilir.



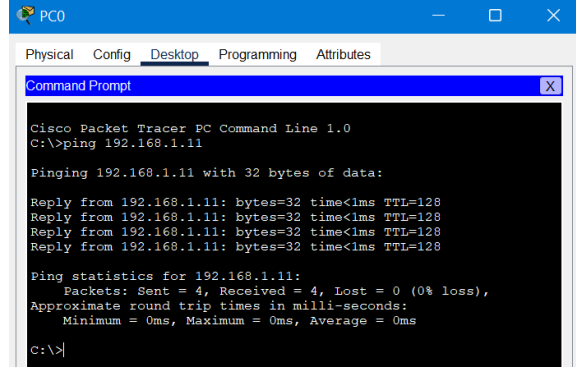
Şekil 8: ARP paketi yayın çerçevesi.

PC0 üzerinde ARP paketi görünür. ARP, LAN içinde IP çakışmasını önlemek için oluşturulan kontrol protokolüdür. Paketin üzerine tıklandığında OSI modeline göre 2. katmanda Ethernet II çerçevesinin hedef MAC adresinin FFFF.FFFF.FFFF olduğu görülür. Hedef MAC adresin FFFF.FFFF.FFFF olması paketin bir yayın paketi olduğu anlamına gelir. Yayın paketleri bulundukları VLAN üzerinde tüm portlardaki bilgisayarlara iletilir [11].



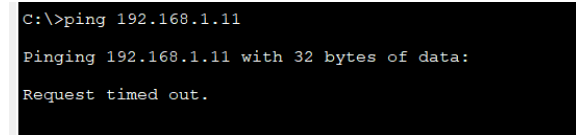
Şekil 9: VLAN10 için ARP yayın alanı.

Simülasyon oynatıldığında PC0, VLAN 10 arayüzlerinden birine bağlı olduğu için ARP yayın paketleri sadece VLAN 10'un arayüzlerine bağlı diğer PC'lere gidecektir. Diğer bir deyişle PC1 ve printer cihazlarına iletilecektir. VLAN20 ve VLAN30 arayüzlerine yayın paketi gönderilmeyecektir.



Şekil 10: Başarılı ping iletişim test.

PC1'e 192.168.1.11 IP adresi atanır. PC0'dan PC1'e ping komutu ile iletişim testi gerçekleştirirsek sonuç şekil 10 gibi başarılı olacaktır.



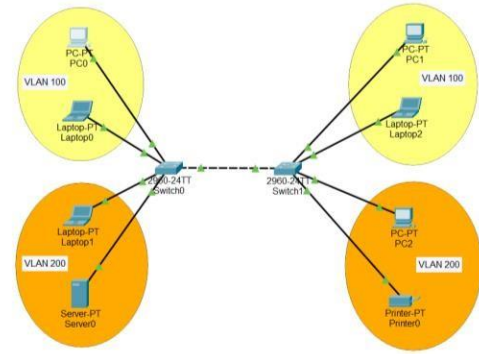
Şekil 11: Başarısız ping iletişim test.

PC1'i anahtarlama cihazında fa0/8 arayüzüne bağlarsak ve yeniden ping komutu ile iletişim testi yaparsak şekil 11 gibi başarısız bir iletişim testi gerçekleşecektir. Çünkü PC1 artık VLAN 10 arayüzüne bağlı değildir. VLAN 10'daki PC0'dan gelen trafik PC1'e iletilemez.

## VI. ANAHTAR CİHAZLARDA ARAYÜZ TRUNK DURUMU

Farklı VLAN'ların trafiğini anahtar cihazdan başka bir cihaza aktarmak için arayüzün birden fazla VLAN'ın trafiğini aktaracak bir protokole sahip olması gerekir. Arayüzler tek VLAN'a erişim durumunda Ethernet II protokolünü kullanırken farklı VLAN trafiklerini aktarım için 802.1q protokolünü kullanır. Arayüzü 802.1q protokolünü konuşmaya hazır hâle getiren işleme trunk durumu denir. Farklı anahtarlama cihazları ile VLAN'ların fiziksel alanları genişletilebilir [12]. Anahtarlama cihazları arasında VLAN'ları haberleştirmek için her VLAN'ın arayüzünden karşılıklı olarak kablo kullanılabilir ancak bu, her VLAN için ayrı bir kablo ve maliyetin artması anlamına gelir. Bunun yerine ayrılmış arayüzleri trunk durumuna getirerek tüm

VLAN'ların trafiği karşılıklı olarak aktarılabilir. İlgili arayüzü trunk durumuna almak için arayüzde "switchport mode trunk" komutu kullanılır [13].



Şekil 12: Uç cihaz VLAN topolojisi.

Şekil 12'deki görselde gösterilen topoloji Cisco Packet Tracer programında oluşturulmuştur. İki anahtar cihaz arasındaki bağlantı iki cihazda da fastEthernet0/24 arayüzünden yapılmıştır.

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#vlan 100
Switch(config-vlan)#name SariGrup
Switch(config-vlan)#exit
Switch(config)#vlan 200
Switch(config-vlan)#name TuruncuGrup
Switch(config-vlan)#exit
Switch(config)#interface range fastEthernet 0/1-5
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 100
Switch(config-if-range)#exit
Switch(config)#interface range fastEthernet 0/11-15
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 200
Switch(config-if-range)#exit
Switch(config)#show vlan

```

Şekil 13: İki anahtar cihaz üzerinde VLAN yapılandırması.

Her iki anahtar cihaz üzerinde de vlan 100, "SariGrup" ve vlan 200, "TuruncuGrup" olarak isimlendirilmiştir. Daha sonra switchler üzerinde arayüz bağlantıları yapılandırılmıştır.

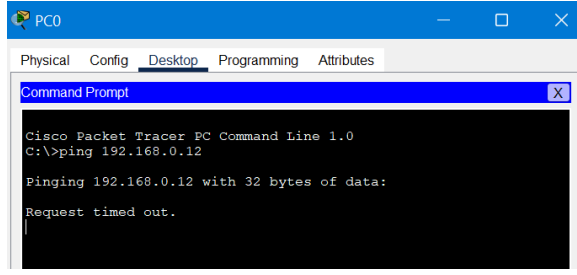
```
Switch#show vlan
```

| VLAN Name               | Status | Ports  |
|-------------------------|--------|--|
| 1 default               | active | Fa0/6, Fa0/7, Fa0/8, Fa0/9<br>Fa0/10, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23, Fa0/24, Gig0/1, Gig0/2 |
| 100 SariGrup            | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5  |
| 200 TuruncuGrup         | active | Fa0/11, Fa0/12, Fa0/13, Fa0/14<br>Fa0/15   |
| 1002 fddi-default       | active |  |
| 1003 token-ring-default | active |  |
| 1004 fddinet-default    | active |  |
| 1005 trnet-default      | active |  |

Şekil 14: "show vlan" komutu.

Şekil 14'te gösterilen tabloyu elde etmek için "show vlan" komutu kullanılmış ve VLAN'lar görselleştirilmiştir.





Şekil 15: Başarısız ping iletişim testi.

PC0 ve PC1 iletişim testini ping komutu ile gerçekleştirilmiştir. Testin, “Request time out” cevabı döndürdüğü görülmüştür. İletişim bu aşamada başarısızdır.

```
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

Şekil 16: “switchport mode trunk” komutu.

VLAN 100 ve VLAN 200 trafiğinin her iki anahtar cihazda gönderimi için fastethernet0/24 arayüzlerini trunk konumuna getirmemiz gerekir. Bunun için fastethernet0/24 arayüzünde “switchport mode trunk” komutu kullanılmıştır.

```
Switch#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/24    on        802.1q         trunking    1

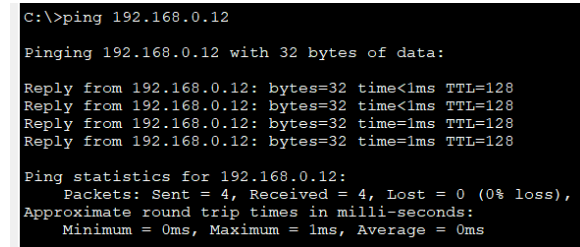
Port      Vlans allowed on trunk
Fa0/24    1-1005

Port      Vlans allowed and active in management domain
Fa0/24    1,100,200

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/24    1,100,200
```

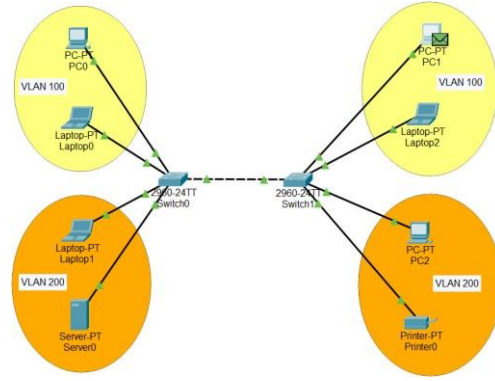
Şekil 17: “show interface trunk” komutu.

“show interface trunk” komutu ile Şekil 17’de gösterilen tablo elde edilmiştir. Tabloda görüldüğü üzere, Fa0/24 arayüzünde trunk modu aktif hale getirilmiştir.



Şekil 18: Başarılı ping iletişim testi.

Trunk modu aktif hale getirildikten sonra, PC0 ve PC1 arasında yeniden iletişim testi ping komutu ile gerçekleştirilmiştir. Testin sonunda “Reply from 192.168.0.12: bytes=32 times=1ms TTL=128” cevabı döndürdüğü görülmüş ve test başarılı olmuştur.



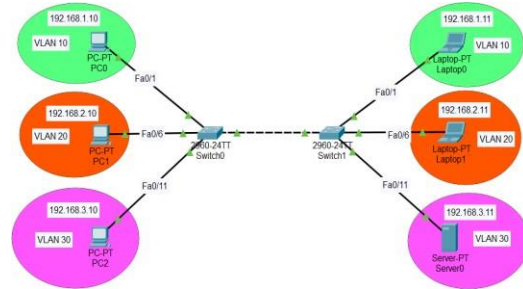
Şekil 19: VLAN için ARP yayın alanı.

Simülasyon ortamında sadece ARP paketleri seçilerek PC1’in IP adresi 192.168.0.20 olarak değiştirilmiştir. ARP paketlerin yayın alanı gözlemlenmiştir. ARP paketlerinin Anahtar 1 cihazı VLAN 100 yayın alanında bulunan uç cihazlara PC1, Laptop1 ve Laptop2’ye eriştiği gözlemlenmiştir.

## VII. TRUNK ARAYÜZLER İÇİN İZİN VERİLEN VLAN TRAFİĞİ

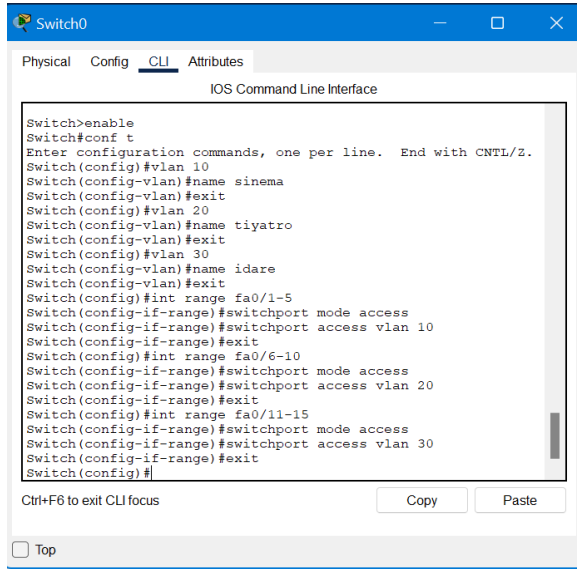
Trunk trafiği izin verilen VLAN’lar için filtrelenebilir. Filtrelemenin amacı; güvenlik veya trafik yoğunluğunu düşürmek için yapılabilir. Böylelikle izin komutunda belirtilmeyen VLAN’lar trunk arayüzünün diğer tarafına geçemez ve güvenlik sağlanmış olur [10]. Anahtar cihazlarında varsayılan olarak tüm VLAN’ların trafiği trunk arayüzlerinde izinlidir. İzin verilen VLAN için trunk arayüzünde;

“switchport trunk allowed vlan VLANNumarası” komutu yazılır. VLAN numaraları arasına “,” koyularak birden fazla VLAN’a izin verilebilir.



Şekil 20: Uç cihaz VLAN topolojisi.

VLAN topolojisi Şekil 20’deki gibi Cisco Packet Tracer programında gerçekleştirilmiştir. Bilgisayarların IP ve bağlantıları belirlenmiştir ve statik olarak atanmıştır.



**Şekil 21:** İki anahtar cihaz üzerinde VLAN yapılandırması.

İki anahtar cihaz üzerinde de belirlenen VLAN isimleri ve arayüzler ilişkilendirilmiştir.

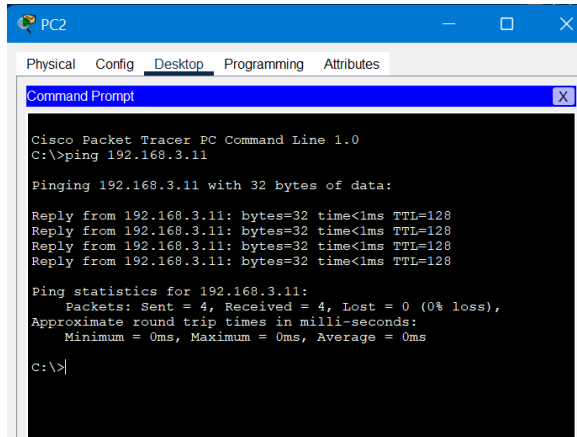
```
Switch(config)#interface fastEthernet 0/24
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/24, changed state to up
```

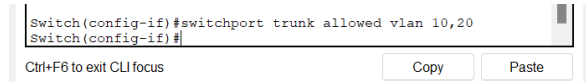
**Şekil 22:** “switchport mode trunk” komutu.

Switch 1 anahtar cihazı üzerinde trunk modu “switchport mode trunk” komutu ile aktif hale getirilmiştir.



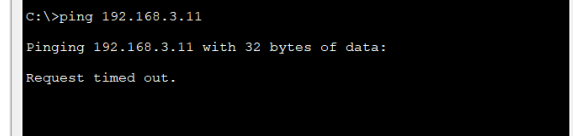
**Şekil 23:** PC2’den Server0’a başarılı ping iletişim testi.

Anahtar 1 cihazında trunk moduna geçildiği için PC2’den Server0’a ping iletişim testi başarılı olmuştur.



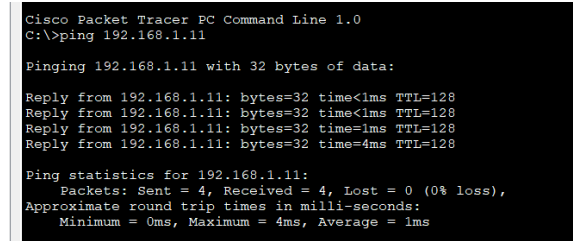
**Şekil 24:** Anahtar 1 cihazında vlan 10 ve vlan 20 trafiğine izin verilmesi.

Anahtar 1 cihazı üzerinde “switchport trunk allowed vlan 10,20” komutu ile sadece vlan 10 ve vlan 20 trafiğine izin verilmiştir. Vlan 30 trafiğine izin verilmemiştir.



**Şekil 25:** PC2’den Server0’a başarısız ping iletişim testi.

Vlan 30 üzerinde bulunan PC2’den Server0’a ping iletişim testi uygulandığında test başarısız olmuştur. Çünkü switch1 üzerinde yalnızca vlan 10 ve vlan 20 trafiğine izin verilmiştir.



**Şekil 26:** PC0’den Laptop0’a başarılı ping iletişim testi.

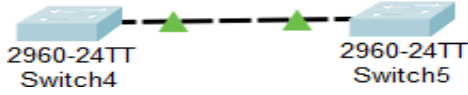
PC0’den Laptop0’a ping iletişim testi başarılı olmuştur. Bunun sebebi ise Switch üzerinde vlan 10 trafiğine izin verilmiş olmasıdır.

## VIII. ANAHTAR CİHAZLARDA ARAYÜZ DİNAMİK DURUM GÜNCELLEMESİ

Anahtar cihazlarda arayüzler, karşı arayüzün durumuna göre kendini konumlandırma özelliği ile yapılandırılır. Bu varsayılan yapılandırma erişim ve trunk modlarının dışındadır [14]. Switch(config-if)#switchport mode dynamic auto veya Switch(config-if)#switchport mode dynamic desirable komutları kullanılır. Anahtar cihazlarda arayüzler dynamic auto ile yapılandırılmıştır.

| Anahtar 1 \ Anahtar 2 | Dynamic Auto | Dynamic Desirable | Trunk     | Access    |
|-----------------------|--------------|-------------------|-----------|-----------|
| Dynamic Auto          | Access       | Trunk             | Trunk     | Access    |
| Dynamic Desirable     | Trunk        | Trunk             | Trunk     | Access    |
| Trunk                 | Trunk        | Trunk             | Trunk     | Önerilmez |
| Access                | Access       | Access            | Önerilmez | Access    |

**Şekil 27:** Arayüz Durum Tablosu.



**Şekil 28:** Değişen arayüz durumları örneği topolojisi örneği.

Anahtar 4 cihazını fa0/21 ve Anahtar 5 cihazını fa0/22 arayüzlerinden bağlantıları yapılır. Daha sonra Anahtar 1 fa0/21 arayüzü Trunk olarak yapılandırılır.

```
Switch>show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/22    auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/22    1-1005

Port      Vlans allowed and active in management domain
Fa0/22    1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/22    none

Switch>
```

**Şekil 29:** Otomatik uyarlanmış trunk arayüzleri listesi.

Anahtar 5 cihazında “show interface trunk” komutunu uygulandığında trunk arayüzleri tablosu görülecektir. Anahtar 5 cihazı fa0/22 arayüzünde trunk yapılandırılmamış olmasına rağmen otomatik olarak trunk durumuna geçiş yaptığı görülür. Otomatik olarak öğrenilmiş trunk arayüzleri auto durumunda ve n-802.1q ile tabloda belirtilir.

```
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/21
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode access
```

**Şekil 30:** Anahtar 4 cihazı fa0/21 arayüzünü “switchport mode access” komutu ile erişim durumuna getirilmesi.

```
Switch>show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/22    auto      n-802.1q       trunking    1

Port      Vlans allowed on trunk
Fa0/22    1-1005

Port      Vlans allowed and active in management domain
Fa0/22    1

Port      Vlans in spanning tree forwarding state and not pruned
Fa0/22    1

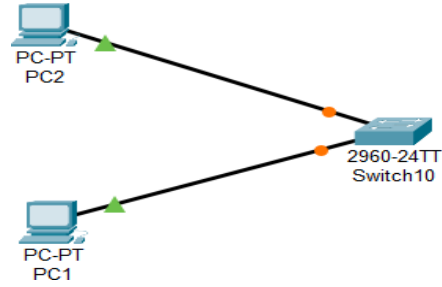
Switch>
```

**Şekil 31:** Anahtar 5 cihazı fa0/21 arayüzünü “switchport interface trunk” komutu ile erişim durumuna getirilmesi.

Anahtar 5 cihazında tekrar “show interface trunk” komutunu kullanıldığı takdirde bu kez arayüz tablosu boş bir şekilde görülecektir. Bunun sebebi Anahtar 4 cihazda 21. arayüz erişim durumuna gelirse Anahtar 5 cihazında kendisini otomatik olarak erişim durumuna taşıyacaktır.

## IX. YÖNETİM VLAN'LARI VE VLAN ARAYÜZLERİ

VLAN ağlarında uç cihazların anahtar cihazlarına erişimi ve yönetimi için VLAN arayüzleri oluşturulmaktadır. Bu arayüzler sanaldır, fiziksel değildir ve IP adresi atanabilir. Bu IP üzerinden anahtar cihazla iletişim kurulabilir. Anahtar cihazlarda fiziksel arayüzler IP adresi alamaz, anahtar cihazın yönetimi için VLAN arayüz yapılandırmalarına IP adresi atanması gerekmektedir. VLAN'lara IP adresi atamak için “interface vlan Numara” komutu aracılığıyla VLAN arayüzlerine giriş yapılmalıdır. Ardından “ip address” komutu ile IP adresi ve alt ağ maskesine giriş yapılmalıdır [15].



**Şekil 32:** Uç cihaz VLAN topolojisi.

| PC  | Arayüzler | IP Adresi     |
|-----|-----------|---------------|
| PC2 | Fa0/1     | 192.168.1.10  |
| PC1 | Fa0/20    | 192.168.20.10 |

**Şekil 33:** Uç cihaz VLAN topoloji tablosu.

PC1 ve PC2 cihazlarını tablodaki verilen değerlere göre anahtar arayüzlerine bağlanılır ve IP atamaları yapılır.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#
```

**Şekil 34:** VLAN1 arayüzünde IP adresi ve alt ağ maskesi atama.

Anahtar cihazında VLAN 1 arayüzüne girip 192.168.1.2 IP adresi ve 255.255.255.0 alt ağ maskesi atanır.

```
Switch(config)#interface vlan 20
Switch(config-if)#ip address 192.168.20.2 255.255.255.0
Switch(config-if)#
```

**Şekil 35:** VLAN20 arayüzünde IP adresi ve alt ağ maskesi atama.

Anahtar cihazında VLAN 20 arayüzüne girip 192.168.20.2 IP adresi ve 255.255.255.0 alt ağ maskesi atanır.



```
Switch(config)#interface range fa0/1-19
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 1
Switch(config-if-range)#
```

**Şekil 36:** Fa0/1 aralığındaki tüm arayüzler VLAN1'e dahil edilir.

```
Switch(config)#interface range fa0/20-24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport Access vlan 20
```

**Şekil 37:** Fa0/20-24 aralığındaki tüm arayüzler VLAN20'e dahil edilir.

PC0'dan 192.168.20.2 IP adresi ile anahtar cihazına, PC1'den 192.168.1.2 IP adresi ile anahtar cihazına ping komutu ile iletişim testi gerçekleştirilir.

```
Switch(config)#line vty 0 4
Switch(config-line)#password 1234
Switch(config-line)#login
```

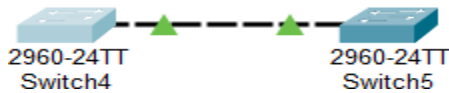
**Şekil 38:** Anahtar cihazında uzaktan erişimleri açılması.

PC0'dan ve PC1'den sırası ile anahtar cihazına "telnet 192.168.1.2" ve "telnet 192.168.20.2" komutları ile uzaktan erişim gerçekleştirilir. Erişim parolası 1234 olacaktır.

## X. VTP (VLAN TRUNKING PROTOCOL)

VTP yani Sanal Yerel Ağ Aktarım Protokolü, çoklu anahtar sistemlerinde VLAN'ları trunk arayüzleri üzerinden diğer anahtar cihazlarına aktarılması için kullanılmaktadır. Bu protokolün amacı sadece bir anahtarda VLAN'ları oluşturmak ve diğer anahtar cihazlara VLAN'ları aktarmaktır [16].

Böylece diğer anahtar cihazlarda VLAN oluşturmaya gerek kalmayacaktır. VTP alanına girecek anahtarlardan biri VLAN aktarımı için sunucu, diğerleri ise VLAN alımı için istemci rolündedir. VTP aktarımı için bir etki alanı ve bu etki alanına girmek için bir parola gerekmektedir [17].



**Şekil 39:** VTP VLAN aktarım topolojisi örneği.

```
Switch(config)#vlan 10
Switch(config-vlan)#name Satis
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name Danisma
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name Yonetim
Switch(config-vlan)#exit
Switch(config)#
```

**Şekil 40:** Anahtar 4 cihazında VLAN'lar oluşturulur.

```
Switch(config)#vtp domain anahtar.sw
Changing VTP domain name from NULL to anahtar.sw
Switch(config)#vtp password 123456
Setting device VLAN database password to 123456
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#
```

**Şekil 41:** Anahtar 4 cihazında VTP yapılandırılır.

```
Domain name already set to anahtar.sw.
Switch(config)#vtp password 123456
Setting device VLAN database password to 123456
Switch(config)#vtp mode client
Setting device to VTP CLIENT mode.
Switch(config)#
```

**Şekil 42:** Anahtar 5 cihazında VTP yapılandırılır.

Anahtar 4 cihaz VLAN'ları aktaracak taraf, Anahtar 5 ise VLAN'ları alıcı taraftır. VTP yapılandırmasında etki adı anahtar.sw olacaktır. VTP parolası ise 123456'dır. Buna göre Anahtar 4 cihazda vt server yapılandırmasını yapılmalıdır.

```
Switch#show vlan
```

| VLAN Name               | Status | Ports  |
|-------------------------|--------|--|
| 1 default               | active | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10, Fa0/11, Fa0/12<br>Fa0/13, Fa0/14, Fa0/15, |
| Fa0/16                  |        |  |
| Fa0/20                  |        | Fa0/17, Fa0/18, Fa0/19,  |
| Gig0/1                  |        | Fa0/21, Fa0/23, Fa0/24,  |
| 10 Satis                | active | Gig0/2   |
| 20 Danisma              | active |  |
| 30 Yonetim              | active |  |
| 1002 fddi-default       | active |  |
| 1003 token-ring-default | active |  |
| 1004 fddinet-default    | active |  |
| 1005 trnet-default      | active |  |

**Şekil 43:** Anahtar 5 cihazında "Show vlan" komutunun kullanılması.

Şekilde görüldüğü üzere 10, 20 ve 30 VLAN'ları VTP ile Anahtar 5 cihazına aktarılmıştır.

## XI. VLAN VERİ TABANINI SİLME

Anahtar cihazlarda VLAN bilgisi startup.config dosyasına yazılmamaktadır. VLAN bilgileri cihazın flash belleğine yazılır. VLAN'ları silme ve güncelleme işlemi komutla yapılabilir, ayrıca doğrudan cihaz flash belleği üzerinden topluca da yapılabilir. VLAN veri tabanı dosyası silinirse yeni VLAN'lar oluşturulduğunda yeniden vlash bellekte VLAN veri tabanı yazılmaktadır [19]. VLAN veri tabanı dosyası cihaz flash belleğinde "vlan.dar" dosya adı ile tutulmaktadır.

```
Switch(config)#vlan 10
Switch(config-vlan)#name odal
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name oda2
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name oda3
Switch(config-vlan)#exit
```

**Şekil 44:** Anahtar cihazda VLAN 10, 20 ve 30 ağılarını

sırası ile oda1, oda2, oda3 adı ile oluşturulur.

```
Switch#show flash:
Directory of flash:/

 1  -rw-   4670455      <no date>  2960-lanbasek9-mz.150-2.SE4.bin
 2  -rw-    736        <no date>  vlan.dat

64016384 bytes total (59345193 bytes free)
```

**Şekil 45:** Anahtar cihazda “show flash:” komutunun kullanılması.

Anahtar cihazda flash bellek içeriği bu komutla görüntülenir. Şekilde VLAN kayıtlarının tutulduğu “vlan.dat” dosyası görülmektedir.

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

**Şekil 46:** Anahtar cihazda “delete flash:vlan.dat” komutunun kullanılması.

Bu komut anahtar cihazındaki “vlan.dat” dosyasının silinmesini sağlamaktadır.

```
Switch#reload
System configuration has been modified. Save? [yes/no]:yes
Building configuration...
[OK]
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)FX, RELEASE SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K bytes of
memory.
2960-24TT starting...
Base ethernet MAC Address: 0060.5C1C.31A3
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 2 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
```

**Şekil 47:** Anahtar cihazda “reload” komutunun kullanılması.

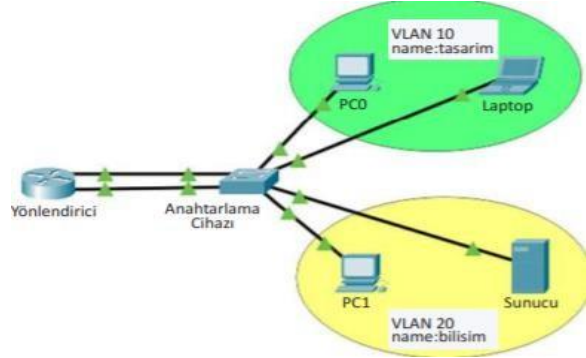
Cihaz bu komut ile yeniden başlatılır ve “show vlan” komutu ile VLAN tablosunda daha önce oluşturulan VLAN’ların olmadığı görüntülenir.

## XII. VLAN’LAR ARASI YÖNLENDİRME

**Yönlendirme:** Farklı mantıksal ağlar arasındaki trafiğin aktarılması işlemine yönlendirme denir. Trafiğin kontrolünü gerçekleştiren cihazlara ise yönlendirici cihazlar denmektedir. VLAN’lar anahtarlama cihazlarında farklı mantıksal ağlardan oluştuğundan aralarında veri aktarımı için bir yönlendirici cihaza ihtiyaç duymaktadır. VLAN’ların mantıksal ağlara bölünmesi sadece farklı ağlardaki cihazların birbirinden tamamen ayrılması için değildir. Yönlendirme ile farklı VLAN’lardaki cihazlar birbirleri ile daha güvenli iletişim kurabilmektedirler. Güvenliğin artmasındaki diğer bir sebep ise VLAN trafiklerinin karşı tarafa aktarılmasında uç cihazların MAC adreslerinin gizlenmesidir [19].

**Yönlendirici Cihazda Farklı Fiziksel Arayüzler ile VLAN Yönlendirme:** Yönlendirici cihazlarda, tıpkı

anahtar cihazlarda olduğu gibi Ethernet II protokolü ile iletişim kurabilen yerel ağ bağlantı arayüzleri vardır. Lakin bu arayüzlerin sayısı anahtar cihazlara nazaran oldukça sınırlı olmakla beraber her yerel ağ için bir tane arayüz bulunmaktadır [20]. Farklı VLAN trafiğinin bu arayüzlere fiziksel olarak bağlanması ve yönlendirici cihazda ilgili arayüzlere uygun mantıksal IP’ler tanımlanması gerekmektedir. Yerel ağlardaki uç cihazlarda ise yönlendirici arayüz IP adresinin varsayılan ağ geçidi (gateway) olarak tanımlanması gerekmektedir.



**Şekil 48:** Uç cihaz VLAN topolojisi.

| VLAN    | Name    | Arayüzler           |
|---------|---------|---------------------|
| Vlan 10 | tasarım | Fa0/1-fa0/10 arası  |
| Vlan 20 | bilisim | Fa0/11-fa0/20 arası |

**Şekil 49:** Kullanılan VLAN tablosu.

| Cihaz                    | IP          | Alt Ağ Maskesi | Varsayılan Ağ Geçidi | Anahtar Arayüzü |
|--------------------------|-------------|----------------|----------------------|-----------------|
| Yönlendirici Arayüz g0/0 | 192.168.0.1 | 255.255.255.0  |                      | Fa0/1           |
| Yönlendirici Arayüz g0/1 | 192.168.1.1 | 255.255.255.0  |                      | Fa0/11          |
| PC0                      | 192.168.0.2 | 255.255.255.0  | 192.168.0.1          | Fa0/2           |
| Laptop                   | 192.168.0.3 | 255.255.255.0  | 192.168.0.1          | Fa0/3           |
| PC1                      | 192.168.1.2 | 255.255.255.0  | 192.168.1.1          | Fa0/12          |
| Sunucu                   | 192.168.1.3 | 255.255.255.0  | 192.168.1.1          | Fa0/13          |

**Şekil 50:** Uç cihaz IP ve anahtar arayüz tablosu.

```
Switch(config)#vlan 10
Switch(config-vlan)#name tasarim
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name bilisim
Switch(config-vlan)#exit
```

**Şekil 51:** Anahtar cihazında VLAN 10 ve VLAN 20’nin oluşturulması.

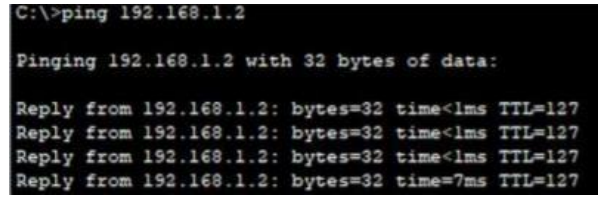
```
Switch(config)#interface range fa0/1-10
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 10
Switch(config-if-range)#exit
Switch(config)#interface range fa0/11-20
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 20
Switch(config-if-range)#exit
```

**Şekil 52:** Anahtar cihazında ilgili arayüzlerin VLAN’lara dahil edilmesi.

Daha sonra ise tabloda belirtildiği üzere uç cihazların IP girişleri yapılmalıdır.

```
Router(config)#interface gigabitEthernet 0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface gigabitEthernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

Yönlendirici cihazda IP tablosunda olduğu gibi IP girişlerini yapılır. Buradaki örnekte yönlendirici cihazda iki tane arayüz bulunmaktadır. Bu arayüzler sırası ile VLAN 10 ve VLAN 20 ile aynı mantıksal ağ grubunda olacaktır.



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time<1ms TTL=127
Reply from 192.168.1.2: bytes=32 time=7ms TTL=127
```

Şekil 53: Ping işleminin gerçekleştirilmesi.

PC0 ile PC1 arasında ping iletişim testi gerçekleştirildiğinde iletişimin başarılı olduğu görülecektir.

**Trunk - VLAN Arası Yönlendirme:** VLAN'lar arasında yönlendirme işleminde her VLAN için yönlendirici arayüzüne fiziksel erişim mümkün olmayabilmektedir. VLAN sayısı arttıkça her VLAN için fiziksel erişime ihtiyaç gerektiğinden yönlendiricide arayüz olmayabilir. Üstelik bu, kablo ve arayüz maliyetinin de artması anlamına gelmektedir. Anahtar cihazlarda arayüzler trunk durumu ile birden fazla VLAN trafiğini iletebilir. VLAN'lar arası yönlendirme yapılacaksa yine trunk yönteminden kolaylıkla yararlanılabilir. Yönlendiriciye gelen trafik, yönlendirici arayüzünde her VLAN için alt sanal arayüzler oluşturularak karşılanabilir.

Yönlendirici cihazdaki fiziksel arayüz herhangi bir ağ için tanımlanmaz. Anahtar cihazının trunk arayüzünden gelen her VLAN trafiği için bir sanal arayüz oluşturulmalıdır ve bu sanal arayüzlerin trunk VLAN trafiğini iletebilmesi için 802.1q protokolünü kullanması gerekir [17].

Yönlendirici cihazda fiziksel arayüzde sanal alt arayüzler oluşturmak için "Router(config)#interface gigabitEthernet 0/0.10" komutu kullanılır. Fiziksel arayüzün isim ve numarasından sonra "." (nokta) ile VLAN için bir alt arayüz numarası belirlenir ve bu komutta alt arayüz numarası 10'dur. Bu numara VLAN

numarası ile aynı olmak zorunda değildir lakin uyum ve anlaşılabilirliğin artması için aynı numarayı vermek daha doğru olacaktır [20].

Alt arayüzün trunk trafiğini aktarabilmesi için "Router(config-subif)#encapsulation dot1q 10" komutu kullanılmaktadır. Bu komut alt arayüzü 802.1q protokolü ile iletişime hazır hâle getirir. "encapsulation dot1q" komutundan sonra girilen numara alt arayüzün iletişime geçeceği VLAN'ın numarası ile aynı olmak zorundadır. Bu komut satırında VLAN 10 için dot1q numarası 10 olmalıdır. VLAN ile iletişime geçebilmesi için alt arayüzde bir IP adres bilgisi gereklidir. Bu IP adresi aynı zamanda VLAN'daki cihazların varsayılan ağ geçidi olacaktır. "Router(config-subif)#ip address 192.168.0.1 255.255.255.0" yönlendiricide alt arayüz oluşturma işlemi trunk hattından gelen yönlendirme yapılacak tüm VLAN'lar için yapılmalıdır. Sanal alt arayüzlerin aktif olabilmesi için alt arayüzün içinde olduğu fiziksel arayüzün açık konumda olması gerekmektedir.

```
"Router(config)#interface gigabitEthernet 0/0"
```

"Router(config)#no shutdown" komutu ile fiziksel arayüz, tüm alt arayüzler için açık konuma getirilmektedir. Alt arayüzlerde tek tek açma işlemi yapılmamaktadır. Fiziksel arayüze herhangi bir IP adresi yazılmamaktadır.

### XIII. SONUÇLAR VE ÖNERİLER

LAN'lar, yönetilebilirlik, esneklik ve kolay gözlemlenebilmeleri açısından VLAN'lara bölünebilirler. VLAN'lar farklı türlere sahiptirler. Bu çalışmada VLAN türlerine değinilmiştir. Literatürde yer alan ve bu çalışmayla benzerlik gösteren çalışmalar araştırılmış, bu çalışmaya göre avantajları ve dezavantajları Bölüm II'de detaylı olarak verilmiştir. Cisco Packet Tracer programı aracılığıyla; anahtar cihazlarda arayüz vlan erişim durumu, anahtar cihazlarda arayüz trunk durumu, trunk arayüzler için izin verilen vlan trafiği, trunk arayüzler için izin verilen vlan trafiği, anahtar cihazlarda arayüz dinamik durum güncellemesi, yönetim vlan'ları ve vlan arayüzleri, vtp (vlan trunking protocol), vlan veri tabanını silme ve vlan'lar arası yönlendirme konuları simülasyonlarla beraber işlenmiştir.

Kurumların ve firmaların mevcut ağlarında bulunan Ethernet anahtarları üzerinde çalışabilen bir trafik yük dengelemesi algoritması geliştirilerek maliyet açısından avantaj sağlanabilir. Ağ teknolojisinin hızlı ve güvenli olması, kurumlar açısından oldukça önemlidir. VLAN ağları, kullanıcılar açısından güvenli ağ sistemi sunar. Ağ üzerindeki trafiği dengeleyerek, ağdaki trafiği azaltır. Bu durum performansın artmasını sağlar.

## KAYNAKLAR

1. Muhammed Fatih Tarlacı (2018), "Kablosuz Kampüs Ağlarında Dinamik Vlan Yapılandırmasının Ağ Performans Parametreleri Üzerindeki Etkisi", 1-80.
2. Serdar Kırıçoğlu (2018), "Kurumsal Ağların Sistematiik Tasarımı İçin Yeni Bir Dinamik Vlan Yaklaşımı", Doktora Tezi Elektrik-Elektronik Ve Bilgisayar Mühendisliği Anabilim Dalı, 1-67.
3. İsmail Arık (2018), "İdeal Kampüs Ağ Yapısının Tasarımı Ve Güvenlik Performansının Değerlendirilmesi", 1-119, <https://Acikerisim.Aku.Edu.Tr/Xmli/Bitstream/Handle/11630/6454/10145840.Pdf?Sequence=1&IssaIlowed=Y>.
4. Ozgur Karatas (2008), "VLAN Ağ Mimarisi-CISCO Ağlarda VLAN (Virtual Lan) Adaptasyonu", 1-6, <https://docplayer.biz.tr/23568500-Cisco-aglarda-vlan-virtual-lan-adaptasyonu.html>.
5. "Virtual Local Area Networks (VLANs)", 25, 1-10, [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config\\_guide/sup720/15\\_1\\_sy\\_swcg\\_720/vlans.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup720/15_1_sy_swcg_720/vlans.pdf).
6. "The Virtual LAN Technology Report", decisys, 2-20, [https://perso.liris.cnrs.fr/alain.mille/enseignements/DESS/reseau\\_virtual\\_3com.pdf](https://perso.liris.cnrs.fr/alain.mille/enseignements/DESS/reseau_virtual_3com.pdf).
7. AlliedWare Plus™ OS, VLANs (Virtual LANs), Allied Telesis, 1-13, [https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/overview\\_vlans.pdf](https://www.alliedtelesis.com/sites/default/files/documents/configuration-guides/overview_vlans.pdf).
8. Gangjun Zhai, Zhu Long, Jianxun Zhong, Yunpeng Cui (2012), "Design and Research of VLAN Communication Experiment Based on the WEB Environment", 2012 International Workshop on Information and Electronics Engineering (IWIEE), 1-6, <https://www.sciencedirect.com/science/article/pii/S1877705812003475>.
9. Fatih Ertam, Türker Tuncer ve Engin Avcı (2013), "Adli Bilişimde Ağ Cihazlarının Önemi Ve Güvenilir Yapılandırmaları", E-Journal of New World Sciences Academy, 1-11, <https://dergipark.org.tr/tr/download/article-file/186061>.
10. Serdar Kırıçoğlu, Resul Kara, İbrahim Özçelik (2019), "A new SNMP-based algorithm for network traffic balancing in virtual local area networks", Journal of the Faculty of Engineering and Architecture of Gazi University, 34:1, 365-380, <https://dergipark.org.tr/tr/download/article-file/679892>.
11. Nimmagadda Lakshmi Sowjanya, Dr Raju Anitha (2020), "An Efficient VLAN Implementation to decrease Traffic Load in a Network", International Journal of Advanced Trends in Computer Science and Engineering, 9, 2, 2147-2153, <http://www.warse.org/IJATCSE/static/pdf/file/ijatse189922020.pdf>.
12. "VLANs: Virtual Local Area Networks", Logically Partitioning a Physical Network into Several Separate LANs, 31-41, [https://booksite.elsevier.com/9780123850591/Lab\\_Manual/Lab\\_04.pdf](https://booksite.elsevier.com/9780123850591/Lab_Manual/Lab_04.pdf).
13. Agwu Chukwuemeka Odi, Nweso Emmanuel Nwogbaga, Ojiugwo Chukwuka N. (2013), "The Proposed Roles of VLAN and Inter-VLAN Routing in Effective Distribution of Network Services in Ebonyi State University", 4, 7, 2608-2615, [https://www.researchgate.net/publication/329033784\\_The\\_Proposed\\_Roles\\_of\\_VLAN\\_and\\_Inter-VLAN\\_Routing\\_in\\_Effective\\_Distribution\\_of\\_Network\\_Services\\_in\\_Ebonyi\\_State\\_University](https://www.researchgate.net/publication/329033784_The_Proposed_Roles_of_VLAN_and_Inter-VLAN_Routing_in_Effective_Distribution_of_Network_Services_in_Ebonyi_State_University).
14. Dlnya Abdulahad Aziz (2018), "The Importance of VLANs and Trunk Links in Network Communication Areas", International Journal of Scientific & Engineering Research, 9, 9, 10-15, [https://www.researchgate.net/publication/327824310\\_The\\_Importance\\_of\\_VLANs\\_and\\_Trunk\\_Links\\_in\\_Network\\_Communication\\_Areas](https://www.researchgate.net/publication/327824310_The_Importance_of_VLANs_and_Trunk_Links_in_Network_Communication_Areas).
15. Nikhil Kumar H S, Dr. S.K Manju Bargavi (2021), "Inter-Vlan Routing Using Sub-Interfaces And Separate Physical Gateways", 3, 5, 3100-3103, [https://www.researchgate.net/publication/353646221\\_inter-vlan\\_routing\\_using\\_sub-interfaces\\_and\\_separate\\_physical\\_gateways](https://www.researchgate.net/publication/353646221_inter-vlan_routing_using_sub-interfaces_and_separate_physical_gateways).
16. Siti Farah binti Hussin (2020), "Virtual Lan Applications (Vlan Apps)", 26-31, [https://www.researchgate.net/publication/346331540\\_virtual\\_lan\\_applications\\_vlan\\_apps](https://www.researchgate.net/publication/346331540_virtual_lan_applications_vlan_apps).
17. Md. Turab Hossain (2020), "implementing vLAN & VPN for an organization", 1-11, [https://www.researchgate.net/publication/349411945\\_Implementing\\_vLAN\\_VPN\\_for\\_an\\_organization](https://www.researchgate.net/publication/349411945_Implementing_vLAN_VPN_for_an_organization).
18. Muhammet Baykara, Resul Daş (2019), "SoftSwitch: a centralized honeypot-based security approach using software-defined switching for secure management of VLAN networks", 27, 5, 3309 – 3325, <https://dergipark.org.tr/tr/pub/tbtkelektrik/issue/50810/662302>.
19. Gürçan Çetin, Muhammed Fatih Tarlacı, Mahmut Tenruh (2019), "Dinamik VLAN Yapılandırmasının Kablosuz Yerleşke Alan Ağlarında Performans Analizi", 11, 2, 108-117, <https://dergipark.org.tr/tr/pub/utbd/issue/49032/596199>.
20. Serdar Kırıçoğlu, Resul Kara, İbrahim Özçelik (2018), "Sanal yerel alan ağlarında ağ trafiği dengeleme için snmp tabanlı yeni bir algoritma", Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 2-22, [https://www.researchgate.net/publication/324589132\\_sanal\\_yerel\\_alan\\_aglarında\\_ag\\_trafiği\\_dengeleme\\_icin\\_snmp\\_tabanlı\\_yeni\\_bir\\_algoritma](https://www.researchgate.net/publication/324589132_sanal_yerel_alan_aglarında_ag_trafiği_dengeleme_icin_snmp_tabanlı_yeni_bir_algoritma).