Anahtarlama Temelleri (Switching Basics)

Katman 2'de (Veri Bağlantı Katmanı) çalışan switchler (anahtarlar), yerel ağdaki (LAN) cihazların birbirleriyle haberleşmesini sağlayan en temel ağ cihazlarıdır. Gelen veri çerçevelerini (frames) içindeki MAC adreslerine bakarak sadece ilgili hedefe yönlendirirler.

1. Çakışma Alanı (Collision Domain) ve Yayın Alanı (Broadcast Domain)

Ağ tasarımında ve sorun gidermede bu iki kavramı bilmek hayati önem taşır.

- **Çakışma Alanı (Collision Domain):** Ağ üzerindeki iki cihazın aynı anda veri gönderdiğinde sinyallerinin çarpışma (çakışma) ihtimalinin olduğu fiziksel alandır.
    - Hub (Dağıtıcı) kullanılan bir ağda tüm portlar tek bir çakışma alanı içindedir.
    - **Switchlerin her bir portu ayrı bir çakışma alanıdır.** Switchler, doğaları gereği çakışmaları böler ve mikro bölümler (micro-segmentation) oluşturur.
- **Yayın Alanı (Broadcast Domain):** Bir cihazın ağa gönderdiği bir "Broadcast" (bire-tüm) mesajının (örneğin bir ARP isteği veya DHCP keşif paketi) ulaşabildiği sınırların tamamıdır.
    - Switchler broadcast mesajlarını bölemez; gelen bir broadcast mesajını aldığı port hariç diğer tüm portlara iletir (Flood).
    - **Broadcast alanını yalnızca Router (Yönlendirici) veya VLAN'lar (Sanal LAN) bölebilir.** Routerların her bir bacağı ayrı bir yayın alanıdır.

2. Switch MAC Adreslerini Nasıl Öğrenir? (MAC Learning)

Switchler ağdaki cihazların nerede olduğunu **MAC Adres Tablosu (CAM Table - Content Addressable Memory)** oluşturarak öğrenir. Tablo oluşturma işlemi daima paketi gönderen cihazın adresine bakılarak yapılır.

Öğrenme ve İletme Adımları:

1. **Öğrenme (Learning):** Switch bir portundan çerçeve aldığında, çerçevenin içindeki **Kaynak MAC (Source MAC)** adresini ve o çerçevenin geldiği port numarasını MAC tablosuna kaydeder (Bu kayıtlar genellikle 5 dakika boyunca tutulur).
2. **İletme veya Taşma (Forwarding / Flooding):** Daha sonra switch, çerçevenin içindeki **Hedef MAC (Destination MAC)** adresine bakar.
    - Eğer hedef MAC adresi tabloda **varsa**, çerçeveyi sadece o hedefin bulunduğu porta yönlendirir (Forwarding / Unicast iletişim).

    - Eğer hedef MAC adresi tabloda **yoksa** (Bilinmeyen Unicast) veya hedef MAC bir Broadcast adresi ise (`FF:FF:FF:FF:FF:FF`), çerçeveyi geldiği port hariç ağdaki tüm portlara gönderir (Flooding). Hedef cihaz cevap verdiğinde onun da kaynak MAC adresini öğrenir ve tabloyu günceller.

Komut Notu: Switch üzerindeki MAC tablosunu görmek için ayrıcalıklı modda (Privileged EXEC) `show mac address-table` komutu kullanılır.

3. Duplex (Çift Yönlü İletişim) Modları

İki cihaz arasındaki veri iletiminin yönünü ve eşzamanlılığını belirler. Bağlanan cihazın portu hangi modda çalışıyorsa, switch otomatik olarak o moda geçer (Auto-negotiation).

- **Half-Duplex (Yarı Çift Yönlü):** Veri iletimi ve alımı aynı anda yapılamaz. Telsiz mantığıyla çalışır; biri konuşurken diğeri dinlemelidir. Çakışma (Collision) riski vardır (Hub'lar bu modda çalışır).
- **Full-Duplex (Tam Çift Yönlü):** Aynı anda hem veri gönderilip hem veri alınabilir. Telefon görüşmesi gibidir. Çakışma olmaz. Modern Switchler ve bilgisayarlar varsayılan olarak bu modda çalışır.

4. Çerçeve İletim Yöntemleri (Frame Forwarding Methods) *[CCNA Ek Bilgi]*

Bir switch, gelen veriyi diğer porta aktarırken arka planda iki ana yöntemden birini kullanır:

- **Store-and-Forward (Depola ve İlet):** Switch çerçevenin *tamamını* alır ve sonundaki Artbilgi (FCS) kısmına bakarak hata kontrolü yapar. Hata yoksa hedefe iletir. Güvenilirdir ancak çerçevenin boyutu büyüdükçe mikro saniyelik gecikmeler (latency) artar. Cisco switchlerin LAN ortamlarındaki varsayılan yöntemidir.
- **Cut-Through (Kestirme):** Switch sadece çerçevenin başındaki hedef MAC adresini okur okumaz (ilk 14 byte) veriyi hedefe iletmeye başlar. Hata kontrolü yapmaz. Çok hızlıdır ancak bozuk paketleri de ağa yayma riski barındırır.

Sanal Yerel Ağlar (VLAN) ve Trunking

VLAN (Virtual Local Area Network), fiziksel bir yerel ağı (LAN) mantıksal olarak daha küçük alt ağlara bölme teknolojisidir. Normalde bir switch üzerindeki tüm portlar aynı yayın alanındadır (Broadcast Domain). VLAN'lar sayesinde, aynı fiziksel switch üzerinde olsalar bile cihazları farklı ağlardaymış gibi izole edebiliriz.

VLAN Kullanmanın Avantajları:

1. **Yayın Alanını (Broadcast Domain) Küçültmek:** Ağdaki gereksiz ARP ve DHCP trafiğinin tüm ağı meşgul etmesini engeller. Her VLAN kendi başına bir yayın alanıdır.
2. **Güvenlik:** Muhasebe departmanı ile Misafir ağını birbirinden yalıtarak izinsiz erişimleri engeller.
3. **Yönetim Kolaylığı:** Cihazların fiziksel konumundan bağımsız olarak mantıksal gruplandırma yapılmasını sağlar.

1. VLAN Çeşitleri

- **Veri (Data) VLAN'ı:** Sadece kullanıcı verilerini (web trafiği, e-posta vb.) taşımak için oluşturulan VLAN'lardır.
- **Varsayılan (Default) VLAN:** Cisco switchler kutudan çıktığında tüm portlar **VLAN 1**'e atanmıştır. Silinemez veya adı değiştirilemez.
- **Native VLAN:** Trunk bağlantılarında *etiketlenmemiş (untagged)* trafiğin taşındığı VLAN'dır. Varsayılan olarak VLAN 1'dir ancak güvenlik amacıyla değiştirilmesi (örneğin VLAN 99 yapılması) önerilir.
- **Yönetim (Management) VLAN'ı:** Switchlere uzaktan erişim (SSH/Telnet) sağlamak için SVI (Switched Virtual Interface) oluşturduğumuz VLAN'dır.
- **Ses (Voice) VLAN'ı:** IP telefonlar üzerinden geçen ses trafiğine ağda öncelik (QoS - Quality of Service) tanımak için ayrılan özel VLAN'dır.

2. Temel VLAN Yapılandırması

Bir switch üzerinde VLAN oluşturmak ve bir portu o VLAN'a atamak oldukça basittir. Güvenlik en iyi uygulaması olarak, son kullanıcı cihazlarının bağlandığı portlar statik olarak `access` moduna alınmalıdır.

```
Switch(config)# vlan 10
Switch(config-vlan)# name Muhasebe
Switch(config-vlan)# exit

Switch(config)# interface fastEthernet 0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)# end
```

Doğrulama Komutu: `show vlan brief` komutu ile oluşturulan VLAN'ları ve atanan portları görebilirsiniz. `no vlan 10` komutu ile VLAN silinebilir. Birden fazla portu aynı anda yapılandırmak için `interface range fastEthernet 0/1-24` komutu kullanılır.

3. Voice (Ses) VLAN Yapılandırması

Cisco IP telefonların arkasında dahili bir mini-switch bulunur. Bu sayede duvardaki tek bir ağ prizinden hem telefona hem de bilgisayara kablo çekilebilir. Bu durumda switch portunun hem veri hem de ses trafiğini taşıması gerekir.

```
Switch(config)# interface fastEthernet 0/5
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10      (Bilgisayar için Veri VLAN'ı)
Switch(config-if)# switchport voice vlan 50       (IP Telefon için Ses VLAN'ı)
```

4. Trunking ve IEEE 802.1Q

Birden fazla VLAN'ın trafiğini iki switch arasında (veya switch ile router arasında) tek bir kablo üzerinden taşımaya **Trunking** denir.

Standart Ethernet çerçevelerinde VLAN bilgisi bulunmaz. Çerçeveler Trunk bağlantısından geçerken, switch çerçevenin içine 4 Byte'lık bir **802.1Q etiketi (Tag)** ekler. Bu etiket içinde VLAN ID'si (TCI başlığında) bulunur. Karşıdaki switch bu etiketi okur, çerçevenin hangi VLAN'a ait olduğunu anlar ve etiketi sökerek ilgili access portuna iletir. *(Not: Native VLAN trafiğine etiket eklenmez).*

Trunk Yapılandırması:

```
Switch(config)# interface gigabitEthernet 0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 99       (Güvenlik için değiştirildi)
Switch(config-if)# switchport trunk allowed vlan 10,20   (Sadece bu VLAN'lara izin ver)
```

Doğrulama Komutu: `show interfaces trunk` komutu ile trunk olan portları ve üzerinden geçmesine izin verilen VLAN'ları görebilirsiniz.

5. DTP (Dynamic Trunking Protocol)

Switch portlarının aralarında anlaşıp otomatik olarak Trunk veya Access moduna geçmesini sağlayan Cisco'ya özgü bir protokoldür.

- **Modlar:** `dynamic auto` (Karşı taraf teklif ederse trunk olur) ve `dynamic desirable` (Aktif olarak trunk olmayı teklif eder).
- **Güvenlik Riski:** DTP varsayılan olarak açıktır. Bir saldırgan bilgisayarına DTP sinyali üreten bir yazılım kurarak switch portunu trunk moduna geçirebilir ve tüm VLAN'ların trafiğini izleyebilir (VLAN Hopping Attack).
- **Çözüm (Best Practice):** Trunk portları manuel olarak `mode trunk` yapılmalı ve DTP görüşmeleri kapatılmalıdır:

Switch(config-if)# switchport nonegotiate

6. VTP (VLAN Trunking Protocol)

Ağda onlarca switch varsa, her birine tek tek bağlanıp aynı VLAN'ları oluşturmak zahmetlidir. VTP (Cisco proprietary), ağdaki bir switch'te (Server) oluşturulan, silinen veya adı değiştirilen VLAN veritabanının trunk bağlantıları üzerinden diğer tüm switchlere otomatik olarak yayılmasını (senkronize edilmesini) sağlar.

VTP Çalışma Modları:

1. **Server (Sunucu):** VTP'nin varsayılan modudur. VLAN oluşturulabilir, silinebilir ve düzenlenebilir. Değişiklikleri diğer switchlere duyurur.
2. **Client (İstemci):** Üzerinde manuel VLAN oluşturulamaz veya silinemez. Server'dan gelen güncellemeleri alır, kendi veritabanına yazar ve diğer switchlere iletir.
3. **Transparent (Şeffaf):** Bağımsızdır. VTP senkronizasyonuna katılmaz. Kendi üzerinde sadece kendisine ait lokal VLAN'lar oluşturulabilir. Ancak Server'dan gelen VTP reklam paketlerini yutmaz, içinden geçirip diğer switchlere iletir.

   Önemli Not: VTP, port atamalarını senkronize etmez, sadece VLAN ID'lerini ve isimlerini senkronize eder. VTP'nin çalışması için switchler arasındaki bağlantıların Trunk olması, VTP Domain (Alan) isimlerinin ve parolalarının aynı olması gerekir. Günümüzde VTP kullanımı yapılandırma hatalarının tüm ağı silmesi riskinden dolayı genellikle **Transparent** modda bırakılması tavsiye edilir.

VTP Yapılandırması:

Switch(config)# vtp mode server

Switch(config)# vtp domain MUSTERI_AGI

Switch(config)# vtp password cisco123

Doğrulama Komutu: `show vtp status` ve `show vtp password` komutlarıyla VTP yapılandırmasını kontrol edebilirsiniz.

Sanal Yerel Ağlar (VLAN) ve Trunking

VLAN (Virtual Local Area Network), fiziksel bir yerel ağı (LAN) mantıksal olarak daha küçük alt ağlara bölme teknolojisidir. Normalde bir switch üzerindeki tüm portlar aynı yayın

alanındadır (Broadcast Domain). VLAN'lar sayesinde, aynı fiziksel switch üzerinde olsalar bile cihazları farklı ağlardaymış gibi izole edebiliriz.

VLAN Kullanmanın Avantajları:

1. **Yayın Alanını (Broadcast Domain) Küçültmek:** Ağdaki gereksiz yayın mesajlarının tüm ağı meşgul etmesini engeller.
2. **Güvenlik:** Departmanları (Örn: Muhasebe ile Misafir ağını) birbirinden yalıtarak izinsiz erişimleri engeller.
3. **Yönetim Kolaylığı:** Cihazların fiziksel konumundan bağımsız olarak mantıksal gruplandırma yapılmasını sağlar.

1. VLAN Çeşitleri

- **Veri (Data) VLAN'ı:** Kullanıcı verilerini taşıyan standart VLAN'dır.
- **Varsayılan (Default) VLAN:** Cisco switchlerde tüm portlar varsayılan olarak **VLAN 1**'e atanmıştır. Silinemez.
- **Native VLAN:** Trunk bağlantılarından *etiketsiz (untagged)* geçen trafiğin atandığı VLAN'dır. Güvenlik için değiştirilmesi önerilir.
- **Yönetim (Management) VLAN'ı:** Switch'e uzaktan (SSH/Telnet) erişmek için sanal bir IP (SVI) atadığımız VLAN'dır.
- **Ses (Voice) VLAN'ı:** IP telefon trafiğine öncelik (QoS) tanımak için ayrılır.

2. Temel VLAN Yapılandırması ve Port Atamaları

VLAN oluştururken isimlendirmek, sorun gidermede büyük kolaylık sağlar. Son kullanıcı cihazlarının bağlandığı portlar kesinlikle `access` (erişim) modunda olmalıdır.

! Tekil VLAN Oluşturma ve İsimlendirme

Switch(config)# vlan 10

Switch(config-vlan)# name MUHASEBE

Switch(config-vlan)# exit

! Çoklu VLAN Oluşturma (Cihaz modeline göre desteklenir)

Switch(config)# vlan 20,30,40-50

Switch(config-vlan)# exit

! Tek Bir Portu VLAN'a Atama

Switch(config)# interface fastEthernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10

Switch(config-if)# exit

! Birden Fazla Portu (Range) Aynı Anda VLAN'a Atama

Switch(config)# interface range fastEthernet 0/10-20

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# switchport access vlan 20

Switch(config-if-range)# end

Doğrulama Komutları:

- `show vlan brief` : Ağdaki tüm VLAN'ları ve onlara atanmış portları özet tablo halinde listeler.
- `show vlan id 10` : Sadece 10 numaralı VLAN'ın detaylarını gösterir.
- `show interfaces fastEthernet 0/1 switchport` : İlgili portun hangi modda (Access/Trunk) çalıştığını ve hangi VLAN'da olduğunu detaylıca gösterir

3. Voice (Ses) ve Yönetim (Management) VLAN Yapılandırması

Cisco IP telefonların arkasında dahili bir switch bulunur. Bu sayede switch portunun hem veri hem de ses trafiğini aynı anda taşıması gerekir.

! Voice VLAN Yapılandırması

Switch(config)# interface fastEthernet 0/5

Switch(config-if)# switchport mode access

Switch(config-if)# switchport access vlan 10 ! (Bilgisayar için Veri VLAN'ı)

Switch(config-if)# switchport voice vlan 50 ! (IP Telefon için Ses VLAN'ı)

Switch(config-if)# exit

! Yönetim (Management) VLAN'ı için SVI (Sanal Arayüz) Oluşturma

Switch(config)# interface vlan 99

Switch(config-if)# ip address 192.168.99.10 255.255.255.0

Switch(config-if)# no shutdown

4. Trunking ve IEEE 802.1Q Etiketleme

Birden fazla VLAN'ın trafiğini iki cihaz (Switch-Switch veya Switch-Router) arasında tek bir kablo üzerinden taşımaya **Trunking** denir.

Çerçeveler Trunk bağlantısından geçerken, switch çerçevenin içine 4 Byte'lık bir **802.1Q etiketi (Tag)** ekler. Karşıdaki switch bu etiketi okur, trafiği ilgili VLAN'a ayırır.

! Temel Trunk Yapılandırması

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# switchport trunk encapsulation dot1q ! (Bazı eski cihazlarda bu komut gerekebilir)

Switch(config-if)# switchport mode trunk

! Güvenlik: Native VLAN'ı değiştirme (Varsayılan 1'den 99'a alıyoruz)

Switch(config-if)# switchport trunk native vlan 99

! Güvenlik: Sadece belirli VLAN'ların geçişine izin verme

Switch(config-if)# switchport trunk allowed vlan 10,20,30

! İzin Verilenler Listesini Düzenleme Komutları

Switch(config-if)# switchport trunk allowed vlan add 40   ! Mevcut listeye 40'ı ekler

Switch(config-if)# switchport trunk allowed vlan remove 20 ! Listeden 20'yi çıkarır

Switch(config-if)# switchport trunk allowed vlan all ! Tümüne tekrar izin verir

Switch(config-if)# end

5. DTP (Dynamic Trunking Protocol)

Switch portlarının otomatik olarak Trunk veya Access moduna geçmesini sağlayan Cisco protokolüdür.

- Güvenlik açığı (VLAN Hopping Attack) yaratmaması için **Trunk bağlantılarında DTP kapatılmalıdır.**

Switch(config)# interface gigabitEthernet 0/1

Switch(config-if)# switchport mode trunk

Switch(config-if)# switchport nonegotiate ! DTP paketleri gönderilmesini engeller

6. VTP (VLAN Trunking Protocol)

Ağdaki bir switch'te (Server) oluşturulan VLAN veritabanının, trunk bağlantıları üzerinden diğer tüm switchlere otomatik olarak kopyalanmasını sağlar. **VTP port atamalarını kopyalamaz, sadece VLAN ID'lerini kopyalar.**

- **Modlar:** `Server` (Oluşturur/Dağıtır), `Client` (Sadece alır/İletir, VLAN oluşturulamaz), `Transparent` (Bağımsızdır, kendi VLAN'larını kurar, VTP mesajlarını sadece içinden geçirir).

! VTP Server (Sunucu) Yapılandırması

Switch(config)# vtp mode server

Switch(config)# vtp domain SIRKET_AGI ! Domain adı birebir aynı olmalıdır

Switch(config)# vtp password cisco123 ! Parolalar aynı olmalıdır

Switch(config)# vtp version 2 ! (Opsiyonel) VTP versiyonunu belirler

! VTP Client (İstemci) Yapılandırması (Diğer Switch'te)

Switch2(config)# vtp mode client

Switch2(config)# vtp domain SIRKET_AGI

Switch2(config)# vtp password cisco123

Doğrulama Komutları:

- `show vtp status` : Switch'in VTP modunu, domain adını ve senkronizasyon (Configuration Revision) numarasını gösterir.
- `show vtp password` : Yapılandırılan VTP parolasını gösterir.

Spanning Tree Protocol (STP) ve Döngü Koruması

Ağ tasarımında yedeklilik (redundancy) çok önemlidir. Bir kablo koptuğunda veya bir switch arızalandığında ağın çalışmaya devam etmesi için switchler arasına yedek kablolar çekilir. Ancak Katman 2'de (Ethernet) paketlerin yaşam süresini (TTL - Time to Live) belirten bir mekanizma yoktur. Bu yüzden yedekli yollar, ağda sonsuza kadar dönen **Katman 2 Döngülerine (Layer 2 Loops)** ve **Yayın Fırtınalarına (Broadcast Storms)** sebep olur. Bu da ağı saniyeler içinde çökertir.

STP (IEEE 802.1D), yedekli fiziksel yolları tespit edip bazı portları mantıksal olarak "engelleyerek" (blocking) döngüleri önleyen ve ağda tek bir aktif yol bırakan protokoldür. Aktif yolda bir kopukluk olursa, engellenen portu otomatik olarak açarak iletişimin devam etmesini sağlar.

1. STP Nasıl Çalışır? (Spanning Tree Algoritması)

Switchler ağın topolojisini çıkarmak ve hangi portun engelleneceğine karar vermek için birbirlerine her 2 saniyede bir **BPDU (Bridge Protocol Data Unit)** adı verilen özel paketler gönderirler.

STP'nin algoritması şu 4 adımla işler:

Adım 1: Root Bridge (Kök Köprü) Seçimi

Ağdaki tüm switchler içinden bir tanesi "Ağın Patronu" yani **Root Bridge** olarak seçilir. Seçim kriteri **Bridge ID (Köprü Kimliği)** değeridir.

- **Bridge ID = Priority (Öncelik) + MAC Adresi**
- Varsayılan Priority değeri tüm switchlerde **32768**'dir. Priority değeri 4096'nın katları şeklinde artırılıp azaltılabilir.

- Seçim Kuralı: Bridge ID'si (Öncelikle Priority'si, eşitse MAC adresi) **EN DÜŞÜK** olan switch Root Bridge seçilir.

Adım 2: Root Port (Kök Port) Seçimi

Root Bridge seçildikten sonra, diğer tüm switchler (Non-Root Bridges) köprüye giden **en kısa maliyetli (Path Cost)** portlarını **Root Port (RP)** olarak seçerler. Her switch'in sadece 1 tane Root Port'u olabilir.

- *Maliyetler (Cost):* 10 Mbps = 100 | 100 Mbps (FastEthernet) = 19 | 1 Gbps (Gigabit) = 4 | 10 Gbps = 2

Adım 3: Designated Port (Atanmış Port) Seçimi

Ağdaki her bir fiziksel segment (kablo) için trafiği Root Bridge'e doğru iletecek tek bir **Designated Port (DP)** seçilir. Root Bridge'in tüm portları her zaman DP'dir.

Adım 4: Alternate / Blocked Port (Engellenen Port) Seçimi

Root Port veya Designated Port seçilemeyen geri kalan tüm portlar **Engellenen Port (Blocked/Alternate Port)** durumuna düşer. Bu portlardan veri trafiği akmaz, sadece BPDU paketleri dinlenir (Yedekte bekler).

2. STP Çeşitleri (Protokol Türleri)

- **STP (802.1D):** Orijinal standarttır. Tüm VLAN'lar için tek bir ağaç oluşturur (CST). Yakınsama (ağın toparlanma) süresi çok uzundur (30-50 saniye).
- **PVST+ (Per-VLAN Spanning Tree):** Cisco'nun varsayılan standardıdır. Her VLAN için ayrı bir STP algoritması çalıştırır. (Örn: VLAN 10 için soldaki yol açıkken, VLAN 20 için sağdaki yolu açarak yük dengelemesi yapabilirsiniz).
- **RSTP (802.1w - Rapid STP):** STP'nin gelişmiş halidir. Yakınsama süresini saniyenin altına indirir.
- **Rapid PVST+:** Cisco cihazlarda her VLAN için ayrı çalışan hızlı STP standardıdır. **Modern ağlarda kullanılması önerilen moddur.**
- **MSTP (802.1s - Multiple STP):** Çok sayıda VLAN'ı gruplayıp tek bir STP örneğine (instance) bağlayarak işlemci yükünü azaltır.

3. STP / Rapid PVST+ Yapılandırması ve Doğrulama

Genellikle Root Bridge seçimini şansa (veya en eski, MAC adresi en düşük olan zayıf bir switch'e) bırakmamak için merkezdeki (Core/Distribution) güçlü switch manuel olarak Root Bridge yapılır.

```
! Tüm switchlerde STP modunu Rapid PVST+ olarak ayarlama (Best Practice)
Switch(config)# spanning-tree mode rapid-pvst

! Bir switch'i manuel olarak Root Bridge (Kök Köprü) yapma
```

! Yöntem 1: Priority değerini düşürerek (Varsayılan 32768'den küçük bir 4096 katı verilir)
Switch(config)# spanning-tree vlan 1 priority 4096

! Yöntem 2: Makro komut kullanarak (Cisco arka planda priority'i otomatik ayarlar)
Switch(config)# spanning-tree vlan 1 root primary

! Yedek Switch'i Secondary Root Bridge yapma (Birincisi çökerse bu devralır)
Switch(config)# spanning-tree vlan 1 root secondary

Doğrulama Komutu: `show spanning-tree` veya belirli bir vlan için `show spanning-tree vlan 1` *Bu komut çıktısında switch'in Root olup olmadığını ("This bridge is the root"), port rollerini (Desg, Root, Altn) ve durumlarını (FWD, BLK) görebilirsiniz.*

4. PortFast ve BPDU Guard Yapılandırması (STP Güvenliği)

Uç cihazların (Bilgisayar, Yazıcı, IP Telefon) bağlandığı Access (Erişim) portlarında STP'nin çalışmasına ve hesaplama yapmasına gerek yoktur. Çünkü bir bilgisayar ağda döngü (loop) yaratmaz.

- **PortFast:** Bilgisayar bağlanan bir portun 30 saniyelik Dinleme ve Öğrenme (Listening/Learning) aşamalarını atlayarak anında İletim (Forwarding) durumuna geçmesini sağlar. Aksi takdirde bilgisayar açıldığında 30 saniye boyunca IP adresi alamaz (DHCP zaman aşımına uğrar).
- **BPDU Guard:** PortFast etkinleştirilmiş bir porta yanlışlıkla başka bir switch (veya hub) takılırsa ağ loop'a girebilir. BPDU Guard, uç portlardan BPDU paketi (switch sinyali) geldiği an portu koruma amacıyla **hata nedeniyle kapatır (err-disable)**.

Uygulama Adımları (Sadece Access Portlarına Uygulanmalıdır!):

! Arayüz Bazında PortFast ve BPDU Guard Yapılandırması
Switch(config)# interface range fastEthernet 0/10-24
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# spanning-tree portfast ! Portu anında açar
Switch(config-if-range)# spanning-tree bpduguard enable ! İzinsiz switch takılmasını önler
Switch(config-if-range)# exit

! Global Olarak (Tüm Access Portlarında) Etkinleştirme Kısayolu
Switch(config)# spanning-tree portfast default
Switch(config)# spanning-tree portfast bpduguard default

Sorun Giderme Notu: BPDU Guard nedeniyle kapanan (err-disable durumuna düşen) bir portu tekrar açmak için fiziksel müdahaleden (izinsiz takılan switch'i söktükten) sonra portun içine girip sırayla `shutdown` ve ardından `no shutdown` komutları yazılmalıdır.

EtherChannel (Bağlantı Kümeleme) ve Yük Dengeleme

Switchler arasına bant genişliğini (hızı) artırmak ve yedeklilik sağlamak için birden fazla kablo çektiğimizde, Spanning Tree Protocol (STP) döngü (loop) oluşmasını engellemek için bu kablolardan sadece birini açık bırakır, diğerlerini kapatır (bloklar).

EtherChannel, birden fazla fiziksel portu (kabloyu) mantıksal olarak tek bir portmuş (Port-Channel) gibi birleştirme teknolojisidir.

- STP, bu birleştirilmiş port grubunu tek bir kablo olarak gördüğü için hiçbirini kapatmaz.
- Hem boşta yatan kablolar kullanılarak hız katlanır (Örn: 4 adet 1 Gbps kablo = 4 Gbps mantıksal hız), hem de kablolardan biri koparsa sistem kesintiye uğramadan kalan kablolardan trafiği iletmeye devam eder.

1. EtherChannel Oluşturma Ön Koşulları

İki switch arasında EtherChannel kurulabilmesi için birleştirilecek tüm fiziksel portların **birebir aynı özelliklere** sahip olması gerekir. Aksi takdirde portlar "err-disable" (hata) durumuna düşer.

1. **Hız ve Duplex:** Tüm portların hızları (Örn: 1000 Mbps) ve Duplex modları (Full-Duplex) aynı olmalıdır.
2. **VLAN Eşleşmesi:** Tüm portlar aynı Access VLAN'a atanmış olmalı veya tümü Trunk modunda olmalıdır.
3. **Trunk Özellikleri:** Eğer portlar Trunk ise, izin verilen VLAN (Allowed VLAN) listeleri ve Native VLAN'ları aynı olmalıdır.

2. EtherChannel Protokolleri ve Modları

EtherChannel statik olarak (protokolsüz) kurulabileceği gibi, switchlerin karşılıklı anlaşıp hataları tolere etmesini sağlayan dinamik protokollerle de kurulabilir.

A. LACP (Link Aggregation Control Protocol)

- **Standardı:** IEEE 802.3ad (Açık standarttır. Cisco ile HP, Juniper gibi farklı marka switchler arasında kullanılabilir. **Modern ağlarda en çok tercih edilen protokoldür.**)
- **LACP Modları:**
    - **Active (Aktif):** Karşı tarafa aktif olarak LACP paketi gönderir ve EtherChannel kurmayı teklif eder.
    - **Passive (Pasif):** Beklemededir. Sadece karşıdan LACP teklifi gelirse kabul edip EtherChannel kurar.

B. PAgP (Port Aggregation Protocol)

- **Standardı:** Cisco Proprietary (Sadece Cisco cihazlar arasında çalışır).
- **PAgP Modları:**
    - **Desirable (İstekli):** Karşı tarafa aktif olarak PAgP paketi gönderir ve EtherChannel kurmayı teklif eder.
    - **Auto (Otomatik):** Beklemededir. Sadece karşıdan PAgP teklifi gelirse kabul edip EtherChannel kurar.

C. Statik (Protokolsüz - No Protocol)

- **Mod: On (Açık):** Herhangi bir protokol kullanılmaz, paket gönderilmez. Portlar zorla EtherChannel moduna sokulur. Karşı tarafın hatalı yapılandırılması ağda döngülere (loop) sebep olabilir. Önerilmez.

Önemli Eşleşme Kuralı: > İki taraf da Pasif (veya Auto) olursa, ikisi de birbirinden teklif bekleyeceği için EtherChannel **KURULAMAZ**. En az bir tarafın Aktif (veya Desirable) olması şarttır.

3. EtherChannel Yapılandırması (LACP Örneği)

En iyi uygulama (Best Practice) olarak LACP kullanılarak iki switch arasında yapılandırma adımları:

```
! Switch 1 Yapılandırması (Active Mod)
Switch1(config)# interface range gigabitEthernet 0/1-4
Switch1(config-if-range)# channel-group 1 mode active   ! LACP kullanılarak Grup 1 oluşturuldu
Switch1(config-if-range)# exit

! Oluşan Sanal Portun (Port-Channel 1) İçine Girip Trunk Yapma
Switch1(config)# interface port-channel 1
Switch1(config-if)# switchport mode trunk
Switch1(config-if)# switchport trunk allowed vlan 10,20,30
Switch1(config-if)# exit

! Switch 2 Yapılandırması (Passive veya Active Mod)
Switch2(config)# interface range gigabitEthernet 0/1-4
Switch2(config-if-range)# channel-group 1 mode passive  ! LACP Pasif mod
Switch2(config-if-range)# exit

Switch2(config)# interface port-channel 1
Switch2(config-if)# switchport mode trunk
```

4. Doğrulama ve Sorun Giderme (Troubleshooting)

EtherChannel yapılandırmasını kontrol etmek için kullanılan en kritik komut şudur:

Switch# show etherchannel summary

Bu komutun çıktısında portların yanındaki bayraklara (Flags) dikkat edilmelidir:

- **(SU) - Layer 2 (S) / In Use (U):** Her şey yolunda, EtherChannel Layer 2 modunda sorunsuz çalışıyor demektir.
- **(SD) - Layer 2 (S) / Down (D):** Port-Channel kapalı veya kurulamamış demektir. (Hız/VLAN uyuşmazlığı olabilir).
- **(I) - Stand-alone:** Fiziksel port gruptan düşmüş ve tek başına çalışıyor demektir.

Diğer Faydalı Doğrulama Komutları:

- `show etherchannel port-channel` : Bağlantı noktasının detaylarını, kullanılan protokolü ve sanal portun durumunu gösterir.
- `show interfaces port-channel 1` : Mantıksal portun toplam hızını ve MAC adresini gösterir.