CİSCO SWİTCH KOMUTLARI

**HAZIRLAYAN**

İbrahim Can MERCAN

İçindekiler

[1. Cisco Switch’e RS232 ile Bağlantı 3](#_Toc162517677)

[2. Switch’de Modlar 4](#_Toc162517678)

[3. Cisco Komutları 4](#_Toc162517679)

[3.1 Bir Porta Bağlanmak 4](#_Toc162517680)

[3.2 Switch içerisinde Saat ayarlama 5](#_Toc162517681)

[3.3interface vlan 1 sanal portu açma 5](#_Toc162517682)

[3.4 Switch’e Parola Verme Komutları 5](#_Toc162517683)

[3.5 Switch’e Telnet ile Bağlanma 5](#_Toc162517684)

[3.6 Enable Ayrıcalıklı Moda Parola Verme 5](#_Toc162517685)

[3.7 Tüm Parolaları Encrypt Yapma Komutu 5](#_Toc162517686)

[3.8 Gateway Yapılandırma Komutu 6](#_Toc162517687)

[3.9 Rastgele Sorgu Önleme 6](#_Toc162517688)

[3.10 Switch Hostname Değiştirme ve Ekstra Komutlar 6](#_Toc162517689)

[3.11 Yaptığımız Konfigurasyonları Kaydetmek 6](#_Toc162517690)

[3.12 Vlan Tanımlama 6](#_Toc162517691)

[3.13Port 1/0/1 i Access Mode’a alma 7](#_Toc162517692)

[3.14 Ekstra Komutlar 7](#_Toc162517693)

[3.15 Switchlerimizde 1 numaralı gigabit portları Trunk yapma işlemi 7](#_Toc162517694)

[3.16Native Vlan 8](#_Toc162517695)

[3.17 Ekstra Notlar 8](#_Toc162517696)

[3.18 Cisco DTP (Dinamik Trunk Protokolü) 8](#_Toc162517697)

[3.19 Cisco VTP (VLAN Trunk Protokolü) 9](#_Toc162517698)

[3.20 Switch Potlarını Aralık belirleyerek Konfigure Etme 9](#_Toc162517699)

[3.21 İp Yönlendirme 9](#_Toc162517700)

[3.22 Cisco Switch Port Güvenlik Kodları 9](#_Toc162517701)

[3.23 DHCP Snooping Yapılandırması 10](#_Toc162517702)

[3.24 Cisco Switch Ssh Yapılandırması 10](#_Toc162517703)

[3.25 Cisco Switch ACL 10](#_Toc162517704)

[3.26 VOİCE VLAN 11](#_Toc162517705)

[3.27 Vlan Güvenliği 11](#_Toc162517706)

[3.28 Spanning Tree 11](#_Toc162517707)

[3.29 RAPİD SPANNİNG TREE 12](#_Toc162517708)

[3.30 EtherChannel 12](#_Toc162517709)

[3.31 Switch Resetleme Komutları 12](#_Toc162517710)

[3.32 Porta ip Adresi verme 12](#_Toc162517711)

[3.33 Cisco Switch Yedekleme Komutları 13](#_Toc162517712)

[3.34 Switch içerisindeki Dosyaları görme Komutu 13](#_Toc162517713)

[3.35 Cisco Switch e Yeni version kopyalama 13](#_Toc162517714)

[3.36 Cisco Switch DHCP Yapılandırması 13](#_Toc162517715)

[3.37 Cisco CDP ile Cihaz keşfi. Cisco Discovery Protokol 14](#_Toc162517716)

[3.38 Cisco Switch Parola Kurtarma 14](#_Toc162517717)

[3.39 NTP Yapılandırma (Network Time Protokol 14](#_Toc162517718)

[3.40 Cisco Switch SYSLOG Yapılandırması 15](#_Toc162517719)

[3.41 Switch arayüzü kapatma 15](#_Toc162517720)

[3.42 İGMP SNOOPİNG 15](#_Toc162517721)

[4. Cisco’da Siber Güvenlik için Gerekli Konfigurasyon Ayarları 16](#_Toc162517722)

[4.1 Cisco CAM savunması: 16](#_Toc162517723)

[4.2 Cisco CDP Savunması**:** 16](#_Toc162517724)

[4.3 DHCP Savunması**:** 16](#_Toc162517725)

[4.4 ARP Savunması 17](#_Toc162517726)

[4.5 SPOOFFİNG Savunması DTP (Dynamic Trunk Protocol): 17](#_Toc162517727)

[4.6 VTP Savunması: 17](#_Toc162517728)

[4.7 STP Savunması Spanning Tree Protocol 17](#_Toc162517729)

[5. Bir Ağın Yapı Yapılandırılması 18](#_Toc162517730)

**ÖNSÖZ**

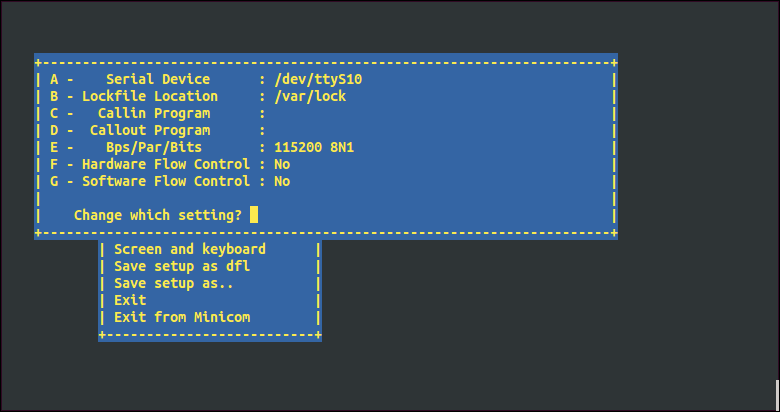
Bu dökümanı, gemi içerisinde, belli cisco switch komutlarının kullanımını görmek ve switch yapılandırmasına yardımcı olacağını düşündüğüm için hazırladım. Döküman içerisinde komutların kullanımını kalın yazı tipiyle işaretleyip , normal yazı ile yanlarına işlevleri ile alakalı notlar çıkardım.

# Cisco Switch’e RS232 ile Bağlantı

Cisco Switch sıfırdan kurulurken **mavi konsol kablosu(RS232)** , Cisco Switch arkasındaki **konsol portuna** takılarak kurulmaktadır. Pc ‘mize bu kabloyu çevirici yardımıyla taktığımızda, hangi bağlantı noktasının oluştuğuna dikkat edilmelidir. Windows’ta aygıt yöneticisinden bağlantı noktalarına bakarak kontrol edebiliriz.

Linux’ta dmesg ile bağlantı noktasını kontrol ederek Minicom programında bu bağlantı noktasını konfigürasyonda bağlantı tanımıyla set etmemiz gerekmektedir. Baud ayarını da 9600 yapmaya özen göstermeliyiz.

Windows’ta **putty** , Linux’ta **minicom** programları yardımıyla switch’e bağlanabiliriz. Cisco switch’e bağlandığımızda işletim sistemi iostur. İos açılımı **internetwork Operation System’dir**.



Resimde görüldüğü üzere Bps/Par/Bits kısmını 115200 olarak gözüküyor . Bunu 9600 olarak güncellememiz gerekmektedir. Ayrıca seri bağlantı kısmımız doğru değilse kontrolünü sağlayıp doğru seri device name i girmemiz gerekmektedir.

# Switch’de Modlar

* Switch’e ilk bağlandığımızda **switch>** olarak gözükmektedir. Bu modun adı User exe moddur.Bu modda yapılandırma yapılmamaktadır. Sadece belli görüntüleme işlemleri yapılmaktadır.
* **Enable** komutuyla ayrıcalıklı moda geçeriz . Bu modda olduğumuzu **switch#** diez işaretinden anlarız.
* Genel yapılandırma moduna geçmek için **configuration terminal** yazmalıyız. Bu komutu yazdığımızda terminal sol satırı **Switch(config) #** olarak gözükmektedir.

# Cisco Komutları

## Bir Porta Bağlanmak

**Switch> enable**

**Switch # configuration terminal**

**Switch(config) # interface fastEthernet 1/0/1** switchin 1/0/1. Numaralı portu içerisine yapılandırma için girer.

**Switch(config) # exit** çıkış için kullanılır.

--------------------------------------

**NOT:** Komutları kullanırken soru işareti ? kullandığımızda kullanabileceğimiz komut varyasyonlarını gösterir.

## Switch içerisinde Saat ayarlama

**Switch> Show clock**  switch saat bilgisini gösterir.

**Switch> Clock set 08:36 Feb 12 2024**  komutuyla saati değiştirebiliriz.

## 3.3interface vlan 1 sanal portu açma

**Switch(config) # interface vlan 1**  varsayılan vlandır.

**Switch(config-if) # ip adress 192.168.1.58 255.255.255.0** interface vlan 1 e ip tanımı yapılması.

**Switch(config-if) # no shutdown** interface vlan 1 sanal portu açma komutu.

**Switch # Show ip interface bri** Özet olarak interface’lerin ip yapılandırmasını göster komutu.

## 3.4 Switch’e Parola Verme Komutları

**Switch (Config)# line vty 0 4** Aynı anda 5 tane terminal kullanılır . 0 1 2 3 4

**Switch (Config-line)# password cisco** parolayı cisco verdik.

**Switch (Config-line)# login**  girişte login ekranında bu parolayı sor dedik.

## 3.5 Switch’e Telnet ile Bağlanma

Önceki Vlan 1 ‘e verdiğimiz ip üzerinden telnet ile switche bağlanabiliriz.

**telnet 192.168.1.58**  diyerek switch ekranına bağlanabiliriz. Bize parola soracaktır. Parolayı cisco olarak belirlemiştik.

## 3.6 Enable Ayrıcalıklı Moda Parola Verme

**Switch (Config)# enable password cisco**  bu komutlada enable parolasını da cisco olarak ayarlayabiliriz.

**Switch (Config)# enable secret cisco1** Burdada enable secret parolası veririz . Bu parola encrypt olarak gözükür.

**Switch # Show run** Bu komutu kullandığımızda secret parolası gözükmez.

## 3.7 Tüm Parolaları Encrypt Yapma Komutu

**Switch (Config)# service password-encryption** Bu komutla verdiğimiz ve vereceğimiz bütün parolalar encrtypt edilir.

Bu şifreli parolaları cisco type 7 password decrypt Google da aratarak çok rahat kırabiliriz.

## 3.8 Gateway Yapılandırma Komutu

WAN wide area network’ten switchimize bağlanmak istediğimizde default bir gateway olması gerekmektedir. Bunu ‘da router da yapılandırmaktayız.

**Switch (Config)# ip default-gateway 192.168.1.1**  ağ dışından bağlanma ayarını yapmış olduk.

## 3.9 Rastgele Sorgu Önleme

**Switch> ASD**  Bu şekilde rastgele bir sorgu yaptığımızda switch bunu çözümlemeye çalışmaktadır. Bunu iptal edebilmek için:

**Switch (Config)# no ip domain-lookup** Bu komut ile artık Dns ten bu sorguları çözmeye uğraşmayacaktır.

## 3.10 Switch Hostname Değiştirme ve Ekstra Komutlar

**Switch (Config)# hostname icm-SW1** Bu komut switch adını icm-SW1 olarak konfigure etmeye yarar.

**İcm-SW1 (Config)# line console 0** dediğimizde konsol erişimini konfigure ederiz.

**İcm-SW1 (Config-line)# password konsol** konsola bağlandığımızda parolayı koyduk.

**İcm-SW1 (Config)# login** Belirlediğimiz parolayı sorması için kullanmamız gereken komuttur.

**İcm-SW1 (Config)#exec-timeout 4** Switche bağlanıp 4 dakika bir işlem yapmadığımızda oturum kapanmaktadır.

**İcm-SW1(config)# banner motd !Yetkisiz Giriş Yasaktır.!** Switche bağlanırken banner olarak gözükür.

## 3.11 Yaptığımız Konfigurasyonları Kaydetmek

**İcm-SW1 # copy running-config startup-config** Yaptığımız değişiklikleri konfigirasyon dosyasına kaydeder.

**İcm-SW1 # wr** Yaptığımız değişiklikleri konfigirasyon dosyasına kaydeder. WRİTE

## 3.12 Vlan Tanımlama

**İcm-SW1> en**

**İcm-SW1 # conf t**

**İcm-SW1(config) # vlan 10** 10 adında vlan tanımlar

**İcm-SW1(config-vlan) # Name HVL** vlan 10 adını HVL yapar.

iki farklı VLAN'daki makinelere aynı ip'yi verebilir miyiz?

Bu vlanlar arasında erişim varsa ip çakışması olacağından aynı ip yi veremeyiz. Eğer vlanlar arası bir erişim yoksa aynı ipleri verebiliriz.

**-\*-\*-\*-\*-\***

## 3.13Port 1/0/1 i Access Mode’a alma

**Switch’lerin arayüzlerini son kullanıcı aygıtları için yapılandırmak isterseniz, o portları Access Port olarak belirlemeniz gerekir.**

**İcm-SW1> en**

**İcm-SW1 # conf t**

**İcm-SW1 (config)# interface fastEthernet 1/0/1**

**İcm-SW1(config-if)# switchport mode Access**

**İcm-SW1(config-if)# switchport Access vlan 10** 1/0/1 portunu vlan 10 a atadık .

## 3.14 Ekstra Komutlar

**İcm-SW1 # Show vlan** bu komut ile ilgili vlanları görebiliriz.

**İcm-SW1 # conf t**

**İcm-SW1 (config) # no vlan 10** vlanı siler.

**İcm-SW1 (config) # end**

**İcm-SW1 (config) # do wr** bu komutla bir üst modda yazacağımız kodları yazabiliriz. Wr kaydetme komutu.

## 3.15 Switchlerimizde 1 numaralı gigabit portları Trunk yapma işlemi

2 Switchi birbirine bağlarken tanımlı olan vlanların geçmesi için switchlerin birbirine bağlı olduğu portlar trunk olmalıdır.

Trunk Portta VLAN bilgisi Port üzerinden geçmeden önce kapsülleme işlemine uğrar ve bu kapsülleme (Encapsulation) ISL ya da 802.1Q’dur.

**İcm-SW1> en**

**İcm-SW1 # conf t**

**İcm-SW1(config) # interface gigabitEthernet 1/0/1**

**İcm-SW1(config) # switchport mode trunk**

**İcm-SW1(config) # end**

## 3.16Native Vlan

Trunk bağlantısı olarak yapılandırılan portlar üzerinde 802.1Q ve ISL tag’leri geçebilir. Fakat, iki Switch arasında Trunk bağlantısı yapılandırılmadıysa, sadece Native VLAN yani VLAN1 üzerindeki bilgisayarlar haberleşebilir.

Native VLAN tag’sız bir VLAN’dır. Switch’lerde varsayılan olarak VLAN1 aktiftir ve tag’sız olduğu için, iki Switch arasındaki iki bilgisayar herhangi bir işleme uğramadan haberleşebilirler.

Herhangi bir vlan etiketine sahip olmayan frameler , bunların trunk portlardan geçmesi için kullanılmaktadır.

## 3.17 Ekstra Notlar

**İcm-SW1 # Show interfaces trunk** Trunk olan portların bilgilerini görüntüler.

**İcm-SW1 # Show interfaces gigabitEthernet 1/0/1 switchport**  Daha ayrıntılı bilgi gösterir.

**İcm-SW1(config) # interface gigabitEthernet 1/0/1**

**İcm-SW1(config) # switchport trunk allowed vlan 10**  Sadece vlan 10 trafiği diğer switche geçsin. Diğer switchde de yapılmalıdır.

**İcm-SW1(config) # switchport trunk allowed vlan add 20** vlan 20 yi ekler

**İcm-SW1(config) # end**

## 3.18 Cisco DTP (Dinamik Trunk Protokolü)

Bir switch de diğer switch e bağlı portu trunk yaptığımızda karşınında otomatik trunk olmasını sağlayan protokol.

Bunu kapatmak için:

**İcm-SW1(config) # switchport nonegotitate**

-\*-\*-\*-\*-\*

## 3.19 Cisco VTP (VLAN Trunk Protokolü)

Bir sw de diğer sw ye bağlı portu trunk yaptığımızda karşınında otomatik vlanları almasını sağlayan protokol.Varsayılan olarak tüm sw lerde server olarak gelir.

**İcm-SW1(config) # vtp domain icm.com**

**İcm-SW1(config) # vtp mode server** vlan trunk protokülünde sw yi server yapar.

**İcm-SW1(config) #vtp mode client** vlan trunk protokülünde sw yi client yapar.

**İcm-SW1(config) #vtp mode transparant** vlan trunk protokülünde sw yi transparant köprü yapar. Bu yapılandırma olduğunda 2 switch arasında bağlantıyı sağlayan switch için yapılır. Bu moddaki switch bilgileri kendi veri tabanına yazmaz.

**İcm-SW1(config) #vtp password 123** vtp ye parola koyar

**İcm-SW1# Show vtp status** vtp ile ilgili durumu gösterir.

## 3.20 Switch Potlarını Aralık belirleyerek Konfigure Etme

**İcm-SW1(config) # interface range fastEthernet 1/0/1-10** Switchin 10 portunu aynı anda konfigure etmeye yarar.

**İcm-SW1(config-if-range) # switchport mode access**

## 3.21 İp Yönlendirme

**İcm-SW1(config)# ip routing** ip yönlendirmeyi aktif hale getirir.

**İcm-SW1(config)#interface vlan 10**

**İcm-SW1(config)#ip address 192.168.10.1 255.255.255.0**

**İcm-SW1(config)# no sh**  vlan 10 için gateway ip oluşturduk.

## 3.22 Cisco Switch Port Güvenlik Kodları

**İcm-SW1(config)# interface fastEthernet 1/0/1**

**İcm-SW1(config-if)# switchport port-security mac-address sticky**

**İcm-SW1(config-if)# switchport port-security maximum 1**

**İcm-SW1(config-if)# switchport port-security violation shutdown/protect/restrict**

**İcm-SW1(config-if)# do Show port-security interface fastEthernet 1/0/1**

Port herhangi bir durumda kapandığında o porta gidip shutdown no shutdown yapmak gerekmektedir.

-\*-\*-\*-\*-\*-

## 3.23 DHCP Snooping Yapılandırması

Bir ağda dhcp server kullanırken güvenlik açısından yapılması gereken yapılandırmadır.

**İcm-SW1(config)# ip dhcp snooping vlan 1**

**İcm-SW1(config)#int fa1/0/4**  dhcp sunucunun switche bağlı olduğu port

**İcm-SW1(config)#ip dhcp snooping trust**

**-\*-\*-\*-\*-\***

## 3.24 Cisco Switch Ssh Yapılandırması

**NOT: Bu yapılandırmayı yaparken hostname ve domain name girmemiz gerekir.**

**İcm-SW1(config)#crypto key generate rsa**

**İcm-SW1(config)# username admin**

**İcm-SW1(config)# user name admin password cisco**

**İcm-SW1(config)#enable secret cisco**

**İcm-SW1(config)# line vty 0 4**

**İcm-SW1(config)#login local**

**İcm-SW1(config-line)#transport input ssh**

**İcm-SW1(config-line)#exit**

**İcm-SW1(config)#interface vlan 1**

**İcm-SW1(config-if)#ip address 192.168.1.10 255.255.255.0**

**İcm-SW1(config-if)#no sh**

**İcm-SW1(config)#exit**

## 3.25 Cisco Switch ACL

**Access list izni ssh için izin verilen ip yi gireriz.**

**İcm-SW1(config)#access-list 1 permit 192.168.1.2**

**İcm-SW1(config)#line vty 0 4**

**İcm-SW1(config-line)#access-class 1 in**

**İcm-SW1(config-line)#end**

## 3.26 VOİCE VLAN

Voice vlanı tanımlarken tanımladığımız portlara

**İcm-SW1(config)#switchport voice vlan 3**  şeklinde tanımlıyoruz.

## 3.27 Vlan Güvenliği

**İcm-SW1(config-if )#switchport trunk allowed vlan 1,10,20**  Trunk olan porttan geçecek vlanlara izin verme.

## 3.28 Spanning Tree

Switchler arasında lopları broadcast stormları, MAC adresi kopyalamayı , güvenlik açıklarını engellemek, döngüleri engellemek için yapılmış bir protokoldür.

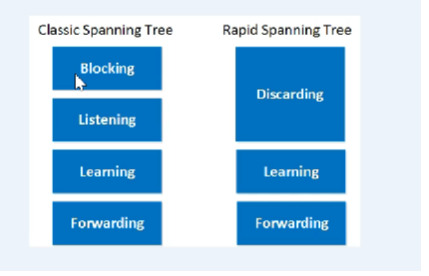
**İcm-SW1# sh spanning tree**  yapılandırmayı gösterir. Bu yapılandırmada switchlerden birisi root-bridge olarak seçilir.

**İcm-SW1(config)# spanning-tree vlan 1 priority 4096**

**İcm-SW1(config)# spanning-tree portfast**

-\*-\*-\*-\*

## 3.29 RAPİD SPANNİNG TREE



**İcm-SW1(config)#spanning-tree mode rapid-pvst**

## 3.30 EtherChannel

Switchler arası 1 den fazla link kullanmamızı sağlar. Konfigure ettiğimiz 2 portu spanning tree protokolü tek bir port gibi gösterir. Ve Portlar down olmaz.

**İcm-SW1(config)#interface range fastEthernet 0/1-2**

**İcm-SW1(config-if-range)# channel-group 1 mode on**

**İcm-SW1(config-if)#switchport trunk encapsulation dot1q**

**İcm-SW1(config-if)#switchport mode trunk**

2 switchtede yapılmalıdır.

**İcm-SW1# Show etherchannel summary** etherchannel statüsünü gösterir.

-

## 3.31 Switch Resetleme Komutları

**İcm-SW1# erase startup-config**

**İcm-SW1#delete vlan.dat**

**İcm-SW1#reload**

## 3.32 Porta ip Adresi verme

Örneğin switchimizin 3 nolu portuna ip vermek istiyoruz. Bunun için:

**İcm-SW1(config)# interface fastEthernet 1/0/3**

**İcm-SW1(config-if)#no switchport**

**İcm-SW1(config-if)# ip address 172.11.123.3 255.255.255.0**

**İcm-SW1(config-if)#no sh**

**İcm-SW1(config-if)#do Show ip route**  komutuyla ip yi porta atanmış olarak görüyoruz.

**-\*-\*-\*-\***

**Ek Bilgi :**  Switch içerisinde sunucuya ping atabilmekteyiz.

## 3.33 Cisco Switch Yedekleme Komutları

**İcm-SW1# copy running-config tftp:**  komutu koştuğumuzda tftp ip adresi ve dosya ismi ister. Tamamlayarak kopyalamayı yapabiliriz.

Tftp sunucudan switche kopyalama içinse;

**İcm-SW1# copy tftp: running-config**  yine ip adresi ve dosya ismini vererek konfigürasyonu kopyalayabilriz.

**İcm-SW1#copy flash: tftp:** Yine switchten tftp servera dosya kopyalama.

## 3.34 Switch içerisindeki Dosyaları görme Komutu

**İcm-SW1# Show flash**

## 3.35 Cisco Switch e Yeni version kopyalama

**İcm-SW1# copy tftp: flash:**  burada yeni version örneğin c2960-lanbase 1.150 yi seçerek bu versionla güncelleyeceğiz. Bunu komutu koştuktan tftp serverdaki dosya adını belirtiyoruz.

**İcm-SW1#delete flash:**  eski versionu seçip siliyoruz.

Yada:

**İcm-SW1(config)# boot system yeni\_version**  diyerek Cisco İOS u güncelliyoruz.

**İcm-SW1#write**

**İcm-SW1#reload**  diyerek işlemi tamamlamış oluruz.

## 3.36 Cisco Switch DHCP Yapılandırması

**İcm-SW1(config)# ip dhcp pool asd**

**İcm-SW1(dhcp-config)# network 192.168.1.0 255.255.255.0**  belirttiğimiz ip bloğundan dağıtım yapacaktır.

**İcm-SW1(dhcp-config)# default-router 192.168.1.1**

**İcm-SW1(dhcp-config)# dns-server 8.8.8.8**

**İcm-SW1(dhcp-config)#exit**

**İcm-SW1(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10**  bu ipleri özel olarak belirterek bu ip leri kendimize ayırıyoruz. Bu ip yi örneğin gateway ip olarak belirleyebiliriz.

**İcm-SW1# Show ip dhcp binding**  bu komut hangi cihaz hangi ipyi almış görebiliyoruz.

**İcm-SW1# ip dhcp conflict** dhcp çakışmayı gösteren koddur.

## 3.37 Cisco CDP ile Cihaz keşfi. Cisco Discovery Protokol

**Ağımızdaki cisco cihazların tespiti için kullanılan protokoldür.**

**İcm-SW1# Show cdp**  burda cdp ile ilgili calısma prensiplerine bakabiliriz. Örneğin cdp paketleri 60 snde bir gitmektedir.

**İcm-SW1(config)#** **Show cdp neighbros**

**İcm-SW1(config)#**int fa0/14

**İcm-SW1(config-if)# cdp en**

**İcm-SW1(config-if)# no cdp en**  port bazında cdp açıp kapamak

**İcm-SW1(config)# no cdp run**  tüm switchte cdp yi kapatırız.

## 3.38 Cisco Switch Parola Kurtarma

Cihazın gücünü tamamen kesiyoruz. Tekrar takıp Mode düğmesine 3 saniye basıyoruz.Switchi açtığımızda **flash\_init** yazıyoruz.

**Switch: rename flash:config.text flash:config.text.old**

**Switch: reset**

Bu şekilde switchi açabiliriz. Parola vs. sormayacaktır.

Eski konfigürasyonu geri getirmek içinde tekrar

**Switch# copy flash: running-config** gelen soruya config.text.old dersek konfigürasyon geri gelecektir.

\*-\*-\*-\*-\*

3.39 NTP Yapılandırma (Network Time Protokol**)**

**İcm-SW1(config)# ntp server time.google.com**

**İcm-SW1(config)#end**

**İcm-SW1#show ntp status**

## 3.40 Cisco Switch SYSLOG Yapılandırması

**Syslog**  logları depolamamızı ve yönetmemizi sağlayan bir standarttır.

**İcm-SW1(config)# logging host 192.168.1.15**  belirttiğimiz ip adresindeki sunucuya logglarımızı gönderir.

**İcm-SW1(config)# service timestamps log datetime msec** bu komut loğlara milisaniye zaman damgası ekler.

Logların seviyesii 1’den 7’ye kadardır. Buna **logging trap** diyip soru işareti ile inceleyebiliriz.

**Logging trap debugging**  komutu bütün log seviyelerini sunucuya gönderir.

**no logging console**  yazarsanız artık console bu logu basmaz.

## 3.41 Switch arayüzü kapatma

**İcm-SW1(config)#no ip http server**

**İcm-SW1(config)# no ip secure-server**

## 3.42 İGMP SNOOPİNG

IGMP snooping, IGMP ağ trafiğini dinleme protokolüdür. IGMP snooping, isminden de anlaşıldığı gibi 2.katman ve 3.katman arasındaki host ve routerlar arasındaki konuşma iznini veren protokoldür. Bir switche bu protokolden bağlanıldığı zaman bağlı hostlar arasındaki tüm IGMP paketlerini analiz eder. Bir switch yeni bir multicast grubu için host'a IGMP raporu sunar. Bu grup için host multicast listesine yeni bir port numarası ekler.

İgmp snooping ayarları:

**İcm-SW1(config)#ip igmp snooping**

**İcm-SW1(config)#ip igmp snooping explicit-tracking**

**İcm-SW1(config)#ip igmp snooping fast-leave**

**İcm-SW1(config)#ip igmp snooping last-member-query-interval seconds**

**İcm-SW1(config)#ip igmp snooping report-suppression**

**İcm-SW1(config)#ip igmp snooping mrouter interface interface**

**İcm-SW1(config)#ip igmp snooping static-group group-ip-addr interface interface**

# Cisco’da Siber Güvenlik için Gerekli Konfigurasyon Ayarları

## 4.1 Cisco CAM savunması:

Savunma yapacağımız port örneğin 0/3

**En**

**Conf t**

**İnterface gigabitEthernet 0/3**

**Switchport mode Access**

**Switchport port-security**

**Switchport port-security maximum 3 (**Maximum 3 Mac adresi girer**)**

**Switchport port-security mac-address sticky (**Öğrendiği Macleri kalıcı hale getirir.**)**

**Switchport port-security violation shutdown (**Violation saldırı olduğunda ne yapılacağı yazılır. Örneğin shutdown diyoruz. Farklı seçeneklerde vardır.**)**

**Errdisable recovery cause psecure-violation (**hataya düştüğünde sistemi tekrar kurtar**)**

**Errdisable recovery interval 50 (**Saniyeyi belirtiriz. 50 sn sora tekrar açar**)**

## 4.2 Cisco CDP Savunması**:**

**Show cdp neighbors (**komşu ciscoları gösterir**)**

**Show cdp traffic (**trafiği gösterir.**)**

**Clear cdp table (**Cdp tablosunu temizler**)**

**No cdp enable (** Cdp protokolünü kapatır. Tüm portlara uygulanarak kurtulabiliriz.**)**

## 4.3 DHCP Savunması**:**

**İp dhcp snooping vlan 1**

**İnterface gigabitethernet 0/3**

**İp dhcp snooping trust**

## 4.4 ARP Savunması

Wiresharkla ilgili interface i dinlediğimizde Arp request olmadan sürekli Arp response u aldığımızı görmekteyiz. Aynı zamanda wireshark info sütununda hangi ip ve MAC e saldırı olduğunu da görmekteyiz. Private Request OpCode :Replay (1) olmalıdır. Saldırıda 2 gözükmektedir.

**İp dhcp snooping**

**İp dhcp snooping vlan 1**

**İp arp inspection vlan 1**

**İnterface gigabitEthernet 0/3**

**İp dhcp snooping trust**

**İp arp inspection trust**

## 4.5 SPOOFFİNG Savunması DTP (Dynamic Trunk Protocol):

İlgili interface içerisine girip

**Switchport mode access**

**Switchport nonegotiate**

## 4.6 VTP Savunması:

Switch içerisinde;

**Vtp password 123123**

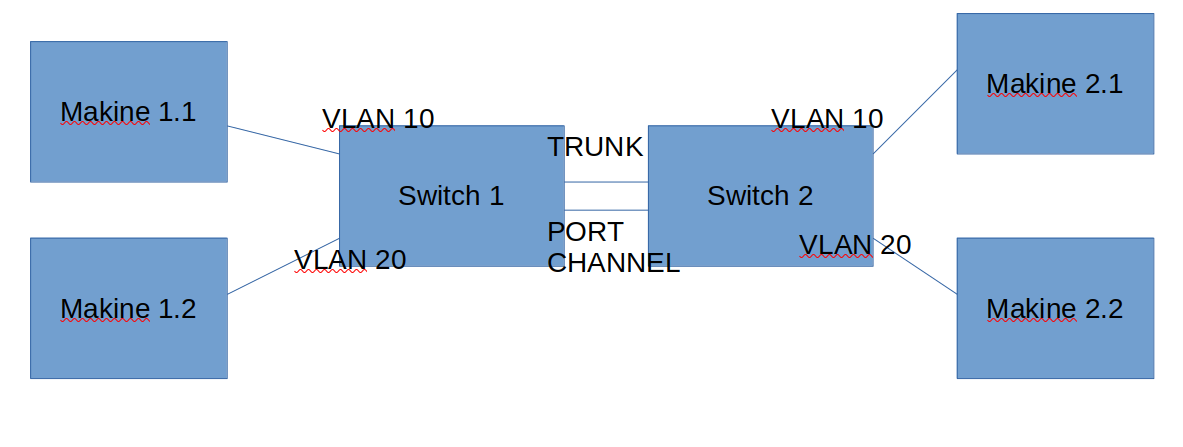
**Vtp mode transparent**

## 4.7 STP Savunması Spanning Tree Protocol

İlgili porta

**Spanning tree guard root**

# Bir Ağın Yapı Yapılandırılması



**Switch 1 ve 2 Konfigurasyonları** : Aşağıdaki adımlar 2 switchte de yapılmalıdır.

Vlan 10 ve Vlan 20 Tanımı

**İcm-SW1(config)#en**

**İcm-SW1(config)#conf t**

**İcm-SW1(config)#vlan 10,20**

Switch 1 ve 2 nin interfaceGigabit 1/2 ve interfaceGigabit 1/3 portları üzerinden tek bir switch gibi haberleştirmek istiyoruz. Ether Channel konfigürasyonu yaparak Switchler arası 1 den fazla link kullanmamızı sağlar. Konfigure ettiğimiz 2 portu spanning tree protokolü tek bir port gibi gösterir. Ve Portlar down olmaz.

**İcm-SW1(config)#interface range fastEthernet 1/2-3**

**İcm-SW1(config-if-range)# channel-group 1 mode on**

**İcm-SW1(config-if)#switchport trunk encapsulation dot1q**

**İcm-SW1(config-if)#switchport mode trunk**

**Soru**: Makine 1.1 in Switch 1 e 0/5 numaralı porttan bağlı olduğunu düşündüğümüzde bunu nasıl ispat edebiliriz?

Makine 1.1. in bağlı olduğu interface in MAC adresini inceleriz. Bunu görebilmek için kullandığımız OS in interface configurasyon görme komutunu yazmamız gerekmektedir. Bizim genelde kullandığımız Linux sistemlerde bu **ifconfig** komutu görmekteyiz. Buradan switche bağlı olan interface’in MAC adresini Not almalıyız.

Switch 1 e bağlanarak **Show Mac address-table** komutuyla ilgili MAC adresini bularak hangi Makinenin hangi switch e bağlı olduğunu bulabiriz.

