

TEMEL CİHAZ KONFIGÜRASYONU

Erişim Metotları

- Console bağlantısı, cihazların üzerinde bulunan fiziksel bir porttur. Cihazlarda ilk konfigürasyonu yapmak için kullanılan bağlantı çeşididir. Bağlantılarda port tipi seri port olduğu için USB/Seri port dönüştürücü kullanılır.
- Aux bağlantısı, sadece routerlarda bulunur. Aux portu erişilmesi zor konumlardaki cihazlara ikinci bir erişim seçeneği oluşturmak için kullanılıyor. Örnek bir kullanım şekli olarak Aux portuna farklı bir ISP'nin modemi bağlanıyor. Bu sayede normalde hizmet alınan ISP'de sorun olduğunda router'a erişmek için Aux portuna bağlanan modem üzerinden routera uzak bağlantı kurularak konfigürasyonlar yapılabilir.
- Telnet bağlantısı, cihazlara uzaktan erişim için kullanılan protokollerden biridir. Genelde network cihazları ayrı bir odada (sistem odalarında) tutulduğu veya fiziksel erişimin mümkün olmadığı durumlarda cihazın yanına gidip Console portundan bağlanabilmek mümkün olmuyor. Bu nedenle cihazlara bir ip adresiyle parola verilip uzaktan erişilebilir olması sağlanıyor. Bu sayede cihazların yanına gidilmeden cihazlar konfigüre edilebiliyor.
|-> Telnet bağlantısında network trafiği şifrelemediği için güvenli görülüyor, bu nedenle kullanılması önerilmiyor.
- SSH (Secure Shell) bağlantısı, cihazlara uzaktan erişim için kullanılan bir başka protokoldür. Bu bağlantı tipinde network trafiği şifreli iletilir.

Cihazlara herhangi bir metotla erişebilmek için bilgisayarlarda Putty veya Terra Term gibi terminal Emulation yazılımları kullanılıyor.



PuTTY



TERA TERM

Cisco IOS (Internetworking Operation System) Kullanıcı Modları

- **User Exec**, cihaza bağlanıldığında kullanıcıyı karşılayan ilk moddur. Bu modda sadece bazı temel kontrol komutları kullanılabilir.
- **Privileged Exec**, cihazlardaki en yetkili moddur. Yetkilendirilmiş mod veya Enable modu da deniliyor. User Exec modundan “**enable**” komutu kullanılarak geçiş yapılıyor.
- **Global Configuration**, cihazla ilgili genel konfigürasyonların tanımlandığı moddur. Privileged Exec modundan “**configure terminal**” komutu kullanılarak geçiş yapılıyor.
- **Interface Configuration**, router ve switch portlarının konfigürasyonları için kullanılan moddur.
- **Line Interface**, SSH, Telnet veya Aux bağlantılarının konfigürasyonları için kullanılan moddur.

Cihazlara Uygulanan Temel Konfigürasyonlar

- Saat Tarih Bilgilerinin Güncellemesi; Cihazlarda tutulan Log kayıtlarının saat bilgilerinin doğru değerlendirilebilmesi gibi nedenlerden dolayı cihazın saat bilgisinin güncellenmesi gerekiyor. Bu konfigürasyon Enable modunda gerçekleştiriliyor (Genelde saat ve tarih güncellemeleri NTP adı verilen sunucular kullanılarak merkezi bir sunucudan yapılıyor). Saat ve tarih konfigürasyonu için **"clock set <HH:MM:mm> <Day Month Year>"** komutu kullanılıyor (Konfigürasyon kontrolü için **"show clock"** komutu kullanılıyor)
 - o Server mode, kimlik denetimini ve daha fazla konfigürasyon için https://cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/system_management/503_n1_1/b_cisco_n5k_system_mgmt_cg_rel_503_n1_1/b_cisco_n5k_system_mgmt_cg_rel_503_n1_1_chapter_010000.pdf.

```
Switch#clock set 10:10:00 1 jan 2022
Switch#sh clock
10:10:1.82 UTC Sat Jan 1 2022
Switch#
```

- Cihaz İsimlendirmesi; Sorun giderme sürecinde (Troubleshooting) cihazların diğer cihazlardan ayırt edilebilmesi için cihazlara isimler tanımlanıyor. Cihazlarda hostname tanımlama işlemi global konfigürasyon modunda **"hostname <Name>"** komutu kullanılarak gerçekleştiriliyor.

```
Switch>en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname SW1
SW1(config)#
```

- Enable Girişine Parola Atama; Cihazlarda Privileged Exec modu aslında en yetkili moddur. Privileged Exec moduna giriş yapıldıktan sonra bir kez daha parola sorulmaz. Bu nedenle Privileged Exec moduna giriş yaparken parola sorması için global konfigürasyon modundan **"enable secret <Password>"** komutuyla parola tanımlanıyor. Konfigürasyonda kullanılan **"secret"** kelimesi sayesinde oluşturulan parola bilgisi konfigürasyon dosyasında Salted MD5 Hash algoritması kullanılarak tutuluyor.

```
Switch(config)#enable secret MyEnablePass
```

- Console Portuna Parola Ataması; Cihaza Console portundan bağlantı kurulduğunda yetkisiz erişimlerin önüne geçmek için parola ataması yapılıyor. Bunun için **"line console 0"** komutuyla Line Configuration moduna giriş yapıyoruz. Burada "0" değeri tek Console portunu temsil ediyor. Ardından **"password <Password>"** komutuyla parola tanımlanıyor. Son olarak Console bağlantılarında tanımladığımız parolayı sorulması için **"login"** komutunu kullanıyoruz.
| → Burada cihaz üzerinde **"username <Username> password <Password>"** gibi bir kullanıcı oluşturulduktan sonra **"login"** komutu yerine **"login local"** komutuyla cihaza Console portundan yapılan bağlantılarda kullanıcı adı ve parola sorulması sağlanabilir. Benzer şekilde uzak bir sunucudan da kullanıcı adı ve parola doğrulaması yapılabilir ama bu kullanım ilerleyen konularda işlenecek.

■ Bu kullanım diğer bağlantı tiplerinde (Console, AUX, Telnet, SSH) de uygulanabiliyor.

```
Switch(config)#line console 0
Switch(config-line)#password MyPassConsole
Switch(config-line)#login
Switch(config-line)#exit
```

- Aux Portuna Parola Ataması; Aux portuna parola ataması için “**line aux 0**” komutuyla line konfigürasyon moduna girilir. Ardından “**password <Parola>**” komutuyla parola tanımlıyoruz. Son olarak da “**login**” komutuyla tanımladığımız parolanın Aux portundan bağlanıldığında sorulması sağlanır.

```
Router(config)#line aux 0
Router(config-line)#password MyAuxPass
Router(config-line)#login
Router(config-line)#exit
```

- Telnet Konfigürasyonu; Her ne kadar güvensiz olduğu için kullanılsa da Telnet konfigürasyonu için öncelikle cihaza bir ip adresi atanması gerekiyor. Switchlerde ve routerlarda ip adresi atamaları farklılık gösteriyor.
| → Router portları L3 portları olduğu için fiziksel portlarına ip adresleri atanabiliyor. Bunun için “**interface <Interface ID>**” komutuyla ilgili arayüze giriş yapılarak “**ip address <Ip Address> <Subnet Mask>**” komutuyla ip adresi ve Subnet bilgileri tanımlanıyor (“**ipv6 address <Ip Address/Prefix Length>**” komutuyla IPv6 adres de verilebiliyor. IPv4’ten farklı olarak Subnet bilgisinde Prefix uzunluğu yazılıyor.). Ardından L3 portları varsayılanda kapalı geldiği için “**no shutdown**” komutuyla port açılıyor. Burada tanımlanan ip adresleri aynı zamanda bu portun bağlı olduğu networkteki istemciler için Gateway adresi oluyor. (“**description <Description>**” komutuyla arayüz hakkında açıklamalar bırakılabilir.)

```
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#description ISP side interface
Router(config-if)#no shutdown
Router(config-if)#exit
```

| → Switchler ise L2 cihazlardır ve fiziksel portları da L2’ de çalışmaktadır. Bu nedenle switchlerde ip adresleri sanal arayüz olan VLAN arayüzlerine tanımlanıyor. Bunun için “**interface vlan <Vlan Number>**” komutuyla ilgili VLAN arayüzüne girilerek routerlarda olduğu gibi ip adresi ataması yapılıyor. Son olarak “**no shutdown**” komutuyla port açılıyor (Varsayılanda L2 portları açık gelirken, L3 portları kapalı geliyor. Bu nedenle switchlerde “**no shutdown**” kullanılmayabilir. Güvenlik nedeniyle switchlerde kullanılmayan portlar kapatılabilir. Bu gibi durumlarda sorunlarla karşılaşmamak için kullanmakta fayda var). L2 switchlerde portların varsayılanda açık geldiği “**sh run**” komutu kullanarak da görüntülenebilir.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

Temel konfigürasyon için bu kısımdan sonraki yapılandırmalar routerda da switchde de aynı gerçekleştiriliyor.

Telnet Konfigürasyonu; Telnet konfigürasyonu için “**line vty 0 15**” komutuyla line Konfigürasyon moduna giriliyor. Komutta kullanılan 0 15 parametresinin anlamı aynı anda bu cihaza 16 kullanıcının bağlanabilmesini sağlamaktır. Network cihazlarında varsayılanda hem Telnet hem de SSH açık geliyor. Her ne kadar açık olsalar da ihtiyaç duydukları konfigürasyonlar yapılmadan kullanılmıyor. Cihaza sadece Telnet kullanılarak bağlantı kurulabilmesi isteniyorsa “**transport input telnet**” komutu kullanılıyor. Ardından “**password <Password>**” komutuyla parola tanımlanır ve son olarak da “**login**” komutuyla tanımlanan parolanın Telnet bağlantılarında sorulması sağlanıyor. (Konfigürasyonda parola tanımlanmadan cihaza Telnet bağlantısı kurulamıyor.)

```
Switch(config)#line vty 0 15
Switch(config-line)#password MyConsolePass
Switch(config-line)#login
Switch(config-line)#exit
```

SSH Konfigürasyonu; SSH konfigürasyonu için öncelikle cihaza Hostname verilmesi gerekiyor. Hostname verildikten sonra bağlantı için kullanılacak arayüzlerine ip adreslerinin atanması gerekiyor. Bu tanımlamalardan sonra global konfigürasyon modunda "**ip domain name <Domain Name>**" komutuyla bir alan adı tanımlanıyor. Cisco bu alan adını sertifikada kullandığı için alan adı vermeden RSA algoritması için Key oluşturulmuyor (RSA algoritmasının çalışma şekline küçük bir örnek <https://www.cs.utexas.edu/~mitra/honors/soln.html>). Daha sonra RSA algoritması için "**crypto key generate rsa**" komutuyla bir Key oluşturuluyor ve boyutu belirleniyor. Burada minimum 1024 bit kullanılması öneriliyor. SSH bağlantısında kullanılacak kullanıcı adı ve parola için "**username <Username> secret <Password>**" komutu kullanılıyor. Bu işlemleri tamamladıktan sonra "**line vty 0 15**" komutuyla Line Configuration moduna giriliyor ve "**transport input ssh**" komutuyla sadece SSH bağlantısı üzerinden cihaza bağlanması sağlanıyor. Son olarak "**login local**" komutuyla SSH bağlantılarında kullanıcı doğrulamasının cihaz üzerinde tanımlanan kullanıcı adı ve parola bilgileriyle kontrol edileceği belirtiliyor.

```
Switch(config)#hostname SW1
SW1(config)#ip domain-name cisco.com
SW1(config)#crypto key generate rsa
The name for the keys will be: SW1.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

SW1(config)#username myadmin secret MySshPass
*Mar 1 0:0:40.102: %SSH-5-ENABLED: SSH 1.99 has been enabled
SW1(config)#line vty 0 15
SW1(config-line)#transport input ssh
SW1(config-line)#login local
SW1(config-line)#exit
```

| -> SSH konfigürasyonunda varsayılanda hem SSH v1 hem de SSH v2 devreye girmektedir. SSHv1 zafiyetlere sahip olduğu için v2 kullanılması tercih ediliyor. Bunu "**ip ssh version 2**" komutunu kullanarak sadece SSH v2 kullanılması sağlanabiliyor.

```
Switch(config)#ip ssh version ?
<1-2> Protocol version
Switch(config)#ip ssh version 2
```

| -> SSH bağlantılarında yanlış giriş sayısını sınırlama ve Time-Out gibi özellikler de "**ip ssh (authentication-retries | time-out)**" komutuyla konfigüre edilebiliyor.

```
Switch(config)#ip ssh authentication-retries ?
<0-5> Number of authentication retries
Switch(config)#ip ssh time-out ?
<1-120> SSH time-out interval (secs)
Switch(config)#
```

| -> Telnet veya SSH konfigürasyonlarında switchlere network dışından erişilmek isteniyorsa "**ip default-gateway <Gateway Ip Address>**" komutuyla gateway adresleri de tanımlanmalı.

```
Switch(config)#ip default-gateway 192.169.1.1
```

Parola Bilgilerini Şifreleme; Konfigürasyonlarda tanımlanan parola bilgileri ayrı bir konfigürasyon yapılmadıkça Config.text dosyasında açık bir şekilde tutulur. Parola bilgilerini şifreli olarak tutabilmek için “**service password-encryption**” komutu kullanılıyor. Bu sayede parola bilgileri Level7 adı verilen bir şifreleme algoritması kullanılarak şifreleniyor. Bu algoritma çift yönlü ve çözülebilir bir parola olduğu için yeteri kadar güvenlik sağlamayacaktır. Sadece konfigürasyon yapıldığı zamanlarda **Shoulder Surfing** yapılmasına engel olacaktır.

```
SW1(config)#service password-encryption
```

- Banner Ekleme; Cihaza giriş yapılırken parola kısmında kullanıcıya açıklama bırakmak için Banner eklenebiliyor. Bunun için “**banner motd <End Character>**” komutu kullanılıyor. Açıklama tek satırdan oluşmayabilir. Bu nedenle Banner girişini sonlandırmak için bir sembol seçiliyor. Girilen açıklama tamamlandıktan sonra belirlenen sembol girerek Banner girişi sonlandırılıyor.

```
SW1(config)#banner motd !
Enter TEXT message. End with the character '!'.
Sonlandırıcı sembol unlem secildi
Unlem girilene kadar girilen metinler
Eklenebiliyor
!
SW1(config)#
```

Cihazda uygulanmış konfigürasyonları kontrol edebilmek için Enable modunda “**show running-config**” komutu kullanılabilir. Bu komut cihaz çalışır durumdayken tanımlanan konfigürasyonları gösteriyor. Konfigürasyon sonunda tanımlanan komutlar cihazda geçici bellek olan RAM’da tutuluyor. Bu tanımlamaları kalıcı hafıza birimi olan NVRAM ünitesine kaydetmek için “**write**” veya “**copy running-config startup-config**” komutları kullanılıyor (komutta kullanılan “**startup-config**”, cihaz açılırken yüklenecek konfigürasyon dosyasını temsil ediyor.). Bu sayede cihaz yeniden başlatıldığında tanımlanan konfigürasyonlar Config.text dosyasından tekrar yüklenebiliyor.

Cihaz üzerinde tanımlanan tüm konfigürasyonları silmek için “**eraser startup-config**” komutu kullanılabilir. Startup-config dosyası silindikten sonra Running-config dosyasının da bu değişimi algılayabilmesi için “**reload**” komutuyla cihazın yeniden başlatılması gerekiyor. Aksi takdirde cihaz yeniden başlatılana kadar RAM’a yüklenen konfigürasyonlar çalışmaya devam edecektir.

NOTLAR:

- Cihazda yanlış komut kullanıldığında işletim sistemi bu komutu anlamlandırabilmek için bunu bir cihaz adı olarak görüp ad çözümlemesi yapmaya/ip adresini bulmaya çalışıyor. Bunu durdurmak için Ctrl+Shift+6 kombinasyonu kullanılıyor.
- İşleyen süreçleri durdurmak için ise ayrıca Ctrl+C kombinasyonu da kullanılıyor.
- Uygulanan bir konfigürasyonu iptal edebilmek için konfigürasyonda kullanılan komutun başına “**no**” komutu getirilerek uygulanan konfigürasyonlar geri alınabiliyor.
- Uzun çıktılarda “Enter” tuşu satır atlamak için kullanılırken “Space” tuşu sayfa atlamak için kullanılıyor. Çıktıdan çıkış yapabilmek için ise herhangi bir tuşa basmak yeterli oluyor.
- Network cihazları “**reload**” komutuyla yeniden başlatılabilir ama yeniden başlatılması uzun sürdüğü için uygun zamanlarda yapılması gerekiyor.
- Kullanıcı modlarında kullanılabilecek/izin verilen komutları görüntüleyebilmek için “?” sembolü kullanılıyor. Bu sembol eksik komutları tamamlamak için kullanılabildiği gibi alternatif komutları listelemek için de kullanılıyor.

- Kullanıcı modları arasında “**exit**” komutuyla bulunulan modun bir alt moduna geçiş yapılabilir. “**end**” komutuyla User Exec modu dışında herhangi bir moddan Privileged Exec moduna doğrudan geçiş yapılabilir. Ayrıca Ctrl+Z kombinasyonu da aynı işlem için kullanılabilir.
- Herhangi bir kullanıcı modunda komutun başına “**do**” ekleyerek alt kullanıcı modlarına geçiş yapmadan istenilen komutlar çalıştırılabilir. Bu şekilde kullanılan komutlarda “?” sembolü kullanılarak yardım alınabilir.
- Komutlar kısaltılmış olarak kullanılabilir. Kullanılan komut dışında temsil edecek başka bir kısaltma yoksa komutun tamamlanmasına gerek kalmıyor. Tamamlamak istendiğinde Tab tuşuyla tamamlanabilir. (örnek olarak “configure terminal” → “conf ter” kullanılabilir.)

```
Switch>en
Switch#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#lin vty 0 15
Switch(config-line)#
Switch(config-line)#do sh run
Building configuration...

Current configuration : 1080 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
```

Terminolojiler:

| -> **Hot Swap**, cihaz kapatılmadan veya yeniden bağlatılmadan ek bileşenlerin (kart takılması gibi) takılabilmesine deniyor. Hot Swap olmayan cihazlarda ek bileşenler takmak için cihazın önce kapatılması, ek bileşen takıldıktan sonra cihazın açılması gerekiyor.

Kontrol Komutları

- **show running-config**, cihazda çalışan konfigürasyonu görüntülemek için kullanılıyor.
- **show ntp {status | statistics | ...}**
- **show ip interface brief**, arayüzlere atanmış ip adreslerini ve durumlarını görüntülemek için kullanılıyor.
- **sh ip route**, routerlarda yönlendirme tablosunu gösteriyor. Yönlendirme tablosunda routerun öğrendiği networkler bulunuyor.
- **show interface <Interface ID>**, arayüzün L1 ve L2 bilgileriyle beraber arayüz hakkında çalışma şekli, arayüzden geçen paket istatistikleri gibi daha birçok detaylı bilgi listeler.
- **sh ip interface <Interface ID>**, arayüzdeki L3’de tanımlı yapılandırmaları görüntülemek için kullanılıyor