2.1 TEMEL CİHAZ KONFİGÜRASYONU

Erişim Metotları;

- Console bağlantısı, cihazların üzerinde bulunan fiziksel bir porttur. Cihazlara ilk konfigürasyonu yapmak için kullanılan bağlantı şeklidir. 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. Kullanım olarak Aux portuna farklı bir ISP'nin modemi bağlanıyor. Bu sayede normalde hizmet alınan ISP'de sorun olduğunda router'a erişmek için Aux portuna bağlanılan modem üzerinden routera uzak bağlantı kurularak konfigürasyonlar yapılabiliyor.
- Telnet bağlantısı, cihazlara uzatan erişim için kullnılan 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 görülmüyor, bu nedenle kullanılması önerilmiyor.
- SSH (Secure Shell) bağlantısı, cihazlara uzaktan erişiim için kullanılan bir başkla protokoldür. Bu bağlantı tipinde network trafiği şifreli iletilir.

NOT: Cihazlara herhangi bir metotla erişebilmek için bilgisayarlarda Putty veya Terra Term gibi terminal emulation yazılımları kullanılıyor.

PuTTY

Cisco IOS (Internetworking Operation System) Kullanıcı Modları

- User Exec, cihaza bağlanıldığında kullanıcıyı karşılayan ilk moddur. Sadece bazı temel kontrol komutlarının kullanılabilir.
- Privileged Exec, cihazlardaki en yetkili moddur. Yetkilendirilmiş mod veya Enable modu da deniliyor. User Exec modunda "enable" komutu kulanılarak geçiş yapılıyor.
- Global Confiuration, cihazla ilgili genel konfigürasyonları tanımlandığı moddur. Privileged Exex modundan "configure terminal" komutu kullanılarak geçiş yapılıyor.
- Interface Configuration, router ve switch portlarının konfigürasyonları için kullanılan moddur.
- Line Interface, SSH, Telnet veya Aux portlarının konfigürasyonları için kullanılan moddur.

NOTLAR:

- Kullanıcı modlarında kullanılabilecek/izin verilen komutları görüntüleyebilmek için “?” sembolü kullanılıyor. Bu sembol eksik komutları tamamlamak için kullanılabilecek alternatif komutları listelemek için de kullanılıyor.
- Kullanıcı modları arasında “exit” komutuyla bulunulan modun bir alt moduna geçiş yapılabiliyor. “end” komutuyla User Exec modu dışında herhangi bir moddan Privileged Exec moduna geçiş yapılabiliyor. Ayrıca Ctrl+Z kombinasyonu da aynı işlem için kullanılabiliyor.
- Herhangi bir kullanıcı modunda komutun başına “do” ekleyerek alt kullanıcı kodlarına geçiş yapmadan istenilen komutlar çalıştırılabiliyor. Bu şekilde kullanılan komutlarda “?” sembolü kullanılarak yardım alınamıyor.
- Komutlar kısaltılmış olarak kullanılabiliyor. Kullanılan komut dışında temsil edecek başka bir kısaltma yoksa komutun tamamlanmasına gerek kalmıyor. Tamamlamak istendiğinde “Tab” tuşuyla tamamlanabiliyor. (örnek olaral configure terminal –> conf ter kullanılabiliyor.)

```
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
```

Temel Cihazlara Uygulanan Konfigürasyonlar:

- Saat Tarih Bilgilerinin Güncellemesi; Cihazlarda tutulan log kayıttlarının saat bilgilerinin doğru değerlendirilebilmesi gibi nedenlerden dolayı cihazın saat bilgisinin güncellenmesi gerekiyor. Bu konfigürasyon enable modunda gerçekleştiriliyor. Saat ve tarih güncellemeleri genelde NTP adı verilen sunucular kullanılarak merkezi bir sunucudan yapıluıyor.
  |-> Format : clock set SS:DD:ss Gün AY Yıl
  |-> Konfigürasyon kontrolü için “show clock” komutu kullanılıyor.

```
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 gidermede (Troubleshooting) cihazların diğer cihazlardan ayırt edilebilmesi için cihazlara isimler tanımlanıyor. Bu konfigürasyon global konfigürasyon modunda 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 moduna giriş yaparken parola sorması için global konfiggürasyon modundan “enable secret” komutuyla parola tanımlanıyor. Bu sayede oluşturulan parola bilgsi konfigürasyon dosyasında Salted MD5 Hash algoritması kullanılarak tutuluyor.

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

- Console Portuna Parola Ataması; Cihaza console poprtundan bağlantı kurulduğunda yetkisiz erişimlerin önüne geçmek için parola ataması yapılıyor. Bunun için “line console 0” komutuyla Line Configuration moduna giriş yapıyoruz. Burada 0 anlamı tek console portunu temsiil ediyor. Ardından “password” komutuyla parola tanımlanıyor. Son olarak console bağlantılarında tanımladığımız parolayı sorulması için “login” komutunu kullanıyoruz.

```
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 giriyoruz. Ardından “password” komutuyla parola tanımlıyoruz. Son olarak da “login” komutuyla tanımladığımız parolayı Aux portundan bağlanıldığında sorulmasını sağlıyoruz.

```
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 kullanılmasa da Telnet konfigürasyonu için öncelikle cihaza bir ip adresi atanması gerekiyor. Switchlerde ve routerlarda ip adresi atamaları farklılık gösteriyor.

  |-> Router portları L3 porlar olduğu için fiziksel portlarına ip adresleri atanabiliyor. Bunun için “interface” komutuyla ilgili arayüze giriş yapılarak “ip address” komutuyla ip adresi ve subnet bilgileri tanımlanıyor (“ipv6 address” 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 porta bağlanan network için gateway adresi oluyor. (“description” komutuyla arayüz hakkında açıklamalar bırakılabiliyor.)

```
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 adresilerini sanal arayüz olan VLAN arayüzlerine tanımlıyoruz. Bunun için “interface vlan” komutuyla ilgili VLAN arayüzüne girilerek roterlarda olduğu gibi ip adresi ataması yapılıyor. Son olarak “no shutdown” komutuyla port açılıyor. Bu kısma ek olarak varsayılanda L2 portları açık gelirken, L3 portları kapalı geliyor. Güvenlik nedeniyle switchlerde kullanılmayan portlar kapatılabiliyor. Portların varsayılanda açık geldiğini “sh run” komutu kullanarak da görüntülenebiliyor.

```
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
```

İp adres ataması yapıldıktan sonraki adımlar routerda da switchde de aynı geçekleştiriliyor. “line vty 0 15” komutuyla line Konfigürasyon moduna giriliyor. Komutta kullanılan 0 15 parametresinin anlamı aynı anda bu cihaza 16 kullanıcının bağlanabileceği belirtiliyor. Network cihazlarında varsayılanda hem Telnet hem de SSH açık geliyor. Her ne kadar açık olsalar da ihtiyaç duydukları konfigürasyonlar yapılmadan kullanılamıyor. Sadece Telnet kullanılarak cihaza bağlantı kurulabilmesi istendiğinde “transport input telnet” komutu kullanılıyor. Ardından “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 cihazlarda hostname verilmesi gerekiyor. Hostname verildikten sonra bağlantı için kullanılacak arayüzleirne ip adresleri atanması gerekiyor. Ardından Global Configuyration modunda "ip domain name" komutuyla bir alan adı tanımlanmalı. Cisco bu alan adını sertifikada kullandığı için alan adı vermeden RSA algoritması için key oluşturulamıyor (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 myadmin secret MySshPass" komutu kullanılıyor (Burada “secret” kullanarak parola bilgisi config dosyasında Salt MD5 Hash algoritması kullanılarak saklanması sağlanıyor.) Bu işlemleri tamamladıktan sonra "line vty 0 15" komutuyla Line Configuration moduna giriliyor ve "transport input ssh" komutuyla sadece ssh kullanılarak cihaza bağlanılması 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 bağlantılarda yanlış giriş sayısını sınırlama ve time-out gibi özellikler de “ip ssh” 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)#
```

NOT:

- Telnet veya SSH konfigürasyonlarında switchlere netwokr dışından erişilmek isteniyorsa “ip default-gateway” komutuyla gateway adresleri de tanımlanmalı.

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

Parola Bilgilerini Şifreleme; Konfigürasyonlarda tanımlanan parola bilgileri ayrı bir konfigüürasyon yapılmadıkça “config.text” dosyasında plain text olarak tutulur. Bu parola bilgilerini şifreli olarak tutabilmek için “service password-encryption” komutu kullanılıyor. Bu sayede parola bilgileri level7 adı verilen bir şifrelememem algoritması kullanılarak şifreleniyor. Bu algoritma çift yönlü ve çözülebilir bir parola olduğu için yeteri kadar güvenlik sağlamayacaktır. Konfigürasyon sırasında 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” komutu kullanılıyor. Açıklama tek satırdan oluşmayabilir. Bu nedenle komut sonunda sonlandırmak için bir sembol seçiyoruz ve istenilen açıklamayı tamamladıkran sonra belirlediğimiz sembolü girerek açıkalmanın sonlandığını belirtiliyor.

```
SW1(config)#banner motd !
Enter TEXT message.  End with the character '!'.
Sonlandirici 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 tanımolanan 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 başlatışdığında tanımlanan konfigürasyonlar “config.text” dosyasından tekrar yüklenebiliyor.

Cihaz üzerinde tanımlanan tüm konfigürasyonları silmek için “eraser startup-config” komutuyla kayıtlı konfigürasyonlar silinebiliyor. Cihazdaki güncellemelerin “running-config”’e aktarılması için “reload” komutuyla cihaz yeniden başlatılıyor.

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 klombinasyonu da kullanılıyor.
- Uygulanan bir konfigürasyonu iptal edebilmek için konfigürasyonda kullanılan komutun başına “no”komutu ekleyeerek konfigürasyo iptal edilebiliyor.
- 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 başlatılabiliyor ama yeniden başlatılması uzun sürdüğü için uygun zamanlarda yapılması gerekiyor.

Kontrol Komutları

|-> show running-config, cihazda çalışan konfigürasyonu görüntülemek için kullanılıyor.

|-> 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 ArayüzBilgisi, arayüzün L1 ve L2 bilgileriyle beraber arayüz hakkında çalışma şekli, arayüzden geçen paket istatistikleri gibi daha birçok detaylı bilgi listeler.

|-> sh ip interface ArayüzBilgisi, arayüzdeki L3’de tanımlı yapılandırmaları görüntülemek için kullanılıyor

Öğrenilen 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.