Huawei Genel Notlar

Cisco switchler üzerinde uygulanan temel konfigürasyonların Huawei switchler üzerinde uygulayabilmek için ilk olarak "**system-view**" komutuyla ayarlamaların/konfigürasyonların yapılacağı moda giriş yapılması gerekiyor. System-view moduna giriş yapıldıktan sonra;

- Switchlerde "**sysname <Name>**" komutuyla yeni bir isim tanımı yapılabiliyor.

```
[~HUAWEI]sysname CE6800_1
[*HUAWEI]commit
[~CE6800_1]
```

- Switch portları varsayılanda L2 olarak geliyor ama L3 gelmesi durumunda Portları L2'ye çekmek için "**int <Interface Id>**" komutuyla portların arayüzüne giriş yapılarak "**portswitch**" komutu kullanılıyor. Portlar L3'e çekilmek istendiğinde ise (switch destekliyorsa) "**undo portswitch**" komutu kullanılıyor.

```
[~CE6800_1]interface ge 1/0/0
[~CE6800_1-GE1/0/0]portswitch
[~CE6800_1-GE1/0/0]undo sh
[~CE6800_1-GE1/0/0]quit
```

- Swİtchler üzerinde tarih ve saat bilgilerini manuel olarak düzenlenebildiği gibi bir NTP sunucusu üzerinden alması da sağlanabiliyor. Bunun için "**CTRL+Z**" kombinasyonuyla CLI açıldığında kullanıcıyı karşılayan kullanıcı moduna;
    - Manuel olarak konfigürasyon yapmak için "**clock datetime HH:MM:SS YYYY-MM-DD**" komutuyla ayarlama yapılabildiği gibi "**clock timezone time-zone-name { add | minus } HH:MM:SS**" komutuyla saat dilimi de ayarlanabiliyor (Varsayılanda UTC 00:00:00 zaman dilimiyle geliyor).

```
<HUAWEI>clock datetime ?
  HH:MM:SS  Specify the time
  utc       Universal Time Coordinated
```

        - Saat dilimi ayarı yapılırken "**add**" parametresiyle "+" yönünde saat dilimi, "**minus**" komutuyla "-" yönünde saat dilimi tanımı yapılıyor.

```
<CE6800_1>clock timezone TR add 03:00:00
<CE6800_1>display clock
2024-02-03 16:33:54+03:00
Saturday
Time Zone(TR) : UTC+03:00
```

    - Switchin zaman bilgisini bir NTP server üzerinden alabilmesi için "**ntp unicast-server <Ip Address>**" komutuyla ip adresi tanımlanabiliyor.
        - Burada NTP Server tanımı öncesinde switchin NTP Master olan cihaza erişebilmesi için arayüzlerinden birine (VLANif arayüzü) ip atanması gerekiyor. Bu arayüze atanan ip adresi NTP Master cihaza erişebilir durumda olmalıdır. Aksi takdirde zaman bilgisi senkronize edilemez.
        - Switchler NTP Client olabileceği gibi üzerinde bir NTP sunucusu da ayağa kaldırılabiliyor. Bunun için ilk olarak NTP sunuculuğu yapacak switchin

erişilebilir olması için kullanılan VLAN arayüzüne (Varsayılanda bütün portlar VLAN 1'e dâhil geliyor. Sadece portların açılması gerektiğini unutma) "**interface vlanif <VLAN ID>**" komutuyla giriş yapılıp "**ip address <Ip Address>/<Subnet Mask>**" komutuyla ip konfigürasyonu yapılmalıdır.

```
[~CE6800_1]interface vlanif 1
[~CE6800_1-Vlanif1]ip address 192.168.0.140 24
[~CE6800_1-Vlanif1]undo sh
[~CE6800_1-Vlanif1]quit
[~CE6800_1]commit
```

- Ip konfigürasyonu yapıldıktan sonra NTP Server hizmeti vermeden önce zaman bilgilerinin ayarlanması gerekiyor. Bu ayarlama manuel yapılabileceği gibi yine farklı bir NTP sunucusundan alınması da sağlanabilir. Zaman bilgileri güncellendikten sonra "**undo ntp server disable**" komutuyla NTP Server hizmetinin devreye alınması sağlanıyor. Son olarak da "**ntp refclock-master <Stratun Value>**" komutuyla NTP sunucusunun hangi Stratum değeriyle hizmet vereceği belirleniyor.

```
[~CE6800_2]undo ntp server disable
[~CE6800_2]ntp refclock-master ?
  INTEGER<1-15>  Stratum number, the default value is 8
  X.X.X.X        IP address of the local clock 127.127.1.<0-3>, the default
                 value is 127.127.1.0
  <cr>

[~CE6800_2]ntp refclock-master 1
```

- NTP Server hizmeti temelde bu komutlar kullanılarak ayağa kaldırılabiliyor. İsteğe bağlı olarak kimlik denetimi yapılması da sağlanabiliyor. Bunun için NTP sunucusunda da NTP istemcisinde de birkaç ek konfigürasyon gerekiyor (Bu konfigürasyon öncesinde cihazların aralarında erişilebilir durumda olduğundan emin olunmalıdır).
    - İlk olarak NTP sunucusunda yapılması gerekenlere bakıldığında "**ntp refclock-master <Stratum Value>**" komutuyla Stratum değeri belirlendikten sonra "**ntp authentication enable**" komutuyla kimlik doğrulama mekanizmasının devreye alınması gerekiyor. Kimlik doğrulama mekanizması devreye alındıktan sonra "**ntp authentication-keyid <Key Id> authentication-mode <Hash Algorithm> <Password>**" komutuyla kimlik doğrulama sürecinde kullanılacak algoritma ve parola bilgilerinin tanımlanması gerekiyor (Key Id değeri burada tanımlanan kimlik doğrulama bilgilerini temsil etmek için kullanılıyor ama Lab üzerinde NTP sunucu ve istemci arasında aynı olmadığında senkronize olamadığını ve kimlik doğrulama hatası oluştuğunu gördüm). Kimlik doğrulama süreci için son olarak "**ntp trusted authentication-keyid 45**" komutuyla tanımlanan kimlik doğrulama bilgilerinin devreye alınması gerekiyor. NTP sunucu tarafında son yapılması gereken şey ise "**undo ntp server disable**" komutuyla cihaz üzerinde NTP sunucu hizmetinin devreye alınmasıdır (Lab ortamında uyguluyorsan tanımlamalar sonunda "**commit**" komutuyla konfigürasyonları uygulamayı unutma!!).

```
[*CE6800_2]ntp refclock-master 1
[*CE6800_2]ntp authentication enable
[*CE6800_2]ntp authentication-keyid  40 authentication-mode hmac-sha256 Huawei123
[*CE6800_2]ntp trusted authentication-keyid 40
[*CE6800_2]undo ntp server disable
```

- NTP istemcisinde yapılması gerekenlere bakıldığında ilk olarak "**ntp authentication enable**" komutuyla kimlik doğrulama mekanizmasının açılması gerekiyor. Ardından "**ntp authentication-keyid <Key Id> authentication-mode <Hash Algorithm> <Password>**" komutuyla NTP sunucu cihaz üzerinde tanımlanan bilgiler burada da tanımlanmalıdır. Kimlik doğrulama süreci için son olarak "**ntp trusted authentication-keyid 45**" komutuyla tanımlanan kimlik doğrulama bilgilerinin devreye alınması gerekiyor. Son adımda ise "**ntp unicast-server <Ip Address> authentication-keyid <Key Id>**" komutuyla NTP sunucunun ip adresi ve tanımlanan kimlik doğrulama bilgilerin temsil eden Key Id değeri ile eşleştiriliyor.

```
[~CE6800_1]ntp authentication enable
[~CE6800_1]ntp authentication-keyid 40 authentication-mode hmac-sha256 Huawei123
[*CE6800_1]ntp trusted authentication-keyid 40
[*CE6800_1]ntp unicast-server 192.168.0.140 authentication-keyid 40
[*CE6800_1]commit
```

- Cihazlara ilk erişim için kullanılan Console portuna parola tanımlamak için "**user-interfaec Console 0**" komutuyla Console arayüzüne giriş yapılır (Fiziksel bir switche Console portundan bağlanılarak ilk kurulum yapılırken karşılaşılan ilk konfigürasyon cihaza Console parolası belirlenmesidir. Console parolası tanımlandıktan sonra komut satırına erişiliyor). Burada parola tanımı yapılabileceği gibi AAA protokolü kullanılarak tanımlı kullanıcıların giriş yapabilmesi sağlanabilir. Sadece parola kullanarak giriş yapılabilmesi için önce "**authentication-mode password**" komutuyla doğrulama işleminin tanımlanacak parola bilgisiyle yapılacağı belirlenir. Ardından "**set authentication password cipher <Password>**" komutuyla Console erişimlerinde kullanılacak parola tanımı yapılır (Console parolası değiştirilmek istendiğinde de aynı tanımlar kullanılıyor).

```
[CE6800-1]user-interface console 0
[CE6800-1-ui-console0]authentication-mode ?
  aaa       AAA authentication, and this authentication mode is recommended
  password  Authentication through the password of a user terminal interface
[CE6800-1-ui-console0]authentication-mode password
[CE6800-1-ui-console0]set authentication password cipher
Warning: The "password" authentication mode is not secure, and it is strongly re
commended to use "aaa" authentication mode.
Enter old password:
Enter Password(<8-128>):
Confirm password:
```

- Her ne kadar günümüzde kullanılmasa da uzaktan bağlantılar için Telnet konfigürasyonu yapılması gerektiğinde bağlantı yapılacak arayüze ip adresi tanımlandıktan sonra;
    - İlk olarak devrede gelmiyorsa "**undo telnet server disable**" komutuyla Telnet hizmetinin devreye alınması gerekiyor. Daha sonra "**user-interface vty 0 <Simultaneously Connect User Count>**" komutuyla aynı anda kaç kullanıcının bağlanılmasının isteniyorsa belirtilir ve bu arayüz altında "**protocol inbound telnet**" komutuyla sadece Telnet ile bağlanılması sağlanır (Cisco cihazlarda belirtilmediği

takdirde varsayılanda hem SSH hem de Telnet hizmeti devrede oluyordu). Son olarak kimlik doğrulama işlemi için kullanıcı bilgilerinin nasıl kontrol edileceğini belirten "**authentication-mode <Authentication Mode>**" komutu kullanılıyor.

```
[~CE6800_1-ui-vty0-4]authentication-mode ?
  aaa       AAA authentication
  none      Login without checking
  password  Authentication through the password of a user terminal interface
```

- Burada AAA hizmeti kullanılabileceği gibi "**authentication-mode password**", "**set authentication password cipher <Password>**" ve "**user privilege level <Privilege Level>**" komutlarıyla bir parola ve bir yetki seviyesi belirlenip kullanıcıların bu parola üzerinden bağlanılması da sağlanabilir. Benzer şekilde bu arayüz altında daha pek çok özelleştirme de gerçekleştirilebilmektedir.

```
[*CE6800_1]user-interface vty 0 4
[*CE6800_1-ui-vty0-4]protocol inbound telnet
[*CE6800_1-ui-vty0-4]authentication-mode password
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use
 "aaa" authentication mode.
[*CE6800_1-ui-vty0-4]set authentication password cipher Huawei123
Warning: The "password" authentication mode is not secure, and it is strongly recommended to use
 "aaa" authentication mode.
[*CE6800_1-ui-vty0-4]user privilege level 3
```

Cihaz üzerinde AAA konfigürasyonu için "**aaa**" komutuyla AAA arayüzüne giriş yapılır. Burada ilk olarak "**local-user <Username> password irreversible-cipher <Password>**" komutuyla yerel bir kullanıcı oluşturulur. Bu kullanıcıya "**local-user <Username> service-type telnet**" komutlarıyla Telnet üzerinden bağlanabilmesi sağlanır. Kullanıcının Telnet üzerinden hangi yetki seviyesinde bağlanılması isteniyorsa "**local-user <Username> level <Privilege Level>** komutuyla ayarlanabilir.

```
[~CE6800_1]aaa
[~CE6800_1-aaa]local-user nadmin password irreversible-cipher Huawei.123
Info: A new user is added.
[*CE6800_1-aaa]local-user nadmin service-type telnet
Warning: The service type configured contains unsecured protocol(telnet). It is recommended to c
onfigure the secure service type only.
[*CE6800_1-aaa]local-user nadmin level 3
[*CE6800_1-aaa]quit
[*CE6800_1]commit
[~CE6800_1]
```

- Günümüzde cihazlara uzaktan erişim için tercih edilen SSH konfigürasyonu yapılmak istendiğinde bağlantı yapılacak arayüze (L2 switcler için VLAN arayüzlerine) ip adresi tanımlandıktan sonra;
  - İlk olarak "**stelnet server enable**" komutuyla SSH hizmetinin devreye alınması gerekiyor. "**user-interface vty 0 <Simultaneously Connect User Count>**", "**protocol inbound ssh**" ve **authentication-mode <Authentication Mode>** komutları sırasıyla çalıştırılarak SSH ayarlamaları yapılır.
    Kimlik doğrulama süreci için swiitchde "**aaa**", "**local-user <Username> password irreversible-cipher <Password>**", "**local-user <Username> service-type ssh**" ve "**user privilege level <Privilege Level>**"" komutlarıyla kullanıcı tanımı yapılır (Özetle komutlarda Telnet yerine SSH yazılıyor).

Son adımda Telnet hizmetinden farklı olarak "**rsa local-key-pair create**" komutuyla bağlantı sürecinde trafiği şifrelemek için kullanılacak RSA şifreleme algoritması için anahtar oluşturulması gerekiyor.

```
[~CE6800_2]stelnet server enable
Info: The STelnet server is already started.
[~CE6800_2]user-interface vty 0 4
[~CE6800_2-ui-vty0-4]protocol inbound ssh
[~CE6800_2-ui-vty0-4]authentication-mode aaa
[~CE6800_2-ui-vty0-4]quit
[~CE6800_2]
[~CE6800_2]aaa
[~CE6800_2-aaa]local-user newadmin password irreversible-cipher Huawei.123
Info: A new user is added.
[*CE6800_2-aaa]local-user newadmin service-type ssh
[*CE6800_2-aaa]local-user newadmin level 3
[*CE6800_2-aaa]quit
[*CE6800_2]
[*CE6800_2]rsa local-key-pair create
The key name will be:CE6800_2_Host
```

- Oluşturulan kullanıcı tanımını kaldırmak için "**aaa**" ve "**undo loca-user <Username>**" komutlarını kullanmak yeterlidir.

- Doğrudan AAA arayüzüne giriş yapıp kullanıcı tanımı yapmak yerine "**ssh user <Username>**", "**ssh user <Username> service-type stelnet**" ve "**ssh user <Username> authentication-type <Authentication Type>** " komutlarıyla SSH bağlantılarında kullanılacak kullanıcı tanımı da yapılabiliyor. Kullanıcı tanımı yapıldıktan sonra yine AAA arayüzüne giriş yapıp parola tanımı, yetki seviyesi gibi tanımların yapılması gerekiyor.

```
[*CE6800-2]ssh user nladmin
Info: Succeeded in adding a new SSH user.
[*CE6800-2]ssh user nladmin service-type stelnet
[*CE6800-2]ssh user nladmin  authentication-type password
[*CE6800-2]aaa
[*CE6800-2-aaa]local-user nladmin password irreversible-cipher Huawei.123
Info: A new user is added.
[*CE6800-2-aaa]local-user nladmin level 3
[*CE6800-2-aaa]local-user nladmin service-type ssh
[*CE6800-2-aaa]quit
[*CE6800-2]commit
[~CE6800-2]rsa local-key-pair create
The key name will be:CE6800-2_Host
% RSA keys defined for HUAWEI_Host already exist.
Confirm to replace them? Please select [Y/N]:y
The range of public key size is (2048 ~ 2048).
NOTE: Key pair generation will take a short while.
[*CE6800-2]commit
```

- Router üzerinde SSH hizmeti devreye alınmak istendiğinde "**interface <Interface Id>**" komutuyla bir arayüzün altına giriş yapılarak "**ip address <Ip Address> <Subnet Mask>**" komutuyla ip adresi tanımlanması gerekiyor. Son olarak "**undo shutdown**" komutuyla port açılması gerekiyor. Bu tanımlamalar sonrasında switchler üzerinde uygulanan SSH konfigürasyonu aynen uygulanarak SSH hizmeti devreye alınabilir.

Huawei switch ve routerlara web arayüzü üzerinden erişilerke konfigüre etmek de mümkün. Bunun için;

- İlk olarak cihaz üzerinde bulunan AAA hizmeti altında "**local-user <Username> password irreversible-cipher <Password>**" komutuyla bir kullanıcı tanımı oluşturulması gerekiyor. Bu kullanıcıya "**local-user <Username> privilege level <Level>**" komutuyla cihaz üzerindeki en yüksek erişim yetkilerinin (15) verilmesi ve bu kullanıcıya "**local-user <Username> service-type http**" komutuyla HTTP hizmeti üzerinden cihaza erişim sağlamasına izin verilmesi gerekiyor.

```
aaa
local-user admin1 password irreversible-cipher Ab*45678
local-user admin1 service-type http
local-user admin1 privilege level 15
quit
```

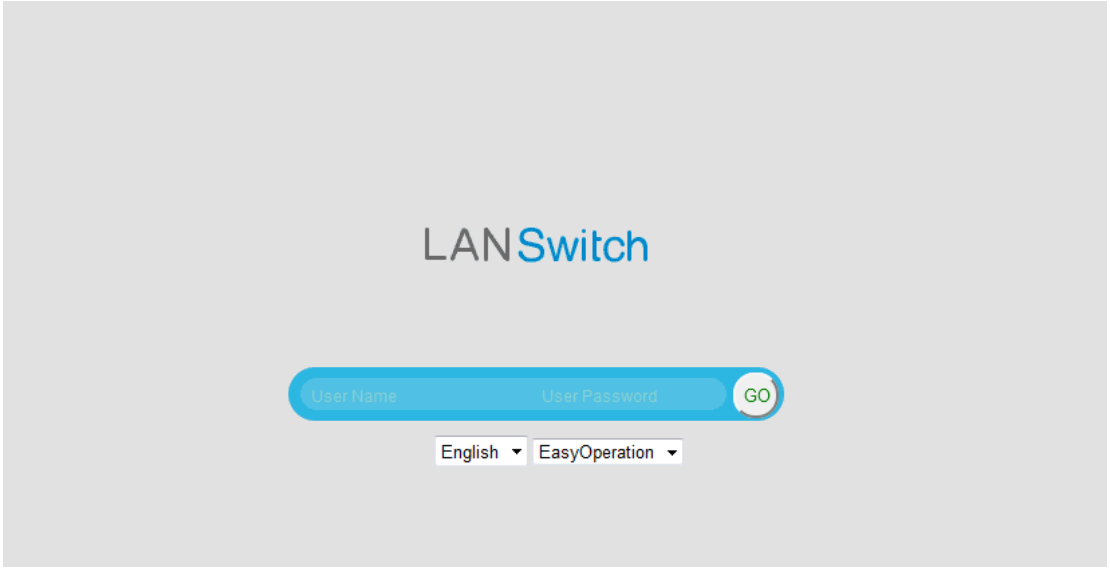
- Kullanıcı tanımı oluşturulduktan sonra cihaza erişim için bir arayüzüne ip verilmesi gerekiyor. Bunun için varsayılanda cihaz portları L2 ve **Desirable** modunda (İlerleyen bölümlerde açıklanacaktır. Aynı zamanda bu bir güvenlik zaafiyetidir) gelecektir. Bu durumda herhangi bir farklı konfigürasyon yapılmadan, bilgisayarınızı doğrudan bağlayarak erişmek için VLANIF1 arayüzüne "**int vlanif 1**" komutuyla giriş yaparak erişmek istediğiniz herhangi bir ip adresini "**ip address <IP Address> <Subnet Mask>**" komutuyla atayabilirsiniz (Burada bilgisayarınıza da aynı networke dahil olacak şekilde bir ip adresi atanmalıdır).

```
int vlanif 1
ip address 192.168.1.200 24
quit
```

- Son adım olarak varsayılanda Huawei cihazlarda Web erişimi kapalı geliyor. Cihaz üzerinde Web erişimini devreye almak için "**http secure-server enable**" komutu kullanılmalıdır. İsteğe bağlı olarak Web erişimi için kullanılması istenen arayüz "**http server-source –i <Interface ID>**" komutuyla kısıtlanabiliyor.

```
http secure-server enable
http server-source -i Vlanif 1
```

- Artık herhangi bir tarayıcı üzerinden Huawei cihazın Web arayüzüne erişim sağlayarak oturum açabilirsin.



Notlar

- Komut satırında yazılan komutları silmek için imleci komutun başına getirmek gerekiyor veya "**CTRL+X**" kombinasyonuyla tek hamlede bütün komut silinebiliyor.
- Cihaz üzerinde kullanılan komutlar "**commit**" komutuyla uygulanmadığı veya bir alt moda geçiş yapılırken kaydedilmesi istenilip istenmediği sorulduğunda kaydedilmediği sürece sistem üzerinde uygulanmıyor. Konfigürasyon sonunda konfigürasyonların kalıcı olarak kaydedilmesi için "**save**" komutunun kullanılması gerekiyor.
- "**CTRL+Z**" kombinasyonuyla bir alt moda geçiş yapılabiliyor.
- Cihaz üzerindeki bütün konfigürasyonlar sıfırlanmak isteniyorsa "**reset saved-configuration**" komutundan sonra "**reboot**" komutuyla cihaz yeniden başlatılmalıdır.
- Varsayılanda bütün portlar kapalı geliyor. Bu nedenle kullanılacak her bir arayüzün altına giriş yapılarak "**undo sh**" komutuyla açılması gerekiyor.
- Uygulanmasa da servisler üzerinde pek çok özelleştirme yapılabiliyor.

```
[*CE6800_2]ssh server ?
  acl                     Set the SSH server ACL
  assign                  Set the key
  authentication-retries  Set the authentication times
  authentication-type     Authentication type
  cipher                  The encryption algorithm
  compatible-sshlx        Set the compatible sshlx
  dh-exchange             Set the minimum value of the
                          Diffie-hellman-group-exchange key exchange algorithm
                          for the SSH server
  dscp                    Set the dscp value
  hmac                    The HMAC algorithm
  ip-block                IP block feature
  keepalive               Set the keepalive attribute
  key-exchange            The key exchange algorithm
  login-failed            Configure administrator type authentication login
                          failed alarm
  port                    Set the port attribute
  publickey               set ssh server public key type
  rekey                   Rekey configuration
  rekey-interval          Set the interval generated by the SSH server key
  timeout                 Set the authentication timeout
```

- Aruba cihazların üzerinde olduğu gibi Huawei cihazların üzerinde de fiziksel Management portu bulunuyor. Bu port üzerinden varsayılanda gelen ip adresi kullanılarak web arayüzüne erişim sağlanabiliyor (Kullanıcı tanımı yapıldığı takdirde - https[:]//support.huawei.com/enterprise/en/doc/EDOC1100097996).
    - Bu port kullanılarak switchlerin Web üzerinden yönetimini sağlamak üzere bir network altyapısı kurulabilir. Bu sayede switch/Router yönetimi için ayrı bir altyapı kurulabilir.

```
          -SW1>dis ip int bri
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 3
The number of interface that is DOWN in Physical is 1
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 2

Interface                         IP Address/Mask      Physical   Protocol
MEth0/0/1                         192.168.1.253/24     down       down
NULL0                             unassigned           up         up(s)
Vlanif1                           unassigned           up         down
```

- Console portu ise sadece cihazın konsoluna erişim için kullanılıyor.
- Arayüzlere toplu konfigürasyon uygulanacağı zaman "**int range <Start Interface Id> <End Interface Id>**" komutuyla aynı anda birden fazla arayüze uygulanabilir.

Kontrol Komutları

- Display clock
- Display current-configuration
- Display ntp {status | sessions | event clock-unsync}
- Display telnet {server | client}
- Display aaa local-user

Kaynaklar

- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100095728
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178166/aed8a823/basic-configuration-on-the-device-at-first-login
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000039339/18b98c59/configuring-ntp-to-synchronize-time
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100212501/4adec9f7/saving-the-configuration-file
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100127196/b3180b88/configuring-telnet-login
- https[:]//www.youtube.com/watch?v=whlq6Xa4fJo
- https[:]//salihaltuntas.com/huawei-ssh-yapilandirmasi/
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100097996