Aruba Genel Notlar

Aruba cihazında konsola erişildiğinde ilk göze çarpan detay Cisco IOS'a benzerliği oluyor. Bu nedenle anlatımda Cisco IOS üzerinden örnekler verilerek/benzetmeler yapılarak anlatılmaya çalışılmıştır. Lab ortamı için kullanılan Aruba CX model switchlerde giriş ekranında kullanıcı adı ve parola bilgisi soruluyor. Varsayılanda kullanıcı adı kısmına "admin", parola kısmını boş bırakılarak devam edildiğinde yeni bir parola tanımlanması isteniyor. Burada yeni bir parola tanımı yapılmalıdır.

Komut satırına ulaşıldığında kullanıcıyı Cisco IOS'daki Privilege Exec mod olarak tarif edilen mod karşılıyor. Bu mod cihaz üzerindeki hizmetlerin durumunu görüntülemek gibi temel işlemler yapılabiliyor. Konfigürasyon arayüzüne giriş yapabilmek için "**configure terminal**" komutu kullanılıyor. Cihaza ilk erişimde yapılabilecek konfigürasyonlar için konfigürasyon moduna geçiş yapılarak;

- İlk adımda cihazı yeniden isimlendirmek için "**hostname <Device Name>**" komutu kullanılıyor.

- Kullanıcı parolasını değiştirmek için "**user <Username> password {plaintext | ciphertext}**" komutu kullanılıyor. Komut sonrasında yeni parola bilgileri isteniyor.

- Kullandığım modelin portlar L3 geldiği için "**interface <Start Interface Id >-<End Interface Id>**" komutuyla aynı anda birden fazla portun arayüzüne giriş yapılarak "**no routing**" ve "**no sh**" komutlarıyla L2'ye çekilmesi ve açılması gerekiyor. Her ne kadar portlar L2'ye çekilse de varsayılanda STP protokolü de devre dışı geliyor. Loop oluşma ihtimaline karşın devreye almak faydalı olacaktır. Varsayılan ayarlarda devreye almak için "**spanning-tree**" komutu kullanılıyor (Detaylı konfigürasyonunu STP notlarında bulabilirsin).

```
ArubaCX-1(config)# interface 1/1/1-1/1/6
ArubaCX-1(config-if-<1/1/1-1/1/6>)# no routing
ArubaCX-1(config-if-<1/1/1-1/1/6>)# no sh
ArubaCX-1(config-if-<1/1/1-1/1/6>)# exit
ArubaCX-1(config)# spanning-tree
```

- Cihaz üzerindeki tarih ve saat bilgileri manuel veya bir NTP sunucusu üzerinden ayarlanabiliyor.
    - İlk olarak "**clock {time < HH:MM:SS > | date <YYYY-DD-MM> |datetime <YYYY-DD-MM HH:MM:SS> | timezone <Timezone>}**" komutuyla manuel olarak ayarlanabiliyor.

```
ArubaCX-1(config)# clock
  date      Configures date on system & RTC
  datetime  Configures date & time on system & RTC
  time      Configures system & RTC time
  timezone  Configures Timezone and associated DST rule
```

    - Bir NTP sunucusundan (Kimlik denetimi devreye alınmamış) zaman bilgilerinin güncellenmesi için öncelikle "**ntp enable**" komutuyla NTP hizmetinin devrye alınması sağlanıyor (Hem istemci hem de sunucu modunda devreye giriyor). NTP hizmeti devreye alındıktan sonra "**ntp server <Ip Address> brust**" NTP sunucusunun ip adresi tanımlanıyor. Bu tanımdan sonra switch NTP protokolü üzerinden varsayılan ayarlarda zaman bilgilerini güncellemeye başlıyor.

- Benzer şekilde birden fazla NTP Server tanımı da yapılabiliyor. Her NTP sunucusu için ayarlamalar ip adresleri üzerinde gerçekleştiriliyor (“**ntp server <Ip Address> <Settings>**“).
- Switch üzerinde NTP Server ayağa kaldırmak için cihaz üzerinde ip ayarlamaları yapılıp (varsayılanda L2’ye alınan bütün portlar VLAN 1’e dahil geldiği için VLAN 1 arayüzüne ip adresi tanımlanabilir) zaman bilgisi ayarlandıktan sonra “**ntp enable**” komutunun kullanılması yeterli oluyor. Bu komut sonrasında switch hem istemci hem de sunucu modunda devreye alınıyor.

```
ArubaCX-1(config)# ntp enable
ArubaCX-1(config)# ntp server 192.168.1.200 iburst
ArubaCX-1(config)# ntp server 192.168.1.200
  burst     NTP Association use burst mode
  iburst    NTP Association use iburst mode
  key-id    NTP Key ID
  maxpoll   NTP maximum poll time to use configuration
  minpoll   NTP minimum poll time to use configuration
  prefer    NTP Association preference configuration
  version   NTP Association version configuration
  <cr>
```

- Aruba switch üzerinde NTP Server devreye almak için switch üzerindeki zaman bilgisini güncelledikten sonra yine “**ntp enable**” komutunu kullanmak yeterli oluyor. Ek olarak Stratum değerini güncellemek ve çalışacağı VRF’i belirlemek için “**ntp master stratum <Stratum> vrf <VRF Name>**” komutu kullanılması gerekiyor (NTP Server’ın VRF ve Stratum tanımı yapılıyor). Burada dikkat edilmesi gereken bir konu var. NTP Server ve NTP Client aynı VRF (Virtual Routing and Forwarding) üzerinde çalıştırılamıyor. Bu edenle NTP Server ayağa kaldırılacak switch üzerinde “**ntp vrf <VRF Name>**” komutu kullanılarak NTP istemci modunda çalışılacak VRF farklı bir VRF’e alınmalıdır (default veya mgmt VRF’lerine ayrılabilir). Ayrıca NTP Client üzerinde de NTP sunucuya bağlanabilecek VRP üzerinde olduğundan emin olmalısın.

```
ArubaCX-2(config)# clock timezone turkey
ArubaCX-2(config)#
ArubaCX-2(config)# ntp vrf mgmt
ArubaCX-2(config)#
ArubaCX-2(config)# ntp master vrf default stratum 4
ArubaCX-2(config)# ntp enable
```

- NTP istemci üzerinde kimlik denetimini devreye almak öncelikle “**ntp enable**” komutuyla NTP hizmetinin devreye alınması gerekiyor. NTP hizmeti devreye alındıktan sonra Huawei switch üzerinde olduğu gibi “**ntp authenticate**” komutuyla kimlik doğrulama hizmetinin devreye alınması gerekiyor. Ardından “**ntp authentication-key <Key Id> <Hash Algorithm> <Password/Key>**” komutuyla kimlik doğrulama sürecinde kullanılacak anahtar tanımı yapılır. Son olarak “**ntp trusted-key <Key Id>**” komutuyla kimlik doğrulama işlemi için tanımlanan anahtar bilgilerinin devreye alınması gerekiyor. Tanımlanan kimlik doğrulama bilgileri doğrultusunda “**ntp server <Ip Address> brust <Key Id>**” komutuyla sunucu ip adresi ayarlanarak NTP sunucusuna bağlanılması sağlanır.

- Aruba switchlerde daha önce de bahsedildiği gibi ”**ntp enable**” komutuyla hem istemci hem de sunucu hizmeti devreye giriyordu. Bu doğrultuda istemci switch üzerinde uygulanan her komut (son komut dışında -> “**ntp server <Ip Address> brust <Password/Key>**”) NTP Server hizmeti veren switch üzerinde uygulanması gerektiği anlaşılacaktır. Ek olarak switch üzerinde çalıştırılacak NTP server ve NTP Client’in çalışacağı VRF’lerin değiştirilmesi gerekiyor.

```
ArubaCX-1(config)# ntp authentication
ArubaCX-1(config)# ntp authentication-key 35 sha1 Aruba123
ArubaCX-1(config)# ntp trusted-key 35
ArubaCX-1(config)# ntp server 192.168.1.200 burst key-id 35
ArubaCX-1(config)# ntp enable
```

Client

```
ArubaCX-2(config)# clock timezone turkey
ArubaCX-2(config)#
ArubaCX-2(config)# ntp vrf mgmt
ArubaCX-2(config)#
ArubaCX-2(config)# ntp authentication
ArubaCX-2(config)# ntp authentication-key 35 sha1 Aruba123
ArubaCX-2(config)# ntp trusted-key 35
ArubaCX-2(config)# ntp master vrf default stratum 4
ArubaCX-2(config)# ntp enable
```

Server

- Gördüğüm kadarıyla kullandığım Aruba CX switch üzerinde Telnet desteği bulunmuyor. Desteklenen switchler üzerinde Telnet konfigürasyonu yapılmak istendiğinde Huawei switch üzerinde uygulanan komutlarla neredeyse birebir aynıdır (https[:]//support.hpe.com/hpesc/public/docDisplay?docId=sf000048968en_us&docLocale=en_US&page=index.html).

```
telnet server enable

user-interface vty 0 4
authentication-mode password
authentication password simple secret
user privilege level 3
exit
```

- Uzak bağlantı için SSH konfigürasyonu için aslında farklı bir konfügrasyon yapılmasına gerek kalmıyor. Varsayılanda SSH konfigürasyonu Management arayüzünde (MGMT VRF) devrede ve konfigüre edilmiş geliyor (isteğe bağlı olarak “**ssh server vrf default**” komutuyla **Default VRF** üzerine çekilmesi ve farklı fiziksel portlara (L3 olmalı) veya VLAN’lar gibi sanal arayüzlere (portlar L2 olmalı) ip adresleri atandıktan sonra erişilmesi de sağlanabilir – Denendi çalıştı). Sadece bağlantı kurabilmek için Management arayüzüne ip adresinin tanımlanması yeterli oluyor. Bağlantı kurulduğunda cihaz üzerinde tanımlı herhangi bir kullanıcı hesabıyla oturum açılabilir.

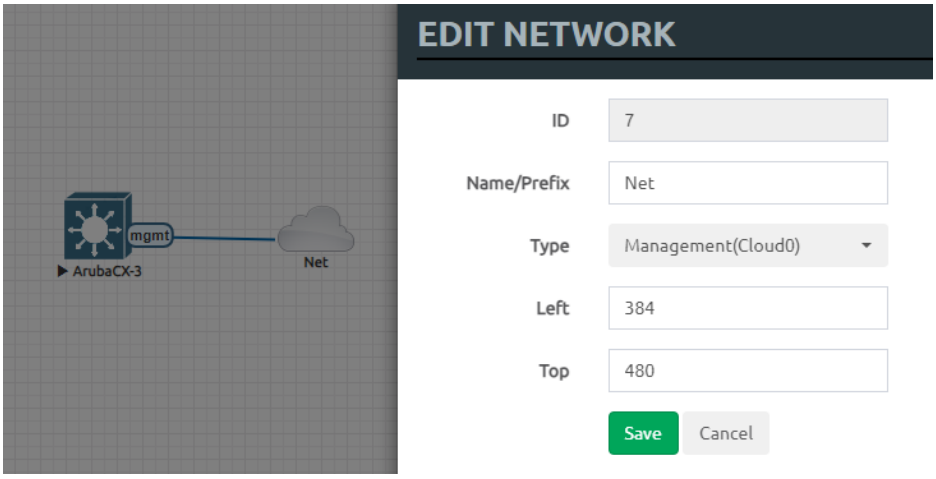
```
ArubaCX-1(config)# int mgmt
ArubaCX-1(config-if-mgmt)# ip dhcp
ArubaCX-1(config-if-mgmt)# no shutdown
ArubaCX-1(config-if-mgmt)# exit
ArubaCX-1(config)# do sh int mgmt
  Address Mode                  : dhcp
  Admin State                   : up
  Mac Address                   : 50:00:00:01:00:00
  IPv4 address/subnet-mask      : 192.168.0.115/24
  Default gateway IPv4          : 192.168.0.1
  IPv6 address/prefix           :
  IPv6 link local address/prefix: fe80::5200:ff:fe01:0/64
  Default gateway IPv6          :
  Primary Nameserver            : 192.168.0.1
  Secondary Nameserver          :
ArubaCX-1(config)#
```

```
C:\Users\VMUser>ssh admin@192.168.0.115

The End User License Agreement (EULA) and Additional License Authorization
(ALA) documents are available at the following URL:
www.arubanetworks.com/arubaos-cx-ova
By downloading, copying, or using the ArubaOS-CX OVA you agree to both the
End User License Agreement and the Additional License Authorization.
ArubaOS-CX Virtual Platform is provided for Training purposes only.
As a reminder, there is no support or warranty associated with this platform.

(C) Copyright 2017-2019 Hewlett Packard Enterprise Development LP

                    RESTRICTED RIGHTS LEGEND
Confidential computer software. Valid license from Hewlett Packard Enterprise
Development LP required for possession, use or copying. Consistent with FAR
12.211 and 12.212, Commercial Computer Software, Computer Software
Documentation, and Technical Data for Commercial Items are licensed to the
U.S. Government under vendor's standard commercial license.


admin@192.168.0.115's password:

Last login: 2024-02-17 14:46:49 from the console
User "admin" has logged in 19 times in the past 30 days
ArubaCX-1# conf ter
ArubaCX-1(config)#
```

- İsteğe bağlı olarak “**ssh <Preferences>**” komutuyla özelleştirmeler yapılabiliyor.

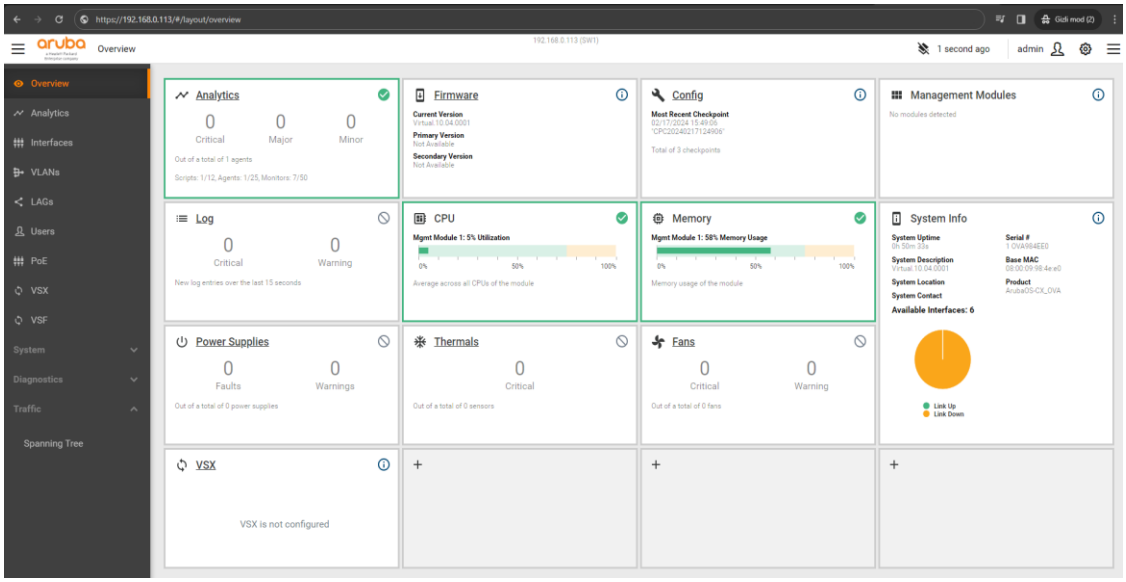
```
ArubaCX-1(config)# ssh
  certified-algorithms-only  Allow certified crypto algorithms only.
  host-key                   SSH server host-keys.
  known-host                 Client trusted servers list.
  maximum-auth-attempts      Configure the maximum number of authentication
                             attempts (Default: 6).
  password-authentication    Password authentication method enabled by default.
  public-key-authentication  Publickey authentication method enabled by
                             default.
  server                     Configure SSH server.
  two-factor-authentication  Enable two factor authentication with X.509v3
                             certificate and password.
```

- Aruba switchlerde web tarayıcısı üzerinden de erişilebiliyor. Bunun için switch üzerinde MGMT (Management) portu bulunuyor (cihaz üzerinde sadece konfigürasyonları yapabilmek için kullanılan arayüzdür. Cihazın Web arayüzüne erişebilmek için kullanılabilecek tek bağlantı seçeneğidir). Switch üzerindeki MGMT arayüzüne fiziksel olarak bağlanıp kullanıcı oturumu açıldıktan sonra ”**int mgmt**”, “**ip {dhcp | static <Ip Address>/<Subnet Mask>}**” ve “**no shutdown**” komutları kullanılarak Management arayüzüne ip adresi tanımlanır (Tanımlama sonrasına Ping atarak sağlıklı bir şekilde bağlantı kurulup kurulamadığını kontrol edebilirsin). Tanımlama sonrasında belirlenen ip adresiyle herhangi bir web tarayıcısı üzerinden bağlanabilirsin.
  Siz de benim gibi Eve-ng üzerinde çalışıyorsanız ve Eve-ng üzerinde çalışan Aruba CX switch arayüzüne nasıl bağlanabileceğinizi merak ediyorsanız, ilk olarak topolojide Mouse üzerine sağ tıklayıp “**network**” kısmında “**Management (Cloud0)**” seçeneği seçilmelidir (Bu seçenekle NAT işlemi yapılıyor). Topoloji ortamına çıkan ikon ile Aruba switchin Management portu birbirine bağlanmalıdır (VLAN arayüzüne ip adresi verildiyse portlardan birisi L2’ye çekilerek Managemen VLAN’a dahil edilmeli).



Bu adımdan sonra “**int mgmt**” komutuyla Management arayüzüne giriş yapılarak “**ip dhcp**” ve “**no shutdown**” komutlarıyla arayüz konfigürasyonu yapılmalıdır. Artık “**do sh int mgmt**” komutuyla Management arayüzünün aldığı ip adresi kontrol edilerek bir web tarayıcısından giriş yapılabilir.

```
SW1(config)# int mgmt
SW1(config-if-mgmt)# ip dhcp
SW1(config-if-mgmt)# no shutdown
SW1(config-if-mgmt)# exit
SW1(config)# do sh int mgmt
  Address Mode                  : dhcp
  Admin State                   : up
  Mac Address                   : 50:00:00:08:00:00
  IPv4 address/subnet-mask      : 192.168.0.113/24
  Default gateway IPv4          : 192.168.0.1
  IPv6 address/prefix           :
  IPv6 link local address/prefix: fe80::5200:ff:fe08:0/64
  Default gateway IPv6          :
  Primary Nameserver            : 192.168.0.1
  Secondary Nameserver          :
```

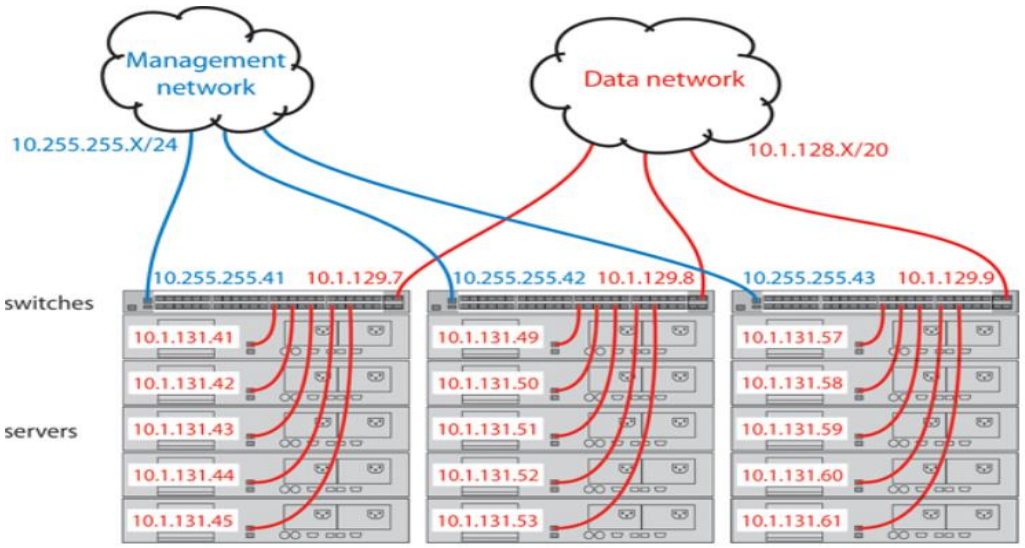


|→ Web UI üzerinden cihazın genel durumu hakkında bilgiler görüntülenebildiği gibi çeşitli konfigürasyonlar da gerçekleştirilebiliyor.

Notlar

- Eve-ng üzerinde Aruba switchlere 2 CPU ve 2GB altında RAM verilmesi durumunda switch doğru çalışmıyor (Aynı switche bağlı iki istemci birbirine ping dahi atamıyor). Bu nedenle konfigürasyona başlamadan önce istemcilerin birbirine ping atabildiklerinden emin olmalısın (Portlar L2'ye alınıp STP protokolü devreye alındıktan sonra).
- Farklı VRF üzerinde (default VRF'den farklı bir VRF üzerinden) ping atılmak isteniyorsa "**do ping <Ip Address> vrd <VRF Name>**" komutu kullanılabilir.
- **Her ne kadar kimlik denetimini devreye almadan NTP Client ve Server konfigüre etmek için uğraşsam da zaman bilgilerini set etmelerini sağlayamadım (ilk konfigürasyon ettikğimde çalıştı sadece). Cihazlara lab ortaında ayırdığım kaynak miktarının az olmasıdan kaynaklı doğru çalışmıyor olabilir veya cihazlar üzerinde kullanılan işletim sisteminin sürümünden kaynaklı bir hata olabilir.**
- Anladığım kadarıyla Aruba switchlerin Management portları (MGMT) daha çok Management VLAN'in L3 versiyonu gibi kullanılıyor. Farklı ve avantajlı olan yanı ise, bu arayüzün fiziksel olması ve varsayılanda farklı VRF'e dahil gelmesi. Bu sayede switch/Router yönetimi için ayrı bir altyapı kurulabiliyor. Kurulan bu altyapı (bir tür yönetim topolojisi de denilebilir) veri iletiminin yapıldığı portlardan (**In Band**) izole çalıştığı için veri iletimi gerçekleştirilen portların

olumsuz yanlarından (bant genişliğinin veri aktarımı için kullanılması, olası saldırı vektörlerini barındırıyor olması …) etkilenilmeden cihazların yönetilebilmesi sağlanıyor (Detaylar için https[:]//techhub.hpe.com/eginfolib/networking/docs/switches/WB/15-18/5998-8162_wb_2920_mcg/content/apb.html sitesini ziyaretedebilirsiniz.– Yönetim için kullanılan portlar **Out Of Band Management** olarak geçiyor).



Kontrol Komutları

- Sh run
- Sh clock
- Sh ntp <associations | statics | status | master | authentication-keys>
- Sh int mgmt

Kaynaklar

- https[:]//support.hpe.com/hpesc/public/docDisplay?docId=c04432839&docLocale=en_US
- https[:]//www.arubanetworks.com/techdocs/AOS-S/16.10/MCG/KB/content/kb/ntp-ser.htm
- https[:]//techhub.hpe.com/eginfolib/networking/docs/switches/K-KA-KB/16-02/5200-1666_K_MCG/content/ch02.html
- https[:]//community.arubanetworks.com/discussion/arubaos-cx-as-an-ntp-time-server
- https[:]//www.arubanetworks.com/techdocs/ArubaOS_63_Web_Help/Content/ArubaFrameStyles/Management_Utilities/Setting_the_System_Clock.htm
- https[:]//www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/ntp.html
- https[:]//arubase.club/wp-content/uploads/2019/05/CLI_Reference_Guide_for_ArubaOS-CX_ArubaOS-Switch_Comware_and_Cisco_IOS.pdf
- https[:]//www.arubanetworks.com/techdocs/AOS-CX/10.07/PDF/AOS-CX_10-07_hardening.pdf