

Network Management

CDP (Cisco Discovery Protocol) Protokolü ile Cihaz Keşfi

CPD, Cisco'ya özel bir protokoldür. Open Standard karşılığı IEEE tarafından çıkarılan LLDP (Link Layer Discovery Protocol) protokolüdür. L2 protokolüdür ve çalışma prensibi olarak her cihaz bağlı olduğu (komşu) cihazlara belirli aralıklarla (varsayılanda 60 sn anons – 180 sn gönderilmezse tablodan silinir) CDP paketi göndererek kendine ait bilgileri paylaşıyor (Sadece doğrudan bağlı olduğu (komşu) cihazları bilgilendiriyor). Bu bilgiler ışığında her cihazda komşu cihazlara **(sadece kendisine doğrudan bağlı cihazlar)** ait bilgilerin bulunduğu komşuluk tablo oluşturuluyor. Bu tablonun asli amacı network yöneticilerini bilgilendirmek (Bu her cihazın oluşturduğu komşuluk tablosu kullanılarak network topolojisi de oluşturulabiliyor).

Varsayılanda bütün Cisco cihazlarda CDP protokolü açıktır. Cihazları kendine ait bilgileri paylaştığı için aslında CDP protokolü bir güvenlik zafiyeti olarak görülmektedir (Saldırgan cihazın herhangi bir portuna bağlanarak cihaz hakkında bütün detayları elde edebiliyor). Bu nedenle cihazlarda devre dışı bırakılabilir.

CDP protokolü cihazın bütün portlarında kapatılmak isteniyorsa Global konfigürasyon modunda “no cdp run” komutu kullanılıyor. Port bazlı kapatılmak isteniyorsa portların arayüzüne girilerek “no cdp enable” komutu kullanılıyor.

```
SWX(config)#int fa 0/1
SWX(config-if)#no cdp enable ➡ Port Bazlı Kapatma
SWX(config-if)#exit
SWX(config)#
SWX(config)#no cdp run ➡ Bütün Portlarda Kapatma
```

| → LLDP protokolü varsayılanda kapalı geliyor. Devreye almak için Global konfigürasyon modunda “lldp run” komutuyla bütün portlarda devreye alınabiliyor. Port bazlı devreye alınmak istendiğinde arayüze giriş yapılarak “lldp transmit” komutuyla lldp paketlerini komşu cihazlara gönderilmesi sağlanabiliyor. Ardından “lldp receiver” komutuyla komşu cihazlarda gelen lldp paketlerinin alınıp işlenmesi sağlanabiliyor (Yani cihazdan sadece lldp paket gönderebiliyor veya sadece lldp paketleri alınabiliyor – Kontrol komutları cdp ile benzerdir).

```
SWX(config)#lldp run ➡ Bütün Portlarda Devreye Alma
SWX(config)#
SWX(config)#int fa 0/1
SWX(config-if)#lldp transmit ➡ Port Bazlı Devreye Alma
SWX(config-if)#lldp receive
SWX(config-if)#exit
```

NTP (Network Time Protocol)

NTP protokolü, hem saat hem de tarih bilgileri network cihazlarına öğretmek için kullanılan bir protokoldür. UDP 123 portunu kullanır. Bu sayede networkteki bütün cihazların saatleri senkronize olmaktadır. Cihazların saat bilgisi daha çok log takibinde önem kazanıyor.

NTP protokolü bir hiyerarşi içerisinde oluşmaktadır. Genelde kurum networklerinde bir NTP sunucusu kurulur ve bütün cihazlar bu sunucudan doğrudan (Stratum 1) saat ve tarih bilgisini alır. Cihazların NTP sunucusundan ip alabilmesi Global konfigürasyon modundan “ntp server” komutuyla NTP sunucusunun ip adresi tanımlanır.

```
SWX(config)#ntp server 209.165.100.200
```

| → Cihazlara manuel olarak tarih ve saat bilgisi “clock set” komutuyla tanımlanıyor.

```
SWX#clock set 09:15:00 20 dec 2022
```

Networkte herhangi bir cihaz üzerinden bütün cihazlara saat ve tarih bilgilerinin öğretilebilmesi için tarih ve saat bilgisini dağıracak cihaz üzerinde Global konfigürasyon moduna girilerek “ntp master” komutunun kullanılması yeterli. Bu komut sonrasında cihaz kendisine manuel olarak tanımlanan veya farklı bir kaynaktan öğrendiği saat ve tarihi bilgisini networkteki cihazlara öğretmeye başlar (Komut sonuna sayısal değer eklenerek stratum değeri değiştirilebiliyor).

```
SWX(config)#ntp master ?  
<1-15> Act as NTP master clock  
<cr>  
SWX(config)#ntp master
```

Saat bilgisi bir kaynaktan alınmıyorsa (doğrudan cihazın kendinde manuel tanımlanan bilgi paylaşıyorsa) bu değer varsayılanda 8 (Stratum) kabul ediliyor.

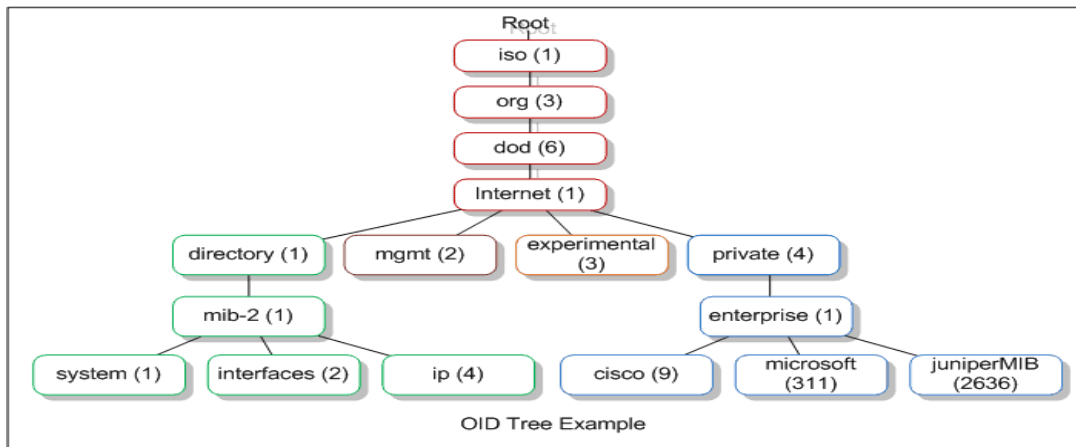
SNMP (Simple Network Management Protocol)

SNMP protokolü, networkü monitor etmek için/networkteki cihazların durumu hakkında bilgi toplayabilmek için kullanılan protokolüdür. Bu süreçte networkte bir NMS Manager bulunur ve SNMP Agent'lara isteklerde bulunarak cihazların durumu hakkında bilgi toplar.

SNMP protokolü kullanılarak cihazlardan çok çeşitli bilgiler talep edilebiliyor. Bu bilgiler marka kapsamında özellikler için olabilirken open standard bazlı özellikler de olabiliyor. Bu ayrımı bir standard haline getirebilmek için MIB (Management Information Base) adında bir tablo oluşturulmuştur. Bu tablo ilk olarak ISO (International Standardization Organization) tarafından oluşturulmuştur ve günümüzde de yaygın kullanılan tablodur (farklı tablolar da oluşturulmuştur. İsteğe bağlı kullanılabiliyor).

MIB tablosu hiyerarşik (tree) bir yapıdadır. Bu yapıda sorguya eklenen her elemana Object adı verilir. Her Object'i temsil edecek bir ID değeri atanmıştır. Örnek olarak aşağıdaki görsel göz önünde bulundurulduğunda cihazın herhangi bir arayüzü hakkında bilgi alabilmek için “1.3.6.1.1.2...” gibi bir örüntü kullanılarak cihaza istekte bulunuluyor. Marka bazlı bir özellik sorgulanmak istendiğin ise “1.3.6.1.4.1...” gibi bir örüntünün kullanılması gerekiyor.

Bu sayede yazılımlar kullanılarak cihazlara belirli sıklıklarda sorgular yapılması sağlanıyor ve bu doğrultuda alınan dönüşlerin grafiklerle dökülmesiyle network cihazları monitör edilebiliyor. Bu grafikler sayesinde networkte değişim/anomali tespiti yapılabiliyor (SolarWinds, Cacti, Zabbix ...).



SNMP Paket Tipleri

- Get-request, SNMP Manager'ın cihazlardan bilgi alırken kullandığı istek paketidir.
- Get-text-request, uzun sorguları parçalar halinde gönderebilmek için kullanılan istek paketidir.
- Get-bulk-request, uzun sorguları tek seferde iletebilmek için kullanılan istek paketidir.
- Get-response, cihazlardan SNMP Manager'ın istekte bulunduğu bilgi gönderilirken kullanılan dönüş paketidir.
- Set-request, uzaktan cihaz üzerinde değişiklik yapılırken kullanılan pakettir (cihazda hostname değiştirmek gibi basit konfigürasyonlar gerçekleştirilirken kullanılıyor).

SNMP Versiyonları

- SNMPv1, ilk SNMP versiyonudur. Güvenlik önlemlerinin çok zayıf olduğu bir versiyondur. Günümüzde kullanılmamaktadır.
- SNMPv2c, bu versiyonla beraber Bulk-retrieval seçeneği ve Detailing Error Message gibi özellikler sunulmuştur. Güvenlik konusunda ciddi sorunlar içermektedir. Authentication mekanizması için kullanılan parola bilgileri paket içerisinde şifrelenmeden iletilmektedir.
- SNMPv3, veri aktarımında çeşitli Hash algoritmalarıyla Authentication mekanizması sağlanmaktadır. Ayrıca DES, 3DES ve AES gibi şifreleme algoritmalarıyla veriler şifrelenerek iletilmektedir.

SNMPv2 Konfigürasyonu

- Konfigürasyon için Global konfigürasyon moduna girilerek "snmp-server community" komutuyla önce parola (Community String) bilgisi, parola'ya verilecek erişim yetkisi (Read or Read-Write) tanımlanıyor.

| → Parola bilgileri aynı olmadığı sürece birden fazla tanımlama yapılabilir.

```
SWX(config)#snmp-server community CoNflg ?  
ro Read-only access with this community string  
rw Read-write access with this community string  
<cr>  
SWX(config)#snmp-server community CoNflg rw
```

| → Bu parolayla cihaz üzerinde SNMP sorgusunu yapabilecek istemcileri kısıtlamak için ise basit bir Standard ACL tanımı yapılabilir. Bu sayede kaynak ip ile SNMP sorgusu yapabilecek istemciler filtrelenebilir. Tanımlanan Standard ACL ise ACL numarası kullanarak SNMP konfigürasyonunda kullanılan komutun sonuna ekleniyor (Sorgu yapabilmek için anahtar kelime bilinmese dahi parola denemeleri yapılarak cihazın CPU'su çatlatılabilir Bu nedenle erişimleri kısıtlamak gerekiyor – Bu durum SNMP versiyonu farketmeksizin geçerlidir).

```
SWX(config)#access-list 5 permit 192.168.10.100  
SWX(config)#snmp-server community CoNflg rw 5  
SWX(config)#
```

- Bu konfigürasyon sonrasında SNMP sunucusunda konfigürasyonlar yapılarak cihazlar monitor edilmeye başlanabilir.

Normalde SNMP ile sorgu yapılmadığı sürece cihazlar bilgi paylaşmazlar. Cihazlarda **belirli durumlar oluştuğunda** kediliğinden NMS'e bildirmesi için SNMP Agent Trap özelliği kullanılabilir. Cihaz üzerinde gerçekleşecek spesifik olaylarda NMS'den istek paketi gönderilmesine gerek kalmadan cihazın cevap paketi göndermesi sağlanabilir (Bir tür Syslog gibi çalışıyor).

Syslog

Log, bir cihazın üzerinde gerçekleşen değişimlerin kayıt altına alınmasıdır. Bu kayıtlar cihazlarda birincil veya ikincil depolama alanlarında tutulabiliyor. Router ve switchlerde de bu kayıtlar RAM üzerinde tutuluyor. Cihazların elektriği kesildiğinde kaydedilen loglar da kaybediliyor. Bu nedenle cihaz üzerinde oluşan logların harici bir kaynak üzerinde tutulması gerekiyor. Bu işlem Syslog adı verilen protokol ile gerçekleştiriliyor (genelde UDP 514 portunu kullanıyor).

Cihazlar üzerinde oluşan her olayın/değişimin logu tutuluyor. Önemli bir değişim gerçekleştiğinde bunu oluşan diğer loglardan ayırt edebilmek adına loglar arasında seviyelendirme işlemi yapılmıştır. Bu seviyelendirmede oluşan logların seviyesi yükseldikçe logun önem/kritikliği de azalmaktadır.

Level Number	Severity Level	Description
0	emergencies	System is unusable.
1	alert	Immediate action is needed.
2	critical	Critical conditions.
3	error	Error conditions.
4	warning	Warning conditions.
5	notification	Normal but significant conditions.
6	informational	Informational messages only.
7	debugging	Debugging messages only.

Konfigürasyonu için İstemciler (switch-router) üzerinde Global konfigürasyon moduna girilerek “logging” komutuyla Syslog sunucusunun sadece ip adresi tanımlanıyor. Tanımlama sonrasında varsayılanda level-6’dan (seviye 6 ve alt seviyeler için logları gönderir) yazmaya başlar. Bu özellik “logging trap” komutuyla istenen seviye (belirtilen seviye ve alt seviyeleri dahil oluyor) belirtilerek değiştirilebiliyor.

```
SWX(config)#logging ?
A.B.C.D    IP address of the logging host
buffered   Set buffered logging parameters
console    Set console logging parameters
host       Set syslog server IP address and parameters
on         Enable logging to all enabled destinations
trap       Set syslog server logging level
SWX(config)#logging 192.168.10.100
SWX(config)#logging trap ?
debugging  Debugging messages                (severity=7)
<cr>
SWX(config)#
```

Router ve Switchlerin Dosya Sistemleri

Router ve switchler içerisinde basit bir bilgisayar barındıran cihazlardır. İçerisinde yönetimi için kullanılan işletim sistemi dosyaları ve network admini tarafından tanımlanan konfigürasyon dosyaları bulunmaktadır. Bu dosyalar cihazlarda kalıcı depolama alanı olarak kullanılan Flash ünitesinde bulunmaktadır (Privileged Exec modunda “dir” komutuyla görülebilir). Switchlerde farklı olarak routerlarda NVRAM adından fiziksel olarak kalıcı depolama alanı da bulunmaktadır (Privileged Exec modunda “cd nvram” ve “dir” komutlarıyla görülebilir – switchlerde ise Flash dosyası içerisinde sanal bir alandır. Fiziksel bir depolama bulunmuyor) ve cihaz üzerinde kaydedilen konfigürasyonlar burada tutulmaktadır. Cihaz açılırken bütün dosyalar kalıcı hafızalardan RAM’e taşınır.

Cihaz üzerinde bulunan dosyalarla işletim sistemi silinebilir, cihaz sıfırlanabilir, güncelleme işlemi yapılabilir, konfigürasyon yedekleri alınabilir (“sh run” çıktısını bir text’e kopyalanıyordu). Özetle bu ve bunlara benzer çok daha fazla işlem yapılabilmektedir. Örnek olarak CCNA – 2.2 notunda cihazın Enable parolası unutulduğunda cihaz sıfırlama işlemi açıklanmıştı. Cihazı sıfırlamadan konfigürasyonu kurtarmak için;

- İlk olarak cihazın gücü kesilir. Ardından Console portundan bağlanılır (cihazın yanında olunmalı).
- ROMMonitor moda düşebilmek için cihazdan cihaza farklılık gösterebilmektedir (ihaz üzerinde bulunan “mode” tuşuna basılabiliyor, açılırken “ESC” tuşuna basılması istenebiliyor ... – Packet Tracer’de uygulama yapıyorsan cihaz yüklenirken CTRL+C kombinasyonunu uygulaman yeterli).
- Rom monitor moda düşüldüğünde “?” ile kullanılacak komutlar görülebiliyor.
- Cihazın startup-config dosyasını atlayarak açılması için cihazın açılırken hangi yazılımların yüklenip çalışacağını belirleyen “confreg” değişkeninin set edilmesi gerekiyor. Bu nedenle “confreg 0x2142” komutu kullanılıyor (<https://www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html>).
- Komut sonrasında cihaz “reset” komutuyla yeniden başlatıldığında temiz konfigürasyonla açılıyor.

```
Final autoboot attempt from default boot device...
Located isr4300-universalk9.16.06.04.SPA.bin
#####
monitor: command "boot" aborted due to user interrupt
rommon 1 > ?
boot                | boot up an external process
confreg             | configuration register utility
dir                 | list files in file system
help                | monitor builtin command help
reset               | system reset
set                 | display the monitor variables
tftpdnld            | tftp image download
unset               | unset a monitor variable
rommon 2 > confreg 0x2142
rommon 3 > reset
```

- Cihaz açıldıktan sonra Enable moduna girilerek “copy startup-config running-config” komutuyla parolası unutilan konfigürasyon dosyası running-config’e yeniden yükleniyor.
- Artık Enable modundan olduğu için eski konfigürasyon dosyasından tanımlanan parola sorulmadan Global konfigürasyon moduna girilip “enable secret” komutuyla yeni bir parola tanımlanıyor. Son olarak cihaz yeniden başlatıldığında temiz konfigürasyonla açılmaması için “confreg “ değişkeninin değerinin “config-register 0x2102” komutuyla güncellenmeli.

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

Router>en
Router#copy startup-config running-config
Destination filename [running-config]?

705 bytes copied in 0.416 secs (1694 bytes/sec)
RX#
%SYS-5-CONFIG_I: Configured from console by console

RX#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
RX(config)#enable secret MyPass123
RX(config)#config-register 0x2102
RX(config)#exit
RX#
```

Bir bilgisayar (tftpd64 gibi) veya sunucu üzerinde bir TFTP sunucusu ayağa kaldırarak cihazlara herhangi bir dosya yükletilebiliyor veya çekilebiliyor. Örnek olarak (bir TFTP sunucu ayağa kaldırıldıktan sonra) cihazda çalışır durumdaki konfigürasyon dosyası yedeklenmek isteniyorsa sadece cihaz üzerinde Privileged Exec modunda girip “copy running-config tftp” komutu kullanılarak TFTP sunucusunun ip adresi ve ardından sunucuya yüklenecek dosya ismi veriliyor. Bu tanımlamalar sonrasında cihaz TFTP sunucusuna erişerek belirtilen dosyayı gönderiyor.

Benzer şekilde TFTP sunucusundan cihaza dosya yüklenmek isteniyorsa (running-config) bunun için yine privileged Exec modunda “copy tftp: sturtup-config” komutuyla hedef TFTP sunucunun ip adresi, kaynak dosya ismi (sunucuda yüklenecek dosya ismi) ve hedef dosya isimleri tanımlamak yeterli oluyor.

- İlk olarak işlem yapılacak cihaz cihaz üzerinde bir TFTP sunucusu kur ve erişim kontrolü yap.
- Cihazda “sh flash” komutuyla yüklü OS’leri görüntülenebilir. OS yedekleyebilmek için “copy flash: tftp:” komutu kullanılıyor. Daha sonra Flash ünitesinden TFTP sunucusuna kopyalanacak dosya isim ve TFTP sunucusunun ip adresi tanımlanıyor (isteğe bağlı destination address bilgisi için TFTP sunucusunda kaydedilecek isim de girilebiliyor). Bu işlem sonunda cihazda belirtilen OS, TFTP sunucusuna kopyalanıyor.

Physical Config **Services** Desktop Programming Attribut

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP**
- DNS
- SYSLOG
- AAA
- NTP
- EMATI

Service

- YeniYedekOS.bin**
- asa842-k8.bin
- asa923-k8.bin
- c1841-advipservicesk9-mz.124-15.T1.bin

İşletim sistemini güncellemek için ;

- Cihazın işletim sistemini güncelleyebilmek için Flash ünitesinde yer varsa ikinci bir işletim sistemi yüklenip cihazın bu işletim sistemiyle boot edimlesi sağlanabiliyor. Cihazda ikinci bir işletim sistemi için yeterli alan yoksa Flash ünitesinde kayıtlı işletim sistmei silinip TFTP sunucusundan yeniden yüklenerek cihazın yeniden başlatılması gerekiyor.

| → Bu işlem sırasında işletim sistemi RAM'a yüklendiği için Flash ünitesinden silinen işletim sistemi dosyası cihazın çalışmasına etki etmeyecektir (cihaz restart edilmediği sürece). İşletim sistemini Privileged Exec modunda “delete flash: <file_name>” komutuyla siliniyor (Dosya adı verilmezse bütün dosyaları siler).

| → Bu işlem öncesinde oluşabilecek her ihtimale karşı işletim sisteminin yedeği alınması gerekiyor.

| → Bu durumda cihazın yeniden başlatılması, TFTP sunucusundan yüklenmesi gibi işlemler zaman alacağı için yedekleme veya güncelleme işlemlerinin yapıldığı saatler önemlidir.

- İşletim sistemini cihaza yüklemek için “copy tftp: flash:” komutu kullanıldıktan sonra TFTP sunucu ip adresi, TFTP sunucusundan alınacak dosya adı ve cihazda kaydedilecek isim (destination adres) tanımlandıktan sonra yükleme gerçekleşiyor.

[illegible]

- Yükleme tamamlandıktan sonra cihazın Flash ünitesinde birden fazla işletim sistemi görünüyorsa cihaz aksi belirtilmedikçe eski işletim sistemini boot etmeye devam edecektir. Yeni işletim sistemiyle boot olmas için Global konfigürasyon modunda “boot systemem flash flash:/<OS name>” komutuyla boot edilmesi istenen işletim sistemi tanımlanıyor.
- Son adım olarak konfigürasyonları kaydetmeyi unutma.

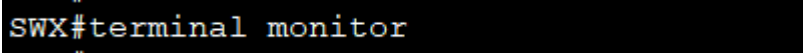
```
R1#sh flash:

System flash directory:
File      Length  Name/status
  4      486899872YeniYedekOS.bin
  3      486899872isr4300-universalk9.16.06.04.SPA.bin
  2       28282    sigdef-category.xml
  1       227537    sigdef-default.xml

[974055563 bytes used, 2274994037 available, 3249049600 total]
3.17338e+06K bytes of processor board System flash (Read/Write)

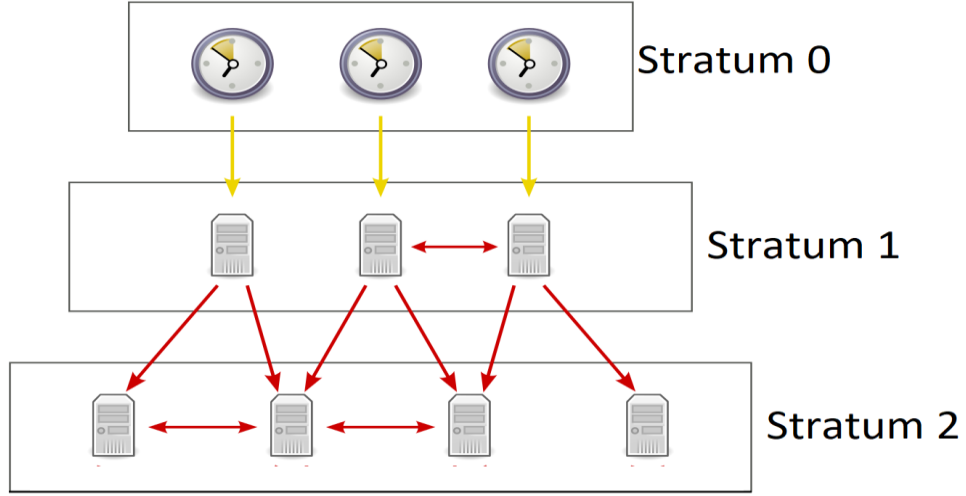

R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#boot system flash flash:/YeniYedekOS.bin
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
R1#
```

NOT

- Belirli yazılımlar kullanılarak CDP veya LLDP protokolleriyle sayesinde network topolojileri oluşturulabiliyor.
- Bazı cihazlara atom saati takılabiliyor. Atom saatlerinin hata /kayma olasılığı ok düşüktür.
- NTP sunucusunda güvenliği arttırmak adına kimlik denetim mekanizması devreye alınabiliyor (<https://www.cisco.com/c/en/us/td/docs/routers/sdwan/command/iosxe/qualified-cli-command-reference-guide/m-ntp-commands.pdf>).
- Markalar SNMP ile sorgulanabilecek özelliklerin MIB tablosundaki karşılığını (numarasını) kendi sayfasında paylaşıyor. Bu değerleri network yöneticisinin bilmesine gerek yok. Daha çok bu tür monitoring yazılımı geliştiren developerları ilgilendiriyor. Developer yazılımı geliştirirken kullanılan marka/model cihazların kendi sitelerine girip SNMP protokolüyle sorgulamak istediği özelliği karşılayan MIB değerlerini öğreniyor ve bunu değerlerle cihazlara istekte bulunan yazılımlar geliştiriyor.
- SNMP protokolü ile bazı özellikler için sadece istekte bulunabilirken (CPU kullanım yüzdesi gibi) bazı özelliklere hem istekte bulunulabiliyor hem de bu özellik değiştirilebiliyor (Hostname bilgisi gibi).
| → Bunun için community string'e (sorgulamalarda kullanılan parola/hesaba) hem okuma hem de yazma yetkilerinin verilmesi gerekiyor (sadece okuma yetkisi de berebilir. Bu durumda MIB değişkenlerine erişebilir ama değiştiremez/cihazlarda konfigürasyonlar yapamaz).
- Switch ve routerlarda gerçekleştirilen işlemler Console portlarından bağlanılarak gerçekleştirilmişse Console ekranına log atacaktır ama SSH veya Telnet gibi uzak bağlanıtı yapıldığı durumlarda Console'a log atmaz. Bu özelliği devreye alabilmek için Enable modunda "terminal monitor" komutu kullanılıyor.

- Cisco'da kontrol amaçla iki tane kontro seri vardır. Biri "Show"komutları diğeri ise "Debug" komutlarıdır. Show komutları o anki durumu/konfigürasyonu (o anki saat bilgisi, çalışan konfigürasyonlar) gösterir. Debug ise gerçek zamanlı değişimler oluştuğunda log atılmasını sağlamaktadır (Örnek olarak ICMP paketigeldiğinde log oluşturulması istenebilir).
| → Debug'da çok yüklü log satırı oluşturacak debug özelliklerini açmamak gerekiyor. Açıldığı takdirde cihazın CPU'su çatlayabilir.
- Cihazlara Console portuyla bağlandıktan sonra komutların yazılı olduğu bir konfigürasyon dosyasını cihaza Tera Term yazılımıyla göndererek dosyada kaydedilen konfigürasyonların cihaz üzerinde satır satır uygulanması sağlanabiliyor.
| → Cihazla Tera Term yazılımıyla bağlandıktan sonra sol köşede "file->send file" tablarına tıklanıyor ve cihaza komut satırında uygulanacak konfigürasyon dosyası seçilerek gönderiliyor.
| → Bu kullanım şelinde cihaz üzerinde yatanımlı bir konfigürasyon varsa karmaşıklıklar çıkabiliyor (running-config'de daha önce tanımlanmış bir satırın üzerine yazmak yarine yeni bir satır eklenebiliyor). Bu nedenle daha uygun bir çözüm olarak bir TFTP sunucusundan konfigürasyon dosyayı çekerek "Sturtup-Config" dosyasıyla değiştirip cihazı yeniden başlatmak olacaktır. Bu sayede konfigürasyon dosyası tamamiyle değişecektir.
- Cihazlara dosyalar doğrudan USB portları kullanarak da yüklenebiliyor/çekilebiliyor (cihazın yanında olmak gerekiyor).

Terminolojiler

- Stratum, hiyerarşik NTP sunucularında bir sunucunun merkez saate (ana kaynağa) olan uzaklığını temsil etmek için kullanılan bir tanımdır. Stratum en yüksek 15 (birim uzakta) olması isteniyor (Stratum 16 kabul edilebilir bir uzaklık değil).



| → Stratum 0 -> ana kaynak

| → Stratum 1 -> kaynağa doğrudan bağlı sunucu

- SNMP Manager (NMS – Network Management System), SNMP sorgusu yapan cihazlar için kullanılan terimdir.
- SNMP Agent, SNMP sorgusuna cevap veren (bilgi alınan) cihazlar için kullanılan terimdir.

Kontrol Komutları

- sh cdp
- sh cdp neighbors
- sh cdp neighbors detail
- sh cdp interface
- sh clock
- sh clock detail
- sh ntp associations
- sh ntp status
- sh file system