Switchlerde Password Recovery ve Switch Ledleri

Switch Hafiza Birimleri

- RAM, hızlı ve geçici bilgilerin tutulduğu hafıza birimidir. Burada ciahaz çalışır durumdayken kullanılan yapılandırma dosyaları, ARP tabloları ve yönlendirme tabloları gibi veriler tutulur.
- NVRAM, routerlarda fiziksel, switchlerde sanal olarak (flash ünitesi içinde config.text isimli bir dosya olarak görünüyor) bulunan küçük bir hafıza birimidir. Cihazdaki konfigürasyonlar burada tutulur ve cihaz açılırken kaydedilen konfigürasyonlar buradan yüklenir.
- FLASH, kalıcı ama yavaş hafıza birimidir. Switch ve routerlarda kullanılan IOS yazılımı/işletim sistemi bu hafıza biriminde depolanır.
- ROM, bootstrap işlemi için kullanılan programların bulunduğu hafıza birimidir. İçeriği değiştirilemez.

Switch Ledleri

Switch Ledleri, cihaz portları ve genel durumu hakkında özet bilgiler alabilmeyi sağlanıyor. Cihaz üzerindeki ledler cihazın geneli hakkında bilgi verirken, portların üzerindeki ledler portların durumu hakkında bilgi verir. Ledlerin tepkileri cihazların modeline göre farklılıklar gösterebiliyor (2960 model bir switch için).

İlk iki led sürekli aktif durumdadır ve cihazın genel durumu hakkında bilgi verir.

- System Led (SYST), cihazın güç alıp almadığını ve düzgün çalışıp çalışmadığını gösterir.
  |-> Yeşil, cihaz güç alıyor ve sorunsuz çalışyor.
  |-> Turuncu, cihazın güç aldığını ama düzgün çalışmadığını, bir problem olduğunu gösterir.
  |-> Kapalı, cihaz güç almıyor.

- Redudant Power Supply Led (RPS), cihazlarda güç kesilmelerine karşı yedek güç sağlayıcıları takılabiliyor. RPS ledi yedek güç sağlayıcısı hakkında bilgi vermektedir.
  |-> Yeşil, yedek güç sağlayıcısı bağlı ve kullanıma hazır.
  |-> Turuncu, yedek güç sağlayıcısı bağlı ama kullanılamıyor.
  |-> Kapalı, yedek güç sağlayıcısı bağlanmamış.

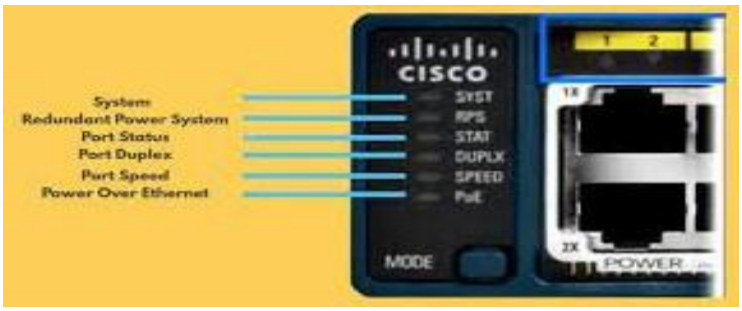
  Bu kısımdan sonraki ledler sürekli aktif durumda değildir. Cihaz üzerinde bulunan “mode” tuşu kullanılarak kontrol ediliyor ve portların üzerinde bulunan ledleri kontrol etmek için kullanılıyor. Her “mode” tuşuna basıldığında yanan led özelliği için port üzerindeki ledlerin durumu kontrol ediliyor.

- Port Status Led (STAT), portun bağlantı durumu hakkunda bilgi verir.
  |-> Yeşil, porta bağlı cihaz vardır.
  |-> Yanıp sönen yeşil, bağlantı olduğunu ve veri akışı olduğunu gösterir.
  |-> Turuncu, porta bağlı cihaz olduğunu ama portun bloklanmış/veri aktarımı engellenmiş olduğunu gösterir.
  |-> Kapalı, porta bağlı cihaz olmadığını gösterir.

- Poty Duplex Led (DUPLX), portun çalışma modunu gösterir.
  |-> Yeşil, portun full-duplex çalıştığını gösterir.
  |-> Kapalı, portun half-duplex çalıştığını gösterir.

- Port Speed Led (SPEED), portun çalıştığı hızı gösterir.
  |-> Yanıp sönen yeşil, 1Gb hızda çalışıyor.
  |-> Yeşil, 100Mb hızda çalışıyor.
  |-> Kapalı, 10Mb hızda çalışıyor.

- Power over Ethernet (PoE), ip telefon veya access point gibi cihazların elektiriği Ethernet kabosu üzerinden verilebiliyor. Bu özellik porta bağlı cihaza Ethernet kablosu üzerinden elektrik verilip verilmediğii gösterir.
  |-> Yeşil, Ethernet kablosu üzerinden elektrik veriliyor.
  |-> Kapalı, Ethernet kablosu üzerinden elektrik verilmiyor.



Cisco 2960X model Switch İçin Switchlerde Password Recovery

Password recovery işlemi marka ve modeller arasında dahi farklılk gösterse de kullanılan yöntem genelde aynı oluyor.

Switchlerde password recovery işlemi için öncelikle cihazın yanında olunmalı ve putty gibi bir emilatör yazılıyla tek erişim seçeneği olan Consol portundan bağlanılması gerekiyor. Cihazın elektriğini kesip "mode" tuşuna basılı şekilde tekrar elektrik verilmesi gerekiyor. Bu tuş switch'in markasına göre değişiyor. Switch açıldığında "Rom-Monitor" adı verilen modda açılıyor.

Rom monitör modunda bilindik Cisco IOS komutları çalışmıyor. Komut satırında “**?**” sembolü ile kullanılabilecek komutlar listelenebiliyor. ilk olarak "**flash_init**" komutuyla flash ünitesinin tanınması sağlanıyor. Daha sonra "**dir flash:**" komutu kullanarak dizinde bulunan konfigürasyon dosyalarını listeleyebiliyoruz. "**rename flash:config.text flash:config.old**" komutuyla cihaza önceden uygulanmış konfigürasyonları bulunduğu ve açılırken buradan yüklenen config dosyasının ismini değiştiriyoruz. Son olarak "**reset**" komutuyla switch yeniden başlatıldığında boş konfigürasyonla açılacaktır. Eğer ki eski konfigürasyon geri yüklenmek isteniyorsa "**copy flash:config.old running-config**" komutuyla konfigürasyonlar yeniden yüklenebilir. Eski konfigürasyonlar running-config üzerine yüklendiğine göre artık istenilen bağlantı tipine istenilen parola bilgisi atanarak (Privileged Exec modda olunduğu için eski parolayı bilmeye gerek kalmadan parola değiştirilebiliyor) eski konfigürasyonlar kullanılmaya devam edilebilir.

|→ Switchlerde uzaktan bağlantı kurabilmek için kullanılacak ip adresleri VLAN arayüzlerine tanımlanıyordu. Bu **tanımlamalarda İpv6 desteği eski model switchlerde gelmeyebiliyor**. Bunu düzeltmek için “**sdm prefer dual-ipv4-and-ipv6 default**” komutu kullanılıyor. Bu komut sonrasında switch “**reload**” komutuyla yeniden başlatılması gerekiyor.

Cisco 4331 Model Router İçin Password Recovery

Cisco 2960 model switchde de yapıldığı gibi öncelikle cihaza Consol portundan bağlanılıyor. Ardından cihaz yeniden başlatılıyor ve işletim sistemi yüklenirken “Ctrl+C” kombinasyonu uygulanarak RomMon moduna giriliyor.

RomMon moduna kullanılabilecek komutları görebilmek için “**?**” sembolü kullanılıyor. ilk olarak “**confreg 0x2142**” komutuyla (https[:]//www.cisco.com/c/en/us/support/docs/routers/10000-series-routers/50421-config-register-use.html - confreg değişkeninin ayarlanabileceği değerler ve açıklamaları) cihaz açılırken konfigürasyon dosyası yüklenmeden açılması (temiz konfigürasyon) sağlanır. Daha sonra “**reset**” komutuyla cihaz yeniden başlatılır.

```
rommon 8 > ?
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 9 > confreg 0x2142
rommon 10 > reset
```

Cihaz açıldıktan sonra Privileged Exec moduna girilerek “**copy startup-config running-config**” komutu kullanılarak startup-config dosyasında kaydedilen konfigürasyonlar running-config’e yeniden yüklenir. Bu noktada Global konfigürasyon moduna girilerek parola bilgileri değiştirilebilir. Son olarak parola değişimi yapıldıktan sonra cihazda “**reload**” komutu kullanılarak yeniden RomMon moduna girilmeli ve Confreg değeri “**confreg 0x2102**” komutu kullanılarak yeniden set edilmeli. Confreg değeri set edilmesze cihaz her yeniden başlatmada konfigürasyon dosyasını yüklemeden açılacaktır.

Cisco SG-300 Model Switch İçin Password Recovery

Eski bir Cisco SG-300 model switchde password recovery işlemi için seri portunda bir dönüştürücü yardımıyla bağlandıktan sonra cihazın gücünü kesilir. Cihaza tekrar güç verdikten sonra Prom/RomMon moduna girmek için cihaz açılırken "ESC" tuşuna basılıyor. Bu adımdan sonra kullanıcıya flash dosyasını silme, parola kurtarma gibi seçenekler sunulmaktadır. Burada parola kurtarma seçeneği için konsola listede belirtilen numara girilir. Son olarak varsayılan parolanın yok sayılmasını onaylamak için onay istenir ve ardından switch parola yok sayılır durumda yeniden başlatılır.

Switchlerde Port Konfigürasyonları

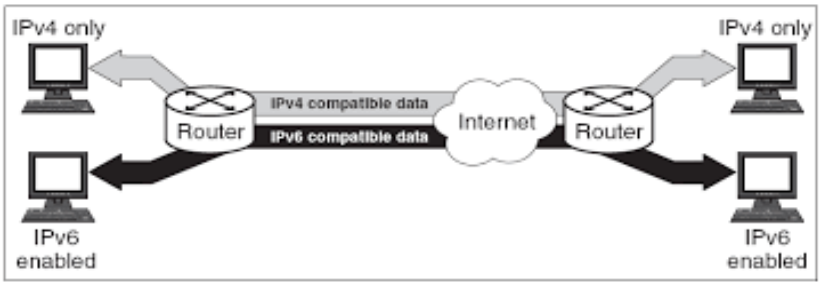
Bu özellikler varsayılanda otomatik modda gelmektedir. Yani karşısına bağlanan cihazın özelliklerine göre kendiliğinde değişiklik gösterebilmektedir. Bu konfigürasyonlar özelleştirilmek istendiğinde ilgili portun arayüzüne girilerek;

- "**speed <Speed Mbit>**" komutuyla portun bant genişliği değiştirilebiliyor.
- "**duplex <Duplex Type>**" komutuyla portun çalışma modu değiştirilebiliyor.
- MDIX özelliği kablo seçiminde çapraz-düz kablo ayırt etmeksizin, porta bağlanan cihazın tipine göre kendiliğinden kabloyu cross veya straigh kullanımına karar veren ve duruma göre kendini revize etmesini sağlayan özelliktir. Bu özellik istendiğinde "**no mdix auto**" komutuyla kapatılabiliyor veya "**mdix <Connect State of Cable>**" komutuyla özelleştirilebiliyor.

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#speed ?
  10     Force 10 Mbps operation
  100    Force 100 Mbps operation
  auto   Enable AUTO speed configuration
Switch(config-if)#duplex ?
  auto   Enable AUTO duplex configuration
  full   Force full duplex operation
  half   Force half-duplex operation
Switch(config-if)#mdix auto ?
  <cr>
Switch(config-if)#
```

Dual Stack Topology

IPv4 ip adreslerinde IPv6 adrelere geçiş sürecinde kullanılan bir teknolojidir. Cihalara IPv4 ip adresleri verildiğinide IPv6 ip adresine sahip cihalara erişemiyorlar. Bu durumda IPv4'ten IPv6 adreslere geçiş sürecinde cihazlara hem IPv4 hem de IPv6 adresler ile erişilebilmesini sağlayan teknolojidir (IPv4 adrese sahip bir istemci IPv6 adrese sahip bir web sayfasına erişebilirken IPv6 adrese sahip bir istemci IPv4 adrese sahip bir web sayfasına erişebiliyor).



Çıktıları Filtrelemek

CLI'da kullanılan komutunların çıktıları çok uzun olabiliyor. Uzun çıktılar arasında istenen kısımları filtreleyebilmek mümkün. Bunu CLI'da kullanılan komutların ardına pipe (|) sembolü ve filtrelerden biriyle beraber aranacak anahtar kelimeler girilir. Kullanılan filtreler;

- **seciton**, anahtar kelimenin geçtiği satırları ve altında bu satırla ilgili bölümleri filtreliyor.
- **include**, anahtar kelimenin bulunduğu satırları listeliyor.
- **exclude**, anahtar kelimeyi içermeyen satırları listeliyor.
- **begin**, anahtar kelimenin bulunduğu satırdan itibaren çıktının kalan kısmını listeliyor.

Çıktıların uzunluklarını belirlemek için Terminal Length özelliği değiştirilebiliyor. Bu konfigürasyon Privileged Exec modunda "**terminal length <Length Number>**" komutuyla gerçekleştirilir (Her space tuşuna basıldığında kaç satır gösterilmesi isteniyorsa o değer komutun sonunda belirtilir). Bu değer varsayılanda 24 satırdır. Çıktının duraksamadan/tamamının listelenmesi için 0 değeri verilir.

Terminolojiler

- POST (Power on Self Test), cihazın açlırken kendini test etme sürecidir. Cihazın ihtiyaç duyduğu yazılım ve donanımlar kontrol edilerek, cihazın çalıştırılabilir durumda oluıp olmadığı belirlenir. Burada CPU'yu, kurulu DRAM ve flash miktarını ve tüm arayüzleri kontrol eder. Bu yazılım ROM hafıza biriminde tutulur.
- Boot Loader Software (Bootstrap), IOS işletim sistemini RAM hafızaya yükleyerek başlatılmasını sağlayan yazılıma deniliyor. ROM hafızada bulunuyor.
- ROMMonitor, işletim sistemiyle ilgili sorunlar yaşandığında kullanılan yazılım parçasıdır. ROM hafizada bulunur. Örnek olarak işletim sistemi silindiğinde veya password recovery gibi işlemlerde bu moda girilerek düzenlemeler yapılır.

Kontrol Komutları

- show flash, flash ünitesinde bulunan dosyaları listeler.
- show startup-config, yedeklenen/kaydedilen konfigürasyonları listeler.
- show version, cihaz ve üzerinde çalışan işletim sistemi hakkında detaylı bilgiler verir.
- show mac address-table, cihazdaki mac adres tablosundaki kayıtları listeler.
- show ssh, ssh ile hangi crypto tekniklerini desteklediğini gösteriyor.
- show ip ssh, SSH bağlantılarında giriş için deneme sayısı ve zaman aşım bilgileri listeleniyor.
- show history, CLI'da çalıştırılan son 10 komutun kaydını listelemek için kullanılıyor. Kayıt miktarı Privileged Exec modunda "**terminal history size <Size>**" komutuyla değiştirilebiliyor.
- show int <Interface ID>, arayüzün L1 ve L2 bilgilerini gösteriri. Burada önemli kısımlardan biri de port üzerinden geçen trafiğin istatistiğidir.
    - Input Errors, bir arayüze giriş yönünde alınan hataların toplamıdır. Yani Runts, Gaints, CRC gibi hataların toplamıdır.
    - Runts, bir Ethernet frame 64 bayttan küçük olamaz. Porta 64 bayttan küçük/bozuk frame geliyorsa bu kablolamada sorunlar olduğunu gösterir (64 bayttan küçük frame gelmesi durumudur).
    - Giants, bir Ethernet frame aynı zamanda farklı bir özellik devreye alınmadığı sürece (Burada Jumbo Frame özelliği devreye alınarak 1500 bayttan büyük framelere izin verilebiliyor) 1500 bayttan büyük olamaz (L2'de de 18 bayt başlık bilgisi ekleniyordu). 1500 bayttan büyük boyutlu frame gelmesi durumudur.
    - CRC, L2'de başlık bilgisine hata kontrol /Frame Check Sequence bitleri ekleniyordu. CRC, bozuk frameleri kontrol etmek için kullanılan algoritmaya verilen isimdir (algoritmanın çalışma mekanizması https[:]//ww1.microchip.com/downloads/en/AppNotes/00730a.pdf). Bu bozulmaya örnek olarak iletimde bakır kablo kullanılıyorsa ve bakır kablo yol boyunca herhangi bir elektromanyetik alandan etkileniyorsa/bitler değişiyorsa bozuk framelerle karşılaşılabilir.

- Collusion, half-duplex çalışan ortamlarda birden fazla cihazın networke aynı anda veri göndermesiyle gerçekleşen durumdur. Farklı iletim yöntemlerini (half/full duplex) kullanan cihazlar arasında görür.
- Late Collusion, collusion oluşacağı ilk 512 bitte fark edilmemişse oluşuyor. İlk 512 bitte fark edilmediğinde, iletim sonlanana kadar trafik durdurulamıyor.