

Switchlerde Password Recovery ve Switch Ledleri

Switch Hafıza Birimleri

- RAM, hızlı ve geçici bilgilerin tutulduğu hafıza birimidir. Burada cihaz 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.) bulunun 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.

Terminolojiler

- POST (Power on Self Test), cihazın açılırken kendini test etme sürecidir. Cihazın ihtiyaç duyduğu yazılım ve donanımlar kontrol edilerek, cihazın çalıştırılabilir durumda olup 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 hafızada bulunur. Örnek olarak işletim sistemi silindiğinde veya password recovery gibi işlemlerde bu moda girilerek düzenlemeler yapılır.

Switch Ledleri

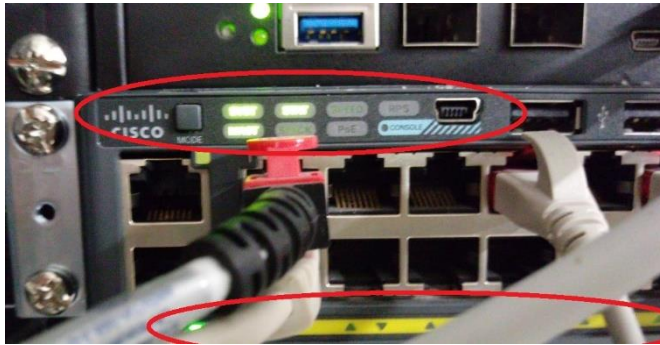
Switch Ledleri, cihaz ve portları hakkında özet bilgiler alınmasını sağlıyor. Cihaz üzerindeki ledler cihazın geneli hakkında bilgi verirken, portların üzerindeki ledler portların durumu hakkında bilgi vermektedir. Ledlerin tepkileri cihazların modeline göre farklılıklar gösterebiliyor (2960 model bir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

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

- System Led (SYST), cihazın güç alıp almadığını ve düzgün çalışıp çalışmadığını gösterir.
 - | -> Yeşil, cihaz güç alıyor ve sorunsuz çalışıyor.
 - | -> Turuncu, cihaz güç alıyor ama düzgün bir problem var.
 - | -> Kapalı, cihaz güç almıyor.
- Redundant 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 yana led özelliği için port üzerindeki ledlerin durumu kontrol ediliyor.

- Port Status Led (STAT), portun bağlantı durumu hakkında bilgi verir.
 - |-> Yeşil, porta bağlı cihaz vardır.
 - |-> Yanıp sönen yeşil, bağlantı olduğunu ve veri akışı olduğunu gösterir.
 - |-> Turuncu, porta bağlı cihaz var ama portun bloklanmış/veri aktarımı engellenmiş.
 - |-> Kapalı, porta bağlı cihaz yok.
- Port 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 elektriği Ethernet kabosu üzerinden verilebiliyor. Bu özellik porta bağlı cihaza Ethernet kablosu üzerinden elektrik verilip verilmediği gösterir.
 - |-> Yeşil, Ethernet kablosu üzerinden elektrik veriliyor.
 - |-> Kapalı, Ethernet kablosu üzerinden elektrik verilmiyor.



Switchlerde Password Recovery (2960 model bir switch için)

Password recovery işlemi yeni model switchlerde genelde benzer oluyor.

Switchlerde password recovery işlemi için öncelikle cihazın yanında olunmalı ve putty gibi bir emilatör yazılıyla tek erişim seçeneği olan consol portundan bağlanılıyor. 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 geçiliyor.

Rom monitör modunda bilindik Cisco IOS komutları çalışmıyor ama "?" sembolü kullanılarak kullanılabilecek komutlar listelenebiliyor. İlk olarak "flash_init" komutuyla flash ünitesini tanımasını sağlıyor. Daha sonra "dir flash:" komutu kullanarak dizinde bulunan konfigürasyon dosyalarını listelebiliyoruz. "rename flash:config.text flash:config.old" komutuyla cihazdaki tanımlı konfigürasyonları tanımlı olduğu ve açılırken buradan yüklenen config dosyasının ismini değiştiriyoruz. Son olarak "reset" komutuyla switch yeniden başlatıldığında boş konfigürasyonla açılacaktır. Eğer ki eski konfigürasyon geri yüklenmek istendiğinde "copy flash:config.old running-config" komutuyla konfigürasyonlar yeniden yüklenebiliyor.

NOT

- Switchlere uzaktan yönetebilmek için L2 switchlerin vlan arayüzlerine ip adresleri tanımlanıyordu. Bu tanımlamalarda ipv6 desteği eski model switchlerde gelmeyebiliyor. Bunu düzeltmek için "sdm prefer dual-ipv4-and-ipv6 default" komutu kullanıldıktan sonra switch "reload" komutuyla yeniden başlatılıyor.

Eski bir Cisco SG-300 model switchde password recovery işlemi için seri portunda bir dönüştürücü yardımcıyla bağlandıktan sonra cihazın gücünü kesilir. Cihaza tekrar güç verdikten sonra prom 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

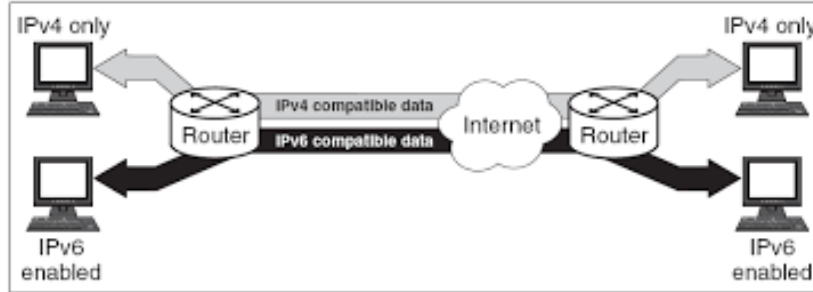
Bu özellikler varsayılanda otomatik gelmektedir. Yani karşısına bağlanan cihaz özelliklerine göre kendiliğinde değişiklik gösterebilmektedir.

- Speed, konfigüre edilmek istenen portun arayüzüne giriş yapılarak "speed" komutuyla portların hızları sınırlandırılabilir.
- Duplex, konfigüre edilmek istenen portun arayüzüne giriş yapılarak "duplex" komutuyla half-duplex veya full-duplex seçimi yapılabilir.
- MDIX, kablo seçiminde çapraz-düz kablo ayırt etmeksizin, porta bağlanan cihazın tipine göre kendiliğinden kabloyu cross veya straight kullanımına karar veren ve duruma göre kendini revize etmesini sağlayan özelliktir. Bu özellik istendiğinde "no mdix auto" komutuyla kapatılabilir.

```
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 geçişte kullanılan bir teknolojidir. Cihazlara IPv4 ip adresleri verildiğinde IPv6 ip adresine sahip cihazlara erişemiyorlar. Bu nedenle IPv4'ten IPv6 adreslere geçiş sürecinde cihazlara hem IPv4 hem de IPv6 adresler atanmasına deniliyor.



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 giriliyor. Kullanılan filtreler;

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

Çıktıların uzunluklarını belirlemek için terminal length özelliği değiştirilebiliyor. Bu konfigürasyon Privileged Exec modunda "terminal length" komutuyla gerçekleştirilir. Her space tuşuna basıldığında kaç satır gösterilmesi isteniyorsa o değerkomutun sonunda belirtilir. Bu değer varsayılanla 24 satırdır. Çıktının duraksamadan/tamamının listelenmesi için 0 değeri verilir.

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 int ArayüzBilgisi, arayüzün L1 ve L2 bilgilerini gösterir. Burada önemli kısımlardan biri de port üzerinden geçen trafiğin istatistiğidir.
 - |-> Input Errors, bir arayüze giriş yönünde alınan hataların toplamıdır. Yani Runts, Giants, CRC gibi hataların toplamıdır.
 - |-> Runts, bir ethernet frame 64 bayttan küçük olamaz. Porta 64 bayttan küçük/bozuk frame geliyorsa bu durum kablolamada sorunlar olduğunu gösterir.
 - |-> Giants, bir ethernet frame aynı zamanda farklı bir özellik devreye alınmadığı sürece 1500 bayttan büyük olamaz (L2'de de 18 bayt başlık bilgisi ekleniyordu). Burada Jumbo Frame özelliği devreye alınarak 1500 bayttan büyük framelere izin verilebiliyor.
 - |-> CRC, L2'de başlık bilgisine hata kontrol /Frame Check Sequence bitleri ekleniyordu. CRC, bozuk framerleri kontrol etmek için kullanılan algoritmaya verilen isim (algoritmanın çalışma şekli için

<https://ww1.microchip.com/downloads/en/AppNotes/00730a.pdf>). Örnek olarak iletimde bakır kablo kullanılıyorsa ve bakır kablo yol boyunca herhangi bir elektromanyetik bir alandan etkileniyorsa/bitler değişiyorsa bu gibi bozuk framelerle karşılaşılabilir.

|-> Output Errors, bir arayüzün çıkış yönünde alınan hataların toplamıdır.

|-> No Buffer,

|-> Overrun,

|-> Ignores,

|-> Collusion, half-duplex çalışan ortamlarda birden fazla cihazın aynı anda trafik oluşturmasıyla oluşan hatalardır. Farklı iletim yöntemlerini (half/full duplex) kullanan cihazlar arasında görülür.

|-> Late Collusion, collusion oluşacağı ilk 512 bitte fark edilmemişse oluşuyor. İlk 512 bitte fark edilmediğinde, iletim sonlanana kadar trafik durdurulamıyor.

- show ssh, ssh ile hangi crypto tekniklerini desteklediğini gösteriyor.
- show ip ssh, SSH bağlantılarında giriş için deneme sayısı ve zaman aşımı bilgileri listeleniyor.
- show history, CLI'da çalıştırılan son 10 komutun kaydını listelemke için kullanılıyor. Kayıt miktarı Privileged Exec modunda "terminal history size" komutuyla değiştirilebiliyor.