Packet Forwarding

(Bu not daha çok CCNA eğitiminin genel bir tekrarı niteliğindedir. Detaylı bilgiler için CCNA notlarına bakabilirsin. Belki son kısımlarda yeni bilgiler bulabilirsin).

Networkün ana görevi paketlerin bir noktadan farklı bir noktaya (bozulmadan) iletilmesini (Packet Forwarding) sağlamaktır. CCNA eğitiminde de bahsedildiği gibi bu işlem için OSI veya TCP/IP gibi katmanlı mimariler kullanılıyor.

Networklerde Hub kullanıldığı zamanlarda;

- Hub cihazı kendisine gönderilen paketleri bütün portlarına anahtarlıyordu (karar verme mekanizması olmadığı için).
- Half-duplex çalıştığı için sahip olunan bant genişliği tam anlamıyla kullanılamıyordu.
- Aynı anda birden fazla istemci trafik oluşturduğunda Collusion oluşabiliyordu (Bu çakışmaları önlemek için CSMA/CA ve CSMA/CD gibi algoritmalar kullanılıyordu). Collusion oluştuğunda paketlerin yeniden gönderilmesi gerekiyor. Bu durum networkün performansını olumsuz yönde etkiliyordu.

Switch kullanılarak Hub ile karşılaşılan problemlere büyük ölçüde çözüm getirilmiştir.

- Switch kendisine bağlanan istemcilerin MAC adreslerini CAM (MAC Address Table) adı verilen bir tabloya kaydediyor. Switche iletilmek üzere bir paket gönderildiğinde swtich paketi öncelikle bir Buffer'a kaydediyor. Ardından paketin hedef MAC adresi ile oluşturduğu CAM tablosundaki adresleri göz önünde bulunduruyor ve paketi hedef MAC adresinin bulunduğu porta anahtarlıyor.
    - Paketteki hedef MAC adresi CAM tablosunda kayıtlı olmadığı durumlarda, paket geldiği port dışındaki bütün portlara anahtarlanıyor (Bu anahtarlama işlemi broadcast yayın değil. Buna "**Unicast Flooding**" deniyor).
- Bu süre içerisinde aynı anda birden fazla istemci trafik oluştursa dahi switche gelen bütün paketler Buffer'da tutuluyor. Bu sayede hattın kullanımda olup olmadığına bakılmaksızın her an gönderilen paketler (Buffer'a kaydedildiği için) Collusion oluşmadan hedef adreslerine anahtarlanabiliyor.
- Switch portları varsayılanda Full-Duplex çalıştığı için sahip olunan bant genişlikleri daha verimli kullanılabiliyor.

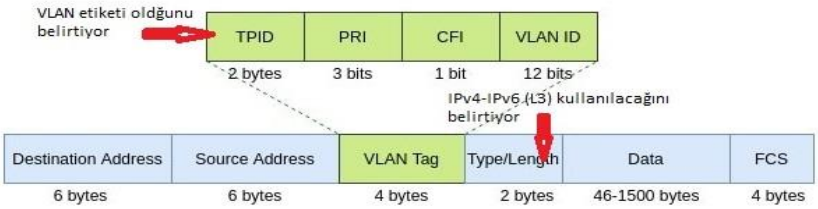
Switch kullanılarak Collusion gibi çeşitli problemlere çözüm getirilmiş olunsa da ARP ve DHCP gibi protokollerin kullandığı ve beraberinde problemlere neden olan broadcast yayınlara çözüm getirememektedir. Broadcast yayının neden olduğu iki büyük probleme bakıldığında;

- İstemci sayısı yüksek networklerde aynı anda birden fazla istemcinin yapacağı broadcast yayın, networkün genelinde bant genişliğinin verimsiz kullanılmasına neden olacaktır (Broadcast paketleri networke bağlı bütün istemcilere gönderildiği için paketle ilişkisi olmayan istemcilerin de bant genişlikleri gereksiz yere meşgul edilmiş oluyor).
    - Bu durum güvenlik problemine de neden olmaktadır. Örnek olarak broadcast paketleri kullanılarak networkün bant genişliği doldurulabilir.

- Broadcast yayınlardan dönen yanıtlarda kimlik doğrulama mekanizması (paketin legal kaynaktan gelip gelmediği anlaşılmadığı için) olmadığı için çeşitli güvenlik açıklarına neden olabiliyor.

Broadcast trafiğini sınırlandırabilmek için normalde router gibi L3 cihazlar kullanılıyor. LAN içerisinde ise broadcast yayınlarının kapsamını küçültmek (networkleri birbirinden izole etmek/aynı işi yapan cihazları gruplandırmak) için VLAN teknolojisi kullanılıyor. VLAN özetle, her network için fiziksel bir switch kullanmak yerine bir switch portlarını farklı sanal networklere atayarak gruplandırabilmeyi/izole etmeyi sağlayan teknolojidir (VLAN konusunda daha detaylı bilgi için CCNA notlarını inceleyebilirsin).

Aşağıdaki görselde de belirtildiği gibi paket içerisinde kullanılan başlık bilgisine **EtherType** alanındaki değere bakılarak karar veriyor (https[:}//en.wikipedia.org/wiki/EtherType → 0x8100 = VLAN, 0x0800 = IPv4 gibi).



Trunk moduna alınan portlardan gönderilecek paketlere VLAN başlık bilgisi eklenir. Native VLAN, Trunk moduna alınan portlarda paketlere VLAN başlık bilgisi eklenmeden iletilmesini sağlayan özelliktir. Native VLAN sadece bir VLAN için kullanılabiliyor. Dikkat edilmesi gereken nokta Native VLAN bilgisi karşılıklı bağlı her iki switch üzerinde de aynı VLAN olarak seçilmesi gerekiyor (Native VLAN portlara özeldir ve karşılıklı bağlanmış portlarda aynı olması gerekir). Aksi taktirde VLAN'lar birbirine girecektir.

Cisco cihazlarda Trunk modna alınan portlarda varsayılanda bütün VLAN trafiğine izin veriliyordu (farklı marka switchlerde Trunk moduna alındıktan sonra trafiğine izin verilmesi istenen VLAN'ların ayrıca tanımlanması gerekiyor). Cisco switchler üzerinde de belirli Trunk portlardan VLAN'lara ait trafiklerin geçirilmesi isteniyorsa bu VLAN'ların ilgili portun arayüzü altında "**allowed vlan**" komutuyla belirtilmesi gerekiyor (daha sonra ekleme yapılmak istendiğinde "**allowed vlan add**" komutuyla ekleme yapılıyor. Ekleme yapılmak istendiğine sadece "**allowed vlan**" komutu kullanılırsa daha önce tanımlanan VLAN'lar geçersiz sayılacaktır).

Bir paket hedef adrese gönderilmek üzere kaynak istemciden çıkıp bir switche gönderildiğinde paketin hedef ip adresinin aynı networke ait bir istemciye ait olup olmadığı kontrol edilir. Hedef ip adresi aynı networke dâhil bir istemciye ait ise ARP sorgusu yapılarak hedef adresin MAC adresi öğrenilir ve paket hedef istemciye anahtarlanır. Eğer ki paketteki hedef ip adresi farklı bir networke ait ise bu durumda networkteki gateway ip adresine ait MAC adresini öğrenebilmek için ARP sorgusu yapılır ve paket routera gönderilir. Paket routera geldiğinde statik veya dinamik olarak öğrenilen rotalarla oluşturulan yönlendirme tablosu göz önünde bulundurularak gönderilmesi gereken bir sonraki router tespit edilir. Yönlendirilecek router tespit edildikten sonra paketin gönderileceği routerun MAC adresi öğrenilir ve bu doğrultuda paketin L2 bilgileri yeniden düzenlenerek paket hedef routera gönderilir (hedef ip adresinin hiçbir zaman değişmediğini unutma. Sadece kaynak ip adresi NAT yapılıyorsa networkün internete çıkış yaptığı routerda veya firewall'da Private ip adresi Public ip adresiyle değişebilir). Bu sayede L2 bilgileri her Hop için yeniden düzenlenerek paketin routerlar arasında iletiminin gerçekleştirilmesi ve hedef istemciye iletilmesi sağlanır.

Forwarding Architectures

Cihazlarda (router, switch) bulunan CPU'ların aslında cihazların hassas noktası olduğundan daha önce de bahsedilmişti. Bu nedenle cihazlarda CPU'ları olabildiğince az kullanılmaya çalışılır. Buna rağmen bazı durumlarda cihazların CPU'su kullanılmak zorunda kalınabiliyor. Bu tür durumlara örnek vermek gerekirse;

- **PBR** (**Policy-Based Routing**) kullanılan routerlarda routerun CPU'su kullanılarak paketler yönlendiriliyor.
- Paketler yönlendirilirken veya anahtarlanırken bir sonraki (Next Hop) cihazın MAC adresini öğrenebilmek için yapılan ARP sorgusu routerların CPU'su kullanılarak gerçekleştiriliyor.
- SSH gibi uzak bağlantılar kurulduğunda yine cihazların CPU'su kullanılıyor.

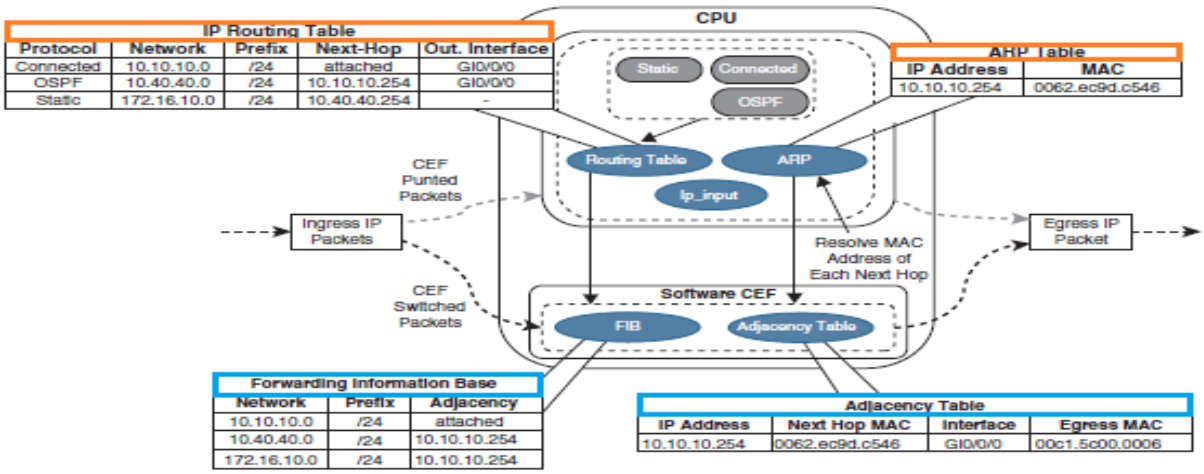
CEF (Cisco Express Forwarding)

CEF, ağ performansını arttırmak için Cisco tarafından üretilmiş (farklı markaların benzer çözümleri bulunmaktadır) bir paket anahtarmala mekanizmasıdır.

Hardware CEF, paket anahtarlama işlemini hızlandırabilmek için cihazlara fazladan ASIC, CAM veya TCAM adı verilen ve paket anahtarlama işlemine özel üretilmiş donanımlar kullanılarak gerçekleştirilmesidir.

- TCAM (Temary Content Addressable Memory), L3 cihazlarda donanımsal anahtarlama yapabilmek için kullanılan RAM donanımı olarak tanımlanabilir.
    - Sorgu yapıldığı anda (gelen paketlerin iletimi için kullanılan karar mekanizmasında) 3 farklı cevap dönebilyor (True, False, Ignore).
- CAM (Content Addressable Memory), L2 cihazlarda donanımsal anahtarlama yapabilmek için özel oluşturulan RAM donanımı olarak tanımlanabilir.
    - Sorgu yapıldığı anda iki farklı cevap dönebiliyor (True, False).

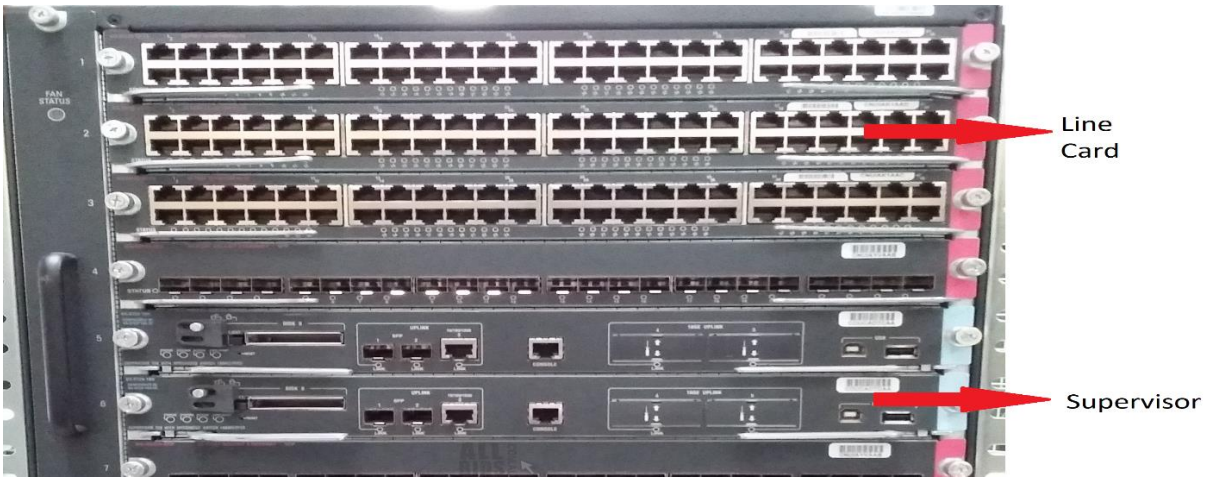
Software CEF, routerlarda gelen paketler hedef adreslerine yönlendirme tablosu ve MAC Address tablosuna ayrı ayrı (iki kez Lookup yapılıyordu. 1-> Hedef ip adresi için rota belirleme. 2-> Next Hop routerun MAC adresini öğrenmek için) bakarak karar veriyordu. Bu süreçte tablolar büyüdükçe Lookup işlemi de zaman kaybettirmektedir. Zaman kaybını düşürmek ve karar verme mekanizmasını hızlandırmak adına yönlendirme tablosu yerine **Forwarding Information Base**, MAC Address tablosu yerine **Adjacency table** adında iki farlı özelleştirilmiş tablo oluşturulmuş. Bu tablolar kullanılara paket anahtarlama işleminin yazılım temelinde/bazında hızlandırılmasına Software CEF denilmektedir.



|→ Software CEF ile kullanılan Adjecency tablosunda bir MAC adresinin kaydı bulunmadığı durumlarda (Buna "**Glean State**" deniliyor) ARP sorgusu yapılarak MAC adresinin öğrenilebilmesi için yine cihazın CPU devreye giriyor. ARP sorgusuyla öğrenilen MAC adres bilgileri Adjacency tablosuna ekleniyor.

Modular switchlerde paket anahtarlama işlemi için **DFC** (**Distributed Forwarding Card**) ve **CFC** (**Centralized Forwarding Card**) olmak üzere iki farklı şekilde gerçekleştirilebiliyor.

- **DFC**, modüler switche eklenen Line kartların üzerinde bulunan donanımsal işlemci ve donanımsal RAM birimleri kullanılarak (yönlendirme tabloları switch üzerinde bulunan her Line kartına dağıtılıyor. Bu sayede paketlerin Route Process'a gelmesine gerek kalmadan paketler doğrudan anahtarlanıyor) portlara gelen paketler Route Processor'a ihtiyaç duymadan anahtarlanmasını sağlayan kullanım şeklidir.
- **CFC**, paketlerin Route Process' a gelip anahtarlanacağı hedef porta yönlendirilmesiyle gerçekleştirilen kullanım şeklidir.



https[:]//community.cisco.com/t5/routing/what-is-the-difference-between-dfc-and-cfc/td-p/2818823

SSO (Stateful Switchover), modüler bir swtich üzerinde aktif kullanılan Supervisor üzerinde bir problem oluştuğunda yedek Supervisor'a en az gecikmeyle geçilmesini sağlayan ve yönlendirme işleminin aksamadan gerçekleştirilmeye devam etmesini sağlayan teknolojidir (https[:]//study-ccnp.com/understanding-sso-cisco-stateful-switchover/).

- Bu süreçte kullanımda olan Supervisor üzerinde oluşturulan **Forwarding Information Base** ve **Adjacency** tabloları sürekli/gerçek zamanlı olarak yedek Supervisor'a yedekleniyor. Bu sayede kullanımda olan Supervisor üzerinde bir problem oluştuğunda yedek Supervisor doğrudan çalışmaya devam edebiliyor.

SDM Templates (**Switching Database Manager**), normalde anahtarlama işleminin yanında ACL kontrolü, QoS konfigürasyonu gibi daha birçok işlemin donanımsal RAM (TCAM) tarafından gerçekleştirilmesi sağlanabiliyor (TCAM kapasitesi yettiğince – Switch modeline bağlı olarak TCAM'a yaptırılabilecek özellikler de, TCAM kapasitesi de değişiklik gösteriyor). Bu işlemler "**sdm prefer {vlan |advanced}**" komutu kullanılarak gerçekleştiriliyor. Komut sonrasında cihaz "**reload**" komutuyla yeniden başlatılması gerekiyor.

```
SWX(config)#sdm prefer ?
  default              Default bias
  dual-ipv4-and-ipv6   Support both IPv4 and IPv6
  lanbase-routing      Lanbase routing
  qos                  Qos bias
SWX(config)#
```

|→ Burada Cisco 2960 gibi eski model bir L2 switch dahi basit seviyede yönlendirme işlemi yapabildiği görülüyor ("**sdm prefer lanbase-routing**" komutu).

|→ Switch üzerinde TCAM'a uygulatılmak istenen her özellik için ne kadar alan ayırdığı "**sh sdm prefer**" komutu kullanılarak görülebilir (Bütün alan gerçekleştirilecek işlemler arasında paylaştırılıyor). Donanımsa RAM (TCAM)'a yaptırılmak üzere yeni bir özellik eklendiğinde/devreye alındığında her özelliğe ayrılan alan miktarı yeniden düzenleniyor ve bütün alan özellikler arasında yeniden paylaştırılıyor.

```
SWX#sh sdm prefer
 The current template is "default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 0 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  8K
  number of IPv4 IGMP groups + multicast routes:    0.25K
  number of IPv4 unicast routes:                    0
  number of IPv6 multicast groups:                  0
  number of directly-connected IPv6 addresses:      0
  number of indirect IPv6 unicast routes:           0
  number of IPv4 policy based routing aces:         0
  number of IPv4/MAC qos aces:                      0.125k
  number of IPv4/MAC security aces:                 0.375k
  number of IPv6 policy based routing aces:         0
  number of IPv6 qos aces:                          20
  number of IPv6 security aces:                     25
```

|→ Burada görüldüğü gibi MAC Address tablosu için toplamda 8KB alan ayrılmış. Cihazda ACL veya QoS gibi farklı özelliklikler de devreye alındığında (TCAM'A yaptırılmak istendiğinde) MAC Address tablosu için ayrılan alan daha da azalacaktır. MAC adresleri için ayrılan alan dolduğunda ise yeni MAC adresleri öğrenilemeyeceği için switch hub gibi çalışacak ve kendisne gelen paketleri bütün portlarına anahtarlayacaktır (Bu durumun ne kadar ciddi sorunlara neden olduğu CCNA notlarında açıklanmıştı). Bu nedenle switchlerde "**sdm prefer**" komutu dikkatli bir şekilde kullanılmalıdır.

NOT

- Switchler üzerinde Port Security konfigürasyonu yapmadan portlara statik MAC adres tanımlaması yapılarak da farklı MAC adresine sahip cihazların bu porta bağlanıp trafik oluşturmasının önüne geçilebiliyor. Statik MAC adres konfigürasyonu için Global konfigürasyon moduna gitilerek "**mac address-table static <MAC-Address> vlan <vlan-id> interface <Interface-ID>**" komutu kullanılıyor.

```
SWX(config)#mac address-table static 0010.2020.3030 vlan 1 interface fastEthernet 0/1
```

  - MAC Address tablosundaki belirli kayıtlar veya öğrenilmiş tüm MAC adresleri temizlemek için "**clear mac address-table dynamic (address <MAC address> | interface <Interface ID> | vlan <VLALN ID>)**" komutu kullanılıyor.

- Switchlerde "**mac address-table static <MAC-Address> vlan <vlan-id> drop**" komutu kullanılarak komutta belirtilen MAC adresine sahip paketlerin switch üzerinden geçmesi engellenebiliyor.

```
SWX(config)#mac address-table static 0010.2020.3030 vlan 1 drop
```

- "**sh mac address-table**" komutuyla kullanıcı takibi yapılabiliyor, yeni bir cihaz bağlanması gerektiğinde öncesinde bir bilgisayar bağlatılarak bilgisayarın MAC adresi MAC Adres tablosunda aratılarak konfigüre edilecek port bilgisi öğrenilebiliyor. Bu ve bu gibi daha birçok işlemde kullanılıyor.
    - Switch bağlı portlar üzerinden birden fazla MAC adresi öğrenilebiliyordu (farklı switchler üzerinde bağlı iki istemci haberleşmek istediğinde). Port Security konfigürasyonu yapılırken portlarda öğrenilebilecek MAC adersi sayıları belirlenirken dikkat edilmesi gereken konulardan biridir.
- "**sh int status**" komutuyla switch üzerindeki portların Port ID, Name, Durum, VLAN bilgisi, duplex ve hız bilgisinin yanında bağlantıda kullanılan kablo tipi dahi görüntülenebiliyor. Bu nedenle networkte Throubleshooting yaparken kullanılması gereken komutlardandır.

```
SW1#show interfaces status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        notconnect   1            auto   auto 10/100BaseTX
Fa0/2                        notconnect   1            auto   auto 10/100BaseTX
Fa0/3                        notconnect   1            auto   auto 10/100BaseTX
Fa0/4                        connected    1          a-full  a-100 10/100BaseTX
Fa0/5                        connected    1          a-full  a-100 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        notconnect   1            auto   auto 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
```

- Routerun bir aratüzüne birden fazla ip adresi ataması yapılabiliyor. Bu atama routerun arayüzüne girilip "**ip address <Ip Address> <Subnet Mask>**" komutuyla ilk ip adresi tanımlandıktan sonra "**ip address <Ip Address> <Subnet Mask> secondary**" komutuyla ikinci bir ip adresi de tanımlanabiliyor.
    - Bu kullanım arayüze bağlı networkte cihaz sayısı arttığı durumlarda kullanılabilyor (Örnek olarak C sınıfı bir ip adresi kullanılıyorken cihaz sayısı 500'e çıkmış olabilir. Bu durumda ip sayısı yetersiz kalacaktır. Bu durumda router arayüzüne ikinci bir ip adresi tanımlanarak sorun giderilebilir).
    - Benzer şelilde IPv6 adresi atanırken de birden fazla ip adresi tanımlanabiliyor. Sadece ilk tanımlamadan sonra "**secondary**" anahtar kelimesinin kullanılması gerekmiyor.
- Farklı bir çözüm olarak da bir L3 switche bir network tanımlandığı zaman switch, belirli zaman aralıklarında tanımlanan ip aralığındaki bütün ip adresleri için ARP sorgusu yapıyor ki Adjacency tablosunda bilinmeyen MAC adresi kalmasın ve Glean State durumuna düşülmesin.

Terminolojiler

- **SPAN**, switch üzerinde bulunan bir porttan geçen trafiğin kopyasının aynı switch üzerindeki farklı bir porta gönderilmesini sağlayan özelliktir. Bu sayede portlardan geçen trafik dinlenebilmektedir.
- **RSPAN** (Remote SPAN), switch üzerinde bulunan bir porttan geçen trafiğin bir kopyasının farklı bir switch portuna gönderilmesini sağlayan özelliktir.
- **Policy-Based Routing**, normalde routerlarda yönlendirme işlemi paketlerin sadece hedef ip adresi göz önünde bulundurularak Data Plane (ASIC + TCAM) üzerinden gerçekleştiriliyor. Policy-Based Routing ise routerlarda belirli politikalar belirtilerek bu politikalar doğrultusunda yönlendirme işleminin yapılmasıdır. Bu yöntem kullanılarak gerçekleştirilen yönlendirme işleminde paketler Control Plane (CPU + RAM) kullanılarak yönlendiriliyor.
- **Supervisor**, Cisco model modüler switchlerin beyni olarak tanımlanabilir. Switchler/Line kartları bu donanım ile kontrol edilirler.

Kontrol Komutları

- sh mac address-table
- sh mac address-table address <MAC Address>
- sh mac address-table {dynamic | static}
- sh mac address-table vlan <VLAN ID>
- sh int <Interface ID> switchport
- sh ip int brief
- sh sdm prefer
- sh int status