Packet Forwarding

(Bu not daha çok CCNA eğitiminin genel bir tekrarını içermektedir. Belki NOT kısmında 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 kullnılıyordu). 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 istecilerin MAC adresielrini CAM (MAC Address Table) adı verilen bir tabloya kaydediyor. Switche iletilmek üzere bir paket gönderildiğinde swtich paketi öncelikle Buffer'a kaydediyor. Ardından paketin hedef MAC adresi ile oluşturduğu CAM tablosundaki adresleri göz önünde bulunduruyor ve paketi hedef MAC adresinin bulunduğu porta anahtarlıyor.
    - Paketin hedef MAC adresi CAM tablosunda kayıtlı olmadığı durumlarda paketi geldiği port dışındaki bütün portlara anahtarlıyordu (Bu Broadcast yayın değil. Buna "Unicast Flooding" deniyor).
- Bu süre içerisinde aynı anda birden fazla istemci trafik oluşturduğunda switche gelen bütün paketler Buffer'da tutuluyor. Bu sayede hattın kullanılıp kullanılmadığına bakılmaksızın her an gönderile paketler Buffer'a kaydediliyor ve Collusion oluşmadan paketler hedef adreslerine anahtarlanabiliyor.
- Switch portları (varsayılanda) full-duplex çalıştığı için sahip olunan bant genişlikleri daha verimli kullanılabiliyor.

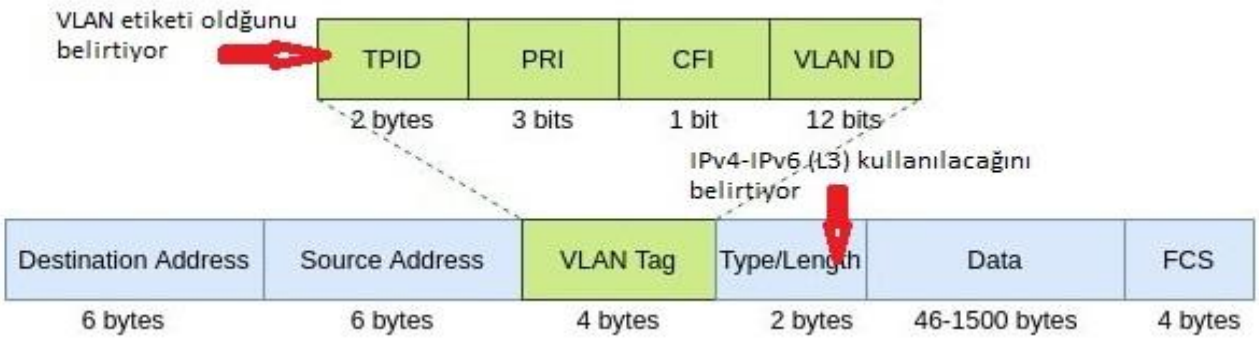
Switch kullanılarak Collusion gibi çeşitli problemlere çözüm getirmiş olsa da ARP ve DHCP gibi protokollerin kullandığı Broadcast yayınların getirdiği sorunlara çözüm getirememektedir. Broadcasy yayının neden olduğu iki büyük problem;

- İstemci sayısı yüksek networklerde aynı anda birden fazla istemcinin yapacağı Broadcast yayını networkün ve networkteki istemcilerin bant genişliğinin verimsiz kullanılmasına neden oluyor (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. 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 olabilmektedir.

Broadcast trafiğini sınırlandırabilmek için normalde router gibi L3 cihazlar kullanılıyor. LAN içerisinde ise Broadcast yayınlarının kapsamını küçültmek (networkelri 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 notlarına bakılabilir).

Aşağıdaki görselde de belirtildiği gibi başlık bilgisine EtherType değerine bakarak karar veriyor (https[:}//en.wikipedia.org/wiki/EtherType → 0x8100 = VLAN, 0x0800 = IPv4 gibi).



Trunk moduna alnınan portlarda paketlere VLAN başlığı eklenerek iletiliyordu. 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'lar ayrıca tanımlanması gerekiyor). Belirli VLAN'lara ait trafiklerin geçirilmesi isteniyorsa bu VLAN'lar "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).

NOT

- Switchler üzerinde Port Security konfigürasyonu yapmadan portlara static MAC adres tanımlaması yapılarak da farklı MAC adresine sahip cihazların bu porta bağlanarak trafik oluşturamaması sağlanabiliyor. 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
```

    - “clear mac address-table dynamic (address <MAC address> | interface <Interface ID> | vlan <VLALN ID>)” komutula MAC Address tablosundaki belirli kayıtlar veya öğrenilmiş tüm MAC adresleri temizlenebiliyor.
- 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 thtoubleshooting 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
```

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.

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 int status