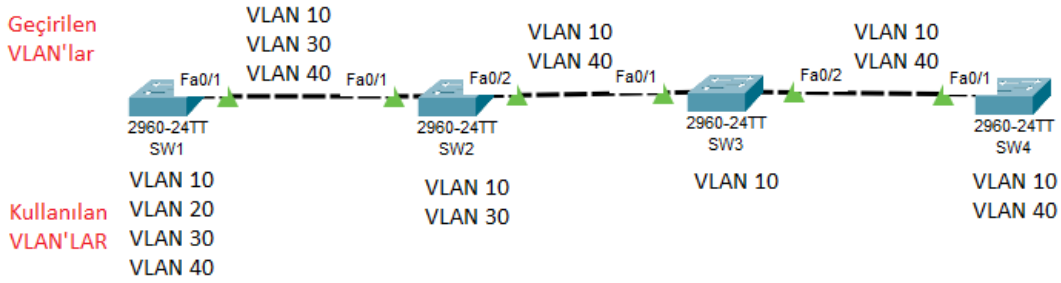
VLAN Trunks and EtherChannel Bundles

VLAN Trunking Protocol (VTP), Cisco marka switchler arasında VLAN konfigürasyonunu kolaylaştırmak adına geliştirilen bir protokoldür. Cisco'ya özeldir. İki önemli işlevi bulunmaktadır;

- Topolojide bulunan bir cihaz (VTP Server) üzerinde bulunan VLAN veritabanının (sadece oluşturulan VLAN tanımları bulunuyor) domain kapsamında bulunan diğer switchlere (VTP Client) otomatik olarak uygulanmasını sağlıyor. Örnek olarak VTP Server üzerinde bir VLAN oluşturulduğunda veya silindiğinde bu değişim domainde bulunan VTP Client'ler üzerinde otomatik olarak oluşturuluyor.
- **VTP Pruning**, Cisco marka switchlerde portlar Trunk moduna alıdığında varsayılanda bütün VLAN trafiğine izin verilir. Bu durumun büyük networklerde switch portlarını gereksiz yere meşgul ettiğinden bahsedilmişti (CCNA - 2.03 – VLANs – Özetle switch sayısı ve VLAN sayısı yüksek networklerde her VLAN içerisinde broadcast yayın yapıldığında bu paket bütün Trunk portlara anahtarlanıyordu. Bu durumda switch üzerinden geçmesine gerek duyulmayan VLAN trafikleri switchlerin Trunk portlarını gereksiz yere meşgul ediyordu). VTP Pruning özelliği sayesinde üzerinde switchlerin Trunk portlarında gerekli izinler otomatik tanımlanarak gereksiz VLAN trafiklerinin geçişi engelleniyor (VTP Pruning özelliği kullanılmadığında, topolojideki her switchin Trunk portlarına girilerek trafiğine izin verilmesi gereken VLAN'ların tek tek tespit edilip tanımlanması gerekecekti). Switchler üzerinde tanımlı VLAN'lar değiştiğinde VTP Pruning özelliği sayesinde değişim algılanarak tanımlamalar düzenleniyor.



VTP protokolünde switchler 4 farklı rolde olabiliyor;

- **Server**, üzerinde VLAN ekleme ve silme gibi işlemler yapılabilen VTP modudur. Üzerinde tanımlanan VLAN bilgilerini kendisine Trunk ile bağlı olan VTP Client switchlerle paylaşır.
- **Client**, üzerinde VLAN ekleme ve silme gibi işlemlerin yapılamadığı VTP modudur. Bu bilgileri Trunk modunda bağlandığı VTP Server modundaki switchlerden alır. Aldığı VLAN bilgilerini yine kendisine bağlı VTP Client modundaki switchlerle de paylaşır.
- **Transparent**, üzerinde VLAN ekleme ve silme gibi işlemler yapılabilen VTP modudur. Tanımlanan VLAN bilgilerini bir başka switch ile paylaşmaz. Yalnızca kendisine VTP Server veya VTP Client modundaki switchlerden genel VLAN bilgilerini kendisine bağlı VTP Client modundaki switchlere iletir (VTP Server veya VTP Client modundaki switchlerden gelen bilgileri kendisi öğrenmez sadece iletir).
    - Önceleri VTP özelliği cihazlarda kapatılamıyordu. Cihazlar Transparent moda alınarak VTP özeliği bir anlamda devre dışı bırakılmış olunuyordu.
    - Tanımlanan VLAN sayısı bazı cihazlar için fazla gelebiliyor. Bu gibi durumlarda da VTP özelliği kapatılarak kullanılacak VLAN'lar manuel olarak tanımlanabiliyor.
- **Off**, VTP özelliğinin devre dışı bırakıldığı moddur.

Switchlerde varsayılanda VTP versiyon 1 devrede gelmektedir. VTP versiyon 1 ve versiyon2 sadece VLAN 1-1005 arasında kullanılabilmektedir. Versiyon1 veya versiyon2 kullanıldığı halde 1005'den yüksek VLAN kullanıldığı tespit edilirse switch kendisini Transparent moduna alacaktır. VTP versiyon 3 ile beraber VTP protokolünün kullanım aralığı VLAN 1-4096 aralığına genişletildi.

Sunucu modundaki switchlerin belirli kapsamdaki VTP Clientlere VLAN bilgilerini öğretmesi sağlanıyor. Bu kapsama domain deniliyor.

VTP protokolünde kullanılan 3 paket yapısı vardır. Bunlar;

- **Summary**, her 300 saniyede bir VLAN'larda bir değişim olup olmadığını bildirmek üzere yayınlanıyor. Bu paket içerisinde VTP versiyonu, domain, Configuration Revision Number ve zaman damgası bulunuyor. Bu sayede son güncellemeleri almayan VTP Client moduna alınmış switchler son bilgileri alabiliyor.
- **Subset**, VLAN'lar üzerinde bir değişiklik yapıldığında bunu domainde bulunan switchlere bildirmek için kullanılan paket tipidir.
- **Client Request**, Client modundaki siwtchlerin güncellemeleri istemek için kullandığı paket tipidir.

VTP Versiyon 1-2 Konfigürasyon

- Global konfigürasyon modunda öncelikle "**vtp version <1 | 2 | 3>**" komutuyla VTP protokolünün versiyonu belirtiliyor.
    - Konfigürasyondan önce dikkat edilmesi gereken konulardan biri switchler arasında Trunk modunda bağlanmış olması gerekiyor (VTP, Trunk portlar üzerinden çalışıyor).
- Sürüm bilgisi tanımlandıktan sonra "**vtp domain <Domain Name>**" komutuyla domain bilgisi tanımlanıyor.
    - Switch üzerinde domain tanımı yapılmazsa switch kullanılan domain bilgisini bağlı olduğu switchlerden öğrenebiliyor. Bu durum tek seferliktir ve aynı VLAN güncellemelerini almak isteyen cihazlar arasında domain bilgileri de aynı tanımlanmalıdır.
- Switchin çalışacağı modu belirlemek için "**vtp mode <server | client | transparent | none>**" komutu kullanılıyor
- İsteğe bağlı olarak "**vtp pruning**" komutuyla VTP Pruning özelliği devreye alınabiliyor.
- Harici bir kaynaktan VTP anonsu yapılma ihtimaline karşı isteğe bağlı olarak switchler arasında "**vtp password <Password>**" komutuyla parola ataması yapılabiliyor.
    - Parola ataması bağlı switchlerde farklı tanımlanırsa switchler arasında güncellemeler aktarılmaz (tanımlı konfigürasyon kalmaya devam eder).

```
SWX(config)#vtp version 2
SWX(config)#vtp domain dom.to
Changing VTP domain name from NULL to dom.to
SWX(config)#vtp mode ?
  client       Set the device to client mode.
  server       Set the device to server mode.
  transparent  Set the device to transparent mode.
SWX(config)#vtp mode server
Device mode already VTP SERVER.
SWX(config)#vtp password CCNPPass
Setting device VLAN database password to CCNPPass
SWX(config)#
```

VTP Versiyon 3 Konfigürasyon

- VTP versiyon 3 konfigürasyonu için öncelikle "**vtp domain <Domain Name>**" komutuyla domain bilgisi tanımlanıyor.
    - Versiyon 3 kullanılıyorsa mutlaka domain adı tanımlanması gerekiyor. Aksi taktirde versiyon 3 kullanılamıyor. Aynı VLAN güncellemeleri alması istenen switchlerde domainler aynı olması gerekiyor.
- Domain belirlendikten sonra "**vtp version <1 | 2 | 3>**" komutuyla VTP protokolünün versiyonu belirtiliyor.
    - VTP versiyon 3 ile artık Extended VLAN'lar da destekleniyor.
    - Parola gizlemek gibi çeşitli güvelik önlemleri alınabiliyor.
- VTP versiyon 3 için değişen bir başka özellik ise VTP Server moduna alınan switchler Primary ve Secondary olmak üzere kategorilere ayrılıyor.
    - **Primary VTP Server**, topolojide sadece bir tane olabiliyor. VLAN ekleme ve silme gibi işlemlerin yapılabildiği VTP Server Switch modudur. VTP Server switchler arasında Primary switch seçilmesi istenen switch üzerinde "**vtp primary**" komutu kullanılıyor. Eğer ki topolojide daha önce bir switch Primary VTP Server seçilmişse bunu değiştirmek için herhangi bir Secondary VTP Server seçilen switch üzerinde "**vtp primary force**" komutu kullanılarak Primary Server seçilmesi sağlanabiliyor.
    - **Secondary VTP Server**, Primary olmayan her VTP Server switch Secondary VTP Server olarak tanımlanıyor. Bu switchler üzerinde VLAN tanımlama veya silme gibi işlemler yapılamıyor.
- Parola ataması için "**vtp password <Password> hidden**" komutu kullanılarak tanımlanıyor. Bu sayede;
    - Parolanın "**sh vtp password**" çıktısında görünmesi engelleniyor.
    - VLAN tanımlarında değişim yapabilmek için "**vtp primary**" komutuyla Primary moduna girmek gerekiyor. Parola tanımlanırken "**hidden**" kelimesi kullanıldığında Primary moduna girişlerde parola bilgisi isteniyor ("**hidden**" kelimesiyle kullanılmadan parola bilgisi tanımlandığında Primary moduna girişlerde parola bilgisi sorulmuyor. Bu durumda istenilen switch parola bilgisine ihtiyaç duyulmadan Primary VTP Server seçilebiliyor). Bu sayede parola bilinmeden VLAN veritabanına müdahale edilemiyor.

VTP Versiyon 3 Özellikleri

- Primary VTP Server: yalnızca Primary VTP Server VLAN'ları oluşturabilir/değiştirebilir/silebilir.
- Extended VLANs: Extended VLAN aralığındaki (1006 – 4094) VLAN'lar da senkronize edilebiliyor.
- Private VLANs: Private VLAN'lar olarak yapılandırılmış VLAN'lar varsa, bunları da VTP versiyon 3 kullanılarak senkronize edilebiliyor.
- RSPAN VLANs: Remote SPAN VLAN'lar senkronize edilebiliyor.
- MST Support: MST protokolünün sorunlarından biri, her switchte manuel olarak konfigüre edilmesi gerekiyordu. VTP versiyon 3 ile MST yapılandırmaları switchler arasında senkronize edilebiliyor.
- Authentication: VTP versiyon 3 önceki versiyonlara kıyasla kimlik doğrulama için daha güvenli yöntemlere sahip.
- Off Mode : Versiyon 1 ve versiyon 2'de VTP devre dışı bırakılmak için Transparent moda alınıyordu. VTP versiyon 3'de Off Modu getirilmiştir.

DTP

DTP (Dynamic Trunking Protocol), switchlerde portlarında karşısına takılan cihazın türüne göre kendisini Trunk veya Access moduna çeken moddur. Varsayılanda switchlerin bütün portlarında (DTP Dynamic Auto modunda) devrede gelmektedir. Bu mod güvenlik zafiyeti olarak görüldüğü için switchlerde kapatılması veya bütün portlarına Access moduna alınması tavsiye ediliyor (**Detaylar için CCNA – 2.03 – VLANs notlarını inceleyebilirsin**).

EtherChannel Bundle

EtherChannel, switchler arasında kullanılan birden fazla fiziksel bağlantının/kablonun tek bir mantıksal bağlantı gibi görünmesini sağlayan teknolojidir. Bu sayede switchler arasında yedeklilik sağlanırken aynı zamanda switchler arasında kurulan fiziksel bağlantıların aktif olarak kullanılması sağlanıyor. Bu sayede switchler arasındaki bant genişliği yükselmiş oluyor.

|→ Switchler görünen bant genişliğinin tamamı kullanılamıyor. Nedeni, switchlerde gelen trafikler belirli kriterlere göre yedeklenen bağlantılar arasında dağıtılmaktadır. Yani tam olarak Load Balance işlemi gerçekleştirilmiyor. Bu kriterin nasıl konfigüre edildiği CCNA notlarında açıklanmıştır.
|→ Günümüzde switchler ile sunucular arasında sıkça kullanılmaktadır.

EtherChannel ile bağlanacak portlarda konfigürasyonar yapıldıktan sonra kablolar farklı portlara bağlandığında Loop oluşturma riski vardır. Bu nedenle kabloların konfigüre edilen portlara takılıp takılmadığını konrtol etmek üzere EtherChannel yapılacak portlar arasında **PAgP** (Cisco) veya **LACP** (Open Standart – 802.3AD) gibi protokoller kullanılıyor (**Detaylar için CCNA - 2.06 - EtherChannel - Link Aggregation notlarını inceleyebilirsin**).

EtherChannel dinamik (LACP, PAgP gibi protokoller kullanılarak) olarak oluşturulabilirken statik olarak da oluşturulabiliyor. Mecbur kalınmadığı sürece statik oluştulması tevsiye edilmiyor. Nedeni, statik oluşturulduğumda dikkatsizlik sonucu yanlış porta bağlan kabloların Loop oluşturma ihtimali vardır.

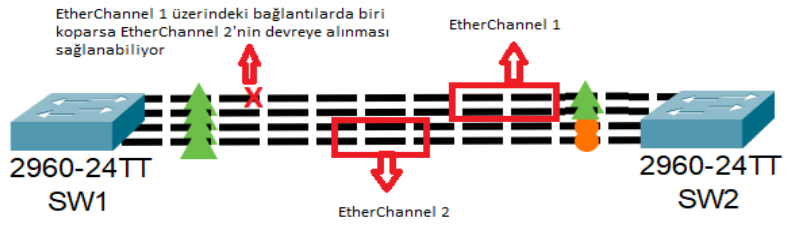
EtherChannel oluşturulurken kullanılan protokolü belirleyen nokta sadece kullanılan Mode isimleridir. Konfiürasyon için CCNA notlarına göz atabilirsin. Özetlemek gerekirse, PaGP veya LACP protokolünde portların atanabildiği üç mod vardır.

- **Auto**, pasif moddur (EtherChannel açılmaz). Karşı porttan EtherChannel kurma isteği gelirse EtherChannel'ın devreye alındığı moddur.
    - LACP protokolünde karşılığı **Passive Mode**'dur.
- **Desirable**, aktif moddur (EtherChannel açılmaz). Karşı porta EtherChannel kurma isteği gönderilir. Karşı port kapalı (on modunda) olmadığı sürece EtherChannel yapısının devreye alındığı moddur.
    - LACP protokolünde karşılığı **Active Mode**'dur.
- **On**, statik EtherChannel oluşturmak için kullanılan moddur. Portta hiçbir kontrol yapılmadan EtherChannel açılır (Karşı porta herhangi bir istek gönderilmez). Yani EtherChannel kurulacak portlar arasımda herhangi bir kontrol mekanizması istenmediği durumlarda kullanılan moddur.
    - On moduna alınan portun karşısındaki port Desirable veya Auto moduna alınması Loop riski oluşturur. Nedeni, On modundaki portta konrtol edilmeden (herhangi bir

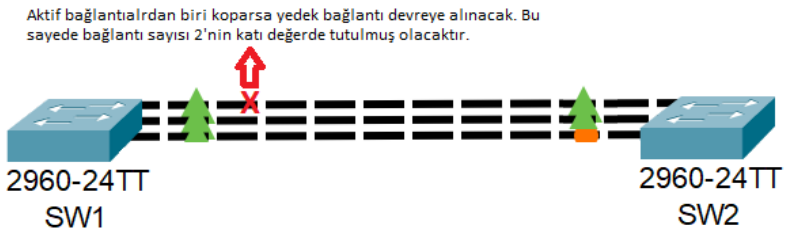
paket gönderilmeden) EtherChannel açılırken karşı porta herhangi bir paket gönderilmediği için EtherChannel devreye alınmayacaktır.

EtherChannel konfigürasyonunda LACP kullanmanın avantajları bulunmaktadır. Bu avantajşar;

- **LACP Fast**, normalde portlar arasında her 30 saniyede bir LACP paketleri gönderiliyor. 90 saniye boyunca LACP paketi alınmazsa EtherChannel bozuluyor. LACP Fast özelliğiyle portlar arasında 1 saniyede bir LACP paketleri gönderiliyor. Eğer ki 3 saniye içerisinde LACP paketi alınmazsa EtherChannel bozuluyor.
    - "**lacp rate fast**" komutuyla bu özellik devreye alınabiliyor.
    - "**sh lacp internal**" komutu çıktısında "S" sembolü normal modda çalıştığını, "F" sembolü Fast modunda çalıştığını gösteriyor.
- **Minimum Number of Port-Channel Member Interface**, EtherChannel yapılan portlar arasında minimum bağlantı sayısını sınırlandırmak için kullanılıyor. Örnek vermek gerekirse, minimum bağlantı sayısı 2 olarak belirlenen bir EtherChannel bağlantısında minmum 2 bağlantı devredeyse EtherChannel devreye alınır. Bağlantılardan biri koptuğunda yani bağlantı sayısı 2'nin altına düştüğünde LACP devre dışı bırakılır.
    - Switchlerde karşılıklı olarak oluşturulan sanal arayüzlerinin (EtherChannel arayüzü) altında "**lacp max-bundle <Min Bundle Count>**" komutuyla kullanılıyor.
    - Switchler arasında birden fazla EtherChannel yapıldığı durumda STP ile EtherChannel'lardan biri bloklanacaktır. Bu özellik sayesinde aktif kullanılan EtherChannel üzerindeki bağlantılardan biri koptuğunda LACP ile EtherChannel bağlantısının devre dışı kalması sağlanıyor. Bu sayede STP ile bloklanan port devreye alınabiliyor.



- **Maximum Number of Port-Channel Member Interface**, EtherChannel yapılan portlar arasında maximum kaç bağlantının aktif olarak kullanacağını belirlemek için kullanılıyor. Örnek olarak EtherChannel ile 4 bağlantı birleştirilmişse ve en fazla 2 bağlantının aktif kullanılması istendiğinde kullanılıyor. Ne zaman aktif bağlantılardan birinde sorun/kesinti yaşanırsa o zaman yedek bağlantılardan biri devreye alınır.
    - Switchlerde karşılıklı olarak oluşturulan sanal arayüzlerinin (EtherChannel arayüzü) altında "**lacp min-bundle <Max Bundle Count>**" komutuyla kullanılıyor.
    - EtherChannel konfigürasyonunda sağlıklı şekilde Load Balance yapılabilmesi için aktif bağlantı sayısını 2'nin katında tutabilmek için kullanılabiliyor.



Maximum Number of Port-Channel Member Interface veya Minimum Number of Port-Channel Member Interface özelliklerinde aktif bağlantıların hangileri olacağına karar verebilmek için Priority değerleri atanabiliyor. System Priority ve Port Priority olmak üzere iki adet Priority değeri bulunuyor.

- **System Priority**, aktif bağlantıların hangisi olacağına karar verecek switchi belirlemek için kullanılıyor. Varsayılanda bu değer bütün switchlerde 32768.MAC Address şeklinde oluşmaktadır. İsteğe bağlı olarak switchlerde "**lacp system-priority <System Priority Number>**" komutuyla bu değer değiştirilebiliyor (Düşük Priority değerine sahip switch aktif bağlantıları belirliyor).
- **Port Priority**, EtherChannel bağlantıları arasında hangi portların aktif seçileceğini belirlemek için kullanılıyor. Priority değeri düşük olan portlar aktif seçiliyor. Varsayılanda bu değer bütün portlarda 32768.PortID şeklinde oluşmaktadır. İsteğe bağlı olarak portların arayüzüne girilerek "**lacp port-priority <Port Priority Number>**" komutuyla değiştirilebiliyor (Düşük Priority değerine port aktif bağlantı olarak seçilir).

Throubleshooring sürecinde en sık kullanılan "**sh etherchannel summary**" komutu çıktısı incelendiğinde;

- D – EtherChannel'ın çalışmadığını gösteriyor.
- S – L2 cihazlar arasıda kurulduğunu gösteriyor
- R – L3 cihazlar arasıda kurulduğunu gösteriyor
- U – EtherChannel'ın kullanıldığını gösterir
- P – portlarda sorunsuzca çalıştığını gösteriyor.
- I – karşı porttan LACP paketleri gelmediği için EtherChannel kurulmadığını (Stand-Alone durumunda kalındığını) gösteriyor.
    - "**sh lacp counters**" komutuyla LACP sürecinde karşıdan kaç paket geldiği görülebiliyor.
    - Bu değer "**clear lacp counters**" komutuyla sıfırlanabiliyor.
- w, karşı porta paket yollandığını, dönüş paketinin beklendiğini gösterir.
- r, modüler switchde modülün çıkarıldığını/bozulduğunu gösteriyor.
- H –LACP konfigürasyonunda portlardan birinin Bundle'a dahil olmadığını (yedek durumdaysa) gösteriyor (Maximum Number of Port-Channel Member Interface özelliğinde).
- M – LACP konfigürasyonunda minimum bağlantı sayısı karşılanmadığı için LACP protokolünün devre dışı kaldığını gösterir (Minimum Number of Port-Channel Member Interface özelliğinde).

```
SWX#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------

1      Po1(SD)           PAgP   Fa0/1(D) Fa0/2(D)
SWX#
```

NOT

- VTP Pruning özelliğinin sadece Server modundaki switch üzerinde devreye alınması yeterli oluyor.
- EtherChanel özelliği L2 cihazlar arasında yapılabildiği gibi L3 (router gibi) cihazlar arasında da kullanılabiliyor.
- PAgP –> 0X0104, LACP ->
- EtherChannel konfigürasyonu silent modda çalışıyormuş. İsteğe bağlı olrarak portlar arasında **Unidireciton Link** oluşması ihtimaline karşı portlarda "**non-silent**" parametresi de eklenebiliyor ("**channel-group <Channel ID> mode <auto | desirable> {non-silent}**" şeklinde kullanılıyor). Bu sayede portlarda karşılıklı olarak trafik akışı kontrol ederek Unidirectional Link oluşması durumunda tespit edilebiliyormuş (Bu özellik **UDLD** (Unidirectional Link Detection) çözümü geliştirilmeden önce kullanılıyormuş).
- EtherChannel konfigürasyonu için portların temiz konfigürasyon olması istenir. Nedeni, EtherChannel oluşturacak portlar aynı konfigürasyona sahip olmalı. Portlar mantıksal bir gruba alındıktan sonra portlarda yapılmak istenen bütün konfigürasyonlar bu mantıksal grupta tanımlanır. Oluşturulan mantıksal grupta tanımlanan konfigürasyonlar mantıksal gruba alınan portların arayüzlerine de otomatik olarak uygulanıyor. Bu sayede portlar aynı konfigürasyona sahip oluyor.
- **EtherChannel konfigürasyonunda 2 ve katları sayılarda bağlantılar arasında kullanılması tavsiye ediliyor.** Nedeni, portlar arasında Load Balance yapılırken paketler üzerindeki belirli adresler matematiksel işlemlere tabi tutuluyordu ve sonucuna modüler aritmetik uygulanarak gönderilecek bağlantı belirleniyordu. Bu durum bağlantı sayısı ikinin katı olmadığı zamanlarda problemlere neden olabiliyor. **Örnek olarak EtherChannel için 3 bağlantı kullanıldığında ilk iki bağlantıya toplam trafiğin %25'ini gönderirken üçüncü bağlantıya %50'sini gönderiyor.**
    - Bu durmda tek sayıda bağlantı kullanılarak LACP konfigürasyonu yapılıyorsa Maximum Number of Port-Channel Member Interface özelliği kullanılarak kullanılan bağlantı sayısı 2'nin katına çekilebiliyor.
    - Max 8 bağlantı ile EtherChannel yapılabiliyordu.
- **Port Type - Port Mode -Narive VLAN - Allowed VLAN – Speed – Duplex – MTU – Load Interval – Storm Control** gibi özelliklerin EtherChannel yapılan portlar içerisinde de karşılıklı portlarda (switchler arasında karşılıklı olarak) da aynı tanımlanması gerekiyor ki EtherChannel sorunsuz çalışabilsin.
- EtherChannel özelliğinde bağlantılar arasında Load Balance için bakılan adres bilgisi "**port-channel load-balance <Addresses>**" komutuyla değiştirilebiliyor. Bu sayede hesaplanan Hash değerinin cok daha çeşitli olması sağlanabiliyor (Bu konfigürasyon switch üzerindeki bütün EtherChannel portlar için geçerli oluyor).
    - Önerilen kullanım ip adresi ve port numarasıan bakılarak gerçekleştirilmesi. Bu seçim kullanıldığı duruma göre değişmektedir (Değişim gösteren adres tipi seçilmeli ki çeşitlilik oluşsun).

Terminolojiler

- **Configuration Revision Number**, VTP protokolünde domainde gerçekleştirilen son güncellemeleri temsil etmek için kullanılan bir sayısal değerdir. Sıfırdan başlar ve her güncellemede bir arttırılır. Bu değer Summary paketi içerisinde bulunur ve VTP Client modundaki switchlerde bu değer aynı değilse VTP Client switchlerin son güncellemeleri almadığını anlayarak komşu switchden güncellemeleri istemesini sağlıyor.
    - Bu değer güvenlik zafiyeti olarak da görülebiliyor. Nedeni, Revision Number değeri topolojideki cihazlardan daha yüksek bir switch topolojiye eklenirse topolojideki bütün switchlerin VLAN tanımını değiştirecektir. Bu ihtimalin gerçekleşebilmesi için cihazların;
        - Domain bilgileri aynı olması gerkeiyor.
        - Parola bilgilerinin aynı olması gerekiyor.
        - Trunk bağlı olması gerekiyor
        - Revision Number değeri topolojideki günvellemelerden daha yüksek olmak zorunda.
          Bu şartların hepsinin oluşması durumunda VLAN veritabanını değiştirebiliyor.
    - Ek olarak switch üzerindeki Revision Number değeri Transparent moda alınıp yeniden Server moduna alındığında veya domain değikliği yapıldığında sıfırlanmaktadır.

Kontrol Kmutları

- sh vtp status
- sh vtp password

```
Switch#sh vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 :
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 00D0.FF64.DC00
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 255
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A
                                    0xF0 0x58 0x10 0x6C 0x9C 0x0F 0xA0 0xF7

Switch#
```

Tanımlanan Domain bilgisi
Pruning özelliğinin durumu
Her yeni VTP mesajı gönderildiğinde bir SNMP mesajının üretilmesine neden olur (Bir tür loglama özelliği)
Gerçekleştirilen son güncellemenin zaman bilgileri
Son güncellemenin yapıldığı switchin ip adresi
Güvenlik kullanılıyorsa Hash'lenmiş anahtarı gösteriyor

- sh etherchannel port
- sh etherchannel summary
- sh lacp neighbor {detail}
- sh lacp internal
- sh pagp neighbor {detail}
- sh lacp counters
- sh lacp sys-id