Huawei Genel Notlar

LAN kapsamında kullanılan protokollere yönelik çeşitli saldırılar gerçekleştirilebiliyor. Bu yazıda Huawei switchler üzerinde gerçekleştirilebilecek saldırı çeşitlerine karşı devreye alınabilecek çeşitli güvenlik özellikleri açıklanmaya çalışılacaktır.

Huawei switchler üzerinde alınabilecek önlem varsayılanda açık gelen fiziksel portlar arasından kullanılmayanları "**shutdown**" komutuyla kapatılmasıdır. Bu sayede bir noktaya kadar boşta olan portlar üzerinden networke yetkisiz erişimler engellenebilecektir.

Port Security

Portlara erişimleri kısıtlamak üzere kullanılan güvenlik özelliğidir. Portlara bağlanan MAC adresleri baz alınarak erişimleri kısıtlamaktadır. Bu sayede MAC Address Flood saldırısına karşı da koruma sağlamaktadır. Huawei switchlerde Port Security konfigürasyonu için;

- Port bazında devreye almak için ilgili portun arayüzü altında "**port-security {enable | disable}**" komutunun kullanılması gerekiyor. Bu komut sonrasında Port Security özelliği varsayılan ayarlarda devreye alınacaktır (Maksimum 1 MAC adresi öğrenilebilir, Restrict modunda çalışır).
- Port Security özelliği devreye alındıktan sonra yapılabilecek özelleştirmelere bakıldığında;
    - "**port-security maximum <Max Number>**" komutuyla port üzerinde öğrenilebilecek maximum MAC adres sayısı güncellenebilir (switch bağlı portlar üzerinde birden fazla MAC adresi öğrenildiği için switchler arası portlarda).
    - Port üzerinde MAC adresler üzerinde özelleştirmeler yapabilmek için ilk olarak "**port-security mac-address sticky**" komutuyla Sticky özelliğinin devreye alınması gerekiyor (sonrasında "**commit**" komutuyla uygulanmadığı sürece manuel/statik MAC adresi tanımlanamıyor). Ardından isteğe bağlı olarak "**port-security mac-address sticky (<MAC Address> vlan <VLAN Id>)**"komutuyla porta bağlanacak istemcinin MAC adresinin manuel/statik olarak tanımlanması da sağlanabiliyor (FARKLI MAC ADRESİN SAHİP CİHAZ BAĞLANDIĞINDA PORTUN AKSİYON ALMASI İSTENİYORSA CİHAZLARIN MAC ADRESLERİ PORT ALTINDA MUTLAKA MANUEL OLARAK TANINLAMLIDIR).
        - Port üzerinde öğrenilebilecek MAC adres sayısı arttırılarak bir kısmının manuel/statik olarak tanımlanması, bir kısmının da Sticky özelliği ile dinamik şekilde öğrenilmesi sağlanabilir.
    - "**port-security protect-action {protect | restrict | error-down}**" komutuyla Port Security özelliği devreye alınan portta kural ihlali yapıldığında gerçekleştirilmesi istenen aksiyon belirtilebiliyor.
        - **Error-down**, port kapatılır ve kural ihlali loglanır. Portu tekrar devreye alabilmek için önce "**sh**" komutuyla port manuel olarak kapatılır. Ardından "**undo sh**" komutuyla tekrar açılır.
        - **Restrict**, portta kural ihlali olduğunda port kapanmaz ama kural ihlali yapan istemci loglanır ve bloklanır.
        - **Protect**, portta kural ihlali yapıldığında port hizmet vermeye devam eder. Kural ihlali yapan istemci bloklanır ama loglanmaz.

```
[~CE6800-2]int ge 1/0/7
[~CE6800-2-GE1/0/7]port-security enable
[~CE6800-2-GE1/0/7]port-security maximum 4
[~CE6800-2-GE1/0/7]port-security mac-address sticky
[~CE6800-2-GE1/0/7]commit
[~CE6800-2-GE1/0/7]port-security mac-address sticky  AA-BB-CC vlan 1
[~CE6800-2-GE1/0/7]port-security mac-address sticky  12-54-23 vlan 1
[~CE6800-2-GE1/0/7]port-security protect-action error-down
Info: If the interface is triggered to error-down state, you need to recover the
 interface manually or enable error-down auto-recovery globally.
[*CE6800-2-GE1/0/7]quit
```

Port Isolation

Çoğu zaman aynı switch üzerinde bulunan cihazların arasında haberleşmesine ihtiyaç yoktur (ip telefon benzeri sistemler bu kapsam dışındadır). Bu haberleşmeyi engellemek için Port Isolation özelliğiyle portlar birbirinde izole edilebilmektedir.

Switch üzerinde Port Isolation özelliğini devreye almak için ilgili port altında "**port-isolate enable**" komutunu kullanmak yeterlidir**. Eğer ki arasında haberleşmemesi gereken belirli bir grup istemci bulunuyorsa** bu durumda "**port-isolate enable group <Isolation Group Number>**" komutuyla bu istemci portları belirli bir gruba alınarak arasında haberleşmesi engellenebilir. **Bu özellik devreye alınmadan önce aynı switch üzerinde arasında haberleşmesi gereken sistemlerin olup olmadığına dikkat edilmelidir**.

Aşağıdaki konfigürasyon sonucunda portlar aynı VLAN'da olmalarına rağmen 1. Port ve 2. Port arasında iletişim kuramayacaktır (her iki port da 3. Portla iletişim kurabilir). 3. Port ise bütün portlar ile iletişim kurabilecektir.

```
[CE6800-1] interface ge 1/0/1
[CE6800-1-GE1/0/1] port link-type access
[CE6800-1-GE1/0/1] port default vlan 10
[CE6800-1-GE1/0/1] port-isolate enable group 3
[CE6800-1-GE1/0/1] quit

[CE6800-1] interface ge 1/0/2
[CE6800-1-GE1/0/2] port link-type access
[CE6800-1-GE1/0/2] port default vlan 10
[CE6800-1-GE1/0/2] port-isolate enable group 3
[CE6800-1-GE1/0/2] quit

[CE6800-1] interface ge 1/0/3
[CE6800-1-GE1/0/3] port link-type access
[CE6800-1-GE1/0/3] port default vlan 10
[CE6800-1-GE1/0/3] quit
```

DHCP Protection

Önceki bölümde de açıklandığı üzere DHCP protokolüne yönelik saldırılarda DHCP Starvation ve Route DHCP Server saldırılar gerçekleştirilebiliyordu. Bu saldırılara karşı önlem olarak DHCP Snooping özelliği devreye alınabiliyor.

Normal şartlarda L2 switchlerde MAC-Address tablosu tutulur ve bu tabloda port-MAC eşleniği tutulur. DHCP Snooping özelliğiyle beraber L2 switchler üzerinde istemcilerin DHCP sunucularında aldığı ip adresleri de tutulmaya başlanır. IP adresleri istemcilerin DHCP sunucusundan ip alma sürecinde DHCP sunucusunun istemciye gönderdiği paketler dinlenerek oluşturulur. Bu bilgiler doğrultusunda L2 switch üzerinde DHCP Snooping özelliği açık olan portlarına bağlı istemcilerin **MAC adresinin - Port numarası - IP adresinin** tutulduğu **Snooping Binding** tablosu oluşturulur.

DHCP Snooping özelliği açılan portlarda sadece istemcilerin DHCP sunucusundan ip alma sürecinde oluşturabilecekleri paketlerin geçişine izin verilir. İstemci DHCP sunucusundan ip almadığı/alamadığı takdirde Snooping Binding tablosunda kaydı oluşmayacağı için istemcinin trafik oluşturmasına izin verilmeyecektir. Bu nedenle ip adresi Static verilen, Uplink portları veya ip kullanmayan sistemlerin bulunduğu portlar "Trusted" olarak tanımlanmalıdır.

DHCP Snooping özelliğinin DHCP paketlerini dinleyerek Snooping Binding tablosunda kayıt oluşturduğundan bahsedilmişti. Switch üzerinde DHCP paketlerinin dinlenebilmesi için DHCP Snooping özelliği devreye alınmadan önce switch üzerinde DHCP hizmetinin devreye alınmış olması gerekiyor. Switch üzerinde DHCP hizmetini devreye alınmamışsa system-view altında "**dhcp enable**" komutuyla devreye alınabilir.

DHCP Snooping özelliğini switch üzerinde port bazında ve VLAN bazında olmak üzere iki farklı şekilde devreye alınabiliyor.

- Port bazında devreye alabilmek için ilk olarak system-view modu altında "**dhcp snooping enable [ipv4 | ipv6]**" komutuyla switch genelinde DHCP Snooping özelliğinin devreye alınması gerekiyor.
    - DHCP Snooping özelliği cihaz genelinde devreye alındıktan sonra DHCP Snooping özelliğinin açılacağı portların atına giriş yapılarak "**dhcp snooping enable**" komutunun kullanılması yeterli olacaktır.
    - DHCP Snooping özelliği cihaz genelinde devreye alındıktan sonra DHCP Snooping özelliğinin açılacağı VLAN arayüzüne giriş yapılarak "**dhcp snooping enable**" komutunu kullanmak yeterli olacaktır. Bu komut sonrasında bu VLAN'a dâhil edilen bütün portlarda otomatik olarak DHCP Snooping özelliği devreye alınmış olacaktır.
- DHCP Snooping hizmeti switch üzerinde devreye alındıktan sonra DHCP Snooping özelliğinin devreye alındığı potların trafik oluşturabilmesi için **switch Uplink portunun** "**dhcp snooping trusted**" komutuyla Trusted olarak tanımlanması gerekmektedir. Aksi takdirde Uplink üzerinden de sadece DHCP sunucusundan ip alma sürecinde istemcilerin oluşturabileceği DHCP paketlerine izin verilecektir. Dolayısıyla switch üzerinde DHCP Snooping özelliğinin devreye alındığı hiçbir port trafik oluşturamayacaktır. Bu tanımların sonrasında aşağıdaki gibi kayıtlar oluşmaya başlayacaktır.
    - **Benzer şekilde statik ip alan veya ip kullanmayan sistemlerin bağlı olduğu switch portlarının da Trusted olarak tanımlanması gerekmektedir**.

```
                                dis dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P)/(BD-VLAN) Interface      Lease
-------------------------------------------------------------------------------
10.10.           e073-e7         10  /--  /--             GE0/0/1        2006.10.16-14:53
```

Özetle uygulanması gereken komutlar aşağıdaki gibi olacaktır;

```
[CE6800-1] dhcp enable
[CE6800-1] dhcp snooping enable ipv4

[CE6800-1] interface ge 1/0/1
[CE6800-1-GE1/0/1] port link-type access
[CE6800-1-GE1/0/1] port default vlan 10
[CE6800-1-GE1/0/1] dhcp snooping enable
[CE6800-1-GE1/0/1] quit

[CE6800-1] interface ge 1/0/2
[CE6800-1-GE1/0/2] port link-type access
[CE6800-1-GE1/0/2] port default vlan 10
[CE6800-1-GE1/0/2] dhcp snooping trusted
[CE6800-1-GE1/0/2] quit

[CE6800-1] interface x 0/0/1
[CE6800-1-XGE0/0/1] description 10GE_Uplink_Port
[CE6800-1-XGE0/0/1] port link-type trunk
[CE6800-1-XGE0/0/1] port trunk allow-pass vlan 2 to 4094
[CE6800-1-XGE0/0/1] dhcp snooping trusted
[CE6800-1-XGE0/0/1] quit
```

ARP Protection

Önceki yazıda da açıklandığı üzere ARP protokolüne yönelik MITM gibi daha pek çok saldırı gerçekleştirilebiliyordu. ARP Snooping özelliği ARP protokolüne yönelik saldırıların önüne geçmek için kullanılan güvenlik özelliklerinden birisidir. DHCP Snooping özelliğiyle oluşturulan Snooping Binding tablosunu temel alarak çalışır. Dolayısıyla ARP Snooping konfigürasyonuna başlamadan önce DHCP Snooping özelliğinin devreye alınması gerekmektedir.

ARP Snooping özelliğinin devreye alındığı portlardan gönderilen ARP paketleri dinlenir. Port üzerinden gönderilen ARP paketlerindeki kaynak IP ve MAC adresi Snooping Binding tablosundan hangi port ile eşleştirildiği kontrol edilir. **Snooping Binding tablosunda port, kaynak IP adresi ile MAC adresinin eşleştirildiği kayıtlı bulunuyorsa bu doğrultuda trafiğe izin verilir**. Eğer ki Snooping Binding tablosunda ilgili porttan gönderilen ARP paketindeki kaynak IP adresi ile kaynak MAC adresinin eşleştirildiği bir satır bulunmuyorsa, bu porttan bu IP ve MAC adresleriyle oluşturulan paketlere izin verilmiyor.

DHCP Snooping özelliğinde statik ip alan cihazların bağlı olduğu portların Trusted olarak belirlenmesi gerekiyordu. ARP Snooping özelliğinde de aynı şekilde statik ip verilen cihazların bağlı olduğu portların Trusted olarak belirtilmesi gerekiyor. Aksi takdirde MAC-IP eşleniği Snooping Binding tablosunda bulunmayacağından dolayı ARP trafiği engellenecektir. Dolayısıyla herhangi bir hedefin MAC adresini çözümleyemeyecek, erişim sağlayamayacaktır.

ARP Snooping özelliği de DHCP Snooping özelliğinde olduğu gibi switch üzerinde port bazında ve VLAN bazında olmak üzere iki farklı şekilde devreye alınabiliyor. Bu işlem öncesinde ARP Snooping özelliğinin çalışabilmesi için DHCP Snooping özelliğinin devreye alınması gerekiyor. DHCP Snooping özelliği devreye alındıktan sonra;

- İlk olarak System-View modu altında "**arp snooping enable**" komutuyla ARP Snooping özelliğinin cihaz genelinde açılması gerekiyor.
- ARP Snooping özelliği cihaz genelinde açıldıktan sonra;

- Port altında teker teker açılmak isteniyorsa ilgili portun altında “**arp snooping enable**” komutunu kullanmak yeterli olacaktır.
- VLAN bazında açılmak isteniyorsa ilgili VLAN tanımının altında “**arp snooping enable**” komutunu kullanmak yeterli olacaktır. Bu komut sonrasında bu VLAN’a dâhil edilen bütün portlarda otomatik olarak ARP Snooping özelliği devreye alınmış olacaktır

- ARP Snooping hizmeti switch üzerinde devreye alındıktan sonra ARP Snooping özelliğinin devreye alındığı potların trafik oluşturabilmesi için **switch Uplink portunun** “**arp snooping trusted**” komutuyla Trusted olarak tanımlanması gerekmektedir. Aksi takdirde Uplink portunda ip alan istemci olmayacağı için Snooping Binding tabosunda kaydı olmayacaktır. Dolayısıyla ARP paletlerine izin verilmeyecektir.
  - **Benzer şekilde statik ip alan veya ip kullanmayan sistemlerin bağlı olduğu switch portlarının da Trusted olarak tanımlanması gerekmektedir**. **Özetle DHCP Snooping özelliğinde Trusted olarak tanımlanan portlarda ARP Snooping için de Trunsted tanımı yapılması gerekiyor denilebilir**.

```
[CE6800-1] dhcp enable
[CE6800-1] dhcp snooping enable ipv4
[CE6800-1] dhcp snooping enable

[CE6800-1] interface ge 1/0/1
[CE6800-1-GE1/0/1] port link-type access
[CE6800-1-GE1/0/1] port default vlan 10
[CE6800-1-GE1/0/1] dhcp snooping enable
[CE6800-1-GE1/0/1] arp snooping enable
[CE6800-1-GE1/0/1] quit

[CE6800-1] interface ge 1/0/2
[CE6800-1-GE1/0/2] port link-type access
[CE6800-1-GE1/0/2] port default vlan 10
[CE6800-1-GE1/0/2] dhcp snooping trusted
[CE6800-1-GE1/0/2] arp snooping trusted
[CE6800-1-GE1/0/2] quit

[CE6800-1] interface x 0/0/1
[CE6800-1-XGE0/0/1] description 10GE_Uplink_Port
[CE6800-1-XGE0/0/1] port link-type trunk
[CE6800-1-XGE0/0/1] port trunk allow-pass vlan 2 to 4094
[CE6800-1-XGE0/0/1] dhcp snooping trusted
[CE6800-1-XGE0/0/1] arp snooping trusted
[CE6800-1-XGE0/0/1] quit
```

STP Protections

Switch portlarında alınabilecek önlemlerden birisi de STP protokolüne yönelik saldırılarak karşı Loop-Guard ve PBDU-Filter özellikleridir. Bilindiği üzere Edge switch portlarına istemci bağlanacak portlarına bir istemci bağlandığında istemci STP protokolünden kaynaklı 15+15 (STP’nin Listening ve Learning adımları) toplamda 30 saniye Loop oluşturup oluşturmayacağını belirleyebilmek için kontrollerini sağlıyor (RSTP protokolünde switch bağlandığında 2 saniyenin altında kontroller sağlansa da porta istemci bağlandığında bu süre yine 30 saniyeyi buluyor).

İstemci bağlanacak portlarda STP protokolünden kaynaklı gecikmelerin önüne geçebilmek adına **Edge-Port** özelliği kullanılıyor. Edge-Port özelliğini devreye almak için ilgili port altında "**stp edge-port enable**" komutu kullanılıyor. Edge-Port tanımı yapılan portlarda STP protokolü devre dışı bırakılıyor. Bu sayede istemci porta bağlanır bağlanmaz DHCP'den ip alarak trafik oluşturabiliyor. Bir anlamda da Loop kontrolü için switch kaynakları da gereksiz yere işgal edilmemiş oluyor.

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] stp edge-port enable
[SwitchA-GigabitEthernet0/0/1] quit
```

Edge switch konfigürasyonu sonrasında portlara herhangi bir switch bağlanması durumunda çeşitli saldırılara neden olabilecektir. Bunun önüne geçmek için Edge-Port tanımı bulunan portlar altında BPDU-Protecton özelliği de devreye alınmalıdır.

BPDU-Protection özelliği System-View modu altında "**stp bpdu-protection**" komutu kullanılarak devreye alınıyor. **Bu komut sonrasında switch üzerinde Edge-Port tanımı yapılan bütün portların altında otomatik olarak devreye alınıyor**. Devreye alındığı portlardan herhangi bir BPDU paketi gönderildiği takdirde portu bloklanarak trafik oluşturmasının önüne geçilir (yani bu portlara bir switch takıldığı durumda Loop oluşturma ihtimaline karşı port kapanacaktır). Bu sayede BPDU paketlerinin gelmesini engelleyerek istemcilerin daha yüksek Bridge ID Priority değerine sahip BPDU paketleri gönderip STP ağacındaki Root Bridge üzerinde değişimlere neden olarak network üzerinde kesintilere neden olmasının da önüne geçmektedir.

```
<SwitchA> system-view
[SwitchA] stp bpdu-protection
```

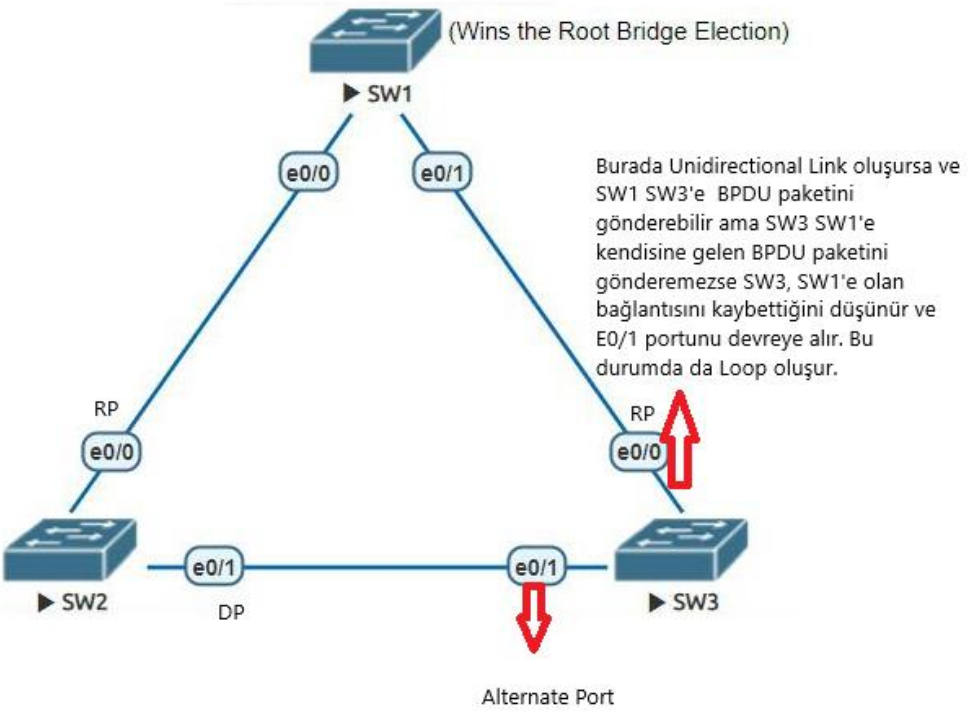
STP protokolünde daha düşük Bridge ID Priority değerine sahip BPDU paketleri gönderilip STP ağacında değişimlere neden olunarak kesintilere veya trafiği yönlendirme gibi çeşitli saldırıların yapılabilme tehlikesi bulunuyor. Bu durumu engellemek için **networkte bulunan Primary ve Secondary Root Bridge durumundaki switchlerin portlarına Root-Protection tanımı eklenebilir.** Root-Protection özelliği, açıldığı portlarda Root Bridge'in sahip olduğu daha düşük Bridge ID Priority değerine sahip PBDU paketlerinin Drop edilmesini sağlayarak Root Bridge'i korumaya yönelik kullanılan özelliktir Root- Protection özelliğini devreye almak için ilgili port altında "**stp root-protection**" komutunu kullanmak yeterli olacaktır.

```
<SwitchA> system-view
[SwitchA] [SW1]stp instance 1 root primary
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 5 10 15 20
[SwitchA-GigabitEthernet0/0/1] stp root-protection
[SwitchA-GigabitEthernet0/0/1] quit
```

BPDU paketleri sadece Root Bridge tarafından gönderilir. Topolojide bir değişiklik meydana geldiğinde bu değişikliğin meydana geldiği (switch Uplink portlarından birisi Up veya Down olması durumunda veya yeni bir switch eklenmesi durumunda) switch tarafından topolojideki Root Bridge'e bu durum TCN (Topology Change Notification) mesajıyla bildirilir. Root Bridge ise değişikliğin meydana geldiği switche TCA mesajıyla dönüş yapar. Topolojide değişiklik olduğunu öğrenen Root

Bridge, topolojideki her switche TCN mesajını ileterek yeniden hesaplama yapılması gerektiğini bildirir. Dolayısıyla STP ağacı yeniden hesaplanır ve bu doğrultuda Mac Address tablosunu günceller. Hesaplama sürecinde switchler hizmet veremez durumda olacaktır. Dolayısıyla TCN mesajları bir saldırgan cihazı üzerinden belirli aralıklarla yapıldığı takdirde, topolojideki switchlerin tekrar tekrar hesaplama sürecine girecek ve bu süreçte hizmet veremeyecektir. Bu kesintinin önüne geçebilmek için **STP TC Protection** özelliği devreye alınabilmektedir. TC Protection özelliği, saldırıyı gerçekleştiren cihazın MAC adres ve ARP kayıtlarını silerek tekrar tekrar TCN mesajı göndermesinin önüne geçmektedir. Tc Protection özelliğinin topolojideki tüm switchlerde devreye alınması gerekiyor. Devreye almak için System-View modu altında "**stp tc-protection**" komutunu kullanmak yeterli olacaktır.

STP protokolü çalışan bir topoloji üzerinde, bağlantı yığılması ya da **Unidirectional Link** hatası nedeniyle BPDU paketi gönderilebildiği ama alınamadığı durumlarda, switch port rolünü yeniden seçerek BPDU ve veri trafiğini iletmeye devam eder. Böyle bir durumda tek yönlü bağlantı hatası yaşanan switchin bağlı olduğu komşu switch BPDU mesajını alamayacağı için komşu switchin bağlantısının kesildiğini düşünerek kendisine bağlı ve engellediği alternate durumunda bulunan portlardan birisini açarak designated durumuna çevirir. Bu durumda networkte Loop oluşacaktır.



Bu tür durumların önüne geçebilmek için **Loop-Protection** özelliği devreye alınmalıdır. Loop-Protection özelliği BPDU paketi alınamayan portları rolünü Discarding olarak belirleyerek trafik akışının tamamını keser. Bu sayede tek yönlü trafik oluşturulamaz. Dolayısıyla Loop oluşumunun da önüne geçilmiş olacaktır.

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] port default vlan 10
[SwitchA-GigabitEthernet0/0/1] stp loop-protection
[SwitchA-GigabitEthernet0/0/1] quit
```

VLAN Protections

Huawei switchlerde varsayılanda portlar Desirable modunda gelmektedir. Desirable modu karşısına bağlanan cihaz tipine göre portun Access veya Trunk port gibi çalışmasını sağlayan moddur. Portlar bu modda bırakıldığı takdirde saldırgan porta bağlanıp kendisini switch gibi göstererek bağlandığı switch portunun Trunk modunda çalışmasını sağlayabilir (**normalde switch portları Trunk moduna alınıp herhangi ek bir tanım yapılmadığı takdirde sadece VLAN 1 trafiğini geçirmektedir. Oysa ki Desirable modunda bir port Trunk modunda çalışmaya başladığında varsayılanda bütün VLAN trafiklerine izin verilmiş şekilde çalışıyor**). Bu şekilde networkteki bütün VLAN trafiğini dinleyebilir ve trafik oluşturabilmektedir. Bu nedenle Portlar kullanılmasa dahi "**port link-type access**" Access moduna alınması daha sağlıklı olacaktır. Bu durumda herhangi bir VLAN belirtilmediği sürece VLAN 1 trafiği geçirilecektir.

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] quit
```

Varsayılanda Native VLAN'da VLAN 1'de gelmektedir. Her ne kadar saldırı kapsamı sınırlı olsa da VLAN Hoping saldırısının önüne geçebilmek adına switch Trunk modunda çalışan Uplink portlarının da bağlandığı switch portlarıyla karşılıklı olarak "**port trunk pvid vlan <VLAN ID>**" komutuyla Native VLAN değerinin kullanılmayan bir VLAN ile değiştirilmesi gerekmektedir.

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allowpass vlan 10 20
[SwitchA-GigabitEthernet0/0/1] port trunl pvid vlan 10
[SwitchA-GigabitEthernet0/0/1] quit
```

Other Protections

Bu özellikler dışında switchler üzerinde alınabilecek güvenlik önlemlerine bakıldığında;

- Edge switch portlarında LLDP protokolü "**lldp disable**" komutuyla devre dışı bırakılabilir (doğrudan cihaz genelinde de devre dışı bırakılabilir ama bu sağlıklı olmayabilir). Bu sayede bağlanan cihazların switch üzerindeki bilgileri elde etmesinin önüne geçilebilir.
    - Burada Voice VLAN gibi sağlıklı çalışması için LLDP protokolüne ihtiyaç duyan cihazlara dikkat edilmelidir.
- Yazının başında da belirtildiği üzere kullanılmayan portların kapatılmasının yanında bu portlarda "**mac-address learning disable**" komutu kullanılarak MAC adresinin dinamik olarak öğrenilmesinin de önüne geçilebilir. Bu sayede port dikkatsizlik sonucu açılsa dahi MAC adresi öğrenilemeyeceği için trafik oluşturamayacaktır.

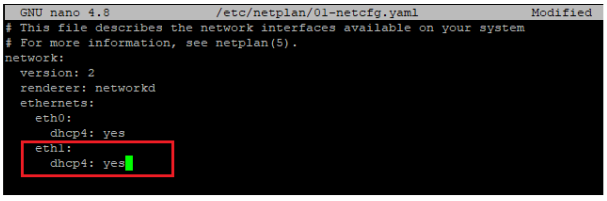
```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type access
[SwitchA-GigabitEthernet0/0/1] mac-address learning disable
[SwitchA-GigabitEthernet0/0/1] lldp disable
[SwitchA-GigabitEthernet0/0/1] quit
```

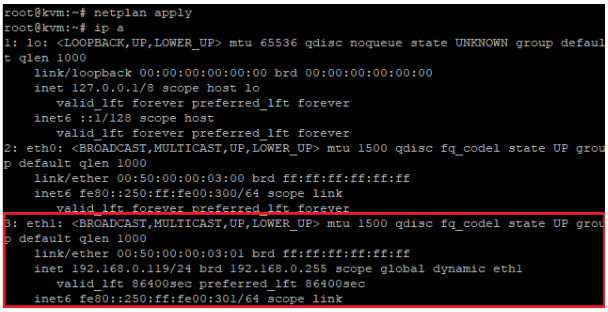
- Switchler üzerinde VLAN trafiklerini test etmek için switch üzerinde VLANIF tanımları yapılabiliyor (**Bir switch üzerinde birden fazla VLANIF tanımı yapılması durumunda bu VLAN'lar aralarında haberleşecektir. Dikkatli OL!!!**). Bu durum eğer ki SSH tanımında erişim için kaynak arayüz "**ssh server-source all**" komutuyla All olarak ayarlanması durumunda farklı VLAN'lardan da switche erişim sağlanabilecektir. Bunun önüne geçmek için "**ssh server-source –i <MGM VLAN Interface>**" komutuyla sadece MGMT olarak belirlenen VLAN üzerinde SSH yapılabilmesi sağlanmalıdır.

```
<SwitchA> system-view
[SwitchA] ssh server-source -i vlanif100
```

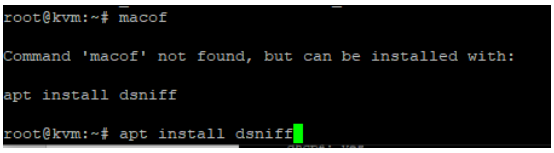
Notlar

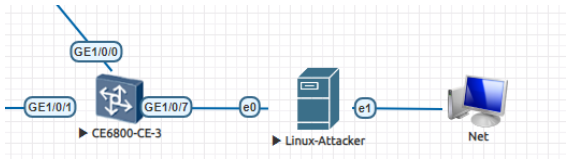
- Ubuntu server üzerine **Macof** aracını yüklemek için;
    - İlk olarak sunucunun internete erişimi sağlanmalıdır. Bunun için Eve-ng üzerinde "Mouse Left Click – Network – Type:Management(Cloud0)" yolu izlenerek bir network tanımı eklenmelidir. Bu tanım sunucunun NAT'lanarak internete çıkmasını sağlayacaktır.
    - Ubuntu Server açıldığında DHCP sunucusundan ip almasını sağlamak için "**/etc/netplan/01-netcfg.yaml**" dosyası içinde "**eth1:**" komutuyla internete çıkacak arayüz tanımı yapılıp "**dhcp4: yes**" komutuyla DHCP'den ip alacağı tanımlandıktan sonra komut satırı üzerinde "**netplan apply**" komutuyla tanımlanan değişikliklerin uygulanması sağlanmalıdır.





- Herhangi bir ip adresine Ping atılarak internet erişimi kontrol edildikten sonra "**apt install dsniff**" komutuyla Macof aracı yüklenebilir.





- Ubuntu sunucu üzerinde herhangi bir arayüzüne hızlıca statik ip adresi atayabilmek için "**ip addr add <Ip Address> /<Prefix Length> dev <Interface Id>**" komutu kullanılabiliyor. Ek olarak "**ip route add <DG Address> dev <Interface Id>**" komutuyla Default Gateway tanımı da yapılabiliyor.

Kontrol Komutları

- Display port-security interface <Interface Id>
- Display mac-address security {interface <Interface Id> | vlan <VLAN Id>}
- display dhcp snooping
- display arp snooping

Kaynaklar

- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178177/8770ce55/configuring-port-security
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178177/f077fec3/configuring-the-sticky-mac-address-function#dc_cfg_portsec_0010
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178177/90b07726/configuring-the-secure-mac-address-function#dc_cfg_portsec_0009
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178177/e7b747b0/example-for-configuring-port-security
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178165/834147df/vlan-configuration-commands
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000069520/bc91b28e/typical-dhcp-snooping-configuration
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178177/3e40f025/example-for-configuring-dhcp-snooping-attack-defense
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100127062/8a2874e3/enabling-dhcp-snooping
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100197672/5b04bc0b/dhcp-snooping-trusted
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1000178172/9c3a495a/example-for-configuring-port-isolation
- https[:]//support.huawei.com/enterprise/en/doc/EDOC1100276765/24689be5/configuring-the-arp-snooping-function
- https[:]//networklessons.com/spanning-tree/spanning-tree-topology-change-notification-tcn
- **https[:]//www.mustafakaya.com.tr/spanning-tree-protokolu-saldiri-ve-korunma-yontemleri.html**