1. AAA Protokolü nedir?
   1.1. Küçük networklerde AAA protokol yapılandırması,
   1.2. Büyük networklerde AAA protokol yapılandırması,
   1.3. AAA'de debug işlemi,
   1.4. TACACS+ ve RADİUS protokolleri ve aralarındaki farklar,

2. DHCP Güvenliği
   2.1. DHCP SNOOPİNG nedir?
   2.2. DHCP STARVATİON saldırısının network üzerindeki etkisi,
   2.3. DHCP SPOOFİNG saldırısının network üzerindeki etkisi,
   2.4. DHCP Saldırıları nasıl engellenir.
   2.5. DHCP SNOOPİNG Debug.

3. ARP Güvenliği
   3.1. ARP Nedir?
   3.2. ARP SAHTEKARLIGI (SPOOGİNG) saldırısının network üzerindeki etkisi.
   3.3. ARP İSTİLASI(FLOODİNG) saldırısının network üzerindeki etkisi.
   3.4. DİNAMİC ARP İNSPECTİON (DAİ) yapılandırması.

4. STP Güvenliği
   4.1. BPDU GUARD
   4.2. ROOT GUARD
   4.3. LOOP GUARD

AAA nedir

AAA aslında Authentication, Authorization, Accountining terimlerinin kısaltmasıdır. AAA layer2 ve layer3 ag cihazlarına erişim sırasında kullanılan hesabın Kimlik doğrulama, yetkilendirme ve hesabın yetki yönetimi konusunda bizlere yardımcı olmaktadır.

Ag cihazlarına erişimin 2 farklı yolu bulunmaktadır.

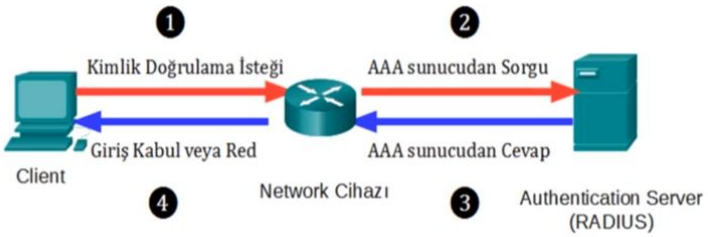
Birinci yöntem basit bir şifre doğrulamadır;

Konsol, Vty hattı ve aux portlarını korumak için şifre ve oturum açma hattı yapılandırma komutları kullanılır. Bu zayıf ve en güvenilmez yöntemdir ve hiçbir şekilde hesap yönetimi sağlanamamaktadır.

İkinci yolsa yerel veritabanı doğrulama;

Yerel cihazın veri tabanında tutulan ve username secret password gibi komutlarla oluşturulmuş olan accountlardır. Bir saldırganın password haricinde username bilgisini bilmesi gerektiği için bu yöntem cihazların erişiminde ekstra bir güvenlik sıkılaştırması olarak görülebilir. Username bilgisi daha sonra AAA'in Authorization, Accountining bölümlerinde bizler için vazgeçilmez bir data olacaktır.

Cisco cihazların desteklediği AAA protokolleri Radius ve Tacacs+ dır. Bu protokoller network içerisinde bir sunucu üzerine kurulumu gerçekleştirilir. Herhangi biri Radius veya Tacacs+ protokollerinin yapılandırılmış olduğu network cihazlarında, oturum açmak istediği vakit cihaz bu bu protokollerin kurulu olduğu sunuculara giderek kullanıcı adı ve passwordu doğrular ve oturum açma isteğine onay veya red verilir.



Küçük networklerde AAA protokol yapılandırması

R1(config)#username aaa algorithm-type scrypt secret deneme123
R1(config)#aaa new-model
R1(config)#aaa authentication login default local-case enable
R1(config)#aaa authentication login [**LİSTE**] / [**DEFAULT**] local-case

1. aaa authentication login enable
    - Enable şifresi ile giriş yapmamızı saglar username sormaz
2. aaa authentication login [**LİSTE**] / [**DEFAULT**] local
    - Cihazın DB üzerinden match olup oyle kabul eder

2.1. aaa authentication login [**LİSTE**] / [**DEFAULT**] local-case
    - Büyük küçük harf duyarlı olmakta
      (username: Tuna ise tuna yazman durumunda kabul görünmüyor)

2.2. aaa authentication login [**LİSTE**] / [**DEFAULT**] none
    - Herhangi bir kimlik doğrulama olmaz (Güvenlik sebebiyle önermiyoruz)

2.3. aaa authentication login [**LİSTE**] / [**DEFAULT**] Radius
    - Radius server üzerinden doğrulama yapar (Büyük networklerde mantıklı)

2.4. aaa authentication login [**LİSTE**] / [**DEFAULT**] tacacs+
    - tacacs+ server üzerinden doğrulama yapar (Büyük networklerde mantıklı)

2.5. aaa authentication login [**LİSTE**] / [**DEFAULT**] group [group name]
    - Radius ve tacacs+ grup sunucularını kullanarak doğrulama yapabiliriz.

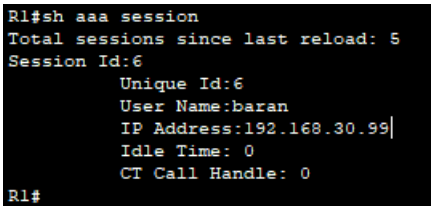
R1(config)#line vty 0 4
R1(config-line)#login authentication [**LİSTE**] /[**DEFAULT**]
R1(config-line)#exi

R1(config)#line console 0
R1(config-line)#login authentication [**LİSTE**] /[**DEFAULT**]
R1(config-line)#do wri

Session Bilgileri:

R1#sh aaa session

aaa session ları hakkında bilgi verir



Büyük networklerde AAA protokol yapılandırması

Bu yapılandırmadan önce bir Radius server kurulumu yapılması gerekmektedir ve bağlantı alacak olan cihazın Radius veya Tacacs+ server üzerinde tanıtılması şarttır aksi halde SSH veya Telnet üzerinde session time out olacaktır.

Radius server bilgilerim:

Server ip addres: **192.168.30.100**

Secret key: **cisco**

Client İp: **192.168.30.1**

NOT:Network cihazlarının bulundukları vlanlarındaki gateway bilgisini yazıyoruz

(Ben topolojimde roas yapısını kullanmıştım switch ve routerlar vlan 30 da 192.168.30.0 networkünde bulunmaktaydı bu networkün gateway bilgisi 192.168.30.1 dir)

Radius yapılandırması:

Router(config)#aaa new-model
Router(config)#radius server RADİUS-SERVER

Router(config-radius-server)#address ipv4 192.168.30.100

Router(config-radius-server)#key cisco

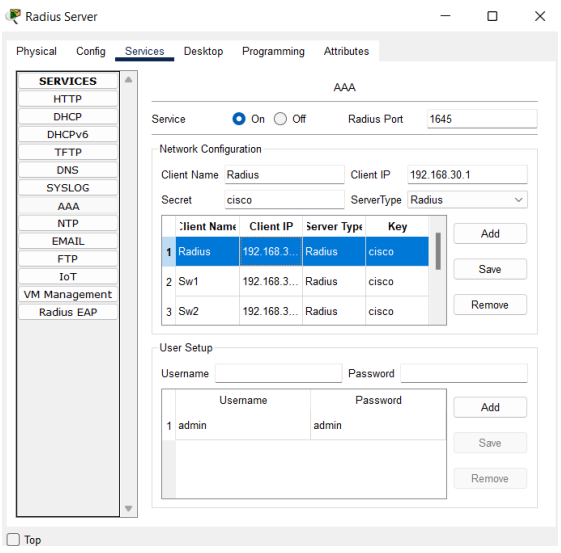
Router(config-radius-server)#exi

Router(config)#aaa authentication login default group radius local-case

Router(config)#line vty 0 4
Router(config-line)#login authentication default

Router(config-line)#exi

Router(config)#line console 0
Router(config-line)#login authentication default
Router(config-line)#do wri



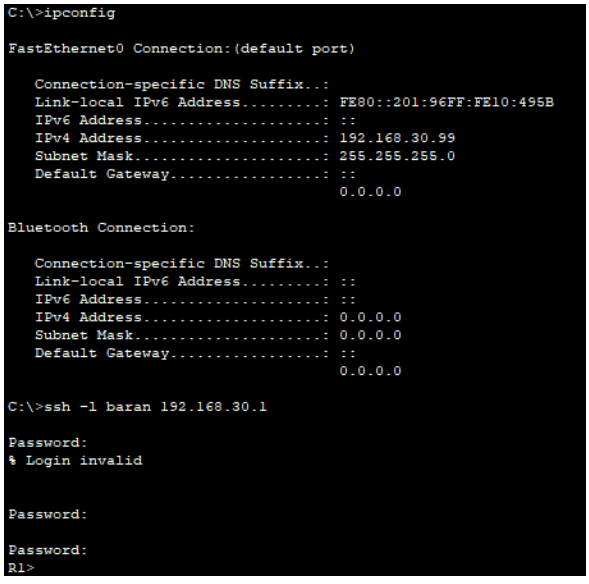
```
kenarswl(config)#aaa new-model
kenarswl(config)#radius server RADUS-SERVER
kenarswl(config-radius-server)#address ipv4 192.168.30.100
kenarswl(config-radius-server)#key cisco
 WARNING: Command has been added to the configuration using a type 0 password. However,
type 0 passwords will soon be deprecated. Migrate to a supported password type
*Jul 15 02:23:03.394: %AAAA-4-CLI_DEPRECATED: WARNING: Command has been added to the
configuration using a type 0 password. However, type 0 passwords will soon be deprecated.
Migrate to a supported password type
kenarswl(config-radius-server)#exi
kenarswl(config)#aaa authentication login default group radius local-case
kenarswl(config)#line vty 0 4
kenarswl(config-line)#login authentication default
kenarswl(config-line)#exi
kenarswl(config)#line console 0
kenarswl(config-line)#login authentication default
kenarswl(config-line)#do wri
Building configuration...
[OK]
kenarswl(config-line)#do wri mem
Building configuration...
[OK]
```

DEBUG İşlemi

R1#debug aaa authentication

Resim 1:

Resim 1 de 192.168.30.99 ip verdiğimiz bir client cihazdan routerımıza ssh üzerinden erişiyoruz, bu authentication işlemi sırasında router cihazımıza gelen logları resim 2 de görebilirsiniz.



Resim2 :

User bilgisi: baran

Source ip: 192.168.30.99

Tarih / Saat: 11 Temmuz 9:31

Login Failed

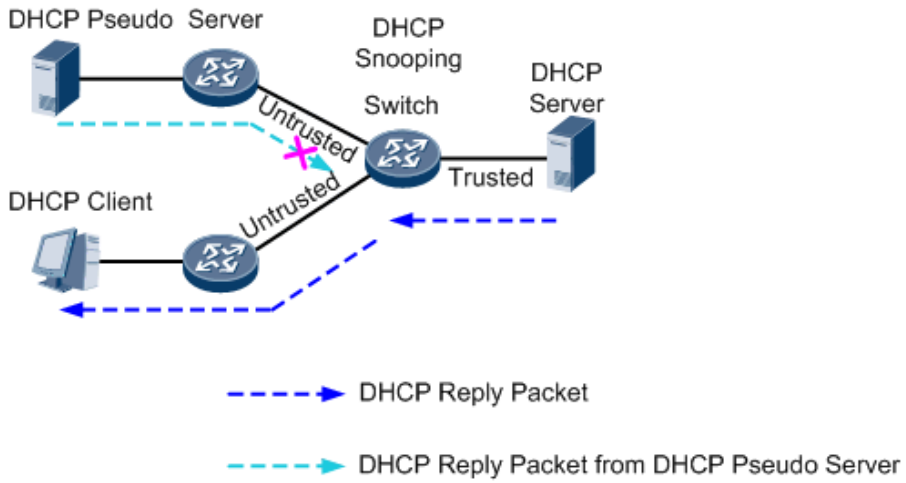
```
*Tem 11 09:31:45.917: AAA/BIND(3): Bind i/f

*Tem 11 09:31:45.917: AAA/AUTHEN/LOGIN(3): Pick method list 'aaa'
%SEC_LOGIN-5-LOGIN_FAILED: Login failed [user: baran] [Source: 192.168.30.99] [localport:
22] [Reason: Login Authentication Failed] at 21:39:45 UTC Sun Jul 10 2022
```

TACACS+ ve RADİUS protokolleri ve aralarındaki farklar

Özellikler	TACACS+	RADİUS
Kullanan profil	Ağ cihazları	Kullanıcılar
Taşıma sırasında kullandıkları protokoller	TCP	UDP
Kimlik doğrulama portu	49	1645,1812
Protokol parolayı şifreler mi	Evet	Evet
Protokol trafiği şifreler mi	Evet	Hayır
Her kullanıcıya ayrı yetki verebilir miyiz	Evet	Hayır
Tanımlayan	Cisco	RDC 2864

Radius protokolü AAA tek bir modül olarak alır ve erişim talebini onayladığı her kullanıcı ağ cihazlarına privilege 15 (admin) olarak bağlanır ancak bu konu TACACS+ için böyle işlememektedir. Tacacs+ onayladığı her accounta ayrı yetki verebilir, bir kullanıcı enable moddayken configure terminal komutu yazdığı zaman network cihazı TACAS+ sunucusuna yetki için sorgu gönderir ve bu trafik TCP üzerinden şifreli bir şekilde gerçekleşmektedir. Radius server da giriş doğrulama işlemi UDP protokolü ile yapılır trafik şifrelenmez sadece account'un password kısmı şifrelenir. Username bilgisi dahil olmak üzere diğer bilgiler şifrelenmeden Radius Server gönderilmektedir.

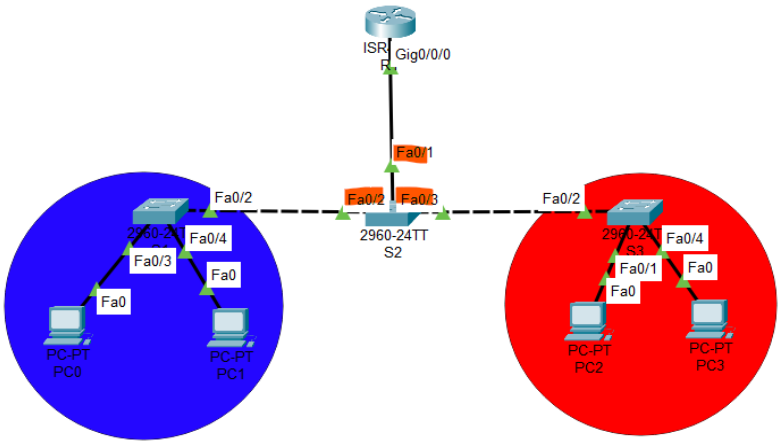
DHCP SNOOPİNG nedir



Öncelikle Baran DHCP SNOOPİNG protokolünü mahşerin 3 atlısının 2 li hali olarak düşün.

Dhcp Snooping dendiği zaman port securtiy aklına gelsin çünkü ikisini aynı LAN üzerinde kullandığın zaman

- **DHCP STARVATİON ATTACK**
  - Açlık saldırısı olarak aklında kalsın, bir hostun sahte maclerle tüm ip blogunu tüketmesi;
- **DHCP SPOOFİNG ATTACK**
  - Bir cihazın içerisinde dhcp server kurulur ve networke ip dağıtır boylelikle LAN trafiği 3. Kişinin üstünden geçer.



Router 0:

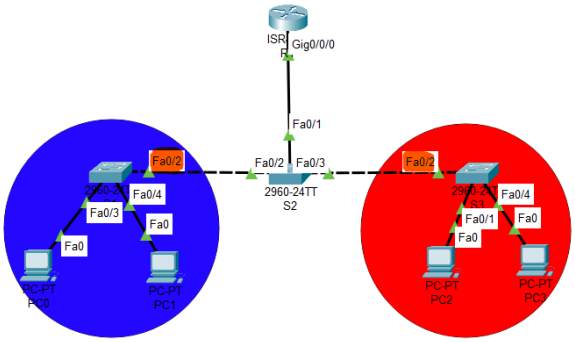
Routerımız bu topolojide aynı zamanda bir DHCP server görevi görmektedir. Tüm Dhcp talepleri R1 cihazına gelir ve R1 cihazı Local agımıza bağlanan her cihaz ip havuzundan uygun ipleri atar. DHCP snooping protokolü switchlerin configure kısımında etkinleştiriliyorken tüm ayarları swtichlerin port kısımlarında yapılmaktadır.

S2 Switch:

```
s2(config)#ip dhcp snooping
s2(config)#int range fa0/1-3
s2(config-if-range)#ip dhcp snooping trust
s2(config-if-range)#do wri
Building configuration...
[OK]
s2(config-if-range)#
```

Bu Switch'e Dhcp istekleri trunk portlar üzerinden geleceklerdir fa0/2, fa0/3 bu yüzden networkümüzün mavi kısmına bakan fa0/2 ve kırmızı kısmına bakan fa0/3 portlarına DHCP istekleri gelmesi durumunda kabul et demek için fa0/2 ve fa0/3'ü trust olarak işaretliyoruz. fa0/1 ise routera paket ulaştırıldığında ip alarak geri dönen paketin drop olmaması için portu trunk olarak çalıştırıp, trust olarak işaretlememiz gerekmektedir.

S1 swtich (Mavi taraf)



S2 Switch in fa0/2 portunu kullanarak S1 switchin fa0/2 portuna gelen paketlerin drop olmaması için S1 switchin fa0/2 portunuda trust olarak işaretlememiz gereklidir. Bunun sebebi S1 switchin boşta olan bir portuna DHCP server gibi davranan bir cihazın bağlanıp S1 switchine connect olan tüm cihazlara DHCP spoofing saldırısı yapabilmesine olanak sağlamasıdır.

S1 switchin fa0/3-4 portlarında client cihazlarımız baglıdır bu portları trust olarak işaretlemek güvenlik zafiyetine sebeb olacaktır. Bu sebeple yaratılacak olan trafiğini sınırlandırarak portlardan gelecek olan DHCP isteklerini kabul ediyoruz. Tanımladığımız ip DHCP snooping limit rate komutu saniye başına alınabilecek DHCP discovery iletisini sınırlandırarak DHCP STARVATİON saldırısını engellemiş oluruz.

```
s1(config)#ip dhcp snooping
s1(config)#int fa0/2
s1(config-if)#ip dhcp snooping trust
s1(config-if)#int range fa0/3-4
s1(config-if-range)#ip dhcp snooping limit rate 6
s1(config-if-range)#exi
s1(config)#ip dhcp snooping vlan 10,20
s1(config)#
```

S3 Switch (Kırmızı taraf)

Aynı ayarlar kırmızı taraf içinde geçerli olmaktadır;

Dipnot: Topolojideki portların değişmesi durumunda ayarların yazılacağı portların değişiklik göstermesi gerekmektedir.

DHCP SNOOPİNG aktif olup olmadığını aşağıdaki resimden görebilirsiniz.

```
sl(config)#do sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
none
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/2            yes        unlimited
sl(config)#
```

ARP NEDİR

Address Resolution Protokol

Arp protokolü yerel ağda IP addresi bilinen cihazların mac adresini bulmak için kullanılır.Layer 2 haberleşmesinde cihazlar birbirleri arasındaki iletişimi mac adreslerini kullanarak kurarlar.Eğer local networkde bir cihaz gitmek istedigi cihazın mac adresini bilmiyorsa ARP protokolünü kullanarak destination tarafındanki mac adresini ögrenmektedir.

ARP SAHTEKARLIGI (SPOOGİNG)

ARP spoofing'de saldırganın mac adresi, ARP paketlerinde kurbanın IP adresiyle birleştirilir ve yönlendirici, PC'nin birbirleri yerine saldırgana bağlanmasına neden olur.

ARP spoofing saldırısında siber suçlular, yerel alan ağını sahte ARP paketleriyle doldurur. Bu manipülasyonun ardından, tüm trafik, hedeflenen varış yerine ulaşmadan önce saldırganın bilgisayarına yönlendirilir. Üstüne üstlük, saldırgan verileri gerçek alıcıya iletmeden önce bozabilir veya tüm ağ iletişimini durdurabilir.

ARP İSTİLASI(FLOODİNG)

Mac Adres Taşması (MAC Flooding), ağı aktif olarak dinleme yöntemlerinden biridir. Atak yapan bilgisayarın hızlı bir şekilde gönderdiği binlerce mac (Media Access Control – Ortam Erişim Kontrolü) adresi ile switchin sahip olduğu mac adres tablosu doldurur bu olay Mac Flooding olarak adlandırılır. Bu durum iletişim ortamında güvenliğin sağlanamaması, ağ hızının düşürülmesi gibi sorunlara sebep olur.

Atak yapan bilgisayar tarafından anahtarlayıcıya hızlı bir şekilde art arda sahte mac adresleri gönderilir. Hafızası dolan anahtarlayıcı çoklayıcı (hub) mantığı ile çalışmaya başlar. Yani anahtarlayıcı, üzerine gelen ağ trafiğini sadece iletişime geçeceği bilgisayara değil, atağı gerçekleştiren bilgisayar dahil ağdaki tüm bilgisayarlara gönderir.

DİNAMİC ARP İNSPECTİON (DAİ)

ARP Zehirlemeleri ve buna karşı Ortadaki Adam Saldırılarını Switch tarafında önleyebilecek bir yapılandırmadır.

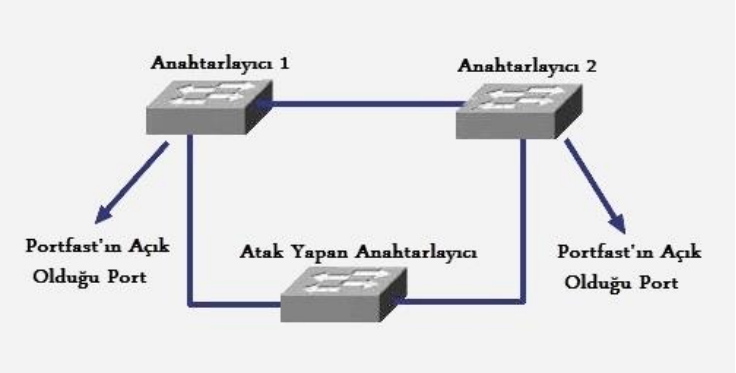
Fakat bu yapılandırmayı uygulayabilmek için mutlaka DHCP Snooping yapılandırmasını yapmak zorundayız. Bunun sebebi ARP Inspection, DHCP Snooping veri tabanını kullanmasından kaynaklıdır. DHCP Snooping burada hangi MAC adresi hangi IP adresini aldığını kendi veri tabanında tutar ARP Inspection da buna bakarak çalışır.

NOT: Default olan bir networkte aktif olan vlan 1 dir bu yüzden komutun normal yazımı;

İp arp inspection vlan 1 dir ancak kullandığım topoloji üzerinde 10, 20, 30 vlanları aktif durumdayken vlan 1 shutdown durumunda bulunmaktadır.bu sebeble DAİ protokolünü vlan 10, 20,30 için aktif ettim

```
kenarswl(config)#ip arp inspection vlan 10,20,30
kenarswl(config)#int range fa0/4-7
kenarswl(config-if-range)#ip arp inspection trust
kenarswl(config-if-range)#do wri
Building configuration...
[OK]
kenarswl(config-if-range)#do wri mem
Building configuration...
[OK]
kenarswl(config-if-range)#exi
kenarswl(config)#
```

BPDU GUARD



Bdpu paketi içerlerinde BRİDGE id değeri taşımaktadırlar. Eğer ki kral switchden gelen BDPU paketleri client tarafa ulaşırsa wiresshark üzerinden dinleme yapan 3. şahıs bizim BDPU paketlerimize ulaşabilir bu durumda *priority* ve mac adres bilgilerimize ulaşıp kendi *priority* değeriyle oynayarak cihazını local networkteki yeni kral switch olarak yapılandırma imkanını elde etmiş olur.

(Yedekli networkte tüm trafik kral switch üzerinden geçtiği için wiresshark açan 3. Kişi tüm trafiği dinleme imkanı bulacaktır)

Switch(config)#int range fa0/1-7
Switch(config-if)#spanning-tree bpduguard enable
Switch(config-if)#exi

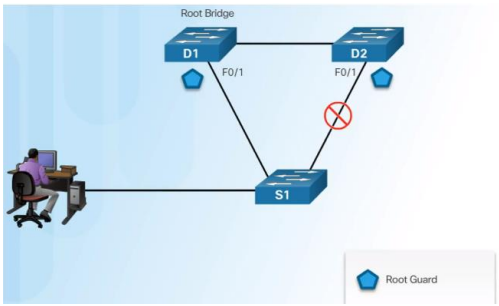
Ya da, global configuration mode içindeyken bu komutu yazarak aktive edebilirsiniz.

Switch(config)#spanning-tree portfast bpduguard default ***PT desteklemez*

-Dipnot: Bpdu guard sadece client cihazların bulunduğu portlara uygulanması gerekmektedir.

-Dipnot: Portfast sadece access portlara uygulanır yani clientların olduğu tarafa ama portfast uygulanan portlara bir gün switch veya hup takılma ihtimaline karşı Bpdu guard vakit kaybetmeksizin uygulanması gerekmektedir

ROOT GUARD



Root Guard yedekli şekilde çalışan networkünüze yanlış konfigüre edilmiş bir switch'in bağlanması sonucu Root Bridge değişimini engellemektedir. Root Guard yalnızca trunk portlar üzerinde aktif hale getirilmelidir. Root Guard, Root switch üzerindeki portlardan, sadece hattın diğer ucundaki switchlerin root seçilmemesi gerektiğinden emin olunan switchler için aktif duruma getirilir. Eski switchlere bağlanan portlarından, daha düşük priority ile Root Bridge olmak isteyen yeni bir switch görürse Root Guard, bu paketi aldığı portu "incostintent port" olarak işaretler ve kapatır. Böylece yanlışlıkla bir switch'in Root Bridge seçilmesini engellenmiş olur.
Aşağıdaki komutla port bazında Root Guard 'ı açabilirsiniz.

- Dipnot: Trunk portlara yap
- Dipnot: İstersen sadece Root Switch portlarına tanımla yada resimdeki gibi de tanımlayabilirsin

Switch(config)#int fa0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#exi

LOOP GUARD

Bir spanning tree portu BPDU mesajlarını almayı durdurduğu zaman networkte loop oluşmaktadır. Spanning Tree loop guard özelliği katman 2 döngülerine karşı ek güvenlik sağlıyor.

- Dipnot: Root guard tanımlamadığın tüm trunk portlarda loop guard tanımla.
- Dipnot: Port fast ile aynı port da kullanılmamalıdır.

Switch# configure terminal
Switch(config)# spanning-tree loopguard default
Switch(config-if)#exi

Ya da sadece bir porta;

Switch# configure terminal
Switch(config)#int fa0/1
Switch(config-if)#spanning-tree guard loop

Switch(config-if)#exi