STP Protect Mechanizm

STP protokolünde bir saldırganın bilgisayarıyla bir switche bağlanılıp BPDU paketleri göndererek topolojide seçilen Root Bridge'in sürekli değişmesini sağlayabilmektedir (bu ihtimal CCNA notlarında da bahsedilmişti). Bu durumda sürekli Root Bridge seçimi yapılması sağlanarak protokol meşgul ediliyor ve trafik akışı engellenebiliyor (veya doğru şekilde konumlanırsa trafiği kısmen de olsa dinleyebiliyor). Bu saldırıya karşı önlem olarak istemci bağlanan portlarda BPDU Guard koruması açılabiliyor. Bu korumaya ek olarak Root Bridge'in değiştirilmesine karşı Root Guard koruması da kullanılabiliyor. STP protokolünde kullanılabilen bu ve benzeri koruma mekanizmalarına bakıldığında;

1- STP Root Guard

Root Guard koruması, Root Bridge'e daha düşük Bridge ID değerine sahip (yani Root Bridge olmayı talep eden switchlere karşı) BPDU paketi gönderilmesine karşı önlem olarak portun bloklanmasını (**Inconsistent State**) sağlayan korumadır. Bu korumayı devreye almak için portların arayüzlerine girilerek "**spanning-tree guard root**" komutu kullanılıyor. Bu sayede Root Guard koruması açık olan porttan daha düşük Bridge ID değerine sahip BPDU paketi gönderildiği tespit edilirse switch bu portunu blokluyor. Bu sayede Root Bridge'e Bridge ID değeri düşük BPDU paketleri ulaşamıyor.

|→ Bu özellik daha çok Root Bridge'e doğru giden portlarda (Root Port) uygulanıyor.

2- STP PortFast – BPGU Guard

PortFast özelliği switchlerin istemci bağlanacak portlarında kullanıcıların 30 saniye beklemeden veri alışverişine başlayabilmesi için devreye alınan özellikti (Bu özelik sayesinde istemcilerin switche bağlandığında DHCP sunucusundan ip bilgileri alabilmesi da sağlanabiliyordu). Her ne kadar kullanıcı dostu görünse topolojide Loop oluşumuna neden olabiliyor.

PortFast özelliğinin devreye alındığı portlarda aynı zamanda BPDU Guard koruması açılsa da BPDU paketi BPDU Guard özelliği devreye alınan switch portuna gelene kadar geçen sürede oluşan Loop networkü çökertebiliyor. Bu nedenle PortFast özelliğinin kullanımına dikkat edilmesi gerekiyor.

PortFast konfigürasyonu için ilgili port arayüzüne girilerek "**spaning-tree portfast**" komutu kullanılıyor. Eğer ki Access moduna (VLAN'larda istemci bağlanacak portlar için kullanılıyordu) alınan portların tamamında PortFast özelliği devreye alınmak isteniyorsa Global konfigürasyon modunda "**spanning-tree portfast default**" komutu kullanılıyor. PortFast özelliğini devre dışı bırakmak için "**no spaning-tree portfast**" veya "**spaning-tree portfast disable**" komutu kullanılıyor.

Normal şartlarda Trunk moduna alınan portlarda PortFast özelliği açılamıyordu. Eğer ki Trunk portlarda da PortFast özelliği açılmak isteniyorsa ilgili portun arayüzüne girilip "**spanning-tree portfast trunk**" komutu kullanılarak açılabiliyor (Daha çok sanallaştırma yapılan sunucular için kullanılıyor. Üzerinde birçok sanal makina bulunacağı için birçok VLAN trafiği tek kablo üzerinde taşınması gerekiyor. Bu nedenle port Trunk moduna alınıyor. Port Trunk modunda da olsa ucunda sunucu bağlıdır. Sunucu bekletilmek istenmediği durumlarda kullanılabiliyor).

3- BPDU Guard

BPDU Guard özelliği porta bir BPDU paketi geldiğinde portun Err_Disable'a alınmasını sağlayan özelliktir. PortFast özelliği devreye alınan portlarda BPDU paketlerinin gönderilmesini önlemek için kullanılır. Switch üzerinde PortFast özelliği açılan bütün portlarda BPDU Guard korumasını devreye almak için Global konfigürasyon modunda "**spanning-tree portfast bpduguard default**" komutu kullanılıyor. Belirli bir arayüzde BPDU Guard özeliğini devreye almak için "**spanning-tree bpduguard (enable | disable)**" komutu kullanılıyor.

BPDU Guard korumasının devrede olduğu porta BPDU paketi geldiğinde port Err_Disabled (bu porta gelen trafikler Drop ediliyordu) oluyordu. Normal şartlarda portun tekrar kullanılabilir duruma getirilebilmesi için yönetici tarafından manuel olarak portun kapatılıp yeniden açılması gerekiyordu. Bunun yerine portun belirli bir süre sonunda kendiliğinden açılabilmesi "**errdisable recovery cause bpduguard**" ve "**errdisable recovery intervar <Time-Seconds>**" komutlarıyla sağlanabiliyor. Normalde birçok nedenden dolayı port Err_Disable olabilir ama komutlardan da anlaşıldığı gibi sadece BPDU Guard korumasından kaynaklı kapanan portlar için tanımlanıyor. Bu işlem farklı nedenlerden dolayı Err_Disable durumuna geçen portlar için de kullanılabiliyor (Detaylar için → https[:]//www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html).

4- BPDU Filter

BPDU paketlerinin gönderilmesi de alınması da istenmeyen portlarda devreye alınan özelliktir. Dikkatli kullanılması gerekiyor çünkü devreye alındığı portlarda Loop oluşma ihtimali doğuruyor. Bu özelliği port bazında devreye alabilmek/devre dışı bırakabilmek için ilgili portun arayüzüne girilerek "**spanning-tree bpdufilter (enable | disable)**" komutu kullanılırken switch üzerinde Access moduna alınan bütün portlarda uygulanması isteniyorsa Global konfigürasyon modunda "**spanning-tree bpdufilter default**" komutu kullanılıyor.

|→ "**spanning-tree bpdufilter default**" komutu kullanıldığında BPDUFilter özelliği hemen devreye girmiyor. Önce portlardan birkaç BPDU paketi gönderiyor. Eğer ki gönderdiği BPDU paketine karşılık geldiğini görülürse BPDUFilter özelliği devreye alınmıyor (BPDUFilter özelliği sadece bir arayüze uygulanıyorsa bu durum geçerli değil. BPDUFilter özelliği doğrudan devreye alınır).

Unidirectional Link

Fiber Optik kablolarda, cihazlar arasında veri aktarını için kullanılan bir gidiş, bir dönüş (karşı cihazdan gönderilen) olmak üzere iki bağlantı vardır. Bu bağlantılardan biri koptuğu zaman taraflardan biri veri gönderememektedir. Buna **Unidirectional Link** denilmektedir. Bunu daha rahat açıklayabilmek adına SW1 ve SW2, aralarında Fiber Optik ile bağlanmış iki cihaz olarak düşünelim. SW1, SW2'ye veri gönderebilse de SW2'den SW1'e veri göndermek için kullanılan bağlantı koptuğu için SW2'den SW1'e herhangi bir paket gönderilemiyor. Bu durum tespit edilip düzeltilmediği takdirde SW1 veri göndermeye devam edecektir ama SW2 SW1'e BPDU paketi de gönderemediği için SW1 SW2'ye olan bağlantının koptuğunu düşünerek (Max Age süresini bekledikten sonra) STP ile bloklanan portunu da devreye alacaktır. Bu durumda SW1'den SW2'ye aynı anda iki bağlantı üzerinden veri gönderilecektir. Bu durum Loop oluşmasına neden olacaktır.

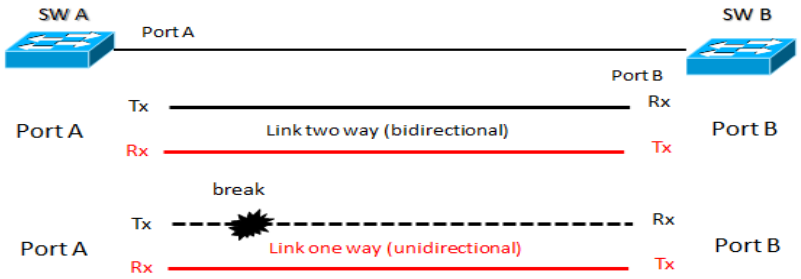
Unidirectional Link tespit edilip bloklanabilmesi için kullanılabilecek iki alternatif çözüm bulunmaktadır. Bu çözümler;

1- STP Loop Guard koruması ile switchler arasındaki bağlantıda bir tutarsızlık olduğu tespit edilerek (switchden BPDU paketi gönderilebiliyorken – yani bağlantı var görünüyorsa- karşı switchden BPDU paketi gelmiyorsa) portların bloklanması sağlanabiliyor. **STP Loop Guard** konfigürasyonu (karşılıklı her iki porta da uygulanması gerekiyor) belirli bir porta uygulamak için "**spanning-tree loopguard**" komutu kullanılırken, switch üzerinde bulunan portların tamamına uygulamak için Global konfigürasyon modunda "**spanning-tree loopguard default**" komutu kullanılıyor. STP Loop Guard korumasıyla bloklanan portları "**sh spaning-tree inconsistent-ports**" komutuyla görüntülenebiliyor.

2- **UDLD** (Unidirectional Link Detection), Cisco tarafından geliştirilmiş bir çözümdür. Portların karşılıklı olarak birbirlerine belirli periyotlarda Hello paketleri (L2) göndererek ayakta olduklarını bildirdikleri bir özelliktir. UDLD özelliği Enable ve Aggressive olmak üzere iki modda açılabiliyor.
   - **Enable**, Undirectional Link tespit edildiğinde bu durum sadece kayıt altına alınır (loglanır). Bu durum için herhangi bir aksiyon alınmaz.
   - **Aggressive**, Undirectional Link tespit edildiğinde link doğrudan bloklanır (Inconsistent State).

   UDLD özelliği port bazlı açılmak istendiğinde ilgili portun arayüzüne girilerek "**udld port aggressive**" komutu, switchdeki bütün portlarda açılmak isteniyorsa "**udld (enable | aggressive | message time <Time>)**" komutu ("**message time**" komutuyla bağlantılar arası kullanılan Hello paleterinin sıklığı da ayarlanabiliyor. Varsayılanda 15 saniye geliyor), herhangi bir portta devre dışı bırakılmak isteniyorsa "**udld port disable**" komutu kullanılıyor.

   Undirectional Link tespit edilip port bloklandıktan belirli bir süre sora otomatik olarak kontrol edilmesi ve bir düzelme olması durumunda portun tekrar açılması isteniyorsa "**udld recovery interval <Time>**" komutu kullanılıyor (Detaylı bilgi için https[:]//www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swudld.pdf).



Terminolojiler

- **Inconsistent State**, Root Guard koruması devreye alınmış switch portundan Root Bridge'den daha yüksek Bridge ID değerine sahip BPDU paketleri gönderene kadar portun bloklandığı durumdur. Bu porttan Root Bridge'den daha düşük Bridge ID değerine sahip BPDU paketleri gönderilmeye başlandığında port tekrar devreye alınır.

Kontrol Komutları

- sh spaning-tree inconsistent-ports