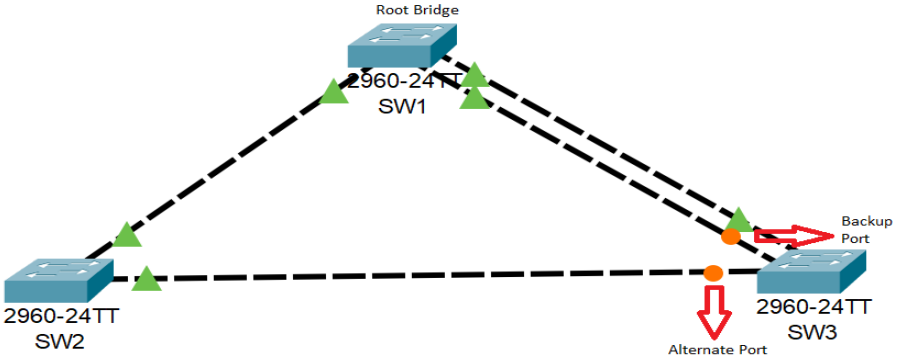
RSTP

802.1D protokolünde yedek (bloklanmış) bağlantıya geçiş süresi çok uzun (30 sn) sürmektedir. Bu süreyi kısaltmak için IEEE tarafından RSTP protokolü (2sn) geliştirilmiştir. Yeni model switchlerde varsayılanda RSTP protokolü aktif gelmektedir.

İki switchi birbirine bağlanıyorsa ve switchler aralarında RSTP protokolü çalışıyorsa switchler 2 saniye içerisinde veri iletimine başlar. Eğer ki switch portuna bir istemci veya hub bağlanıyorsa bu durumda port üzerinden veri iletimine başlayabilmek için yine 30 saniye beklemek gerekiyor. RSTP protokolüde 4 farklı port durumu bulunuyor. Bu durumlara bakıldığında;

- Root Port, Root Bridge'e giriş yönünde olan portlara verilen isimdir.
- Designated Port, Root Bridge'den çıkış yönünde olan potlara verilen isimir.
- Alternate port, Root Bridge'e alternatif bir switch üzerinden gidiliyorsa (bloklanmış) kullanılan isimdir.
- Backup port, Root Bridge'e giden bağlantı aynı switch üzerinden çıkıyorsa (bloklanmış) kullanılan isimdir (Genelde böyle durumlarda EtherChannel konfigürasyonu yapılır).

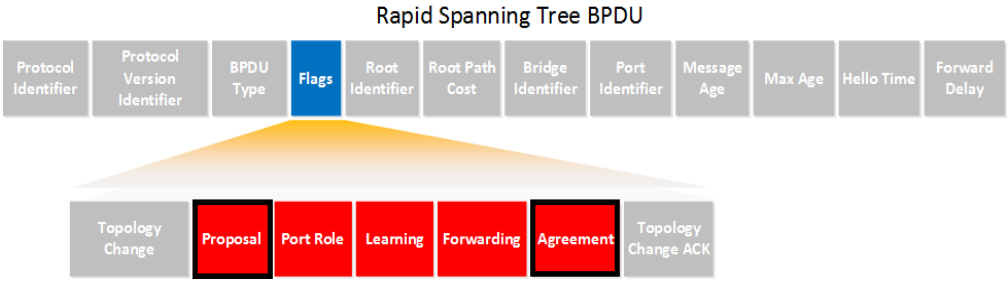


RSTP protokolünün hızlı olmasının nedeni STP protokolünde bulunmayan onay mekanizmasının olmasıdır. Cihazlar birbirine fiziksel olarak bağlandıktan sonra BPDU paketi içerisinde Proposal ve Agreement bitleri kullanılarak paketin karşı switche ulaşıp ulaşmadığı kontrol ediliyor. Paket alışverişi (bilgi) yapıldıktan sonra Loop olmadığı anlaşılır ve portlardan veri aktarılmaya başlanır.

- RSTP protokolünün çalışabilmesi için portların Full-Duplex bağlantı olması gerekiyor.
- Discarding, RSTP protokolünde bloklanan portlara verilen isimdir. Forwarding, veri aktarılan aktif portlara verilen isimdir.

Switch portuna istemci bağlandığında istemciden RSTP onay (BPDU) paketi gelmeyeceği istemci veri alışverişi için 30 saniye Listening durumda bekleyecektir. Bu süre içersinde MAC adreslerini öğrenmeye başlıyor.

- RSTP'de Port-Fast özelliği vardır. İsteğe bağlı istemci bağlanacak portlarda konfigüre edilebilir.



RSTP Protokolünde 3 farklı port tipi/rolü bulunuyor. Bunlar;

- Edge Port, PortFast özelliğinin açık olan portlar için kullanılıyor.
- Root Port, Root Bridge'e giden port için kullanılıyor.
- Point-to-Point port, portun FullDuplex çalıştığını gösterir.
- Shared port, ucuna hub bağlanan portlar için kullanılan tanımdır. Bu portlarda RSTP protokolü özelliklerini kaybederek standart STP gibi çalışıyor.

STP Root Bridge ve Backup Root Bridge Seçimi (RSTP - Rapid-PVST)

STP protokolünde topolojide hangi switchin Root Bridge seçildiği önemlidir. Bu nedenle bu seçimin kontrol altında yapılması istenir. Root Bridge seçilen router devre dışı kaldığında ise yeni Root Bridge seçiminin de kontrol altında yapılabilmesi için iki seçenek vardır.

- İlk seçenek switchierin priority değerleriyle oynanarak Root Bridge switch seçilmesi istenen switchlere "**spanning-tree vlan <VLAN ID> priority <Priority Value>**" komutuyla daha düşük öncelik değerleri atanmalı (örnek olarak ilk switchde 0, ikinci/yedek olması istenen switchde 4096 Priority değeri atanabilir).
    - Her VLAN için farklı switch Root Bridge seçilebilir. Komutta da görüldüğü gibi komutlar VLAN özelinde yazılıyor.
- İkinci seçenek olarak Root Bridg ve yedek Root Bridge seçilmesi istenen switchlerde "**spanning-tree vlan <VLAN ID> root (Primary | Secondary)**" komutu kullanılarak Root Bridge seçimine müdahale edilebilir.
    - Bu komutun kullanıldığı switchlerde Primary seçiminde switchin Priority değeri 24576, Secondary seçiminde ise Priority değeri 28672 olarak belirleniyor. Eğer ki topoloji üzerinde Priority değeri 24576'dan daha düşük (örneğin 4096) bir switch varsa bu durumda Primary seçilen switchin Root Bridge seçilebilmesi için düşük Priority değerine sahip switchden (4096) daha düşük bir değere kadar çekiyor (Bu durum Secondary seçilen switch için geçerli değil. Secondary seçilen switch için Priority değeri sabit kalıyor).

Bir topolojide birbirine en uzak (arada bulunan switch sayısı olarak) iki switch arasıda kullanılan toplam switch sayısına diameter deniliyor. Bu değer kullanılarak timer'ların optimize edilebilmesi sağlanıyor. Root Bridge ve Backup Root Bridge seçiminde diameter belirtilebiliyor. Diameter belirleme işlemi için "**spanning-tree vlan <VLAN ID> root (primary |secondary) diameter <Diameter>**" komutu kullanılıyor.

Port Seçimi

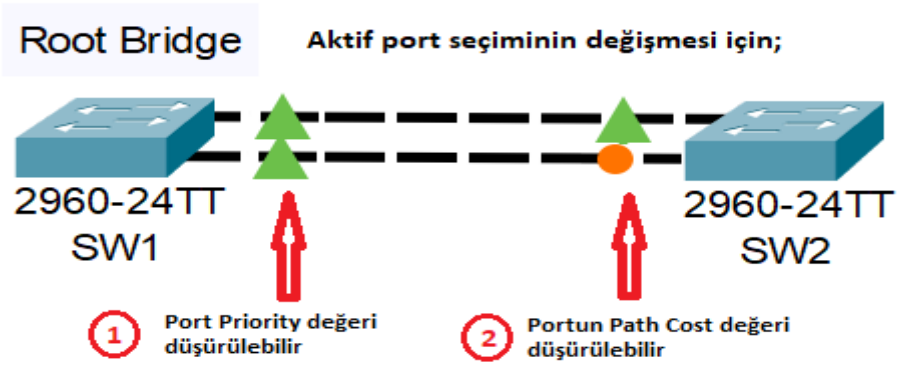
STP protokolünde switch portlarının Path Cost değerleri ile oynanarak aktif port seçilmesi veya bloklanması istenen portlar kontrol edilebiliyor. Bu işlem için ilgili portun arayüzüne girilerek "**spanning-tree vlan <VLAN ID> cost <Cost Value>"** veya "**spanning-tree cost <Cost Value>"** komutu kullanılıyor.

Cost değeri (bant genişlikleri) aynı olan portlarda Cost değerleri değiştirilmeden port seçimine müdahale edilmek isteniyorsa bu durumda Global konfigütasyon modunda "**spanning-tree vlan <VLAN ID> port priority <Port Priority Value>**" veya "**spanning-tree port priority <Port Priority Value>**" komutuyla portların Priority değerleri değiştirilebiliyor. Bu sayede bloklanacak portlar

kontrol edilebiliyor (Daha düşük Priority değerine sahip port aktif seçiliyor - Detaylı bilgi için → https[:]//www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xe-3s/asr903/lanswitch-xe-3s-asr903-book/Spanning_Tree_Protocol.pdf).

|→ Path Cost değeri switchin kendisi tarafından belirlenen değerdir ve bağlı olunan switchlerle bu bilgi paylaşılmaz. Port Priority değeri ise BPDU paketleri içerisinde bağlı olunan switchler ile paylaşılıyor. Bu durumda Root Bridge'e doğrudan iki kablo ile bağlanan bir switch üzerinde (SW2) aktif port seçiminin değiştirilmesi isteniyorsa bunu gerçekleştirmenin iki yolu vardır.

- İlk seçenek Root Bridge (SW1) üzerinde ilgili portun Port Priority değeriyle oynanabilir. Port Priority değeri bağlanılan switchlere de iletileceği için bloklanan port doğrudan devreye alınır (Port Priority değeri Global konfigürasyon modunda uygulandığı için switchdeki bütün portların priority değerini düşürüyor).
- İkinci seçenek Root Bridge'e bağlı switch üzerinde (SW2) ilgili portun Cost değeriyle oynanabilir. Yani Cost değerleriyle sadece switch üzerindeki bloklanan portlara müdahale edilebiliyor. Her iki durumda da bloklanan port devreye alınacaktır.



Koruma Mekanizmaları

STP protokolünde bir saldırganın bilgisayarıyla bir switche bağlanıp 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 engelleniyordu (veya doğru şekilde konumlanırsa trafiği kısmen de olsa dinleyebiliyordu). Bu saldırıya karşı önlem olarak istemci bağlanan portlarda BPDU Guard koruması açılabiliyordu. Bu korumaya ek olarak Root Bridge'in değiştirilmesine karşı Root Guard koruması da kullanılabiliyor.

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 (Designated Port) uygulanıyor.

2- STP PortFast

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 ve 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 açılan bütün portlarda BPDU Guard korumasını devreye almak için Global konfigürasyon modunda "**spanning-tree portfast bpduguard default**" komutu kullanılıyor. Belirli bir arayüzde BPDU Guard özeliğiini devreye almak için "**spanning-tree portfast bpduguard default (enable | disable)**" komutu kullanılıyor.

BPDU Guard korumasının devrede olduğu porta BPDU paketi geldiğinde port ERRDisabled (kapanıyor) 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 ERRDisable olabilir ama komutlardan da anlaşıldığı gibi sadece BPDU Guard korumasından kaynaklı kapanan portlar için tanımlanıyor. Bu işlem farklı nedenlerden dolayı ERRDisable olan 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

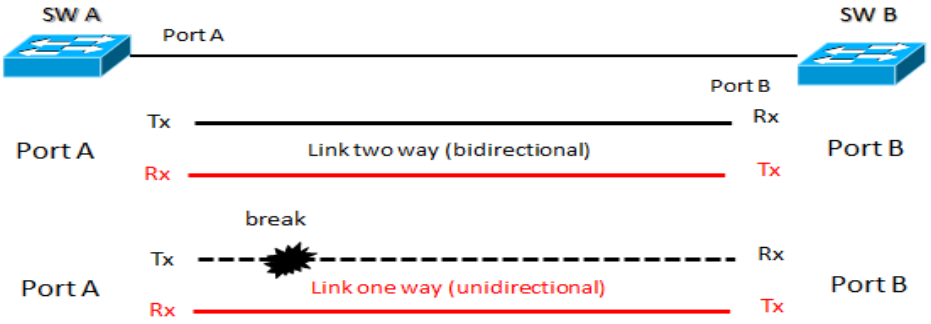
Fiber Optik kablolarda, cihazlar arasında veri aktarını için kullanılan bir gidiş, bir dönüş (karşı cihazdan gönderilen) olmak üzere iki bağlantı vardır. Bu bağlantılardan biri koptuğu zaman taraflardan biri veri gönderemenektedir. Buna Unidirectional Link denilmetedir. Bunu daha rahat açıklayabilmek 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 taktirde 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 ve bu durum Loop oluşacaktır.

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

- 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 (karşlıklı 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.
- UDLD (Unidirectional Link Detection), Cisco tarafından geliştirilmiş bir çözümür. 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 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}**” komutu, 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 edilip düzelme olması durumunda portun tektat açılması isteniyorsa “**udld recovery interval <Time>**” komutu kullanılıyor (Detaylı bilgi için https[:]//bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/udld-unidirectional-link-detection-tek-yonlu-baglanti-tespiti).



NOT

- STP ve RSTP portokollerinin çalıştığı iki farklı switch birbirine bağlandığında RSTP karşı portun STP çalıştığını anlıyor ve kendi de STP gibi çalışıyor. Yani eski versiyon STP protokollerle de uyumlu çalışabiliyor.
- STP konfigürasyonunda varsayılanda bütün switchlerin Priority değerleri aynı geliyordu. Bu durumda Root Bridge seçilmek istenen switche en düşük Priority değer, yedek olarak seçilmesi istenen switche ikinci en küçük Priority değeri veriliyor.

Terminolojiler

- inconsistent state, Root Guard koruması devreye alınmış switch portundan Root Bridge'den daha yüksek Bridge ID değerine sahip BPDU paketleri gönderene kadar port bloklanmasıdır. Porttan bu Root Bridge'den daha düşük Bridge ID değerine sahip BPDU paketleri gönderilmeye başlandığında port tekrar devreye alınır.

Kontrol Komutları

- sh spanning-tree interface <Interface ID>
- sh spanning-tree interface <Interface ID> detail
- show errdisable recovery
- sh spaning-tree inconsistent-ports
- sh udld neighbors
- sh udld <Interface ID>
- sh spanning-tree interface <Interface ID>