مفهوم الـ STP/RSTP

م. هاشم بن مسعود الشريف

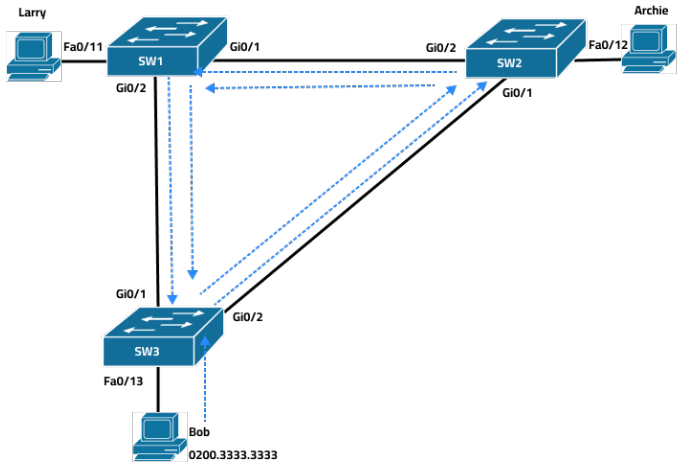
عضو هيئة التدريب بالكلية التقنية بحائل

محاضر معتمد لدى أكاديمية سيسكو

تمنع الـ STP/RSTP ثلاثة مشاكل متواجدة على شبكات الـ LAN وهذه الإشكالات الثلاثة هي انعكاس لحقيقة واحدة وهي أنه لولا وجود الـ STP/RSTP لأصبحت البيانات تدور داخل الشبكة لفترة من الزمن قد تصل لساعات أو أيام أو للأبد لو بقيت أجهزة الشبكة ووسائطها تعمل بدون انقطاع.

الإشكالات التي تمنعها الـ STP/RSTP:

١. **Broadcast storm:** الترجمة الحرفية للمشكلة الأولى هي "عاصفة البث" وتحدث عندما يبدأ إطار واحد من البيانات بالدوران بين الأجهزة، سواء كان هذا الإطار من نوع Broadcast أو Multicast أو Unknown-destination Unicast. الـ Broadcast storm يستطيع إغراق جميع الوسائط بنسخ من نفس الإطار وبشكل متكرر مما يمنع الإطارات الجيدة والمرغوب فيها من الوصول لوجهتها، بل يزداد الأمر سوءً بسبب الضغط الذي يسببه ذلك على معالجات أجهزة الحاسوب للمستخدمين نظراً لاستقبالها للعدد الكبير من رسائل البث والتي بدورها تؤثر على ادائها. ولفهم كيفية حدوث ذلك تمثل الرسمة أدناه نموذج لشبكة يقوم فيها Bob بإرسال إطار من نوع Broadcast وهي الرسائل العامة التي يفترض أن تصل لجميع الأجهزة على الشبكة المحلية. تمثل الأسهم باللون الأزرق حالة الرسائل ودورانها بين أجهزة الـ Switch وكيف ستكون بدون وجود STP/RSTP.



لا ننسى أنه من خصائص جهاز الـ Switch اذا استلم رسالة بث Broadcast فإنه يقوم بتمريرها لجميع المنافذ ماعدا المنفذ الذي وصلت منه وعليه سيتم الدفع بها من SW3 الى SW2 والأخيرة بدورها تدفع بها الى SW1 وتبدأ عملية الدوران Looping والتي تستمر الى أن يحدث شيء يوقفها مثل (إغلاق أحد المنافذ، إعادة تهيئة جهاز الـ Switch ، أو أي يعمل يكسر حلقة الدوران)

٢. **MAC table instability:** وهذا هو الإشكال الثاني والذي تتلخص فكرته في التغير المستمر وعدم استقرار وثبات جدول عناوين الـ MAC address table بسبب كثرة الرسائل التي تصل من منافذ مختلفة وتحمل نفس عنوان المصدر للرسالة. لتوضيح الفكرة لنتخيل وبناء على الرسمة السابقة عندما بدأ Bob بإرسال رسالته والتي وصلت لـ SW3 والتي بناء عليها كان جدول عناوين الـ MAC address table الخاص بـ SW3 يعطي القراءة:

0200.3333.3333 Fa0/13 VLAN1

ولنأخذ في الاعتبار الآن مزية جهاز الـ Switch والتي تم الإشارة لها سابقاً من كونه يستطيع التعلم وبناء جدول عناوينه بنفسه، ولنتخيل الإطار وهو يخرج من جهاز SW3 ومن ثم لجهاز SW2 وبعدها لجهاز SW1 ويعود مرة أخرى للجهاز الذي خرج منه لأول مرة SW3 وسيدخل هذه المرة عبر المنفذ Gi0/1 حينها سيعيد جهاز SW3 ترتيب جدول عناوينه لأنه سيرى أن الرسالة التي وصلته الآن والتي تحمل عنوان رقم 0200.3333.3333 قد وصلت هذه المرة من منفذ آخر غير الذي كانت عليه مسبقاً ومسجلة في جدوله فيقوم بتحديث بيانات جدوله لتصبح القراءة:

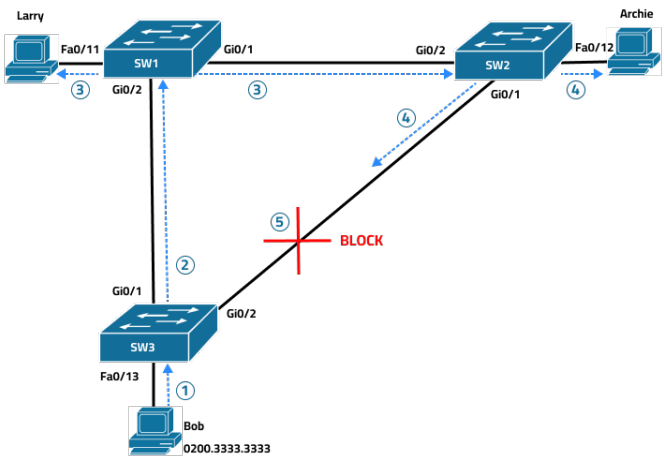
0200.3333.3333 Gi0/1 VLAN1

عند هذه النقطة حتى SW3 والمرتبط بشكل مباشر مع جهاز Bob لم يعد يعرف تحديداً أين موقع Bob في الشبكة بسبب تحديث الجدول الأخير، وعليه لو وصلت رسالة الآن لـ SW3 موجهة لـ Bob فإنه بكل بساطة سيقوم بتمريرها عبر المنفذ Gi0/1 وبالتالي لن تصل لوجهتها وستسبب ازدحام وضغط على وسائط الشبكة.

٣. **Multiple copies of the frame arrive at the destination:** المقصود بها هو تكرار النسخ من الرسائل التي تصل لنفس الوجهة ولتوضيح المقصود لنفترض أن Bob أراد إرسال رسالة الى Larry في الوقت الذي جميع أجهزة الـ Switches الموجودة في الشبكة لا تعرف مكانها بعد ولم تضفها الى الآن في جداول عناوينها، ما سيفعله SW3 الآن هو أنه سيقوم ببث هذه الرسالة لجميع المنافذ عدا المنفذ الذي وصلت منه مما يعني أنها ستصل للجهازين SW2 و SW1 والذين سيقومان بدورهما أيضاً ببث الرسالة من جميع المنافذ عدا التي وصلت منها، هنا SW1 سيوصل هذه الرسالة الى وجهتها أكثر من مرة، مرة لأنه وصلته من SW3 ومرة أخرى لأنها وصلته من SW2 مما يعني أن جهاز Larry سيستقبل العديد من نسخ الرسالة نفسها.

ما هو دور الـ STP في معالجة المشكلة:

يمنع دوران الرسائل وذلك عن طريق تخصيص أوضاع المنافذ لتكون إما على الوضع (forwarding) أو على الوضع (blocking). وضع (forwarding) يعمل بشكل طبيعي بحيث يستقبل ويمرر جميع الرسائل التي تصل إليه. بينما لا تمرر المنافذ التي على وضع (blocking) إلا رسائل الـ STP وبعض الرسائل العليا. فالمنافذ التي تكون على الوضع (blocking) لا تمرر رسائل المستخدم ولا تقوم كذلك بالتعلم وتحديث جداولها للعناوين فيما يخص عناوين الأجهزة التي ترد منها الرسائل ولا تقوم بأي معالجة للرسائل الواردة. الرسمة أدناه توضح كيف يقوم STP بحل مشكلة دوران الرسائل عن طريق وضع أحد منافذ SW3 على الوضع (blocking).



الخطوات التي تمت في الرسمة أعلاه:

١. Bob أرسل رسالته لـ SW3.
٢. SW3 مرر الرسالة الى SW1 عبر المنفذ Gi0/1 فقط ولم يمررها لـ SW2 عبر المنفذ Gi0/2 لأنه على الوضع (blocking).
٣. SW1 قام ببث الرسالة لجميع المنافذ عدا المنفذ الذي وصلت منه الرسالة وذلك عبر منفذيه Fa0/11 و Gi0/1.
٤. SW2 قام ببث الرسالة لجميع المنافذ عدا المنفذ الذي وصلت منه الرسالة وذلك عبر منفذيه Fa0/12 و Gi0/1.
٥. الرسالة القادمة من SW2 بانجاه SW3 وصلت فعلياً، ولكنها تجاهلتها وذلك لأن المنفذ Gi0/2 على الوضع (blocking).

آلية عمل الـ STP/RSTP:

تسمى أحياناً الآلية المستخدمة في عمل الـ STP بالـ spanning-tree algorithm (STA)، وتقوم باختصار باختيار المنافذ التي ستكون على وضع (forwarding) وما عداها سيكون على (blocking). وهي تستخدم ثلاثة معايير لاختيار المنافذ التي ستضعها على الوضع (forwarding) وهي:

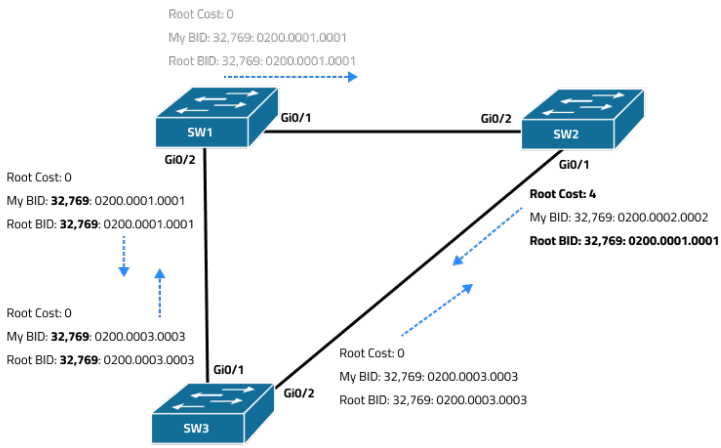
١. ترشح STP/RSTP أحد أجهزة الـ Switch لتكون الجهاز الأصل (root Switch) ودائماً ما تكون جميع المنافذ على الـ (root Switch) على وضع (forwarding).
٢. جميع أجهزة الـ Switch الأخرى غير الـ (root Switch) تعتبر أن أحد منافذها لديه أقل تكلفة إدارية (administrative cost) بينه وبين الـ (root Switch) من بقية المنافذ. تسمى تلك التكلفة بالتكلفة الجذرية (root cost) للـ Switch. تقوم الـ STP/RSTP بوضع منفذها والذي يعد جزءاً من أقل مسار للتكلفة الجذرية على وضع (forwarding) ويسمى ذلك المنفذ بالـ root port (RP) لذلك الـ Switch .
٣. يمكن توصيل العديد من الـ Switches بنفس الجزء من الشبكة، ولكن نظراً لحقيقة أن الوسائط أو الكيابل تربط جهازين مع بعضهما، وعليه لن يكون لأي وسيط أو كبل أكثر من جهازي Switch على طرفيه، وبوجود جهازين فقط سيتم وضع الـ Switch صاحب الأقل تكلفة جذرية (root cost) على الوضع (forwarding). هذا الـ Switch المختار سيطلق على منفذه المحدد بالـ designated port (DP).

وصف المنفذ	حالة الـ STP للمنفذ	الوصف
منافذ الـ root switch	Forwarding	يعتبر هذا الـ switch مرشح و منتخب من بين جميع أجهزة الـ switch على الشبكة
الـ root port لبقية الـ switches	Forwarding	هو المنفذ صاحب أقل تكلفة للوصول للـ root switch
منافذ الـ designated port	Forwarding	هو منفذ الـ switch والذي يمرر رسائل Hello لذلك الجزء من الشبكة ويكون صاحب أقل تكلفة
بقية المنافذ التي تعمل في الشبكة	Blocking	هذه المنافذ لا تقوم باستقبال أو إرسال أي رسالة على الشبكة

ذُكر في المعيار الأول من معايير اختيار المنافذ التي ستكون على الوضع (forwarding) أن STP/RSTP تقوم بترشيح الـ root Switch من بين جميع أجهزة الـ Switches في الشبكة ولفهم آلية ذلك الترشيح من المهم بدايةً معرفة آلية إرسال الرسائل بين أجهزة الـ Switches ومعرفة مفهوم المعرّف الفريد(الهوية) لكل Switch. هناك مصطلح يسمى bridge ID (BID) وهي قيمة فريدة ووحيدة وغير متكررة لكل Switch حجمها 8-byte. في الـ (BID) يوجد حقل حجمه 2-byte يسمى حقل الأولوية (priority filed) والمتبقي 6-byte تكون خاصة بالـ system ID والذي يعتبر جزء من الـ MAC address للجهاز مما يجعل لكل جهاز Switch هويته الفريدة والمتفق على تسميتها بالـ bridge ID (BID). يقوم الـ STP/RSTP بتعريف رسائل تسمى bridge protocol data unit (BPDU) والتي تستخدمها أجهزة الـ Switches لتبادل المعلومات فيما بينها. أشهر هذه الرسائل هو ما يسمى بالـ Hello BPDU والذي يحوي العديد من المعلومات من ضمنها الـ bridge ID (BID).

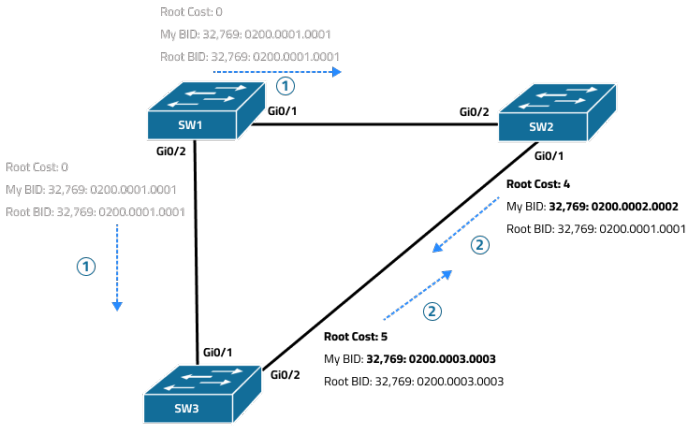
بعد هذه المقدمة فإن ترشيح الـ root switch يتم بناءً على الـ BIDs والتي تم تبادلها عن طريق الـ BPDU. كما ذُكر فإن الـ root switch هو صاحب القيمة الأقل للـ bridge ID (BID) وحيث أنه يحوي جزئين هما حقل الأولوية (priority filed) وعنوان الـ MAC address فإن المقارنة تتم أولاً بناءً على حقل الأولوية فإن كان لهما نفس القيمة تتم المقارنة بناءً على عنوان الـ MAC address. وتبدأ عملية الترشيح عندما يقوم كل Switch بإرسال Hello BPDU مدعياً فيها أنه هو الـ root switch وبمجرد أن تصل لأحدهم رسالة Hello BPDU أفضل منه (أقل BID) يتوقف عن الادعاء بأنه الـ root switch حتى تنتهي المنافسة على الـ root switch الحقيقي صاحب أقل BID.

المثال أدناه يوضح فكرة الترشيح للـ root switch

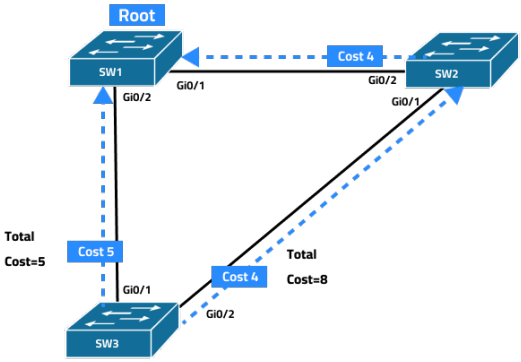


الرسمة أعلاه توضح بداية آلية الترشح وفي هذه الحالة قام SW1 بعرض نفسه كـ root switch كما قام بذلك أيضاً كلاً من SW2 و SW3 ولكن SW2 أدرك مباشرةً بأن ادعائه في غير محله وأن SW1 أفضل منه وعليه قام بتمرير محتوى رسالة الـ Hello BPDU الواردة اليه من SW1 بإتجاه SW3 في حين أن SW3 لإزال يدعي بأنه الأفضل وقام بإرسال الـ Hello BPDU الخاص به. الآن المنافسة قائمة بين SW1 و SW3 وعند مقارنتهما لحقل الأولوية وجد أنهما يحملان نفس القيمة مما يعني انتقالهما للمقارنة بناء على الـ MAC address وبالمقارنة نحصل الغلبة لـ SW1 لأنه الأقل ويصبح هو الـ root switch في هذه الشبكة.

الرسمة أدناه توضح نتائج الترشح للـ root switch



ذكر في المعيار الثاني من معايير اختيار المنافذ التي ستكون على الوضع (forwarding) **لأجهزة الـ** Switch **الأخرى غير الـ** root switch **وهو البحث عن المنفذ صاحب التكلفة الجذرية الأقل لكل** Switch **والموصلة للـ** root switch **وتمت تسميته بالـ**(RP) root port . **الرسمة أدناه توضح الفكرة**

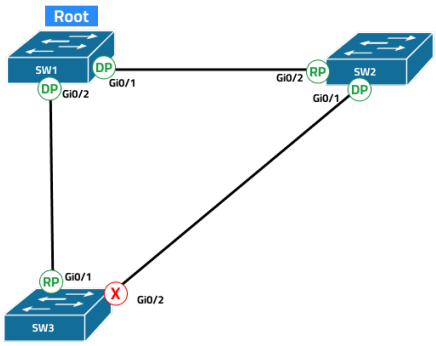


وحيث إن SW1 **تم ترشيحه كـ** root switch **سيتم الآن إيجاد الـ** root port (RP) **لـ** SW3 (**ملاحظة: سيتم لاحقاً توضيح قيمة الـ** Cost **وكيف نحسب وما في الرسمة موضوع وفق إعدادات افتراضية لتوضيح الفكرة فقط**). **يمتلك** SW3 **طريقين للوصول للـ** root switch **والذي يمثل في هذا المثال** SW1 **الطريق الأول الذي يمر من خلال** SW2 **والتكلفة لهذا الطريق عبارة عن حاصل جمع جميع التكاليف في الطريق الموصلة لـ** SW1 **وكما هو واضح ان التكلفة للطريق الآخر والمباشر لـ** SW1 **هو الأقل لأنه يساوي ٥ بينما الطريق الآخر يساوي ٨ وعليه سيقوم** SW3 **بتحديد المنفذ** Gi0/1 **كـ** root port (RP).**في بعض الأحيان وبناء بنية الشبكة يكون هناك أكثر من طريق تتساوى فيها التكلفة الجذرية وللخروج من هذه الإشكالية ولأجل تحديد الطريق الأنسب تستخدم الـ** Switches **ثلاثة معايير في المفاضلة وهي :**

١. **الاختيار بناء على الـ** BID **الأقل.**
٢. **الاختيار بناء على الـ حقل الأولوية الأقل.**
٣. **الاختيار بناء على رقم المنفذ الداخلي الأقل.**

ذكر في المعيار الثالث من معايير اختيار المنافذ التي ستكون على الوضع (forwarding) أن يتم تحديد المنافذ التي ستكون على الوضع Designated port وهذه هي الخطوة الأخيرة في عمل الـ STP/RSTP ويتم اختيار تلك المنافذ بناء على كونها منفذ الـ switch الذي يمرر رسائل Hello لذلك الجزء من الشبكة ويكون صاحب أقل تكلفة.

وبناء على ما سبق أعلاه سيكون المنتج النهائي للـ STP/RSTP كما في الرسمة والجدول ادناه.



الـ Switch والمنفذ	الحالة	السبب
SW1, Gi0/1	Forwarding	لأنها منفذ لـroot switch يتم تعيينها DP
SW1, Gi0/2	Forwarding	لأنها منفذ لـroot switch يتم تعيينها DP
SW2, Gi0/2	Forwarding	لأنها الـ RP لـ SW2
SW2, Gi0/1	Forwarding	لأنها الـ Designated port في ذلك الجزء لـ SW3
SW3, Gi0/1	Forwarding	لأنها الـ RP لـ SW3
SW3, Gi0/2	Blocking	ليست RP وليست Designated port

<u>قيمة التكلفة (Cost):</u>

تعمل الـ STP/RSTP بشكل تلقائي على أجهزة الـ Switches وعليه فإن جميع ما تم توضيحه أعلاه يعمل بشكل افتراضي. مر معنا أن لكل Switch هوية خاصة تسمى الـ (BID) وهذه الهوية تحوي جزئين أساسيين الأول هو حقل الأولوية (priority field) والثاني هو الـ MAC address. قيمة حقل الأولوية قيمة افتراضية لجميع الأجهزة. وكذلك جميع منافذ أجهزة الـ Switch لديها قيمة افتراضية (Cost) مبنية على السرعة الفعلية لهذه المنافذ.

قد يحتاج مهندس الشبكة لسبب ما أن يتحكم في إعدادات الـ STP/RSTP حتى يستطيع التحكم في خيارات وقرارات الـ STP/RSTP التي تتم على تلك الشبكة. وهنا يمتلك المهندس خيارين لتحقيق ذلك:

١. **التحكم في الـ BID وتغيير إعداداته:** للتحكم في الـ BID بالإمكان التحكم في جزء حقل الأولوية (priority field) بينما لا يمكن التحكم في الـ MAC address وهذا كافي جداً لتحيق الهدف لأنه وكما مر معنا سابقاً أن المقارنة تعقد أولاً بناء على حقل الأولوية (priority field) فإن كان لهما نفس القيمة تتم المقارنة بناء على الـ MAC address.

٢. **التحكم في تكلفة (Cost) المنافذ:** المنافذ أيضاً لها قيم افتراضية. وبالإمكان تغيير تلك الإعدادات الافتراضية، والتي بدورها ستغير من الحسابات التي تقوم بها أجهزة الـ Switch فمثلاً عند الرغبة في تجنب منفذ معين من نقل البيانات ببساطة يتم إعطاؤه تكلفة (Cost) أعلى وهكذا.

إن معرفة القيم الافتراضية للتكلفة الخاصة بالمنافذ من الأمور التي تساعد مهندس الشبكة في التعامل مع الـ STP/RSTP فمن خلالها يستطيع التحكم في تلك القيم وبالتالي توجيه حركة الشبكة. الجدول أدناه يوضح قيم التكلفة الافتراضية للمنافذ والمعيارية من قبل منظمة IEEE.

السرعة	IEEE Cost: 1998	IEEE Cost: 2004
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1 Gbps	4	20,000
10 Gbps	2	2000
100 Gbps	غير موجود	200
1 Tbps	غير موجود	20

يجب مراعاة أن التكلفة للمنفذ تقاس بالسرعة الفعلية المطبقة على الكيبل وليست بالسرعة القصوى للمنافذ. بمعنى أنه لو كان هناك منفذ يدعم السرعات 10/100/1000 لكنه يعمل لسبب ما بالسرعة 10 Mbps فإن قيمة التكلفة له هي 100 هذه التكلفة خاصة لأجهزة الـ Switches الخاصة بـ Cisco وفي الـ STP. وفي حال الرغبة في استخدام القيم الافتراضية الأخرى الموجودة في العمود الأيسر من الجدول أعلاه فيجب مراعاة أن أجهزة Cisco Catelyst switches تتطلب إعداد معين لجعل تلك القيم هي الافتراضية لها.

جميع ما سبق يمكن تطبيقه على كلاً من STP وRSTP وهناك بعض الفروق بينهما تكمن في آلية استجابة كل منهما فيما لو حدث هناك أي تغيير أو إشكال في بنية الشبكة وهذا ما سيتم توضيحه بعد قليل.

تفاصيل تخص الـ STP فقط:

عندما تنتهي جميع الإعدادات الخاصة بالـ STP يجب أن تكون هذه الإعدادات ثابتها وغير متغيرة على الأقل حتى تتغير نفس بنية الشبكة. ما يحدث هو أن الـ root switch يرسل رسائل الـ Hello كل ثانيتين بشكل افتراضي بحيث تحمل هذه الرسالة التكلفة (Cost=0) عبر جميع منافذه والتي هي على الوضع (forwarding) ليستلمها بقية الـ Switches وبدورهم يقومون بتمرير هذه الرسالة لجميع الـ Designated port (DP) وذلك بعد أن إجراء بعض التغييرات البسيطة عليها وهي إضافة ما يلي:

١. إضافة الـ BID الخاص بالـ switch لتوضيح المرسل الأخير للرسالة.
٢. إضافة التكلفة (Cost) الخاصة به.

يتكرر هذا الأمر كل ثانيتين إلى أن تحدث مشكلة تمنع هذا التكرار. فعندما لا يستطيع الـ switch في استقبال رسالة الـ Hello سيفهم أن هناك إشكالية محتملة حصلت للشبكة. لأن جميع الـ Switches تعتمد على تلك الرسالة لمعرفة أن الطريق باتجاه الـ root switch يعمل بكفاءة ولا يوجد أي خلل في أداء الشبكة. فلو وصلت مثلاً رسائل الـ Hello وقد تغير فيها بعض التفاصيل أو أنها لم تتصل هنا ستبدأ الأجهزة بالتعامل مع هذا التغيير على أنه فشل وخلل في الـ STP وستقوم بالبدء في إجراءات تغيير بنية الـ STP.

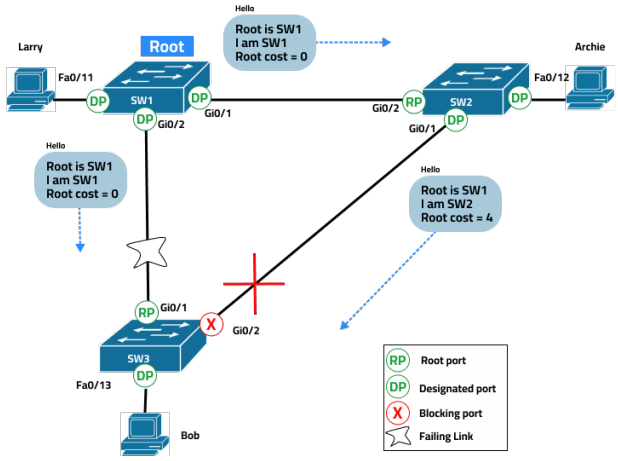
المؤقتات الزمنية التي الإفتراضية لتغيير لإعداد الـ STP:

هناك ثلاث مؤقتات تتعامل معها أجهزة الـ Switches بصفة عامة لمعرفة سلامة بنية الـ STP وتعتمد عليها في اتخاذ أي قرارات لمعالجة أي إشكالات قد تطرأ وهي:

المؤقت	القيمة الإفتراضية	الوصف
Hello	(٢) ثانية	تمثل المدة الزمنية بين كل رسالتي Hello من الـ root switch
MaxAge	(١٠) أضعاف وقت الـ Hello	الوقت الواجب على الـ switch انتظاره بعد توقف استلام رسائل Hello وذلك قبل البدء في إجراءات تغيير بنية الـ STP
Forward delay	(١٥) ثانية	التأخير الضروري والمرتبط بالأداء والذي يحدث عندما تتغير حالة المنفذ من الوضع (blocking) إلى الوضع (forwarding)، حيث يبقى المنفذ في حالة استماع مؤقتة(١٥ ثانية)، ثم في حالة تعلم مؤقتة(١٥ ثانية)

عندما لا يتلقى الـ Switch رسالة Hello المتوقعة وذلك في إطار المدة الزمنية المخصصة لذلك وهي (٢ ثانية) يبقى الـ Switch على وضعه الطبيعي ويكمل أداؤه بدون أي تغيير أو تعديل، ولكن اذا تجاوزت المدة الزمنية الـ MaxAge (١٠ أضعاف وقت الـ Hello = ٢٠ ثانية) يبدأ الـ Switch حينها في أتخاذ الإجراءات اللازمة لتغيير بنية الـ STP حيث يبدأ في الإجراءات الخاصة بتحديد الـ root switch من استقبال وإرسال رسائل الـ Hello وإجراء المقارنات التي سبق توضيحها.

الرسمة أدناه توضح الفكرة:



تمثل الرسمة أعلاه نفس البنية التي عملنا عليها في الأمثلة السابقة ويظهر فيها أن منفذ Gi0/2 لـ SW3 في وضع (blocking) بينما منفذ Gi0/2 لـ SW1 للتو تعطل الكيبل المرتبط به، وهنا يتعامل SW3 مع الموقف لأنه لم يتلقى رسالة Hello من منفذه Gi0/1، بينما SW2 لا يحتاج للقيام بأي إجراء لأنه لازال يتلقى رسائل الـ Hello من الـ SW1 من خلال منفذه Gi0/2، ففي هذه الحالة SW3 وكما ذكرت سابقاً سيبدأ في التعامل مع الموقف ولا فرق في نظره بين كون المشكلة الحاصلة هي بسبب خلل في الكبل الرابط بينه وبين SW1 أو كانت المشكلة هي بسبب منفذه Gi0/1 والذي لسبب ما تعطل ففي كلتا الحاتين لم تصل اليه رسائل الـ Hello والفرق فقط هو أنه في الحالة الأولى سينتظر انتهاء المؤقت MaxAge بينما في الحالة الثانية سيبدأ مباشرة لأنه سيفترض أن رسائل الـ Hello لن تصله أبداً من منفذه.

ستكون البداية بإعادة التقييم لمعرفة من سيكون الآن الـ root switch. لا يزال SW3 يتلقى رسائل الـ Hello من الـ SW2 والذي كما مر معنا يمررها من SW1 بعد إضافة الـ BID خاصته وإضافة تكلفته الجذرية. طبعاً لازال SW1 هو صاحب الـ BID الأقل وبمجرد وصول هذه الرسالة لـ SW3 يقرر مرة أخرى بأن SW1 كسب الترشيح مرة أخرى ويبدأ في خطوة الثانية وهي تحديد منافذه التي سيجعلها على الوضع root port (RP) وفي هذه الحالة لم يعد SW3 يتلقى رسائل الـ Hello الا من منفذ واحد فقط وهو Gi0/2 وبناء على هذا الوضع سيتخذ القرار بتغييره من وضع (blocking) الى وضع root port (RP) وسيقوم كذلك بإعادة تقييم المنافذ التي ستكون على الوضع Designated port (DP) والتي في هذه الحالة هي فقط منفذ واحد هو Fa0/13.

تغيير حالة المنفذ في الـ STP:

تستخدم الـ STP فكرة الدور (Role) والحالة (State)، فأما الدور فمثل الـ root port وdesignated port وهي المتعلقة بكيف يحلل ويرتب الـ STP بنية الشبكة المحلية، وأما الحالة فمثل الـ (forwarding) والـ (blocking) ويقصد بها توجه الـ switch وقراره بشأن استقبال وإرسال الرسائل. فعندما يتغير وضع الـ STP يقوم الـ switch باختيار الدور الجديد له وبناء على هذا الدور يتم تحديد وضع الحالة الخاصة بمنافذه لتكون إما (forwarding) أو (blocking).

الـ Switch الذي يتعامل مع الـ STP يستطيع ببساطة ومباشرةً نقل أحد منافذه من الحالة(forwarding) الى الحالة (blocking) لكنه يحتاج لمزيد من الوقت للقيام بالعكس وهو نقل أحد منافذه من الحالة (blocking) الى الحالة (forwarding) وذلك لأن الـ switch قبل القيام بذلك يضع المنفذ في حالتين متتاليتين بشكل مؤقت وذلك منعاً لإشكالية دوران الرسائل (Looping). والحالتين هما:

١. **الاستماع (Listening):** وهي شبيهة بحالة (blocking) فالمنفذ لا يقوم بتمرير الرسائل، ويقوم أثنائها الـ Switch بإزالة البيانات القديمة لجدول الـ MAC address table لأنها ببساطة قد تكون هي سبب دوران الرسائل في الشبكة (Looping).
٢. **التعلم (Learning):** هنا يبدأ المنفذ في مرحلة التعلم وجمع المعلومات مع استمراره بعدم تمرير الرسائل فيقوم فقط ببناء جدوله الخاص بعناوين الـ MAC address table وذلك من خلال الرسائل التي تصل لمنفذه.

وعليه فإن الـ STP ينقل حالة المنفذ من الـ (blocking) الى الـ (listening) ومن ثم الى الـ (learning) ووصولاً الى الـ (forwarding)، حيث يجبر الـ STP المنفذ على المرور بالحالتين (listening) و (learning) وذلك لمدة زمنية محددة تساوي مدة مؤقت الـ (Forward delay) وهي (١٥ ثانية) والذي تمت الإشارة اليه سابقاً في جدول المؤقتات الزمنية، فيكون إجمالي الوقت الذي يحتاجه المنفذ للانتقال من الحالة (blocking) الى الحالة (forwarding) هو (٣٠ ثانية). كما أنه من الممكن أن يزيد الوقت عن ذلك بسبب المؤقت MaxAge والذي يمتد لـ (٢٠ أضعاف وقت الـ Hello = ٢٠ ثانية) وذلك قبل أن يتخذ الـ Switch قرار الانتقال من (blocking) الى (forwarding). وعليه يكون مجموع المدة الزمنية للانتقال تصل الى (٥٠ ثانية).

تفاصيل تخص الـ RSTP فقط:

في البداية يجب التنويه الى أن الـ STP قدم ولا يزال يقدم خدمات متميزة في مجاله، ولكن التطور الهائل الذي تشهده كلاً من الأجهزة (Hardware) والبرامج (Software) دفع بالعديد من البروتوكولات للظهور والتعامل مع هذا التطور المتسارع ومنافسة الموجود سابقاً. وقبل الحديث عن الـ RSTP وما هو الجديد الذي قدمه لابد من توضيح بعض المعايير المهمة ذات الصلة فالمعيار IEEE 802.1w والمرتبط بالـ RSTP ما هو الا تعديل وتطوير للمعيار IEEE 802.1D والمرتبط بالـ STP، فقد ظهر المعيار IEEE 802.1D في عام ١٩٩٠ ومن ثم تم تحديثه تحديث أولي في عام ١٩٩٨ واستمر التحديث الى أن تم الإعلان عن المعيار IEEE 802.1w

في عام ٢٠٠١ والذي كان هذا المعيار هو الأول لـ RSTP، وكغيره من المعايير تم تطويره مع مرور السنين وإضافة كامل تفاصيله إلى معيار جديد هو IEEE 802.1Q.

مقارنة بين RSTP وSTP:

تعمل RSTP بالضبط مثل STP في عدة أمور وتختلف عنها في أمور أخرى **أما نقاط التشابه فهي:**

- كلاهما يرشح الـ root switch وبنفس الطريقة والآلية.
- أجهزة الـ switch معهما تستخدم نفس القواعد في تحديد الـ root port.
- كلاهما يرشح الـ designated port (DP) بنفس الطريقة والآلية.
- كلاهما يحدد حالة المنافذ من كونها (forwarding) أو (blocking) مع فارق بسيط هو أن الـ RSTP يسمي حالة (blocking) بـ (discarding).

وفي الحقيقة عند الحديث عن أجه التشابه فإن الـ RSTP تعمل بشكل مشابه ومتكامل مع لـ STP حتى إنه بالإمكان أن يعملا سوياً في نفس الشبكة. وهنا قد نتساءل عن سبب وجود الإصدار المطور RSTP مع وجود كل هذا التشابه مع الإصدار السابق STP. **السبب الأساسي** وراء ذلك هو التغلب على عنصر التأخير وعلى الوقت الطويل الذي تستغرقه الـ STP لأجل معالجة الخلل في بنية الـ STP ومن هنا جاءت التسمية للـ RSTP والتي يمثل حرف الـ (R) فيها الكلمة (Rapid) والتي تعني "سريع" أو "خاطف".

فقد مر معنا أن عملية تغيير بنية الـ STP تمر بمراحل متتالية تستغرق من الوقت (٥٠ ثانية) بينما مع الـ RSTP فيمكن إنجاز الموضوع كاملاً في حدود (١٠ ثواني) فقط. فقد تميزت الـ RSTP عن سابقتها بأنها تجنبت العديد من المؤقتات المستخدمة في الـ STP حيث نتج عن ذلك سرعة الانتقال من حالة الـ (forwarding) إلى حالة الـ discarding (blocking)، والعكس صحيح.

ولتوضيح ذلك بشكل أكثر تفصيل فإن RSTP أضافت بعض الآليات التي جعلت الـ switch يتجنب الانتظار لبعض المؤقتات وهي:

- أضافت الـ RSTP آلية جديدة تمكن جهاز الـ switch من تغيير الـ root port الخاص به بدون أي انتظار في بعض الحالات.
- أضافت الـ RSTP آلية جديدة تمكن جهاز الـ switch من تغيير الـ designated port الخاص به بدون أي انتظار في بعض الحالات.
- قامت الـ RSTP عند ضرورة الانتظار بتقليص الوقت الافتراضي لذلك الانتظار.

فمثلاً لو حدث عطل لسبب ما وأصبح أحد الـ Switches غير قادر على استلام رسائل الـ Hello من طرف الـ root switch، كان الإجراء المتبع في الـ STP هو الانتظار للمؤقت الـ MaxAge والذي يمثل (١٠ أضعاف مؤقت رسالة Hello = ٢٠ ثانية) بينما الإجراء الافتراضي مع الـ RSTP هو الانتظار فقط (٣ أضعاف مؤقت رسالة Hello = ٦ ثواني) إضافة الى إضافة ميزة رائعة جداً وهي أن الـ switch يستطيع القيام بإرسال رسالة استعلام لأقرب switch له للسؤال عن الوضع لديه وهل يواجه نفس المشكلة.

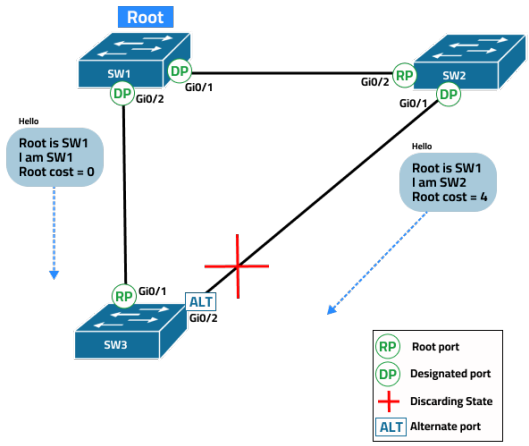
أفضل طريقة لفهم عمل هذه الآليات هو من خلال التعرف على كيفية عمل الـ alternate port والـ backup port في الـ RSTP. فيقصد بالـ alternate port المنافذ التي لديها المؤهلات لتقوم بنفس الدور الذي يقوم به الـ root port الحالي وذلك فيما لو طرأ خلل فيه. أما الـ backup port فيتمثل مفهومه في تزويد منفذ احتياطي في جهاز الـ switch وذلك عوضاً عن الـ designated port (**ملاحظة مهمة:** الـ backup

يستخدم فقط في الشبكات التي لإزالت تستخدم أجهزة الـ hub فهي في الحقيقة قليلة الاستخدام في شبكات اليوم).

لتلخيص ما سبق الجدول أدناه يوضح أدوار المنافذ في الـ RSTP وعمل كل واحد منها:

دور المنفذ	عمله
Root port	المنفذ الذي يعتبر الـ switch أفضل طريق باتجاه الـ root switch
Alternate port	المنفذ الذي سيحل محل الـ root port عندما يتعرض لأي خلل وفشل
Designated port	منافذ الـ switch التي تمرر الرسائل لداخل مجال التصادم
Backup port	المنافذ التي ستحل محل الـ designated port عندما تتعرض لأي خلل أو فشل
Disabled port	المنافذ التي تم تعطيلها بشكل إداري

أما نقاط الاختلاف بين الـ RSTP والـ STP فعلى سبيل المثال في الـ STP كان الـ root switch هو من يرسل رسالة الـ Hello وبقية الأجهزة تمررها مع بعض الإضافات بينما في الـ RSTP كل جهاز switch يقوم بشكل مستقل بإنشاء رسالته الـ Hello إضافة الى ذلك أصبح بالإمكان ارسال رسائل الاستعلام فيما بين الـ Switches. في الـ RSTP تقوم الـ Switches غير root switch بتحديد منفذ واحد ليكون designated port تماماً مثل المعمول به في الـ STP الا أن الـ RSTP تزيد خطوة أخرى وهي تحديد منافذ أخرى تصلح لأن تكون designated port وتقوم بتسميتها بالـ alternate port. من خصائص هذه المنافذ أنها تقوم باستلام رسائل الـ Hello القادمة أيضاً من الـ root switch تماماً مثل designated port. المثال أدناه يوضح الفكرة:

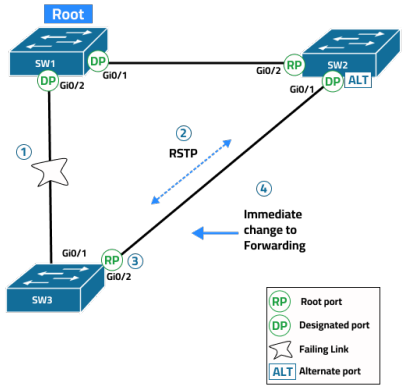


في المثال أعلاه SW1 يمثل الـ root switch ويقوم SW3 باستلام رسالتي Hello من المنفذين Gi0/1 و Gi0/2 وكلتا الرسالتين تؤكدان على أن SW1 يمثل الـ root switch وبناء على خصائص الـ alternate port في الـ RSTP والتي تنص على أن أي منفذ خلاف الـ root port يستلم رسائل الـ Hello يمكن أن يكون alternate port يقوم بناء على ذلك SW3 بوضع المنفذ Gi0/2 ليكون alternate port. فهو باختصار يعمل كأفضل ثاني خيار ليكون الـ root port ويستطيع بسرعة فائقة أخذ دور الـ root port بدون مؤقتات وانتظار لأي فترات زمنية. فعلى سبيل المثال لو حدثت أي مشكلة أو خلل في الـ root port أو أنه لم يعد يستلم رسائل الـ Hello من الـ root switch. يقوم مباشرة ذلك الـ switch بتغيير الـ root port السابق دوراً وحالةً على النحو التالي:

١. يتغير الدور من كونه root port الى disabled port.
٢. تتغير الحالة من كونها forwarding الى discarding والتي تكافئ في الـ STP حالة blocking.

ثم وبدون الانتظار لأي مؤقتات يقوم الـ switch بتغيير دور وحالة الـ alternate port ليصبح دوره هو الـ root port ولتصبح حالته هي الـ (forwarding). كما أنه لا يستنفذ أي وقت للانتقال بين حالتي الـ (learning) أو (listening) وانما مباشرة ينتقل للـ (forwarding).

المثال أدناه يوضح الانتقال السريع و آليته في الـ RSTP.

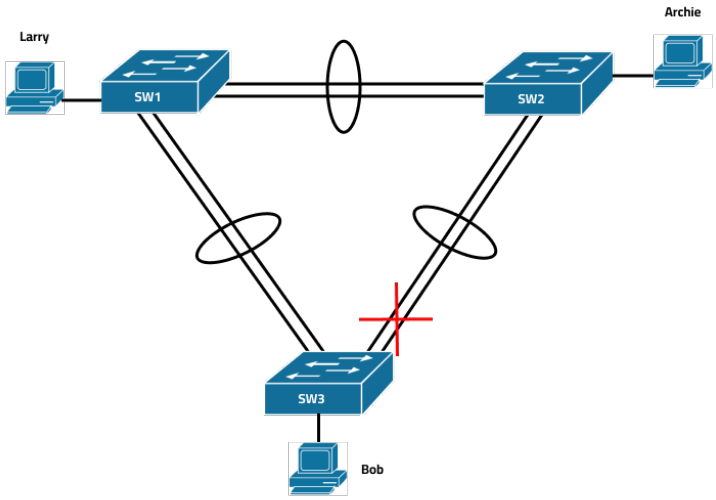


الخطوات التي تمت هي:

١. حدث فشل ما في الكبل بين SW1 و SW3 وبالتالي حدث خلل في منفذ SW3 المتصل بذلك الكبل Gi0/1.
٢. يقوم SW2 و SW3 بتبادل رسائل الـ RSTP وذلك لتأكيد أن SW3 ستقوم بتغيير الـ alternate port الخاص بها ليكون هو الـ root port وهذا الاجراء يفيد SW2 في تحديث جدوله الخاص بعناوين الـ MAC address table.
٣. يقوم SW3 بتغيير دور Gi0/1 ليكون disabled ودور Gi0/2 ليكون الـ root port.
٤. يقوم SW3 بتغيير حالة Gi0/2 لتكون forwarding مباشرةً وبدون الدخول في المرحلة المؤقتة للتعلم (learning).

ملاحظات مهمة:

١. **EtherChannel:** من أحد الطرق التي يمكن الاستفادة منها في تقليص المدة الزمنية المستغرقة لتغير بنية الـ STP هي تجنب فكرة التغيير من أساسها ويمكن أن يتم ذلك عن طريق الـ EtherChannel وتكمن فكرته ببساطة في دمج أكثر من كبل مع بعضها بشكل متوازي بين جهازي switch ويمكن أن يصل عدد الوسائط المستخدمة الى ٨ كيابل تدمج مع بعضها لتشكل الـ EtherChannel، تتعامل الـ switches معها على أنها تتبع منفذ واحد فقط للـ STP، وكنتيجة لذلك لو حصل خلل لأي من هذه الوسائط وبقي على الأقل كبل واحد فقط يعمل فلن يحتاج الـ STP للقيام بالتغيير. المثال أدناه يوضح نفس بنية الشبكة التي كنا نعمل عليها الا أن هناك كبلين من نوعية Gigabit يربطان بين كل جهازي switch، وستناقش فكرة الـ EtherChannel بالتفصيل في ورقة مستقلة بعون الله.



٢. **BPDU Guard: للأسف يفتح كلاً من الـ STP و الـ RSTP أبواباً من المخاطر الأمنية التي يجب الانتباه لها وأخذها في عين الاعتبار مثل:**

a. **يستطيع المهاجم الاتصال بأحد أجهزة الـ switch من خلال أحد منافذها وإعطاء ذلك المنفذ قيمة للتكلفة وجعلها الأقل وذلك حتى يتمكن من جعل ذلك الـ switch هو الـ root switch.**

b. **يستطيع المهاجم أن يتصل بعدة منافذ في عدة switches ومن ثم إعادة توجيه حركة البيانات بدون أن يلاحظ ذلك موظفو الشبكة المحلية.**

c. **قد يتسبب بعض المستخدمين للشبكة المحلية بالضرر بالشبكة وذلك بحسن نية عندما يقومون بإضافة جهاز switch من النوعية غير المكلفة والتي لا تدعم أي من الـ STP أو الـ RSTP فيتسبب للشبكة المحلية كاملةً بحدوث مشكلة دوران البيانات (Looping).**