سیسکو به پارسی

بهینه سازی Spanning Tree Protocol

نوشته:

شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

انجمن سیسکو به پارسی http://forum.shafagh.com

بهبود Convergence در STP

همانطور که اشاره شد Convergence در شبکه حالتی است که شبکه پس از ناپایداری به حالت پایدار میرسد. زمان Convergence هر چه کمتر باشد بهتر است. از طرق مختلف میتوان زمان Convergence در سطوح access، uplink و backbone را بهبود بخشید:

- **PortFast** برای اتصال سریع کامپیوترها به سوئیچ های access.
- **UplinkFast** برای بکار افتادن لینک redundant در سوئیچ های access به مرکز شبکه.
- **BackboneFast** برای بهبود convergence در backbone بعد از وقوع تغییرات.

PortFast

همانطور که میدانیم، برای بالا آمدن یک پورت و رسیدن به وضعیت forwarding، دو زمان learning و listening هر کدام 15 ثانیه و در مجموع 30 ثانیه وقت صرف میشود (Forwarding Delay). اگر از تکنولوژی های دیگر نظیر PAgP نیز روی لینک استفاده کرده باشیم (20 ثانیه تاخیر مربوط به Etherchannel) این زمان را به 50 ثانیه افزایش میدهد که برای یک پورت متصل به یک Computer نسبتا طولانی است و ممکن است در عملکرد یک Host نظیر دریافت IP از DHCP اختلال ایجاد کند.

با تنظیم PortFast روی پورت هایی که به Workstation ها متصلند و نیازی به احتیاط اولیه در STP نبوده و پورت مراحل Listening و Learning را طی نمیکند و مستقیم به وضعیت Forwarding جهش میکند. در نتیجه زمان اتصال پورت مطلوب خواهد شد.

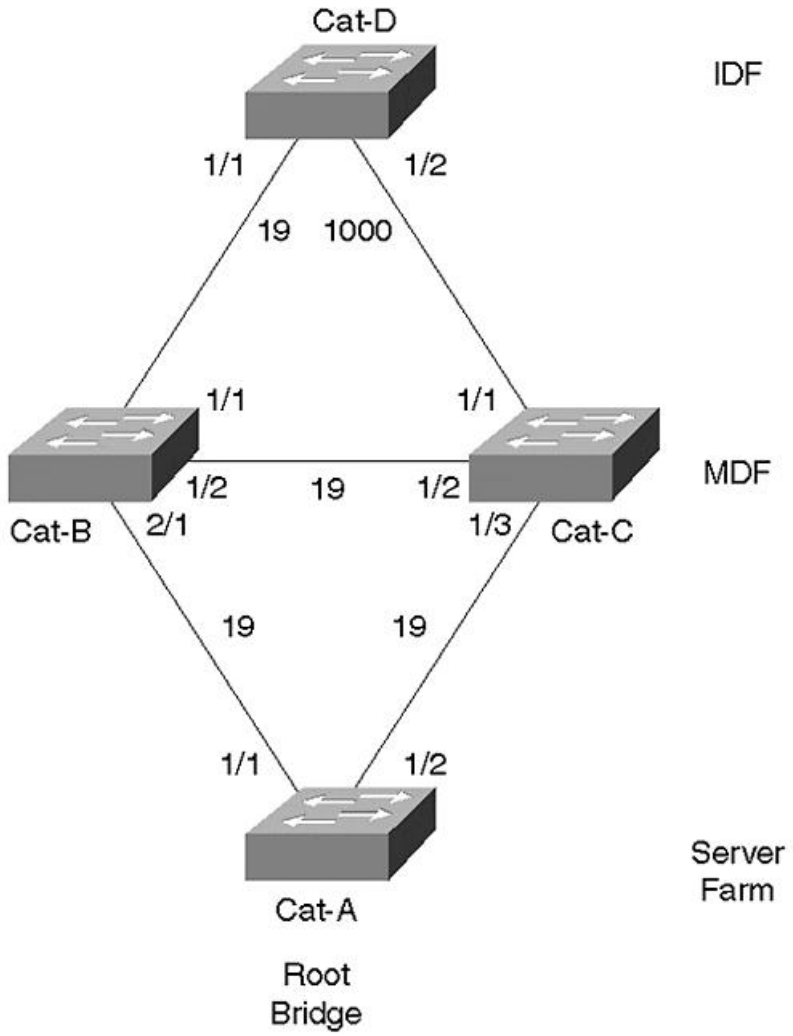
با وجود PortFast، پورت مستقیما به حالت forwarding بالا می آید. از دیگر مزایای PortFast این است که به ازای تغییر وضعیت پورت، TCN ایجاد نمیگردد.

```
Switch(config-if)# spanning-tree portfast
```

Cisco in Persian

UplinkFast

در حالتی که سوئیچ Access به دو Distribution Switch متصل باشد، پورت Redundant به 50 ثانیه زمان نیاز دارد تا پس از قطع شدن پورت اصلی شروع به کار کند. با UplinkFast این زمان به حداقل ممکن رسیده و طی چند ثانیه این اتفاق رخ میدهد و لینک Backup جایگزین لینک اصلی اما مختل شده میشود. روی سوئیچ های Access تنها باید UplinkFast را فعال کنیم.



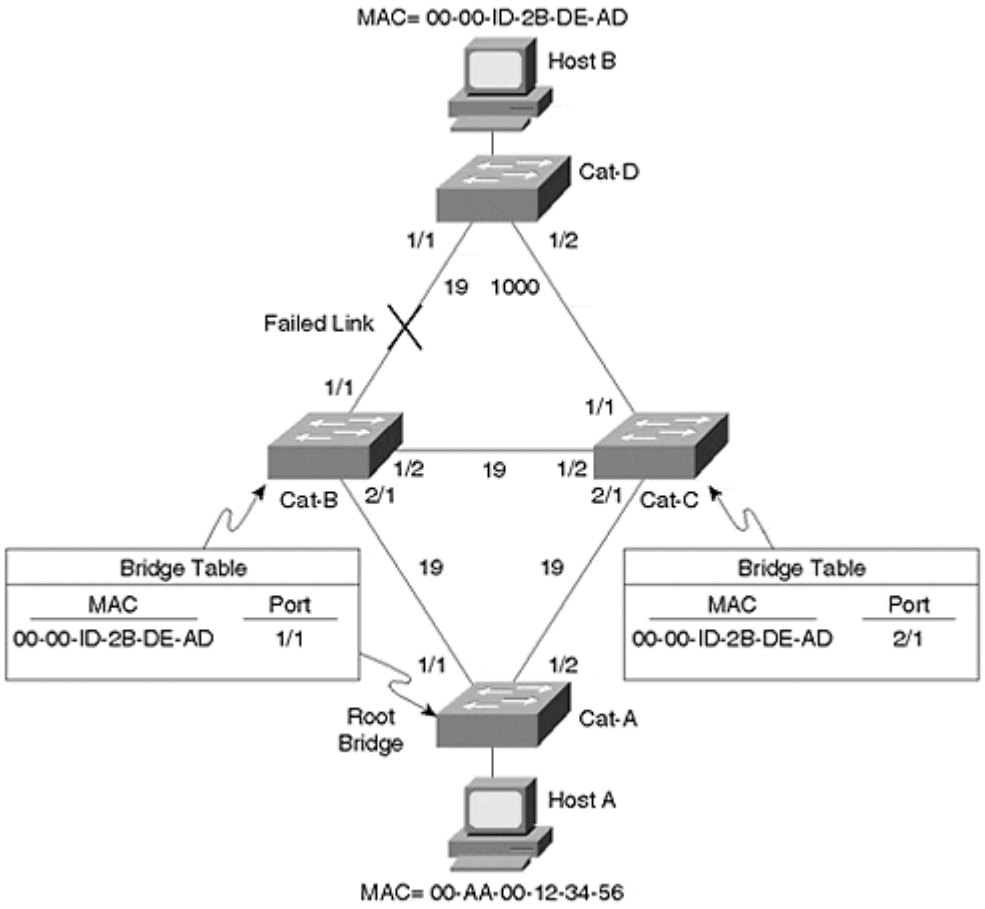
در شکل بالا، Cat-D برای اتصال از پورت 1/1 استفاده میکند اما پورت دوم بحالت آماده باش برای سریع Uplink شدن در می آید. شبکه از بخش های IDF یا Intermediate Distribution Frame که همان Access است و MDF یا Main Distribution Frame (که در واقع Core/Distribution) است تشکیل شده است.

UplinkFast پورت کاندید Root Port را به حالت Backup Root Port در می آورد تا در زمان نیاز بسرعت لینک برقرار گردد .

دستور زیر UplinkFast را در سوئیچ فعال میکند:

```
Switch(config)# spanning-tree uplinkfast [max-update-rate pps]
```

بمحض ورود این دستور، UplinkFast در کل سوئیچ درون تمامی VLAN ها اعمال میگردد. تمایل سوئیچ برای Root Bridge شدن کم شده و Priority به 49152 میرسد. دلیل آن این است که سوئیچ Transit بقیه سوئیچ ها نشود. علاوه بر تغییر در اولویت، به Cost پورت ها 3000 واحد افزوده میشود. مسلما این دستور روی Root Bridge مجاز نیست و برای سوییچ های Access در نظر گرفته شده است.



و اما قسمت آخر دستور فوق بعنوان Max-update-rate چه فایده ای دارد؟

سوئیچ در هنگام تغییر لینک، Bridge Table خود و پورت خروجی را بسادگی تغییر میدهد اما باید به سوئیچ بالاتر نیز این تغییر و جابجائی MAC Address ها را از لینکی به لینک دیگر گزارش دهد تا عملیات سرعت گیرد.

این عملیات با ارسال یک سری Multicast Frame به آدرس 0100.0ccd.cdcd که آدرسی ساختگی است، از آدرس فرستنده های داخل CAM (Content Addressable Memory) انجام میشود و سرعت ارسال این فریم ها در واحد ثانیه با **max-update-rate** قابل تنظیم است که بصورت پیش فرض 150pps است.

BackboneFast

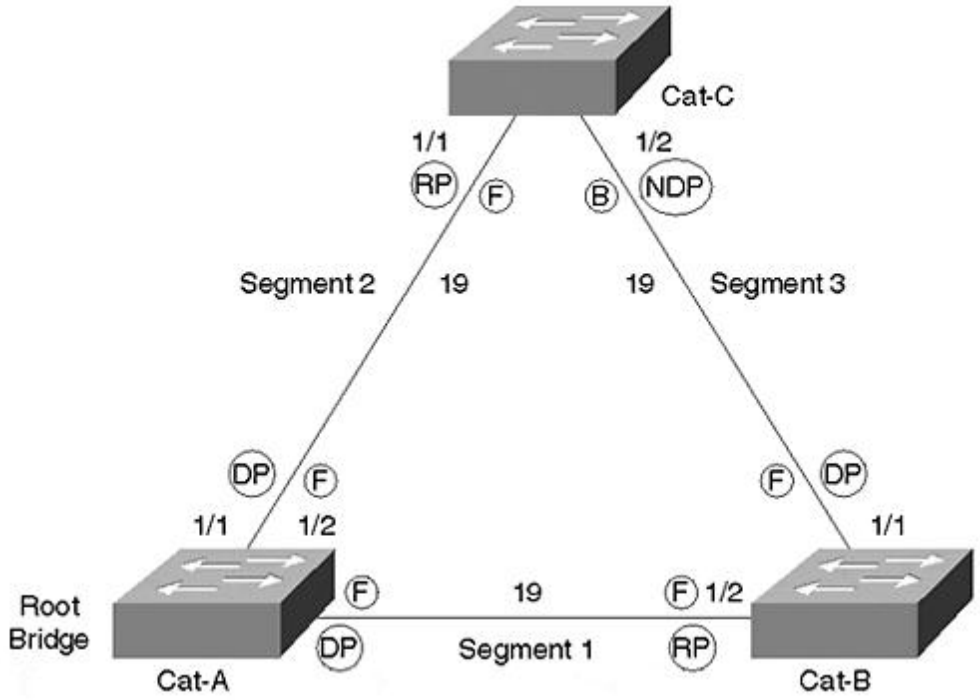
BackboneFast برای بهبود زمان Max Age در نظر گرفته شده و نهایتا زمان Convergence را از 50 ثانیه به 30 ثانیه کاهش میدهد. BackboneFast روی تمامی سوئیچ ها باید فعال شود و بصورت پیش فرض غیر فعال است. BackboneFast قطع شدن یک سوئیچ را از روی لینک دیگر سوییچ ها تشخیص میدهد. به این تشخیص indirect link-failure detection میگویند. این تشخیص با دریافت Inferior BPDU قابل استنباط است. Inferior BPDU، BPDU ای است که از سمت یک سوئیچ که Root خود را گم کرده ارسال میشود. در این پیام آن سوییچ خود را Root اعلام میکند.

Inferior BPDU ها، از طرف سوئیچی ارسال میگردند که ارتباط خود را با Root Bridge از دست داده و خود را Root اعلام میکند. در حالت عادی، برای اینکه سوئیچ به Inferior BPDU ها توجه کند و یا خود را Root اعلام کند، باید Max Age سپری شود. اما BackboneFast این زمان را از بین برده و موجب تسریع عملیات میگردد.

سوئیچ RLQ یا Root Link Query میفرستد تا Root Bridge را پیدا کند، اگر جواب را روی Root Port خود دریافت کند، نشان دهنده آن است که حداقل مسیر او تا Root سالم است. اما اگر روی پورتهای Block شده دریافت کرد، باید یک Root Port دیگر انتخاب کند پس فورا Max Age را صفر میکند.

سوئیچ بالاتر که RLQ را دریافت میکند در صورتیکه Root Bridge باشد یا Root Bridge را گم کرده باشد، RLQ Reply میفرستد، در غیر اینصورت RLQ را به سوئیچ های بالاتر خود فرستاده تا شاید Reply برای فرستنده فرستاده شود.

Cisco in Persian



در شکل بالا Cat-B وقتی Segment 1 را قطع شده میبیند، خود را Root Bridge اعلام میکند. اما Cat-C با ارسال RLQ ارتباط خود با Root را مطمئن شده و به Inferior BPDU ها عمل نمیکند. در نهایت Root Port در Cat-B تغییر میکند.

Cisco in Persian

مقابله با BPDU های مخرب

- **Inferior BPDU**: BPDU ی که از سمت یک سوئیچ که Root خود را گم کرده ارسال میشود. در این پیام سوییچ خود را Root اعلام میکند.

- **Superior BPDU**: این BPDU توسط سوییچی ارسال میشود که از BID بهتری نسبت به Root فعلی برخوردار است و خود را Root اعلام میکند پس مستحق Root شدن است. اما این BPDU میتواند مخرب باشد: اگر این BDPU از سوی سوییچ یک مشتری یا کاربر باشد میتواند شبکه را دچار اختلال کند. زیرا Root شبکه خواهد شد، توپولوژی شبکه ما را به هم ریخته و نهایتا مسیر عبور ترافیک ترانزیت را تغییر خواهد داد.

برای مقابله با انواع مخرب BPDU، از دو راه حل زیر میتوان استفاده کرد:

- **Root Guard**: وقتی این دستور روی پورتی تنظیم شود، در صورت دریافت Superior BPDU، پورت به وضعیت root-inconsistent در آمده و بلوکه میشود. این وضعیت زمانی از بین میرود (به حالت نرمال برمیگردد) که دیگر از Superior BPDU ها خبری نباشد.

در واقع با این تکنیک محدوده و قلمرویی برای Root شدن تعیین میکنیم (Root Guard بصورت پیش فرض غیرفعال است.)

```
Switch(config-if)# spanning-tree guard root
```

- **BPDU Guard**: اگر هرگونه BPDU از پورتی که BPDU Guard دارد دریافت شود پورت فورا در وضعیت errdisable قرار میگیرد و دیگر ترافیکی را از خود عبور نخواهد داد. این خصوصیت بصورت پیش فرض غیرفعال است و پیشنهاد میشود روی پورت هایی که PortFast دارند، از آنجاییکه از این پورت ها انتظار دریافت BPDU را نداریم ، فعال گردد. **باید توجه داشت که PortFast به منزله غیرفعال کردن STP روی پورت نیست بلکه پورت را مستقیما به مرحله Forwarding میبرد.**

```
Switch(config-if)# spanning-tree bpduguard enable
```

مقابله با گم شدن BPDU

سیسکو برای BPDU های مخرب، راه حل Root Guard و BPDU Guard را ارائه کرده است. اما در حالتی که اصلا BPDU دریافت نشود چه راهکاری برای سوییچ موجود است؟ یکی از بزرگترین مشکلات STP اشکالات سخت افزاری است که ممکن است در شبکه رخ دهد و باعث اختلال در عملکرد STP شود.

Cisco in Persian

BPDU Skew Detection

تاخیر در دریافت BPDU ها را محاسبه میکند و گزارش میدهد. زمان تاخیر تحت نام skew time اندازه گیری و ثبت میشود و از طریق Syslog به مدیر شبکه گزارش میشود. این Feature روی CatOS ارائه شد.

Loop Guard

اگر در بازه زمانی Max-Age پیامی از Root دریافت نشود، پورت بلوکه شده به حالت Forwarding در می آید. اگر به دلیل مشکلی سخت افزاری (نظیر یک طرفه شدن ارتباط سوییچ با سوییچ بالاتر) پیام های Hello در زمان لازم نرسد، با به کار انداختن پورت بلوکه شده، شبکه واقعا دچار Loop میشود. این خصوصیت بصورت پیش فرض غیرفعال است و عموما روی پورت هایی که Designated port نیستند، نظیر Backup Uplink ها (و خود Uplink ها) استفاده میشود تا اگر Root بخاطر تاخیر یا هر علتی روی پورت Backup پیدا نشد و زمان به Max-Age رسید، از Forwarding شدن آن پورت جلوگیری شده و شبکه بخاطر تاخیر در STP، Loop نشود.

توسط دستور زیر روی پورت فعال میشود:

```
Switch(config-if)# spanning-tree guard loop
```

اگر سوییچ روی پورت های افزونه خود - پورتهای Redundant که به ROOT وصل اند - BPDU دریافت نکند پورت Blocking خود را به حالت نرمال برمیگرداند چون به اشتباه تصور میکند که در شبکه Loop وجود ندارد پس نیازی به Block کردن پورت Alternate یا Backup نیست. در این حالت در شبکه واقعا Loop ایجاد میشود!!! در صورتیکه نخواهید این کار را انجام دهد از Loop Guard استفاده کنید. (چون میدانید که Forwarding شدن آن پورت فایده ای ندارد و تنها موجب ایجاد Loop میشود.) Loop Guard به ازای هر پورت تنظیم میشود و در حالتی که BPDU دریافت نشود پورت را بحالت Loop-Inconsistent در می آورد. وقتی BPDU روی آن پورت دریافت شود پورت خود به خود به حالت نرمال برمیگردد هنگام چنین رخدادی تنها یک پیام Log میشود. شاید تصور کنید که اگر واقعا مشکلی در شبکه باشد در این صورت Loop Guard مانع بهبود وضعیت شبکه میشود اما این طور نیست - Loop-guard یک مزیت الحاقی به Spanning-Tree است که توسط سیسکو ارایه شده - فراموش نکنید که در زمان رخداد این اتفاقات سوییچ کماکان روی Root Port خود از Root پیام های BPDU را دریافت میکند و تنها پورت افزونه خود را بحالت Forwarding در نمی آورد.

Cisco in Persian