مبانی اولیه سیسکو

CCNA

CISCO CERTIFIED CCNA Security

جلسه چهارم: Spanning Tree

✔ آموزش کامل Routing & Switching

✔ به همراه سناریو

نویسنده: مهندس امیرحسین خالقی

فهرست

پیشگفتار ۳
فصل چهارم : Spanning Tree ۴
- دستورات Spanning Tree Protocol ۶

پیشگفتار

سپاس پروردگار را که این امکان را داد که تا باز بتوانیم مجموعه ای پر مطلب و پر فهم را کمتر از یک سال بنویسیم.

این کتاب با توجه به سرفصل های کتاب CCNA ICND 1 & ICND 2 برای علاقه مندان به شبکه و سیسکو نوشته شده است. در تهیه این کتاب سعی بر آن شده است تا فهم مطالب و مباحث به صورت روان و گیرا مطرح گردد.

در ابتدای کتاب سر فصل مطالب قید شده است. در انتهای هر فصل سناریویی طراحی شده که می تواند در فهم و یادگیری سریع تر شما کمک کند. توصیه می شود که این سناریو ها حتما کار شود. در انتهای کتاب به بررسی نمونه سوالات آزمون Cisco پرداخته ایم.

درصورت هرگونه مشکل در این کتاب میتوانید با ایمیل نویسنده (info@akhaleghi.ir) تماس حاصل فرمایید تا با بررسی آن بتوانیم کتابی کامل و با زبان فارسی در اختیار شما دوستان و همکاران ارجمند قرار دهیم.

در پایان از تمامی عزیزانی که ما را در تهیه و تنظیم این کتاب یاری نموده اند کمال تشکر را داریم.

باشد که موثر باشیم ....

امیرحسین خالقی

فصل چهارم : Spanning-Tree

به منظور پیشگیری از مسئله " آشفتگی انتشار " و سایر اثرات جانبی در رابطه با Looping شرکت DEC پروتکلی با نامSTP ، (Spanning-tree Protocol) را ایجاد نموده است . پروتکل فوق با مشخصه ۸۰۲,۱ توسط موسسه IEEE استاندارد شده است. Spanning tree از الگوریتم STA (Spanning-tree algoritm)استفاده می نماید. الگوریتم فوق بررسی خواهد کرد آیا یک سوئیچ دارای بیش از یک مسیر برای دستیابی به یک گره خاص است ؟ در صورت وجود مسیرهای متعدد ، بهترین مسیر نسبت به سایر مسیرها کدام است ؟ نحوه عملیات STP بشرح زیر است:

به هر سوئیچ ، مجموعه ای از مشخصه ها (ID) نسبت داده می شود. یکی از مشخصه ها برای سوئیچ و سایر مشخصه ها برای هر یک از پورت ها استفاده می گردد .مشخصه سوئیچ ، BID (Bridge ID) نامیده شده و دارای هشت بایت است . دو بایت بمنظور مشخص نمودن اولویت و شش بایت برای مشخص کردن آدرس MAC استفاده می گردد. مشخصه پورت ها ، شانزده بیتی است . شش بیت بمنظور تنظیمات مربوط به اولویت و ده بیت دیگر برای اختصاص یک شماره برای پورت مورد نظر است.

برای هر مسیر یک Path Cost محاسبه می گردد. نحوه محاسبه پارامتر فوق بر اساس استانداردهای ارائه شده توسط موسسه IEEE است. بمنظور محاسبه مقادر فوق ، ۱,۰۰۰ مگابیت در ثانیه (یک گیگابیت در ثانیه) را بر پهنای باند سگمنت متصل شده به پورت ، تقسیم می نمایند. بنابراین یک اتصال ۱۰ مگابیت در ثانیه ، دارای Cost به میزان ۱۰۰ است (۱,۰۰۰ تقسیم بر ۱۰) . بمنظور هماهنگ شدن با افزایش سرعت شبکه های کامپیوتری استاندارد Cost نیز اصلاح می گردد. جدول زیر مقادیر جدید STP Cost را نشان می دهد. (مقدار Path cost می تواند یک مقدار دلخواه بوده که توسط مدیریت شبکه تعریف و مشخص می گردد)

Bandwidth	STP Cost Value
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

هر سوئیچ فرآیندی را به منظور انتخاب مسیرهای شبکه که می بایست توسط هر یک از سگمنت ها استفاده گردد ، آغاز می نمایند. اطلاعات فوق توسط سایر سوئیچ ها و با استفاده از یک پروتکل خاص با نام BPDU(Bridge protocol data units) به اشتراک گذاشته می شود. ساختار یکBPDU بشرح زیر است:

Root BID پارامتر فوق BID مربوط به Root Bridge جاری را مشخص می کند.

Path Cost to Bridge مسافت root bridge را مشخص می نماید. مثلا" در صورتیکه داده از طریق طی نمودن سه سگمنت با سرعتی معادل ۱۰۰ مگابیت در ثانیه برای رسیدن به Root bridge باشد ، مقدار cost بصورت(۰+۱۹+۱۹=۳۸) بدست می آید. سگمنتی که به Root Bridge متصل است دارای Cost معادل صفر است.

Sender BID مشخصه BID سوئیچ ارسال کننده BPDU را مشخص می کند.

Port ID پورت ارسال کننده BPDU مربوط به سوئیچ را مشخص می نماید.

تمام سوئیچ ها به منظور مشخص نمودن بهترین مسیر بین سگمنت های متفاوت ، بصورت پیوسته برای یکدیگر BPDU ارسال می نمایند. زمانیکه سوئیچی یک BPDU را (از سوئیچ دیگر) دریافت می دارد که مناسبتر از آن چیزی است که خود برای ارسال اطلاعات در همان سگمنت استفاده کرده است ، BPDU خود را متوقف (به سایر سگمنت ها ارسال نمی نماید) و از BPDU سایر سوئیچ ها بمنظور دستیابی به سگمنت ها استفاده خواهد کرد.

یک Root Bridge بر اساس فرآیندهای BPDU بین سوئیچ ها ، انتخاب می گردد. در ابتدا هر سوئیچ خود را بعنوان Root در نظر می گیرد. زمانیکه یک سوئیچ برای اولین بار به شبکه متصل می گردد ، یک BPDU را بهمراه BID خود که بعنوان Root BID است ، ارسال می نماید. زمانیکه سایر سوئیچ ها BPDU را دریافت می دارند ، آن را با BID مربوطه ای که بعنوان Root BID ذخیره نموده اند، مقایسه می نمایند. در صورتیکه Root BID جدید دارای یک مقدار کمتر باشد ، تمام سوئیچ ها آن را با آنچیزی که قبلا ذخیره کرده اند، جایگزین می نمایند. در صورتیکه Root BID ذخیره شده دارای مقدار کمتری باشد ، یک BPDU برای سوئیچ جدید بهمراه BID مربوط به Root BID ارسال می گردد. زمانیکه سوئیچ جدید BPDU را دریافت می دارد ، از Root بودن خود صرفنظر و مقدار ارسالی را بعنوان Root BID در جدول مربوط به خود ذخیره خواهد کرد.

با توجه به محل Root Bridge ، سایر سوئیچ ها مشخص خواهند کرد که کدامیک از پورت های آنها دارای کوتاهترین مسیر به Root Bridge است . پورت های فوق، Root Ports نامیده شده و هر سوئیچ می بایست دارای یک نمونه باشد.

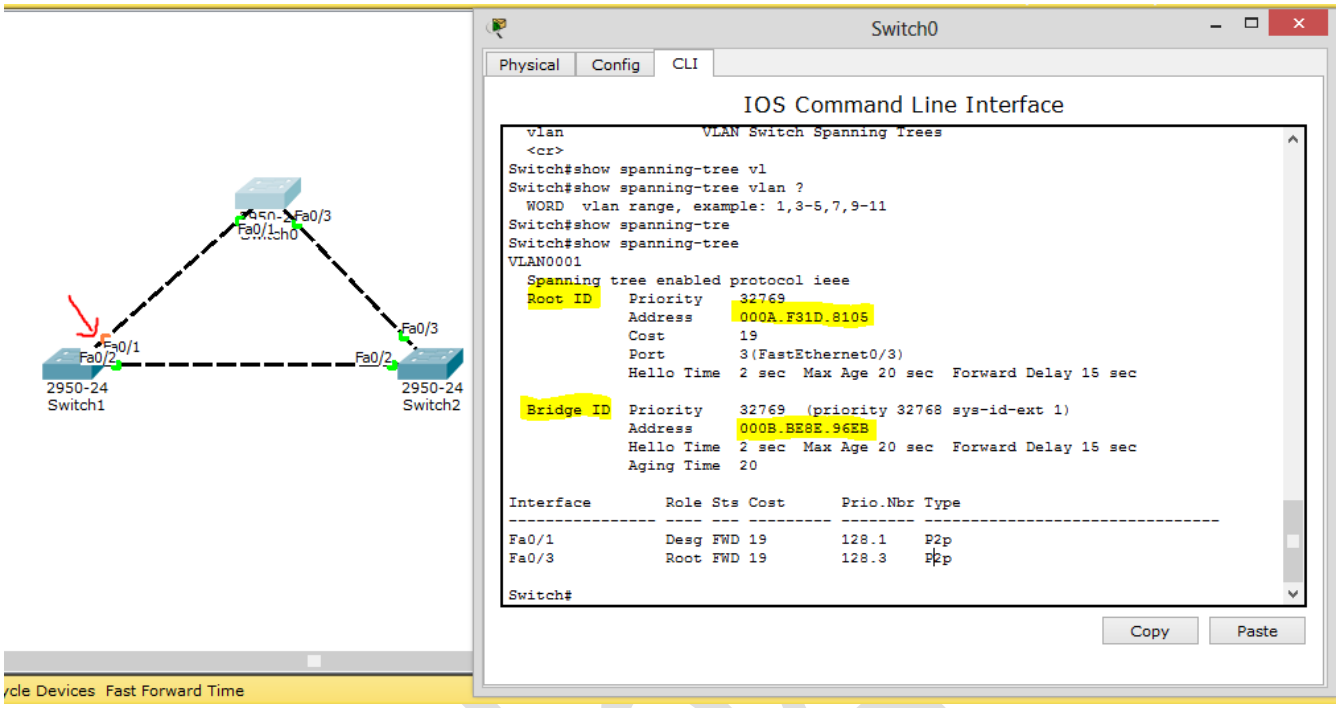
سوئیچ ها مشخص خواهند کرد که چه کسی دارای پورت های Designated است . پورت فوق ، اتصالی است که توسط آن بسته های اطلاعاتی برای یک سگمنت خاص ارسال و یا از آن دریافت خواهند شد. با داشتن صرفا یک نمونه از پورت های فوق ، تمام مشکلات مربوط به Looping برطرف خواهد شد.

پورت های Designated بر اساس کوتاهترتن مسیر بین یک سگمنت تا Root Bridge انتخاب می گردند. با توجه به اینکه Root Bridge دارای مقدار صفر برای Path cost است ، هر پورت آن بمنزله یک پورت Designated است (مشروط به اتصال پورت مورد نظر به سسگمنت). برای سایر سوئیچ ها، Path Cost برای یک سگمنت بررسی می گردد. در صورتیکه پورتی دارای پایین ترین Path Cost باشد ، پورت فوق بمنزله پورت Designated سگمنت مورد نظر خواهد بود. در صورتیکه دو و یا بیش از دو پورت دارای مقادیر یکسان Path Cost باشند ، سوئیچ با مقادر کمتر BID اتخاب می گردد.

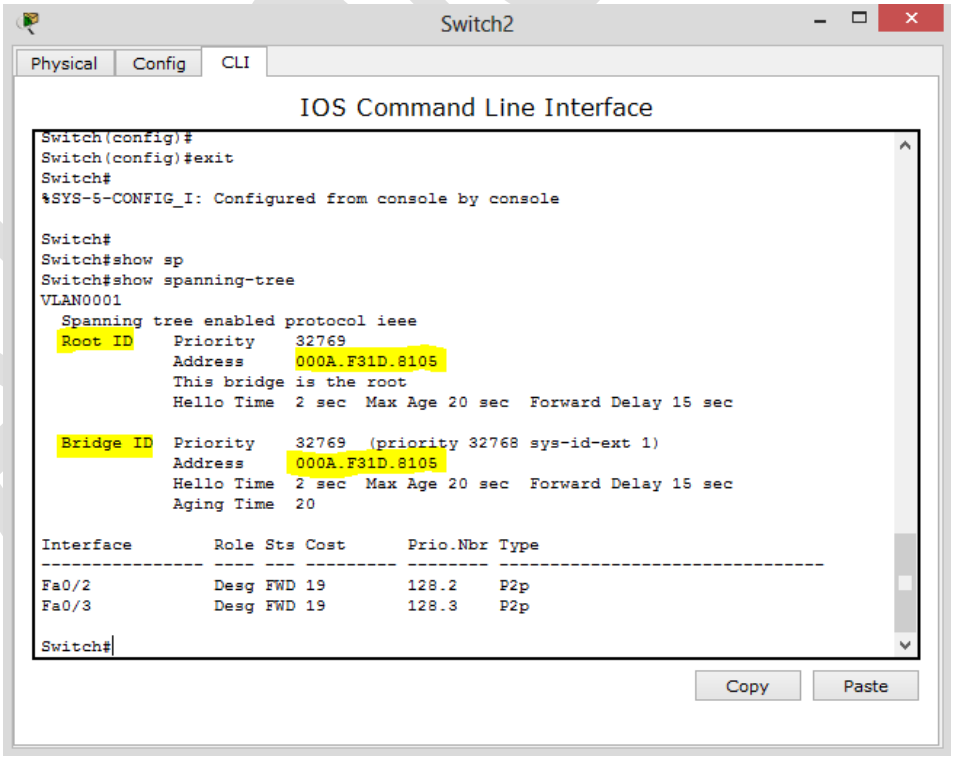
پس از انتخاب پورت Designated برای سگمنت شبکه ، سایر پورت های متصل شده به سگمنت مورد نظر بعنوان non-designated port در نظر گرفته خواهند شد . بنابراین با استفاده از پورت های Designated می توان به یک سگمنت متصل گردید.

هر سوئیچ دارای جدول BPDU مربوط به خود بوده که بصورت خودکار بهنگام خواهد شد. بدین ترتیب شبکه بصورت یک Spanning Tree بوده که Root Bridge بمنزله ریشه و سایر سوئیچ ها بمنزله برگ خواهند بود. هر سوئیچ با استفاده از Root Ports قادر به ارتباط با Root Bridge بوده و با استفاده از پورت های Designated قادر به ارتباط با هر سگمنت خواهد بود.

مثال برای درک بهتر Spanning Tree : مطابق شکل زیر سه سوییچ را با کابل Cross به هم متصل کنید. سپس در یکی از سوییچ ها در محیط Enable Mode دستور Show Spanning-Tree را مینویسیم. با توجه به شکل زیر Root ID و Bridge ID مشخص می شود.



در دو سوییچ دیگر نیز همان دستور را مینویسیم. همانطور که در شکل زیر میبینید Root و Bridge یکی است پس سوییچ ۲ Root می باشد.



برای تغییر Root به یکی دیگر از سوییچ ها بصورت زیر عمل میکنیم: (میخواهیم Root را از سوییچ ۲ به ۰ منتقل کنیم)

```
Switch(config)#spanning-tree vlan 1 root ?
  primary    Configure this switch as primary root for this spanning tree
  secondary  Configure switch as secondary root
Switch(config)#spanning-tree vlan 1 prior
Switch(config)#spanning-tree vlan 1 priority ?
  <0-61440>  bridge priority in increments of 4096
Switch(config)#spanning-tree vlan 1 priority 4096
```

همچنین برای انتخاب Spanning-Tree برای یک Vlan به صورت زیر عمل میکنیم:

```
Switch(config)#spanning-tree vlan 1 priority 4096
Switch(config)#do show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    4097
              Address     000B.BE8E.96EB
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    4097  (priority 4096 sys-id-ext 1)
              Address     000B.BE8E.96EB
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------
Fa0/1            Desg FWD 19        128.1    P2p
Fa0/3            Desg FWD 19        128.3    P2p
```

یکی از مسائل در حال رشد که امروزه مدیران شبکه با آن برخورد میکنند نحوه کنترل دسترسی افراد به شبکه داخلی سازمانشان میباشد. به عنوان مثال آیا هر شخصی میتواند وارد سازمان شده، لپ تاب خود را به پریز شبکه متصل کرده و به شبکه داخلی دسترسی داشته باشد؟ ممکن است جواب شما به این پرسش این باشد که هر پریز شبکه روی دیوار به سوئیچ متصل نیست. ولی اگر شخصی کابل اترنت را از سیستم در حال کاری جدا کند و به شبکه متصل شود چطور؟ شاید این سناریو غیر ممکن به نظر بیاید ولی این اتفاق بارها در سازمانهای مختلف پیش آمده است. مسئلهای که بیش از هرچیز در این مورد نگران کننده است ویروسها وworm های مختلفی است که سیستم شخص غیر مجاز متصل شده به شبکه ممکن است داشته باشد. در زیر برای امنیت بیشتر به چند مورد اشاره میکنیم:

Bpduguard : کار Bpduguard اینست که از ورود BPDU جلوگیری کند. ما روی پورتی که به کامپیوتر وصل است میزنیم که User نتواند روی آن پورت هاب یا سویچ نصب کند که ساختار Spanning Tree ما را خراب نکند. سویچ ها برای برقراری ارتباط با یک دیگر از BPDU استفاده می کنند. نحوه ی فعال کردن Bpduguard به صورت زیر است:

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

Port Fast کارش این است که STP را غیر فعال میکند و بهتر است بر روی Port های access فعال گردد. بدین صورت که بر روی access Port میرویم و Command زیر را میزنیم:

```
sw6(config-if)#spanning-tree portfast ?
  disable  Disable portfast for this interface
  trunk    Enable portfast on the interface even in trunk mode
  <cr>
sw6(config-if)#spanning-tree portfast tr
sw6(config-if)#spanning-tree portfast trunk
```

Switch port security نیز برای حل این مشکل به شما کمک میکند .مفاهیم اولیه در ساده ترین حالت Port Security آدرس MAC متصل به پورت سوئیچ را به خاطر میسپارد و فقط به همان آدرس MAC اجازه برقراری ارتباط با پورت سوئیچ را میدهد. اگر آدرس MAC دیگری بخواهد از طریق همان پورت به شبکه متصل شود، پورت مذکورغیرفعال میشود. اکثر اوقات مدیران شبکه سوئیچ را طوری تنظیم میکنند که یک SNMP trap به سیستم مانیتورینگ مبنی بر غیر فعال شدن یک پورت به دلایل امنیتی فرستاده شود. اگر چه پیاده سازی راه حل های امنیتی همیشه شامل یک

trade-off میباشد ولی این کاهش سهولت در مقابل افزایش امنیت سیستم میباشد. وقتی شما از Port Security استفاده میکنید میتوانید از دسترسی دستگاههای مختلف به شبکه جلوگیری کنید و این امر موجب افزایش امنیت میشود. ولی از طرف دیگر فقط مدیر شبکه است که میتواند پورت را فعال کند و این امر در جایی که به دلایل مجاز قرار به تغییردستگاهها باشد ایجاد مشکل میکند.

برای فعال سازی به صورت زیر عمل میکنیم:

```
sw6(config-if)#switchport port-security ?
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode
  <cr>
```

اگر ما mac-address را انتخاب کنیم یا باید mac-address را به صورت دستی وارد کنیم و یا اینکه خود سیستم به صورت Sticky وارد میکند.

```
sw6(config-if)#switchport port-security mac-address ?
  H.H.H    48 bit mac address
  sticky   Configure dynamic secure addresses as sticky
```

اگر گزینه ی Maximum را بزنیم تعداد mac-address ها را میتوانیم از پیشفرض ۱ تغییر دهیم که از ۱ تا ۱۳۲ می باشد.

```
sw6(config-if)#switchport port-security maximum ?
  <1-132>  Maximum addresses
```

همچنین گزینه ی Violation به دستگاه می گوید که اگه تعداد بیشتری mac-address به دستگاه متصل کن Port را یا Shutdown که حالت پیش فرض می باشد و یا restrict که به مدیر شبکه هشدار میدهد و یا protect که بسته هایی که دریافت میکند دور میریزد.

```
sw6(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode
```

نحوه ی انتخاب DP ها : ۱- Cost ۲- BID

نحوه ی Up شدن Port ها:

- ✓ Listening => 15 s
- ✓ Learning => 15 s
- ✓ Forwarding => sent Data & Sent BPDU
- ✓ Block => Data not Sent & Sent BPDU

برخی از Show ها بصورت زیر است:

```
Switch#show spanning-tree ?
  active             Report on active interfaces only
  detail             Detailed information
  inconsistentports  Show inconsistent ports
  interface          Spanning Tree interface status and configuration
  summary            Summary of port states
  vlan               VLAN Switch Spanning Trees
  <cr>
```