بسمه تعالی

امن‌سازی پایه زیرساخت شبکه

بخش هفتم: زیرساخت سوئیچینگ

امنیت پایه سوئیچینگ با در دسترس بودن لایه ۲ شبکه در ارتباط است. این بخش مراحل کلیدی تامین امنیت و حفظ زیرساخت‌های سوئیچینگ را شرح می‌دهد:

- محدود کردن دامنه‌های همه‌پخشی
- امنیت پروتکل STP
- بهترین شیوه‌های امن‌سازی VLAN

زیرساخت سوئیچینگ از دید CSF

نتایج حاصل از اعمال روش CSF درمورد امنیت سوئیچینگ در جدول ۱ و ۲ ارائه شده است.

دید کلی:

جدول ۱: زیرساخت سوئیچ – دید کلی

مانیتور
ورود: • Syslog • SNMP

کنترل کامل :

جدول ۲: زیرساخت سوئیچ – کنترل کامل

اجرا	انزوا	سختی
• امنیت STP ✓ غیرفعال کردن ترانکینگ پویا ✓ PVST ✓ BDPU ✓ گارد ریشه • بهترین شیوه رایج VLAN	• محدود کردن دامنه های همه‌پخشی • VLAN • طراحی سلسله مراتبی L3	

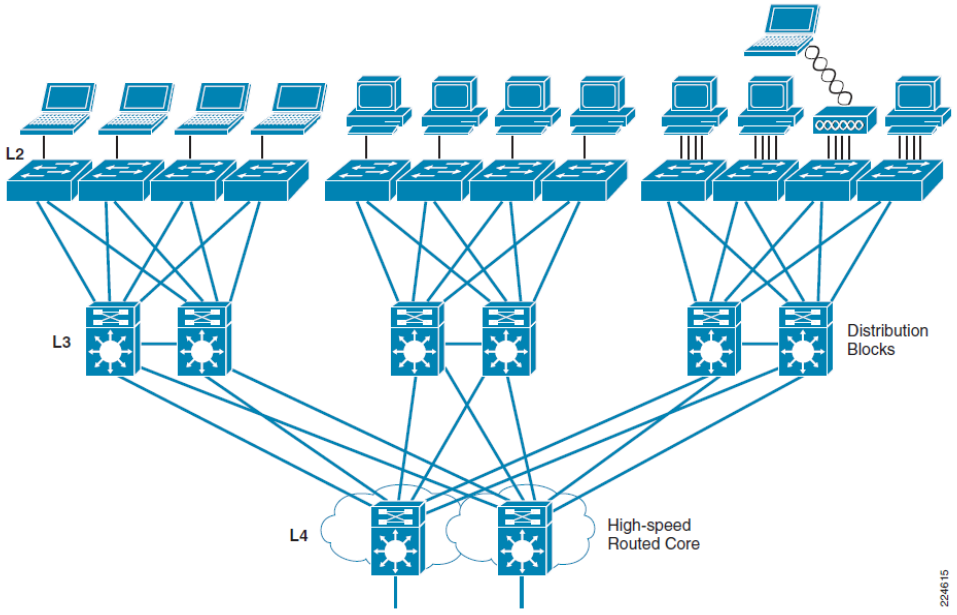
محدود کردن دامنه‌های همه‌پخشی

طبق تعریف، سوئیچ‌های شبکه مسئول انتقال فریم‌های ناشناخته، فریم‌های چندپخشی وهمه‌پخشی می‌باشند. در حالی که دامنه‌های همه‌پخشی اتصال لایه ۲ بین سیستم‌ها در شبکه محلی را تسهیل می‌کنند، طراحی شبکه با محدوده‌های بزرگ همه‌پخشی غیرضروری، یک اشکال بالقوه محسوب می‌شود.

اول آنکه در شبکه‌های بزرگ، جاری شدن جریانی ناشناخته، چندپخشی و همه‌پخشی ممکن است عملکرد شبکه را کاهش دهد. علاوه بر این، در یک دامنه همه‌پخشی در صورت بروز مشکل، تمام سیستم‌ها و سوئیچ‌های موجود در بخش LAN آسیب می‌بینند. بنابراین دامنه‌های همه‌پخشی بزرگ‌تر، احتمال بروز حوادث امنیتی بیشتری را موجب می‌شود.

برای جلوگیری از چالش‌های بالا، راه حل آن است که دامنه‌های همه‌پخشی را به چندین زیرشبکه IP و یا VLAN ها با استفاده از طراحی سلسله مراتبی تقسیم کرد. طراحی سلسله مراتبی شبکه‌ای مقیاس‌پذیر و قابل اعتماد را فراهم می‌کند.

شکل ۱ یک طراحی سلسله مراتبی را نشان می‌دهد. طراحی سلسله مراتبی کمک می‌کند تا اندازه دامنه‌های همه‌پخشی محدود شوند. این امر با جداسازی یک VLAN به یک سوئیچ انجام می‌شود. به عنوان یک نتیجه، همگرایی بهتر و تعادل بار می‌تواند از طریق استفاده از پروتکل‌های لایه ۳ حاصل شود. طرح‌های لایه ۳ محدودیت پهنای باند لایه ۲ را ندارند و خرابی به جای آن‌که بر روی کل دامنه همه‌پخشی تأثیر بگذارد، معمولاً به همسایه و یا مسیر از دست رفته محدود می‌شود.



شکل ۱- طراحی سلسله مراتبی

امنیت STP

پروتکل STP یک پروتکل مدیریت لینک می‌باشد و در IEEE 802.1D برای شبکه‌های پل تعریف شده است. STP امکان داشتن مسیر اضافی را فراهم می‌کند، در حالی که از تشکیل حلقه‌های نامطلوب در شبکه‌هایی که متشکل از مسیرهای چندگانه می‌باشند، جلوگیری می‌کند.

حلقه زمانی رخ می‌دهد که چند مسیر در بین سیستم‌ها وجود داشته باشد و می‌تواند یک حلقه بی‌پایان از ترافیک در شبکه را به‌وجود آورده و شبکه را از کار بیاندازد. STP یک الگوریتم پیاده‌سازی برای تضمین توپولوژی بدون حلقه می‌باشد. با STP، تمام سوئیچ‌ها و پل‌ها در شبکه، پیام‌های BPDU حاوی اطلاعات توپولوژی ارسال می‌کنند. الگوریتم STP از اطلاعات توپولوژی به منظور ساخت یک درخت توپولوژیک استفاده می‌کند که در آن تنها یک مسیر فعال در یک زمان بین هر دو میزبان وجود دارد. مسیرهای اضافی خاموش هستند و به عنوان پشتیبان برای زمان خرابی مسیرهای اصلی می‌باشند.

یک نسخه جدیدتر از STP به نام STP سریع وجود دارد که در IEEE 802.1w تعریف شده است. STP سریع (RSTP) شبیه به STP کار می‌کند اما پس از خرابی در یک سوئیچ، شبکه همگرایی بهتری ارائه می‌کند.

RSTP به طور قابل توجهی زمان پیکربندی مجدد توپولوژی فعال شبکه را هنگامی که تغییری در توپولوژی فیزیکی یا پارامترهای پیکربندی آن ایجاد می‌شود، کاهش می‌دهد.

STP یک پروتکل مفید است اما هر دو نسخه پروتکل فاقد امنیت لازم می‌باشند و هر دو در معرض انواع مختلفی از حملات هستند. STP هیچ‌گونه احراز اصالت و رمزگذاری برای محافظت از تبادل BPDU ها پیاده-سازی نمی‌کند. درنتیجه به علت عدم احراز اصالت، هر کسی می‌تواند با یک دستگاه که STP روی آن فعال شده باشد، صحبت کند. تغییر اجباری به توپولوژی STP می‌تواند به محرومیت از خدمات منجر شود و یا به مهاجم اجازه حمله مردی در میان را بدهد. علاوه بر این، به دلیل اینکه BPDU ها رمزگذاری شده نیستند، شنود BPDU ها در زمان انتقال و به‌دست آوردن اطلاعات مهم توپولوژی نسبتاً ساده می‌باشد.

STP موجب بروز برخی تهدیدات امنیتی می‌شود اما در توپولوژی‌هایی که در آن امکان ایجاد یک طراحی بدون حلقه ممکن نیست، STP باید استفاده شود. بدون استفاده از STP، امکان وقوع حملاتی دیگر وجود دارد.

اقدامات ممکن	ریسک و اهداف حمله	آسیب پذیری‌های STP و حملات
غیرفعال کردن ترانکینگ پویا		ترانک غیرقانونی
محدود کردن دامنه STP با استفاده PVST	حمله برروی یک VLAN، بقیه VLAN ها را تحت تاثیر قرار می‌دهد.	گسترش vlan با STP
• گارد BDPU • گارد ریشه	بی‌ثباتی شبکه مهاجم فریم‌هایی را می‌بیند که نباید ببیند. می‌تواند برای MITM، DoS استفاده شود.	مشارکت در درخت پوشا به صورت غیرمجاز بسته‌های جعلی BPDU ارسال می‌شود تا به پل ریشه تبدیل شود.

IOS سیسکو از تعدادی از ویژگی‌هایی استفاده می‌کند که از شبکه‌های پل با استفاده از STP در برابر حملات رایج محافظت می‌کند. در زیر بهترین شیوه‌های توصیه شده فهرست شده‌اند:

- غیر فعال کردن ترانکینگ پویای VLAN ها بر روی پورت‌های کاربران
- استفاده از PVST

- پیکربندی گارد BPDU
- پیکربندی گارد ریشه STP
- غیر فعال کردن پورت‌های بدون استفاده و قرار دادن آن‌ها را در یک VLAN استفاده نشده
- پیاده‌سازی امنیت پورت
- فعال کردن کنترل موج ترافیک

غیر فعال کردن ترانکینگ پویا

مذاکره ترانکینگ پویا یک ویژگی به منظور تسهیل ارتباط سوئیچ‌ها از طریق ارتباطات ترانک با یکدیگر است. با این حال، این ویژگی به راحتی می‌تواند در تنظیم یک ترانک غیرقانونی مورد سوء استفاده قرار گیرد. به همین دلیل، ترانکینگ پویا باید در تمام پورت‌های متصل به کاربران انتهایی غیرفعال گردد.

IOS سیسکو به طور پیش فرض، یک اینترفیس را درحالت مذاکره پویا تنظیم می‌کند. این حالت را می‌توان با استفاده از دستور switchport فعال کرده و مد پورت را به نوع access تنظیم کرد. یک مثال در زیر نشان داده شده است:

```
Router(config)# interface type slot/port
Router(config-if)# switchport mode access
```

PVST

درخت پوشا به ازای هر VLAN یا همان PVST یکی از ویژگی‌های موجود در سری ۴۵۰۰ و ۶۵۰۰ می‌باشد که یک نمونه مجزا از درخت پوشا را برای هر VLAN در شبکه پیکربندی می‌کند. داشتن یک نمونه مجزای STP در هر VLAN باعث می‌شود شبکه نسبت به حملات علیه درخت پوشا انعطاف‌پذیرتر گردد. اگر یک مشکل در یک VLAN رخ دهد، اثرات آن در همان VLAN موجود می‌باشد و بقیه شبکه نسبت به این مشکل محافظت می‌شوند.

به طور پیش فرض در IOS سیسکو PVST فعال می‌باشد و توصیه می‌شود که PVST همیشه فعال باشد. در سری ۴۵۰۰ یا ۶۵۰۰ با IOS سیسکو، به طور پیش فرض پروتکل درخت پوشا PVST + نیز در این سیستم عامل‌ها پشتیبانی می‌شود.

در IOS سیسکو، مد درخت پوشا می‌تواند با استفاده از دستور spanning-tree mode تغییر یابد. به عنوان مثال، برای پیکربندی +PVST داریم:

```
Router(config)# spanning-tree mode rapid-pvst
```

از آنجا که STP هیچ احراز اصالت و یا رمزگذاری برای محافظت از تبادل BPDU ها پیاده‌سازی نمی‌کند، نسبت به مشارکت غیر مجاز و حملات مشابه آسیب‌پذیر می‌باشد. IOS سیسکو ویژگی گارد BDPU را برای محدود کردن مشارکت در درخت پوشا ارائه می‌دهد.

پورت‌های متصل به کاربر انتهایی نباید در درخت پوشا شرکت داده شوند و با فعال کردن گارد BPDU در آن پورت‌ها، در صورت دریافت BDPU پورت خاموش می‌شود. در نتیجه گارد BPDU از مشارکت غیر مجاز درخت پوشا و تزریق جعلی BPDU جلوگیری می‌کند.

BPDU می‌تواند در هر پورت یا به صورت کلی پیکربندی شود. هنگامی که به صورت کلی پیکربندی شود، گارد BPDU تنها در پورت با وضعیت PortFast تاثیر می‌گذارد.

گارد BPDU به STP PortFast نیاز دارد که آماده پیکربندی بر روی یک پورت باشد.

در IOS سیسکو، گارد BDPU می‌تواند بر روی یک اینترفیس با استفاده از PortFast فعال گردد و سپس دستور spanning-tree bpduguard به صورت زیر استفاده می‌گردد:

```
Router(config)# interface fastethernet 3/1
Router(config-if)# spanning-tree portfast
Router(config-if)# spanning-tree bpduguard enable
```

در IOS سیسکو، گارد BDPU می‌تواند به صورت کلی با استفاده از دستور spanning-tree portfast bpduguard به صورت زیر استفاده گردد:

```
Router(config)# spanning-tree portfast bpduguard default
```

درصورتی‌که حالت کلی فعال باشد، گارد BDPU بر روی تمام اینترفیس‌های با وضعیت PortFast اعمال می‌شود.

گارد ریشه STP

همانطور که قبلاً مشخص شده است، درصورتی‌که STP بدون هیچ مکانیزم احراز اصالت و یا رمزگذاری برای محافظت از تبادل BPDU ها پیاده‌سازی شود، نسبت به مشارکت غیر مجاز آسیب‌پذیر است. IOS سیسکو ویژگی‌های گارد ریشه STP را برای اجرای پل ریشه پیشنهاد می‌کند.

گارد ریشه STP یک پورت را مجبور می‌کند که به یک پورت designated تبدیل شود. در نتیجه هیچ سوئیچی در انتهای دیگر لینک نمی‌تواند به یک سوئیچ ریشه تبدیل شود. اگر پورت که برای گارد ریشه پیکربندی شده باشد، یک BPDU با اولویت بالا دریافت کند، پورتی که دریافت بر روی آن بوده است، مسدود می‌گردد. در این روش، گارد ریشه STP دیگر دستگاه‌ها را از تلاش برای تبدیل شده به پل ریشه باز می‌دارد.

گارد ریشه STP باید در روی همه پورت‌هایی که هیچ‌گاه به یک پل ریشه متصل نمی‌شوند، فعال گردد (برای مثال، تمام پورت‌های کاربران انتهایی). این نکته تضمین می‌کند که یک پل ریشه هرگز بر روی آن پورت‌ها مورد مذاکره قرار نمی‌گیرد.

گارد ریشه STP به STP PortFast نیاز دارد که بر روی یک پورت پیکربندی شود. همچنین گارد ریشه STP بر هر پورت می‌تواند پیکربندی شود.

در IOS سیسکو، گارد ریشه STP را می‌توان در یک اینترفیس با استفاده از دستور spanning-tree guard root فعال کرد.

```
Router(config)# interface fastethernet 3/1
Router(config-if)# spanning-tree guard root
```

توصیه‌هایی درخصوص پیکربندی VLAN

VLAN hopping حمله‌ای است که باعث می‌شود کلاینت‌ها به دیگر VLAN های موجود بر روی یک سوئیچ، که مجوز استفاده از آن را ندارند، دسترسی پیدا کنند. این نوع حمله می‌تواند به راحتی با استفاده از شیوه‌های زیر کاهش یابد:

- همیشه از یک VLAN ID اختصاص داده شده برای تمام پورت‌ها استفاده شود.
- غیر فعال کردن همه پورت‌های بدون استفاده و قرار دادن آن‌ها در یک VLAN بدون استفاده
- برای هر منظوری از VLAN شماره ۱ استفاده نشود.
- پیکربندی تمام پورت‌های کاربران به صورت بدون ترانکینگ
- پیکربندی صحیح ترانکینگ بر روی پورت های زیرساخت
- استفاده از مد علامت‌دار برای VLAN ترانک‌ها و دور ریختن فریم‌های بدون علامت
- تنظیم پیش فرض تمام پورت‌ها به «disable»