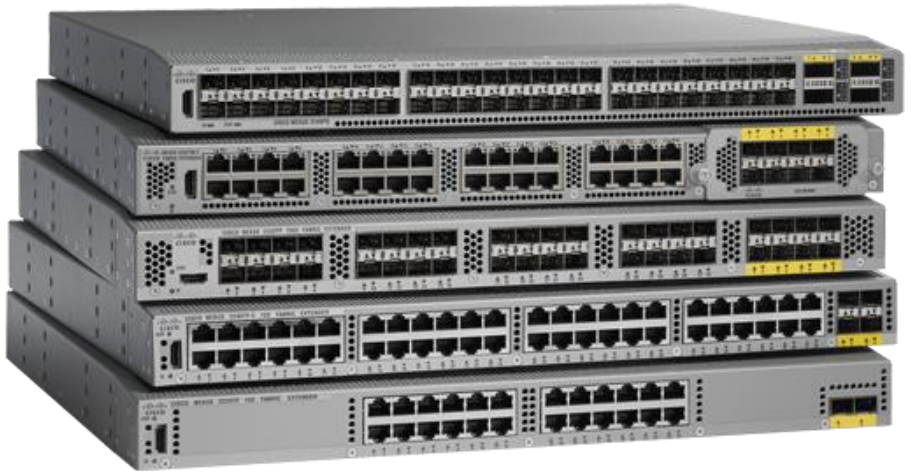
شبکه های کامپیوتری

(آمادگی برای آزمون Network+)

اسلاید هشتم

نحوه کارکرد سوییچ لایه ۲، Bridge، VLAN، تفاوت Backplane وUplink و ترانک، مفهوم Black Hole Vlan، پروتکل STP



محمد سعید صفایی صادق

(استفاده از اسلایدها صرفا برای دانشجویان مجاز می باشد!)

۱۴۰۳

درس
شبکه های کامپیوتری
۸

نحوه کارکرد سوییچ

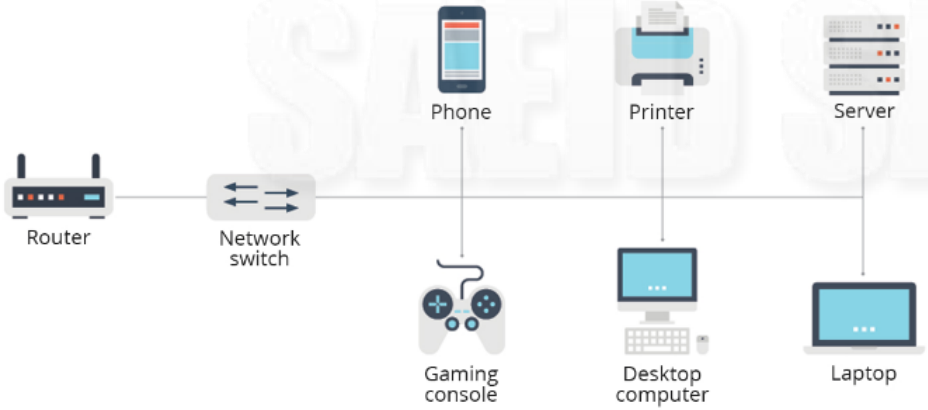
مفهوم مسیریابی

مسیریابی Routing در شبکه به فرآیند انتخاب بهترین مسیر برای ارسال داده‌ها از یک مبدا به یک مقصد در یک شبکه ارتباطی گفته می‌شود.

این فرآیند در شبکه‌هایی که از پروتکل‌های لایه ۳ مدل OSI مانند IP استفاده می‌کنند، اجرا می‌شود.

اما چنانچه پیش تر گفتیم سوییچ در لایه ۲ Data Link Layer عمل می‌کند و از آدرس‌های MAC برای هدایت بسته‌ها استفاده می‌کند.

اگر به طور ساده تر مثال زد می توان سوییچ را به عنوان یک خیابان مثال زد.



خیابان‌ها در یک شهر به‌گونه‌ای طراحی شده‌اند که خودروها (داده‌ها) بتوانند بین خانه‌ها (دستگاه‌ها) در داخل یک محله (شبکه محلی یا LAN) حرکت کنند.

سوییچ، مانند یک خیابان، وظیفه دارد مسیر خودروها را به درستی هدایت کند تا هر خودرو به مقصد درست (خانه‌ی مورد نظر) برسد.

مثلا:

یک کامپیوتر می‌خواهد داده‌ای را به پرینتری که در همان شبکه است ارسال کند.

سوییچ، مانند خیابانی در همان محله، خودرو (بسته داده) را مستقیماً به پرینتر هدایت می‌کند.

عناصر خیابان و سوییچ

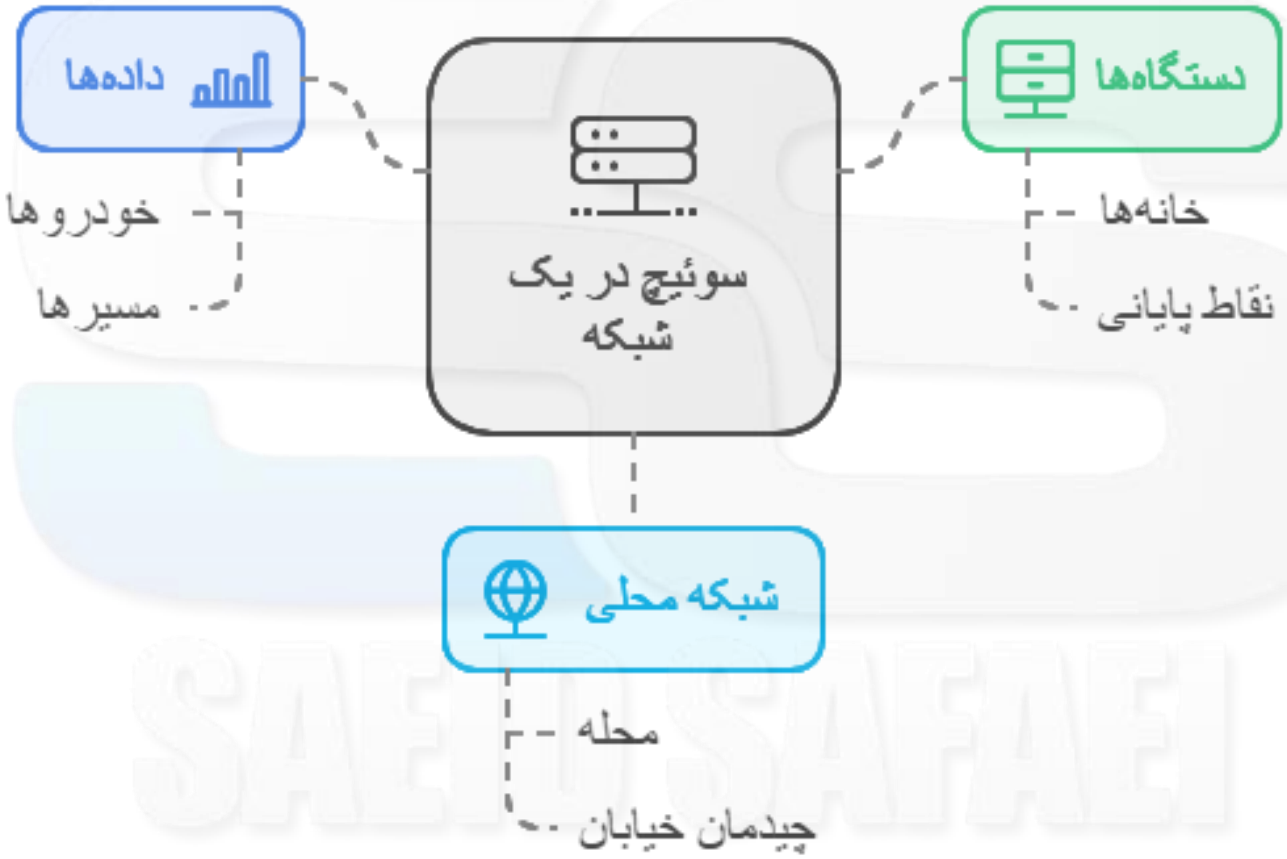
۱- خانه‌ها (دستگاه‌ها): در خیابان، هر خانه معادل یک دستگاه (مانند کامپیوتر، پرینتر یا سرور) در شبکه است.

۲- پلاک خانه ها MAC Address Table : سوییچ با استفاده از یک جدول آدرس MAC مشخص می‌کند هر دستگاه (خانه) به کدام پورت متصل است و خودرو (داده) را به مسیر درست هدایت می‌کند.

۳- چراغ‌های راهنمایی Collision Management : سوییچ به طور هوشمند از برخورد داده‌ها (ترافیک) جلوگیری می‌کند و اجازه می‌دهد هر خودرو (داده) بدون توقف به مقصد برسد.

۴- خیابان اصلی Backplane : خیابان اصلی داخل یک محله مانند مسیر اصلی داده در سوییچ عمل می‌کند که تمام اتصالات بین دستگاه‌ها از طریق آن صورت می‌گیرد.

عناصر خیابان و سوییچ



تعریف Backplane:

Backplane در تجهیزات شبکه (مانند سوییچ‌ها و روترها) یا دستگاه‌های الکترونیکی، یک زیرساخت فیزیکی است که برای اتصال اجزای مختلف داخلی دستگاه استفاده می‌شود.

این مفهوم در تجهیزات شبکه اهمیت زیادی دارد، زیرا عملکرد آن به‌طور مستقیم بر سرعت و کارایی انتقال داده در دستگاه تاثیر می‌گذارد.

پس:

Backplane به مسیری داخلی و پرسرعت گفته می‌شود که تمام پورت‌ها و ماژول‌های یک دستگاه (مانند یک سوییچ) را به هم متصل می‌کند و به آن‌ها اجازه می‌دهد داده‌ها را با سرعت بالا تبادل کنند.

نحوه عملکرد Backplane

وظیفه اصلی Backplane این است که داده‌ها را بین پورت‌های ورودی و خروجی یا ماژول‌های داخلی منتقل کند.

در یک سوییچ شبکه، وقتی داده‌ای از یک دستگاه وارد یکی از پورت‌ها می‌شود، از طریق Backplane به پورت مقصد هدایت می‌شود.

سرعت و ظرفیت Backplane مشخص می‌کند که یک سوییچ یا روتر تا چه اندازه می‌تواند ترافیک را مدیریت کند.

ویژگی‌های کلیدی Backplane

۱- سرعت انتقال بالا: Backplane باید ظرفیت انتقال داده‌های موردنیاز تمام پورت‌های دستگاه را به‌صورت همزمان داشته باشد.

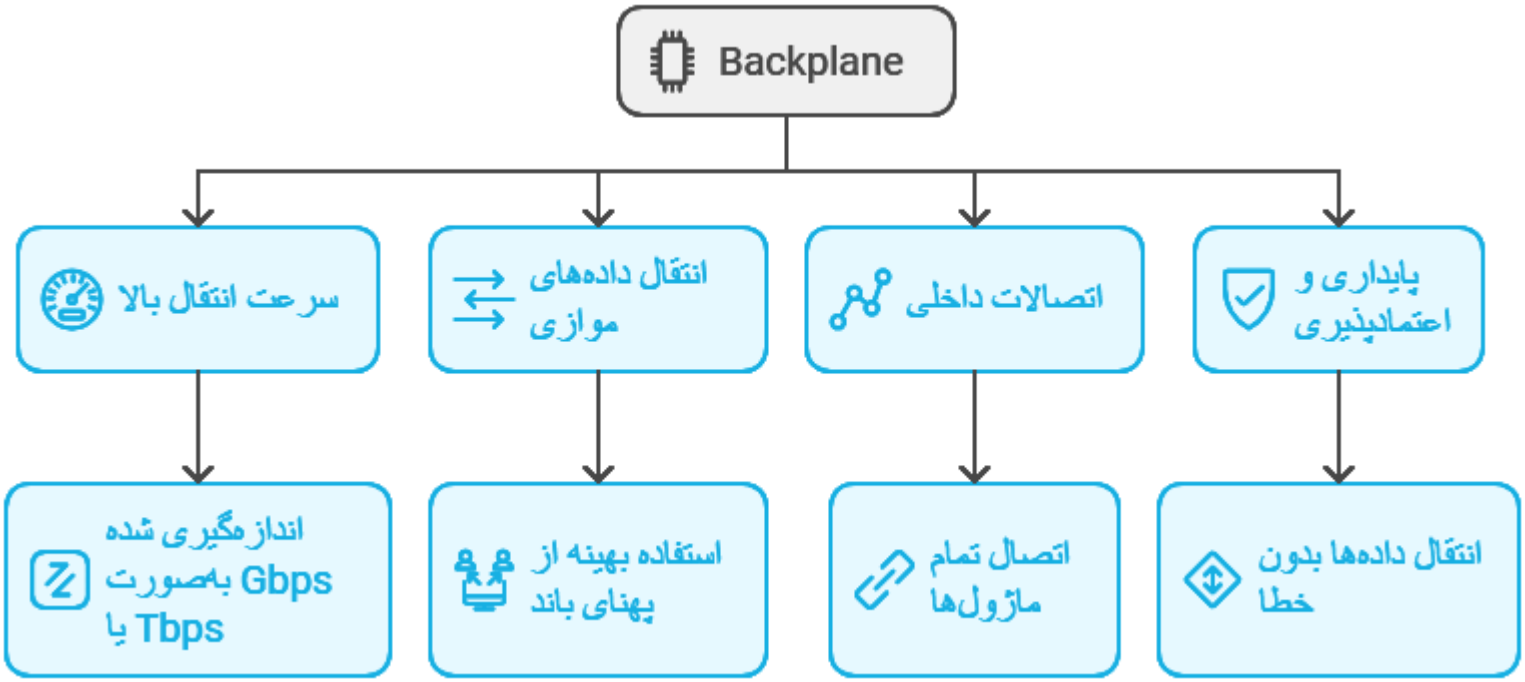
معمولاً سرعت آن به‌صورت Gbps یا Tbps بیان می‌شود.

۲- موازی‌سازی داده‌ها: Backplane داده‌ها را به‌صورت موازی (نه سریالی) انتقال می‌دهد تا از تمام پهنای باند استفاده شود.

۳- اتصالات داخلی: Backplane به‌عنوان یک ستون فقرات برای ارتباطات داخلی عمل می‌کند و تمام ماژول‌ها و اجزای دستگاه را به هم متصل می‌سازد.

۴- پایداری و اعتمادپذیری: طراحی Backplane باید به گونه‌ای باشد که حتی در شرایط سنگین و فشار ترافیکی، داده‌ها بدون تأخیر یا خطا منتقل شوند.

ویژگی‌های کلیدی Backplane



Backplane مسئول انتقال داده‌ها بین پورت‌های سوییچ است.

مثلاً در یک سوییچ با ۴۸ پورت Gbps۱، ظرفیت Backplane باید حداقل Gbps۹۶ باشد (۴۸ پورت برای ارسال و ۴۸ پورت برای دریافت).

ظرفیت Backplane

1-Non-blocking Backplane:

در این نوع، Backplane ظرفیت کافی برای انتقال همزمان تمام ترافیک ورودی و خروجی دارد. این ویژگی برای سوییچ‌های حرفه‌ای و با کارایی بالا ضروری است.

2-Blocking Backplane:

در این نوع، ظرفیت Backplane کمتر از مجموع ترافیک ورودی و خروجی است و ممکن است در شرایط پرترافیک، داده‌ها با تأخیر مواجه شوند.

تعریف Uplink:

آپ‌لینک Uplink در شبکه به اتصال یا پورتی گفته می‌شود که برای ارسال داده‌ها از یک دستگاه به دستگاه دیگر در سطح بالاتر یا شبکه دیگر استفاده می‌شود.

این مفهوم معمولاً در سوییچ‌ها، روترها، مودم‌ها و دستگاه‌های مشابه به کار می‌رود.

در واقع آپ‌لینک پورت یا کانکشن خاصی است که برای اتصال یک دستگاه شبکه (مانند سوییچ) به یک دستگاه دیگر یا یک شبکه بالادستی (مانند روتر یا سوییچ مرکزی) استفاده می‌شود.

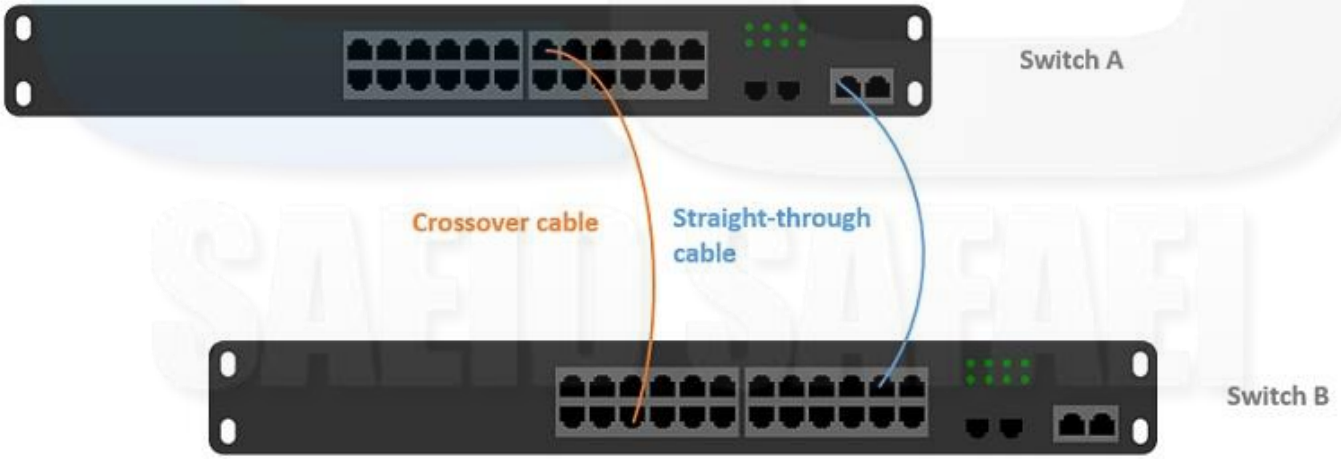
وظیفه آن فراهم کردن راه ارتباطی بین شبکه‌های مختلف یا دستگاه‌های مستقل است.

تعریف Uplink:

اگر شبکه را به یک ساختمان تصور کنیم:

آپ‌لینک: آسانسوری است که افراد را از طبقات پایین‌تر به طبقات بالاتر (مثلاً از سوییچ طبقه ۱ به سوییچ مرکزی) منتقل می‌کند.

دان‌لینک: آسانسوری است که افراد را از طبقات بالاتر به پایین‌تر می‌آورد.



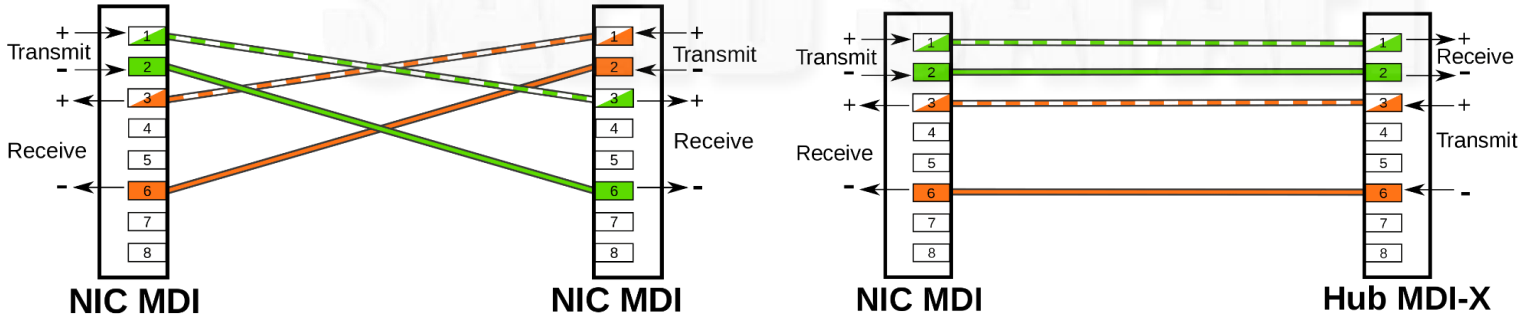
پورت‌های اختصاصی Uplink :

در بسیاری از سوییچ‌ها، پورت‌های خاصی برای آپ‌لینک طراحی شده‌اند که سرعت بالاتری دارند یا از فیبر نوری پشتیبانی می‌کنند.

این پورت‌ها معمولاً جدا از پورت‌های عادی (مثلاً پورت‌های RJ-45 قرار دارند.) **(اتصال به صورت استریت)**

استفاده از پورت‌های عادی برای Uplink :

اگر پورت اختصاصی Uplink وجود نداشته باشد، یکی از پورت‌های عادی برای این منظور استفاده می‌شود. **(اتصال به صورت کراس آور در صورت عدم وجود** Auto-MDI/MDIX)



نحوه کارکرد Uplink

فرض کنید یک شرکت دارای چندین طبقه است:

در هر طبقه، چند دستگاه (کامپیوترها و پرینترها) به یک سوییچ کوچک متصل شده‌اند.

این سوییچ‌ها از طریق پورت آپ‌لینک به سوییچ اصلی در مرکز داده متصل می‌شوند.

سوییچ اصلی داده‌ها را مدیریت کرده و به روتر یا شبکه گسترده‌تر WAN/Internet انتقال می‌دهد.

مقایسه آپ‌لینک و بک‌پلین

ویژگی	آپ‌لینک (Uplink)	بک‌پلین (Backplane)
محل استفاده	اتصال بین دستگاه‌های شبکه	اتصال داخلی بین اجزای یک دستگاه
هدف اصلی	ارتباط بین شبکه‌ها یا دستگاه‌های مختلف	مدیریت ارتباطات داخلی در یک دستگاه
نوع اتصال	خارجی (کابل شبکه یا فیبر نوری)	داخلی (بدون کابل)
پهنای باند	محدود به سرعت پورت (مثلاً 1Gbps)	معمولاً بسیار بالا (چندین Tbps)
مثال	اتصال یک سوییچ به یک روتر	انتقال داده بین پورت‌های یک سوییچ

آپ‌لینک: مثل یک جاده بین دو شهر است که شهر اول (سوییچ کوچک) را به شهر دوم (سوییچ مرکزی یا روتر) متصل می‌کند.

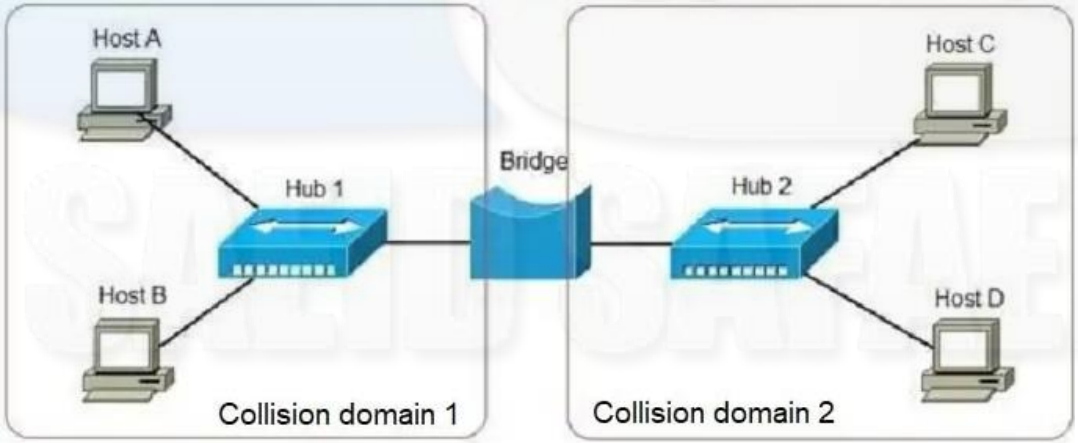
بک‌پلین: مثل خیابان‌های داخل یک شهر است که محله‌ها (پورت‌ها) را به هم متصل می‌کند.

Bridge

تعریف پل یا Bridge

بریج Bridge در لایه ۲ مدل OSI یکی از ابزارهای مهم شبکه‌های کامپیوتری است که برای متصل کردن چندین شبکه محلی LAN به یکدیگر و مدیریت جریان داده بین آنها استفاده می‌شود.

این دستگاه در لایه داده‌لینک Data Link Layer کار می‌کند و بر اساس آدرس‌های فیزیکی MAC Address عمل می‌کند.

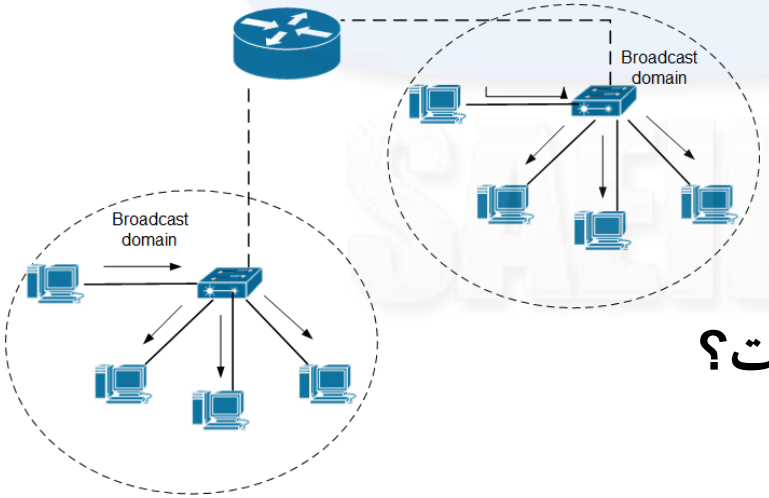


تعریف Broadcast Domain

(دامنه انتشار) به بخشی از یک شبکه گفته می‌شود که در آن تمام دستگاه‌ها می‌توانند پیام‌های Broadcast (پیام‌های همه‌پخشی) را دریافت کنند.

پیام‌های Broadcast برای ارسال اطلاعات به همه دستگاه‌های موجود در یک شبکه محلی LAN استفاده می‌شوند.

پس به زبان ساده به محدود ای از شبکه گفته می شود که اگر یک پره در شبکه برادکست کند، سایر گره های موجود در آن محدوده صدای او را می شنوند.



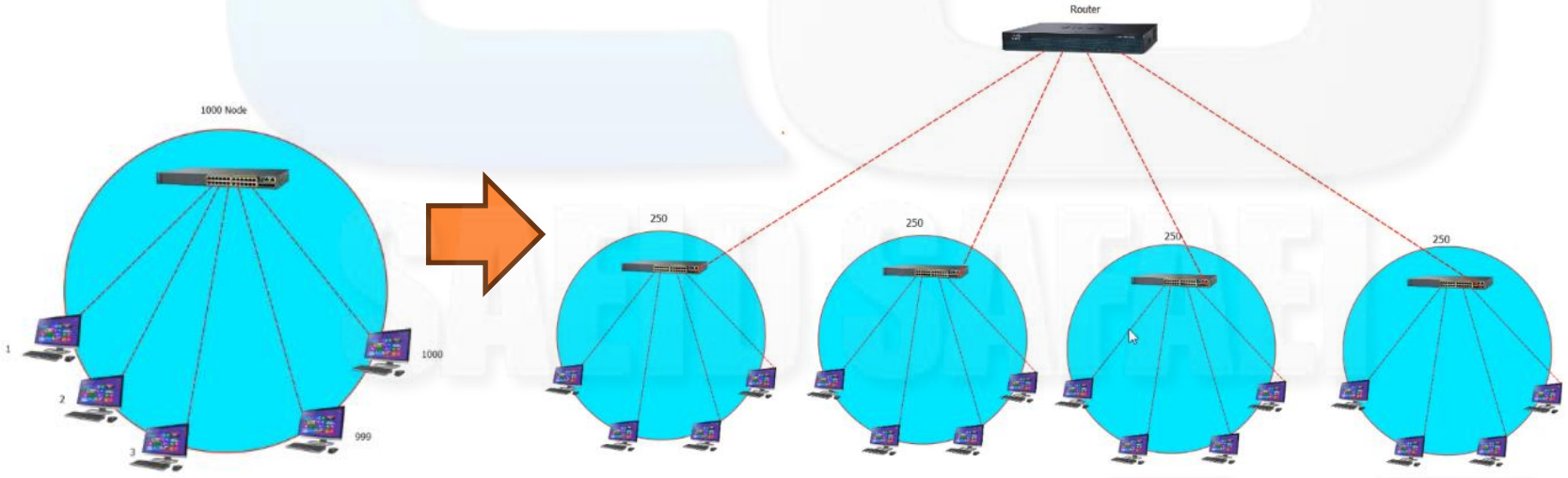
اینجا سوال پیش می آید:

اگر محدوده پخش بزرگ باشد خوب است؟

تعریف Broadcast Domain

در جواب این سوال فرض کنید یک دستگاه می خواهد DHCP بگیرد، باید برادکست کند، حال تمامی دستگاه های موجود در دامنه پیام اورا دریافت میکنند! (لزومی وجود ندارد همه درگیر این بار ترافیک شوند)

پس بهتر است در یک شبکه به جای یک برادکست دامین چندین برادکست دامین داشته باشیم. مثل (VLAN) یا استفاده از روتر (در فصل بعد میخوانیم!)



تعریف Collision Domain

Collision Domain یا دامنه برخورد مفهومی در شبکه‌های کامپیوتری است که به محدوده‌ای از شبکه اشاره دارد که در آن اگر دو دستگاه به طور همزمان داده ارسال کنند، برخورد Collision رخ می‌دهد.

این اتفاق معمولاً در شبکه‌های اترنت و هنگام استفاده از تکنولوژی‌های مبتنی بر CSMA/CD رخ می‌دهد.

در یک Collision Domain، تمامی دستگاه‌هایی که به یک محیط انتقال مشترک (مثل کابل یا هاب) متصل هستند، سیگنال‌های ارسالی یکدیگر را دریافت می‌کنند.

اگر دو دستگاه به‌طور همزمان داده ارسال کنند، سیگنال‌ها با هم تداخل پیدا می‌کنند و برخورد رخ می‌دهد.

این باعث می‌شود داده‌ها خراب شوند و نیاز به ارسال مجدد باشد.

تعریف Collision Domain

۱- هاب:

همه دستگاه‌های متصل به هاب در یک Collision Domain مشترک هستند.

برخوردها زیاد است و عملکرد شبکه کاهش می‌یابد.

۲- سوئیچ: هر پورت سوئیچ یک Collision Domain جداگانه ایجاد می‌کند. سوییچ از کانال ارتباطی Full Duplex استفاده میکند.

این معماری برخورد را تقریباً به صفر می‌رساند.

۳- روتر: روترها علاوه بر ایجاد Collision Domain جداگانه، Broadcast Domain ها را هم جدا می‌کنند.

استفاده از روترها یا سوئیچ‌های مدیریتی برای طراحی شبکه‌های بزرگ مناسب است.

مثال برای Collision Domain دامنه برخورد:

تصور کنید شما در یک اتاق شلوغ (مانند یک سالن جلسه) هستید، و همه افراد در حال صحبت با صدای بلند هستند. در این شرایط:

اگر دو نفر همزمان شروع به صحبت کنند، صدای آن‌ها با هم تداخل پیدا می‌کند و دیگران نمی‌توانند هیچ‌کدام را به‌درستی بشنوند.

برای جلوگیری از تداخل، هر نفر باید منتظر شود تا نفر قبلی صحبتش را تمام کند.

این دقیقاً مشابه اتفاقی است که در یک Collision Domain رخ می‌دهد.

در یک شبکه اترنت با تکنولوژی نیم‌دوبلکس Half-Duplex یا زمانی که دستگاه‌ها به یک هاب Hub متصل هستند:

- مکانیزم نیم‌دوبلکس به‌طور کامل نمی‌تواند تضمین کند که دستگاه‌ها دقیقاً **نوبتی** ارسال کنند.
- همه دستگاه‌ها در یک محیط انتقال مشترک هستند.
- اگر دو دستگاه به طور همزمان داده ارسال کنند، برخورد رخ می‌دهد و ارسال مجدد لازم می‌شود.

افزایش Collision Domain

در اکثر موارد افزایش تعداد Collision Domain برای بهبود عملکرد شبکه مفید است، زیرا این امر باعث کاهش احتمال برخورد داده‌ها می‌شود. اما این نکته به نوع دستگاه‌های شبکه و ساختار کلی شبکه نیز بستگی دارد.

۱- **کاهش برخورد داده‌ها**: هرچه تعداد Collision Domain ها بیشتر باشد، تعداد دستگاه‌ها در هر دامنه کمتر خواهد بود.

۲- **بهبود کارایی شبکه**: با کاهش برخوردها، دستگاه‌ها کمتر مجبور به ارسال مجدد داده‌ها می‌شوند. این باعث کاهش تأخیر و افزایش بهره‌وری می‌شود.

۳- **تفکیک بهتر ترافیک**: افزایش تعداد Collision Domain ها به این معنا است که هر دستگاه یا گروه کوچکتری از دستگاه‌ها می‌توانند بدون تداخل در یک دامنه جداگانه فعالیت کنند.

تفاوت برخورد و ازدحام

اگر شبکه از هاب Hub استفاده کند، تمام دستگاه‌ها در یک کالیژن دامین قرار دارند. بنابراین، اگر دو دستگاه به طور همزمان درخواست ARP ارسال کنند، احتمال برخورد وجود دارد.

شبکه‌های مبتنی بر سوییچ:

در شبکه‌های مدرن که از سوییچ استفاده می‌شود، هر پورت سوییچ یک کالیژن دامین مجزا است. بنابراین، برخورد در سطح لینک فیزیکی Layer 1 رخ نمی‌دهد.

اما اگر تعداد بسیار زیادی دستگاه به یک سوییچ متصل باشند و همزمان درخواست ARP ارسال کنند، ممکن است **ازدحام Congestion** در جدول ARP یا بافرهای سوییچ رخ دهد، ولی این به معنای برخورد نیست.

برخورد در بریج

بریج مانند سوییچ، شبکه را به کالیژن دامین‌های مجزا تقسیم می‌کند، اما نه به صورت کامل.

هر پورتی از بریج می‌تواند ترافیک را جدا کند، اما اگر چندین دستگاه در یک طرف بریج باشند (مثل شبکه‌ای که به یک پورت متصل است)، برخورد در همان طرف امکان‌پذیر است.

برخلاف سوییچ که برای هر پورت یک کالیژن دامین جدا ایجاد می‌کند، بریج معمولاً به تعداد لینک‌های اصلی تقسیم می‌شود.

در بریج‌ها برخورد می‌تواند در همان کالیژن دامین‌هایی که دستگاه‌ها به بریج متصل هستند، رخ دهد. برخلاف سوییچ، بریج نمی‌تواند کالیژن دامین‌ها را به صورت کامل و مجزا مدیریت کند.

جدول MAC (MAC Address Table) :

در بریج یکی از اجزای کلیدی است که برای مسیریابی و انتقال فریم‌ها استفاده می‌شود. این جدول، اطلاعاتی درباره آدرس‌های MAC دستگاه‌های متصل به شبکه و پورت‌های فیزیکی که از طریق آن‌ها به بریج متصل شده‌اند، ذخیره می‌کند.

در بریج جدول مک های دو شبکه به اشتراک گزاشته می شود.

ساختار جدول MAC :

جدول MAC معمولاً شامل ستون‌های زیر است:

آدرس MAC :آدرس فیزیکی دستگاه (به صورت ۱۲ کاراکتر هگزادسیمال).

شماره پورت: پورتی که دستگاه به آن متصل است.

مدت زمان Age : مدت زمانی که آدرس در جدول باقی می‌ماند.

آدرس MAC	شماره پورت	زمان باقی‌مانده
00:1A:2B:3C:4D:5E	Port 1	300 ثانیه
00:1F:2E:3D:4C:5B	Port 2	200 ثانیه

تفاوت بریج و سوییچ در رابطه با Collision

بریج Bridge، محدود کردن تصادم:

بریج شبکه را به چند Collision Domain تقسیم می‌کند.

اگر دو دستگاه در دو بخش مختلف شبکه که بریج آن‌ها را جدا کرده، داده ارسال کنند، تصادم رخ نمی‌دهد.

اما درون هر بخش از شبکه که بریج آن را مدیریت نمی‌کند، همچنان امکان تصادم وجود دارد.

عملکرد:

بریج یک جدول آدرس MAC دارد که از آن برای ارسال بسته‌ها به بخش مربوطه استفاده می‌کند.

اما چون بریج معمولاً تعداد **پورت‌های کمتری** دارد (معمولاً ۲ یا ۴ پورت)، در مقایسه با سوییچ تأثیر کمتری در کاهش تصادم دارد.

تفاوت بریج و سوییچ در رابطه با Collision

سوییچ Switch، جلوگیری کامل از تصادم:

هر پورت در سوییچ یک Collision Domain جداگانه ایجاد می‌کند.

به این معنی که حتی اگر دو دستگاه در پورت‌های مختلف سوییچ داده ارسال کنند، تصادمی رخ نمی‌دهد.

عملکرد:

سوییچ پیشرفته‌تر از بریج است و از یک جدول آدرس MAC بزرگ‌تر و کارآمدتر استفاده می‌کند.

هر دستگاه مستقیماً به یک پورت متصل است، و ارتباط بین دستگاه‌ها به‌صورت مستقیم از طریق همان پورت انجام می‌شود.

پس :

اگر دو شبکه را باهم بریج کنیم با توجه که هر پورت بریج شامل کالیژن دامین مجزا است دو کالیژن دامین خواهیم داشت و برخورد های هر شبکه روی شبکه دیگر تاثیر نخواهد گزاشت.

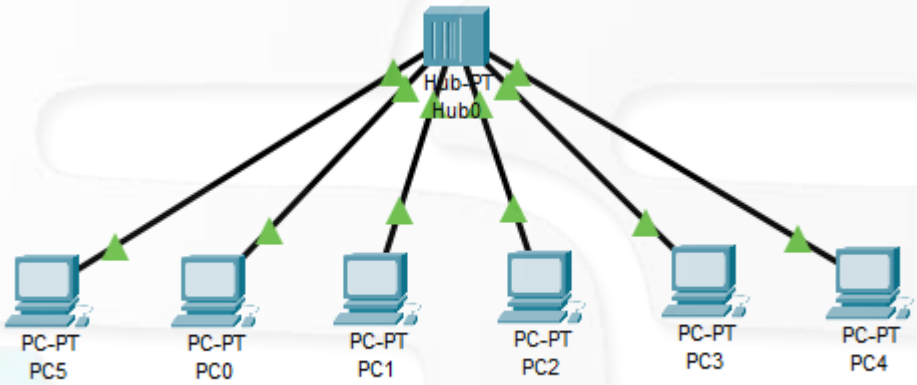
بریج تصادم را کاهش می‌دهد اما نمی‌تواند کاملاً از آن جلوگیری کند، زیرا هر بخش از شبکه که به بریج متصل است، همچنان یک Collision Domain باقی می‌ماند.

سوییچ با ایجاد یک Collision Domain برای هر پورت، تصادم را عملاً به صفر می‌رساند.

افزایش تعداد Collision Domain تجزیه آن‌ها خوب است و باعث کاهش تصادم می‌شود.

بررسی سناریوهای مختلف :

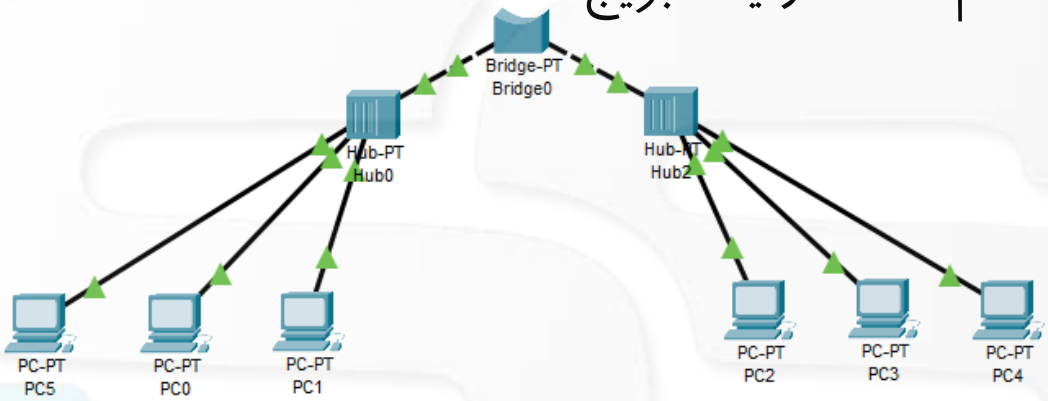
یک هاب با ۶ PC :



در شبکه‌ای که از یک هاب با ۶ کامپیوتر استفاده می‌کند، تمام دستگاه‌ها در یک Collision Domain و یک Broadcast Domain قرار دارند، که ممکن است باعث ایجاد مشکلاتی مانند تصادم‌های زیاد و ترافیک بیشتر شود.

بررسی سناریوهای مختلف :

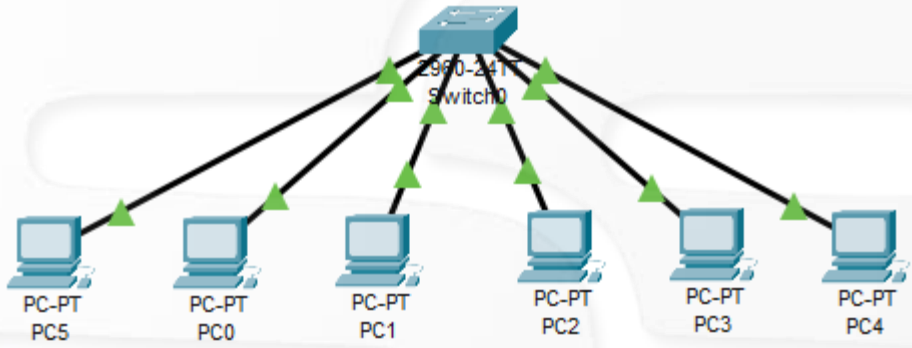
دو هاب هر کدام PC۳ و یک بریج:



- Collision Domain ها: دو عدد (هر هاب یک Collision Domain جداگانه ایجاد می‌کند).
- Broadcast Domain یک عدد (تمام دستگاه‌ها در یک Broadcast Domain قرار دارند).
- مزایا: کاهش تصادم‌ها در مقایسه با استفاده از یک هاب واحد.

بررسی سناریوهای مختلف :

یک سوییچ و ۶ PC



Collision Domain : ۶ عدد (هر پورت سوییچ یک Collision Domain جداگانه برای دستگاه‌های متصل دارد).

Broadcast Domain ۱ عدد (تمام دستگاه‌ها در یک Broadcast Domain قرار دارند).

مزایا:

کارایی بالا به دلیل جداسازی Collision Domainها.

کاهش قابل توجه تصادم‌ها در مقایسه با هاب.

امکان ارسال داده‌ها به صورت مستقیم بین دستگاه‌ها.

VLAN

Virtual Local Area Network

IEEE 802.1Q Higher Layer LAN

چالش شرکت با چندین بخش مختلف:

فرض کنید شرکت یک شرکت چندملیتی است که در سه بخش مختلف فعالیت دارد:

۱- بخش حسابداری

۲- بخش منابع انسانی

۳- بخش فناوری اطلاعات IT

در این شرکت، شبکه باید طوری پیکربندی شود که هر بخش به‌طور جداگانه و ایمن بتواند به منابع خود دسترسی داشته باشد و همچنین ترافیک‌های مختلف به‌طور بهینه مدیریت شود.

در شبکه این شرکت، هر بخش باید جداگانه عمل کند تا امنیت و عملکرد بهتری داشته باشد.

اهمیت جداسازی بخش های مختلف:

۱- جداسازی ترافیک: (اضافه کردن برادکست یا مدیریت Broadcast Domain)

ترافیک شبکه بخش حسابداری از ترافیک منابع انسانی جدا می‌شود. به این معنی که هیچ تداخلی بین اطلاعات مالی و اطلاعات پرسنلی وجود ندارد.

۲- امنیت بیشتر:

اگر کسی به شبکه دسترسی پیدا کند، فقط می‌تواند به اطلاعات بخش خود دسترسی داشته باشد، نه بخش‌های دیگر.

۳- کاهش شلوغی شبکه:

هر بخش فقط اطلاعات خودش را می‌فرستد، بنابراین شلوغی در شبکه کمتر می‌شود.

برای این منظور از VLAN استفاده می‌شود.

VLAN چیست؟

VLAN به شما اجازه می‌دهد تا دستگاه‌های متصل به یک یا چند سوئیچ فیزیکی را به گروه‌های منطقی تقسیم کنید، به‌طوری‌که این گروه‌ها مانند یک شبکه محلی جداگانه عمل کنند.

این جداسازی، بدون توجه به محل فیزیکی دستگاه‌ها انجام می‌شود و دستگاه‌های یک VLAN می‌توانند در ساختمان‌های مختلف باشند.

VLAN با استفاده از **برچسب‌گذاری Tagging** در **بسته‌های داده frames** اترنت کار می‌کند.

Tagging به معنای برچسب‌گذاری فریم داده در شبکه است.

در واقع، Tagging در شبکه‌های اترنت برای شناسایی و مدیریت بسته‌های داده‌ای که از چندین VLAN عبور می‌کنند، استفاده می‌شود.

چطور Tagging کار می‌کند؟

Tagging یک VLAN ID به هر بسته داده اضافه می‌کند.

این VLAN ID نشان می‌دهد که بسته به کدام VLAN متعلق است.

بسته‌های داده **به‌طور پیش‌فرض بدون این برچسب‌ها** ارسال می‌شوند، اما وقتی از VLAN استفاده می‌شود، باید این برچسب‌ها اضافه شوند تا هر بسته مشخص کند که در کدام VLANقرار دارد.

استاندارد IEEE 802.1Q برای برچسب‌گذاری Tagging بسته‌های داده در VLANها استفاده می‌شود.

هر فریم داده یک VLAN ID (**بین ۱ تا ۴۰۹۴**) دارد که مشخص می‌کند فریم متعلق به کدام VLAN است.

سوئیچ‌ها از این برچسب برای تصمیم‌گیری در مورد مسیریابی بسته استفاده می‌کنند.

انواع VLANها:

1-Data VLAN:

برای انتقال داده‌های کاربران معمولی استفاده می‌شود.

این VLAN به‌صورت جدا از ترافیک مدیریتی یا صوتی کار می‌کند.

2-Voice VLAN:

مخصوص ترافیک صوتی VoIP طراحی شده است.

برای اطمینان از کیفیت تماس‌ها، به ترافیک صوتی اولویت داده می‌شود.

3-Management VLAN:

برای مدیریت دستگاه‌های شبکه مانند سوئیچ‌ها و روترها.

معمولاً به VLANخاصی اختصاص داده می‌شود تا دسترسی به آن محدودتر باشد.

انواع VLANها:

4-Default VLAN

VLAN 1به‌طور پیش‌فرض در بیشتر سوئیچ‌های سیسکو و سایر سوئیچ‌های شبکه استفاده می‌شود.

5-Native VLAN

Native VLAN به VLAN ای گفته می‌شود که بدون Tagging برچسب زدن از طریق پورت‌های Trunkعبور می‌کند.

6-Private VLAN (PVLAN):

این نوع VLAN به دستگاه‌ها اجازه می‌دهد که در یک VLAN مشترک باشند، اما نتوانند به یکدیگر دسترسی داشته باشند.

دو نوع پورت در VLAN:

۱- Access Port پورت دسترسی:

برای اتصال دستگاه‌های کاربری (کامپیوتر، پرینتر، دوربین و غیره) به سوئیچ.

این پورت فقط به یک VLAN خاص تعلق دارد.

۲- Trunk Port پورت ترانک:

برای اتصال سوئیچ‌ها به یکدیگر یا اتصال به روتر.

می‌تواند چندین VLAN را حمل کند و با استفاده از پروتکل Q۸۰۲.۱، هر بسته داده را با شناسه VLAN (VLAN ID) برچسب‌گذاری می‌کند.

پورت ترانک Trunk Port چیست؟

یک نوع پورت در سوئیچ‌های شبکه است که برای انتقال ترافیک مربوط به چندین VLAN بین سوئیچ‌ها یا دیگر دستگاه‌ها (مانند روتر یا سرور) استفاده می‌شود.

پورت‌های ترانک اجازه می‌دهند که بسته‌های داده مربوط به چندین VLAN از یک پورت عبور کنند.

در حالت معمول، یک پورت سوئیچ فقط متعلق به یک VLAN خاص است.

اما پورت ترانک به گونه‌ای پیکربندی می‌شود که می‌تواند ترافیک مربوط به چندین VLANرا منتقل کند.

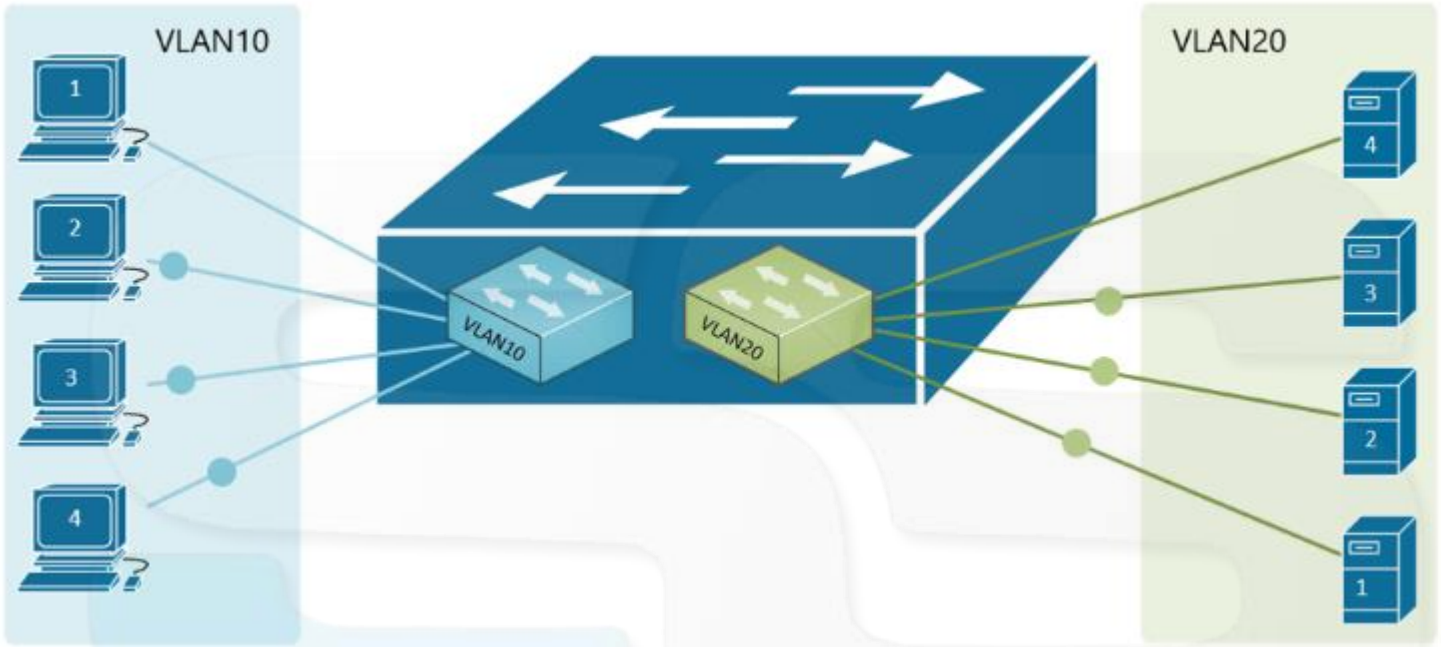
برای این کار، بسته‌های داده به یک برچسب VLAN (VLAN Tag) مجهز می‌شوند که نشان می‌دهد هر بسته به کدام VLAN تعلق دارد.

چطور برودکست در VLAN کار می‌کند؟

زمانی که یک دستگاه در VLAN خاصی مثلاً VLAN 10پیامی به‌صورت برودکست ارسال می‌کند، این پیام به‌طور مستقیم به تمامی دستگاه‌های دیگر در VLAN 10 ارسال می‌شود.

این پیام‌ها شامل پروتکل‌هایی مانند ARP، DHCP Discoverو دیگر پیام‌های برودکست هستند.

با این‌کار، فقط دستگاه‌هایی که در همان VLAN قرار دارند، این پیام‌ها را دریافت می‌کنند.



سوییچ در حالت عادی دارای یک Broadcast Domain یا دامنه برادکست است.
مثلا پیام‌های ARP (Address Resolution Protocol) که برای شناسایی آدرس MAC دستگاه‌ها در یک شبکه استفاده می‌شود، برای همه پورت ها برادکست میشود.
اما با تشکیل VLAN میتوانیم سوییچ را دارای چندین BD کنیم به عبارتی **تبدیل یک BD به چندین BD را VLAN می گویند.**

ویژگی‌های برودکست در VLAN :

محدود به VLAN خود: برودکست فقط در همان VLAN منتشر می‌شود. به این معنی که ترافیک برودکست نمی‌تواند از یک VLANبه VLANدیگر ارسال شود.

کاهش شلوغی در شبکه: بر خلاف شبکه‌های بدون VLAN، که ترافیک برودکست ممکن است تمام شبکه را شلوغ کند، در شبکه‌هایی که VLAN دارند، پیام‌های برودکست تنها در همان VLANمحدود می‌شوند.

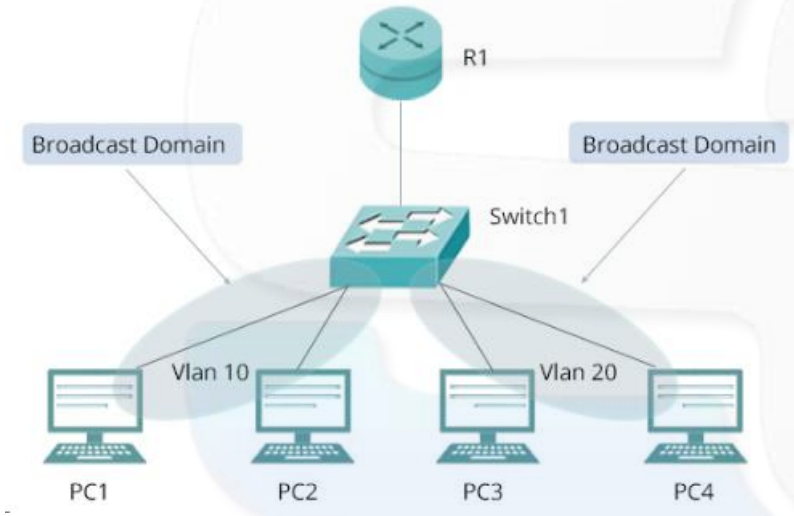
پروتکل‌هایی که از برودکست استفاده می‌کنند:

ARP (Address Resolution Protocol) برای پیدا کردن آدرس MACدستگاه‌ها.

DHCP Discover برای پیدا کردن سرور DHCP و درخواست آدرس IP

مثال: کاربرد VLANدر یک شرکت

یک شرکت می‌تواند از VLANها برای جداسازی بخش‌های مختلف استفاده کند:



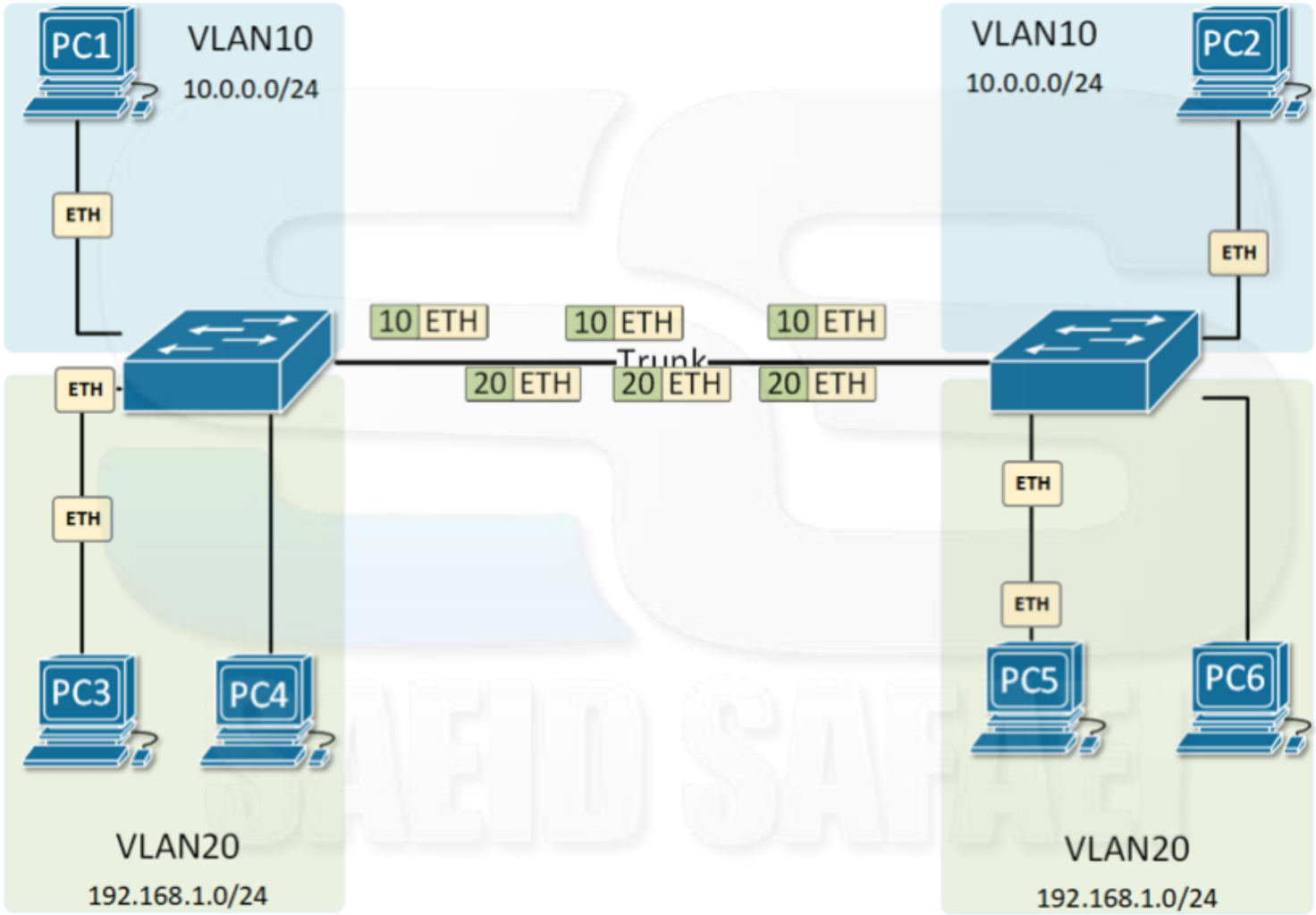
VLAN 10 برای تیم IT

VLAN 20 برای تیم حسابداری.

VLAN 30 برای منابع انسانی

سوئیچ‌ها ترافیک هر VLANرا جداگانه مدیریت می‌کنند و فقط از طریق روتر یا سوئیچ لایه ۳، این VLANها با یکدیگر ارتباط برقرار می‌کنند.

VLAN



آیا پورت ترانک نقش آپ لینک را ایفا می‌کند؟

بله، یک پورت ترانک می‌تواند آپ لینک باشد، به‌خصوص زمانی که چندین VLAN از یک سوئیچ به سوئیچ دیگر منتقل می‌شود. در این صورت، پورت ترانک به عنوان آپ لینک عمل می‌کند و ترافیک مربوط به چندین VLAN را بین دو سوئیچ منتقل می‌کند.

مثال:

فرض کنید دو سوئیچ در یک ساختمان داریم که VLANهای مختلف دارند و باید با هم ارتباط برقرار کنند. برای اتصال این دو سوئیچ از یک پورت ترانک استفاده می‌شود که امکان انتقال ترافیک مربوط به چندین VLANرا از طریق یک لینک فراهم می‌کند.

این لینک می‌تواند به عنوان آپ لینک عمل کند، زیرا ترافیک سوئیچ‌ها را از طریق این لینک به هم متصل می‌کند.

در یک سوئیچ، شما می‌توانید از یک پورت ترانک برای انتقال ترافیک مربوط به چندین VLAN استفاده کنید.

این یعنی اگر سوئیچ شما سه VLAN مثلاً VLAN 10، VLAN 20و VLAN 30 داشته باشد، نیازی نیست که سه پورت ترانک جداگانه برای هر VLAN ایجاد کنید.

یک پورت ترانک می‌تواند ترافیک مربوط به چندین VLANرا از طریق یک لینک واحد منتقل کند. این به کمک برچسب‌گذاری VLAN که معمولاً با پروتکل Q۸۰۲.۱ انجام می‌شود انجام می‌شود.

به این ترتیب، ترافیک برای هر VLAN با استفاده از برچسب VLAN (VLAN Tag) مشخص می‌شود تا دستگاه مقصد بتواند تشخیص دهد که بسته به کدام VLAN مربوط است.

مثال عملی:

فرض کنید شما یک سوئیچ دارید که سه VLAN به نام‌های VLAN 10، VLAN 20 و VLAN 30 تعریف شده‌اند.

اگر بخواهید ترافیک این سه VLAN را بین سوئیچ‌ها انتقال دهید، می‌توانید فقط یک پورت ترانک بین سوئیچ‌ها برقرار کنید.

پورت ترانک با استفاده از پروتکل Q۸۰۲.۱ برای هر بسته‌ای که ارسال می‌شود، یک برچسب VLAN اضافه می‌کند.

این برچسب به سوئیچ مقصد کمک می‌کند تا بسته را به VLAN مناسب هدایت کند.

VLAN

ویژگی	پورت ترانک	بک پلین	آپ لینک
تعریف	پورت‌های شبکه‌ای که برای انتقال ترافیک چندین VLAN از یک سوئیچ به سوئیچ دیگر یا دستگاه‌های دیگر استفاده می‌شود.	مسیر داخلی در یک دستگاه (مانند سوئیچ) که اجزای مختلف دستگاه را به هم متصل می‌کند.	ارتباطی که یک دستگاه شبکه (معمولاً سوئیچ) را به دستگاه دیگر یا شبکه‌های بالاتر متصل می‌کند.
موقعیت	بین سوئیچ‌ها، روترها یا دیگر دستگاه‌ها برای ارتباط بین چندین VLAN.	داخل یک دستگاه شبکه برای انتقال داده‌ها بین بخش‌های مختلف (مثلاً پورت‌ها و پردازنده‌ها).	معمولاً بین سوئیچ‌ها و روترها برای انتقال ترافیک به شبکه‌های دیگر (مانند اینترنت).
هدف اصلی	انتقال ترافیک مربوط به چندین VLAN از یک پورت از سوئیچ به سوئیچ یا دستگاه‌های دیگر.	فراهم کردن ارتباطات داخلی بین بخش‌های مختلف دستگاه مانند پردازنده، حافظه و پورت‌ها.	ارتباط با دستگاه‌ها یا شبکه‌های بیرونی به منظور انتقال داده‌ها و ترافیک شبکه.
پروتکل‌ها	معمولاً از **پروتکل 802.1Q** برای برچسب‌گذاری بسته‌ها استفاده می‌شود.	معمولاً پروتکل خاصی ندارد، چون مربوط به ارتباطات داخلی دستگاه است.	معمولاً از پروتکل‌های مانند **Ethernet** برای اتصال به شبکه‌های بالاتر یا اینترنت استفاده می‌شود.
نقش	انتقال ترافیک VLANهای مختلف بین دستگاه‌ها.	ارتباط داخلی در دستگاه‌ها برای هماهنگی اجزا.	اتصال دستگاه‌های شبکه به یکدیگر یا به شبکه‌های بیرونی.
مثال	ارتباط بین دو سوئیچ با پورت‌های ترانک برای انتقال ترافیک VLAN 10 و VLAN 20.	بک پلین در سوئیچ که داده‌ها را بین پردازنده و پورت‌های مختلف سوئیچ منتقل می‌کند.	اتصال سوئیچ به روتر یا اینترنت از طریق پورت آپ لینک.

کد CLI برای تعریف Vlan در سوییچ Cisco

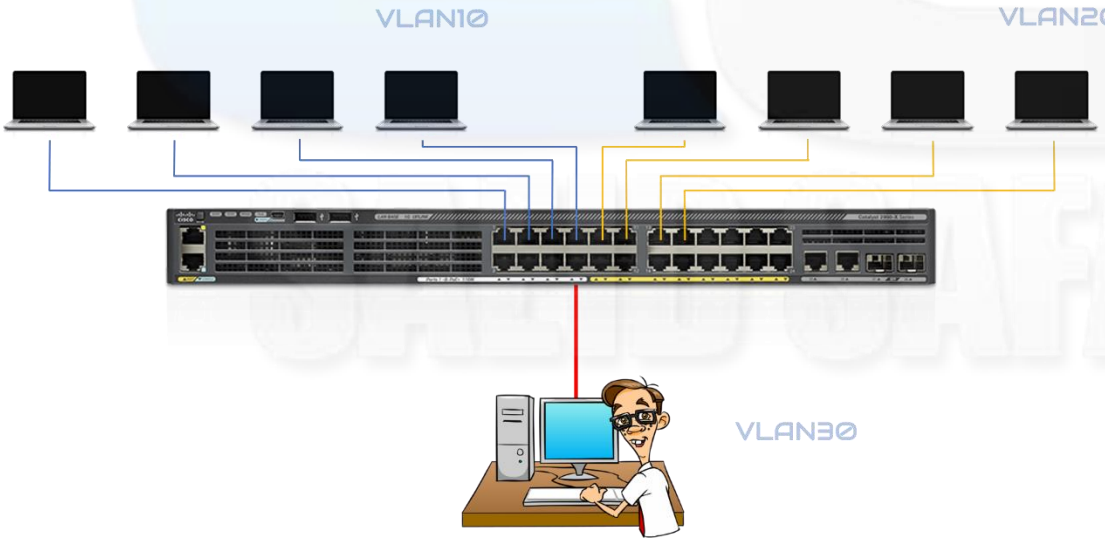
```
enable
configure terminal
# تعریف VLAN ها
vlan 10
name VLAN10
exit
vlan 20
name VLAN2
exit
# پیکربندی پورت‌های ۱ تا ۱۰ به VLAN 10
interface range GigabitEthernet0/1 - 10
switchport mode access
switchport access vlan 10
exit
# پیکربندی پورت‌های ۱۱ تا ۲۰ به VLAN 20
interface range GigabitEthernet0/11 - 20
switchport mode access
switchport access vlan 20
exit
```

```
# پیکربندی پورت ۲۵ به‌عنوان ترانک
interface GigabitEthernet0/25
switchport mode trunk
switchport trunk allowed vlan 10,20
exit
```

مفهوم Black Hole VLAN

بلک هول VLAN (Black Hole VLAN) یک مفهوم در شبکه‌های کامپیوتری است که معمولاً به VLAN هایی اطلاق می‌شود که ترافیک شبکه به آن‌ها هدایت می‌شود اما هیچ‌گونه دستگاه یا موجودیتی در آن‌ها وجود ندارد تا بتواند ترافیک را پردازش کند یا پاسخی ارسال کند.

این وضعیت معمولاً منجر به گم شدن بسته‌ها و از دست رفتن ارتباطات در شبکه می‌شود.



مفهوم Black Hole VLAN

پس باید :

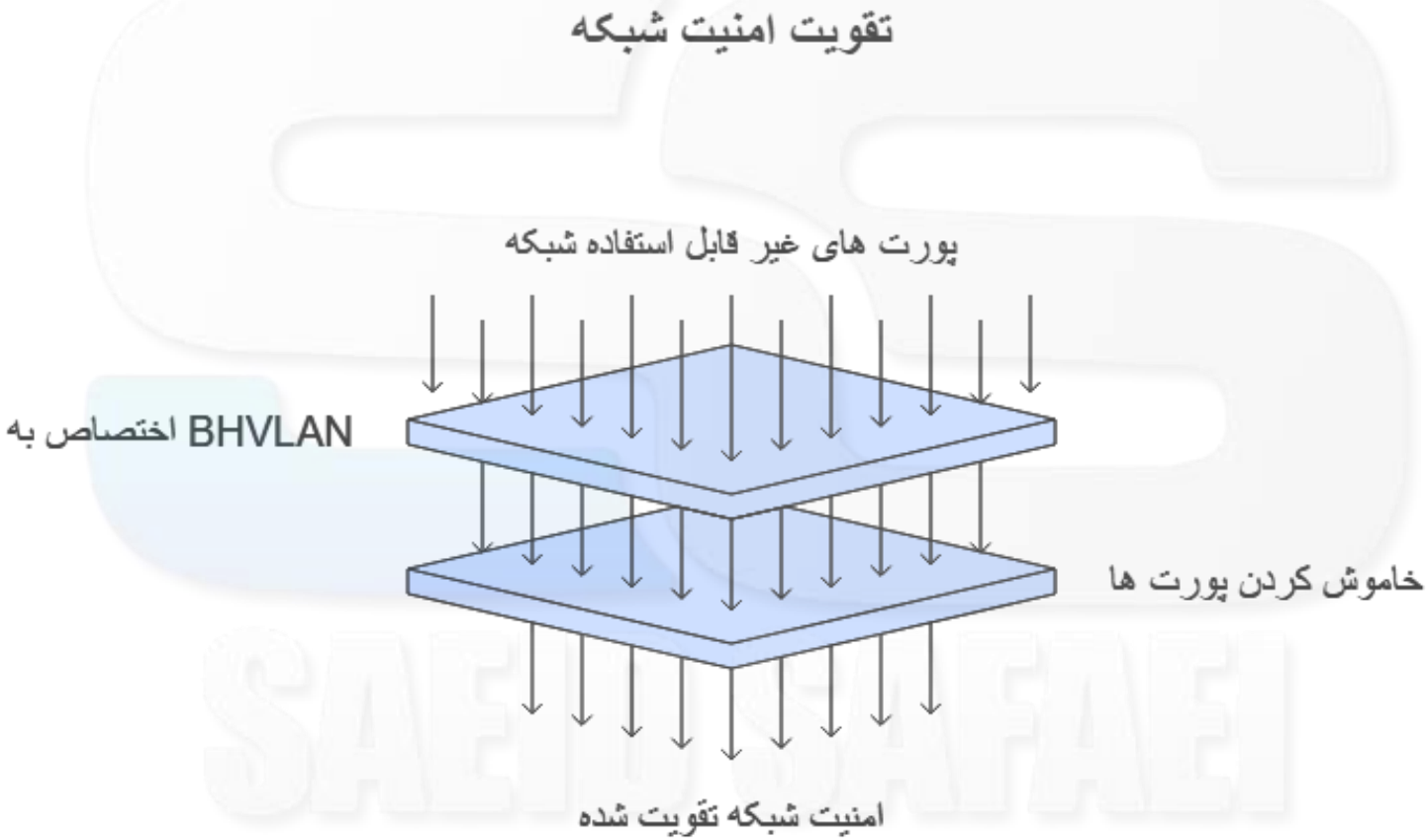
۱- تمام پورت های غیر قابل استفاده را در یک VLAN دیگر(BHVLAN) قرار دهیم.

۲- تمام پورت های غیر قابل استفاده را خاموش کنیم.

استفاده از Black Hole VLAN و خاموش کردن پورت‌های غیرقابل استفاده به روش‌های مختلف، هر دو راهکارهایی هستند که می‌توانند در جلوگیری از مشکلات شبکه و امنیت کمک کنند.

هنگامی که پورت‌ها به این VLAN اختصاص می‌یابند، سوئیچ‌ها دیگر نیازی به مدیریت ترافیک برای این پورت‌ها نخواهند داشت و ترافیک به این VLAN گم می‌شود.

مفهوم Black Hole VLAN



STP

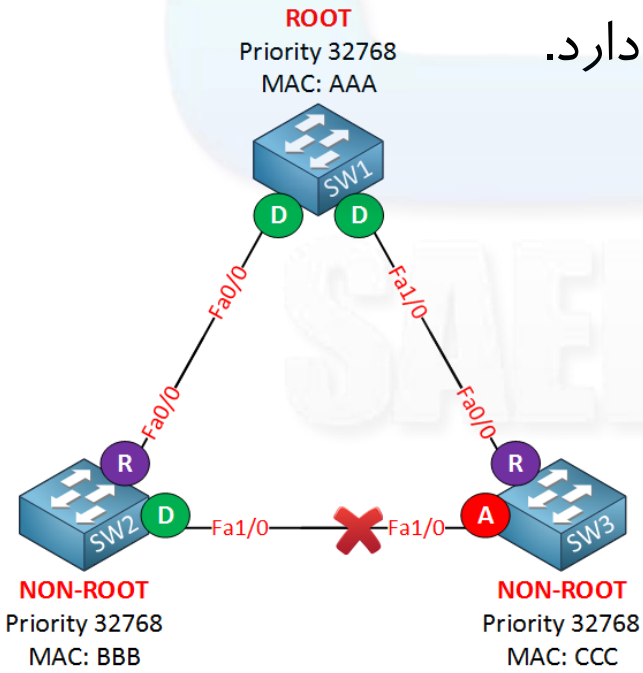
Spanning Tree Protocol

IEEE 802.1D Higher Layer LAN

STP یا Spanning Tree Protocol :

یک پروتکل لایه ۲ در شبکه‌های کامپیوتری است که برای جلوگیری از حلقه‌های (Loop) شبکه‌ای و مدیریت مسیرهای انتقال در شبکه‌های سوئیچ شده استفاده می‌شود.

این پروتکل توسط IEEE 802.1D تعریف شده است و به سوئیچ‌ها کمک می‌کند تا یک توپولوژی بدون حلقه ایجاد کنند و مطمئن شوند که فقط یک مسیر برای انتقال داده‌ها بین دو دستگاه وجود دارد.



نسخه های مختلف STP

ویژگی‌ها	STP	RSTP	MSTP	PVST	+PVST	+RPVST
استاندارد IEEE	802.1D	802.1w	802.1s	-	-	-
زمان همگرایی	30-50 ثانیه	کمتر از 6 ثانیه	وابسته به Instance	طولانی	طولانی	سریع
مدیریت VLAN	ندارد	ندارد	دارد	دارد	دارد	دارد
تعداد Instanceها	1	1	قابل تنظیم	به تعداد VLAN	به تعداد VLAN	به تعداد VLAN
سازگاری	استاندارد	استاندارد	استاندارد	سیسکو	سیسکو	سیسکو
کاربرد	ساده	شبکه‌های کوچک	شبکه‌های VLAN محور	سیسکو محور	مختلط	سیسکو VLAN محور

برای شبکه‌های ساده، STP اصلی کافی است.

برای شبکه‌هایی که نیاز به همگرایی سریع دارند، RSTP یا +RPVST مناسب است.

برای شبکه‌های بزرگ با VLAN های متعدد، MSTP گزینه بهتری است.

اگر از تجهیزات سیسکو استفاده می‌کنید، +PVST یا +RPVST بهترین انتخاب هستند.

هدف پروتکل STP :

هدف اصلی STP جلوگیری از حلقه‌های شبکه‌ای است.

حلقه‌های شبکه‌ای زمانی رخ می‌دهند که چندین مسیر به صورت دایره‌ای به یکدیگر متصل شوند.

در این حالت، داده‌ها به طور بی‌پایان بین سوئیچ‌ها حرکت می‌کنند و باعث افت عملکرد و ایجاد ترافیک اضافی می‌شوند.

STP به سوئیچ‌ها کمک می‌کند تا بهترین مسیر را برای انتقال داده‌ها انتخاب کنند و مسیرهای غیرضروری را به طور موقت غیرفعال کنند.

در صورتی که مسیر فعال دچار مشکل شود، STP به طور خودکار یک مسیر جدید انتخاب می‌کند.

حلقه‌ها و مشکلات ایجاد شده توسط آنها:

حلقه‌ها در شبکه می‌توانند مشکلات زیادی ایجاد کنند:

۱- **ترافیک اضافی**: داده‌ها به صورت بی‌پایان در شبکه گردش پیدا می‌کنند.

۲- **افزایش ترافیک بر روی سوئیچ‌ها**: سوئیچ‌ها مجبور به پردازش و ارسال داده‌های اضافی خواهند شد.

۳- **نقص در انتقال داده‌ها**: از آنجا که سوئیچ‌ها در شبکه نمی‌دانند کدام مسیر بهترین است، ممکن است داده‌ها به مقصد نرسند یا به تأخیر بیفتند.

مثال از عملکرد STP :

فرض کنید سه سوئیچ A، Bو C داریم که به صورت دایره‌ای به هم متصل شده‌اند:

سوئیچ A به سوئیچ B متصل است.

سوئیچ B به سوئیچ C متصل است.

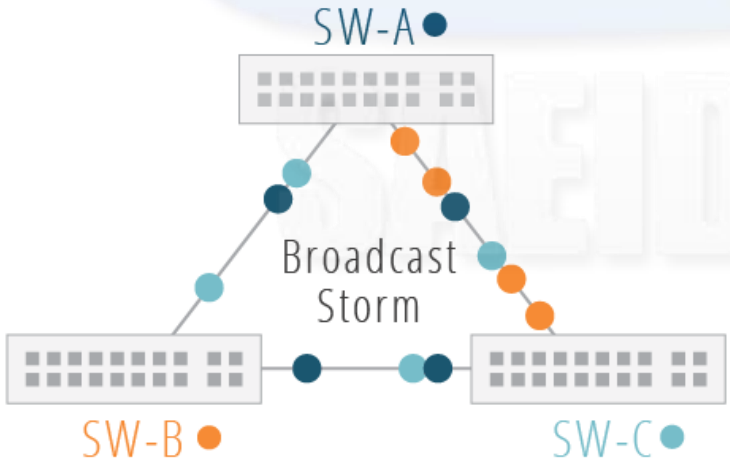
سوئیچ C به سوئیچ A متصل است.

اگر STP فعال باشد، یکی از این مسیرها به عنوان مسیر اصلی برای ارسال داده‌ها انتخاب می‌شود و مسیرهای دیگر به صورت مسدود می‌شوند تا حلقه‌ای در شبکه ایجاد نشود.

طوفان برادکست (Broadcast Storm):

در لایه دو TTL نداریم، فرض کنیم در یک شبکه لوپ تمامی دستگاهها به یک دیگر Ping بزنند، در این صورت با تعداد زیادی ARP به صورت برادکست، مواجه می شویم حال چنانچه گفته شد با توجه به فقدان TTL این پیام ها تا ابد در شبکه میچرخند و بلاک نمی شود وهمین باعث ایجاد ازدحام بسیار زیادی می گردد. به این واقعه **طوفان برادکست** گفته می شود.

جهت جلوگیری از این مشکل در لایه ۲ نیاز به پروتکل SNP می باشد.



عناصر اصلی STP :

1- Bridge Protocol Data Units (BPDU):

این پیام‌ها به سوئیچ‌ها اجازه می‌دهند که اطلاعات مربوط به توپولوژی شبکه را با یکدیگر به اشتراک بگذارند. BPDUs اطلاعاتی مانند اولویت سوئیچ و آدرس MAC سوئیچ‌ها را شامل می‌شود.

2- Root Bridge:

اولین و مهم‌ترین سوئیچ در شبکه که مسئول تعیین بهترین مسیرها برای ارسال داده‌ها است. سوئیچی که BPDU های معتبر را با کمترین اولویت دارد به عنوان Root Bridge انتخاب می‌شود.

3- Root Port:

پورت هر سوئیچ که نزدیک‌ترین مسیر به Root Bridge را دارد.

عناصر اصلی STP :

4- Designated Port:

پورت‌هایی که به عنوان بهترین مسیر برای ارسال داده‌ها به شبکه دیگر انتخاب می‌شوند.

5- Blocked Ports:

پورت‌هایی که به دلیل جلوگیری از ایجاد حلقه‌های شبکه غیرفعال شده‌اند. این پورت‌ها هیچ ترافیکی را ارسال نمی‌کنند.

مراحل عملکرد STP

۱- انتخاب Root Bridge:

تمامی سوئیچ‌ها یک BPDU ارسال می‌کنند که شامل اولویت و آدرس MAC آن‌ها است.

سوئیچی که کمترین اولویت را دارد به عنوان Root Bridge انتخاب می‌شود.

۲- انتخاب Root Port :

هر سوئیچ نزدیک‌ترین پورت به Root Bridge را به عنوان Root Port انتخاب می‌کند.

این پورت مسیریابی داده‌ها به سمت Root Bridge را مدیریت می‌کند.

مراحل عملکرد STP

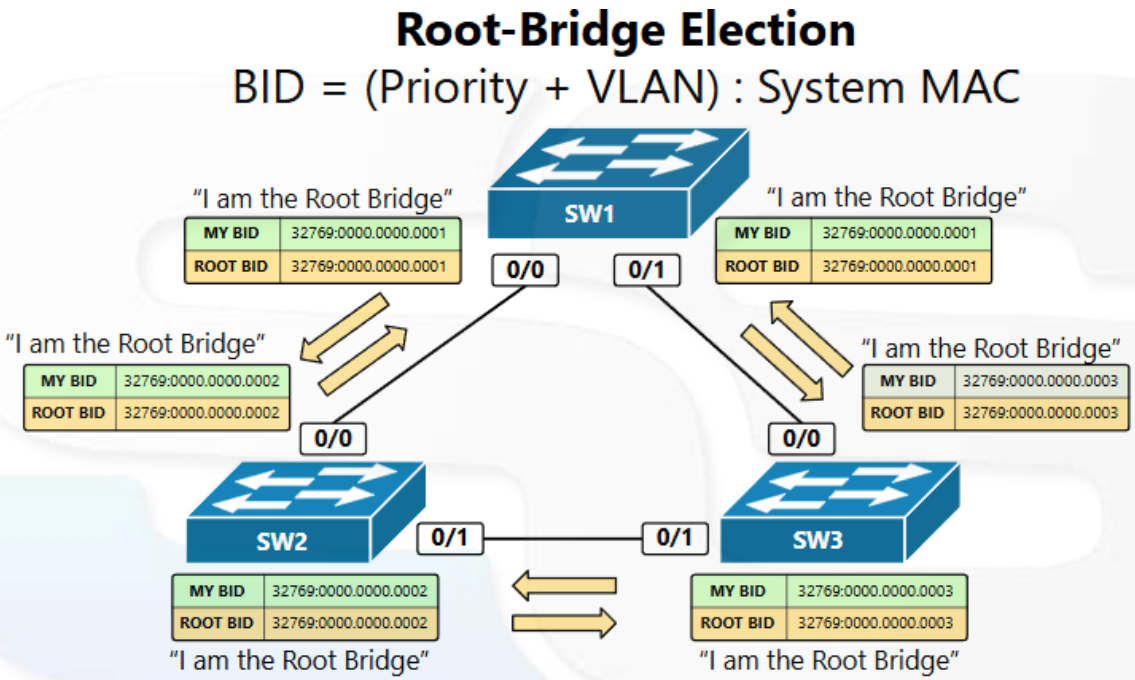
۳- انتخاب Designated Port:

پورت‌هایی که بهترین مسیر را برای ارسال داده‌ها به شبکه‌های دیگر دارند به عنوان Designated Port انتخاب می‌شوند.

۴- غیرفعال‌سازی پورت‌ها:

پورت‌هایی که هیچ کاربردی در ارسال داده‌ها ندارند یا باعث ایجاد حلقه می‌شوند، به طور مسدود یا Blocked در می‌آیند.

مراحل عملکرد STP



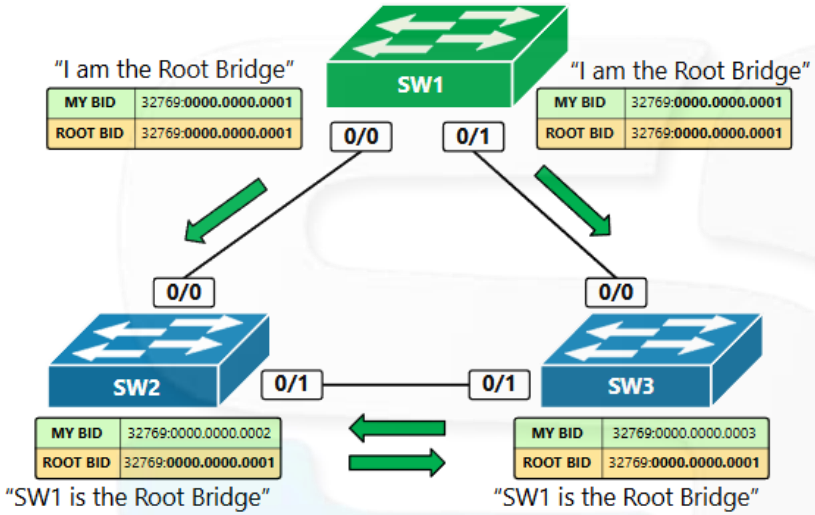
در این مثال سه سوئیچ با تنظیمات پیش‌فرض نشان داده شده‌اند که به صورت مثلث به یکدیگر متصل شده و به تازگی روشن شده‌اند.

فرآیند Spanning-Tree با این شروع می‌شود که تمام سوئیچ‌ها خود را به‌عنوان Root Bridge توپولوژی انتخاب کرده و اعلام می‌کنند.

در پیام‌های BPDU، هر سوئیچ مقدار BIDخود و BIDمربوط به Root Bridgeکه در همان لحظه می‌شناسد را قرار می‌دهد. اساساً هر سوئیچ می‌گوید: «من Root هستم».

مراحل عملکرد STP

Root-Bridge Election



سوئیچ SW2 دو پیام BPDU دریافت می‌کند، یکی از SW1 و دیگری از SW3 پیام BPDU از SW1 اعلام می‌کند که Root Bridge مقداری برابر با ۳۲۷۶۹:۰۰۰۰.۰۰۰۰.۰۰۰۱ دارد.

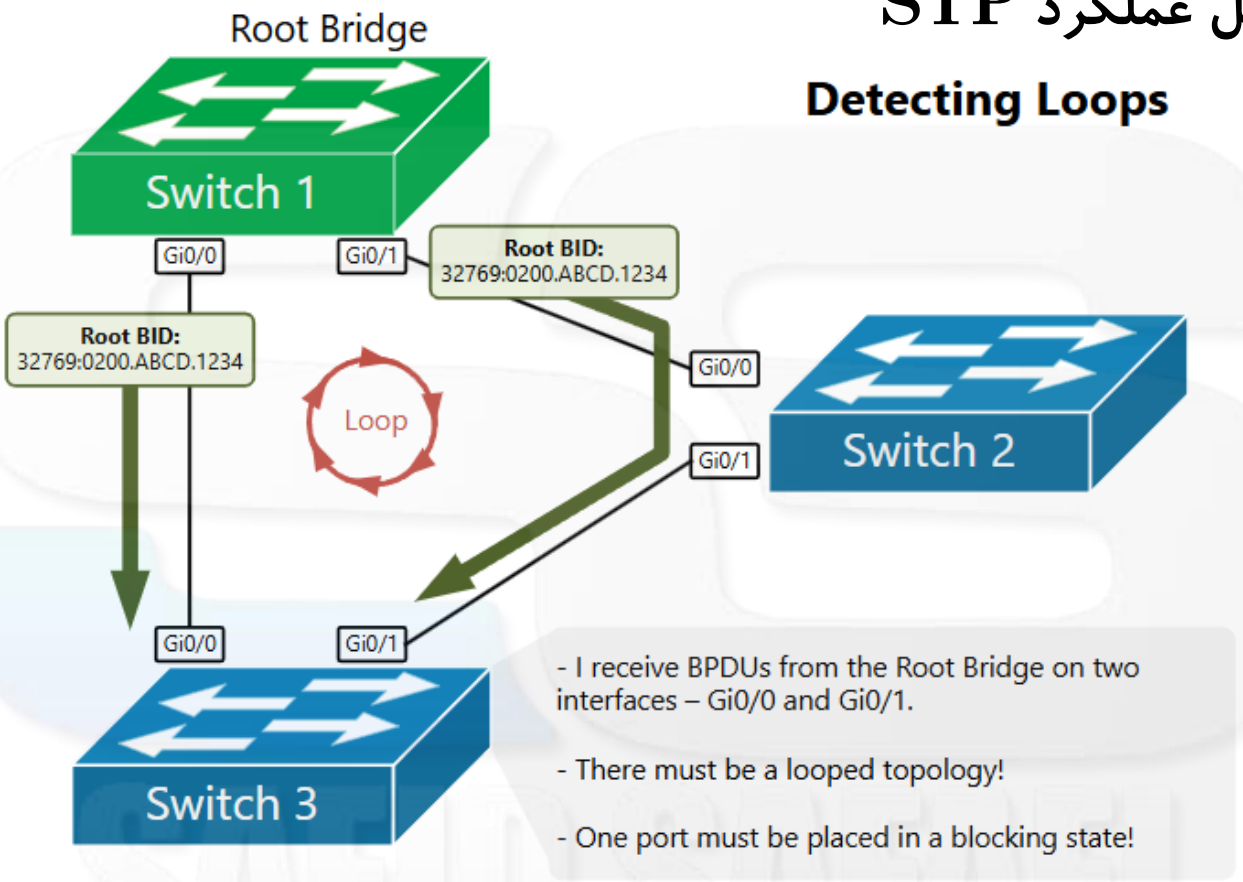
وقتی SW2 این مقدار را با مقدار Root Bridge که در آن لحظه می‌شناسد، یعنی ۳۲۷۶۹:۰۰۰۰.۰۰۰۰.۰۰۰۲ مقایسه می‌کند، واضح است که مقدار دریافت شده کمتر است. یک پیام BPDU که مقدار Root BID کمتری نسبت به مقدار خود سوئیچ دارد، Superior BPDU (پیام برتر) نامیده می‌شود.

هنگامی که SW2 این پیام برتر را دریافت می‌کند، تبلیغ خود به‌عنوان Root را متوقف کرده و شروع به ارسال این Superior BPDUبه سمت پایین‌دست Downstream به دیگر سوئیچ‌ها می‌کند

Downstream به این معنی است که ارسال BPDU ها به سمت Root متوقف می‌شود و فقط به دیگر پل‌ها ارسال می‌شود.

در پایان این فرآیند، تمام سوئیچ‌های موجود در توپولوژی باید توافق کنند که فقط یک Root Bridge وجود دارد و از دید همه سوئیچ‌ها، این Root Bridge یکسان است.

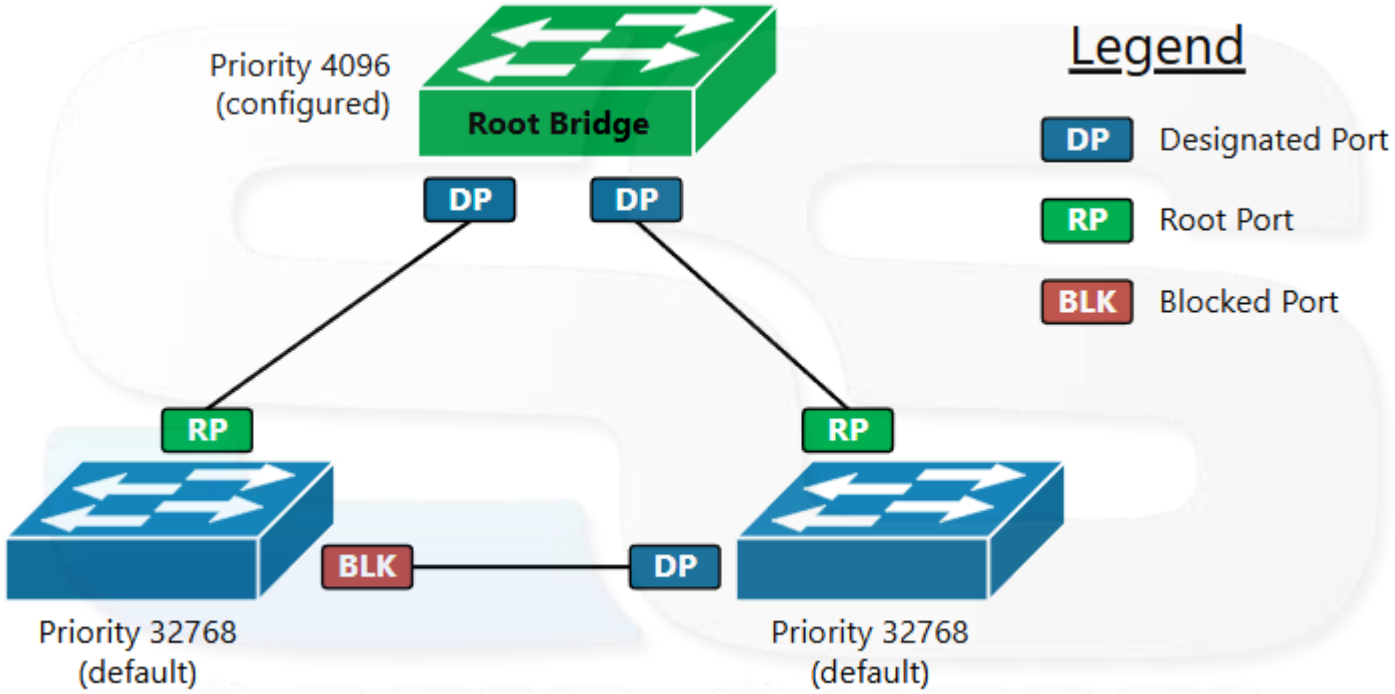
مراحل عملکرد STP



یک سوئیچ زمانی متوجه وجود یک حلقه می‌شود که BPDU هایی را از Root Bridge را از بیش از یک اینترفیس دریافت کند.

اگر یک سوئیچ BPDU های برتر Superior BPDUs را بیش از یک پورت دریافت کند، قطعاً یک حلقه وجود دارد و آن پورت باید در حالت Blocking قرار گیرد.

مراحل عملکرد STP



زمانی که توپولوژی به حالت همگرا Converged می‌رسد و هر سوئیچ پورت‌های خود را در نقش‌های صحیح قرار می‌دهد، همچنان BPDU ها بین سوئیچ‌ها مبادله می‌شوند تا وضعیت لینک‌ها را بررسی کنند.

اگر هر سوئیچی یک تغییر در توپولوژی را تشخیص دهد، همه سوئیچ‌ها دوباره نقش پورت‌های خود را محاسبه می‌کنند تا یک توپولوژی جدید بدون حلقه Loop-Free ایجاد شود.

با تشکر از همراهی شما

محمد سعید صفایی صادق