



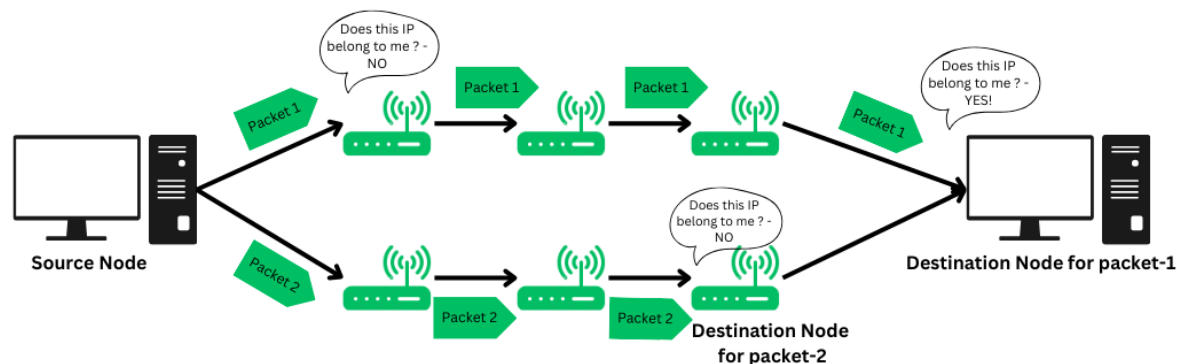
شبکه های کامپیوتری

(آمادگی برای آزمون Network+)

اسلاید نهم

(بخش اول مسیریابی)

مفاهیم مسیریابی: Routing: Hop و Leg، VLSM، FLSM، مفهوم سیستم خودمختار AS، جدول مسیریابی، دروازه پیش فرض، انواع اصلی پروتکل های مسیریابی، مفهوم AD



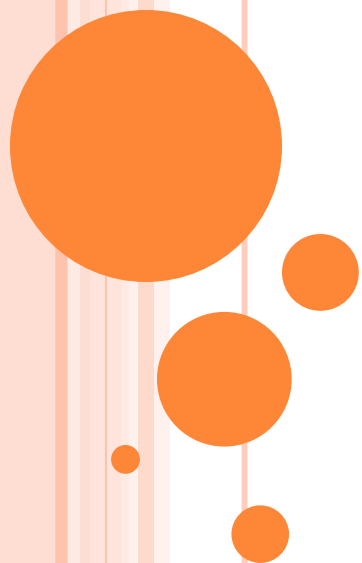
محمد سعید صفایی صادق

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

۱۴۰۳

مفاهیم مسیریابی

Routing Concepts



مسیر یابی

در فصل قبل به طور ساده سویچ را به عنوان یک خیابان مثال زدیم. حالا اگر بخواهیم از یک خیابان به خیابان دیگر برویم باید چکار کنیم؟ مثلاً یک بسته اطلاعاتی را بخواهیم از شبکه محلی به یک سرور در قاره ای دیگر ارسال کنیم...

آیا میتوان تمام جهان را با سویچ به یکدیگر متصل کرد؟ وقتی می‌خواهید از یک خیابان به خیابان دیگری بروید، از تقاطع استفاده می‌کنید.

در شبکه‌های کامپیوتری هم همین‌طور است. برای انتقال داده از یک شبکه محلی به یک شبکه دیگر (مثلاً از خانه شما به اینترنت)، به روتر نیاز داریم. روترها مانند تقاطع‌های بزرگ‌تری هستند که شبکه‌های مختلف را به هم متصل می‌کنند.

مسیر یابی

مثال: فرض کنید می‌خواهید از کامپیوتر خود در خانه، به یک وب‌سایت در اینترنت دسترسی پیدا کنید. این اتفاق چگونه می‌افتد؟

۱- ارسال درخواست: کامپیوتر شما درخواست را به صورت بسته‌های اطلاعاتی کوچک ارسال می‌کند.

۲- سفر در شبکه محلی: این بسته‌ها از طریق کابل شبکه به سویچ می‌رسند.

۳- انتخاب مسیر توسط روتر: سویچ بسته‌ها را به روتری که به اینترنت متصل است، هدایت می‌کند. روتر بهترین مسیر را برای رسیدن بسته‌ها به وب‌سایت انتخاب می‌کند.

۴- سفر در اینترنت: بسته‌ها از طریق شبکه جهانی اینترنت به سرور وب‌سایت مورد نظر می‌رسند.

۵- دریافت پاسخ: سرور وب‌سایت، پاسخ را به صورت بسته‌های اطلاعاتی به سمت کامپیوتر شما ارسال می‌کند.

۶- بازگشت به کامپیوتر: بسته‌ها مسیر برگشت را طی می‌کنند و به کامپیوتر شما می‌رسند.

تعاریف مختلف از Router یا مسیریاب:

۱- در واقع، روتر Router دستگاهی در شبکه‌های کامپیوتری است که وظیفه اصلی آن اتصال شبکه‌های مختلف و مسیریابی بسته‌های داده بین این شبکه‌ها است.

این اتصال شامل ارتباط بین NetID های مختلف یا زیرشبکه‌های متفاوت Subnets است.

۲- روتر با استفاده از پروتکل‌های مسیریابی مانند OSPF، RIP یا BGP مسیر بهینه برای ارسال بسته‌های داده به مقصد را پیدا می‌کند.

۳- روتر پیام‌های Broadcast را از عبور به شبکه‌های دیگر جلوگیری می‌کند و بدین ترتیب دامنه Broadcast را محدود می‌کند.

۴- روتر می‌تواند آدرس‌های داخلی Private را به آدرس‌های عمومی Public ترجمه کند تا دستگاه‌ها بتوانند به اینترنت دسترسی داشته باشند.

مسیر یابی

چرا به روتر نیاز است با همان سویچ نمی توان متصل شد؟

تصور کنید در یک شهر کوچک زندگی می کنید. در این شهر، چندین خیابان وجود دارد که هر کدام به خانه های مختلف منتهی می شوند.

برای اینکه ساکنان این خیابان ها بتوانند با هم ارتباط برقرار کنند، از یک سیستم تلفن محلی استفاده می کنند. این سیستم تلفن محلی را می توان به یک سوئیچ تشبیه کرد.

سوئیچ: در این مثال، سوئیچ مانند یک مرکز تلفن محلی است که تماس های تلفنی را بین خانه های یک خیابان یا یک منطقه کوچک جابه جا می کند. سوئیچ ها برای اتصال دستگاه هایی که در یک شبکه محلی قرار دارند، بسیار مناسب هستند.

حالا فرض کنید می خواهید با کسی در شهر دیگری تماس بگیرید. برای این کار، به یک مرکز تلفن اصلی نیاز دارید که بتواند تماس شما را به شهر دیگر وصل کند. این مرکز تلفن اصلی را می توان به یک روتر تشبیه کرد.

روتر: روتر مانند یک مرکز تلفن اصلی است که تماس های تلفنی را بین شهرها یا مناطق مختلف جابه جا می کند. روترها برای اتصال شبکه های مختلف به هم استفاده می شوند.

مسیریابی

چرا به روتر نیاز داریم؟

۱- انتخاب مسیر: روترها بهترین مسیر را برای رسیدن بسته‌های اطلاعاتی به مقصد انتخاب می‌کنند. این کار باعث می‌شود که بسته‌ها سریع‌تر و با کمترین تأخیر به مقصد برسند.

۲- اتصال شبکه‌های مختلف: روترها شبکه‌های محلی را به شبکه‌های گسترده‌تر مانند اینترنت متصل می‌کنند.

۳- تبدیل پروتکل‌ها: روترها می‌توانند پروتکل‌های مختلف شبکه را به یکدیگر تبدیل کنند.



مسیر یابی

در واقع، سویچ‌ها و روترها مکمل یکدیگر هستند:

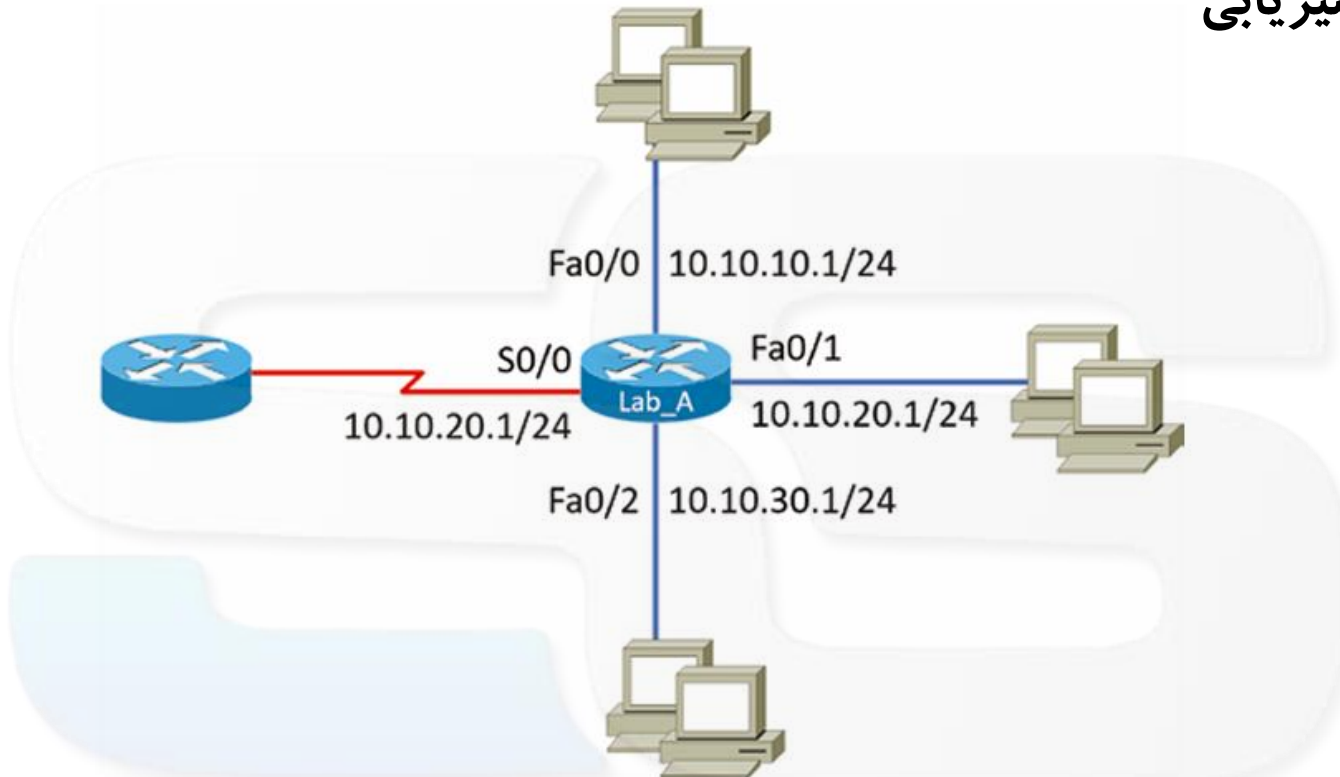
- سویچ‌ها وظیفه دارند که داده‌ها را در یک شبکه محلی جابه‌جا کنند.

- روترها وظیفه دارند که داده‌ها را بین شبکه‌های مختلف جابه‌جا کنند.

به عبارت ساده‌تر، اگر بخواهیم از یک خیابان به خیابان دیگری برویم، به یک تقاطع نیاز داریم (سویچ).

اما اگر بخواهیم از یک شهر به شهر دیگری برویم، به یک بزرگراه و یک سیستم راهنمایی و رانندگی نیاز داریم (روتر).

در نتیجه، برای ایجاد یک شبکه گسترده و پیچیده مانند اینترنت، به هر دو سوئیچ و روتر نیاز داریم.



- C 10.10.10.0/24 is directly connected, FastEthernet0/0
- C 10.10.20.0/24 is directly connected, FastEthernet0/1
- C 10.10.30.0/24 is directly connected, FastEthernet0/2
- C 10.10.40.0/24 is directly connected, Serial 0/0

دامنه پخش Broadcast Domain : مجموعه‌ای از دستگاه‌ها که می‌توانند همه بسته‌های پخش را دریافت می‌کنند.

دامنه کالیژن Collision Domain : مجموعه‌ای از دستگاه‌ها که ممکن است در هنگام ارسال داده با هم تداخل داشته باشند.
روترها مرز بین دامنه‌های پخش هستند.

به عبارت دیگر، هر طرف یک روتر یک دامنه پخش مجزا را تشکیل می‌دهد.
وقتی یک فریم پخش به روتر می‌رسد، روتر آن را در شبکه مقصد پخش نمی‌کند، بلکه آن را متوقف می‌کند. (روترها برادکست را دراپ می‌کند)

تصور کنید یک ساختمان اداری را که به چندین بخش تقسیم شده است. هر بخش یک شبکه محلی جداگانه دارد. اگر از روتر برای اتصال این شبکه‌ها استفاده شود، فریم‌های پخش که در یک بخش ارسال می‌شوند، به بخش‌های دیگر منتقل نمی‌شوند. این باعث می‌شود که ترافیک شبکه در هر بخش جداگانه باقی بماند و از ایجاد ترافیک اضافی در کل ساختمان جلوگیری شود.

تصور کنید یک ساختمان بزرگ با چندین طبقه و آپارتمان وجود دارد. هر طبقه یک شبکه محلی LAN جداگانه است.

روتر در این ساختمان مانند یک نگهبان عمل می‌کند که بسته‌های پستی (بسته‌های داده) را دریافت کرده و آن‌ها را به مقصد درست هدایت می‌کند.

دامنه پخش: اگر ساکن یکی از آپارتمان‌ها بخواهد به همه ساکنین ساختمان اطلاعیه‌ای بدهد، باید این اطلاعیه را در صندوق پستی همه آپارتمان‌ها قرار دهد. این کار شبیه به ارسال یک فریم پخش در شبکه است.

نقش روتر: اگر ساکن یکی از آپارتمان‌ها بخواهد نامه‌ای را برای ساکن دیگری در طبقه دیگر ارسال کند، نامه را به نگهبان (روتر) می‌دهد. نگهبان آدرس روی نامه را خوانده و نامه را به صندوق پستی صحیح در طبقه دیگر می‌برد.

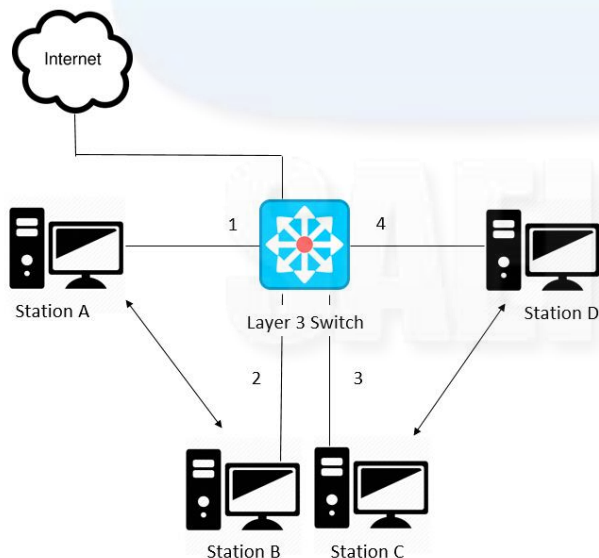
در اینجا روتر با بررسی آدرس مقصد، بسته را به شبکه صحیح هدایت می‌کند و از ارسال آن به سایر شبکه‌ها جلوگیری می‌کند.

تفاوت سویچ لایه ۲ و لایه ۳:

سویچ ها بر اساس Mac آدرس کار می کنند (لایه ۲)

حالا سویچ های L3 می توانند (IP ها را هم بشناسند) یعنی هم می توانند سویچینگ انجام دهد هم مسیریابی انجام می دهد.

سوئیچ لایه ۳ دستگاهی است که قابلیت های سوئیچینگ لایه ۲ و مسیریابی لایه ۳ را با هم ترکیب می کند. به عبارت دیگر، این نوع سوئیچ علاوه بر انتقال فریم های Ethernet بین پورت های خود، می تواند بسته های IP را نیز مسیریابی کند و از معماری کولپس کور Collapsed Core پیروی میکند.

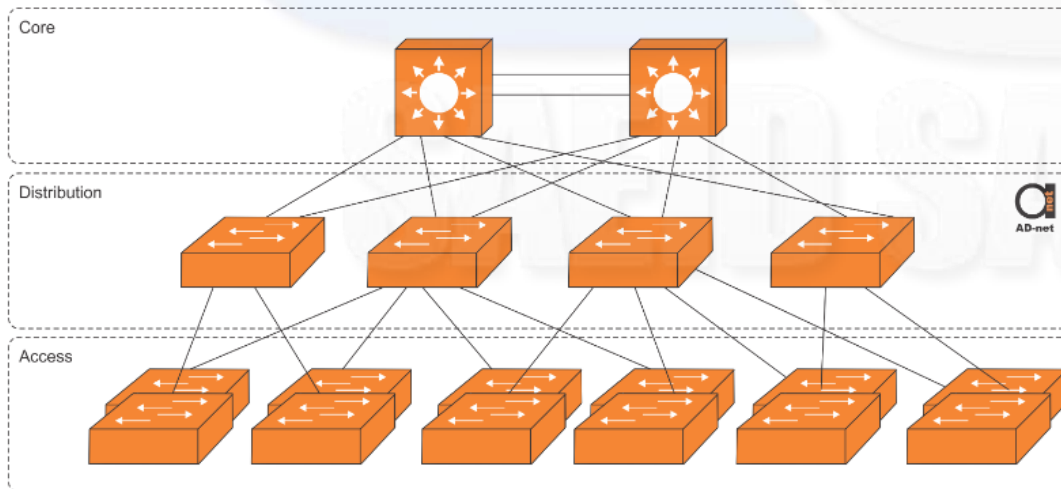


لایه‌های شبکه سنتی : Three-Tier Architecture :

۱- **Access Layer** : جایی که کاربران و دستگاه‌ها به شبکه متصل می‌شوند. (سوییچ‌هایی که مستقیم به دستگاه‌ها متصل هستند)

۲- **Distribution Layer** : مسئول مسیریابی و اعمال سیاست‌های شبکه. (سوییچ‌های این لایه بسیار قدرتمند هستند یعنی به هر پورت می‌توان یک سوییچ وصل کرد)

۳- **Core Layer** : ستون فقرات شبکه که وظیفه انتقال سریع داده‌ها بین بخش‌های مختلف شبکه را بر عهده دارد.

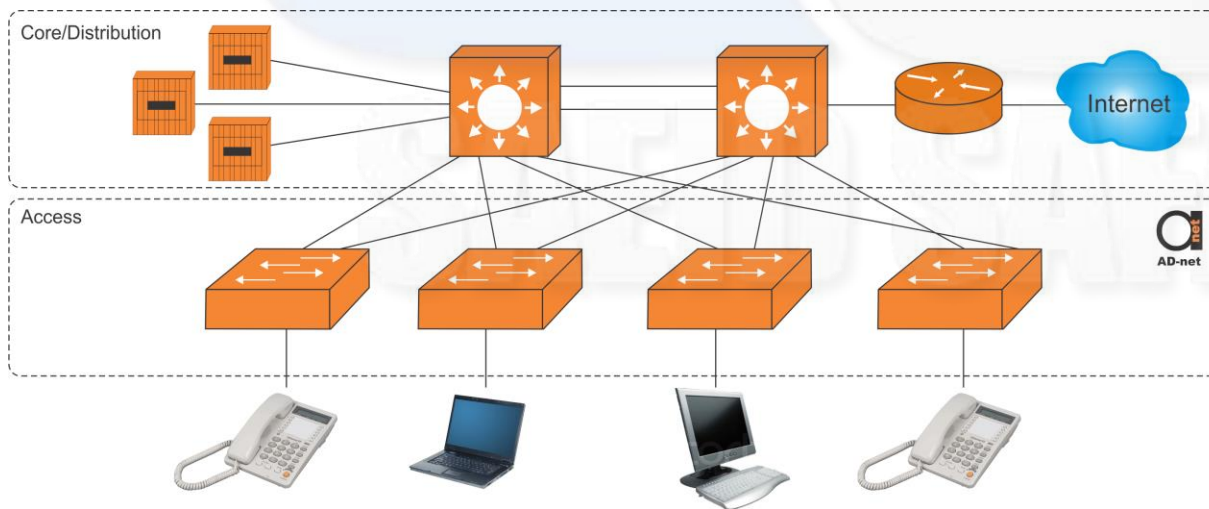


ویژگی‌های معماری کولپس کور:

ترکیب Core و Distribution:

در این معماری، لایه Distribution حذف شده و وظایف آن به لایه Core منتقل می‌شود.

در نتیجه تعداد تجهیزات شبکه و پیچیدگی طراحی کاهش می‌یابد و مناسب برای شبکه‌های کوچک یا متوسط که نیازی به جداسازی عملکرد لایه‌های Core و Distribution ندارند.



تعریف Leg در روتر:

معنی ساده: هر پورت یا رابطی که روتر برای اتصال به دستگاه‌های دیگر یا شبکه‌های دیگر از آن استفاده می‌کند، می‌تواند به عنوان یک Leg در نظر گرفته شود.

به عبارتی تمام اینترفیس‌های فعال در روتر را در هر سمت یک Leg روتر می‌گویند.

در برخی پیکربندی‌های خاص روتر، ممکن است از اصطلاح Leg برای اشاره به یک بخش مشخص از پیکربندی (یک دست روتر) استفاده شود.

در زمینه‌های تخصصی‌تر شبکه، از اصطلاحات دقیق‌تری مانند "رابط"، "مسیر"، "پورت" و ... استفاده می‌شود.

در سویچ دستگاه‌ها، به هم متصل می‌شوند اما در روتر شبکه‌ها با هم مرتبط می‌گردند. برای مثال، روتر می‌تواند شبکه محلی شما را به اینترنت متصل کند.

تعریف Hop در روتر:

در شبکه‌های کامپیوتری، هاپ Hop به هر جهش یا پرشی که یک بسته داده از یک دستگاه شبکه به دستگاه دیگری انجام می‌دهد، گفته می‌شود.

به عبارت ساده‌تر، هر بار که یک بسته داده از یک روتر به روتر دیگر یا از یک دستگاه به یک روتر حرکت می‌کند، یک هاپ اتفاق می‌افتد.

تصور کنید می‌خواهید از کامپیوتر خود به یک وب‌سایت دسترسی پیدا کنید. بسته داده‌ای که از کامپیوتر شما ارسال می‌شود، باید از چندین روتر عبور کند تا به سرور وب‌سایت برسد. هر بار که این بسته داده از یک روتر عبور می‌کند، یک هاپ اتفاق می‌افتد.

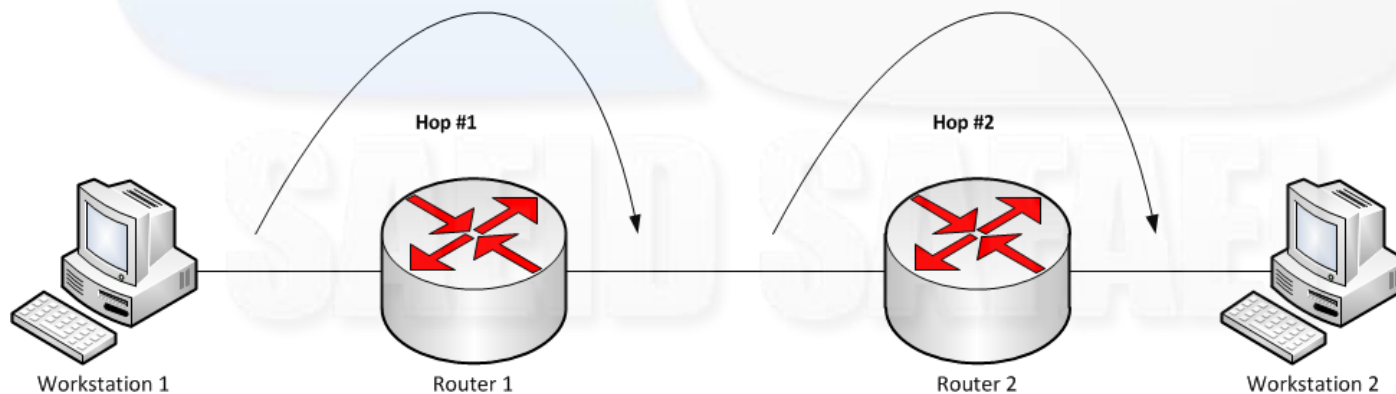
Hop Count : تعداد کل هاپ‌هایی که یک بسته داده برای رسیدن به مقصد طی می‌کند، Hop Count نامیده می‌شود.

تفاوت Hop و Leg در روتر:

Hop : به هر جهش یک بسته داده از یک دستگاه به دستگاه دیگر اشاره دارد.

Leg : به یک بخش مشخص از مسیر ارتباطی اشاره دارد و معمولاً در ارتباطات صوتی VoIP استفاده می‌شود.

یک Leg می‌تواند شامل چندین Hop باشد.



مسیریابی بر اساس آدرس IP در روترها

مسیریابی بر اساس آدرس IP یکی از اصول اساسی کار روترها است.

به زبان ساده، زمانی که یک بسته داده از یک دستگاه به دستگاه دیگری در شبکه ارسال می‌شود، روتر با بررسی آدرس IP مقصد این بسته، بهترین مسیر را برای رساندن آن به مقصد انتخاب می‌کند.

روترها به لطف کار در لایه ۳ می‌توانند شبکه‌های مختلف با آدرس‌های IP متفاوت را به هم متصل کنند.

روترها به عنوان دروازه بین شبکه‌ها عمل می‌کنند و با بررسی آدرس IP بسته‌های داده، بهترین مسیر را برای رسیدن به مقصد انتخاب می‌کنند.

به همین دلیل، روترها در لایه ۳ مدل OSI کار می‌کنند که به لایه شبکه معروف است. اما چگونه؟

روترها چگونه مسیریابی را انجام می‌دهند؟

- ۱- جدول مسیریابی: هر روتر دارای یک جدول مسیریابی است. این جدول حاوی اطلاعاتی درباره شبکه‌های مختلف، مسیرهای دسترسی به آن‌ها و بهترین مسیر برای رسیدن به هر شبکه است.
- ۲- بررسی آدرس IP: وقتی یک بسته داده به روتر می‌رسد، روتر ابتدا آدرس IP مقصد را بررسی می‌کند.
- ۳- مقایسه با جدول مسیریابی: سپس، روتر آدرس IP مقصد را با آدرس‌های IP موجود در جدول مسیریابی خود مقایسه می‌کند.
- ۴- انتخاب بهترین مسیر: روتر بر اساس اطلاعات موجود در جدول مسیریابی، بهترین مسیر را برای رساندن بسته داده به مقصد انتخاب می‌کند و بسته را به آن مسیر هدایت می‌کند.

جدول مسیریابی (Routing Table) :

تصور کنید اینترنت را به یک بزرگراه تشبیه کنیم. هر وبسایت یک ساختمان در این بزرگراه است و آدرس IP آن ساختمان مانند آدرس پستی است. وقتی شما می‌خواهید به یک وبسایت خاص دسترسی پیدا کنید، درخواست شما به صورت یک بسته داده از کامپیوتر شما ارسال می‌شود.

این بسته داده باید از طریق بزرگراه اینترنت به ساختمان مورد نظر برسد. روترها مانند چراغ‌های راهنمایی و تابلوهای راهنمایی و رانندگی عمل می‌کنند و بسته‌های داده را به سمت مقصد مورد نظر هدایت می‌کنند.

جدول مسیریابی در واقع یک نقشه راه برای روترها است تا بدانند بسته‌های داده را به کدام مسیر ارسال کنند.

این جدول حاوی اطلاعاتی درباره شبکه‌های مختلف، بهترین مسیر برای رسیدن به آنها و گیت‌وی‌های پیش‌فرض است.

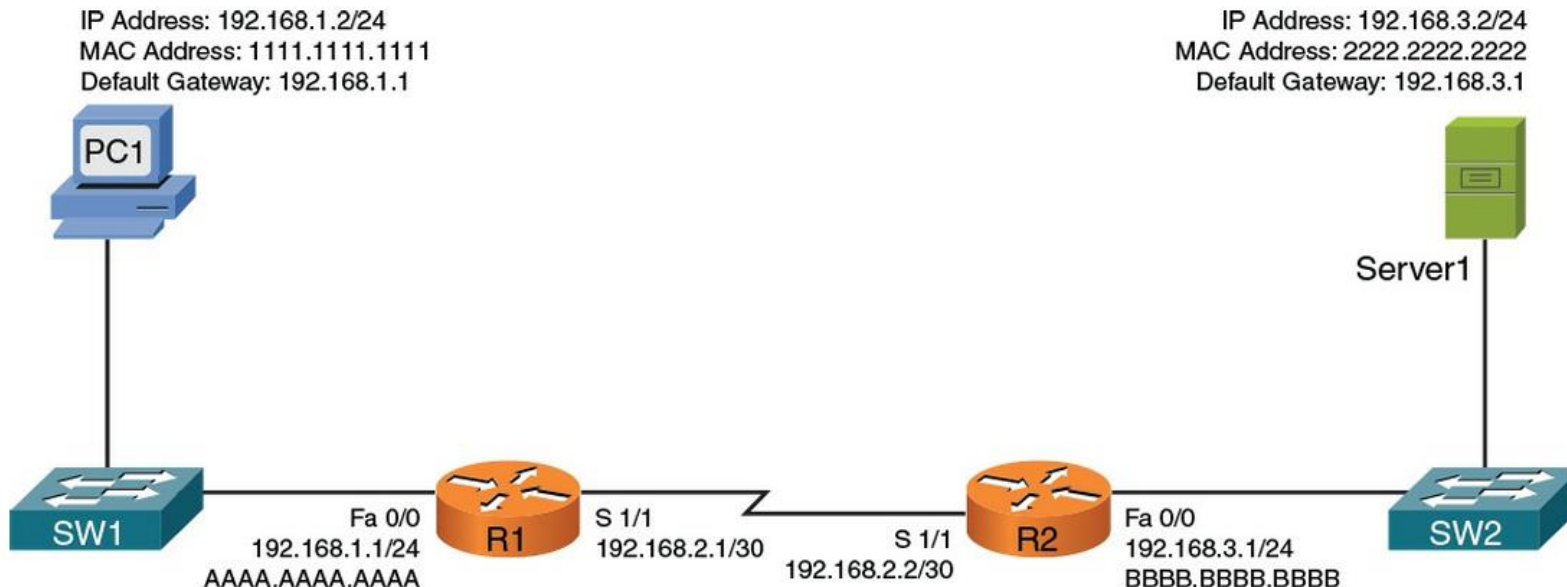
اطلاعات موجود در جدول مسیریابی

- ۱- شبکه مقصد: آدرس شبکه‌ای که بسته داده باید به آن ارسال شود.
 - ۲- ماسک زیرشبکه **Subnet Mask**: مشخص می‌کند که کدام قسمت از آدرس IP برای شناسایی شبکه استفاده می‌شود.
 - ۳- گیت‌وی پیش‌فرض **Default Gateway**: روتری که بسته داده باید برای رسیدن به شبکه مقصد به آن ارسال شود.
 - ۴- هزینه مسیر **Cost**: یک مقدار عددی که برای مقایسه مسیرهای مختلف استفاده می‌شود. (مانند پهنای باند، نرخ انتقال، MTU و ...)
- مسیر با بهترین هزینه معمولاً بهترین مسیر انتخاب می‌شود.

مراحل اولیه پردازش در Router:

برای درک فرآیندهای مسیریابی پایه، به شکل توجه کنید.
در این توپولوژی، PC1 نیاز دارد ترافیک را به Server1 ارسال کند.
دقت کنید که این دستگاه‌ها در شبکه‌های مختلف قرار دارند.
بنابراین، سؤال این است که:

چگونه یک بسته با آدرس IP مبدا ۱۹۲.۱۶۸.۱.۲ به آدرس IP مقصد ۱۹۲.۱۶۸.۳.۲ مسیریابی می‌شود؟



مراحل اولیه پردازش در Router:

مرحله ۱:

PC1 آدرس IP و Subnet Mask خود (۱۹۲.۱۶۸.۱.۲/۲۴) را با آدرس IP مقصد (۱۹۲.۱۶۸.۳.۲/۲۴) مقایسه می کند.

PC1 به این نتیجه می رسد که آدرس مقصد در یک زیرشبکه دوردست Remote Subnet قرار دارد.

بنابراین، PC1 باید بسته را به دروازه پیش فرض Default Gateway خود ارسال کند. این دروازه ممکن است به صورت دستی روی PC1 تنظیم شده باشد یا به صورت پویا از طریق پروتکل DHCP (Dynamic Host Configuration Protocol) دریافت شده باشد.

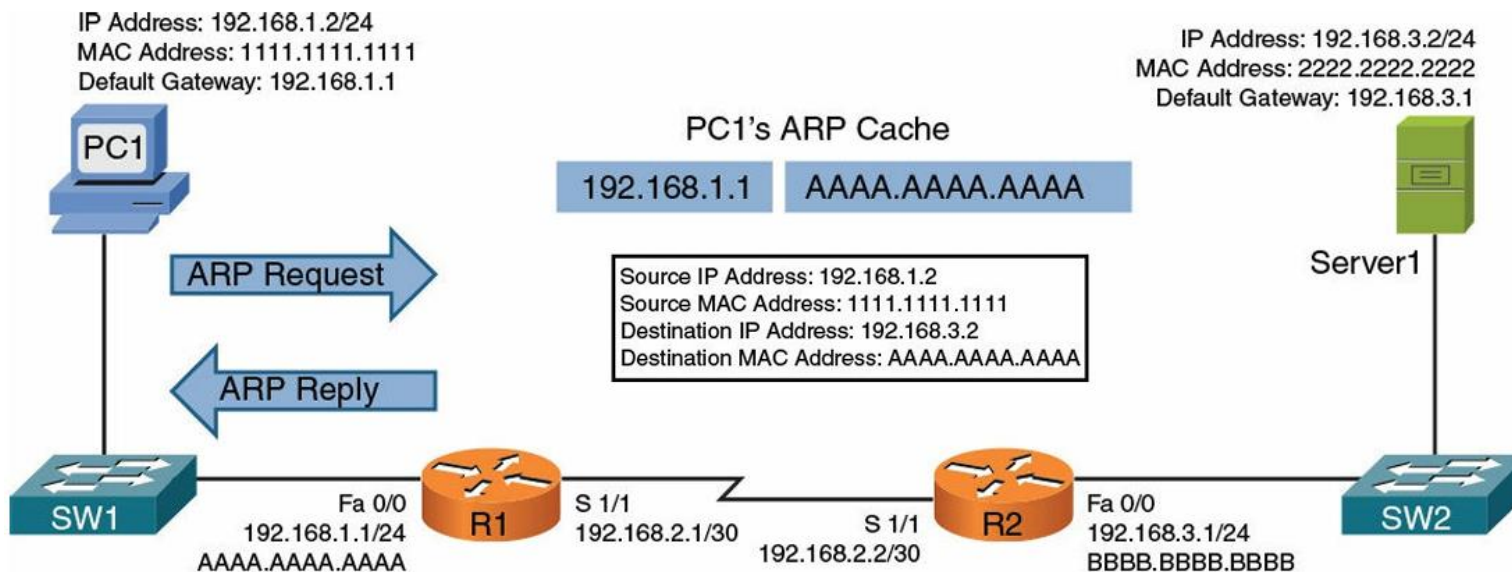
در این مثال، دروازه پیش فرض PC1 آدرس ۱۹۲.۱۶۸.۱.۱ روتر R1 است.

مراحل اولیه پردازش در Router:

برای ساخت یک فریم لایه ۲ Layer 2 Frame، PC1 نیاز به آدرس MAC دروازه پیش فرض خود نیز دارد.

بنابراین، PC1 یک درخواست ARP برای آدرس MAC روتر R1 ارسال می کند. پس از دریافت پاسخ ARP از روتر R1، PC1 آدرس MAC روتر R1 را به کش ARP خود اضافه می کند.

اکنون PC1 داده های خود را در قالب یک فریم لایه ۲ ارسال می کند که مقصد آن Server1 است.



مراحل اولیه پردازش در Router:

نکته: ARP یک پروتکل مبتنی بر پخش Broadcast است و به همین دلیل، بسته های آن از زیر شبکه محلی Local Subnet فرستنده فراتر نمی روند.

چون برادکست وقتی به روتر میرسد دراپ می شود.

مرحله ۲:

روتر R1 فریمی که از PC1 دریافت کرده را پردازش می کند و به سربرگ IP آن نگاهی می اندازد. سربرگ IP شامل یک فیلد به نام **Time To Live (TTL)** است که با هر عبور بسته از یک روتر، یک واحد کاهش می یابد.

بنابراین، روتر R1 مقدار فیلد TTL بسته را کاهش می دهد.

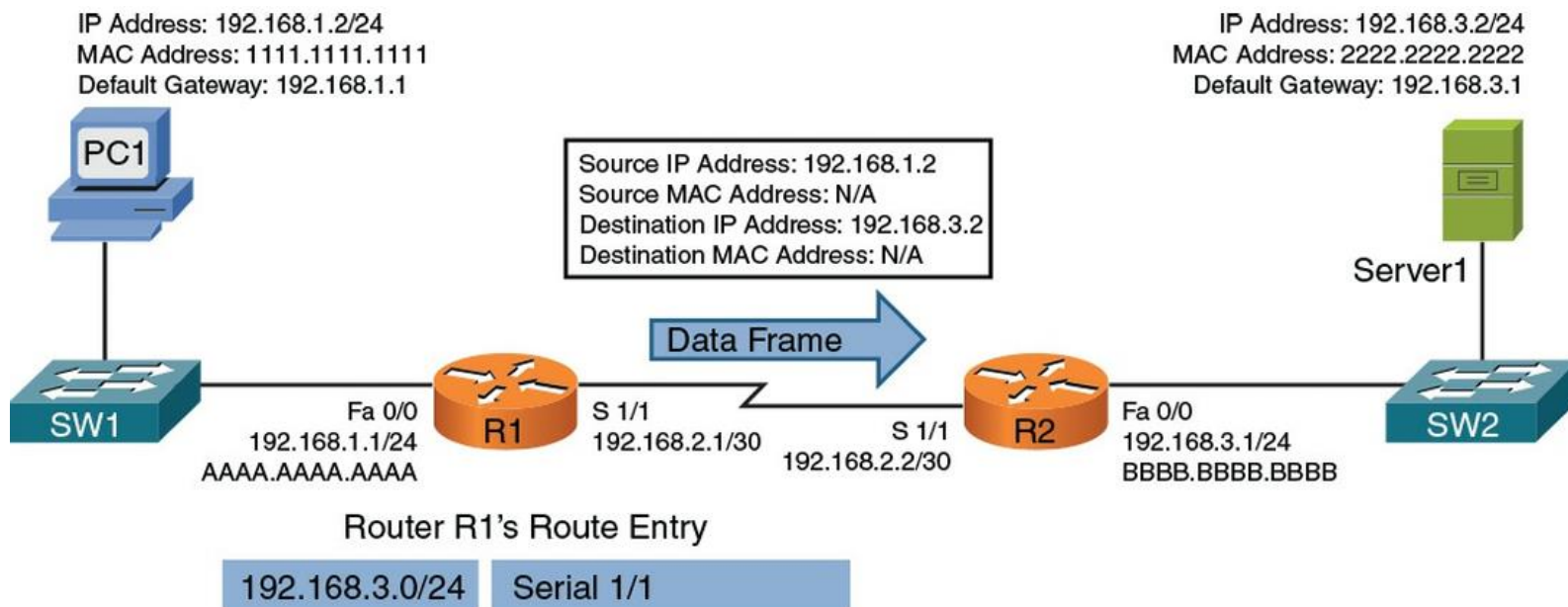
اگر مقدار TTL به صفر برسد، روتر فریم را دور انداخته و یک پیام "Time Exceeded" از طریق پروتکل ICMP (Internet Control Message Protocol) به فرستنده بسته ارسال می کند.

در صورتی که مقدار TTL به صفر نرسد، روتر R1 جدول مسیریابی خود را بررسی می کند تا بهترین مسیر برای رسیدن به شبکه ۱۹۲.۱۶۸.۳۰/۲۴ را مشخص کند.

مراحل اولیه پردازش در Router:

در این مثال، جدول مسیریابی روتر R1 دارای یک ورودی است که نشان می‌دهد شبکه ۱۹۲.۱۶۸.۳.۰/۲۴ از طریق رابط Serial 1/1 قابل دسترسی است. توجه داشته باشید که پروتکل ARP برای رابط‌های سریال مورد نیاز نیست، زیرا این نوع رابط‌ها آدرس MAC ندارند.

در نتیجه، روتر R1 فریم را از طریق رابط Serial 1/1 خود ارسال می‌کند.



مراحل اولیه پردازش در Router:

مرحله ۳:

هنگامی که روتر R2 فریم را دریافت می کند، مانند روتر R1، مقدار TTL در سربرگ IP را یک واحد کاهش می دهد.

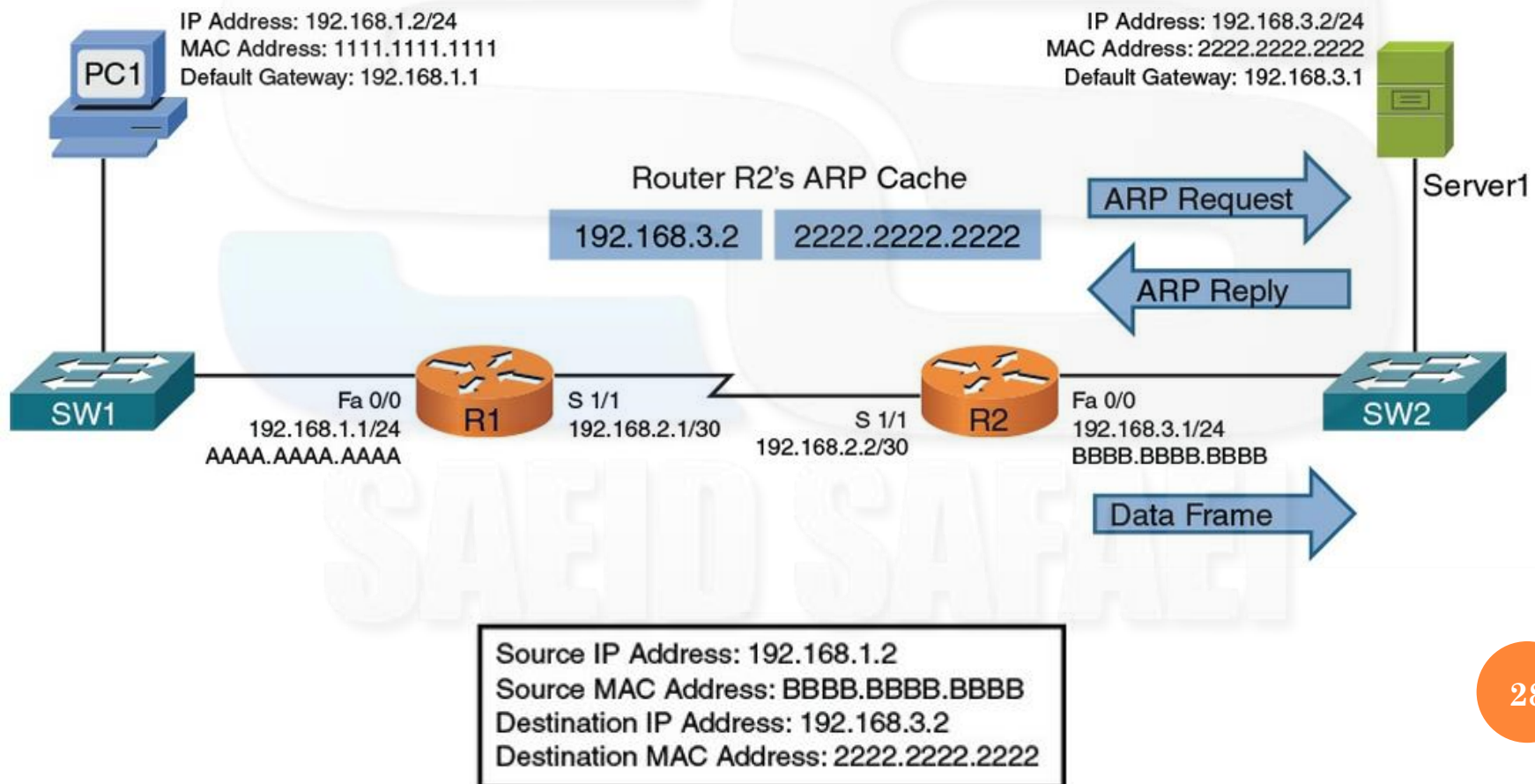
باز هم، در صورتی که مقدار TTL به صفر نرسیده باشد، روتر R2 سربرگ IP را بررسی می کند تا شبکه مقصد را شناسایی کند.

در این مورد، شبکه مقصد ۱۹۲.۱۶۸.۳.۰/۲۴ مستقیماً به رابط Fast Ethernet 0/0 روتر R2 متصل است.

مشابه روشی که PC1 برای تعیین آدرس MAC دروازه پیش فرض خود از ARP استفاده کرد، روتر R2 نیز یک درخواست ARP ارسال می کند تا آدرس MAC Server1 را به دست آورد.

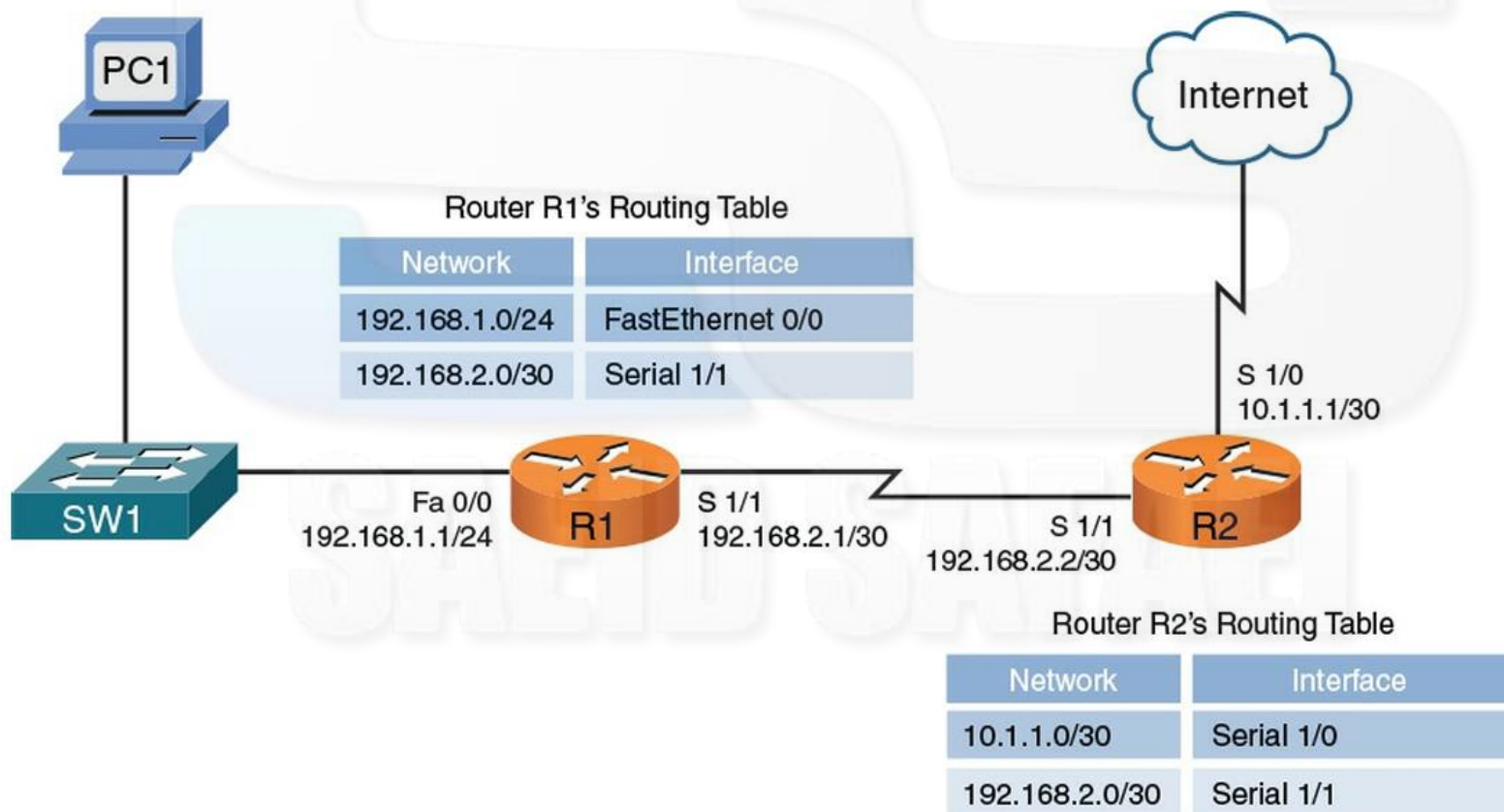
مراحل اولیه پردازش در Router:

پس از دریافت پاسخ ARP از Server1، روتر R2 فریم را از طریق رابط Fast Ethernet 0/0 خود به Server1 ارسال می کند.



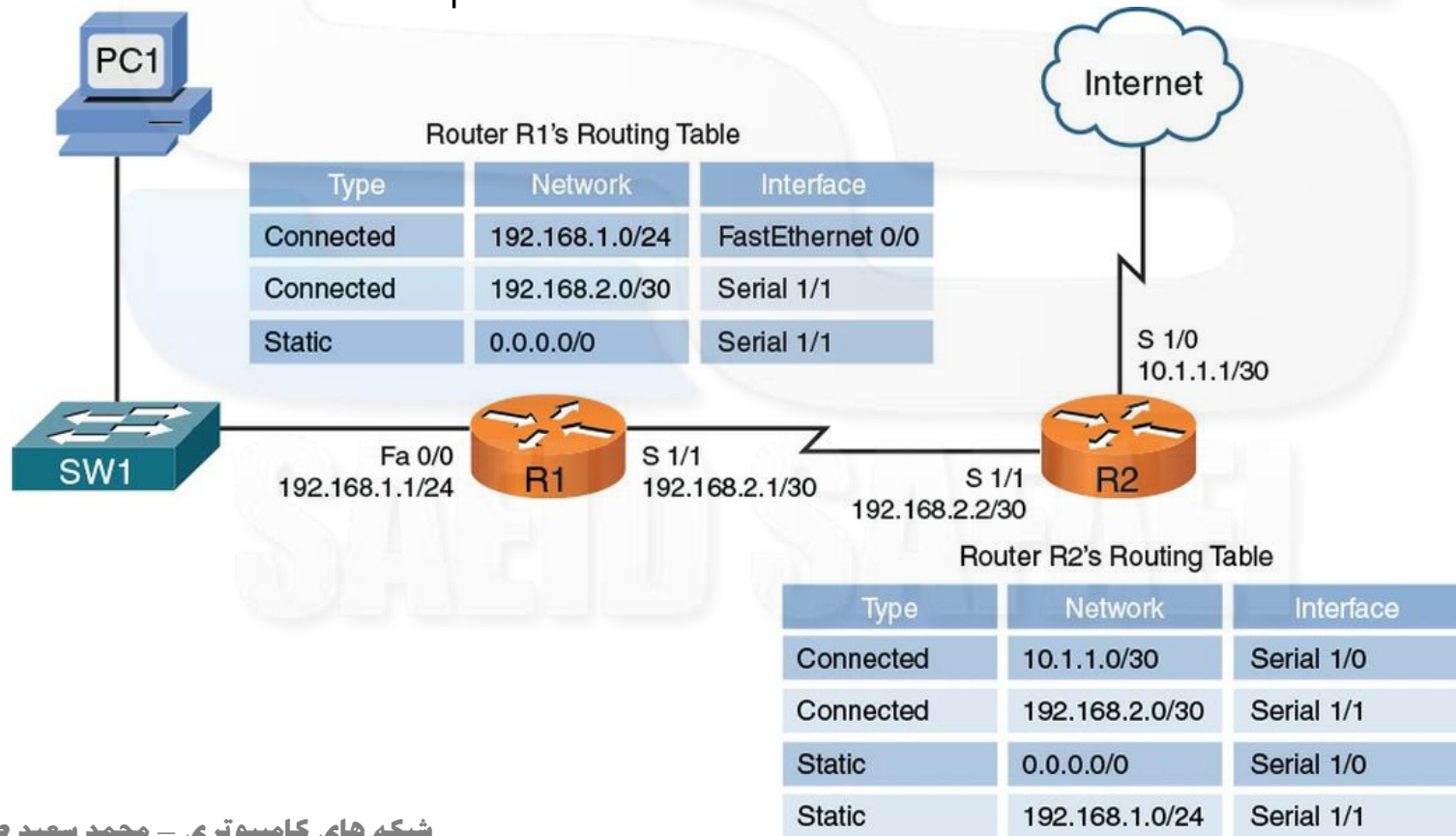
مفهوم مسیرهای مستقیماً متصل Directly Connected Routes

یکی از روش‌هایی که یک روتر می‌تواند مسیر دسترسی به یک شبکه مقصد خاص را بداند، این است که روتر یک رابط Interface داشته باشد که مستقیماً در آن شبکه شرکت می‌کند.



چگونه جدول مسیریابی به روز می شود؟ (انواع کلی پروتکل های مسیریابی)

- ۱- پیکربندی دستی: مدیر شبکه می تواند به صورت دستی اطلاعات مورد نظر را به جدول مسیریابی اضافه کند. (مانند Inter-VLAN)
- مناسب برای شبکه های کوچک و ساده با تغییرات کم.



چگونه جدول مسیریابی به روز می شود؟ (انواع کلی پروتکل های مسیریابی)

۱- پیکربندی دستی:

نکته:

یک مسیر استاتیک Static Route همیشه به یک رابط محلی Local Interface اشاره نمی کند.

بلکه ممکن است یک مسیر استاتیک به آدرس IP گام بعدی اشاره داشته باشد، که همان آدرس IP یکی از رابط های روتر بعدی است که ترافیک باید به آن ارسال شود.

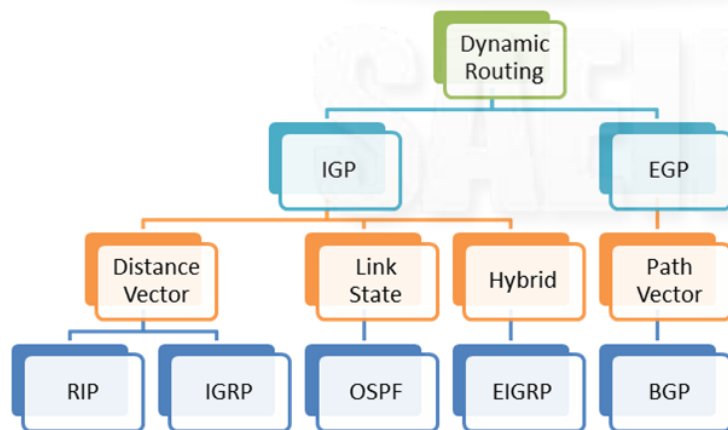
آدرس شبکه ای که برای مسیر پیش فرض Default Route استفاده می شود، ۰/۰/۰/۰ است.

چگونه جدول مسیریابی به روز می شود؟ (انواع کلی پروتکل های مسیریابی)

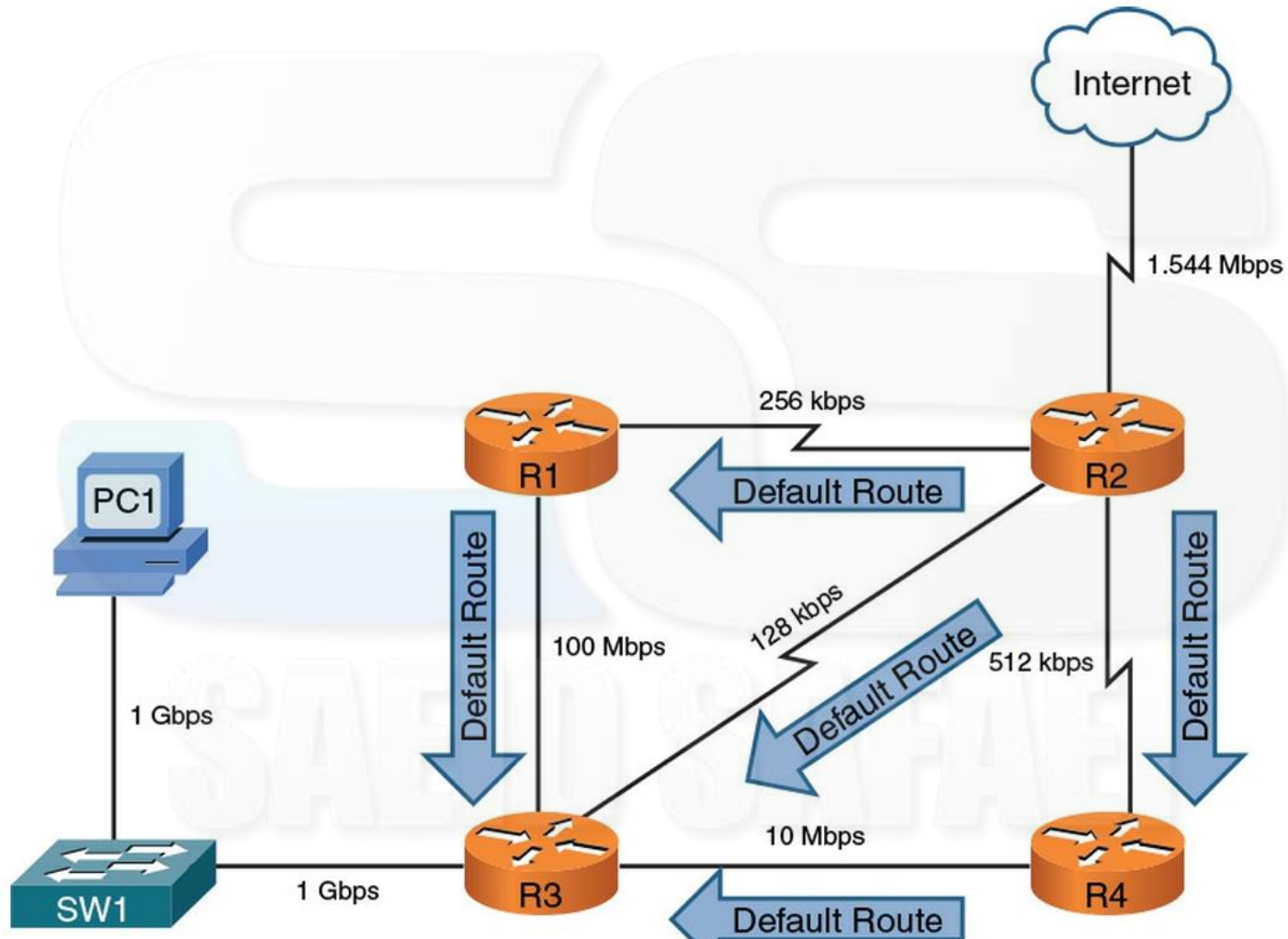
۲- پروتکل های مسیریابی دینامیک: پروتکل هایی مانند RIP, OSPF و BGP به روترها اجازه می دهند تا به صورت خودکار اطلاعات مسیریابی را با هم تبادل کنند و جدول مسیریابی خود را به روز کنند.

اگر بخواهید اطلاعات مسیریابی را به روترها در شبکه های پیچیده تر اضافه کنید، مسیریابی استاتیک به خوبی مقیاس پذیر نیست.

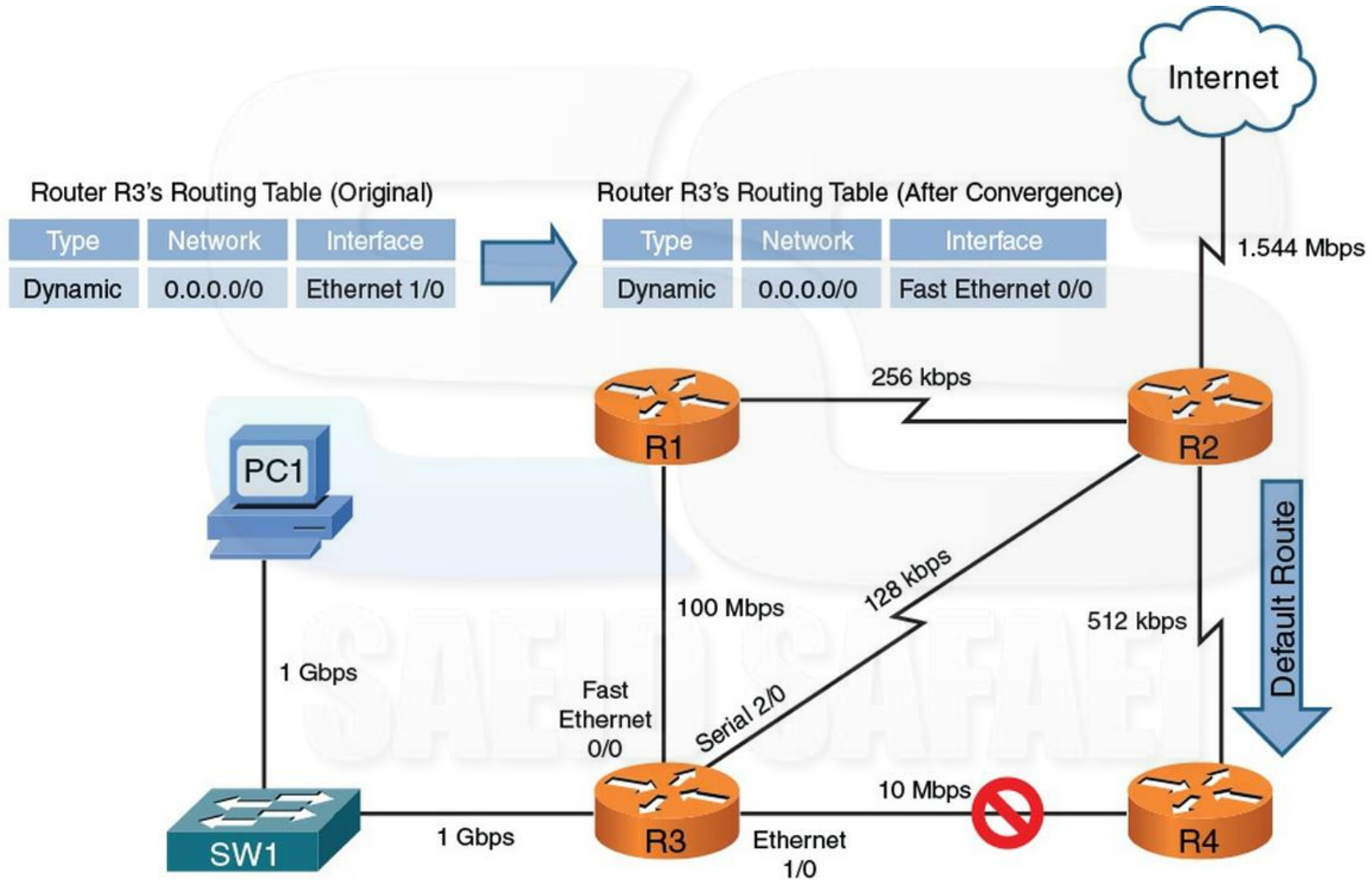
پروتکل های مسیریابی پویا به روتر این امکان را می دهند تا جدول مسیریابی خود را با توجه به تغییرات شرایط شبکه به روزرسانی کند.



۲- مسیریابی دینامیک:



۲- مسیریابی دینامیک:



Inter-VLAN Routing (مسیریابی بین VLAN ها)

به فرآیند مسیریابی ترافیک بین VLAN های مختلف در یک شبکه گفته می‌شود. (VLAN (Virtual Local Area Network یک تکنولوژی است که برای تقسیم شبکه‌های محلی به بخش‌های مجزا به کار می‌رود.

هر VLAN به صورت یک شبکه مستقل عمل می‌کند، و برای ارتباط بین VLAN ها نیاز به مسیریابی است.

هر VLAN به عنوان یک Broadcast Domain جدا عمل می‌کند. برای اینکه دستگاه‌های موجود در یک VLAN بتوانند با دستگاه‌های دیگر VLAN ها ارتباط برقرار کنند، باید از مسیریاب **Router** یا سوئیچ لایه ۳ استفاده کرد.

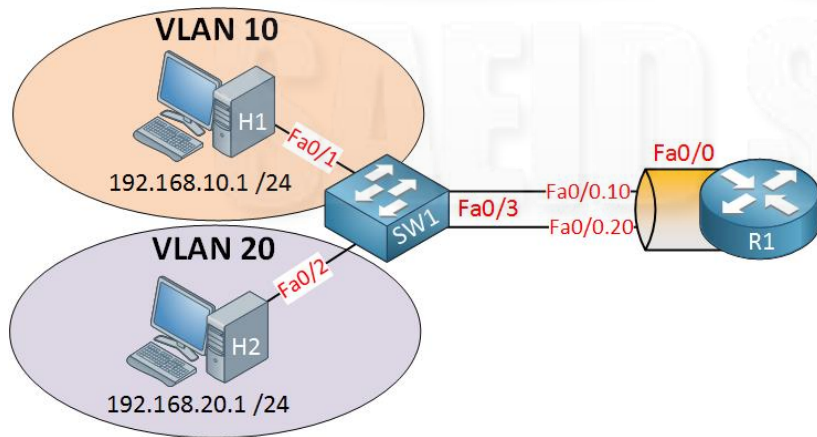
روش‌های پیاده‌سازی Inter-VLAN Routing

۱- Router-on-a-Stick روتر بر روی یک لینک :

در این روش، یک روتر با یک پورت فیزیکی برای ارتباط با سوئیچ استفاده می‌شود.

پورت فیزیکی روتر در حالت Trunk تنظیم می‌شود و ترافیک از تمام VLAN ها را مدیریت می‌کند.

برای هر VLAN یک Subinterface روی پورت روتر تعریف می‌شود و آدرس‌های IP مربوط به هر VLAN به این Subinterface اختصاص می‌یابد.



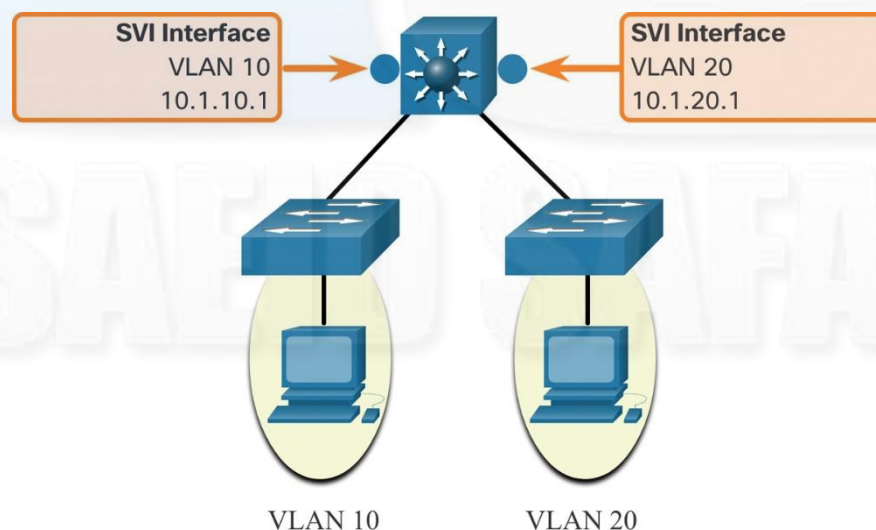
روش‌های پیاده‌سازی Inter-VLAN Routing

۲- استفاده از سوئیچ لایه ۳ :

در این روش، از سوئیچ لایه ۳ که قابلیت مسیریابی دارد استفاده می‌شود.

هر VLAN به یک SVI (Switched Virtual Interface) در سوئیچ لایه ۳ متصل می‌شود.

ترافیک بین VLAN ها مستقیماً توسط سوئیچ لایه ۳ مسیریابی می‌شود.



روش پیکربندی Inter-VLAN Routing در سویچ L3

فرض کنید دو VLAN ۱۰ و ۲۰ داریم؛ (برای هر VLAN یک SVI تنظیم کنید. SVI نوعی اینترفیس مجازی است که به VLAN اجازه مسیریابی می‌دهد.)

```
vlan 10
name Sales

vlan 20
name IT

interface vlan 10 //Switch Virtual Interface VLAN 10
ip address 192.168.10.1 255.255.255.0
no shutdown

interface vlan 20 //Switch Virtual Interface VLAN 20
ip address 192.168.20.1 255.255.255.0
no shutdown
ip routing
```

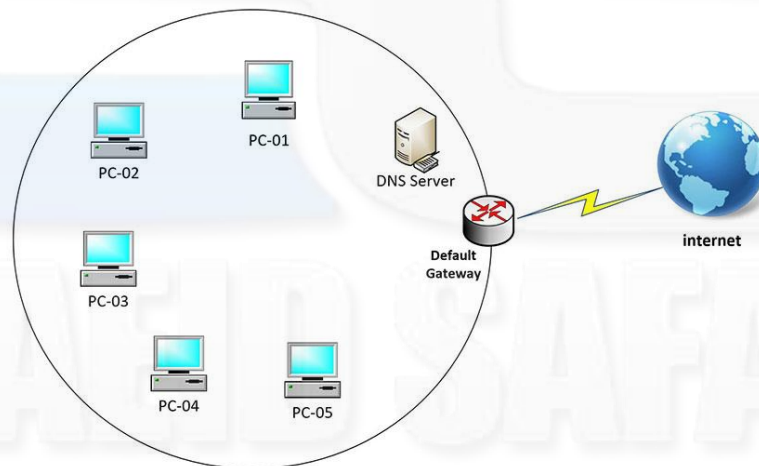
روش‌های پیاده‌سازی Inter-VLAN Routing

- برای استفاده از Inter-VLAN Routing، باید ترافیک VLAN ها از طریق پورت Trunk منتقل شود.
 - در شبکه‌های بزرگ معمولاً از سوئیچ‌های لایه ۳ برای بهینه‌سازی مسیریابی استفاده می‌شود.
 - اطمینان از اختصاص صحیح آدرس IP به هر VLAN ضروری است.
- این نوع مسیریابی معمولاً از نوع Static Routing می باشد.

Default Gateway یا دروازه پیش فرض چیست؟

دروازه پیش فرض Default Gateway در یک شبکه، آدرس IP روتری است که دستگاه‌های شما برای ارتباط با شبکه‌های دیگر (مانند اینترنت) از آن استفاده می‌کنند.

به عبارت ساده‌تر، دروازه پیش فرض مانند یک درب خروجی است که دستگاه‌های شما را از شبکه محلی به دنیای بزرگ‌تر متصل می‌کند.



پس می‌توان گفت مرز بین شبکه LAN و شبکه WAN را می‌گویند.

Default Gateway چگونه کار می کند؟

۱- ارسال درخواست: زمانی که شما درخواستی برای دسترسی به یک منبع خارجی ارسال می کنید (مثلاً باز کردن یک وبسایت)، این درخواست به سمت دروازه پیش فرض روانه می شود.

۲- انتقال درخواست: دروازه پیش فرض درخواست شما را دریافت کرده و با استفاده از جداول مسیریابی خود، بهترین مسیر برای رسیدن به مقصد را پیدا می کند.

۳- ارسال به مقصد: دروازه پیش فرض درخواست شما را به سمت مقصد نهایی هدایت می کند.

۴- دریافت پاسخ: پس از دریافت پاسخ از مقصد، دروازه پیش فرض پاسخ را به دستگاه شما باز می گرداند.

آدرس IP دروازه پیش فرض معمولاً آدرس IP روتر شما است.

آیا میتوان تمام جهان را با سویچ به هم متصل کرد؟

در تئوری، می توان تمام دستگاه های شبکه در جهان را با استفاده از سوئیچ ها به هم متصل کرد، اما در عمل چنین چیزی امکان پذیر نیست و مشکلات زیادی به وجود می آید.

سوئیچ ها در لایه ۲ مدل OSI کار می کنند و تمامی دستگاه های متصل به آنها در یک Broadcast Domain قرار می گیرند.

اگر تمام دستگاه های جهان به یک Broadcast Domain متصل باشند: هر پیام Broadcast مثل ARP یا DHCP به تمام دستگاه ها در جهان ارسال می شود.

این مسئله باعث ازدحام شدید شبکه Broadcast Storm و کاهش کارایی یا حتی از کار افتادن شبکه می شود.

آیا میتوان تمام جهان را با سویچ به هم متصل کرد؟

Default Gateway نقطه مرزی برای Broadcast Domain محسوب می شود.

دستگاه ها در یک Broadcast Domain از یک زیر شبکه Subnet استفاده می کنند.

وقتی یک دستگاه در شبکه بخواهد با دستگاهی خارج از Subnet خود ارتباط برقرار کند، بسته ها را به Default Gateway ارسال می کند.

Broadcast Traffic مثلاً پیام های ARP یا DHCP فقط در داخل Broadcast Domain فعلی ارسال می شود.

Default Gateway این Broadcast را به دیگر شبکه ها منتقل نمی کند، زیرا Broadcast Traffic به صورت پیش فرض توسط روتر مسدود می شود.

آیا میتوان تمام جهان را با سوئیچ به هم متصل کرد؟

پس: برای اتصال جهان به هم، از ساختار چندلایه‌ای شبکه استفاده می‌شود:

۱- لایه ۲: سوئیچ‌ها برای ایجاد شبکه‌های محلی LAN

۲- لایه ۳: روترها برای اتصال شبکه‌های مختلف WAN

۳- پروتکل‌هایی مانند BGP و IP برای ارتباط بین شبکه‌های جهانی (مانند اینترنت).

در نتیجه :

اتصال تمامی جهان فقط با سوئیچ‌ها ممکن نیست و به فناوری‌های پیشرفته‌تر مانند روترها و مسیریابی نیاز است.

طراحی اینترنت به همین دلیل به صورت لایه‌بندی شده و توزیع شده انجام شده تا مشکلات فوق را برطرف کند.

آیا میتوان تمام جهان را با سویچ به هم متصل کرد؟



در تصویر، مفهوم اتصال کل جهان فقط با استفاده از سوئیچها نشان داده شده است. این تصویر به شکلی نمادین نشان می‌دهد که چگونه این ایده منجر به یک شبکه پیچیده و بیش از حد شلوغ می‌شود، با سوئیچها و کابل‌هایی که به تمام نقاط زمین متصل شده‌اند و یک Broadcast Domain بزرگ ایجاد کرده‌اند.

تعریف سیستم مستقل یا Autonomous System (AS) :

Autonomous System (AS) یا سیستم مستقل به یک گروه از شبکه‌های متصل به هم گفته می‌شود که تحت کنترل یک یا چند مدیر شبکه قرار دارند و از یک سیاست مسیریابی یکسان برای مدیریت داده‌ها استفاده می‌کنند.

این دامنه مدیریتی (Administrative Domain) شامل شبکه‌هایی است که در یک سازمان (مثل یک شرکت یا ISP) کنترل می‌شوند و سیاست‌های مسیریابی آنها توسط همان سازمان تعیین می‌شود.

به کلام ساده به مجموعه روترهایی که درون یک شرکت (IGP) کانفیگ می‌شود و جداول مسیریابی خود را با یکدیگر به اشتراک می‌گذارند.

ویژگی‌های اصلی یک Autonomous System :

۱- یکپارچگی مدیریتی: یک AS توسط یک سازمان یا شرکت مدیریت می‌شود (مانند یک ارائه‌دهنده خدمات اینترنتی (ISP)، شرکت بزرگ یا دانشگاه).

۲- سیاست مسیریابی یکسان: تمام روترهای داخل AS از یک سیاست واحد برای مسیریابی داده‌ها پیروی می‌کنند.

۳- شماره منحصر به فرد: هر AS در اینترنت یک شماره شناسایی یکتا به نام ASN (Autonomous System Number) دارد که توسط سازمان‌های مربوطه (مثل IANA یا RIR ها) اختصاص داده می‌شود.

مثال:

فرض کنید یک شرکت ارائه‌دهنده خدمات اینترنتی ISP دارای یک AS است.

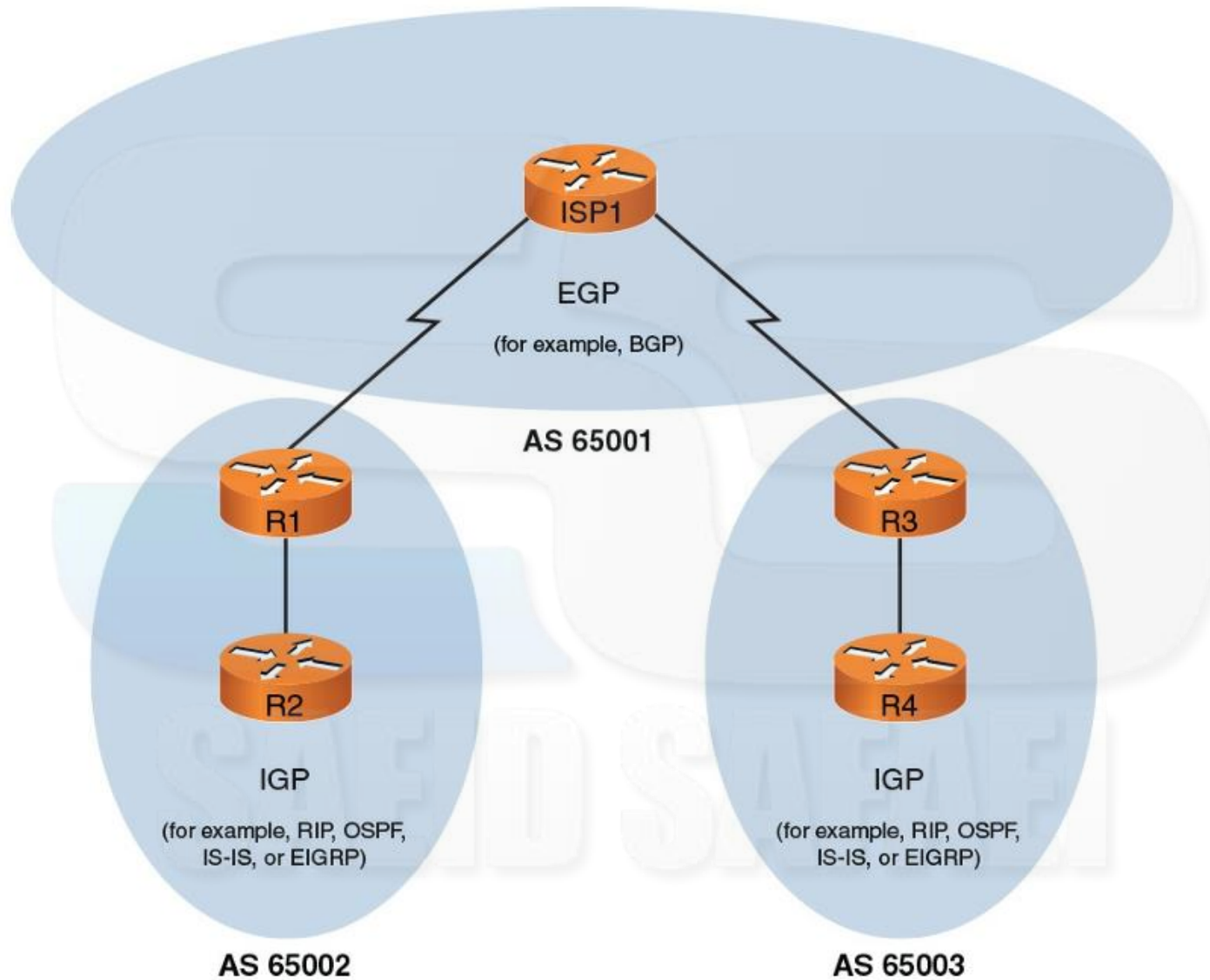
تمام شبکه‌های داخلی این ISP تحت یک شماره AS فعالیت می‌کنند و از سیاست‌های مسیریابی مشخصی استفاده می‌کنند.

این ISP برای ارتباط با سایر ISP ها و عبور داده‌ها از پروتکل BGP استفاده می‌کند.

شماره AS در عمل:

ASN ها معمولاً یک عدد ۳۲ بیتی (مثلاً ۶۴۵۱۲) هستند.

برخی ASN ها برای استفاده خصوصی رزرو شده‌اند، مشابه آدرس‌های IP خصوصی.



انواع ASN

۱- شماره AS عمومی Public ASN :

برای مسیریابی خارجی و اتصال به اینترنت عمومی استفاده می‌شود. این شماره‌ها باید از سازمان‌های اختصاص‌دهنده شماره‌های اینترنتی (مثل APNIC, ARIN, RIPE) درخواست شوند. مثال: یک ISP که با سایر ارائه‌دهندگان یا مراکز داده ارتباط دارد، از یک ASN عمومی برای مدیریت مسیریابی خود استفاده می‌کند. این شماره از ۱ تا ۶۴۵۱۱ می‌باشد.

انواع ASN

۲- شماره AS خصوصی Private ASN :

برای مسیریابی داخلی یا ارتباطات خصوصی که به اینترنت عمومی متصل نمی‌شوند استفاده می‌شود.

شماره‌های خصوصی نیازی به ثبت ندارند.

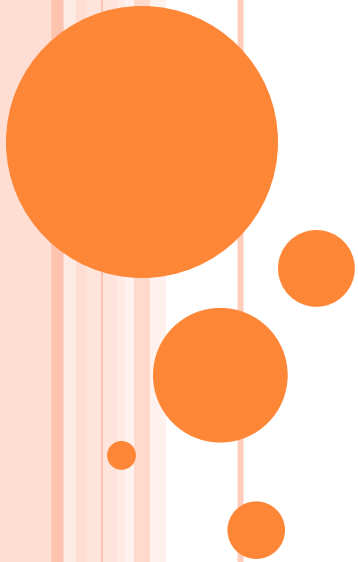
محدوده شماره‌های AS خصوصی طبق استاندارد IANA :

۶۴۵۱۲ تا ۶۵۵۳۴ (برای ۱۶ بیتی)

۴۲۰۰۰۰۰۰۰ تا ۴۲۹۴۹۶۷۲۹۴ (برای ۳۲ بیتی)

VLSM

Variable Length Subnet Masking



تعریف VLSM:

VLSM مخفف (Variable Length Subnet Mask) به معنای استفاده از ماسک زیر شبکه با طول متغیر است.

این تکنیک به مدیران شبکه اجازه می‌دهد تا شبکه را به زیربخش‌هایی با اندازه‌های مختلف تقسیم کنند، که بهینه‌تر از روش‌های سنتی ثابت یا Fixed-Length Subnet Mask است.

در روش معمول Subnetting، تمام زیربخش‌ها از یک اندازه (یا تعداد آدرس‌های IP یکسان برخوردارند).

این می‌تواند باعث اتلاف آدرس‌ها در شبکه‌هایی با اندازه‌های مختلف شود.

چگونه VLSM کار می کند؟

VLSM از ماسک های مختلف (مانند ۲۴، ۲۵، ۲۶) در یک بلوک آدرس شبکه استفاده می کند. با این روش، می توان یک بلوک آدرس IP را به بخش های کوچک تر با اندازه های مختلف تقسیم کرد.

مثال:

فرض کنید بلوک آدرس شما ۱۹۲.۱۶۸.۱۰۰/۲۴ است.

می خواهید این بلوک را برای سه شبکه با نیازهای زیر تقسیم کنید:
شبکه ای با ۵۰ دستگاه.

شبکه ای با ۲۵ دستگاه.

شبکه ای با ۱۰ دستگاه.

مرحله ۱: تخصیص اولین زیر شبکه

برای ۵۰ دستگاه به حداقل 2^6 (۶۴ آدرس) نیاز داریم. پس از ماسک ۲۶/ استفاده می‌کنیم: زیر شبکه ۱: ۱۹۲.۱۶۸.۱.۰/۲۶ (۶۴ آدرس، از ۱۹۲.۱۶۸.۱.۰ تا ۱۹۲.۱۶۸.۱.۶۳)

مرحله ۲: تخصیص دومین زیر شبکه

برای ۲۵ دستگاه به حداقل 2^5 (۳۲ آدرس) نیاز داریم. پس از ماسک ۲۷/ استفاده می‌کنیم: زیر شبکه ۲: ۱۹۲.۱۶۸.۱.۶۴/۲۷ (۳۲ آدرس، از ۱۹۲.۱۶۸.۱.۶۴ تا ۱۹۲.۱۶۸.۱.۹۵)

مرحله ۳: تخصیص سومین زیر شبکه

برای ۱۰ دستگاه به حداقل 2^4 (۱۶ آدرس) نیاز داریم. پس از ماسک ۲۸/ استفاده می‌کنیم: زیر شبکه ۳: ۱۹۲.۱۶۸.۱.۹۶/۲۸ (۱۶ آدرس، از ۱۹۲.۱۶۸.۱.۹۶ تا ۱۹۲.۱۶۸.۱.۱۱۱)

مزایای VLSM در روتینگ:

- ۱- کاهش بار روی شبکه: از طریق خلاصه‌سازی مسیرها و کاهش تعداد ورودی‌های جدول مسیریابی.
- ۲- استفاده بهینه از آدرس‌ها: جلوگیری از هدررفت آدرس‌های IP.
- ۳- سازگاری با پروتکل‌های پیشرفته: امکان استفاده در طراحی شبکه‌های مدرن.

Router A

```
| -- 192.168.1.0/26 --> Router B (شبکه بزرگتر)
| -- 192.168.1.64/27 --> Router C (شبکه متوسط)
| -- 192.168.1.96/28 --> Router D (شبکه کوچکتر)
```

مثال در مورد FLSM :

در رنج ۱۹۲.۱۶۸.۱۰۰.۰/۲۴ چهار رنج یکسان IP بساز؟

192.168.10.0/24 256

$24+1=25$ 128

192.168.10.0/25

192.168.10.128/25

$25+1=26$ 64

192.168.10.0/26 1-62 BCIP:63

192.168.10.64/26 64-126 BCIP:127

192.168.10.128/26 128-190 BCIP:191

192.168.10.192/26 192-254 BCIP:255

مثال در مورد VLSM :

در رنج ۱۹۲.۱۶۸.۱۰۰.۰/۲۴ چهار رنج متفاوت IP با ۱۲۶ و ۶۲ و ۳۰ و ۱۴ کاربر بساز؟

192.168.10.0/24

$24+1=25$

192.168.10.0/25 1-126 BCIP:127

192.168.10.128/25

$25+1=26$

192.168.10.128/26 129-190 BCIP:191

192.168.10.192/26

$26+1=27$

192.168.10.192/27 193-222 BCIP:223

192.168.10.224/27

$27+1=28$

192.168.10.224/28 225-238 BCIP=239

192.168.10.240/28

پروتکل های مسیریابی چیست؟

پروتکل های مسیریابی Routing Protocols مجموعه ای از قوانین و الگوریتم ها هستند که برای تبادل اطلاعات مسیریابی بین روترها استفاده می شوند.

این پروتکل ها کمک می کنند روترها بهترین مسیر را برای انتقال بسته های داده در شبکه پیدا کنند.

پروتکل های مسیریابی داینامیک به دو دسته اصلی تقسیم می شوند:

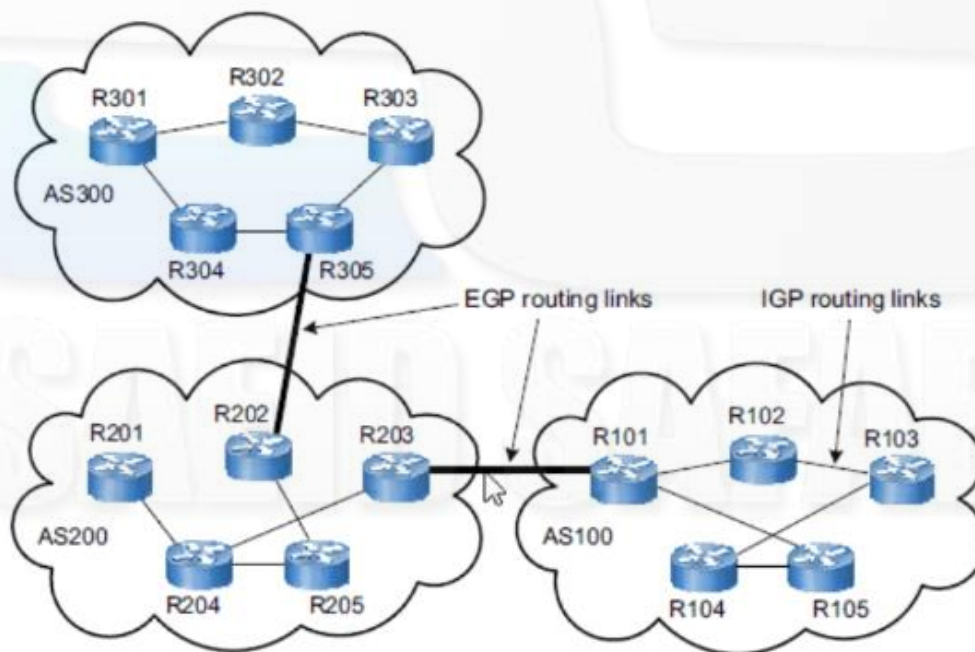
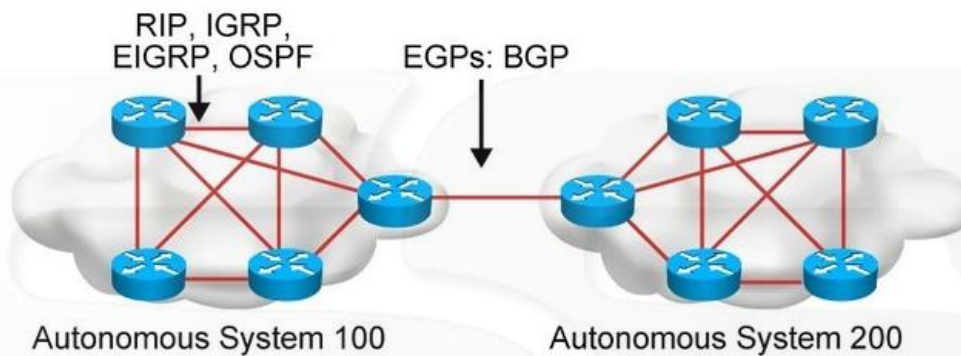
۱. پروتکل های مسیریابی داخلی Interior Gateway Protocols - IGP:

برای مسیریابی درون یک سیستم مستقل AS استفاده می شوند.

۲. پروتکل های مسیریابی خارجی Exterior Gateway Protocols - EGP:

برای مسیریابی بین سیستم های مستقل AS استفاده می شوند.

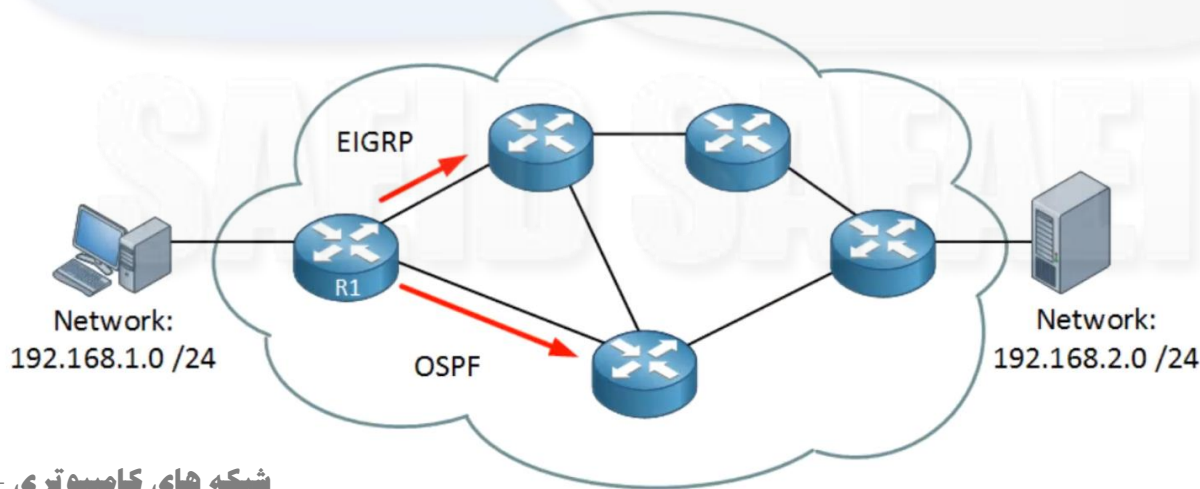
پروتکل های مسیریابی چیست؟



مفهوم Administrative Distance یا AD :

(پروتکل، قانون یا) ساختاری که در روتر قرار گرفته است و هنگامی که باید بین پروتکل های مختلف در هر Leg یا دست، تصمیم گیری برای انتخاب باشد از این **جدول** استفاده میشود. (البته این جدول را میتوان در روتر تغییر داد)

به عبارتی: عددی است که روترها از آن برای تعیین اولویت بین چندین مسیر به یک مقصد استفاده می کنند. وقتی یک روتر از چند پروتکل مسیریابی (مانند RIP, OSPF, EIGRP) اطلاعاتی درباره یک مقصد خاص دریافت می کند، عدد AD مشخص می کند کدام مسیر معتبرتر یا قابل اعتمادتر است.



جدول Administrative Distance یا AD :

پروتکل یا منبع	Administrative Distance (AD)
Directly Connected (اتصال مستقیم)	0
Static Route (مسیر استاتیک)	1
EIGRP (اینترنال)	90
OSPF	110
RIP	120
EIGRP (اکسترنال)	170
Unreachable (غیرقابل دسترس)	255

فرض کنید روتر برای رسیدن به شبکه ۱۹۲.۱۶۸.۱۰۰/۲۴ سه مسیر دریافت می کند:

۱- از RIP (AD = 120)

۲- از OSPF (AD = 110)

۳- از EIGRP (AD = 90)

روتر این مقایسه را انجام می دهد:

EIGRP معتبرتر است زیرا کمترین (90) AD را دارد.

مسیر EIGRP به جدول مسیریابی اضافه می شود و باقی مسیرها نادیده گرفته می شوند.

مفهوم Administrative Distance یا AD :

اما اگر مقادیر AD یکی بود، در مرحله بعد Hop Count یا Bandwidth را نگاه می کند و اولویت را بر اساس آن قرار می دهد.

پس جدول AD به عنوان یک جدول پیش فرض است اگر همه چیز یکی بود، از آن استفاده می شود و گرنه روتر ها همیشه در حال آپدیت هستند و عوامل دیگر می تواند روی آن تاثیر بگذارند مثل تاخیر، پهنای باند و غیره...

و این جدول در اصل نمایانگر Reliability می باشد یعنی مثلا اطمینان این مسیر از آن یکی بالاتر است.

حالا اگر همه شرایط یکسان بود، Load-balance صورت میگیرد و اطلاعات را از هر دو برداشت می کند.

پس در کل AD یک پروتکل است که می گوید اگر از دو مسیر پیام رسید، کدام را بیشتر باور کن و با قابلیت اطمینان بالاتر دریافت کن.

انواع (کلاس های) پروتکل های مسیریابی IGB از نظر الگوریتم:

1. Distance Vector:

مسیر را بر اساس تعداد Hop ها محاسبه می کند. اطلاعات مسیریابی به صورت دوره ای به روترهای مجاور ارسال می شود.

مثال ها: RIP و IGRP

2. Link State:

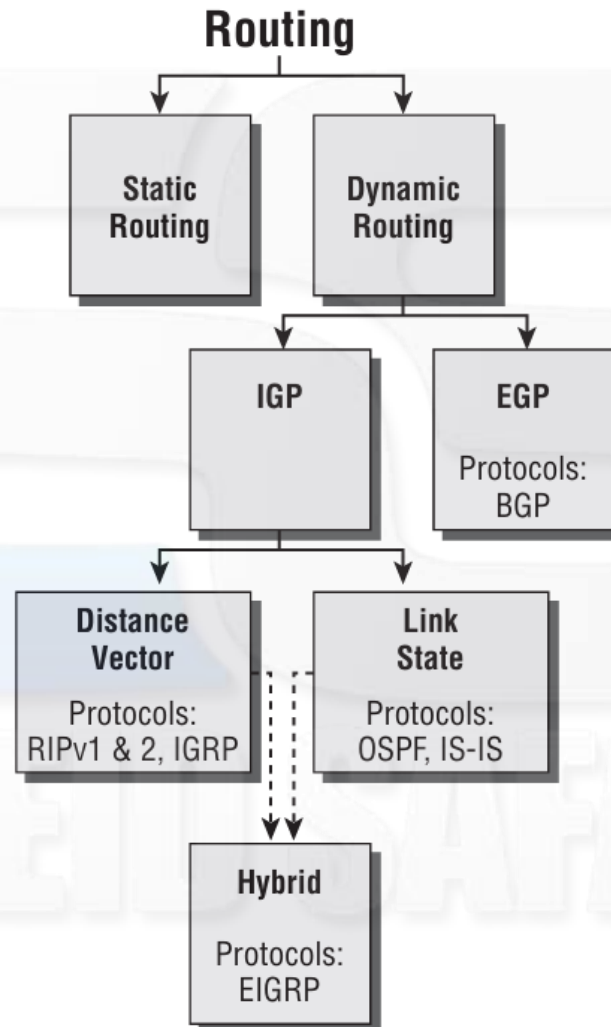
اطلاعات توپولوژی کل شبکه را جمع آوری می کند. هر روتر نقشه ای از کل شبکه را نگه می دارد. از الگوریتم Dijkstra برای یافتن کوتاه ترین مسیر استفاده می کند.

مثال ها: OSPF و IS-IS

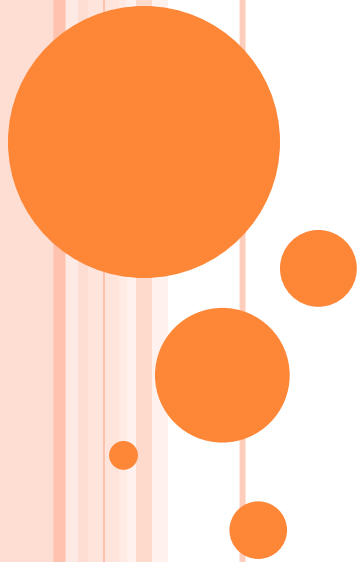
3. Hybrid

ترکیبی از Distance Vector و Link State.

انواع پروتکل‌های مسیریابی :



Distance Vector Routing Protocol



پروتکل Distance Vector:

این پروتکل از معیاری به نام Hop Count یا تعداد پرش استفاده میکند. برای مثال می گوید اگر در یک مسیر تعداد روتر ها بیشتر باشد، عدد بیشتری به آن تعلق می دهد و اولویت کمتری خواهد داشت.

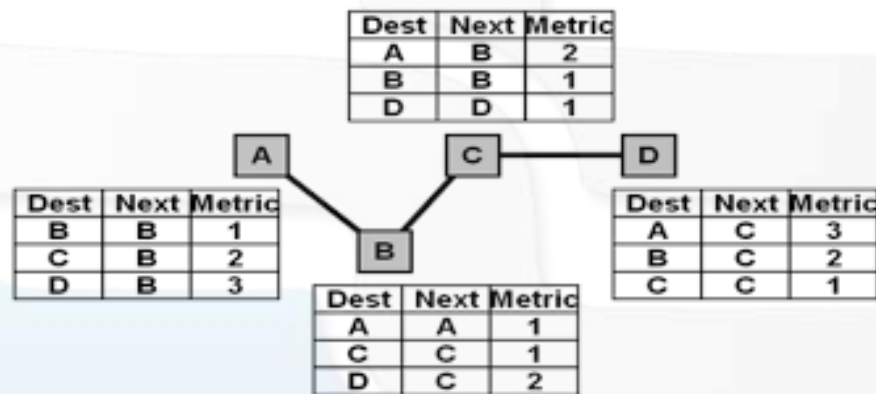
این پروتکل عموماً برای شبکه های کمتر از ۱۶ روتر کانفیگ می شود و با کاهش تعداد لوپ های شبکه، باعث می شود شبکه منسجم و سریعتری داشته باشیم.

اما مشکل اصلی آن این است اطلاعات موجود در جدول آدرس دهی با کوچکترین تغییر برای روتر بعدی ارسال میشود.

و این باعث Incremental Update می شود یعنی جداول مدام در حال آپدیت هستند و همین باعث کندی شبکه می شود.

پروتکل Distance Vector:

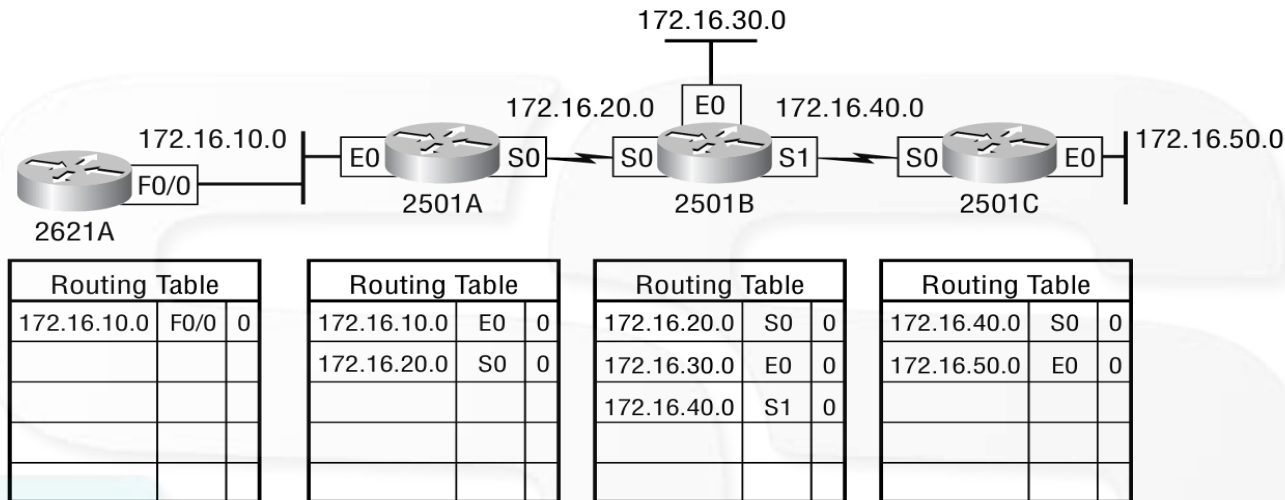
در شبکه‌های ناپایدار، ممکن است به دلیل ارسال سریع اطلاعات، رفتار ناپایدار (مثل انتشار حلقه‌های مسیریابی) رخ دهد.



در این حالت حتی اگر اطلاعات تغییر نکند مدام آپدیت انجام می شود و همین باعث سربار ترافیک و پهنای باند می شود.

ارسال اطلاعات به صورت Broadcast می باشد.

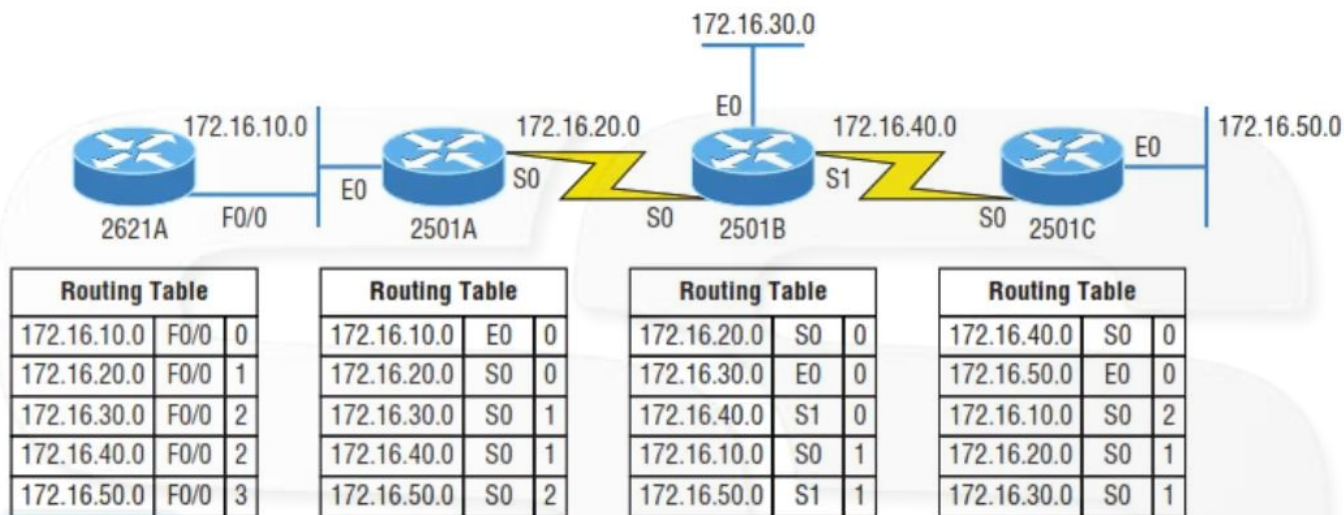
پروتکل Distance Vector:



در لحظه روشن شدن روتر هر کدام از روتر ها جدول مسیر یابی خود را نسبت به هر Leg در جدول پر میکنند.

و بعد روتر ۱ اطلاعات خود را به روتر ۲ می دهد، روتر ۲ اطلاعات خود را به روتر ۳ و ۱ میدهد و هنگامی که روتر ۳ اطلاعات خود را به روتر ۲ و ۴ میدهد در همین حین روتر ۱ دوباره آپدیت می شود چون اطلاعات روتر ۲ آپدیت می شود. (این کار تا زمان به روز رسانی کامل تکرار می شود)

پروتکل Distance Vector:

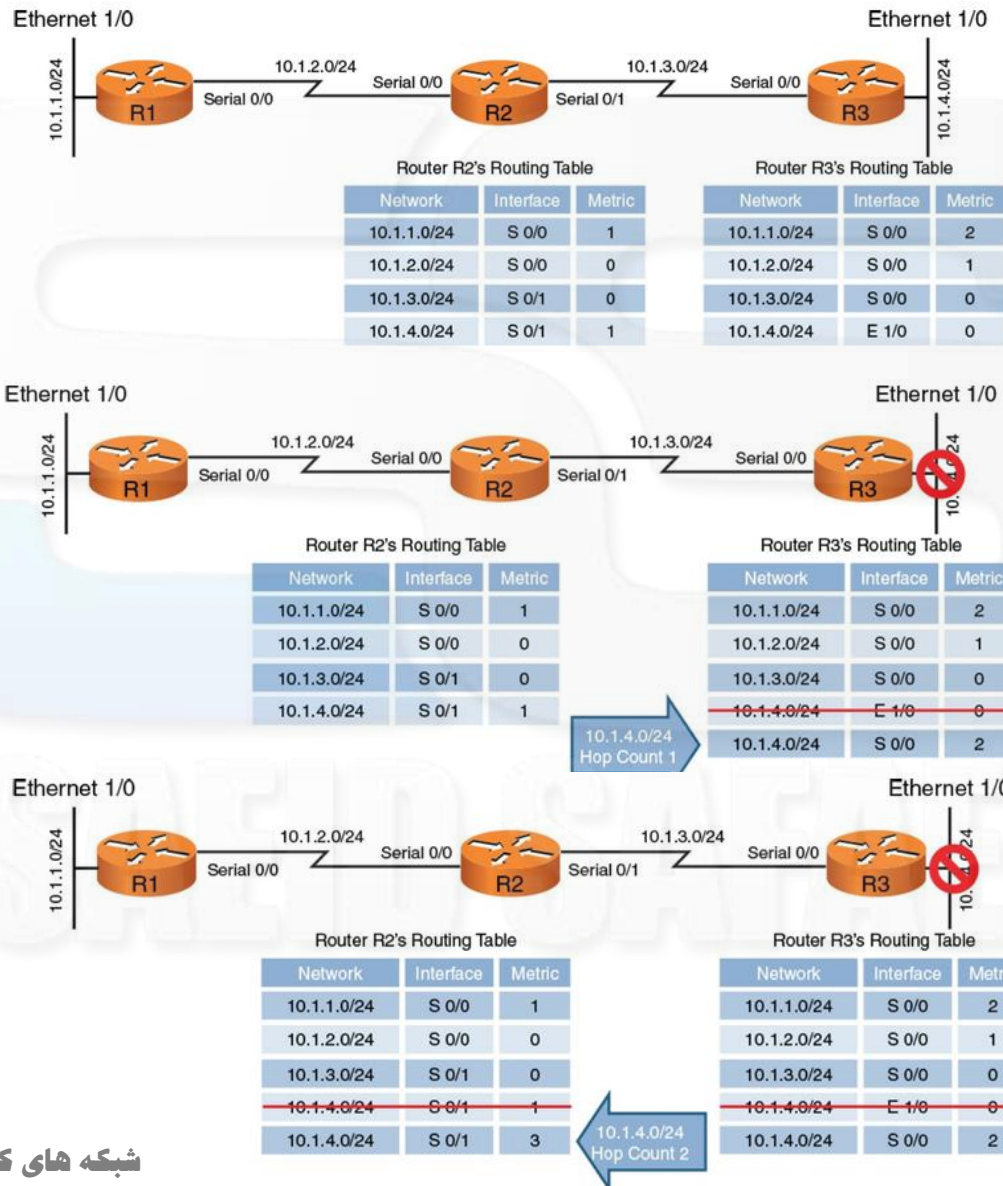


بعد از اینکه همه اطلاعات رد و بدل شد به این شکل می‌رسیم.

یعنی در جداول مسیر یابی IP روتر ها، نام روتر (اینترفیس) و تعداد هاپ های آن مشخص می‌شود.

به این حالت، **Converged Routing Table** می‌گویند، یعنی همه از حال هم با خبر هستند و تمام روترهای موجود در یک AS به یک وضعیت هماهنگ و پایدار از اطلاعات مسیریابی دست یافته‌اند.

پروتکل Distance Vector

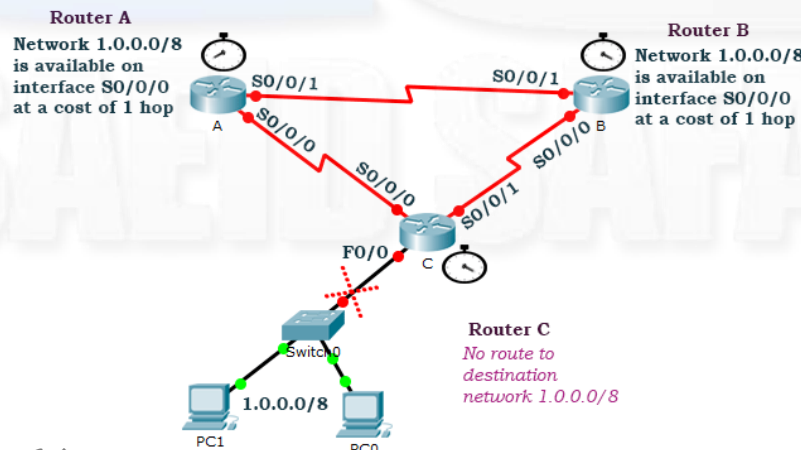


حلقه‌های مسیریابی Routing Loops یا لوپ لایه ۳:

به وضعیتی در شبکه اشاره دارند که در آن بسته‌ها به طور مداوم بین روترها در حال گردش هستند و هیچ‌گاه به مقصد نهایی نمی‌رسند.

این مشکل معمولاً به دلیل اطلاعات نادرست یا قدیمی در جدول مسیریابی روترها رخ می‌دهد و می‌تواند باعث از دست رفتن ترافیک، کاهش کارایی شبکه و بروز مشکلاتی در عملکرد مسیریابی شود.

اگر یک روتر اطلاعات اشتباهی در مورد مسیرها داشته باشد، این اطلاعات ممکن است به سایر روترها منتقل شود و باعث تشکیل حلقه مسیریابی شود.



مسیریابی

پروتکل‌های مسیریابی DV معمولاً از دو رویکرد برای جلوگیری از حلقه‌های مسیریابی Routing Loops استفاده می‌کنند:

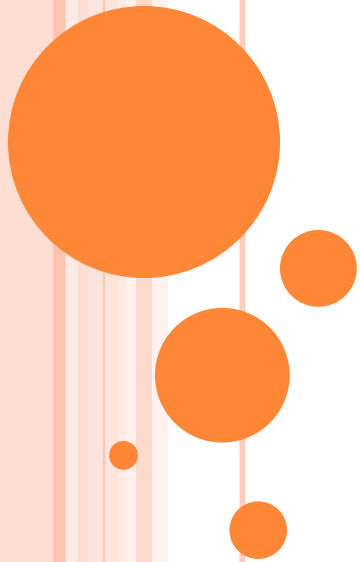
1- Split Horizon:

ویژگی Split Horizon مانع از آن می‌شود که مسیری که از یک رابط یاد گرفته شده است، دوباره از همان رابط به بیرون Advertise شود.

2- Poison Reverse:

ویژگی Poison Reverse باعث می‌شود که مسیری که از یک رابط دریافت شده است، با یک متریک بی‌نهایت Infinite Metric به همان رابط بازگشت داده شود.
این کار برای جلوگیری از حلقه‌های مسیریابی انجام می‌شود.

Link State Routing Protocol



پروتکل مسیریابی Link State:

در این حالت بر خلاف مدل قبل، شبکه را فقط بر اساس تعداد هاپ ها یا روتر ها نمیبینند.

در ضمن اطلاعات به صورت Multicast ارسال می شود و تنها وقتی جداول تغییر کند برای سایر روتر ها ارسال می شود و همین باعث پایداری بیشتر شبکه می شود.

در صورت آپدیت شدن یا تغییر، ارسال اطلاعات در قالب **Link State Advertisement** یا **LSA** ارسال می شود و کل اطلاعات ارسال نمی شود.

پس در LS ها بر خلاف DV ها فقط متوجه تغییر می شویم و خود روتر باید پردازش را انجام دهد. (پس نیاز به memory و CPU دارد) تا بقیه مسیر را، مسیریابی کند.

:Link State Advertisement (LSA)

یک بسته (پکت) است که تغییرات ایجاد شده در LS را در خود درج می کند.

ارسال این پکت باعث می شود:

۱- یک توپولوژی دقیق از شبکه بسازند:

هر روتر اطلاعات دقیقی درباره لینک ها و روترهای متصل به آنها دارد.

۲- بهینه ترین مسیر را محاسبه کنند:

با استفاده از الگوریتم **Dijkstra** و اطلاعات **LSA**، کوتاه ترین مسیر تا مقصد محاسبه می شود.

ویژگی‌های مهم LSA :

۱- انتشار سراسری Flooding :

LSA ها به همه روترها در ناحیه (Multicast) ارسال می‌شوند، نه فقط به همسایگان مستقیم.

۲- عدم انتشار دوره‌ای :

برخلاف پروتکل‌هایی مانند LSA, RIP فقط در صورت تغییر توپولوژی یا به صورت دوره‌ای (با عمر مشخص) ارسال می‌شود.

۳- به‌روزرسانی سریع :

اگر تغییری در شبکه رخ دهد، LSA ها فوراً به‌روزرسانی شده و به همه روترها ارسال می‌شوند.

ویژگی‌های مهم LSU :

LSU مخفف Link-State Update است و یکی از پیام‌های کلیدی در پروتکل OSPF (Open Shortest Path First) است.

این پیام بخشی از فرآیند انتشار اطلاعات توپولوژی شبکه بین روترهای OSPF محسوب می‌شود.

مشابه یک سیستم موقعیت‌یاب جهانی GPS در یک اتومبیل، روتر می‌تواند الگوریتمی را برای محاسبه بهترین مسیر (یا مسیرها) به یک شبکه مقصد اجرا کند.

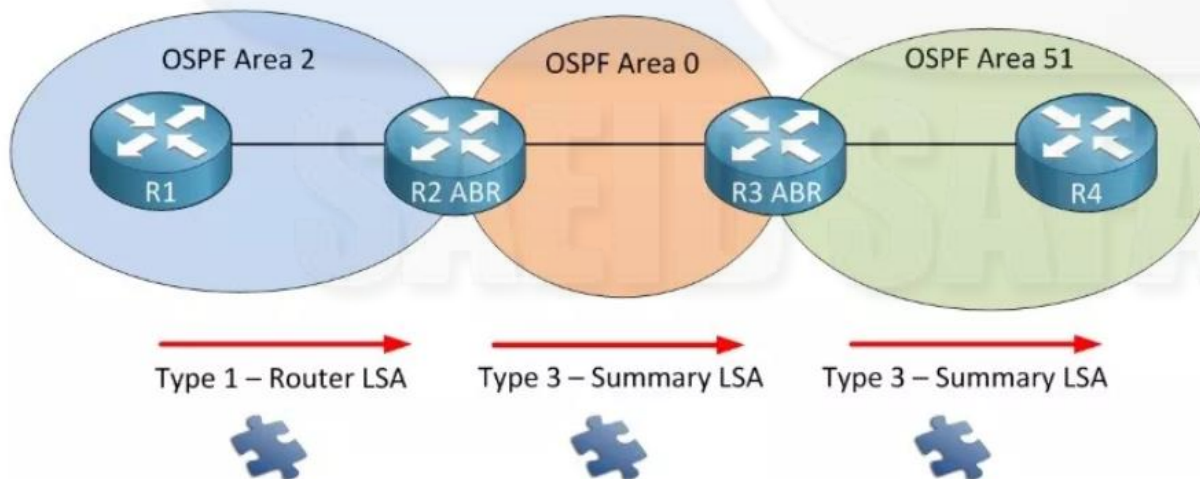
روترها LSAs را ارسال می‌کنند تا شبکه‌هایی را که می‌دانند چگونه به آنها دسترسی پیدا کنند، Advertise کنند.

تفاوت های Link State و Distance Vector

۱- LS ها نیاز به پردازش یعنی CPU و Ram هستند پس دیوایس های گرانتری هستند.

۲- LS ها Multicast انجام میدهند در مقابل DV ها که برادکست هستند.

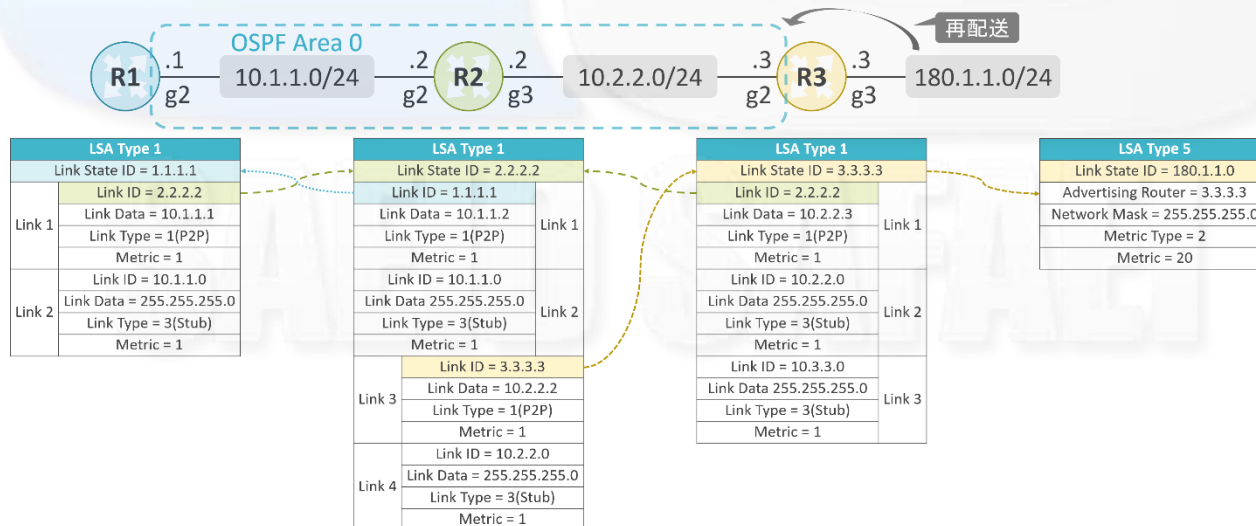
۳- در LS ها فقط وقتی دیتا (LSA) ارسال می شود که تغییر ایجاد شده است اما در DV ها به صورت دوره ای ارسال (کل اطلاعات جدول) انجام میشود.



Topological Database چیست؟

Link State Topological Database که معمولاً در پروتکل‌های مسیریابی Link State مانند OSPF و IS-IS استفاده می‌شود، پایگاه داده‌ای است که هر روتر اطلاعاتی درباره توپولوژی شبکه، شامل وضعیت لینک‌ها و روترهای متصل، را در آن ذخیره می‌کند.

این پایگاه داده شامل اطلاعات دقیقی است که روتر از پیام‌های Link State Advertisement (LSA) دریافت می‌کند.



Topological Database چیست؟

به جای اینکه روترهای همسایه جدول‌های مسیریابی کامل خود را با یکدیگر مبادله کنند، یک پروتکل مسیریابی Link-State به صورت Adjacency به روترها این امکان را می‌دهد که نقشه توپولوژیکی از شبکه بسازند.

این نقشه توپولوژیکی به روترها کمک می‌کند تا اطلاعات دقیق‌تری در مورد ساختار شبکه و مسیرهای بهینه برای رسیدن به مقصدها داشته باشند. بدون اینکه نیاز به ارسال تمام جداول مسیریابی بین روترها باشد.

به طور خلاصه، Adjacency به فرایند برقراری ارتباط و هماهنگی بین روترها برای تبادل اطلاعات مسیریابی اشاره دارد.

مراحل ایجاد و استفاده از Topological Database :

- ۱- دریافت پیام‌های LSA : هر روتر اطلاعات لینک‌های خود را از طریق LSA به سایر روترها ارسال می‌کند.
- ۲- ذخیره در پایگاه داده: LSA ها به صورت سازمان‌دهی شده در Topological Database ذخیره می‌شوند.
- ۳- محاسبه توپولوژی: روتر با استفاده از الگوریتم Dijkstra، بهترین مسیرها را برای هر مقصد محاسبه می‌کند.
- ۴- به‌روزرسانی پایگاه داده: اگر تغییری در توپولوژی شبکه رخ دهد، پیام‌های جدید LSA دریافت و پایگاه داده به‌روزرسانی می‌شود.

تفاوت Routing Table و Topological Database :

جدول مسیریابی Routing Table :

- ۱- **محتویات:** شامل اطلاعاتی در مورد مسیرهای فعلی است که برای رسیدن به مقاصد مختلف استفاده می‌شود.
- ۲- **هدف:** استفاده می‌شود برای تصمیم‌گیری در مورد ارسال بسته‌های داده به مقصد نهایی.
- ۳- **نحوه استفاده:** روترها از جدول مسیریابی برای تصمیم‌گیری در مورد ارسال هر بسته استفاده می‌کنند.
- ۴- **به‌روزرسانی:** به‌روزرسانی می‌شود بر اساس اطلاعاتی که از پروتکل‌های مسیریابی دریافت می‌کند.

تفاوت Routing Table و Topological Database

پایگاه داده توپولوژیکی Topological Database

۱- **محتویات:** شامل اطلاعاتی در مورد توپولوژی شبکه است، مانند:

لیستی از روترها و دستگاه‌های شبکه

ارتباطات بین آن‌ها (لینک‌ها)

ویژگی‌های لینک‌ها (مانند سرعت، تاخیر، هزینه)

۲- **هدف:** استفاده می‌شود برای محاسبه مسیرهای بهینه بین مقاصد مختلف در شبکه.

۳- **نحوه استفاده:** پروتکل‌های مسیریابی مانند OSPF و IS-IS از این پایگاه داده استفاده می‌کنند تا مسیرهای بهینه را محاسبه کنند.

۴- **به‌روزرسانی:** به طور مداوم به‌روزرسانی می‌شود تا تغییرات در توپولوژی شبکه را منعکس کند.

تفاوت Topological Database و Routing Table:

پایگاه داده توپولوژیکی یک نقشه جامع از شبکه است که برای محاسبه مسیرهای بهینه استفاده می‌شود شامل اطلاعات توپولوژی نظیر MTU، پهنای باند و سایر Cost ها می‌باشد، در حالی که جدول مسیریابی یک لیست از مسیرهای فعلی است که برای ارسال ترافیک استفاده می‌شود.

هر دو جزء مهمی از فرآیند مسیریابی در شبکه‌های کامپیوتری هستند.

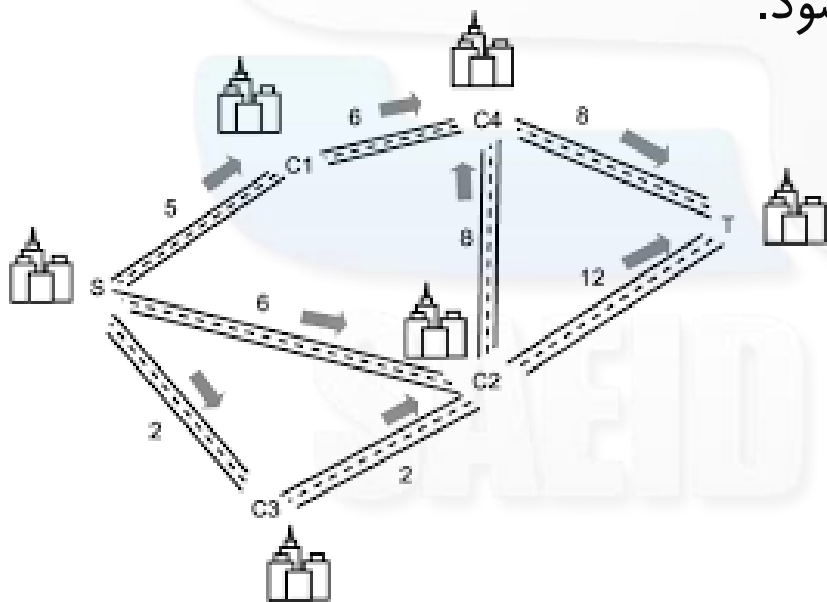
Topological Database	Routing Table
شامل اطلاعات خام درباره توپولوژی شبکه	شامل مسیرهای نهایی برای ارسال بسته‌ها
ساخته می‌شود LSA از	تولید می‌شود (مانند Dijkstra) از محاسبات الگوریتم
به تمام شبکه نگاه می‌کند	فقط بهترین مسیرها را ذخیره می‌کند
استفاده می‌شود Link State در پروتکل‌های	وجود دارد (Link State یا Distance Vector) در همه روترها

مسیر یابی

الگوریتم دایجسترا **Dijkstra Algorithm** : (براساس کوتاه ترین مسیر)

الگوریتم دایجسترا یکی از معروف ترین الگوریتم ها برای یافتن کوتاه ترین مسیر از یک گره مبدأ به سایر گره ها در یک گراف وزن دار است.

این الگوریتم توسط ادسخر دایجسترا Edsger Dijkstra در سال ۱۹۵۶ ارائه شد و به طور گسترده در شبکه های کامپیوتری، سیستم های مسیریابی و بسیاری از زمینه های دیگر استفاده می شود.



مراحل الگوریتم دایجسترا:

۱- مقداردهی اولیه:

هزینه رسیدن به گره مبدأ برابر با ۰ در نظر گرفته می شود.

هزینه سایر گره ها به ∞ (بی نهایت) مقداردهی می شود.

یک مجموعه از گره های بازدید نشده Unvisited ایجاد می شود.

۲- انتخاب گره با کمترین هزینه:

از میان گره های بازدید نشده، گره ای که کمترین هزینه را دارد انتخاب می شود.

۳- به روزرسانی هزینه گره های همسایه:

برای هر همسایه گره فعلی، هزینه رسیدن به آن گره محاسبه و در صورت کمتر بودن، مقدار به روزرسانی می شود.

مراحل الگوریتم دایجسترا:

۴- علامت گذاری گره به عنوان بازدید شده:

گره فعلی به مجموعه بازدید شده اضافه می شود و دیگر بررسی نمی شود.

۵- تکرار:

مراحل ۲ تا ۴ تکرار می شود تا همه گره ها بررسی شوند.

1. مقداردهی اولیه:

`Distance[Source] = 0`

`Distance[OtherNodes] =  $\infty$`

`Mark all nodes as Unvisited`

2. While there are unvisited nodes:

a. Select the unvisited node with the smallest Distance

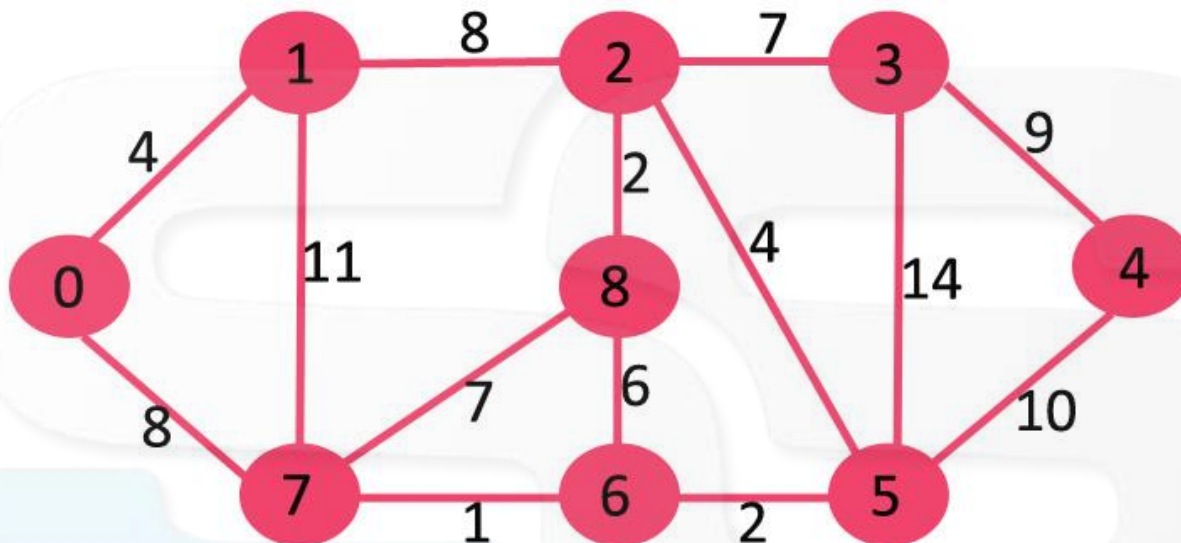
b. For each neighbor of the current node:

i. Calculate the distance through the current node

ii. If the new distance is smaller, update it

c. Mark the current node as Visited

مثال الگوریتم دایجسترا:



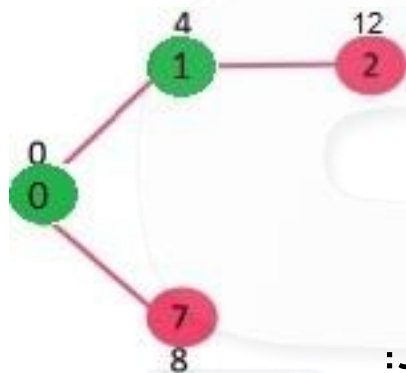
۱- ابتدا به گره 0 مقدار ۰ داده و سایر گره‌ها را ∞ در نظر می‌گیریم

۲- در مرحله بعد همسایگان 0 را پیدا می‌کنیم و وزن آنها را قرار می‌دهیم



مثال الگوریتم دایجسترا:

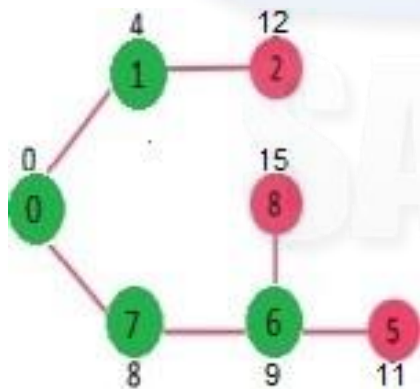
۳- حالا از کمترین وزن یعنی گره 1 همسایه هایش را پیدا میکنیم و وزن دهی میکنیم.



با توجه به اینکه یال 1 به 2 دارای وزن ۸ می باشد پس هزینه 0 به 2 برابر ۱۲ میشود.

این مقدار از مقدار 0 به 7 بیشتر است پس در مرحله بعد:

۴- از سمت گره 7 همسایه با کترین هزینه را پیدا میکنیم، یعنی گره 6 و مجموع هزینه 0 تا 6 برابر ۹ می شود.

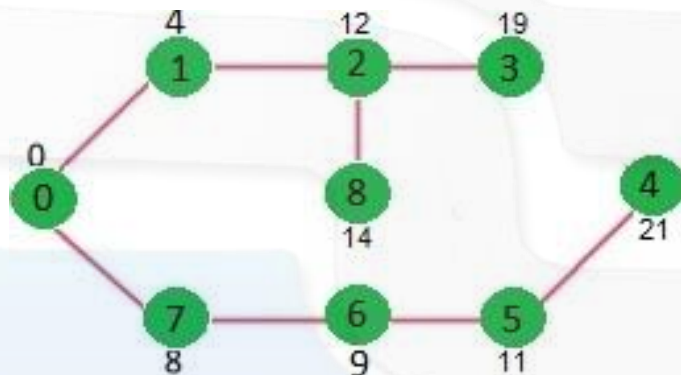


۵- در مرحله بعد مبینیم 0 به 5 بهترین فاصله را دارد یعنی ۱۱ پس آنرا انتخاب میکنیم.

مثال الگوریتم دایجسترا:

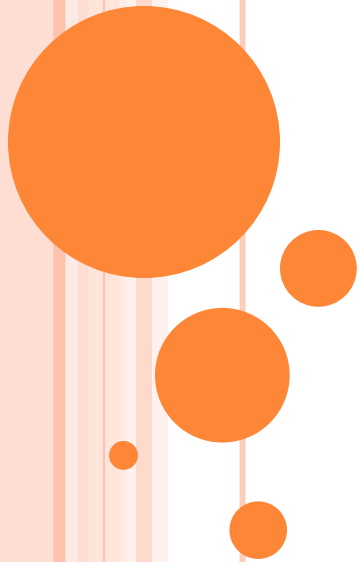
۶- در مرحله بعد میبینیم یال ۵ به ۴ دارای هزینه ۱۰ است یعنی در مجموع ۲۱، پس دوباره به سمت یال ۲ می رویم.

۷- این کار را بارها انجام میدهیم تا در نهایت، درخت کوتاهترین مسیر حاصل می شود.



در پروتکل OSPF، روترها از الگوریتم دایجسترا برای محاسبه کوتاهترین مسیر (Short Path Factor) به تمام مقاصد استفاده می کنند. اطلاعات توپولوژی از Link State Database (LSDB) گرفته شده و الگوریتم بر اساس آن اجرا می شود.

Hybrid Routing Protocol



پروتکل‌های مسیریابی Hybrid چیست؟

پروتکل‌های مسیریابی Hybrid ترکیبی از ویژگی‌های Distance Vector و Link State هستند.

این پروتکل‌ها سعی دارند نقاط قوت هر دو روش را در کنار هم استفاده کنند و ضعف‌های آن‌ها را کاهش دهند.

در این نوع پروتکل‌ها، از مکانیزم‌های Distance Vector برای انتشار اطلاعات مسیر و از روش‌های Link State برای ارائه جزئیات توپولوژی دقیق‌تر یا بهبود تصمیم‌گیری استفاده می‌شود.

ویژگی‌های پروتکل‌های Hybrid :

- ۱- ترکیب بهینه‌سازی شده: بهره‌گیری از محاسبات دقیق Link State و سادگی انتشار اطلاعات Distance Vector .
- ۲- مقیاس‌پذیری: مناسب برای شبکه‌های بزرگ‌تر نسبت به Distance Vector و ساده‌تر از Link State .
- ۳- انتشار بهینه اطلاعات: فقط تغییرات مهم Incremental Updates را به اشتراک می‌گذارد، نه کل توپولوژی.
- ۴- کاهش بار پردازشی: مانند Distance Vector ، نیازی به نگهداری کامل توپولوژی شبکه ندارد.
- ۵- پایداری و سرعت همگرایی: زمان همگرایی Convergence نسبت به Distance Vector سریع‌تر است.

مقایسه الگوریتم ها با یکدیگر:

ویژگی	Distance Vector	Link State	Hybrid
دقت توپولوژی	کم	زیاد	متوسط تا زیاد
زمان همگرایی	کند	سریع	سریع
مصرف پهنای باند	زیاد (دوره‌ای)	متوسط	کم (انتشار تغییرات)
مصرف منابع پردازشی	کم	زیاد	متوسط
مثال پروتکل‌ها	RIP, IGRP	OSPF, IS-IS	EIGRP, BGP



با تشکر از همراهی شما

محمد سعید صفایی صادق

