معماری و طراحی شبکه‌های رایانه‌ای

Architecture and Design of Computer Networks

نسخه ۲٫۶

دوره مهندسی فناوری شبکه‌های رایانه‌ای

مدرس: احسان خان احمدی

LinkedIn
https://www.linkedin.com/in/ehsan-khanahmadi-22a3776a/

خصوصیات دوره

یادداشت برداری مهم است

نظری

+

کاربردی

ملاحظات دوره

ابتدا:

- مقررات دانشگاه و کلاس رعایت شود.
- تلفن همراه فراگیر در کلاس خاموش یا در حالت بی‌صدا قرار داده شود.
- در کلاس با تلفن همراه کار نشود.
- فراگیر با هم‌گروهی‌ها برای انجام تمرین‌ها و موارد دوره هماهنگ باشد.
- موارد مهم نکته‌برداری شود. (درس و ارائه‌ها)

نیازمندی‌های درس «معماری و طراحی شبکه‌های رایانه‌ای» مهیا شود:

- یک لغت‌نامه خوب برای مطالعه و ترجمه اصطلاحات تخصصی
- مرور و مطالعه پیش‌نیاز: شبکه‌های پیشرفته رایانه‌ای

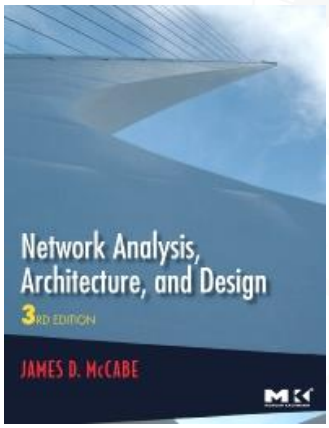
ارائه درس(۲ واحد نظری/۱ واحد عملی)**:**

سخنرانی، کار گروهی و مشارکتی، تمرین و تکرار، منابع دیداری و شنیداری

نکته: مواردی که به زبان غیر از فارسی آمده است در کلاس تشریح می‌شود، نکته برداری شود.

منابع

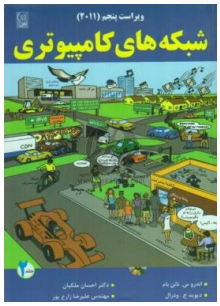
- **Network Analysis, Architecture, and Design**
  - **James McCABE, Elsevier, 2007**
  - **مطالب مطرح شده در طول دوره**

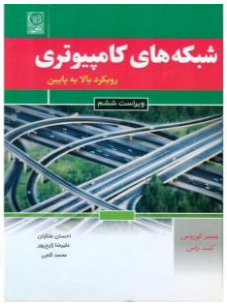


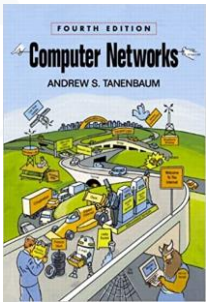
منابع کمکی

- **شبکه‌های رایانه‌ای**، تننباوم، ترجمه دکتر حسین پدرام، انتشارات نص، ۱۳۸۵
- **شبکه‌های رایانه‌ای، رویکرد بالا به پایین**، ویراست ششم، جیمز کوروس, کیت راس، احسان ملکیان، علیرضا زارع پور, محمد گنجی، انتشارات نص ۱۳۹۹

- **Network Analysis, Architecture and Design**
  - **James Mcabe, Elsevier, 2007**





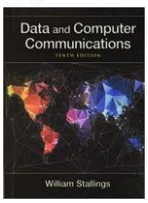


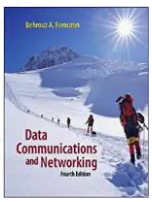
منابع کمکی و نرم‌افزارهای مورد نیاز

- **شبکه‌های رایانه‌ای و کارگاه، انتشارات کیان رایانه**
- **انتقال داده‌ها و شبکه‌های رایانه‌ای**، ویلیام استالینگز، ترجمه قدرت سپیدنام، علوم رایانه، ۱۳۸۸
- **Network+**

- **Data and Computer Communications**
  - **10th Edition by William Stallings, Pearson; 2007 (or 2013)**
- **Data Communications and Networking**
  - **4th edition, by Behrouz Forouzan, McGraw-Hill; 2003 (or 2006)**

- نرم افزار شبیه‌ساز شبکه: Cisco Packet Tracer 6.2
- نرم افزارهای: Zenmap/NMAP/Wireshark





انتظارات، فعالیت‌های کلاسی و نمره نهایی

نمره نهایی از ارزیابی دانشجو مبتنی بر شاخص‌های زیر انجام خواهد شد:

- **نمره میان‌نیمسال و ارزیابی فعالیت‌های مستمر:**
  - آمادگی هر جلسه برای مرور مطالبی که از ابتدای نیمسال مطرح شده
  - حل تمرین‌های داده شده و چند Quiz در طول نیمسال
- **آزمون پایانی**
- **ارائه فایل مطالعه شده و فایل ویدئویی توضیح آن با رعایت نکات زیر:**
  - به تایید رساندن موضوع فایل مطالعه شده توسط مدرس
  - برای تایید شدن موضوع لازم است چند دقیقه در کلاس توضیح داده شود و موضوع مرتبط با هدف درس باشد.
  - آماده کردن فایل مطالعه شده با فرمت مشخص شده در صفحه بعد به صورت PPT (نام فایل همان نام دانشجو – نام درس به انگلیسی باشد) و ارسال به مدرس
  - دست کم نیمی از نمره فایل مطالعه شده مربوط به «**چکیده آنچه فرا گرفتم و پرسش و پاسخ**» است که باید توسط دانشجو پس از مطالعه متن فایل مطالعه شده، آن مقدار که فرا گرفته نگاشته شود.
  - ارائه یا ارسال یک ویدئوی حدود ده دقیقه‌ای از ارائه فایل PowerPoint با تأکید بر تشریح مطالب اصلی درس
  - **پیشینه زمان ارسال فایل‌های مطالعه شده و ویدئو به مدرس:**
    - **پیش از آزمون میان نیمسال: تا پایان فصل اول و سه جلسه پیش از جلسه آخر: فایل کامل**
  - Subject شامل مشخصات فردی و دانشگاهی، درس، روز و ساعت کلاس باشد

مثال Subject: دانشگاه انفورماتیک ایران، رایان معماری اصل، معماری و طراحی شبکه‌های رایانه‌ای، پنج‌شنبه ۱۴:۰۰-۱۶:۰۰

نام فایل: Network-Rayan-MemariAsl.ppt

نکته: در دوره‌های مجازی ارتباط از طریق سامانه مجازی دانشگاه انجام می‌شود.

ارزیابی اصلی در طول نیمسال انجام می‌شود

قالب مستندات پروژه PPT

قلم و اندازه: Tahoma

- عنوان‌ها Bold 24 or 28، (متن نمابرگ‌ها Normal 14 تا Normal 16 به صلاح‌دید فراگیر)
- درج **شماره نمابرگ** و **عنوان** برای همه‌ی نمابرگ‌های پرونده‌ها ضروری است. (حتی اگر تکرار شود)
- اجرای Animation: نمابرگ‌ها حرکت و تغییر نداشته باشند (اما برخی اجزا می‌توانند)

محتوای صفحات:

- نمابرگ۱: بنام خدا، موضوع، نام و رایانامه دانشجو، نام و رایانامه مدرس، نام درس، تاریخ
- نمابرگ ۲: فهرست (با تلیک روی هر موضوع، نمابرگ آن موضوع نمایش داده شود)
- **نمابرگ۳: آنچه فرا گرفتم (خلاصه هر چه دانشجو فراگرفته)**

فصل اول:

- نمابرگ ۵ به بعد: بیست پرسش و پاسخ از همه موضوع‌ها (هیچ موضوع اصلی از قلم نیفتد)
  - **همه مباحث اصلی در فصل اول بررسی شود**

فصل دوم:

- نمابرگ‌های بعد: تشریح یک موضوع تخصصی (از زبان محاوره ای در مستندات بررسی استفاده نشود)
  - **یک موضوع تایید شده (با جزئیات) در این فصل بررسی شود.**
- نتیجه‌گیری و پیشنهادها
- منابع (برای منابع اینترنتی فقط URL کافی است، منابع مکتوب: نام کتاب با ذکر شماره صفحات، تجربه کاری: نام محل کار، سمت و تاریخ)
- واژه‌های پر استفاده در این درس به انگلیسی و فارسی (این نمابرگ اختیاری است)
- ترجمه نمابرگ۱ به انگلیسی (در صورتی که برای این نمابرگ مشکل دارید، در کلاس از مدرس کمک بگیرید)
- ؟ (در صورت ارائه در کلاس)

مشاهده‌ی نمونه ویدئوی آموزش شیوه‌ی آماده‌سازی PowerPoint: aparat.com/v/jEB4 یا KhanAhmadi.ir

هدف و عناوین (برای هر مورد دست کم یک اسلاید در فصل اول مستند ایجاد شود)

هدف درس: دست‌کم ۲ هدف قابل سنجش و اندازه‌گیری

- شناخت اصول طراحی شبکه‌های رایانه‌ای
- شناخت معماری و خدمات شبکه‌های رایانه‌ای

مباحث اصلی:

۱) مفاهیم معماری و طراحی شبکه‌های رایانه‌ای

۲) اصول و مبانی لایه پیوند فیزیکی و منطقی

۳) شبکه محلی

۴) آدرس‌دهی و مسیریابی

۵) شبکه‌های بی‌سیم

جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

۱) مفاهیم معماری و طراحی شبکه‌های رایانه‌ای

۱) معماری شبکه‌های رایانه‌ای

۲) طراحی شبکه‌های رایانه‌ای

۳) اصول طراحی شبکه‌های رایانه‌ای

۴) معماری لایه‌ای شبکه‌های رایانه‌ای

۵) معماری خدمات

۶) پروتکل‌های کلیدی و تکامل آنها

۷) ساختار اینترنت

۸) روندهای تکامل معماری شبکه

۹) معماری TCP/IP

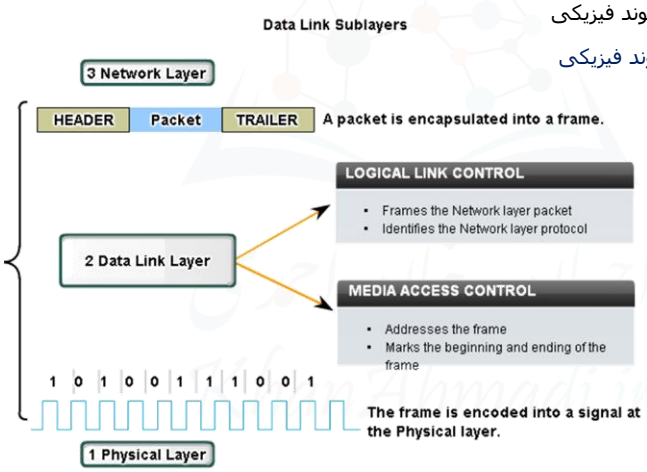
۱۰) معماری OSI

جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

۲) اصول و مبانی لایه پیوند فیزیکی و منطقی

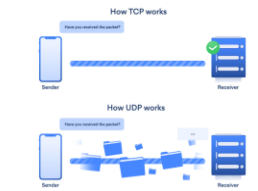
۱) مبانی لایه پیوند فیزیکی

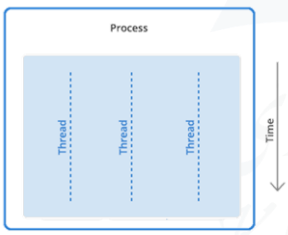
۲) اصول لایه پیوند فیزیکی



جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

۳) شبکه محلی





۱) شبکه محلی و اجزای آن

۲) سرویس

۳) TCP در مقابل UDP و موارد دیگر

۴) فرمت‌های بسته

۵) برنامه‌های کاربردی سرویس‌گیرنده-سرور

۶) مقیاس پذیری

۷) Thread vs Process

۸) Sockets ،Remote Procedure Calls (RPC) برای ارتباط

۹) پروتکل Zenmap/NMAP/Wireshark و تجزیه و تحلیل پورت

جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

۴) آدرس‌دهی و مسیریابی

۱) معماری شبکه‌های جدید
۲) مسیریابی بین شبکه‌ای
۳) الگوریتم‌های مسیریابی
۴) مسیریابی بین دامنه بدون کلاس CIDR
۵) مسیریابی بین دامنه IDR
۶) ویژگی‌های BGP و IBGP
۷) شبکه انتقال Backbone
۸) شبکه انتقال نوری
۹) IP از طریق SDH
۱۰) IP از طریق WDM/ASON
۱۱) IP از طریق WDM/GbEthernet
۱۲) MPLS
۱۳) از MPLS تا GMPLS (Generalized MPLS)
۱۴) SDN (Software-Defined Networking)
۵۱) پروتکل‌های جدید شبکه و انتقال
۱۶) IPv4-IPv6
۱۷) MIP آی پی موبایل
۱۸) IP Multicast
۱۹) HIP (Host Identity Protocol)
۲۰) TCP چند مسیره
۲۱) QUIC (Quick UDP Internet Connection)
۲۲) ...

جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

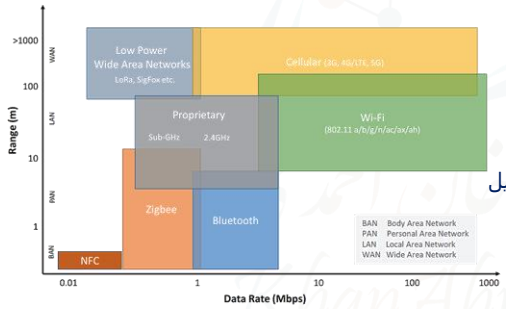
۴) ادامه موارد آدرس‌دهی و مسیریابی

۲۲) انتقال قابل اعتماد در مقابل غیر قابل اعتماد
۳۲) کنترل تراکم
۴۲) پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی
۵۲) اعمال فیلترها در TCPdump و Wireshark Assignment
۲۶) ARP، مسیریابی IP و ابزارهای عیب‌یابی

جزئیات مباحث و عناوین اصلی معماری و طراحی شبکه‌های رایانه‌ای

۵) شبکه‌های بی‌سیم

۱) ارتباطات بیسیم Wi-Fi
۲) شبکه‌های سلولی
۳) رسانه و عملکرد
۴) قدرت سیگنال
۵) فشرده‌سازی و تشخیص سیگنال
۶) تأخیر، از دست دادن توان عملیاتی
۷) طراحی شبکه‌های بی‌سیم و موبایل

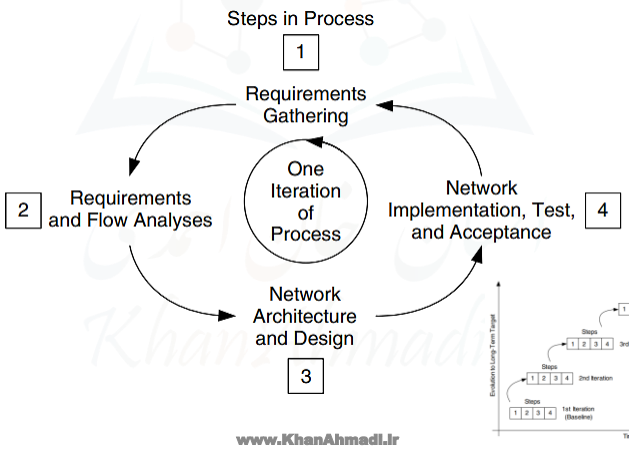


محدوده و نرخ داده برای فناوری‌های مختلف بی‌سیم

مقدمه مفاهیم معماری و طراحی شبکه

اهمیت عملیاتی و راهبردی

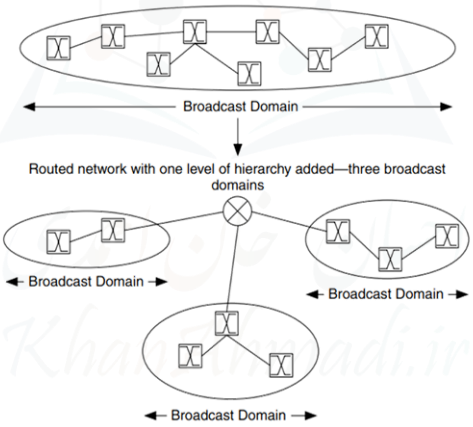
- ماهیت چرخه‌ای و تکرار شونده فرآیندها



مقدمه مفاهیم معماری و طراحی شبکه

اهمیت عملیاتی و راهبردی

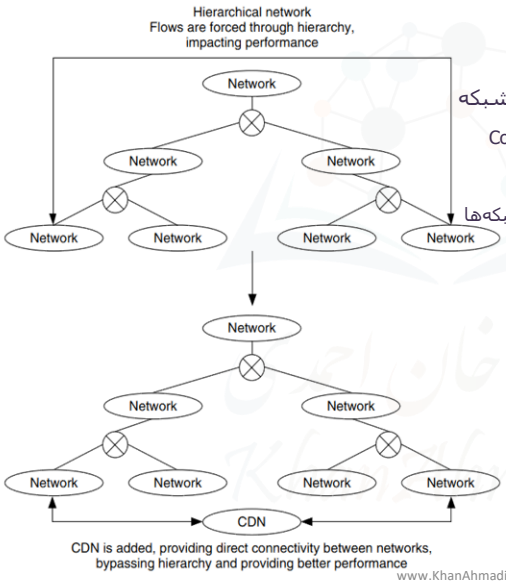
- اضافه شدن سلسله مراتب به یک شبکه



مقدمه مفاهیم معماری و طراحی شبکه

اهمیت عملیاتی و راهبردی

- اضافه شدن سلسله مراتب به یک شبکه
- کاربرد: Content Delivery Network (**CDN**)
  - اضافه شدن CDN
  - فراهم شدن اتصال مستقیم بین شبکه‌ها
  - دور زدن سلسله مراتب
  - ارائه عملکرد بهتر
    - با اصلاح رفتار مسیریابی



مدل سلسله مراتبی شبکه

تمرین: تفاوت مدل سلسله مراتبی شبکه (Hierarchical internetworking model) را با مدل Leaf-Spine با رسم شکل توضیح داده و Backbone را در شکل‌ها مشخص کنید.

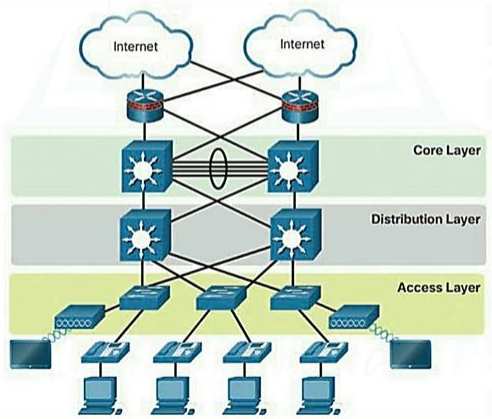
پاسخ را تا جلسه آینده آماده کنید...

در کلاس مثال‌های مختلفی ارائه و نکته برداری شود.

https://patelrasesh.wordpress.com/2014/09/04/spine-and-leaf-vs-traditional-hierarchical-architecture/#:~:text=Hierarchical%20designs%20consist%20of%20three,and%20the%20leaf%20%5Baccess%5D.

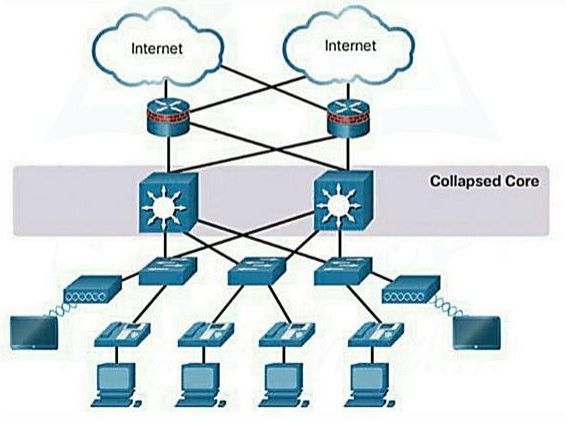
مدل سلسله مراتبی شبکه Hierarchical internetworking model

- با این روش طراحی، ترافیک کاربران در لایه access نگه داشته می‌شود تا درصورتی‌که نیاز باشد به لایه‌های بالاتر منتقل شوند.
- برای افزایش پهنای باند بین سوییچ‌های core از ether channel استفاده می‌شود.



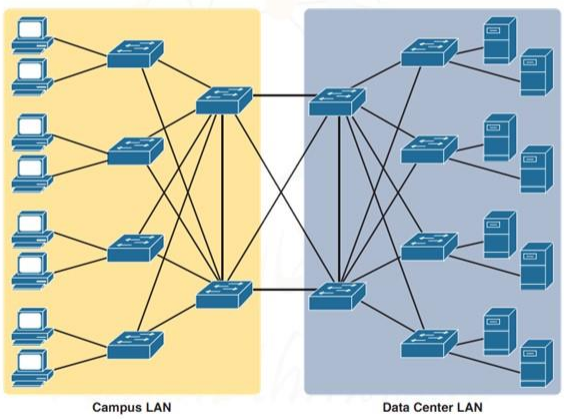
مدل سلسله مراتبی شبکه

- از روش طراحی Collapsed Core برای شبکه‌های کوچک‌تر استفاده می‌شود تا هزینه کمتری برای راه اندازی داشته باشد.
- لایه Core و Distribution با یکدیگر ادغام می‌شوند.



مدل سلسله مراتبی شبکه

- اگر سازمان علاوه بر LAN، دارای مرکز داده هم باشد معمولا طراحی شبکه از شکل زیر پیروی می‌کند.

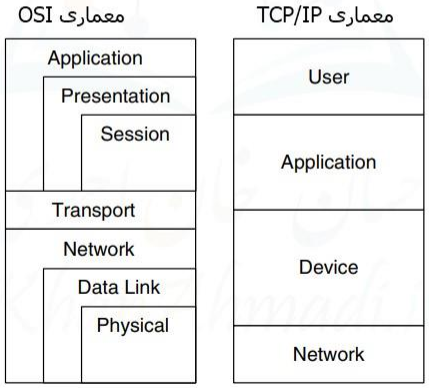


Campus LAN and Data Center LAN, Conceptual Drawing

مقدمه مفاهیم معماری و طراحی شبکه

معماری و طراحی شبکه

- مقایسه لایه‌های OSI با سطوح سیستم



معماری OSI

معماری OSI در هفت لایه از بالا به پایین

- **لایه کاربرد:** رابط میان کاربر و شبکه بوده و تنها لایه مدل OSIاست که کاربر می‌تواند تا حدودی با آن ارتباط برقرار کند. لایه‌ای که واسط میان دو برنامه کاربردی است که هر یک روی کامپیوترهای دیگری قرار دارند.
- **لایه ارائه:** مسئولیت فشرده‌سازی/قالب‌بندی مجدد و/یا رمزگذاری داده‌ها را به شکلی دارد که برنامه مقصد بتواند اطلاعات را بخواند.
- **لایه نشست/جلسه:** توضیح می‌دهد که اگر پیام‌ها با موفقیت با مقصد نرسیدند، چگونه داده‌ها میان برنامه‌های کاربردی همگام‌سازی شده و بازیابی شوند.
- **لایه انتقال**: وظیفه دارد تا بارداده‌های لایه کاربرد را از یک برنامه به برنامه دیگر انتقال دهد. دو پروتکل اصلی به‌کار گرفته شده در این زمینه TCP و UDP است.
- **لایه شبکه:** تا رسیدن بسته‌ها به مقصد، پیام‌ها را از یک گره شبکه به گره دیگری و از یک شبکه به شبکه دیگر انتقال می‌دهد.
- **لایه پیوند داده**: برقراری ارتباط با سخت‌افزار تنها روی شبکه محلی را عهده‌دار هستند.
- **لایه فیزیکی:** تعیین می‌کند که داده از کدام مجرا و به چه شکلی باید به شبکه ارسال شود.

اصول و مبانی لایه پیوند فیزیکی و منطقی

مبانی لایه پیوند فیزیکی

پایین‌ترین لایه در مدل OSI لایه فیزیکی است و مسئول برقراری اتصالات فیزیکی بین دستگاه‌های شبکه است. این لایه به انتقال سیگنال‌هایی مانند الکتریکی، نوری یا مغناطیسی بین دستگاه‌ها می‌پردازد و شامل مشخصات سخت‌افزاری مانند نوع کابل، ولتاژ یا طیف نور و سرعت انتقال داده است.

اجزای کلیدی

رسانه: شامل کابل‌های جفت تابیده، فیبر نوری یا اتصالات بی‌سیم
سیگنال‌ها: تعریف نوع سیگنال (الکتریکی، نوری) و نحوه کدگذاری آن
تجهیزات: شامل مسیریاب‌ها، سوئیچ‌ها و تکرارکننده‌ها که برای انتقال داده‌ها استفاده می‌شوند

ویژگی‌ها

انتقال بیت‌ها: اطلاعات به صورت بیت (۰ و ۱) منتقل می‌شوند.
مدل‌های انتقال: شامل simplex یک طرفه، half duplex دو طرفه غیرهمزمان و full duplex دو طرفه همزمان
نظارت بر اتصالات: این لایه نظارت بر ایجاد و قطع اتصالات را نیز بر عهده دارد

اصول و مبانی لایه پیوند فیزیکی و منطقی

مبانی لایه پیوند منطقی

لایه پیوند منطقی بین لایه فیزیکی و لایه شبکه قرار دارد. این لایه مسئول مدیریت انتقال داده‌ها بدون خطا بین دستگاه‌های متصل به یکدیگر است. این لایه با افزودن سرآیند و دنباله به بسته‌های دریافتی از لایه شبکه، آن‌ها را به Frame تبدیل کرده و برای ارسال به لایه فیزیکی آماده می‌کند.

اجزای کلیدی

فریم‌ها: بسته‌های دریافتی از لایه شبکه به فریم تبدیل شده و شامل نشانی‌های MAC مبدا و مقصد هستند.
کنترل خطا: این لایه اطلاعاتی برای تشخیص خطا در فریم‌ها قرار می‌دهد تا صحت داده‌های دریافتی را تأیید کند.
کنترل دسترسی به رسانه: تعیین نحوه دسترسی دستگاه‌ها به رسانه انتقال داده.

ویژگی‌ها

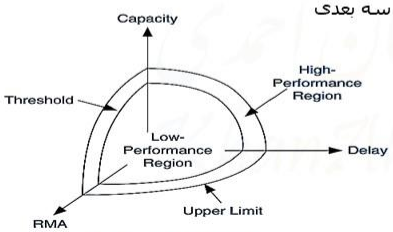
تعامل با سخت‌افزار: این لایه به عنوان واسط بین سخت‌افزار شبکه و نرم‌افزار عمل می‌کند.
تقسیم‌بندی به زیرلایه‌ها: شامل دو زیرلایه Logical Link Control (LLC) که وظایفش شبیه لایه شبکه است و Media Access Control (MAC) که وظایفش بیشتر شبیه لایه فیزیکی است.

در طراحی شبکه‌های رایانه‌ای، درک اصول و مبانی لایه‌های پیوند فیزیکی و منطقی ضروری است. لایه فیزیکی روی انتقال داده]ای خام مانند سیگنال‌های خام تمرکز دارد، در حالی که لایه پیوند منطقی روی مدیریت داده‌ها و اطمینان از انتقال بدون خطا تأکید دارد. این دو لایه به طور مشترک زیرساخت لازم برای ارتباط مؤثر در شبکه‌های رایانه‌ای را فراهم می‌کنند.

مقدمه مفاهیم معماری و طراحی شبکه

معماری و طراحی شبکه

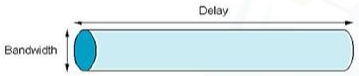
- تمرکز تجزیه و تحلیل، معماری و طراحی شبکه به طور سنتی بر برنامه‌ریزی ظرفیت
- مهندسی شبکه برای ارائه پهنای باند و کمک گرفتن از بافر و کاهش تأخیر
- ویژگی‌های عملکرد:
  - ظرفیت: شامل پهنای باند bandwidth، توان عملیاتی throughput یا goodput
  - تاخیر: تفاوت زمانی در انتقال اطلاعات یا زمان انجام کار. Delay مدت زمانی است که سیگنال به مقصد می‌رسد اما Jitter تنوع در این Delay Time است. صوت و ویدئو به jitter حساسند. Latency همان Delay به اضافه زمانی است که Acknowledgement به مبدا برگردد.
  - RMA: بهینه‌سازی شبکه از طریق قابلیت‌های اطمینان، نگهداری و در دسترس بودن
  - f(R,M)=A → f(**R**eliability, **M**aintainability) = **A**vailability
  - دامنه عملکرد: نمونه‌ای از دامنه عملکرد سه بعدی



بازده عملکرد سه بعدی

مقدمه مفاهیم معماری و طراحی شبکه

- مشخصه‌های کمی‌زیر در کیفیت خدمات شبکه نقش دارند.
  - **تاخیر delay:** میانگین زمان تولید بسته در مبدا و تحویل آن به مقصد
    - تاخیر انتشار خط delay propagation: سرعت انتشار در رسانه
    - تاخیر صف‌بندی delay queuing: معطلی بسته‌ها درون بافرها
    - تاخیرگام‌های مسیر hops
    - تعداد سوئیچ یا مسیریاب در مسیر
    - switching delay تأخیرسوئیچینگ
    - زمان مسیریابی در مسیریاب
  - **پهنای باند bandwidth:** نرخ ظرفیت ارتباط برحسب بیت بر ثانیه
  - **jitter:** نرخ اختلاف در زمان رسیدن بسته‌ها به مقصد یا تاخیر بسته‌های مختلف نسبت به مقدار میانگین تاخیر

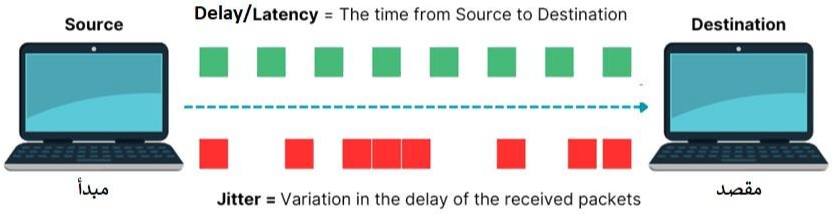


  - **نرخ از دست رفتن بسته‌ها packet lost:** میانگین از بین رفتن بسته‌های یک جریان

MTBF: میانگین زمان بین خرابی‌ها، MTTR: میانگین زمان تا تعمیر، MTTF: زمان کارکرد درست

مقدمه مفاهیم معماری و طراحی شبکه

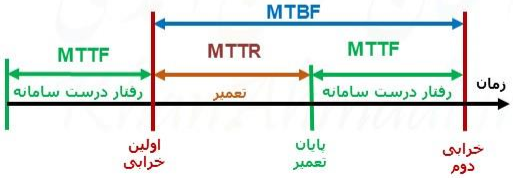
تفاوت delay با Jitter



مقدمه مفاهیم معماری و طراحی شبکه

معماری و طراحی شبکه

- دانش چارچوب‌های ارائه خدمات ITSM شامل ITIL، Cobit و برای امنیت ISMS
- رعایت الزامات استانداردهای ارائه خدمات مانند ISO 20000 و امنیت ISO 27000
- خدمات شبکه شامل کارایی و عملکرد است و به کاربران، برنامه‌ها و دستگاه‌ها ارائه می‌شود تا بتوانند کار خود را روی سامانه انجام دهند.
- با توجه به سامانه‌ها، خدمات و ویژگی‌های آنها، کمیت‌سازی خواسته‌ها از شبکه‌ها عملی می‌شود. به شرطی که الزامات سامانه جمع آوری، تحلیل و درک شود.
- Availability = (MTBF)/(MTBF + MTTR) زمان در دسترس و آماده‌ی استفاده بودن



مقدمه مفاهیم معماری و طراحی شبکه

سوکت Socket = IP Address + Port Number

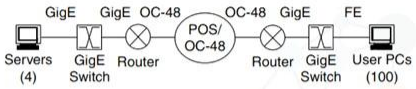
- سوکت‌ها نقاط پایانی برای ارسال و دریافت داده در شبکه هستند. آنها در سطح پایین عمل می‌کنند، معمولا با استفاده از پروتکل TCP یا UDP
- **مدل ارتباطی:** سوکت‌ها راهی برای برقراری ارتباط بین دو دستگاه (کلاینت و سرور) فراهم می‌کنند و به آنها اجازه می‌دهند تا مستقیم با ارسال جریان بایت‌ها ارتباط برقرار کنند. سوکت یک نشانی IP و یک شماره Port را ترکیب می‌کند.
- **انعطاف پذیری:** سوکت انعطاف پذیری بیشتری در قالب داده و پروتکل‌های ارتباطی دارند و اجازه می‌دهند پروتکل‌های سفارشی پیاده‌سازی شود.
- **موارد استفاده:** معمولا در برنامه‌هایی که نیاز به ارتباط بلادرنگ دارند، مانند برنامه‌های چت، بازی‌های برخط یا خدمات Stream استفاده می‌شود.
- هر ارتباط دو سوکت (فرستنده و گیرنده) نیاز دارد.
- مثالی از یک نشانی سوکت: 192.168.110.27:71
- دستور netstat در cmd و wf.msc برای مشاهده و مدیریت پورت‌های در حال استفاده

مقدمه مفاهیم معماری و طراحی شبکه

درخواست رویه از راه دور Remote Procedure Calls (RPC)

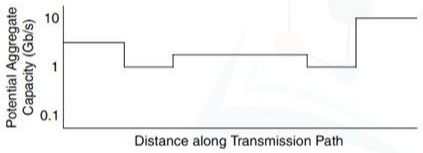
- RPC در سطح بالاتر عمل می‌کند که به یک برنامه اجازه می‌دهد تا یک رویه را روی یک سرور از راه دور اجرا کند، گویی که یک فراخوانی محلی است.
- **مدل ارتباطی:** RPC بسته‌بندی درخواست‌ها و پاسخ‌ها، از جمله پشت‌سرهم‌سازی داده‌ها را کنترل می‌کند و پیاده‌سازی سامانه‌های توزیع شده را برای توسعه دهندگان بدون نگرانی در مورد جزئیات اساسی شبکه آسان‌تر می‌کند.
- **سادگی:** فرآیند ارتباط از راه دور را با اجازه دادن به توسعه دهندگان برای فراخوانی توابع بر روی یک سرور از راه دور به طور مستقیم، با استفاده از همان شیوه فراخوانی‌های تابع محلی، ساده است.
- **موارد استفاده:** در معماری‌های میکروسرویس‌ها برای برقراری ارتباط روی شبکه و در سامانه‌هایی که اجرای از راه دور توابع مورد نیاز است.
- اشتراک گذاری فایل از راه دور RFS از RPC در توزیع پایگاه‌های داده استفاده می‌کند. سیستم فایل شبکه NFS و WCF هم از پروتکل RPC استفاده می‌کند.

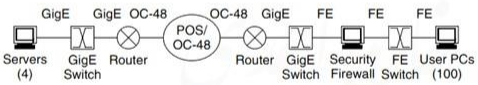
مقدمه مفاهیم معماری و طراحی شبکه

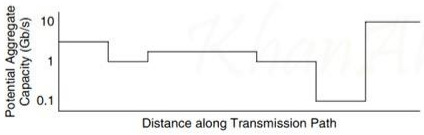


معماری و طراحی شبکه

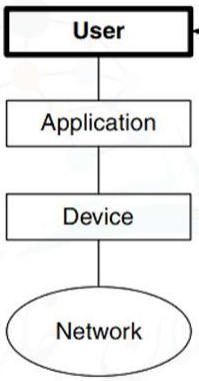
- فاصله در مسیر انتقال
  - ظرفیت هر نقطه در مسیر انتقال
    ۱. قبل از اضافه شدن دیوار آتش
    ۲. پس از اضافه شدن دیوار آتش







مفاهیم معماری و طراحی شبکه



انواع نیازهای کاربر

- به موقع بودن
- تعامل
- قابلیت اطمینان
- کیفیت ارائه
- سازگاری
- امنیت
- مقرون به صرفه بودن
- عملکرد
- قابلیت پشتیبانی
- رشد آینده

انواع نیازهای برنامه‌ها

- انواع کاربرد
- گروه‌های کاربردی
- مکان‌های برنامه

انواع الزامات دستگاه

- انواع دستگاه
- ویژگی‌های کارایی
- مکان‌های دستگاه

انواع الزامات شبکه

- محدودیت‌های شبکه‌های موجود
- مقیاس مورد انتظار شبکه‌های موجود
- قابلیت همکاری بین شبکه‌ها
- شبکه موجود و خدمات پشتیبانی
- دستورالعمل‌های معماری و طراحی موجود

فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

- آغاز با ورودی از کاربران، حکمرانی و مدیریت
- سپس تحلیل و اصلاح با استفاده از تجربه و دانش
- جمع‌آوری و فهرست کردن نیازمندی‌ها
  - برقراری ارتباط با کاربران برای جمع‌آوری نیازهای آنها
  - بحث در مورد شرایط اولیه شبکه
- توسعه معیارهای خدمات
- توصیف و مشخص کردن رفتار
- توسعه نیازمندی‌ها / نگاشت نیازمندی‌ها

تعیین شرایط اولیه

- **نوع پروژه شبکه:** شبکه جدید، اصلاح شبکه موجود، تحلیل مشکلات، برون‌سپاری، یکپارچه‌سازی، ارتقاء
- **محدوده پروژه شبکه:** اندازه شبکه، تعداد سایت‌ها، فاصله بین سایت‌ها
- **اهداف اولیه معماری/طراحی:** ارتقاء فناوری/فروشنده، بهبود عملکرد بخشی یا کل شبکه، پشتیبانی از کاربران و برنامه‌ها یا دستگاه‌های جدید، حل مشکلات مشخص، افزایش امنیت، پشتیبانی از قابلیت جدید

فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

مراحل الزامات جمع‌آوری و فهرست‌بندی

۱) تعیین شرایط اولیه (انواع پروژه‌های شبکه، ابعاد، اهداف معماری و طراحی)
۲) تنظیم انتظارات مشتری
   - ارزیابی سریع و اولیه از مشکل/نیاز
   - برآورد منابع و برنامه
۳) کار با کاربران
   - ایجاد نظرسنجی، پیگیری با تلفن، پیگیری تماس‌ها با ملاقات حضوری با افراد منتخب، جلسه‌های تخته‌سفید برای استخراج ایده هنگام مواجهه با چالش، همراه شدن با کاربران در حین کار برای درک بهتر کاری که انجام می‌دهند و چگونه انجام کارها
۴) اندازه‌گیری عملکرد (ایجاد بستر آزمون)
۵) ردیابی و مدیریت نیازمندی‌ها
۶) نقشه‌برداری اطلاعات موقعیت مکانی

فرایند معماری و طراحی شبکه

ردیابی و مدیریت نیازمندی‌ها به صورت جدولی

ID/Name	Date	Type	Description
NR - 1.0-102	01Jan2007	Original	All network equipment shall be capable of software-based upgrades to allow it to support changes to high-speed data service features and functions.
	07Mar2007	Change	"All network equipment" changed to "Technology A"
	01Apr2007	Change	"software-based upgrades" changed to "software or firmware-based upgrades"
	17Apr2007	Deletion	Change of 01Apr2000 deleted
	20May2007	Change	"high-speed" changed to "any"

فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

توسعه معیارهای خدمات

- معیارهای خدمات برای RMA:
  - **قابلیت اطمینان**، بر حسب میانگین زمان بین خرابی MTBF و میانگین زمان بین شکست‌های حیاتی مأموریت MTBCF
  - **قابلیت نگهداری**، از نظر میانگین زمان تعمیر MTTR
  - **در دسترس بودن**، از نظر MTBF، MTBCF، MTTR
  - گزینشی: زمان uptime و downtime درصدی از کل زمان، نرخ خطا و تلفات در سطوح مختلف، مانند نرخ خطای بسته، نرخ خطای بیت BER، نسبت از دست دادن سلول CLR، نسبت درج اشتباه سلول CMR، نرخ از دست دادن فریم و بسته
- معیارهای خدمات برای ظرفیت:
  - **نرخ داده**، بر حسب نرخ اوج PDR، نرخ داده پایدار SDR و کمینه نرخ داده MDR
  - **اندازه داده‌ها**، از جمله اندازه‌های انفجاری و مدت زمان
- معیارهای خدمات برای تأخیر:
  - تأخیر End-to-end یا رفت و برگشت (round-trip)، تاخیر Latency و تنوع تأخیر

سازوکارهای فعلی برای پیکربندی و اندازه‌گیری معیارهای خدمات در بن‌سازه‌های مدیریت شبکه وجود دارد که از پروتکل مدیریت شبکه ساده SNMP و پروتکل اطلاعات مدیریت مشترک CMIP استفاده می‌کنند، که به MIBها به عنوان متغیرهای توصیف کننده مدیریت عمومی و خاص شرکت دسترسی دارند.

شبکه محلی و اجزای آن

شبکه محلی یا LAN (Local Area Network) نوعی از شبکه‌های رایانه‌ای است که دستگاه‌ها را در یک ناحیه جغرافیایی محدود، مانند یک ساختمان، دفتر یا دانشگاه به یکدیگر متصل می‌کند. این شبکه‌ها به کاربران این امکان را می‌دهند که به سرعت و به راحتی اطلاعات و منابع را به اشتراک بگذارند.

اجزای شبکه محلی

تعدادی از اجزای اصلی یک شبکه محلی:

- **سرور:** دستگاه ارائه دهنده خدمات مانند ذخیره‌سازی داده‌ها و ارائه صفحات وب
- **ایستگاه کاری**: رایانه و دستگاهی که با اتصال به شبکه از خدمات سرور استفاده می‌کند.
- **کارت شبکه**: سخت‌افزاری که امکان اتصال دستگاه‌ها به شبکه را فراهم می‌کند.
- **سوئیچ**: دستگاهی که ترافیک داده‌ها را بین دستگاه‌های متصل در شبکه مدیریت می‌کند.
- **دیوار آتش:** ابزاری برای تأمین امنیت شبکه که ترافیک ورودی و خروجی را مهار می‌کند.
- **نرم‌افزارهای مدیریتی و امنیتی:** برای نظارت و مدیریت عملکرد شبکه استفاده می‌شوند.

ویژگی‌های شبکه محلی

شبکه‌های محلی معمولاً دارای سرعت بالای انتقال داده هستند و این امکان را فراهم می‌آورند که کاربران بتوانند به راحتی فایل‌ها، چاپگرها و دیگر منابع را به اشتراک بگذارند. همچنین، این نوع شبکه‌ها معمولاً در محیط‌های محدود مانند دانشگاه‌ها، دفاتر اداری و مدارس مورد استفاده قرار می‌گیرند نه در سطح ملی یا بین‌المللی.

سرویس در شبکه محلی

خدمت (سرویس Service)

- تعریف عمومی: ایجاد ارزش برای مشتری است.
  - اجاره اتاق در هتل، سپردن پول نزد بانک، مسافرت با هواپیما، معاینه پزشک
  - مشاوره و آموزش

- انواع خدمت از دید چارچوب فرآیند کسب و کار:
  - مشتری می‌بیند و مستقیم خدمت را دریافت می‌کند
  - پشتیبانی کننده است و در پشت صحنه حضور دارد

- **خدمت در مدیریت خدمات فناوری اطلاعات**

خدمت راهی برای خلق ارزش برای مشتری و ارائه به اوست، با تأمین خواسته او (خروجی دارد)، بدون داشتن مخاطرات یا هزینه‌های خاص

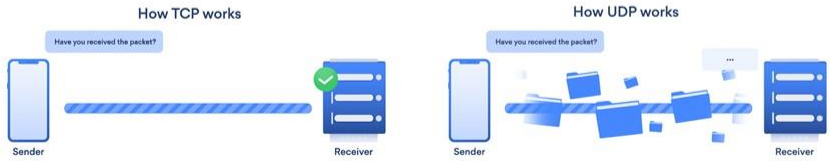
مانند:

سرویس پشتیبانی کاربران، سرویس Hosting، سرویس ارائه دسترسی به منابع شبکه، سرویس ارائه تنظیمات TCP/IP توسط DHCP، سرویس شبکه محلی بی‌سیم Wi-Fi

شبکه محلی: TCP در مقابل UDP و موارد دیگر

TCP در مقابل UDP

- **اطمینان**
  - به عنوان مثال، اگر برنامه‌ای که داده‌ها را در شبکه انتقال می‌دهد، از پروتکل TCP استفاده کند، خدمت با قابلیت اطمینان انتقال براساس لزوم دریافت ACK به ازای هر بسته ارسالی تضمین می‌شود. اما اگر از UDP استفاده شود، هیچ تضمین برای رسیدن همه بسته‌ها وجود ندارد و پایایی از لایه انتقال به لایه‌های Data-link و فیزیکی منتقل می‌شود یا باید توسط خود برنامه ارائه شود.



فرمت‌های بسته در شبکه محلی

فرمت‌های بسته

در شبکه‌های محلی، بسته‌ها به فرمت‌های مختلفی تقسیم‌بندی می‌شوند که هر یک از آن‌ها برای اهداف خاصی طراحی شده‌اند. این فرمت‌ها معمولاً شامل اطلاعاتی درباره آدرس‌دهی، کنترل خطا و نوع داده هستند. فرمت‌های بسته در شبکه‌های محلی به نوع پروتکل و هم‌بندی شبکه بستگی دارند. هر یک از این فرمت‌ها ویژگی‌ها و ساختار خاص خود را دارند که به انتقال مؤثر داده‌ها کمک می‌کند. انتخاب فرمت مناسب بسته مبتنی بر نیازهای خاص شبکه و نوع داده‌های منتقل‌شونده انجام می‌شود.

تعدادی از فرمت‌های بسته در شبکه‌های محلی عبارتند از:

Ethernet Frame، Token Ring Frame، Token Bus Frame، IPX/SPX، FDDI، ATM

فرمت‌های بسته در شبکه محلی

فرمت‌های بسته

۱. بسته اترنت (Ethernet Frame)

- ساختار: سرآیند، داده و دنباله
  - سرآیند: نشانی MAC مبدا و مقصد، نوع پروتکل و اطلاعات کنترل جریان
  - داده: حاوی اطلاعات و محتوای واقعی که قرار است منتقل شود
  - دنباله: اطلاعات کنترل خطا مانند CRC برای تشخیص خطا در انتقال داده

۲. بسته توکن رینگ (Token Ring Frame)

- ساختار: مشابه بسته اترنت اما با تفاوت‌هایی در شیوه آدرس‌دهی و کنترل دسترسی
  - سرآیند: شامل نشانی MAC و اطلاعات کنترلی برای مدیریت توکن
  - داده: اطلاعات منتقل شده بین دستگاه‌ها
  - دنباله: شامل اطلاعات کنترل خطا

۳. بسته توکن باس (Token Bus Frame)

- ساختار: طراحی شده برای توپولوژی باس.
  - سرآیند: شامل نشانی MAC و اطلاعات توکن
  - داده: حاوی اطلاعات اصلی
  - دنباله: شامل اطلاعات کنترل خطا

فرمت‌های بسته در شبکه محلی

فرمت‌های بسته

۴. بسته IPX/SPX

- این پروتکل معمولاً در شبکه‌های Novell استفاده می‌شد
  - سرآیند IPX: شامل نشانی‌های مبدأ و مقصد و نوع پروتکل
  - داده: حاوی اطلاعات واقعی منتقل شده

۵. بسته FDDI (Fiber Distributed Data Interface)

- طراحی شده برای شبکه‌های فیبر نوری
  - شامل سرآیند، داده و دنباله با قابلیت انتقال داده با سرعت بالا

۶. بسته ATM (Asynchronous Transfer Mode)

- این نوع بسته‌ها کوچک و اندازه ثابت هستند (۵۳ بایت)
  - شامل سرآیند برای مدیریت ترافیک و فریم برای داده‌ها

برنامه‌های کاربردی سرویس‌گیرنده – سرور در شبکه محلی

برنامه‌های کاربردی سرویس‌گیرنده – سرور

برنامه‌های کاربردی Client-Server از معماری سرویس گیرنده/سرویس دهنده برای تبادل اطلاعات و ارائه خدمات استفاده می‌کنند. این برنامه‌ها به طور معمول شامل یک کلاینت (مشتری) و یک سرور (ارائه دهنده خدمت) هستند که با یکدیگر ارتباط برقرار می‌کنند.

FTP (File Transfer Protocol)

پروتکلی برای انتقال فایل‌ها در شبکه با امکان بارگذاری و بارگیری فایل‌ها با سرعت بالا اما امنیت پایین که بهتر است از SFTP که امنیت را هم تضمین می‌کند استفاده شود.

Telnet

پروتکلی برای دسترسی به سیستم‌ها از راه دور. به عنوان نمونه می‌توان به سوئیچ‌ها و سرورهای دیگر متصل شده و آن‌ها را کنترل کرد اما فاقد رمزنگاری است که بهتر است از SSH (Secure Shell) استفاده شود.

HTTP (Hypertext Transfer Protocol)

پروتکلی برای انتقال صفحات وب. مرورگر (کلاینت) درخواست‌هایی را به سرور وب ارسال کرده و سرور پاسخ‌هایی شامل صفحات وب را ارسال می‌کند اما امن نیست که بهتر است از https که از TLS/SSL برای رمزگذاری داده‌ها در حین انتقال استفاده می‌کند، استفاده شود.

برنامه‌های کاربردی سرویس‌گیرنده – سرور در شبکه محلی

برنامه‌های کاربردی سرویس‌گیرنده – سرور

SMTP (Simple Mail Transfer Protocol)

پروتکلی برای ارسال رایانامه‌ها. کلاینت رایانامه درخواست ارسال را به سرور SMTP می‌فرستد و سرور مسئولیت انتقال رایانامه به مقصد نهایی را بر عهده دارد که امن نیست. بهتر است از SMTPS (SMTP Secure) یا STARTTLS که روش‌هایی برای رمزگذاری رایانامه‌ها در حین انتقال هستند استفاده شود. این پروتکل‌ها مانع از دسترسی غیرمجاز به محتوای رایانامه‌ها می‌شوند.

DNS (Domain Name System)

سیستمی که نام‌های دامنه را به نشانی‌های IP تبدیل می‌کند. کلاینت DNS درخواست نام دامنه را به سرور DNS می‌فرستد و سرور پاسخ متناظر را برمی‌گرداند که امن نیست. DNSSEC یک مجموعه از افزونه‌ها است که امنیت DNS را با تأیید اعتبار پاسخ‌های DNS افزایش می‌دهد و مانع از حملاتی مانند DNS Spoofing می‌شود.

پروتکل‌های چاپ شبکه‌ای

مانند IPP (Internet Printing Protocol)، که امکان ارسال درخواست‌های چاپ از کاربران به سرور چاپ را فراهم می‌کند. بهتر است IPP را با TLS امن کرد.

برنامه‌های کاربردی سرویس‌گیرنده – سرور در شبکه محلی

برنامه‌های کاربردی سرویس‌گیرنده – سرور

پروتکل‌های پایگاه داده

مانند ODBC (Open Database Connectivity) که اجازه می‌دهد کلاینت‌ها به پایگاه داده‌ها متصل شده و عملیات خواندن یا نوشتن داده‌ها را انجام دهند.

پروتکل DHCP

تخصیص خودکار تنظیمات TCP/IP مانند IP Address، Subnet Mask و نشانی‌های DNS، default gateway و DHCP را انجام می‌دهد و منحصر به فرد بودن Ipهای تخصیص داده شده به هر Client را تضمین می‌کند. این فرآیند شامل ارسال درخواست از کلاینت به سرور و دریافت پاسخ از سرور است. با استفاده از DHCP، مدیران شبکه به راحتی نشانی‌های IP را مدیریت کرده و از بروز مشکلاتی مانند تداخل نشانی‌ها جلوگیری می‌کنند.

در حالی که DHCP مزایای زیادی دارد، اما به طور ذاتی امنیت ندارد و ممکن است در معرض حملات مختلف DHCP Spoofing قرار گیرد. برای افزایش امنیت، می‌توان از روش‌هایی برای مقابله با DHCP Spoofing که مهاجم به عنوان سرور جعلی مانند MITM پاسخ‌های جعلی به کلاینت‌ها ارسال می‌کند و حمله DHCP Starvation که مهاجم به عنوان کلاینت تعداد زیادی DHCP Request جعلی ایجاد می‌کند و باعث می‌شود که کل محدود IP تعیین شده برای DHCP سرور پر شود یا تعداد این DHCP Request انقدر زیاد می‌شود که سرور توان پاسخگویی به ان را نداشته باشد

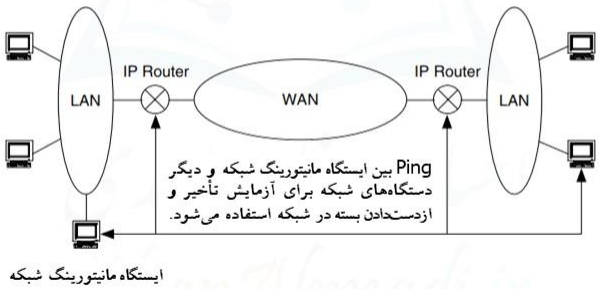
فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

توسعه معیارهای خدمات

- ابزارهای اندازه‌گیری

استفاده از Ping و IP Packet Loss به عنوان معیارهای سرویس برای RMA



فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

توسعه معیارهای خدمات

- مثال معیار اندازه‌گیری خدمت

Service Metric		Where Metric Will be Measured in System	Measurement Method
1	LAN Delay	Between NM Device and Each Router in LAN	Ping
2	Wan Delay 1	Between NM Device and Local Router Interface to WAN	Ping
3	WAN Delay 2	Between NM Device and Remote Router Interface to WAN	Ping
4	LAN Packet Loss	At Each Local Router	SNMP

- جاهایی که از معیارهای خدمات استفاده کنیم
  - رسیدن به اهداف مانند تفکیک مسئولیت‌ها
  - جداسازی و ردیابی مشکلات در شبکه (به خصوص شبکه‌های دارای گروه‌های متعددی مسئول)

فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

توصیف رفتار

توصیف برای انواع رفتار: User behavior، Application behavior و Network behavior

- مدل‌سازی و شبیه‌سازی
  - توسعه مدل‌ها یا شبیه‌سازی رفتار کاربر، برنامه‌ها و شبکه اغلب در پیش‌بینی، تعیین، یا برآورد الزامات و جریان داده‌ها مفید است.

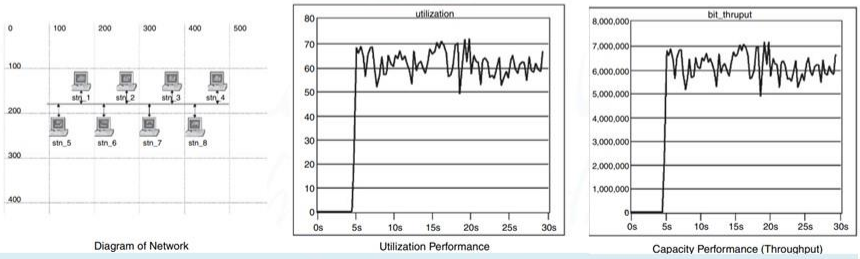


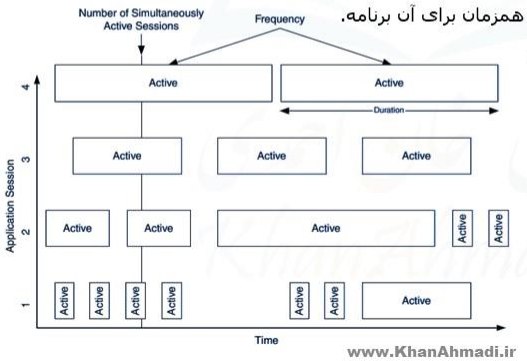
Diagram of Network | Utilization Performance | Capacity Performance (Throughput)

شبیه‌سازی رفتار عملکرد شبکه

فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

- رفتار کاربر و برنامه در شبکه:
  - درک چگونگی استفاده کاربران سامانه از برنامه‌ها مفید برای شناسایی معیارهای خدمات شبکه
  - الگوهای ساده رفتار کاربر شامل زمان‌ها و طول مدت زمان‌های کاری کاربر است. برای هر برنامه، تعداد کل کاربران، تعداد دفعاتی که کاربر برنامه را در حال اجرا دارد، مدت زمان متوسط استفاده از برنامه، تخمین تعداد مورد انتظار جلسات همزمان برای آن برنامه.
  - ویژگی رفتار کاربران از یک برنامه:



فرایند معماری و طراحی شبکه

فرآیند تحلیل نیازمندی‌ها

- توسعه الزامات RMA
  - **قابلیت اطمینان:** یک شاخص آماری از فراوانی خرابی شبکه و اجزای آن است و نشان دهنده قطعی‌های برنامه‌ریزی نشده خدمت است. معیارهای قابلیت اطمینان: MTBCF و MTBF است.
    - MTBCF بر عملکرد سامانه در طول ماجراهای مأموریت خاص تمرکز می‌کند.
  - **قابلیت نگهداری:** پایداری یک معیار آماری از زمان برای بازگرداندن سامانه به وضعیت عملیاتی است، پس از آنکه یک خطا را تجربه کرده است و به آن «میانگین زمان تعمیر» یعنی MTTR می‌گویند.
  - **در دسترس بودن:** در دسترس بودن رابطه بین فراوانی خرابی امور حیاتی و زمان بازیابی خدمت است. بسته به شرایط، دو فرمول برای محاسبه آن می‌توان در نظر گرفت.
    - A = MTBCF/MTBCF+MTTR
    - A = MTBF/MTBF+MTTR
    - Uptime و Downtime: یک معیار رایج در دسترس بودن است. به عنوان مثال، در RFP از یک مشتری بالقوه ممکن است زمان مورد نیاز در دسترس بودن ۹۹٫۹۹۹٪ (معمولا به عنوان five nines یعنی "پنج نه" شناخته می‌شود) باشد.

فرایند معماری و طراحی شبکه

Uptime and Downtime

- زمان آماده به کار بودن در دوره‌های زمانی مختلف اندازه‌گیری می‌شود
- ممکن است موارد دیگری نیز نیاز به اندازه‌گیری داشته باشد مانند «کیفیت خدمات»

% Uptime	Amount of Allowed Downtime in Hours (h), Minutes (m), or Seconds (s) per Time Period			
	Yearly	Monthly	Weekly	Daily
99%	87.6 h	7.3 h	1.68 h	14.4 m
99.9%	8.76 h	44 m	10 m	1.4 m
99.99%	53 m	4.4 m	1 m	8.6 s
99.999%	5.3 m	26.3 s	6 s	0.86 s

مقدمه مفاهیم معماری و طراحی شبکه

توسعه معیارهای خدمات

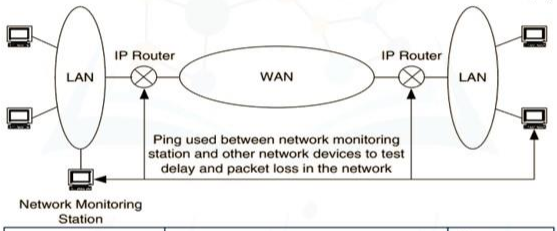
مثال‌هایی از معیارهای خدمات service metrics:

- Bytes in/out (per interface)
- IP packets in/out (per interface)
- Dropped Internet Control Message Protocol (ICMP) messages/unit time (per interface)
- Service-level agreement (SLA) metrics (per user) توافق سطح خدمات
  - Capacity limit محدودیت ظرفیت
  - Burst tolerance تحمل فشار
  - Delay تأخیر
  - Downtime زمان از کار افتادن

مقدمه مفاهیم معماری و طراحی شبکه

توسعه معیارهای خدمات

مثال‌هایی از معیارهای خدمات service metrics:



	Service Metric	Where Metric Will be Measured in System	Measurement Method
1	LAN Delay	Between NM Device and Each Router in LAN	Ping
2	Wan Delay 1	Between NM Device and Local Router Interface to WAN	Ping
3	WAN Delay 2	Between NM Device and Remote Router Interface to WAN	Ping
4	LAN Packet Loss	At Each Local Router	SNMP

فرایند معماری و طراحی شبکه

توسعه الزامات عملکرد تکمیلی Developing Supplemental Performance Requirements

Operations and Support	
Operations	**Support**
Management	Management
Personnel	Maintenance Support
Tools	Technical Documentation
Consumables	Storage
Transportation	Supply Support
Leasing	Modifications
Facilities	

عملیات: میزان عملیاتی شدن

- مدیریت
- کارکنان
- ابزار
- مواد مصرفی
- حمل و نقل
- واسپاری
- امکانات

پشتیبانی: حفظ کارایی مانند روز تحویل

- مدیریت
- پشتیبانی تعمیر و نگهداری
- مستندات فنی
- ذخیره سازی
- پشتیبانی تامین
- اصلاحات

Confidence "**اطمینان**"، معیاری است از توانایی شبکه برای ارائه داده‌ها بدون خطا و حفظ توان عملیاتی مورد نیاز

فرایند معماری و طراحی شبکه

ساختار تعمیر و نگهداری سه لایه:

عامل محلی سریع مشکل را شناسایی کرده، واحد قابل تعویض را برای بازیابی خدمت جایگزین می‌کند. سپس واحد تعمیر محلی LRU به Tier 2 یا کارخانه برای بازسازی ارسال می‌شود.

- ابزار و تجهیزات آزمایش
- تعمیر و نگهداری اصلاحی
- نگهداری پیشگیرانه

Level	Location	Who	Tools and Test Equipment	Corrective Maintenance	Preventive Maintenance
Organi-zational	Operations Sites	Operators	• Common tools • Operator consoles and controls • Inexpensive special tools	• Day-to-day monitoring • Troubleshooting • Fault isolation • Replacing LRUs • Reconfiguring system	• Monitoring performance • Minor on-site cleaning and adjustments • Scheduled replacement of LRUs
Inter-mediate	On call to work onsite	Trained personnel whose primary role is maintenance	Special or expensive portable tools with limited use	On-site repair of offline equipment	• Major on-site upgrades where shipment to factory is impractical • Supplement operators
Depot	Vendor or factory	Vendor or factory personnel	Equipment to refurbish components	Overhaul and refurbishment	Scheduled overhaul or disassembly of LRUs

فرایند معماری و طراحی شبکه

محدودیت‌های خاص محیط

مشخص شدن ابزارها یا برنامه‌های high-performance

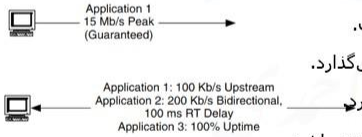
الزامات عملکرد قابل پیش‌بینی و تضمین شده:

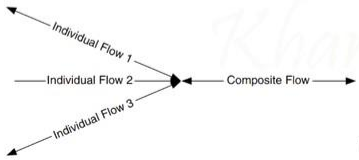
- 1. What the performance requirements are
- 2. When and where they apply
- 3. How they will be measured and verified
- 4. What happens when a requirement is not met

جریان تحلیل معماری و طراحی شبکه

تحلیل جریان: جریان داده

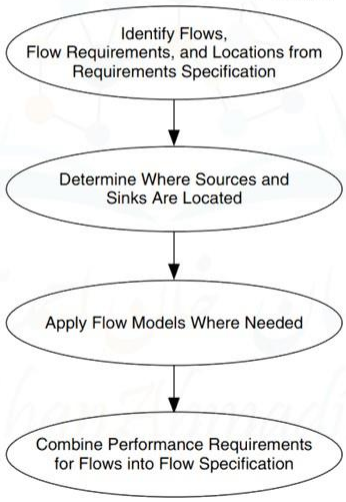
- جریان‌ها (جریان‌های ترافیکی یا جریان‌های داده‌ای) مجموعه‌ای از ترافیک شبکه (اطلاعات کاربردی، پروتکل و کنترل) هستند که ویژگی‌های مشترکی مانند نشانی مبدأ/مقصد، نوع اطلاعات، جهت‌گیری یا سایر اطلاعات end-to-end را دارند.
- شناسایی جریان‌های منفرد، ترکیبی و بحرانی مبتنی بر منابع اطلاعاتی و مدل‌های جریان و چاه‌ها
  - جریان منفرد، جریانی برای یک جلسه از یک برنامه است.
  - جریان ترکیبی مسیر یا شبکه مشترک را به اشتراک می‌گذارد.
  - جریان بحرانی عملکرد بالاتر یا الزامات سخت‌گیرانه‌ای دارد.
- چاه: data sink می‌تواند data storage یا archival device باشد.





جریان تحلیل معماری و طراحی شبکه

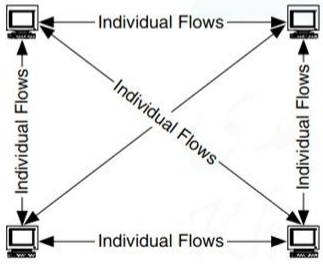
فرآیند شناسایی و توسعه جریان‌ها



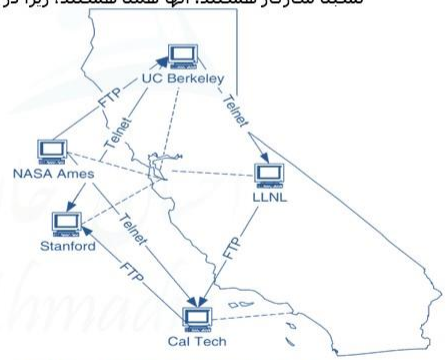
جریان تحلیل معماری و طراحی شبکه

مدل‌های جریان

- Peer-to-peer
  - یکی از مواردی است که در آن کاربران و برنامه‌های کاربردی در رفتارهای جریان خود در سراسر شبکه نسبتاً سازگار هستند. آنها همتا هستند، زیرا در یک سطح در سلسله مراتب عمل می‌کنند.



Peer-to-Peer Flow Model

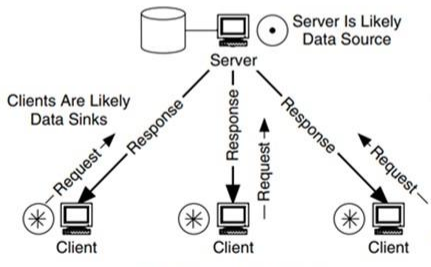


An Example of Peer-to-Peer Flows in the Early Internet

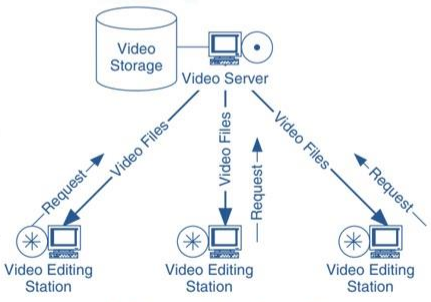
جریان تحلیل معماری و طراحی شبکه

مدل‌های جریان

- Client–server
  - عدم تمایز بین جریان‌ها در این مدل، یا همه جریان‌ها حیاتی‌اند یا هیچ کدام
  - توصیف آنها با یک مشخصات واحد به دلیل معادل بودن همه‌ی جریان‌ها



Client–Server Flow Model

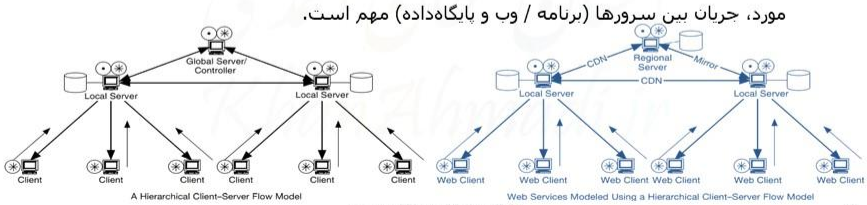


An Example of Client–Server Flows

جریان تحلیل معماری و طراحی شبکه

مدل‌های جریان

- کلاینت-سرور سلسله‌مراتبی Hierarchical client–server
  - کار کردن چندین برنامه با هم برای انجام کار، یا زمانی که برنامه‌های کاربردی سرویس گیرنده-سرور متعدد (یا چندین جلسه از یک برنامه) توسط یک برنامه کاربردی سطح بالاتر مدیریت می‌شوند.
  - جریان‌های حیاتی به رفتار برنامه وابسته است. معمولاً زمانی که سرورها با یکدیگر ارتباط برقرار می‌کنند (به‌روزرسانی DB)، جریان سرور به سرور علاوه بر جریان مشتری-سرور، حیاتی است. برای همگام‌سازی پردازش یا اطلاعات توسط مدیر، آن جریان نیز حیاتی است.
  - مثال: شبکه‌های تحویل محتوا یعنی Content Delivery Networks (CDN) و Mirrorها برای انتقال محتوای وب بین سرورها و ارائه دسترسی محلی به محتوا برای کاربران استفاده می‌شوند. در این مورد، جریان بین سرورها (برنامه / وب و پایگاه‌داده) مهم است.



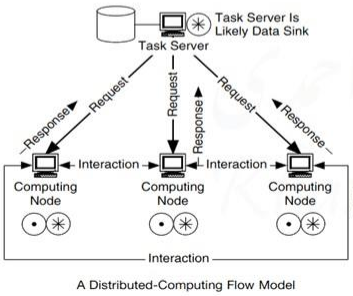
A Hierarchical Client–Server Flow Model

Web Services Modeled Using a Hierarchical Client–Server Flow Model

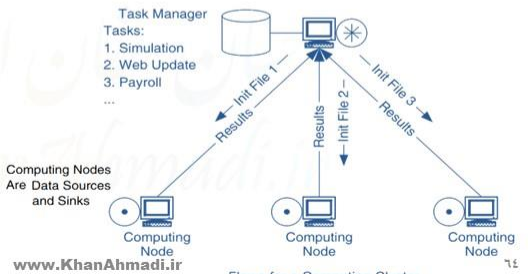
جریان تحلیل معماری و طراحی شبکه

مدل‌های جریان

- محاسبات توزیع شده Distributed computing
  - تخصصی ترین مدل جریان
  - معکوس یا ترکیبی از ویژگی‌های مدل‌های جریان همتا به همتا و مشتری-سرور
  - برقراری جریان‌ها عمدتاً بین مدیر وظیفه و دستگاه‌های محاسباتی آن (مانند مدل مشتری-سرور) یا بین دستگاه‌های محاسباتی (مانند یک مدل همتا به همتا)
  - اختصاص وظایف بر اساس در دسترس بودن منابع



A Distributed-Computing Flow Model



Flows for a Computing Cluster

جریان تحلیل معماری و طراحی شبکه

اولویت‌بندی جریان

- اهداف کسب و کار و تأثیر یک جریان بر تجارت
- اهداف سیاسی
- الزامات کارایی جریان (ظرفیت، تاخیر، RMA و کیفیت خدمات)
- الزامات امنیتی هر جریان
- تعداد کاربران، برنامه‌ها و/یا دستگاه‌هایی که یک جریان به آنها خدمت می‌کند و ...

هدف از اولویت‌بندی جریان‌ها مشخص شدن جریان‌هایی است که بیشترین/سریع‌ترین دسترسی به منابع را دریافت داشته باشند. نمونه‌هایی از اولویت‌بندی بر اساس قابلیت اطمینان و بر اساس تعداد کاربر

Flow ID	Performance Requirements			Number of Users	Budget	Priority
	Reliability	Capacity	Delay			
CF1	99.95%	500 Kb/s	100 ms	1750	$375 K	1
F2	99.5%	100 Kb/s	N/A	550	$141 K	2
F3	99.5%	15 Kb/s	100 ms	100	$141 K	2
F1	N/A	1.2 Mb/s	10 ms	1200	$31 K	3
CF2	N/A	100 Kb/s	100 ms	2100	$31 K	3
CF3	N/A	3 Mb/s	100 ms	50	$31 K	3

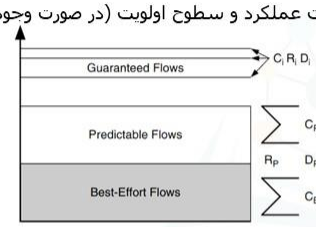
Total Budget for Network Project: $750 K

Flow ID	Performance Requirements			Number of Users	Budget	Priority
	Reliability	Capacity	Delay			
CF2	N/A	100 Kb/s	100 ms	2100	$274 K	1
CF1	99.95%	500 Kb/s	100 ms	1750	$228 K	2
F1	N/A	1.2 Mb/s	10 ms	1200	$157 K	3
F2	99.5%	100 Kb/s	N/A	550	$72 K	4
F3	99.5%	15 Kb/s	100 ms	100	$13 K	5
CF3	N/A	3 Mb/s	100 ms	50	$6 K	6

Total Budget for Network Project: $750 K

جریان تحلیل معماری و طراحی شبکه

مشخصات جریان: فهرست جریان‌های شبکه به همراه الزامات عملکرد و سطوح اولویت (در صورت وجود)



A Multi-Part Flow Specification

انواع مشخصات جریان:

- یک قسمتی یا واحد: الزامات بهترین تلاش
- دو قسمتی؛ علاوه بر موارد فوق دارای الزامات قابل پیش‌بینی
- چند قسمتی: علاوه بر موارد فوق دارای الزامات تضمین شده

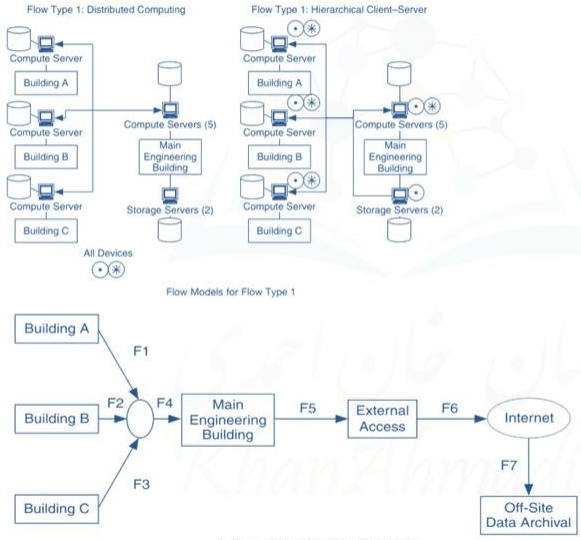
توصیف مشخصات جریان

Flow Specification Type	Types of Flows	Performance Description
One-Part	Best-Effort Individual and Composite	Capacity Only
Two-Part	Best-Effort and Stochastic, Individual and Composite	Reliability, Capacity, and Delay
Multi-part	Best-Effort, Stochastic, and Guaranteed, Individual and Composite	Reliability, Capacity, and Delay

Descriptions of Flow Specifications

جریان تحلیل معماری و طراحی شبکه

مشخصات جریان: مثال



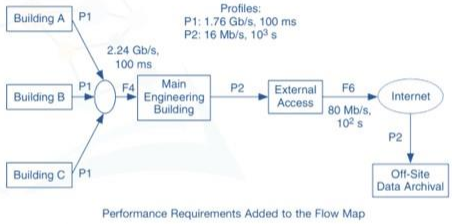
A Flow Map for the Example

جریان تحلیل معماری و طراحی شبکه

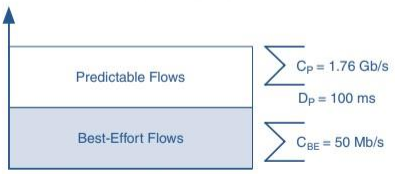
Flow ID	Performance Requirements	
	Capacity (Mb/s)	Delay (ms)
F1: Flow Type 1		
Synchronization Files	320	100
Update Files	1600	1000
Final Files	160	10^5
Result for Flow Type 1	1600	100
F1: Flow Type 2		
Update Files	80	10^4
Final Files	160	10^5
Result for Flow Type 2	160	10^4
Result for F1	**1760**	**100**
Result for F2	**1760**	**100**
Result for F3	**1760**	**100**
F4: Flow Type 1	1600	100
F4: Flow Type 2		
Update Files	320	10^4
Final Files	640	10^5
Result for Flow Type 2	640	10^4
Result for F4	**2240**	**100**
Result for F5	**16**	**10^3**
Result for F6	**80**	**10^2**
Result for F7	**16**	**10^3**

Performance Requirements for Flows

مشخصات جریان: ادامه مثال



Performance Requirements Added to the Flow Map



Two-Part Flowspec for Each Flow with Performance Profile P1

جریان تحلیل معماری و طراحی شبکه

معماری اینترنت و معماری اطلاعات

معماری شبکه

مقایسه بین معماری و طراحی

معماری شبکه‌های جدید:

تشکیل راه‌حل معماری شبکه از متغیرهای زیادی مانند «عملکرد، امنیت و مدیریت شبکه» و ارتباط بین آنها

طراحی		معماری
متمرکز	حوزه	وسیع
عمیق	سطح جزئیات	عمومی
فناورانه	توصیف	روابط
وابسته	مکان	مستقل

مقایسه بین معماری و طراحی

معماری شبکه

معماری ترکیبی

«معماری ترکیبی»، توصیفی از چگونگی و محل هر عملکرد از مجموعه‌ای از سازوکارها (سخت افزار و نرم افزار) شبکه در آن شبکه است. چهار قابلیت مهم در عملکرد شبکه:

- **نشانی‌دهی/مسیریابی، مدیریت شبکه، کارایی و امنیت**

سایر عملکردهای عمومی مانند: زیرساخت، ذخیره‌سازی و عملکردهای خاصی برای هر شبکه سازوکارها، سخت‌افزار و نرم‌افزاری هستند که به شبکه کمک می‌کنند تا به هر قابلیتی دست یابد.

سبک سنگین کردن، وابستگی‌ها و محدودیت‌ها برای بهینه‌سازی عملکرد شبکه انجام می‌شود.

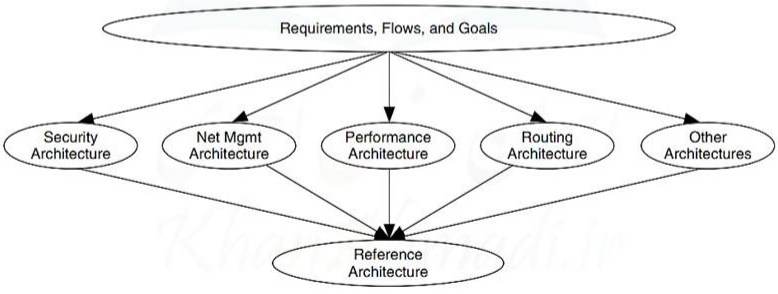
Function	Description of Capability	Example Subset of Mechanisms Used to Achieve Capability
Addressing/Routing	فراهم کردن اتصال قوی و انعطاف پذیر بین دستگاه‌ها	• Addressing: Ways to allocate and aggregate address space • Routing: Routers, routing protocols, ways to manipulate routing flows
Network Management	فراهم کردن نظارت، پیکربندی و عیب‌یابی شبکه	• Network management protocols • Network management devices • Ways to configure network management in the network
Performance	فراهم کردن منابع شبکه برای پشتیبانی از الزامات ظرفیت، تاخیر و RMA	• Quality of Service • Service-Level Agreements • Policies
Security	محدود کردن دسترسی، استفاده و دید غیرمجاز در شبکه برای کاهش تهدید و اثرات حملات.	• Firewalls • Security policies and procedures • Filters and access control lists

معماری شبکه

معماری ترکیبی

معماری ترکیبی، نیازمندی‌ها، جریان‌ها و اهداف همه از طریق معماری مرجع (Reference Architecture) در هم تنیده شده‌اند.

مناطقی که معمولاً مورد استفاده قرار می‌گیرند شامل دسترسی (لبه)، توزیع، هسته (backbone)، و رابطهای خارجی (External Interfaces) و DMZ هستند.



معماری شبکه

معماری ترکیبی Addressing/Routing

- از منظر Addressing: سازوکارها شامل زیرشبکه، زیرشبکه با طول متغیر، Supernetting، آدرس‌دهی پویا، آدرس‌دهی خصوصی، شبکه‌های محلی مجازی VLAN، IPv6 و ترجمه نشانی شبکه NAT

- از منظر مسیریابی (راه‌گزینی): سازوکارها شامل سوئیچینگ و مسیریابی، انتشار مسیر پیش‌فرض، مسیریابی بین دامنه‌ای بدون کلاس CIDR، چندپخشی multicasts، IP موبایل، تسفیه مسیر، همتاسازی، سیاست‌های مسیریابی، اتحادها، انتخاب و مکان‌یابی IGP و EGP

مثال: یک شبکه ارائه‌دهنده خدمات ممکن است بر سازوکارهایی مانند Supernetting، CIDR، چندپخشی، همتاسازی، خط‌مشی‌های مسیریابی و اتحادها تمرکز کند.

در حالی که شبکه سازمانی متوسط بر روی آدرس‌دهی classful یا خصوصی و NAT، VLAN، سوئیچینگ تمرکز می‌کند.

معماری شبکه

معماری ترکیبی مدیریت شبکه

سازوکارهای مدیریت شبکه شامل نظارت و جمع آوری داده‌ها شامل:

- مانیتورینگ: به دست آوردن مقادیر ویژگی‌های مدیریت شبکه، هر پیوند، مسیر و هر عنصر
- ابزار دقیق: ابزارهای نظارت و بررسی شبکه با داده‌های مدیریتی
- پیکربندی: تنظیم پارامترها در دستگاه شبکه برای عملکرد و کنترل آن عنصر
- اجزای FCAPS: مجموعه‌ای از اجزای خطا، پیکربندی، حسابداری، کارایی و مدیریت امنیت
- مدیریت ورودی و خروجی: جداسازی مسیر داده‌های مدیریتی از مسیر داده‌های کاربر
- مدیریت متمرکز و توزیع‌شده: بن‌سازه‌های سخت‌افزاری از چندین ویژند
- مقیاس بندی ترافیک مدیریت شبکه: ذخیره میزان ظرفیت مدیریت شبکه
- بررسی و تعادل: سازوکارهای متعدد برای نمایش درست داده
- مدیریت داده‌های مدیریت شبکه: بارگیری و در دسترس بودن ذخیره‌ساز، به‌روزرسانی داده‌ها
- انتخاب MIB: پایگاه اطلاعات مدیریت مختلف
- ادغام در OSS: نحوه ارتباط سامانه مدیریت با سامانه پشتیبانی عملیات سطح بالاتر

معماری شبکه

معماری ترکیبی کارایی

کارایی شامل مجموعه سازوکارهایی است که برای پیکربندی، بهره‌برداری، مدیریت، تهیه و حسابرسی منابع در شبکه استفاده می‌شود تا مشخص شود چه میزان کارایی به کاربران، برنامه‌ها و دستگاه‌ها اختصاص یابد که شامل برنامه‌ریزی ظرفیت و مهندسی ترافیک و همچنین انواع سازوکارهای خدماتی است. این کار با اولویت‌بندی، زمان‌بندی و شرطی‌سازی جریان‌های ترافیک شبکه انجام می‌شود.

معماری شبکه

معماری ترکیبی امنیتی مبتنی بر اصول Confidentiality, Integrity, Availability

امنیت یک الزام برای تضمین محرمانه بودن، یکپارچگی و در دسترس بودن اطلاعات و منابع فیزیکی کاربر، برنامه، دستگاه و شبکه که اغلب با حریم خصوصی همراه است. سازوکارهای امنیتی:

- تجزیه و تحلیل تهدید امنیتی: لزوم محافظت کدام اجزاء و انواع خطرات امنیتی (تهدید)
- سیاست‌ها و رویه‌های امنیتی: بیانیه‌های رسمی قوانین دسترسی و استفاده از منابع
- امنیت فیزیکی و آگاهی: محافظت فیزیکی دستگاه‌ها، دسترسی، آسیب آموزش کاربران
- امنیت پروتکل و برنامه: ایمن‌سازی مدیریت و پروتکل‌های شبکه و برنامه‌ها
- رمزگذاری: غیرقابل خواندن کردن داده‌ها با اعمال الگوریتم‌های رمزی با کلید مخفی
- امنیت محیطی شبکه: محافظت از رابطهای خارجی بین شبکه‌های
- امنیت دسترسی از راه دور: ایمن کردن دسترسی به شبکه بر اساس dial-in، جلسات نقطه به نقطه و اتصالات شبکه خصوصی مجازی

معماری شبکه

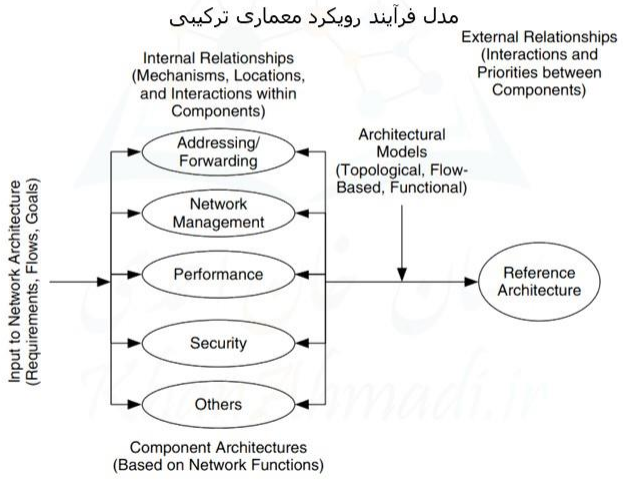
بهینه‌سازی معماری ترکیبی

تعیین و درک مجموعه‌ای از روابط داخلی، معماری هر جزء را قادر می‌سازد تا برای یک شبکه خاص بهینه شود. بهینه‌سازی مبتنی بر ورودی برای آن شبکه خاص، الزامات، جریان ترافیک تخمینی و اهداف آن شبکه انجام می‌شود.

معماری شبکه

معماری مرجع

مدل فرآیند رویکرد معماری ترکیبی



مقیاس‌پذیری شبکه محلی

مقیاس‌پذیری

در طراحی شبکه‌های محلی باید توانایی آنها را برای گسترش و تطبیق با نیازهای حال و تغییر سازمان‌ها و کاربران در آینده در نظر گرفت.

ابعاد مقیاس‌پذیری در شبکه‌های محلی

۱. مقیاس‌پذیری بار کاری

این نوع مقیاس‌پذیری به توانایی شبکه برای افزایش یا کاهش منابع خود بر اساس بار کاری اشاره دارد. به عنوان مثال، با افزایش تعداد کاربران یا دستگاه‌های متصل به شبکه، زیرساخت شبکه باید بتواند به طور مؤثر این بار را مدیریت کند و از افت عملکرد جلوگیری کند

۲. مقیاس‌پذیری جغرافیایی

این بعد به توانایی شبکه برای حفظ کارایی و عملکرد مناسب بدون توجه به پراکندگی جغرافیایی دستگاه‌ها اشاره دارد. با استفاده از فناوری‌های مدرن، شبکه‌های محلی می‌توانند به راحتی در مکان‌های مختلف گسترش یابند و همچنان عملکرد خوبی داشته باشند.

مقیاس‌پذیری شبکه محلی

ابعاد مقیاس‌پذیری در شبکه‌های محلی

۳. مقیاس‌پذیری اجرایی

این نوع مقیاس‌پذیری به توانایی افزایش تعداد سازمان‌ها یا کاربرانی که از یک شبکه مشترک استفاده می‌کنند، اشاره دارد. با رشد کسب‌وکارها، نیاز به دسترسی همزمان چندین کاربر به منابع شبکه نیز افزایش می‌یابد

۴. مقیاس‌پذیری کارکردی

این بعد به قابلیت ارتقاء سیستم با افزودن کارکردهای جدید بدون نیاز به تغییرات عمده در زیرساخت اشاره دارد. این ویژگی باعث می‌شود که سازمان‌ها بتوانند به راحتی خدمات و برنامه‌های جدید را اضافه کنند.

مقیاس‌پذیری شبکه محلی

مزایای مقیاس‌پذیری در شبکه‌های محلی

انعطاف‌پذیری: سازمان‌ها می‌توانند به راحتی زیرساخت‌های خود را بر اساس نیازهای جدید گسترش دهند، بدون اینکه نیاز به تعمیرات اساسی پرهزینه باشد.

کاهش هزینه‌ها: با استفاده از فناوری‌های مقیاس‌پذیر، سازمان‌ها می‌توانند از هزینه‌های اضافی جلوگیری کرده و منابع خود را بهتر مدیریت کنند.

افزایش بهره‌وری: مقیاس‌پذیری باعث می‌شود که کاربران بتوانند به راحتی و بدون وقفه به منابع دسترسی داشته باشند که این موضوع بهره‌وری را افزایش می‌دهد.

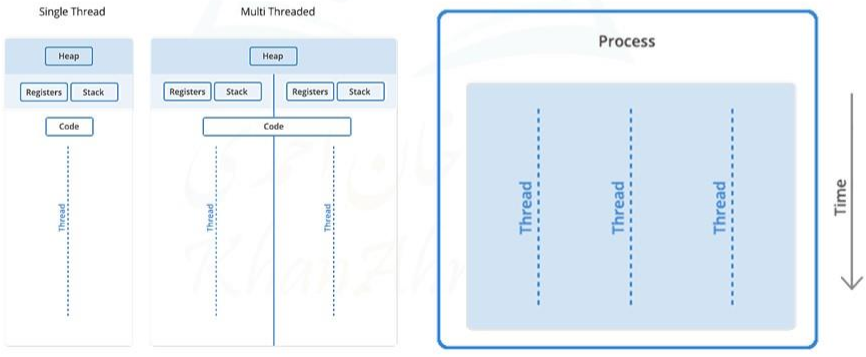
مقیاس‌پذیری یکی از ویژگی‌های کلیدی در طراحی و پیاده‌سازی شبکه‌های محلی است که به سازمان‌ها اجازه می‌دهد تا با رشد و تغییرات سریع دنیای فناوری سازگار شوند. با توجه به ابعاد مختلف مقیاس‌پذیری، سازمان‌ها باید راهبردهایی را برای مدیریت مؤثر منابع و زیرساخت‌های خود تدوین کنند تا بتوانند از مزایای این ویژگی بهره‌مند شوند.

Threadدر مقایسه با Process در شبکه محلی

Threadدر مقایسه با Process

Process نمونه‌ای از یک برنامه است که در حال اجرا یا پردازش است.

Thread بخشی از یک Process یا یک Process سبک وزن است که توسط زمان‌بند به طور مستقل مدیریت می‌شود.



شبکه محلی

Sockets و Remote Procedure Calls (RPC) برای ارتباط

- Socketها رابط برنامه‌نویسی برای ارتباط بین دو برنامه در شبکه هستند. این روش به برنامه‌نویسان اجازه می‌دهد تا با استفاده از پروتکل‌های TCP/IP یا UDP، داده‌ها را بین کلاینت و سرور منتقل کنند.

شیوه‌ی استفاده

- ایجاد Socket: یک Socket سمت سرور ایجاد می‌شود که به یک پورت نرم‌افزاری خاص متصل می‌شود.
- پذیرش اتصال: سرور منتظر اتصالات کلاینت‌ها می‌ماند.
- ارسال و دریافت داده: پس از برقراری اتصال، داده‌ها بین کلاینت و سرور ارسال و دریافت می‌شوند.
- بستن اتصال: پس از اتمام کار، اتصال بسته می‌شود.

شبکه محلی

Sockets و Remote Procedure Calls (RPC) برای ارتباط

- Remote Procedure Calls (RPC) پروتکلی است که به برنامه‌ها اجازه می‌دهد تا رویه‌ها یا توابع را در یک سیستم دیگر (معمولاً در یک سرور) فراخوانی کنند، گویی که این توابع محلی هستند. این تکنیک باعث می‌شود که توسعه‌دهندگان بتوانند بدون نیاز به مدیریت جزئیات شبکه، از خدمات موجود در سرور استفاده کنند.

نحوه استفاده

تعریف رابط: ابتدا باید رابط RPC با استفاده از زبان توصیف رابط IDL تعریف شود.

تولید Stub: با استفاده از ابزارهای مناسب، Stubهای کلاینت و سرور تولید می‌شوند که وظیفه تبدیل پارامترها و مدیریت ارتباطات شبکه را بر عهده دارند.

فراخوانی RPC: کلاینت با استفاده از Stub، درخواست خود را به سرور ارسال می‌کند.

پردازش درخواست در سرور: سرور درخواست را پردازش کرده و نتیجه را به کلاینت بازمی‌گرداند.

مدیریت پاسخ: کلاینت پاسخ دریافتی را مدیریت کرده و ادامه کار خود را انجام می‌دهد.

شبکه محلی

Sockets و Remote Procedure Calls (RPC) برای ارتباط

مزایا:

- سادگی در فراخوانی توابع از راه دور.
- کاهش پیچیدگی کدنویسی برای تعاملات شبکه‌ای.
- پشتیبانی از زبان‌های مختلف برنامه‌نویسی.

معایب:

- ممکن است مشکلاتی مانند تأخیر شبکه وجود داشته باشد.
- نیاز به مدیریت امنیت و اعتبارسنجی برای جلوگیری از حملات.

Socketها مناسب‌تر برای ارتباطات سطح پایین و کنترل دقیق‌تر بر روی داده‌ها هستند، در حالی که RPC برای برنامه‌نویسان راحتی بیشتری فراهم می‌کند تا بتوانند به سادگی خدمات موجود در سرور را فراخوانی کنند. انتخاب بین این دو بستگی به نیازهای خاص معماری مورد نظر دارد.

شبکه محلی

NMAP (Network Mapper)

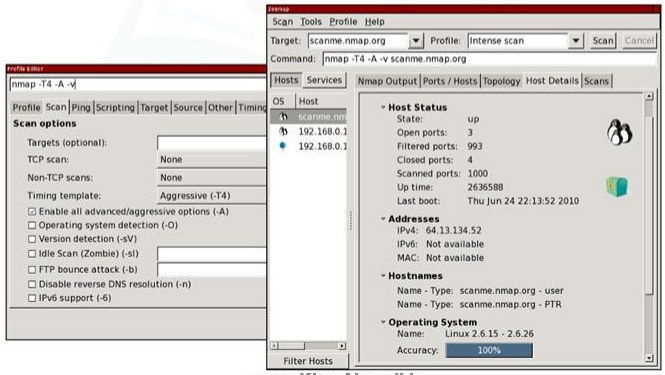
یک ابزار متن باز برای کاوش شبکه و ممیزی امنیتی است. از بسته‌های IP استفاده می‌کند تا تعیین کند چه میزبان‌هایی در شبکه در دسترس هستند، چه خدماتی (نام و نسخه برنامه) ارائه می‌دهند، چه سیستم‌عامل‌هایی با چه نسخه‌هایی در حال اجرا هستند و ده‌ها ویژگی دیگر. آرگومان‌های مورد استفاده در این مثال A– برای تشخیص سیستم‌عامل و نسخه آن و T4- برای اجرای سریعتر و سپس نام میزبان: # nmap -A -T4 khanahmadi.ir

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT     STATE    SERVICE      VERSION
22/tcp   open     ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
| ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open     http         Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp  filtered ldp
1720/tcp filtered H.323/Q.931
9929/tcp open     nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
11  17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

شبکه محلی

Zenmap

Zenmap رابط کاربری گرافیکی رسمی (GUI) برای Nmap Security Scanner است. این برنامه چند سکویی، رایگان و منبع باز است که برای آسان کردن Nmap برای مبتدیان طراحی شده است و در عین حال ویژگی‌های پیشرفته را برای کاربران فراهم می‌کند.



شبکه محلی

Wireshark: تحلیل‌گر پروتکل شبکه متن باز

Wireshark امکان مشاهده در سطح جزئیات شبکه را فراهم می‌کند. توسعه آن از سال ۱۳۷۷ (1998) آغاز شده است و به لطف مشارکت متخصصان شبکه پیشرفت می‌کند. برخی امکانات:

- بازرسی عمیق پروتکل‌ها
- ضبط رویدادهای زنده و تجزیه و تحلیل آفلاین
- چندسکویی: قابل اجرا روی ویندوز، لینوکس، FreeBSD

Wireshark یک تحلیل‌گر بسته‌های شبکه است. Network Packet Analyzer، داده‌های بسته ضبط شده را با بیش‌ترین جزئیات ممکن ارائه می‌دهد.

می‌توان تحلیل‌گر بسته شبکه را به عنوان یک دستگاه اندازه‌گیری برای بررسی آنچه درون کابل شبکه اتفاق می‌افتد در نظر گرفت، درست مانند یک برق کار از یک ولت‌متر برای بررسی آنچه درون کابل برق اتفاق می‌افتد استفاده می‌کند (البته در سطح بالاتر).

در گذشته، چنین ابزارهایی بسیار گران قیمت/اختصاصی بودند اما Wireshark به صورت رایگان در دسترس است و یکی از بهترین تحلیل‌کننده‌های بسته است.

شبکه محلی

Wireshark: تحلیل‌گر پروتکل شبکه متن باز

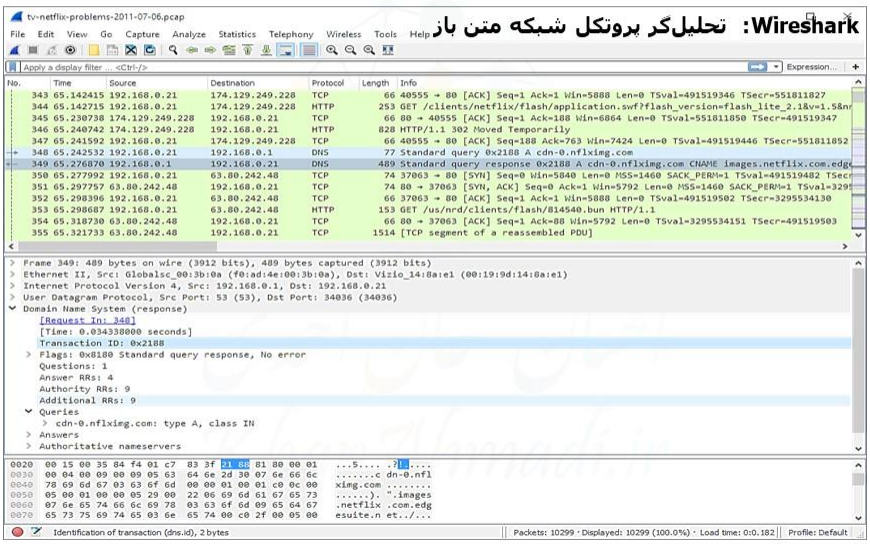
دلایل استفاده از Wireshark:

- عیب‌یابی مشکلات شبکه توسط مدیران شبکه
- بررسی مشکلات امنیتی توسط مهندسان امنیت شبکه
- تایید برنامه‌های شبکه توسط مهندسان تضمین کیفیت QA
- اشکال‌زدایی پیاده‌سازی‌های پروتکل توسط توسعه دهندگان
- یادگیری پروتکل‌های داخل شبکه

تحت مجوز عمومی همگانی گنو GPL منتشر می‌شود. می‌توان آزادانه از Wireshark روی هر تعداد رایانه‌ای که نیاز باشد استفاده کرد، بدون اینکه نگران کلیدهای مجوز یا هزینه‌ها یا مواردی از این دست بود. تمام کد منبع به صورت رایگان تحت GPL در دسترس است.

شبکه محلی

Wireshark: تحلیل‌گر پروتکل شبکه متن باز

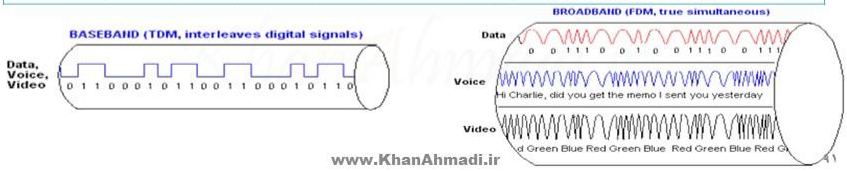


معماری‌های شبکه Network Architectures

روش‌های ارسال سیگنال:

- **الف) Base Band:** در این روش سیگنال دیجیتال (یعنی رشته‌ای از صفر و یک) ارسال می‌شود. برای تقویت این سیگنال از انواع Repeater استفاده می‌شود.(دوجهته)
  - مانند Ethernet
- **ب) Broad Band:** در این روش سیگنال آنالوگ ارسال می‌شود. یعنی سیگنال سینوسی با فرکانس متغیر که برای تقویت آن از آمپلی‌فایر استفاده می‌شود.(یک جهته)
  - مانند Cable television, ISDN,DSL, T1 and T3

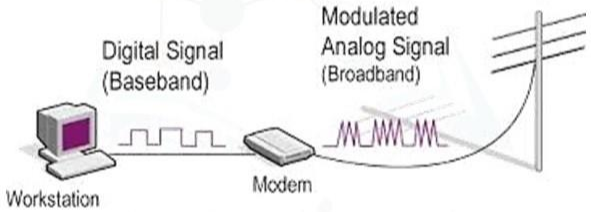
Baseband	Broadband
Digital signaling	Analog signaling (requires RF modem) FDM possible-multiple channels for data, video, audio
Bidirectional	Unidirectional
Bus topology	Bus or tree topology
Distance: up to a few kilometers	Distance: up to tens of kilometers



معماری‌های شبکه Network Architectures

معماری شبکه:

مجموعه‌ای از ویژگی‌های شبکه از قبیل نوع همبندی، کابل، سرعت و ... را مشخص می‌کند.

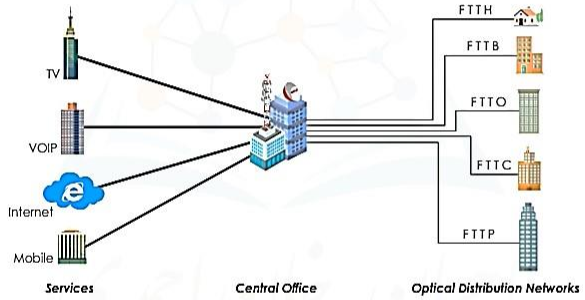


انواع معماری‌های شبکه: Local Talk، Ethernet و Token Ring

- **Local Talk:** این معماری مخصوص شبکه‌های Apple بوده و به Bus Tree هم شهرت دارد.

انواع FTTx

Fiber to the x(FTTX)



- A generic term of last-mile fiber-based broadband access networks and services
- Many different deployment methods and infrastructures, such as
  - Fiber to the Premises (FTTP), Fiber to the Home(FTTH), Fiber to the Building (FTTB), Fiber to the Office (FTTO), Fiber to the Cabinet (FTTC), and many others

آدرس‌دهی و مسیریابی

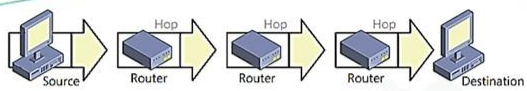
معماری شبکه‌های جدید

معماری شبکه از اطلاعات فرآیند تحلیل برای توسعه استفاده می‌کند. در توسعه معماری شبکه انتخاب فناوری و هم‌بندی درست اهمیت دارد. همچنین روابط بین عملکرد شبکه (آدرس‌دهی/مسیریابی، مدیریت شبکه، کارایی و امنیت) و چگونگی بهینه‌سازی معماری در این روابط تعیین کننده است. معمولا یک معماری یا طراحی "درست" یکتایی برای شبکه وجود ندارد. در معماری شبکه‌ها باید به نیازهای فناوری و خدمات توجه شودکه به طور کلی شامل دو جنبه کلیدی هستند: آدرس‌دهی و مسیریابی.

آدرس‌دهی در شبکه‌های جدید معمولاً مبتنی بر پروتکل IP (Internet Protocol) انجام می‌شود. با ظهور IPv6 بجای IPv4، امکان آدرس‌دهی بیشتر و بهینه‌تر فراهم شده است زیرا فضای آدرس‌دهی وسیع‌تر و قابلیت‌های مدیریت بهتر شبکه‌های بزرگ و پیچیده را دارد.

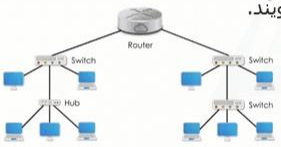
مسیریابی در شبکه‌های کوچک، دستی Static انجام می‌شود و در شبکه‌های با تعداد زیاد تغییرات و تعداد زیاد مسیریاب به صورت پویا Dynamic با استفاده از پروتکل‌های مسیریابی انجام می‌شود. این پروتکل‌ها دو دسته‌اند: بردار فاصله Distance Vector و حالت لینک Link State

آدرس‌دهی و مسیریابی



مفاهیم مسیریابی

- **هدف:** هدایت اطلاعات به مقصد از بهترین مسیر با تشکیل جدول مسیریابی
- **گام (Hop):** به عبور یک بسته از یک Router، گام و به تعداد مسیریاب‌هایی که یک بسته از مبدأ تا مقصد می‌پیماید، تعداد گام (Hop Count) گفته می‌شود.
- **Convergence:** به حالت پایداری الگوریتم‌های مسیریابی می‌گویند.
- **Metric:** همان معیار است.
- **دامنه‌ها:** جداسازی دامنه پخشی و دامنه تصادم با مسیریاب



آدرس‌دهی و مسیریابی

مسیریابی بین شبکه‌ای

- **دستی Static**

مدیر شبکه به صورت دستی، تک‌تک مسیریاب‌ها را برای همه‌ی شبکه‌های مقصد پیکربندی می‌کند و به ازای هر تغییری باید همه‌ی مسیریاب‌های مشارکت‌کننده در تغییر دوباره پیکربندی شوند. پیاده‌سازی این روش پیچیدگی ندارد و ساده، امن، قابل پیش‌بینی و با کارایی بالا است.

این روش برای شبکه‌هایی که تغییرات و تعداد مسیریاب‌ها کم باشد مناسب است.

- **پویا Dynamic**

پروتکل‌هایی مبتنی بر الگوریتم‌های مسیریابی روی مسیریاب‌ها پیکربندی و اجرا می‌شوند تا مسیریابی به صورت خودکار توسط مسیریاب انجام شود. پروتکل‌های پویا در دو نوع درونی Interior مانند RIP و ODPF و بیرونی Exterior مانند BGP طبقه‌بندی می‌شوند.

این روش برای شبکه‌هایی که تغییرات یا تعداد مسیریاب‌ها زیاد باشد مناسب است.

آدرس منطقی و آدرس پورت

آدرس منطقی:

- آدرسی است که توسط CPU در هنگام اجرای یک برنامه تولید می‌شود.

IP Address (نسخه ۴) یک آدرس منطقی ۳۲ بیتی است یک دستگاه میزبان (Host) در شبکه است. مانند: 192.168.10.1

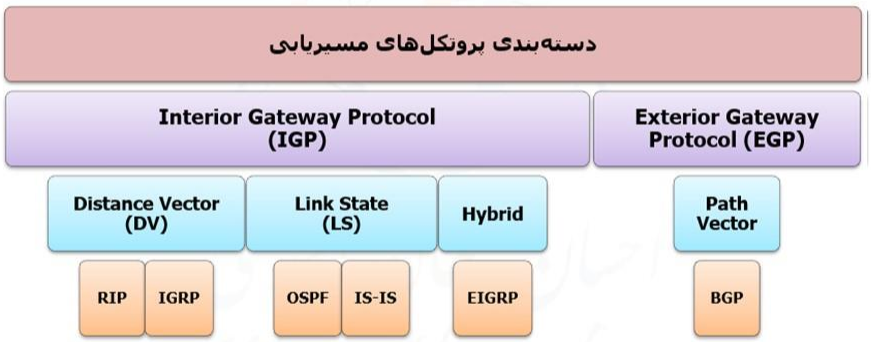
آدرس پورت:

- یک پورت شماره‌ای است که برای دریافت داده‌ها به یک پردازه شبیه به یک برنامه کاربردی یا یک سرویس تخصیص داده شده است. یک پورت/درگاه برای پیدا کردن پردازه‌ای که روی رایانه‌ای در حال اجرا است استفاده می‌شود.

https://fa.mldunbound.org/contrast/difference-between-logical-address-and-physcal-address-4f5c83/
https://b2n.ir/n23102

آدرس‌دهی و مسیریابی

پروتکل‌های مبتنی بر الگوریتم‌های مسیریابی Classification of Routing Protocols



الگوریتم‌های مسیریابی

انواع الگوریتم‌های مسیریابی Interior

- در الگوریتم‌های غیرمتمرکز، مسیریاب اطلاعات کاملی از زیرساخت شبکه ندارد و فقط هزینه ارتباط با مسیریاب‌هایی را که بطور **مستقیم و فیزیکی** با آنها در ارتباطند، محاسبه و ارزیابی می‌کند و در فواصل زمانی منظم، جدول مسیریابی خود را فقط برای **مسیریاب‌های مجاور** ارسال می‌کند. مسیریاب با دریافت این جداول و مقادیری که مستقیم اندازه گرفته با الگوریتم‌های (DV) **Distance Vector** جدول خود را برای هدایت بسته بروز می‌کند. پروتکل‌های **RIP**، IGRP و BGP از این روش استفاده می‌کنند.
- در الگوریتم‌های متمرکز، هر Router اطلاعات کاملی از **تمام** مسیریاب‌های دیگر، ارتباطات بین آنها و هزینه هر خط دارد و بهترین مسیر بین دو مسیریاب توسط الگوریتم‌های **Link State** (LS) انتخاب می‌شود. پروتکل‌های OSPF و IS-IS برای مسیریابی از الگوریتم‌های متمرکز استفاده می‌کنند.
- اگر از برخی ویژگی‌های LS و برخی ویژگی‌های DV در یک Protocol استفاده شود، به آن نوع ترکیبی یا Hybrid گفته می‌شود. مانند EIGRP

الگوریتم‌های مسیریابی

روش ارسال سیل‌آسا (Flooding):

سریع‌ترین الگوریتم برای ارسال بسته‌های Broadcast تنظیمات است. در این روش هر مسیریاب با دریافت این‌گونه بسته‌های تنظیمات آن را روی تمام مسیرهای خروجی خود غیر از مسیر ورودی آنها ارسال می‌کند. از این روش در موارد خاص مثل اعلام جداول مسیریابی در پروتکل‌های OSPF و IS-IS استفاده می‌شود.

راه حل‌های مشکل حلقه بی‌نهایت در شبکه:

۱. قرار دادن شماره شناسایی منحصربفرد برای هر بسته که هر مسیریاب پس از دریافت هر بسته، آن را در یک جدول ثبت کرده و در صورت دریافت دوباره‌ی بسته، آن را حذف می‌کند.
۲. قرار دادن طول عمر یا TTL برای هر بسته که باعث می‌شود با به صفر رسیدن TTL، بسته از شبکه حذف شود.

الگوریتم‌های مسیریابی Link State (LS)

در الگوریتم‌های LS هر مسیریاب باید پنج عمل زیر را انجام دهد:

۱) مسیریاب‌های مجاور خود را که به صورت فیزیکی به آنها متصل است شناسایی کرده و نشانی آنها را بدست آورد.

۲) هزینه مسیریاب‌های مجاور خود را اندازه‌گیری نماید.

۳) یک بسته بسازد و تمام اطلاعات مسیریاب‌های مجاور خود را در آن قرار دهد.

۴) بسته ساخته شده را به روش Flooding برای تمام مسیریاب‌های شبکه ارسال کرده و بسته‌هایی را که از مسیریاب‌های دیگر می‌رسد ذخیره کند.

۵) با الگوریتمی مناسب، مسیر بهینه را بین هر دو مسیریاب در شبکه پیدا کند.

الگوریتم‌های مسیریابی Distance Vector (DV)

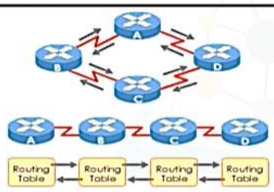
در روش DV برخلاف الگوریتم LS، هر مسیریاب بدون اطلاع از هزینه لینک‌های ارتباطی در زیرشبکه، جدول مسیریابی را در حافظه خود نگه می‌دارد که در آن به ازای هر مسیریاب در زیرشبکه یک رکورد وجود دارد و هر رکورد دو فیلد مجزا دارد:

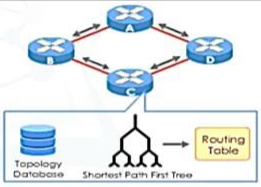
- **فیلد مسیر:** این فیلد خط خروجی مناسب برای رسیدن به یک مسیریاب خاص در شبکه را مشخص می‌کند.
- **فیلد مقدار تقریبی هزینه:** این فیلد هزینه تقریبی رسیدن یک بسته تا مسیریاب مقصد را مشخص می‌کند.

معیار هزینه می‌تواند تأخیر یا تعداد گام در نظر گرفته شود. در این روش هر مسیریاب باید هزینه خطوط فیزیکی با مسیریاب‌های دیگر را محاسبه و در جدول خود درج کند. هزینه سایر خطوط در این جدول بی‌نهایت درنظر گرفته می‌شود. الگوریتم‌های DV برای مسیریابی در یک شبکه کوچک با حداکثر ۱۵ مسیریاب هنوز کاربرد دارد.

مقایسه الگوریتم‌های DV با LS

Distance-Vector vs Link-State Routing



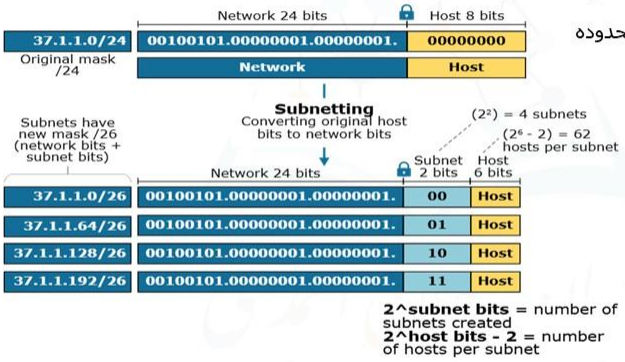


Distance-Vector(RIP, IGRP)	Link-State Routing(OSPF, IS-IS)
Each router only shares its routing table with its neighbors	Each router shares its complete map of the network with all other routers
Making routing decisions based on limited information	With a complete view of the network, routing decisions are more accurate and reliable
Easy to set up and configure	Difficult to set up and configure
Slow convergence	Fast convergence
The metric is typically based on the number of hops between the source and destination	The metric can be based on a variety of factors, such as the bandwidth or delay of a link
Suited for smaller networks	Suited for larger networks

آدرس‌دهی و مسیریابی

مسیریابی بین دامنه بدون کلاس CIDR

- تقسیم‌بندی ساده‌ی محدوده



- به عنوان نمونه نشانی 192.168.7.0/24 در CIDR نشان می‌دهد که ۲۴ بیت اول این نشانی مربوط به بخش شبکه است و ۸ بیت باقی‌مانده برای نشانی‌دهی به دستگاه‌ها استفاده می‌شود.

```
Network:    192.168.7.0/24      11000000.10101000.00000111 .00000000 (Class C)
Broadcast:  192.168.7.255       11000000.10101000.00000111 .11111111
HostMin:    192.168.7.1         11000000.10101000.00000111 .00000001
HostMax:    192.168.7.254       11000000.10101000.00000111 .11111110
```

آدرس‌دهی و مسیریابی

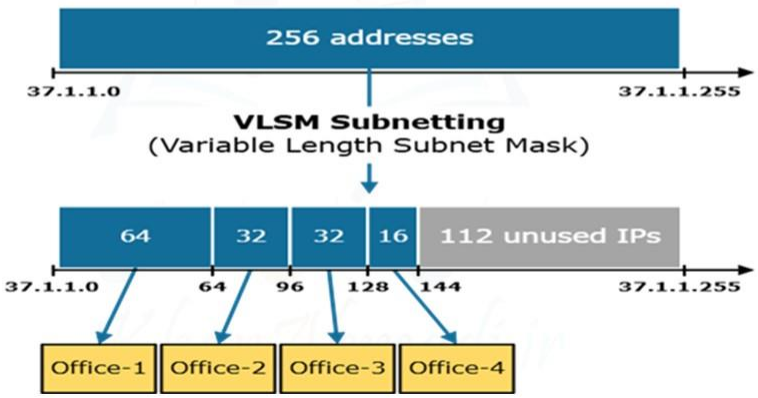
مسیریابی بین دامنه بدون کلاس CIDR

- در روش مسیریابی بین دامنه بدون کلاس یا Classless Inter-Domain Routing، هر نشانی IP با یک عدد اضافی همراه می‌شود که نشان‌دهنده تعداد بیت‌های ثابت در بخش شبکه نشانی است. این عدد پیشوند شبکه، با یک ممیز (/) از نشانی IP جدا می‌شود.
- هدف CIDR، کاهش سرعت رشد جدول‌های مسیریابی روی مسیریاب‌ها در اینترنت و کمک به کاهش سرعت هدر رفتن نشانی‌های IPv4 است.
- مهم‌ترین بیت‌ها پیشوند شبکه است که کل شبکه یا زیرشبکه را مشخص می‌کند و کم‌اهمیت‌ترین مجموعه شناسه میزبان را تشکیل می‌دهد که یک نقطه اتصال خاص از یک میزبان در آن شبکه را مشخص می‌کند. این روش مبتنی بر VLSM است.

آدرس‌دهی و مسیریابی

مسیریابی بین دامنه بدون کلاس CIDR

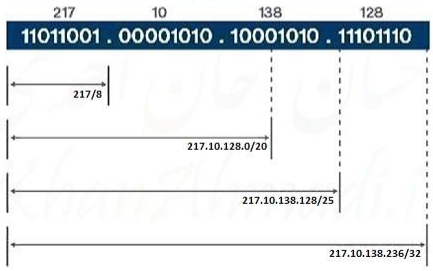
- تقسیم‌بندی ساده‌ی محدوده



آدرس‌دهی و مسیریابی

مسیریابی بین دامنه بدون کلاس CIDR

- این روش امکان می‌دهد تا به جای محدود شدن به کلاس‌های از پیش تعریف شده، دقیقاً تعداد نشانی‌های مورد نیاز مشخص شود. ویژگی دیگر CIDR، امکان تجمیع نشانی‌هاست.
- این قابلیت به مسیریاب‌ها اجازه می‌دهد تا چندین محدوده نشانی مجاور را در یک قاعده مسیریابی واحد ترکیب کنند که به آن Supernet گفته می‌شود. این کار باعث کاهش چشمگیر اندازه جداول مسیریابی و در نتیجه افزایش کارایی شبکه می‌شود.



الگوریتم‌های مسیریابی

مسیریابی بین دامنه IDR (Inter-Domain Routing)

- مسیریابی بین دامنه‌ای کنترل جریان داده و تعامل بین رایانه‌های کنترل کننده دامنه اولیه Primary Domain Controller (PDC) است.
- یک ارائه دهنده خدمات اینترنتی، ISP، با یک نشانی دسترسی به URL منحصر به فرد ارائه می‌شود. این نشانی یک شماره منحصر به فرد است. شماره هر ISP در یک سرور DNS ذخیره می‌شود. سرورهای DNS نام دامنه URL ISP را تفسیر کرده و شماره نشانی IP مناسب را ارائه می‌دهند. دامنه تحت کنترل یک رایانه تخصصی به نام PDC (کنترل کننده دامنه اولیه) است. این رایانه سوابقی از تمام حساب‌های کاربری در دامنه، حقوق آنها برای دسترسی به اطلاعات، و فهرست‌های عملیاتی سامانه تأیید شده را در خود نگه می‌دارد.
- پروتکل های اینترنتی که بر روی IDR متمرکز هستند:
  - Border Gateway Multicast Protocol, Classless Inter-Domain Routing, Multicast Source Discovery Protocol, Protocol Independent Multicast.

آدرس‌دهی و مسیریابی

ویژگی‌های BGP و IBGP

پروتکل BGP مخفف Border Gateway Protocol و از دسته EGP است که از پروتکل TCP:179 استفاده می‌کند. دو مسیریاب برای برقراری ارتباط در BGP ابتدا یک نشست TCP برقرار می‌کنند.

پروتکل BGP مانند سایر پروتکل‌های مسیریابی از روش همسایگی استفاده می‌کند که به صورت دستی انجام شود و امکان برقراری همسایگی به صورت پویا وجود ندارد.

بر خلاف IGP، در پروتکل مسیریابی BGP امکان تشکیل رابطه همسایگی با مسیریابی چند گام آن طرف‌تر نیز وجود دارد.

تمرکز اصلی سایر پروتکل‌های مسیریابی روی مسیریابی و انتخاب بهترین مسیر برای هدایت ترافیک بود ولی سیاست طراحی BGP اعمال سیاست می‌باشد یعنی در BGP با مؤلفه‌های مدیریتی بیشتری می‌توان در مقیاس بالا (حتی در حد چند صد هزار مسیر) استفاده کرد که برای سایر پروتکل‌های مسیریابی امکان‌پذیر نیست.

آدرس‌دهی و مسیریابی

انواع همسایگی در BGP

۱. **همسایگی درون AS‌ی iBGP**

- اگر یک مسیریاب با مسیریابی در AS خودش تشکیل رابطه همسایگی دهد به آن همسایگی iBGP گفته می‌شود.

۲. **همسایگی برون AS‌ی eBGP**

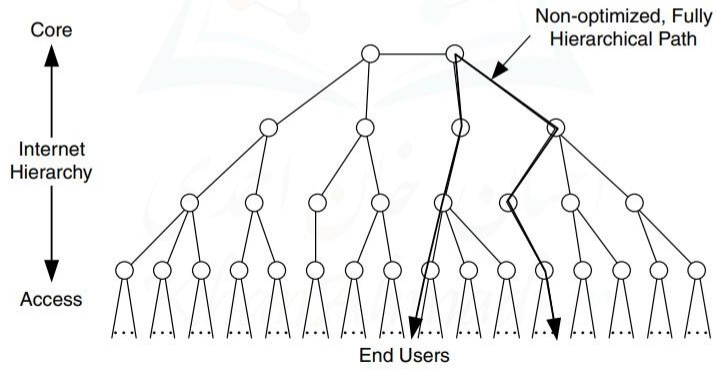
- اگر یک مسیریاب با مسیریابی در AS دیگر تشکیل همسایگی دهد به آن همسایگی eBGP گفته می‌شود. همسایگی‌های برون AS‌ی فقط با یک گام صورت می‌گیرد نه بیشتر پس در شرایطی که با IP مورد نظر بیش‌تر از یک گام فاصله است باید از ویژگی ebgp-multihop استفاده شود.

پیش شرط همسایگی دو مسیریاب در BGP، قابلیت دسترسی مسیریاب‌ها به یکدیگر از طریق نشانی مورد نظر است.

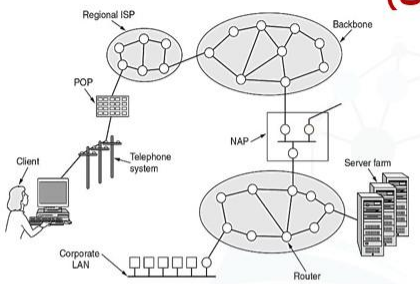
شبکه انتقال Backbone (ستون فقرات)

معماری اینترنت و ستون فقرات

- بالاترین لایه Core نام دارد و به عنوان ستون فقرات Backbone است.



شبکه انتقال Backbone (ستون فقرات)



یک تصویر کلی از اینترنت

معماری اینترنت و ستون فقرات

- ارتباط مشتری با ISP از طریق مودم و خط تلفن
- تبدیل سیگنال دیجیتال به آنالوگ توسط مودم
- تبدیل سیگنال آنالوگ به دیجیتال با ورودبه ISP (یعنی Point Of Presence (POP))
- ورود سیگنال دیجیتال به شبکه منطقه ای ISP و انتقال به مقصد با Packet Switching
- اگر مقصد در شبکه منطقه ای ISP موجود نبود، ارسال سیگنال به Backbone Operator
- یافتن ISP مقصد در Backbone Operator و ارسال سیگنال به نزدیک ترین Router
- برای عبور بهتر بسته‌ها بین شاه‌راه‌های ارتباطی،Routerهای متعدد در NAP قرار می‌گیرند.

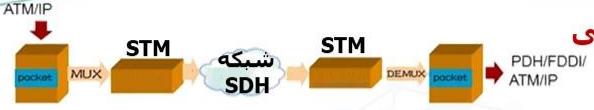
آدرس‌دهی و مسیریابی

شبکه انتقال نوری

مسیریابی در شبکه‌های انتقال نوری یکی از چالش‌های کلیدی در طراحی و مدیریت این شبکه‌ها است. با توجه به افزایش تقاضا برای پهنای باند بالا و نیاز به انتقال داده‌های بزرگ، روش‌ها و الگوریتم‌های مختلفی برای بهینه‌سازی مسیریابی در این شبکه‌ها توسعه یافته‌اند.

برخی جنبه‌های مهم مسیریابی در شبکه‌های نوری:

- تخصیص طول موج از چالش‌های اصلی در شبکه‌های نوری است. الگوریتم‌های مسیریابی، طول موج‌ها را به طور مؤثر تخصیص میدهند تا از تداخل بین سیگنال‌ها جلوگیری شود.
- الگوریتم‌هایی مانند الگوریتم ژنتیک به حل مسائل مسیریابی و تخصیص طول موج در شبکه‌های نوری و افزایش کیفیت خدمات، کاهش تأخیر و افزایش نرخ انتقال کمک می‌کنند.
- در شبکه‌های نوری، همبندی ممکن است به صورت پویا تغییر کند. این امر نیازمند الگوریتم‌هایی است که قادر به انطباق با تغییرات همبندی باشند و بتوانند مسیرهای جدید را شناسایی کنند. استفاده از همبندی‌های خاص مانند شبکه‌های روی تراشه NoC نیز در مسیریابی نوری مورد توجه قرار گرفته است.
- مدیریت ترافیک یک ضرورت است. الگوریتم‌های مسیریابی باید ترافیک حجم بالای ترافیک شبکه‌های نوری را به طور مؤثر مدیریت کرده و از ایجاد گلوگاه جلوگیری کنند. کیفیت خدمات QoS در مسیریابی شامل تضمین کاهش تأخیر، افزایش نرخ انتقال و جلوگیری از افت کیفیت سیگنال است.
- استفاده از روش‌های هوشمند مانند الگوریتم‌های مبتنی بر یادگیری ماشین به بهبود عملکرد مسیریابی کمک می‌کند. با شناسایی الگوهای ترافیکی، مسیرهای بهینه پیشنهاد می‌شود.



آدرس‌دهی و مسیریابی

IP از طریق SDH

SDH (Synchronous Digital Hierarchy) یک فناوری انتقال اطلاعات بر روی بسترهای نوری است. این فناوری امکان انتقال سیگنال‌های مختلف دیجیتال، از جمله IP، را به صورت همزمان و با کارایی بالا با مالتی‌پلکس کردن آنها به یک سیگنال نوری میسر می‌کند.

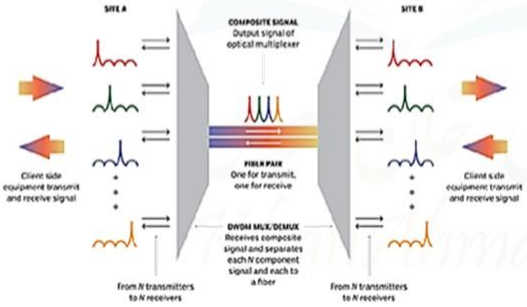
ویژگی‌های کلیدی SDH:

- **انتقال IP روی SDH**
  - SDH از روش Multiplexing برای ترکیب چندین سیگنال با نرخ‌های مختلف به یک سیگنال با نرخ بالاتر استفاده می‌کند. این ویژگی به SDH اجازه می‌دهد تا سیگنال‌های IP را در کنار سایر سیگنال‌ها مانند صوت و ویدئو منتقل کند.
  - SDH دارای سازوکار قوی مدیریت خطا و نظارت بر کیفیت خدمات است. این امر باعث می‌شود که انتقال IP با کمترین اختلال و تأخیر انجام شود.
- **مزایای استفاده از SDH برای انتقال IP**
  - SDH قادر است داده‌ها را با سرعت‌های بالا (تا چند گیگابیت در ثانیه) منتقل کند.
  - SDH قابلیت پشتیبانی از پروتکل‌های مختلف مانند Ethernet و MPLS را دارد، که این امر انعطاف‌پذیری بیشتری را برای انتقال IP فراهم می‌کند.
  - SDH امکان مدیریت و نظارت مؤثر بر ترافیک شبکه را فراهم می‌کنند.
- **ساختار فریم SDH**
  - فریم‌های SDH به دو بخش تقسیم می‌شوند: سربار Overhead و محموله Payload. سربار شامل اطلاعات مدیریتی و کنترل است، در حالی که محموله شامل داده‌های واقعی منتقل شده (مانند بسته‌های IP است.

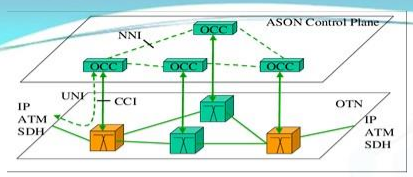
آدرس‌دهی و مسیریابی

پهنای باند SDH فریم آمریکایی را OC می‌گویند و SDH اروپایی را STM:

- STM-1 (155 megabits per second)
- STM-4 (622 Mbps)
- STM-16 (2.5 gigabits per second)
- STM-64 (10 Gbps)
- STM-256 (40 Gbps)



Optical Transmission System SDH Equipment Huawei OSN 3500



آدرس‌دهی و مسیریابی

IP از طریق WDM/ASON

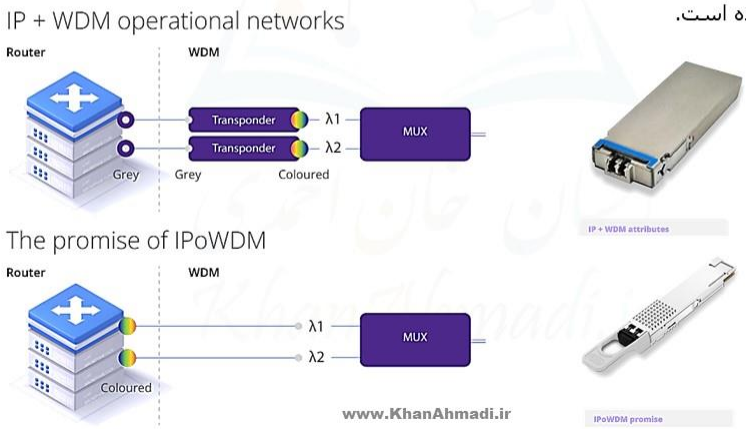
فناوری ASON (Automatic Switched Optical Network): شبکه نوری «هوشمند» که می‌تواند به طور خودکار سیگنال‌دهی و مسیریابی را از طریق شبکه مدیریت کند.

- فناوری حفاظتی شبکه‌های نوری WDM (Wavelength-Division Multiplexing)
- برای استفاده از پهنای باند و کشف شبکه برای دستیابی به حفاظت انعطاف پذیر
- استفاده با هم‌بندی‌های Mesh
- کار مبتنی بر GMPLS (Generalized Multi-Protocol Label Switching)
- بستگی صفحه کنترل ASON به ۳ پروتکل OSPF TE، LMP و RSVP TE
- دارای چندین SLA برای محافظت از شبکه WDM مانند سطح خدمات الماس، طلا، نقره
- نیاز IPoWDM به بسته نرم افزاری خاصی برای بارگذاری در optical Network Elements (NE)
- محافظت در برابر چندین خطا با استفاده از روش حفاظت و بازیابی از شبکه WDM

آدرس‌دهی و مسیریابی

IP از طریق WDM/ASON و IP از طریق WDM/GbEthernet

مفهوم IP over WDM (IPoWDM) سالهاست که وجود داشته است. فرض اساسی آن همیشه توانایی استقرار اپتیک‌های انتقال در سکوهای مسیریابی برای به تأخیر انداختن و ساده‌سازی شبکه‌ها بوده است.



آدرس‌دهی و مسیریابی

MPLS (Multi-protocol label switching)

این با ایجاد مسیرهای از پیش تعیین شده‌ی کارآمد، مشکل تصمیم‌گیری زمان‌بر هر مسیریاب برای هدایت هر بسته، مبتنی بر سرایند آن بسته را برطرف کرد. به محض ورود بسته به شبکه، به یک کلاس FEC (forwarding equivalence class) اختصاص داده می‌شود و با افزودن یک bit sequence کوتاه (برچسب) نشانه‌گذاری می‌شود. بنابراین مسیریاب‌ها نیازی به تجزیه و تحلیل سرآیند ندارند بلکه، مسیریاب‌های بعدی از آن برچسب استفاده می‌کنند.

با این روش بسته‌های حامل ترافیک آنی، مانند صدا یا ویدئو، به‌راحتی در مسیرهای کم تأخیر در شبکه قرار داده می شوند.

اجزای MPLS:

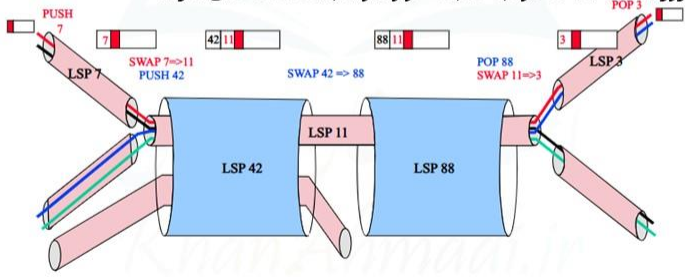
- برچسب Label شامل اطلاعات مقاصد، بیت‌های Experimental برای تضمین کیفیت خدمات QoS، Bottom-of-Stack نشانه آخرین بسته، TTL طول عمر بسته

ادعا می‌شود SD-WANآمده است تا جای MPLSرا بگیرد.

آدرس‌دهی و مسیریابی

MPLS (Multi-protocol label switching)

مسیریاب‌های MPLSمبتنی بر معیارهای موجود در FEC، یک مسیر label-switched path (LSP) یک‌طرفه ایجاد می‌کنند، مسیری که از قبل برای ترافیک در یک شبکه MPLSتعیین شده است.
هنگامی که یک کاربر ترافیکی را به شبکه MPLS ارسال می‌کند، یک برچسب MPLS توسط مسیریاب ورودی MPLS که در لبه شبکه قرار دارد، بدان اضافه می‌شود.

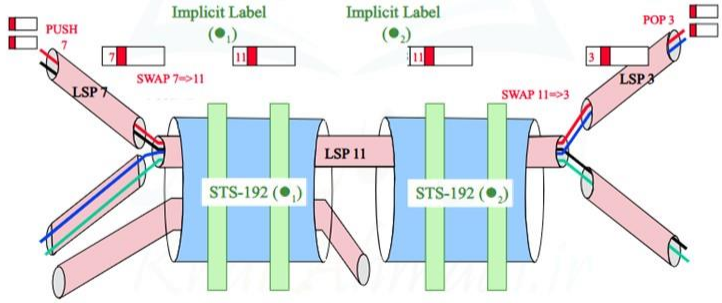


- "Virtual" Muxing - No Utilization Penalty
- This Is A Key Driver For Replacing TDM

آدرس‌دهی و مسیریابی

از MPLS تا GMPLS (Generalized MPLS)

GMPLS یعنی تعمیم یافته با MPLS سنتی تفاوت دارد زیرا پشتیبانی را به انواع مختلف سوئیچینگ مانند سوئیچینگ TDM، طول موج و فیبر گسترش می‌دهد. GMPLS امکان سوئیچینگ شبکه سریع و قابل اعتماد جریان داده را در هر نوع زیرساخت شبکه فراهم می‌کند.

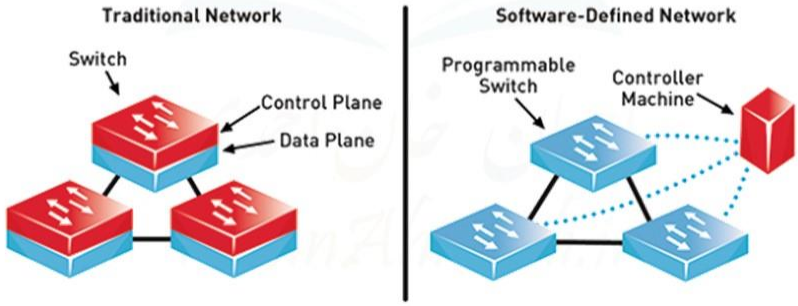


GMPLS: Generalized MPLS

آدرس‌دهی و مسیریابی

SDN

SDN یک رویکرد معماری شبکه است که شبکه را قادر می‌سازد تا با استفاده از برنامه‌های کاربردی نرم‌افزاری، به‌طور هوشمند و مرکزی کنترل یا برنامه‌ریزی شود. به این ترتیب اپراتورها کمک می‌شود تا بدون توجه به فناوری شبکه، کل شبکه را به طور مداوم و جامع مدیریت کنند.



آدرس‌دهی و مسیریابی

پروتکل‌های جدید شبکه و انتقال

- 5G و فراتر از آن: برخی از روندها و نوآوری‌های در حال ظهور در پروتکل‌های شبکه مربوط به 5G و فراتر از آن هستند. محققان در حال حاضر روی 6G و فراتر از آن کار می‌کنند که هدف آن دستیابی به نرخ داده در سطح ترابیت، تأخیر زیر میلی ثانیه، اتصال گسترده و مدیریت هوشمند شبکه است.
- QUIC و HTTP/3 : QUIC یک پروتکل انتقال جدید است که ویژگی‌ها و مزایای TCP و UDP را ترکیب می‌کند.
- RINA و شبکه بازگشتی Recursive Networking: RINA معماری ساده‌ساز با تعمیم بنیادی پشته پروتکل اینترنت فعلی با استفاده پروتکل یکسان در تمام لایه های شبکه!
- BBR: الگوریتم جدید کنترل تراکم
- DNS over HTTPS (DoH): پروتکلی امن‌ساز ارتباط بین کلاینت و DNS با استفاده از HTTPS
- CoAP: پروتکل کاربردی سبک برای دستگاه ها و شبکه های محدود مانند IoT

نشانی‌های IP و نسخه‌های آن

IP (Internet Protocol):
تعریف قالب بسته‌های پیام و پروتکل آنها که در لایه ۳ از OSI تعریف می‌شود.

نسخه ۴: (۳۲ بیتی)
تعداد نشانی‌ها 2^{32} است که با افزایش دستگاه‌های نیازمند IP، نشانی‌های این نسخه در حال اتمام است.

$2^{32}=4,294,967,296$

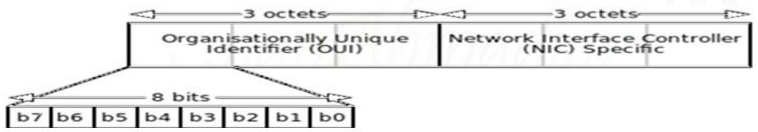
نسخه ۶: (۱۲۸ بیتی)
تعداد نشانی‌ها از 2^{32} به 2^{128} افزایش یافت.
یعنی می‌توان به همه تجهیزات شبکه فعلی و تجهیزات خانگی، شخصی، عمومی و همه وسائل ساخت بشر IP منحصر به فرد اختصاص داد و باز هم این نشانی‌ها به اتمام نرسد!

$2^{128}=340,282,366,920,938,463,463,374,607,431,768,211,456$

نشانی‌ها و خدمات اصلی در اینترنت و اینترانت

- **نشانی‌های Public:** نشانی‌هایی که یکتا هستند و به زبان عامیانه IP Valid نامیده می‌شوند. این نشانی‌ها برای نشانی‌دهی در اینترنت استفاده می‌شوند.

- **نشانی‌های Private:** نشانی‌هایی که در داخل شبکه‌های محلی یا اختصاصی استفاده می‌شوند و در آن شبکه یکتا هستند. محدوده نشانی‌های Private در کلاس A، B و C عبارتند از:
  - **10**.0.0.0 : a single class **A** network
  - **172.16**.0.0 through **172.31**.0.0 : 16 contiguous class **B** networks
  - **192.168.0**.0 through **192.168.255**.0 : 256 contiguous class **C** networks
- **Loopback:** نشانی بازگشت به خود. همه IPهای 127.x.x.x رابطی هستند برای کپی داده‌ها از بافر انتقال به بافر دریافت کارت شبکه یعنی NIC
- **Gateway:** نشانی خارج شدن بسته از شبکه فعلی (در صورت موجود نبودن مقصد درون شبکه)
- **DNS:** تبدیل نام FQDN به نشانی IP Address (و بالعکس)
- **DHCP:** اجاره تنظیمات TCP/IP (مانند IP Address و Subnet Mask, DNS, DHCP, Gateway Address)
- **Mac Address یا Physical Address:** نشانی یکتا در دنیا که توسط کارخانه سازنده روی interface ارتباطی تجهیزات شبکه درج می شود.



کلاس‌های نشانی IP نسخه ۴: IPV4: W.X.Y.Z

IP Address Class	W	Network ID	Host ID	تعداد شبکه	تعداد سیستم در هر شبکه
A	1-126	W	X.Y.Z	126	$(256)^3$ -2
B	128-191	W.X	Y.Z	64 * 256	$(256)^2$ -2
C	192-223	W.X.Y	Z	32 * $(256)^2$	256 -2
D	224-239	برای گروه‌بندی سیستم روی مسیریاب Multicast			
E	240-255	مخصوص پنتاگون			

- با محاسبه Subnet Mask می‌توان فهمید IPها در یک شبکه هستند یا نه
- Subnet Mask پیش فرض برای کلاس‌های A، B و C عبارتند از:
  - 255.0.0.0 برای کلاس A، 255.255.0.0 برای کلاس B و 255.255.255.0 برای کلاس C
- از Octet اول (یعنی W) می‌توان فهمید که IP Address در چه کلاسی قرار دارد
- دستگاه نمی‌تواند نشانی‌های کلاس D و E را به عنوان IP خود قبول کند
- در ستونی که مشخص کننده تعداد دستگاه در هر شبکه است، از تعداد کل دستگاه‌ها ۲ واحد کم شده است زیرا در هر شبکه اولین و آخرین نشانی آن شبکه غیرمعتبر(Invalid) است. یعنی برای IP یک دستگاه از شبکه، همه‌ی بیت‌های Host ID نمی‌تواند صفر یا همگی یک باشند. اگر همه‌ی بیت‌های هر Octet یک باشد با ۲۵۵ نمایش داده می‌شود.
  - اگر Host ID همگی صفر باشد نشان دهنده نشانی شبکه است و اگر همه بیت‌های آن 1 باشد نشان دهنده نشانی ارسال پخشی به همه اعضای شبکه است یعنی Broadcast Address است
  - **مثال:** 10.0.0.0، 172.16.0.0 و 192.168.100.0 نشانی ۳ شبکه مختلف در سه کلاس متفاوت هستند. همچنین 10.255.255.255، 172.16.255.255 و 192.168.100.255 نشانی Broadcast همان شبکه‌ها هستند.

نشانی‌های IP v6 - IP (IP نسخه ۶)

نشانی‌های IPv6 از ۸ بخش hexadecimal چهار digits(۱۶ بیتی) استفاده می کنند که بخش‌ها با علامت دو نقطه (:) از هم جدا شده‌اند. بخش‌های ۱۶ بیتی که به صورت اعداد مبنای ۱۶ هستند بین 0000 و FFFF واقع شده‌اند مانند:

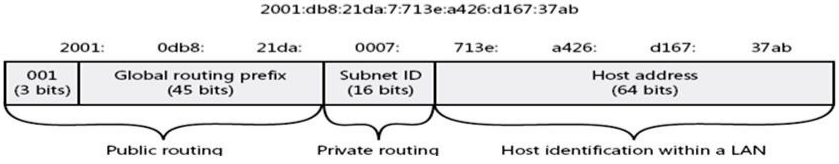
2001:0DB8:3FA9:0000:0000:0000:00D3:9C5A

می‌توان 0های پیش از اعداد را حذف کرد یعنی *2001:DB8:3FA9:0:0:0:D3:9C5A*

اگر هر بخش فقط 0 داشت می‌توان کل بخش را حذف کرد،(فقط یکبار) یعنی:

2001:DB8:3FA9::D3:9C5A

اگر چه پیشرفت‌های IPv6 در مقایسه با IPv4 شامل مواردی از جمله کیفیت سرویس (QoS)، مسیریابی کارآمدتر، پیکربندی ساده و بهبود امنیت است اما افزایش فضای نشانی در IPv6 مهم‌ترین ویژگی آن به شمار می‌رود.



آدرس‌دهی و مسیریابی

IPv4-IPv6

دو نسخه از پروتکل اینترنت هستند که برای شناسایی و ارتباط دستگاه‌ها در شبکه‌های رایانه‌ای استفاده می‌شوند. با نیاز به نشانی‌های بیشتر، IPv6 جانشین IPv4 شد. امنیت و کارایی بیشتر مزایای دیگر IPv6 هستند. با وجود اینکه بسیاری از شبکه‌ها هنوز از هر دو پروتکل استفاده می‌کنند، روند انتقال به IPv6 در حال افزایش است تا نیازهای روزافزون کاربران برآورده شود.

IPv4 از ۳۲ بیت استفاده می‌کند که امکان ایجاد حدود ۴٫۳ میلیارد نشانی را دارد.

- به صورت دودویی است اما برای سادگی ده دهی نمایش داده می‌شود 192.168.100.23
- پیکربندی به صورت دستی یا خودکار با استفاده از DHCP
- امنیت اختیاری با استفاده از پروتکل IPsec تأمین می‌شود.
- دارای سرآیند پیچیده که ممکن است باعث کاهش کارایی مسیریابی شود.
- برای مدیریت کمبود نشانی، نیازمند NAT (Network Address Translation)

IPv6 از ۱۲۸ بیت استفاده می‌کند که امکان حدود ۳۴۰ تریلیون تریلیون تریلیون نشانی را دارد.

- نمایش به صورت هگزادسیمال در ۸ گروه ۱۶ بیتی مانند 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- امکان پیکربندی خودکار SLAAC بدون نیاز به سرور DHCP توسط دستگاه تولید می‌شود.
- امنیت از طریق IPsec به عنوان یک ویژگی استاندارد گنجانده شده است،
- سرآیند ساده‌ای دارد که باعث افزایش سرعت مسیریابی و کارایی کلی شبکه می‌شود.
- نیازی به NAT ندارد و قابلیت multicast را هم برای ارسال به چندین مقصد فراهم می‌کند.

آدرس‌دهی و مسیریابی

آی پی موبایل: Mobile IP یا MIP

MIP با توسعه IP ایجاد شده است بنابراین برای اینترنت مقیاس‌پذیر است و هر دستگاهی که IP را پشتیبانی می‌کند می‌تواند MIP را نیز پشتیبانی کند.

Mobile IP به کاربران دستگاه تلفن همراه اجازه می‌دهد تا از یک شبکه به شبکه دیگر حرکت کنند و در عین حال همان نشانی IP دائمی را حفظ کنند.

مفهوم و نقش Mobile IP در حوزه فناوری محاسبات موبایل بسیار مهم است زیرا ارتباط را بی‌عیب و نقص می‌کند و تضمین می‌کند که ارتباط بدون قطع شدن جلسات یا اتصالات کاربر انجام می‌شود.

آدرس‌دهی و مسیریابی

آی پی موبایل: Mobile IP یا MIP

در شبکه‌های IP، وقتی دستگاهی در شبکه خانگی خود قرار دارد، مسیریابی مبتنی بر اساس نشانی‌های IP ثابت است. دستگاه در یک شبکه از طریق مسیریابی IP معمولی توسط نشانی IP اختصاص داده شده در شبکه متصل می‌شود. مانند نحوه تحویل نامه پستی به نشانی ثابت روی پاکت است. مشکل زمانی رخ می‌دهد که دستگاه از شبکه خانگی خود دور می‌شود و با استفاده از مسیریابی IP معمولی دیگر قابل دسترس نیست. در این شرایط، جلسات فعال دستگاه خاتمه می‌یابند. ایده موبایل IP برای حل این مشکل مطرح شد تا به کاربران کمک کند، هنگام رفتن به یک شبکه دیگر یا یک اپراتور بی‌سیم دیگر، نشانی IP یکسانی را بدون اختلال در ارتباط یا بدون قطع شدن جلسات یا اتصالات، حفظ کنند. قابلیت جابجایی‌پذیر شدن IP موبایل به جای لایه فیزیکی بر روی لایه شبکه انجام می‌شود.

آدرس‌دهی و مسیریابی

IP Multicast

روش انتقال داده به گروهی از گیرندگان در شبکه‌های رایانه‌ای است. با ارسال یک نسخه از داده‌ها به چندین گیرنده کارآمدتر است. منابع شبکه بهتر مدیریت می‌شوند و از مصرف غیرضروری پهنای باند جلوگیری می‌شود. با توجه به افزایش نیاز به خدمات چندرسانه‌ای و ارتباطات گروهی، اهمیت IP Multicast روزبه‌روز بیشتر می‌شود. IP Multicast کاربردهای زیادی دارد، از جمله پخش زنده ویدئو، وبینارها و توزیع نرم‌افزار

در مقایسه با Unicast (انتقال داده از یک فرستنده به یک گیرنده) و Broadcast (انتقال داده به تمام دستگاه‌های موجود در یک شبکه)، Multicast اجازه می‌دهد داده‌ها به گروه خاصی از گیرندگان ارسال شوند. این ویژگی باعث کاهش بار ترافیکی و افزایش کارایی شبکه می‌شود.

- نشانی‌های IP Multicast در IPv4 در محدوده 224.0.0.0 تا 239.255.255.255 قرار دارند و تنها به عنوان نشانی مقصد قابل استفاده است. در IPv6، با پیشوند ff00::/8 شروع می‌شوند.
- از پروتکل IGMP برای مدیریت عضویت دستگاه‌ها در گروه‌های multicast استفاده می‌شود تا به دستگاه‌ها اجازه دهد به مسیریاب‌های محلی اعلام کنند که به کدام گروه ملحق می‌شوند یا از آن بیرون می‌شوند.

آدرس‌دهی و مسیریابی

Host Identity Protocol (HIP)

فناوری شناسایی میزبان برای استفاده در شبکه‌های IP طراحی شده است. این پروتکل برای جداسازی نقش‌های شناساپی و مکان‌یابی نشانی‌های IP توسعه یافته و از یک فضای نام جدید به نام Host Identity (HI) استفاده می‌کند که بر پایه زیرساخت امنیتی کلید عمومی است و پیاده‌سازی آن نیازی به تغییر برنامه‌ها یا مسیریاب‌ها ندارد.

- HIP با معرفی فضای نام HI، نقش‌های شناسایی Identifier و مکان‌یابی Locator نشانی‌های IP را از هم جدا می‌کند و IPها دیگر به عنوان شناسه‌ها استفاده نمی‌شوند و به جای آن از شناسه‌های رمزنگاری شده استفاده می‌شود. HIP از کلیدهای عمومی برای شناسایی میزبان‌ها استفاده می‌کند.
- HIP در برابر حملاتی مانند Denial-of-Service (DoS) و Man-in-the-Middle (MitM) مقاوم است. HIP می‌تواند با پروتکل‌های امنیتی مانند Encapsulated Security Payload (ESP)، ترکیب شود تا حفاظت از درستی و رمزگذاری برای پروتکل‌های بالاتر TCP/UDP را فراهم کند.
- قابلیت multi-homing برای اتصال همزمان به بیش از یک شبکه و جابجایی mobility برای اجازه دادن به دستگاه‌ها برای جابجایی بدون نیاز به تغییر نشانی IP را دارد.

آدرس‌دهی و مسیریابی

TCP چند مسیره

برای اتصال یک میزبان یا دستگاه به چندین شبکه استفاده می‌شود. قابلیت اطمینان، توزیع ترافیک و بار از مزایای این فناوری است. سازمان‌ها قادر خواهند بود تا در صورت بروز مشکل در یکی از اتصالات، همچنان ارتباط خود را حفظ کنند و از مزایای سرعت بالاتر و توزیع بار بهره‌مند شوند.

- TCP برای اطمینان از انتقال مطمئن بین دو دستگاه در شبکه با استفاده از سازوکارهایی مانند تأیید دریافت ACK و ارسال دوباره‌ی بسته‌ها برای تضمین تحویل عمل می‌کند.
- TCP چند مسیره اتصال یک دستگاه به چندین شبکه یا ISP است.
- در TCP چند مسیره اگر یکی از اتصالات دچار مشکل شود، TCP می‌تواند از اتصال دیگر برای ادامه انتقال داده‌ها استفاده کند که باعث کاهش زمان قطعی و افزایش پایداری می‌شود.
- امکان ارسال همزمان وجود دارد، که باعث افزایش سرعت و کاهش تأخیر می‌شود.
- با توزیع ترافیک بین اتصالات مختلف منابع شبکه بهینه استفاده شده و از ازدحام ترافیک جلوگیری می‌شود.
- مدیریت چندین اتصال و نشانی IP پیچیده است و نیازمند پیکربندی دقیق است.
- برای پیاده‌سازی به پروتکل‌های مسیریابی مناسب مانند BGP (Border Gateway Protocol) نیاز است تا ترافیک بین مسیرهای مختلف به طور مؤثر مدیریت شود.

آدرس‌دهی و مسیریابی

QUIC (Quick UDP Internet Connections)

یک پروتکل انتقال داده جدید است که توسط گوگل توسعه یافته و به منظور بهبود سرعت و امنیت ارتباطات اینترنتی طراحی شده است. این پروتکل برای استفاده در ترافیک HTTP و به عنوان جایگزینی برای پروتکل‌های قدیمی‌تر مانند TCP و TLS ایجاد شده است. با ترکیب مزایای UDP و ویژگی‌های امنیتی TCP، تجربه‌ای سریع‌تر و ایمن‌تر برای کاربران اینترنت فراهم می‌آورد.

- QUIC بر پایه پروتکل UDP (User Datagram Protocol) طراحی شده است، تا بدون نیاز به مراحل پیچیده اتصال، داده‌ها را سریع‌تر منتقل کند. این ویژگی باعث کاهش زمان تاخیر در برقراری ارتباط می‌شود.
- برخلاف TCP که نیاز به چندین مرحله handshake برای برقراری اتصال دارد، QUIC با یک مرحله سریع و با استفاده از رمزنگاری TLS 1.3 ارتباطات امن را برقرار می‌کند تا سرعت بارگذاری صفحات وب افزایش یابد.
- برای امنیت بالا طراحی شده و تمامی ارتباطات آن به صورت رمزنگاری شده انجام می‌شود.
- کنترل ازدحام و تحویل مطمئن از قابلیت‌های QUIC است که از TCP به ارث برده است و همچنین تحویل مطمئن داده‌ها را بدون مسدودسازی خط جلو Head-of-line blocking ارائه می‌دهد، که در شبکه‌های پرترافیک مفید است.
- امکان مهاجرت اتصال را فراهم می‌کند. مثلا حین استفاده از یک سرویس وب IP تغییر کند از Wi-Fi به LTE

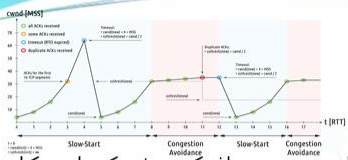
آدرس‌دهی و مسیریابی

انتقال قابل اعتماد در مقابل غیرقابل اعتماد

انتقال داده‌ها در شبکه‌ها می‌تواند به دو صورت قابل اعتماد و غیرقابل اعتماد انجام شود. انتخاب بین انتقال قابل اعتماد و غیرقابل اعتماد بستگی به نیازهای خاص هر کاربرد دارد. در حالی که انتقال قابل اعتماد برای کاربردهایی که نیاز به دقت و اطمینان دارند مناسب است، انتقال غیرقابل اعتماد برای مواردی که سرعت اولویت دارد، انتخاب بهتری خواهد بود.

- انتقال قابل اعتماد به پروتکل‌هایی اشاره دارد که تضمین می‌کنند پیام‌ها به طور درست و کامل به گیرنده منتقل شوند. این پروتکل‌ها معمولاً شامل سازوکارهایی برای شناسایی و تصحیح خطاها هستند. تأیید دریافت، بازفرستادن پیام در صورت عدم دریافت تأیید، ترتیب درست پیام‌ها از ویژگی‌های این پروتکل‌هاست. TCP (Transmission Control Protocol) یکی از معروف‌ترین پروتکل‌های قابل اعتماد است.
- انتقال غیرقابل اعتماد، به پروتکل‌هایی اشاره دارد که هیچ تضمینی برای موفقیت‌آمیز بودن انتقال داده‌ها ندارند اما معمولاً سریع‌ترند و ممکن است منجر به از دست رفتن داده‌ها شود. عدم تأیید دریافت، عدم ترتیب خاص که گیرنده باید خودشان ترتیب را مدیریت کند، مورد استفاده آن جایی است که سرعت بیشتر از دقت اهمیت دارد، مانند بازی‌های آنلاین یا پخش زنده رسانه‌ای. پروتکل UDP (User Datagram Protocol) یک نمونه از پروتکل‌های غیرقابل اعتماد است که در بسیاری از برنامه‌های کاربردی رسانه‌ای و صوتی استفاده می‌شود.

آدرس‌دهی و مسیریابی



کنترل تراکم

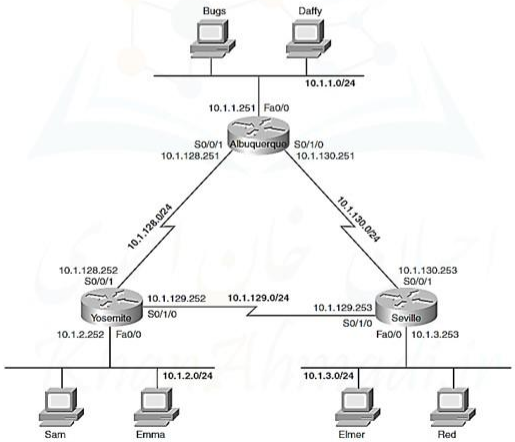
به مجموعه‌ای از روش‌ها و پروتکل‌ها گفته می‌شود که برای مدیریت ترافیک در شبکه‌ها به کار می‌روند. هدف اصلی این فرآیند جلوگیری از بروز پدیده ازدحام و تراکم congestion در شبکه است، که می‌تواند منجر به کاهش کیفیت خدمات و افت سرعت انتقال شود. مانند پروتکل TCP

- سازوکارهای پیشگیرانه که از بروز تراکم جلوگیری می‌کنند.
  - آغاز آهسته Slow Start که فرستنده با یک اندازه پنجره کوچک شروع می‌کند و به تدریج آن را افزایش می‌دهد تا زمانی که به بیشینه ظرفیت شبکه برسد.
  - افزایش جمعی و کاهش ضربی Additive Increase/Multiplicative Decrease (AIMD) که به فرستنده اجازه می‌دهد تا در صورت عدم بروز تراکم، اندازه پنجره را افزایش دهد و در صورت بروز مشکل، اندازه پنجره را نصف کند.
- سازوکارهای واکنشی زمانی فعال می‌شوند که تراکم در شبکه تشخیص داده شود.
  - تایمرها: استفاده از تایمرها برای مدیریت زمان انتظار و ارسال مجدد بسته‌هایی که تأیید نشدند.
  - اعلان تراکم صریح Explicit Congestion Notification به فرستنده اطلاع می‌دهد که باید سرعت ارسال داده‌ها را کاهش دهد.

آدرس‌دهی و مسیریابی

پیاده‌سازی مسیریابی دستی Static

Internetwork زیر را پیاده‌سازی کنید و ارتباط شبکه‌ها را برقرار کنید.



آدرس‌دهی و مسیریابی

پیاده‌سازی مسیریابی دستی Static

دستورات برای یک مسیریاب R1 آورده شده است، برای بقیه هم مانند نمونه انجام می‌شود.

```
R1-Albuquerque#show ip route
R1-Albuquerque#ping 10.1.128.252
R1-Albuquerque#ping 10.1.2.252
```

R1-Albuquerque only has routes for its three connected subnets. So, R1-Albuquerque's ping 10.1.2.252 command creates the packets, but discards the packets because no routes exist.

```
R1-Albuquerque(config)#ip route 10.1.2.0 255.255.255.0 10.1.128.252
R1-Albuquerque(config)#ip route 10.1.3.0 255.255.255.0 10.1.130.253
R1-Albuquerque#show ip route
10.0.0.0/24 is subnetted, 5 subnets
C    10.1.1.0 is directly connected, FastEthernet0/0
S    10.1.2.0 [1/0] via 10.1.128.252
S    10.1.3.0 [1/0] via 10.1.130.253
C    10.1.128.0 is directly connected, Serial0/0/0
C    10.1.130.0 is directly connected, Serial0/0/1
R1-Albuquerque#ping 10.1.2.252
```


آدرس‌دهی و مسیریابی

پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی

پروتکل RIP (Routing Information Protocol) مبتنی بر الگوریتم DV است و معیار هزینه در آن تعداد گام است یعنی هزینه بین دو مسیریاب مساوی ۱ است. RIP برای مبادله جداول مسیریابی از پروتکل UDP استفاده می‌کند.

در پروتکل RIP یک بسته اطلاعاتی درون بسته دیگری کپسوله نمی‌شود بلکه مسیریابی مبتنی بر Header بسته IP یا IPX انجام می‌شود. مسیریاب با دریافت بسته، ابتدا Header بسته را می‌خواند. سپس فیلد آدرس مقصد آن استخراج می‌شود و در صورت نیاز به مسیریابی، RIP مسیرهای ممکن تا رسیدن به مقصد را در جدول مسیریابی جستجو می‌کند. اگر بیش از یک مسیر وجود داشت مسیر کم هزینه‌تر انتخاب می‌شود. سپس RIP فیلد TTL بسته IP را تغییر داده و بسته را به مقصد می‌فرستد.

RIP پروتکلی است با سرعت بالا و عدم پیچیدگی و عملیاتی بودن که برای محیطهای کوچک و یک‌دست طراحی شده و دارای محدودیت‌های فراوان و قابلیت‌های کمی است. لذا با افزودن به قابلیت‌های آن پروتکل IGRP به وجود آمد.

آدرس‌دهی و مسیریابی

پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی

دستورات نمونه پیاده‌سازی RIPv2

```
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.0.0.0
Router(config-router)#network 172.16.0.0
Router(config-router)#network 192.168.111.0
```


آدرس‌دهی و مسیریابی

پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی

پروتکل OSPF از الگوریتم LS برای محاسبه بهترین مسیر استفاده می‌کند.

هزینه Cost هر لینک از تقسیم ۱۰۸ بر پهنای باند آن لینک به دست می‌آید.

هنگام خرابی یک مسیریاب، جداول مسیریابی به سرعت همگرا می‌شوند.

در OSPF موازنه بار انجام می‌شود و نیز از مسیریابی سلسله مراتبی پشتیبانی می‌شود.

در OSPF شبکه Areaبندی می‌شود و Routing Tableها فقط کافی است Area مربوط به خود را بشناسند نه همبندی کل شبکه را.

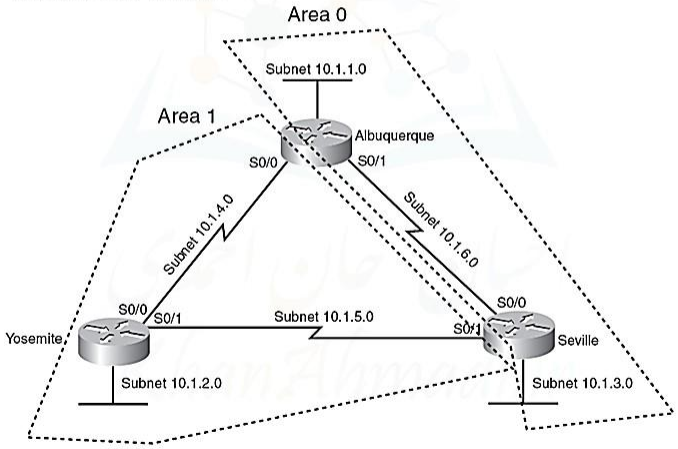
بر خلاف RIP، به‌روزرسانی به صورت Partial update است نه Full update و هر تغییری اتفاق بیفتد، فقط مسیریاب‌های همان Areaی مورد تغییر، الگوریتم را دوباره محاسبه می‌کنند و مسیریاب‌های دیگر Areaها هیچ عکس‌العملی نشان نمی‌دهند.

آدرس‌دهی و مسیریابی

پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی

OSPF

Multiarea OSPF Network



آدرس‌دهی و مسیریابی

پیاده‌سازی الگوریتم‌ها و پروتکل‌های مسیریابی

دستورات نمونه پیاده‌سازی OSPF

```
R1-Albuquerque(config)#interface fastEthernet 0/0
R1-Albuquerque(config-if)#ip address 10.1.1.1 255.255.255.0
R1-Albuquerque(config)#interface serial 0/0/0
R1-Albuquerque(config-if)#ip address 10.1.4.1 255.255.255.0
R1-Albuquerque(config-if)#interface serial 0/0/1
R1-Albuquerque(config-if)#ip address 10.1.6.1 255.255.255.0
R1-Albuquerque(config-if)#exit
R1-Albuquerque(config)#router ospf 1
R1-Albuquerque(config-router)#network 10.0.0.0 0.255.255.255 area 0
R1-Albuquerque(config-router)#network 10.1.1.1 0.0.0.0 area 0
R1-Albuquerque(config-router)#network 10.1.4.1 0.0.0.0 area 1
R1-Albuquerque(config-router)#network 10.1.6.1 0.0.0.0 area 0
```

آدرس‌دهی و مسیریابی

اعمال فیلترها در TCPdump و Wireshark Assignment

TCPdump و Wireshark دو ابزار قدرتمند برای تحلیل و نظارت بر ترافیک شبکه هستند. این دو ابزار به کاربران اجازه می‌دهند تا بسته‌های شبکه را ضبط و فیلتر کنند تا اطلاعات مورد نیاز خود را استخراج کنند.

استفاده از فیلترها در TCPdump و Wireshark کمک می‌کند تا ترافیک شبکه به طور مؤثری مدیریت شود و اطلاعات مورد نیاز سریع‌تر استخراج شود. با تسلط بر این ابزارها و فیلترهای آن‌ها، می‌توان تحلیل‌های دقیق‌تری از وضعیت شبکه داشت.

TCPdump برای سیستم‌عامل‌های مبتنی بر UNIX طراحی شده است، اما برای کاربران ویندوز، ابزار WinDump وجود دارد که شبیه قابلیت‌های TCPdump را ارائه می‌دهد. برای استفاده از WinDump می‌توان از وبگاه WinPcap برنامه و مستندات را بارگیری کرد.

آدرس‌دهی و مسیریابی

اعمال فیلترها در TCPdump و Wireshark Assignment

TCPdump ابزاری خط فرمانی مبتنی بر UNIX است که امکان می‌دهد تا بسته‌های شبکه ضبط و فیلتر شوند. TCPdump و به کاربران اجازه می‌دهد بسته‌های داده را در شبکه‌های رایانه‌ای مشاهده کنند. قبل از استفاده از TCPdump، باید آن را بر روی سیستم نصب کرد. در اکثر توزیع‌های لینوکس، می‌توان از مدیر بسته استفاده کرد:

برای توزیع‌های مبتنی بر دبیان #sudo apt-get install tcpdump

برای توزیع‌های مبتنی بر ردهت #sudo yum install tcpdump

دستور کلی: tcpdump [options] [filters]

فیلترهای رایج در TCPdump:

فیلتر مبتنی بر پروتکل:

برای ضبط بسته‌های TCP	tcpdump -i any tcp
برای ضبط بسته‌های UDP	tcpdump -i any udp

آدرس‌دهی و مسیریابی

اعمال فیلترها در TCPdump و Wireshark Assignment

فیلتر آدرس IP و ضبط ترافیک یک هاست خاص: tcpdump -i any host 192.168.1.100

فیلتر بر اساس پورت و ضبط ترافیک از یک پورت خاص:

tcpdump -i any port 80

فیلتر ترکیبی:

استفاده از از عملگرهای منطقی برای ترکیب چند فیلتر:

tcpdump -i any src 192.168.1.100 and port 80

ذخیره خروجی در فایل:

برای ذخیره ترافیک در یک فایل pcap:

tcpdump -i any -w output.pcap

برای خواندن و تحلیل فایل ذخیره شده:

tcpdump -r output.pcap

آدرس‌دهی و مسیریابی

اعمال فیلترها در TCPdump و Wireshark Assignment

Wireshark یک ابزار گرافیکی است که امکان می‌دهد تا بسته‌های شبکه قابل مشاهده و تحلیل شوند. فیلترهای Wireshark به دو دسته تقسیم می‌شوند: فیلترهای نمایش و فیلترهای ضبط.

فیلترهای نمایش:

این فیلترها پس از ضبط بسته‌ها، برای محدود کردن نمایش آن‌ها استفاده می‌شوند. مثال:

tcpdump -ni igb1 tcp port 80

فیلترهای ضبط:

این فیلترها قبل از شروع ضبط بسته‌ها اعمال می‌شوند. مثال: ضبط ترافیک TCP از نشانی خاص:

tcpdump tcp and host 192.168.1.100

```
# tcpdump -ni igb1 -T carp -c 2 carp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on igb1, link-type EN10MB (Ethernet), capture size 65535 bytes
14:50:07.426993 IP 198.51.100.12 > 224.0.0.18: CARPv2-advertise 36: vhid=11 advbase=1
   advskew=0 authlen=7 counter=5449924379588860810
14:50:08.436849 IP 198.51.100.12 > 224.0.0.18: CARPv2-advertise 36: vhid=11 advbase=1
   advskew=0 authlen=7 counter=5449924379588860810
2 packets captured
78 packets received by filter
0 packets dropped by kernel
```

آدرس‌دهی و مسیریابی

ARP، مسیریابی IP و ابزارهای عیب‌یابی

ARP (Address Resolution Protocol)

ARP یک پروتکل شبکه است که برای تبدیل نشانی‌های IP به نشانی‌های MAC در شبکه‌های محلی LAN استفاده می‌شود. این پروتکل به دستگاه‌ها کمک می‌کند تا نشانی سخت‌افزاری MAC یک دستگاه دیگر را با توجه به نشانی IP آن پیدا کنند.

مراحل عملکرد ARP:

۱. ارسال درخواست ARP: زمانی که یک دستگاه نیاز به ارسال داده به یک نشانی IP خاص دارد، یک پیام درخواست ARP به شبکه می‌فرستد.

۲. پاسخ ARP: دستگاهی که نشانی IP مورد نظر را دارد، پاسخ می‌دهد و نشانی MAC خود را به فرستنده ارسال می‌کند.

۳. ذخیره‌سازی اطلاعات: دستگاه فرستنده نشانی MAC را در جدول ARP خود ذخیره می‌کند تا برای ارتباطات بعدی نیاز به ارسال مجدد درخواست نداشته باشد.

آدرس‌دهی و مسیریابی

ARP، مسیریابی IP و ابزارهای عیب‌یابی

ابزارهای عیب‌یابی

برای شناسایی و حل مشکلات مربوط به ARP و مسیریابی IP، ابزارهای مختلفی وجود دارند که شامل موارد زیر هستند:

Ping: بررسی دسترسی بین دو دستگاه در شبکه و اندازه‌گیری زمان رفت و برگشت بسته‌ها.

Traceroute/Tracert: شناسایی مسیر بسته‌ها از مبدا تا مقصد و نمایش زمان تأخیر در هر Hop.

pathping khanahmadi.ir: شبیه Tracert عمل می‌کند.

ARP –a: این دستور در سیستم‌های ویندوزی برای نمایش جدول ARP و مشاهده ارتباطات بین نشانی‌های IP و MAC استفاده می‌شود.

TCPdump: ابزاری مبتنی بر UNIX خط فرمانی برای ضبط ترافیک شبکه و تحلیل بسته‌ها، که می‌تواند برای بررسی مشکلات مربوط به ARP و مسیریابی استفاده شود.

Wireshark: ابزاری گرافیکی برای تجزیه و تحلیل ترافیک شبکه که امکان مشاهده جزئیات بسته‌ها و فیلتر کردن آن‌ها را فراهم می‌کند.

آدرس‌دهی و مسیریابی

ARP، مسیریابی IP و ابزارهای عیب‌یابی

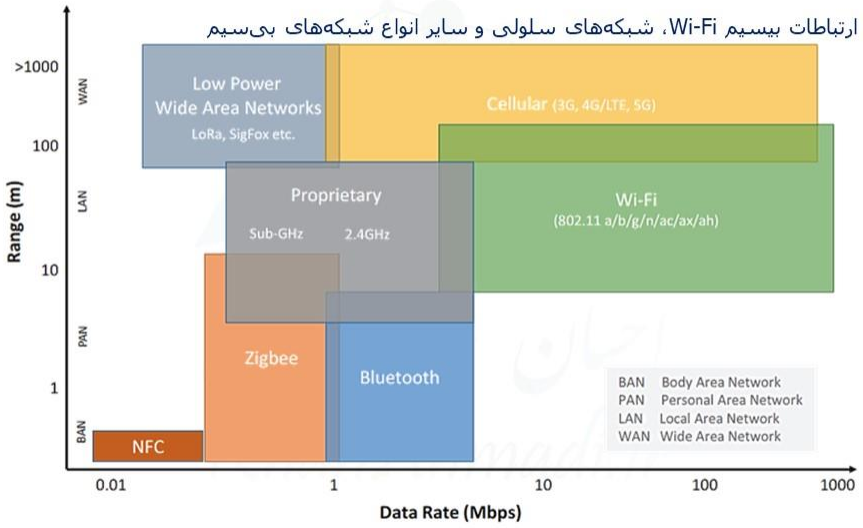
مثال ابزارهای عیب‌یابی: Tracert و ARP –a

```
C:\>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168
  2     4 ms     7 ms     1 ms  n41-akl
  3     1 ms     1 ms     1 ms  ae3-130
  4    24 ms    24 ms    25 ms  xe-4-0-
  5    24 ms    24 ms    24 ms  as15169
  6    25 ms    25 ms    25 ms  216.239
  7    25 ms    25 ms    25 ms  216.239
  8    25 ms    25 ms    25 ms  google-

Trace complete.
```

```
C:\WINDOWS\system32>arp -a

Interface: 10.0.0.9 --- 0x4
  Internet Address      Physical Address      Type
  10.0.0.1              10-56-11-c8-6a-9a     dynamic
  10.0.0.48             be-c5-bb-0a-ed-f8     dynamic
  10.0.0.153            7a-aa-ab-0b-c3-fa     dynamic
  10.0.0.204            00-04-7d-0d-d7-b1     dynamic
  10.0.0.251            fa-7b-8c-a6-b7-bc     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  169.254.185.26        e0-37-17-ea-11-5e     dynamic
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```


شبکه های بی سیم

ارتباطات بیسیم Wi-Fi، شبکه‌های سلولی و سایر انواع شبکه‌های بی‌سیم



شبکه های بی سیم

شبکه‌های بی‌سیم

نوعی از شبکه‌های رایانه‌ای هستند که در آن‌ها ارتباط بین اجزاء شبکه بدون استفاده از کابل و سیم برقرار می‌شود. این نوع شبکه‌ها به کمک امواج الکترومغناطیسی، مانند امواج رادیویی، مادون قرمز و مایکروویو، داده‌ها را منتقل می‌کنند.

ویژگی‌ها:

- عدم نیاز به سیم و کابل‌کشی موجب کاهش هزینه‌ها و سهولت در نصب و گسترش می‌شود.
- انعطاف‌پذیری دارد و کاربران می‌توانند به راحتی در فضا حرکت کنند.
- سرعت انتقال داده کمتر از کابلی است اما پیشرفت‌های چشم‌گیری در راه است.
- مواجه با چالش‌های امنیتی، تداخل سیگنال و محدوده پوشش محدود و تأثیر موانع

انواع شبکه‌های بی‌سیم:

- شبکه‌های محلی بی‌سیم WLAN مانند Wi-Fi
- شبکه‌های شخصی بی‌سیم WPAN مانند Bluetooth و Zigbee
- شبکه‌های سلولی مانند تلفن همراه
- شبکه‌های حسگر بی‌سیم مانند حسگر جمع‌آوری اطلاعات از محیط صنعتی و محیط زیست
- شبکه‌های ماهواره‌ای برای ارتباطات جهانی شامل ایستگاه‌های زمینی و ماهواره‌ها

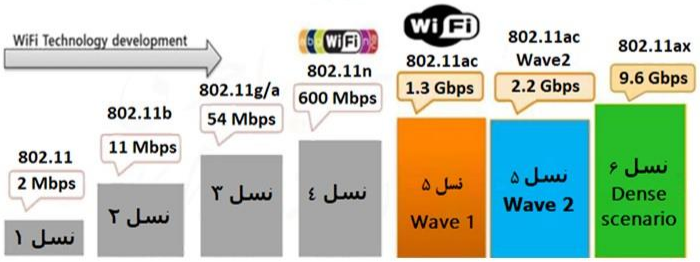
شبکه های بی سیم

ارتباطات بی‌سیم Wi-Fi

Wi-Fi از پرکاربردترین فناوری‌های ارتباطات بی‌سیم است. این فناوری از امواج رادیویی برای انتقال داده‌ها استفاده می‌کند و معمولاً در فرکانس‌های ۲٫۴ گیگاهرتز و ۵ گیگاهرتز عمل می‌کند.

ویژگی‌های Wi-Fi

عدم نیاز به کابل، پوشش‌دهی گسترده محل کار کوچک یا خانه و وسیع‌تر نسبت به بلوتوث، سرعت بالای استانداردهای جدید Wi-Fi مانند 802.11ac و 802.11ax در دسترسند.



شبکه های بی سیم

شبکه‌های سلولی

شبکه‌های سلولی Cellular Networks برای ارتباطات صوتی و داده‌ای در دستگاه‌های موبایل استفاده می‌شوند. با پیشرفت فناوری و ظهور نسل‌های جدید، این شبکه‌ها موجب افزایش دسترسی و راحتی کاربران شده است.

ساختار شبکه‌های سلولی

شبکه‌های سلولی به نواحی جغرافیایی تقسیم می‌شوند که به آن‌ها "سلول" گفته می‌شود. هر سلول معمولاً توسط یک ایستگاه پایه Base Transceiver Station یا BTS پوشش داده می‌شود که مسئول ارسال و دریافت سیگنال‌ها از و به دستگاه‌های موبایل است. این سلول‌ها معمولاً به صورت شش‌ضلعی (مدل لانه زنبوری) طراحی می‌شوند تا حداکثر پوشش را فراهم کنند.

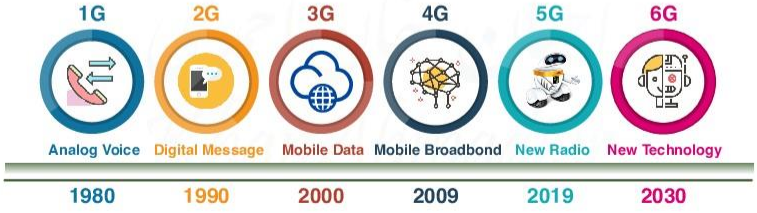
کنترل‌کننده ایستگاه پایه BSC مسئول مدیریت چندین ایستگاه پایه و تخصیص منابع رادیویی است.

مرکز سوئیچینگ MSC وظیفه مدیریت تماس‌ها و انتقال داده‌ها را بر عهده دارد.

شبکه های بی سیم

شبکه‌های سلولی: نسل‌های مختلف شبکه‌های سلولی

- نسل اول 1G: در دهه ۱۹۸۰ آنالوگ عمل می‌کرد. خدمات آن محدود به تماس‌های صوتی بود.
- نسل دوم 2G: با فناوری رقومی امکان ارسال متن و داده فراهم شد. این نسل شامل سامانه‌های رقومی GSM (Global System Mobile) شد.
- نسل سوم 3G: با هدف ارائه سرعت بالاتر برای انتقال داده‌ها و خدمات چندرسانه‌ای توسعه یافت. WCDMA (Wideband Code Division Multiplexing Access) در این نسل استفاده شد.
- نسل چهارم 4G: بر پایه IP دسترسی سریع‌تر به اینترنت و خدمات چندرسانه‌ای را فراهم کرد.
- نسل پنجم 5G: ارائه سرعت بالاتر، تأخیر کمتر و امنیت پیشرفته و زیستی
- نسل ششم 6G: در حال تحقیق و توسعه برای سرعت ۱ ترابیت بر ثانیه و تأخیر کمتر از 1ms



شبکه های بی سیم

رسانه و عملکرد

رسانه شبکه‌های بی‌سیم

- امواج رادیویی: رایج‌ترین روش انتقال داده‌ها در شبکه‌های بی‌سیم مانند Wi-Fi
- مادون قرمز: برای ارتباطات کوتاه‌برد مانند کنترل‌های از راه دور و برخی از دستگاه‌های بی‌سیم
- مایکروویو: برای فواصل دورتر مانند ارتباطات ماهواره‌ای یا بین ساختمان‌ها
- FSO (Free-space optical communication): انتقال داده با نور در فضای آزاد

عملکرد شبکه‌های بی‌سیم برای انتقال داده با استفاده از امواج الکترومغناطیسی

- تبدیل داده‌ها از رقومی الکتریکی به سیگنال‌های رادیویی
- انتقال سیگنال از طریق یک مودم یا مسیریاب به دستگاه‌های مختلف
- دریافت سیگنال دستگاه‌های کاربر و تبدیل آن‌ها به داده‌های رقومی الکتریکی

شبکه های بی سیم

قدرت سیگنال

قدرت سیگنال در شبکه‌های بی‌سیم یکی از عوامل کلیدی است که تأثیر مستقیمی بر کیفیت و سرعت اتصال دستگاه‌ها دارد. واحد اندازه‌گیری قدرت سیگنال بی‌سیم dBm دسیبل میلی‌وات است و مقادیر آن به صورت منفی بیان می‌شوند.

مورد نیاز برای:	کیفیت مورد انتظار	قدرت سیگنال
بازی و تلویزیون 4K	بیشترین مقدار سیگنال قابل دستیابی	-30 dBm
تماشای ویدیوهای HD	قدرت سیگنال عالی	-50 dBm
تماشای ویدیوهای SD	قدرت سیگنال خوب و قابل اعتماد	-60 dBm
کمینه قدریت برای فعالیت برخط بسته به پایداری سیگنال مانند تماس صوتی بر بستر Wi-Fi یا گوش دادن صوت	قدرت سیگنال قابل اعتماد	-67 dBm
مرور اینترنت در حد کم و ارسال و دریافت ایمیل‌های کم حجم	قوی نبودن قدرت سیگنال	-70 dBm
اتصال به یک شبکه	قدرت سیگنال غیر قابل اعتماد و ناکافی برای اکثر فعالیت‌های آنلاین	-80 dBm
	شانس متصل شدن هم خیلی کم	-90 dBm

شبکه های بی سیم

قدرت سیگنال

عوامل مؤثر بر قدرت سیگنال

- موانع فیزیکی مانند دیوارها، درها و وسایل باعث کاهش قدرت سیگنال می‌شوند
- تعداد دستگاه‌های متصل هر چه بیشتر باشد، قدرت سیگنال و کیفیت کاهش می‌یابد
- نوع آنتن مورد استفاده تأثیر زیادی بر قدرت سیگنال دارد
- تداخل فرکانسی در صورت وجود دستگاه‌های دیگر که از فرکانس مشابه استفاده می‌کنند، می‌تواند باعث تداخل در سیگنال شود و کیفیت ارتباط را کاهش دهند.

نحوه اندازه‌گیری قدرت سیگنال

- برای اندازه‌گیری قدرت سیگنال دریافتی، می‌توان از نرم‌افزارهای پایش Wi-Fi استفاده کرد که مقدار RSSI (Received Signal Strength Indicator) را نشان می‌دهند.
- در ویندوز از دستور netsh wlan show interface و نرم‌افزارهای مختلف بهره برده می‌شود.

شبکه های بی سیم

فشرده‌سازی و تشخیص سیگنال بی‌سیم

فشرده‌سازی سیگنال

به معنای کاهش حجم داده‌ها بدون از دست رفتن کیفیت اطلاعات است. این روش در شبکه‌های حسگر بی‌سیم WSN که محدودیت منابع انرژی و پهنای باند دارند، کاربرد دارد.

روش‌های فشرده‌سازی:

- در فشرده‌سازی مبتنی بر سنجش فشرده Compressed Sensing به جمع‌آوری داده‌ها از طریق نمونه‌برداری کمتر از نرخ نایکوئیست می‌پردازد و امکان بازیابی سیگنال را با کیفیت بالا فراهم می‌کند. این تکنیک به ویژه برای سیگنال‌های تنک sparse signals مناسب است.
- در روش PCA (تحلیل مؤلفه‌های اصلی) با کاهش ابعاد و فشرده‌سازی داده‌ها می‌توان ویژگی‌های فضایی و زمانی سیگنال‌ها را استخراج کرد.

شبکه های بی سیم

فشرده‌سازی و تشخیص سیگنال بی‌سیم

تشخیص سیگنال

تشخیص سیگنال به فرآیند شناسایی و استخراج اطلاعات از سیگنال‌های دریافتی اشاره دارد.

فرآیند:

- جمع‌آوری داده توسط حسگرها از محیط و ارسال به مرکز پردازش
- تحلیل داده پس از دریافت داده‌ها با الگوریتم‌های تحلیل برای شناسایی ویژگی‌های سیگنال
- بازیابی سیگنال با استفاده از روش‌هایی مانند سنجش فشرده

چالش‌ها و مسائل تحقیقاتی

- کیفیت بازسازی سیگنال و افت کیفیت در حد قابل قبولی
- به دلیل تداخل و ازدست رفتن بسته‌ها نیازمند پروتکل‌های robust برای مدیریت مشکلات

شبکه های بی سیم

تأخیر

تأخیر مدت زمانی است که اطلاعات از یک دستگاه به دستگاه دیگر منتقل می‌شوند و زمانی که این اطلاعات در مقصد نمایش داده می‌شوند. کمینه کردن تأخیر در کاربردهایی مانند بازی‌های آنلاین، تماس‌های صوتی و ویدئویی و برنامه‌های کاربردی حساس به زمان اهمیت دارد.

عوامل مؤثر بر تأخیر:

- فاصله فیزیکی بین دستگاه‌ها بیشتر، زمان لازم برای ارسال و دریافت داده‌ها نیز بیشتر
- ترافیک شبکه باعث افزایش تأخیر (تعداد زیاد دستگاه‌ها همزمان ارسال کنند)
- ظرفیت محدود شبکه باعث تشدید تأخیر
- تجهیزات شبکه قدیمی یا کم‌کیفیت باعث افزایش تأخیر
- تداخل سیگنال الکترومغناطیسی یا تداخل‌های دیگر باعث اختلال در ارتباطات و افزایش تأخیر
- از دست رفتن بسته Packet Loss نیاز به ارسال مجدد ایجاد کرده که منجر به افزایش تأخیر
- رزولوشن DNS یعنی مدت زمانی که طول می‌کشد تا نام دامنه به آدرس IP تبدیل شود

شبکه های بی سیم

تأخیر

راهکارهای کاهش تأخیر

- بهینه‌سازی پیکربندی شبکه با تجهیزات به‌روز و پیکربندی درست
- استفاده از شبکه‌های توزیع محتوا CDN برای دریافت محتوا از نزدیک‌ترین سرور به کاربر
- تغییر اتصال اینترنت با پهنای باند کافی
- پایش مستمر بر عملکرد شبکه برای شناسایی مشکلات و تغییرات

شبکه های بی سیم

از دست دادن توان عملیاتی

از دست دادن توان عملیاتی در شبکه‌های بی‌سیم به کاهش کارایی و سرعت انتقال داده‌ها به ویژه در شبکه‌های بی‌سیم متحرک و با شرایط متغیر محیطی منجر می‌شود.

علل از دست دادن توان عملیاتی

- گم شدن بسته‌ها به دلیل تداخل سیگنال، ازدحام شبکه و خطاهای انتقال ناشی از مشکلات فیزیکی مانند موانع یا تداخل فرکانسی
- ازدحام شبکه که تعداد زیادی از دستگاه‌ها به طور همزمان داده‌ها را ارسال کنند
- قدرت سیگنال ضعیف، احتمال گم شدن و نیاز به ارسال دوباره بسته‌ها را افزایش می‌دهد
- نوع پروتکل‌های انتقال مانند TCP رفتارهای متفاوتی در مواجهه با گم شدن بسته‌ها دارند

اثرات از دست دادن توان عملیاتی: کاهش سرعت انتقال، افزایش تأخیر و کاهش کیفیت خدمات

راهکارهای بهبود توان عملیاتی:

- استفاده از پروتکل‌های مناسب، بهینه‌سازی زیرساخت‌ها، مدیریت ترافیک برای جلوگیری از ازدحام، افزایش قدرت سیگنال و طراحی پوشش مناسب و کاهش نقاط مرده در شبکه

شبکه های بی سیم

طراحی شبکه‌های بی‌سیم و موبایل به صورت عملی

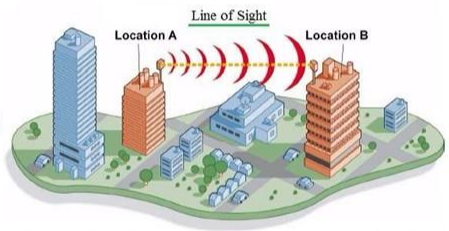
طراحی شبکه‌های بی‌سیم و موبایل نیازمند درک عمیق از اصول فنی، نیازهای کاربران و چالش‌های محیطی است.

مراحل طراحی شبکه‌های بی‌سیم

۱) تحلیل و شناسایی نیازهای کاربران و نوع خدمات مورد نظر (اینترنت، VoIP، ویدیو کنفرانس) و تعداد دستگاه‌ها و نوع ترافیک مورد انتظار
۲) Site Survey و بررسی محل با بازدید و شناسایی چالش‌های محیطی و موانع فیزیکی (دیوارها، سقف‌ها) و استفاده از ابزارهای اندازه‌گیری تعیین قدرت سیگنال و نقاط کور
۳) انتخاب تجهیزات Access Pointها، آنتن‌ها و دیگر تجهیزات مناسب(مسیریاب‌ها، سوئیچ‌ها).
۴) طراحی منطقی و فیزیکی شامل هم‌بندی مناسب و قرار دادن APها در مکان‌های مناسب
۵) استفاده از نرم‌افزارهای طراحی بی‌سیم برای تحلیل پوشش و شناسایی نقاط کور
۶) پیاده‌سازی و نصب تجهیزات باکیفیت و اجرای و پیکربندی حرفه‌ای تجهیزات و کابل‌کشی‌ها
۷) آزمایش و عیب‌یابی عملکرد شبکه پس از نصب و انجام تنظیمات لازم
۸) نگهداری و اعمال بهبود با نظارت بر عملکرد شبکه و انجام بهینه‌سازی‌های مستمر و ارتقاء

سیگنال‌های بی‌سیم و Line Of Sight (LOS)

- سیگنال‌های بی‌سیم در مسیر حرکت از انتقال‌دهنده به دریافت‌کننده، مستقیم و به صورت یک خط راست حرکت می‌کنند.
- به این نوع از انتشار، Line Of Sight (LOS) یا خط دید افقی می‌گویند.

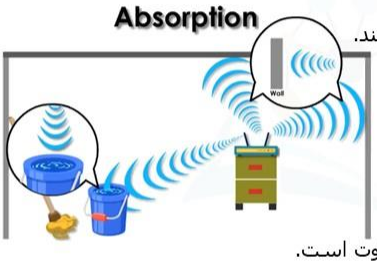


- LOS از حداقل انرژی استفاده می‌کند و منجر به دریافت واضح‌ترین سیگنال ممکن می‌شود.
- حداکثر توان (Throughput) از نظر تئوری برابر 54 Mbps است اما توان مؤثر حدود نصف یا یک سوم این مقدار است.

عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

۱) جذب (Absorption): بعضی از مواد قدرت سیگنال‌های بی‌سیم را کاهش می‌دهند و همه انرژی بالقوه آن را می‌گیرند.

- دیوارهای آجری و آب دو جذب‌کننده بزرگ هستند.



- میزان جذب سیگنال در انواع مختلف دیوار متفاوت است.

عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

۲) انعکاس (Reflection): وقتی امواج الکترومغناطیس با مانعی روبرو می‌شوند و به سمت منبع خود بازمی‌گردند، سیگنال از دست می‌رود (Loss می‌شود)

- در شکل، کامپیوتر سیگنال را بطور غیرمستقیم با انعکاس از طریق سقف دریافت می‌کند.
  - بعضی از سیگنالها توسط سقف جذب می‌شوند.
  - بعضی از سیگنالها به سمت منبع خود بازمی‌گردند.

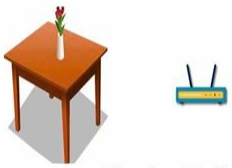
- بنابراین ارتباط بین کامپیوتر و مسیریاب بی‌سیم تحت تأثیر قرار می‌گیرد.

عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

- **نکته:** انعکاس سیگنالهای بی‌سیم لزوماً بد نیست.
- داخل یک اتاق، انعکاس به سیگنالها کمک می‌کند تا در نهایت به مقصد برسند.
- اگر تمام سیگنالها در مسیر با دیوار برخورد کنند و انعکاس وجود نداشته باشد، در این حالت کامپیوتر هیچ سیگنالی دریافت نمی‌کند.

عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

۳) انکسار (Diffraction): هنگامی رخ می‌دهد که یک موج الکترومغناطیس با مانعی برخورد کرده و به امواج ثانویه تقسیم شود. امواج ثانویه در جهتی که تقسیم شده بودند، منتشر می‌شوند.



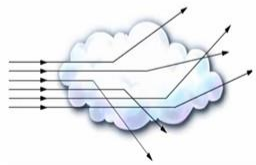
- اگر سیگنالهای بی‌سیم در حال انکسار قابل دیدن بودند، به نظر می‌رسید که آنها به اطراف مانع خم می‌شوند.
- اشیاء دارای دیواره‌های شفاف، می‌توانند موجب انکسار امواج شوند.

عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

۴) پراکنده شدن (Scattering): پراکندگی یعنی انتشار سیگنال بی‌سیم در هنگام برخورد با اشیایی که سطح ناهمواری دارند.

- با تابش چراغ قوه به یک توپ آینه‌ای نیز پراکندگی رخ می‌دهد.

- هنگام برخورد با سطوح زبر یا ناهموار، سیگنال اصلی به صورت چند سیگنال بازتابی از هم می‌پاشد.
- این پدیده می‌تواند منجر به ایجاد چند سیگنال ضعیف‌تر یا از دست رفتن سیگنال شود.
- برگ گیاهان، گرد و خاک، دود یا قطرات ریز آب در هوا می‌توانند بخش‌هایی از سیگنال را پراکنده کنند.



عوامل تضعیف یا گم شدن سیگنال‌های بی‌سیم

۵) تداخل (Interference): انواع لوازم خانگی مانند تلفن‌های بی‌سیم، مانیتورهای کوچک و ماکروفرها می‌توانند ایجاد تداخل کنند.

- هروسیله‌ای که با فرکانس 2.4 GHz ارتباط برقرار کند، می‌تواند با سیگنالهای Wi-Fi در خانه ایجاد تداخل کند.

امید است این فایل برای خوانندگان مفید بوده باشد.
خوشحال می‌شوم اشکالات و انتقادات را برای اینجانب بفرستید.

اطلاعات تماس در سایت شخصی بنده موجود است.

www.khanahmadi.ir

خان احمدی
مدرس دروس امنیت، شبکه و مدیریت فناوری اطلاعات