مقدمه ای بر

نصب و پیکربندی تجهیزات شبکه

introduction to

Installation and Configuration of Network Equipment

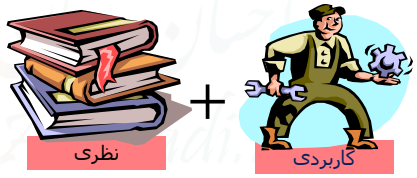
نسخه ۳٫۷

دوره مهندسی فناوری شبکه‌های رایانه‌ای

مدرس: احسان خان احمدی

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

خصوصیات دوره



یادداشت برداری مهم است

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 «نصب و پیکربندی تجهیزات شبکه» مهیا شود:

- یک لغت‌نامه خوب برای مطالعه و ترجمه اصطلاحات تخصصی
- تخته سفید، فراتاب، تجهیزات مورد نیاز راه‌اندازی شبکه
- مرور و مطالعه پیش‌نیاز: شبکه‌های پیشرفته رایانه‌ای

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

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

نکته۱: مواردی که به زبان غیر از فارسی آمده است، در کلاس به فارسی تشریح می‌شود.

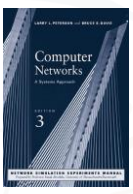
نکته۲: از همه‌ی محتوای ارائه شده در کلاس یادداشت برداری شود.

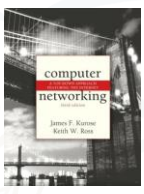
منابع کمکی

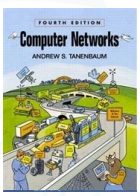
۱. **فناوری شبکه**، عطا الهی، مترجم علی اصغر الهی، انتشارات ناقوس

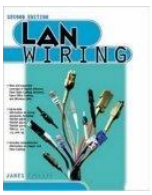
۲. **مهندسی اینترنت**، ملکیان، انتشارات ناقوس

3. Peterson L, Dave B., **Computer Networks: A system Approach**, 3rd Edition, 2003, Publisher: Morgan Kaufmann.
4. Kurose, James F., Ross, Keith W., **Computer Networking: A Top-Down Approach Featuring the Internet**, Addison Wesley; 3rd edition (May 13, 2004)
5. Tanenbaum Andrew S., **Computer Networks,** 4th Edition, 2003, Prentice Hall
6. Trulove James, **LAN Writing**, McGrow Hill





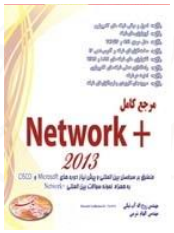


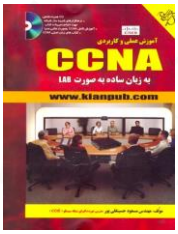


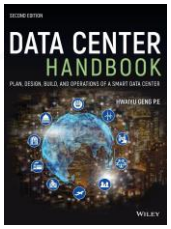
- نرم افزار شبیه‌ساز شبکه: Cisco Packet Tracer 6.2

منابع کمکی

- کتاب‌های کمکی:
  - شبکه‌های کامپیوتری و کارگاه، انتشارات کیان رایانه
  - Network+
  - CCNA
  - **Data Center Handbook**: Plan, Design, Build, and Operations of a Smart Data Center







انتظارات، فعالیت‌های کلاسی و نمره نهایی

نمره نهایی از ارزیابی دانشجو مبتنی بر شاخص‌های زیر انجام می‌شود:

- **نمره میان‌نیمسال و ارزیابی فعالیت‌های مستمر و مشاهده رفتار**
  - آمادگی هر جلسه برای مرور مطالبی که از ابتدای نیم‌سال مطرح شده، چند Quiz در طول نیم‌سال
  - حل تمرین‌ها، پوشه کار و ارائه گزارش
- **آزمون کتبی**
- **ارائه پروژه و ارائه پرونجای مطالعه شده و پرونجای ویدئویی توضیح پروژه با رعایت نکات زیر:**
  - به تایید رساندن موضوع پرونجای 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 پرونجای مطالعه شده با قالب مشخص شده در صفحه بعد به صورت PPT (نام پرونجا همان نام دانشجو – نام درس به انگلیسی باشد) و ارسال به مدرس
  - دست کم نیمی از نمره پرونجای مطالعه شده مربوط به «**چکیده آنچه فرا گرفتم و پرسش و پاسخ**» است که باید توسط دانشجو پس از مطالعه متن پرونجای مطالعه شده، آن مقدار که فرا گرفته نگاشته شود.
  - ارسال یک ویدئوی حدود ده دقیقه‌ای از ارائه پرونجای PowerPoint با تأکید بر تشریح مطالب اصلی درس
  - **بیشینه زمان ارسال پرونجاهای مطالعه شده و ویدئو به مدرس:**
    - **پیش از آزمون میان نیم‌سال: تا پایان فصل اول و سه جلسه پیش از جلسه آخر: پرونجای کامل**
  - Subject شامل مشخصات فردی و دانشگاهی، درس، روز و ساعت کلاس باشد

مثال Subject: دانشگاه انفورماتیک ایران، امین نصاب، نصب و پیکربندی تجهیزات شبکه، پنج‌شنبه ۱۸:۰۰-۱۶:۰۰

نمونه‌ی نام پرونجا: NetImp-Amin-Nassab.ppt

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

ارزیابی اصلی در طول نیم‌سال انجام می‌شود

قالب مستندات پروژه PPT

قلم و اندازه: Tahoma
- عنوان‌ها Bold 28 or 24، (متن نمابرگ‌ها Normal 14 تا Normal 16 به صلاح‌دید فراگیر)
- درج **شماره نمابرگ** و **عنوان** برای همه‌ی نمابرگ‌های پرونده‌جا 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 تأیید 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/iJEB4 یا KhanAhmadi.ir

نصب و پیکربندی تجهیزات شبکه

مباحث اصلی

۱) طراحی زیرساخت شبکه
۲) خدمات کابل‌کشی شبکه
۳) طراحی اتاق و تجهیزات پایش شبکه
۴) اتصالات دوربین‌های شبکه و اتصال به شبکه آن
۵) کابل‌کشی برق و اتصالات برق تجهیزات
۶) نصب و راه‌اندازی تجهیزات برق اضطراری UPS
۷) نصب و راه‌اندازی سامانه و تجهیزات مرکزی تلفن
۸) نصب سامانه‌های امنیتی و دیوارآتش‌های سخت‌افزاری
۹) نصب تجهیزات استقرار سرور، طراحی و نصب رک‌ها
۱۰) نصب و راه‌اندازی سامانه‌های ورود و خروج
۱۱) نصب سوئیچ‌ها، مسیریاب‌ها و کانکتورهای شبکه برای اتصال بخش‌های مختلف به یکدیگر
۲۱) راه‌اندازی تجهیزات اتاق‌سرور و تجهیزات نگهداری از اتاق‌سرور
۳۱) نصب و راه‌اندازی تجهیزات شبکه‌های بی‌سیم
۴۱) آزمایش و عیب‌یابی تجهیزات شبکه

یادآوری تعریف شبکه، شبکه ارتباطی، شبکه‌های رایانه‌ای

- فناوری کلیدی قرن بیستم
- تعاریف اولیه
  - سامانه‌های منفرد یا Single Systems: تمرکز منابع محدود روی یک دستگاه مستقل
  - سامانه‌های چندکاربره یا Multi User Systems: دسترسی چند کاربر به سامانه
  - شبکه‌های رایانه‌ای یا Computer Networks
    - تعدادی رایانه متصل بهم به شرط استقلال سیستم‌ها، فناوری واحد، تبادل داده
    - طراحی قابلیت اطمینان، اشتراک منابع، ملاحظات امنیتی
  - عوامل ارتباطی شبکه‌ها
    - کابلی(مسی، فیبر نوری) و بی‌سیم(ماکروویو، مادون قرمز و ...)
  - Distributed System: یک سامانه متجانس شامل مجموعه رایانه‌های مستقل، پیاده‌سازی توسط یک لایه نرم افزاری Middleware
- پیوند رایانه و مخابرات
- شبکه رایانه‌ای و سامانه توزیع شده
  - نیاز هر دو به انتقال فایل (داده)
  - در شبکه: ملموس بودن تفاوت سخت افزار و نرم افزار، Log on to Computer
  - در Distributed System: اجرای نرم افزار روی شبکه
- وب World Wide Web: شبکه یا یک سیستم توزیعی؟

کاربردهای شبکه‌های کامپیوتری

- **Business Applications**
- **Home Applications**
- **Mobile Users**
- **Social Issues**

کاربردهای شبکه‌های کامپیوتری(کاربردهای تجاری)

- منابع قابل اشتراک Resource Sharing

پاسخ را تا جلسه آینده آماده کنید...

در کلاس مثال‌های مختلفی ارائه و نکته برداری شود.

- رایانامه E-Mail
- کنفرانس ویدئویی(Video Conferencing)
- تجارت الکترونیک(Electronic commerce) E-Commerce
- مدل مشتری - سرویس دهنده (Client-Server)
- کاربردهای مشهور

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on-line
P2P	Peer-to-peer	File sharing

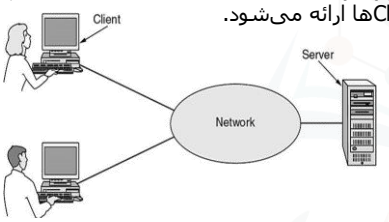
کاربردهای تجاری – مدل خدمات: مدل مشتری - سرویس دهنده

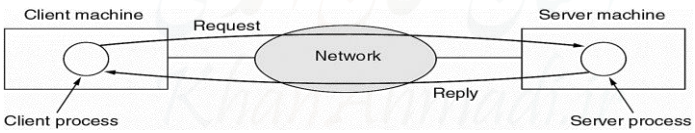
مدل Client/Server:

در ارتباط کارگزار/مشتری یا خدمت دهنده/خدمت گیرنده، خدمت دهنده و خدمت گیرنده همیشه ثابت هستند.

این شبکه‌ها (مبتنی بر Domain) توسط سروری بنام Domain **C**ontroller (DC)، خدمتی به نام Active Directory Domain Services برای مدیریت Clientها ارائه می‌شود.

- Server: ماشین ارائه دهنده خدمات
- Client: ماشین گیرنده خدمات



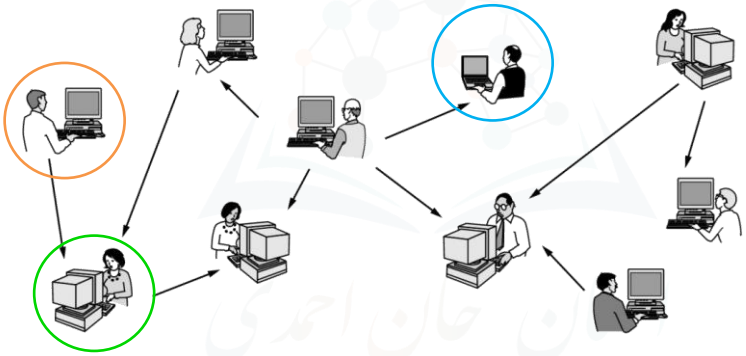


مدل Client/Serverمبتنی بر درخواست‌ها و پاسخ‌ها است.

کاربردهای شبکه‌های کامپیوتری(کاربردهای خانگی)

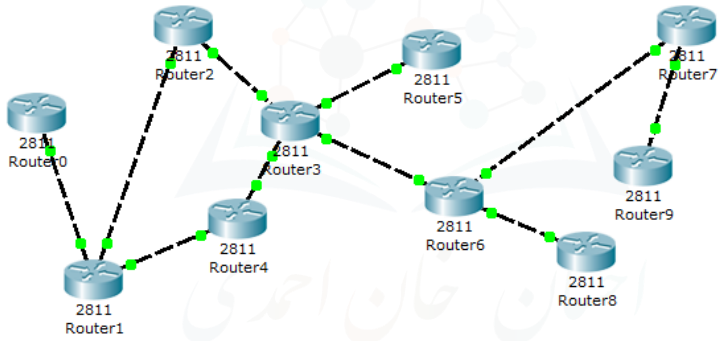
- دسترسی به اطلاعات پراکنده در سراسر دنیا
- آموزش از راه دور
  - TeleLearning
  - E-Learning
- سرگرمی‌های تعاملی Interactive
  - پخش فیلم بر حسب تقاضا VoD (Video-on-Demand)
    - IPTV
    - IP-Media
  - بازیهای تعاملی
- Home Shopping
- درمان از راه دور (Telemedicine)
- ارتباطات دوجانبه (همتا-به-همتا) (Peer-to-Peer)
  - Server or Client؟

کاربردهای خانگی ارتباطات دوجانبه Peer-to-Peer



در یک سیستم همتا-به-همتا مشتری یا سرویس دهنده ثابتی وجود ندارد.

کاربردهای خانگی ارتباطات دوجانبه Peer-to-Peer



معمولا مسیریاب‌ها در شبکه‌های WAN با این روش کار می کنند.

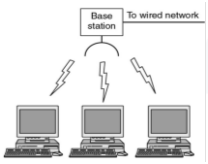
کاربردهای شبکه‌های کامپیوتری(کاربران سیار)

- کامپیوترهای کتابی و دستیاران دیجیتالی (PDA: Personal Digital Assistant)
  - انجام کارهای روزانه حتی در سفر
  - قرائت کنتورهای مختلف خانگی
  - کامپیوتر کتابی
- شبکه‌های بی‌سیم(Wireless Network)
  - شبکه‌های بی‌سیم ثابت (Fixed Wireless)
    - ارتباط قرارگاه با لشگر
  - شبکه‌های بی‌سیم سیار (Cell Phone)
    - Tabletها
- کاربردهای سیار/بی‌سیم

Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

تقسیمات شبکه‌های بی‌سیم Wireless Networks

- **تقسیمات شبکه‌های Wireless**
  1. ارتباطات بین تجهیزات
     - اتصال تجهیزات مختلف به رایانه
     - Bluetooth برمبنای الگوی اصلی-پیرو (Master-Slave)

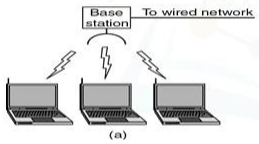


  2. LANهای بی‌سیم
     - مودم رادیویی و آنتن
     - کارت‌های شبکه بی‌سیم و Access Pointها
     - IEEE 802.11
  3. WANهای بی‌سیم
     - دستگاه‌های تلفن همراه
       - نسل‌های اول تا پنجم
     - اینترنت پرسرعت

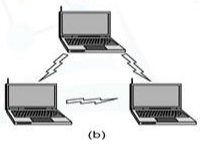
شبکه‌های محلی بی‌سیم IEEE 802.11

- ارتباط کامپیوترها با یکدیگر با تجهیز آنها به فرستنده – گیرنده های رادیویی بُرد کوتاه
- استاندارد 802.11 یا Wi-Fi برای سازگاری شبکه‌های بی‌سیم با یکدیگر در دو حالت:

a) در صورت وجود ایستگاه مرکزی: تبادل تمام پیام‌ها از طریق ایستگاه مرکزی(access point)
b) در صورت نبود ایستگاه مرکزی: ارتباط مستقیم کامپیوترها با یکدیگر



(a) با ایستگاه مرکزی



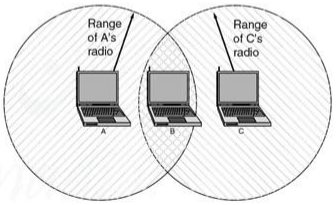
شبکه بی‌سیم(b) بدون ایستگاه مرکزی

- شبکه بی‌سیم با سرعت های 1Mbps و 2Mbps کار می کرد.

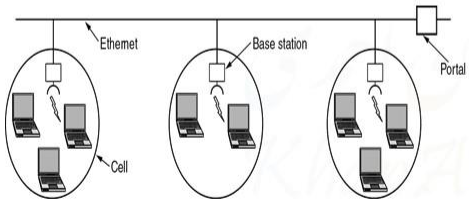
- تعدادی از انواع استاندارد شبکه بی‌سیم IEEE 802.11:
  - 802.11a: باند فرکانسی وسیع تر از ۸۰۲.۱۱، سرعت تا 54 Mbps
  - 802.11b: باند فرکانسی همانند ۸۰۲.۱۱، سرعت 11 Mbps (بعلت مدولاسیون متفاوت)
  - 802.11g: با باند فرکانسی 802.11b و مدولاسیون 802.11a
  - 802.11n: از جدیدترین نسخه هاست

مسائل شبکه‌های بی‌سیم Wireless Networks

- مسایل مربوط به امواج رادیویی:
  - مسئله ایستگاه پنهان
  - محو شدگی چند مسیره
    - (انعکاس چندباره امواج با برخورد به اجسام سخت)
  - مسئله ایستگاه آشکار
  - مسائل نرم افزاری

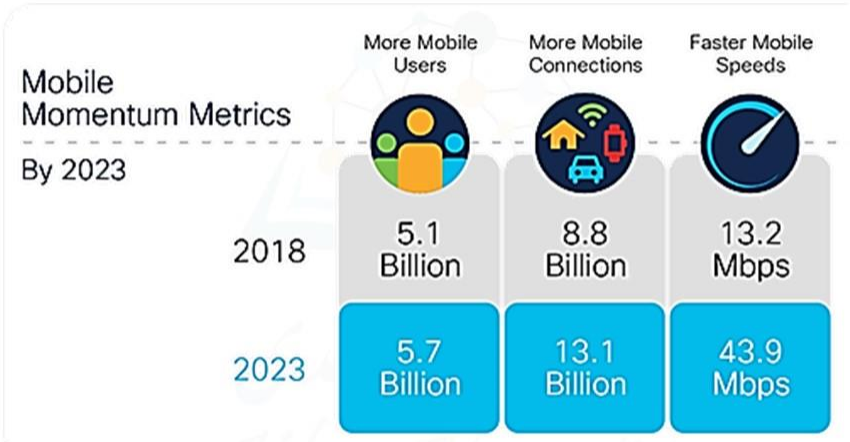


گاهی برد امواج رادیویی برای پوشش دادن به تمام شبکه کافی نیست



A multicell 802.11 network.

معیارهای شبکه بی‌سیم جهانی



شبکه‌های خانگی

افق آینده شبکه‌های خانگی

- رایانه‌ها
(رومیزی، سفری، PDA، Tablet، وسایل جانبی)
- وسایل سرگرمی
(تلویزیون، DVD،ویدئو، دوربین دیجیتال، استریو، MP3)
- وسایل مخابراتی
(تلفن معمولی وهمراه، فکس، دستگاه های ارتباط داخلی)
- لوازم خانگی
(مایکروویو، یخچال، ساعت، بخاری، تهویه مطبوع، چراغ)
- وسایل اندازه‌گیری از راه دور
(اخطار دود یا دزدی، قرائت کنتور، ترموستات، دوربین اتاق بچه)

کاربردهای شبکه‌های کامپیوتری(تبعات اجتماعی)

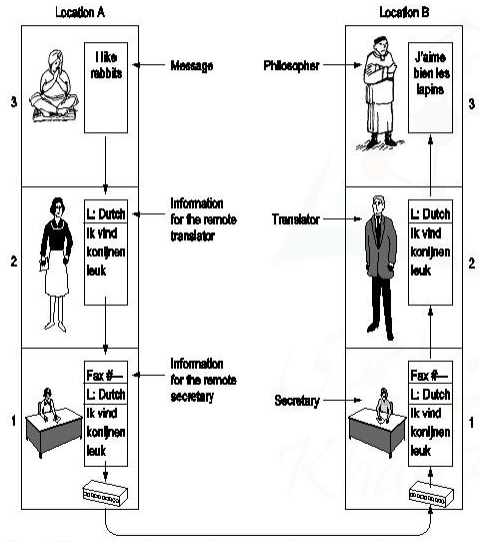
- مسائل اجتماعی،اخلاقی وسیاسی
  - تبادل آزاد و سریع اطلاعات
  - جلوگیری از دردسرها با خط قرمز؟
  - سیاست، مذهب، فرهنگ
- فلسفه "زندگی کن، و بگذار زندگی کنند"!
  - اکثریت مردم چه می‌گویند؟ همه مردم یا جوانان؟ همه مردم یا حباب؟ فرهنگ هر جامعه
  - آیا توهین هم مجاز است؟ آزادی بیان تا چه حد؟
- رابطه دولت با شهروندها
  - قانون حق تجسس
  - اداره آگاهی (FBI)

شبکه شبکه‌ها و تعاریف پایه

- دروازه Gateway
  - اتصال شبکه‌های مختلف و تبدیل داده‌ها از قالبی به قالب دیگر
- internet
  - یا internetwork مجموعه‌ای از شبکه‌های بهم پیوسته
- Internet
  - با حرف اول (Capital) I، همان شبکه جهانی اینترنت
- مفاهیم زیر شبکه، شبکه و شبکه شبکه‌ها
  - Subnet: مجموعه‌ای از مسیریاب‌ها و خطوط مخابراتی به غیر از میزبان
  - Network: همان زیرشبکه است با میزبان
  - Internetwork: مجموعه‌ای از شبکه‌ها

- کوکی‌ها (Cookie)
  - مرورگرهای وب و ذخیره اطلاعات در فایلهای کوچک ← سرعت بیشتر در مراجعات بعد
  - امنیت
- اسپم (Spam)
  - تبلیغات، کلاه‌برداری، پیام‌های بدون نام و نشان حقیقی و ...

سلسله مراتب شبکه



The philosopher-translator-secretary architecture.

سلسله مراتب پروتکل‌ها

- طراحی شبکه‌ها به صورت مجموعه‌ای از چند لایه برای کاهش پیچیدگی
- مکالمه لایه n یک ماشین با لایه n دیگری با قواعد و قراردادی به نام Protocol
- معماری شبکه (Network Architecture): مجموعه‌ای جامع و دقیق از لایه‌ها و پروتکل‌ها

مثال: دو فیلسوف که زبان مشترک ندارند.

نرم افزار شبکه (سلسله مراتب پروتکل‌ها)

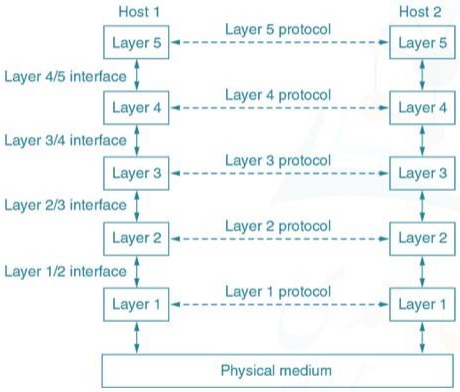
- طراحی به شکل لایه‌ای و ماشین مجازی

۱. پنهان کردن اطلاعات

۲. انواع داده مجرد

۳. کپسولی کردن داده‌ها

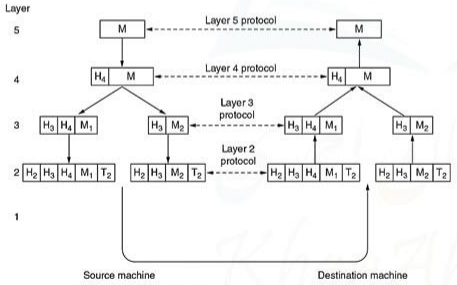
۴. برنامه نویسی شیءگرا



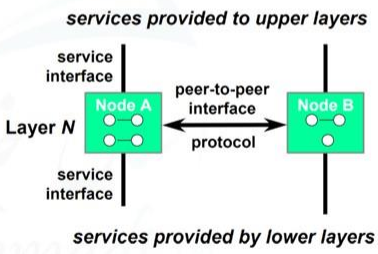
لایه‌ها، پروتکل‌ها، و واسطها

نرم افزار شبکه (سلسله مراتب پروتکل‌ها)

- تعریف همتا، واسط
  - همتا (Peer): اجزایی که در یک لایه هستند که با استفاده از پروتکل تبادل داده می کنند
  - واسط (Interface): که بین هر دو لایه بالا و پایین است، مشخص می کند هر لایه چه سرویس‌هایی به لایه بالاتر بدهد
- پشته پروتکل (Protocol Stack): مجموعه پروتکل‌های یک سیستم



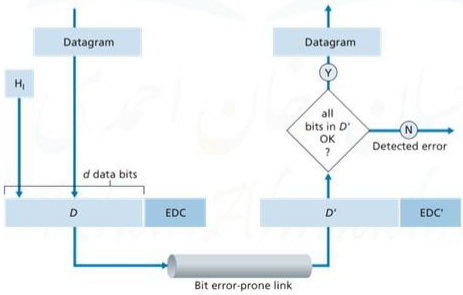
انتقال اطلاعات در یک شبکه پنج لایه



https://courses.cs.vt.edu/~cs5516/spring02/introduction_1.pdf

نرم افزار شبکه – سرویس‌ها – ترکیب‌ها

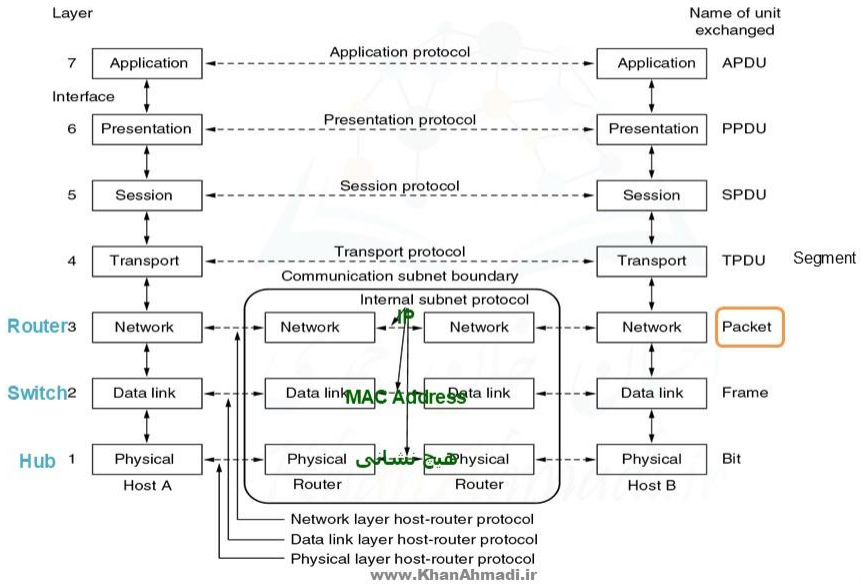
- ملاحظاتی در طراحی لایه‌ها
  - Addressing: سازوکاری برای شناسایی Sender و Receiver
  - Flow Control: چگونگی رفتار گیرنده‌های کند با فرستنده‌های تند
    - ارسال بازخورد وضعیت گیرنده به فرستنده در هر لحظه
    - توافق دو طرف بر سر نرخ انتقال اطلاعات
  - Error Control: هیچ ارتباطی صد در صد عاری از خطا نیست پس باید:
    - توافق دو طرف بر سر یکی از کدهای کشف و تصحیح خطا
    - اعلام صحت دریافت هر پیام از گیرنده به فرستنده



مدل‌های مرجع

- **مدل مرجع OSI**
  - یک مدل مفهومی با هدف ایجاد قابلیت همکاری سامانه‌های ارتباطی مختلف با پروتکل‌های ارتباطی استاندارد است.
  - هنگامی که دستگاه A می‌خواهد به دستگاه B داده بفرستد، این داده‌ها از هفت لایه مختلف عبور می‌کنند و در هر لایه Headerهایی به آن اضافه می‌شود. (در لایه Data Link علاوه بر Header، Trailer هم به داده اضافه می‌شود) در نهایت Packet آماده برای ارسال به شبکه خواهد شد.
- **مدل مرجع TCP/IP**
- مقایسه OSI و TCP/IP
- نگاهی انتقادی به مدل OSI و پروتکل‌های آن
- نگاهی انتقادی به مدل TCP/IP

مدل‌های مرجع (مدل OSI)



۲۹

مفهوم Encapsulation و Decapsulation

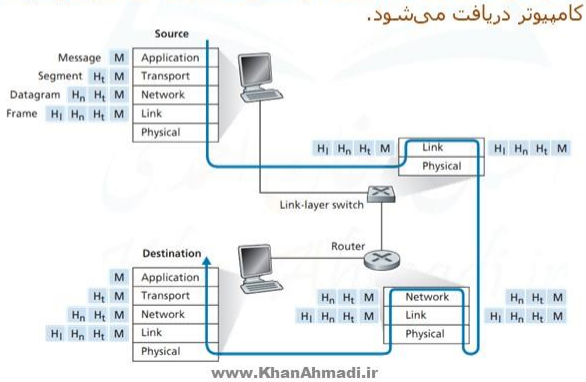
با بالا و پایین رفتن داده در میان لایه‌های شبکه، Encapsulation و Decapsulation رخ می‌دهد.

Encapsulation:

- زمانی اتفاق می‌افتد که تکه‌های اطلاعاتی به داده‌های شبکه (IP, MAC, ...) اضافه می‌شود. یعنی زمانی که داده از یک کامپیوتر ارسال می‌شود.

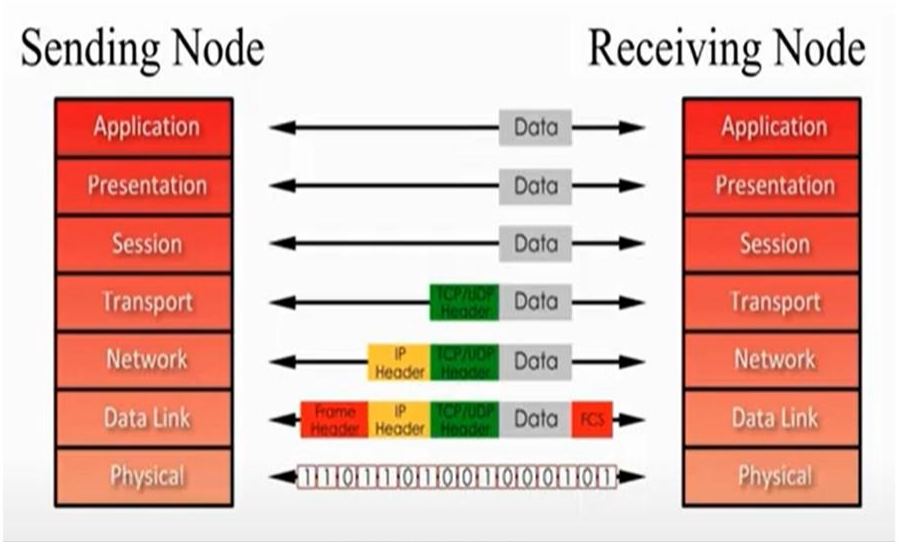
Decapsulation:

- زمانی اتفاق می‌افتد که تکه‌های اطلاعات از داده‌های شبکه جدا می‌شود. یعنی زمانی که داده در یک کامپیوتر دریافت می‌شود.



۳۰

مدلهای مرجع: OSI



لایه‌های مدل OSI – چکیده وظایف لایه‌ها

لایه کاربرد: رابط میان کاربر و شبکه بوده که کاربر می‌تواند با آن ارتباط برقرار کند.

لایه ارائه: فشرده‌سازی/قالب‌بندی دوباره و/یا رمزگذاری داده‌ها را به شکلی دارد که برنامه مقصد بتواند اطلاعات را بخواند.

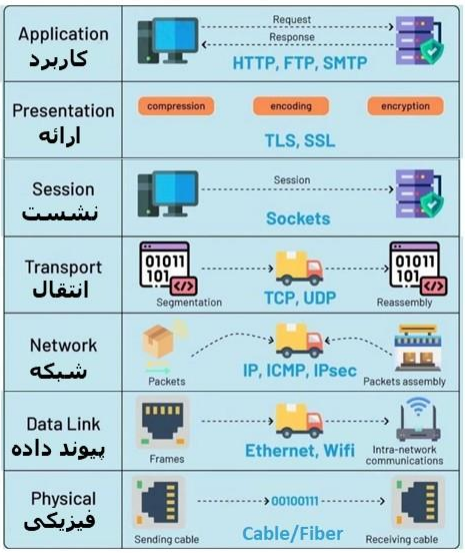
لایه نشست/جلسه: داده‌ها در ارتباطی میان برنامه‌های کاربردی همگام‌سازی می‌شوند.

لایه انتقال: انتقال داده‌ها بین برنامه‌ها توسط دو پروتکل TCP و UDP انجام می‌شود.

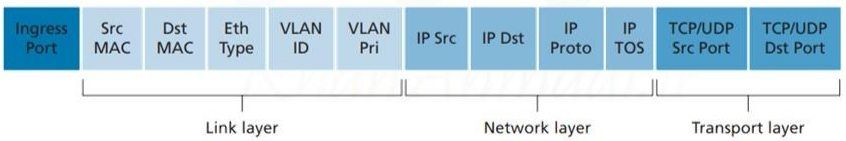
لایه شبکه: تا رسیدن بسته‌ها به مقصد، پیام‌ها را از یک گره شبکه به گره دیگری و از یک شبکه به شبکه دیگر انتقال می‌دهد.

لایه پیوند داده: ارتباط با سخت‌افزار روی شبکه محلی در این لایه برقرار می‌شود.

لایه فیزیکی: تعیین می‌کند که داده از کدام مجرا و به چه شکلی باید به شبکه ارسال شود.



مدل OSI سرایند اضافه شده در هر لایه (Headers , Trailer)



مدل OSI(لایه فیزیکی) - ۱

۱) لایه فیزیکی Physical Layer

تعیین می‌کند که داده از کدام مجرا و به چه شکلی باید به شبکه ارسال شود.

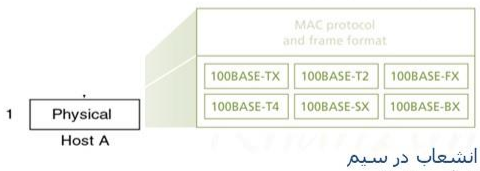
A. انتقال بیت های خام
B. اختلاف ولتاژ
C. انتقال همزمان یک جهته یا دو جهته
D. رابط شبکه Network Connector
E. مکانیکی، الکتریکی، رسانه فیزیکی انتقال

انواع اتصالات لایه فیزیکی:

- کابلی(مسی، فیبر نوری) و بی‌سیم(ماکروویو، مادون قرمز و ...)
  - **کابلی مسی:** کواکسیال Coaxial و زوج بهم تابیده TP در Catهای مختلف
  - **کابل فیبر نوری:** تک حالته Single Mode و چند حالته Multi Mode

Device:

HUB در لایه فیزیکی عمل می‌کند



نشانی:

این لایه هیچ نوع آدرس‌دهی ندارد.

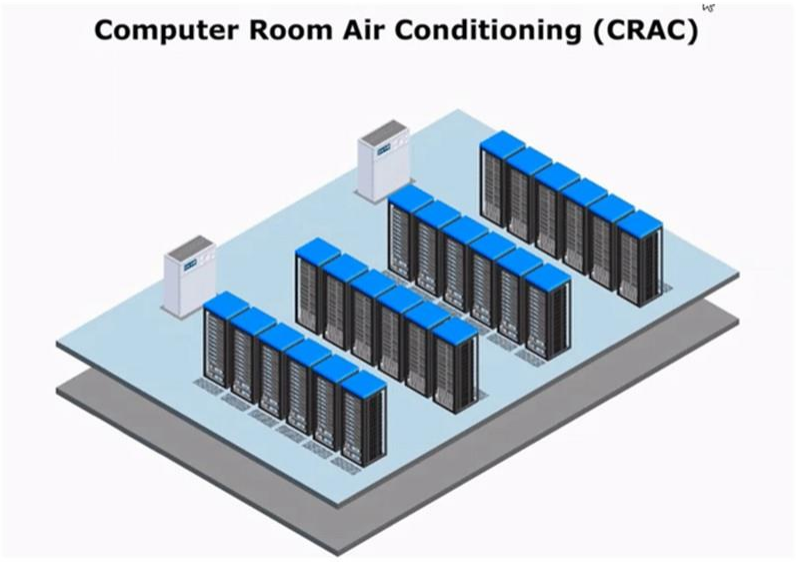
امنیت:

Wire Tapping برای جلوگیری از ایجاد انشعاب در سیم

سیم‌ها درون یک لوله که با گاز تحت فشار پر شده

فاجعه‌های طبیعی

راهرو سرد و گرم در اتاق رایانه‌ی مراکز داده



وظایف لایه‌های مختلف مدل مرجع : OSI

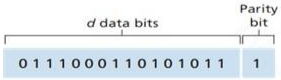
۲) لایه پیوند داده Data Link Layer

پس از تعریف استاندارد 802 توسط IEEE در 1980، ایرادی به لایه دوم وارد شد که دارای وظایفی سخت‌افزاری است که شبیه لایه ۱ است و بعضی از وظایفش هم نرم‌افزاری و شبیه لایه ۳ است.
لذا IEEE پیشنهاد داد لایه ۲ به دو زیرلایه تقسیم شود:

- سرآیند این لایه شامل Source MAC Address/Destination MAC Address است.
- Ethernet سرعت 10 Mbps، FastEthernet سرعت 100 Mbps و GigabitEthernet سرعت 1 Gbps دارد.

۱) Logical Link Control (LLC)

- وظیفه LLC تبدیل خط فیزیکی پر از خطا به یک خط ارتباطی بدون خطا برای لایه شبکه است. این کار با شکستن داده‌های ورودی به تکه‌های کوچک چند صد یا چند هزار بایتی (به نام Data Frame) و ارسال آنها انجام می‌شود. گیرنده با دریافت هر تکه، با محاسبه Parity یک پیام درستی دریافت (Acknowledgement Frame) به فرستنده می‌فرستد تا آنرا از دریافت درست تکه آگاه کند. وظیفه دیگر تعیین شیوه هماهنگ کردن یک گیرنده کند با فرستنده تند است. برای این منظور سازوکاری انجام می‌شود تا فرستنده در هر لحظه از مقدار Buffer گیرنده آگاه باشد. Buffer یا انبارک فضای حافظه‌ای است که داده‌ها تا زمان رسیدن نوبت در آنجا صف می‌بندند.



۲) Medium Access Control (MAC)

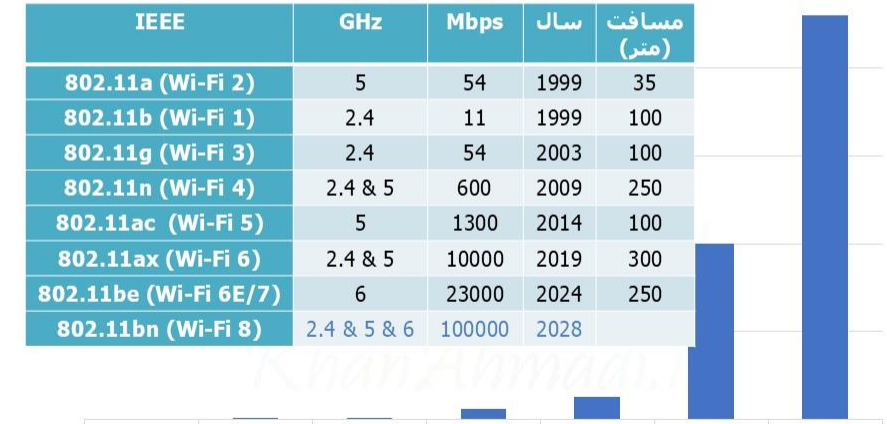
- مهار دسترسی به یک مجرای مشترک در شبکه‌های Broadcast

وظایف لایه‌های مختلف مدل مرجع : OSI

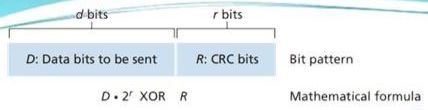
۲) لایه پیوند داده Data Link Layer

استاندارد شبکه بی‌سیم محلی Wi-Fi: IEEE 802.11

IEEE	GHz	Mbps	سال	مسافت (متر)
802.11a (Wi-Fi 2)	5	54	1999	35
802.11b (Wi-Fi 1)	2.4	11	1999	100
802.11g (Wi-Fi 3)	2.4	54	2003	100
802.11n (Wi-Fi 4)	2.4 & 5	600	2009	250
802.11ac (Wi-Fi 5)	5	1300	2014	100
802.11ax (Wi-Fi 6)	2.4 & 5	10000	2019	300
802.11be (Wi-Fi 6E/7)	6	23000	2024	250
802.11bn (Wi-Fi 8)	2.4 & 5 & 6	100000	2028	



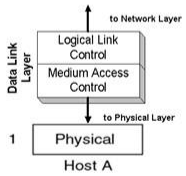
مدل OSI(لایه پیوند داده) - ۲

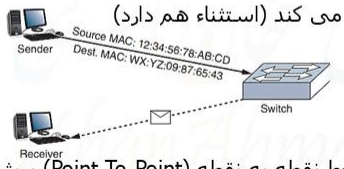


۲) لایه پیوند داده Data Link Layer

A. روش‌های کشف و تصحیح خطا با اضافه کردن CRC یا Checksum به عنوان Trailer
B. شکستن داده‌های ورودی (Data Frame)
C. قاب درستی دریافت (**ack**nowledgement frame)
D. همزمانی (گیرنده کند – فرستنده تند) (Buffer حافظه موقتی)
E. مهار دسترسی (به یک مجرای مشترک در شبکه‌های Broadcast)
F. زیر لایه‌ها:
- **LLC**: Logical Link Control وظایفی شبیه لایه ۳
- **MAC**: Medium Access Control وظایفی شبیه لایه ۱

IS-IS, LLC, MAC, L2TP, X.25 LAPB, **ATM**, **ARP**, **IEEE 802.3**, **Frame Relay**





Device:
Switch در لایه Data Link عمل می کند (استثناء هم دارد)

نشانی:
آدرس‌دهی: MAC Address

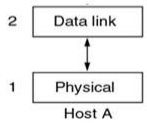
امنیت:
بسته‌های ارسالی بر روی خطوط نقطه به نقطه (Point To Point) پیش از بیرون رفتن از ماشین مبدأ، رمزنگاری شده و با ورود به ماشین مقصد رمزگشایی می‌شود.

مدل OSI(لایه پیوند داده) - ۲

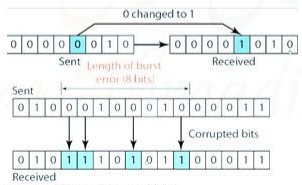
۲) لایه پیوند داده Data Link Layer

A. مفهوم Frame
- ساختار یک Frame در Ethernet

- هنگام ارسال یک دیتاگرام IP از یک میزبان به میزبان دیگر، یک فریم اترنت می‌تواند بسته‌های لایه شبکه را نیز حمل کند. آداپتور ارسال کننده، آداپتور A، دارای آدرس MAC AA-AA-AA-AA-AA-AA و آداپتور گیرنده B، دارای آدرس MAC BB-BB-BB-BB-BB-BB باشد. آداپتور ارسال کننده دیتاگرام IP را در یک فریم اترنت کپسوله می‌کند و فریم را به لایه فیزیکی ارسال می‌کند.
- آداپتور گیرنده فریم را از لایه فیزیکی دریافت می‌کند، دیتاگرام IP را استخراج می‌کند و دیتاگرام IP را به لایه شبکه ارسال می‌کند.



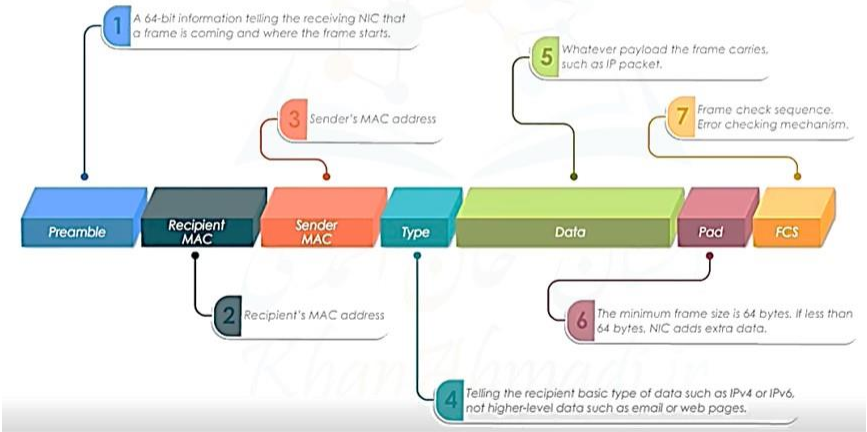
❖ **انواع خطا:**
- Bit Error
- Burst Error



مدل OSI(لایه پیوند داده) - ۲

۲) لایه پیوند داده Data Link Layer

A. اجزای Frame



وظیفه لایه شبکه - ۳

۳) لایه شبکه Network Layer

این لایه دو وظیفه اصلی بسیار مهم و چند وظیفه فرعی دارد:

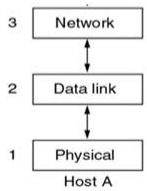
۱) تعیین نشانی IP مبدأ و مقصد (Logical Address)

۲) مسیریابی (Routing): از مبدأ به مقصد، مهار شدآمد و انتخاب مسیرهای بهتر برای حرکت Packet

۳) بهم پیوستن شبکه‌های ناهمگن هنگامیکه آدرس‌دهی در دو شبکه متفاوت باشد یا بسته ارسالی در شبکه مقصد به علت اندازه بزرگ یا متفاوت بودن پروتکل‌ها پذیرفته نشود.

۴) کیفیت سرویس

- تأخیر انتشار بسته‌ها و زمان انتقال آنها
- مهار ازدحام (Congestion) و راه‌بندان ناشی از تعداد زیاد بسته‌های در حال حرکت در یک زیرشبکه



- سرآیند این لایه که در Packet است شامل:
  - Source IP Address/Destination IP Address
  - Routing Protocol

مدل OSI(لایه شبکه) - ۳

۳) لایه شبکه Network Layer

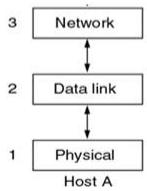
A. آدرس‌دهی: مبتنی بر IP (دستی یا خودکار)
- وظیفه DHCP:
  - اجاره خودکار IP Address، Subnet Mask، Default Gateway و سایر تنظیمات TCP/IP

B. شیوه مسیریابی Routing (Dynamic/Static) و نیمه Static

C. مهار عملکرد subnet

D. مهار کیفیت سرویس QoS
- ازدحام congestion
- گلوگاه bottleneck

IP، ICMP، IPsec، IPX، AppleTalk، X.25 PLP



Device:
Router در لایه Network عمل می‌کند

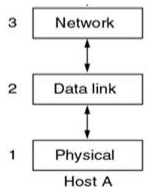
نشانی:
آدرس‌دهی: IP Address

امنیت:
استفاده از دیوار آتش یا Firewall و پشتیبانی از پروتکل IPSec (IP Security)

مدل OSI(لایه شبکه) - ۳

۳) لایه شبکه Network Layer

پروتکل‌ها:
- **IPX/SPX**: برای سیستم عامل Novel NetWare
  - طراحی شده برای LAN بدون نیاز به DHCP و تنظیم
  - نیازمند سخت‌افزار پرهزینه برای کپسوله‌سازی
  - IPX: چطور داده ارسال و دریافت شود در لایه شبکه، غیر متصل
  - SPX: در لایه انتقال برقراری و نگهداری از اتصال اتصال‌گرا
  - برای شبکه‌های بزرگ مانند اینترنت مناسب نبود و با TCP/IP جایگزین شد.
- **TCP/IP**:
  - پروتکل اینترنت IP که در مجموعه TCP/IP قرار دارد: داده‌ها چگونه باید بسته‌بندی و آدرس‌دهی شوند، منتقل شوند، مسیریابی و دریافت شوند و فراهم کردن ارتباطات میان کامپیوترها و اینترنت
- و ICMP خطایابی، IPsec امنیت، AppleTalk، X.25 PLP



سوکت Socket: ترکیبی از یک آدرس IP و پورت TCP یا پورت UDP

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.

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

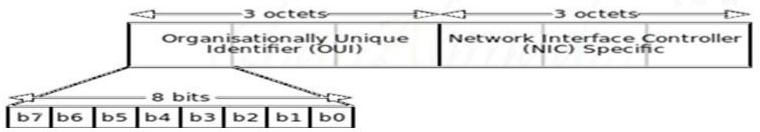
نسخه ۶: (۱۲۸ بیتی)
تعداد نشانی‌ها از 2^{32} به 2^{128} افزایش یافت.
یعنی می‌توان به همه تجهیزات شبکه فعلی و تجهیزات خانگی، شخصی، عمومی و همه وسائل ساخت بشر IP منحصر به فرد اختصاص داد و باز هم این نشانی‌ها به اتمام نرسد!

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

آدرس‌دهی IP 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 (درصورت 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 می‌شود.



شیوه کلاس‌بندی نشانی‌های 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.

آدرس‌دهی Classless و اجرای Subnetting

فرمول: عدد n برای محاسبه کمینه تعداد بیت لازم برای شیفت دادن 1 به راست بکار برده می‌شود. تعداد Subnet $\leq 2^n$

مثال۱: برای تقسیم یک شبکه کلاس A به ۲ زیرشبکه داریم: $2 = 2^n$ بنابراین $n = 1$

- Subnet Mask پیش فرض کلاس A را نوشته و سپس بسته به مقدار n محاسبه شده، بعد از بیتهای مربوط به Net ID، از چپ به راست n بیت را به یک تبدیل می کنیم.

Default Subnet Mask : 255.0.0.0→ 11111111.00000000.00000000.00000000
Subnet Mask+n bits 1: 11111111.10000000.00000000.00000000 → 255.128.0.0

مثال۲: برای تقسیم شبکه‌ی کلاس B به ۷ عدد Subnet داریم: $7 \leq 2^n$ که $7 \leq 8$ بنابراین $n = 3$

Default Subnet Mask : 255.255.0.0 → 11111111.11111111.00000000.00000000
Subnet Mask + n bits 1: 11111111.11111111.11100000.00000000 → 255.255.224.0

- با محاسبه اولین بیت غیر صفر Subnet Mask از سمت راست به دسیمال، طول بازه محدوده نشانی‌ها بدست می آید.

در مثال ۱ طول بازه $2^7=128$ و در مثال دوم $2^5=32$ است.

- برای اختصار Subnet Mask را می‌توان با تعداد 1هایش معرفی کرد: 199.1.1.0/25 یعنی:

subnet mask: 11111111.11111111.11111111.10000000 → 255.255.255.128

مثال: محدوده‌های نشانی IP: 172.16.17.18/20 را مشخص کنید.

راه حل: Class B → Default subnet mask: 255.255.0.0 → 11111111.11111111.00000000.00000000 → 20-16=4 →
$2^n = 16$ → n = 4 → Subnet Mask: 11111111.11111111.11110000.00000000 → 255.255.240.0

طول محدوده نشانی‌ها = 2^4 = 16 تایی است. در هر محدوده اولین نشانی نشانی شبکه و آخرین نشانی نشانی Broadcast هر subnet است.

	Network address		Broadcast address	
Subnet 1:	172.16.0.0	تا	172.16.15.255/20	
Subnet 2:	172.16.16.0	تا	172.16.31.255/20	→ مشاهده می‌شود 172.16.17.18/20در این محدوده قرار دارد
.	.		.	
Subnet 16:	172.16.240.0	تا	172.16.255.255/20	

نشانی‌های IP - IPv6 (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:

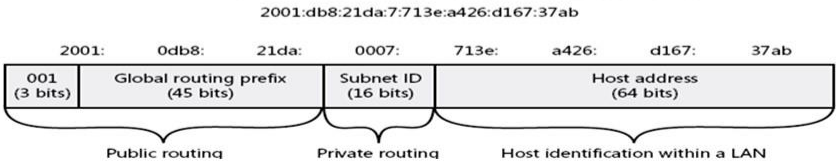
2001:0DB8:3FA9:0000:0000:0000:00D3:9C5A

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.



نشانی‌های IP - IPv6 (IP نسخه ۶):

Global address

نشانی Unicast address:

3 bits	45 bits	16 bits	64 bits
001	Global routing prefix	Subnet ID	Interface ID

نشانی Global address: مشابه Public Address IPv4 می‌تواند در اینترنت مسیریابی شود. بیشتر با 2000::/3 شروع می‌شوند، 3/ یعنی سه بیت اول 001 ثابت هستند.

Link local address

64 bits	64 bits
1111 1110 1000 0000 0000 0000 0000 .... 0000 FE80::/64	Interface ID

نشانی Link Local Address: شبیه APIPA با پیکربندی خودکار در IPv4 است. با FE80 شروع می‌شود و اجازه عبور از local link یا در اینترنت را ندارند.

Loopback address

127 bits	1 bit
0000 0000 0000 0000 000	1

نشانی Loopback address: مشابه Loopback IPv4 که با ۱۲۷ آغاز می‌شود هستند. 1::

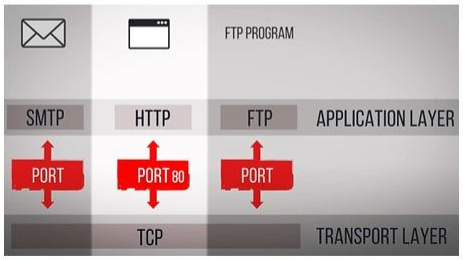
نشانی‌های Multicast address برای ارسال همگانی به همه‌ی Nodeهای شبکه و گروه multicast کاربرد دارد و Anycast address چندین مقصد را شناسایی می‌کند و بسته‌ها به نزدیک‌ترین مقصد تحویل داده می‌شوند.

وظایف لایه‌های مختلف مدل مرجع : OSI

۴) لایه انتقال Transport Layer

این لایه Packet را به اجزاء تبدیل می‌کند. معمولا" اندازه Packet بین ۰/۵ تا ۴ کیلوبایت است.
در مقصد لایه Transport صبر می‌کند تا تمام اجزاء Packet دریافت شوند و بعد به لایه بعدی می‌فرستد.

با ایجاد ارتباطی بنام Connection، در لایه Transport، اطمینان پیدا می‌شود که Packet به مقصد رسیده است یعنی به ازاء هر چند بایت، یک رسید (Acknowledge) توسط مقصد برای مبدأ ارسال خواهد شد.

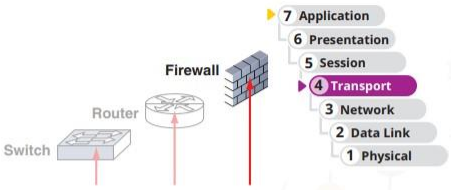


در سرآیند این لایه موارد زیر اضافه می‌شود:

- Seq No.
- تعیین نوع پروتکل TCP/UDP
- شماره Port
- اطلاعات مهار جریان Flow Control

مدل OSI(لایه انتقال) - ۴

۴) لایه انتقال Transport Layer



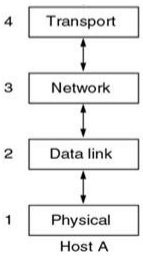
A. شکستن داده‌ها به قطعات کوچکتر

B. ارسال به لایه شبکه

C. کشف و تصحیح خطا برای حصول اطمینان از دریافت درست

D. تعیین خدمات لایه نشست

E. ایجاد ارتباط Connection



پروتکل‌ها:

- **TCP:** با دریافت Ack حصول اطمینان از دریافت شدن بسته و ادامه ارسال
- **UDP:** فقط ارسال بدون نیاز به دریافت Ack برای ادامه ارسال

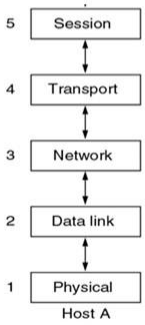
امنیت:
رمزنگاری کل Connection بین مبدأ و مقصد
یعنی امنیت انتها به انتها (End-To-End)

مدل OSI(لایه نشست) - ۵

۵) لایه نشست Session Layer

برگزاری نشست بین ماشین‌های مختلف

برقراری (Establishment)، مدیریت Maintenance و قطع ارتباطی به نام Session
تعیین سرعت ارتباط و مهار رفت و آمد داده (چند بایت ارسال و دریافت شده)



A. مهار دیالوگ:
- مهار اینکه نوبت چه کسی است

B. مدیریت نشانه: Token Management
- جلوگیری از تداخل اعمال مهم

C. همزمان سازی: Synchronization
- مهار عملیات انتقال درازمدت
- از سرگیری آن از نقطه قطع شده در صورت بروز اختلال

- NetBIOS، SAP، PPTP، RTP

امنیت:
دیوار آتش و تجهیزات پیشرفته

وظایف لایه‌های مختلف مدل مرجع : OSI

۶) لایه ارائه Presentation Layer

ساختار داده‌ها مدیریت شده و به زبانی قابل فهم برای لایه کاربرد تبدیل می‌شوند. برای نمونه پروتکل امنیت لایه انتقال ((Transport Layer Security (TLS) در این لایه عملیاتی می‌شود.

در حالتی که سامانه گیرنده نیاز داشته باشد اطلاعات ارسال‌شده را به شیوه خاصی مشاهده کند، لایه نمایش وارد عمل می‌شود. از آنجایی که در پیاده‌سازی‌های عملی از این لایه معمولاً صرف نظر می‌شود، بسیار پیش می‌آید که قراردادهای لایهٔ ۷ با قراردادهای لایهٔ ۵ ارتباط برقرار کنند.

برخی کاربردهای لایهٔ نمایش:

ترجمهٔ اطلاعات ارائه‌شده برای سامانه‌های مختلف شبکه، Compression یا فشرده‌سازی برای بالابردن توان عملیاتی شبکه و رمزنگاری داده‌ها. در وبگاه‌هایی که نشانی با https آغاز می‌شود روی اطلاعات رمزنگاری یا Encryption انجام می‌شود.

مدل OSI(لایه نمایش) – ۶

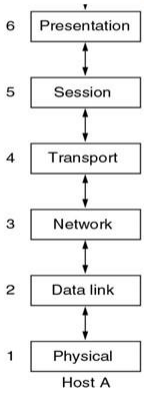
۶) لایه ارائه Presentation Layer

A. تمرکز روی ساختار پیام‌ها و مفهوم آنها برای مدیریت این ساختارها

B. لایه ارائه یا مترجم شبکه

- تبدیل فرمت اطلاعات به شکل قابل ارسال در شبکه

C. عملیات Compression یا متراکم‌سازی



امنیت:
عملیات Encryption یعنی رمزگذاری

مدل OSI(لایه کاربرد) – ۷

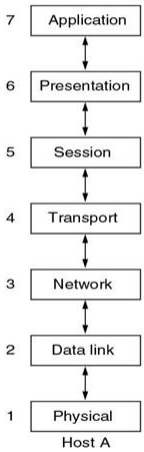
۷) لایه کاربرد Application Layer

A. فراهم آوردن امکان دسترسی نرم‌افزارها به شبکه

B. مدیریت ارتباط بین دو نرم‌افزار در مبدأ و مقصد

C. تعریف پروتکل‌های مورد نیاز کاربران مانند:

- HTTP: وب
- TFTP, FTP: انتقال فایل
- SMTP, POP ,IMAP: رایانامه
- SNMP, DNS: پشتیبانی
- NNTP: انتقال خبر



امنیت:
- احراز هویت کاربران (Authentication)
- غیرقابل انکار بودن محتوای پیام‌ها (Non-Repudiation)

مدل OSI(لایه کاربرد) – ۷: معماری Email، معرفی پروتکل‌های SMTP، MIME، POP

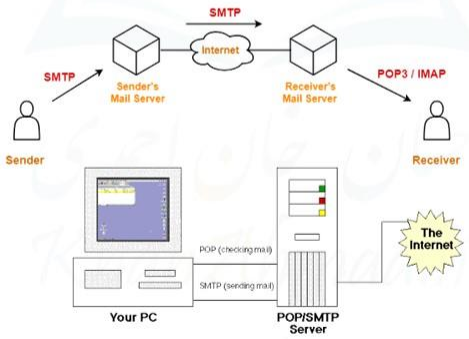
۷) لایه کاربرد Application Layer

معماری Email، معرفی پروتکل‌های SMTP، MIME، POP

a) SMTP پروتکل ارسال ایمیل است که نامه الکترونیکی را تحویل می‌دهد.

b) MIME برای ارسال محتویات غیر متن مانند تصاویر یا کلیپ‌های ویدئویی است.

c) POP3 کلاینت ایمیل‌های جدید را بر روی رایانه دانلود می‌کند و کاربر می‌تواند بدون ارتباط مستقیم با سرور، ایمیل‌ها را مطالعه کند.

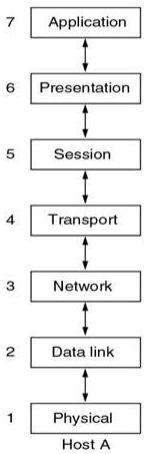


مدل OSI(لایه کاربرد) – ۷: بررسی Domain Name System (DNS)

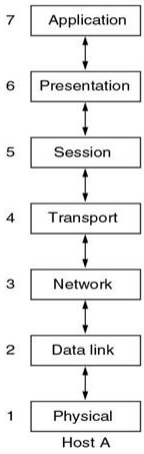
۷) لایه کاربرد Application Layer

بررسی Domain Name System (DNS)

- هدف DNS: تبدیل نام FQDN به نشانی و بالعکس
- DNS Server یک بانک اطلاعاتی از Hostnameها و IP Addressهای متناظر آنها را نگهداری می‌کند و با دریافت Query کاربران، IP Address متناظر را ارائه می‌دهد.



مدل OSI(لایه کاربرد) – ۷: Dynamic Host Configuration Protocol (DHCP)

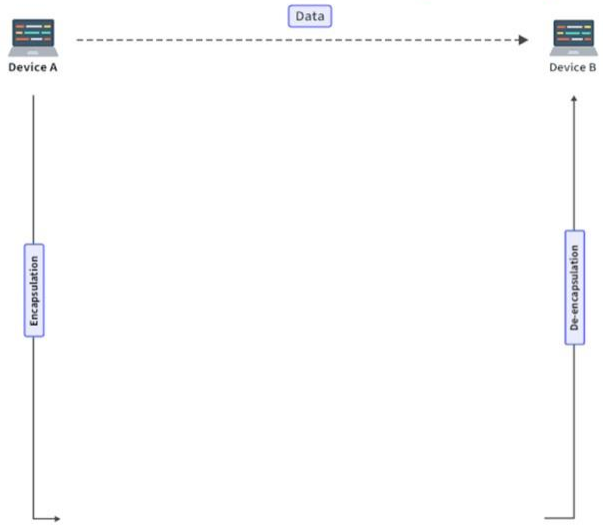


۷) لایه کاربرد Application Layer

بررسی Dynamic Host Configuration Protocol (DHCP)

- اجاره خودکار تنظیمات TCP/IP شامل:
  - IP Address
  - Subnet Mask
  - Default Gateway
  - سایر تنظیمات TCP/IP و مدت زمان اجاره

مدل OSI (Headers , Trailer)

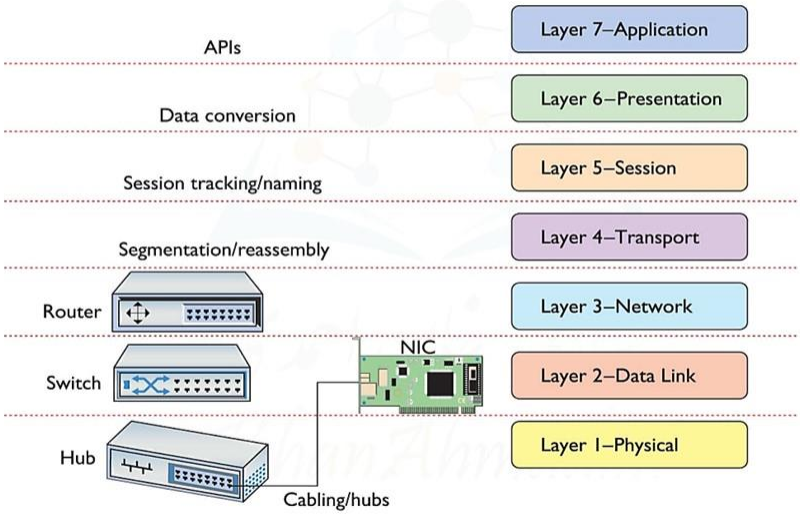


* PH : Presentation Header

مدل OSI (Headers , Trailer) - چکیده

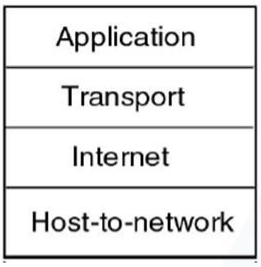
	Data unit	Layer	Function
Host layers	Data	7. Application	فرآیند شبکه به کاربرد
		6. Presentation	نمایش داده‌ها، رمزگذاری و رمزگشایی، تبدیل داده‌های وابسته به ماشین به داده‌های مستقل از ماشین
		5. Session	ارتباط بین میزبان‌ها، مدیریت جلسات بین برنامه‌ها
	Segments	4. Transport	تحویل مطمئن بسته‌ها بین نقاط شبکه
Media layers	Packet/ Datagram	3. Network	آدرس دهی، مسیریابی و تحویل دیتاگرام‌ها بین نقاط شبکه
	Bit/Frame	2. Data link	یک اتصال داده مستقیم نقطه به نقطه قابل اعتماد
	Bit	1. Physical	یک اتصال داده مستقیم نقطه به نقطه (لزوما قابل اعتماد نیست)

مدل OSI (Headers , Trailer) - چکیده



مدل TCP/IP

TCP/IP



۱) **لایه میزبان به شبکه**

A. انتظار دارد میزبان به نحوی به شبکه وصل شود
B. ارسال بسته‌ها

۲) **لایه اینترنت**

A. سوئیچینگ بسته (Packet Switching) مبتی بر ارتباطات Connectionless
B. تعریف قالب بسته‌های پیام و پروتکل آنها به نام IP (Internet Protocol)
C. مسیریابی و پیشگیری از ازدحام در مسیرهای شلوغ

مدل TCP/IP(ادامه)

۳) **لایه انتقال**

- مکالمه عناصر همتا در رایانه‌های مبدأ و مقصد
- پروتکل‌های انتقال Peer-to-Peer:

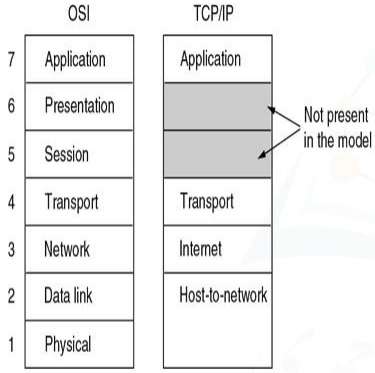
TCP: (Transmission Control Protocol) اتصالگرا و قابل اعتماد (بدون خطا)، Flow Control
UDP: (User Datagram Protocol) غیرمتصل و غیرقابل اعتماد، سرعت مهمتر از دقت؟

۴) **لایه کاربرد**

شامل پروتکل‌های سطح بالا:

- پروتکل انتقال صفحات آبَرمتن HTTP
- پروتکل انتقال فایل FTP
- پروتکل نام ناحیه DNS (تبدیل نام FQDN به IP Address و برعکس)
- پروتکل ارسال رایانامه SMTP
- پروتکل ترمینال مجازی TELNET (ورود به دستگاه‌ها از راه دور)
- پروتکل انتقال خبر NNTP

مقایسه OSI و TCP/IP



شباهت:

۱) هر دو دارای مجموعه‌ای پروتکل‌های مستقل
۲) عملکرد لایه‌های بالاتر به صورت نقطه به نقطه

تفاوت:

۱) مفاهیم محوری مدل OSI: سرویس، واسط، پروتکل
عدم وضوح مفاهیم محوری در مدل اولیه TCP/IP
۲) زمان اختراع مدل
- قبل از اختراع پروتکل‌ها مدل OSI
- بعد از اختراع پروتکل‌ها مدل TCP/IP

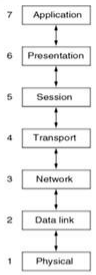
۳) تفاوت در تعداد لایه‌ها
۴) خدمات Connection Less و Connection Oriented
- مدل OSI

در لایه شبکه پشتیبانی از هر دو نوع ارتباط اتصال‌گرا و غیرمتصل
در لایه انتقال فقط اتصال‌گرا

- مدل TCP/IP

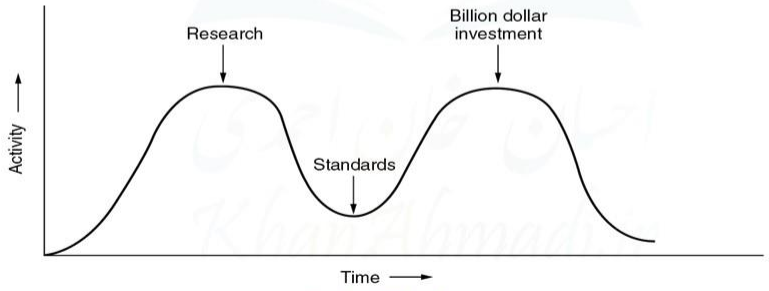
در لایه شبکه فقط غیرمتصل
در لایه انتقال پشتیبانی از هر دو نوع ارتباط اتصال‌گرا و غیرمتصل

نگاهی انتقادی به مدل OSI و پروتکل‌های آن



چرا مدل OSI در ابتدا محبوبیت جهانی نیافت؟

۱. زمان نامناسب (نظریه ملاقات فیل‌ها: دو فیل موج تحقیق و موج سرمایه گذری)
۲. فناوری نامناسب
۳. پیاده‌سازی نامناسب
۴. سیاست‌های نامناسب



نظریه ملاقات فیل‌ها

نگاهی انتقادی به مدل TCP/IP و پروتکل‌های آن

- عدم تفکیک مفاهیم سرویس، واسط و پروتکل از یکدیگر
- مدل TCP/IP یک مدل کلی نیست و نمی‌توان از آن برای توصیف شبکه‌های غیر TCP/IP استفاده کرد
- لایه میزبان-به-شبکه در اصل فقط یک واسط (بین لایه‌های شبکه و پیوند داده) است و یک لایه واقعی نیست
- عدم وجود تمایز بین لایه‌های فیزیکی و پیوند داده در این مدل (با وجود وظایف کاملا" متفاوت این دو لایه)

TCP/IP

Application
Transport
Internet
Host-to-network

طراحی زیرساخت شبکه

مفاهیم کلیدی طراحی زیرساخت شبکه

- استانداردهای کابل‌کشی ساختاریافته ANSI/TIA 568 جدا از اینکه چه کسی قطعات مختلف را تولید یا به فروش می‌رساند، توصیف می‌کند.
- دستگاهی که مشخص می‌کند شبکه ISP پایان می‌یابد و شبکه سازمان آغاز می‌شود، نقطه علامت‌گذاری (demarcation point) است.
- اتصالات منشعب شده از MDF شامل کابل‌های اترنت متصل به مناطق کاری، کابل‌های متصل به IDFها در ساختمان‌های دیگر یا در طبقات دیگر همان ساختمان و اتصال ورودی از ساختمان ارائه دهنده خدمات است.
- VoIP (Voice over IP) استفاده از شبکه (عمومی/خصوصی) برای حمل سیگنال‌های صوتی با استفاده از پروتکل‌های TCP/IP است. یک دستگاه دروازه صوتی voice gateway، سیگنال‌های تجهیزات تلفن آنالوگ را به داده‌های IP تبدیل می‌کند تا از راه اینترنت سفر کنند. پروتکل لایه کاربرد رایج که توسط دروازه‌های صوتی برای آغاز و حفظ ارتباطات استفاده می‌شود، پروتکل سیگنال‌دهی اولیه نشست SIP است.

طراحی زیرساخت شبکه

مفاهیم کلیدی طراحی زیرساخت شبکه

- بهترین شیوه‌های مدیریت کابل شامل کمینه کردن سیم‌های در معرض خطر، اطمینان از تداوم اتصال و رعایت SLA، پرهیز از اتصال شل، پوشش کابل‌ها، سازماندهی کابل‌ها با سینی‌ها و مجاری کابل، کاهش قرار گرفتن کابل در معرض تداخل الکترومغناطیسی EMI و در صورت لزوم استفاده از کابل FTP یا حتی STP بجای UTP برای جلوگیری از تداخلات الکترومغناطیس، و نگهداری و به‌روزرسانی اسناد و مدارک است.
- حسگرهای HVAC اغلب به شبکه متصل می‌شوند. حسگرهای صنعتی HVAC به SCADA معروفند که کنترل نظارتی و کسب داده انجام می‌دهند و در برخی موارد نظارت بر تاسیسات الکتریکی، آب و فاضلاب، سیگنال‌های ترافیکی، حمل و نقل انبوه، تجهیزات تولیدی، واحدهای تبرید، یا سامانه‌های روشنایی و ورود را نیز شامل می‌شوند.
- دوربین‌های امنیتی نیز به عنوان دستگاه‌های شبکه‌ای به هم متصل هستند، اگرچه معمولا دوربین‌های امنیتی در یک بخش شبکه امن secure network segment ایزوله می‌شوند.

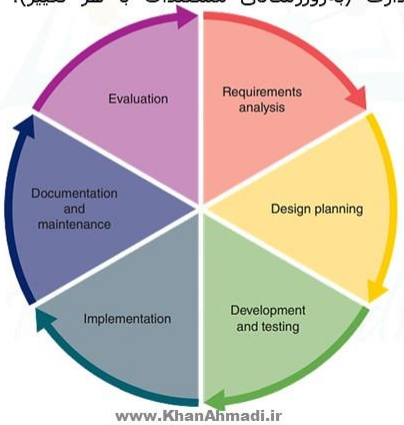
طراحی زیرساخت شبکه

مفاهیم کلیدی طراحی زیرساخت شبکه

- در مدل نظری هفت لایه OSI (Open Systems Interconnection) شیوه‌ی برقراری ارتباط شبکه‌ای تعریف شد و با مدل چهار لایه و عملیاتی TCP/IP مقایسه شد. شیوه‌ی اتصال و هم‌بندی تجهیزات شبکه را توپولوژی شبکه می‌نامند که انواعی مثل Star، Bus و Mesh دارد.
- پهنای باند بیشینه داده‌ای است که می‌تواند در بازه‌ی زمانی مشخصی منتقل شود.
- مهمترین تاخیر Latency در شبکه، زمان بین ارسال و دریافت داده‌ها است.
- Jitter در جریان داده‌ای که پذیرش آن آغاز شده است، اگر بسته‌ها مقادیر متفاوتی از تاخیر را تجربه کنند به آن Jitter گفته می‌شود که ممکن است دریافت بسته‌ها از ترتیب خارج شوند.
- قابلیت اطمینان Reliability در شبکه، امکان ارائه خدمات بدون وقفه در شبکه است.
- مقیاس‌پذیری Scalability در شبکه، امکان تطبیق با رشد و تغییرات شبکه در آینده است.
- امنیت شبکه Network Security در تعریفی ساده، محافظت از شبکه در برابر حملات امنیتی است. مهمترین ابزار امنیتی: دیوار آتش، سامانه‌های تشخیص و جلوگیری از نفوذ IDS/IPS
- تضمین کیفیت خدمات شبکه QoS (Quality of Service) به ویژه برای ویدئو یا صوت VoIP

مراحل طراحی زیرساخت شبکه

- جمع‌آوری و تحلیل نیازها (تعداد کاربران، نوع ترافیک، کاربردها و نیازمندی‌های امنیتی)، طراحی شبکه (مشخص کردن و محاسبات IP، مدل امنیتی، هم‌بندی و تجهیزات مناسب با نیازها منطبق با بودجه)، تهیه تجیزات و آزمایش آنها پیش از نصب، پیاده‌سازی و آزمایش، مستندسازی و نگهداری (به‌روزرسانی مستندات با هر تغییر)، ارزیابی. این چرخه تکرار می‌شود.



استانداردهای مرتبط با طراحی زیرساخت شبکه

- استانداردهای مرتبط با زیرساخت شبکه:
  - IEEE 802.3 استاندارد شبکه کابلی
  - IEEE 802.11 شبکه بی‌سیم محلی Wi-Fi که 802.11n عمومیت دارد و ax جدیدتر است
  - RFC 1918 نشانی IP خصوصی
  - RFC 791 پروتکل IP
  - RFC 768 پروتکل UDP
  - ISO/IEC 27001 استاندارد مدیریت امنیت اطلاعات و NIST چارچوب امنیت سایبری
  - TIA-942 استاندارد طراحی مراکز داده

استاندارد TIA-942 برای طراحی زیرساخت شبکه

TIA-942

با هدف اطمینان از قابلیت اطمینان، انعطاف‌پذیری و مقیاس‌پذیری مرکزداده در تمام سطوح

TIA-942 شامل دستورالعمل‌های دقیق برای:

- طراحی فیزیکی مرکزداده
- زیرساخت شبکه Structured Cabling
- سامانه‌های برق و خنک‌کننده
- امنیت فیزیکی و مدیریت عملیات
- طبقه‌بندی Tier
  - یکی از محورهای کلیدی TIA-942، طبقه‌بندی مراکز داده در چهار سطح Tier:
- Tier I: Basic Capacity
- Tier II: Redundant Capacity Components
- Tier III: Concurrently Maintainable
- Tier IV: Fault Tolerant

طراحی زیرساخت شبکه

زیرساخت شبکه بستری نرم‌افزاری و سخت‌افزاری برای ایجاد راه‌های ارتباطی کاربران و دسترسی ساده به خدمات است. در طراحی زیرساخت شبکه، باید توانایی پاسخ‌گویی به نیازهای حال و آینده کاربران و سازمان پیش‌بینی شده و مورد توجه قرار گیرد.

- **زیرساخت فیزیکی شبکه:** شامل کابل و شبکه، مسیریاب، سوئیچ و سایر سخت‌افزارها
- **زیرساخت منطقی شبکه:** شامل خدمات نرم‌افزاری، پروتکل‌های شبکه و امنیتی، نظام نشانی‌های IP، بخش‌های مهار از راه دور، پایش و سایر بخش‌های نرم‌افزاری شبکه

مراحل زیر در طراحی فیزیکی و منطقی زیرساخت شبکه کمک کننده است:

۱. مستند طراحی کلان HLD (High Level Design) شامل قلمرو پروژه، وضع موجود تا مطلوب
۲. مستند طراحی جزئیات LLD (Low Level Design) شامل جزئیات اجرایی و فنی و حتی config
۳. آماده‌سازی درخواست طرح پیشنهادی RFP، اقلام مورد نیاز LOM و هزینه LOP، خدمات LOS
۴. طراحی و پیاده‌سازی زیرساخت فیزیکی Passive و منطقی
   - مستندسازی، نصب و راه‌اندازی تجهیزات زیرساخت شبکه مانند مسیریاب‌ها و سوئیچ‌ها
   - مستندسازی و کابل‌کشی ساخت‌یافته شبکه و Cable trunking منطبق با استانداردها
۵. مستندسازی نقشه شبکه پیاده‌سازی شده با نرم‌افزارهایی مانند Visio، app.diagrams.net
۶. طراحی، ارائه پیشنهادها و اجرای راه‌حل‌های ارتقا و بهینه‌سازی شبکه و مستندات

طراحی زیرساخت شبکه

شبکه‌های مورد نیاز

شبکه‌های سانترال: شبکه خصوصی سازمان‌های بزرگ برای اشتراک‌گذاری خطوط شهری یا برقراری ارتباط داخل سازمان بدون پرداخت هزینه شبیه یک مخابرات کوچک.

شبکه‌های نظارت تصویری (دوربین‌های مدار بسته): با استقرار دوربین‌ها در نقاط حساس، تصاویری را ضبط کرده و به سرپرستان اجازه مشاهده از راه دور تصاویر دوربین‌ها را می‌دهند. دوربین‌های دارای فناوری PoE می‌توانند برق را نیز از کابل شبکه دریافت کنند. تصاویر باید در مکانی امن مانند فضای ابری ذخیره و نگهداری شوند. (DVR، NVR یا Cloud Based)

شبکه‌های مستقر در مرکز داده: شامل تجهیزات با کیفیت بالای سخت‌افزاری، سرور، ذخیره‌ساز تحت شبکه، قفسه‌های Rack، کابل‌ها، دستگاه‌های تهویه مطبوع و سرمایشی

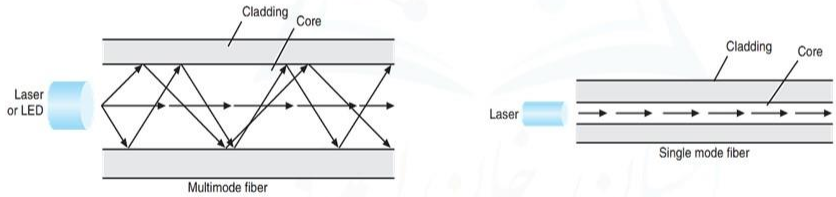
شبکه‌های بی‌سیم: بدون نیاز به کابل‌کشی، داده‌ها را از طریق امواج معمولا رادیویی با پروتکل‌هایی مانند IEEE 802.11n, ac, ax ارسال می‌کند و امنیت آن تضمین شده نیست.

شبکه‌های کابلی: از کابل‌کشی ساخت‌یافته یا Structured Cabling، مبدل‌های شبکه، سوئیچ‌ها و مسیریاب‌ها برای اتصال و اشتراک‌گذاری منابع استفاده می‌کنند.

خدمات کابل‌کشی شبکه

مفاهیم کلیدی کابل‌کشی شبکه

- انواع کابل‌های شبکه:
  - مسی :زوج بهم تابیده مانند U/UTP، S/FTP و کواکسیال مانند: کواکسیال نازک و ضخیم
  - فیبر نوری: تک حالته Single Mode و چند حالته Multi Mode



- کابل‌کشی ساخت‌یافته Structured Cabling با هدف تسهیل مدیریت و نگهداری شبکه با مدیریت کابل‌ها Cable Management برای سازماندهی کابل‌ها
- مهمترین اتصالات شبکه Network Connectors: مسی RJ-45، فیبر نوری SC ، LC

خدمات کابل‌کشی شبکه

مراحل خدمات کابل‌کشی شبکه

۱. طراحی کابل‌کشی: طراحی مسیرها با توجه به محل قرارگیری تجهیزات و ملاحظات امنیتی
۲. نصب داکت‌ها و کانال‌های کابل‌کشی: برای نگهداری و حفاظت کابل‌ها
۳. اجرای کابل‌کشی: رعایت استانداردهای مرتبط و استفاده از ابزارهای مناسب
۴. اتصال کابل‌ها: اتصال تجهیزات شبکه با استفاده از تجهیزات استاندارد
۵. آزمایش کابل‌کشی: برای اطمینان از عملکرد بهینه
۶. مستندسازی: مسیرهای کابل‌کشی، مشخصات کابل‌ها و نتایج آزمایش

استانداردهای اصلی مرتبط:

TIA-568 استاندارد کابل‌کشی ساخت یافته آمریکای شمالی

ISO/IEC 11801 استاندارد جهانی شبکه‌های داده

IEC 60362 استاندارد ایمنی سیم‌کشی الکتریکی و شوک الکتریکی

نکته:

استانداردها مرتب به‌روز می‌شوند. همیشه به آخرین نسخه ان هم از منابع معتبر مراجعه شود.

خدمات کابل‌کشی شبکه

سایر استانداردهای کابل‌کشی شبکه

استانداردهای فیبر نوری:

۱. IEC 60794-1 استاندارد مشخصات فیبرهای نوری
۲. IEC 61755 استاندارد اتصالات و الزامات عملکردی اتصالات فیبر نوری SM
۳. TIA-492 استاندارد فیبر نوری MM

استانداردهای آزمایش و تأیید:

۱. ISO/IEC 14763-3 استاندارد آزمایش و بازرسی کابل‌ها
۲. TIA-568-C.2 استاندارد کابل‌کشی و اجزای مخابراتی زوج بهم تابیده متعادل

استانداردهای مرتبط با ایمنی:

۱. IEC 60364 مجموعه استاندارد نصب الکتریکی ساختمان و الزامات ایمنی کابل‌کشی
۲. NFPA 70 (National Electrical Code - NEC) الزامات ایمنی کابل‌کشی الکتریکی در آمریکا

کابل‌کشی ساخت‌یافته یا Structured Cabling

کابل‌کشی ساخت‌یافته (Structured Cabling):

زیرساخت‌های کابل‌کشی برای ایجاد ارتباط میان اجزاء شبکه در محیط یک ساختمان یا یک فضای خاص با استفاده از اصول و روش‌های استاندارد

اجزاء اصلی:

۱) نقطه علامت‌گذاری یا ورودی (Entrance Facilities , Demarcation point):
- پایان کابل‌کشی مخابرات و آغاز کابل‌کشی داخل ساختمان

۲) اتاق تجهیزات یا ارتباطات (Equipment or Telecommunication Room):
- اتصالات اصلی در شبکه (Main Cross) که کابل ورودی را به کابل داخلی متصل می‌کند و دارای قفسه‌های سرور و patch panelها است.

۳) کابل‌کشی عمودی (Vertical Cabling):
- کابل‌های ستون فقرات (Backbone) یا riser cabling بخش های Entrance Facilities، Equipment Room و Telecommunication Roomرا بهم وصل می‌کند.

۴) کابل‌کشی افقی (Horizontal Cabling):
- کابل‌کشی میان اتاق ارتباطات (TR) و پریزهای شبکه کاربران در محیط کاری

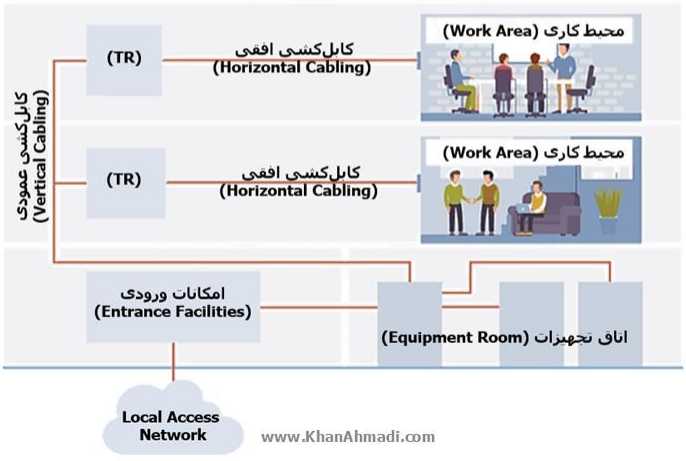
۵) محیط کاری (Work Area):
- تجهیزات کاربران نهایی در این فضا (اتاق‌ها) قرار می‌گیرند مانند پریزهای دیواری (outlet) و کانکتورهای RJ45

مزایا:

۱)ثبات و پایداری ۲) پشتیبانی از سازندگان مختلف ۳) سادگی در جابجایی، اضافه و تغییر
۴) سادگی در عیب‌یابی ۵) پشتیبانی از کاربردهای آینده ۶) جداسازی خطا ۷)کاهش هزینه‌ها

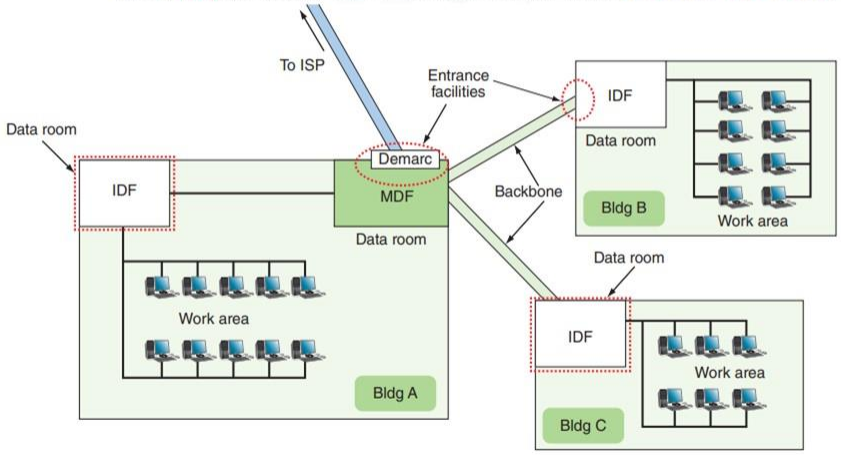
کابل‌کشی ساخت‌یافته یا Structured Cabling

استانداردهای مهم: توسط سازمان‌هایی مانند ISO/IEC، CENELEC و TIA ارائه می‌شود:
ANSI/TIA/EIA-568-B برای مشخص کردن نیازمندی‌های کلی کابل‌کشی در ساختمان‌ها
و TIA-942 استاندارد زیرساخت‌های مراکز داده (Data Center) است.



کابل‌کشی ساخت‌یافته یا Structured Cabling

اتصال ساختمان‌ها: مثالی از اتصال ساختمان‌های یک پردیس طبق ANSI/TIA



ANSI/TIA structured cabling in a campus network with three buildings

مرکز داده Data Center

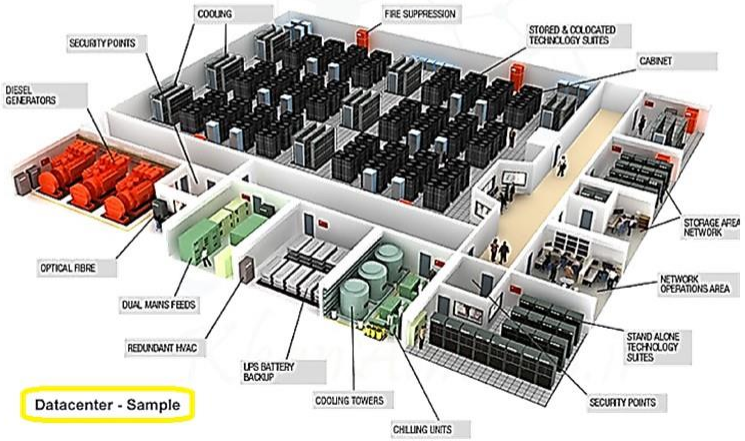
زیرساخت فیزیکی

زیرساخت فیزیکی مرکز داده از بخش‌هایی مانند اتاق‌های سرور امن، سامانه‌های نظارتی، زیرساخت‌های ارتباطی متفاوت، سامانه خنک کننده، دکل‌های رادیویی و ... تشکیل شده است.

مرکز داده Data Center

زیرساخت فیزیکی

۱. ساختمان و فضای فیزیکی: ساختمان مرکز داده باید برای جلوگیری از ورود گرد و غبار، رطوبت، آلودگی هوا، نوسانات دما و رطوبت و حوادث طبیعی مانند زلزله و سیل، مقاوم باشد.

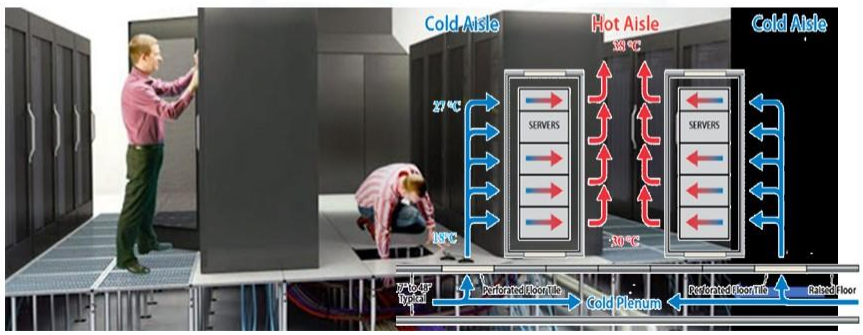


مرکز داده Data Center

زیرساخت فیزیکی

۲. سامانه تهویه: برای مهار دما، رطوبت و تهویه مناسب، طراحی و پیاده‌سازی می‌شود.

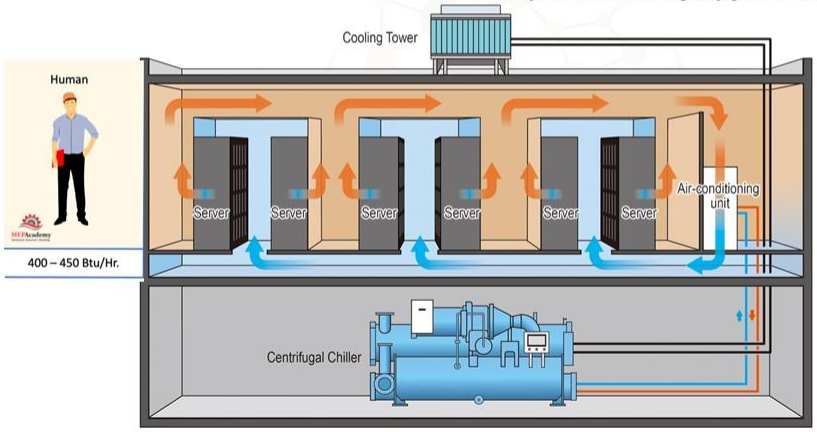
انرژی گرمایی با واحد BTU محاسبه می‌شود. گرمای بدن هر نفر را معادل 400 BTU محاسبه می‌کنند.



مرکز داده Data Center

زیرساخت فیزیکی

۲. سامانه‌های خنک‌کننده: مدیریت دما شامل سامانه‌های خنک‌کننده گازی/آبی، Sky Air، چیلرها Chillers، کولرها و سامانه‌های دیگر است.



مرکز داده Data Center

زیرساخت فیزیکی

۳. سامانه‌های مدیریت: شامل امکاناتی برای مدیریت، مهار تجهیزات و نرم‌افزارها و همچنین دسترسی‌ها است.

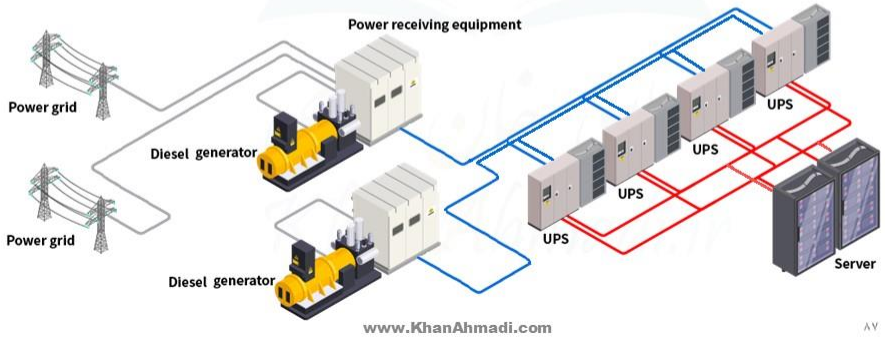
مرکز داده Data Center

زیرساخت فیزیکی

۴. سامانه‌های برق: مهمترین بخش زیرساخت فیزیکی است که برای تامین انرژی مورد نیاز تجهیزات، سرورها و شبکه‌ها طراحی و پیاده‌سازی می‌شود. این بخش شامل سامانه‌های برق بدون وقفه Uninterruptible Power Supply (UPS) و ژنراتورهای برق پشتیبان است.

واحد اندازه‌گیری ظرفیت UPSها گاهی kW (kilowatts) یا بیشتر (kilo-volt-amperes) **kVA** است.

در کابل‌کشی برق باید مسیر کابل‌های شبکه با فاصله از برق باشد. مسیر خنک‌تر برای کابل‌های برق در نظر گرفته می‌شود زیرا این کابل‌ها بیشتر از کابل‌های شبکه حرارت تولید می‌کنند.

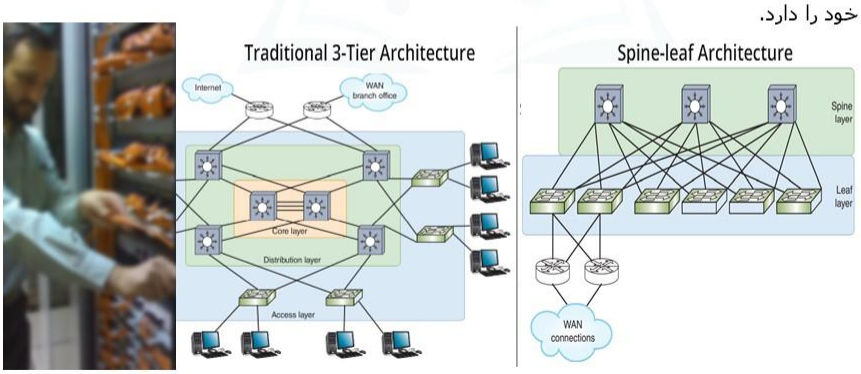


مرکز داده Data Center

زیرساخت فیزیکی

۵. سامانه‌های شبکه: شامل تجهیزات شبکه مانند سوئیچ‌ها، مسیریاب‌ها و ... است که برای ارتباط مرکز داده با اینترنت و شبکه‌های دیگر استفاده می‌شود. این سامانه‌ها باید دارای پهنای باند بالا و قابلیت انطباق با ترافیک بالای شبکه باشند.

شبکه‌ها در مدل سنتی سلسله‌مراتبی سیسکو در سه لایه Core, Distribution, Access طراحی می‌شدند، اما اکنون پیشنهاد بر معماری دولایه‌ای Spine-leaf است که هر لایه تجهیزات خاص خود را دارد.



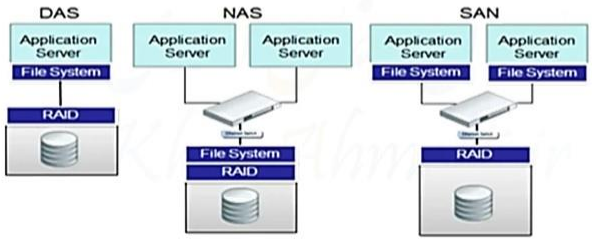
مرکز داده Data Center

زیرساخت فیزیکی

۶. سامانه‌های ذخیره‌سازی: برای ذخیره و مدیریت داده‌های مرکز داده استفاده می‌شوند و شامل سرورهای ذخیره‌سازی، سامانه‌های فایل و سامانه‌های مدیریت داده‌های بزرگ است.

معروف‌ترین ذخیره‌سازها به صورت SAN، NAS و DAS نام برده می‌شوند.

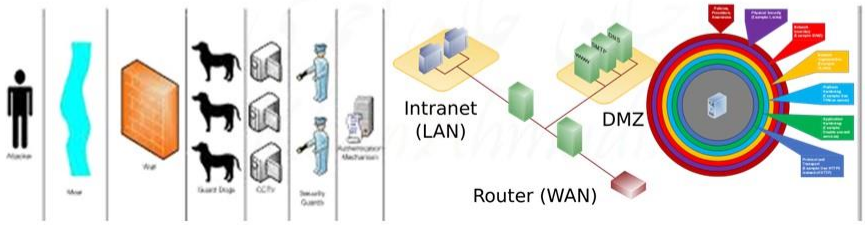
- **DAS (Direct Attached Storage):** سخت‌افزار به رایانه سرور متصل می‌شود. مجموعه دیسک‌های داخلی (Internal HDD) یا SSD از نوع Enterprise که پایداری، سرعت و قیمت بالاتری دارند در محفظه‌هایی معمولا تنظیم شده به صورت RAID (Redundant Array of Independent Disks) به سرور متصل می‌شوند.
- **NAS (Network Attached Storage):** خود دارای سیستم‌عامل و کارت شبکه هستند و مستقیم به شبکه متصل می‌شوند. بنابراین وابستگی زیادی به سرعت شبکه دارند.
- **SAN (Storage Area Network):** شبکه‌ای با کارآیی بالا از ذخیره‌سازها هستند که با سرعت بسیار بالا بین سرورها و واحدهای ذخیره‌سازی با پروتکل FC یا FCoE عمل می‌کنند.



مرکز داده Data Center

زیرساخت فیزیکی

۷. سامانه‌های امنیتی: برای جلوگیری از دسترسی غیرمجاز، حفاظت از داده‌های حساس و جلوگیری از نفوذ با استفاده از رمزنگاری، دوربین‌های مداربسته، پروتکل‌های تشخیص نفوذ و سایر ابزارهای امنیتی مانند EDR (تشخیص و پاسخ نقطه پایانی)، XDR (تشخیص و پاسخ گسترده)، FAM (نظارت بر فعالیت فایل معمولا با چندین ضدبدافزار)، PAM (مدیریت دسترسی ویژه) تشکیل شده است. در سازمان‌ها مرکز عملیات امنیتی (SOC) تشکیل شده تا افراد، فرایندها و داده‌های دریافتی از Agentها را در سامانه مدیریت اطلاعات امنیتی و رویداد SIEM ذخیره کند و در ساختار دفاع در عمق پیاده‌سازی شوند. از طرفی سازمان‌ها باید برای اطلاع از جدیدترین خطرات، شیوه مقابله با آنها و شیوه‌نامه‌های امنیتی با ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای)، سازمان پدافند غیر عامل و افتای ریاست جمهوری در ارتباط و هماهنگ باشند.



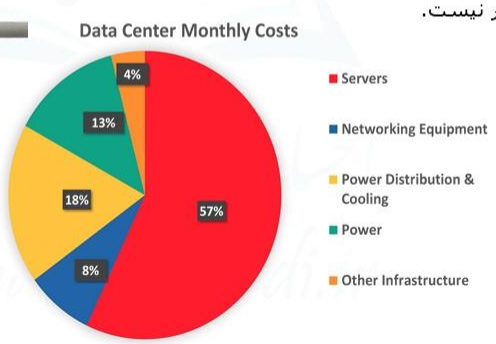
مرکز داده Data Center

زیرساخت فیزیکی

۸. سامانه‌های پایش و ایمنی: سامانه‌های پایش و نظارت دما، رطوبت، برق و تجهیزات دیگر، سامانه‌های مدیریت شدآمد شبکه، سامانه‌های مدیریت رایانامه و ابزارهای نظارتی خودکار، از اجزای آن هستند.

سایر موارد مانند مباحث ایمنی هم نباید از نظر دور بماند.

برای خاموش کردن آتش معمولا از گاز FM200 استفاده می‌شود که به خودی خود برای انسان مضر نیست.



مرکز داده Data Center

استاندارد و سطوح مرکز داده

رایج ترین استاندارد برای طراحی و پیاده‌سازی مرکزداده، ANSI/TIA-942 است.

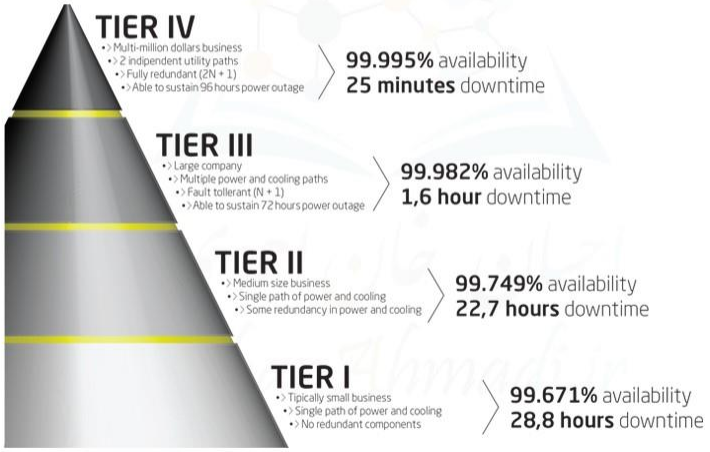
این استاندارد انطباق با یکی از چهار سطح تعریف شده که به **Tier** معروف است را تضمین می‌کند.

۱. **سطح ۱:** زیرساخت پایه
   - این سطح، امکانات فیزیکی محدودی ارائه می‌دهد و دارای تجهیزاتی با ظرفیت محدود و تنها یک مسیر ارتباطی است.
۲. **سطح ۲:** زیرساخت با ظرفیت بیشتر
   - این نوع مرکز داده، امکانات فیزیکی بهتری ارائه می‌دهد که دارای تجهیزات بیشتر و یک مسیر ارتباطی است.
۳. **سطح ۳:** زیرساخت با رویکرد موازی
   - این مراکز داده تقریباً تمامی امکانات فیزیکی را شامل می‌شوند و تجهیزاتی با ظرفیت اضافی و چندین مسیر ارتباطی مستقل Backbone را ارائه می‌دهند. هر یک از اجزای آن می‌تواند بدون ایجاد اختلال در خدمات به کاربران نهایی، حذف یا جایگزین گردد.
۴. **سطح ۴:** زیرساخت مقاوم در برابر خطا
   - در این نوع مراکز داده، بالاترین سطح تحمل خطا و افزونگی ارائه می‌شود. تجهیزاتی با ظرفیت اضافی و چندین مسیر ارتباطی مستقل، قابلیت نگهداری و خطایابی متقارن را در هر نقطه از مرکز داده بدون ایجاد خرابی، امکان پذیر می‌کنند.

مرکز داده Data Center

استاندارد و سطوح مرکز داده

رایج ترین استاندارد برای طراحی و پیاده‌سازی مرکزداده، ANSI/TIA-942 است.



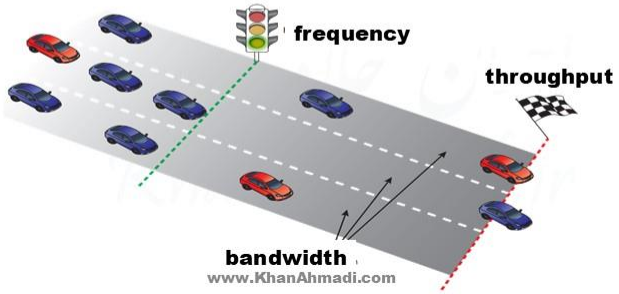
۹۳

تعاریف مرتبط با پهنای باند

Bandwidth پهنای باند شبکه‌های امروزی بر حسب Mbps یا Gbps اندازه‌گیری می‌شود و به مقدار داده‌ای اشاره دارد که بالقوه می‌توان به صورت نظری در طول یک دوره زمانی مشخص با در نظر گرفتن مواردی مانند فرکانس، فاصله و SNR یعنی نسبت سیگنال به نویز، انتقال داده شود.

Throughput توان عملیاتی به آن نرخ بار مفید یا نرخ موثر داده نیز گفته می‌شود و با Mbps یا Gbps اندازه‌گیری می‌شود. توان عملیاتی به تعداد بیت‌های داده ۰ و ۱ که در هر ثانیه در یک اتصال دریافت می‌شوند اشاره دارد و واقعیت محیط شبکه را در نظر می‌گیرد، از جمله تأخیر در رابطهای متقاطع، نویز موثر بر سیگنال‌ها، خطاهایی که منجر به از دست رفتن داده‌ها می‌شوند و غیره.

Frequency فرکانس برای کابل‌کشی شبکه امروزی معمولا بر حسب مگاهرتز یا گیگاهرتز اندازه‌گیری می‌شود که نشان دهنده تعداد مرتبه‌هایی در یک ثانیه است که یک سیگنال الکتریکی می‌تواند حالت‌ها را تغییر دهد مثلا از مثبت به منفی یا بالعکس.



۹٤

پهنای باند

Bandwidth: به اندازه حجم قابل ارسال و دریافت داده در واحد زمان پهنای باند گفته می‌شود. واحد آن بیت بر ثانیه است اما Mbps (megabits per second) یا Gbps (gigabits per second) متداول‌تر شده‌اند. پهنای باند بر دو نوع است:

۱- **Shared Bandwidth**: این نوع پهنای باند ارزان‌تر بوده و در آن تضمینی برای تأمین پهنای باند برای مشترک وجود ندارد. چراکه این پهنای باند بین تعدادی مشترک بوده و همگی از آن استفاده می‌کنند. بنابراین طبیعی است در ساعات پر ترافیک مشترک نتواند از پهنای باند درخواستی خود بهره ببرد.

۲- **Dedicated Bandwidth**: این نوع پهنای باند گران‌تر بوده اما در آن استفاده از سقف پهنای باند در تمام ساعات تضمین شده است. زیرا پهنای باند بصورت اختصاصی به مشترک تخصیص یافته است.

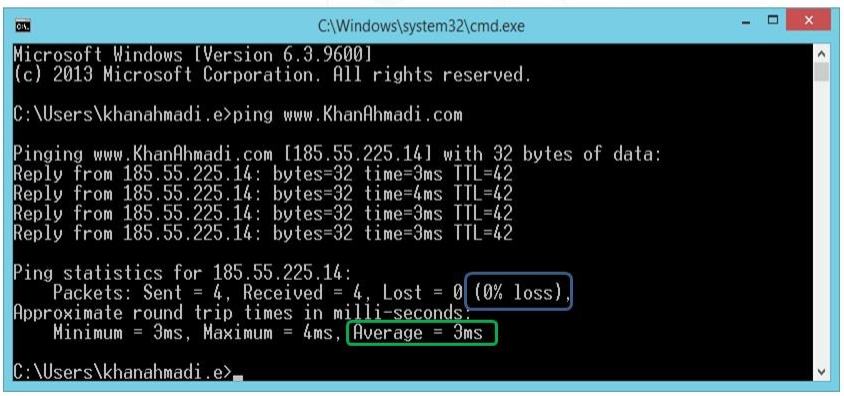
Bandwidth Quality: دو مورد از عواملی که کیفیت پهنای باند به آنها بستگی دارد:

۱- **Ping Time**: به مدت زمانی گفته می‌شود که یک Packet از ISP به مقصد یک Host قوی (مثلا" www.KhanAhmadi.ir) در اینترنت ارسال شده و پس از دریافت پاسخ مناسب دوباره به ISP باز می‌گردد. هرچه این زمان **کمتر** باشد پهنای باند از **کیفیت بهتری** برخوردار است.

۲- **Packet Loss**: هنگامی که یک Packet به اینترنت ارسال می‌شود ممکن است به دلایل مختلف مفقود شده و یا از دست برود. Packet Loss عبارت است از نسبت Packetهای از دست رفته و مفقود شده به کل Packetها. هر چه این نسبت **کمتر** باشد پهنای باند از **کیفیت بهتری** برخوردار است.

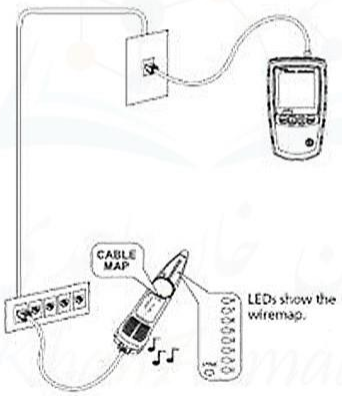
شبکه‌بندی و عیب‌یابی یک شبکه محلی دارای Hub یا Switch

پس از شبکه‌بندی با استفاده از تجهیزاتی که در بخش Network Devices ذکر شد، برای عیب‌یابی و محاسبه کیفیت پهنای باند بین مبدأ با یک نقطه مشخص به عنوان مقصد از دستور Ping و استفاده می‌شود.



شبکه‌بندی و عیب‌یابی یک شبکه محلی دارای Hub یا Switch

شیوه آزمایش کابل‌کشی: با استفاده از Tester کابل شبکه امکان آزمایش درستی و حتی کیفیت کابل‌کشی وجود دارد. معروف‌ترین ویژند آزمایش‌کننده اتصالات کابل شبکه، Fluke است.



دستورات کاربردی در شبکه

Command Prompt

برای کار در محیط شبکه و وب دانستن این دستورات در ویندوز لازم است:

برای استفاده از کمک در نحوه اجرای دستورات (?/ پس از هر دستور)

نکته: برخی دستورات بجای اجرای cmd.exe در حالت معمول، باید Run as administrator یا در Windows PowerShell اجرا شوند.

IPConfig /ALL

بررسی برقرار بودن شبکه و تنظیمات TCP/IP سیستم خود (/ALL: نمایش اطلاعات کامل)

دستور ncpa.cpl برای مشاهده ارتباطات شبکه ای سیستم استفاده می‌شود.

دستور Ipconfig /displayDNS کش DNS سیستم را نشان می دهد، برای پاک کردن DNS Cache دستور ipconfig /flushDNS

دستور ipconfig /release برای رها کردن IP که از DHCP دریافت شده بود.

دستور ipconfig /renew برای دریافت مجدد IP درخواست Broadcast به DHCP ارسال می کند.

Ping –t 192.168.111.10

بررسی برقرار بودن اتصال خود با NIC یا سایت مقصد (t-: تا کنسل شدن ادامه می دهد)

دستور Ping www.khanahmadi.com –n 7 برای مشاهده IP مقصد و تبادل ۷ بسته ۳۲ بایتی

دستور ping 192.168.1.10 –l 1000 برای ارسال بسته ها با حجم 1000 بایت

یا در PowerShell دستور Test-Connection

نکته: حدس زدن سیستم عامل مقصد اگر TTL حدود 128 باشد (ویندوز) و اگر حدود ۶۴ باشد (Linux). سایر کاربردها؟

Tracert -d www.google.com

بررسی تعداد گام‌ها و مسیر مبدا تا مقصد (d- سریع و بدون تبدیل IP به نام و h– تعداد hop را مشخص می کند)

نمایش اطلاعات ارتباط شبکه و connection (r- برای نمایش اطلاعات جدول مسیریابی) **netstat** –r

https://technet.microsoft.com/en-us/library/cc732509(v=ws.10).aspx

دستورات کاربردی در شبکه

Linux

برای کار در محیط شبکه و وب دانستن این دستورات در لینوکس لازم است:

man دستور
info دستور
دستور --help
whatis دستور

برای استفاده از کمک در نحوه اجرای دستورات

ifconfig eth0

بررسی برقرار بودن شبکه و تنظیمات TCP/IP سیستم خود (eth0 نمایش فقط کارت شبکه مشخص شده)
مثال کاربردی: اختصاص IP Address و Subnet Mask به کارت شبکه eth0 با دستور ifconfig eth0 192.168.100.7 netmask 255.255.255.0

Ping –t 192.168.111.10

بررسی ارتباط دو Node در شبکه با PING(Packet INternet Groper)

traceroute 4.2.2.2

بررسی تعداد گامها و مسیر مبدا تا مقصد (در این مثال IP Address یک global DNS server)

نمایش اطلاعات ارتباط شبکه و connection (r- برای نمایش اطلاعات جدول مسیریابی) **netstat** –r

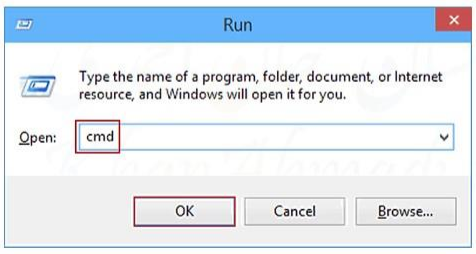
پرس و جو از اطلاعات DNS مانند A Record و غیره **dig** www.khanahmadi.com

http://www.tecmint.com/linux-network-configuration-and-troubleshooting-commands/

دستورات کاربردی در شبکه

Command Prompt

Start → Run → CMD



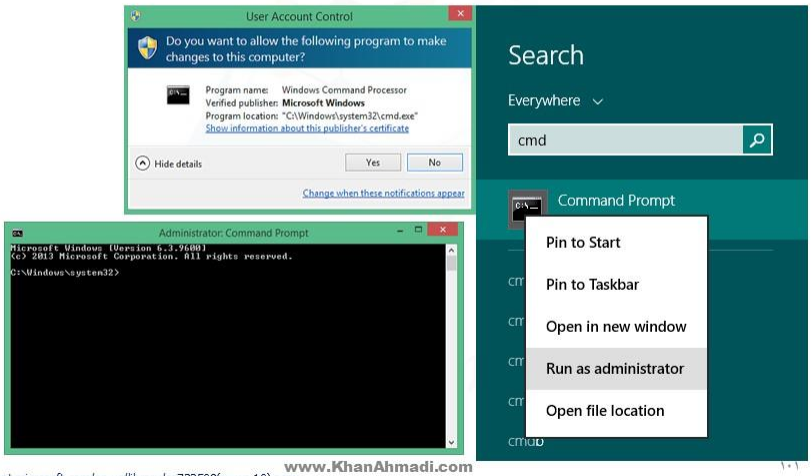
دستورات کاربردی در شبکه

Command Prompt

برای کار در محیط شبکه و وب دانستن این دستورات در ویندوز لازم است:

برای استفاده از کمک در نحوه اجرای دستورات (?/ پس از هر دستور)

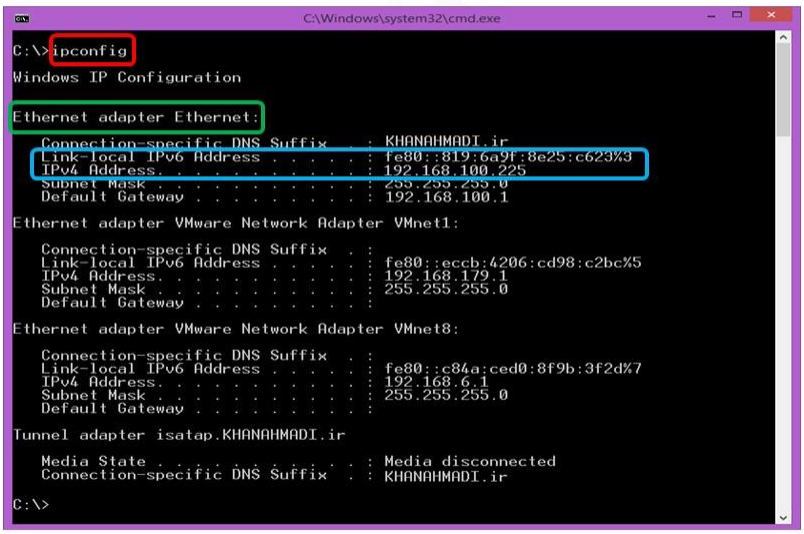
نکته: برخی دستورات بجای اجرای cmd.exe در حالت معمول، باید Run as administrator یا در Windows PowerShell اجرا شوند.



https://technet.microsoft.com/en-us/library/cc732509(v=ws.10).aspx

آزمایش عملی

Command Prompt



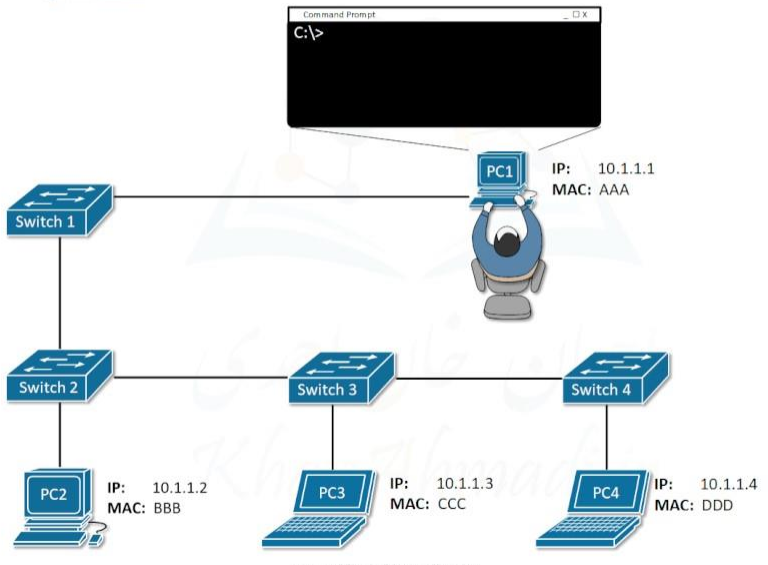
مرور دستورات IP

Command Prompt

1	ipconfig /all	Display full configuration information.
2	ipconfig /release	Release all IP configuration
3	ipconfig /release6	Release the IPv6 address for the specified adapter
4	ipconfig /renew	Renew the IP configuration from DHCP server
5	ipconfig /renew6	Renew the IPv6 address for the specified adapter
6	ipconfig /displaydns	Display the DNS Cache
7	ipconfig /flushdns	Clear DNS Cache
8	ipconfig /registerdns	Re-Register the DNS connections
9	ipconfig /setclassid	Change/Modify DHCP Class ID
10	ncpa.cpl	Open the Network adapter connections
11	control netconnections	Open the Network adapter connections
12	netsetup.cpl	Open network setup wizard
13	ping 192.168.10.100	Check the network connectivity of any IP address
14	tracert	Trace the IP Route
15	netstat	Displays the TCP/IP protocol sessions
16	route	Display Local Route
17	arp	Display Resolved MAC Addresses
18	ipconfig /showclassid	Display DHCP Class Information
19	ipconfig /showclassid6	Displays all the IPv6 DHCP class IDs allowed for adapter
20	nbstat	Displays a list of NetBIOS computer names that have been resolved to IP addresses

مرور دستورات IP

Command Prompt



ادامه دستورات کاربردی

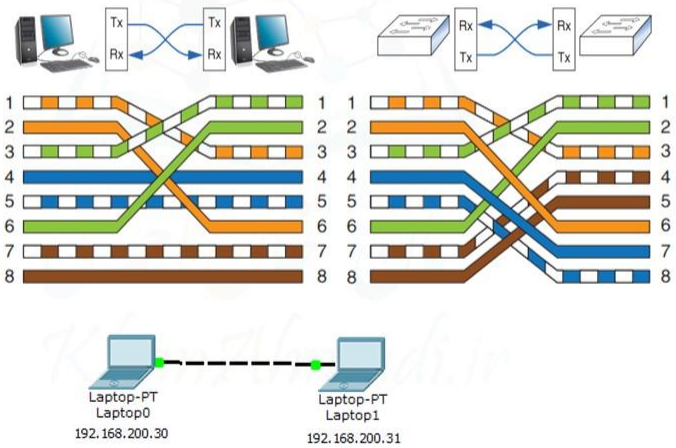
چند نکته کاربردی:

- باز شدن سریع خط فرمان: نگه داشتن کلید Shift و راست کلیک کردن روی Desktop و انتخاب گزینه اجرای CMD یا PowerShell
- پاک شدن صفحه: CLS
- باز شدن سریع Explorer (دسترسی سریع به My Computer): نگه داشتن کلید Windows و فشردن کلید E
- تغییر رنگ پس زمینه و دستورات در CMD: color Background/Foreground مانند color 3e
- نمایش نسخه فنی ویندوز: Ver و winver
- اجرای چند دستور یا باز کردن folder با start: مانند start 1.jpg & 2.jpg یا start folder1

کار عملی: پیاده سازی یک شبکه P-to-P

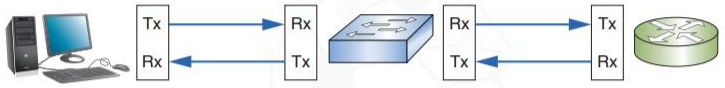
تمرین عملی:

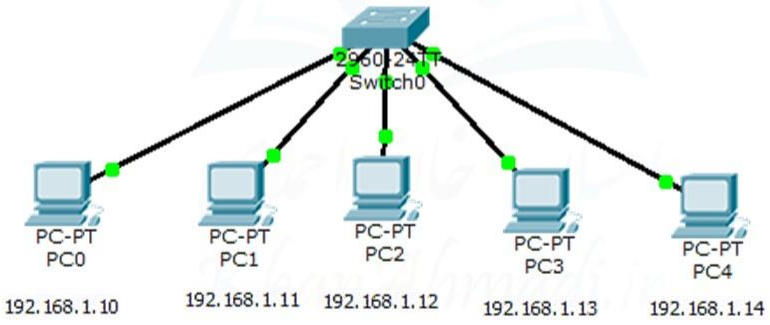
الف – شبکه‌ای به شکل راه‌اندازی کنید.



کار عملی: پیاده سازی یک شبکه با یک Switch

تمرین عملی: شبکه‌ای به شکل راه‌اندازی کنید.

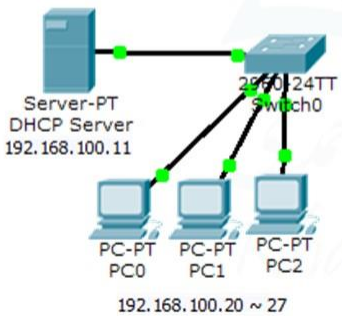




... Static IP Class C ...

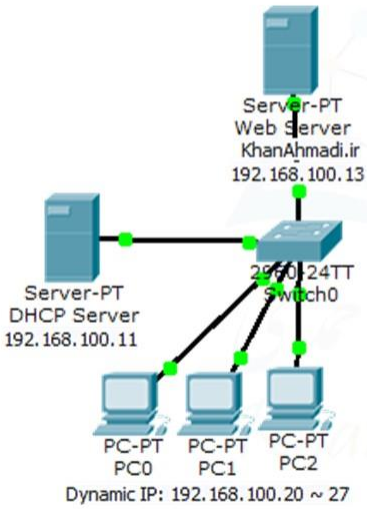
کار عملی: پیاده سازی یک شبکه با یک سرور

تمرین عملی: شبکه‌ای به شکل راه‌اندازی کنید.



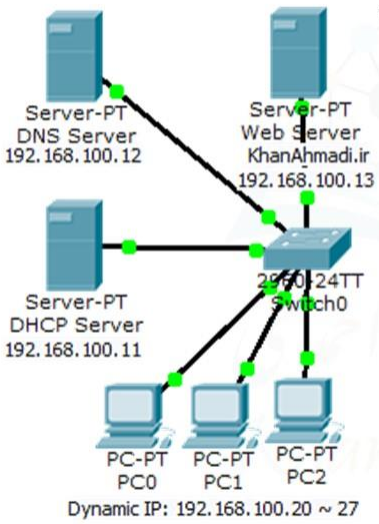
کار عملی: پیاده سازی یک شبکه با چند سرور

تمرین عملی: شبکه‌ای به شکل راه‌اندازی کنید.



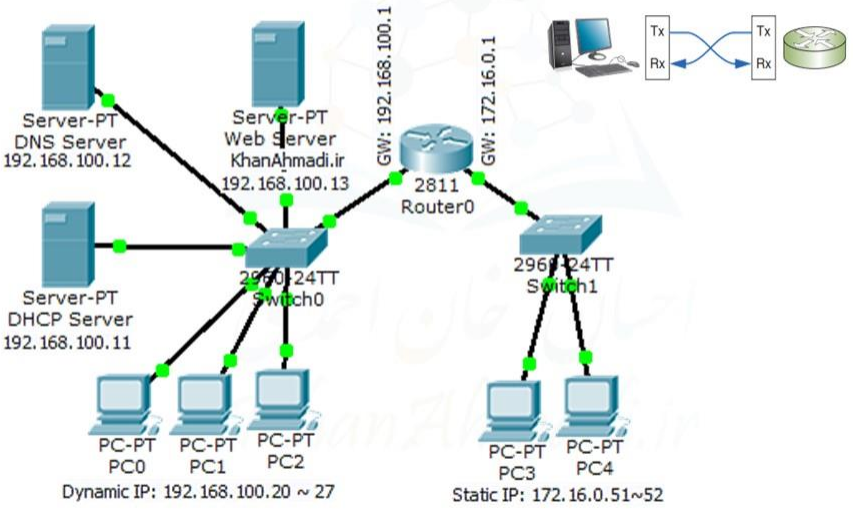
کار عملی: پیاده سازی یک شبکه با چند سرور

تمرین عملی: شبکه‌ای به شکل راه‌اندازی کنید.



کار عملی: پیاده سازی دو شبکه با چند سرور

تمرین عملی: شبکه‌ای به شکل راه‌اندازی کنید.



طراحی اتاق و تجهیزات پایش شبکه

طراحی اتاق
محل(Location)

- اتاق باید در مکانی امن، با دسترسی محدود و محافظت شده در برابر تهدیدات فیزیکی و محیطی قرار گیرد. فاصله از منابع نویز الکترومغناطیسی(EMI)، مهار نوسانات دمایی، رطوبت بالا یا خیلی کم و ارتعاشات زیاد ضروری است. TIA-942 و ISO/IEC 27001

امنیت فیزیکی (Physical Security)

- **دسترسی محدود (Access Control):** سامانه‌های مبتنی بر کارت هوشمند، زیست‌سنجی(Biometrics) یا ترکیبی برای محدود کردن ورود ضروری است. ISO 27002
- **نظارت تصویری (Video Surveillance):** نصب دوربین‌های مدار بسته با کیفیت بالا، دارای قابلیت ضبط و ذخیره‌سازی تصاویر ضروری است. NFPA 72 اعلام حریق و ارتباط اضطراری
- **سامانه اعلام و اطفاء آتش (Fire Detection and Suppression):** نصب سامانه اعلام حریق مطابق با استانداردهای NFPA 72 و اطفاء حریق (مانند گاز FM200)
- **مهار دسترسی به تجهیزات (Equipment Access Control):** استفاده از قفل‌های با کلیدهای منحصر به فرد یا قفل الکترونیکی برای مهار دسترسی به رک‌ها و تجهیزات
- **محافظت در برابر سرقت (Theft Protection):** آشکارسازهای حرکت، دزدگیر و سامانه‌های پایش امنیتی برای تشخیص و جلوگیری از سرقت

طراحی اتاق و تجهیزات پایش شبکه

طراحی اتاق
محیط (Environment)

- **مهار دما و رطوبت (Temperature and Humidity Control):** نگهداری دما بین ۱۸ تا ۲٤ درجه سانتیگراد و رطوبت ۴۰ تا ۶۰ درصد، ضروری است. (انجمن ASHRAE)
- **تهویه (Ventilation):** تهویه مطبوع با ظرفیت کافی برای خنک‌سازی تجهیزات و گردش هوای مناسب، برای جلوگیری از تجمع گرما و گرد و غبار (ASHRAE)
- **کاهش نویز (Noise Reduction):** استفاده از عایق‌های صوتی برای کاهش نویز محیطی و جلوگیری از تداخل با تجهیزات حساس
- **نورپردازی (Lighting):** استفاده از روشنایی مناسب با شدت نور کافی بدون ایجاد خیرگی یا آسیب به تجهیزات
- **اتصال زمین (Earthing/Grounding):** جلوگیری از برق گرفتگی و محافظت در برابر نوسانات ولتاژ و حفاظت در برابر صاعقه (IEC 62305 و IEEE C62.41)

فضای کافی (Sufficient Space): برای تجهیزات، کارکنان و تعمیر و نگهداری آینده‌نگرانه

کابل‌کشی (Cabling): کابل‌کشی سازماندهی شده، برچسب‌گذاری شده و استفاده از داکت‌ها و کانال‌های کابل‌کشی (TIA-568 و ISO/IEC 11801)

تجهیزات پایش شبکه

تجهیزات پایش شبکه

۱. سرورهای پایش (Monitoring Servers) با قابلیت اطمینان بالا و منابع کافی برای جمع‌آوری، پردازش و ذخیره‌سازی داده‌ها

۲. نرم‌افزارهای پایش (Monitoring Software) مانند Nagios، Zabbix، PRTG، SolarWinds و MRTG مبتنی بر نیازها و مقیاس شبکه

۳. سامانه‌های مدیریت شبکه NMS برای پیکربندی، نظارت و مدیریت کل شبکه

۴. سامانه‌های تشخیص و جلوگیری از نفوذ IDS/IPS و EDR، XDR که پیشرفته‌تر هستند

۵. دیوار آتش Firewall برای مهار ترافیک شبکه و جلوگیری از دسترسی غیرمجاز

۶. سامانه‌های ذخیره‌سازی داده Storage با ظرفیت کافی و قابلیت اطمینان بالا برای ذخیره‌سازی لاگ‌ها و داده‌های پایش و استفاده از راه‌حل‌های پشتیبان‌گیری و بازیابی اطلاعات

۷. رک‌ها و کابینت‌های استاندارد Racks and Cabinets

۸. برق فوق اضطراری UPS (Uninterruptible Power Supply) بدون قطعی با ظرفیت متناسب

۹. مولد برق Generator برای مواقع قطع برق طولانی مدت

۱۰. سوئیچ‌ها و مسیریاب‌ها Switches and Routers برای اتصال و مسیریابی ترافیک

تجهیزات پایش شبکه

نرم افزار CACTI برای پایش Linkها

یکی از نرم افزار های رایگان مانیتورینگ شبکه نرم افزار متن باز Cacti است.

نرم افزار Cacti با استفاده از پروتکل ساده مدیریت شبکه SNMP به دستگاه های شبکه متصل و آنها را در بازه های زمانی مشخص شده تحت نظر گرفته و شاخص های مورد نیاز را بررسی می کنند.

همچنین این نرم افزار امکان ارائه پنل مانیتورینگ به مشترکان را ارائه می کند. در این نرم افزار می توان تعیین کرد که مشترک پس از Login به چه Port هایی دسترسی داشته باشد.

برخی از ویژگی‌های این نرم افزار:

- بررسی قطع/وصل شدن پورت ها
- بررسی مصرف بیش از اندازه bps/pps روی پورت ها
- بررسی قطعی های یک یا چند Device در شبکه
- داشتن MAP شبکه
- بررسی Protocol های مسیریابی
- محاسبه میزان مصرف مشترکین در موارد تجاری
- تنظیم ارسال هشدار های گوناگون برای مدیران شبکه

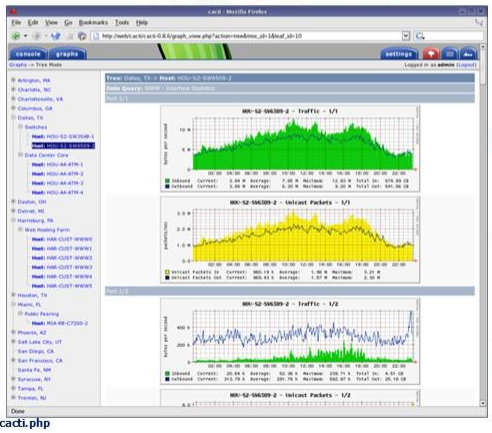
http://www.cacti.net/what_is_cacti.php

http://iranwebadmin.com

تجهیزات پایش شبکه

نرم افزار CACTI

نمایش اطلاعات به صورت گرافیکی و امکان بررسی INTERFACEهای Switchها و Routerها توسط Dual Pane Tree View

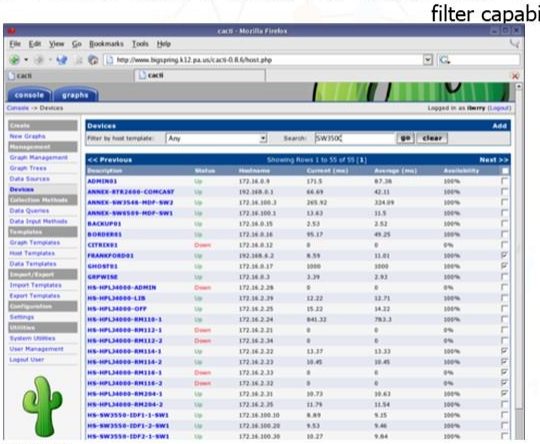


http://www.cacti.net/what_is_cacti.php

تجهیزات پایش شبکه

نرم افزار CACTI

نمایش اطلاعات به صورت گرافیکی برای بررسی و مدیریت Deviceها در host availability statistics وfilter capabilities



http://www.cacti.net/what_is_cacti.php

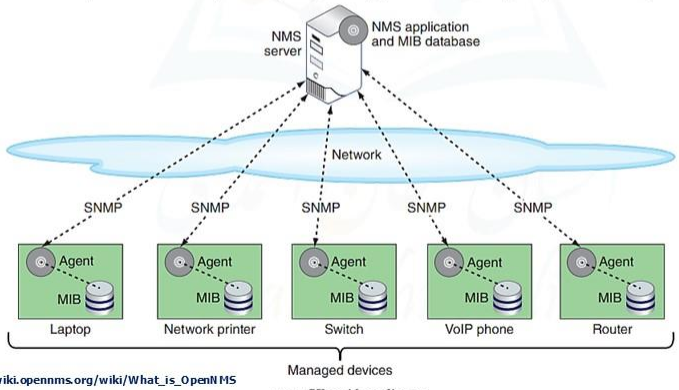
تجهیزات پایش شبکه

نرم افزار NMS:

این نرم افزار Fault Management و Performance Management را در شبکه پشتیبانی می کند.

برخی از ویژگی‌های این نرم افزار:

- مدیریت خطا: گزارش خاموشی و خرابی‌ها/رخدادها و Alarmها، گزارش آماری رخدادها
- مدیریت کارایی: نمایش کارایی سخت افزاری مثل میزان مصرف RAM،CPU و شبکه

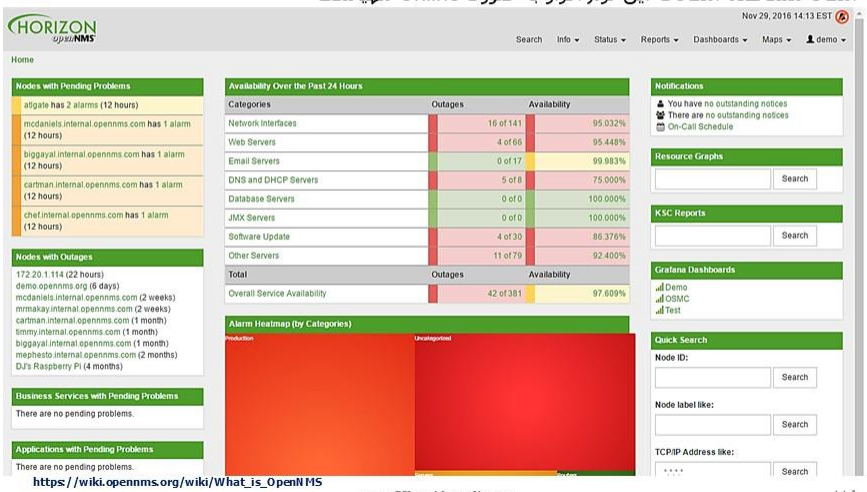


https://wiki.opennms.org/wiki/What_is_OpenNMS

تجهیزات پایش شبکه

نرم افزار NMS:

امکان مشاهده امکانات این نرم افزار به صورت Online مهیاست

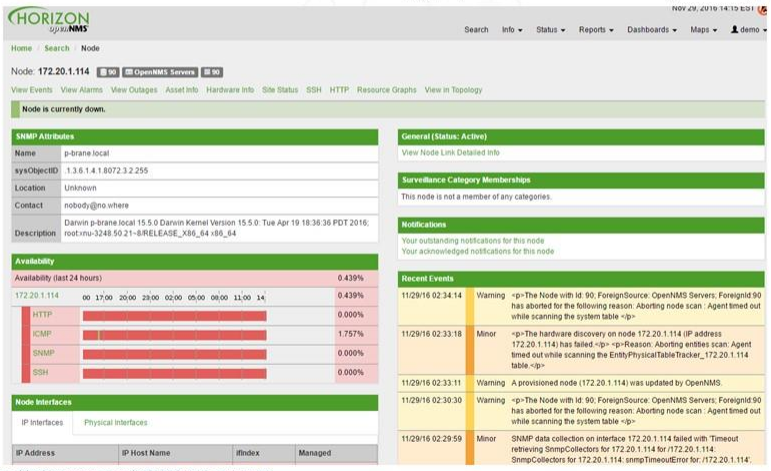


https://wiki.opennms.org/wiki/What_is_OpenNMS

تجهیزات پایش شبکه

نرم افزار NMS:

گزارش online از Network Interfaceها با جزئیات



https://wiki.opennms.org/wiki/What_is_OpenNMS

تجهیزات پایش شبکه

نرم افزار MRTG:

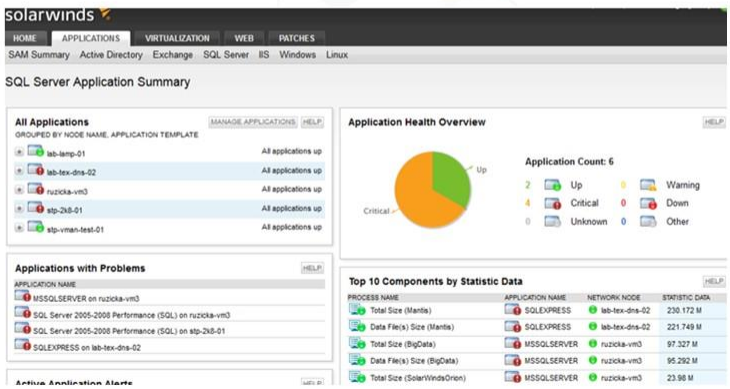
نرم افزار مدیریتی (Multi Router Traffic Grapher) MRTG در سال ۱۹۹۴ تحت (Public General) License ایجادگردید. نرم افزار مذکور برپایه زبان Perl نگارش گردیده و برای اجرا نیاز به مترجم زبان Perl دارد.

از MRTG به عنوان یکی از مهمترین ابزار Monitoring برای کنترل ترافیک Linkهای مختلف در شبکه ها استفاد ه می شود.

MRTG براساس پروتکلSNMP پایه گذاری شده است که به صورت پیش فرض v1 SNMP و درصورت نیاز v2 SNMP مورد استفاده قرار می گیرد. با استفاده از MRTG می توان تجهیزات شبکه را که از پروتکلSNMP پشتیبانی می کنند, بررسی کرد. MRTG با استفاده ازSNMP اطلاعات مورد نیاز برای Monitoring را دریافت و آنها را به صورتGraph نمایش می دهد.

تجهیزات پایش شبکه

نرم افزار مانیتورینگ SolarWinds



تجهیزات پایش شبکه

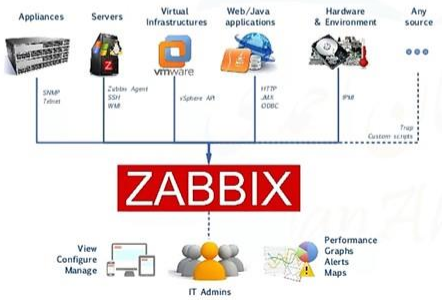
نرم افزار دیگر مانیتورینگ: PRTG

تجهیزات پایش شبکه

نرم افزار Zabbix:

نرم افزار منبع باز و رایگان پایش شبکه، Serviceها، سرورها، سخت‌افزارهای شبکه و برنامه‌هاست.

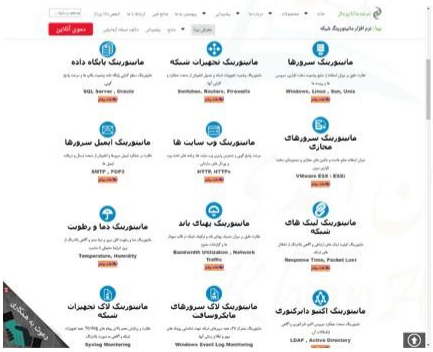
سامانه‌های عامل متنوع، تنوع روش‌های اعلام هشدار، شناسایی هوشمندانه تجهیزات و سرورهای تحت شبکه، طراحی توزیع شده برای پوشش مقیاس‌های بسیار گسترده، امکان ایجاد کلاسترهای وسیع برای پوشش ترافیک سنگین اطلاعاتی، امکان گسترش و سفارشی‌سازی سامانه، مقیاس‌پذیری ساده، پشتیبانی از SNMP، مانیتورینگ زیرساخت مجازی،پایش بانک‌های اطلاعاتی و وب سرویس‌ها، سرورهای جاوا، سخت افزارها، شرایط محیطی



تجهیزات پایش شبکه

امکانات نرم افزار ایرانی مانیتورینگ شبکه بینا:

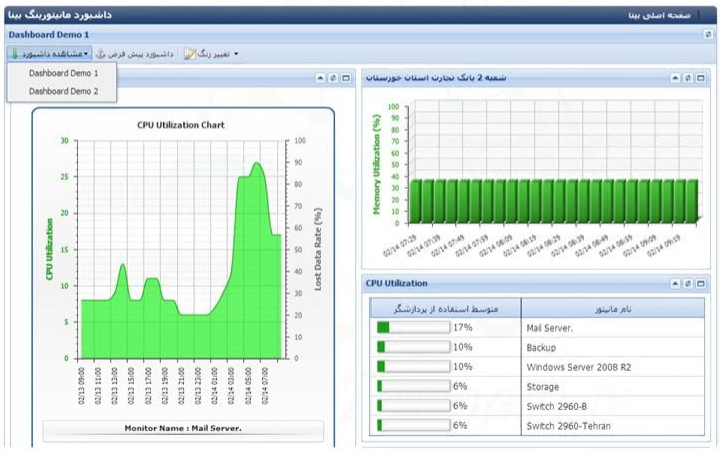
نرم افزار مانیتورینگ شبکه بینا نرم افزاری پیشرفته برای مانیتورینگ شبکه و دیتاسنتر می باشد. بینا کلیه سرویس های موجود بر روی شبکه را به صورت ۲۴ ساعته نظارت می کند و در صورت ردیابی هرگونه اختلال و اشکال، با ارسال انواع اخطار، مسئولان شبکه را از موضوع با خبر می سازد. گزارشات بینا تصویری واضح از سطح کیفیت سرویس های فناوری اطلاعات ارائه می دهد.



http://www.danapardaz.net/site/bina

تجهیزات پایش شبکه

- مانیتورینگ شبکه بینا: (**گزارش ها و داشبورد**)



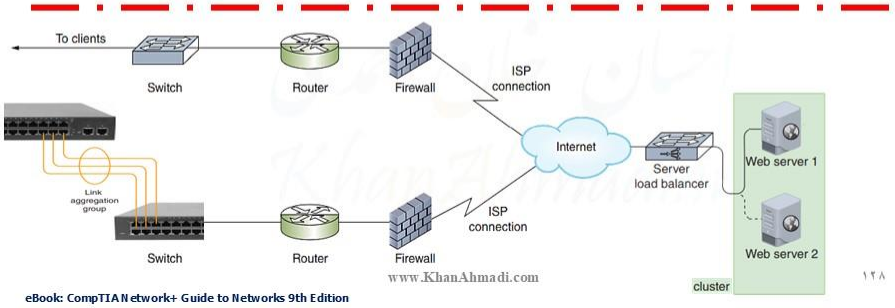
http://www.danapardaz.net/site/bina

پایش شبکه و اندازه‌گیری میزان دردسترس بودن خدمات

- MTBF (mean time between failures)
- MTTR (mean time to repair)

استفاده از Redundancy برای افزایش Availability

- Single Internet link connectivity vs Fully redundant ISP connectivity and cluster web



طراحی اتاق و تجهیزات پایش شبکه

ملاحظات اضافی طراحی اتاق و تجهیزات پایش شبکه

- افزونگی Redundancy برای افزایش قابلیت اطمینان و جلوگیری از اختلال در عملکرد
- طرح بازیابی فاجعه Disaster Recovery Plan را از قبل آماده کرده و تمرین شده باشد
- آموزش کارکنان Staff Training در مورد استفاده و نگهداری از تجهیزات و اقدامات امنیتی و برگزاری مانورهای دوره‌ای و موردی

توجه به استانداردهای

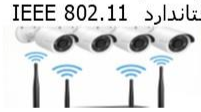
- ISO 27001 استاندارد بین المللی برای سیستم مدیریت امنیت اطلاعات
- NIST Cybersecurity Framework چارچوب سایبری برای مدیریت مخاطرات سایبری
- ITIL (Information Technology Infrastructure Library) بهترین روش‌ها برای خدمات IT
- ISO 22301 استاندارد مدیریت تداوم کسب و کار

اتصالات دوربین‌های شبکه و اتصال به شبکه آن

انواع اتصالات دوربین‌های شبکه

اتصال سیمی Wired Connection: با استفاده از کابل شبکه مانند کابل Cat5e یا Cat6 و پورت اترنت دوربین انجام می‌شود. این روش پایداری و سرعت انتقال داده بالاتری را نسبت به اتصال بی‌سیم ارائه می‌دهد و در محیط هایی که نیاز به امنیت و پایداری بالا وجود دارد، ترجیح داده می‌شود. (استاندارد TIA-568 برای کابل‌کشی ساخت‌یافته و IEEE 802.3 اترنت)

اتصال بی‌سیم Wireless Connection: با استفاده از استانداردهای Wi-Fi مانند IEEE 802.11a/b/g/n/ac/ax انجام می‌شود. این روش انعطاف‌پذیری بیشتری دارد اما ممکن است مستعد تداخل و اختلالات بی‌سیم باشد و سرعت انتقال داده، امنیت و پایداری آن به نسبت اتصال سیمی کمتر است. امنیت در این روش باید به درستی پیکربندی شود. (استاندارد IEEE 802.11 Wi-Fi، WPA2/WPA3 پروتکل‌های امنیتی Wi-Fi)



اتصال فیبر نوری Fiber Optic Connection: در مواردی که مسافت طولانی بین دوربین و دستگاه ضبط یا سوئیچ وجود دارد یا محیط دارای اختلالات الکتریکی است، از اتصال فیبر نوری استفاده می‌شود که اگر درست طراحی و پیاده‌سازی شود امنیت بیشتری هم دارد. این روش انتقال داده با سرعت بالا و بدون افت کیفیت ارائه می‌دهد و در برابر تداخل الکترومغناطیسی مقاوم است. (TIA-492 استاندارد کابل فیبر نوری)

اتصالات دوربین‌های شبکه و اتصال به شبکه آن

ملاحظات اتصال دوربین به شبکه

نشانی IP Address، Subnet Mask و تنظیمات TCP/IP: هر دوربین IP به یک نشانی IP منحصر به فرد در شبکه نیاز دارد که می‌تواند به صورت دستی Static IP یا به صورت پویا Dynamic IP از طریق(Dynamic Host Configuration Protocol) DHCP تخصیص داده شود. استفاده از Static IP برای مدیریت و پیکربندی آسان‌تر دوربین‌ها توصیه می‌شود. برای ارتباط دوربین با شبکه‌ی گسترده نیاز به تنظیم Gateway در تنظیمات دوربین وجود دارد. استاندارد RFC 791 برای IP Protocol

DNS (Domain Name System) برای دسترسی به دوربین از طریق نام دامنه Domain Name، نیاز است DNS در تنظیمات دوربین پیکربندی شود.

دوربین‌های IP از پروتکل‌های شبکه Network Protocols مختلفی مانند TCP/IP, UDP, RTP و HTTP/HTTPS استفاده می‌کنند.

در پیکربندی دوربین‌های IP از روش‌های امنیتی مناسب برای جلوگیری از دسترسی غیرمجاز استفاده می‌شود. مانند استفاده از رمزهای عبور قوی، دیوار آتش، SSL/TLS برای رمزگذاری ارتباطات و به‌روزرسانی‌های منظم نرم‌افزار دوربین. استاندارد ISO/IEC 27001 مدیریت امنیت اطلاعات NIST Cybersecurity Framework

برای تضمین کیفیت انتقال داده‌های ویدئویی در شبکه، QoS (Quality of Service) پیکربندی می‌شود که به اولویت‌بندی ترافیک ویدئویی نسبت به سایر ترافیک‌های شبکه کمک می‌کند.

با تنظیم درست مدیریت پهنای باند Bandwidth Management در دوربین‌های IP، هم پهنای باند کافی برای تمام دوربین‌ها در نظر گرفته می‌شود و هم از روش‌های مدیریت پهنای باند مانند کم کردن رزولوشن تصاویر برخی دوربین‌ها یا Frame Rate در صورت نیاز استفاده می‌شود.

اتصالات دوربین‌های شبکه و اتصال به شبکه آن

اتصال دوربین به دستگاه ذخیره‌سازی و نرم افزار مدیریت NVR/VMS

دوربین‌های IP می‌توانند به یک دستگاه ضبط کننده‌ی ویدئویی شبکه Network Video Recorder که به اختصار NVR نامیده می‌شود یا سامانه مدیریت ویدئویی Video Management System VMS متصل شوند تا تصاویر ضبط و مدیریت شوند. اتصال این دوربین‌ها به NVR/VMS معمولاً از طریق شبکه با پیکربندی درست نشانی‌های IP، پورت‌ها و پروتکل‌ها انجام می‌شود.

RAID (Redundant array of inexpensive Disks) شدن هاردها باعث افزایش سرعت و/یا اطمینان ضبط تصاویر می‌شود.

فناوری PoE برق را از راه شبکه به دوربین‌ها منتقل می‌کند البته به شرط استفاده از سوئیچ PoE

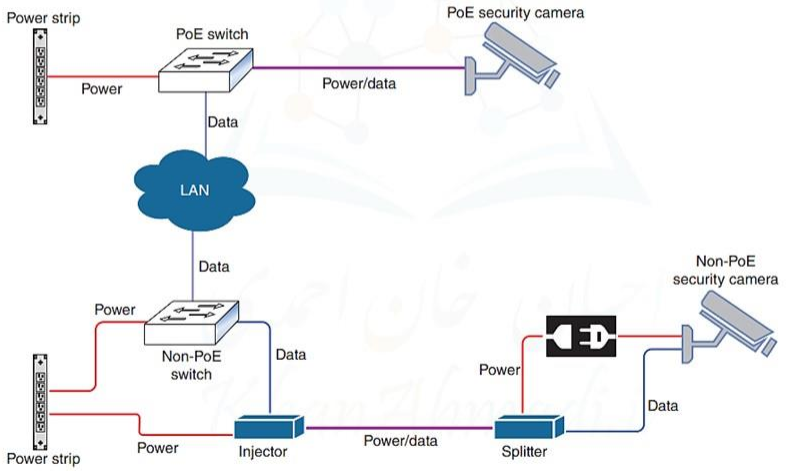
بهترین روش اتصال دوربین‌ها به فضای ابری با استفاده یک ارتباط مطمئن است زیرا دستگاه ذخیره کننده تصاویر در محل نیست و امکان به سرقت رفتن آنها یا ازبین رفتن آنها توسط سارقان یا خراب‌کارها وجود ندارد.

عیب‌یابی

- بررسی کابل‌ها و اتصالات فیزیکی
- بررسی نشانی‌های IP، Subnet Mask و Gateway
- بررسی تنظیمات دیوار آتش و مسیریاب
- بررسی پهنای باند شبکه
- بررسی تنظیمات دوربین و NVR/VMS
- استفاده از ابزارهای عیب‌یابی شبکه

اتصالات دوربین‌های شبکه و اتصال به شبکه آن

آداپتورهای PoE می‌توانند قابلیت PoE را به دستگاه‌های غیر PoE روی شبکه اضافه کنند.



کابل‌کشی برق و اتصالات برق تجهیزات

مراحل کابل‌کشی برق و اتصالات برق تجهیزات

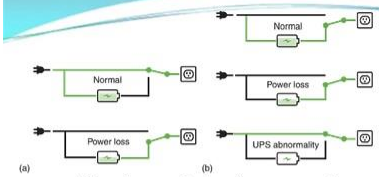
- تعیین نوع و ظرفیت کابل برق مورد نیاز برای هر دستگاه مبتنی بر مشخصات فنی آن
- تعیین مسیر کابل‌کشی با توجه به کمینه شدن مصرف کابل و محل قرارگیری تجهیزات، ملاحظات ایمنی (فاصله از آب، مواد قابل اشتعال) و زیبایی‌شناسی
- کابل‌کشی با استفاده از روش‌های استاندارد با بست‌های مخصوص کابل
- اجرای اتصالات برق با استفاده از ابزارهای مناسب و رعایت ملاحظات ایمنی (قطع برق پیش از اتصال، استفاده از عایق‌بندی مناسب)
- برای تجهیزات حساس، استفاده از محافظهای اضافه ولتاژ (Surge Protector) ضروری است.

نکات کلیدی:

انتخاب نوع مناسب کابل (NYY، NYMHY یا کابل‌های قدرت)، رنگ‌بندی سیم‌ها، محاسبه ظرفیت کابل بر اساس آمپر مورد نیاز، استفاده از جعبه‌های تقسیم برق Junction Boxes، استفاده از فیوزها و کلیدهای محافظ (RCDs) برای ایمنی

ویژگی	کابل NYY	کابل NYMHY
انعطاف پذیری	محدود	بسیاربالا
محیط نصب	زیرزمین، فضای باز، مرطوب	داخل ساختمان خشک
مقاومت الکتریکی	بالا با عایق دولایه	متوسط
هزینه	به نسبت مقرون به صرفه	کمی گران‌تر

نصب و راه‌اندازی تجهیزات برق اضطراری UPS



انواع UPS (Uninterruptible Power Supply)

۱. Standby

- ارزان‌ترین، ساده‌ترین و کم‌هزینه‌ترین نوع است که کمترین کیفیت برق را دارد زیرا offline است و فقط هنگام قطع برق اصلی، برق باتری را به بار می‌دهد. هیچ فیلتر یا تنظیم ولتاژی ندارد. در هنگام سوییچ به باتری ممکن است وقفه‌ای کوتاه در برق ایجاد شود.
- مناسب برای بارهای کم حساس به نویز و تجهیزاتی که به کیفیت برق حساس نیستند مثلا برخی از چاپگرها، مودم ها، تجهیزات VoIP

۲. Line-interactive

- قیمت و کیفیت برق متوسطی دارد زیرا از یک AVR (Automatic Voltage Regulator) برای تنظیم ولتاژ در حالت عادی استفاده می‌کند. در هنگام قطع برق، به باتری سوئیچ می‌کند. کیفیت برق خروجی نسبت به UPSهای آفلاین بهتر است.
- مناسب برای برخی کامپیوترها

۳. Online

- گران‌ترین و پیشرفته‌ترین نوع UPS است زیرا بالاترین کیفیت برق زیرا همیشه از طریق یک Inverter، برق AC را از باتری تولید می‌کند. حتی در حالت عادی، برق از باتری تأمین می‌شود و برق اصلی فقط برای شارژ باتری استفاده می‌شود. در نتیجه، کیفیت برق خروجی بسیار بالا و بدون نویز است. هیچ وقفه‌ای در برق در هنگام سوءپچ به باتری وجود ندارد.
- مناسب برای بارهای حساس مانند سرورها و تجهیزات پزشکی
-

نصب و راه‌اندازی تجهیزات برق اضطراری UPS

شش مرحله نصب و راه‌اندازی UPS (Uninterruptible Power Supply)

- بسته به نوع UPS (آفلاین، لاین‌اینتر اکتیو یا آنلاین) و مدل و ویژند آن متفاوت است اما مراحل کلی به صورت زیر است:

۱. برنامه‌ریزی و آماده‌سازی

- محاسبه میزان توان برق مصرفی مورد نیاز، زمان پشتیبان‌گیری مورد نیاز، حساسیت دستگاه‌ها و انتخاب UPS مناسب با نوع، ظرفیت و ویژگی‌های مناسب برای بار مورد نظر.
- محل نصب UPS دارای تهویه مناسب، فضای کافی و دسترسی آسان برای تعمیر و نگهداری باشد. UPS در محیط‌های مرطوب، گرد و غبار و دمای بالا نباشد.
- بررسی الزامات برق و اطمینان از ظرفیت کافی تأمین برق UPS از منبع برق اصلی (پریز برق) و بار متصل به آن
- آماده‌سازی تجهیزات و کابل‌های مورد نیاز

۲. نصب فیزیکی UPS

- باز کردن بسته‌بندی UPS و بررسی محتویات جعبه
- قرار دادن UPS در محل مناسب، پایدار و محکم
- اتصال کابل برق UPS به منبع تغذیه (پریز برق دارای ارت مناسب)

۳. اتصال تجهیزات به UPS

- اتصال تجهیزات به پورت‌های خروجی UPS با توجه به ترتیب و ظرفیت خروجی‌ها
- بررسی اتصالات قبل از روشن کردن

نصب و راه‌اندازی تجهیزات برق اضطراری UPS

شش مرحله نصب و راه‌اندازی UPS (Uninterruptible Power Supply)

۴. راه‌اندازی و پیکربندی UPS

- روشن کردن UPS
- بررسی وضعیت باتری با نشانگرهایی که برای نمایش وضعیت باتری دارد
- پیکربندی تنظیمات (در صورت نیاز) مثلا، شیوه‌ی واکنش هنگام قطع برق
- نصب نرم‌افزار مدیریت که امکان نظارت و کنترل UPS فراهم شود

۵. آزمایش و تأیید

- آزمایش عملکرد برای اطمینان از عملکرد درست UPS با قطع آزمایشی منبع تغذیه (با احتیاط و رعایت نکات ایمنی) و بررسی تأمین درستی برق پشتیبان
- بررسی و مقایسه زمان پشتیبان‌گیری واقعی UPS با زمان پشتیبان‌گیری اعلام شده

۶. نگهداری

- بررسی منظم و دوره‌ای وضعیت UPS و باتری‌های آن
- آزمایش باتری به طور دوره‌ای و بررسی عملکرد درست آن
- تعویض باتری UPS طبق دستورالعمل سازنده

نصب و راه‌اندازی تجهیزات برق اضطراری UPS

نکات کلیدی نصب و راه‌اندازی UPS (Uninterruptible Power Supply)

- **ظرفیت UPS**
  - توان Power Capacity بر حسب ولت‌آمپر VA یا وات W است که برای دستگاه‌های موتوری، VA مهم‌تر است. ظرفیت UPS باید بیشتر از مجموع توان مصرفی دستگاه‌های متصل باشد.
  - زمان پشتیبان‌گیری Backup Time بر حسب دقیقه یا ساعت که نشان می‌دهد UPS تا چه مدت می‌تواند در زمان قطع برق، برق تأمین کند. این زمان به ظرفیت باتری و مصرف انرژی دستگاه‌های متصل بستگی دارد.

- **نوع باتری**
  - باتری‌های سرب-اسیدی Lead-Acid:
    - قیمت پایین، در دسترس، نگهداری آسان، عمر محدود (۳ سال)، حساس به دما
    - AGM مقاوم به ضربه، ژل Gel Cell مقاوم به ضربه و دما، معمولی Flooded Lead-Acid
  - باتری‌های لیتیوم-یون Lithium-ion
    - عمر مفید طولانی‌تر (تا ۱۰ سال)، وزن کمتر، چگالی انرژی بالاتر، راندمان شارژ بهتر
    - قیمت بالاتر، نیاز به سیستم مدیریت باتری پیشرفته BMS
  - باتری‌های نیکل-کادمیوم Nickel-Cadmium:
    - مشکلات زیست‌محیطی، عملکرد پایین، استفاده کم

نصب و راه‌اندازی تجهیزات برق اضطراری UPS

نکات کلیدی نصب و راه‌اندازی UPS (Uninterruptible Power Supply)

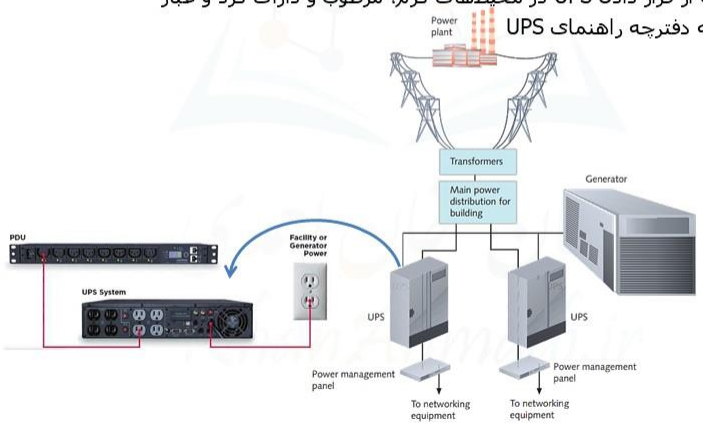
- **اتصال UPS به شبکه برای پایش**
  - از طریق پورت شبکه، پورت سریال، SNMP یا نرم‌افزار اختصاصی، امکان پایش از راه دور متغیرهایی مانند وضعیت باتری، برق ورودی، بار و رویدادها را فراهم می‌کند. این امر به مدیریت مرکزی، هشدارهای خودکار، پیشگیری از خرابی و گزارش‌گیری منجر شده و نیازمند پیکربندی صحیح و سازگاری با پروتکل‌های شبکه است.

- **روش آزمایش باتری Load Test**
  - آزمون بار Load Test یک UPS آزمایش عملکرد باتری آن تحت بار است. در این آزمایش، UPS به یک بار Load مشخص که معمولا به صورت مقاومتی یا شبیه‌ساز بار است، متصل می‌شود و به مدت زمان معین زیر بار قرار می‌گیرد. هدف از این آزمایش بررسی توانایی UPS در تأمین برق به بار در مدت زمان مورد انتظار و ارزیابی سلامت باتری و عملکرد UPS در شرایط نزدیک به شرایط واقعی است. داده‌های به‌دست‌آمده از آزمون بار (مانند ولتاژ، جریان، زمان عملکرد باتری) به ارزیابی سلامت باتری و پیش‌بینی عمر باقی‌مانده آن کمک می‌کند. آزمون بار به‌طور معمول در آزمایش‌های دوره‌ای و پیشگیرانه UPS انجام می‌شود.

نصب و راه‌اندازی تجهیزات برق اضطراری UPS

نکات ایمنی نصب و راه‌اندازی UPS (Uninterruptible Power Supply)

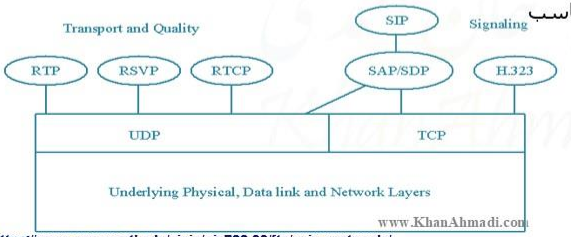
- اطمینان از قطعی برق قبل از کار با UPS و کابل و تجهیزات برق
- جلوگیری از اتصال بیش از حد بار به UPS
- اجتناب از قرار دادن UPS در محیط‌های گرم، مرطوب و دارای گرد و غبار
- مطالعه دفترچه راهنمای UPS



نصب و راه‌اندازی سامانه و تجهیزات مرکزی تلفن

- متناسب با نوع سامانه تلفن آنالوگ یا رقومی و VoIP متفاوت است. در سامانه‌های آنالوگ، از یک PBX (Private Branch Exchange) و کابل‌های تلفن بهره برده می‌شود.
- در سامانه‌های VoIP، معمولا از یک Gateway VoIP و اتصال به اینترنت استفاده می‌شود. کابل‌کشی تلفن و اتصالات به دستگاه‌های تلفن باید به درستی انجام شود. پیکربندی شبکه، نشانی IP و تنظیمات VoIP هم از دیگر اقدامات ضروری است.

- ملاحظات کلیدی:
  - انواع مختلف سامانه‌های تلفن
  - کابل‌کشی تلفن با کابل‌های UTP
  - کابل‌های فیبر نوری
  - چند نمونه از پروتکل‌های VoIP: SIP، RTP، H.323
  - انتخاب PBX و Gateway مناسب

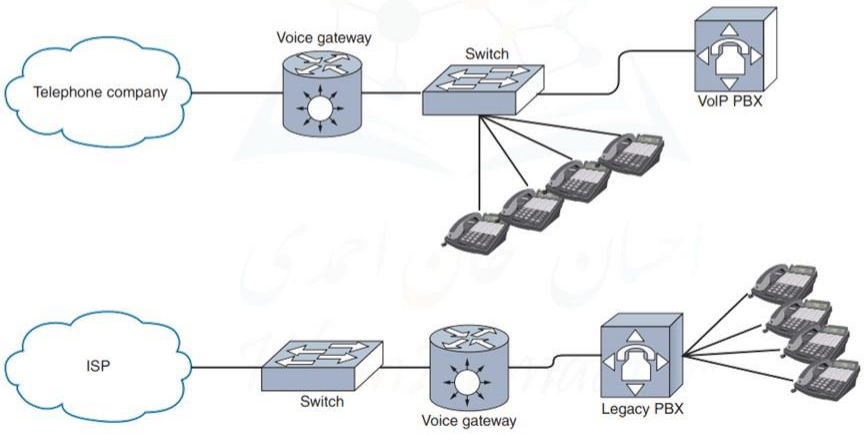


۱۴۱

https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/

نصب و راه‌اندازی سامانه و تجهیزات مرکزی تلفن

- تجهیزات VoIP می‌توانند تلفن‌های VoIP را به یک خط تلفن آنالوگ متصل کنند یا یک سامانه تلفن آنالوگ را به اینترنت ارتباط دهند.



۱۴۲

https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/

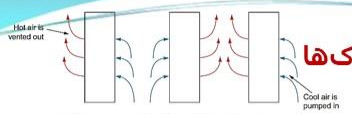
نصب سامانه‌های امنیتی و دیوارآتش‌های سخت‌افزاری

مراحل نصب سامانه‌های امنیتی و دیوارآتش‌های سخت‌افزاری

- نیازسنجی و مستندسازی، تحلیل نیازها
- طراحی و انتخاب دیوارآتش (Firewall) مناسب با توجه به نیازهای امنیتی و طراحی
- آزمایش، نصب و راه‌اندازی فیزیکی دیوارآتش در شبکه
- پیکربندی دیوارآتش و آزمون‌ها، فرآیند به‌روزرسانی، نگهداری، طرح مواجهه با خرابی و تغییر
  - تنظیم قوانین فایروال (Firewall Rules)
  - ایجاد Virtual Local Networks (VLANs) و Trust/Untrust Zones
  - تعریف Access Control Lists (ACLs) و VPN
- ترکیب سامانه‌های امنیتی: IDS/IPS (Intrusion Detection/Prevention System) و XDR

ملاحظات کلیدی:

عملکرد دیوارآتش‌ها (Stateful, Stateless) ، ذخیره و بررسی Logها برای تشخیص حملات، به‌روزرسانی منظم Firmware و نرم‌افزار دیوارآتش، آزمون‌های دوره‌ای و موردی



نصب تجهیزات استقرار سرور، طراحی و نصب رک‌ها

- طراحی و انتخاب رک با توجه به تجهیزات شبکه/سرور/مخصوص تهویه و تعداد و ابعاد تجهیزات
- نصب رک با توجه به وزن، مسائل اتصال به زمین، ابعاد و تهویه و ایجاد راهرو سرد و گرم
- قرار دادن سرورها و سایر تجهیزات در رک با توجه به وزن و تهویه مناسب
- کابل‌کشی سرورها و استفاده از Cable Management برای سازماندهی کابل‌ها
- ظرفیت تحمل وزن رک، تهویه مناسب، زمین کردن مناسب، Cable Management

نصب سامانه‌های ورود و خروج

عوامل انتخاب سامانه ورود و خروج: سطح امنیت مورد نیاز، بودجه، اندازه اتاق و تعداد کاربران

سامانه مکانیکی امنیت پایین، سامانه الکترونیکی با کارت یا رمز عبور امنیتی متوسط و سامانه‌های زیست‌سنجی Biometrics (اثر انگشت، تشخیص چهره) امنیت بالا و ترکیب عوامل مناسب‌تر و گران‌ترند.

مراحل نصب:

- نیازسنجی، طراحی و برنامه‌ریزی مطابق استانداردهای امنیتی، مقاوم بودن در شرایط محیطی مختلف، هماهنگی با سایر سامانه‌ها مانند نظارت تصویری و Redundancy و پشتیبان
- تهیه تجهیزات، نصب سخت‌افزار، اتصال به منبع تغذیه UPS و کابل‌کشی از مسیرهای امن، تله
- پیکربندی نرم‌افزار مدیریت مانند تعریف کاربران، تنظیم ساعات کاری و مجوزهای ورود و خروج و ذخیره‌سازی امن اطلاعات، راه‌اندازی و آموزش
- به‌روزرسانی‌های منظم، نگهداری و پشتیبانی فنی، مدیریت دسترسی و گزارش‌گیری مستمر



نصب سوئیچ‌ها، مسیریاب‌ها و کانکتورهای شبکه برای اتصال بخش‌ها

برنامه‌ریزی و طراحی

- ترسیم نقشه شبکه با جزئیات کامل Nodeها مبتنی بر طرح نیازمندی‌ها با مشخص شدن محل قرارگیری سوئیچ‌ها، مسیریاب‌ها و اتصالات، مسیر و نوع کابل‌کشی فاقد خمیدگی‌های آسیب‌زا و مسیرهای طولانی که نوع کابل (کابل مسی یا فیبر نوری) مبتنی بر فاصله و سرعت مورد نیاز باشد و سپس محاسبه تجهیزات تعداد Nodeهای مشخص شده در نقشه، طول کابل و تجهیزات مورد نیاز در نظر گرفتن فضای اضافی برای گسترش آینده

آماده‌سازی محیط

- مکانی با فضای کافی و دارای اتصال به زمین و تهویه مناسب (دما ۱۸ تا ۲۷ درجه سانتیگراد با رطوبت نسبی ۴۰ تا ۵۵ درصد طبق نظر انجمن ASHRAE)، بدون پنجره مستقیم نفوذ نور خورشید، گرد و غبار و رطوبت

اجرای داکت، سینی، کابل‌کشی، برچسب‌زنی و اتصال کانکتورها

- آزمایش کیفیت تجهیزات و کابل‌ها پیش و پس از اجرا و آرایش کابل‌ها با بست‌های پارچه‌ای، پانچ کانکتورهای RJ45 برای کابل‌های مسی مانند Cat6، Cat6a، Cat7 یا بالاتر و آزمایش
- نکته: سازماندهی منظم کابل‌ها و اتصالات منظم و تولید مستندات دقیق، دسترسی به تجهیزات، توسعه و عیب‌یابی را سریع‌تر و آسان‌تر می‌کند.

نصب سوئیچ‌ها، مسیریاب‌ها و کانکتورهای شبکه برای اتصال بخش‌ها

پیکربندی و آزمایش شبکه برای اطمینان از عملکرد درست و امن شبکه

مراحل عملی:

- پیکربندی IP Address و تنظیمات TCP/IP طبق طرح برای تجهیزات شبکه و Clientها
- پیکربندی VLAN در صورت لزوم به تقسیم شبکه به بخش‌های منطقی و افزایش امنیت
- پیکربندی مسیریاب، قوانین دیوار آتش، ضدبدافزار
- پیکربندی فرآیند به‌روزرسانی تجهیزات و OS، برنامه‌ها و ضدبدافزار Clientها و ابزارهای پایش
- تهیه بازبینه یعنی Checklistنگهداری، بازدید دوره‌ای و آزمایش و به‌روزرسانی بازبینه
- آموزش اجرای بازبینه و استفاده از ابزارهای شبکه مانند ping، traceroute، nslookup، arp
- طراحی فرآیندهای عیب‌یابی، چارچوب خدمات مانند ITIL به خصوص مدیریت رخداد و تغییر، طرح بازیابی فاجعه DRP با بررسی مرحله‌ای مشکلات: کابل، کانکتور، IP، مسیریاب و ...

نکته:

- علاوه بر Backupگیری دوره‌ای، پیش از هر تغییر مهم در پیکربندی، از تنظیمات فعلی شبکه پشتیبان تهیه شود.

راه‌اندازی تجهیزات اتاق‌سرور و تجهیزات نگهداری از اتاق‌سرور

مراحل راه‌اندازی بسته به سطوح Tier 1 تا Tier 4 متفاوت است. برای یک اتاق سرور کوچک:

۱. نیازسنجی، تحلیل نیازها، برنامه‌ریزی و طراحی طبق BICSI 002

- تعیین ظرفیت، اهداف عملکردی و نوع تجهیزات، الزامات شبکه، ذخیره‌سازی و برق، طراحی نگهداری پیشگیرانه + اصلاحی Preventive + Corrective Maintenance

۲. انتخاب محل مناسب برای اتاق‌سرور

- دسترسی محدود و امن، مصالح ضدحریق، نفوذناپذیری منابع نور مستقیم خورشید، رطوبت و گردوغبار، حیوانات

۳. آماده‌سازی زیرساخت فیزیکی

- کف کاذب و مدیریت کابل، تهویه مطبوع HVAC، توزیع برق مستقل برای رک‌ها و تجهیزات، برق اضطراری UPS و ژنراتور، حسگرها، دوربین‌ها و پیکربندی سامانه ضدآتش و دود مطابق NFPA 75 و NFPA 76

۴. نصب رک‌ها و تجهیزات اصلی

- نصب مستحکم رک‌ها و اتصال به زمین، فاصله مناسب رک‌ها و ایجاد راهرو سرد و گرم Hot & Cold Aisle، نصب سرورها، سوئیچ‌ها، تجهیزات ذخیره‌سازی

۵. کابل‌کشی ساخت‌یافته Structured Cabling

- استفاده از کابل‌های Cat6a، Cat7 یا بالاتر یا فیبر نوری، برچسب‌گذاری و مستندسازی دقیق، رعایت مسیرهای مجزا برای برق ترجیحاً از راهرو سرد و داده با فاصله از برق، ISO 11801، NEC (National Electrical Code) مقررات نصب کابل در مسیرهای برق و داده و آزمایش Fluke برای تایید عملکرد لینک‌ها با اندازه‌گیری NEXT(Crosstalk)، RL (Return Loss)، Delay، Loss

راه‌اندازی تجهیزات اتاق‌سرور و تجهیزات نگهداری از اتاق‌سرور

موارد نگهداری استاندارد اتاق‌سرور

۱. پایش و مهار محیطی مستمر

- دما ۱۸–۲۷ درجه سانتی‌گراد، رطوبت: ۴۰–۶۰٪، پایش لحظه‌ای با حسگرها و دوربین

۲. پایش و هشداردهی

- استفاده از سیستم‌های NMS یا DCIM، آگاه‌سازی لحظه‌ای از رخدادها SMS/Email

۳. نگهداری منظم Preventive Maintenance

- بررسی دوره‌ای باتری UPS، اتصالات و سامانه ضدآتش، تمیزکاری رک‌ها و فیلترهای تهویه، آزمایش پشتیبان‌گیری و بازیابی اطلاعات

۴. امنیت فیزیکی و منطقی

- دسترسی با کارت یا مشخصات زیستی یا رمز یا ترکیبی، دوربین CCTV، ثبت ورود و خروج کاربران و تجهیزات، پایش سیگنال‌ها و تغییرات محیط، کاربران و Adminها

۵. مستندسازی و به‌روزرسانی

- نقشه شبکه، فهرست تجهیزات و کابل‌ها و نرم افزارها، سوابق، رخدادها و اقدامات اصلاحی

۶. پیاده‌سازی و تمدید گواهینامه‌های امنیت و خدمات

- پیکربندی استانداردها و چارچوب‌های پیاده‌سازی و نگهداری مانند TIA-942، امنیت مانند ISMS و ISO 27000، ارائه خدمات مانند ITIL و ISO 20000، اجرای دوره‌ای آزمون و مانور

نصب و راه‌اندازی تجهیزات شبکه‌های بی‌سیم

مراحل عملی نصب و راه‌اندازی تجهیزات شبکه بی‌سیم

۱. نیازسنجی، تحلیل نیازها، برنامه‌ریزی و طراحی طبق IEEE 802.11 و سایر

- تحلیل تعداد و حجم نیازمندی هر کاربر، نوع ترافیک و پوشش مورد نیاز
- انتخاب نوع شبکه WLAN، Mesh، Point-to-Point یا WWAN، cellular
- تعیین مکان نصب Access Pointها

۲. بررسی محیط نصب Site Survey

- بررسی محیط واقعی با ابزارهایی مانند Ekahau یا NetSpot WiFi Heat Map Analyzer
- شناسایی نویز interference یعنی تداخل امواج و موانع فیزیکی
- طراحی چیدمان AP بر اساس نتایج heatmap

۳. نصب سخت‌افزار و اتصال به شبکه

- نصب فیزیکی APها در ارتفاع مناسب (توصیه استاندارد: بین ۲٫۴ تا ۳٫۶ متر)
- اتصال APها به سوئیچ PoE برای انتقال برق از کابل شبکه یا منبع تغذیه فوق اضطراری مجزا
- کابل‌کشی ساخت‌یافته تا رک مرکزی TIA-568-C

۴. پیکربندی نرم‌افزاری، آزمایش و بررسی دوره‌ای

- کانال مناسب، اختصاص SSID، رمزنگاری 802.1X + RADIUS و WPA3، تنظیم VLAN، QoS
- تعریف DHCP، دیوار آتش و محدودیت گذاری روی MAC Address
- فعال‌سازی کنترل دسترسی Radius/AAA

نصب و راه‌اندازی تجهیزات شبکه‌های بی‌سیم

تصویر نقشه حرارتی Wi-Fi تولید شده توسط NetSpot

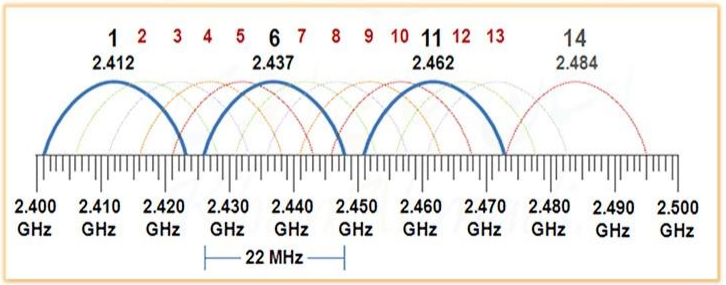
قسمت‌های مختلف نقشه رنگ‌های متفاوتی دارند.
رنگ قرمز به معنای سیگنال بسیار قوی (hot)، سبز به معنای سیگنال متوسط و آبی به معنای سیگنال ضعیف (cold) است.

نصب و راه‌اندازی تجهیزات شبکه‌های بی‌سیم

Wi-Fi Channels

بهینه‌سازی عملکرد و کاهش تداخل interference در شبکه‌های Wi-Fi
اجتناب از هم‌پوشانی فرکانس بین APها مجاور
استفاده از کانال‌های غیرهم‌پوشان می‌تواند عملکرد شبکه وای‌فای را افزایش دهد.
محیط‌های پرتراکم از 5 GHz برای کانال‌های بیشترش (۳۶، ۴۰، ۴۴، ... تا ۱۶۵)
Cisco Prime / Meraki Dashboard برای مدیریت خودکار کانال‌ها در محیط Enterprise

مثالی از Wi-Fi channels: 2.4 GHz تنها سه کانال غیرهم‌پوشان ۱، ۶ و ۱۱ برای Apهای هم‌جوار



امید است این فایل برای خوانندگان مفید بوده باشد.
خوشحال می‌شوم اشکالات و پیشنهادات خود را برای اینجانب ارسال کنید.

www.khanahmadi.com

www.KhanAhmadi.ir

خان احمدی
مدرس امنیت، شبکه و مدیریت فناوری اطلاعات و سواد رسانه