کارگاه آموزشی آشنایی با تحلیل ترافیک شبکه مبتنی بر پروتکل با استفاده از Wireshark

By: Shahab Safaee
Software Engineering PhD
Email: safaee.shx@gmail.com


cibtrc.ir


cibtrc

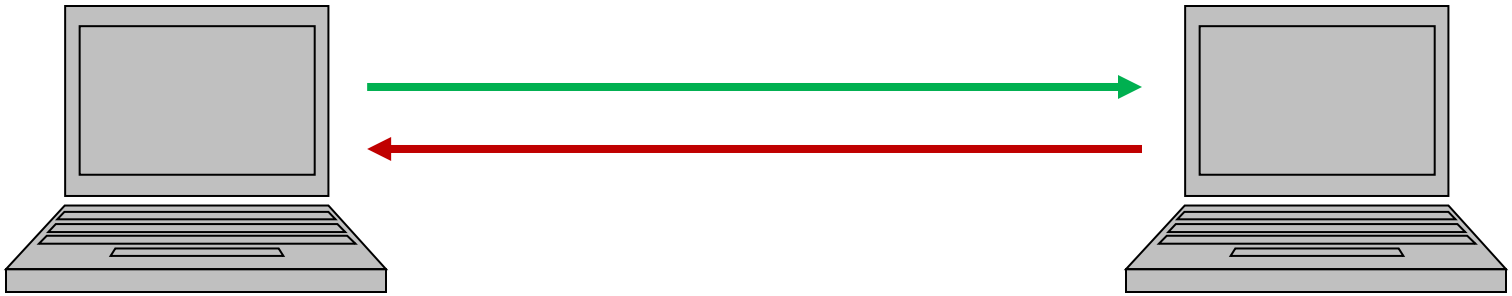

cibtrc

فهرست مطالب

- مروری بر شبکه های کامپیوتری
- پشته پروتکلی TCP/IP
- تحلیل ترافیک شبکه
- ویژگیهای Wireshark

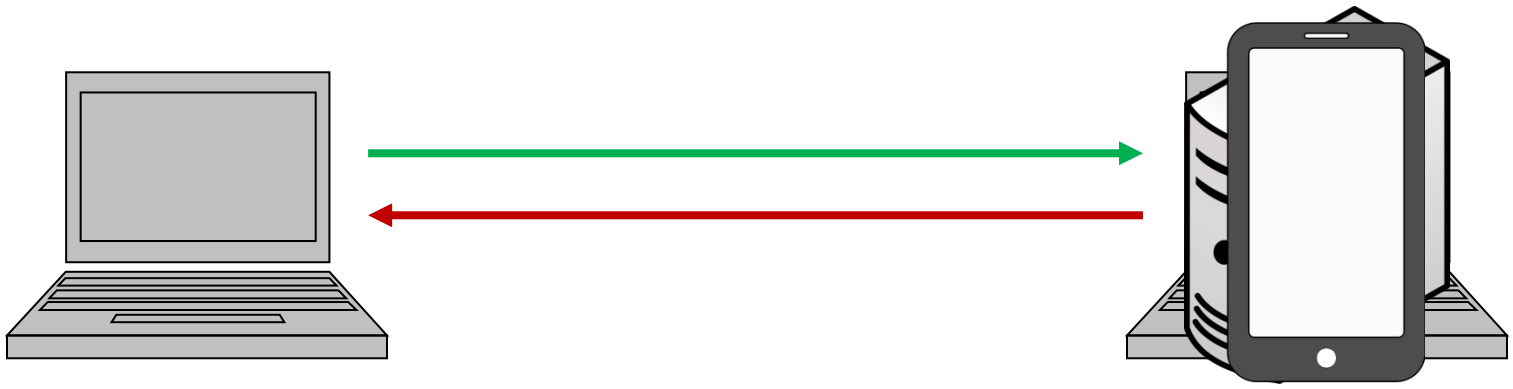
مروری بر شبکه های کامپیوتری (۱)

- سازمان کاری شبکه
  - تبادل پیام (Message)
    - از یک ماشین به ماشین دیگر



مروری بر شبکه های کامپیوتری (۲)

- مهمترین ویژگی
  - سیستم شبکه: از نوع سیستم باز (Open System)
    - امکان تعامل سیستم های ناهمگن با یکدیگر
      - ناهمگنی در سخت افزار
      - ناهمگنی در پلتفرم های نرم افزاری
    - نیاز به استانداردسازی در ارتباطات بین سیستم ها

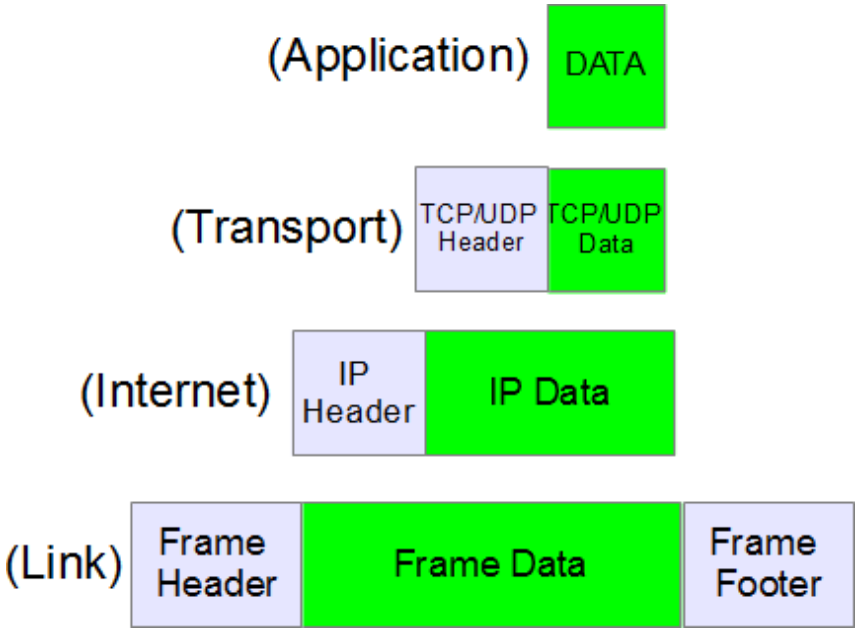


مروری بر شبکه های کامپیوتری (۳)

- مفهوم پروتکل
  - مفهوم کلی
    - مجموعه از قوانین و مقررات استاندارد بین دو ماشین در یک ارتباط جهت انجام عملیات مورد نیاز برای یک کار خاص
  - مفهوم فنی
    - عملیات مورد نیاز بین دو ماشین بصورت یک ساختار الگوریتمی و پیاده سازی شده توسط یک زبان برنامه نویسی بصورت یک برنامه قابل اجرا
  - ساختار فنی هر پروتکل
    - ساختار داده ای با مجموعه ای از فیلدهای مورد نیاز و قابل مقدار دهی بنام Header
    - مجموعه ای از پیام های مورد نیاز جهت تبادل بین دو ماشین
    - برنامه اجرایی پروتکل

مروری بر شبکه های کامپیوتری (۴)

- انواع پروتکل ها
  - بدون اتصال (Connection Less)
  - اتصال گرا (Connection Oriented)
- مثالی از پروتکل ها

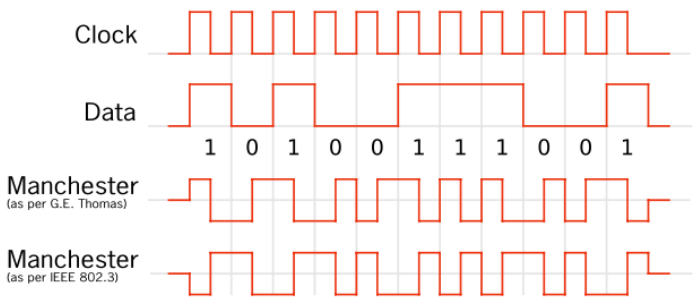


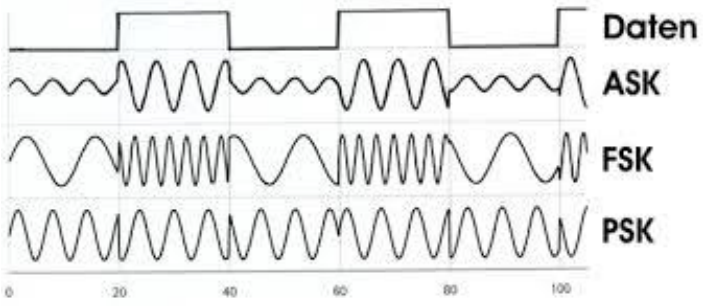
مروری بر شبکه های کامپیوتری (۵)

- مفهوم زیرساخت شبکه
  - فراهم کردن یک بستر ارتباطی جهت تبادل پیام بین ۲ ماشین (Machine-to-Machine-Communication)
- زیرساخت مخابراتی شامل ۲ بخش:
  - زیرساخت مخابراتی یا فیزیکی
  - زیرساخت Link

مروری بر شبکه های کامپیوتری (۶)

- هدف زیرساخت مخابراتی یا فیزیکی
  - فراهم کردن بستری مخابراتی جهت ارسال ۱ bit داده بین یک ماشین فرستنده و یک ماشین گیرنده (Machine-to-Machine Bit Transmit)
    - رسانه انتقال
      - محیط های انتقال هدایت شده
      - محیط های انتقال هدایت نشده
    - تولید سیگنال
      - روش های کدگذاری (Digital-to-Digital)
      - روش های مدولاسیون (Digital-to-Analog)





مروری بر شبکه های کامپیوتری (۷)

- هدف زیرساخت Link
  - ارسال یک فریم داده بدون خطا بین یک ماشین فرستنده و یک ماشین گیرنده (Machine-to-Machine Frame Transmit)
- مفهوم Link
  - یک تصور منطقی از محیط انتقال بین ۲ ماشین، مستقل از تکنولوژی رسانه انتقال و نحوه سیگنالینگ، آماده بهره برداری برای انتقال داده ها
- مفهوم توپولوژی
  - نحوه آرایش و چیدمان ماشین و لینک ها در شبکه

مروری بر شبکه های کامپیوتری (۸)

- مهمترین مسائل در زیرساخت Link
  - Framing
  - Addressing
  - Error Control
  - Flow Control
  - Media Access Control

مروری بر شبکه های کامپیوتری (۹)

- مفهوم تکنولوژی شبکه (Underlying Network Technology)
  - ارائه زیرساخت شبکه در دو بخش مخابراتی و لینک با پشتیبانی از:
    - مقیاس جغرافیایی
    - رسانه انتقال
    - تجهیزات موردنیاز
    - توپولوژی
    - پروتکل دسترسی به لینک
  - نمونه های تکنولوژی های زیرساختی شبکه محلی
- Ethernet (IEEE802.3)
- WIFI (IEEE802.11)
- ...

مروری بر شبکه های کامپیوتری (۱۰)

- مفهوم Networking یا Internetworking
  - مسیریابی و هدایت یک بسته داده از یک شبکه مبدا به یک شبکه مقصد (Network-to-Network Packet Routing & Forwarding)
- مسائل مهم Internetwork
  - نیاز به یک مکانیزم آدرس دهی سراسری و مستقل از تکنولوژی های زیرساختی برای شبکه و ماشین ها
  - پیدا کردن بهترین مسیر بین شبکه مبدا و شبکه مقصد
  - سوئیچینگ و هدایت بسته از شبکه مبدا تا شبکه مقصد
- انواع سوئیچینگ بسته در Internetwork
  - بدون اتصال (Connection Less)
  - اتصال گرا (Connection Oriented)

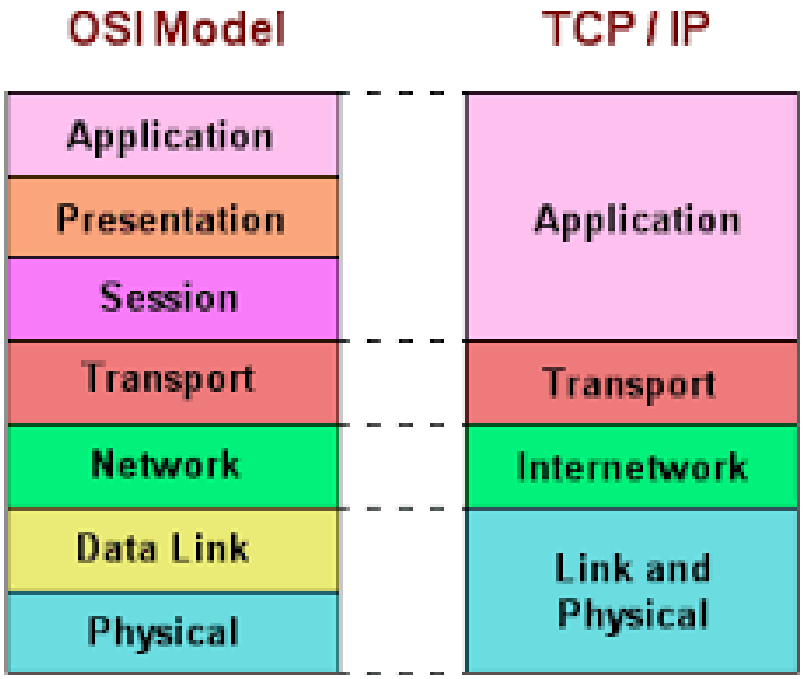
مروری بر شبکه های کامپیوتری (۱۱)

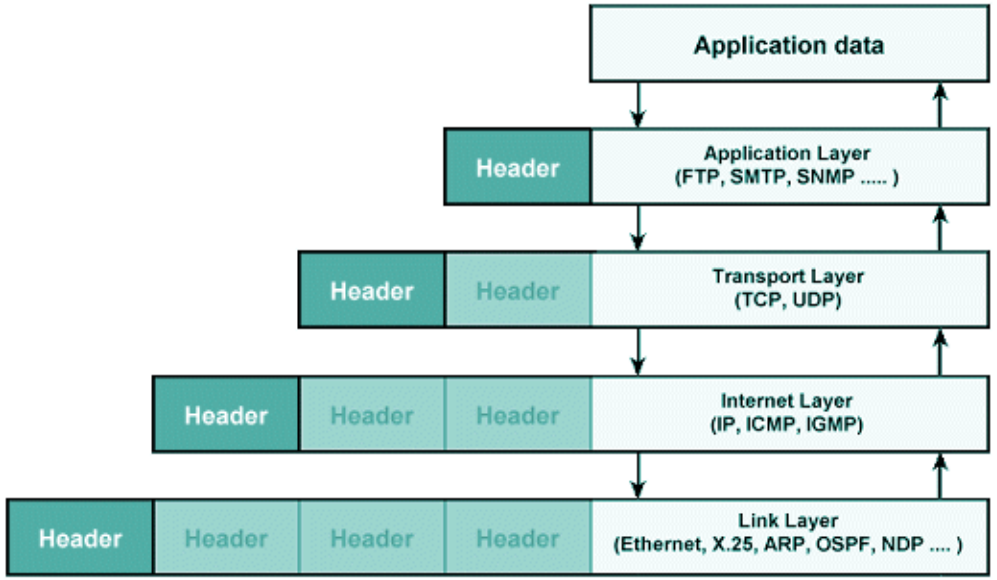
- پروتکل IP (Internetworking Protocol)
  - اولین پروتکل Internetworking
  - ارائه شده توسط وزارت دفاع امریکا
  - یک پروتکل Packet Switch Connection less
  - غیر قابل اطمینان
  - نهایت تلاش بصورت Hop-by-Hop برای مسیریابی و هدایت بسته
  - استفاده از تجهیز میانی بنام Router جهت مسیریابی و هدایت بسته ها

مروری بر شبکه های کامپیوتری (۱۲)

- تحلیل ترافیک شبکه
  - شناخت کامل نحوه کار پروتکل های شبکه از لحاظ:
    - الگوریتم پروتکل
    - پیام های پروتکل
    - Header پروتکل
  - استفاده از ابزارهای نرم افزاری جهت جمع آوری بسته هایی که از کارت شبکه ماشین خارج یا به کارت شبکه ماشین وارد می شوند
  - استفاده از شاخص های آمار
  - مشخص شدن الگوی ترافیکی

پشته پروتکلی TCP/IP





تحلیل ترافیک شبکه

- مزایای تحلیل ترافیک شبکه
  - سنجش شبکه
  - ارائه دید مناسب برای رفع عیب در شبکه
  - ارائه دید مناسب از لحاظ حوزه امنیت برای تشخیص ترافیک های نامتعارف شبکه و شناسایی تهدیدها
- معروفترین ابزارها
  - SolarWinds
  - Wireshark
  - PRTG
  - Tcpdump
  - Kismet
  - ...

ویژگیهای Wireshark

- Wireshark is completely free and easy to use
- Live capture and offline analysis
- Standard three-packet browser
- Read/write many different file formats
- Captures file compressed with gzip
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others


Thank
You
Merci
Gracias
TerimaKasih
Danke
Spacibo
Mèsi
Xièxie
Arigatô
Hvala
KamSahHamnida
Grazie
Takk
aDank
ThintKo
Buznyg
Blagodaram
Rahmat
BarakAllahuFiik
Chokrane
Kiitos
Dziakuju
GratiasAgimus
Motashakkeram
TänanVäga
Tak
Dankie
GratiasAgo
KopKhunKha
Gracie
CámOn
Multumesc
Saha
Salamat
Obrigado
Bayarlalaa
Nirringrazzjak
NajisTuke
Efharisto
Faleminderit
Gràcies
Dakujem
Taiku
Mercé
Matondo
Tanemirt
Tenki
Grandmercé
Chnorakaloutioun
Sagolun
Aabhar
Dhanyavaad
TapadhLeat
Köszönöm
Murakoze
WaadMahadsantahay
Grazzi
Mauruuru
Ačiū
Barkal
Gratzias
KhobChaiDeu
Mamnun
aNiKié
TapadhLeibh
AsanteSana
Shukriya
Enkosi
Ngiyabonga
FaafetaiLava
M-Sapo
Bedankt
Zikomo
Trugarez
Nouari
GoRaibhMaithAgat
Mochchakkeram
KyayTzuTinPaTe
KurreSumanga
TeşekkürEderim
Sobodi
AabhariAahe
Yekeniele
Dhanyabaad
KopKhunKrap
Tau
Nanni
Mieske
Trugéré
Akpé
Misaotra
Tanmirt
Akiba
MaloTeOfa
Gràçie
Asante
Miigwetch
Marahaba
Diky
TakkFyri
Wado
Mahalo
Graciñas
DankJuWel
ÇoxSagOlun
Meharbani
Blagodaria
Merkzi
Akun
Nandri
Dhanyavadalu
Sulpáy
Spas
EskerrikAsko
Dankewol
Diolch
Dankje
Vinaka
KeYaLeboha
Dankon
Barka
Nizzik ajr
Aguyjé
Toda
Mersi
Dhanyavadagalu
TesekkurEdirem
Welalin
TangioTumas
Tanan
Sukriya
Dhanyavad
Waita
Rahmet
Paldies
DjiereDieuf
ANiKié