Administrátor systému:

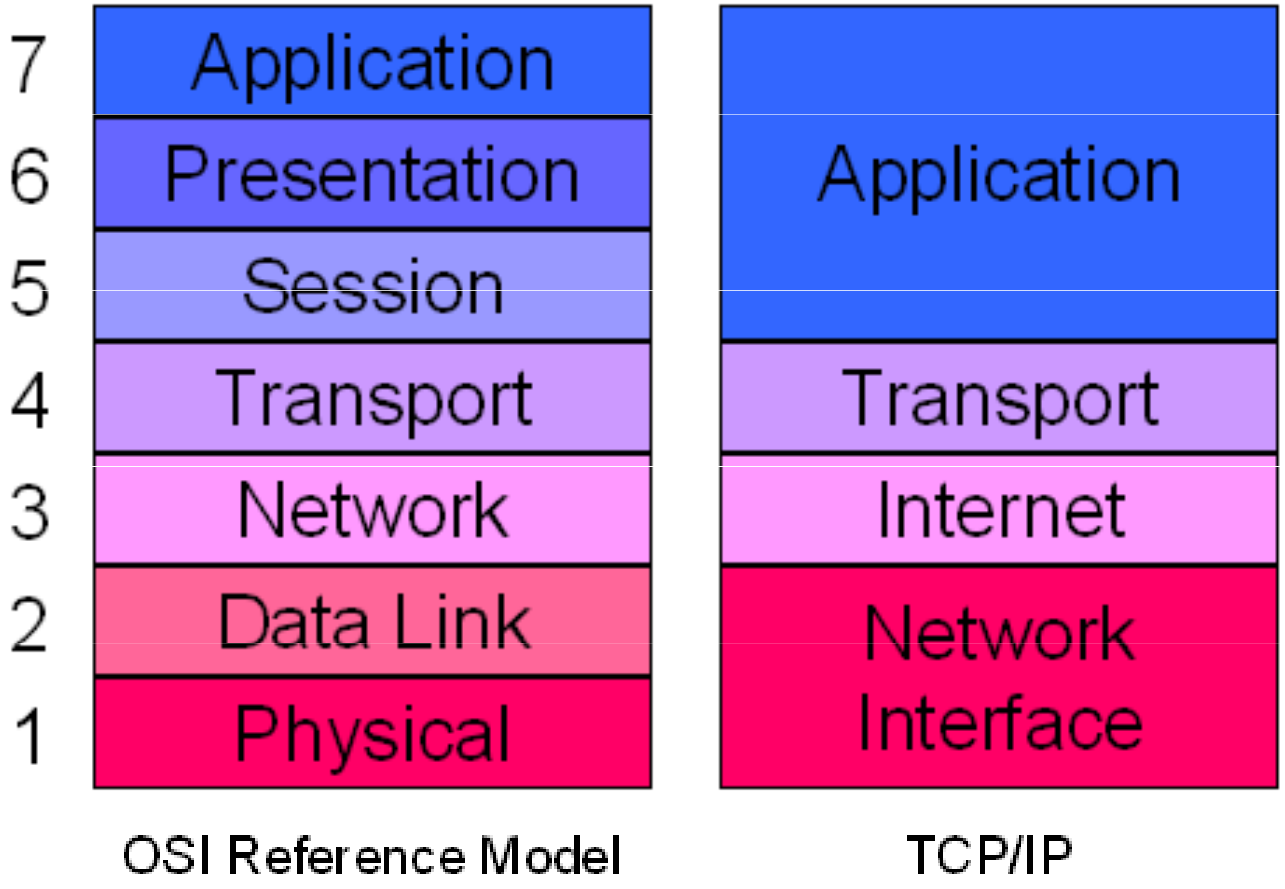
Pracovní doba administrátora se sestává z výměny magnetických pásek v zálohovacích zařízeních, odblokování zablokovaných účtů po třech nepovedených pokusech uživatele o přihlášení a klábosení na chatu s ostatními administrátory v jiných firmách, se kterými si propil ledviny na četných školeních o správcování systému.
Tuto osobu si musíte vždy předcházet - vše v IT funguje jen s jejím tichým souhlasem…

Podzim 2008

PV175 SPRÁVA MS WINDOWS I

Síťové služby

ISO OSI a TCP/IP model



(hardwaresecrets.com)

TCP/IP

- IP (Internet Protocol)
  - Protokol síťové (internetové) vrstvy obstarávající negarantované spojení mezi vzdálenými počítači
- TCP (Transmission Control Protocol)
  - Protokol transportní vrstvy poskytující zajišťující parametry přenosu nad protokolem IP
- UDP (User Datagram Protocol)

IP adresa a maska

- IP adresa
  - 2 části – NetworkID a HostID
  - Privátní / veřejné IP rozsahy
    - A: 10.0.0.0
    - B: 172.16.0.0 – 172.31.0.0
    - C: 192.168.0.0
- Maska podsítě
  - Definuje, kde začíná HostID
  - Umožňuje rozdělení sítě do podsítí
    - Důležitý bezpečnostní prvek

DHCP

- Dynamic Host Configuration Protocol
- Protokol zajišťující přidělení síťových parametrů klientům v síti
  - IP adresa, maska
  - Gateway
  - DNS servery, WINS servery
- Umožňuje vyšší škálovatelnost prostředí

DNS

- Domain Naming System
- Hierarchický systém pro pojmenování uzlů v Internetu
  - př.: DNS jméno: aisa.fi.muni.cz.
- Windows: hosts soubor
  - Lokální překlad IP adres na jména
  - %systemroot%\system32\drivers\etc\hosts
  - pharming

Typy záznamů DNS

- A
  - Překlad doménových jmen na IP adresy
- PTR
  - Překlad IP adres na doménová jména
- SRV
  - Adresy serverů poskytující služby v síti
  - Intenzivně využíváno v Active Directory

ICMP

- Internet Control Message Protocol
- Protokol pro zasílání chybových a informačních zpráv mezi uzly sítě
  - př.: echo request (ping), echo reply, destination host unreachable,…
- Pracuje na stejné úrovni jako IP, tedy na síťové vrstvě
- V současnosti jsou často pakety ICMP z bezpečnostních důvodů zahazovány

Formy adres

- NetBIOS
  - Jméno počítače jedinečné v lokální síti
  - Proměnná %computername%
  - př.: afrodita
- DNS
  - Jméno počítače podle systému DNS
  - př.: afrodita.fi.muni.cz
- UNC
  - Vyjadřuje cestu k prostředku sdílenému v síti
  - př.: \\afrodita\tmp

Grafické nástroje

- ncpa.cpl
  - Povolení / zakázání síťového připojení
  - Nastavení parametrů sítě ručně (IP adresa, maska, gateway, adresy DNS serverů) nebo přes DHCP (implicitní)
  - Alternativní konfigurace
  - Přidání / odebrání síťových protokolů
  - Nastavení pevné přípony DNS
  - Povolení / zakázání souboru lmhosts

Konzolové nástroje I

- Konfigurace síťových rozhraní
  - netsh interface
    - Správa síťových rozhraní z příkazového řádku
    - Konzolový ekvivalent ncpa.cpl z Control panelu
  - ipconfig (ipconfig /all)
    - Zobrazení aktuálních hodnot nastavení sítě
    - Znovunačtení specifikace z DHCP
      - ipconfig /release; ipconfig /renew
    - Vyčištění cache paměti DNS
      - Ipconfig /dnsflush

Konzolové nástroje II

- Překlad adres
  - arp
    - Překlad IP adres na fyzické MAC adresy používané protokolem ARP v lokální síti
    - ARP protokol si udržuje
  - nslookup
    - Překlad DNS jmen na IP adresy a naopak
    - Interaktivní / neinteraktivní mód

Konzolové nástroje III

- Trasování cesty
  - ping (ping -t)
    - Základní testovací nástroj
    - ICMP echo – ověření, že cílový počítač je funkční a dostupný
  - tracert
    - Sledování cesty paketu
    - Umožňuje zjistit, na kterém mezilehlém aktivním prvku dochází k chybám
    - Využívá pole TTL v hlavičce ICMP paketu

Konzolové nástroje IV

- netstat
  - Výpis aktuálně otevřených síťových spojení (zdrojová a cílová adresa, stav, použitý protokol)
- net view
  - Výpis sdílených prostředků počítačů v síti

Dotazy?

Díky za pozornost