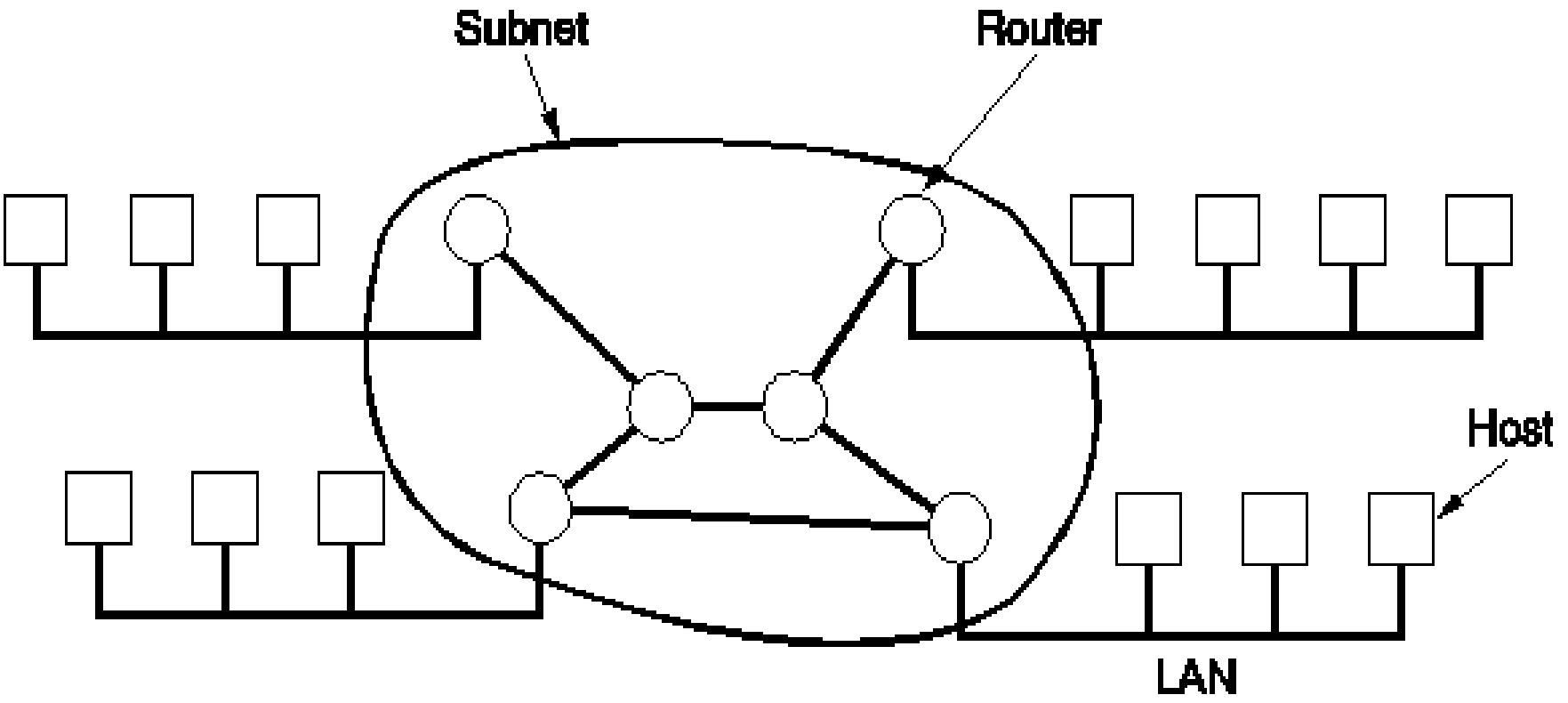
Distribuované systémy
Počítačové siete

RNDr. Jaroslav Janáček
KI FMFI UK

Klasifikácia sietí

- podľa rozsahu (veľkosti)
  - Personal Area Networks (PAN)
    - veľmi malé vzdialenosti (≈10m)
  - Local Area Networks (LAN)
    - malé vzdialenosti, budova, príp. komplex budov
  - Metropolitan Area Networks (MAN)
    - väčšie územia – napr. mesto
  - Wide Area Networks (WAN)
    - veľké geografické územia

WAN



Klasifikácia sietí

- podľa typu komunikačných liniek
  - point-to-point
    - spojené sú 2 zariadenia
    - napr. klasické spojenie cez telefónnu linku
  - broadcast – zdieľané médium
    - niekoľko zariadení je pripojených k spoločnému zdieľanému médiu
    - všetky zariadenia “počujú”, čo sa vyšle z niektorého z nich
    - napr. Ethernet

Klasifikácia sietí

- podľa typu komunikačného média
  - pevné (wired)
    - medené káble
    - optické vlákna
  - bezdrôtové (wireless)
    - rádiové
      - WiFi, Bluetooth, GSM, GPRS/EDGE, UMTS (3G)
    - satelitné
    - svetelné
      - IRDA, laserové

Bezdrôtové siete

- použitie
  - mobilní používatelia
  - ťažko prístupné miesta
  - dočasné siete
- problémy
  - vplyv prostredia, počasia
  - vzájomné ovplyvňovanie sa
  - zahltenie pásma
  - bezpečnosť

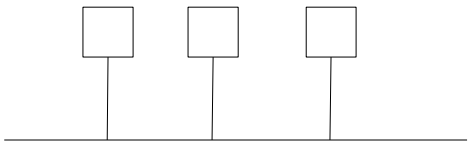
Spájanie sietí

- internetwork (internet) – množina navzájom prepojených sietí
  - siete sa spájajú prostredníctvom brán (gateways)
- Internet (s veľkým I)
  - konkrétny celosvetový internet

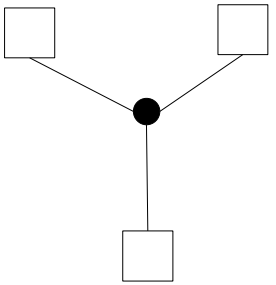
Adresácia v sieťach

- jednotlivé zariadenia v sieťach sú identifikované adresami
  - unicasting
    - posielanie jednému zariadeniu
  - broadcasting
    - posielanie informácie všetkým zariadeniam v sieti (resp. jej časti)
  - multicasting
    - posielanie informácie určitej skupine zariadení v sieti

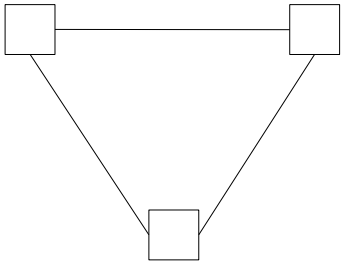
Topológia siete



bus – zbernica



star – hviezda

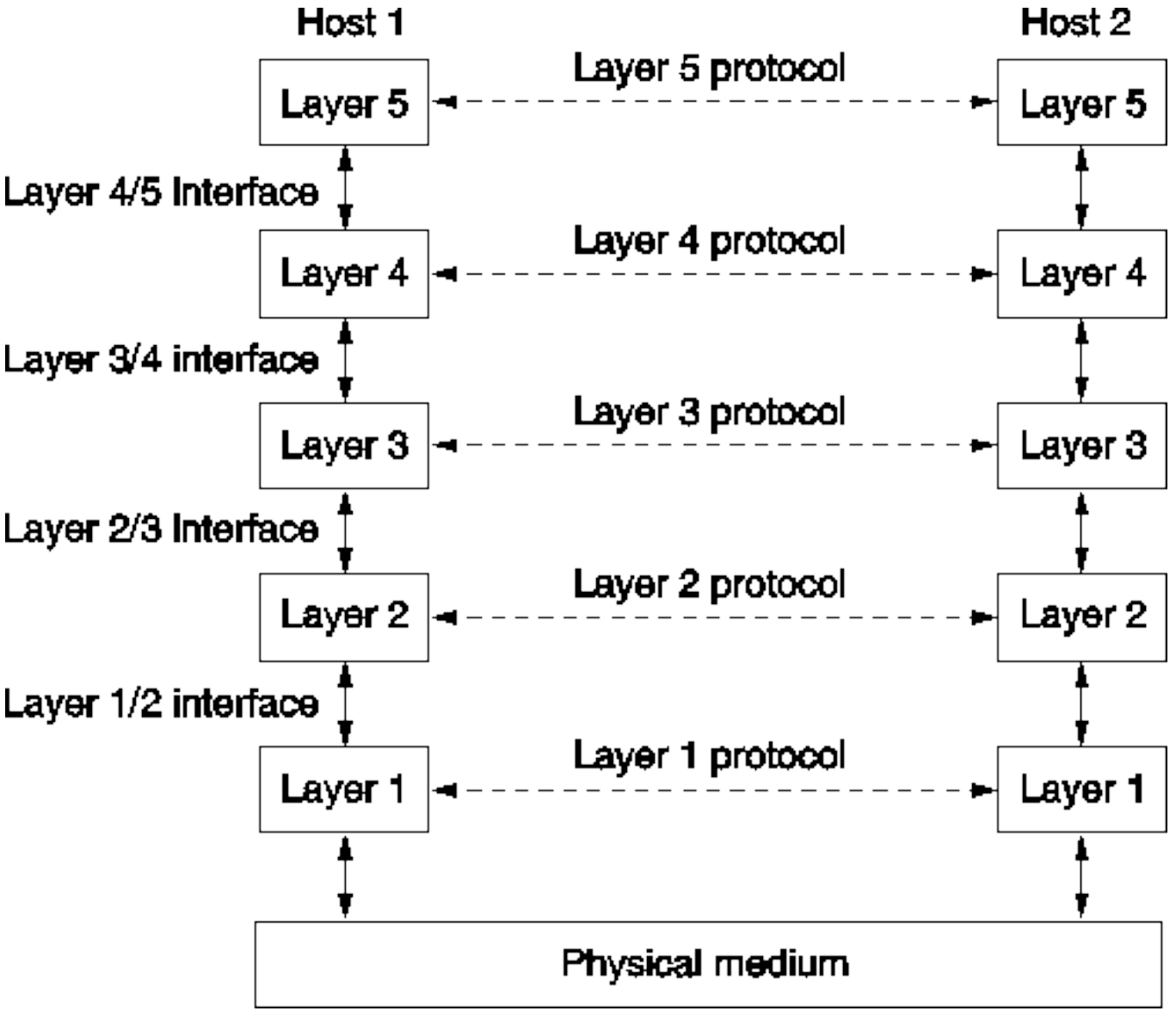


ring – kruh

Kľúčové problémy návrhu sietí

- identifikácia zariadení – adresovanie
- pravidlá komunikácie
  - simplex, half duplex, full duplex
- detekcia a oprava chýb
- problém rýchleho odosielateľa a pomalého prijímateľa
- poradie správ
- obmedzené dĺžky správ
- smerovanie (routing)
- multiplexing, demultiplexing

Vrstvový model



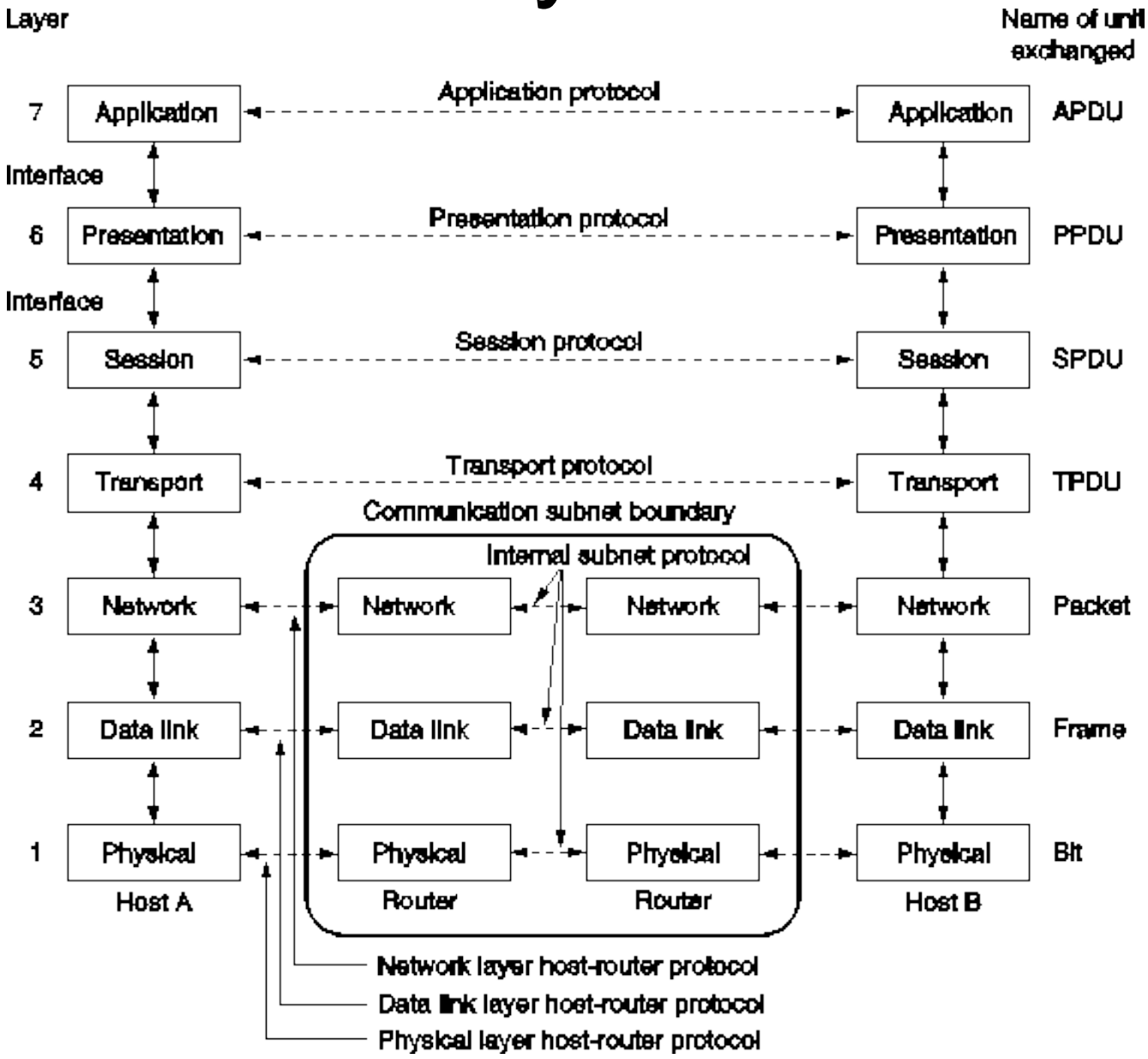
Vrstvy, služby, rozhrania (interface), protokoly

- vrstva N poskytuje *služby* vrstve N+1
- vrstva N s vrstvami N+1 a N-1 komunikuje prostredníctvom *rozhrania (interface)*
- vrtsva N s vrtsvou N na inom zariadení komunikuje použitím súboru pravidiel – *protokolu* príslušnej vrstvy

Rozdelenie služieb

- connection-oriented
  - vytvára sa spojenie, funguje ako “rúra”
- connection-less
  - prenášajú sa samostatné balíky dát – pakety
- reliable (spoľahlivé)
  - doručenie je garantované (alebo sa oznámi chyba)
- unreliable (nespoľahlivé)
  - doručenie nie je garantované

Referenčný model OSI



Referenčný model OSI

- physical layer (fyzická vrstva)
  - prenos bitov cez komunikačný kanál
  - parametre káblov, konektorov, signálov
  - káble, konektory, časť sieťových kariet, modemy
- data link layer (linková vrstva)
  - prenos rámcov (frames) medzi “susednými” zariadeniami
  - pri sieťach typu broadcast riešenie prístupu k médiu
  - časť sieťových kariet, ovládače sieťových kariet

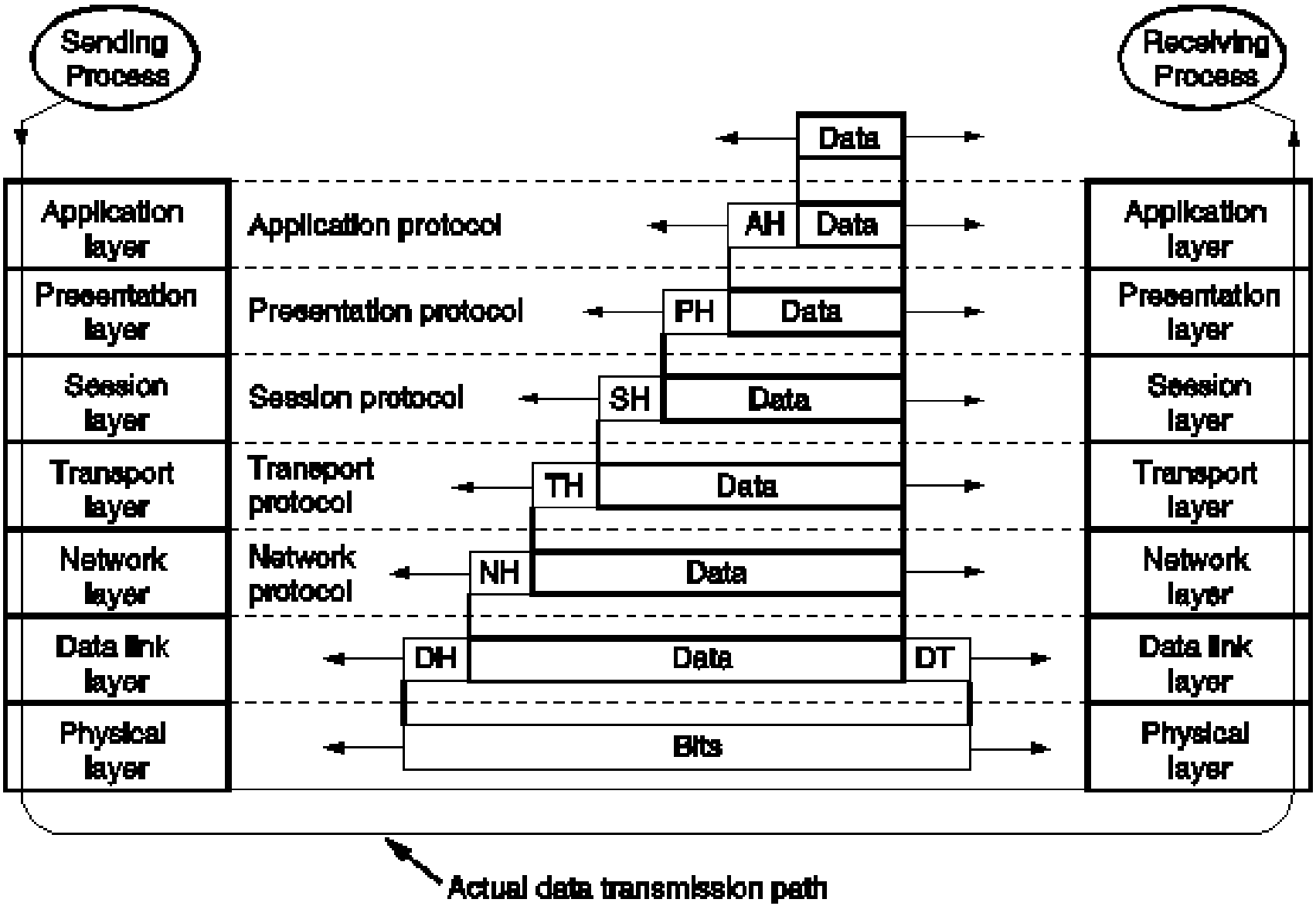
Referenčný model OSI

- network layer (sieťová vrstva)
  - prenos paketov medzi ľubovoľnými uzlami siete
  - smerovanie (routing), riešenie preplnenia siete
  - smerom nahor poskytuje ilúziu siete prepojenej spôsobom každý s každým
- transport layer (transportná vrstva)
  - komunikácia medzi procesmi na koncových zariadeniach
  - rozdeľovanie správ na pakety a ich skladanie

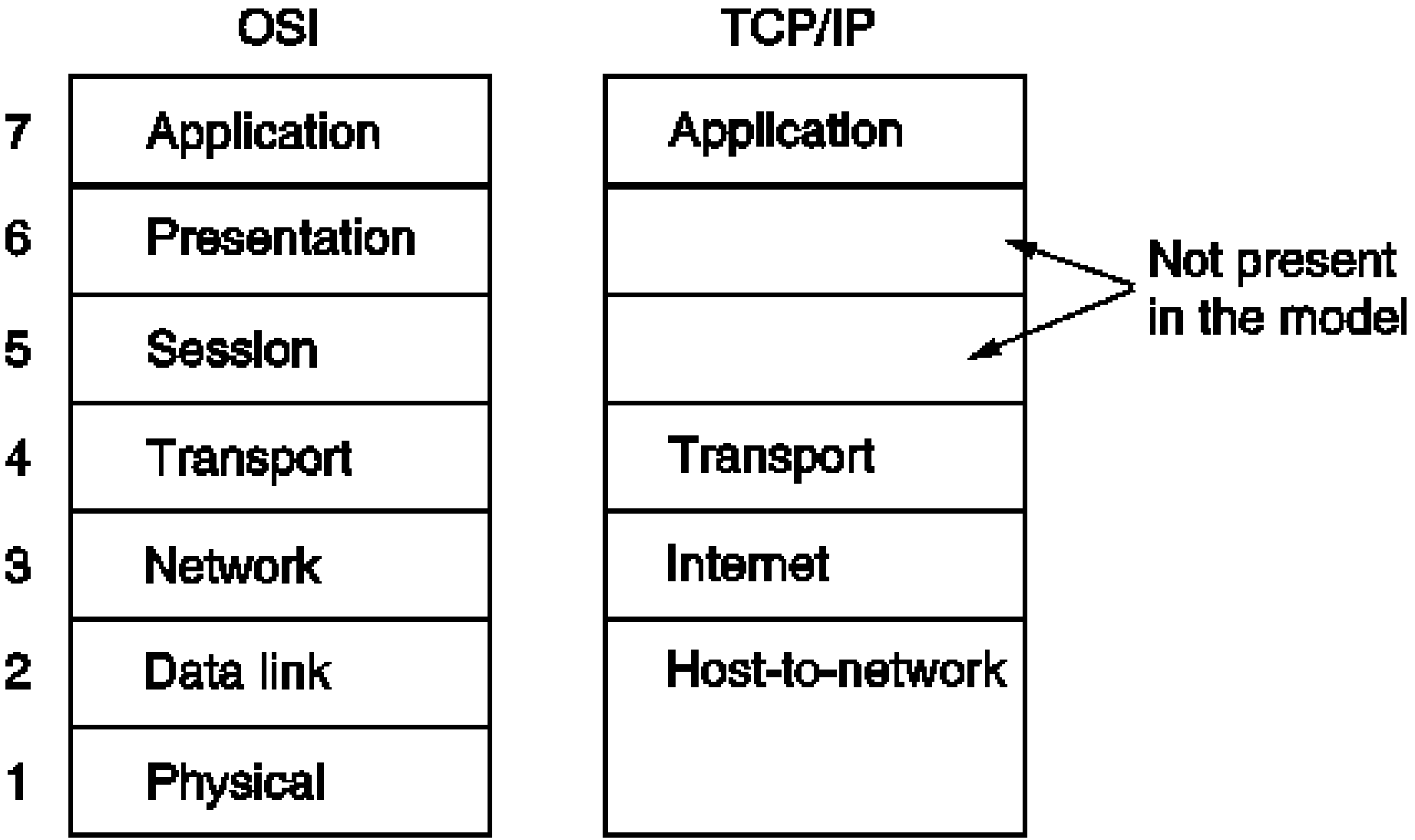
Referenčný model OSI

- session layer (relačná vrstva)
  - riadenie dialógu, synchronizácia
- presentation layer (prezentačná vrstva)
  - konverzia formátov údajov
- application layer (aplikačná vrstva)
  - aplikačné protokoly

Tok dát v OSI


Sending Process
Receiving Process
Application layer
Presentation layer
Session layer
Transport layer
Network layer
Data link layer
Physical layer
Application protocol
Presentation protocol
Session protocol
Transport protocol
Network protocol
Data
AH
PH
SH
TH
NH
DH
DT
Bits
Actual data transmission path

TCP/IP model


OSI
TCP/IP
7
Application
6
Presentation
5
Session
4
Transport
3
Network
2
Data link
1
Physical
Application
Transport
Internet
Host-to-network
Not present
in the model

TCP/IP model

- internet layer
  - protokol IP – connection-less, unreliable
  - prenos paketov medzi ľubovoľnými dvoma uzlami siete
  - zabezpečuje smerovanie (routing)
- host to network layer
  - zabezpečuje možnosť posielať IP pakety medzi susednými zariadeniami

TCP/IP model

- transport layer
  - protokoly
    - TCP – connection-oriented, reliable
    - UDP – connection-less, unreliable
  - poskytuje služby aplikačnej vrstve
- application layer
  - rôzne aplikačné protokoly – HTTP, FTP, telnet, ssh, SMTP, POP3, ...

Ethernet

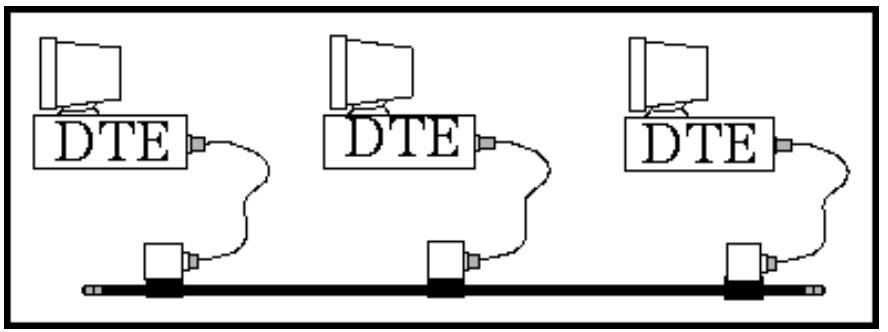
- fyzická a data-link vrstva
- sieť typu broadcast, technológia CSMA/CD
- adresy 48 bitov
  - časť identifikuje výrobcu
  - multicasting
  - broadcasting FF:FF:FF:FF:FF:FF
  - každý frame obsahuje adresu cieľa a zdroja
- 10Mbps, 100Mbps (fast), 1Gbps (gigabit)
- logická topológia: bus

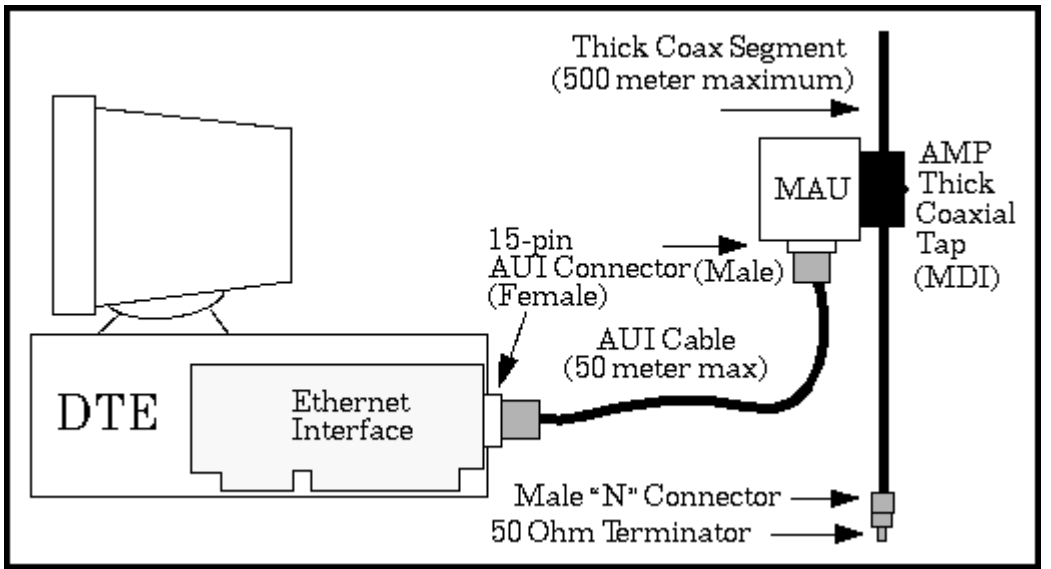
Ethernet

- Carrier Sense
  - kontroluje sa, či je kanál voľný – nikto nevysiela
- Multiple Access
  - keď je nejaký čas ticho, ktorákoľvek stanica môže začať vysielať
- Collision Detection
  - ak začnú 2 naraz, nastane kolízia, prestanú vysielať a počkajú náhodný čas

Ethernet

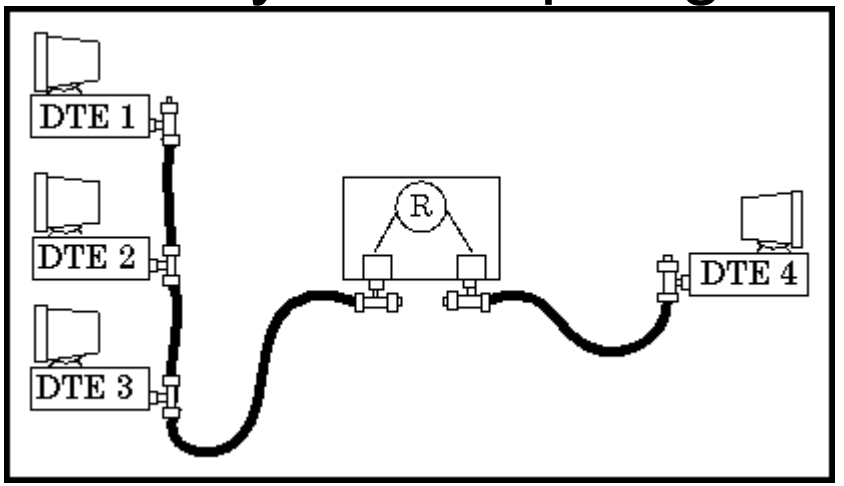
- 10BASE5 – thick Ethernet
  - hrubý (žltý) koaxiálny kábel
    - 1 cm priemer, 50Ω, na koncoch 50Ω terminátory
  - do 500m, 100 zariadení
  - pripájanie cez externý transciever AUI káblom (do 50m)
  - fyzická topológia: bus

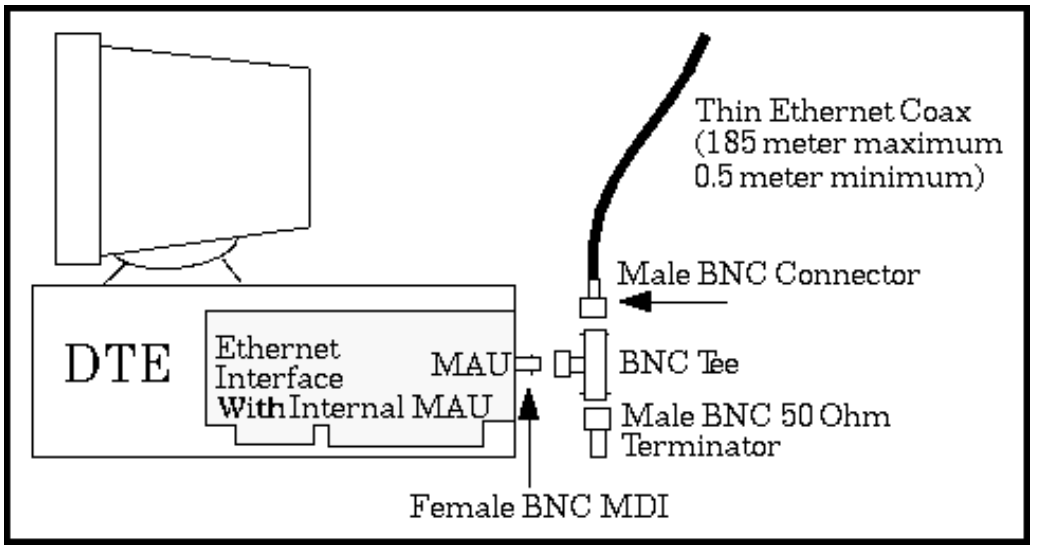




Ethernet

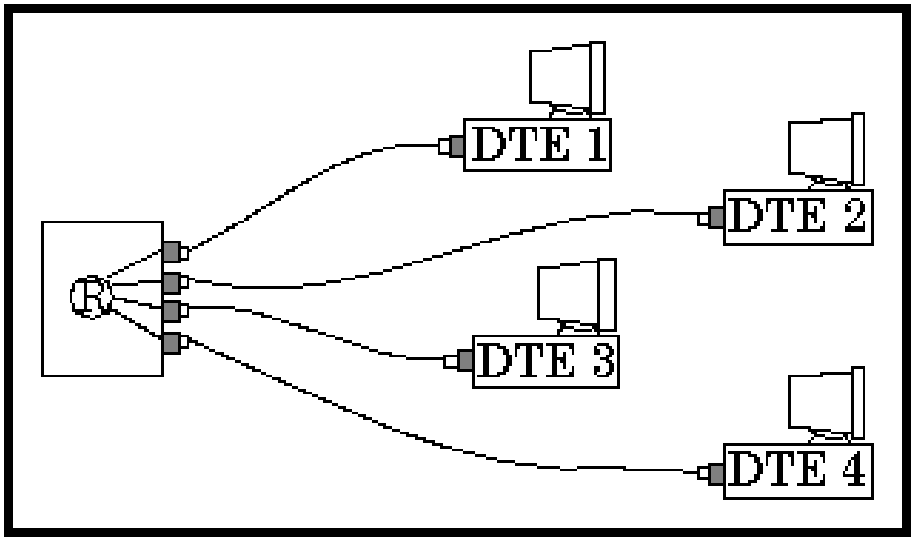
- 10BASE2 – thin Ethernet
  - tenký koaxiálny kábel RG 58
    - 0.5 cm priemer, 50Ω, na koncoch 50 Ω terminátory
  - do 185m, 30 zariadení
  - pripájanie cez T-konektor
  - fyzická topológia: bus





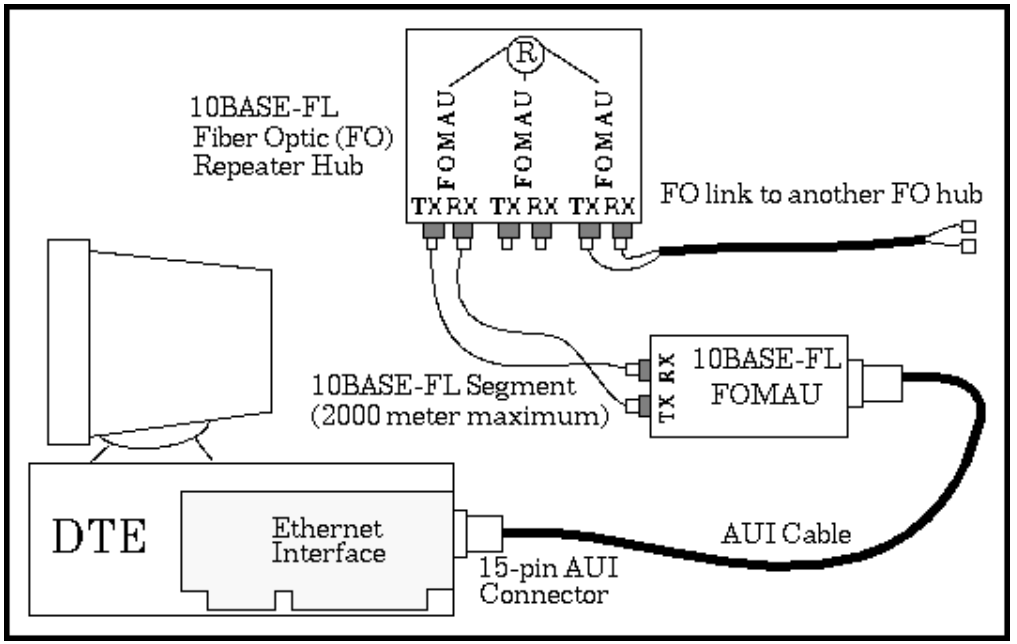
Ethernet

- 10BASE-T – twisted pair (krútená dvojlinka)
  - netienený TP kábel kategórie 3, používa 2 páry
  - do 100m, point-to-point
  - pripájanie konektorom RJ-45
  - fyzická topológia: star, v strede hub/switch



Ethernet

- 10BASE-FL
  - 2 optické vlákna
  - do 2km, point-to-point
  - fyzická topológia: star, v strede hub/switch



Fast Ethernet

- 100BASE-TX
  - twisted pair kat. 5, používa 2 páry, 100m, p-to-p
- 100BASE-FX
  - 2 optické vlákna, 412m, p-to-p
- 100BASE-T4
  - twisted pair kat. 3, používa 4 páry, 100m, p-to-p
- fyzická topológia: star, v strede hub/switch

Gigabit Ethernet

- 1000BASE-T
  - twisted pair kat. 5, používa 4 páry, 100m, p-to-p
- 1000BASE-SX, 1000BASE-LX
  - optické vlákna
- fyzická topológia: star, v strede hub/switch

Rozširovanie Ethernetu

- fyzická vrstva
  - repeater, hub – 1 kolízna doména
    - 10Mbps: max. 4, max. 5 segmentov
    - 100Mbs: max. 1 hub triedy I alebo 2 huby triedy II
- linková vrstva
  - bridge, switch
    - rozpoznáva ethernetové adresy a posiela rámce kam treba
    - umožňuje full-duplex, multi-speed

WiFi (IEEE 802.11)

- CSMA/CA
  - Carrier Sense Multiple Access with Collision Avoidance
  - po tichu čaká náhodný čas
- potvrdzuje príjem rámca na linkovej vrstve
- rovnaké adresy ako Ethernet
  - ľahká integrácia

WiFi (IEEE 802.11)

- 802.11b
  - 11Mbps, 2.4GHz, 13 kanálov
- 802.11g
  - 54Mbps, 2.4GHz, 13 kanálov
- 802.11a
  - 54Mbps, 5GHz

WiFi (IEEE 802.11)

- BSS (basic service set)
  - množina staníc v dosahu tvoriacich spolu základnú bunku siete
  - napr. AP (access point) a niekoľko staníc
- ESS (extended service set)
  - množina BSS tvoriacich jednu sieť na linkovej vrstve
  - jednotlivé BSS sa môžu prekrývať
  - ESSID = identifikátor ESS

WiFi (IEEE 802.11)

- infraštruktúrny režim
  - AP (access point, prístupový bod)
    - stanica sa asociuje k AP
    - zabezpečuje prenos rámcov medzi asociovanými stanicami a DS
  - DS (distribučný systém)
    - prepája AP tvoriace jednu ESS (extended service set)
    - umožňuje roaming medzi BSS
  - portál
    - prepája ESS s inou sieťou

WiFi (IEEE 802.11)

- ad-hoc režim (IBSS, Independent BSS)
  - niekoľko staníc tvoriacich sieť
  - nemá prístup k DS
  - nepotrebuje AP

Sieťová vrstva v TCP/IP

- protokol IP – connection-less, unreliable
- prenos IP paketov medzi ľubovoľnými dvoma počítačmi (zariadeniami)
- fragmentácia paketov
- adresy – 4B čísla (1.2.3.4)
- časť adresy určuje sieť, druhá časť konkrétny uzol (host – počítač, zariadenie)

Triedy IP adries

- 1.x.x.x – 126.x.x.x – A
  - 7 bitov sieť, 24 bitov host
- 128.x.x.x – 191.x.x.x – B
  - 14 bitov sieť, 16 bitov host
- 192.x.x.x – 223.x.x.x – C
  - 21 bitov sieť, 8 bitov host
- 224.x.x.x – 239.x.x.x – D – multicast
- 240.x.x.x – 255.x.x.x – E – vyhradené

Classless Inter-domain Routing

- zapĺňanie adresného priestoru
  - neefektívne prideľovanie A/B/C
- maska
  - určuje, ktoré bity tvoria adresu siete
  - súvislý blok 1, súvislý blok 0
    - 255.255.0.0 = 16 bitov
    - 255.255.255.128 = 25 bitov
    - 255.192.0.0 = 10 bitov

Špeciálne IP adresy

- adresa siete
  - host = 0...0
  - slúži ako identifikátor siete
  - „neznáma“ adresa
- broadcast
  - host = 1...1
  - broadcast pre určenú sieť

Špeciálne IP adresy

- 127.0.0.0/255.0.0.0
  - loopback, lokálny počítač
- 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8
  - pre súkromné siete – nesmú sa dostať do Internetu
- 255.255.255.255
  - broadcast na lokálnej sieti
- 0.0.0.0
  - „neznáma“ adresa (napr. zdroj pri BOOTP/DHCP)

Príklady IP adries

- 158.195.18.0/255.255.255.0 (24)
  - adresy 158.195.18.1 – 158.195.18.254
  - broadcast: 158.195.18.255
- 158.195.16.0/255.255.254.0 (23)
  - adresy 158.195.16.1 – 158.195.17.254
  - broadcast: 158.195.17.255
- 158.195.22.0/255.255.255.128 (25)
  - adresy 158.195.22.1 – 158.195.22.126
  - broadcast: 158.195.22.127

IP paket

- hlavička (20 až 60 B)
  - adresa odosielateľa a cieľa
  - dĺžka paketu, transportný protokol
  - time to live, fragmentačné údaje
  - kontrolný súčet hlavičky
- max. veľkosť teoreticky 65536 B
- každé IP zariadenie musí byť schopné spracovať aspoň 576 B IP paket
- umožňuje fragmentáciu paketov

Routovanie IP

- router – počítač alebo špeciálny HW s aspoň dvoma sieťovými interfejsmi/linkami
  - pre každý sieťový interfejs
    - IP adresa
    - maska siete
- routovacia tabuľka
  - adresa, maska, ďalší router, sieťový interfejs/linka
  - vyberie sa vždy najšpecifickejšia položka

Príklad routovacej tabuľky

- IP: 158.195.18.222, maska: 255.255.255.0
  - 158.195.18.0/255.255.255.0 - eth0
  - 127.0.0.0/255.0.0.0 - lo
  - 0.0.0.0/0.0.0.0 158.195.18.209 eth0
- Router:
  - IP1:158.195.18.209, maska: 255.255.255.0
  - IP2: 158.195.17.163, maska: 255.255.254.0
    - 158.195.18.0/255.255.255.0 - eth0
    - 158.195.16.0/255.255.254.0 - eth1
    - 127.0.0.0/255.0.0.0 - lo
    - 0.0.0.0/0.0.0.0 158.195.16.208 eth1

Address Resolution Protocol

- IP pracuje s IP paketmi a IP adresami
- linková vrstva pri broadcast médiu potrebuje často iné adresy (napr. Ethernet)
- ARP rieši preklad IP adresy na fyzickú (linkovú adresu)
  - vyšle broadcast “Kto má IP a.b.c.d?”
  - zariadenie s IP a.b.c.d odpovie:
    “IP a.b.c.d má zariadenie x:y:z:p:q:s”

Internet Control Message Protocol

- ICMP
- diagnostika a spracovanie chýb
  - ping
  - destination unreachable
  - redirect
  - TTL exceeded
  - ...

Transportná vrstva TCP/IP

- protokoly
  - TCP (Transmission Control Protocol)
    - connection-oriented, reliable
  - UDP (User Datagram Protocol)
    - connection-less, unreliable
- poskytuje služby aplikačnej vrstve
- adresy – navyše číslo portu
  - jednoznačná identifikácia spojenia = IP adresa + port jednej strany a IP adresa + port druhej strany

User Datagram Protocol

- unreliable, connection-less služba
- hlavička
  - zdrojový a cieľový port
  - veľkosť
  - kontrolný súčet (hlavička aj dáta)

Transmission Control Protocol

- reliable, connection-oriented služba
- hlavička
  - zdrojový a cieľový port
  - sekvenčné číslo, potvrdzovacie číslo a veľkosť okna
  - príznaky, kontrolný súčet, ...
- každý paket sa potvrdzuje
- keď nepríde potvrdenie, paket sa pošle znova

TCP – Sliding Window

→ [S=0, W=1000, F=SYN, L=0]	
← [S=0, A=1, W=1000, F=SYN+ACK, L=0]	(okno=1-1000)
→ [S=1, A=1, W=1000, F=ACK, L=0]	
→ [S=1, A=1, W=1000, F=ACK, L=500]	
← [S=1, A=501, W=1000, F=ACK, L=0]	(okno=501-1500)
→ [S=501, A=1, W=1000, F=ACK, L=500]	
→ [S=1001, A=1, W=1000, F=ACK, L=500]	(vyčerpali sme okno)
← [S=1, A=1501, W=500, F=ACK, L=0]	(okno=1501-2000)
→ [S=1501, A=1, W=1000, F=ACK, L=500]	
← [S=1, A=2001, W=0, F=ACK, L=0]	(prázdne okno – stop)
→ [S=2001, A=1, W=1000, F=ACK, L=1]	(pokus)
← [S=1, A=2001, W=0, F=ACK, L=0]	(prázdne okno – stop)
← [S=1, A=2001, W=1000, F=ACK, L=0]	(okno=2001-3000)
→ [S=2001, A=1, W=1000, F=ACK+FIN, L=500]	
← [S=1, A=2502, W=1000, F=ACK+FIN, L=0]	
→ [S=2502, A=2, W=1000, F=ACK, L=0]	

Transmission Control Protocol

- vytvorenie spojenia
  - A pošle B paket s príznakom SYN
  - B pošle A paket s príznakmi SYN a ACK
  - A pošle B paket s príznakom ACK
- ukončenie spojenia
  - A pošle B paket s príznakmi FIN a ACK
  - B pošle A paket s príznakmi FIN a ACK
  - A pošle B paket s príznakom ACK

Network Address Translation (NAT)

- umožňuje komunikáciu zo siete so súkromnými adresami
- source NAT (SNAT)
  - zdroj spojenia má súkromnú adresu
- destination NAT (DNAT)
  - cieľ spojenia má súkromnú adresu
  - používa sa na sprístupnenie služby poskytovanej serverom so súkromnou adresou

Network Address Translation (NAT)

- router
  - si udržiava tabuľku „spojení“
    - adresa a port zdroja a cieľa,
    - protokol
    - preložená (vlastná) adresa a port
  - pri odosielaní prvého paketu spojenia von
    - prepíše adresu zdroja na preloženú
    - prepíše port zdroja na vlastný (voľný)
    - zapíše spojenie do tabuľky

Network Address Translation (NAT)

- router
  - pri odosielaní ďalšieho paketu spojenia von
    - nájde spojenie v tabuľke
    - prepíše adresu a port zdroja podľa tabuľky
  - pri prijatí paketu zvonku
    - nájde spojenie v tabuľke
    - prepíše adresu a port cieľa podľa tabuľky

Network Address Translation (NAT)

- DNAT
  - pri prijatí paketu zvonka na určenú verejnú adresu a port
    - ak je spojenie v tabuľke, prepíše cieľ podľa tabuľky
    - inak prepíše cieľ podľa konfigurácie a spojenie zapíše do tabuľky
  - pri odosielaní paketu von
    - nájde spojenie v tabuľke
    - prepíše zdroj podľa tabuľky

Network Address Translation (NAT)

- Ako dlho držať spojenie v tabuľke?
  - TCP – dá sa využiť sledovanie stavu spojenia
  - UDP – timeout
    - väčší timeout pre prúd UDP prúd (stream)
- Problémy s aplikačnými protokolmi
  - ak aplikačný protokol používa IP adresy a čísla portov
    - potreba podporných modulov pre udržiavanie tabuľky spojení a príp. prepisovanie dát aplikačnej vrstvy
    - napr. FTP

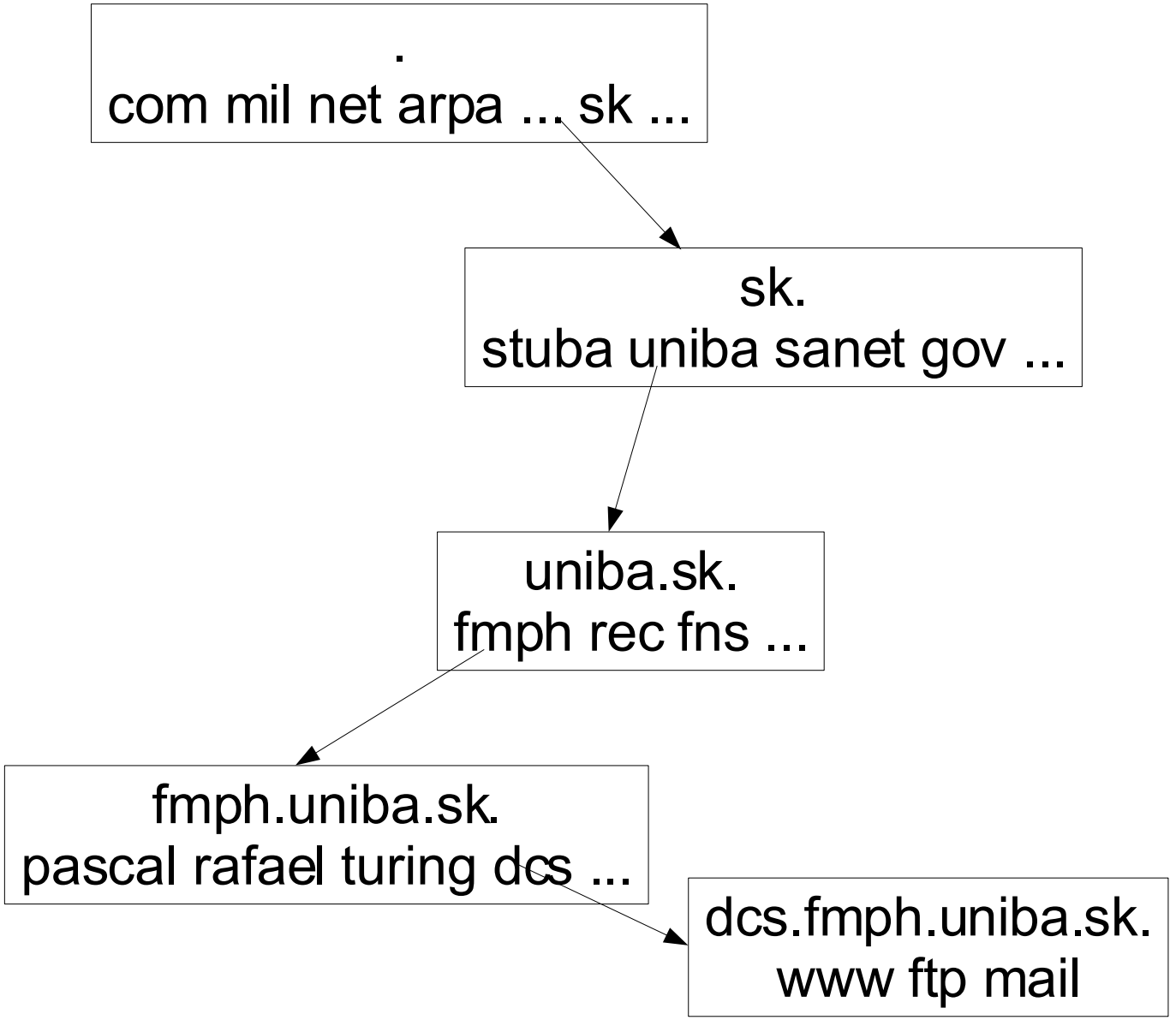
Aplikačná vrstva TCP/IP

- Rôzne aplikačné protokoly využívajúce TCP alebo UDP
  - WWW: HTTP – TCP/80, HTTPS – TCP/443
  - FTP – TCP/21, TCP/20
  - telnet – TCP/23
  - ssh – TCP/22
  - odosielanie e-mailov: SMTP – TCP/25
  - čítanie e-mailov: POP3 – TCP/110, IMAP - TCP/143
  - DNS – UDP/53, TCP/53

Domain Name System (DNS)

- IP adresy sa ľuďom zle pamätajú
- DNS – najväčšia distribuovaná databáza na prevod medzi doménovými menami a IP adresami
- doménové meno:
  - meno.doména_n.doména_n-1. ... .doména_1
  - nič nehovorí o fyzickom umiestnení počítača
  - domény 1. (najvyššej úrovne)
    - generické: com, org, net, edu, gov, mil, int, biz, info, pro
    - podľa krajín: sk, cz, at, pl, hu, de, uk, ...
- informácie poskytujú DNS servery

Domain Name System



Domain Name System

- Rôzne typy záznamov
  - A – IP adresa
  - CNAME – alias
  - MX – mail exchanger – kam sa majú doručovať e-maily
  - NS – IP adresa DNS servera pre poddoménu
  - SOA – základné informácie o doméne
  - PTR – používa sa pri opačnom vyhľadávaní
- A, MX a NS môže byť pre jedno meno aj viac

Domain Name System

- Ako pre danú IP adresu nájsť doménové meno?
- DNS je organizovaný podľa domén
  - prehľadanie celého stromu by trvalo veľmi dlho
- Adresu a.b.c.d vyhľadáme ako záznam typu PTR pre d.c.b.a.in-addr.arpa.
- Informácie na prevod mena na IP a naopak sú nezávislé, preto nemusia vždy súhlasiť.

Bezpečnostné problémy v sieťach

- dôvernosť
- integrita a autentickosť
- dostupnosť
- autentifikácia
  - používateľov
  - systémov
- riadenie prístupu

Bezpečnostné mechanizmy

- fyzická ochrana prístupu
- kryptografia
  - šifrovanie
    - symetrické (DES, 3DES, AES, ...)
    - asymetrické (PKI) (RSA, ...)
  - digitálny podpis (RSA, DSS, ...)
  - hašovacie funkcie s kľúčom (HMAC-SHA1, HMAC MD5, ...)
- organizačné opatrenia

Problém distribúcie kľúčov

- symetrická kryptografia
  - potreba zdieľaného tajného kľúča
  - algoritmy (napr. Diffie-Hellman) na výpočet zdieľaného tajného kľúča
    - potreba vzájomnej autentifikácie na vylúčenie Man-In-the-Middle útoku
  - generovanie kľúča jednou stranou a bezpečný prenos druhej strane
- asymetrická kryptografia
  - distribúcia verejných kľúčov
  - certifikáty

Bezpečnosť na fyzickej vrstve

- fyzická ochrana káblov a sieťových komponentov
- separácia sietí na fyzickej vrstve
- často nefunguje proti vnútornému nepriateľovi
  - keď sa viem dostať k počítaču, viem sa dostať ku káblu
  - použiteľné v kombinácii s organizačnými opatreniami

Bezpečnosť na linkovej vrstve

- nekryptografická
  - VLAN (virtual LAN)
    - separácia sietí na linkovej vrstve
  - riadenie prístupu k portu
    - na báze linkovej adresy
    - IEEE 802.1X
- kryptografická
  - šifrovanie, kontrola autentickosti, autentifikácia
  - známe vo WiFi svete
    - WEP, WPA, WPA2

VLAN (IEEE 802.1Q)

- rozdelenie Ethernetu na logické (virtuálne) siete
- VLAN ID (VID) – 12 bitov (1 – 4094)
- príslušnosť rámca k VLAN
  - tagged frame – podľa údaja v hlavičke
  - untagged frame – podľa portu (PVID)
- switch
  - pre každý port: Port VID (PVID), množina VID
  - pošle rámec len na porty danej VLAN (Egress filtering)
  - **môže** filtrovať rámce z VLAN, do ktorej zdrojový port nepatrí (Ingress filtering)

Bezpečnosť na sieťovej vrstve

- firewall
  - filtrácia komunikácie – riadenie prístupu
  - stateless vs. statefull, NAT
  - deny vs. allow by default
- VPN
  - šifrovanie, kontrola autentickosti, riadenie prístupu
  - IPSec (AH, ESP)
  - OpenVPN (IP/L2 over UDP/TCP)
  - ...

IPSec

- ochrana dôvernosti a/alebo integrity na sieťovej vrstve
- AH (Authentication header)
  - ochrana integrity IP hlavičky a obsahu
- ESP (Encapsulating Security Payload)
  - ochrana integrity a/alebo dôvernosti obsahu
- tunelový mód
  - obsahom je celý IP paket
- transportný mód

IPSec

- správa bezpečnostných asociásií
  - Internet Security Association and Key Management Protocol (ISAKMP)
    - protokol pre automatický manažment bezpečnostných asociácií a kľúčov
  - Internet Key Exchange Protocol (IKE)
    - protokol pre výmenu kľúčov založený na asymetrickej kryprografii (Diffie-Hellman)
    - vzájomná autentifikácia účastníkov výmeny
      - PKI alebo pre-shared secret

Bezpečnosť na transportnej vrstve

- SSL (Secure Socket Layer), TLS (Transport Layer Security)
  - medzi transportnou a aplikačnou vrstvou
  - zabezpečuje autentifikáciu servera a (voliteľne) klienta
    - X.509 certifikáty
  - zabezpečuje vzájomné dohodnutie kľúča
  - šifrovanie, kontrola integrity a autentickosti prenášaných dát
  - treba zabezpečiť bezpečnú distribúciu cert. CA

Bezpečnosť na aplikačnej vrstve

- end-to-end security
- e-mail
  - PGP, S/MIME
- vzdialené prihlasovanie
  - ssh
- autentifikácia používateľov v aplikáciach
  - heslá, jednorazové heslá, SMS-kódy, ...

Bezpečnosť elektronickej pošty

- správa elektronickej pošty = pohľadnica písaná na stroji
  - môže čítať každý, kto ju cestou vidí
  - nemožno dôverovať informácii o odosielateľovi
  - nemožno dôverovať obsahu
- riešenie
  - dôvernosť – šifrovanie
  - integrita a autentickosť – elektronický podpis

Bezpečnosť elektronickej pošty

- PGP (Pretty Good Privacy)
  - treba zabezpečiť bezpečnú distribúciu verejných kľúčov
  - vzájomná dôvera používateľov a podpisovanie kľúčov
- S/MIME (Secure Multipurpose Internet Mail Extensions)
  - použitie X.509 certifikátov
  - treba zabezpečiť bezpečnú distribúciu cert. CA

Bezpečnosť elektronickej pošty

- komunikácia so serverom
  - SMTP – odosielanie pošty
  - POP3, IMAP – čítanie pošty
  - nechránia komunikáciu
    - heslá sú ľahko odhaliteľné
- riešenie
  - SSL, TLS
    - SMTPS, POP3S, IMAPS

Bezpečnosť webu

- protokol HTTP
  - nezabezpečuje ochranu komunikácie
  - ktokoľvek môže vidieť to, čo vidím ja
  - ktokoľvek môže vidieť, čo odosielam
    - heslá, osobné údaje
  - ktokoľvek môže zmeniť to, čo vidím
  - ktokoľvek môže zmeniť to, čo odosielam

Bezpečnosť webu

- riešenie
  - SSL, TLS – HTTPS
- problémy
  - bezpečná distribúcia certifikátu CA
  - kontrola mena servera v certifikáte
  - SSLv2 (zakázať)
    - pripúšťa aj slabé šifry
  - ignorovanie upozornení browsera

Bezpečnosť vzdialeného prihlasovania

- telnet
  - žiadna ochrana
- ssh
  - šifrovanie, kontrola integrity, autentifikácia servera
  - umožňuje tunelovať ďalšie spojenia
    - napr. X11, VNC, SMTP, POP3, IMAP
  - treba zabezpečiť bezpečnú distribúciu verejných kľúčov serverov
  - neveriť slepo verejnému kľúču servera
  - openssh (UNIX, Linux, Cygwin), PuTTY (Windows)

Bezpečnosť ftp

- protokol FTP
  - nezabezpečuje žiadnu ochranu
    - heslá, prenášané dáta
  - má problémy so stateless firewallmi
  - statefull firewally musia podporovať ftp
- scp, sftp
  - náhrady využívajúce ssh
  - openssh, PuTTY, WinSCP (Windows)