



X36LOS – 5. cvičení

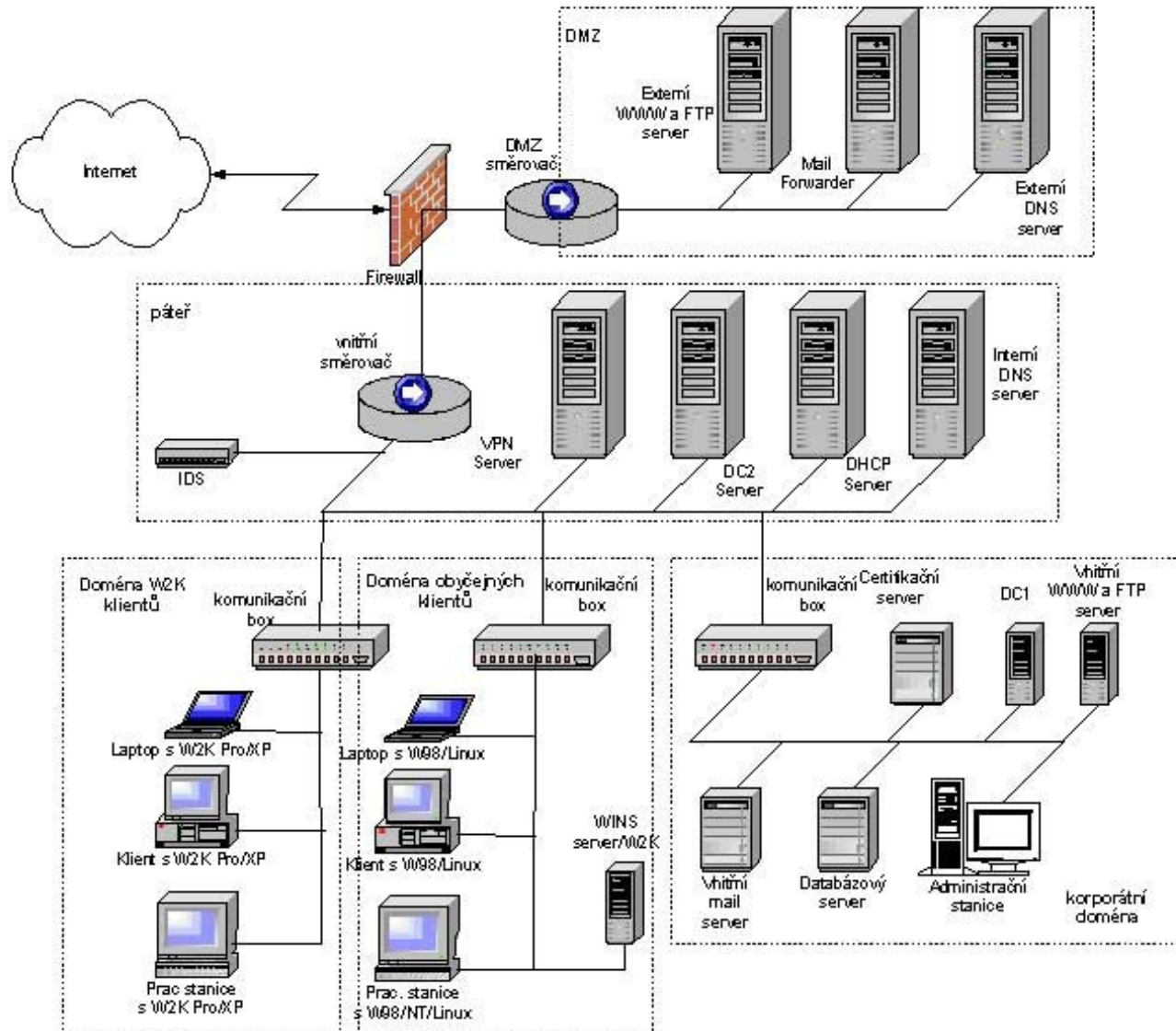
Rozsáhlé sítě a jejich návrhy



Rozdělení

- **PAN – Personal Area Network**
 - malé, „osobní“, např. Bluetooth PAN
- **LAN – Local Area Network**
 - omezené většinou budovou, např. síť v rámci koleje
- **MAN – Metropolitan Area Network**
 - rozsáhlejší, např. školní síť mezi kolejemi
- **WAN – Wide Area Network**
 - velmi rozsáhlé, např. Internet

LAN





Design Basics

- Internetworking devices

- Hubs (repeaters)

- jen zesilování a distribuce signálu

- Bridges

- L2 switching, nezávislé na vyšších vrstvách

- Switches

- jako předchozí, jen více portů; oddělují síť na více kolizních domén

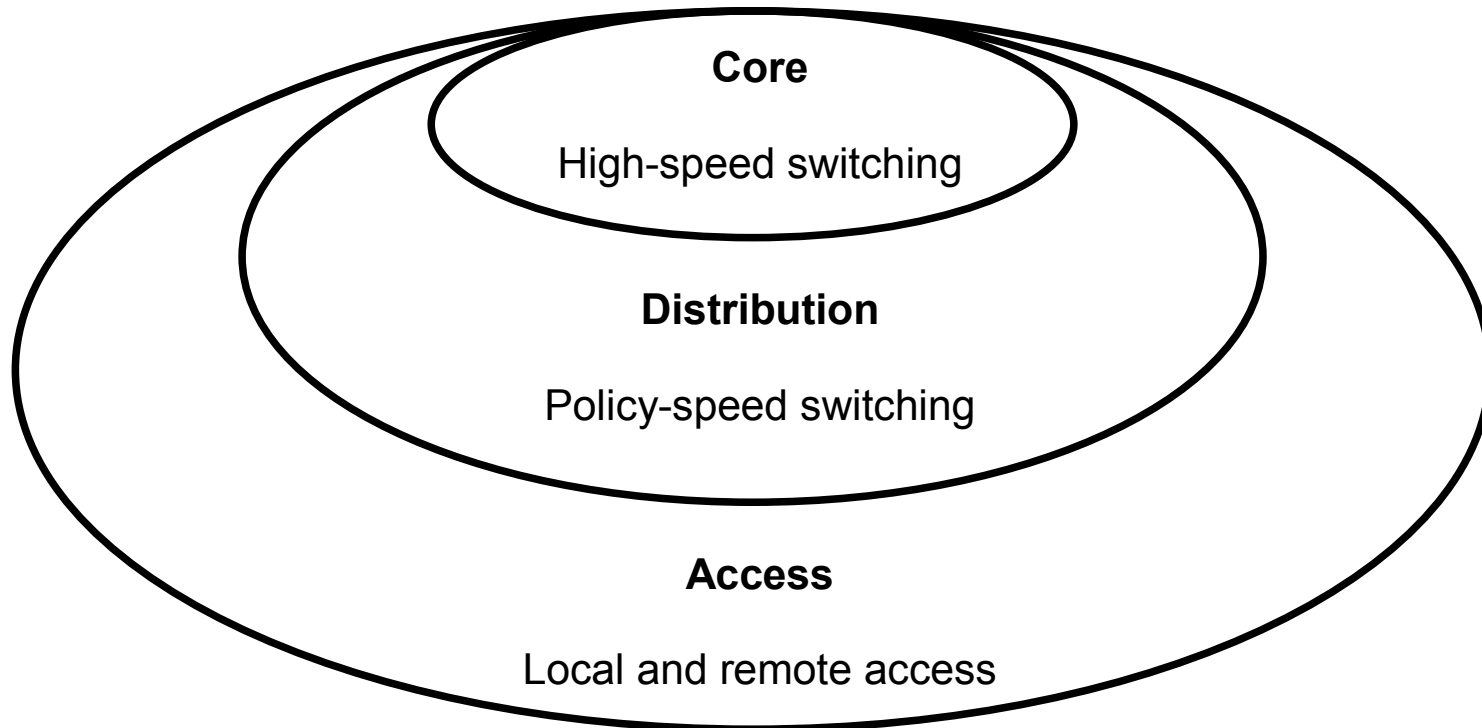
- Routers

- L3 switching, oddělují broadcastové domény



Síťový model

- Hierarchický model (Cisco)



Síťový model

•Hiearchický model

–Core Layer



- co nejrychlejší distribuce dat
- zbytečně nebrzdit (žádné filtrování, access listy ...)

–Distribution Layer



- vymezuje platnost skupin
- vymezuje broadcastovou/multicastovou doménu a routing
- VLANy, bezpečnostní politiky (firewall), QoS

–Access Layer



- vymezuje kolizní doménu – switche, huby
- mikrosegmentace, filtrování MAC adres



Zdroje informací

- Komunikace se zákazníkem
 - analýza potřeb
 - analýza požadavků cílových aplikací
 - distribuované x centralizované
 - zálohování
- Stávající infrastruktura
 - výskyt, zatížení a umístění serverů
 - operační systémy
 - adresářové služby
 - rozbor zatížení komunikačních linek



Co brát v úvahu

- Komplexní řešení
 - nezapomenout na hlasovou infrastrukturu
 - vždy aspoň jednu TP linku (na optiku telefony nejsou)
 - řešit výhledově na dobu 5 a více let
- Zvolit vhodnou „mohutnost“ řešení
- Používat vhodně spektrum přenosových médií
 - nezapomínat na bezdrátové technologie



Infrastruktura

- Dostatečně „silné“ linky pro servery
- Média
 - Optika
 - neodposlechnutelná
 - náchylná na vlhkost
 - problémy se spojováním
 - Metalika
 - široké využití
 - levná
 - pozor na rušení
 - omezení délky segmentu



Infrastruktura

–Bezdrát

- úspory za kabeláž
 - pozor na umístění outdoorové antény – blesk
 - nepředimenzovávat vysílače (dodržování norem)
 - u indoorových antén pozor na vertikální vyzařování
- Vhodné uspořádání „domén“ zařízení
 - výhodné pro definování bezpečnostních politik
 - doména: WinXP/2k klienti, linuxové stanice, korporátní servery, ...

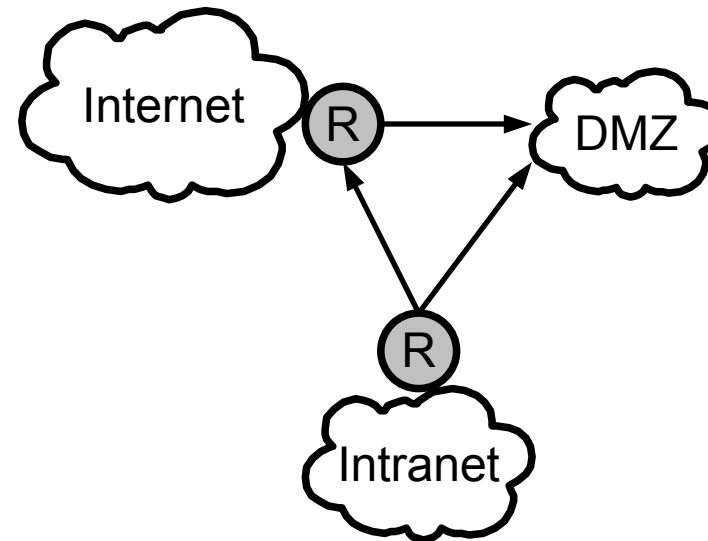
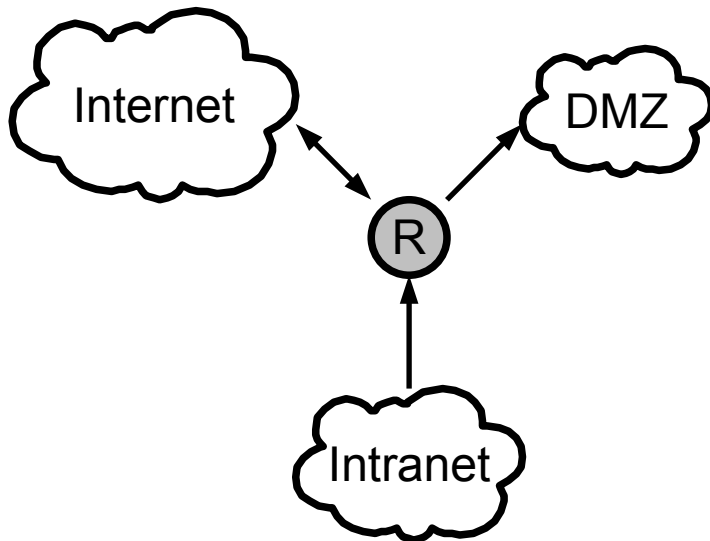


Bezpečnost

- Autentifikace serverů, uživatelů, ...
- IDS (Intrusion-detection systém)
 - analýza spojení a logů – vyhledávání podle vzorů
 - např. Snort, Prelude
- Firewall
 - omezení broadcastů
 - zablokování nepotřebných protokolů a služeb

Bezpečnost

- Použití DMZ (demilitarizovaná zóna)
 - část sítě určená jen pro publikaci dat navenek
 - nejčastěji pro vystavení WWW, FTP, SMTP



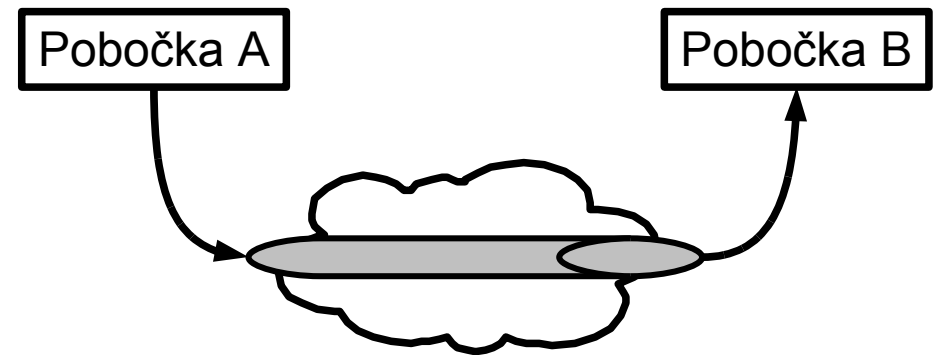
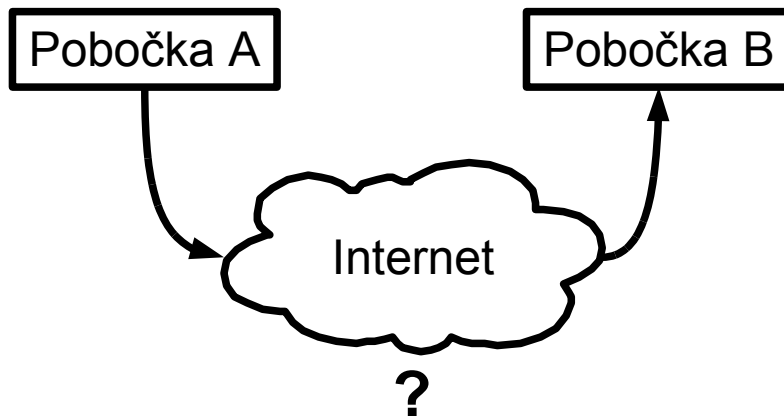
- VPN – Virtual Private Network

- „sít' v síti“

- možnost existence více „oddělených“ sítí na jednom

- fyzickém médiu

- cílem je zajistit bezpečnost jako v případě fyzického oddělení





Podmínky smlouvy

- SLA – Service level agreement
- Definice
 - střední doba výpadku, spolehlivost, poruchovost
- náhrady za neposkytnutou službu
- u QoS definovat
 - spolehlivost, zpoždění, jitter
- bezpečnost a způsoby zabezpečení