



UNIVERSITY OF ŽILINA  
Faculty of Management Science  
and Informatics

# Základy prepínaných sietí a prístupy k dizajnu škálovateľných sietí

## Zložené z:

- SRWE\_2 Switching Concepts (CCNA2v7)
- ENSA\_11 Network Design (**CCNA3v7**)

Pavel Segeč

KIS FRI UNIZA

CCNA/CCNP: CSC010532345



  
CISCO

Networking  
Academy



# Obsah prednášky

- Technológia ethernet
  - Voliteľne opakovanie
- Činnosť prepínača a prepínanie
- Hierarchický dizajn a výber prepínačov

# Úlohy prepínaných sietí

- Technológie prepínaných sietí sú rozhodujúce pre podnikový sieťový dizajn
  - Hlavná technológia je **ethernet**
- Prepínanie umožňuje poslať prevádzku iba tam, kde je to **potrebné**, a poslať ju **rýchlo**
- Prepínaná sieť LAN umožňuje:
  - Viac flexibility
  - Viac manažovania sieťovej prevádzky
  - Podporuje QoS (kvalitu služby)
  - Väčšiu bezpečnosť
  - Bezdrôtové pripojenie
  - IP telefóniu
  - Mobilné služby

# Preto zopár otázok na debatu k Ethernetu

- Otázky na zamyslenie:
  - Ako sa volá PDU na ethernetete? A aký ma formát?
  - Koľko formátov rámca v Ethernetete vlastne existuje?
  - Prečo má rámec stanovenú minimálnu a maximálnu dĺžku?
  - Čo je to kolízia? Aké druhy kolízií existujú?
  - Čo je to kolízna a broadcastová doména?
  - Čo je to slot time?
  - Ako funguje CSMA/CD?
  - Ako pracuje full-duplex na TP kabeláži? Ako súvisí s CSMA/CD?
  - Aké aktívne prvky sa v Ethernetete bežne používali / používajú?
  - Ako pracuje moderný prepínač nad štruktúrovanou kabelážou?
  - Aké sú aktuálne rýchlosti LAN (Ethernet) sietí?



Opakovanie



Pokračovanie



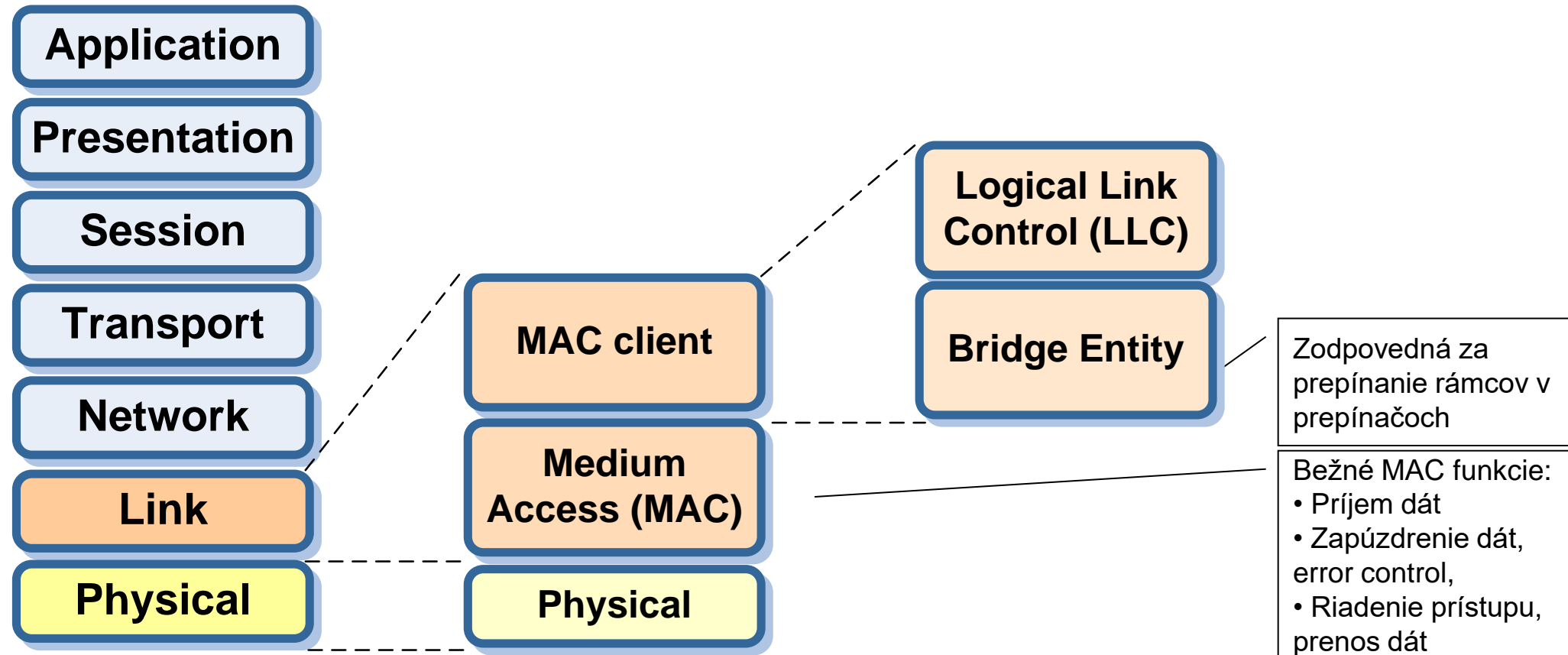
# Opakovanie

Len na zopakovanie z CCNA1, nie je obsahom preberaných kapitol

# Ethernet – na krátke pripomenutie

- Ethernet vznikol v prvej polovici 70. rokov v Xerox-e
  - Jedným z autorov bol Bob Metcalfe, zakladateľ 3Com
  - Lacná, nenáročná, best-effort linková technológia
- V súčasnosti dominantná linková technológia v LAN, významne sa rozmáha v SAN i v MAN / WAN
  - Carrier Ethernet, Data Center Bridging, Synchronous Ethernet
- Rôzne IEEE 802.3 štandardy
  - Líšia sa na L1, zhodné na L2
  - Rýchlosti od 10 Mbps do 100Gbps
  - Od 100m (UTP...) do desiatky km (jednovidové)

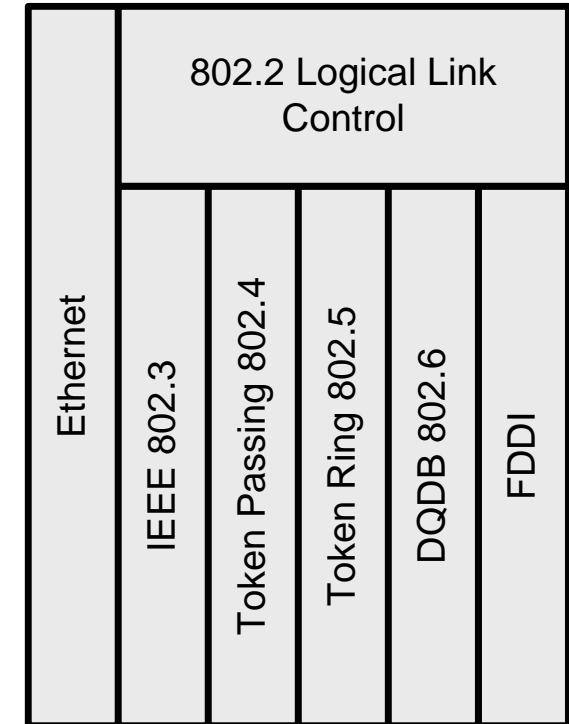
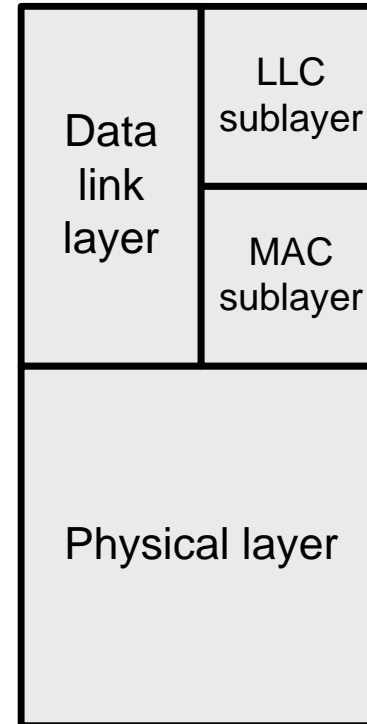
# Ethernet / IEEE 802.3 vs. ISO RM



- Ethernet / IEEE 802.3:
  - Definovaný na prvých dvoch vrstvách ISO OSI
  - Sú plne kompatibilné

# Ethernet - základy

- Použitá metóda riadenia prístupu
  - CSMA/CD (po 1 GigaEthernet vrátane)
    - 10GEthernet CSMA/CD nepoužíva
- Ethernet definuje vlastné PDU
  - Rámec
    - Použité na prenos používateľských dát
    - Min 64B - max. 1518B.
- Používa vlastné adresovanie
- Vyskytujúce sa topológie
  - Fyzická:
    - Bus (10Base2, 10Base5), Star (10BaseT, 100Base\_XX)
  - Logická:
    - Bus (CSMA/CD)
    - Point-to-Point (fullduplexný ethernet, žiadne CSMA/CD)





# Logical Link Control IEEE 802.2 (LLC)

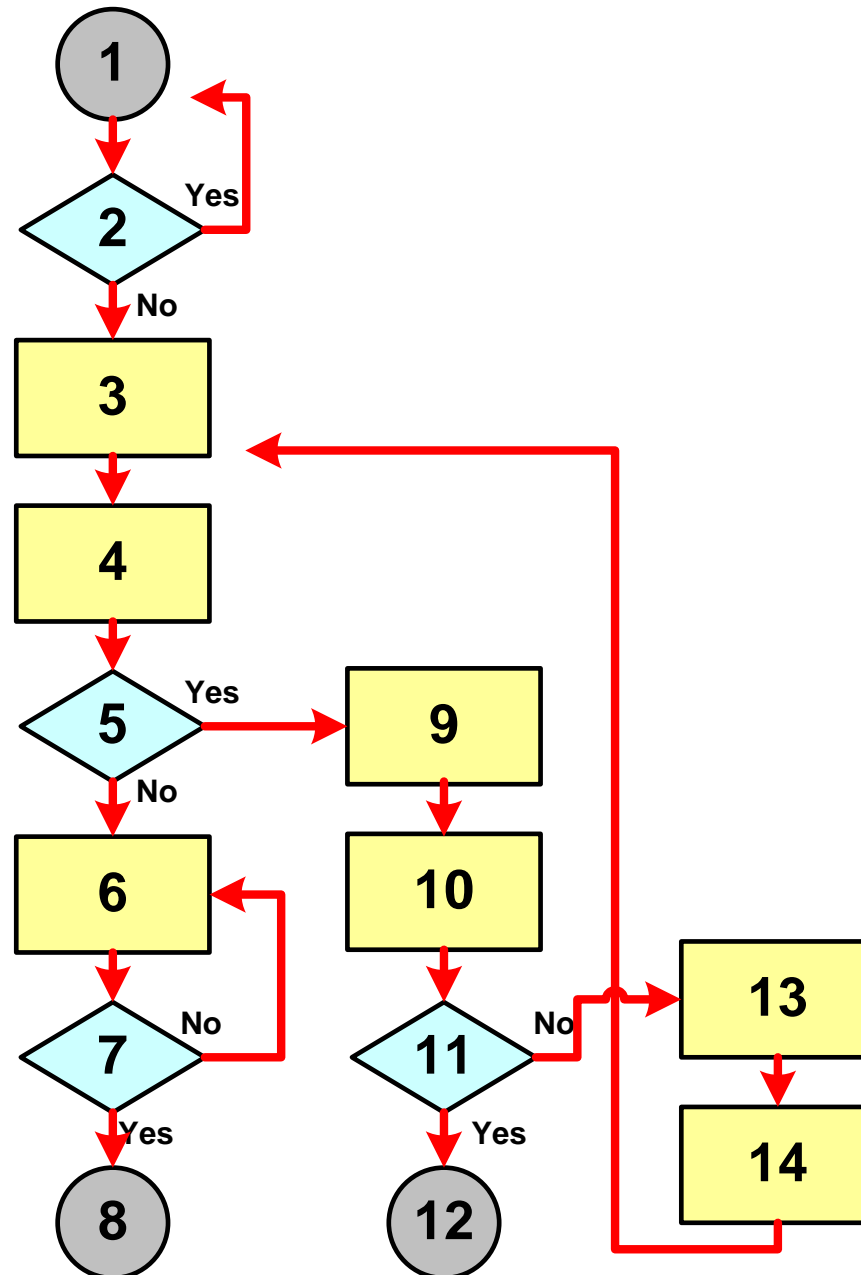
- **Logical Link Control IEEE 802.2 sublayer (LLC)**
  - Logicky oddeľuje vyššiu sieťovú vrstvu od nižšej, špecifickej podvrstvy prístupu k médiu (MAC)
    - Ako napr. IEEE 802.3, IEEE 802.5 a pod.
  - Poskytuje jednotné rozhranie voči sieťovej vrstve
- Funkcie:
  - Riadenie **toku rámcov**, riadenie **opravných procedúr** pri chybe prenosu, služby prenosu
  - Poskytuje pre sieťové protokoly tzv. prístupové body k médiu
    - Service Access Points (SAP)
  - SAP identifikuje sieťový protokol, ktorý predáva pakety na prenos LLC vrstve
    - Cez LLC môže komunikovať viacero sieťových protokolov naraz
      - IP, IPX, STP, NetBIOS apod.
      - Source SAP (SSAP), Destination SAP (DSAP)

# Medium Access Control

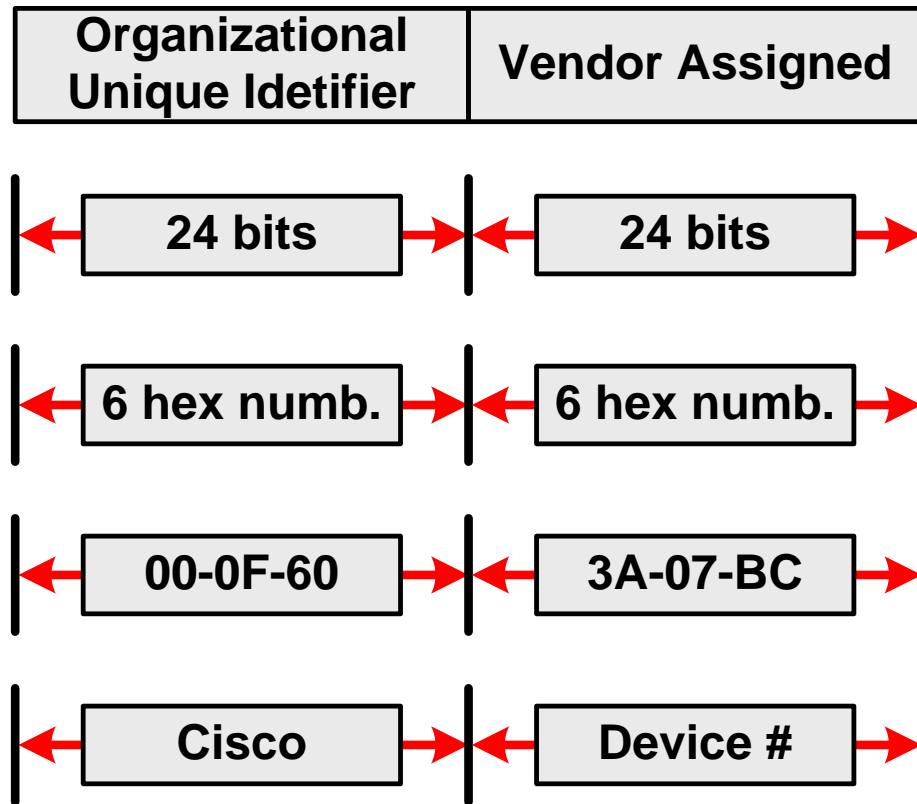
- Medium Access Control sublayer (MAC)
  - **Riadi prístup k médiu**
    - Zabezpečuje zdieľanie prenosového média pre komunikujúcich
  - **Riadi doručovanie dát cez sieť**
    - Adresovanie
      - Doručovanie na základe identifikácie príjemcu a odosielateľa
      - Adresa predstavuje fyzickú adresu zariadenia
    - **Funkcie práce s rámcom**
      - Definícia formátu rámcov (štruktúry)
      - Rozpoznávanie typu a formátu rámcov
      - Zabezpečenie prenosu (počítanie FCS a kontrola FCS pri doručení)
- Niektoré MAC metódy
  - **CSMA/CD** (Carrier Sense Multiple Access / Collision Detect)
  - **CSMA/CA** (Carrier Sense Multiple Access / Collision Avoidance)
  - Token Passing

# CSMA/CD

1. Host wants to transmit?
2. Is carries sensed?
3. Assemble frame.
4. Start transmitting.
5. Is a collision detected?
6. Keep transmitting.
7. Is the transmission done?
8. Transmission completed.
9. Broadcast JAM signal.
10. Attempts = Attempts + 1
11. Attempts > Too many
12. Too many collisions. Abort transmission.
13. Algorithm calculates backoff.
14. Wait for T microseconds.



# Základy Ethernet-u - adresovanie

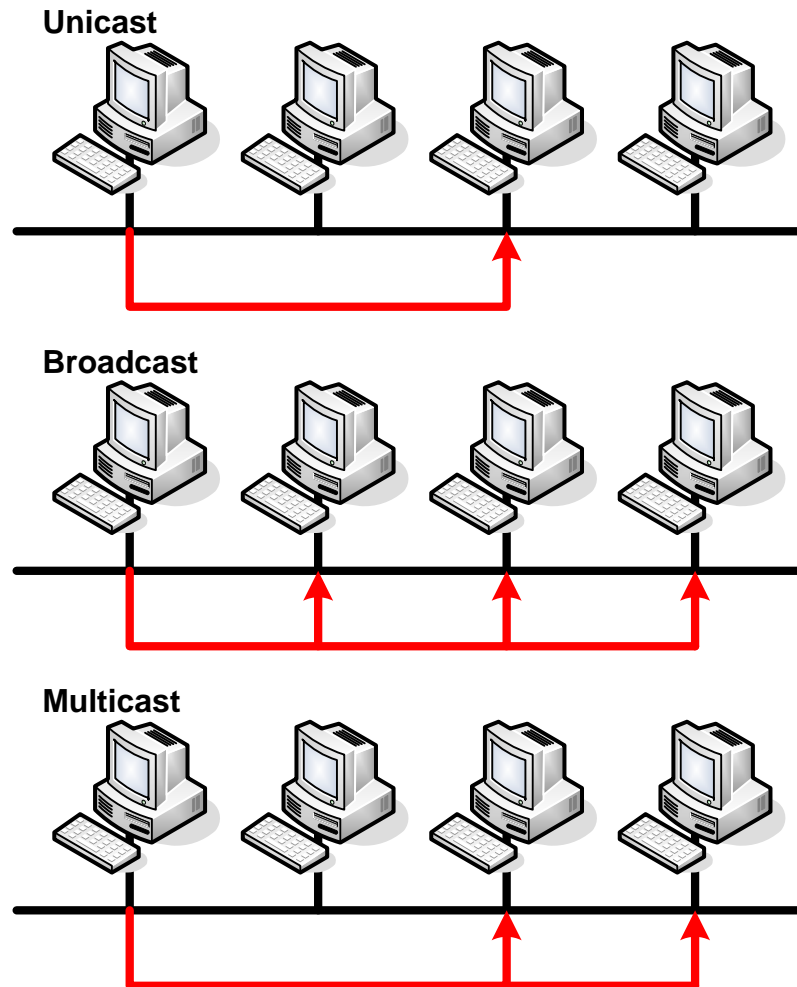


- Komunikácia
  - Komunikujúci musí byť jednoznačne určený - **adresa**
- Ethernet adresovanie
  - Fyzické adresovanie
    - Napálená MAC adresa v NIC
  - Plošné adresovanie
    - Nie sú logické väzby medzi adresami
  - Adresa dlhá **48 bitov**
    - 24 bit OUI
      - Organizational Unique Identifier
      - Riadi IEEE
      - Pozri: <http://standards.ieee.org/regauth/oui/oui.txt>
    - +
    - 24 bitov (pridelených výrobcom)

# Základy Ethernet-u - adresovanie

- Typy adries:
  - **Unicast:**
    - Určuje jedno zariadenie
  - **Multicast:**
    - Určuje skupinu zariadení, ale nie všetky
  - **Broadcast:**
    - Určuje všetky zariadenia na LAN
    - MAC (samé jednotky): FF-FF-FF-FF-FF-FF
- Z typov adries
  - Vyplývajú spôsoby komunikácie v Ethernet LAN

# Základy Ethernet-u - komunikácia



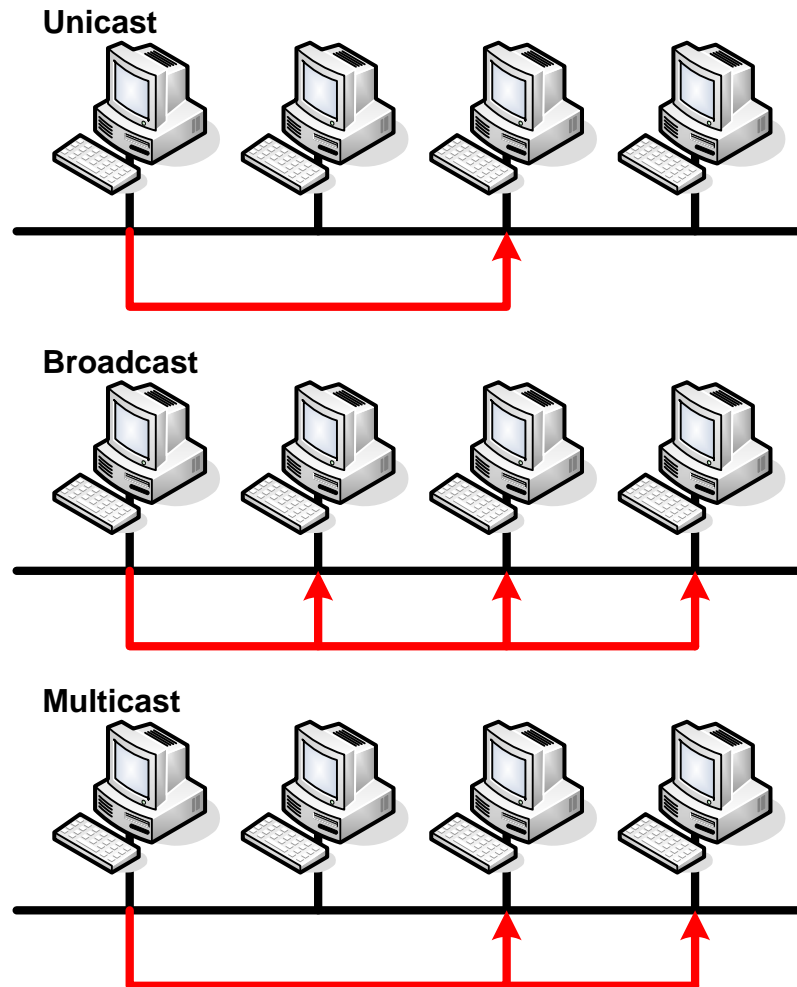
## ■ Unicast

- Najbežnejšia forma komunikácie
- Jeden odosielateľ, jeden príjemca
- Odosielateľ
  - Vyplní rámec s unicast adresou odosielateľa a unicast adresou prijímateľa
- Sieť doručí práve danému prijímateľovi

## ■ Broadcast

- Častá forma komunikácie
- Jeden rámec zaslaný všetkým LAN staniciam
  - LAN zariadenia kopírujú rámec na všetky svoje porty

# Základy Ethernet-u - komunikácia



## ■ Broadcast cont.

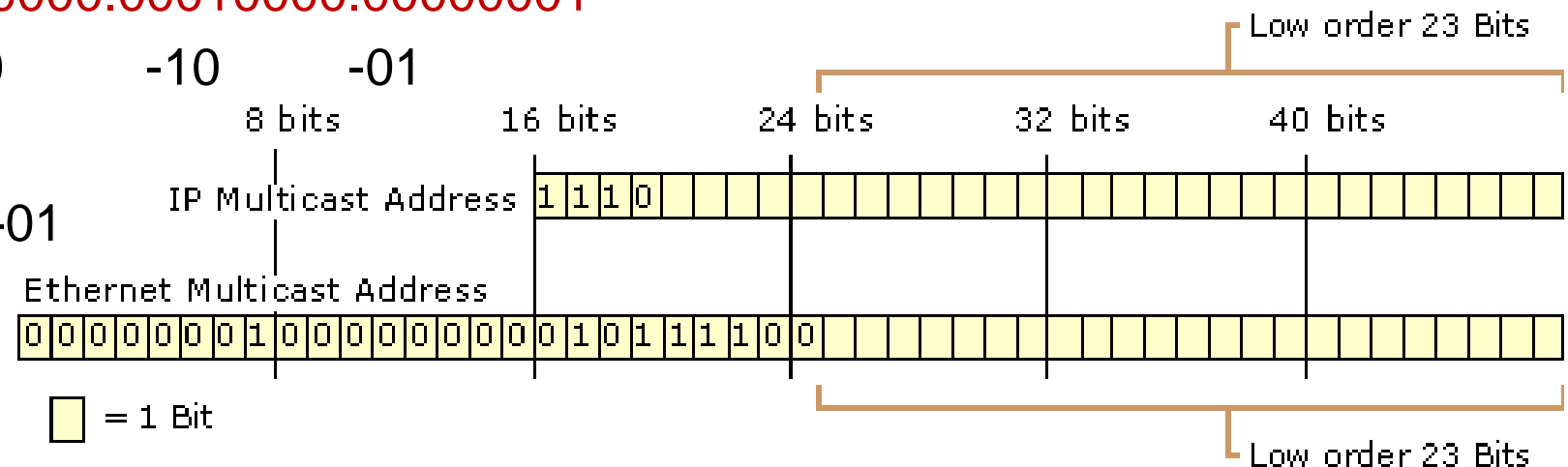
- Odosielateľ
  - Vyplní rámec svojou unicast adresou a všetkých prijímateľov
  - Tzv. Broadcast adresa
    - FF-FF-FF-FF-FF-FF
- Sieť doručí všetkým uzlom

## ■ Multicast

- Skupinová komunikácia
- Jeden rámec zaslaný podskupine prijímateľov (nie všetkým)
- Sieť kopíruje rámec len na porty prijímateľov
- Odosielateľ
  - Vyplní rámec svojou unicast adresou a adresou pod skupiny prijímateľov

# Odvodzovanie mcast MAC adresy z IP mcast adresy

- Ethernet multicast rezervované adresy
  - 01-00-5E-00-00-00 do 01-00-5E-7F-FF-FF
    - 25 najvyšších bitov zo 48 je rezervovaných
- Pri mapovaní IPv4 mcast adresy sa mapuje najnižších 23 bitov
  - Sedem bitov druhého oktetu, celý tretí a štvrtý oktet
- Príklad
  - 224.192.16.1
    - 11100000.11000000.00010000.00000001
    - E0 -C0 -10 -01
  - Sa namapuje do
    - 01-00-5E-40-10-01





# Ethernet – Formát rámca

- V Ethernete existuje niekoľko druhov rámcov, no všetky majú podobnú základnú štruktúru



- Základný formát je zhodný pre všetky varianty Ethernetu
- Varianty formátu rámca:
  - Ethernet II (tzv. DIX)
  - 802.3 (niekedy 802.2 kvôli LLC hlavičke)
  - SNAP (niekedy 802.3 SNAP)
  - Novell Raw (nie je pre nás zaujímavý)

# Ethernet – Formát rámca

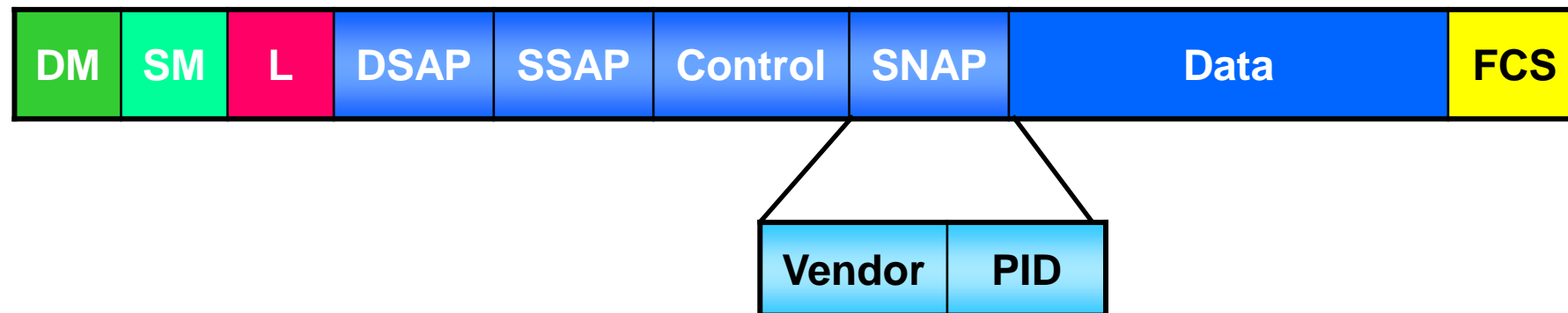
## Ethernet II



## Ethernet 802.2 LLC



## Ethernet 802 SNAP



# Polia ethernet rámcov

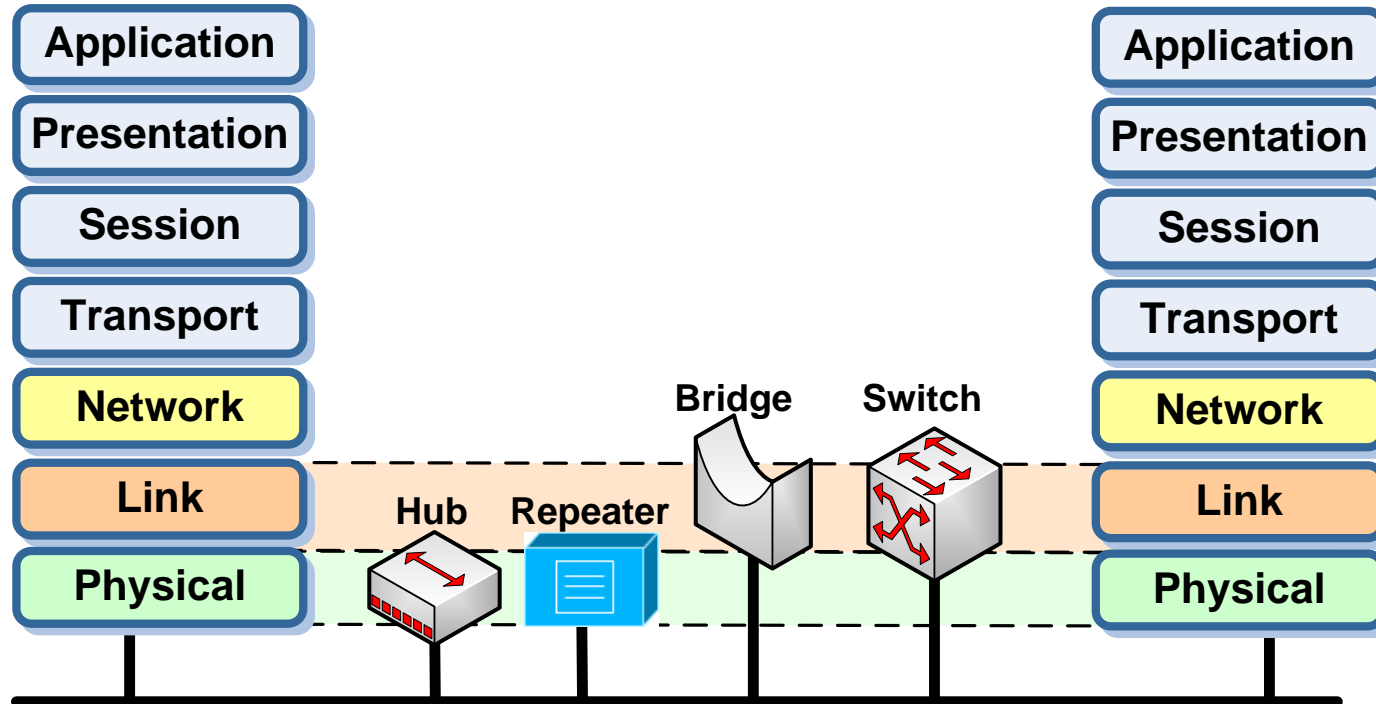
- **Preamble:** 7B IEEE802.3 or 8B (Ethernet)
  - Bitová a rámcová synchronizácia
    - Opakujúca sa postupnosť jednotiek a núl
    - Časová synchronizácia
- **Start Of Frame Delimiter:** 1B
  - Oznamuje koniec časových informácií v preambule
    - Bitová vzorka: 10101011
- **Destination Address:** 6B
  - MAC adresa prijímateľa (adresáta)
- **Source Address:** 6B
  - MAC adresa odosielateľa
- **Length/Type:** 2B
  - IEEE 802.3
    - Ak hodnota < 0x600: Hodnota určuje dĺžku dátovej časti rámca
    - Ak hodnota > 0x600: Hodnota určuje typ sieťového protokolu
  - Ethernet II
    - Type: Hodnota určuje typ sieťového protokolu
    - Napr:
      - 0x0806: ARP protokol
      - 0x0800: IPv4 protokol
- **LLC Header**
  - **DSAP (Destination Service Access Point):** 1B
    - Identifikuje cieľový L3 protokol
  - **SSAP (Source Service Access Point):** 1B
    - Identifikuje zdrojový L3 protokol nesený v rámci
  - **Control:** 1B
    - Identifikuje typ LLC rámca
- **SNAP (SubNetwork Access Protocol) Header**
  - **Protocol ID:** 5B
    - Rozširuje možnosti na identifikáciu viac a ďalších protokolov ako umožňuje LLC
- **Data: Variable Length**
  - Dátová časť
  - Dĺžka závisí od typu rámca
    - 46 až 1500 B dlhá
- **FCS (Frame Check Sequence):** 4B
  - Kontrolná suma (CRC) cez rámec
    - Nezahŕňa sa preambula a SOF
  - Zabezpečenie voči chybám pri prenose

# Formáty ethernetových rámcov - Závěrečné poznámky

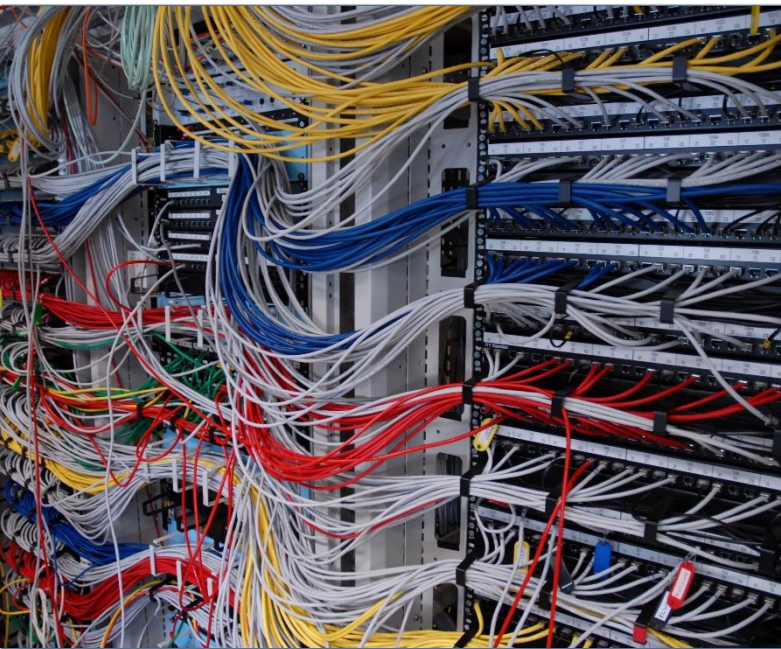
- Všetky tri formáty rámcov sú výlučne vecou softvérovej implementácie – nevyžadujú si špeciálne sieťové karty
  - Sieťová karta môže komunikovať všetkými formátmi naraz
- Najpoužívanejší typ je Ethernet II
  - Drvivá väčšina sieťovej prevádzky vrátane IPv4 a IPv6
- Ostatné typy rámcov sú v úzadí
  - 802.2 LLC – využívaný najmä pre protokoly od IEEE (STP a jeho varianty, LACP, LLDP, ...). Pre IP sa nevyužíva, lebo ARP nemá pridelenú hodnotu SAP
  - 802 SNAP – využívaný najmä pre firemné a proprietárne protokoly (CDP, VTP, DTP, PAgP, ...)



# Ethernet zariadenia



- **Repeater, Hub**
  - Pracujú na fyzickej vrstve (L1)
- **Bridge (Most), Switch (Prepínač), NIC (Sieťová karta)**
  - Pracujú na linkovej vrstve (L2)



... pokračujeme ...  
na LAN Switching

# Layer 2 prepínanie – Ethernet

- L2 prepínače vykonávajú nasledovné funkcie
  - Učia sa MAC adresy z poľa zdrojovej adresy hlavičiek prichádzajúcich rámcov
  - Budujú a udržujú si tabuľku MAC adries a k nim asociovaných portov
    - Pri Cisco nazývaná a realizovaná ako CAM tabuľka
  - Rámce **prepínajú** na základe cieľových L2 adries (hardware based bridging)
  - **Broadcastové a multicastové rámce** sú **záplavovo** posielané von cez všetky porty okrem portu na ktorom bol rámec prijatý
  - Rámce určené pre **neznáme** MAC adresy sú **záplavovo** posielané von cez všetky porty okrem portu na ktorom bol rámec prijatý
  - Bridges a switches komunikujú s inými L2 zariadeniami za účelom ochrany proti vzniku L2 slučiek (Nie je súčasť 802.3 štandardu)
- Implementácia
  - ASIC (application-specific integrated circuits)
    - Hardvérovo vykonávané prepínanie

# LAN Most/Prepínač - Činnosť

- Možné činnosti na základe cieľovej MAC adresy per LAN/VLAN
  - Prepni (forward)
    - Unicast ak je nájdená adresa a cieľový port
  - Rozpošli (Flood)
    - Broadcast alebo neznámy unicast
  - Zahod' (Filter)
- Rozlišuje sa
  - Ingress port (vstupný)
  - Egress port (výstupný)



Forwarding Table

0000.1111.1111: port 2  
0000.2222.2222: port 1  
0000.3333.3333: port 1  
0000.4444.4444: port 2

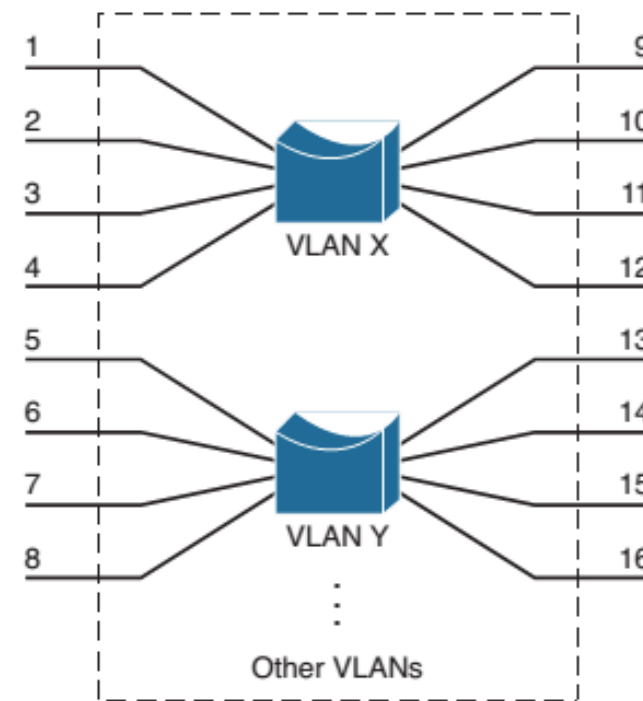
Broadcast: all ports



Forwarding Table

0000.1111.1111: port 4  
0000.2222.2222: port 6  
0000.3333.3333: port 1  
0000.4444.4444: port 2  
0000.5555.5555: port 8  
0000.6666.6666: port 5  
0000.7777.7777: port 3  
0000.8888.8888: port 7

Broadcast: all ports



Forwarding Table

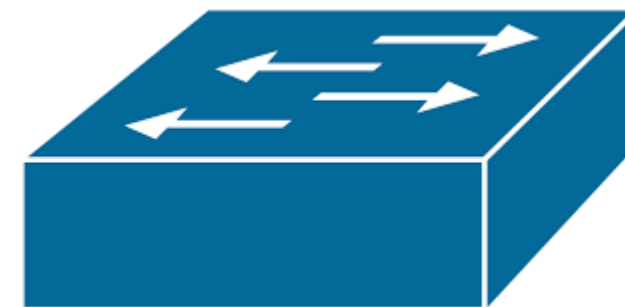
0000.1111.1111: port 11, vlan X  
0000.2222.2222: port 6, vlan Y  
0000.3333.3333: port 1, vlan X  
0000.4444.4444: port 9, vlan X  
0000.5555.5555: port 8, vlan Y  
0000.6666.6666: port 14, vlan Y  
0000.7777.7777: port 3, vlan X  
0000.8888.8888: port 16, vlan Y

Broadcast: VLAN X: all VLAN X ports  
Broadcast: VLAN Y: all VLAN Y ports



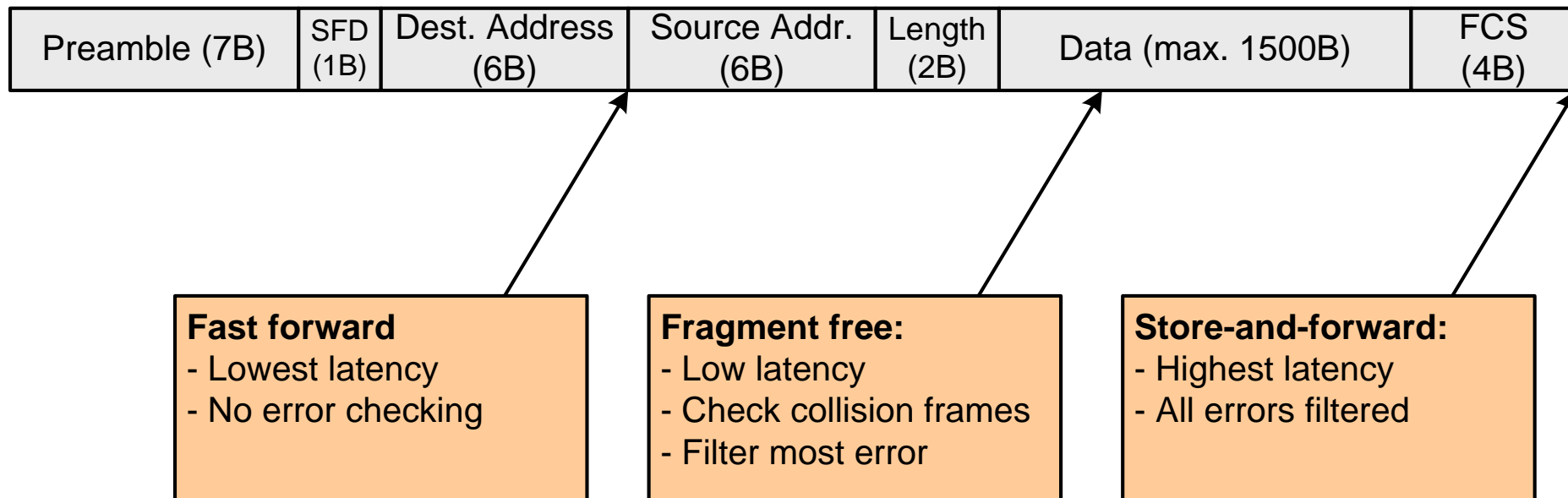
# Režimy prepínania rámcov na prepínačoch

- Prepínačom teoreticky stačí poznať prvých 6B rámca, aby urobili rozhodnutie o ceste a mohli rámec začať prenášať na výstupné rozhranie
- Z tohto faktu plynú viaceré prepínacie metódy
  - **Store and Forward switching**
    - Rámec sa načíta kompletný a odosiela sa až po kontrole správnosti
    - Error kontrola: CRC, veľkosť rámca
    - Prepínač musí rámce na dobu spracovania „bafrovať“
    - Default pre Catalyst prepínače, nedá sa zmeniť
  - **Cut-Through switching**
    - Rámec je prepínaný na výstup skôr, ako je celý prijatý
    - Latencia prepnutia pod 10ms



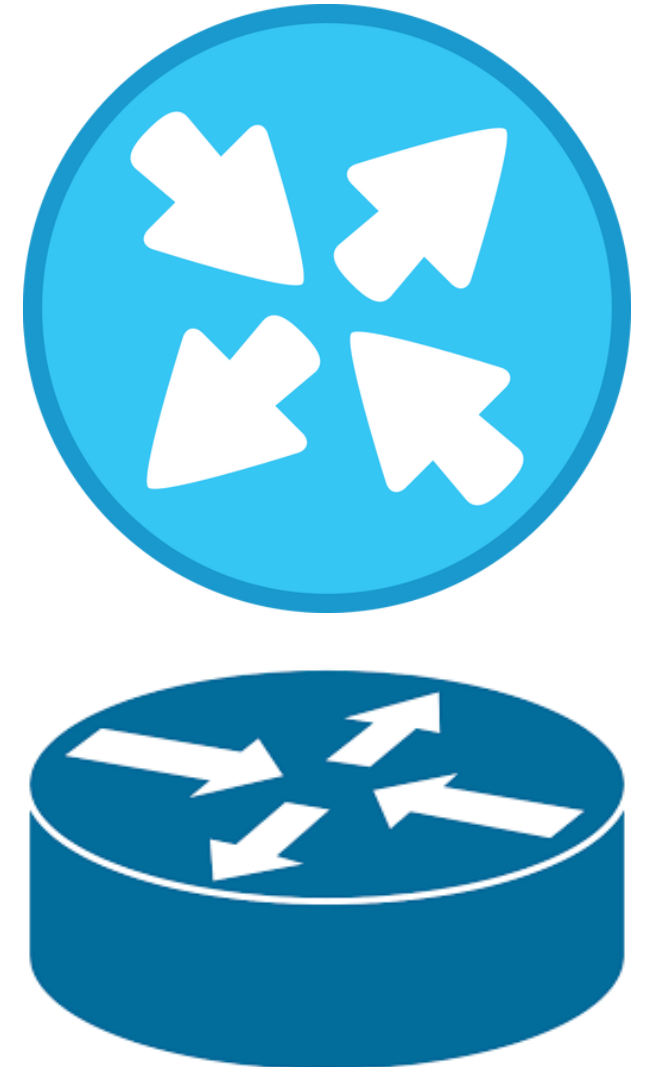
# Režimy prepínania rámcov na prepínačoch

- **Cut-Through** sa delí na dve podkategórie
  - **Fast Forward**
    - Prepínanie sa začína hneď po načítaní cieľovej MAC adresy
    - Default pre **Nexus** prepínače
  - **Fragment Free**
    - Prepínanie sa začína po načítaní prvých 64B rámca



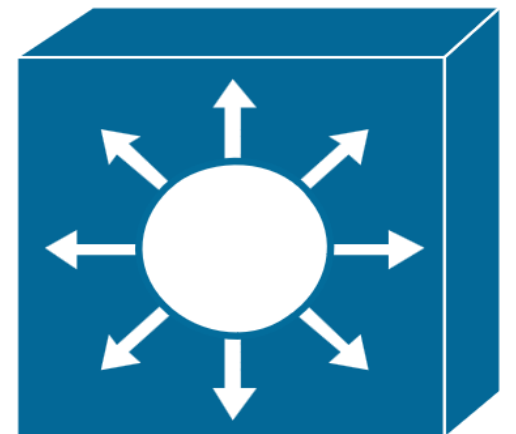
# L3 smerovanie (routing/forwarding)

- L3 smerovače vykonávajú nasledovné funkcie
  - Pakety sú doručované medzi sieťami na základe L3 adries
  - Pre pakety vyberá optimálnu cestu daný router na základe jeho lokálnych informácií a doručuje ho susedovi po ceste
    - Smerovacie rozhodnutie zahŕňa prehľadanie smerovacej tabuľky na základe cieľovej siete, výber next hop smerovača a výstupného rozhrania
  - Výber optimálnej cesty môže byť podmieňovaný mnohými možnosťami
  - Smerovače komunikujú s inými smerovačmi pomocou smerovacích protokolov.
- Smerovanie vykonávané CPU



# Multi-Layer switching (MLS)

- Multilayer switching je pojem pre prepínanie datagramov na rôznych vrstvách OSI
  - **Layer 1** – nie je switching: Prenos a zosilnenie signálu
  - **Layer 2 switching**: Prenos rámcov (určujúca je L2 hlavička)
    - Hardware based bridging
  - **Layer 3 switching**: Prenos paketov (určujúca je L3 hlavička)
    - Hardware based routing
  - **Layer 4 switching**: Prenos segmentov (určujúca je L3 + L4 hlavička)
  - **Layer 7 switching**: Prenos aplikačných dát (určujúci je ich obsah)
- Rozdiel medzi switchingom a routingom?
  - Routing je obvykle softvérový - CPU
  - Switching je realizovaný s hardvérovou podporou – ASIC
- Multilayer switche
  - Switche s podporou prepínania na viacerých vrstvách súčasne
  - Rozšírene používané v Campus net. dizajne



# MLS Cisco prepínače na L3

- Môžu používať tri módy prepínania:
  - Process-based switching
    - **Bežný softvérový routing**
  - Fast switching - [Route caching](#)
    - **Alternatívne názvy: *NetFlow LAN switching, flow-based or demand-based switching, „route once, switch many“***
    - **Prvý paket ako PBS, ďalšie cez cache**
  - Cisco Express Forwarding (CEF) – topology based switching
    - **Sw/hw, centralizované/distribúované**
    - **Forwarding Information Base (FIB)**
      - Routing TCAM or L3 forwarding table
      - „otlačok“ smerovacej tabuľky
    - **Adjacency table (L2 info)**
      - L2 next hop rewrite info

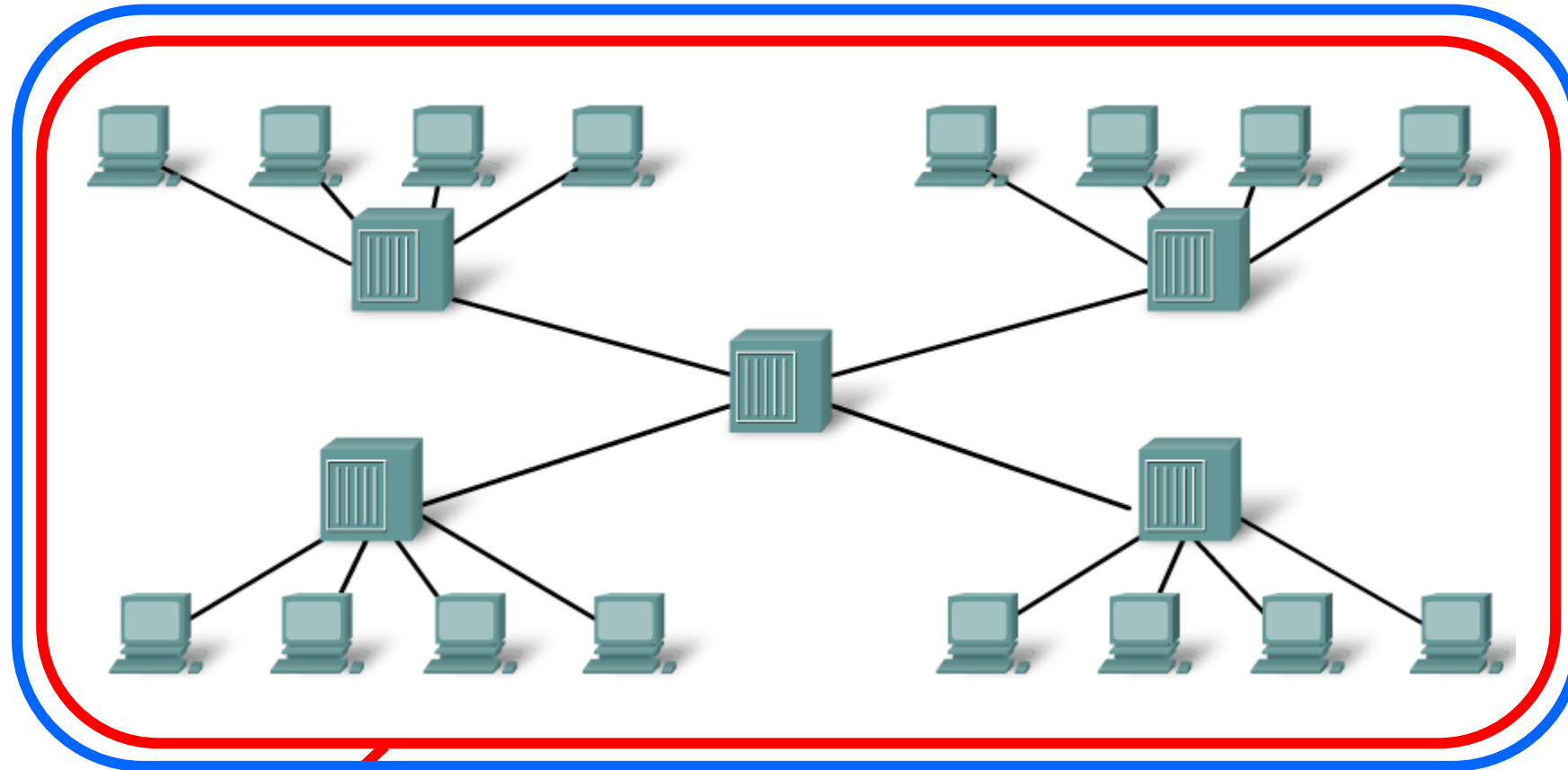
```
Show ip cef [detail]
```

```
Show adjacency ...
```

# Znižovanie miery zahltenia v sieti

- Príspevok prepínačov k výkonnosti siete
  - Jednoduchosť a výkon
  - Segmentáciou LAN do samostatných **kolíznych** domén
  - Segmentáciou LAN do samostatných **broadcast** domén (VLAN)
  - Full-duplexným typom komunikácie medzi zariadeniami (kde?)
  - Veľkým počtom portov (koľko?) per zariadenie
  - Ukladaním rámcov do frontu
  - Vysokorýchlostnými portami
  - Rýchlym prepínaním rámcov

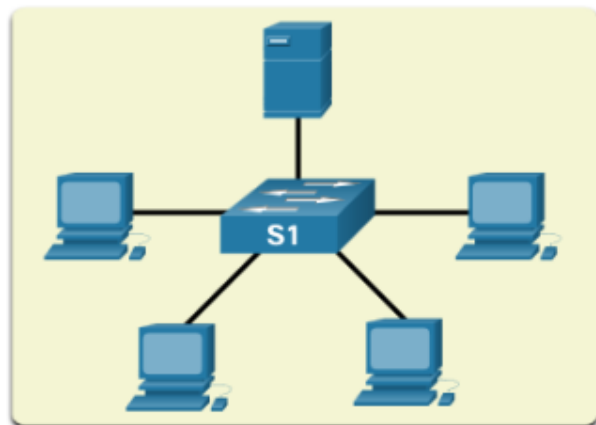
## Kolízna a broadcast doména - Hub



Kolízna doména

Broadcastová doména

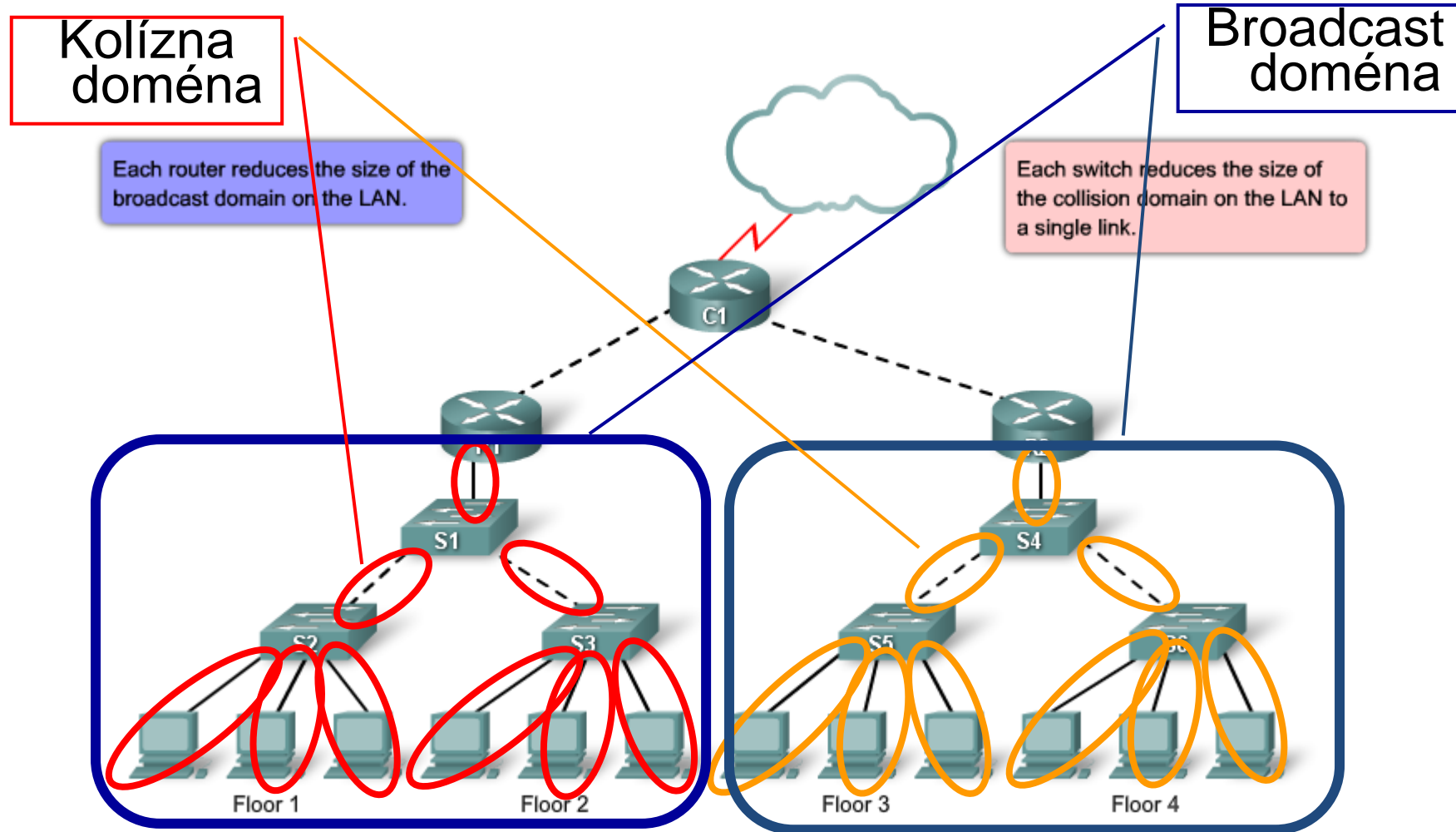
# Kolízna a broadcast doména – Segmentácia prepínačmi na L2

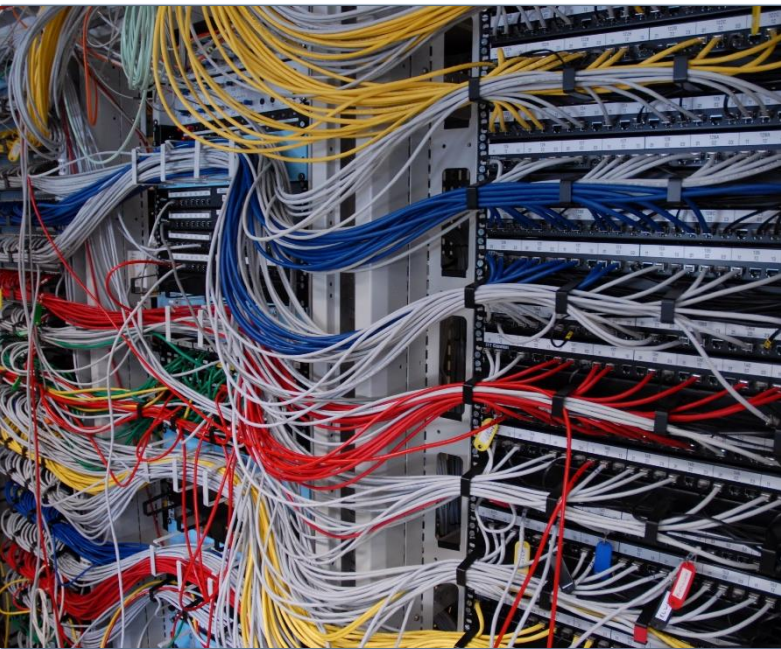


- Keď prepínač vrstvy 2 prijme vysielanie, zaplaví ho všetky rozhrania okrem vstupného rozhrania.
- Broadcast doména
  - Rozprestiera nad všetkými zariadeniami vrstvy 1 alebo 2.
    - Iba L3 zariadenie (smerovač) rozbíja bcast doménu
    - nazýva aj vysielacia doména MAC.
  - Príliš veľa bcastu môže spôsobiť preťaženie a znížiť výkon siete.
  - Zväčšenie počtu zariadení na vrstve 1 alebo 2 spôsobí rozšírenie bcast domény.



# Kolízna a broadcast doména – Segmentácia na L3

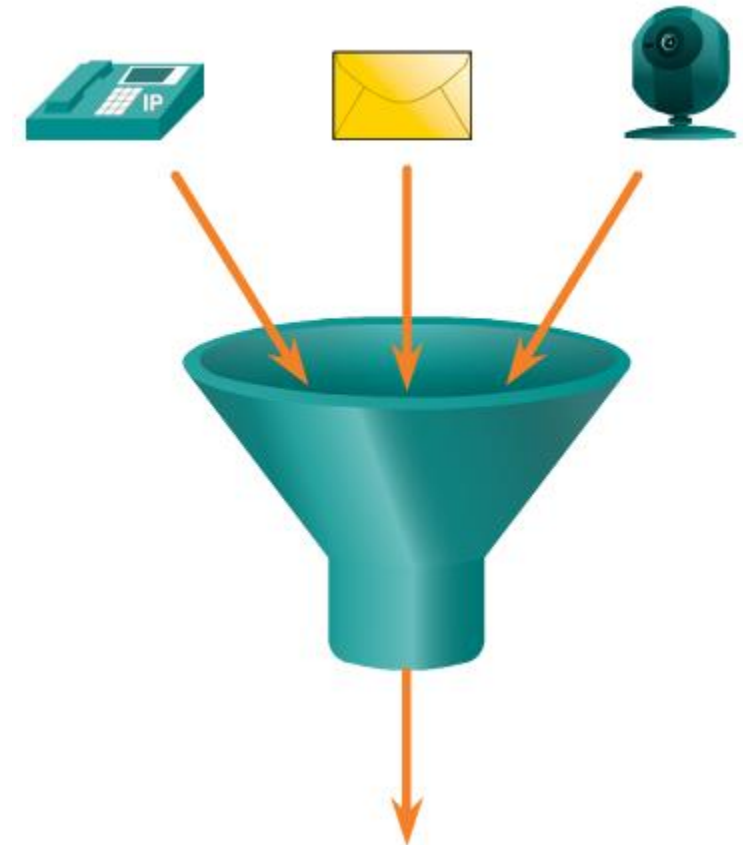




# Dizajn LAN sietí a výber zariadení

# Potreba pre škálovanie prepínaných sietí

- Je potrebné si uvedomiť
  - Žijeme v digitalizovanom svete
    - Komunikujeme elektronicky rôznymi spôsobmi
  - Preto aj typické moderné podnikové siete (ale už aj malé/domáce siete)
    - Prenášajú mix rôznej komunikácie (**konvergencia**):
      - Dátovú komunikáciu používateľov
        - pošta, web, sťahovanie obsahu, kritické aplikácie ...
      - Rôzne multimedia (QoS)
        - Hlasovú, textovú, video (hry, skype, whatsapp, youtube apod.)
      - Manažment a správa siete
        - telnet, ssh, https, snmp, syslog ...
  - Tieto siete tak na poskytnutie požadovaných služieb obsahujú rôzne zariadenia
    - Nielen PC ale aj notebooky, teleprezenčné zariadenia, IPTV, IP telefóny, stream servery a podobne

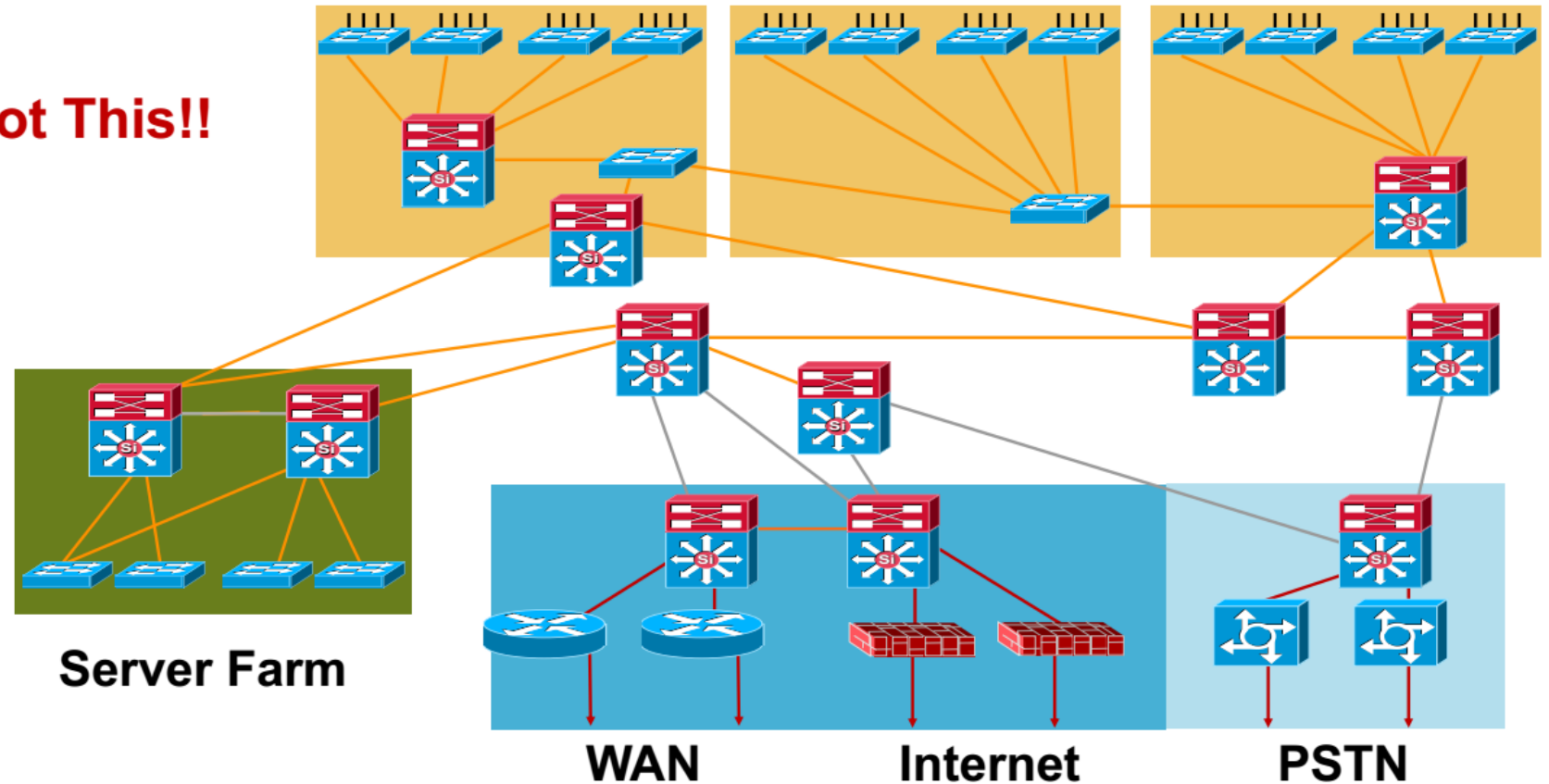


# Potreba pre škálovanie prepínaných sietí

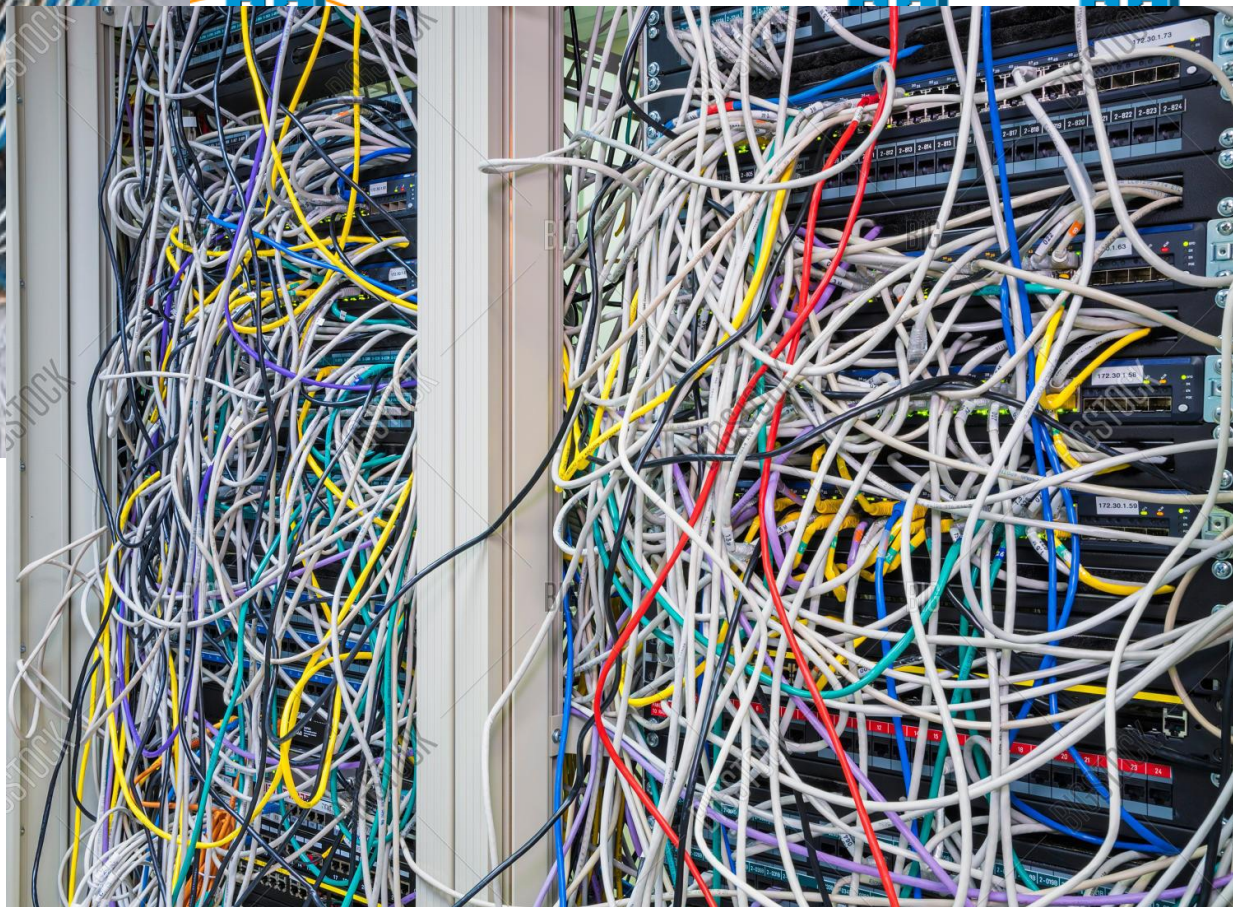
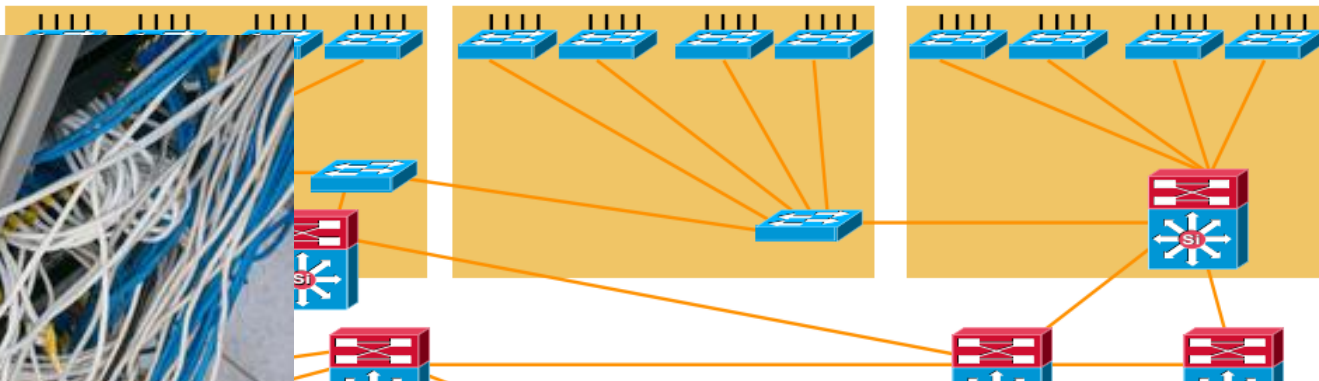
- Uspokojovanie nových požiadaviek a zavádzanie nových služieb vedie k nárastu požiadaviek (a zložitosti) na tieto siete
- Pre firmy je preto kľúčové zabezpečiť správnu činnosť siete, jej aplikácii a služieb
  - => dôležité je sieť dobre navrhnuť od počiatku
    - Aby bola sieť
      - Odolná voči chybám
      - Ľahko udržiavateľná s spravovateľná
      - Ľahko sa rozširujúca či inovujúca
- Dobre zvolená stratégia návrhu neskôr šetrí náklady a ponúka želaný výkon siete
  - Existujú rôzne stratégie návrhu
    - Ad-hoc (univerzálny)
    - Hierarchický model (univerzálny)
    - Borderless networks (Cisco stratégia)

# Prístup buduj podľa potreby (Ad- hoc )

**Not This!!**



- Siete sú mnohokrát budované takzvaným **ad-hoc prístupom**
  - Začnem časťou a postupne podľa požiadavky sa do siete pridávajú nové
  - Takéto siete
    - Po dosiahnutí určitej veľkosti začne byť sieť tak neprehľadná, že je problém ju ďalej prevádzkovať a spravovať
    - Alebo im chýba odolnosť voči poruchám a výpadkom
- Tento návrh **nie je systematický**
  - Preto sa silne neodporúča navrhovať siete týmto spôsobom!



- Siete sú mnohokrát budované takzvaným **ad-hoc prístupom**
    - Začnem časťou a postupne podľa požiadavky sa do siete pridávajú nové
    - Takéto siete
      - Po dosiahnutí určitej veľkosti začne byť sieť tak neprehľadná, že je problém ju ďalej prevádzkovať a spravovať
      - Alebo im chýba odolnosť voči poruchám a výpadkom
- Tento návrh **nie je systematický**
- Preto sa silne neodporúča navrhovať siete týmto spôsobom!

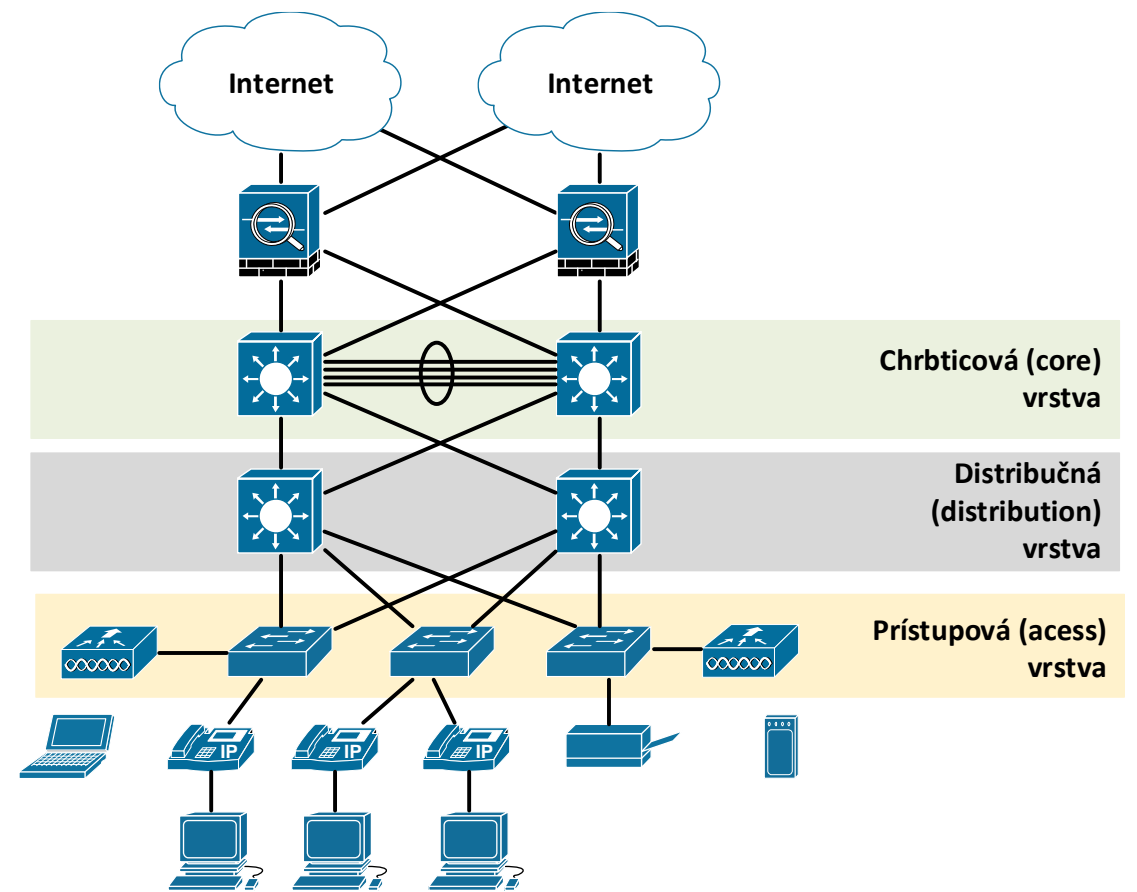
# Podnikové siete

- Pri podnikových sieťach môžeme pozorovať fakt, že:
  - Obsahujú zariadenia rôzneho typu, funkčnosti a výkonu
    - Ideálne nie veľmi veľa rôznych typov a od rôznych výrobcov
  - Je výhodné preto zariadenia rozdeliť podľa ich funkcie, ktorú majú v sieti plniť,
  - Následne organizujeme zariadenia po **vrstvách**:
    - Isté zariadenia budú slúžiť na pripájanie koncových zariadení do siete
    - Iné zariadenia vyššej vrstvy budú navzájom prepájať tieto prístupové zariadenia.
    - Zariadenia na najvyššej úrovni budú tvoriť chrbticu celej siete
- Toto viedlo k vzniku návrhového vzoru sietí  
=> **Hierarchický vrstvový model siete** (klasický prístup)



# Hierarchický model siete

- Rozdeľuje sieť podľa funkcionality do troch vrstiev
- **Access**
  - Poskytuje prostriedky na prístup používateľov a zariadení do siete
  - Riadi kto môže komunikovať cez sieť
  - Definuje bezpečnostnú hranicu
  - Podpora pokročilých služieb (voice, video)
- **Distribution**
  - Škálovateľnosť = Agreguje konektivitu z prístupovej vrstvy
  - Optimalizuje smerovanie medzi nimi
  - Riadi tok dát (smerovacie a ACL politiky)
  - Musí byť vysokorýchlostná a redundantná



- **Core**
  - Tvorí vysokorýchlostnú chrbticu siete
  - Prepája viaceré distro prepínače na iné domény
    - Agreguje dáta od distribučných prepínačov
  - Musí byť vysokodostupná a redundantná
    - Musí zvládať spracovávať veľké objemy dát a veľmi rýchlo
  - Len vo veľkých podnikových sieťach

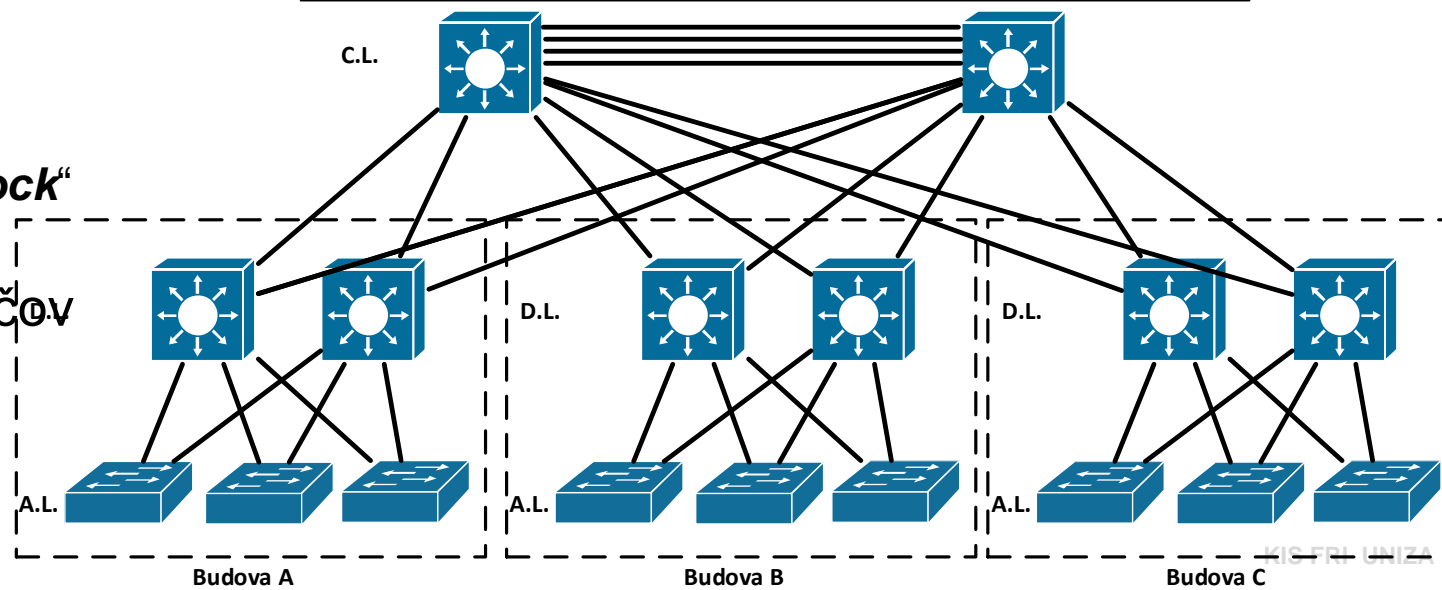
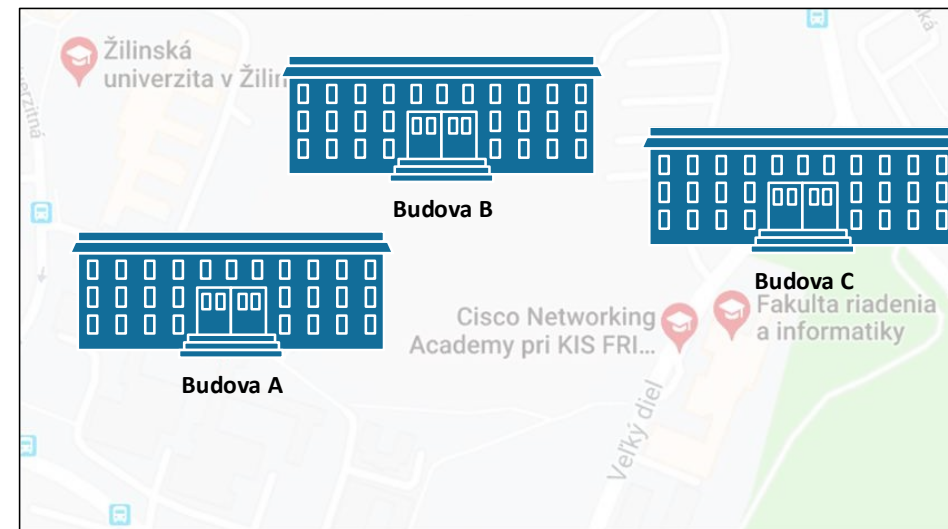


# Hierachický model - aplikovanie

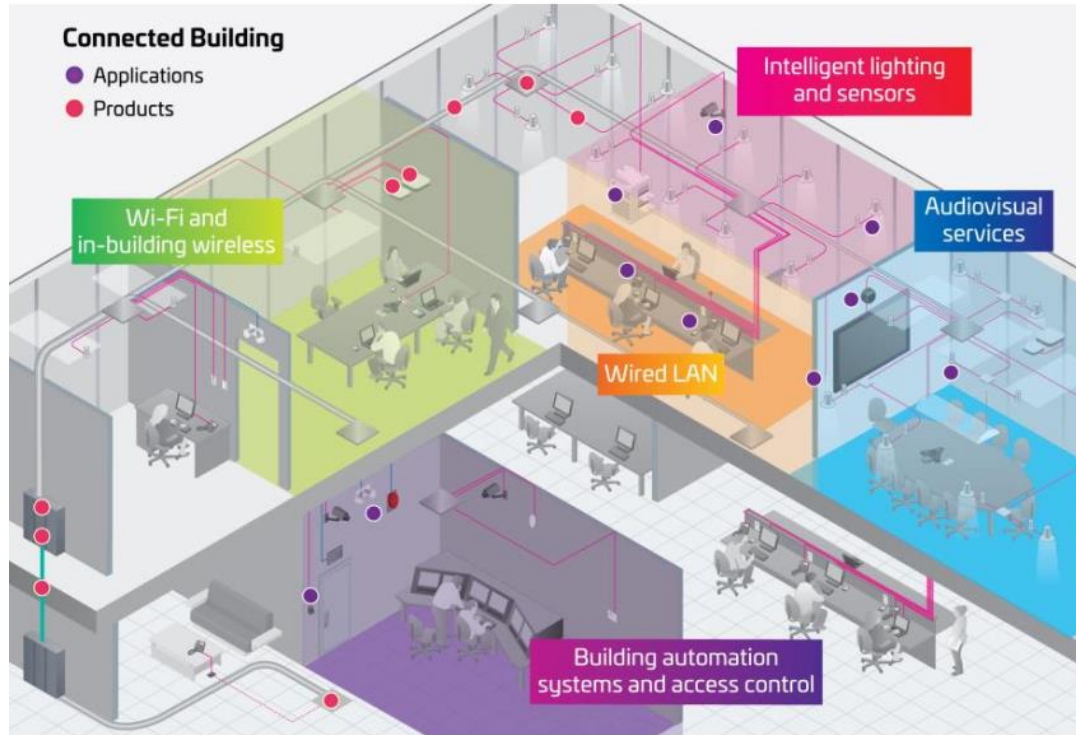
- Príklad aplikácie modelu pri návrhu campus infraštruktúry
- Predpokladajme tri budovy potrebné „zosieťovať“
  - Každá budova bude mať svoju:
    - **Prístupovú vrstvu:**
      - Počet prepínačov (portov) bude závisieť od počtu PC (a iných koncových zariadení) potrebných pripojiť do siete
    - **Distribučnú vrstvu**
      - Ideálne dva prepínače (redundancia)
      - Prepájajú prístupové prepínače
  - Toto sa nazýva aj ako „**switching block**“
- Budovy navzájom sa prepoja prepojením distribučných prepínačov na chrbticové prepínače
  - Pozn. Core zväžiť podľa situácie

- **Campus**

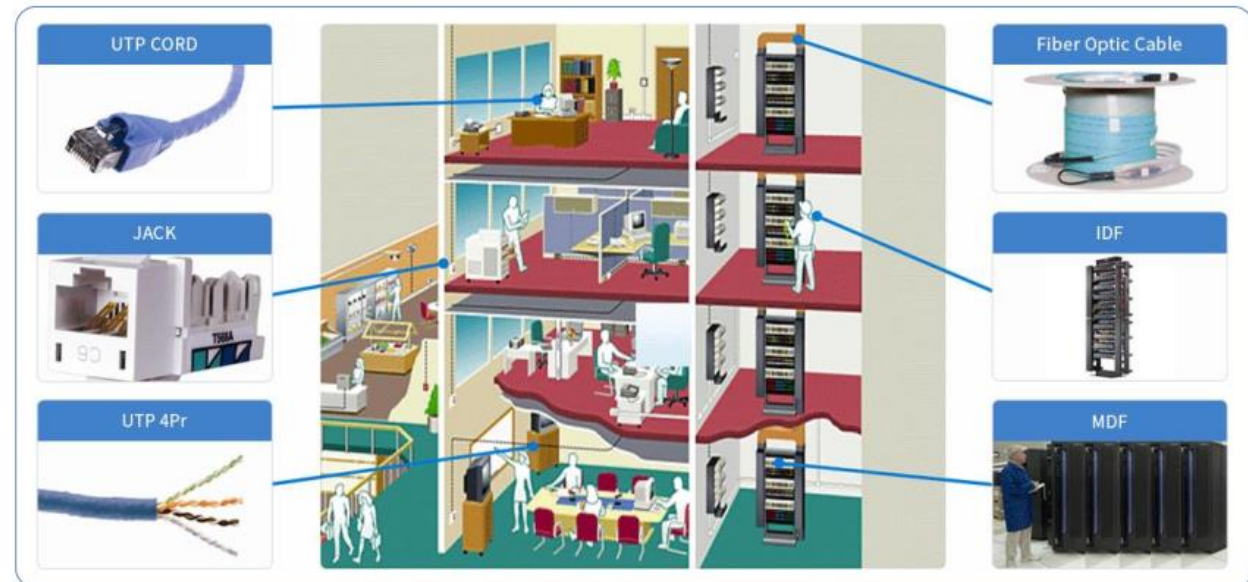
- *A group of one or more buildings, and surrounding grounds, where people and their belongings work together [webster]*



# Campus Networks



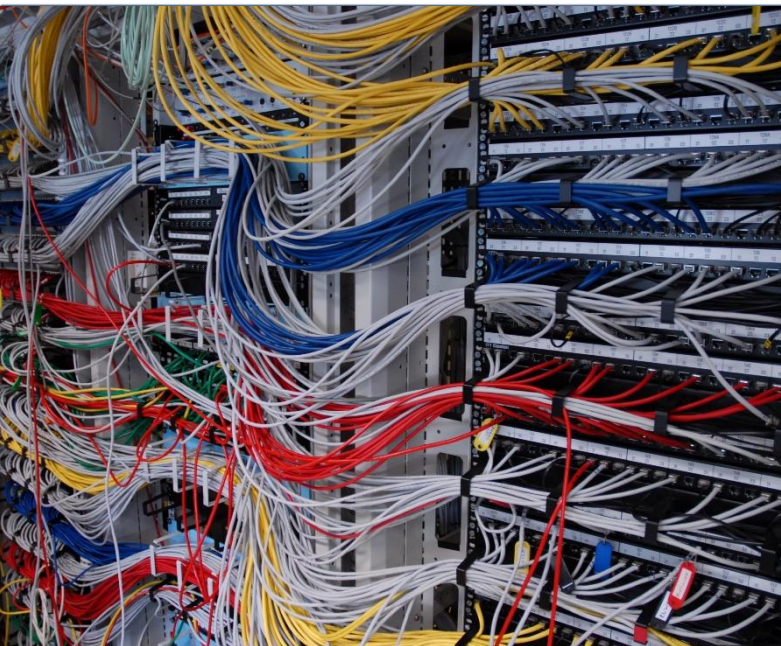
MDF = Main Distribution Framework (Core)  
IDF = Intermediate Distribution Framework (Distro/Access)



■ [www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html](http://www.cisco.com/c/en/us/solutions/design-zone/networking-design-guides/campus-wired-wireless.html)

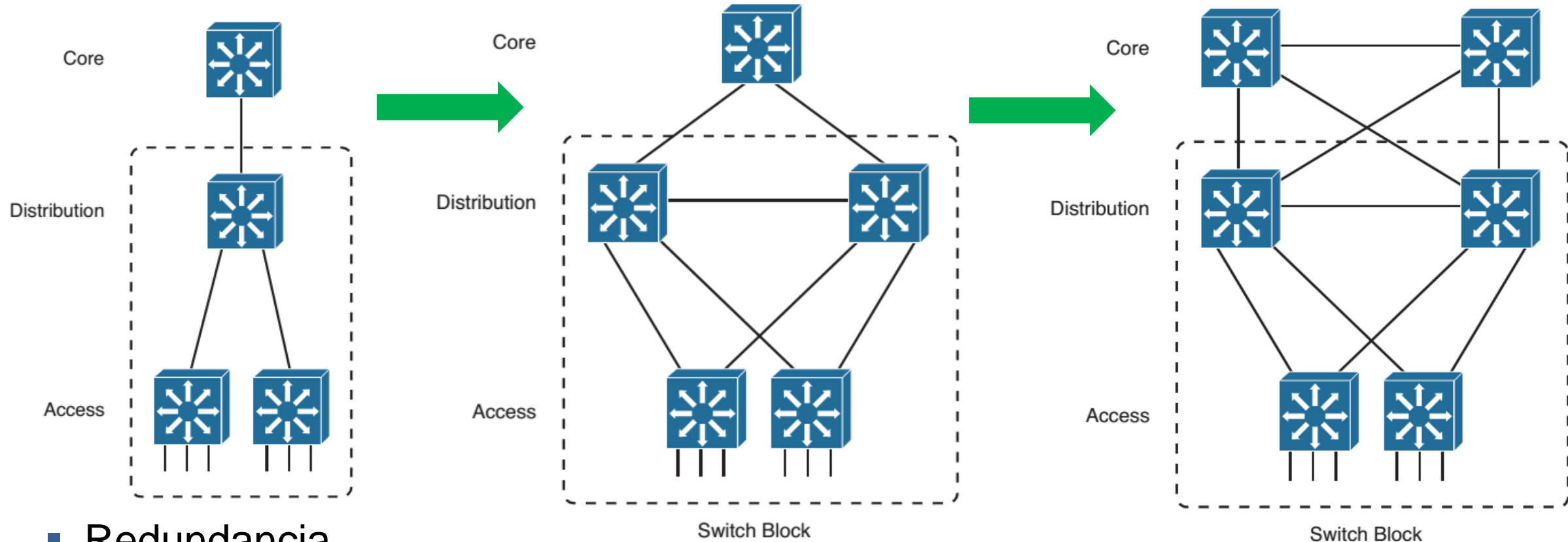
# Hierarchický model siete – hlavné prínosy

- Ohraničuje veľkosť chybových domén
  - Chybová doména = časť siete ovplyvnenej chybou
  - Lepšia odolnosť voči chybám a ich vplyvu na sieť
  - Lepší prehľad o funkčnosti a diagnostika siete
  - Zjednodušuje činnosť rôznych mechanizmov, ktoré pracujú v jednotlivých oblastiach sietí
    - HA, STP, Routing area, a pod
- Podporuje škálovateľnosť riešenia
  - Príprava na ľahšie rozširovanie a rast siete
  - Definuje efektívny adresný dizajn
    - Efektívne pridelovanie IP adries a ich sumarizácia
  - Sprehľadňuje toky dát
  - Jasne oddeľuje funkčné bloky pre L2 switching a L3 routing
  - Zjednodušuje činnosť rôznych mechanizmov, ktoré pracujú v jednotlivých oblastiach sietí – napr. optimalizácia smerovania



# Princípy hierarchického dizajnu

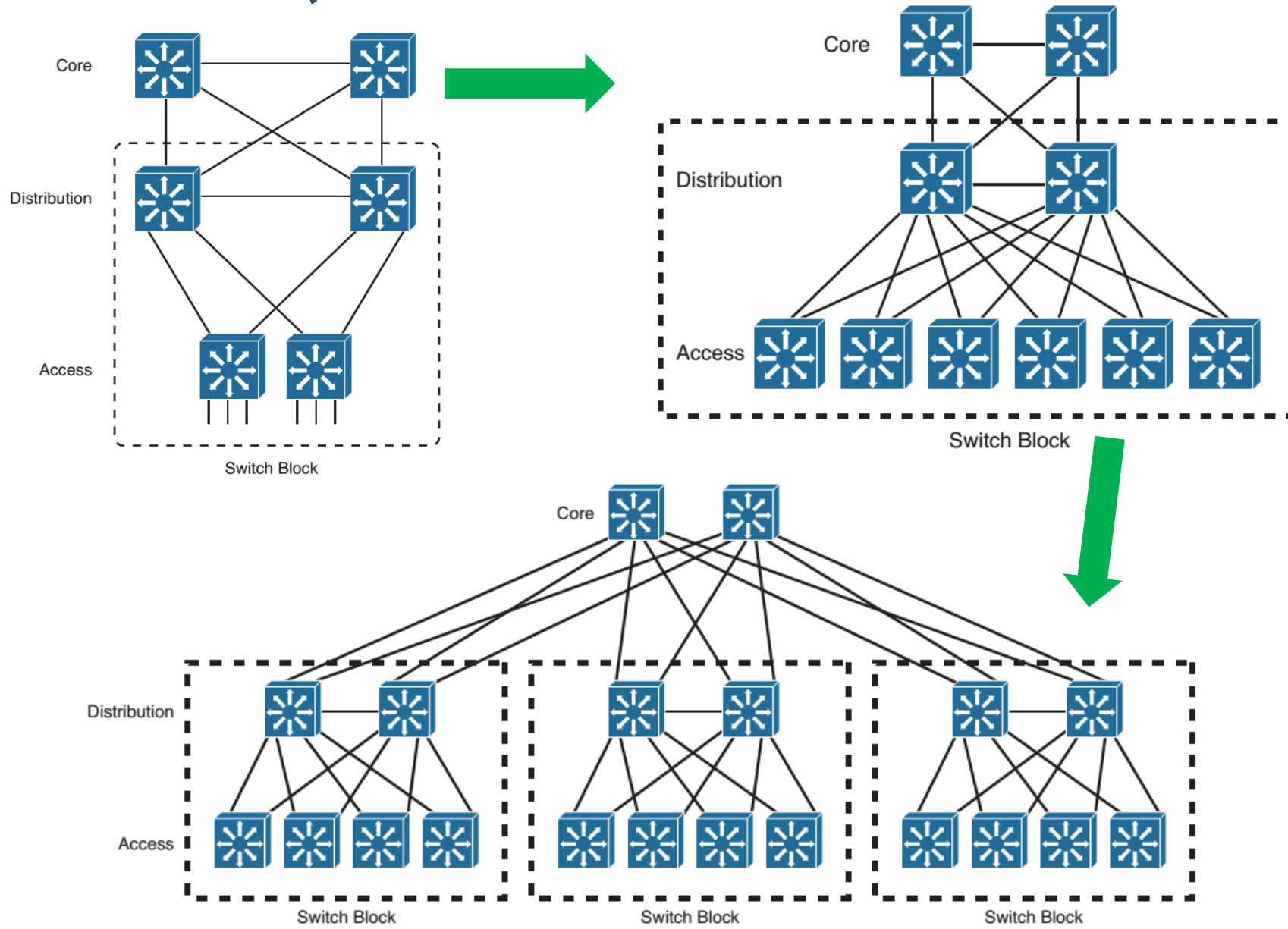
# Fyzická redundancia



- Redundancia

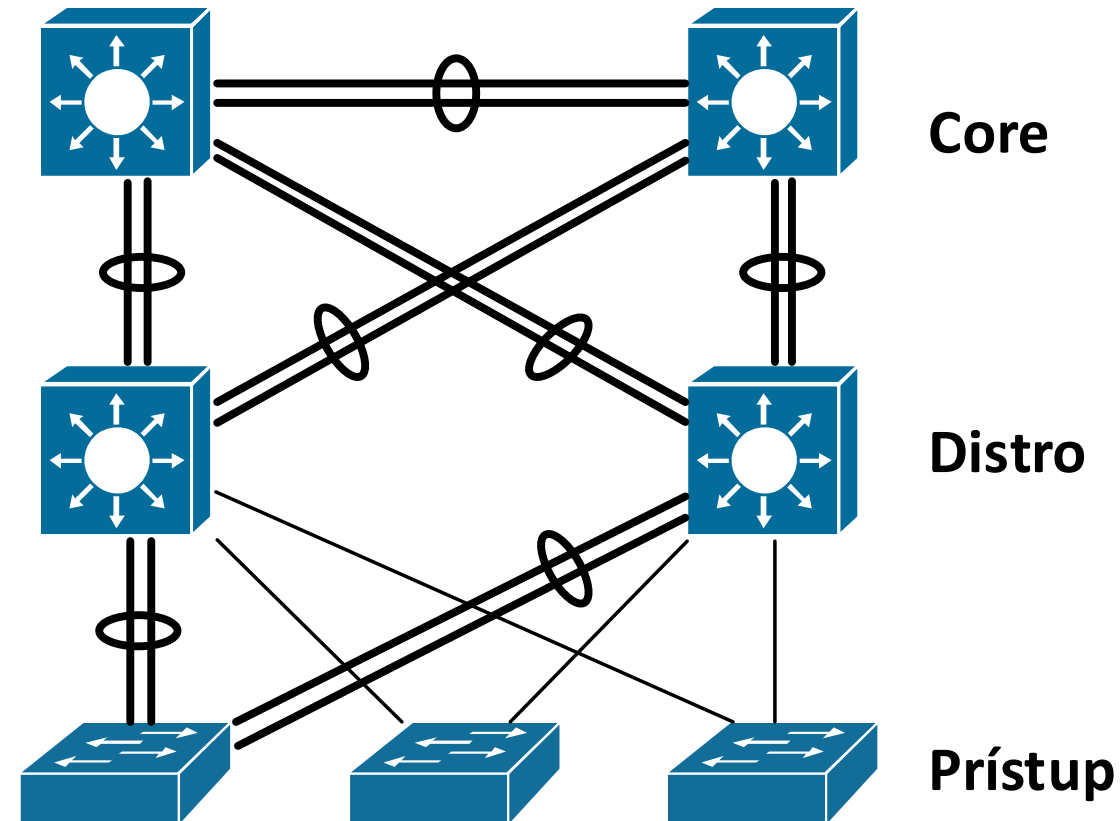
- Zvyšovanie spoľahlivosti a dostupnosti siete
- Zdvojovanie zariadení, modulov (kariet, napájania apod.), liniek

# Škálovateľnosť, udržovateľnosť



# Redundancia a výkonnosť (rozširovanie priepustnosti)

- Logická agregácia (spájanie) liniek
  - Umožňuje zvyšovanie priepustnosti a spoľahlivosti spojenia logickým spájaním fyzických liniek
    - Nie je treba meniť celý prepínač
    - Load balance nad fyzickými linkami
  - Zvyšuje stabilitu siete
    - Výpadok jednej linky nemá vplyv na konvergenciu prepínanej siete
  - Odporúčany pomer kapacity linky
    - Kapacita prepoja prístup. prepínača na distro 4:1 podľa súčtu kapacity liniek na prístupovom prepínači
    - Kapacita prepoja distro prepínača na Core prepínač 4:1
- Pozn.:
  - Cisco volá Etherchannel
  - iný napr. port/channel bonding

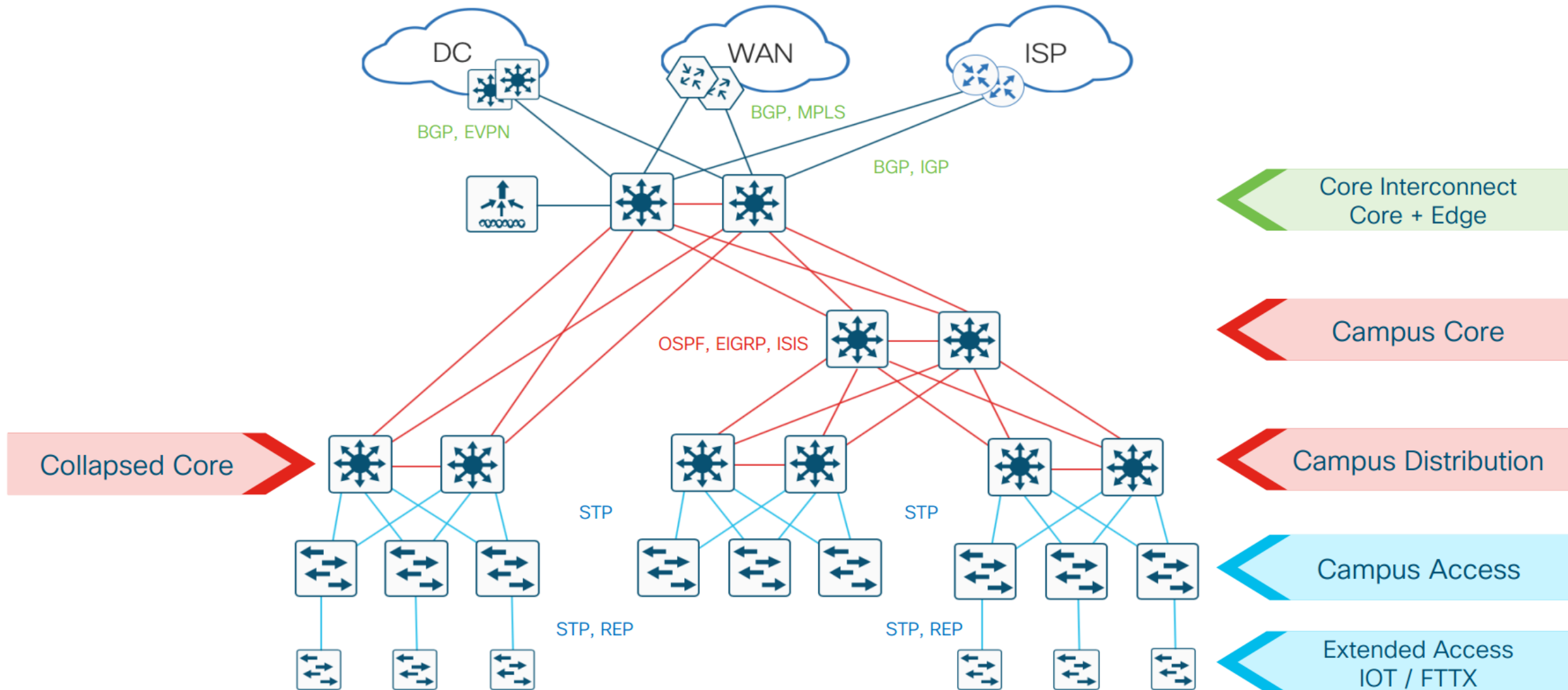


# Vlastnosti dobre navrhutej siete

- **Škálovateľnosť (Scalability)**
  - Ľahká a bezproblémová rozšíriteľnosť siete pri jej raste
- **Redundancia (Redundancy)**
  - Zabezpečenie vysokej dostupnosti (availability) a spoľahlivosti prenosovej cesty
- **Výkonnosť (Performance)**
  - Zohľadnenia prenosových nárokov používateľov a aplikácií
    - „Nech každý dostane to čo potrebuje“
  - Agregácia liniek a vysoko rýchlostné spracovávanie a prepínanie dát
- **Bezpečnosť (Security)**
  - Zabezpečenie siete na rôznych úrovniach
    - Bezpečnosť portov, prístupové pravidlá a pod.
- **Manažovateľnosť (Manageability)**
  - Zjednodušený manažment siete pri jasne definovaných pravidlách, dodržanie konzistentnosti konfiguračných politík naprieč sieťou
- **Udržovateľnosť (Maintainability)**
  - Modulárne siete s jasne definovanou funkcionalitou sa ľahko udržujú



# Trojvrstvý hierarchický model siete – veľké firmy

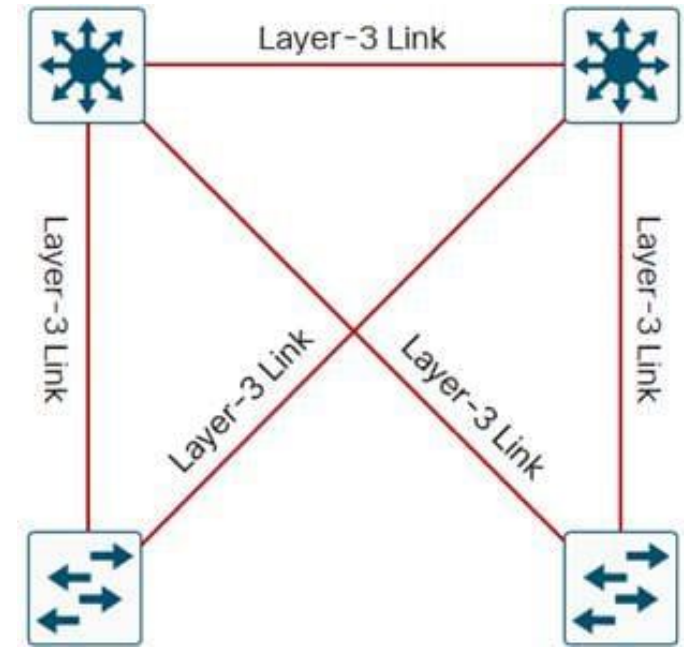
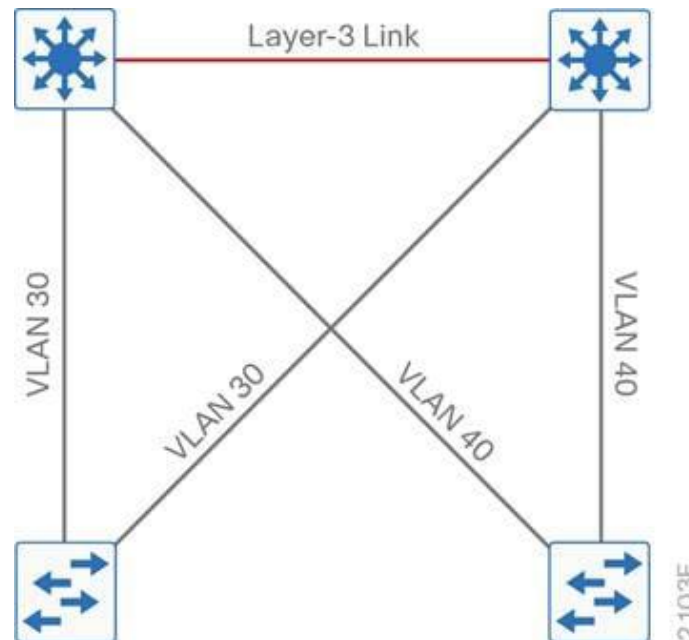
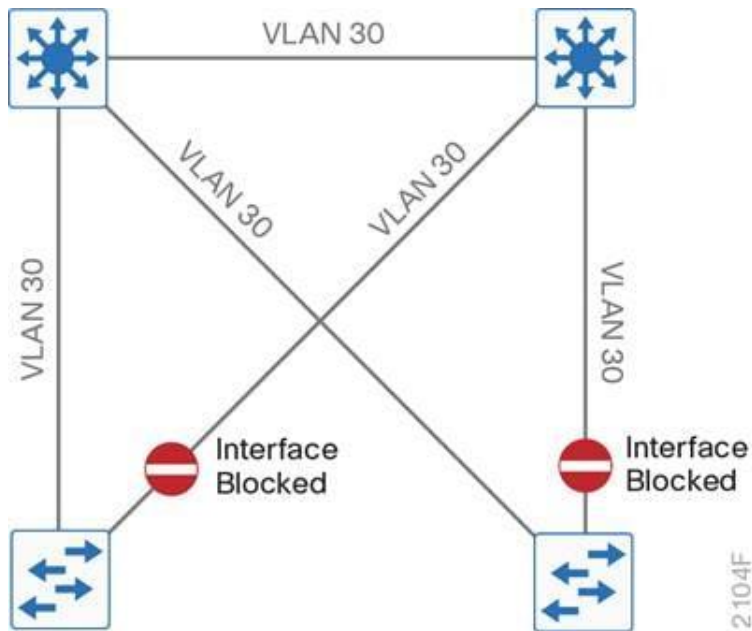


# Aktuálne prístupy podľa Cisco

- Pozn. *Treba si uvedomiť, že jeden prístup k dizajnu nemusí vyhovovať všetkým prípadom nasadenia*
- **Tradičný prístup Access - Dedicated Distribution and Access Layers (L2 or L3) (defacto hierarchický model)**
  - Pôvodný prístup, vhodný ak zariadenia na access potrebujú komunikovať s inými zariadeniami na access, pripojenými aj v iných fyzických „serverovniach“
  - Vyžaduje manuálne vyladenie viacerých protokolov na viacerých vrstvách
  - Najviac manuálnej konfigurácie, najviac náchylný na chyby
- **Zjednodušený prístup–Virtualized StackWise Access & StackWise Virtual Distribution**
  - Zjednodušená distro/core vrstva (stack)
  - Ľahšie nasadenia a diagnostika (troubleshooting)
- **Cisco Software Defined prístup – Campus Fabric and Automation of the Distribution & Access Layers**
  - Softvérovo riadený prístup a riadenie siete

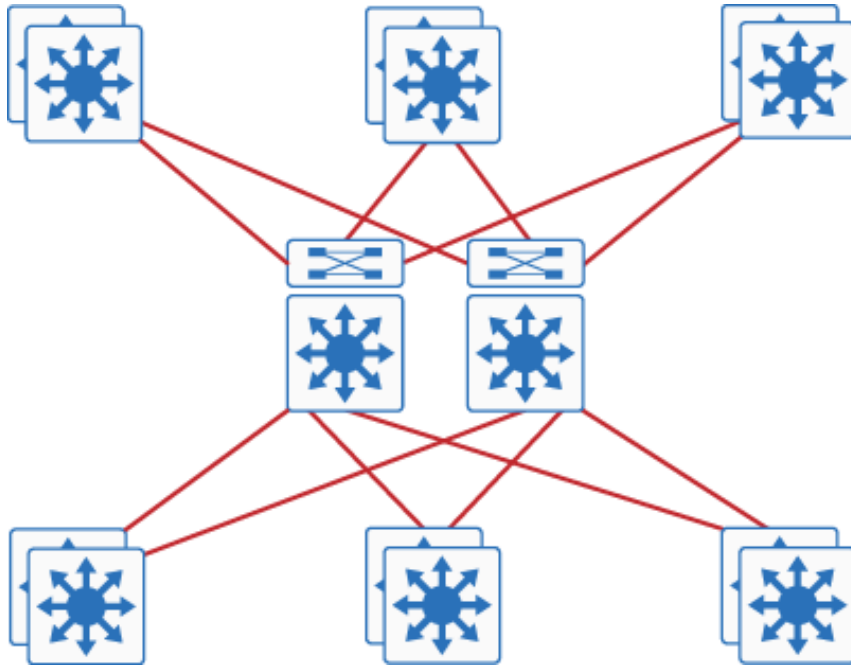
## Dizajnové prístupy na riešenie prepojenia access – distro vrstvy

- Tradičný prístup s riešením slučiek cez STP protokol
- Tradičný prístup s loop free riešenom L3 prepojom na distro
- Kompletne L3 routed prístup



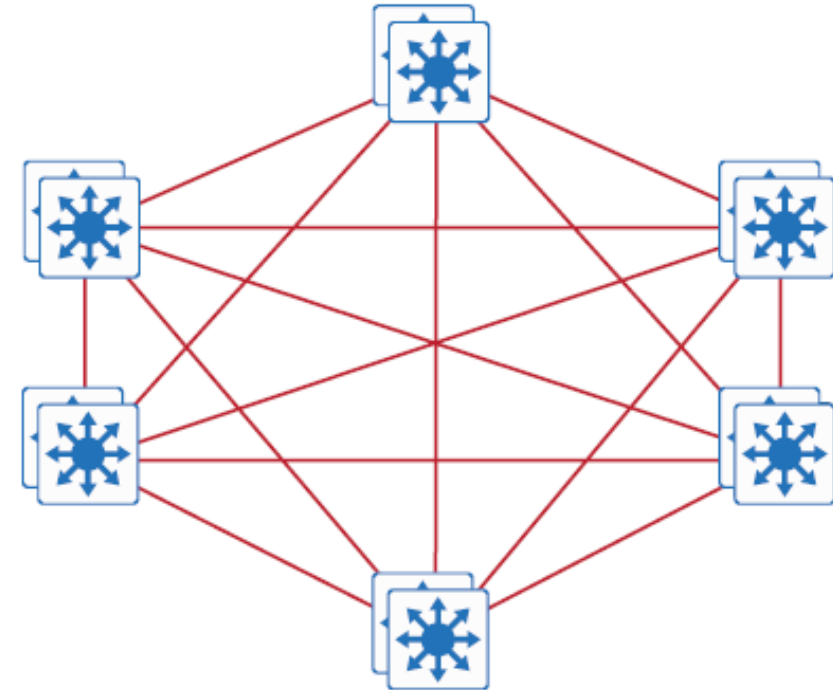
# Potreba core vrstvy

## Topo distro s core vrstvou



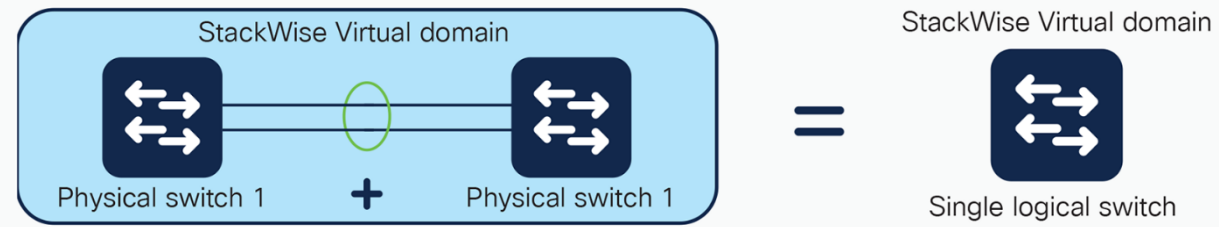
- Vhodné ak access je geo rozptýlený
- Ak sú špeciálne zóny
  - Ako WAN prístup
  - Redundantný firewall perimeter s DMZ
  - Wireless controller klastre
  - DC atď

## Topo bez core vrstvy

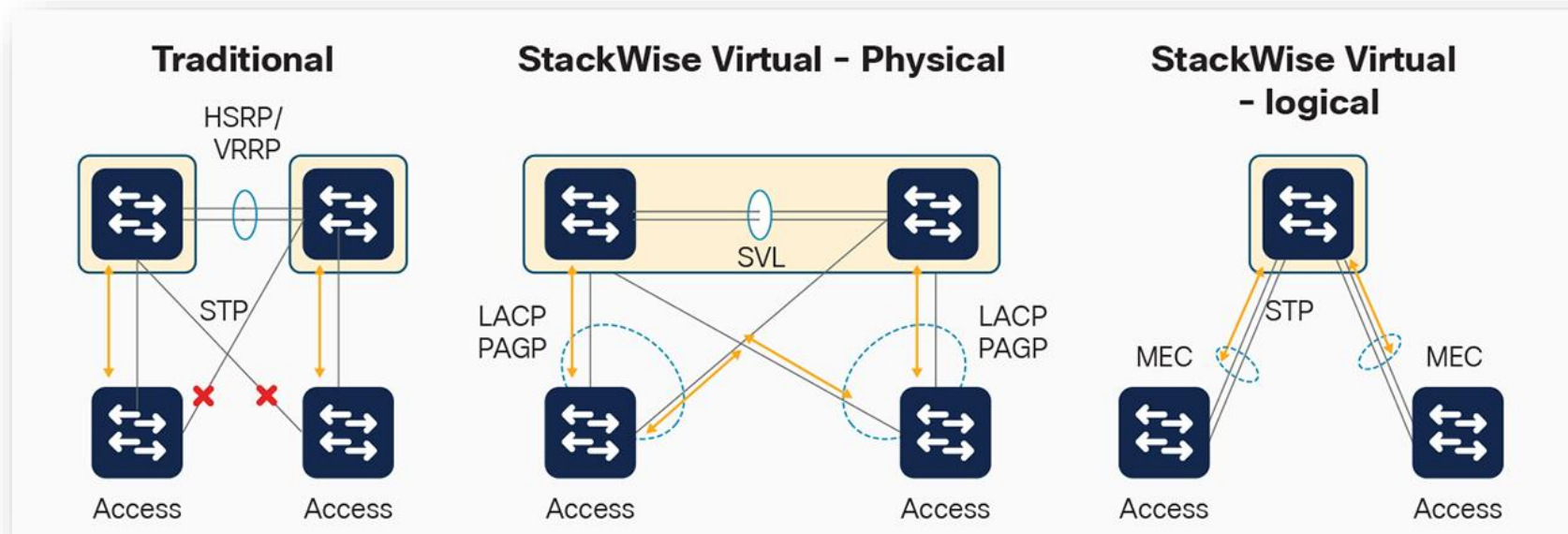


- Počtom distro prepínačov narastá zložitosť riešenia prepojenia
  - A nárast súvisiacich problémov

# StackWise prístup

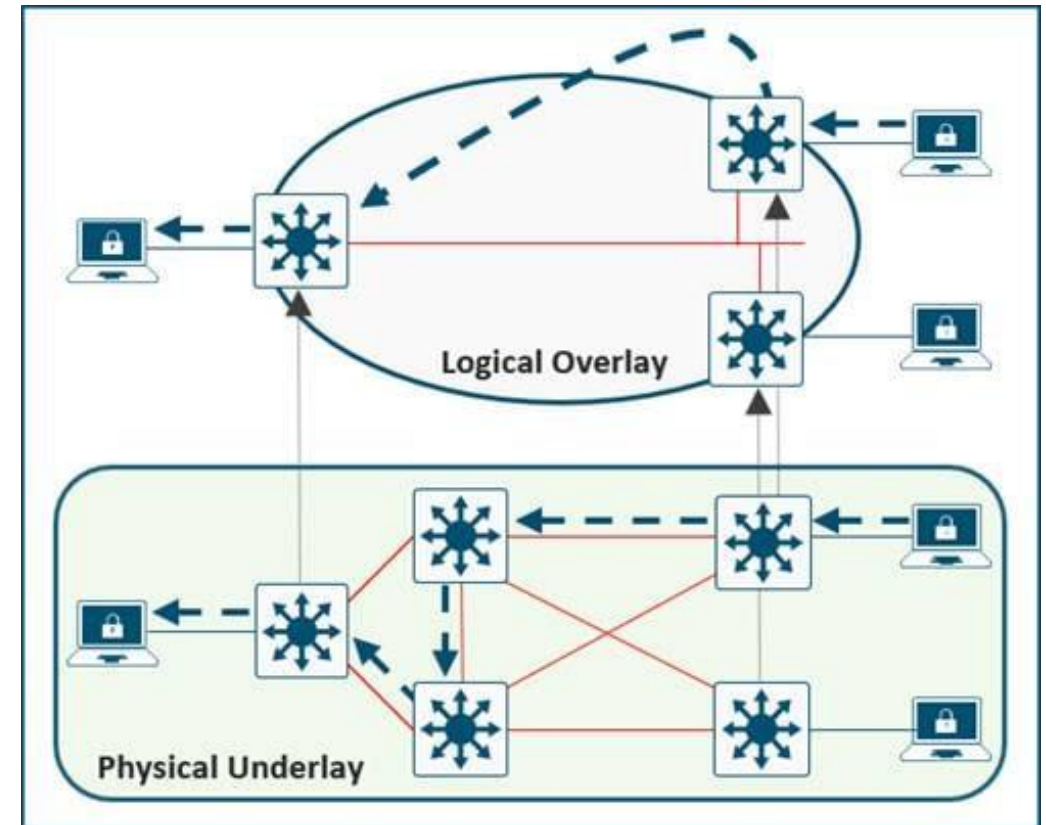


- Cisco StackWise Virtual Pair (SVP)
  - Viaceré fyzické prepínače sa javia a konfigurujú ako jeden
  - Stackwise je dátový aj napájací
  - Dopad na dizajn:



# Prístup Cisco Software-Defined-Access

- Cisco Software-Defined Access (SD-Access)
  - Evolúcia od tradičného hierarchického modelu
  - Oddeľuje forwarding funkcie od riadenia siete
- Využíva viaceré roviny (Planes)
  - Control Plane – LISP => ID a komunikácia medzi zariadeniami
  - Data Plane – VXLAN tunneling
  - Policy Plane – Cisco TrustSec => bezpečnosť a segmentácia
  - Management Plane – Cisco DNA Center => orchestrácia
- SD-Access
  - Nasadený a automatizovaný cez Cisco DNA Center => GUI
  - Vyžaduje vhodné zariadenia s podporou SD
  - Prístup vytvára
    - Fyzickú L2/L3 underlay infraštruktúru, tzv. Fabric infra
    - Logickú L2 overlay infraštruktúru, virtuálnu

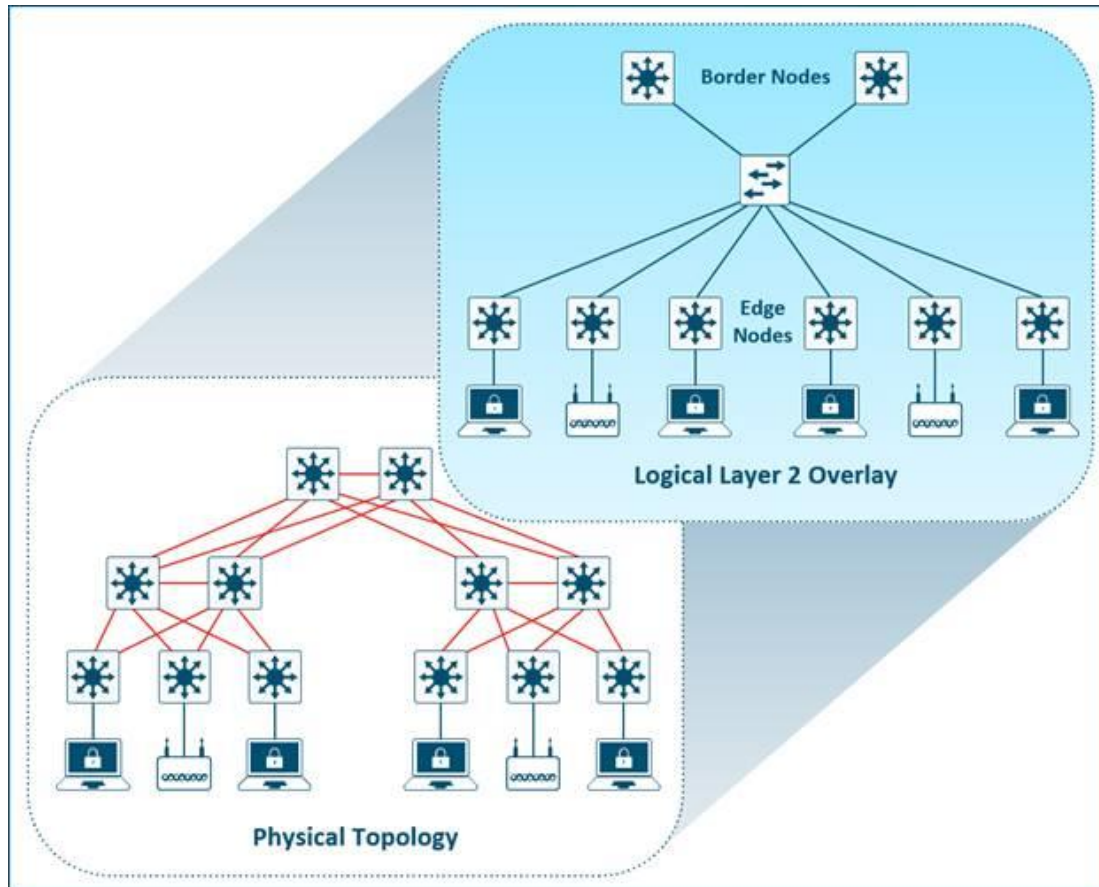


Viac na:

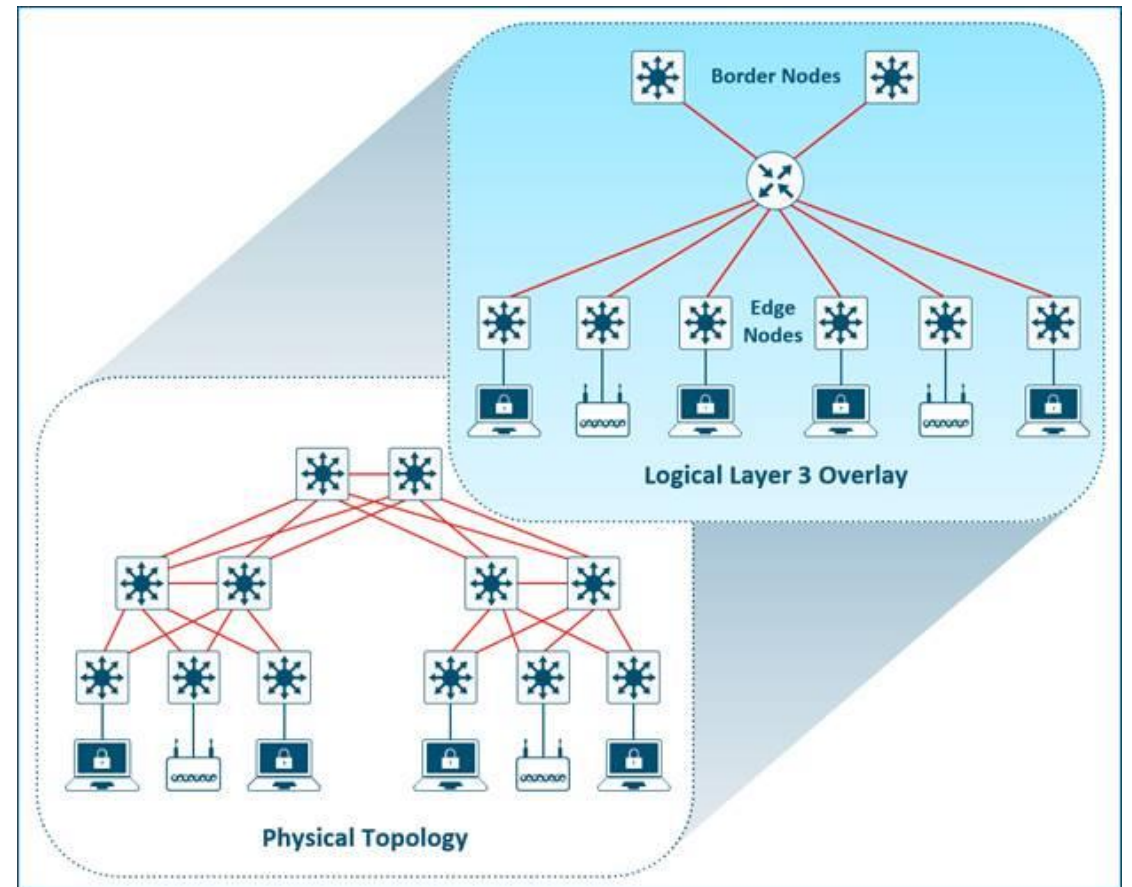
<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

# Prístup Cisco Software-Defined-Access

## Overlay: L2 over SD-A

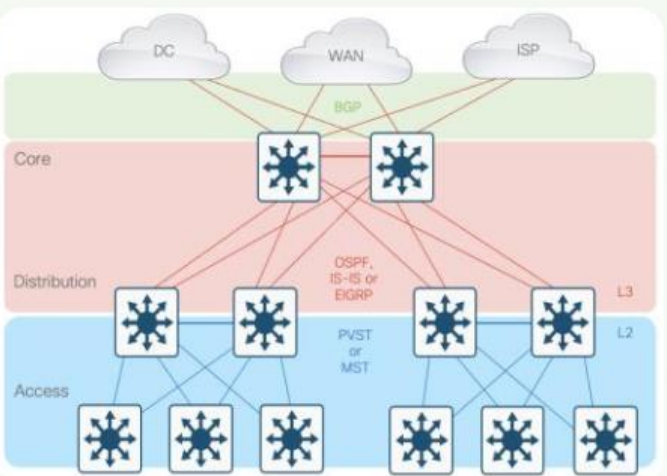


## Overlay: L3 over SD-A



# Redundancia control a data plane

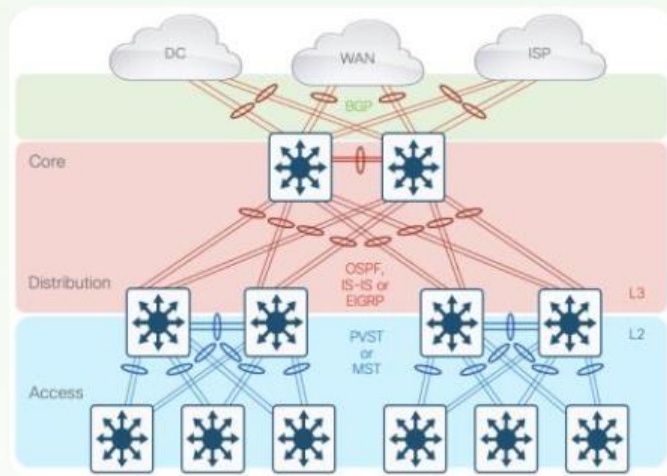
## 1 ECMP (L2/L3 Paths)



- Complex Topology
- **More Nodes, Fewer Cables**
- **More Neighbors (+ Tuning)**
- **Protocol Load-Balancing (ECMP)**
- Node-level Redundancy

L1 : Single Connections  
 L2: STP, MST, REP + ECMP (Port Cost)  
 L3: FHRP, IGP, BGP + ECMP (Port Cost)  
**More Neighbors** = Requires Protocol Tuning

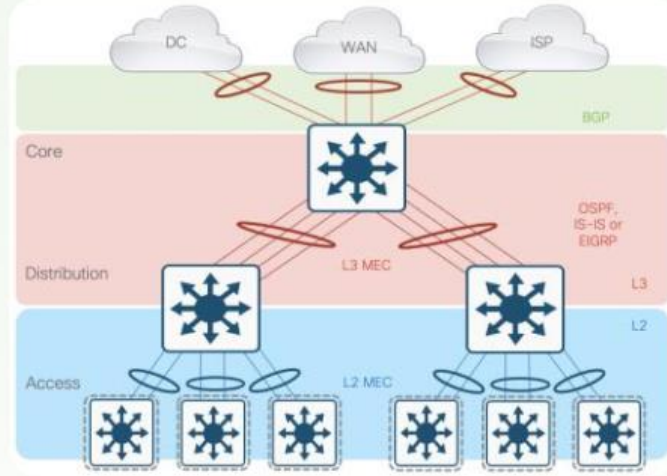
## 2 EtherChannel (L2/L3 LAG)



- Complex Topology
- **Same Nodes, More Cables (2-8)**
- **Same Neighbors (+ Tuning)**
- **EtherChannel Load-Balancing**
- Node and Link-level Redundancy

L1 : Multiple Connections  
 L2: STP, MST, REP + ECMP (Portchannel Cost)  
 L3: FHRP, IGP, BGP + ECMP (Portchannel Cost)  
**More Neighbors** = Requires Protocol Tuning

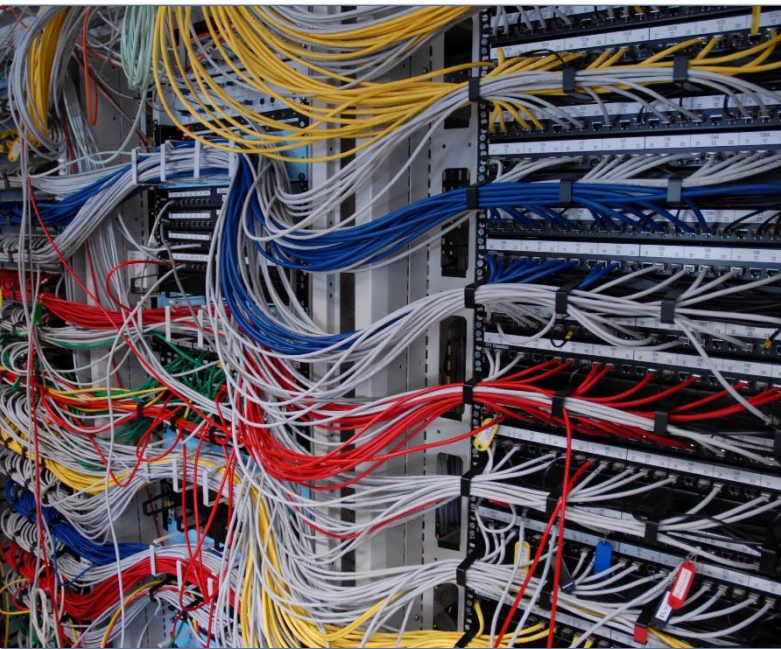
## 3 StackWise (L2/L3 MEC)



- Simple Topology
- **Same Cables, Fewer Nodes**
- **Less Neighbors (No Tuning)**
- **Multi-chassis EtherChannel (MEC)**
- Layer-level Redundancy

L1 : Multiple Connections  
 L2: L2 MEC (No STP or REP)  
 L3: IGP, BGP + L3 MEC (No FHRP)  
**Fewer Neighbors** = No Protocol Tuning





# Zariadenia v podnikových sieťach

# Zariadenia v podnikových sieťach

- Je kľúčové pre biznis zabezpečiť činnosť siete a jej aplikácií a služieb
- Kritický je výber správnych zariadení =>
  - Podnikové siete využívajú zariadenia triedy „**enterprise**“
    - Výkon, prevádzka 24/7, správa, a pod.
    - SOHO segment zariadení nie je preto pre nasadenie v podnikoch vhodný

# Predpoklad pre výber zariadení

- Kritické pre výber zariadení = **Poznaj sieť**
- Analýza súčasných **dátových tokov**
  - Poznanie siete, odhad potrieb, rastu, úzkych miest
    - Počítaj s budúcim rastom
  - Pri prepínači zväž:
    - Výkonnosť zariadenia a jeho miesto nasadenia (access, core, ...)
    - Rozhrania: typ, technológia, priepustnosť
- Analýza **používateľov**, ich **komunit** a **služieb**
  - Tvorba subsietí, zgrupovanie (agregácia)
    - Napr. oddelenia vo firme, prac. skupiny a pod.
  - Pri prepínači zväž:
    - Plánovanie počtu a rozmiestnenia portov
    - Odhad požadovanej priepustnosti
    - Počítaj s budúcim rastom
- Analýza umiestnenia serverov, dátových úložísk
  - Analýza tokov klient server, server-server
  - Zväž ich umiestnenie a dopad na sieť, úzke miesta apod.
  - Pri prepínači zväž:
    - diameter, priepustnosť

# Zariadenia v podnikových sieťach

- **Funkčnosť 24/7**
- Prepínače
  - Dominantné v Campus sieťach
  - Typicky jedna technológia = Ethernet
- Smerovače
  - Redundantné prepájanie viacerých častí cez heterogénnu smerovanú infraštruktúru (na internet ISP, WAN)
    - Rôzne linky a protokoly
- Iné (z pohľadu kurzu R&S mimo)
  - Firewall, Intrusion Detection/prevention zariadenia, load balancers, WAN a VPN koncentrátoři, Bezpečnostné zariadenia (Web a email ochrana), cloud, sieťová virtualizácia (NFV Network Function Virtualization)

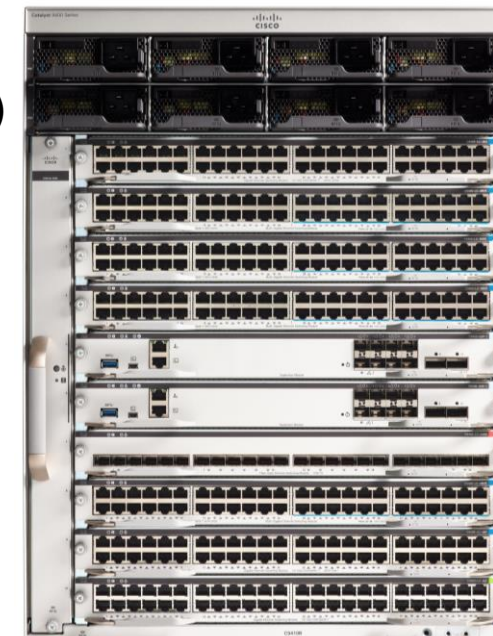
# Prepínače

- Faktory, ktoré treba brať do úvahy:
  - **Veľkosť** (Form factor )
    - výška x šírka x hĺbka (udávané v tzv. „U“)
  - **Hw. konfigurácia**
    - **Fixná konfigurácia**
      - Fixný počet portov na šasi
    - **Modulárna konfigurácia**
      - Zásuvné linkové karty – možnosť osadiť čím je potrebné
      - Riešenia napájania
  - **Stohovateľné (Stackable)**
    - Špeciálne prepojenie viac prepínačov, ktoré sa potom javia a konfigurujú ako jeden
    - Môžu si zdieľať zdroje, ako napr. napájanie
  - **Prenosová kapacita (Forwarding rate)**
    - Výkonnosť zariadenia v bps (bit per second) resp. pps (packet per second)
    - Smerom od prístupových ku chrbticovým zariadeniam výkon rastie
  - **Rýchlosť a typ portov**
    - 100 Mbps, 1 Gbps, 10 Gbps, or 100 Gbps

1 rack unit (1U)



9 rack unit (9U)



## Prepínače (2)

- **Hustota portov** (Port density)
  - Počet portov/rozhraní na zariadenie
  - Fixné riešenia majú do 48portov
  - Modulárne riešenia desiatky až stovky portov
- Redundancia napájania
- Funkcie, ako napr.
  - **Združovanie liniek** (Link aggregation)
    - Možnosť kombinovať viaceré porty do jedného logického prepoja
  - **Power over Ethernet** (PoE)
    - Napájaie zariadení ako IP telefóny, AP, kamery po LAN kabeláži
    - Zvyšuje cenu zariadení
  - **Schopnosti „multilayer“ prepínania/smerovania**
    - Schopnosť prepínača pracovať ako smerovač, prípadne load balancer
    - Prístupové prepínače typicky vykonávajú L2 prepínanie
    - Distro/core prepínače typicky vykonávajú L3 prepínanie (hw. smerovanie)
- Licencie ☹
- **Cena !!!!!!!!!!!!!!!**
  - Odvíja sa od výkonu zariadenia
  - Smerom od prístupových ku chrbticovým zariadeniam cena rastie



Fixné prevedenie,  
24 - portov



Fixné prevedenie,  
48 - portov



Modulárne prevedenie,  
vysoká hustota portov

# Summary - Switch Hardware

## Business Considerations for Switch Selection

Consideration	Description
<b>Cost</b>	The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
<b>Port density</b>	Network switches must support the appropriate number of devices on the network.
<b>Power</b>	It is now common to power access points, IP phones, and compact switches user Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
<b>Reliability</b>	The switch should provide continuous access to the network.
<b>Port speed</b>	The speed of the network connection is of primary concern to end users.
<b>Frame buffers</b>	The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
<b>Scalability</b>	The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

# Copper vs. Fiber

## Category 5, 6 and 7

Unshielded (UTP)

Shielded (STP)

### RJ45 (Access to Endpoints)



Cat6A  
(Offset Wires)

Cat5E  
(Flush Wires)



Category	Frequency	Distance	Data Rate	Shielding
5E	100-350 MHz	100m	1000 Mbps	UTP or STP
6	250-550 MHz	1G - 100m 10G - 50m	1 Gbps 10 Gbps	UTP or STP
6A	500-550 MHz	100m	10 Gbps	UTP or STP
7	600 MHz	100m	10 Gbps	Shielded only



## OM3, OM4 and OM5

Multi-Mode (MMF)

Single-Mode (SMF)

Wave-Division Multiplex (WDM)

### SFP (Access and Distribution)

### QSFP (Core and Edge)



SFP-LC  
LC Duplex

mSFP  
Mini LC Duplex



SMF



MMF

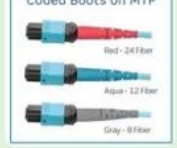


MPO12  
12 Fibers

MPO24  
24 Fibers



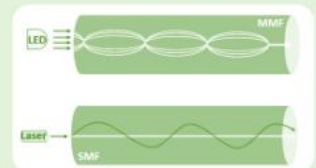
Single-Mode Color Coded Boots on MTP  
Red - 24 Fiber  
Black - 12 Fiber  
Gray - 8 Fiber



Multimode Color Coded Boots on MTP  
Red - 24 Fiber  
Aqua - 12 Fiber  
Gray - 8 Fiber

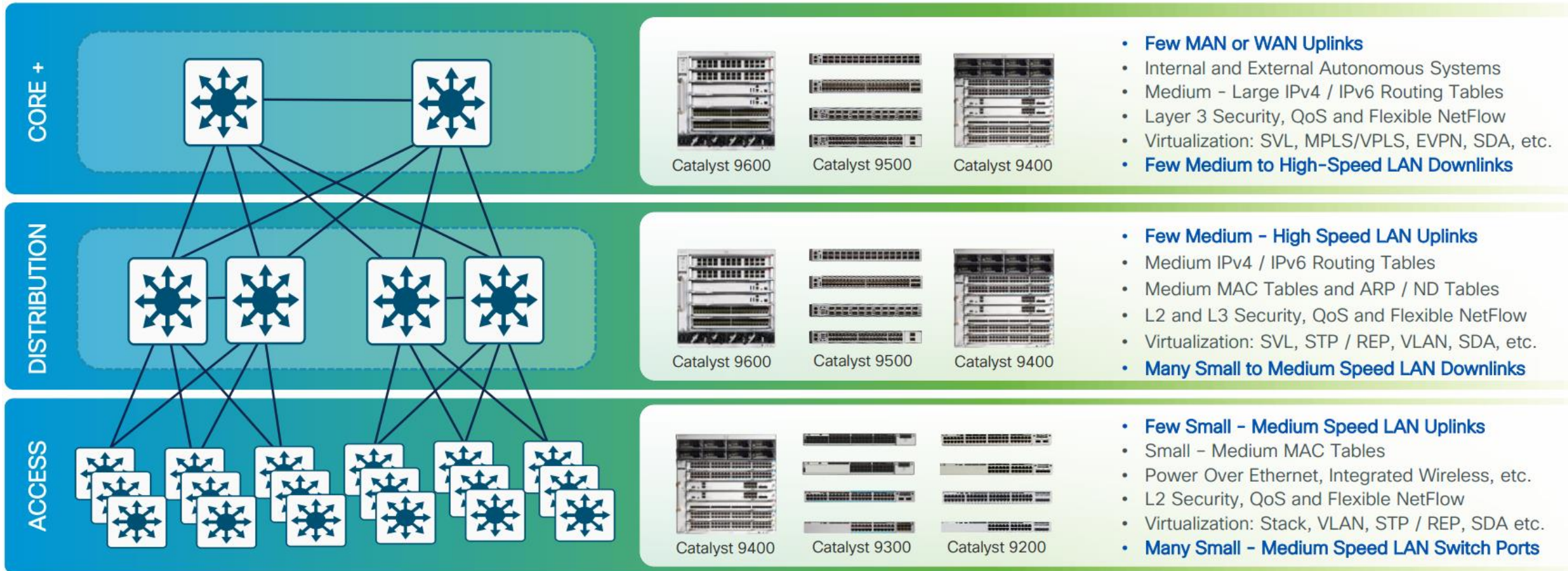
- Multimode**
- Short distance cable runs (less than 1000ft.)
  - High bandwidth support
  - Higher cable cost
  - Lower electronics cost
  - Easier to terminate due to larger core size

- Single Mode**
- Long distance cable runs (greater than 1000ft.)
  - Highest bandwidth support
  - Lower cable cost
  - Higher electronics cost
  - Harder to terminate due to smaller core size





# Campus Multi-Layer Model



# L2/L3 technológia

## IPv4 Unicast

- MP-BGP, VPNv4
- Internet (v4), NAT, PBR
- MPLS-VPN, VRF-Lite
- IPv4 SSO, NSF/NSR, GIR

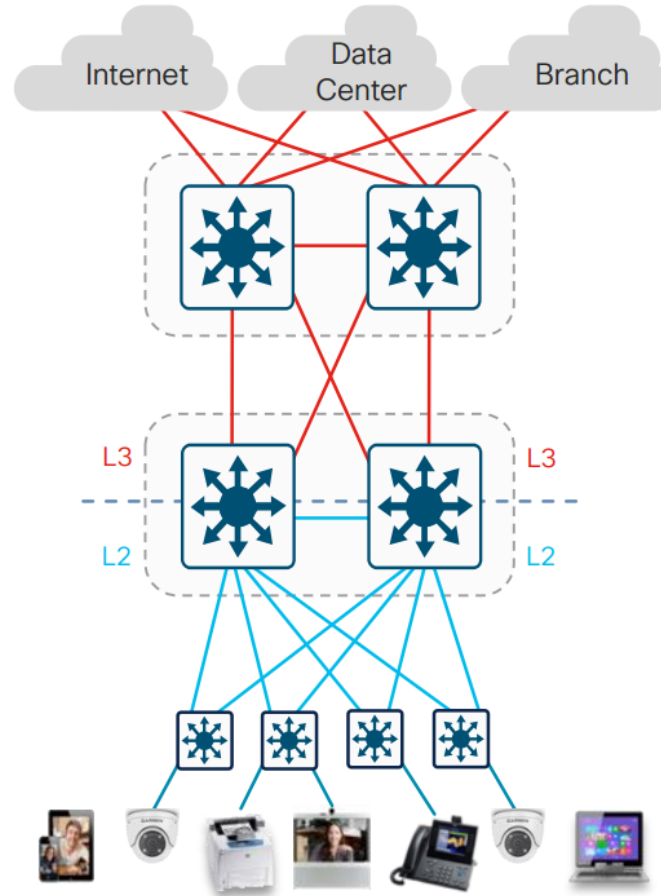
Core

- EIGRP, OSPFv2, ISIS, RIP
- SVI, HSRP/VRRP
- ARP, DHCP Relay
- IPDT/SISF, DAI
- BFD, Echo
- IPv4 SSO, NSF/NSR, GIR

Distribution

- PVST, MST, REP/RENN
- 802.1Q, DTP
- VLANs, VTP
- DHCP Snooping
- MAC Leaning
- L2 SSO

Access



## IPv6 Unicast

- MP-BGP, VPNv6
- Internet2 (v6), NAT64, PBR
- MPLS-VPN, VRF-Lite
- IPv6 SSO, NSF/NSR, GIR

Core

- EIGRPv6, OSPFv3, ISISv6, RIPng
- SVI, HSRPv6/VRRPv6
- NDP, DHCPv6 Relay
- SISF (v4/v6), RA Guard
- BFDv6, Echo
- IPv6 SSO, NSF/NSR, GIR

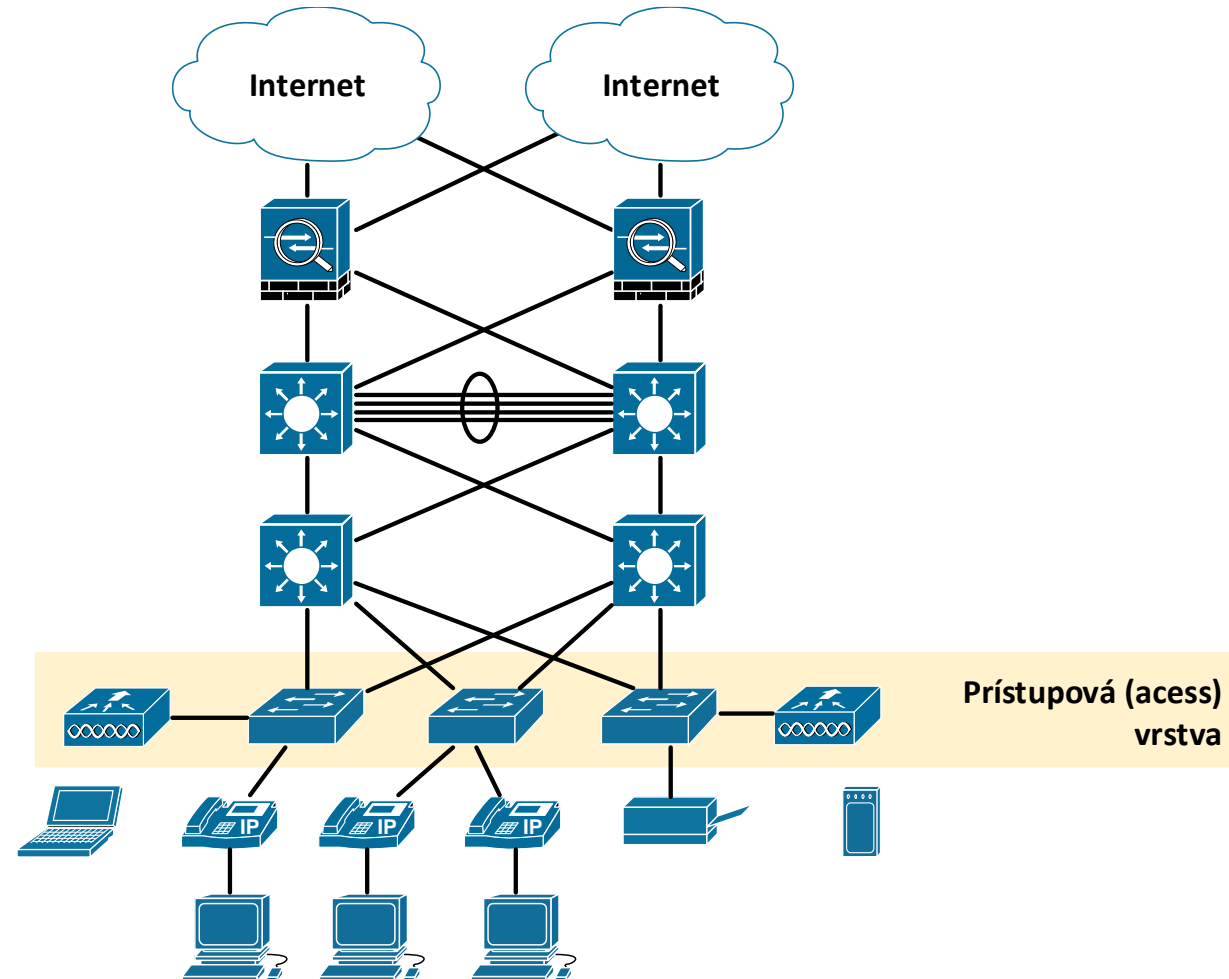
Distribution

- PVST, MST, REP/RENN
- 802.1Q, DTP
- VLANs, VTP
- DHCPv6 Snooping
- MAC Leaning
- L2 SSO

Access

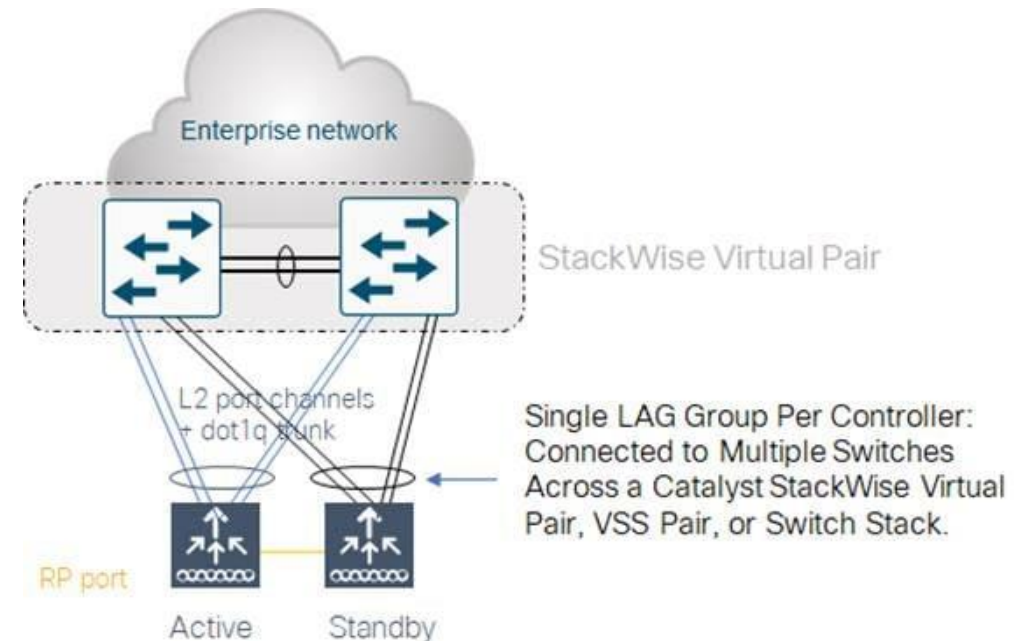
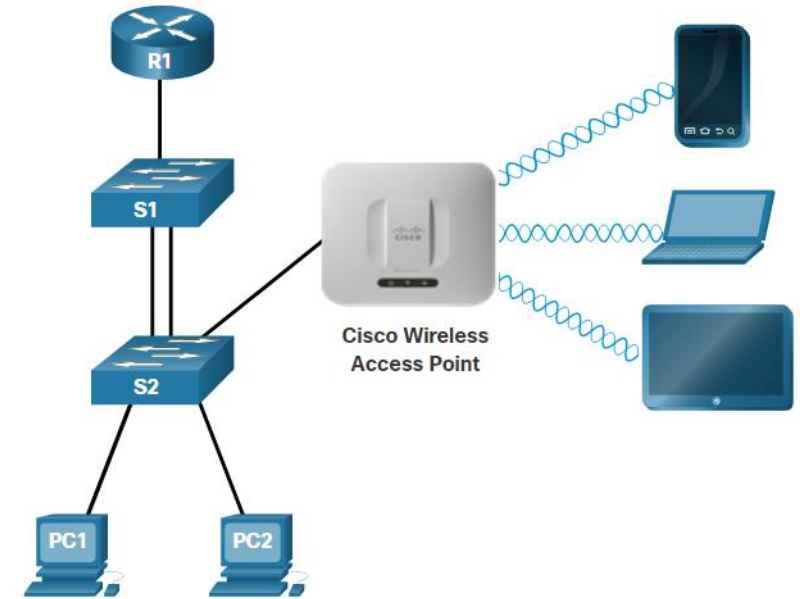
# Vlastnosti prepínačov – prístupová vrstva

- Technológie, využívané na jednotlivých vrstvách
  - Zvážiť pri výbere zariadenia, ak je daná funkčnosť požadovaná
- **Prístupová (access) vrstva**
  - L2 prepínanie (v novších návrhoch L3 prepínanie, tzv. *Smeruj kde sa dá*)
  - Bezpečnosť
    - Port security (Rozhoduje kto sa môže pripojiť)
    - DHCP snooping, ARP inšpekcia, IP inšpekcia
    - ...
  - Vysoká dostupnosť a odolnosť (availability and resiliency)
  - Rapid STP protokol
  - VLANs a trunky
  - Rýchlosť (bežný Gigabit)
  - Power over Ethernet (PoE) (napájanie AP, telefónov a podobne)
  - Agregácia liniek
  - Quality of service (QoS)
  - ACL zoznamy (VLAN ACL, smerované ACL)



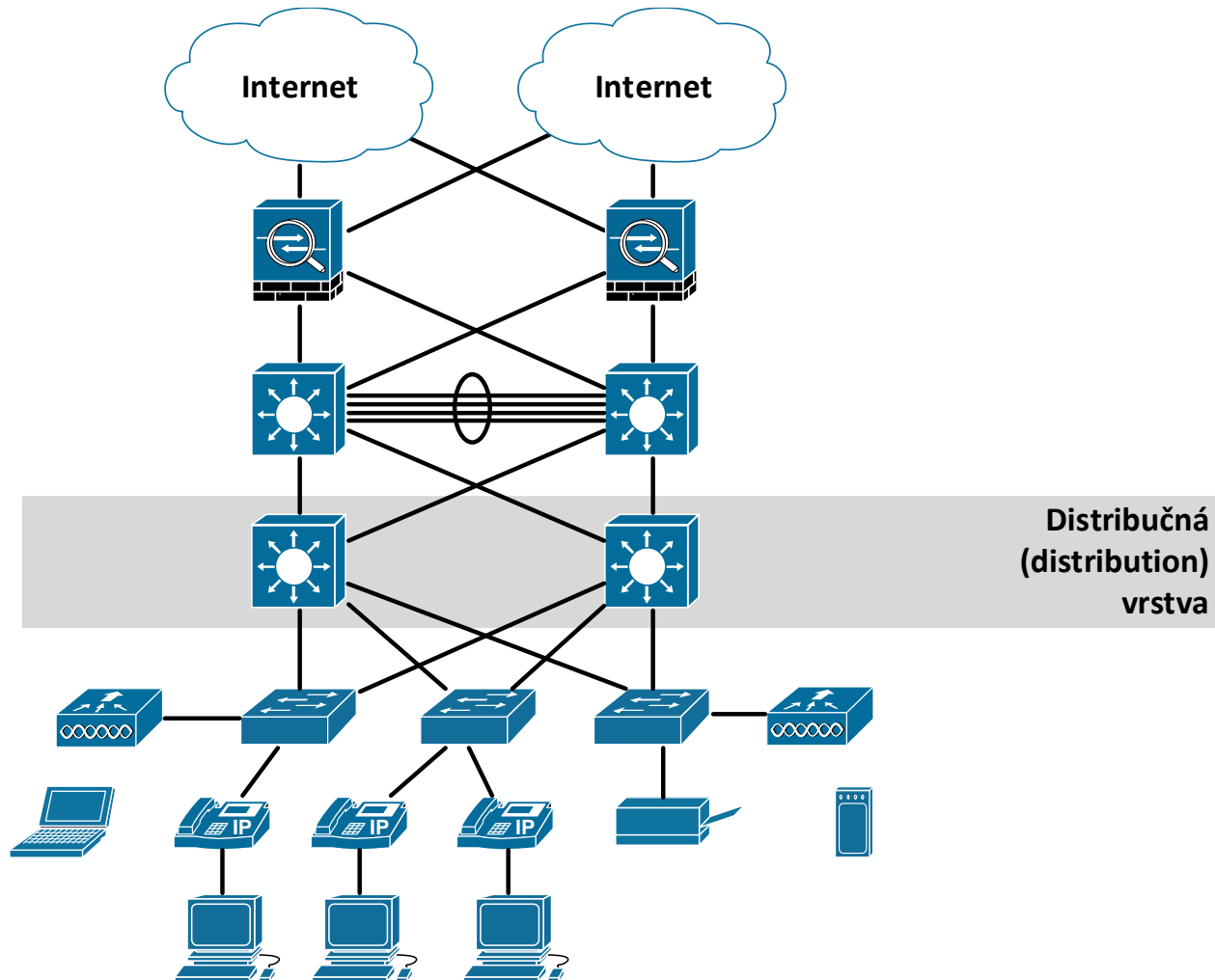
# Rozširovanie access vrstvy

- WiFi
  - V súčasnosti nevyhnutnosť
  - Autonómne AP
    - pripájame na prepínače v Access vrstve
- WiFi Kontrolér riešenia
  - Kontroller – WiFi access switch pripájajúci sa do distra
  - APčka – access layer



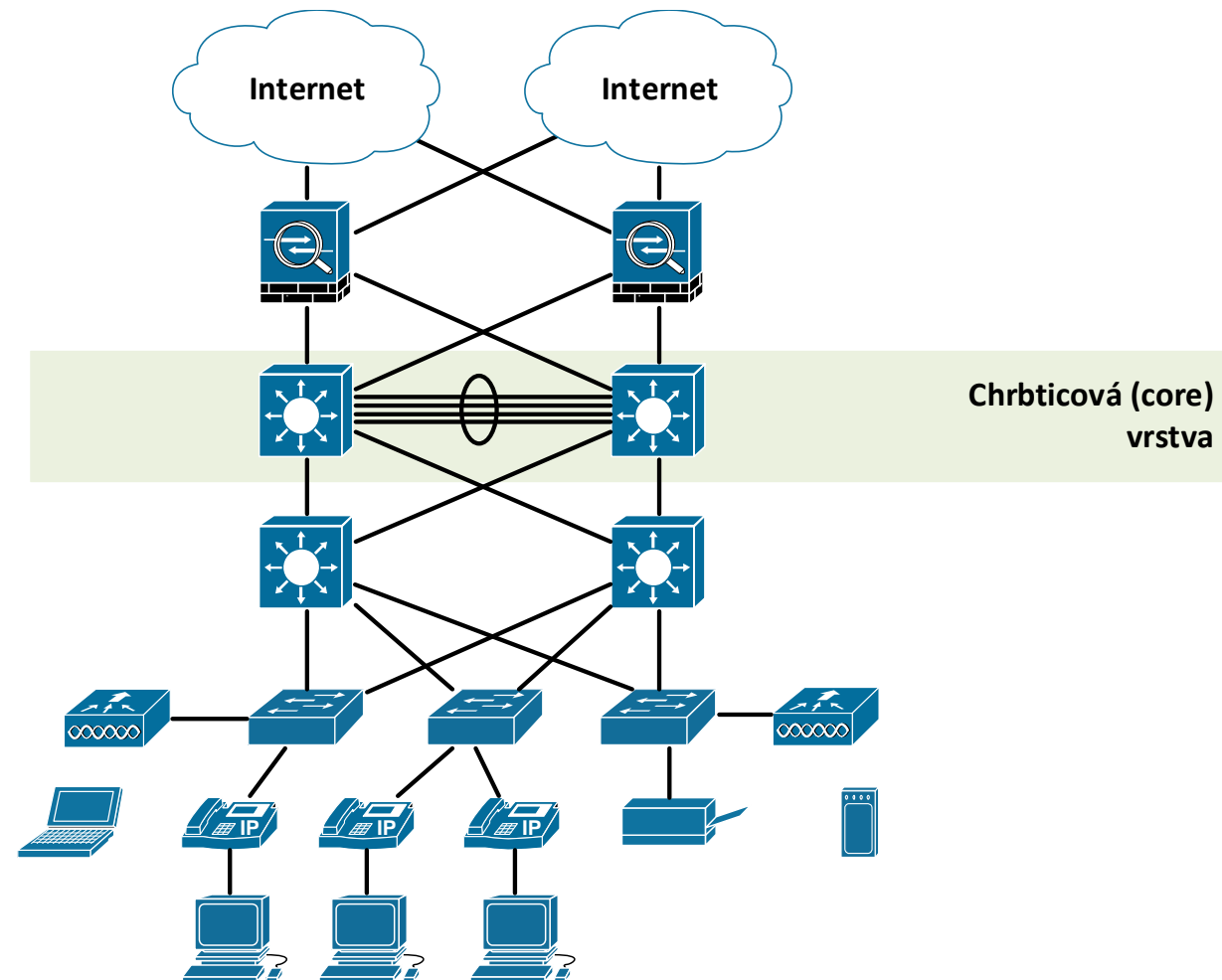
# Vlastnosti prepínačov – distribučná vrstva

- **Distribučná (distribution) vrstva**
  - Izoluje prístupovú vrstvu od chrbtice
  - Úlohy a technológie
    - Podpora MultiLayer smerovania medzi VLAN (aspoň L2/L3)
    - Podpora statického aj dynamického smerovania IPv4/IPv6
      - Agregácia adries
    - Vysoká prepínacia rýchlosť a výkon
    - Rýchlosť portov Gbps or 10Gbps porty
      - Porty primárne optické
    - Redundancia
    - Bezpečnosť
    - Access control lists (ACL)
    - Agregácia Liniek
    - Quality of service
    - Dostupnosť
    - Zálohovanie napájacích zdrojov (Hot swappable)



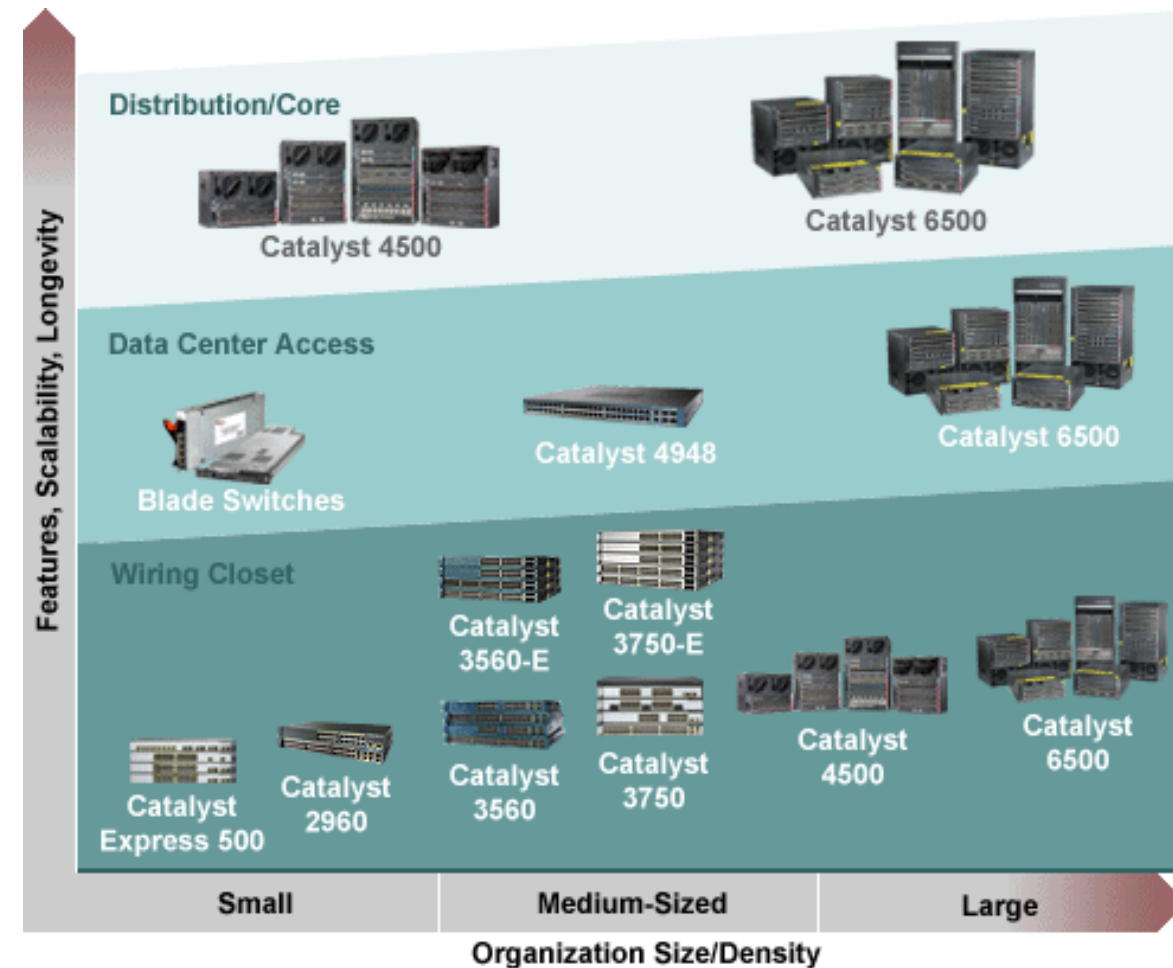
# Vlastnosti prepínačov – chrbticová vrstva

- **Chrbticová (core) vrstva**
  - Viac menej tie isté funkcie čo distribučná vrstva +
    - Zvýšená potreba redundancie, odolnosti voči chybám a znižovanie latencie
  - Je potrebné sa vyhnúť činnostiam vedúcim k spomaleniu činnosti prepínača



# Produktová línia Cisco Catalyst Switch

- Pre siete existujú podľa nasadenia viaceré kategórie prepínačov
  - Podnikové campus LAN (Access, distro, core prepínače)
  - Service Provider
  - Data Center
  - Cloud-Managed
  - Virtual Networking
- Špecifikácie ich vlastnosti sú popisované výrobcami v produktových listoch (data sheets)



## 2020 – DC - Nexus prepínače

- Škálovateľnosť,  
rýchlosť,  
prenosová  
flexibilita



## 2020 – Service provider Ethernet

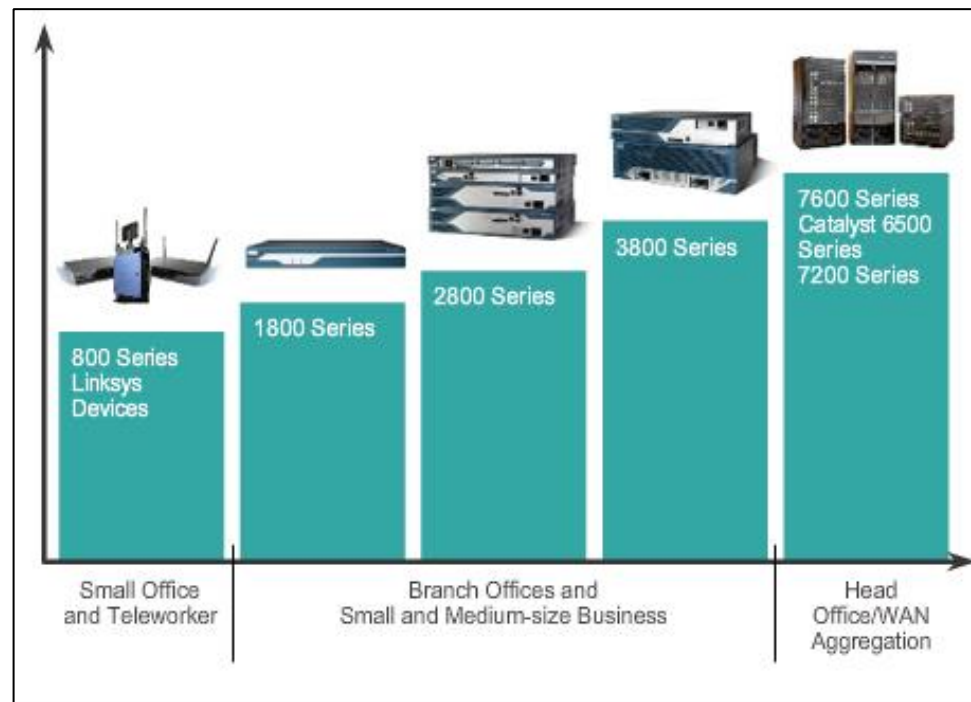
- Bezpečnosť,  
virtualizácia,  
jednoduchý  
manažment, unified  
services, aplikačná  
inteligencia





# Smerovače

- Fixná vs. Modulárna konfigurácia
- Tri kategórie
  - Branch – Highly available 24/7.
  - Network Edge – High performance, high security, and reliable services. Connect campus, data center, and branch networks.
  - Service provider routers



# Zaujímavé referencie

- Cisco Validated Design
  - [cisco.com/go/cvd](https://www.cisco.com/go/cvd)
  - [cs.co/en-cvds](https://www.cs.co/en-cvds)
    - [Campus LAN L2 Access with Simplified Distribution Deployment Guide](#)
    - [Campus LAN and Wireless LAN Design Guide](#)



UNIVERSITY OF ŽILINA  
Faculty of Management Science  
and Informatics



Networking  
Academy

Cisco | Networking Academy®  
Mind Wide Open™

... a my v Žiline hádam tiež ...



Ohodnot' našu CNA na google:

- <https://goo.gl/maps/BAnFvQKYCBpffcEX7>

Vytvorené v rámci projektu KEGA 026TUKE-4/2021