Počítačové sítě 1

Přednáška č.9

Návrh sítě a propojení zařízení

- Úvod do návrhu sítě
  - Vlastnosti dobře navržené sítě
  - Toky dat v síti
  - Klasický trojvrstvý model sítě
- Metodiky návrhu sítě
  - SONA, INN, FCAPS, ITIL, PPDIOO, FCAPS
- Role zařízení v síti

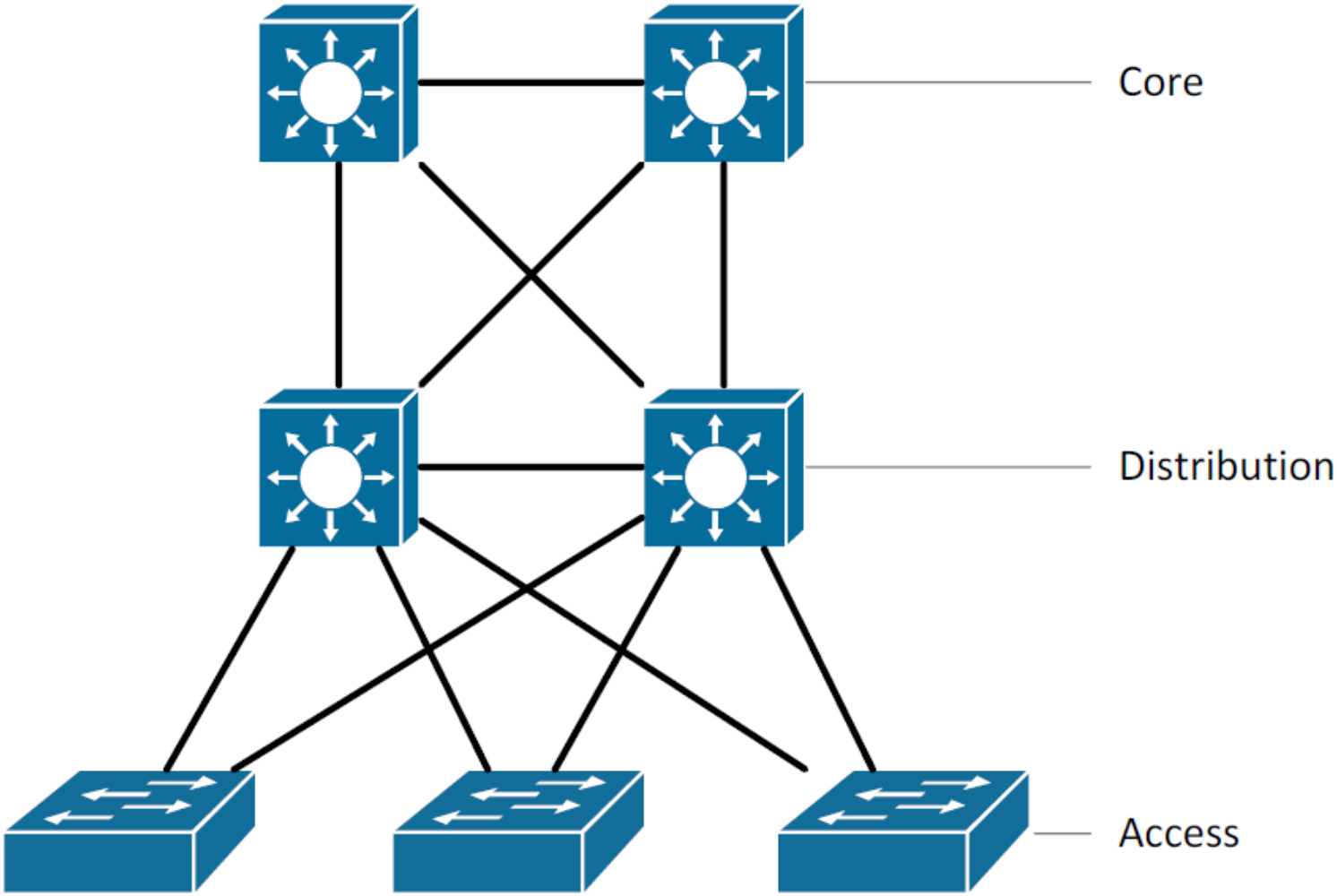
- Klíčem k dobrému návrhu sítě je její **hierarchický design**
- Hierarchická síť
  - Ohraničuje velikost a rozsah kolizních domén
  - Zjednodušuje činnost různých mechanismů, které pracují v jednotlivých oblastech sítě
  - Dovoluje efektivně přidělovat adresy a lehce je sumarizovat ve směrovacích protokolech
  - Zpřehledňuje toky dat
  - Jasně odděluje funkční bloky pro Layer 2 a Layer 3

- Voice and video traffic
  - IP telefonie, video, konference
  - Jedná se o real-time data a ty vyžadují použití QoS nástrojů pro garanci jejich včasného doručení
- Voice application traffic
  - Data související s provozem datových služeb, např. kontaktní centra
- Mission- cririca l traffic
  - Data aplikací kritického významu pro podnik
- Transactional traffic
  - Aplikace pro e-commerce
- Routing protocol traffic
  - Provoz generovaný směrovacími protokoly
- Network management traffic
  - Dohledové protokoly nad sítí

- S postupným růstem sítě se v ní musí nacházet více zařízení

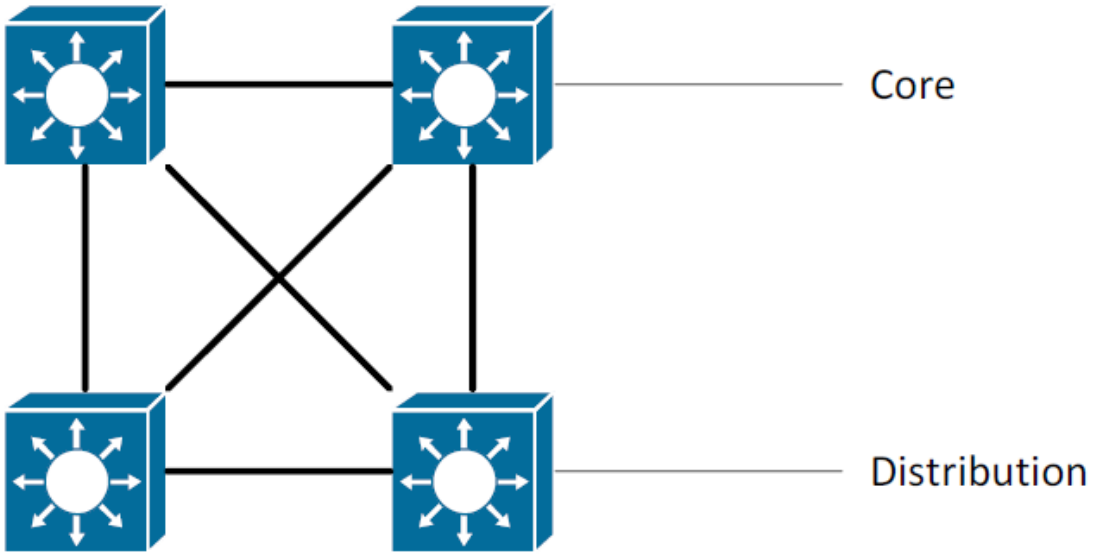
- Proto je vhodné je rozdělit podle funkce, kterou mají v síti plnit, a organizovat je ve vrstvách
  - Jisté zařízení budou sloužit k **připojení koncových zařízení** k síti
  - Jiné, vyšší zařízení budou **navzájem propojovat** přístupové zařízení. Přitom mohou vykonávat **bezpečnostní** nebo **ukončující** operace
  - Zařízení na vyšší úrovni budou tvořit **páteř** celé sítě

- Tento systém třech vrstev **– přístupové, distribuční a páteřní** je klasický starší trojvrstvý model sítě

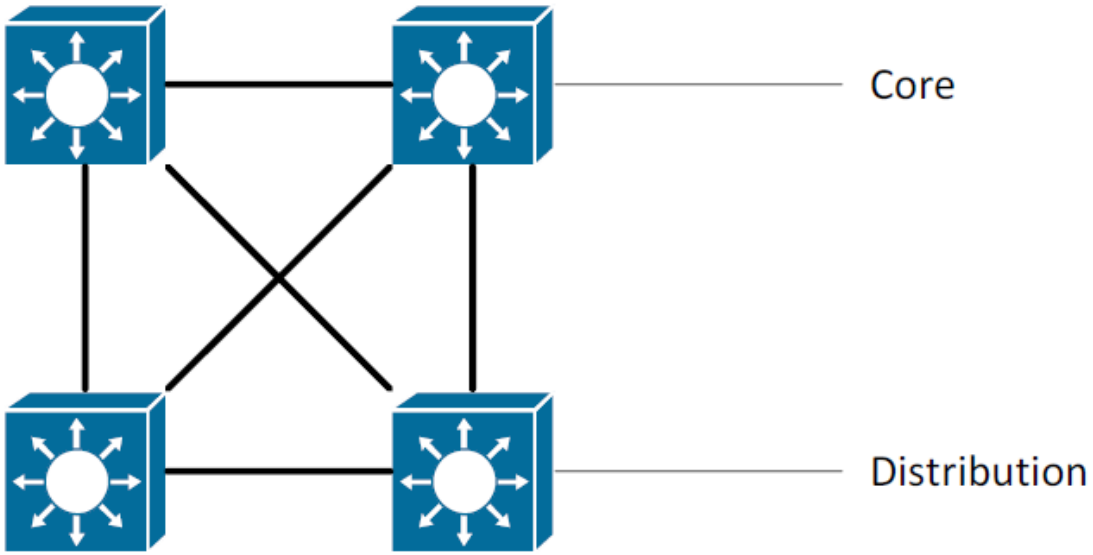

Core
Distribution
Access

- **Přístupová vrstva (Access)**
  - Obvykle přepíná, v poslední době je i směrovaná
  - Zajišťuje přístup klientů do sítě, zařazení do VLAN, implementuje bezpečnostní mechanismy při přístupu a komunikaci, zajišťuje QoS mechanismy
- **Distribuční vrstva (Distribution)**
  - Je obvykle směrovaná
  - Ukončuje VLANy, zajišťuje inter-VLAN routing, sumarizuje adresní rozsahy přístupové vrstvy, implementuje bezpečnostní mechanismy při komunikaci, zajišťuje QoS mechanismy
- **Páteřní vrstva (Core)**
  - Je obvykle směrovaná s nutností rychlé konvergence
  - Obsahuje redundantní spoje s dostatečnou kapacitou, zajišťuje vysokorychlostní přepínání s směrování, implementuje QoS mechanismy

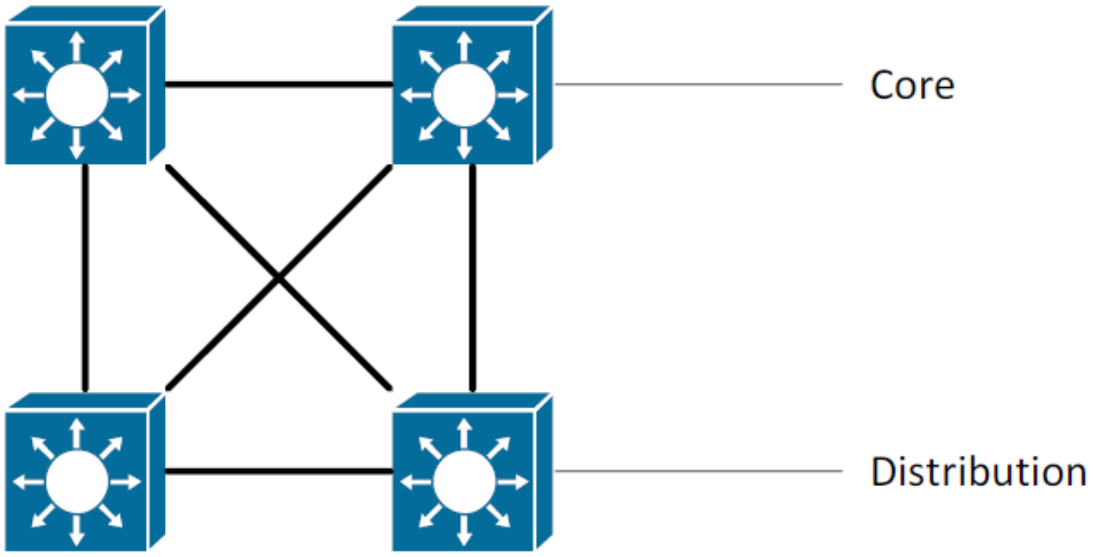
- **Páteřní vrstva (Core)**
  - Využití směrování (L3), které garantuje topologii s využitím všech agregovaných a redundantních linek (proti L2 STP)
    - Dynamické směrovací protokoly jsou preferované proti využití STP protokolu, protože tento koncept dovoluje využití konvergence a equal/unequal load balancingu skrze více cest
    - Je preferované využití protokolu OSPF, díky jeho otevřenému standardu a multivendor interoperabilitě.



- **Páteřní vrstva (Core)**
  - Využití Layer 3 přepínačů v core vrstvě, které poskytují pokročilé služby, jež Layer 2 přepínače nepodporují
    - Inter-VLAN routing
    - Podpora dynamických směrovacích protokolů
    - Virtualizace síťových prvků (stále proprietální technolgie Cisco Systems – VSS Virtual Switching System na Catalyst 6500)

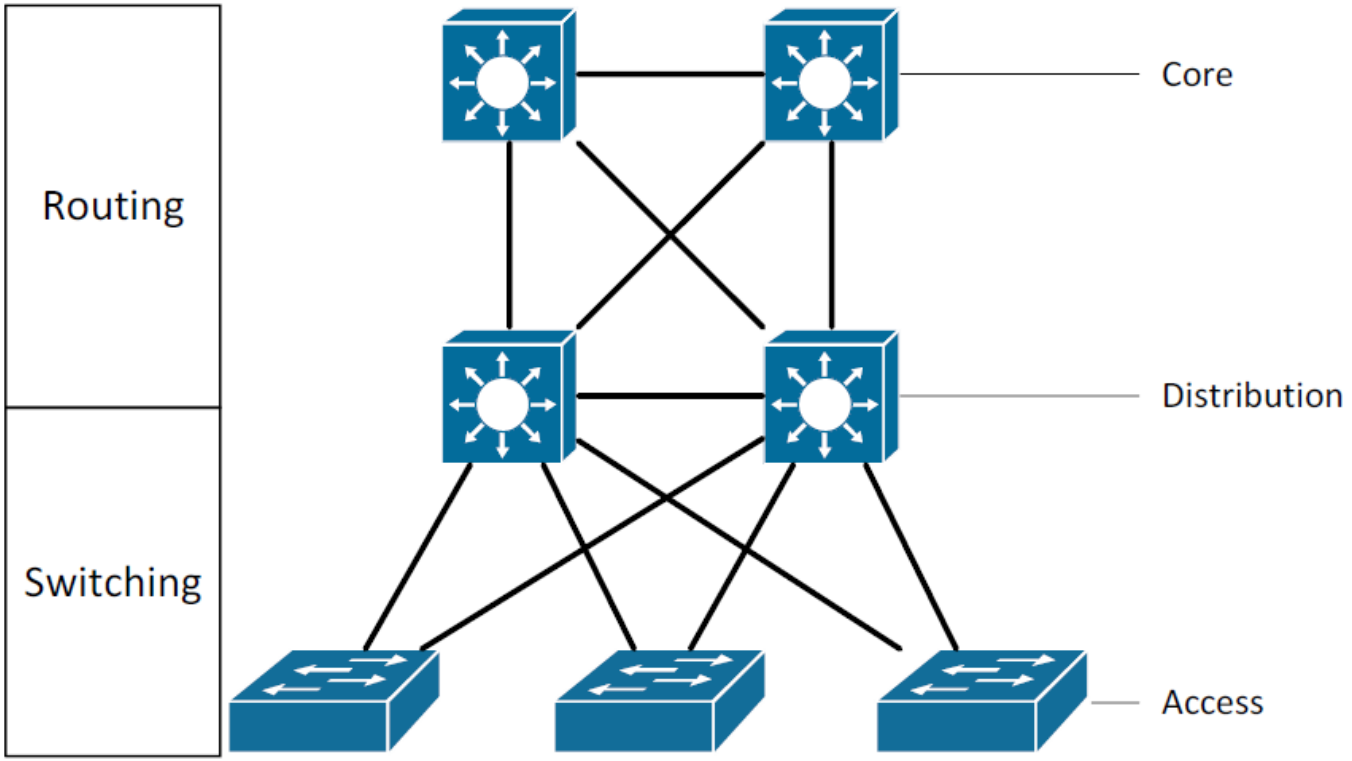


- **Páteřní vrstva (Core)**
  - Využití dvou rovnocenných cest každého core zařízení pro spojení s distribuční vrstvou
    - 2 aktivní cesty poskytují větší šířku pásma než 1 aktivní a 1 záložní cesta (dynamic routing vs. STP)

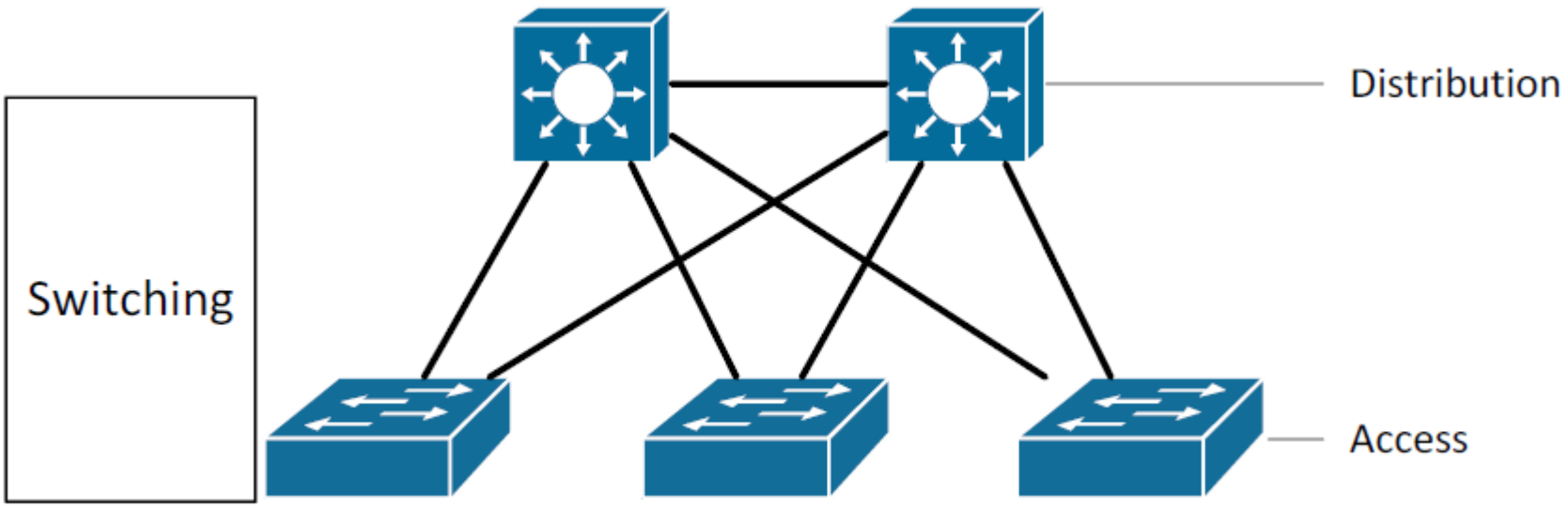


- **Distribuční vrstva (Distribution)**
  - Využití protokolů pro redundanci výchozí brány
    - HSRP je Cisco proprietální technologie, nepodporuje aktivní load-balancing přes více linek ve stejném čase, ale je jednoduchý
    - GLBP je Cisco proprietální technologie, vhodná do prostředí, kde je hlavním požadavkem permanentní dostupnost. Podporuje aktivní load-balancing v tom samém čase
    - VRRP je technologie s otevřeným standardem, nabízí multivendor interoprabilitu, rychlé časy konvergence. Nepodporuje aktivní load-balancing

- **Distribuční vrstva (Distribution)**
  - Využití dynamických směrovacích protokolů mezi distribuční a páteřní vrstvou pro rychlou konvergenci a load-balancing

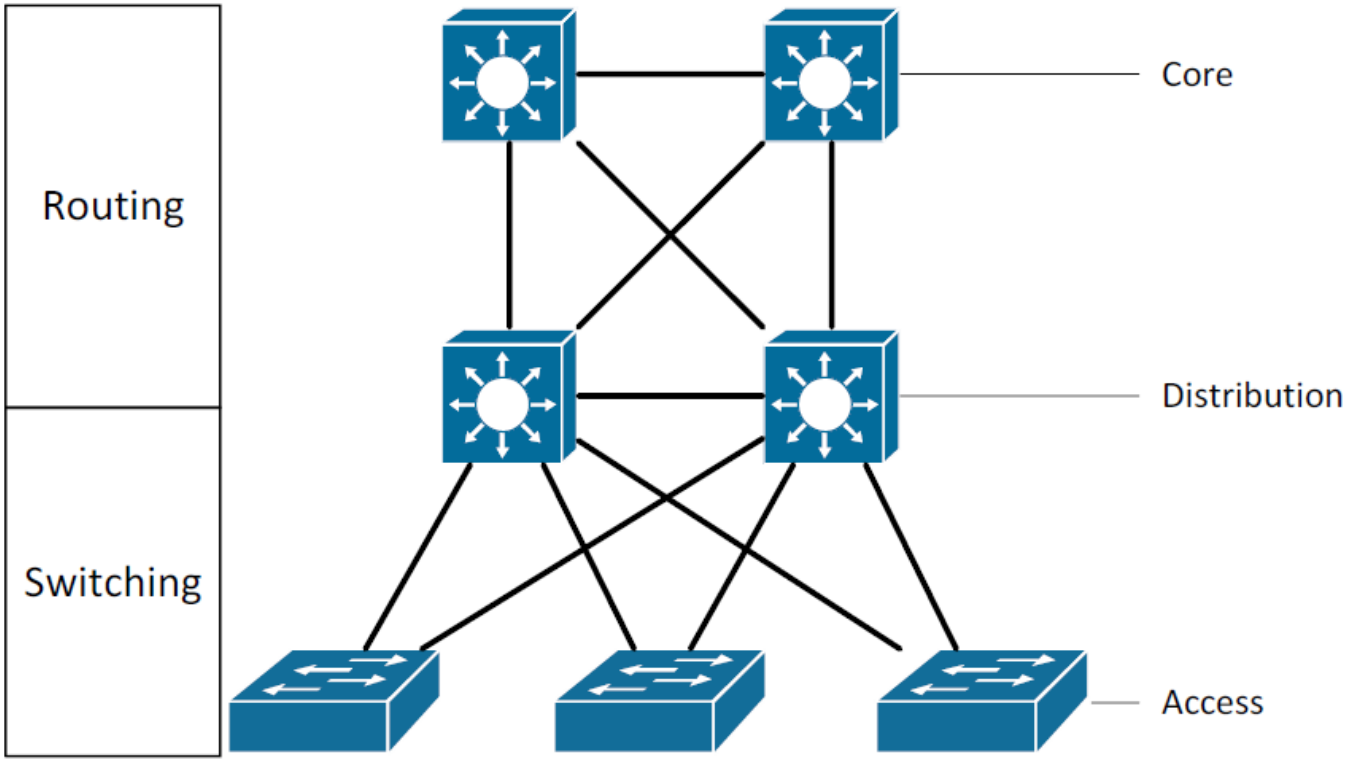


- **Distribuční vrstva (Distribution)**
  - Propojení distribučních přepínačů s vícero přepínači na přístupové vrstvě. To dovolí existenci záložních cest



Distribuční vrstva (Distribution)

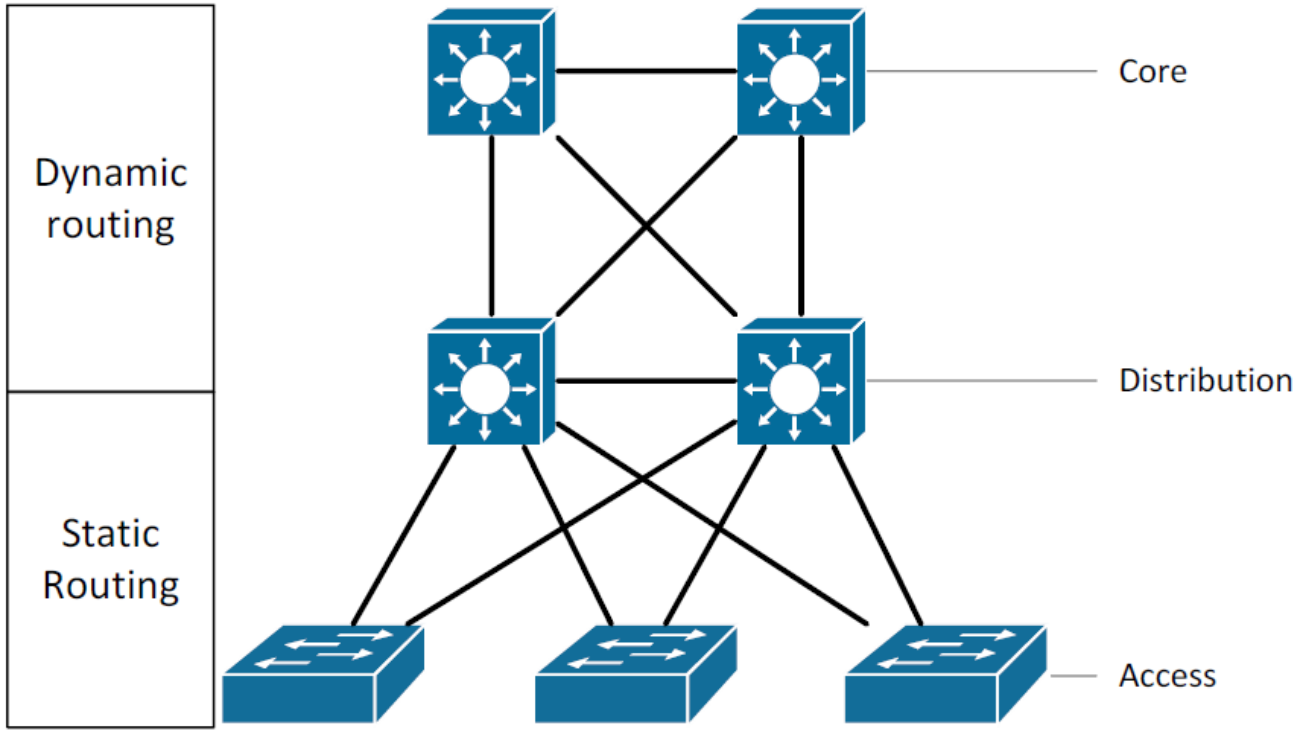
- Sumarizace směrovacích informací na distribuční vrstvě zredukuje reřii dynamických směrovacích protokolů vůči páteřní vrstvě



- **Přístupová vrstva (Access)**
  - Omezení VLAN pokud možno do co nejmenšího počtu přepínačů, zmenší broadcastovou doménu, režii VTP prunningu a obecně činnosti VTP
  - Pokud je potřebná STP protokol, preferujte variantu RSTP nebo RPVST+ (Cisco proprietální)
    - Pokud není dostupná je vhodné použití MST
    - U zařízení Linksys a „Cisco Small Business“ je možné spustit pouze 1 instanci RSTP nad všemi VLANy
  - Vypnutím protokolu DTP, který „domlouvá“ trunkové a přístupové porty je zajištěna vyšší bezpečnost na přístupové vrstvě
  - Využití automatického nebo manuálního VTP prunningu je docíleno zmenšení broadcastových domén

Přístupová vrstva (Access)

- U některých sítí je vhodné zvážení zavedení statického směrování již na přístupové vrstvě, které zpřístupní L3 load-balancing
- Tuto funkcionalitu nabízí i většina L2 Catalyst přepínačů pomocí SMD

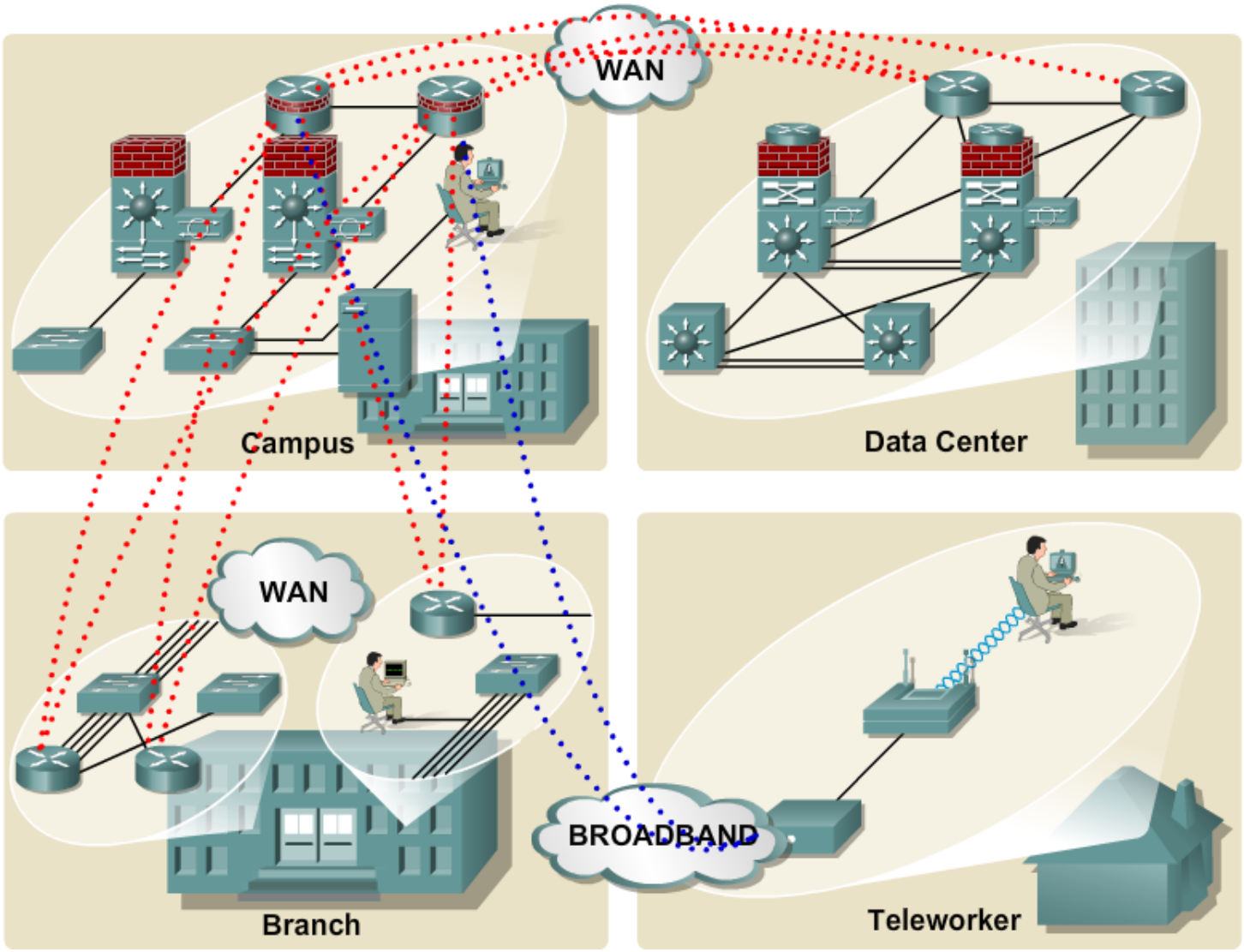


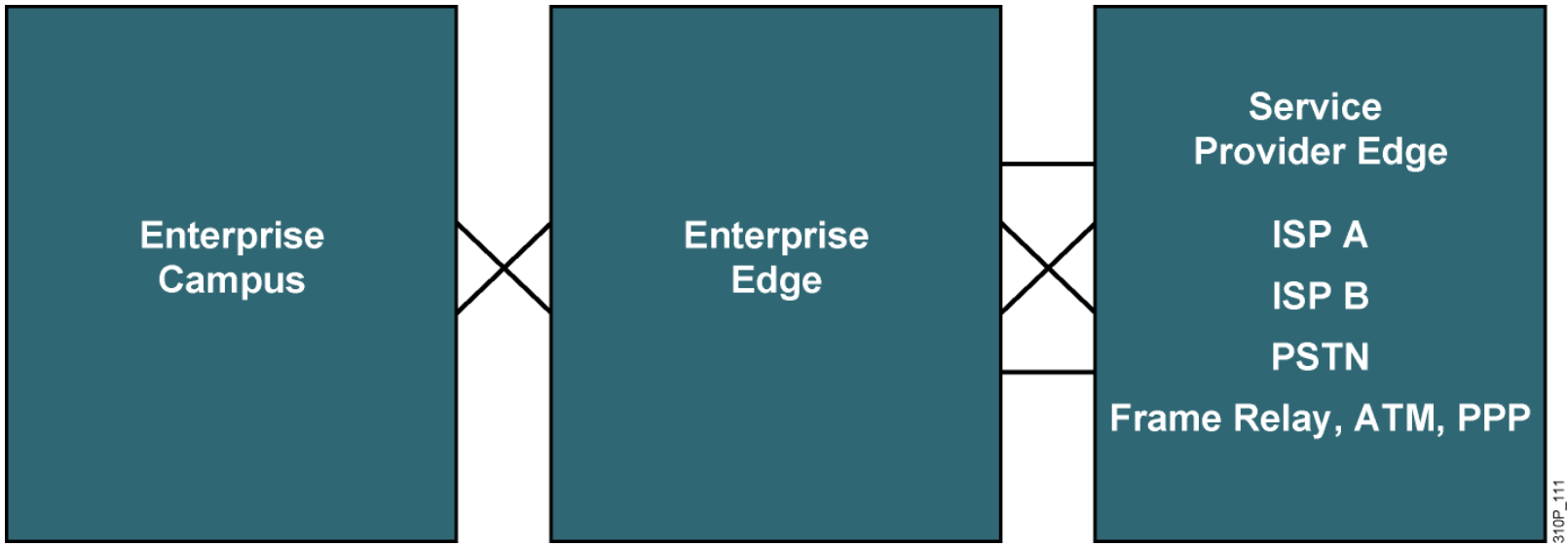
- **Přístupová vrstva (Access)**
  - Je vhodné zajistit bezpečnost na portech přepínačů přístupové vrstvy (port security)
  - Je vhodné zvážit adekvátní poměr mezi
    - Access switch – access port 1:10
    - Access switch – trunk port (port k přepínači distribuční vrstvy) 1:2 nebo 1:4
  - Zvážit vlastnosti přístupových přepínačů
    - Je nutné PoE? (je drahé)
    - Umí PoE dodávat dostatečně vysoké napětí?
    - Je PoE managovatelné?

- Návrh rozsáhlých sítí je netriviální záležitost, která si vynucuje komplexnější model než klasický 3-vrstvý

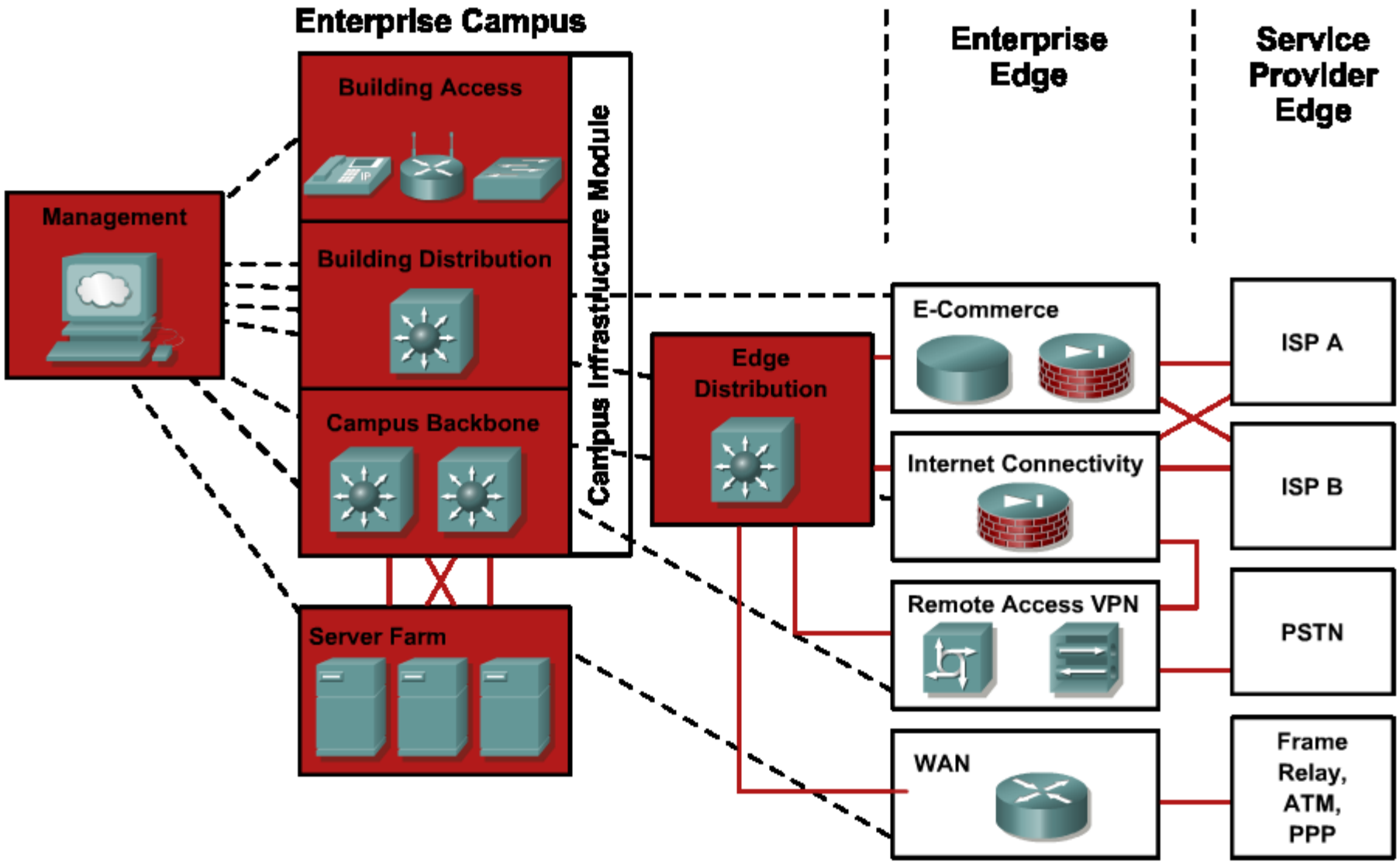
- Existuje mnoho metodik, jak takové sítě navrhovat
  - Z pohledu architektury (topologie)
  - Z pohledu firemních nařízení resp. předpisů
  - Z pohledu poskytovaných služeb
  - Z pohledu inteligence a propojení s jinými systémy

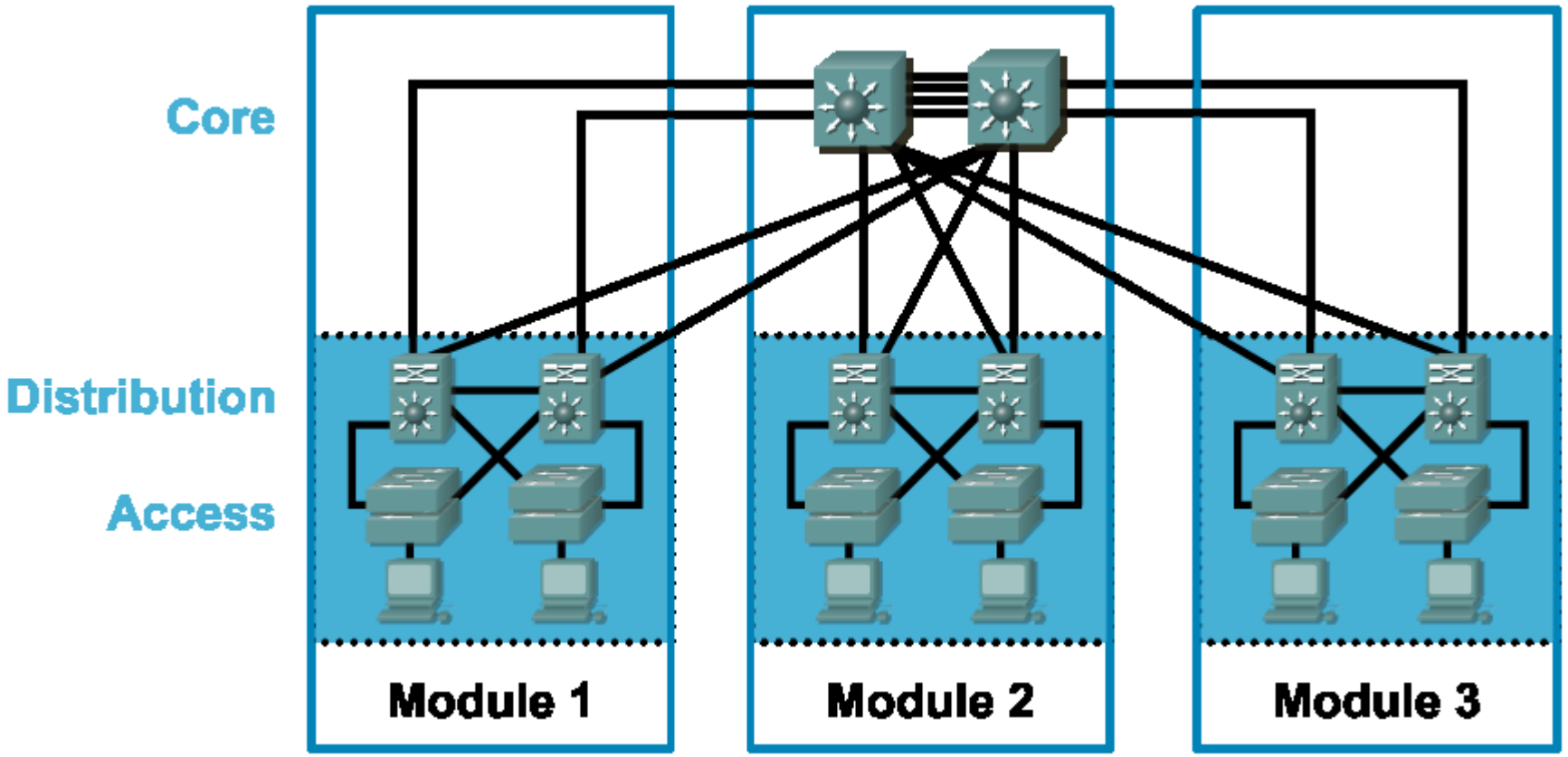
- Cisco má pro architekturu rozsáhlých podnikových sítí model s názvem „Cisco Enterprise Architecture“
  - Obsahuje 6 základních částí: Enterprise Campus, Enterprise Edge, Provider Edge, Enterprise Branch, Enterprise Data Center, Enterprise Teleworkers
  - Každá z těchto částí má doporučenou architekturu a řešení


WAN
Campus
Data Center
WAN
BROADBAND
Branch
Teleworker



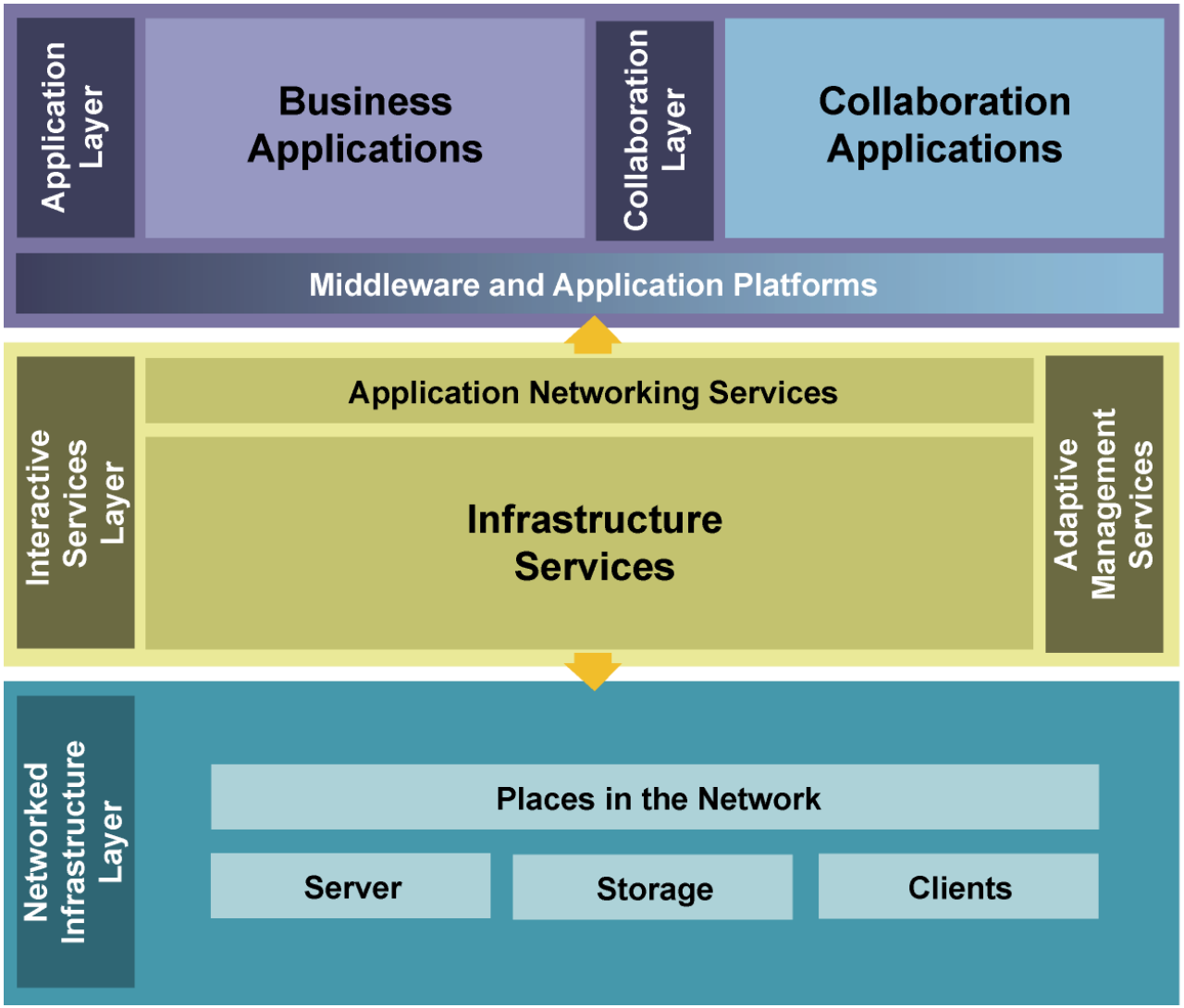
- **Enterprise Campus**
  - Obsahuje moduly pro vybudování výkonné a robustní firemní sítě
- **Enterprise Edge**
  - Sada funkčností týkající se externího přístupu do firemní sítě
- **Service Provider Edge**
  - Přístup síťovým zdrojům mimo firemní síť


Enterprise Campus
Enterprise Edge
Service Provider Edge
Building Access
Building Distribution
Campus Backbone
Campus Infrastructure Module
Management
Server Farm
Edge Distribution
E-Commerce
Internet Connectivity
Remote Access VPN
WAN
ISP A
ISP B
PSTN
Frame Relay, ATM, PPP


Core
Distribution
Access
Module 1
Module 2
Module 3

- Pro Cisco je síť více než jen souvislá komunikační infrastruktura – je to platforma pro integrovaná aplikace
  - Síť se však musí stát „application-aware“

- Cisco zavedlo pojem Service Oriented Network Architecture (SONA) pro architekturální framework
  - Síťová architektura z podstatně vyššího pohledu
  - Framework má tři vrstvy
    - Network Infrastructure Layer
    - Interactive Services Layer
    - Application Layer


Application Layer
Business Applications
Collaboration Layer
Collaboration Applications
Middleware and Application Platforms
Interactive Services Layer
Application Networking Services
Infrastructure Services
Adaptive Management Services
Networked Infrastructure Layer
Places in the Network
Server
Storage
Clients
310P_152

- Inteligent Information Network (IIN) je evoluční vize nové sítě, ve které aktivně spolupracují
  - Informační zdroje
  - Síťové prvky
  - Aplikace

- IIN podle Cisca vzniká ve třech etapách
  - Integrovaný transport
  - Integrované služby
  - Integrované aplikace (Application-Oriented Networking, AON)

- **Integrovaný transport**
  - Společná, konsolidovaná a konvergovaná IP síť pro všechny druhy datovách toků a síťových služeb
- **Integrované služby**
  - Sdružování (pooling), sdílení a virtualizace IT projektů
  - Unifikace kapacity síťových úložišť a datových center
  - Virtualizace serverů, úložišť a síťových prvků
- **Integrované aplikace**
  - Inteligentní síť rozeznávající, jaká druh služby poskytuje a podle toho optimalizuje svojí činnost (application-aware network)
  - Content caching, load balancing, aplikační bezpečnost

- Pro návrh a provoz sítě existuje více metodik
  - **FCAPS** – Fault, Config, Accounting, Performance, Security (ISO)
  - **TMN** – Telecommunication Management Network (ITU-T)
  - **ITIL** – IT Information Library
  - Cisco Lifecycle Services (PPDIOO)

- Cisco Lifecycle Services se někdy také označuje jako model PPDIOO, podle názvu šesti fází ze kterých se skládá
  - Prepare
  - Plan
  - Design
  - Implement
  - Operate
  - Optimize

- **Prepare**
  - Stanovení požadavků organizace či podniku, návrh strategie jejich dosažení, určení klíčových technologií pro dané požadavky, návrh high-level architektury. Představení bussiness-case

- **Plan**
  - Určení požadavků na firemní infrastrukturu, vyhodnocení potřebných rozšíření a doplnění (gap analysis). Vypracování implementačního plánu obsahující jednotlivé úlohy, odpovědných řešitelů, časové etapy a potřebné zdroje na návrh a implementaci projektu

- **Design**
  - Vytvoření návrhu technické infrastruktury na základě informací a požadaveků z předcházejících fází. Projektový (implementační) plán může být v této fázi doplněný a zpřesněný

- **Implement**
  - Implementace řešení vytvořeného ve fázi Design. Zahrnuje rozšíření nebo přestavbu existující síťové infrastruktury. Každý zásah musí být dopředu ohlášený a autorizovaný. Vždy musí existovat i nouzový plán pro návrat do předchozího stavu.

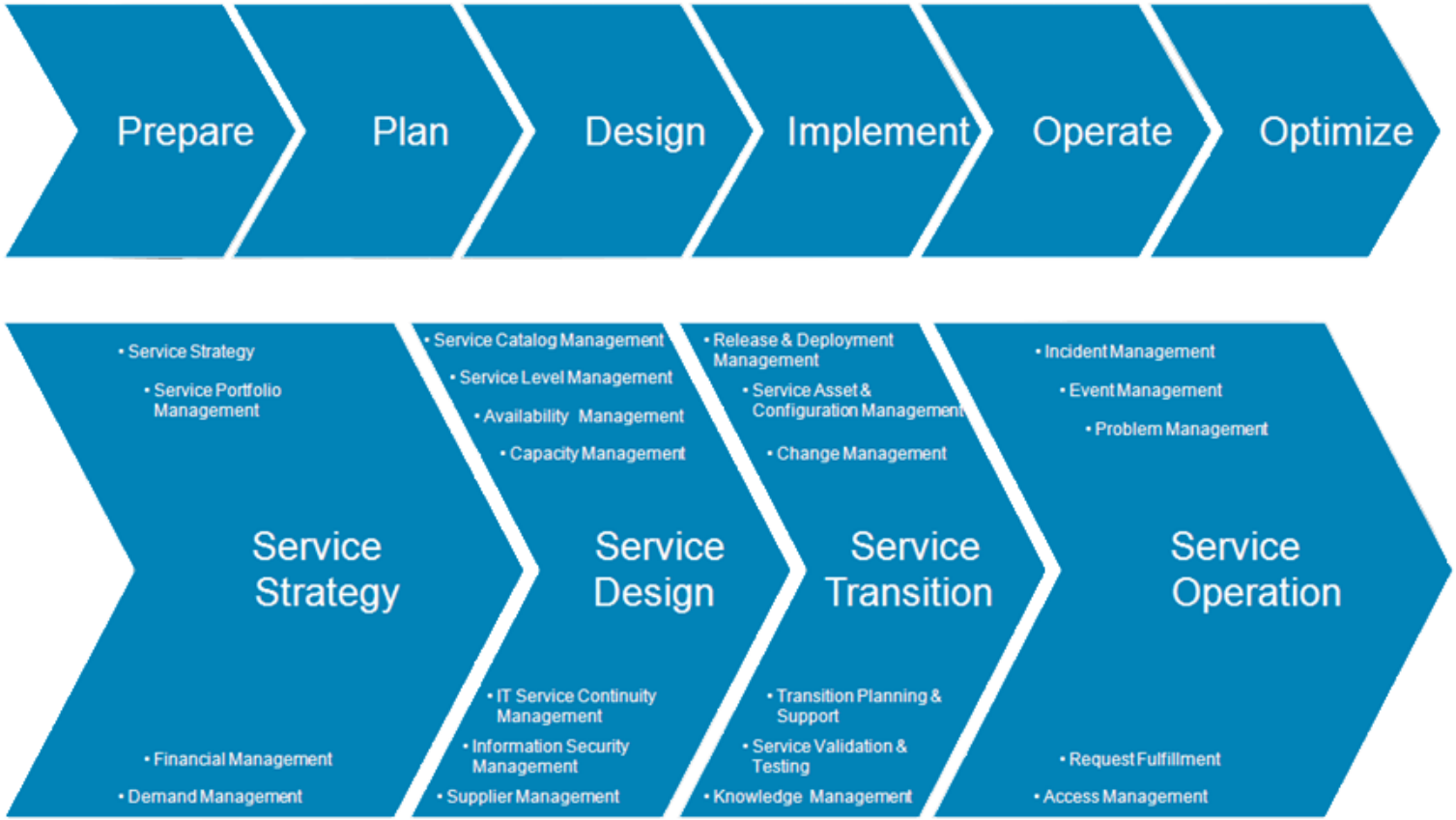
- **Operate**
  - Je fáze, ve které se implementované řešení používá v rutinním provozu. Současně se získávají provozní informace, realizuje se rutinní údržba řešení, aktualizace, odstraňují se běžné chyby.

- **Optimize**
  - Proaktivní sledování a management sítě. Informace o činnosti sítě v této fázi mohou vést k úpravě řešení a k další iteraci cyklu PPDIOO

- Vytvořením implementačního plánu a jeho realizací se zabývají i následující uvedené metodiky
  - **ITIL** je suma tzv. best practices, vytvoření implementačního plánu a jeho realizaci zahrnuje jako jednu ze svých součástí
  - **FCAPS** obsahuje vytvoření implementačního plánu a jeho realizace v kategorii Network management (zejména potom v podčásti Configuration management)
  - **TMN** je podobný FCAPS-u, implementační plán a jeho realizace jsou součástí stavebních bloků v TMN

- Všechny tyto modely představují **strukturovaný přístup** k rozšiřování sítě a řešení problémů
  - Opakem je tzv. **ad-hoc přístup**, který je vhodný pouze pro malé sítě, avšak ve větších sítích může vést k velmi zásadním problémům

= V ITIL lze jednotlivé části iterativního procesu pro návrh a implementaci počítačových sítí namapovat na metodiku Cisco PPDIOO



- FCAPS je obecná metodika pro vytvoření a údržbu IT infrastruktury vytvořená organizací ISO

- Síťový management dělí do pěti kategorií:
  - Fault Management
  - Configuration Management
  - Accounting Management
  - Performance Management
  - Security Management

- **Fault Management**
  - Klade důraz na preventivní údržbu, kontrolu a **správu chyb** počítačové sítě
  - Zabývá minimalizací odezvy zařízení v síti
  - Kroky potřebné pro správu chyb:
    - Rozpoznat problém, izolovat problém
    - Upozornit na problém
    - Informovat uživatele, případně zákazníka
    - Vyřešit problém, pokud je to možné

- **Configuration Management**
  - Obsahuje instrukce pro instalaci, **konfiguraci a kontrolu** síťového hardwaru i softwaru
  - Zabývá se výměnou havarovaných prvků a správou inventáře
  - Kroky pro správu konfigurace:
    - Shromažďovat a ukládat všechna nastavení
    - Zjednodušovat konfiguraci, pokud je to možné
    - Provést změnu v historii konfigurací všech zařízení
    - Nastavit konfiguraci kontrolovaného prvku

- **Accounting Management**
  - Plánování kapacity, škálovatelnosti a cenové efektivity pořízených prvků
  - Přidělování a distrubuce výpočetních a transakčních zdrojů sítě
- **Performance Management**
  - Tato část FCAPS-u se zabývá maximalizací propustnosti počítačové sítě u již pořízených síťových prvků
  - Identifikace bottle-necků v síti
- **Security Management**
  - CIA (Confidentiality, Integrity, Availability)
  - AAA (Authentication, Authorization, Accounting)
  - Šifrování provozu v počítačové sítí
  - Implementace IPS/IDS systémů
    - IPS – Intrusion prevention system
    - IDS – Intrusion detection system

- **TMN** je standardem organizace ITU-T pro návrh, implementaci a údržbu počítačových sítí, optimalizovanou pro provoz telekomunikačních služeb
  - Telefonní operátoři atd.
- Optimalizován zejména pro využití WAN technologií jako:
  - ISDN, B-ISDN, ATM, SDH/SONET, GSM

- Je složen z následujících modulů
  - **Business management**
    - Obsahuje funkcionalitu vztaženou o business aspektům – analýza trendů, kontrola kvality, finanční reporty atd.
  - **Services management**
    - Zabývá se službami v síti, jejich řízením, definicí a jejich účtováním
  - **Network management**
    - Zabývá se distribucí síťových prostředků a zdrojů. Kontrola konfigurace a dohled nad sítí
  - **Element management**
    - Zabývá se jednotlivými síťovými zařízeními, logováním, zálohou a údržbou hardwaru i softwaru

Děkuji za pozornost