víme jak

Efektivní výstavba menších MAN sítí

Setkání informatiků Plzeňského kraje

Petr Vejmělek
manažer OC

21.11.2011

AutoCont

Smart Administration - úrovně elektronizace veřejné správy

Národní úroveň

- **Centrální místo služeb** (…také Internet)
- **ISZR** (základní registry…)
- **Transportní síť MV ČR** (ITS-NGN)

Regionální úroveň

- **Služby nabízené Krajem – TC K**(GIS, ….)
- **IVVS** (Integrovaný varovný a vyrozumívací systém)
- **IZS** (Integrovaný záchranný systém)
- **E-Health** (propojení nemocnic a dalších zdrav. Zařízení)
- **Krajské „Body zájmu“** = krajské organizace

Metropolitní úroveň

- **Služby nabízené ORP (TC ORP) vůči organizacím**
- **Metropolitní body zájmu…** (školy, knihovny, apod…)

Metropolitní sítě - body zájmu více participantů

- **… teprve koncové organizace na této úrovni dávají celému třívrstvému modelu Smart Administration ten klíčový rozměr !**

- **Metropolitní sítě jsou koncipovány jako sítě „přístupové“**
  - … s důrazem na co nejplošnější pokrytí (FTTx, PON, WiMax, Wifi)
  - … s charakterem JKI (jednotné komunikační infrastruktury)

- **Různí zřizovatelé**
  - ministerstvo, kraj, město (obec)

- **Jeden společný jmenovatel**
  - intravilán měst a obcí

Spolupráce mezi participanty

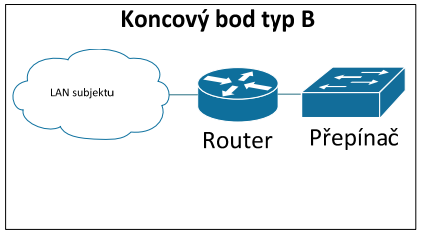
Na co brát ohled při volbě designu JKI

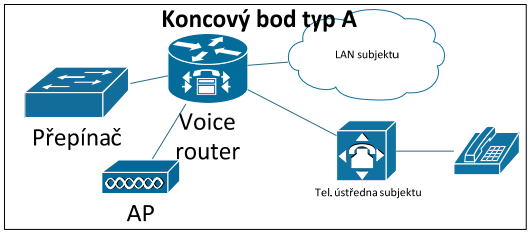
- **Hlavní faktory, ovlivňují návrhu JKI a formy spolupráce**
  - geografické možnosti lokality (jak plošné bude pokrytí lokality)
  - jaké typy organizací ji budou využívat (volba technologií, provozní náklady…)
  - co se bude přenášet (charakter dat a služeb)
  - jak bude zajištěn provoz (provozní model, příjem provozních incidentů =helpdesk…)
  - požadavky na dostupnost (SLA)
  - dynamika předpokládaného rozvoje

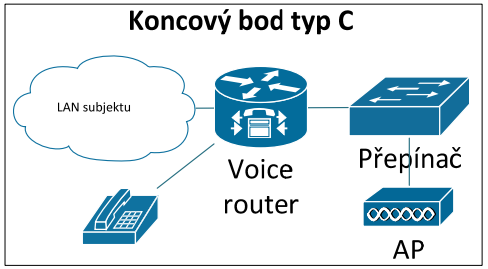
Metropolitní síť – Dlouhodobý plán rozvoje

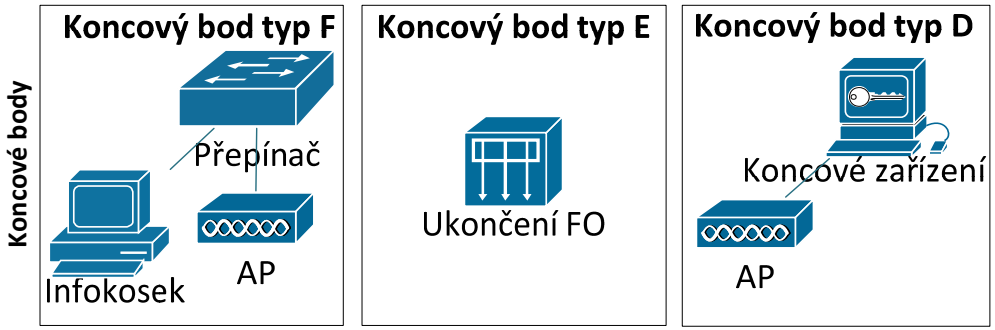
Metropolitní sítě – kategorizace koncových příjemců

- Různé typy organizací = různé nároky a požadavky
- Rozškatulkování - profily
- Profil charakterizuje klíčové očekávání o „bezpečnosti“, „dostupnosti“ a „kvalitě“









Služby metropolitních sítí

- **Úzko a širokopásmový internet**
- **Místní datové okruhy** (tzv. VPN, často v rámci v.s. nebo firem)
- **Distribuce videoslužeb** – IPTV, Video On Demand, místní videookruhy
- **Telefonní a videofonní služby** (např. místní volání zdarma)
- **Bezpečnostní služby** – ostraha budov, správa budov, MKDS
- **Služby datových úložišť (SAN)**
- **Pokročilé el. služby veřejné správy**
- **Podpora turismu** – kiosky, další informační služby, WiFi hotspoty

- **IVVS - integrovaný varovný a vyrozumívací systém**
- **Řízení dopravy**
- **Inteligentní zastávky MHD**
  - automaty nabíjení karet nebo lístky, kamery v prostředcích MHD

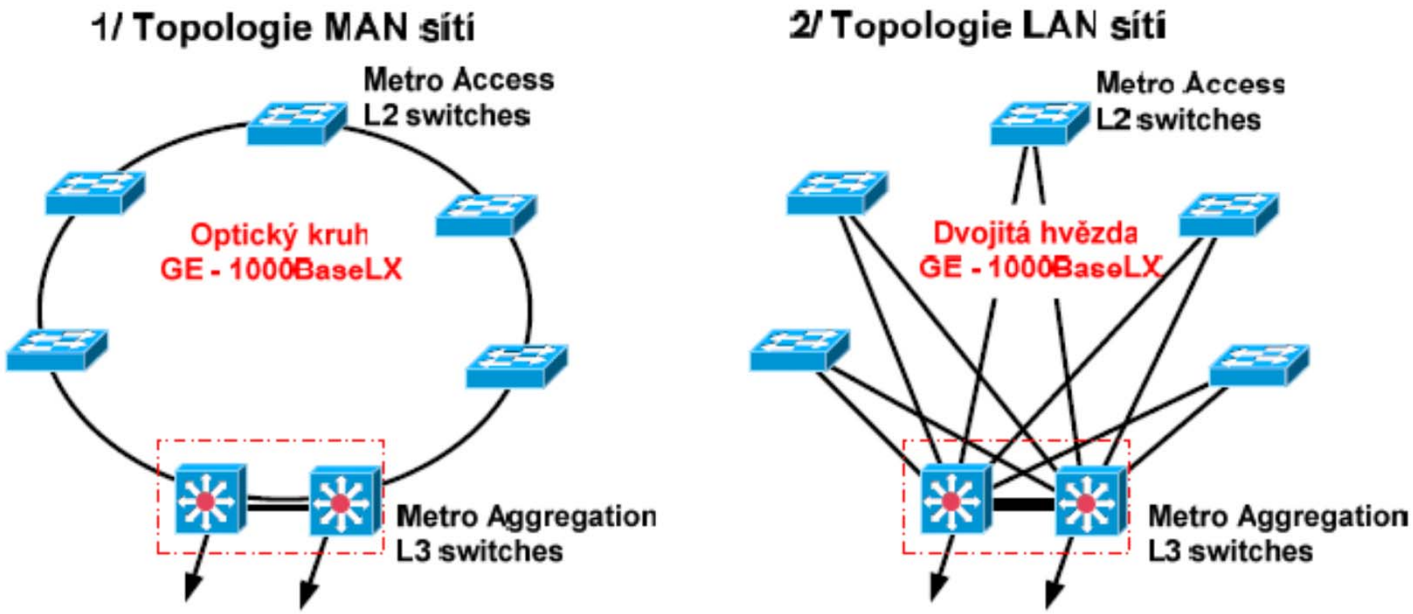
Služby metropolitních sítí – katalog služeb

- **Co by mohl (měl) obsahovat katalog služeb**
  - **Kod a název**
  - **Popis, definice**
  - **Podmínky realizace služby**
  - **Varianty služby**
  - **Volitelné parametry**
  - **Proces zřízení služby**
  - **Doba provozu**
  - **Doba podpory**
  - **Dostupnost – SLA**
  - **Monitoring**
  - **Reporting**
  - **Účtování (cena, forma, četnost…)**

- **Pro provoz JKI a mnoha služeb nad ní je klíčové**
  - Řízení kvality služeb – hierarchický QoS
  - Oddělení datových toků napříč celou sítí
  - Zajištění redundance

METRO Ethernet – obecné architektury

Switche by měly formovat topologické kruhy, které jsou nejúspornější z hlediska infrastruktury, ale stále zaručují redundanci. Některá města používají též topologii dvojité hvězdy, známou z LAN sítí.

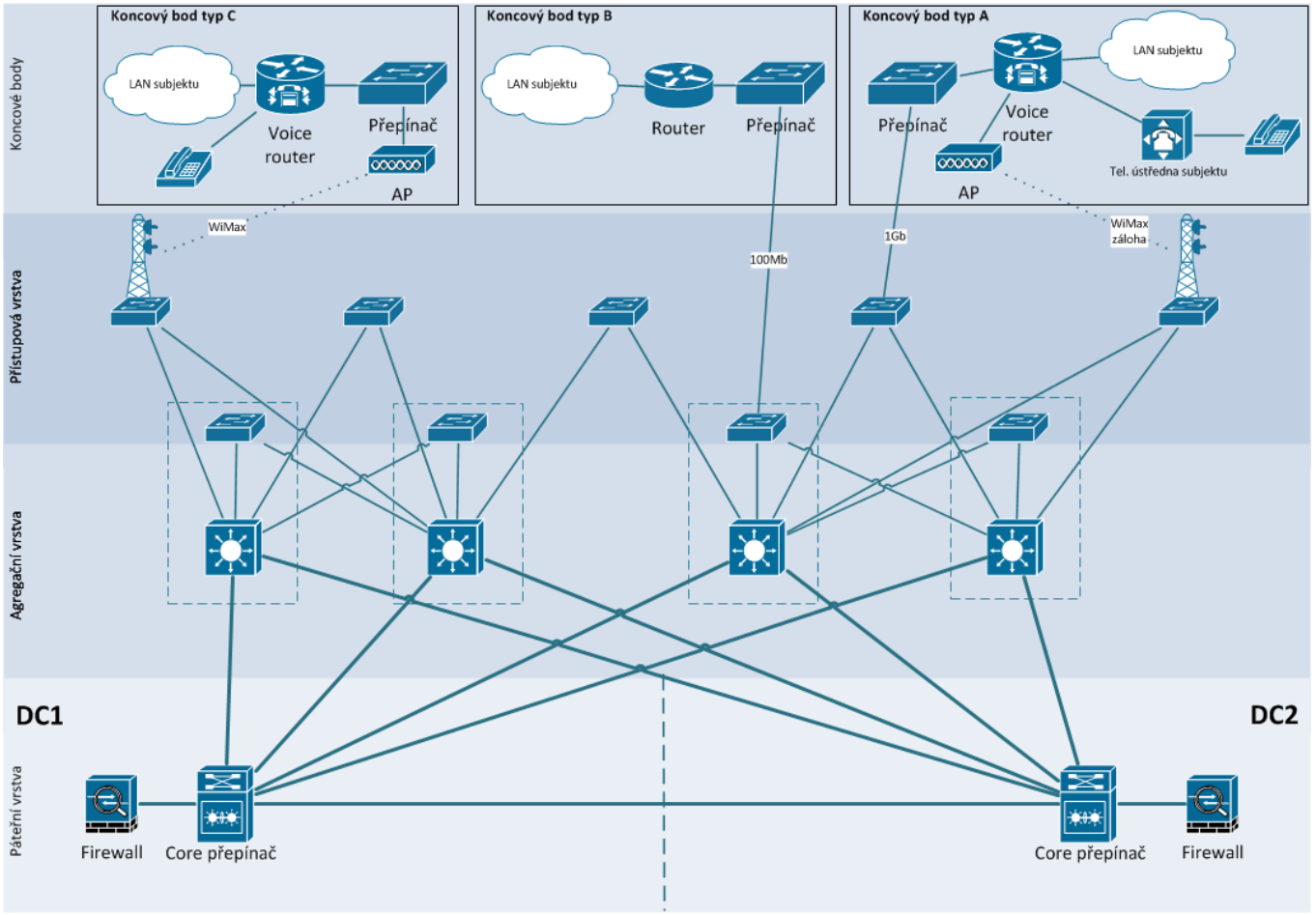


Obr. 18: Doporučené redundantní topologie pro přepínaný L2 Ethernet

Neredundatní bezesmyčková topologie (např. strom) je rovněž použitelná, především pak v malých instalacích bez firemních a multimediálních služeb, kde délka výpadku není tak kritická.

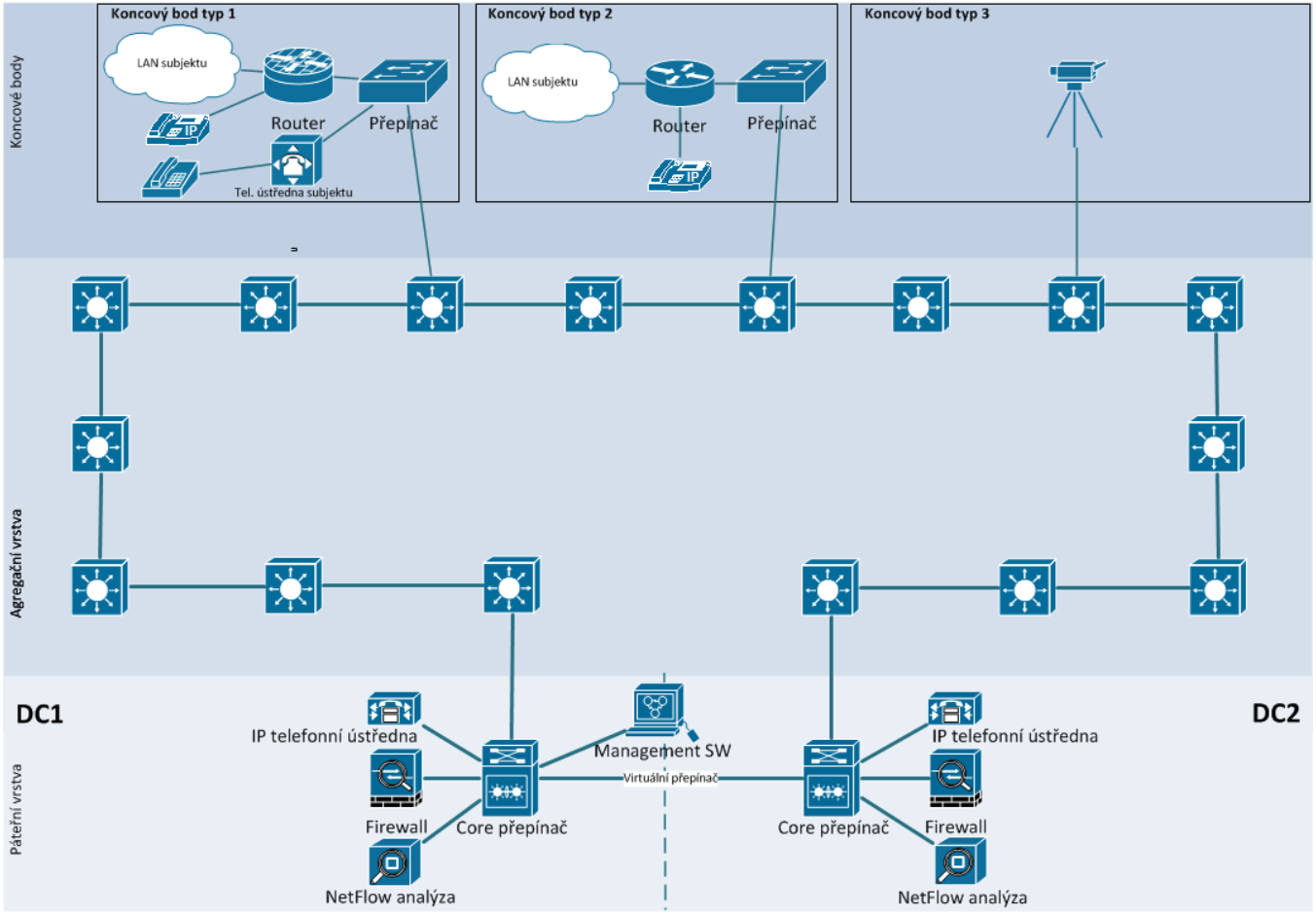
Hierarchie síťových uzlů - hvězda

- Core->Agregace->Přístupové body->Organizace



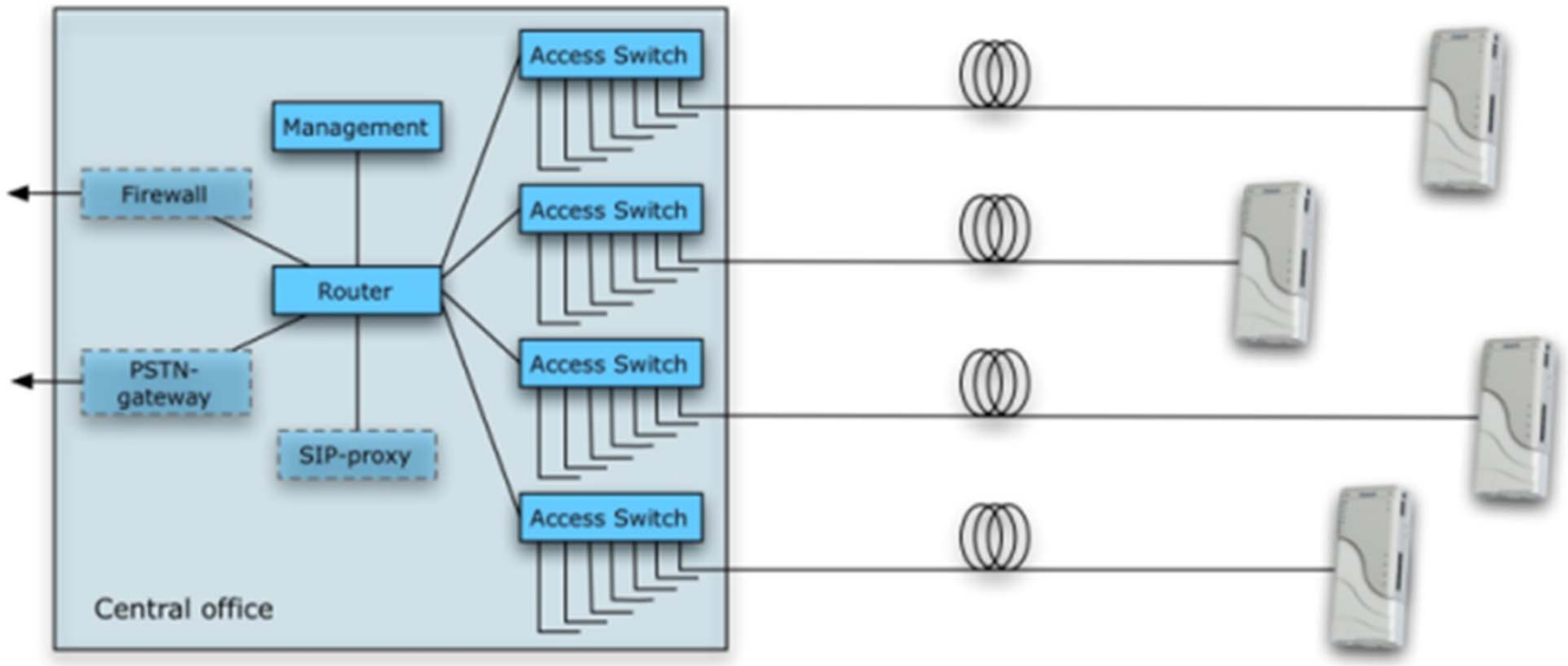
Hierarchie síťových uzlů - kruh

- Core->Agregace=Přístup->Organizace

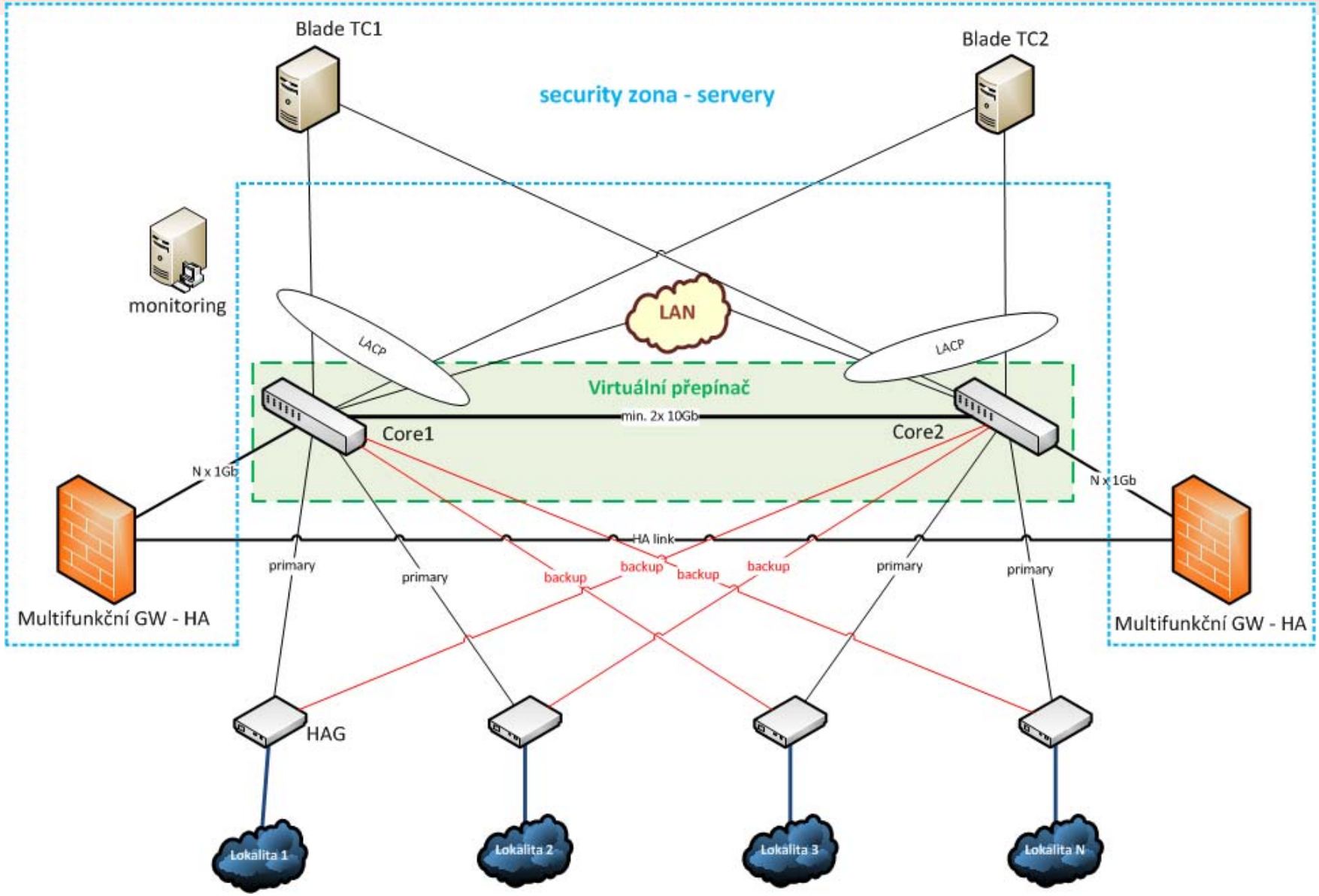


Menší MAN – analogie FTTH výstavby

- Komponenty řešení
  - multifunkční MAN GW
  - switch s SFP sloty
  - inteligentní CPE - HAG



Menší MAN – design AC řešení



Zavádíme a provozujeme užitečné informační technologie v organizacích.

AutoCont

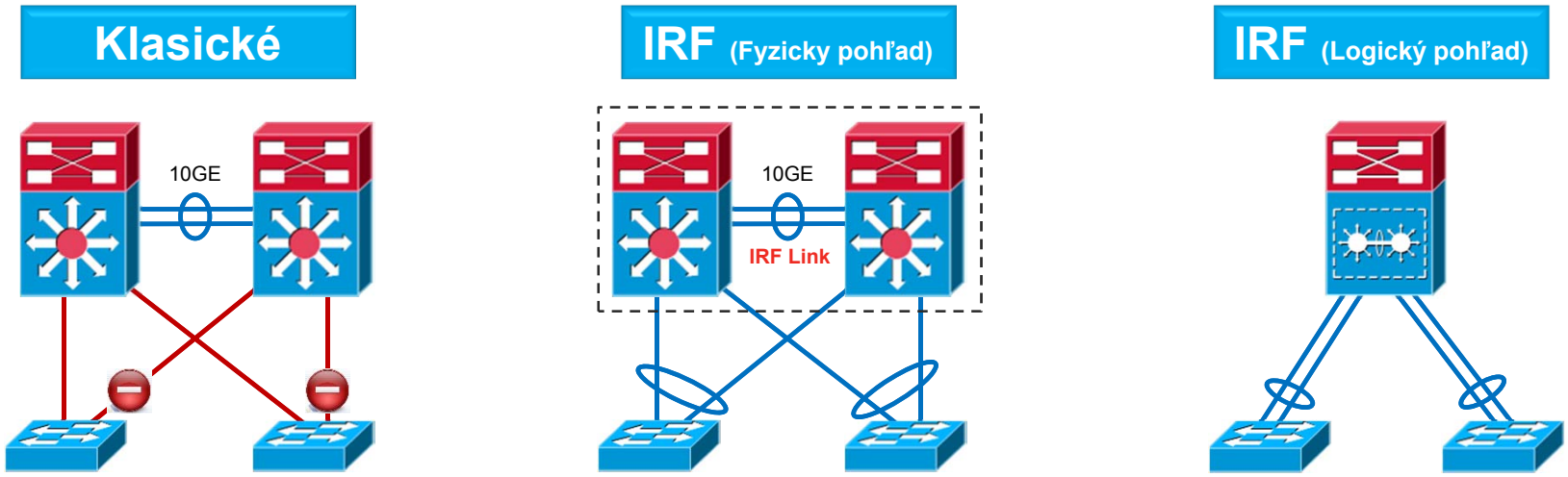
Menší MAN - HAG

- Požadované vlastnosti
  - Gigabitový směrovač
  - 1x 1Gb WDM optický uplinkové port
  - minimálně 4x 1Gb UTP integovaný přepínač
  - podpora NAT a firewall s line rate prpustností (min. 1Gbps)
  - podpora VLAN na integrovaném přepínači
  - podpora směrování (IPv4 a IPv6),
  - podpora volitelných VOIP (SIP) a WIFI modulů (802.11a/b/g/n)
  - diferencovaná obsluha (QoS) podle L2/3/4 atributů, min. 4 HW fronty
  - klasifikace a reklasifikace (Ethernet CoS, IP DSCP/ToS)
  - management pomocí SNMP v1/v2 včetně MIB-II , TR-069

Centrální Switch – L2 logika sítě

- 24x SFP GE, 4x SFP+ 10GE
- Rozšiřující slot
- Výměna komponent za chodu
- 208 Gbps R&S kapacita
- Propustnost 155 Mpps
- IRF stack

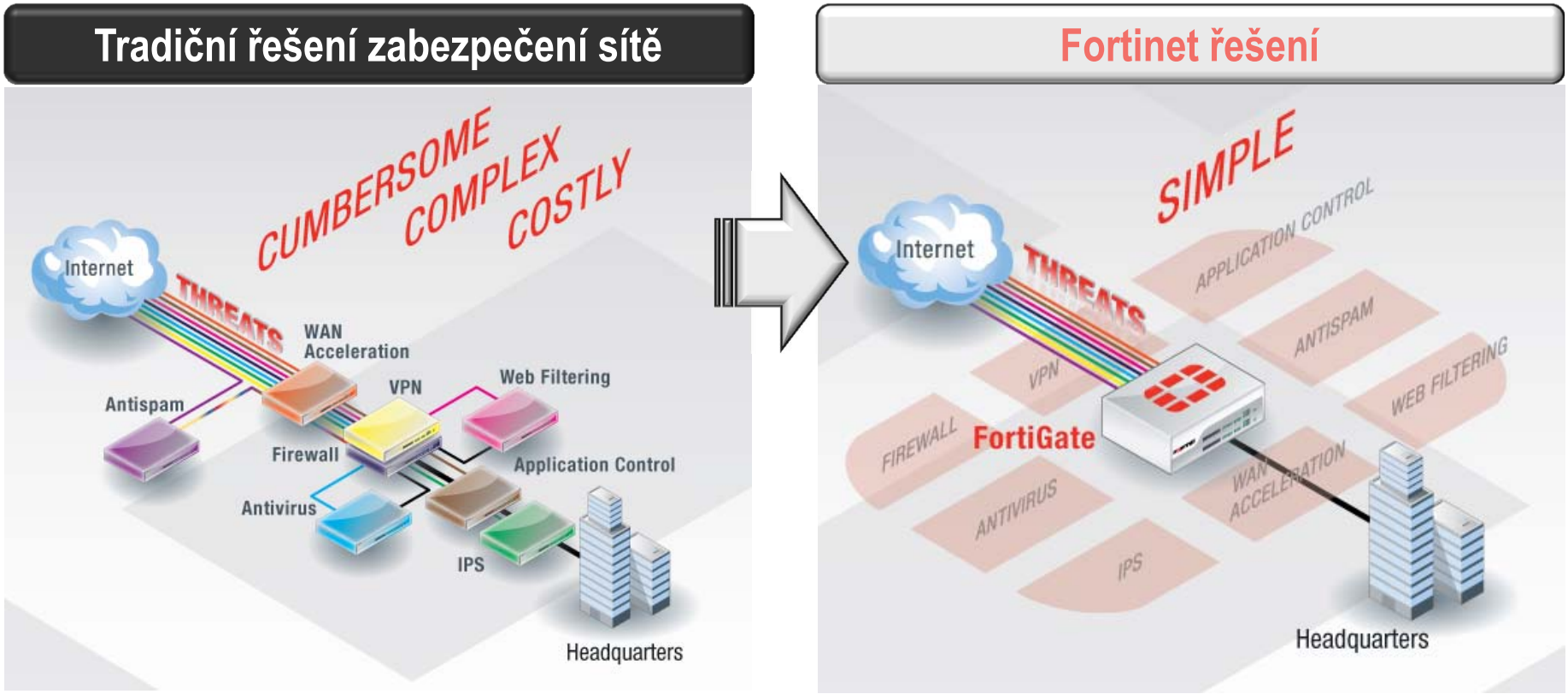
IRF – Intelligent Resilient Framework



- Zjednodušuje manažment zjednotením oboch zariadení do jedného logického celku,
- Topológia bez šmyčiek, minimalizácia závislosti na STP
- Zvyšuje kapacitu pomocou Active-Active Multi-Chassis Etherchannel (LACP/static)
- žiadne blokované porty kvôli Spanning Tree
- Minimalizuje čas konvergencie pri výpadku switchu alebo linky vďaka deterministickému menej ako sekundu trvajúcemu zotaveniu

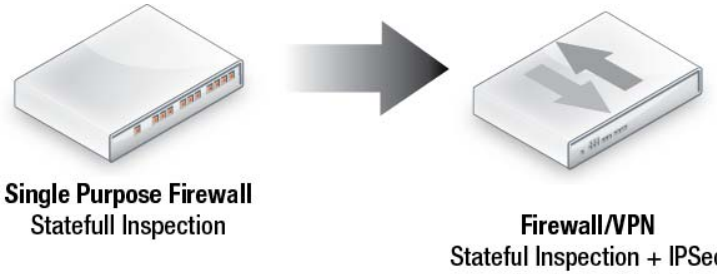
Multifunkční MAN Gateway

- Klíčová role je – bezpečnostní hranice

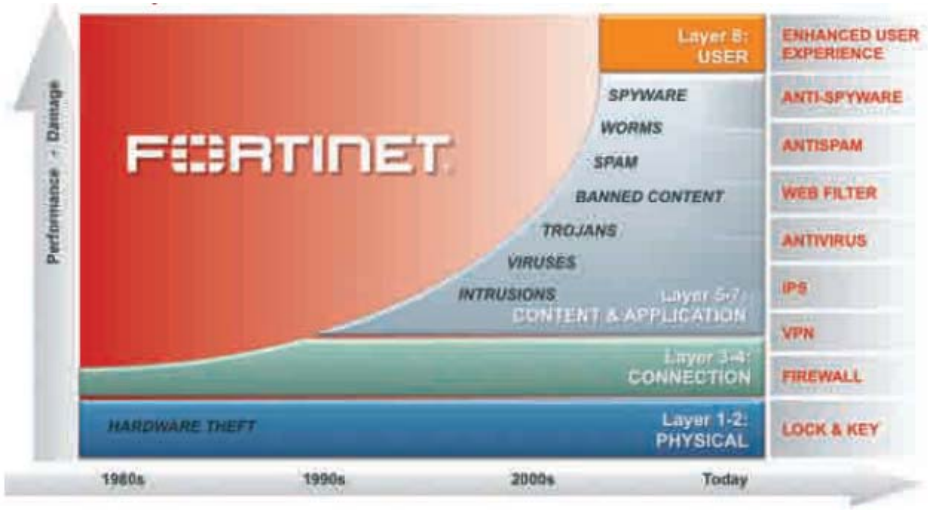


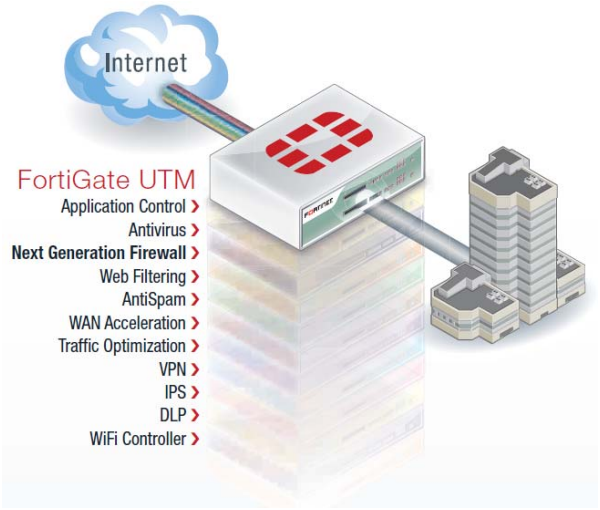
Vývoj nároků na multifunkční GW

- **Klasické vnímání**

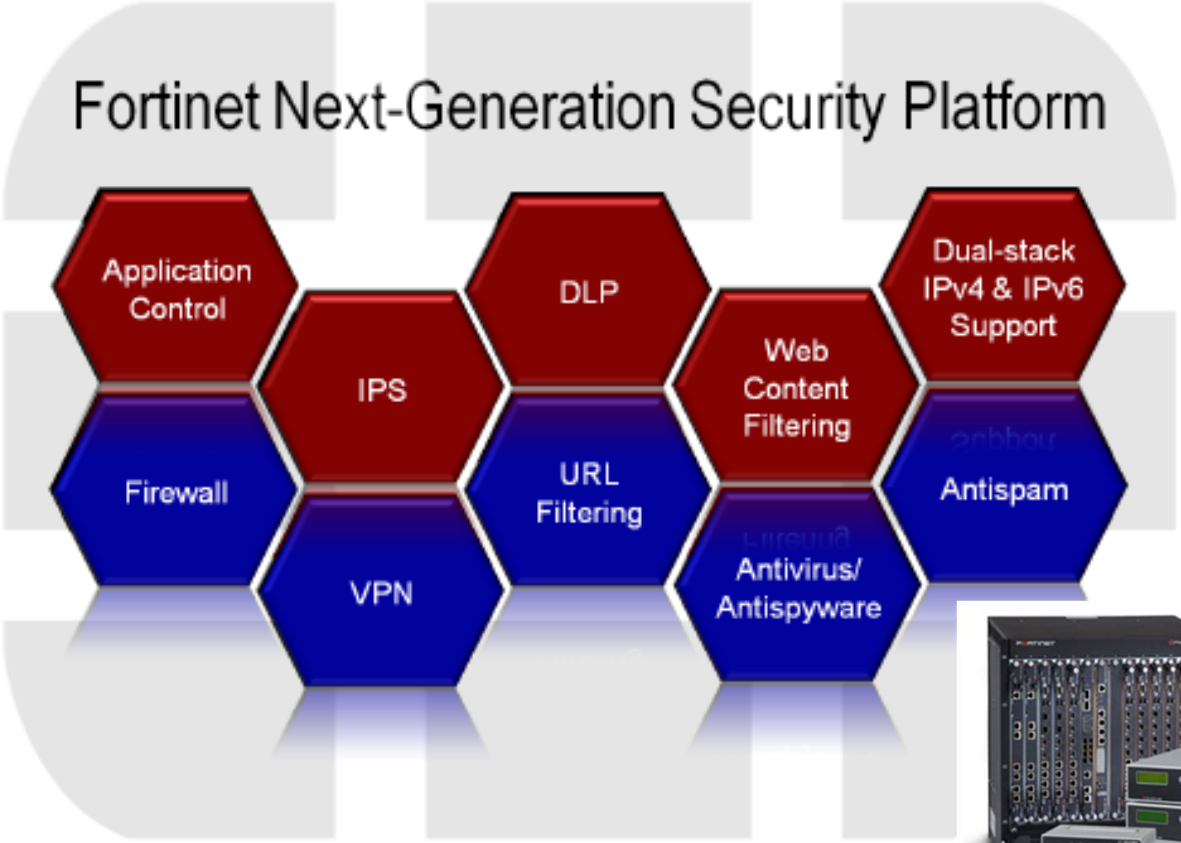


- **Posun vnímaní od „Connection“ kontroly směrem ke „Content- Base“**

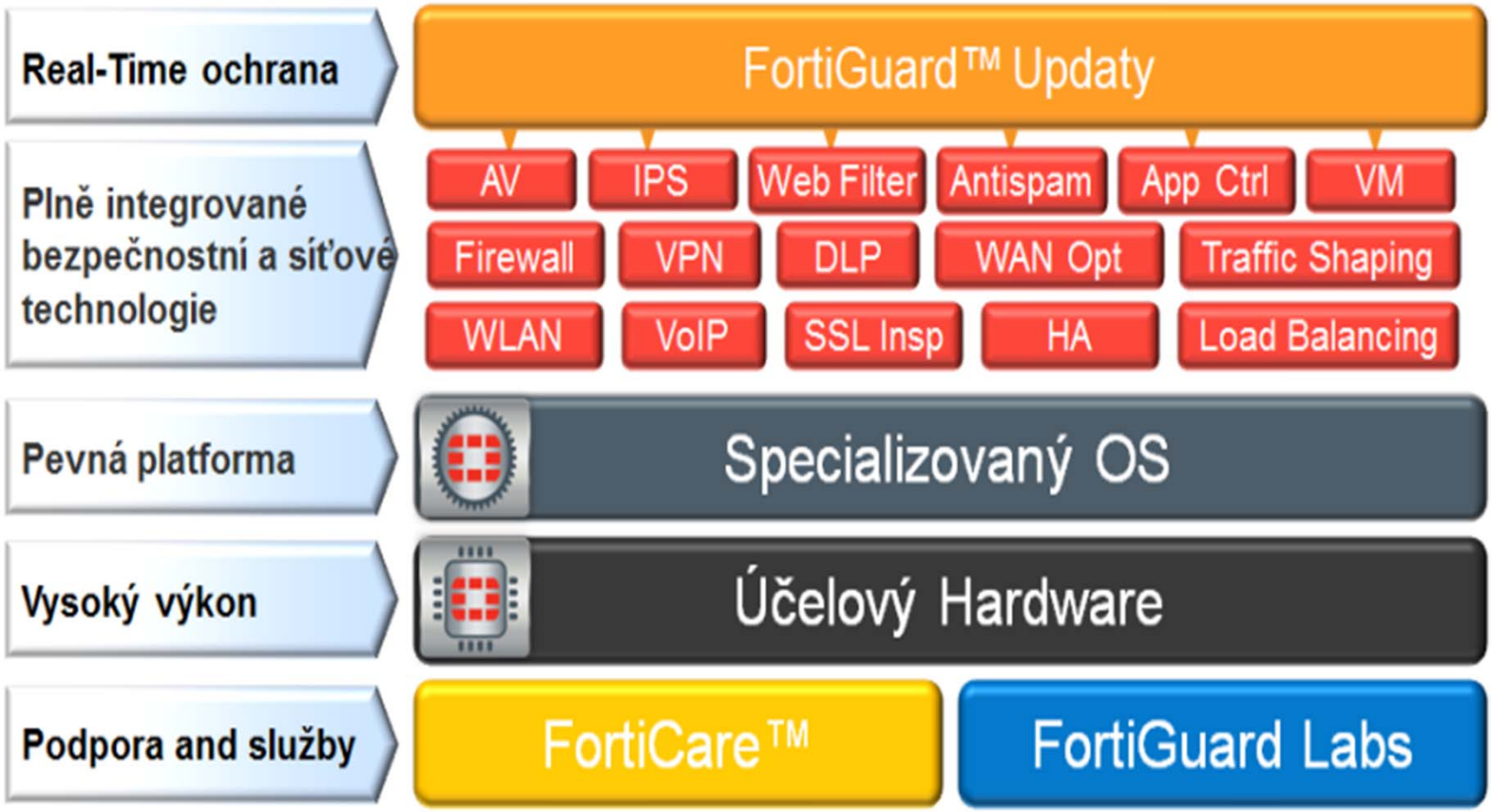




FortiGate – konsolidovaná bezpečnost



FortiGate – 3 klíčové pilíře



FortiOS – specializovaný OS

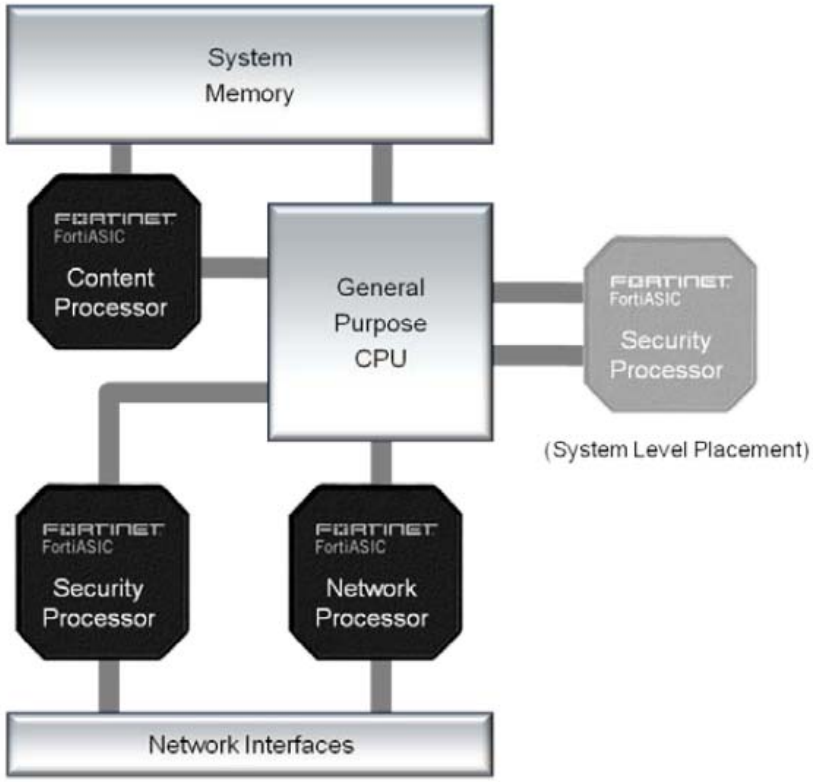
- Firewall, VPN , Traffic Shaping
- Intrusion Prevention System IPS
- Antivirus, Antispyware, Antimalware
- Web Filtering (kontrola webového obsahu)
- Antispam
- Application Control (např. IM, P2P sítě)
- podpora VoIP (H.323 a SCCP)
- směrování na 2/3 vrstvě
- FSAE (aktivní ověřování vůči MS AD)
- Dual WAN
- WAN optimization
- Network Access Control NAC
- High Availability
- Virtual Domain VDOM
- Wireless Controller

FortiOS – specializovaný OS

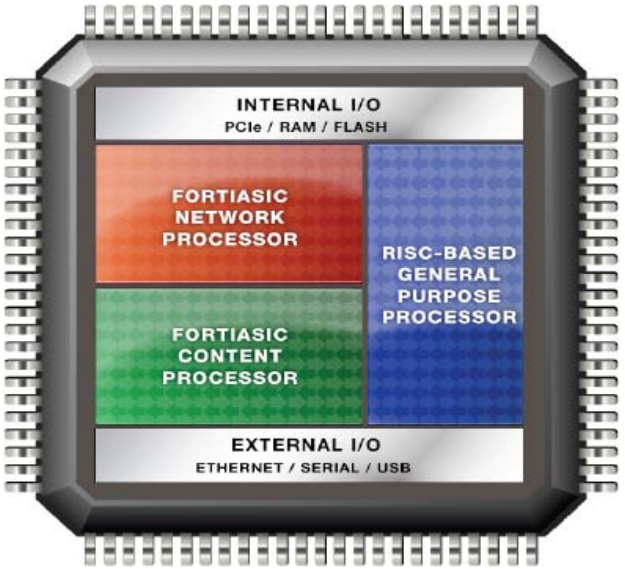
- Jediné místo pro inspekci paketů
- Jediná konzole pro správu všech integrovaných bezpečnostních technologií

FortiASIC – účelový HW

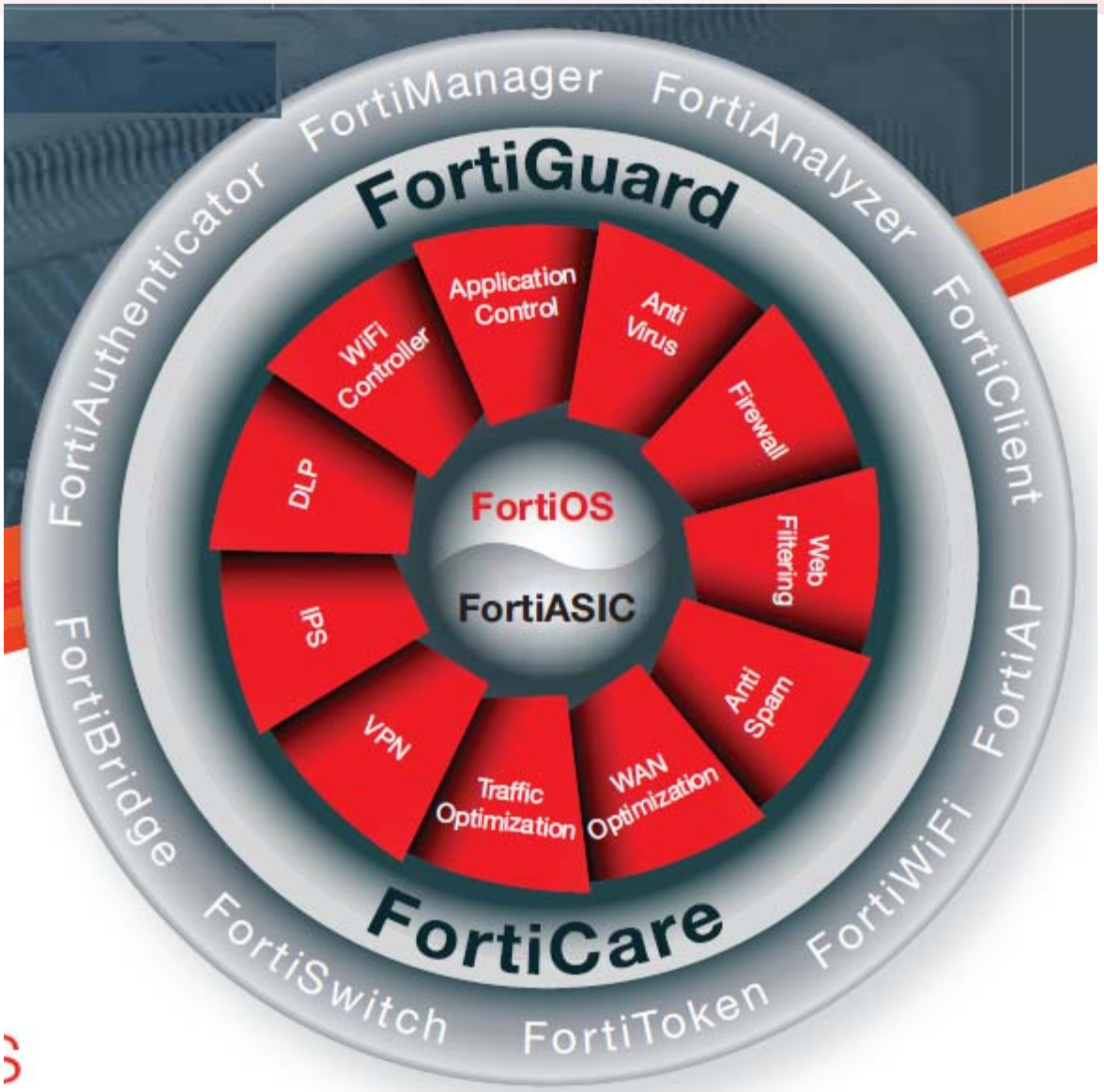
- **Architektura**



- **Provedení System-on-a-chip**



Rozdělení SW a HW řešení služeb



Alternativní technologie výstavby - PON

- Základní srovnání PON a AON

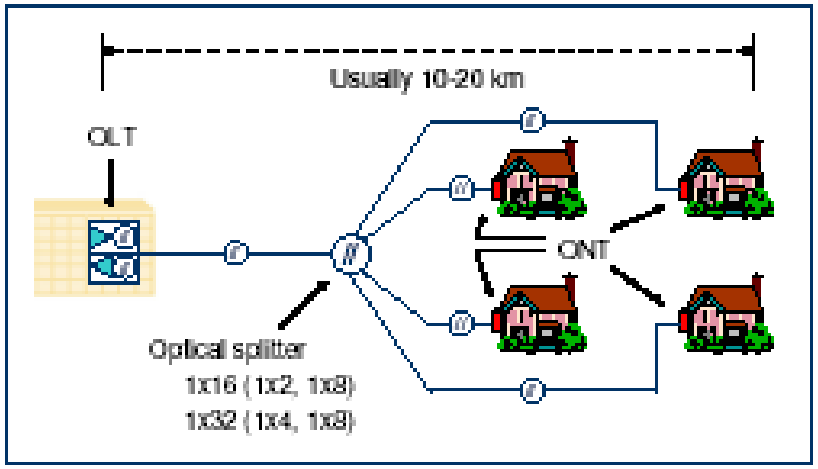


Figure 1: PON Architecture

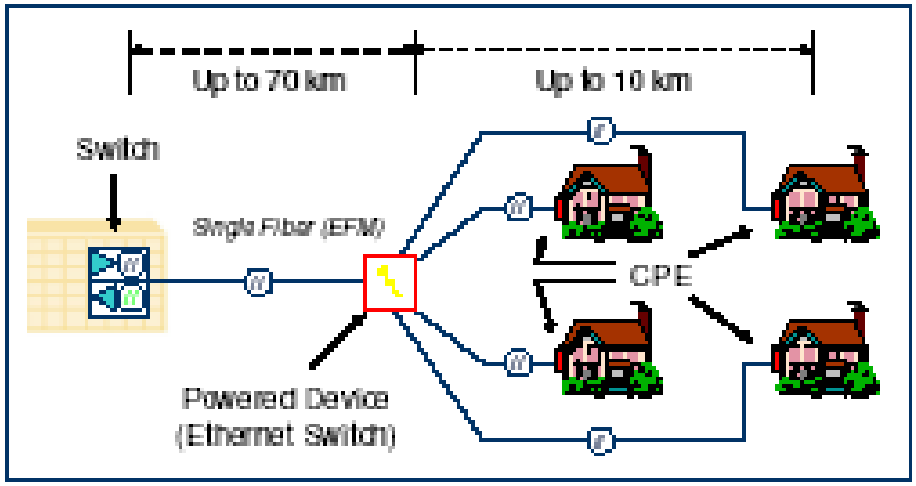


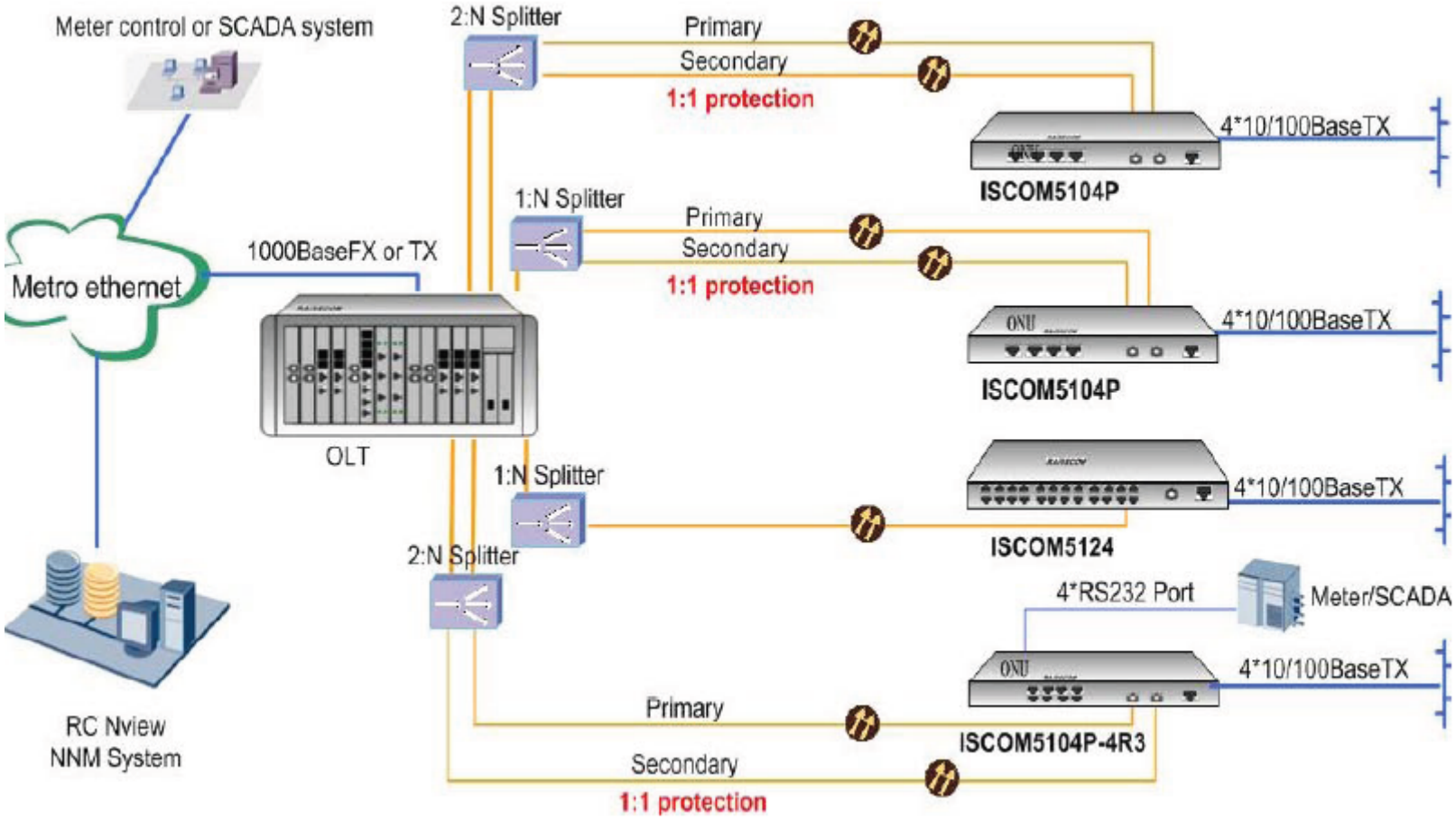
Figure 2: Active Architecture

- **P2MP** – point to multipoint connection
- **OLT** – optical line terminal
- **ONT (U)** – optical network terminal (unit)
- shared bandwidth
- distance 10 – 20 km

- **P2P** – point to point connection
- Ethernet device – in the field
- dedicated, full bi-directional bandwidth
- distance – up to 80 (120) km

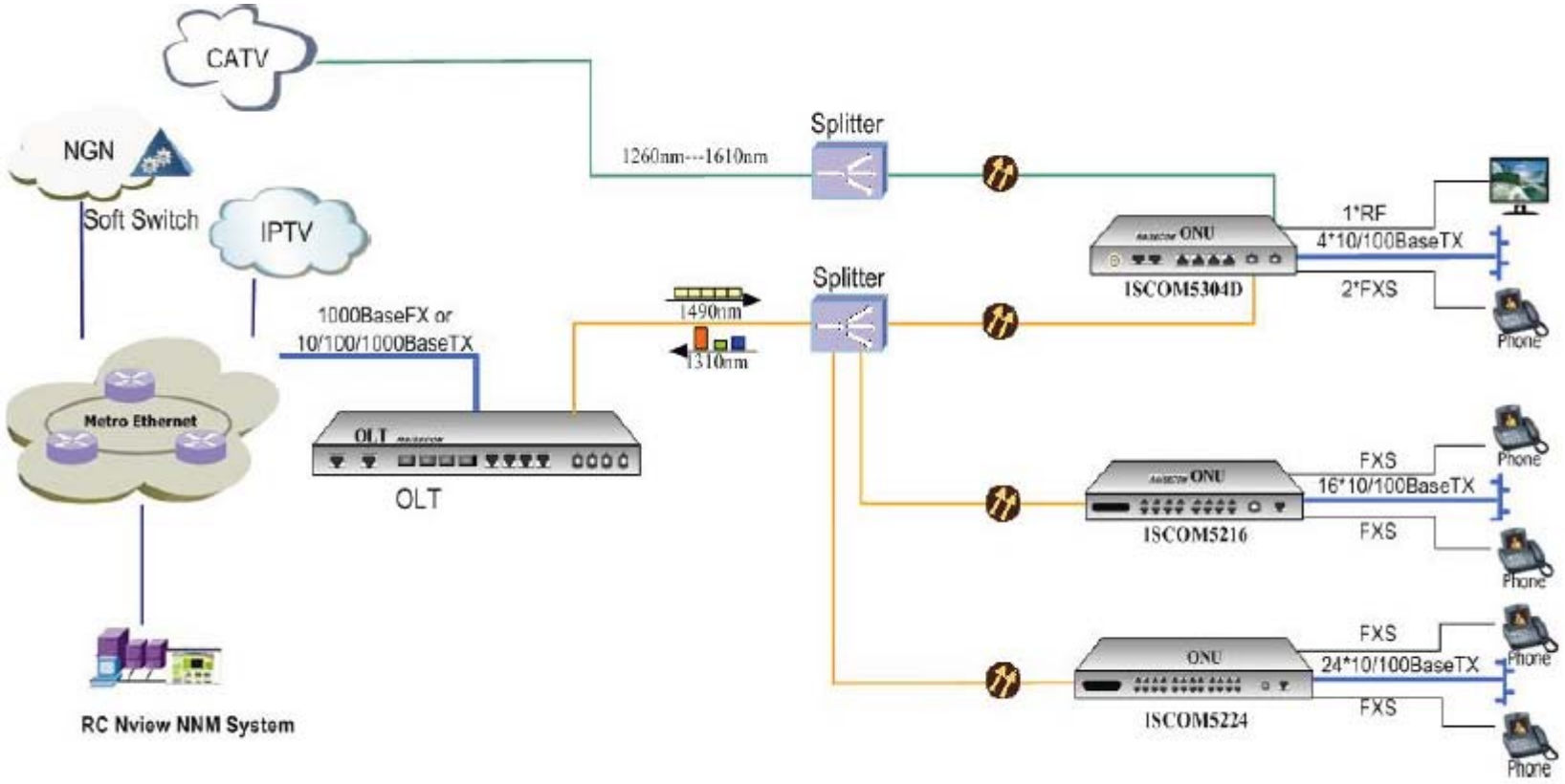
Alternativní technologie výstavby - PON

- Redundance v PON sítích – konečně !!!



Alternativní technologie výstavby - PON

- Další možnosti – CATV…



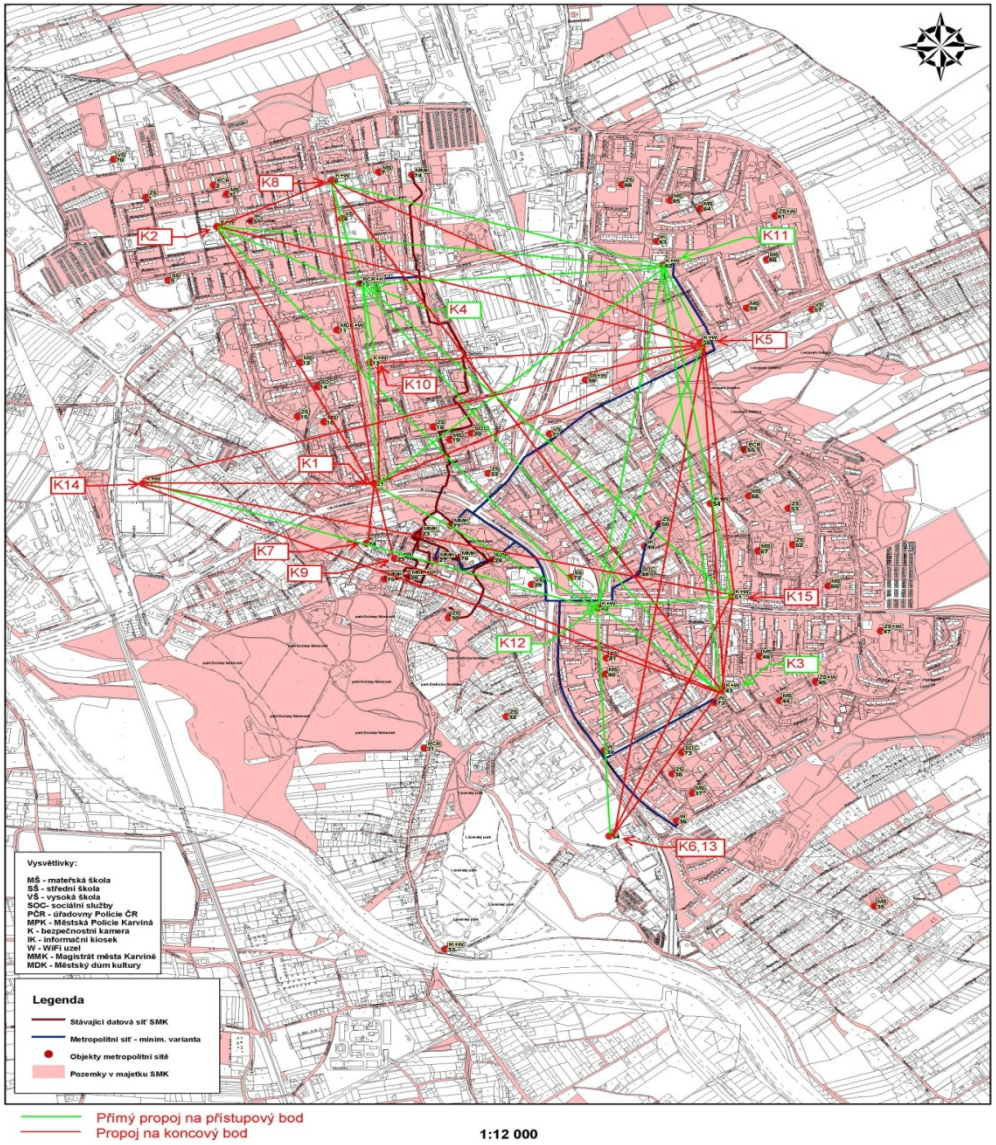
Alternativní technologie výstavby - WiMAX

- WiMAX
  - Provoz v licencovaném pásmu 3,5 GHz
  - Není nutná přímá viditelnost
  - Zabudovaný QoS
  - Asymetrická propustnost 30Mb/5Mb na sektor
  - Mobilní klientské jednotky

Alternativní technologie výstavby – WiFi MESH

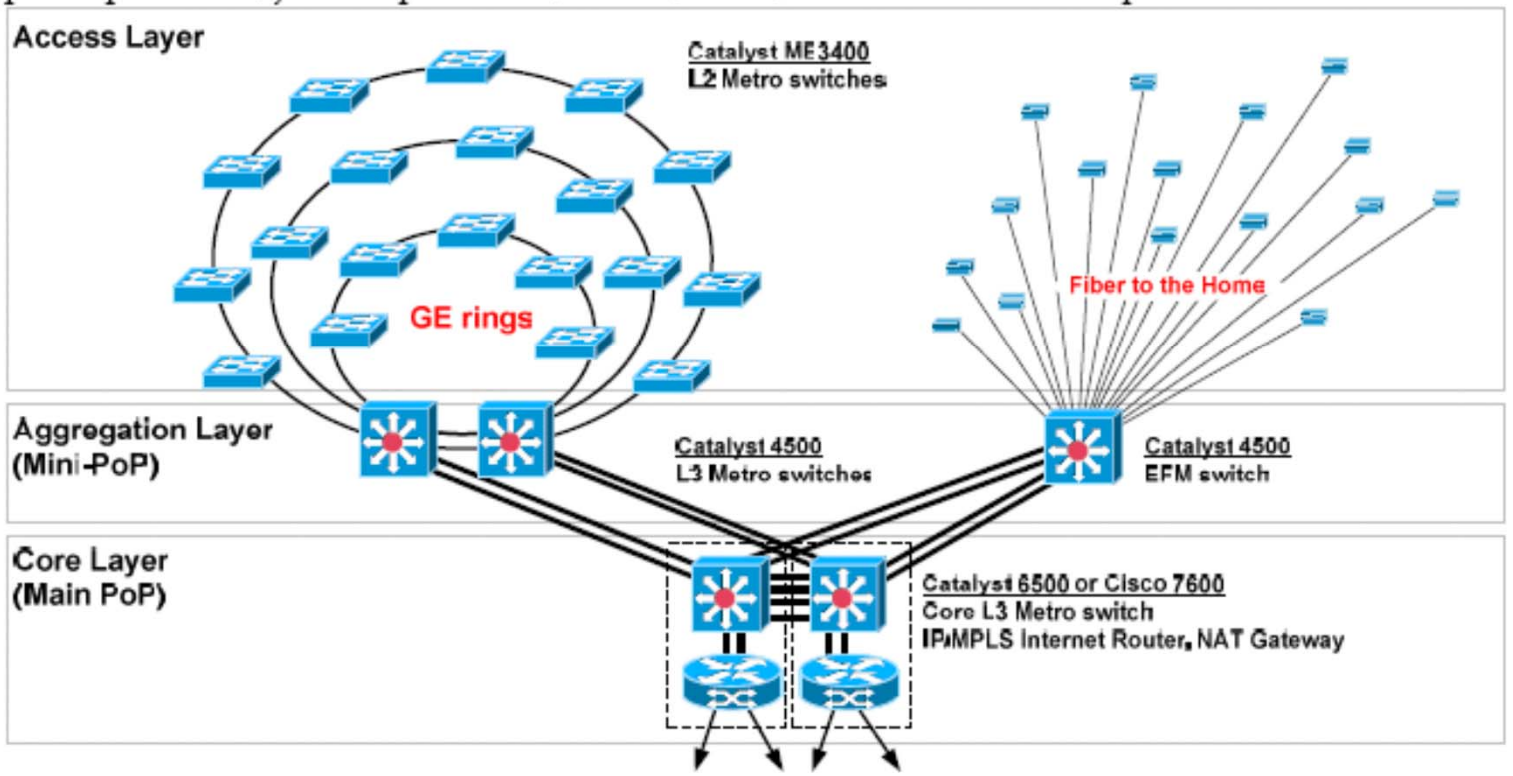
- WiFi MESH
  - Pásma 5GHz pro backbone a 2,4GHz pro klienty
  - Není nutné pevné připojení každého AP
  - AP tvoří full mesh propojení mezi sebou
  - Nutná přímá viditelnost
  - Odolnost proti rušení
  - Možné pro bezdrátové klienty i jako bridge

Ukázky možných topologií – WiFi MESH



Kombinace různých přístupových sítí

Agregační vrstva pracuje na L3, tedy na IP a je možno sem připojovat různé další přístupové sítě, jako např. FTTH, VDSL, WiFi, Ethernet-DSLAM apod.



Q&A

víme jak

Námi navržené a vybudované sítě

VÁS UDRŽÍ !!!

AutoCont

Petr Vejmělek
manažer OC
+420 724 263 249
petr.vejmelek@autocont.cz