Segmentace datové sítě

Ing. Martin Štrof, SUDOP PRAHA

AGENDA

- Základy síťové bezpečnosti
- Segmentace datové sítě
- Úrovně segmentace provozu sítě
- Rozdělení segmentů, pravidla pro definování
- Segmentace datové sítě a bezpečnost

Datová síť

- Rozdělení datové sítě:
  - IT (zde se preferuje spíše bezpečnost)
  - OT (zde se preferuje spíše funkčnost)

- Cílem každé datové sítě je: ….
  - Co nejefektivněji využívat dostupnou přenosovou kapacitu datové sítě tak, aby se jednotlivé přenosy navzájem co nejméně ovlivňovali.
  - Dosahovat co nejvyšší propustnosti datové sítě a co nejefektivněji využít dostupnou infrastrukturu.
  - Provádět řízení politiky datové sítě.

Základy síťové bezpečnosti

- Síťová bezpečnost je jakákoli činnost, jejímž účelem je zachovávat použitelnost a integritu sítě a dat.

  - Řízení přístupu
  - Software na ochranu proti virům a malwaru
  - Bezpečnost aplikací
  - Behaviorální analýza
  - Prevence ztráty dat
  - Emailová bezpečnost
  - Firewally
  - Systémy pro prevenci průniku
  - Bezpečnost mobilních zařízení
  - **Segmentace datové sítě**
  - VPN
  - Webová bezpečnost
  - Zabezpečení bezdrátových sítí

Základy síťové bezpečnosti

- Otevřená a nesegmentovaná datová síť přímo nahrává kybernetickým útokům
- Nesegmentovanou datovou síť neohrožují pouze externí hrozby, ale bez oddělení provozu jednotlivých sítí a omezení představují vysoké potenciální riziko i interní hrozby

Segmentace datové sítě

- Rozděluje datový provoz do různých kategorií (menších logických celků) a usnadňuje uplatňování bezpečnostních pravidel (vytvářet bezpečnostní zóny podle definovaných parametrů) a omezit bezpečnostní hrozby
- Segmentací datové sítě a nastavením příslušných pravidel bude možné zpřístupnit data, činnosti a aplikace, pouze konkrétním subjektům, zaměstnancům apod..
- Přístupová práva lze přidělit podle role, umístění a dalších atributů, aby správní uživatelé měli správná oprávnění a podezřelá zařízení byla izolována a uvedena do řádného stavu.

Segmentace datové sítě

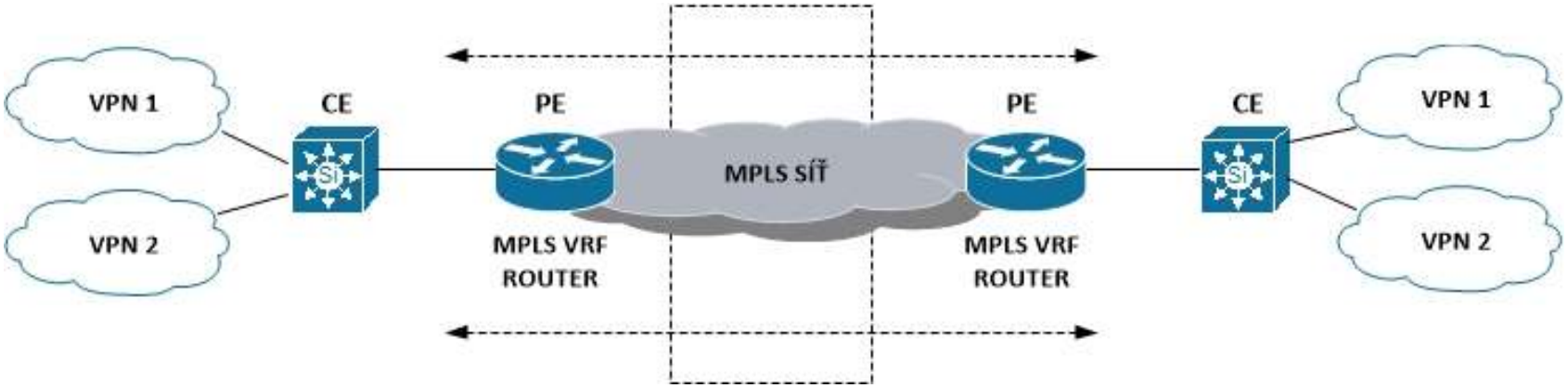
- Segmentace provozu datové sítě se realizuje pomocí VLAN a VRF/VPN

VLAN–Virtual LAN

VRF–Virtual Routing and Forwarding

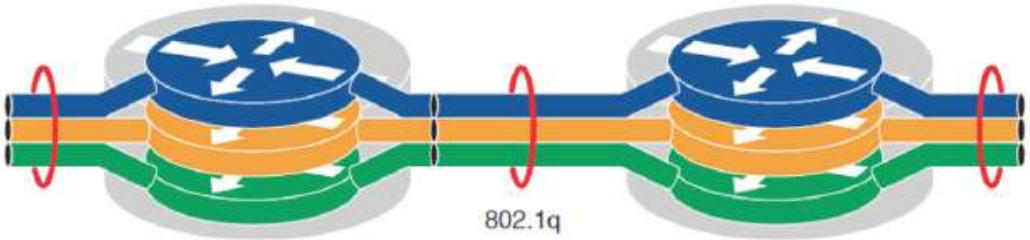
Segmentace datové sítě

- Pro vytváření a provozování bezpečně oddělených a nezávislých VPN pracujících na L2 nebo L3 vrstvě modelu ISO/OSI se používá technologie MPLS

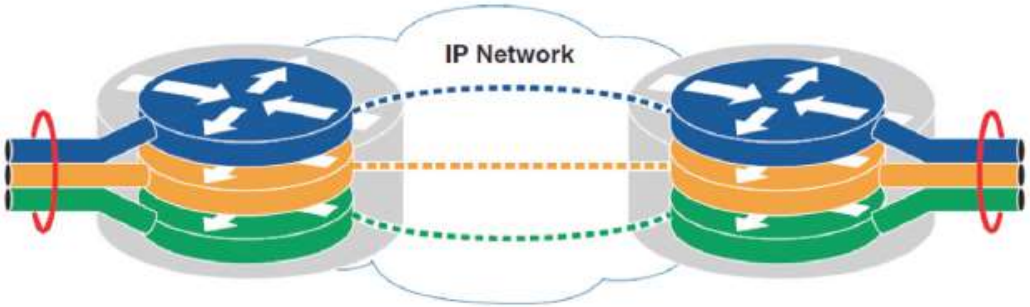


Segmentace datové sítě

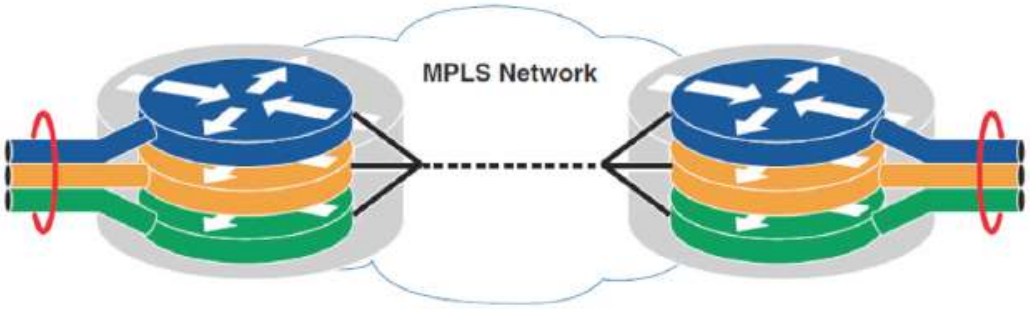
Hop-by-Hop
- VRF-Lite
- 802.1Q trunks



Multi-Hop
- VRF-Lite
- GRE tunnels



Multi-Hop
- MPLS (L3VPN)
- Label Distribution Protocol
- L3 multiprotocol routing



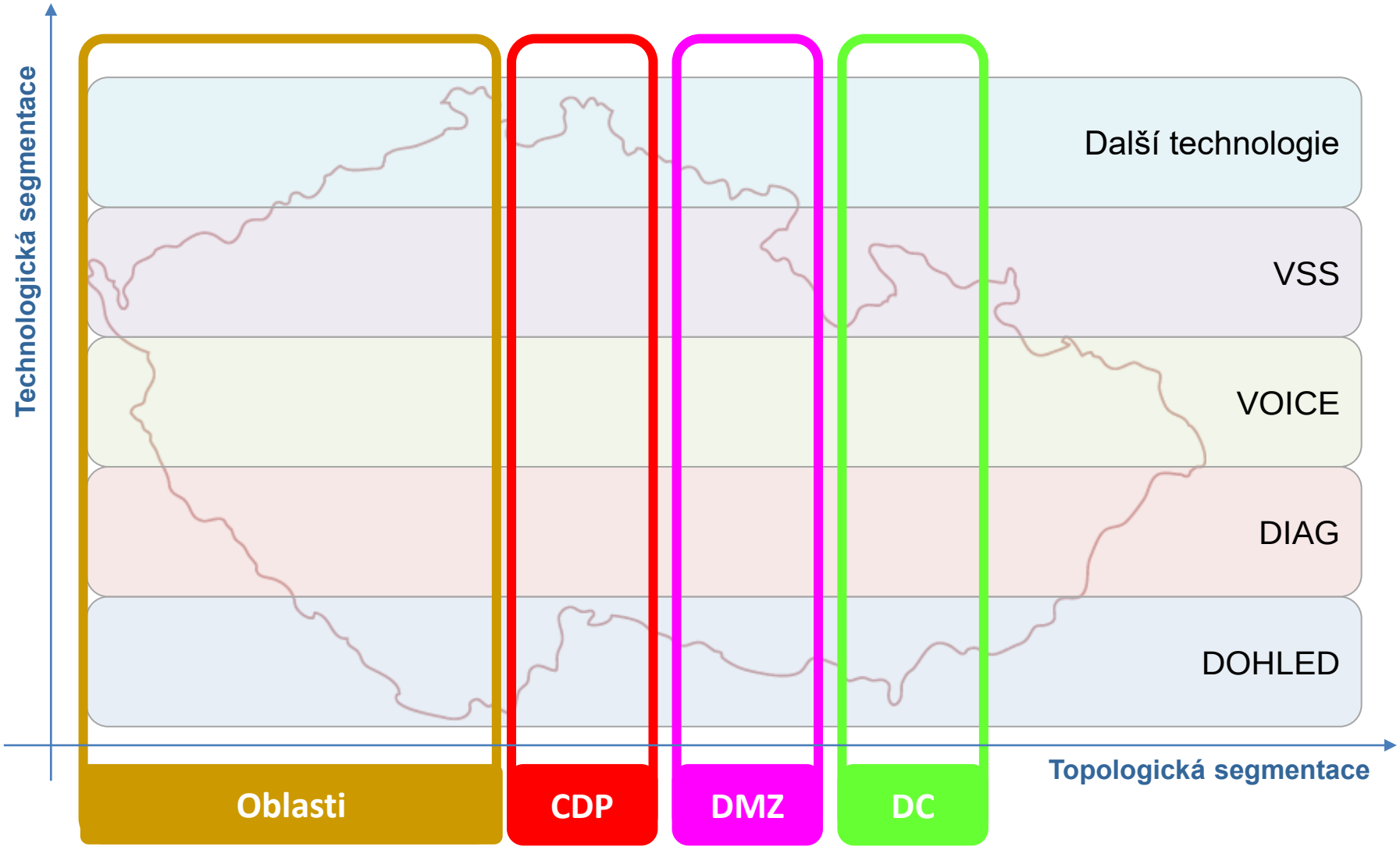
Segmentace datové sítě

- Segmentace datové sítě zajistí využití datové a přenosové infrastruktury pro N (N > 15) logických sítí, které mohou být nad fyzickou infrastrukturou libovolně definovány
- Pro každou novou síť – segment není potřeba vybudovat novou infrastrukturu, pouze se doplní a vyčlení prostředky stávající infrastruktury dle požadavků na nový segment (VRF)

Úrovně segmentace datové sítě

- Využitelné úrovně (metody) segmentace:
  - Zabránění zařízení v určitých sítích VLAN, aby komunikovala se zařízeními v ostatních sítích VLAN
  - Přepínače nebo směrovače s bezpečnostními a filtrovacími funkcemi na úrovni třetí vrstvy
  - Demilitarizovaná zóna (DMZ)
  - Access control lists (ACL)
  - Firewally
  - Systém pro odhalení průniku (IDS)

Rozdělení segmentů, pravidla definování



Rozdělení segmentů, pravidla definování

- Pravidla pro definování segmentů dle typu provozu:
  - Segment je určen typem provozu, resp. technologií která se má v daném segmentu VPN/VRF oddělit.
  - Číslo, resp. název segmentu je stejný pro páteřní i oblastní (např. OŘ) část datové sítě.
- Pravidla pro definování segmentů dle geografického umístění:
  - Příslušnost k oblasti (OŘ) je dána geografickým umístěním zařízení, portu nebo dedikováním zařízení pro danou oblast
  - VRF jsou definovány pro jednotlivé oblasti, případně další lokality např. CDP, DC atp. dle současných, resp. budoucích požadavků.
  - Při přechodu datového spoje mezi různými oblastmi (OŘ) je třeba dodržovat příslušnost k dané oblasti (OŘ).

Rozdělení segmentů, pravidla definování

- Segmenty podle geografického umístění
  - Podle oblastí
    - OŘ Praha
    - OŘ Plzeň
    - OŘ Ústí nad Labem
    - OŘ Hradec Králové
    - OŘ Brno
    - OŘ Olomouc
    - OŘ Ostrava
  - Specifické segmenty dle potřeby
    - CDP Praha
    - CDP Přerov
    - Datová Centra, apod.
  - Globální (páteřní síť) propojující oblasti

Segmentace datové sítě a bezpečnost

- Datová síť pokud zavedeme segmentaci je odolná proti bezpečnostním útokům. Ale nedílnou součástí musí být:
  - Robustní bezpečnostní mechanismy
  - Nástroje pro aktivní monitorování datových toků
  - Ochrana a kontrola přístupu na sdílené SW prostředky v síti
  - Možnost provádět řízení politiky sítě
  - FW s příslušnými funkcionalitami pro kontrolu a sledování provozu jak v oblasti, tak i mezi nimi

Závěr

- **Výhody a potřebnost segmentace datové sítě**
  - Síťový provoz pod kontrolou
  - Stabilní a zabezpečená datová síť
  - Rozčlenění datové sítě na menší a snadněji spravovatelné segmenty
  - Podrobné logování síťového provozu
  - Udělování práv k přístupu do jednotlivých segmentů
  - Možnost monitoringu připojení a odpojení včetně detekce podezřelého chování

Děkuji za pozornost …

SUDOP PRAHA a.s., Olšanská 1a, 130 80 Praha 3, **www.sudop.cz**