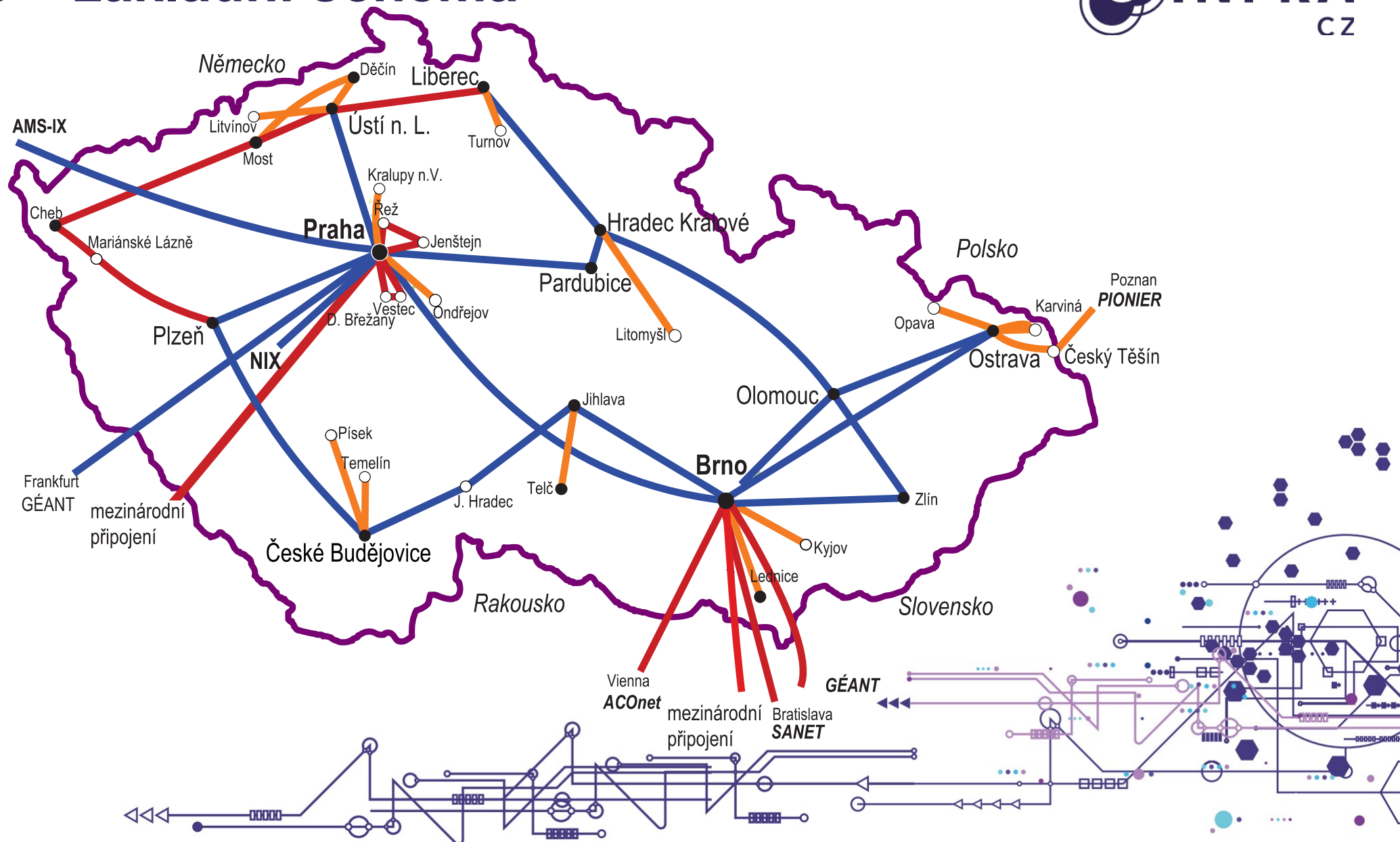


Síťová infrastruktura CESNET3

Jan Růžička, Václav Novák, Petr Adamec,
Radovan Igliar, Tomáš Košnar

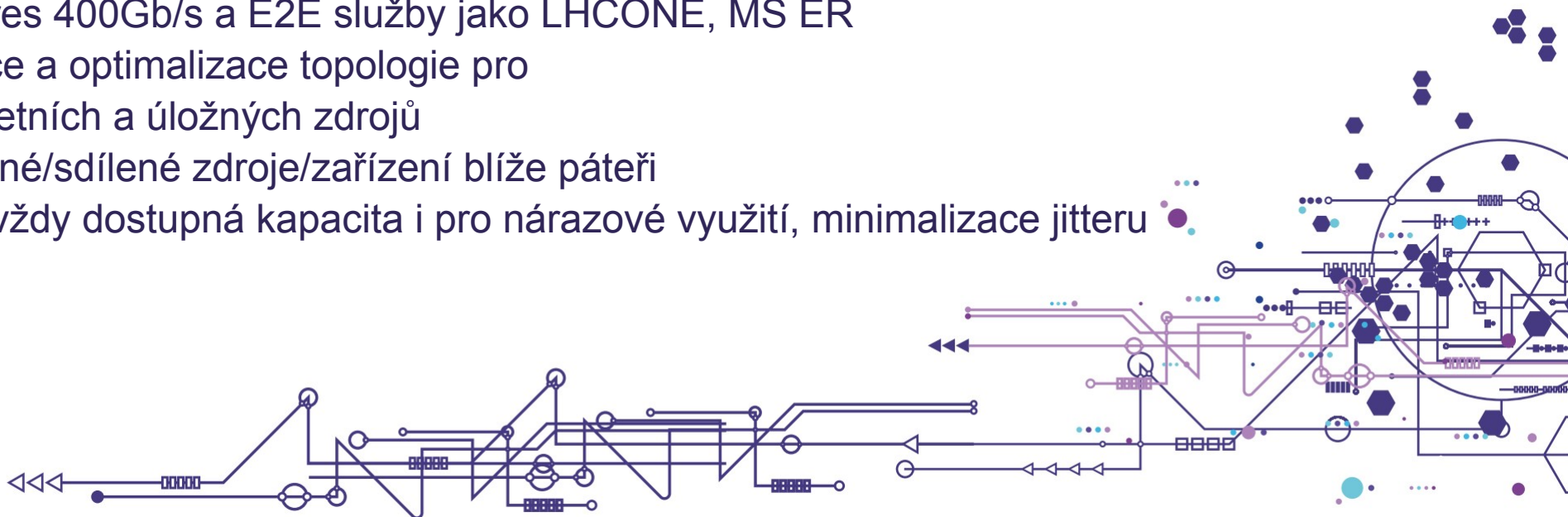
CESNET3 – základní schéma



CESNET3 – základní popis

Síťová část komplexní e-infrastruktury

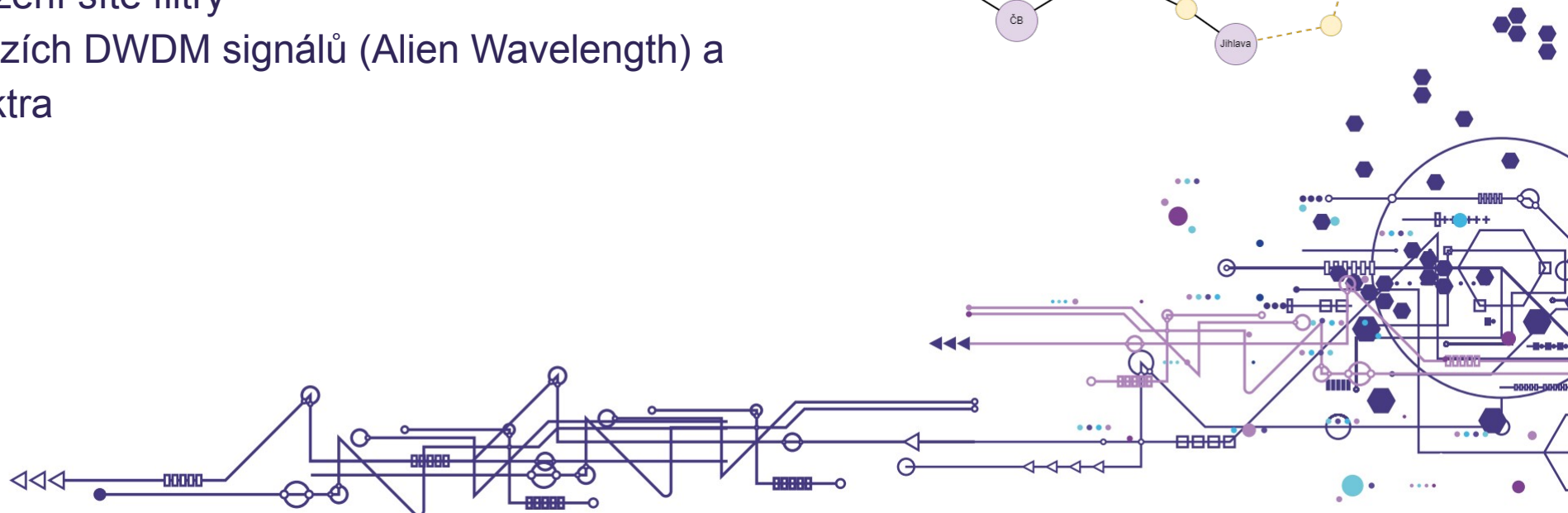
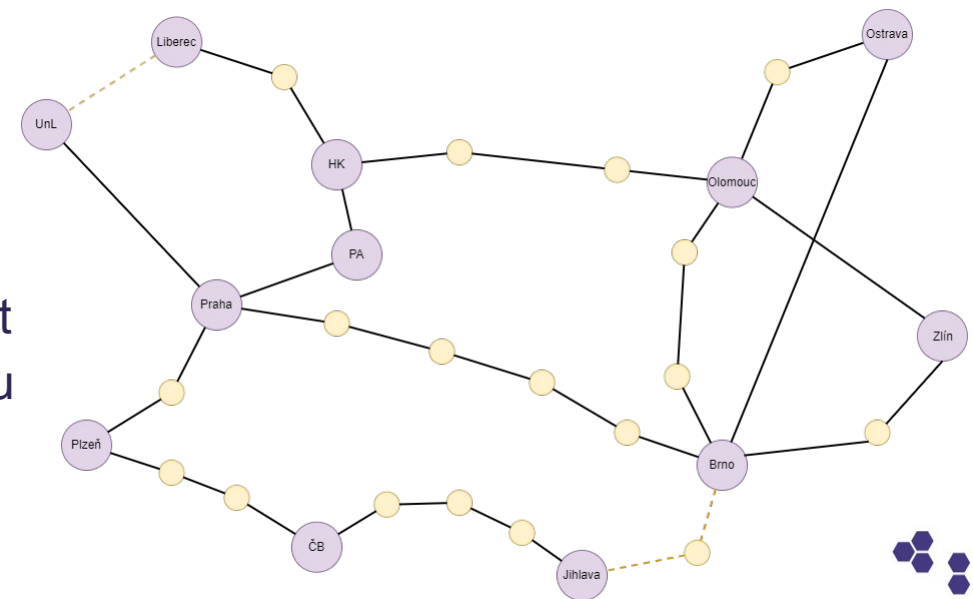
- Koncept tří vrstev pokračuje
 - Fyzická - více jak 6000 km vláken
 - DWDM - efektivní využití pronajatých vláken, optické kanaly přes více hopů
 - IP/MPLS
 - IPv4/v6 dual stack, unicast, multicast,
 - symetrické připojení s možností redundance
 - bez omezení legitimního provozu
- externí konektivita přes 400Gb/s a E2E služby jako LHCONE, MS ER
- specifické konfigurace a optimalizace topologie pro
 - propojení výpočetních a úložných zdrojů
 - specifické/náročné/sdílené zdroje/zařízení blíže páteři
- “over-provisioned” - vždy dostupná kapacita i pro nárazové využití, minimalizace jitteru



Páteří DWDM systém (FWDM0)

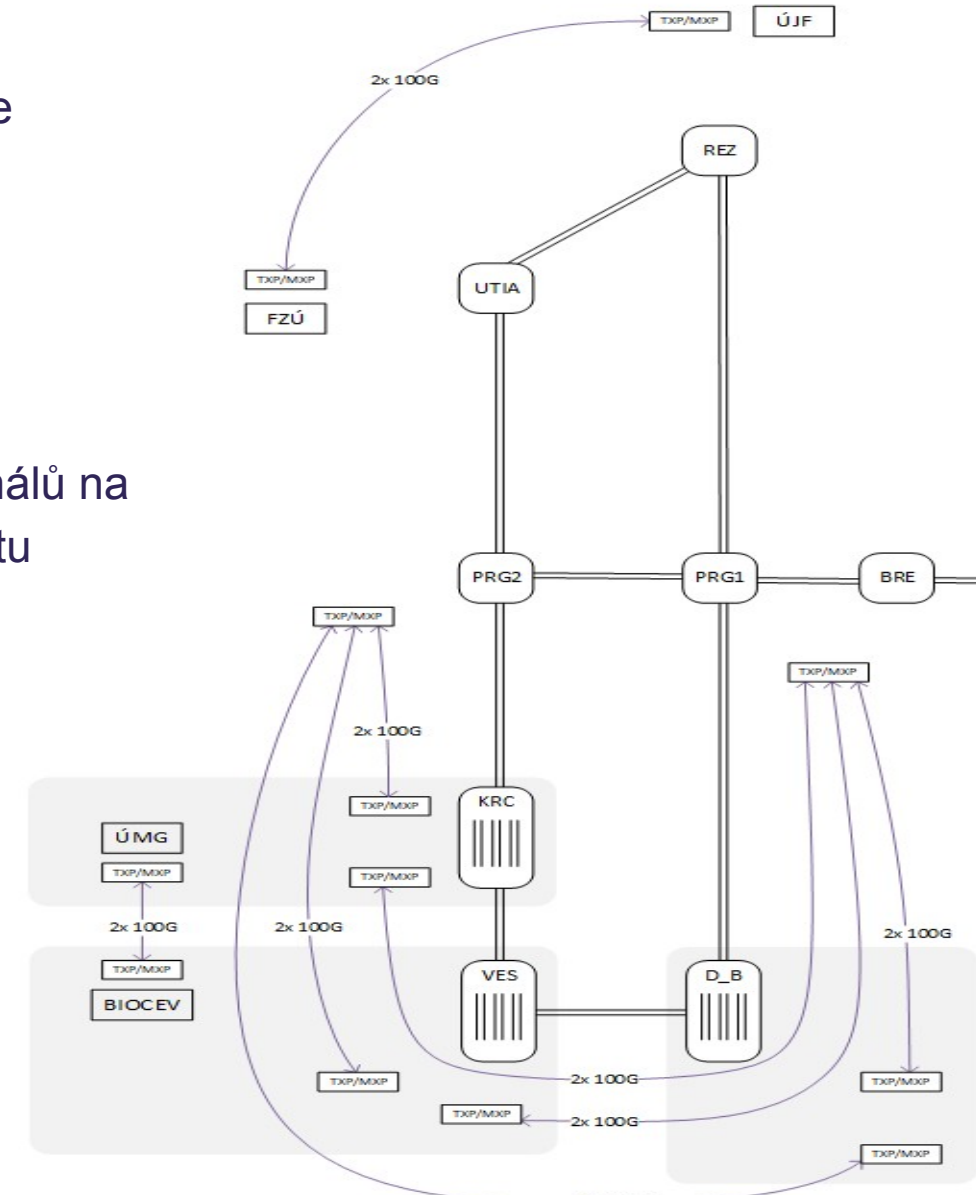
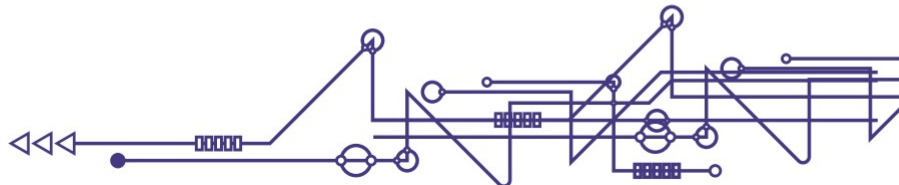
Flexgrid - flexibilní alokace přenosového pásma

- Podpora optických přenosových kanálů 100 Gb/s až 400Gb/s
 - Přes 1 Tb/s pomocí sdružených kanálů
 - Directionless - porty nejsou již vázány na konkrétní směr
 - Contentionless - připojení více zdrojů signálů na jeden port
 - Colorless - porty nejsou vázány jen na jednu vlnovou délku
- Podpora přenosu přesného času a frekvence a QKD klíčů v širším měřítku, osazení sítě filtry
- Podpora přenosu cizích DWDM signálů (Alien Wavelength) a sdílení DWDM spektra



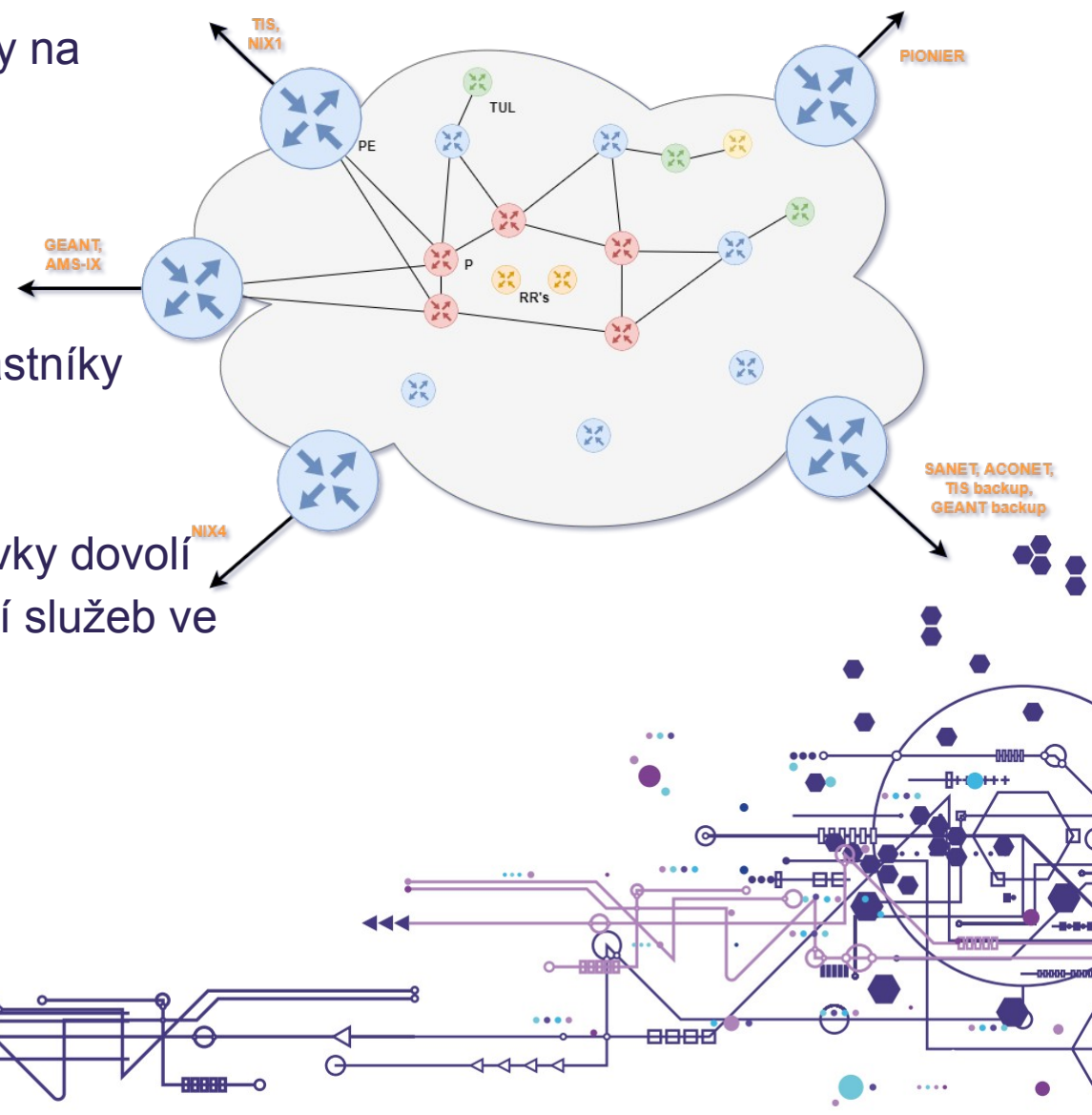
Přístupové části DWDM systému (FWDM1)

- Hlavně jde o významné lokality v okolí Prahy
 - lokality mimo páteřní DWDM síť s požadavky na transport více rychlých kanálů se zálohou
 - hostují významné zdroje - výpočetní a úložné kapacity a jsou významní producenti a konzumenti dat (např. LHCONe)
 - ELI Břežany, BIOCEV Vestec, UMG Krč, Slovanka, Rež
- Flexgrid technologie, kde je potřeba i Colorless a Directionless
- Transpondérové/muxpondérové řešení pro přebarvení DWDM signálů na univerzální šedé rozhraní s možností odstupňování rychlostí a počtu kanálů
- Podpora přenosu přesného času, frekvence a QKD



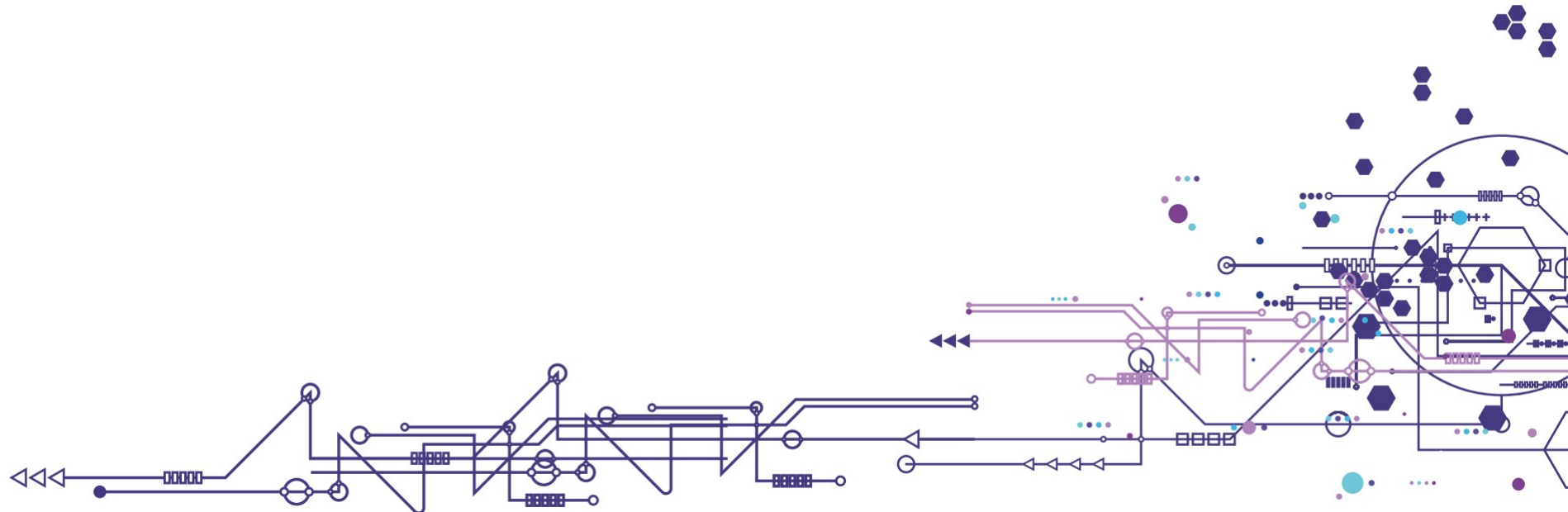
IP/MPLS

- Vyšší přenosové kapacity v jádru sítě s menšími nároky na prostor, spotřebu a chlazení
- Dostatek rychlých přístupových portů
 - 10GE/40GE/100GE, 1GE bude stále k dispozici
- Přechod na Segment Routing IPv6 (SRv6)
 - Unifikovaného prostředí pro služby koncových účastníků (např. pro propojení uzlů DÚ)
 - Nasazení SRv6 v plánu ke konci modernizace
- Streaming Telemetry jako náhrada SNMP, tak jak to prvky dovolí
- Využití automatizace pro jednodušší správu a zavádění služeb ve větším objemu
- Nová architektura uzlu
- Migrace

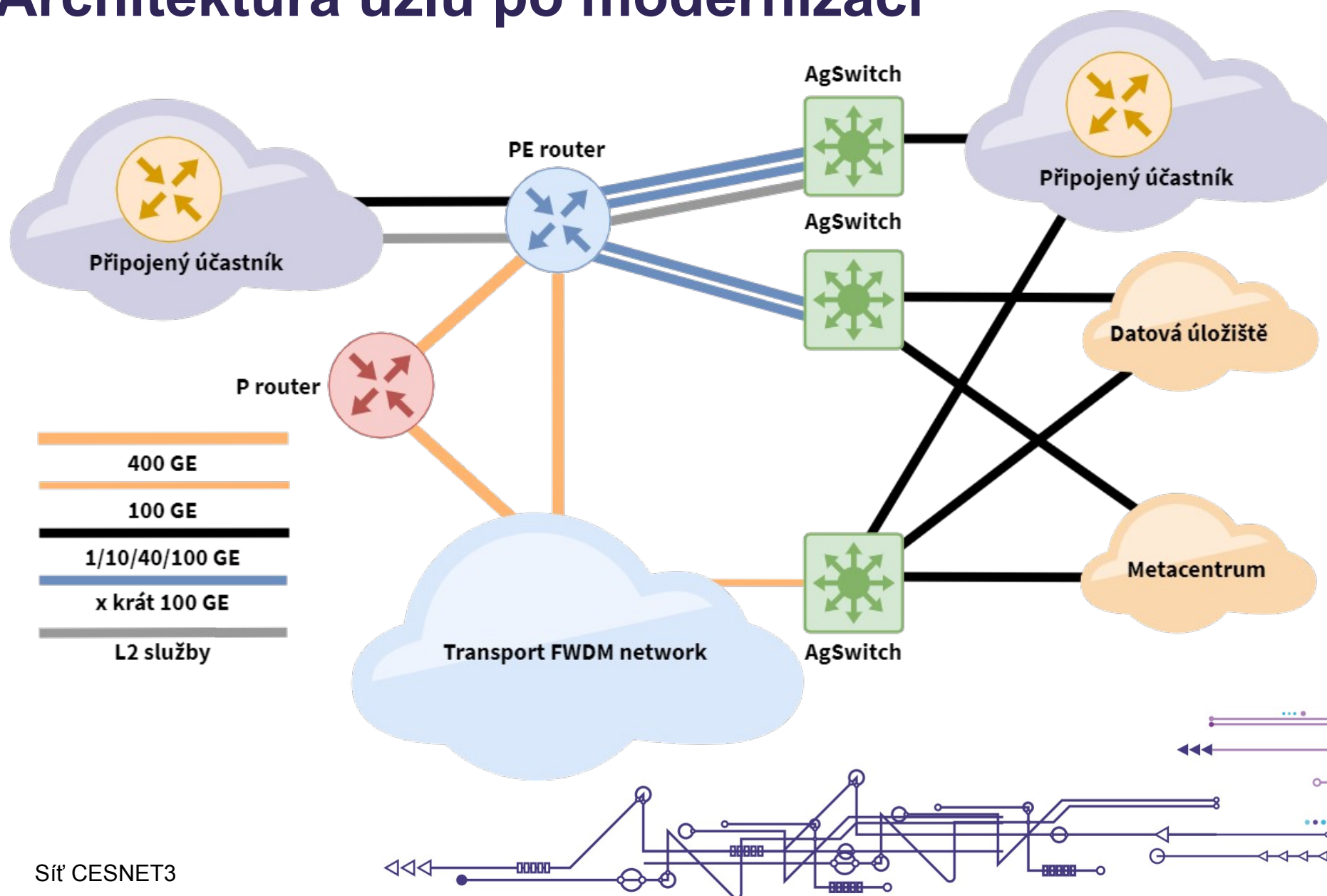


Automatizace

- Zdroj dat a popis sítě - Netbox (Source of Truth)
- Mechanismus - Ansible, CI/CD
- Cíle
 - Automatizovat periodicky opakující se činnosti
 - user management, ACL, VPN, VPLS, VRF atd.
 - Automatizovat pravděpodobně **nebudeme** speciální jednorázové konfigurace
 - některé konfigurace jsou v naší síti jedinečné
 - Poskytnout některé automatizační procedury i našim klientům v rámci projektů

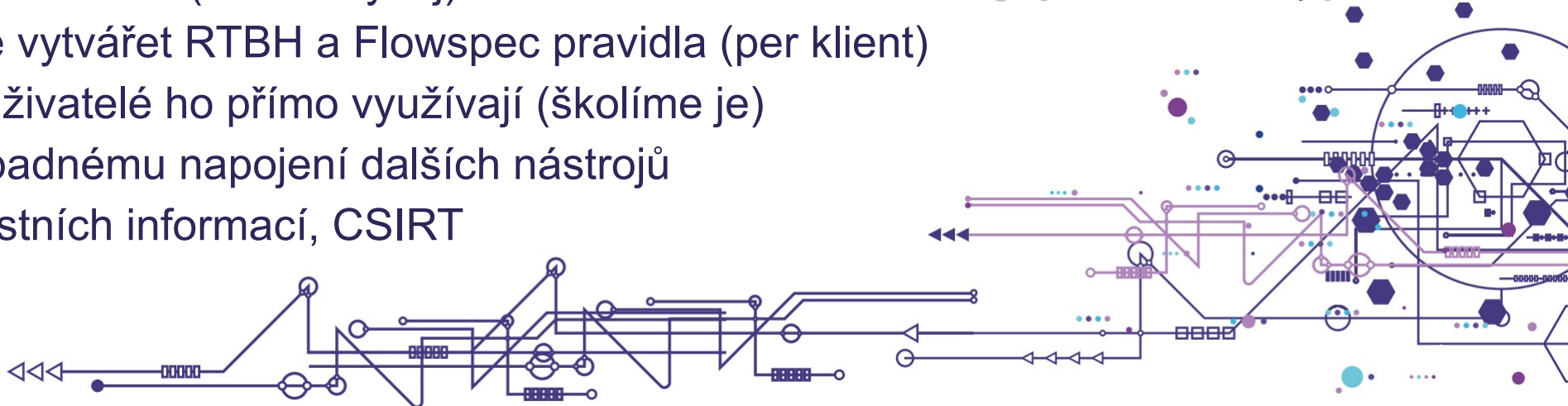
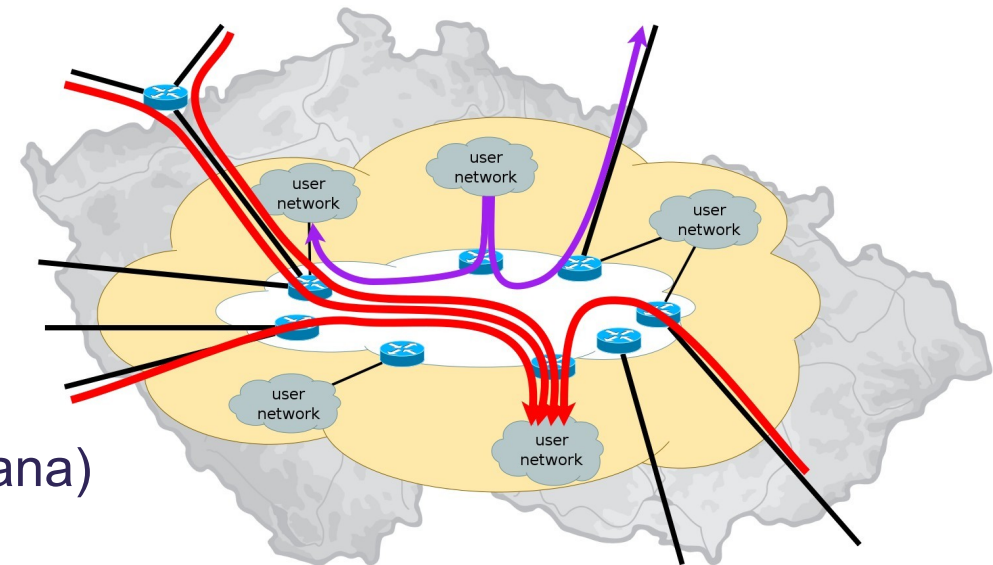


Architektura uzlu po modernizaci



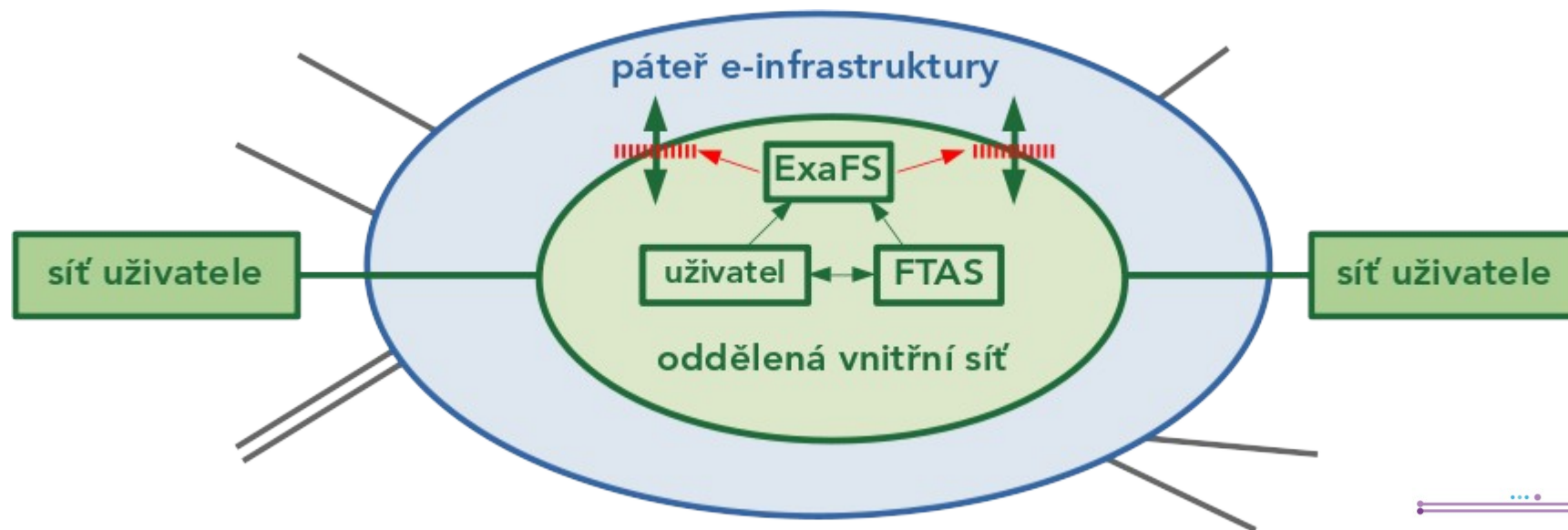
Ochrana síťové infrastruktury

- Monitoring a dohled
 - sběr dat o síťovém provozu z prvků a sond na perimetru sítě
- Vyhodnocení dat
 - FTAS (vlastní vývoj)
- Ochrana (protiopatření)
 - statické ACL, QoS
 - RTBH, BGP Flowspec
 - přesměrování na DDoS Protector (vlastní vývoj)
 - přesměrování do scrubbing centra (AntiDDoS ochrana)
 - Řízeno pomocí ExaFS (vlastní vývoj)
 - umožňuje vytvářet RTBH a Flowspec pravidla (per klient)
 - zkušenosti uživatelé ho přímo využívají (školíme je)
 - API k případnému napojení dalších nástrojů
- Sdílení bezpečnostních informací, CSIRT

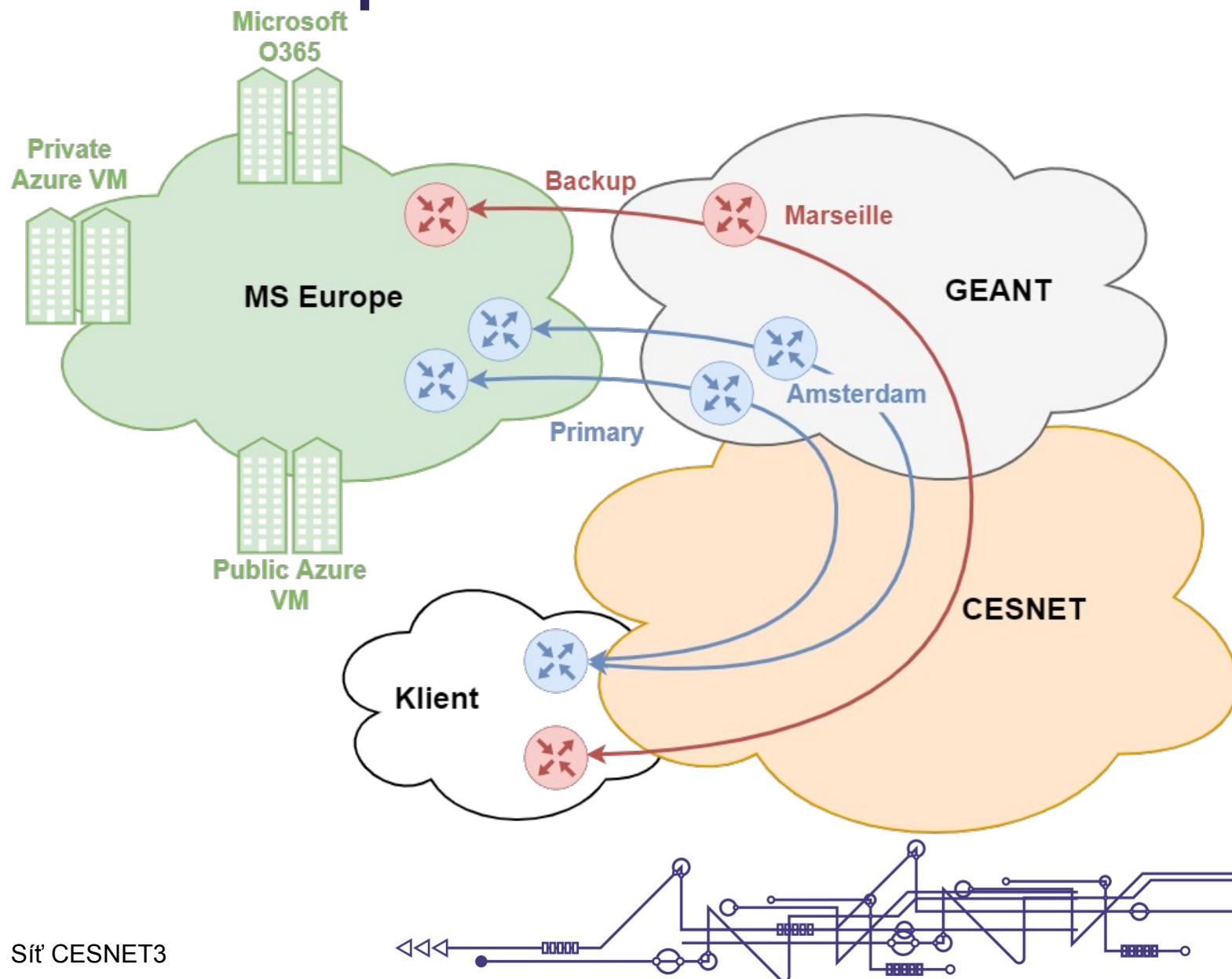


hSOC a hSOC VRF

- Oddělená infrastruktura pro specifickou komunitu
 - jasně vymezená infrastruktura → „sít' v síti“, dvoustupňová ochrana
 - automaticky sdílí prvky obrany celé e-infrastruktury
 - + samostatné instance a nastavení relevantních prvků na propojích do vnitřní sítě
- příklad využití prostředků a znalostí získaných z provozu infrastruktury
- 9 nemocnic zapojeno a další jsou v přípravě

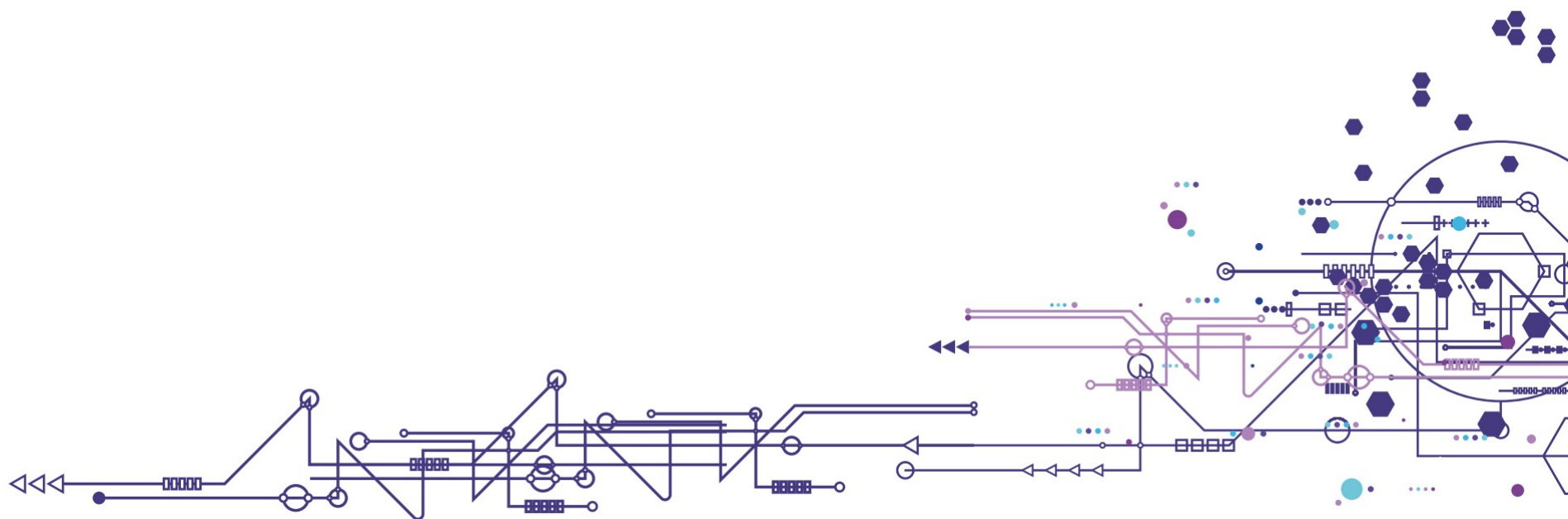


Microsoft Express Route





Děkuji za pozornost





Napište nám
info@e-infra.cz

