

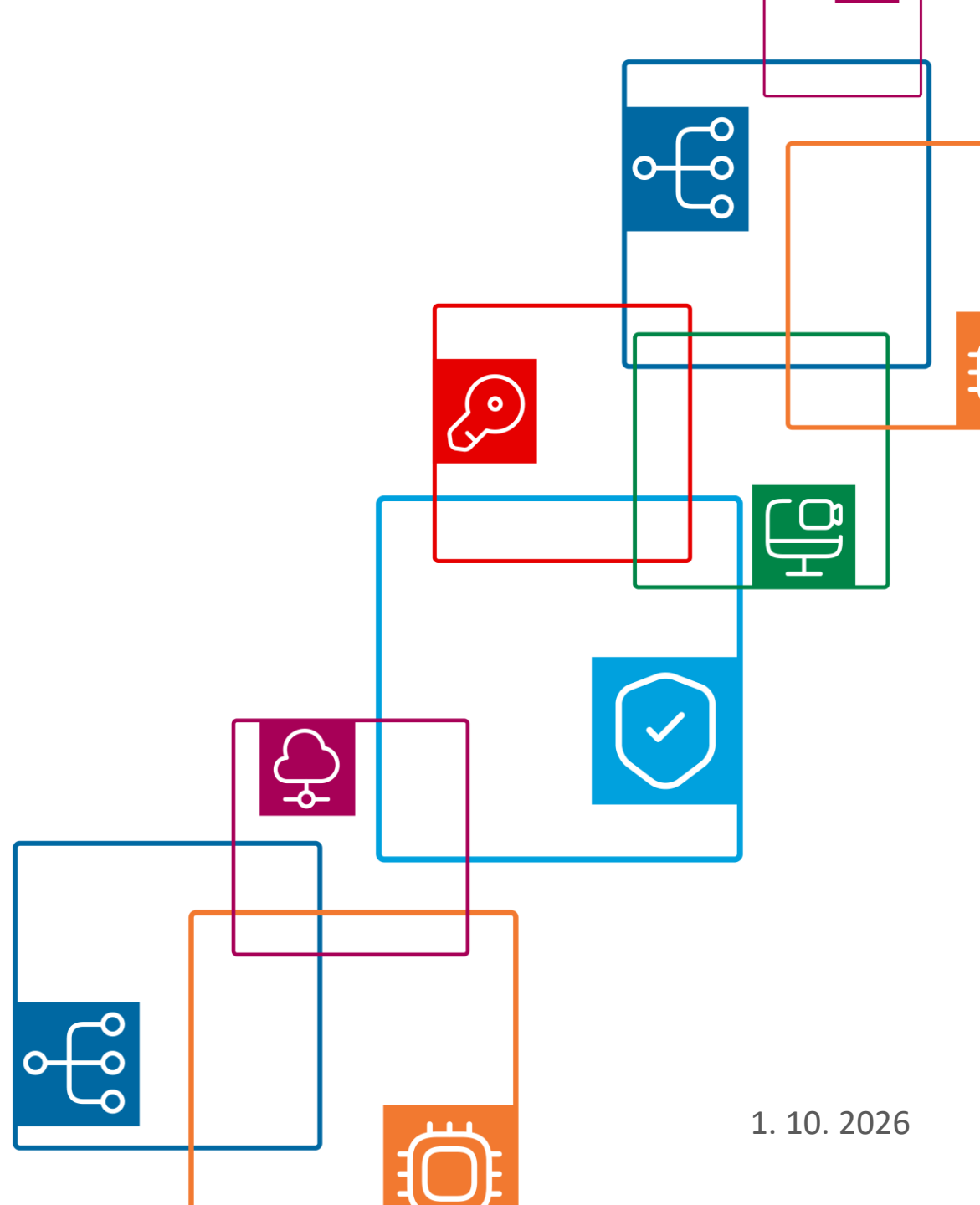


NETCONF: ovládněte svá síťová zařízení

Adam Piecek

Konference e-infrastruktury

CESNET 2026



1. 10. 2026

- **Provoz špatnou cestou**
 - Chyba v pravidle, filtru nebo směrování změní tok provozu.
- **Změna s příliš velkým dosahem**
 - Skript nebo účet může změnit víc, než měl.
- **Bezpečnostní parametry**
 - Pro šifry, protokoly
- **Problém, který není vidět**
 - Chybné logování, alarmy nebo telemetrie zpozdí reakci.



- **Zabezpečené rozhraní**
 - Šifrovaná relace
- **Autorizace**
 - NACM
- **Candidate datastore**
 - NMDA (candidate, running, operational)
- **Validace dat**
 - YANG typy, rozsahy, vazby, podmínky
- **Commit / rollback**
 - NETCONF confirmed commit
- **Stav a notifikace**



- Špatný typ hodnoty
- Hodnota mimo povolený rozsah
- Chybějící povinný údaj
- Odkaz na neexistující objekt
- Nesplněná vazba mezi položkami
- Hodnota mimo bezpečnostní politiku



YANG ukázka

```
container management {  
  leaf enabled {  
    type boolean;  
  }  
  
  leaf interface {  
    type leafref {  
      path "/if:interfaces/if:interface/if:name";  
    }  
    mandatory true;  
  }  
  
  leaf max-session {  
    type uint8 {  
      range "1..10";  
    }  
  }  
}
```

```
leaf label {  
  type string {  
    pattern "[a-zA-Z0-9_-]{3,16}";  
  }  
}  
  
leaf allowed-subnet {  
  when "../enabled = 'true'";  
  type inet:ipv4-prefix;  
  mandatory true;  
  
  must ". != '0.0.0.0/0'";  
}  
}
```

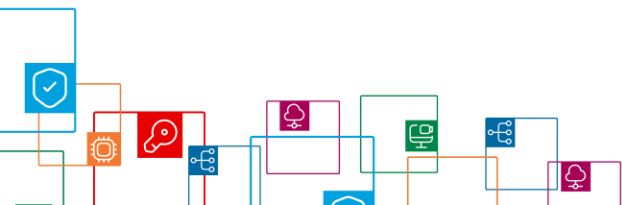
- zabezpečená NETCONF relace
- lock candidate
- edit-config
- confirm-commit
- get / notifikace



```
leaf allowed-subnet {  
  type inet:ipv4-prefix;  
  nacm:default-deny-write;  
}
```

```
leaf ssh-private-key {  
  type string;  
  nacm:default-deny-all;  
}
```

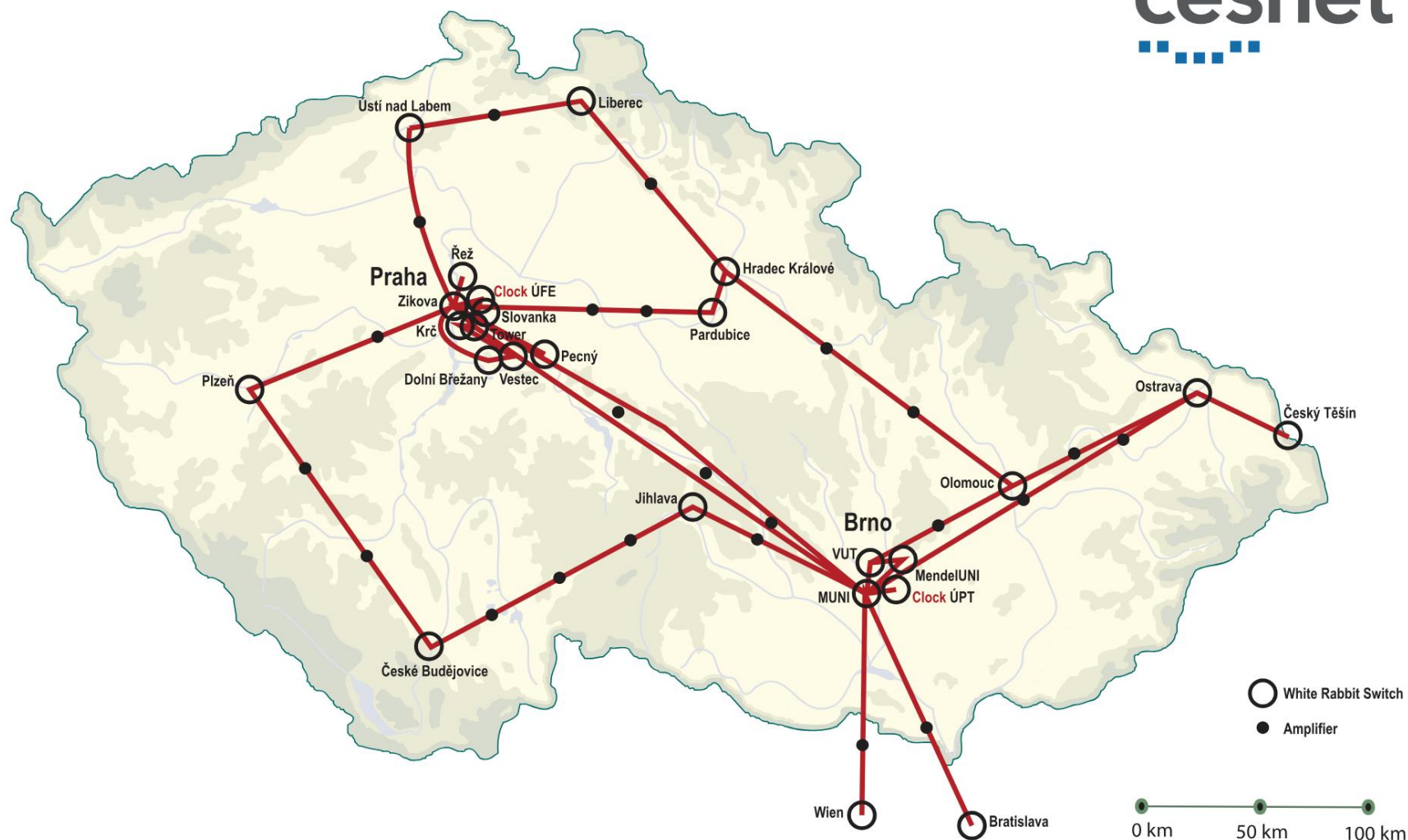
```
<rule-list>  
  <group>operator</group>  
  <rule>  
    <path>/ex:allowed-subnet</path>  
    <access-operations>read update</access-operations>  
    <action>permit</action>  
  </rule>  
</rule-list>  
<rule-list>  
  <group>security-admin</group>  
  <rule>  
    <path>/ex:ssh-private-key</path>  
    <access-operations>update</access-operations>  
    <action>permit</action>  
  </rule>  
</rule-list>
```



- libyang + libnetconf2
 - NETCONF klient
- netopeer2 + libnetconf2 + libyang
 - NETCONF server
- sysrepo
 - YANG datastore, subscriptions / callbacky
- pluginy / aplikace zařízení
 - aplikace změn, stavová data, RPC / actions
- hardware / služba zařízení



CzechLight: běží to u nás v provozu



- partneři: Deutsche Telekom, RACOM, Swisscom, ABB
 - Technologická podpora, nové standardy
 - TAČR projekt, komprese dat, integrace, web gui
 - rozšíření do libyang, nové standardy
 - FreeRTOS port netopeer2
- příprava nového IETF RFC — YANG Schema Comparison



- konzultace ke standardům
- úpravy a pluginy na míru
- pomoc s integrací
- technická podpora



- Hlavní stránka našich open-source projektů
 - <https://www.sysrepo.org/>
- Czechlight
 - <https://czechlight.cesnet.cz/cs/>
- Kontakt
 - `netconf-support@cesnet.cz`

