Automatizovaná konfigurace a správa síťových zařízení

Ladislav Lhotka • lhotka@nic.cz • 20. května 2013

CZ.NIC | SPRÁVCE DOMÉNY CZ

Osnova

1. Konfigurace a správa velkých sítí
2. Protokol NETCONF
3. Modelování dat, jazyk YANG
4. Existující datové modely
5. Implementace a aplikace
6. Nové trendy

Běžná konfigurační rozhraní

- konfigurační soubor a obecný textový editor,
- specializované textové rozhraní (CLI),
- webová aplikace,
- grafická aplikace.

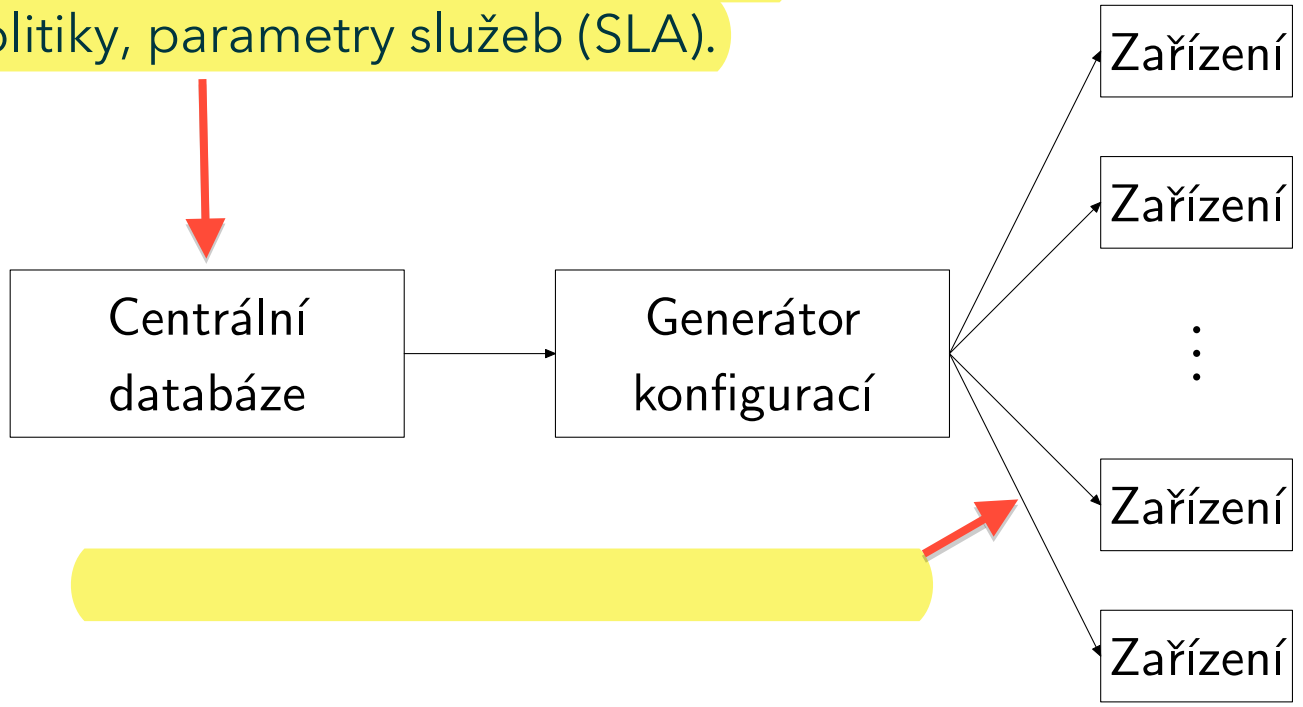
Běžná konfigurační rozhraní

- konfigurační soubor a obecný textový editor,
- specializované textové rozhraní (CLI),
- webová aplikace,
- grafická aplikace.

Všechna tato rozhraní jsou zaměřena na interakci s uživatelem-člověkem.

Typická procedura konfigurace velkých sítí

Databáze obsahuje popis sítě na vyšší úrovni – topologie, směrovací a bezpečnostní politiky, parametry služeb (SLA).



Možnosti automatizované konfigurace

- Simple Network Management Protocol (SNMP)

  Běžně se používá pro sběr stavových informací a statistik, pro konfiguraci jen velmi omezeně.

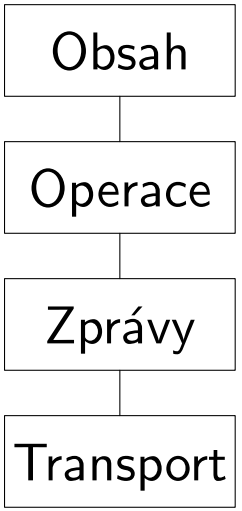
- Simulovaný uživatel, „škrábání obrazovky" (screenscraping)

  Aplikace (skript) se připojuje na CLI, často se používá jazyk Expect. Pracný postup, který může poměrně snadno selhat.

Protokol NETCONF

Jednoduchý protokol typu klient-server definovaný v RFC 6241.

konfigurační aplikace nebo skript



konfigurační a stavová data

dotazy s parametry, odpovědi

vrstva RPC

SSH (RFC 6241, povinný) nebo TLS (RFC 5539)

NETCONF používá XML pro zprávy, operace i datový obsah.

Sada operací je rozšiřitelná.

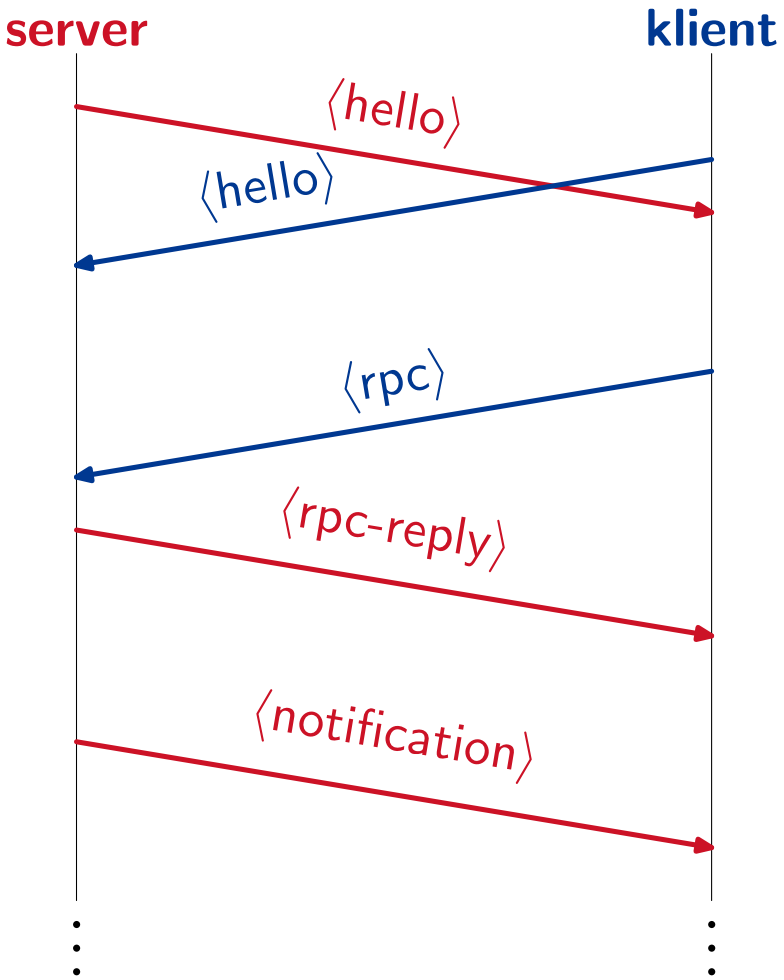
Úložiště konfigurací

Data mají strukturu hierarchických dokumentů (XML) a přechovávají se v ***úložištích (datastore).***

Server používá jedno nebo více úložišť:

- `running` – povinné, aktuální konfigurace,
- `candidate` – alternativní konfigurace, jejíž obsah je možné kdykoli promítnout do `running` (operací `commit`),
- `startup` – aplikuje se po zapnutí/restartu.

Průběh komunikace



V `hello` uvede server i klient verzi protokolu, server dále stanovuje `session-id` a oznamuje podporované datové modely a rozšíření.

Operace: klient posílá dotaz, server odpovídá.

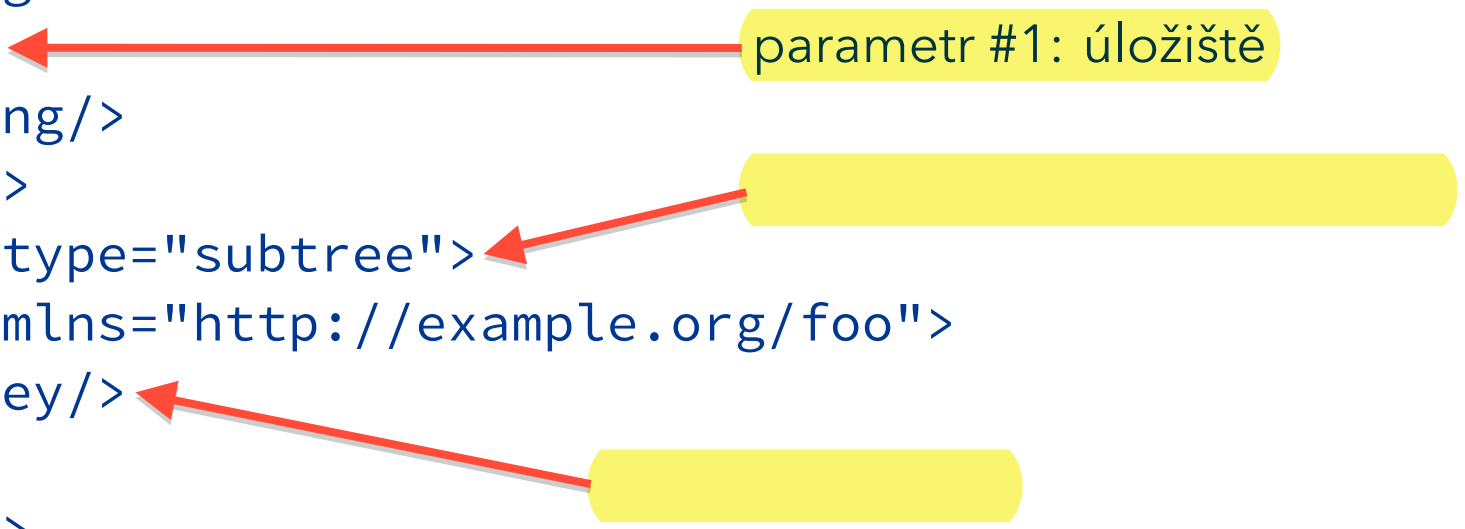
Asynchronní ***notifikace*** (RFC 5277): zprávy od serveru, klienti se mohou přihlásit do zvolených kanálů.

Základní operace

`<get-config>`	Žádost o zaslání celé konfigurace nebo její části.
`<get>`	Žádost o zaslání obsahu úložiště `running` a stavových dat (případně jejich části).
`<edit-config>`	Žádost o modifikaci zvoleného úložiště.
`<copy-config>`	Kopírování celého úložiště.
`<delete-config>`	Vymazání celého úložiště.
`<lock>`	Žádost o uzamčení celého vybraného úložiště. (zamykání části úložiště: RFC 5717).
`<unlock>`	Uvolnění zámku, který má daná seance v držení.
`<close-session>`	Žádost o řádné ukončení seance.
`<kill-session>`	Vynucené ukončení seance.

Příklad: žádost o část konfigurace

```
<rpc message-id="101"
     xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
    <source>
      <running/>
    </source>
    <filter type="subtree">
      <doc xmlns="http://example.org/foo">
        <dopey/>
      </doc>
    </filter>
  </get-config>
</rpc>
```



Kromě filtrování pomocí podstromů lze používat i výrazy XPath.

YANG – jazyk pro modelování dat

Definice v RFC 6020, další informace v dokumentech pracovní skupiny NETMOD při IETF.

Požadavky:

1. schéma, datové typy + ***sémantika***,
2. přehlednost a čitelnost (pro člověka),
3. modularita a rozšiřitelnost.

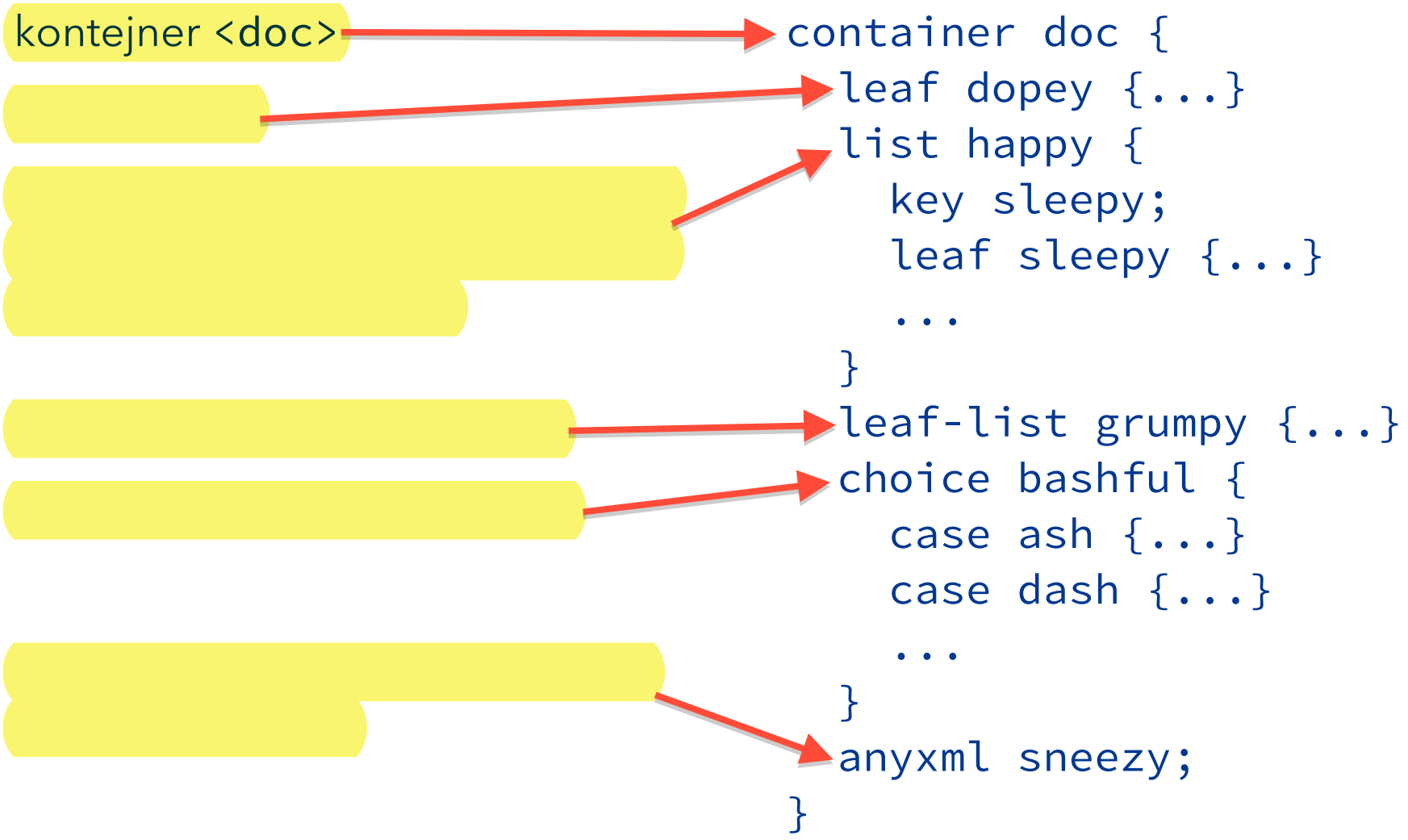
Dvojí využití:

- validace dat,
- dokumentace.

Datové modely popsané jazykem YANG

- Datový model se skládá z ***modulů***, ty mohou být dále rozděleny na ***submoduly***.
- Každý modul definuje vlastní jmenný prostor (unikátní URI), který je sdílen i se všemi submoduly.
- Modul může importovat definice z jiných modulů.
- Jména modulů a URI pro jmenné prostory registruje a spravuje IANA.

Popis schématu



Datové typy

Sada základních datových typů odpovídá knihovně datových typů W3C XML Schema (XSD):

`int8`, `uint8`, `int16`, `uint16`, `int32`, `uint32`, `int64`, `uint64`, `string`, `boolean`, `binary`.

Speciální typy:

- `decimal64`: obdoba `decimal` v XSD, délka je ale vždy 64 bitů (XSD `totalDigits` = 19), počet desetinných míst musí být vždy uveden.
- `enumeration`: výčet, pevná množina řetězů.
- `leafref`: odkaz na jiný list, základní nástroj k propojování částí konfigurace.

Odvozené typy

Nový typ může být definován zadáním omezení na existující typ (základní nebo jiný odvozený).

```
typedef hodina {
  type uint8 {
    range "0..23";
  }
}
```

Jméno odvozeného datového typu patří do jmenného prostoru toho modulu, v němž je typ definován .

RFC 6021 obsahuje dva YANG moduly s obecně použitelnými knihovnami typů:

- `ietf-yang-types` – časové a datové údaje, MAC adresa, čítače s různou sémantikou, aj.
- `ietf-inet-types` – IP adresy, prefixy, doménová jména, aj.

Sémantické podmínky

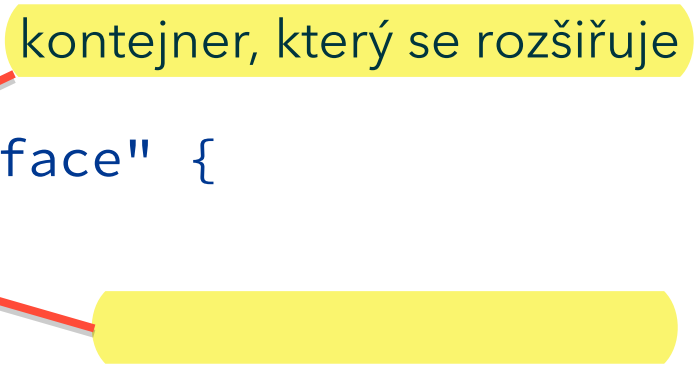
```
list recipient-routing-table {
  must "name != ../../name" {
    error-message
      "Source and recipient routing tables "
    + "are identical.";
    description
      "A routing table MUST NOT appear among
       its recipient routing tables.";
  }
...
}
```

formální podmínka
zadaná výrazem XPath

Rozšiřitelnost datových modelů

Příkaz **augment** umožňuje dodatečně přidávat nová data na libovolné místo v již existujícím modulu, aniž by se musel tento modul jakkoli měnit.

```
import interfaces {
  prefix "if";
}
...
augment "/if:interfaces/if:interface" {
  when "if:type = 'ethernet'";
  container ethernet {
    leaf duplex {
      ...
    }
    ...
  }
}
```



Základní datové modely

Standardní YANG moduly vyvinuté pracovní skupinou NETMOD:

- `ietf-system` – konfigurace hlavních systémových parametrů (identifikace systému, čas, DNS resolver, RADIUS, autentizace uživatelů),
- `ietf-interfaces` – fyzická i logická síťová rozhraní,
- `ietf-ip` – IPv4 a IPv6,
- `ietf-routing` – směrování,
- `ietf-snmp` - SNMP.

Specializované datové modely

- IPFIX a PSAMP (RFC 6728),
- DNSCCM – konfigurace DNS serveru.

Využití v projektech CZ.NIC:

- DNS Collector – aplikace pro monitorování DNS serverů,
- konfigurace OpenWRT.

Open source implementace

- **libnetconf** (C) – knihovna, klient i server,
- **OpenYuma** (C) – klient i server,
- **ncclient** (Python) – knihovna, klient,
- **pyang** (Python) – nástroje pro práci s datovými modely YANG.

Aktuální trendy

- Software-Defined Networks (SDN): OpenFlow, I2RS, …
- RESTful API (`draft-bierman-netconf-yang-api-01`),
- JSON místo XML (`draft-lhotka-netmod-yang-json-01`),

Aktuální trendy

- Software-Defined Networks (SDN): OpenFlow, I2RS, …
- RESTful API (`draft-bierman-netconf-yang-api-01`),
- JSON místo XML (`draft-lhotka-netmod-yang-json-01`),

```
POST /yang-api/datastore/jukebox/artist HTTP/1.1
Host: example.com
Content-Type: application/vnd.yang.data+json
{
  "artist" : {
    "name" : "The Foo Fighters"
  }
}
```

Zdroje dalších informací

- NETCONF Working Group

  `http://datatracker.ietf.org/wg/netconf`
- NETMOD Working Group

  `http://datatracker.ietf.org/wg/netmod`
- NETCONF Central

  `http://www.netconfcentral.org`
- YANG Central

  `http://www.yang-central.org`