Ovládání síťových zařízení

David Rohleder
davro@ics.muni.cz

24. února 2015

Dataplane a controlplane

Fungování síťových zařízení, hlavně přepínačů, můžeme rozdělit na dvě části.

- data plane – vrstva, která pomocí speciálního hardware (ASIC (Application-specific integrated circuit), případně FPGA (Field-programmable gate array)) provádí hlavní činnost přepínače, tj. přehazování rámců z jednoho portu na jiný. Řídí se při tom pravidly, která do této části umístí:
- control plane – vrstva, která řídí přepínač (nebo libovolný jiný síťový prvek) a předává zadané nastavení do data plane. Control plane je obvykle vybaven rozhraním pro komunikaci se správcem systému.

Toto rozdělení umožňuje vyšší výkon systému (hardware a specializované ASIC obvody jsou vždy rychlejší než software). Řídící procesor pak nemusí být příliš výkonný (v dnešní době se používají procesory nenáročné na energii, často úsporné varianty PowerPC nebo MIPS).

Druhy pamětí obvykle použitých v sítových prvcích (Cisco)

- ROM – obsahuje základní zavaděč operačního systému (bootstrap). Najde operační systém a zavede ho do paměti
- RAM – slouží k uložení běžícího operačního systému, programů a dat. Dočasná.
- flash – operační systém je obvykle uložen na pamětech typu flash. Sítové prvky většinou nemají HDD (zvyšuje se tím jejich spolehlivost).
- NVRAM – Nonvolatile RAM. Pamět použitá pro ukládání konfigurace. Není smazána při vypnutí napájení.
- TCAM – Ternary Content Addressable Memory – slouží ke speciálním účelům (rychlé vyhledávání)

Spouštění systému

Spouštění systému sítových prvků probíhá obvykle následovně:

1. spustí se základní zavaděč operačního systému (bootstrap), který provede základní kontrolu inicializaci hardware. U cisco zařízení je možné v této fázi zastavit zasláním signálu BREAK po sériové lince (kermit: Ctrl-\Ctrl-B). V bootstrapu (rommon) je možné provádět pouze některé základní operace s nastavením (smazat konfiguraci, nahrát jiný OS)
2. zavaděč zjistí, co má dělat – podle nastavení registrů a pod. nahraje do paměti plnohodnotný operační systém.
3. operační systém provede inicializaci celého hardware, nahraje konfiguraci z NVRAM, spustí systémové procesy (podle konfigurace) – STP, ssh, telnet, NTP, konzolový přístup, atd.

Přístup do systému

- konzola – sériová linka RS-232. Přistupuje se pomocí programů typu kermit nebo minicom. Různí výrobci používají různá nastavení parametrů. Nejčastější je 9600 bps, 8 bits, no parity, 1 stopbit, no flow control (Cisco, Juniper, některá novější HP (starší používají buď autodetekci rychlosti nebo 19200 bps))). Cisco používá ne úplně standardní konektor RJ-45. Volba tohoto konektoru minimalizuje použitou plochu (narozdíl od standardního konektoru Canon 9) a umožnuje jednodušší propojení na konzolové servery standardními ethernetovými kabely.
- vzdálený terminálový přístup (telnet, SSH)
- webové rozhraní

Úrovně uživatelských oprávnění

- standardní – umožňuje provádět základní operace (show, ping, traceroute, ...). Cisco tento režim označuje user EXEC level, na příkazové řádce se pozná podle zobáku >

```
switch>
```

- privilegovaný uživatelský režim – umožňuje provádět změnu konfigurace, ladění a další nastavení. Cisco tento režim označuje jako enable EXEC level. Enable má u cisco IOS 15 úrovní, do kterých je možné jednotlivé příkazy zařadit. Na příkazové řádce se pozná podle mřížky #. Do privilegovaného režimu se přepíná příkazem `enable` s případným označením úrovně (standardně 15):

```
switch> enable
davro's password:
switch#
```

  Vrátit se do standardního uživatelského režimu je možné příkazem `disable`.

Režimy uživatelského přístupu

- základní (exec) režim – umožnuje provádět nekonfigurační příkazy.
- konfigurační režim – umožnuje provádět konfiguraci, tj. měnit nastavení parametrů systému (hardware, software, rozložení pamětí, atd)

```
switch# configure terminal
switch(config)# interface FastEthernet 0/1
switch(config-if)#exit
switch(config)#end (nebo Ctrl-z)
switch#
```

Hierarchie konfigurace

Konfigurační příkazy je možné sdružovat do skupin, které spolu nějakým způsobem logicky souvisí a tím zpřehlednovat konfiguraci.

```
set vlan name 31 "MaR"
set vlan name 32 "EZS"
set vlan name 33 "CCTV"
set vlan egress 31 ge.1.11-12;ge.1.17-18;ge.2.7;ge.2.23 tagged
set vlan egress 32 ge.1.11;ge.2.7 tagged
set vlan egress 33 ge.1.11;ge.1.17-18;ge.2.7 tagged
set vlan egress 34 ge.1.11;ge.2.7 tagged
```

Hierarchie konfigurace

Konfigurační příkazy je možné sdružovat do skupin, které spolu nějakým způsobem logicky souvisí a tím zpřehlednovat konfiguraci.

Enterasys

```
set vlan name 31 "MaR"
set vlan name 32 "EZS"
set vlan name 33 "CCTV"
set vlan egress 31 ge.1.11-12;ge.1.17-18;ge.2.7;ge.2.23 tagged
set vlan egress 32 ge.1.11;ge.2.7 tagged
set vlan egress 33 ge.1.11;ge.1.17-18;ge.2.7 tagged
set vlan egress 34 ge.1.11;ge.2.7 tagged
```

Hierarchie konfigurace

```
hostname sw12
aaa group server radius radius-servers
 server 1.2.3.4 auth-port 1812 acct-port 1813
 server 5.6.7.8 auth-port 1812 acct-port 1813
 deadtime 5
!
interface FastEthernet0/1
 description C101.1A pokusy
 switchport access vlan 71
 switchport mode access
 load-interval 30
 macro description cisco-desktop
 ip verify source
!
ntp access-group peer 77
ntp server 1.2.3.4
ntp server 5.6.7.8
```

Hierarchie konfigurace

Cisco IOS

```
hostname sw12
aaa group server radius radius-servers
 server 1.2.3.4 auth-port 1812 acct-port 1813
 server 5.6.7.8 auth-port 1812 acct-port 1813
 deadtime 5
!
interface FastEthernet0/1
 description C101.1A pokusy
 switchport access vlan 71
 switchport mode access
 load-interval 30
 macro description cisco-desktop
 ip verify source
!
ntp access-group peer 77
ntp server 1.2.3.4
ntp server 5.6.7.8
```

Hierarchie konfigurace

```
version 12.1R2.9;
system {
    host-name fwtest;
    domain-name test.muni.cz;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "tadybylonejakeheslo";
    }
    name-server {
        1.2.3.4;
    }
    services {
        ssh;
        web-management {
            https {
                system-generated-certificate;
            }
        }
    }
```

Hierarchie konfigurace

Juniper JunOS

```
version 12.1R2.9;
system {
    host-name fwtest;
    domain-name test.muni.cz;
    authentication-order [ tacplus password ];
    root-authentication {
        encrypted-password "tadybylonejakeheslo";
    }
    name-server {
        1.2.3.4;
    }
    services {
        ssh;
        web-management {
            https {
                system-generated-certificate;
            }
        }
    }
```

Hierarchická konfigurace – Cisco

Cisco má poměrně plochou hierarchii, ačkoliv se postupně vyvíví:

- global – nastavování globálních parametrů (hostname, SNMP, služby,...)
- interface – nastavování parametrů fyzických i logických rozhraní
- line – nastavování parametrů sériových a virtuálních linek
- s vývojem vznikají další zanořené části konfigurace (MSTP, class-mapy, access-listy, atd.), úroven obvykle není příliš hluboká.

Konfigurace

Nastavení parametrů v konfiguraci probíhá pouze v RAM, rozlišujeme dva druhy konfigurace:

- running-config – tato konfigurace je uložená pouze v RAM, v případě restartu switche dochází ke smazání. Proto je nutné tuto konfiguraci nejdřív zapsat do
- startup-config – která je uložena v NVRAM (nvram:startup-config). Tato konfigurace se nahrává po spuštění systému. Zápis running config do startup-config je možný následujícími způsoby

```
switch# write memory (nebo)
switch# copy running-config startup-config
```

Ovládání CLI - cisco

Všechny příkazy mohou být zapisovány jednoznačnými zkratkami:

```
     sh conf   show configuration
sh int Te1/6   show interface TenGigabitEthernet 1/6
```

- no příkaz v konfiguračním režimu zruší zadaný příkaz

  ```
  switch(config-if)# no speed 100
  ```

- default XXX nastaví defaultní hodnoty

  ```
  switch(config)# default int range f0/1 - 4 , f0/6 - 48
  ```

Ovládání – pokračování

Ovládání CLI u většiny systémů vychází ze standardního unixového pojetí CLI (emacs & vi). Některé klávesové zkratky jsou vhodné pouze v případě, kdy vám nefungují třeba šipky (kvůli špatně nastavenému terminálu):

?	zobrazí nápovědu k rozepsanému příkazu
TAB	doplňuje nedokončený příkaz do standardního nezkráceného tvaru. V případě, kdy není doplnění jednoznačné, nabídne možné varianty doplnění.
Ctrl-B	kurzor zpět po řádce
Ctrl-F	kurzor vpřed po řádce
ESC-B	zpět jedno slovo
ESC-F	vpřed jedno slovo
Ctrl-A	kurzor na začátek řádku
Ctrl-E	kurzor na konec řádku
Ctrl-D	smaž znak na kurzoru
ESC-D	smaže slovo následující za kurzorem
Ctrl-H	smaž znak před kurzorem (backspace)
Ctrl-W	smaž předchozí slovo
Ctrl-K	smaže řádku od kurzoru do konce řádku
Ctrl-X	smaže řádku od začátku řádku ke kurzoru
Ctrl-Y	vloží na místo kurzoru poslední delete buffer
Ctrl-P	posunuje se v historii příkazů dozadu
Ctrl-N	posunuje se v historii příkazů dopředu

http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf001.html

Ladění

Každý rozumně použitelný síťový prvek musí být vybaven nástroji pro ladění problémů. Čím více možností a specifičtější zadání, tím lépe.

- zapínání ladění

  ```
  switch# debug ?
  ```

- vypínání ladění

  ```
  switch# no debug ?
  switch# undebug ?
  ```

- POZOR: debugování je náročné na zpracování CPU, může dojít k zahlcení systému. Proto nikdy na provozním stroji nezkoušejte

  ```
  switch# debug all
  ```

Užitečná vylepšení

- čas vzniku události je důležitý – zvlášť pro porovnání vzniku události na různých zařízeních

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

Užitečná vylepšení

- čas vzniku události je důležitý – zvlášť pro porovnání vzniku události na různých zařízeních

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

- synchronizace času – je vhodné, aby čas na jednotlivých zařízeních byl stejný.

```
ntp server 1.2.3.4
ntp server 5.6.7.8
```

Užitečná vylepšení

- čas vzniku události je důležitý – zvlášť pro porovnání vzniku události na různých zařízeních

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

- synchronizace času – je vhodné, aby čas na jednotlivých zařízeních byl stejný.

```
ntp server 1.2.3.4
ntp server 5.6.7.8
```

- posílání logů na vzdálený syslog server

```
logging trap debugging
logging 1.2.3.4
logging facility <syslog facility>
```

Užitečná vylepšení

- čas vzniku události je důležitý – zvlášť pro porovnání vzniku události na různých zařízeních

```
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
```

- synchronizace času – je vhodné, aby čas na jednotlivých zařízeních byl stejný.

```
ntp server 1.2.3.4
ntp server 5.6.7.8
```

- posílání logů na vzdálený syslog server

```
logging trap debugging
logging 1.2.3.4
logging facility <syslog facility>
```

- na virtuálních terminálech je nutné vypisování na terminál nejdřív zapnout (jinak se zapisuje pouze do bufferu v paměti nebo na syslog server)

```
switch# terminal monitor
switch# show logging
```

Mikrotik

- Stromová struktura příkazů
- http://wiki.mikrotik.com/wiki/Manual:TOC
- všechny příkazy jsou provedeny hned a současně uloženy do stálé paměti
- pohyb ve stromové struktuře podobně jako v adresářích (bez cd) /, ..

```
[admin@nekde] > /
certificate  ip    port    routing         system  blink   password  setup
driver       ipv6  ppp     snmp            tool    export  ping      undo
file         log   queue   special-login   user    import  quit
interface    mpls  radius  store           beep    led     redo

/            delay    find     if       parse    set      toid   tostr
:            do       for      len      pick     time     toip   totime
environment  error    foreach  local    put      toarray  toip6  typeof
terminal     execute  global   nothing  resolve  tobool   tonum  while
```

Mikrotik

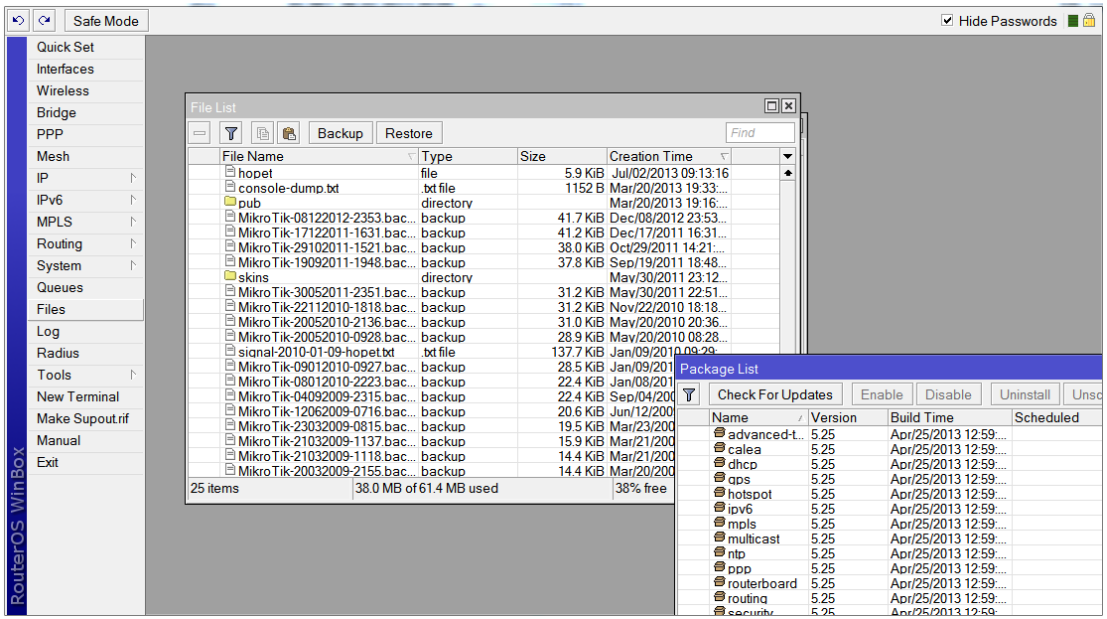
```
[admin@nekde] > /interface bridge print
Flags: X - disabled, R - running
 0  R name="trunk-br" mtu=1500 l2mtu=2290 arp=enabled
      mac-address=00:0C:42:23:CF:7B protocol-mode=none priority=0x8000
      auto-mac=yes admin-mac=00:00:00:00:00:00 max-message-age=20s
      forward-delay=15s transmit-hold-count=6 ageing-time=5m

[admin@nekde] > /interface bridge set name="neco"
```

- Zálohování

```
[admin@nekde] > /export
```

- WinBox
  - jednoduché GUI pro správu
  - možnost připojení jen přes L2 MAC
  - levé menu imituje strukturu CLI + některé zkratky navíc (např. bridge)
  - drag & drop funkcionalita: → Files



- Možnosti skriptování

```
:local interface "wlan2";
/interface wireless monitor $interface once do={
:local status $"status";
:local txrate $"tx-rate";
:local rxrate $"rx-rate";
:local signal $"signal-strength";
:local snr $"signal-to-noise";
:local noise $"noise-floor";
:local thruput $"p-throughput";
:local freq $"frequency";
:local txccq $"tx-ccq";
:local rxccq $"rx-ccq";
:log info ([/system identity get name] . " " . "status: $status, \
rates tx/rx: $txrate/$rxrate, freq: $freq MHz, SNR: $snr dB, signal: \
$signal dBm, noise: $noise dBm, CCQ tx/rx: $txccq%/$rxccq%, thruput: \
$thruput");
};
```