

Cisco IOS 5 - komunikace se switchem

Další část popisu Cisco IOSu se věnuje shrnutí jednotlivých možností, jak se připojit ke switchi, aby bylo možno provádět jeho konfiguraci. Jedná se nejen o popis možností, ale také informace o konfiguraci těchto vlastností a zabezpečení přístupu.

Fyzické připojení

Pro komunikaci se switchem se s ním musíme nejprve nějakým způsobem spojit. Máme dvě možnosti, spojení pomocí

1. **konzolového portu** - jedná se o speciální port na switchi s konektorem RJ45, který spojíme s COM portem na PC, používá se *rollover cable*.
2. **ethernetového portu** - na správně nakonfigurovaný switch (nastavena IP adresa pro VLANu, žádná omezení komunikace a přístupu) se můžeme připojit přes libovolný síťový port switche. Pro úvodní konfiguraci můžeme využít *Express Setup* (switche si nastaví určitou IP). Pro spojení se použije klasický přímý kabel (straight-through cable).

Způsoby komunikace

Se switchem můžeme komunikovat několika metodami, pomocí

1. **webové rozhraní** - některá konfigurace a monitorování lze provádět přes zabudované rozhraní, je potřeba mít instalovaný IOS s tímto rozhranním (standardně ano) a mít jej zapnuté (standardně ano), podle verze IOSu můžeme využívat HTTP nebo i HTTPS.
2. **telnet, SSH, konzola** - tyto metody nám přináší možnost využít **Command Line Interface** - CLI, tedy širokou škálu řádkových příkazů. Konzolový přístup je defaultně aktivní, telnet a SSH musíme nakonfigurovat. Pro SSH musíme mít verzi IOSu s podporou šifrování. Pro tento druh spojení je třeba nějaký program, já používám Putty.
3. **Cisco Network Assistant (CNA)** - případně další speciální aplikace. Pro správu switche lze použít speciální aplikace, které využívají různých protokolů pro řízení switche. **CNA** je slušná grafická aplikace (lze zdarma stáhnout u Cisca), která nám usnadní řadu nastavení a může pracovat s celou skupinou zařízení najednou.
4. **SNMP** - pomocí protokolu SNMP můžeme automatizovat řadu funkcí, číst i nastavovat hodnoty. Případně existuje řada aplikací, které tento protokol využívají.

Zabezpečení - ověřování

Přístup na switch je samozřejmě třeba zabezpečit. Základní dvě možnosti zabezpečení jsou

1. **používat autentizaci** - pro všechny metody komunikace můžeme nastavit heslo (a většinou uživatele). Nejjednodušší je nastavit pouze heslo, které se uloží do konfigurace switche, může být uloženo nešifrované (`password`) nebo pomocí MD5 hashe (`secret`). V lepším případě můžeme využít **AAA** (Authentication Authorization Accounting).
2. **omezit přístup** - záleží na metodě připojení
 1. **konzolový port** - pro použití této metody je třeba fyzický přístup ke switchi, ten by měl být v zabezpečené prostře s omezeným přístupem.
 2. **ethernetový port** - v tomto případě je možný přístup z celé sítě (z té části, kde je switch dosažitelný), proto je dobré povolit určité protokoly pouze do speciální VLANy (managovací) nebo pouze z určité adresy, toho dosáhneme konfigurací nebo pomocí **Access Control List** (ACL).

Konfigurace jednotlivých vlastností

Přístup přes konzoli

Přístup přes konzoli je defaultně povolený a to bez ověřování. Často jej využijeme pro úvodní konfiguraci. Pokud chceme více zabezpečit přístup ke switchi tímto způsobem, můžeme nastavit heslo. Pokud však má někdo fyzický přístup k zařízení (aby mohl využít konzolový přístup), tak jej většinou toto heslo nezastaví. Může provést **password recovery** (u novějších IOSů můžeme vypnout) nebo může resetovat konfiguraci a má plný přístup na switch.

```
SWITCH(config)#line console 0          // přepneme se do konfigurace konzole
SWITCH(config-console)#password c      // nastavíme heslo
```

Pozn.: U routerů ještě musíme zapnout, aby se prováděla kontrola hesla příkazem `login`. To se týká všech přístupů přes `line`.

Přístup pomocí protokolu telnet

Pro vzdálený přístup se používá **Virtual terminal line** (VTY). Přístup pomocí telnetu je aktivní ve chvíli, kdy nastavíme IP adresu pro switch. Ale do chvíle, než nastavíme heslo pro telnet session, se nelze připojit. V nastavení určujeme kolik současných spojení je povoleno, maximálně 16 (záleží na modelu).

```
SWITCH(config)#line vty 0 1            // konfiguruji telnetová spojení s ID 0 až 1
SWITCH(config-line)#password c         // heslo (zde c) pro přístup přes telnet
```

Linky, které nechceme používat, je lepší vypnout

```
SWITCH(config)#line vty 2 15           // spoje 2 až 15
SWITCH(config-line)#transport input none // žádný vstup
```

Hesla pro linky se dají zadat pouze nešifrovaná. Abychom více zabezpečili jejich uložení v konfiguraci, můžeme nastavit službu, která všechna hesla ukládá pomocí MD5 hashe.

```
SWITCH(config)#service password-encryption
```

Přístup pomocí protokolu ssh

Telnet má nevýhodu, že se veškerá data (včetně hesel) zasílají nešifrovaná, takže je možno je odposlechnout. Vhodnější je použít šifrované řešení a tedy ssh. Abychom však mohli ssh použít, potřebujeme verzi IOSu, která obsahuje šifrování. Potom musíme vytvořit uživatele, nastavit parametry ssh a vlastní nastavení přístupu. Vzdálený přístup pomocí ssh se nastavuje obdobně jako telnet, pouze zvolíme jiný vstup.

```
SWITCH(config)#aaa new-model // zapnutí AAA
SWITCH(config)#username cisco secret Heslo // vytvoření uživatele s heslem uloženým pomocí MD5 hash
SWITCH(config)#ip ssh time-out 60 // parametry SSH - vypršení session
SWITCH(config)#ip ssh authentication-retries 2 // parametry SSH - počet pokusů o přihlášení
SWITCH(config)#ip ssh version 2 // parametry SSH - verze
SWITCH(config)#ip domain name oksystem.local // jméno domény pro vytvářený certifikát
SWITCH(config)#crypto key generate rsa // pokud ještě nemáme, vygenerujeme klíč
SWITCH(config)#line vty 0 1 // konfigurace linky s ID 0 až 1
SWITCH(config-line)# transport input ssh // vstup je SSH
```

Přístup do privilegovaného režimu

Ve výchozí konfiguraci se po připojení ke CLI můžeme přepnout do privilegovaného módu zadáním příkazu `enabled`. Protože v tomto módu můžeme měnit konfiguraci switchu, tak se doporučuje zabezpečit tento přístup pomocí hesla. Heslo můžeme zadat tak, že se v konfiguraci uloží jako prostý text nebo pouze MD5 hash.

```
SWITCH(config)#enable password c // heslo (zde c) uložené jako čistý text
SWITCH(config)#enable secret c // heslo (zde c) uložené pomocí MD5 hash
SWITCH(config)#no enable secret // zrušení hesla
```

Webové rozhraní

Potom co nastavíme IP adresu, a máme verzi IOSu spolu s webovým rozhraním, tak je automaticky zapnuté.

```
SWITCH(config)#ip http server // zapne web server
SWITCH(config)#no ip http server // vypne web server
```

Pokud máme verzi IOSu s šifrováním (crypto), tak se automaticky použije přístup přes HTTPS.

```
SWITCH#show ip http server status // zobrazí nastavení
SWITCH(config)#ip http secure-server // zapne HTTPS server
```

SNMP

Ve výchozím stavu je SNMP vypnuto. SNMP se zapne nastavením *community stringů* (něco jako heslo pro SNMP, používá se v SNMPv1 a SNMPv2c, SNMPv3 používá účty).

```
SWITCH(config)#snmp-server community okro ro // nastaví community string pro čtení
SWITCH(config)#snmp-server contact OKsystem // nastaví kontakt
SWITCH(config)#snmp-server location serverovna // nastaví umístění
SWITCH(config)#no snmp-server // vypne SNMP
```

To jsou pouze základní nastavení SNMP. Můžeme samozřejmě vytvářet trapy a nastavovat mnoho dalších parametrů. Pro vytváření uživatelů v SNMPv3 nebo pro nastavení použité verze SNMP slouží příkazy `snmp-server group` a `snmp-server user`.