Cisco IOS 4 - reset, password recovery

Vložil/a Samuraj [1], 3 Prosinec, 2007 - 10:35

- Networks & Protocols [2]

V další části popisu Cisco IOSu se věnuji metodám, jak vymazat existující konfiguraci switche, a tedy dostat jej do výchozího stavu. V druhé části je sepsán postup pro obnovu hesla, pokud to původní zapomeneme.

Reset do továrního nastavení

Je mnoho důvodů, proč bychom mohli potřebovat provést reset zařízení (jeho konfigurace) do výchozího nastavení. Pokud se týče switchů, tak máme k dispozici dvě metody hardwarovou (potřebujeme fyzický přístup ke switchi) a softwarovou (potřebujeme se přihlásit s dostatečným oprávněním).

Pozn.: Než switche zresetujete, tak se doporučuje provést zálohu konfigurace. Také bych doporučil udělat si pro každý switch (nebo spíše produktovou řadu) zálohu IOSu (jak je pospáno v druhém díle).
Hardwarová metoda

Tuto metodu bych doporučil, zdá se mi jednodušší.

1. Na switchi stiskneme a držíme tlačítko MODE. Po cca 3 vteřinách začnou LED diody blikat.
2. Po cca 7 vteřinách přestanou diody blikat, pustíme tlačítko a switche se restartuje.
3. Po nastartování je konfigurace smazána.

Softwarová metoda

Pro zresetování switche potřebujeme vymazat jeho konfiguraci. Ta je uložena v NVRAM paměti v startup-config, plus informace o VLANech je uložena v souboru vlan.dat. Mazání můžeme provést několika způsoby a zohlednit také to co vše chceme smazat.

Pro mazání souborů ve flash paměti (souborovém systému) slouží příkaz delete, pro mazaní souborového systému máme příkaz erase, pomocí něj můžeme mazat bootflash:, flash: či nvram:.

Pozn.: Při mazání souborů se tyto pouze označí jako smazané a můžeme je obnovit příkazem undelete, případně příkazem squeeze opravdu vymazat. Ale po použití příkazu erase je vše opravdu smazáno.

Dříve se používaly tyto dva příkazy

```
SWITCH#erase startup-config   // smaže pouze startup konfiguraci
SWITCH#write erase            // smaže nvram pam??
```

ty jsou většinou stále funkční, ale byly nahrazeny příkazem

```
SWITCH#erase nvram:           // smaže nvram pam??
```

Příkazem erase můžeme také vymazat flash paměť, kde je uložen IOS a konfigurace VLAN. Je asi jen málo situací, kdy toto potřebujeme. Ještě jednou upozorňuji, že použitím následujícího příkazu si vymažeme IOS a switch tedy po restartu nabootuje pouze do omezeného prostředí RxBoot!

```
SWITCH#erase flash:           // kompletní smazání flash pam?ti
```

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

Pokud potřebujeme, tak vymažeme konfiguraci VLAN z flash paměti
```
SWITCH#delete vlan.dat        // smaže soubor vlan.dat
```

Po tom, co smažeme konfiguraci switche, jej potřebujeme restartovat. To můžeme provést příkazem
```
SWITCH#reload                 // restart switche
```

Pozn.: Pokud se vás systém při reloadu zeptá, zda chcete uložit změny v konfiguraci, musíte zvolit ne. Jinak by se aktuální běžící konfigurace uložila do startovací.

Password recovery - ztracené heslo

Může se stát, že zapomeneme heslo ke switchi a potřebujeme se k němu přihlásit. Přitom samozřejmě nechceme přijít o aktuální konfiguraci. Následující postup je pro Catalyst řady 2900, 3500, 3700 (ale může fungovat i jinde). Potřebujeme mít fyzický přístup ke switchi.

Principielně jde o to, že:

* nastartujeme switch bez startup konfigurace
* přihlásíme se do privilegovaného módu (bez hesla)
* zkopírujeme naši původní konfiguraci do běžící
* nastavíme heslo
* konfiguraci uložíme

Zde je přesnější postup:

1. se switchem se spojíme konzolově (sériovým kabelem)
2. vypojíme napájení ze switche
3. stiskneme a držíme tlačítko MODE
4. zapojíme napájení
5. switch se zastaví v úvodu bootování
6. následně zadáme tyto příkazy

```
SWITCH:flash_init
SWITCH:load_helper
SWITCH:dir flash:                                    // výpis pam?ti
SWITCH:rename flash:config.text flash:config.old     // p?ejmenujeme startovací
konfiguraci
SWITCH:boot                                          // nabootujeme
SWITCH>enable                                        // nastartovali jsme bez hesla a
konfigu, privilegovaný mód
SWITCH#rename flash:config.old flash:config.text     // p?ejmenujeme zp?t
SWITCH#copy flash:config.text system:running-config // zkopírujeme do b?žící
konfigurace (p?ipojí se)
Switch#configure terminal
Switch(config)#no enable secret                      // zrušíme heslo (p?ípadn? i
password)
Switch(config)#enable secret Cisco                   // nastavíme nové
Switch(config)#exit
Switch#copy running-config startup-config            // uložíme konfiguraci
```

Z bezpečnostního hlediska můžeme chtít tuto možnost obnovy hesla zakázat. Na novějších verzích IOSu je i toto možné pomocí příkazu:

Switch(config)#no service password-recovery

Potom, pokud se někdo pokusí o postup obnovy hesla, se vymaže paměť.

Samuraj, http://www.samuraj-cz.com/ [3]

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn

URL článku: https://security-portal.cz/clanky/cisco-ios-4-reset-password-recovery

Odkazy:
[1] https://security-portal.cz/users/samuraj
[2] https://security-portal.cz/category/tagy/networks-protocols
[3] http://www.samuraj-cz.com/

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn