INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Tato inovace předmětu Analýza dat je spolufinancována Evropským sociálním fondem a Státním rozpočtem ČR, projekt č. CZ.1.07/2.2.00/28.0014, "Interdisciplinární vzdělávání v ICT s jazykovou kompetencí".

Digitální analýza Cisco směrovačů a přepínačů 3

Analýza dat

Bc. Filip Pávek

Ústav informatiky
Filozoficko-přírodovědecká fakulta
Slezská univerzita v Opavě

filippavek@gmail.com

2012

Obsah prezentace

Obsah prezentace

- Zaměříme se na vlastní sběr dat ze směrovače a přepínače.
- Prezentace je rozděla dle zařízní na dvě části.
- U směrovače i přepínače zmíníme a vysvětlíme příkazy, které použijeme pro sběr nestálých a stálých dat.
- V prezentaci je ukázáno pouze několik výpisů s podrobnějším popisem. Ostatní si ukážeme při cvičení na reálném zařízení.

Při zkoumání aktivních síťových prvků je znalost příkazů a orientace v jednotlivých výpisech klíčová.

Než začneme zkoumat jednotlivé příkazy a jejich výpisy, tak si zapojíme a nakonfigurujeme síťovou topologii. Mnohé výpisy se tak stanou zajímavější.

#show clock details

- Než začneme zkoumát různé příkazy a jejich výpisy, je nutné zmínit tento příkaz.
- Příkaz nelze při sběru dat jasně přiřadit ani k zařízení (směrovač, přepínač) ani ke konkrétnímu typu dat (stálá,nestálá).
- Při forenzní analýze mají údaje čas/datum důležitý význam.
- Příkaz by měl být proveden nejen na začátku a konci zkoumání zařízení (při přihlášení a odhlášení), ale také v jeho průběhu.
- Tím získáme přesnější časovou osu zkoumání.

Sběr stálých dat ze směrovače - přehled příkazů

Sběr stálých dat ze směrovače - přehled příkazů	
Název	**Příkaz**
show version	informace spojené s IOS
show startup-config	konfigurace uložená v NVRAM
show file system	informace o souborovém systému
show interfaces	detailní informace o rozhraních
show diag	verze HW, sériové číslo součástí, chassis,...
show inventory	seriová čísla rozhraní, název, typ, chassis
show controllers	clock rate, DTE, DCE
show flash	velikost paměti Flash a IOS
dir flash:/	soubory a adresáře ve Flash
dir nvram:/	soubory a adresáře v NVRAM

#show version (část výpisu)

- Informace o zařízení, velikost pamětí RAM, NVRAM, Flash.
- Čas od zapnutí zařízení, verze běžícího IOSu, zda proběhl restart.

Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M), Version 12.4(1a), RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Fri 27-May-05 15:09 by hqluong
ROM: ROMMON Emulation Microcode
ROM: C2600 Software (C2600-ADVSECURITYK9-M), Version 12.4(1a), RELEASE SOFTWARE (fc2)
R1 uptime is 51 minutes
Cisco 2621 (MPC860) processor (revision 0x202) with **59392K/6144K bytes of memory**.
Processor board ID FTX0945W0MY (4279256517)
M860 processor: part number 0, mask 0
2 FastEthernet interfaces
128K bytes of NVRAM.
8192K bytes of processor board System flash (Read/Write)
Configuration register is **0x2102**

#show startup-config

- Pokud existuje uložená konfigurace pak jí zobrazí.
- Startup-config se nachází v paměti NVRAM (konfigurace načítaná po restartu zařízení).

```
interface Serial0/1
 ip address 4.4.4.1 255.255.255.248
 ip hello-interval eigrp 1 5
 ip hold-time eigrp 1 15
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 EIGRP_1
 encapsulation frame-relay
 no ip split-horizon eigrp 1
 clock rate 8000000
 frame-relay map ip 4.4.4.3 103 broadcast
 frame-relay map ip 4.4.4.2 102 broadcast
 frame-relay map ip 4.4.4.1 102
 no frame-relay inverse-arp
!
router eigrp 1
 redistribute ospf 1 metric 1500 10 255 1 13000 route-map MAP2EIGRP1
 network 4.4.4.0 0.0.0.7
 no auto-summary
```

#show file systems

- Zobrazí informace o souborových systémech na zařízení.
- Co znamená hvězdička ve výpisu? Zkuste připojit USB flash disk a zopakovat výpis.

```
R1#sh file systems
File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
      127992      126189     nvram     rw   nvram:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
*    8388604           0     flash     rw   flash:
           -           -    opaque     wo   syslog:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:
           -           -    opaque     ro   cns:
```

#show interfaces

- Příkaz vypíše podrobné informace o každém rozhraní na směrovači (obr. ukazuje výpis pro rozhraní Se0/0).

```
R1#show interfaces serial 0/0
Serial0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 3.3.3.2/29
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation FRAME-RELAY, loopback not set
  Keepalive set (10 sec)
  CRC checking enabled
  LMI enq sent  297, LMI stat recvd 294, LMI upd recvd 0, DTE LMI up
  LMI enq recvd 0, LMI stat sent  0, LMI upd sent  0
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DTE  segmentation inactive
  FR SVC disabled, LAPF state down
  Broadcast queue 0/64, broadcasts sent/dropped 0/0, interface broadcasts 0
  Last input 00:00:01, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:49:56
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     542 packets input, 26469 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     535 packets output, 25316 bytes, 0 underruns
```

#dir flash:/

- Příkaz vypíše obsah paměti Flash. Prozkoumejte, jaký je rozdil ve výpisech show flash a dir flash:/.

```
Router#dir
Directory of flash:/

    1  -rw-        2900  Feb 19 2011 00:29:18 +00:00  cpconfig-2811.cfg
    2  -rw-     2941440  Feb 19 2011 00:29:40 +00:00  cpexpress.tar
    3  -rw-        1038  Feb 19 2011 00:29:48 +00:00  home.shtml
    4  -rw-      115712  Feb 19 2011 00:29:58 +00:00  home.tar
    5  -rw-      527849  Feb 19 2011 00:30:10 +00:00  128MB.sdf
    6  -rw-     1697952  Feb 19 2011 00:30:26 +00:00  securedesktop-ios-3.1.1.45-k9.pkg
    7  -rw-      415956  Feb 19 2011 00:30:38 +00:00  sslclient-win-1.1.4.176.pkg
    8  -rw-        1048  Dec 21 2011 17:12:56 +00:00  config.text
    9  -rw-    65841548   Jul 2 2012 08:09:56 +00:00  c2800nm-advipservicesk9-mz.151-4.M3.bin

129753088 bytes total (58187776 bytes free)
```

#show inventory

- Zobrazí informace o instalovaných entitách na zařízení.
- Zkratky ve výpise: PID (Product Identifier) jedinečné číslo produktu, které může být použito při objednání náhradního dílu, VID (Version Identifier) číslo označující verzi produktu, SN (Serial Number) jedinečné seriálové číslo produktu přiřazené výrobcem.

```
R1#show inventory
NAME: "2621 chassis", DESCR: "2621 chassis, Hw Serial#: FTX0945W0MY
 (4279256517), Hw Revision: 0x202"
PID: 2621            , VID: 0x202, SN: FTX0945W0MY (4279256517)

NAME: "C2600 Mainboard", DESCR: "C2600 Mainboard"
PID:                 , VID: 2.2, SN: 2195568560

NAME: "Unknown", DESCR: "Unknown"
PID:                 , VID:    , SN:
```

#show controllers

- Příkaz vypiše ke každému rozhraní instalovanému na zařízení mnoho informací. Na obr. bylo specifikováno rozhraní Se0/0/0.
- Použití příkazu je zpravidla při řešení problému na fyzické vrstvě. Podstatné informace při zkoumání jsou typ kabelu připojený do rozhraní a nastavený clock rate.

```
R1#show controllers serial 0/0/0
Interface Serial0/0/0
Hardware is PowerQUICC MPC860
DCE V.35, clock rate 64000
idb at 0x81081AC4, driver data structure at 0x81084AC0
SCC Registers:
General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8
Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x00
Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E
```

Sběr nestálých dat ze směrovače - přehled příkazů

Sběr nestálých dat ze směrovače - přehled příkazů	
Název	**Příkaz**
show ip protocols	aktuálně běžící routovací protokoly
show running-config	běžící konfigurace v RAM
show banners	obsah nastavených bannerů
show memory	obsah operační paměti
show arp	ARP statistika k rozhraním
show ip access-list	obsah všech ip acess-listů
show ip nat translation	aktuální překlady adres
show ip dhcp binding	informace o pronájmu IP
show ip route	obsah routovací tabulky

Sběr nestálých dat ze směrovače - přehled příkazů

Sběr nestálých dat ze směrovače - přehled příkazů	
Název	**Příkaz**
show ip traffic	statistika provozu IP na zařízení
show tcp	informace o stavech spojení
show logging	záznamy o logování
show history	posledních 10 zadaných příkazů
show users	přihlášení uživatelé
show ssh	aktuální spojení přes SSH
show reload	naplánovaný restart zařízení
show ip interface	detailní informace o IP rozhraních
show ip interface brief	status a IP adresa rozhraních
show process memory	statistika využití paměti běžícími procesy
show process cpu	zobrazení o vytížení procesoru každým procesem

#show ip protocols

- Sítě, které jsou routovány, routovací protokoly běžící na zařízení, filtry, metriky, redistribuce mezi routovacími protokoly, čísla AS, ...

```
R1#sh ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1, ospf 1
  EIGRP NSF-aware route hold timer is 240s
  Automatic network summarization is not in effect
  Maximum path: 4
  Routing for Networks:
    4.4.4.0/29
  Routing Information Sources:
    Gateway         Distance      Last Update
    4.4.4.2              90       00:05:03
    4.4.4.3              90       00:05:51
  Distance: internal 90 external 170
```

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 7.7.7.1
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
    eigrp 1, includes subnets in redistribution
  Number of areas in this router is 2. 1 normal 0 stub 1 nssa
  Maximum path: 4
  Routing for Networks:
    3.3.3.0 0.0.0.7 area 0
    7.7.7.0 0.0.0.3 area 100
  Reference bandwidth unit is 100 mbps
  Passive Interface(s):
    Serial0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:19:24
    7.7.7.1              110      00:24:39
    6.6.6.1              110      00:23:35
    192.168.250.1        110      00:20:38
  Distance: (default is 110)
```

#show running-config

- Příkaz zajistí vypsání aktuálně běžící konfigurace. Zajímavé výsledky může přinést porovnání mezi soubory startup-config (Vaše konfigurace , která by měla běžet na zařízení) a running-config (konfigurace změněna útočníkem a aktuálně běžící na zařízení).

```
interface FastEthernet0/0
 ip address 7.7.7.1 255.255.255.252
 ip ospf priority 10
 duplex auto
 speed auto
!
interface Serial0/0
 ip address 3.3.3.2 255.255.255.248
 encapsulation frame-relay
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 cisco
 ip ospf priority 0
 clock rate 2000000
 frame-relay map ip 3.3.3.2 501
 frame-relay map ip 3.3.3.1 501
 frame-relay map ip 3.3.3.3 501
 no frame-relay inverse-arp
```

#show memory

- Příkaz vypíše obsah paměti RAM. Tím zachytíme velmi citlivá a důležitá data pro zkoumání. Při odpojení od energie o tyto data příjdeme.
- Výpis nám v podstatě ukáže vše, co běží za zařízení.

```
Router1#show memory
                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor   82CF8B00    14638456     9748680     4889776     3915712     3869148
      I/O    3A00000     6291456     1981736     4309720     4309720     4309692



          Processor memory

 Address      Bytes     Prev     Next Ref     PrevF    NextF Alloc PC  what
82CF8B00 0000342164 00000000 82D4C3C4 000  0        8364F5F0 81410B28  *Init*
82D4C3C4 0000020004 82CF8B00 82D51218 001  -------- -------- 80029B68  Managed Chunk Queue El
ements
82D51218 0000010004 82D4C3C4 82D5395C 001  -------- -------- 814038D8  List Elements
82D5395C 0000005004 82D51218 82D54D18 001  -------- -------- 81403918  List Headers
82D54D18 0000000048 82D5395C 82D54D78 001  -------- -------- 818448C0  *Init*
82D54D78 0000001504 82D54D18 82D55388 001  -------- -------- 8140E8D4  messages
82D55388 0000001504 82D54D78 82D55998 001  -------- -------- 8140E900  Watched messages
82D55998 0000001504 82D55388 82D55FA8 001  -------- -------- 8140E9A4  Watched Semaphore
82D55FA8 0000000484 82D55998 82D561BC 001  -------- -------- 8140E9F0  Watched Message Queue
82D561BC 0000001504 82D55FA8 82D567CC 001  -------- -------- 8140EA18  Watcher Message Queue
82D567CC 0000000068 82D561BC 82D56840 001  -------- -------- 81414C58  Resource Owner IDs
 --More--
```

#show ip route

- Příkaz vypíše obsah směrovací tabulky. V případě pateřních směrovačů může tato tabulka obsahovat stovky záznamů. Je nutné ověřit, zda směrovací tabulka obsahuje očekávané cesty. Nebo tam byl nějaký záznam záměrně „vstříknut“?

```
     3.0.0.0/29 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Serial0/0
     5.0.0.0/30 is subnetted, 1 subnets
C       5.5.5.0 is directly connected, FastEthernet0/0
     6.0.0.0/30 is subnetted, 1 subnets
C       6.6.6.0 is directly connected, FastEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
O E2    172.16.0.0 [110/20] via 3.3.3.3, 00:17:30, Serial0/0
     7.0.0.0/30 is subnetted, 1 subnets
O IA    7.7.7.0 [110/74] via 3.3.3.2, 00:21:30, Serial0/0
O IA 192.168.250.0/24 [110/75] via 3.3.3.2, 00:18:33, Serial0/0
     10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
O       10.0.2.0/24 [110/11] via 5.5.5.2, 00:22:00, FastEthernet0/0
O       10.0.3.0/24 [110/11] via 5.5.5.2, 00:22:04, FastEthernet0/0
O       10.0.0.0/22 is a summary, 00:22:04, Null0
O       10.0.1.0/24 [110/11] via 5.5.5.2, 00:22:04, FastEthernet0/0
O       10.0.128.0/24 [110/11] via 6.6.6.2, 00:23:34, FastEthernet0/1
O       10.0.128.0/22 is a summary, 00:23:34, Null0
O       10.0.129.0/24 [110/11] via 6.6.6.2, 00:23:34, FastEthernet0/1
O E1 192.168.0.0/24 [110/84] via 3.3.3.2, 00:03:04, Serial0/0
```

Měl tu být skutečně tento záznam?

#show ip interface

- Zobrazí konfiguraci všech rozhraní na směrovači s protokolem IP. IP adresa, stav rozhraní, aplikované access-listy, ...
- Výpis níže byl specifikován pro rozhraní Se0/0.

```
Serial0/0 is up, line protocol is up
  Internet address is 3.3.3.2/29
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is disabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP CEF Fast switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
```

#show access-list

- Vypíše obsah všech access listů konfigurovaných na směrovači (standard i extended).
- Název access-listu za příkazem výpiše konkrétní access-list.

```
R1#show access-lists
Extended IP access list 101
    permit ip 14.192.0.0 0.0.1.255 14.192.2.0 0.0.0.255
Extended IP access list 103
    permit tcp any 14.192.2.0 0.0.1.255 eq www
    permit tcp any 14.192.2.0 0.0.1.255 eq smtp
    permit tcp any 14.192.2.0 0.0.1.255 eq pop3
Extended IP access list 104
    permit tcp 14.192.2.0 0.0.1.255 14.192.0.0 0.0.1.255 eq www
    permit tcp 14.192.2.0 0.0.1.255 14.192.0.0 0.0.1.255 eq smtp
    permit tcp 14.192.2.0 0.0.1.255 14.192.0.0 0.0.1.255 eq pop3
Extended IP access list 105
    permit tcp any 14.192.0.0 0.0.1.255 eq www
    permit tcp any 14.192.0.0 0.0.1.255 eq smtp
    permit tcp any 14.192.0.0 0.0.1.255 eq pop3
    permit icmp any 14.192.0.0 0.0.1.255
```

#show arp

```
Router#sh arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.1            -   c062.6b4c.1b90  ARPA   FastEthernet0/0
Internet  192.168.0.3            0   f04d.a2eb.d2a3  ARPA   FastEthernet0/0
Internet  192.168.0.4            6   f04d.a2eb.d2a3  ARPA   FastEthernet0/0
Internet  192.168.0.5            0   f04d.a2eb.593b  ARPA   FastEthernet0/0
```

- Zobrazí vstupy v ARP tabulce. Pozor: Obr. výše ukazuje na stopy po ARP spoofingu. Obr. níže klasická ARP tabulka.

```
SW2#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.10.2            -   0002.4A43.AECD  ARPA   Vlan10
Internet  172.16.20.2            -   0002.4A43.AECD  ARPA   Vlan20
Internet  172.16.20.5            2   0006.2AB5.528D  ARPA   Vlan20
Internet  172.16.30.1            -   0002.4A43.AECD  ARPA   Vlan30
Internet  172.16.30.2            1   0090.0C57.E16E  ARPA   Vlan30
Internet  172.16.30.5            2   00E0.A394.38BB  ARPA   Vlan30
Internet  172.16.40.1            -   0002.4A43.AECD  ARPA   Vlan40
Internet  172.16.40.5            2   000A.F3BE.C4E7  ARPA   Vlan40
Internet  172.16.50.1            -   0002.4A43.AECD  ARPA   Vlan50
Internet  172.16.50.2            5   0090.0C57.E16E  ARPA   Vlan50
Internet  172.16.70.2            -   0002.4A43.AECD  ARPA   Vlan70
Internet  172.16.70.4            1   0001.649E.8176  ARPA   Vlan70
Internet  172.16.99.1            -   0002.4A43.AECD  ARPA   Vlan99
```

#show users

- Příkaz vypíše všechny přihlášené uživatele na zařízení (lokálně přes consoly i vzdáleně (Telnet, SSH, HTTPS).

```
R1#
R1#
R1#
R1#show users
    Line       User       Host(s)              Idle      Location
*  0 con 0                 idle                 00:00:00
  66 vty 0     filous     idle                 00:00:41 172.16.0.2
  67 vty 1     christie   idle                 00:00:23 172.16.0.2

  Interface    User               Mode         Idle     Peer Address

R1#
R1#
```

#show process cpu

- Detailní statistiky využití procesoru pro každý proces.
- Link k podrobnějšímu popisu významu zkratek: odkaz.

```
R1#show process cpu
CPU utilization for five seconds: 1%/0%; one minute: 0%; five minutes: 0%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         1          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2         644      2099        306  0.00%  0.00%  0.00%   0 Load Meter
   3         804       151       5324  1.21%  0.12%  0.09%   0 Exec
   4        2324      1072       2167  0.00%  0.01%  0.01%   0 Check heaps
   5           8         2       4000  0.00%  0.00%  0.00%   0 Pool Manager
   6           0         2          0  0.00%  0.00%  0.00%   0 Timers
   7           0         1          0  0.00%  0.00%  0.00%   0 Crash writer
   8           4       351         11  0.00%  0.00%  0.00%   0 Environmental mo
   9           4       183         21  0.00%  0.00%  0.00%   0 ARP Input
  10           0         2          0  0.00%  0.00%  0.00%   0 ATM Idle Timer
  11           0         2          0  0.00%  0.00%  0.00%   0 AAA high-capacit
  12           0         1          0  0.00%  0.00%  0.00%   0 AAA_SERVER_DEADT
  13           0         1          0  0.00%  0.00%  0.00%   0 Policy Manager
```

#show ip dhcp binding

- Tabulka záznamů ve výpise uvedená níže vzniká potom, co DHCP server přiděluje ze svého definovaného poolu IP adresy.
- Níže jsou v tabulce zobrazeny parametry: IP adresa, MAC adresa, doba pronájmu, typ přidělení (automaticky, manuálně).

```
Switch#sh ip dhcp binding
IP address       Client-ID/              Lease expiration        Type
                 Hardware address
10.10.10.3       00E0.A392.44E5          --                      Automatic
10.10.10.4       00E0.F92A.00AE          --                      Automatic
20.20.20.3       0002.1689.2428          --                      Automatic
20.20.20.4       000A.414A.5BB2          --                      Automatic
```

#show tcp a #show tcp statistic

- show tcp zobrazuje stavy všech TCP spojení jdoucích přes směrovač a show tcp statistic vypíše jednu společnou statistiku protokolu TCP pro směrovač.

```
R1#sh tcp

tty66, virtual tty from host 172.16.0.2
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 172.16.0.1, Local port: 23
Foreign host: 172.16.0.2, Foreign port: 16440

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xABB180):
Timer          Starts    Wakeups            Next
Retrans            31          0             0x0
TimeWait            0          0             0x0
AckHold            32          4             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3095194147  snduna: 3095194302  sndnxt: 3095194302     sndwnd:  17366
irs: 3992056932  rcvnxt: 3992057018  rcvwnd:      4043  delrcvwnd:     85
```

```
R1#sh tcp st
R1#sh tcp statistics
Rcvd: 202 Total, 0 no port
      0 checksum error, 0 bad offset, 0 too short
      127 packets (5660 bytes) in sequence
      0 dup packets (0 bytes)
      0 partially dup packets (0 bytes)
      0 out-of-order packets (0 bytes)
      0 packets (0 bytes) with data after window
      0 packets after close
      0 window probe packets, 0 window update packets
      0 dup ack packets, 0 ack packets with unsend data
      110 ack packets (4629 bytes)
Sent: 153 Total, 0 urgent packets
      8 control packets (including 0 retransmitted)
      128 data packets (4621 bytes)
      0 data packets (0 bytes) retransmitted
      0 data packets (0 bytes) fastretransmitted
      17 ack only packets (10 delayed)
      0 window probe packets, 0 window update packets
0 Connections initiated, 4 connections accepted, 4 connections established
4 Connections closed (including 0 dropped, 0 embryonic dropped)
0 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
```

#show banners

- Údajně by příkaz měl vypsat všechny nastavené bannery. Já takový příkaz neznám a výše uvedený příkaz nefunguje.
- Všechny nastavené bannery jsou vidět v konfiguračním souboru running-config nebo startup-config.
- Jaké typy banneru znáte? Jak se nastavují? Jaký text by měl být obsahem banneru?

```
**************************************************
This device is private property. Unauthorized use
prohibited under state and federal law.
**************************************************
```

#show history

- Příkaz vypíše defaultně historii deseti naposledy zadaných příkazů.
- Velikost bufferu lze změnit příkazem #terminal history size 0–250. Historie příkazů může být tedy úplně zrušená nebo naopak velmi bohatá.
- Patří mezi velmi nestálá data, protože historii příkazů můžeme sami zkoumáním přepsat.

```
R1#show history
 enable
 sh users
 show inventory
 sh users
 show inventory
 sh processes memory
 show process cpu
 sh reload
 sh tcp
 sh ip traffic
 sh memory
 sh banners
 conf t
 conf t
 sh tcp statistics
 show history
```

#show tech-support

- Tento příkaz při spuštění provede hned 8 příkazů.
- Mezi příkazy jsou: #show version, #show running-config, #show stacks, #show interface, #show controller, #show process cpu, #show process memory, #show buffer.
- Použijeme-li při zkoumání, na incidentem dotčeném systému, tři příkazy pro sběr dat místo dvaceti, nenecháme za sebou v systému takovou „spoušť“.

```
2 FastEthernet interfaces
128K bytes of NVRAM.
8192K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102

----------------- show running-config -----------------

Building configuration...
Current configuration : 747 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

Kopie souborů ze zařízení

Stálá data

- Předmětem zkoumání jsou především paměti NVRAM a Flash.
- V paměti NVRAM konfigurační soubor startup-config a v paměti Flash IOS. Případně i více operačních systémů.
- Ve Flash paměti může být uloženo prakticky cokoli (nikoli jen operační systémy).

Nestálá data

- Jak jste mohli vidět výše, existuje mnohem více příkazů pro sběr nestálých dat ze směrovače než je tomu u stálých dat.
- Z pamětí nás zajímá především obsah paměti RAM.

Pozor: při vytváření kopií souborů vypočteme kontrolní součet (hash) z originálu i z vytvořené kopie pro zajištění integrity.

Sběr stálých dat z přepínače - přehled příkazů

Sběr stálých dat z přepínače - přehled příkazů	
Název	**Příkaz**
show version	informace spojené s IOS
show startup-config	konfigurace uložená v NVRAM
show vlan	informace o virtuálních LANs
show file system	informace o souborovém systému
show interfaces	detailní informace o rozhraních
show diag	verze HW, sériové číslo součástí, chassis,...
show inventory	seriová čísla rozhraní, název, typ, chassis
show controllers	clock rate, DTE, DCE
show flash	velikost paměti Flash a IOS
dir flash:/	soubory a adresáře ve Flash
dir nvram:/	soubory a adresáře v NVRAM

Sběr nestálých dat z L2 a L3 přepínače - přehled příkazů

Sběr nestálých dat z přepínače - přehled příkazů	
Název	**Příkaz**
show ip protocols	aktuálně běžící routovací protokoly
show running-config	běžící konfigurace v RAM
show banners	obsah nastavených bannerů
show memory	obsah operační paměti
show arp	ARP statistika k rozhraním
show ip access-list	obsah všech ip acess-listů
show ip nat translation	aktuální překlady adres
show ip dhcp binding	informace o pronájmu IP
show ip route	obsah routovací tabulky

Sběr nestálých dat z L2 a L3 přepínače - přehled příkazů

Sběr nestálých dat z přepínače - přehled příkazů	
Název	**Příkaz**
show ip traffic	statistika provozu IP na zařízení
show tcp	informace o stavech spojení
show logging	záznamy o logování
show history	posledních 10 zadaných příkazů
show users	přihlášení uživatelé
show ssh	aktuální spojení přes SSH
show reload	naplánovaný restart zařízení
show ip interface	detailní informace o IP rozhraních
show ip interface brief	status a IP adresa rozhraních
show process memory	statistika využití paměti běžícími procesy
show process cpu	zobrazení o vytížení procesoru každým procesem

Sběr nestálých dat z L2 a L3 přepínače - přehled příkazů

Sběr nestálých dat z přepínače - přehled příkazů	
Název	**Příkaz**
show vlan	informace o VLANs
show mac-address-table	obsah CAM tabulky
show ip dhcp snooping binding	seznam přidělených IP
show port-security	seznam rozhraní s port-security
show spanning-tree	STP pro každou VLAN

- Jak si můžete všimnout, mnoho příkazů je totožných z příkazy uvedenými v sekci o směrovači.
- Příkazů je více, protože zabírají množinu L2 i L3 směrovačů. (V případě L2 zařízení by příkazy, jako show ip protocols, show ip route, atd. ze seznamu vypadly.)
- Čím více pokročilých technologií je v síti nastaveno (zabezpečení proti DHCP snoopingu, ARP spoofingu, FHRP, atd), tím jsou vyžadovány hlubší znalosti při zkoumání.

#show vlan

Základní charakteristika

- Zobrazí informace o VLAN's. Proč vytvářet VLAN's?
- Můžeme vidět, přidělení portů do jednotlivých VLAN's.
- Defaultně jsou všechny porty na Cisco přepínači ve VLAN1.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
10   10                               active
20   20                               active
30   30                               active
40   40                               active
50   serverFarm                       active    Fa0/6
70   webFarm                          active
99   native                           active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

#show mac-address-table

Základní charakteristika

- Vypíše obsah CAM tabulky. Syntax příkazu může být různá!
- Vydíte, za kterým portem je jaká MAC adresa (PC).
- Jak se v tabulce projeví MAC Address Flooding?

```
SW2#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0c8e.3201    DYNAMIC     Po1
   1    0000.0c8e.3202    DYNAMIC     Po1
   1    0000.0c8e.3203    DYNAMIC     Po1
   1    0060.2f83.7839    DYNAMIC     Po1
   1    00d0.bcc6.aa02    DYNAMIC     Fa0/5
   1    00d0.ff71.ed02    DYNAMIC     Fa0/4
  10    0060.2f83.7839    DYNAMIC     Po1
  20    0060.2f83.7839    DYNAMIC     Po1
  20    00d0.bcc6.aa02    DYNAMIC     Fa0/5
  30    00e0.a394.38bb    DYNAMIC     Fa0/5
  70    0001.649e.8176    DYNAMIC     Po1
  70    0002.167c.e12b    DYNAMIC     Po1
  70    0002.4a43.aecd    DYNAMIC     Po1
  70    0060.2f83.7839    DYNAMIC     Po1
  70    0090.0c57.e16e    DYNAMIC     Po1
  70    00d0.ff71.ed02    DYNAMIC     Fa0/4
```

#show spanning-tree

Základní charakteristika

- Vypíše informace o Spanning-tree protokolu na přepínači pro všechny nakonfigurované VLANs.
- Příkaz lze specifikovat pro konkrétní VLAN či rozhraní.
- Níže je na obr. část výpisu týkající se VLAN20.

```
VLAN0020
  Spanning tree enabled protocol rstp
  Root ID     Priority    24596
              Address     0090.0C57.E16E
              Cost        8
              Port        27(Port-channel 1)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    28692  (priority 28672 sys-id-ext 20)
              Address     0002.4A43.AECD
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Fa0/4            Desg FWD 19        128.4    P2p
Fa0/5            Desg FWD 19        128.5    P2p
Po1              Root FWD 8         128.27   Shr
```

#Kopie souborů ze zařízení

Stálá data

- Zájímá nás především obsah paměti NVRAM a Flash.
- V paměti NVRAM konfigurační soubor startup-config a v paměti Flash IOS. V paměti Flash je nově soubor Vlan.dat (pro jednoduchost, může být i směrovači).
- Ve Flash paměti může být uloženo prakticky cokoli, proto děláme kopii všeho.

Nestálá data

- Při sběru nestálých dat nás zajímá především obsah paměti RAM.
- Velmi užitečné mohou být výpisy informující o pokusech obelstít L2 port-securitu.

Pozor: při vytváření kopií souborů vypočteme kontrolní součet (hash) z originálu i z vytvořené kopie pro zajištění integrity.

Výsledky analýzy

- Všechna stálá i nestálá data ze směrovačů a přepínačů jsou již zajištěna.
- Výsledkem analýzy má být zachytit chování na základě získaných podkladů a odpověď tak na několik otázek.
- Forezní analýza prakticky zpětně rekonstruje všechny události (na základě důkazů), které vedli k daným událostem.
- Jde o to určit: co, kdy, jak se to stalo. Výsledkem je i proč se to vůbec mohlo stát (např. nedostatečná nebo chybná konfigurace).
- Jedním z výsledků analýzy může být identifikace škodlivého chování. V tom případě mezi výsledky analýzy patří i určit, kdo (IP adresa, hostname, . . .) např. pronikl do systému.
- Zkoumání je prováděno vždy na kopiích originálních dat. Všechny procesy zkoumání musí být možné zopakovat.

Kde a co při zkoumání hledat

Příklady

- Pokud nebylo na zařízení od posledního restartu pracováno (což se dozvíme od administrátorů), může být zajímavé zkotrolovat historii naposledy zadaných příkazů.
- Odpověď na otázku zda-li bylo zařízení restartováno najdeme ve výpisu show version.
- Víme, že na zařízení je spuštně naše konfigurace (načtena z NVRAM) neznamená, že skutečně tomu je i po incidentu. Porovnejte obě konfigurace.
- Nastavená L2 port securita může prozradit pokusy o připojení neznámého zařízení do naší sítě.
- Zkontrolujte zda nedošlo k záměrnému poškození operačního systému (např. Rootkit). Ověřte porovnáním hash funkcí.

Kde a co při zkoumání hledat

Příklady

- Odpovídá verze nahrátého operačního systému v zařízení dokumentaci?
- ARP cache na zařízení může vykazovat známky útoku ARP spoofing (např. dvě různé IP adresy mají stejnou MAC adresu). „Otrávená cache“ bude i na PC „oběti“.
- Zkontrolujte obsah směrovací tabulky. Nejedná-li se o páteřní směrovač, nemělo by být náročné ověřit zda se v tabulce neobjevila záměrně „injeknutá“ routa.
- Logy mohou mnoho napovědět. Např. pokusy o příhlášení, kde byl mnohosetkrát překročen nastavený limit na zadání chybného hesla (např. brute-force útok) nebo zánamy o konfiguraci zařízení probíhající ve tři hodiny ráno (kdy z administrátorů nikdo nic nedělal).

Kde a co při zkoumání hledat

Příklady

- Co Vás může zajímat u access-listů kromě kontroly zda nebyl nějaký access-list upraven?
- Ověřte, zda použítá kombinace HW a operačního systému (IOS), nemá nějaké známé bezpečnostní „díry“, kterých mohl útočník využít. To může významně zkrátit čas zkoumání. Nenaistalované „patche“ mohou odpověď na otázku, jak se útočník k nám dostal.
- Kontrola rolí ve spanning-tree (proti dokumentaci sítě) může odhalit pokusy o změnu síťové topologie. Kdo je Root Bridge? Jak lze ovlivnit výběr Root Bridge v síti?
- Obsah CAM tabulky a velký traffic na portu může snadno odhalit MAC Address Flooding.

Děkuji za pozornost!