SIECI KOMPUTEROWE – LABORATORIUM 079

Tematyka:
Czynności konserwacyjne i monitorowanie ruterów Cisco. Kontrola i odzyskiwanie IOS, zarządzanie konfiguracjami, zdejmowanie haseł. Monitorowanie ruchu sieciowego i procesów.

Zadanie A: Odzyskiwanie obrazu IOS - serwer TFTP / FTP

1. Należy przygotować do pracy ruter Cisco, łącząc go okablowaniem w układzie PC-ruter.
2. Serwer TFTP umożliwia wymianę danych pomiędzy ruterem i zasobami zewnętrznymi. Należy go uruchomić i przygotować w katalogu zasobów serwera obraz Cisco IOS zgodny z wersją rutera. Sewer nie wymaga autoryzowania.
3. Należy połączyć kabel konsoli do odpowiedniego gniazda w ruterze i stacji PC. Następnie uruchomić ruter wcześniej nawiązując połączenie przez port szeregowy. Po uzyskaniu karetki należy zaktywować tryb uprzywilejowany- komenda *enable* lub *en*.
4. Należy upewnić się, czy ilość pamięci flash w ruterze wystarcza do umieszczenia w niej obrazu (uwaga - w przypadku CatOS nazwa tej pamięci to często bootflash):
   Ruter#show flash:
   Ruter#dir flash:
5. W przypadku obecności w ruterze gniazd wymiennych kart CompactFlash lub PCMCIA możliwe jest korzystanie:
   - z systemów plików o nazwach slot0:, slot1: itp. w sytuacjach, gdy w gnieździe znajduje się karta CompactFlash lub PCMCIA Flash Card (karty te posiadają system zapisu liniowego)
   - z systemów plików o nazwach disk0:, disk1: itp. w sytuacjach, gdy w gnieździe znajduje się karta PCMCIA ATA Flash PC Card (karty te emulują dysk):
   Ruter#dir disk0:
   Ruter#format disk0:
   Ruter#squeze slot0:
   W razie potrzeby - można skasować tylko pojedyncze pliki
   Ruter#delete flash:nazwa_pliku

6. W przypadku braku nośnika wymiennego w ruterze możliwe jest pobranie obrazu ze zdalnego serwera TFTP. W tym celu należy przygotować interfejs IP rutera konfigurując go tak, aby była możliwość komunikowania się z serwerem zdalnym dostarczającym usługę TFTP:
   Router(config)#int fa 0/1
   Router(config-if)#ip address 200.200.200.5 255.255.255.0
   Router(config-if)#no shut

Po uruchomieniu TFTP na komputerze zdalnym (w przykładzie – pod adresem IP 200.200.200.1) i umieszczeniu tam w katalogu udostępnianym przez TFTP pliku z obrazem IOS (w przykładzie: *c2800-mz.124-4.bin*), należy użyć komendy kopiującej plik z TFTP do pamięci flash rutera:

Router#copy tftp:// 200.200.200.1/c2800-mz.124-4.bin flash:

Po zakończeniu kopiowania należy zweryfikować zawartość flash:
Router#dir flash:
oraz zlecić użycie skopiowanego obrazu po ponownym uruchomieniu rutera:
Router(config)#boot system flash:c2800-mz.124-4.bin
Router(config)#exit
Na koniec należy zapisać konfigurację I uruchomić ponownie ruter – już z nowym obrazem IOS:
Router#write memory
Router#reload

7. W niektórych IOS istnieje możliwość wykorzystania serwera FTP (zamiast TFTP) do wymiany danych. W tej sytuacji należy dodatkowo skonfigurować dane identyfikujące użytkownika FTP:
   Ruter#config terminal
   Ruter(config)#ip ftp username cisco
   Ruter (config)#ip ftp password cisco
   Ruter (config)#end
   i następnie uruchomienia kopiowania z użyciem FTP:
   Ruter#copy ftp: running-config

Zadanie B: Odzyskiwanie obrazu IOS - pamięci CompactFlash, USB

1. Zależnie od wyposażenia rutera możliwe jest posługiwanie się pamięciami na mediach typu CompactFlash, USB.
2. Aby sprawdzić dostępne systemy plików (media) należy użyć komendy:
   Ruter#show filesystems
   na liście pamięci USB figurują pod nazwami usbflash0:, usbflash1: natomiast Compact Flash: slot0:, slot1: - zgodnie z opisami gniazd na obudowie rutera.
3. Możliwe jest wymuszanie pobierania systemu oraz konfiguracji rutera z konkretnego medium (inna niż domyślne, czyli pobieranie pamięci wbudowanej z flash i nvram). zmiana źródła konfiguracji:
   Ruter(config)# boot config filesystem:plik
   inna lokalizacja obrazu IOS:
   Ruter(config)# boot system filesystem:plik
4. Przeniesienie systemu na kartę compact Flash: pobierz od prowadzącego kartę CompactFlash lub PCMCIA i umieść ją w ruterze. Sformatuj kartę, np.:
   Ruter#format slot0:
   lub
   Ruter#format disc0:
5. Przenieś obraz z pamięci flash/bootflash na kartę, np.;
   Ruter#copy flash:nazwa_pliku slot0:

skonfiguruj ruter tak, aby uruchomił swój system operacyjny z obrazu zawartego na karcie:
Ruter(config)#boot system slot0:nazwa_pliku
Ruter(config)#write memory
Ruter#reload
po wykonaniu eksperymentu cofnij ustawienia.
Ruter(config)#no boot system slot0:nazwa_pliku
Ruter(config)#write memory

Zadanie C: Disaster recovery - rekonstrukcja obrazu IOS, gdy IOS nie startuje.

1. W przypadku, gdy uszkodzenie zawartości pamięci flash uniemożliwia uruchomienie IOS nie będzie możliwości posługiwania się jego komendami tego systemu w celu aktualizacji flash. W takiej sytuacji należy wykorzystać konsolę rommon. Uruchomienie konsoli: po włączeniu zasilania należy przytrzymać klawisz **break** (w przypadku niepowodzenia **ctrl-break**). Ruter nie uruchomi wówczas ładowania IOS, lecz wejdzie w tryb rommon:
   rommon 1 >
2. Najbardziej popularną metodą *Disaster recovery* jest użycie serwera TFTP dostarczającego nowy obraz flash. Możliwe jest także (zależnie od dostępnych w ruterze rozszerzeń) stosowanie łącza USB, kart PCMCIA a w starszych wersjach sprzętu transmisji RS-232 Xmodem.
3. W celu pobrania nowego obrazu IOS przez TFTP należy skonfigurować zmienne środowiskowe rommon określające parametry połączenia z TFTP i parametry pliku (zmienne określają także dane lokalnego interfejsu IP rutera):
   rommon 1 > IP_ADDRESS=200.200.200.1
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=200.200.200.254
rommon 4 > TFTP_SERVER=200.200.200.5
rommon 5 > TFTP_FILE=c2800-mz.124-4.bin
4. Następnie należy uruchomić komendę kopiująca i likwidującą poprzednią zawartość flash (!):
   rommon 6 > tftpdnld
5. Gdy chcemy zapisać zmienne w NVRAM (czyli trwale, do ewentualnego wykorzystania w przyszłości) stosujemy komendę:
   rommon 7 > sync
6. Następnie uruchamiamy system od początku:
   rommon 8 > reset

Zadanie D: Usunięcie utraconego hasła

1. W przypadku utraty hasła i konieczności uruchomienia systemu bez utraty konfiguracji (hasło zawarte jest w pliku konfiguracji) konieczne jest uruchomienie rutera w trybie rommon (jak w zadaniu B).

2. Następnie należy skonfigurować rejestr startowy rutera z wartości standardowej 0x2102 na 0x2142 (przy tej wartości ruter załaduje system operacyjny, ale nie załaduje konfiguracji z NVRAM więc nie będzie także wymagał hasła):
   rommon 1 > confreg 0x2142
3. Następnie należy wykonać reset rutera:
   rommon 2 > reset
4. Po załadowaniu IOS możemy już wejść do trybu uprzywilejowanego bez podawania hasła (konfiguracja, w tym hasło, nie zostały załadowane):
   Ruter>enable
   Ruter#
   Po przejściu w tryb uprzywilejowany można załadować konfigurację:
   Ruter#copy startup-config running-config
   lub w postaci skróconej:
   Ruter#copy st ru
   W efekcie system wraz z konfiguracją zostanie załadowany, a my jesteśmy "w środku" - czyli w trybie uprzywilejowanym, choć nie podaliśmy hasła.
5. W kolejnym kroku należy usunąć załadowane i nieznane hasło z bieżącej konfiguracji:
   Ruter#conf t
   Ruter(config)#no enable password
   Ruter(config)#no enable secret
6. Po usunięciu - zapisać konfigurację w NVRAM (już bez hasła):
   Ruter#copy running-config startup-config
7. Ostatnią czynnością jest przywrócenie pierwotnej wartości rejestru konfiguracji
   Ruter#conf t
   Ruter(config)#config-register 0x2102
   Po przeładowaniu systemu (*Ruter#reload*) ruter uruchomi się w trybie normalnym, nie pytając już jednak o hasło.
8. Aby sprawdzić zawartość rejestru startowego rutera w czasie pracy IOS stosujemy polecenie:
   Ruter#show version
   Ostatnia linia wyświetlanego wtedy raportu informuje o treści rejestru.

Zadanie E: Debugging system. Embedded packet capture z transmisją TFTP

1. Usługę TFTP można także wykorzystać jako odbiorcę danych pochodzących z systemu monitorowania ruchu śledzonego. Dane te to datagramy przechwycone w wybranych interfejsach. Zaletą rozwiązania jest fakt, że datagramy te można po przesłaniu na serwer TFTP analizować przy użyciu oprogramowania śledzącego typu Wireshark.
2. Aby uruchomić śledzenie należy zaalokować w pamięci rutera bufor na określoną ilość datagramów określonej wielkości (bufor jest cykliczny, wiec nie jego przepełnienie nie zagraża stabilności procesu śledzenia):
   Ruter#monitor capture buffer bufor size 2048 max-size 4000 circular
   Następnie należy zdefiniować punkt śledzenia (obserwowany interfejs) i powiązać go z buforem:
   Ruter#monitor capture point ip cef punkt fastEthernet 0/0 both

Ruter#monitor capture point associate punkt bufor
Opcjonalnie można także nałożyć filtr dla pakietów do śledzenia – przy użyciu listy kontrolnej (ACL), np.:
Ruter(config)#ip access-list extended filtr
Ruter(config-acl)#permit ip host 200.200.201.1 host 200.200.201.5
Ruter(config-acl)#end
Ruter#monitor capture buffer bufor filter access-list lista
W końcu należy uruchomić śledzenie, spowodować wystąpienie ruchu sieciowego podlegającego śledzenie, zatrzymać śledzenie i wysłać wyniki na serwer TFTP
Ruter#monitor capture point start pun
...
oczekiwanie na przechwytywany ruch sieciowy
...
Ruter#monitor capture point stop punkt
Ruter#monitor capture buffer bufor export tftp://200.200.200.1//Capture.pcap
Ruter#monitor capture buffer bufor clear

Po uzyskaniu wyników należy otworzyć plik *Capture.pcap* w programie Wireshark i dokonac analizy przechwyconych datagramów.
Ponocne komendy diagnostyczne:
Ruter#show monitor capture buffer all parameters
Ruter#show monitor capture point all
Ruter#show monitor capture buffer bufor
Ruter#show monitor capture buffer bufor dump

3. Moduł monitorowania zdarzeń wewnątrz systemowych Cisco IOS oparty jest o tzw. sesje. Komunikaty raportujące o zdarzeniach , będące wynikiem śledzenia są umieszczane na konsoli. Aktywowanie śledzenia odbywa się za pomocą ogólnie znanej komendy debug, np.:
Router#debug ip icmp
Sprawdzenie aktywnych sesji śledznia
Router#show debug
Deaktywacja wszystkich sesji:
Router#no debug All
Możliwe jest śledzenie warunkowe, zależne od interfejsu, np:
Router#debug condition interface FastEthernet 0/0
Sprawdzenie:
Router#show debug condition
Przetestuj mechanizm śledzenia zdarzeń w różnych jego wariantach.