System operacyjny Linux

Paweł Rajba

pawel.rajba@continet.pl
http://kursy24.eu/

Zawartość modułu 11

- Konfiguracja sieci
  - Nazewnictwo i uruchamianie
  - Polecenie ifconfig
  - Aliasy
  - Pliki konfiguracyjne
- Narzędzia sieciowe
  - ping, traceroute
  - route, arp
  - nmap, netstat

Konfiguracja sieci

- Nazewnictwo
  - eth0, eth1, ...
  - ppp0, ppp1, ...
- Uruchamianie
  - /etc/init.d/network start|stop|restart|status
  - ifup interfejs
  - ifdown interfejs
  - ifstatus interfejs

Konfiguracja sieci

- ifconfig – konfiguracja interfejsów sieciowych
  - Składnie:
    - ifconfig [interfejs | -a]
    - ifconfig interfejs [up | down]
  - Opcje:
    - -a – wyświetlenie informacji o wszystkich interfejsach
    - up – włączenie interfejsu
    - down – wyłączenie interfejsu

Konfiguracja sieci

- ifconfig c.d.
  - Składnia:
    - ifconfig interfejs adres [opcje]
  - Opcje:
    - netmask adres — ustawia maskę,
    - broadcast adres — ustawia adres rozgłoszenia,
    - [-]arp — ustawia urządzenie, żeby [nie] odpowiadało na zadania protokołu arp,
    - hw ether MAC — ustawia adres MAC

Konfiguracja sieci

- Aliasy
  - Tworzymy poprzez nazwę ethX:Y
- Przykłady
  - ifconfig eth0 down
  - ifconfig eth0 192.168.0.10 netmask 255.255.255.0\ broadcast 192.168.0.255
  - ifconfig eth0 up
  - ifconfig eth0:0 192.168.0.11

Konfiguracja sieci

- Pliki konfiguracyjne
  - /etc/networks
  - /etc/sysconfig/network/config
  - /etc/sysconfig/network/ifcfg.template
  - /etc/sysconfig/network/ifcfg-eth0
  - /etc/sysconfig/network/routes
  - /etc/sysconfig/network/ifroute-config

Konfiguracja sieci

- /etc/networks
  - Zawiera nazwy sieci
  - Przydatne przy starcie systemu, gdy nie ma jeszcze dostępnych serwerów nazw
  - Przykładowe wpisy:
    - loopback 127.0.0.0
    - lokalna 192.168.0.0

Konfiguracja sieci

- /etc/sysconfig/network/config
  - Zawiera ogólne informacje
  - Wpisy są postaci zmienna=wartość
  - Przykładowe zmienne:
    - USE_SYSLOG="yes" | "no" (czy używać sysloga, czy na stderr)
    - MODIFY_RESOLV_CONF_DYNAMICALLY="yes" | "no" (czy pozwalać np. ppp0 na dynamiczną modyfikację pliku /etc/resolv.conf)
    - FIREWALL="yes" | "no" (czy włączyć SuSEfirewall przy starcie sieci)

Konfiguracja sieci

- /etc/sysconfig/network/ifcfg-ethX
  - Konfiguracja interfejsu sieciowego
  - Można się spotkać z plikiem postaci ifcfg-eth-id-*adres-MAC*
  - Konfiguracja polega na ustawieniu szeregu zmiennych
  - Szablon konfiguracji interfejsu znajduje się w /etc/sysconfig/network/ifcfg.template

Konfiguracja sieci

- /etc/sysconfig/network/ifcfg-ethX c.d.
  - Przykładowe zmienne:
    - STARTMODE="onboot"|"manual"|"hotplug"|"off"
    - BOOTPROTO="static"|"dhcp"
    - IPADDR=adres-ip/bity-maski
    - NETMASK=maska
    - PREFIXLEN=ilość-bitów-maski
    - BROADCAST=adres-rozgłoszenia
    - MTU=rozmiar

Konfiguracja sieci

- Ścieżki sieciowe – pliki:
  - /etc/sysconfig/network/routes
    – ustala ścieżki dla wszystkich interfejsów
  - /etc/sysconfig/network/ifroute-eth0
    – ustala ścieżkę dla wybranego interfejsu
  - Czytane przez polecenie ifup-route, które jest uruchamiane przez polecenie ifup

Konfiguracja sieci

- Ścieżki sieciowe – pliki c.d.
  - Konfiguracja plików
    - Pierwsza kolumna – określa adres docelowy; słowo default określa ścieżkę domyślną
    - Druga kolumna – określa bramę; jeśli nie chcemy podawać bramy, piszemy 0.0.0.0
    - Trzecia kolumna – określa maskę dla adresu
    - Czwarta kolumna – określa interfejs, przez który będą szły pakiety

Konfiguracja sieci

- Ścieżki sieciowe – pliki c.d.
  - Przykład konfiguracji pliku routes

```
127.0.0.0       0.0.0.0         255.255.255.0   lo
204.12.35.0     0.0.0.0         255.255.255.0   eth0
default         204.12.35.1     0.0.0.0         eth0
192.168.0.0     10.2.0.254      255.255.0.0     eth1
```


Narzędzia sieciowe

- ping – wysyła pakiety ICMP typu echo
  - Składnia
    - ping [-c liczba] [-i liczba] [-s rozmiar] [-n] host
  - Opcje
    - -c liczba — liczba określa, ile pakietów ma być wysłanych,
    - -i liczba — liczba określa, co ile sekund będą wysyłane pakiety; czas poniżej 0.2 sekundy jest dostępny tylko dla użytkownika root,
    - -s rozmiar — określa ilość wysyłanych danych w pakietach; domyślnie jest 56 bajtów (+8 bajtów nagłówka daje pakiety rozmiaru 64 bajty),
    - -n — adresy IP nie będą zamieniane na nazwy hostów.

Narzędzia sieciowe

- traceroute – sprawdza trasy pakietów
  - Składnia
    - traceroute [-I interfejs] [-n] [-F] host [rozmiar]
  - Opcje
    - -I interfejs — określa, przez który interfejs będą wysyłane pakiety; domyślnie wartość jest pobierana z tablicy routingu,
    - -n — przy wyświetlaniu informacji o hostach adresy IP nie będą zamieniane na odpowiadające im nazwy,

Narzędzia sieciowe

- traceroute c.d.
  - Opcje c.d.
    - -F — ustawia bit zakazujący fragmentowania pakietu; ustawienie tego bitu sprawia, ze routery pośredniczące nie będą próbowały podzielić pakietu, jeśli okaże się, ze jego rozmiar przekracza rozmiar określony przez MTU,
    - host — jest to parametr wymagany, i określa on miejsce, do którego ścieżkę chcemy sprawdzić; możemy podać adres IP lub nazwę hosta,
    - rozmiar — określa rozmiar pakietów, które będą wysyłane; w połączeniu z opcja -F pozwala ustalić rozmiar MTU w sieci; domyślnie rozmiar jest 40.

Narzędzia sieciowe

- route – ustawia ścieżki dla pakietów
  - Składnia
    - route {add | del} [-net | -host] adres [netmask maska] [gw brama] [[dev] int]
  - Opcje
    - add, del — określa odpowiednio, czy ścieżkę dodajemy, czy usuwamy,
    - -net — adresem docelowym jest sieć,
    - -host — adresem docelowym jest host,
    - adres — określa cel ścieżki,
    - netmask maska — określa maskę dla adresu,

Narzędzia sieciowe

- route – ustawia ścieżki dla pakietów c.d.
  - Opcje c.d.
    - gw brama — określa bramę, przez która powinny przechodzic pakiety,
    - dev int — określa interfejs, przez który będą wysyłane pakiety dla ścieżki.
  - Przykłady
    - route add default gw 192.168.0.254 eth0
    - route add -net 192.168.3.0 netmask 255.255.0.0 eth1
    - route add -host 192.168.0.30 gw 192.168.0.2 eth0
    - route del 192.168.0.30

Narzędzia sieciowe

- route – wyświetla tablicę routingu
  - Składnia
    - route [-n]
  - Opcje
    - -n – adresy nie będą zamieniane na odpowiadające im nazwy

Narzędzia sieciowe

- route – wyświetla tablicę routingu c.d.
  - Pola wyniku
    - Destination — adres docelowy scieżki, czyli host lub sieć,
    - Gateway — adres bramy lub, jeśli nie ma bramy – "*",
    - Genmask — maska dla adresu, przy czym, maska dla hosta to 255.255.255.255, a dla domyślnej scieżki to 0.0.0.0,
    - Flags — dodatkowa informacja o scieżce, przykładowe flagi:
      - – U — ścieżka jest aktywna,
      - – H — adresem docelowym jest host,
      - – G — pakiety przechodzą przez bramę,

Narzędzia sieciowe

- route – wyświetla tablicę routingu c.d.
  - Pola wyniku
    - Metric, Ref, Use — zwykle nie uzywane; nie bedziemy omawiac,
    - IFace — interfejs, przez który przechodza pakiety.
  - Przykład

```
Kernel IP routing table
Destination Gateway         Genmask         Flags ... Iface
10.5.5.0    *               255.255.0.0     U     ... eth1
dialog      *               255.255.0.0     U     ... eth0
default     81.168.215.1    0.0.0.0         UG    ... eth0
```


Narzędzia sieciowe

- arp - ma zastosowanie, gdy znamy czyjś adres IP, a chcemy poznać adres MAC.
  - Składnia
    - arp [-vn] [-H typ] [-i if] -a [host]
      wydrukowanie lokalnej tablicy odwzorowań
    - arp [-v] [-i if] -d host
      usunięcie adresu MAC dla podanego hosta
    - arp [-v] [-H typ] [-i if] -s host mac_adr [temp]
      ręczne wprowadzenie skojarzenia
    - arp [-vn] [-H typ] [-i if] -f [plik]
      wprowadzenie konfiguracji z pliku; default: /etc/ethers
      plik ma dwie kolumny w wierszu: adresMAC adresIP

Narzędzia sieciowe

- arp c.d.
  - Opcje:
    - -a — wypisanie wszystkich wpisów,
    - -v — wypisywanie dodatkowych komunikatów,
    - -n — adresy IP nie będą zamieniane na odpowiadające im nazwy,
    - -H typ — określa rodzaj urządzenia; domyślnie jest to ether, a inne dostępne to: arcnet, pronet, ax25, netrom,
    - -i if — wydrukowane zostaną wpisy skojarzone z określonym interfejsem lub przy ustawianiu, dany adres zostanie skojarzony z odpowiednim interfejsem

Narzędzia sieciowe

- arp – przykłady:

```
bobek:~ # arp -s 192.168.0.1 80:60:77:24:14:11 temp
bobek:~ # arp -s 192.168.0.2 80:60:77:24:14:20 temp
bobek:~ # arp -s 192.168.0.3 80:60:77:24:14:30 temp
bobek:~ # arp -a
brama (192.168.0.1) at 80:60:77:24:14:11 [ether] on eth0
kenia (192.168.0.2) at 80:60:77:24:14:12 [ether] on eth0
aster (192.168.0.3) at 80:60:77:24:14:13 [ether] on eth0
bobek:~ # arp -d 192.168.0.3
bobek:~ # arp -d 192.168.0.2
bobek:~ # arp -a -i eth0
brama (192.168.0.1) at 80:60:77:24:14:11 [ether] on eth0
kenia (192.168.0.2) at <incomplete> on eth0
aster (192.168.0.3) at <incomplete> on eth0
```


Narzędzia sieciowe

- nmap – skanuje porty
  - Składnia
    - nmap [-v] [opcje_skanowania] [inne_opcje] [opcje_czasowe]
  - Opcje skanowania
    - -sS — skanowanie oparte na wysyłaniu pakietów SYN,
    - -sT — skanowanie oparte na wywoływaniu funkcji connect(),
    - -sP — skanowanie oparte na wysyłaniu pakietów ICMP,
    - -sU — skanowanie oparte na wysyłaniu pakietów UDP,
    - -sO — skanowanie oparte na wysyłaniu surowych nagłówków IP.

Narzędzia sieciowe

- nmap c.d.
  - Opcje ogólne
    - -O — program będzie próbował ustalić szczegóły dotyczące systemu operacyjnego,
    - -A — jest to skrót dla kilku opcji ustalających jak najwięcej szczegółów,
    - -oN plik — wyniki zostaną dodatkowo przekierowane do pliku o nazwie plik,
    - -oG plik — wyniki zostaną dodatkowo przekierowane do pliku o nazwie plik w postaci przyjaznej dla programu grep,
    - -oX plik — wyniki zostana dodatkowo przekierowane do pliku XML o nazwie plik,

Narzędzia sieciowe

- nmap c.d.
  - Opcje ogólne c.d.
    - -oA plik — wyniki zostaną dodatkowo przekierowane do plików wszystkich typów
      - normalny: plik.nmap
      - dla grepa: plik.gnmap
      - xml: plik.xml
    - -p porty — okreslamy porty, które chcemy skanowac; przykłady: "-p 23", "-p 21-23, 25, 100-120",
    - -n — adresy IP nie beda zamieniane na nazwy hostów,

Narzędzia sieciowe

- nmap c.d.
  - Opcje ogólne c.d.
    - -R — adresy IP zawsze będą zamieniane na nazwy hostów (normalnie zamieniane są adresy dostępnych hostów),
    - -r — nakazuje nie zmieniać (losowo) kolejności portów, w jakiej będą skanowane,
    - --randomize_hosts — hosty będą skanowane w losowej kolejności; utrudnia to detekcje faktu, że ktoś skanuje komputery w sieci.

Narzędzia sieciowe

- nmap c.d.
  - Opcje czasowe
    - -T Paranoid|Sneaky|Polite|Normal|Aggressive|Insane — określa szybkość w jakiej skanowanie będzie wykonywane:
      - Paranoid — pakiety są wysyłane co co najmniej 5 minut, a skanowanie jest serializowane,
      - Sneaky — podobnie jak poprzedni rodzaj skanowania, przy czym pakiety są wysyłane co 15 sekund,
      - Polite — w tym skanowaniu próby są serializowane co ok. 0.4 sekundy,

Narzędzia sieciowe

- nmap c.d.
  - Opcje czasowe c.d.
    - -T c.d.
      - Normal — skanowanie normalne, które jest wykonywane najszybciej jak się da, przy czym bez przeciążania sieci oraz bez przeoczenia hostów lub portów,
      - Aggressive — skanowanie, które jest trochę szybsze; tutaj niezbędna jest dosyć szybka sieć,
      - Insane — skanowanie najbardziej agresywne, w którym możemy przeoczyć niektóre hosty lub porty; tutaj konieczna jest bardzo szybka sieć,

Narzędzia sieciowe

- nmap c.d.
  - Opcje czasowe c.d.
    - --scan_delay milisekundy — określa czas, który nmap ma odczekiwać pomiędzy kolejnymi próbami; możemy w ten sposób zmniejszyć obciążenie sieci oraz zmniejszyć ryzyko zostania wykrytym,
  - Przykłady:
    - nmap -v komputer.domena.com
    - nmap -sS -sU -O komputerek
    - nmap -sS -O 192.168.0.0/24
    - nmap -sT -p 22,53,110,143,4564 198.116.*.1-127
    - nmap -v --randomize_hosts -p 80 *.*.2.3-5

Narzędzia sieciowe

- netstat (1) – informacje o gniazdach
  - Składnia
    - netstat [-t] [-u] [-w] [-l] [-a] [-n] [-e] [-p] [-c]
  - Opcje
    - -t – gniazda połączeń na protokole tcp
    - -u – gniazda połączeń na protokole udp
    - -w – gniazda połączeń na surowym prokole ip (raw ip)
    - -l – gniazda serwerów
    - -a – gniazda serwerów i połączeń
    - -n – adresy ip nie będą zamieniane na nazwy
    - -e – dodatkowe informacje

Narzędzia sieciowe

- netstat (1) c.d.
  - Opcje c.d.
    - -p – identyfikacja procesów (PID + nazwa programu)
    - -c – wywoływanie polecenia cyklicznie co sekundę
  - Przykład
    - netstat -tunap

Narzędzia sieciowe

- netstat (1) c.d.
  - Opis pól wyniku
    - Proto – protokół używany przez gniazdo (tcp, udp, raw)
    - Recv-Q – liczba bajtów nie pobranych przez program użytkownika podłączony do gniazda
    - Send-Q – liczba bajtów nie potwierdzonych przez zdalny host
    - Local Address – adres i port lokalnego hosta
    - Foreign Address – adres i port zdalnego hosta

Narzędzia sieciowe

- netstat (1) c.d.
  - Opis pól wyniku
    - State – stan gniazda (zwykle tylko dla tcp)
      - ESTABLISHED – połączenie nawiązane
      - SYN_SENT – gniazdo próbuje nawiązać połączenie
      - SYN_RECV – żądanie nawiązania połączenia przyszło z sieci (jeśli jest tego za duzo = niedobrze)
      - TIME_WAIT – połączenie jest zamykane
      - CLOSED – gniazdo jest zamknięte
      - LISTEN – gniazdo nasłuchuje
      - UNKNOWN – stan gniazda jest nieznany
    - User – użytkownik będący właścicielem gniazda
    - PID/Program name – pid i nazwa procesu będących właścicielem gniazda

Narzędzia sieciowe

- netstat (2) – lista ścieżek dla pakietów
  - Składnia
    - netstat –r [-n] [-c]
  - Opcje
    - -n – adresy IP nie będą zamieniane na nazwy
    - -c – wykonanie polecenia będzie ponawiane co sekundę
  - Przykład
    - netstat –r
    - netstat -rnc

Narzędzia sieciowe

- netstat (3) – informacja o interfejsach
  - Składnia
    - netstat –i [-e] [-a]
  - Opcje
    - -e – informacje będą pełniejsze
    - -a – wyświetlane są informacje o wszystkich interfejsach

Narzędzia sieciowe

- netstat (4) – informacja o połączeniach maskowanych
  - Składnia
    - netstat -M [-e] [-n]
  - Opcje
    - -e – pełniejszy zestaw informacji
    - -n – adresy IP nie będą zamieniane na nazwy

Narzędzia sieciowe

- netstat (5) – podsumowania dotyczące połączeń
  - Składnia
    - netstat -s [-t] [-u] [-w]
  - Opcje
    - -t – tylko dla protokołu tcp
    - -u – tylko dla protokołu udp
    - -w – tylko dla protokołu raw ip

