System operacyjny Linux

Paweł Rajba

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

Zawartość modułu 16

- DNS
  - Wprowadzenie, struktura
  - Autorytatywny i nieautorytatywny serwer DNS
  - Serwery główne
  - Kwerendy DNS, przesyłanie dalej
  - Odwzorowanie nazw, rodzaje serwerów
  - Konfiguracja klienta i serwera
  - Weryfikacja konfiguracji serwera
  - Dynamiczny DNS
  - Narzędzia do rozwiązywania nazw

Wprowadzenie

- Wstęp
  - Ludziom łatwiej zapamiętać nazwę www.wp.pl, niż adres 212.77.100.101
  - A komputerom łatwiej operować na adresie 212.77.100.101 niż poprzez nazwę www.wp.pl
  - Zamiana nazwy na adres to forward resolution, a zamiana adresu na nazwę to reverse resolution

Wprowadzenie

- Krótki przegląd historyczny
  - na początku każdy lokalnie sam pamiętał pary nazwa – adres; pamiętane to było w pliku hosts.txt
  - z czasem pojawiało się coraz więcej takich par i aktualizacja plików stawała się kłopotliwa
  - a par było coraz więcej...
  - ... i jeszcze więcej
  - ... aż w końcu w 1984 r. powstał DNS

Wprowadzenie

- System DNS obsługuje dostęp do zasobów przy użyciu nazw alfanumerycznych
- System DNS opracowano z myślą o rozwiązaniu problemów związanych ze wzrostem:
  - Liczby hostów w Internecie
  - Natężenia ruchu generowanego przez proces aktualizacji
  - Rozmiaru pliku hosts

Wprowadzenie

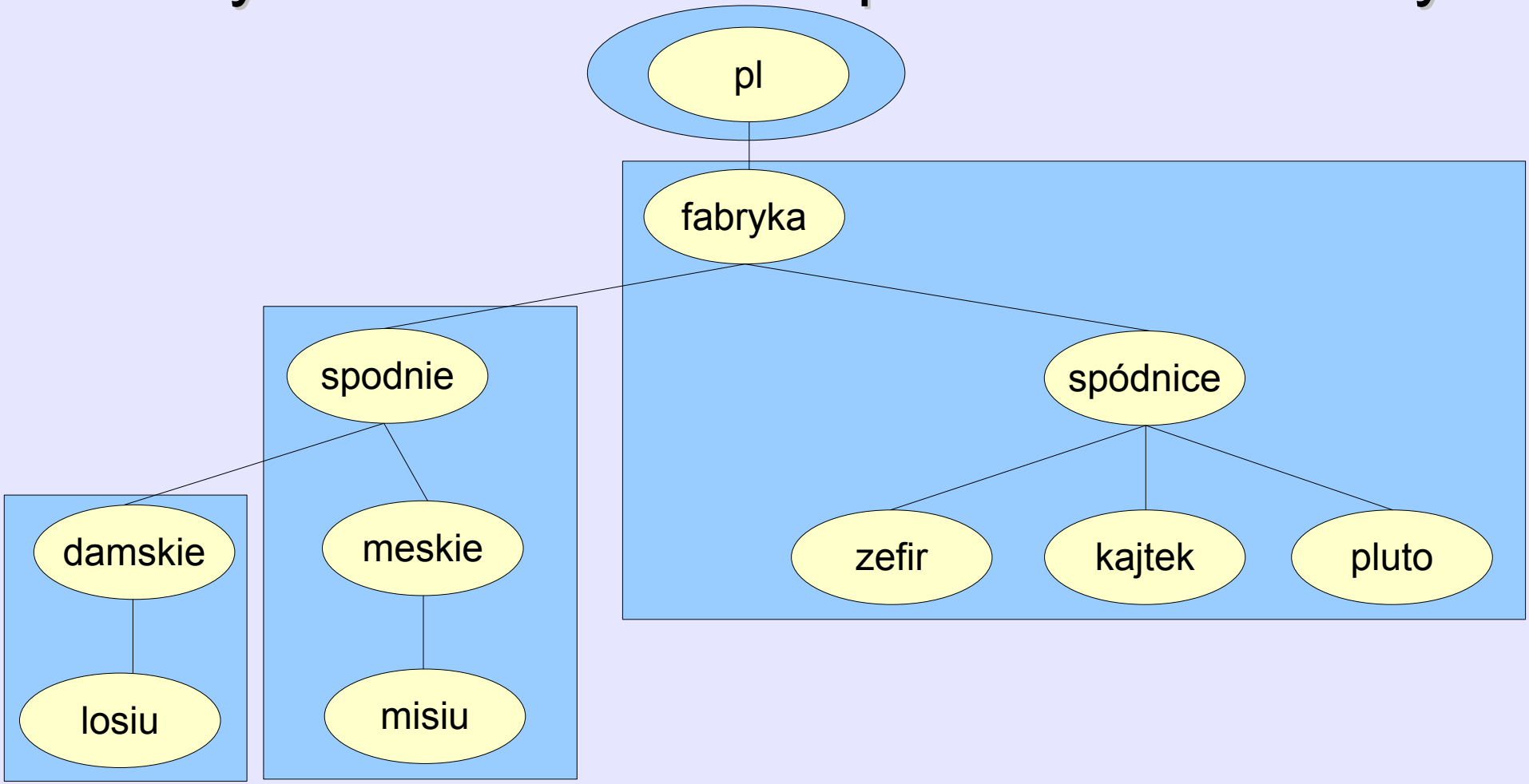
- W nazwach DNS można stosować następujące znaki:
  - A–Z
  - a–z
  - 0–9
  - Dywiz (-)
- Podkreślenie (_) jest znakiem zarezerwowanym

Struktura

- Kilka uwag
  - DNS działa w modelu klient – serwer
  - DNS jest rozproszoną bazą danych
  - DNS jest systemem hierarchicznym zorganizowanym w drzewo
    - Korzeniem drzewa jest ROOT, czyli "."
    - Pierwszy poziom drzewa to główny poziom DNS, albo inaczej TLD (top level domains)
      - dostępne są: com, edu, gov, mil, new ,org, arpa, int, kod kraju
      - niedawno pojawiły się także: biz, info, name, musem, coop, aero
  - Drzewo DNS jest podzielone na strefy
  - Za każdy strefę jest odpowiedzialny jeden serwer główny (nadrzędny, primary server)

Struktura

- Przykładowe drzewko z podziałem na strefy



[Nie]autorytatywny serwer DNS

- Serwer DNS autorytatywny dla obszaru nazw kwerendy:
  - Sprawdza pamięć podręczną, sprawdza strefę, a następnie zwraca żądany adres lub
  - zwraca autorytatywne „Nie”
- Serwer DNS nieautorytatywny dla obszaru nazw kwerendy:
  - przesyła dalej nierozwiązywalną kwerendę do określonego serwera kwerend, nazywanego usługą przesyłania dalej, lub
  - używa wskazówek dotyczących serwerów głównych do znalezienia odpowiedzi na kwerendę
    - inicjuje wyszukiwanie od serwerów głównych

Serwery główne (root hints)

- Rekordy zasobów DNS na serwerze DNS, które zawierają listę adresów IP serwerów głównych DNS
- Znaczenie serwerów głównych
  - Serwer DNS po odebraniu żądania sprawdza pamięć podręczną
  - Następnie stara się ustalić autorytatywny serwer dla danej domeny
  - Dalej, próbuje skontaktować się z jednym z serwerów głównych i ustalić serwer dla TLD
  - Następnie ustalany jest adres serwera dla kolejnej domeny i tak do ustalenia serwera dla szukanej domeny
- Adresy są w pliku /var/lib/named/root.hint

Kwerendy DNS

- Kwerenda to żądanie rozpoznania nazw przesłane do serwera DNS
- Są dwa typy kwerend: cykliczne i iteracyjne.
- Kwerendy dotyczące rozpoznania nazw mogą być inicjowane zarówno przez klientów DNS, jak i przez serwery DNS
- Serwer nazw może być autorytatywny lub nieautorytatywny
  - Serwer autorytatwny zawiera podstawową lub pomocniczą kopię strefy DNS

Kwerendy DNS

- Kwerenda cykliczna to kwerenda skierowana do serwera DNS, w której klient DNS żąda od serwera DNS dostarczenia pełnej odpowiedzi na kwerendę
- Przykładowe działanie:
  - Klient wysyła żądanie do lokalnego serwera DNS
  - Serwer DNS sprawdza, czy sam jest w stanie znaleźć odpowiedź na kwerendę
    - jeśli tak, ustala ją i przesyła do klienta
    - jeśli nie, przesyła kwerendę dalej, stając się klientem DNS
  - Klient dostaje pełną odpowiedź na zadaną kwerendę

Kwerendy DNS

- Kwerenda iteracyjna to kwerenda przesyłana do serwera DNS, w której klient DNS żąda najlepszej odpowiedzi, jakiej może udzielić ten serwer bez pomocy innych serwerów DNS. Wynikiem kwerendy iteracyjnej często jest odwołanie do innego serwera DNS znajdującego się niżej w drzewie DNS
- Odpowiedzi na kwerendy iteracyjne mogą być następujące:
  - Odpowiedzi pozytywne
  - Odpowiedzi negatywne
  - Odwołania do innych serwerów

Przesyłanie dalej

- **Usługa przesyłania dalej to serwer DNS wyznaczony przez inne wewnętrzne serwery DNS do przesyłania dalej kwerend dotyczących rozpoznania zewnętrznych (czyli znajdujących się poza daną lokalizacją) nazw domen DNS**
- **Warukowe przesyłanie dalej**
  - Ma miejsce, gdy korzystamy z usługi w przypadku pewnego zbioru domen
  - Przykładowo, żądania rozpoznania adresu IP hosta w organizacji partnerskiej, która ma prywatną infrastrukturę DNS, przesyłamy dalej do serwera DNS w tej organizacji partnerskiej, podczas gdy wszystkie inne żądania zostałyby spełnione w normalny sposób

Odwzorowanie nazw

- Kroki wyglądają następująco (przykład):
  - jesteśmy w host.delta.com i chcemy poznać IP hosta misiu.meskie.spodnie.fabryka.pl
  - najpierw pytamy nasz lokalny serwer nazw (L)
    - serwer sprawdza swoją pamięc podręczną (nie ma)
    - serwer sprawdza, czy nie ma informacji o serwerach dla domen pośrednich (nie ma)
  - L pyta o host jeden z serwerów dla ROOT (adresy tych serwerów są dołączane do plików instalacyjnych większości serwerów DNS)
  - serwer dla ROOT podaje w odpowiedzi adres serwera DNS dla domeny .pl

Odwzorowanie nazw

- Przykład c.d.
  - L pyta serwer dla .pl
  - serwer dla .pl podaje w odpowedzi adres serwera dla fabryka.pl i kalesony.fabryka.pl o nazwie dns.fabryka.pl
  - L pyta serwer dns.fabryka.pl
  - serwer dns.fabryka.pl podaje w odpowiedzi serwer dla spodnie.fabryka.pl i meskie.spodnie.fabryka.pl
  - serwer pyta ten ostatni serwer dostając żądaną inf.
- L zapamiętuje serwery dla domen pośrednich

Rodzaje serwerów

- Nadrzędne (primary servers)
  - one są odpowiedzialne za informację o domenie
- Podrzędne (secondary servers)
  - te serwer synchronizują swoje bazy z serwerami nadrzędnymi
- Buforujące (caching server)
  - przechowuje informacje o hostach, o które ktoś już kiedyś zapytał
  - dwa pierwsze rodzaje są także buforujące

Konfiguracja klienta

- Plik /etc/hosts
  - w tym pliku podajemy pary adres IP – nazwa
  - przykładowa zawartość

```
# Plik /etc/hosts
# Adres IP    Nazwa domenowa      Nazwa hosta
192.168.0.10  oskar.domain.home   oskar
```

- Plik /etc/host.conf
  - określa konfigurację dla resolvera
  - standardowa zawartość tego pliku

```
order hosts,bind
multi on
```


Konfiguracja klienta

- Plik /etc/nsswitch
  - plik określa, gdzie serwisy powinny szukać swoich konfiguracji
  - klient DNS również ma tam swój wpis który może wyglądać następująco
    `hosts: files dns`
  - może się pojawić dodatkowo klauzula [NOTFOUND] i wpis będzie wtedy wyglądał tak:
    `hosts: files dns [NOTFOUND=return] nis`

Konfiguracja klienta

- Plik /etc/resolv.conf
  - określa domeny poszukujące i adresy serwerów DNS
  - przykładowa zawartość

```
search domain.home home
nameserver 192.168.0.1
nameserver 192.168.0.2
```


Konfiguracja serwera

- Plik podstawowy to /etc/named.conf
  - składa się z bloków postaci

```
instrukcja {
   wpisy;
}
```

  - przykładowe instrukcje:
    - acl – określa aliasy, które można wykorzystać do sterowania dostępem do serwera DNS
      - wartości predefiniowane
        - any – wszyscy
        - none – nikt
        - localhost – lokalny komputer
        - localnet – lokalna sieć

Konfiguracja serwera

- Plik /etc/named.conf
  - przykładowe instrukcje c.d.:
    - options – określa dodatkowe szczegóły konfigruracji
      - directory katalog — lokalizacja pozostałych plików konfiguracyjnych (np. konfiguracja stref),
      - host-statistics yes/no — czy przechowywać statystyki na temat każdego pytającego hosta; domyślnie no,
      - forwarders { lista-ip; } — określa listę adresów IP, które powinny być pytane, gdy serwer nie zna odpowiedzi. Przykład:
        - forwarders {
          192.168.3.111;
          192.168.3.112;
          };

Konfiguracja serwera

- Plik /etc/named.conf
  - przykładowe instrukcje c.d.:
    - options c.d.
      - allow-query { lista-adresów; }; — określa listę adresów, które mogą generować zapytania do serwera; format taki sam, jak przy listach acl; można korzystac ze zdefiniowanych wcześniej list acl poprzez odwołanie przez nazwę listy,
      - allow-transfer { lista-adresów; } — określa listę adresów, które mogą wykonywać transfer strefowy z naszym serwerem DNS; teoretycznie może to kazdy, ale zaleca sie ograniczenie tego do hostów, które faktycznie maja do tego powód; w zasadzie będą to tylko serwery podrzedne,
    - zone nazwa-domeny { ustawienia }; – zdefiniowanie strefy

Konfiguracja serwera

- Plik /etc/named.conf
  - Opis stref
    - dla serwera typu master
      - ogólnie
        - zone nazwa-domeny {
          type master;
          file plik-z-baza-danych;
          };
      - przykłady
        - zone "domain.home" {
          type master;
          file "domain.com.zone";
          }
        - zone "0.168.192.in-addr.arpa" {
          type master;
          file "domain.home.revzone";
          }

Konfiguracja serwera

- Plik /etc/named.conf
  - Opis stref
    - dla serwera typu slave
      - ogólnie
        - zone nazwa-domeny {
          type slave;
          masters lista-adresów-ip;
          file plik-z-baza-danych; // opcjonalne i zalecane
          };

Konfiguracja serwera

- Konfiguracja strefy – składa się z rekordów
  - SOA – start of authority

```
domain.com. IN SOA ns.domain.com. hostmaster.domain.com. (
        1999080801 ; numer seryjny
        10800 ; odswieżanie
        1800 ; powtarzanie
        1209600 ; utrata ważności
        604800 ) ; minimum
```

    - znaczenie opcji
      - domain.com. — nazwa domeny (kropka na końcu jest ważna),
      - IN — ma być,
      - SOA — informuje serwer nazw, ze jest to rekord SOA,
      - ns.domain.com. — to FQDN serwera podstawowego nazw dla tej domeny; zwykle będzie to serwer, na którym będzie sie znajdował ten plik

Konfiguracja serwera

- Konfiguracja strefy
  - SOA – start of authority
    - znaczenie opcji
      - hostmaster.domain.com. — adres e-mail administratora domeny (faktycznie: hostmaster@domain.com)
      - numer seryjny — konwencja jest taka, ze jest to data aktualizacji pliku (ważne żeby zmieniać przy aktualizacji),
      - odswieżanie — przykładowa wartość to 3 godziny; określa, jak często serwery podrzędne powinny sprawdzać, czy została przeprowadzona aktualizacja serwera nadrzednego,
      - powtarzanie — przykładowa wartosc to 30 minut; określa, co jaki czas serwer podrzedny powinien ponawiac próby połaczenia z serwerem nadrzednym,

Konfiguracja serwera

- Konfiguracja strefy
  - SOA – start of authority
    - znaczenie opcji
      - utrata waznosci — przykładowa wartosc to 2 tygodnie; określa, po jakim czasie (w przypadku braku kontaktu z serwerem nadrzednym) należy dane usunać,
      - minimum — przykładowa wartosc to 1 tydzien; określa informacje dla serwerów buforujacych, jak długo maja czekać, zanim usuna wpisy w przypadku braku połączenia z nadrzednym serwerem DNS.

Konfiguracja serwera

- Konfiguracja strefy
  - NS: Name Server
    - określa serwery nazw dla stref
    - poza naszym serwerem możemy podać dodatkowo dowolną ilość serwerów zapasowych.
    - podajemy także adresy serwerów poddomen
    - Przykładowe rekordy:
      - @ IN NS dns.strefa.home.
        IN NS dns2.domain.home.
        IN NS dns3.domain.home.

Konfiguracja serwera

- Konfiguracja strefy
  - A: Address Record
    - służy do kojarzenia nazw hostów z adresami IP.
    - ogólnie
      - nazwa-hosta IN A adres-ip
    - przykładowo
      - andromeda IN A 192.168.0.30
        - Do nazwy andromeda zostanie automatycznie doklejona domena zdefiniowana w rekordzie SOA.

Konfiguracja serwera

- Konfiguracja strefy
  - PTR: Pointer Record
    - służy do kojarzenia adresu IP z nazwami hostów.
    - ogólnie
      - adres-ip IN PTR nazwa-hosta
    - Przykładowo:
      - # nazwa musi byc pełnym FQDN
        10.5.5.20. IN PTR andromeda.gwiazdy.pl.

Konfiguracja serwera

- Konfiguracja strefy
  - MX: Mail Exchanger
    - jest wykorzystywany do zamiany adresów serwerów poczty, wykorzystywane przez programy pocztowe
    - ogólnie
      - nazwa-domeny IN MX znaczenie nazwa-hosta

Konfiguracja serwera

- Konfiguracja strefy
  - MX: Mail Exchanger
    - Parametry:
      - nazwa-domeny — nazwa domeny serwisu pocztowego (z kropka na koncu), w przypadku nie podania domeny, pobrana bedzie domena z rekordu SOA,
      - znaczenie — liczba, im nizsza, tym wieksze znaczenie; ma zastosowanie, gdy jest wiecej serwerów pocztowych,
      - nazwa-hosta — nazwa serwera pocztowego; dla tej nazwy musi byc rekord A.
    - Przykładowe rekordy:
      - domain.home. IN MX 10 mail
IN MX 20 mail2

Konfiguracja serwera

- Konfiguracja strefy
  - CNAME: Canonical Name
    - służy do tworzenia aliasów.
    - ogólnie
      - nowa-nazwa-hosta IN CNAME stara-nazwa-hosta
    - Przykładowo:
      - zaporozec IN A 10.5.5.1
      - kubus IN A 10.5.5.100
      - poczta IN CNAME zaporozec
      - www IN CNAME kubus

Przykłady

- Przykład 1
  - Przeglądamy konfigurację i odtwarzamy ją online
  - Testujemy zadając odpowiednie zapytania
- Przykład 2
  - Przeglądamy się przykładowej konfiguracji pod kątem delegacji domeny domowe.zwierzaki.pl
  - transfery danych z serwera nadrzędnego (afrodyta) do podrządnego (cassiopeia) dla domeny zwierzaki.pl
  - Przeglądniecie pliku z domeną odwrotną

Weryfikacja konfiguracji serwera

- Narzędzia
  - named-checkconf
    - Składnia
      named-checkconf [plik-konfiguracyjny]
      - domyślnie brany jest plik /etc/named.conf
  - named-checkzone
    - Składnia
      named-checkzone nazwa-strefy plik-z-baza
- Testujemy przykładową konfigurację

Dynamiczny DNS

- Polega na automatycznej aktualizacji konfiguracji DNS na podstawie przydzielanych dzierżaw
  - Aktualizacja polega na dodaniu odpowiedniego wpisu do pliku strefy z krótkim czasem ważnosci (np. 1h)
- Bardzo wygodne rozwiązanie, dostępne również w DNS systemu Windows
- Konfiguracja polega na
  - wygenerowaniu klucza uwierzytelniającego DHCP w DNS
  - dodaniu kilku wpisów do plików głównej konfiguracji DHCP i DNS

Dynamiczny DNS

- Tworzymy przykładową konfigurację
  - Generujemy klucz poleceniem genDDNSkey
    - wywołanie polecenia bez parametrów jest równoważne
      genDDNSkey --key /etc/named.keys --key-name DHCP_UPDATER
    - program jest z pakietu bind-utils
  - Konfigurujemy DHCP
    - W pliku /etc/dhcpd.conf dopisujemy
      - ddns-update-style interim;
        ignore client-updates;
        include “/etc/named.keys”;

Dynamiczny DNS

- Tworzymy przykładową konfigurację c.d.
  - Konfigurujemy DHCP c.d.
    - Przykładowa definicja zakresu
      - subnet 10.2.0.0 netmask 255.255.255.0 {
        range dynamic-bootp 10.2.0.50 10.2.0.70;
        zone algorytmy.net. { primary 127.0.0.1;
        key DHCP_UPDATER; }
        zone 0.2.10.in-addr.arpa. { primary 127.0.0.1;
        key DHCP_UPDATER;
        }
    - W pliku /etc/sysconfig/dhcpd do zmiennej DHCPD_CONF_INCLUDE_FILES dopisujemy wartosć /etc/named.keys
      - ze względu na chroot, katalog “/” jest dla usługi DHCP niedostępny

Dynamiczny DNS

- Tworzymy przykładową konfigurację c.d.
  - Konfigurujemy DNS
    - W pliku /etc/named.conf dopisujemy
      - include “/etc/named.keys”;
    - W pliku /etc/named.conf w definicji każdej strefy dopisujemy
      - allow-update { key DHCP_UPDATER; };
    - Być może będzie trzeba w pliku /etc/sysconfig/named w zmiennej NAMED_CONF_INCLUDE_FILES dopisać wartosć /etc/named.keys (u mnie nie było trzeba)
    - WAŻNE: trzeba pamiętać, aby użytkownik named (grupa named) miały prawo do modyfikacji plików stref
      - najlepiej umiescic je w katalogu /var/lib/named/dyn/

Przykład

- Przykład 3
  - Przeglądamy pliki konfiguracyjne
  - Odtwarzamy konfigurację online

Narzędzia do rozwiązywania nazw

- Program host
  - host [-t typ] adres [serwer]
  - host [-l | -a] domena [serwer]
- Program dig
  - dig @serwer {-x adres | nazwa} typ
    - serwer — serwer DNS, do którego wysyłane jest zapytanie,
    - -x adres — tej opcji uzyjemy, jesli chcemy zamienic adres IP na nazwe hosta,
    - nazwa — podajemy nazwe hosta, dla którego chcemy poznac adres IP,
    - typ — rodzaj rekordu (A, PTR, MX,...), który nas interesuje.

Narzędzia do rozwiązywania nazw

- Program nslookup
  - Składnia
    - nslookup [opcje] [name | -] [server]
  - Tryby Interaktywny
    - nslookup
      - przy użyciu domyślnego serwera DNS
    - nslookup - serwerdns
      - przy użyciu wskazanego serwera DNS
    - Niektóre polecenia: exit, help, set type, ?
    - Podanie nazwy hosta to żądanie jej rozwiązania

Narzędzia do rozwiązywania nazw

- Program nslookup
  - Tryb nieinteraktywny
    - nslookup host
      - rozwiązanie nazwy przy użyciu domyślnego serwera DNS
    - nslookup host serwer
      - rozwiązanie nazwy przy użyciu wskazanego serwera
  - Przykłady
    - nslookup www.onet.pl dns.onet.pl
      - dostaniemy autorytatywną odpowiedź
    - nslookup www.onet.pl
      - dostaniemy nieautorytatywną odpowiedź

