Last modified 2 minutes ago

Sieci Komputerowe -- diagnostyka

Teoria

Istnieje wiele programów służących do diagnostyki sieci komputerowych oraz pobierających informacje z baz danych i pozwalających sprawdzić kto odpowiada za adresy, bądź nazwy w Internecie. Sama diagnostyka sieci jest jednak problemem dość złożonym i z tego powodu trudno o oprogramowanie, które w ogólnym przypadku byłoby w stanie bez ingerencji użytkownika zdiagnozować i wskazać konkretny problem i jego przyczynę.

Poniżej znajduje się opis kilku programów dostępnych w różnych systemach operacyjnych (czasami pod nieznacznie różniącymi się nazwami), które pozwalają zweryfikować ustawienia sieci oraz przeprowadzić podstawową diagnostykę.

Komenda `ifconfig/ipconfig`

Komendy:

- `ipconfig` w Windows
- `ifconfig` w systemach *nix

pozwalają sprawdzić oraz zmodyfikować konfigurację sieci. Podstawowe parametry konfiguracyjne jakie można uzyskać przy ich pomocy to:

- adres IP
- maska podsieci
- adres sprzętowy karty sieciowe MAC
- adres domyślnej bramy (w Windows)

Komenda `ping`

Komenda ping dostępna we wszystkich chyba systemach operacyjnych umożliwiających podłączenie do sieci komputerowej pozwala sprawdzić, czy możliwa jest komunikacja z określonym adresem IP. Program ping wysyła komunikaty ICMP Echo Request pod zadany adres. System operacyjny otrzymujący taki komunikat odpowiada pakietem ICMP Echo Reply. Program ping liczy i wyświetla czas odpowiedzi oraz wartość TTL.

Brak komunikacji w sieci może być spowodowany różnymi przyczynami. Jeśli powodem jest błędna konfiguracja lub awaria sprawiająca, że jeden z ruterów w sieci nie ma informacji o tym jak dostarczyć pakiet pod zadany adres IP odsyła adekwatny do tej sytuacji komunikat ICMP. Informację o odebraniu takiego komunikatu wyświetlają *nixowe wersje programu ping pozwalając zorientować się co to miejsca i przyczyny awarii.

Brak odpowiedzi na komunikat ping może być spowodowany tym, że system operacyjny docelowego komputera został poinstruowany, żeby takiej odpowiedzi nie udzielać (np. poprzez konfigurację firewalla).

Informacje na temat uzyskanej odpowiedzi wyświetlane przez program ping mogą posłużyć do oceny ilości przeskoków dzielących komputery oraz oceny jakości i stanu łącza. Pierwsza informacja może być odczytana z wartości TTL, która jest ustawiana przez system wysyłający odpowiedź na ping i zmniejszana przez każdy pośredniczący ruter. Czasy uzyskania odpowiedzi tzw. *round-trip time* zależą od ilości przeskoków i długości połączeń sieciowych. Jednakże nawet w przypadku łącz typu WAN ich wartość powinna być rzędu kilkudziesięciu milisekund, w przypadku sieci LAN kilku milisekund. Ważne jest też jaki jest rozrzut tych czasów.

Komenda `traceroute/tracert`

Komendy:

- tracert w Windows
- traceroute w systemach *nix

służą do wyznaczania trasy w sieci prowadzącej do stacji z określonym adresem. Trasa opisana jest poprzez listę adresów (symbolicznych, bądź IP) ruterów, przez które wykonywane są kolejne przeskoki do określonego adresu. Poza kolejnymi adresami program wypisuje też czasu odpowiedzi uzyskanych od kolejnych ruterów (dla każdego z nich mierzone są trzykrotnie).

Komenda traceroute/tracert pozwala określić jaką drogę przemierzają pakiety do określonego celu, w przypadku awarii lub błędnej konfiguracji pozwala zorientować się w którym miejscu sieci występuje problem (np. z którym ruterem). Czasy podawane przez program pozwalają też zgrubnie ocenić obciążenie poszczególnych segmentów sieci.

Korzystając z programów traceroute/tracert należy pamiętać, że trasy w Internecie wyznaczane są dynamicznie i zmieniają się w czasie. Mogą też występować sytuacje w których trasa w jednym kierunku prowadzi inną drogą (poprzez inny zestaw ruterów) niż w kierunku przeciwnym. Może to powodować nieścisłości w wynikach uzyskiwanych z programów. Na ogół jednak programy te dostarczają użytecznych informacji.

Komenda `route`

Komenda route służy do wyświetlenia oraz modyfikacji tzw. *tablicy rutingu*. Tablica rutingu pozwala zdefiniować poprzez jakie rutery, albo do jakich sieci wysyłane będą pakiety, zależnie od adresów docelowych dla których są przeznaczone. W przypadku komputera podłączonego do pojedynczej sieci (a więc w typowym przypadku stacji roboczej) komenda powinna pokazać:

- domyślną trasę, oznaczoną słowem `default` albo adresem docelowym `0.0.0.0`
- trasę do sieci do której bezpośrednio podłączony jest komputer
- trasę do adresu `127.0.0.1`, tzw. interfejsu `loopback`, pozwalającemu różnym programom na jednym komputerze komunikować się ze sobą tak jakby komunikacja odbywała się za pomocą sieci komputerowej, nawet jeśli sieć nie jest podłączona/skonfigurowana. Każdy komputer pod adresem `127.0.0.1` "widzi" samego siebie.

Komenda `netstat`

Komenda netstat służy do wyświetlania aktywnych połączeń sieciowych i ich stanu. Pozwala zorientować się z jakimi adresami i portami uruchomione programy nawiązały połączenia. Zależnie od systemu operacyjnego komenda ma różny zestaw parametrów i wyświetlanych informacji. W systemach *nix warto wypróbować opcje:

- `-t` -- wyświetla połączenia TCP
- `-u` -- wyświetla aktywne porty UDP
- `-p` -- wyświetla PID procesu, który korzysta z danego połączenia pozwalając zidentyfikować korzystający z niego uruchomiony program

Opcje można łączyć w jednym wywołaniu, np: `netstat -utp`.

Komenda `host`

Komenda host dostępna w systemach *nix służy do odpytywania bazy DNS. Podając jako parametr adres symboliczny uzyskamy odpowiadający mu adres IP i odwrotnie. Odpytywanie innych rekordów DNS możliwe jest dzięki opcji `-t` określającej typ poszukiwanego rekordu. Np. `host -t MX prz-rzeszow.pl` zwróci rekordy MX dla podanej domeny, a więc informację o serwerach pocztowych obsługujących jej pocztę przychodzącą.

Komenda `whois`

Komenda whois dostępna w systemach *nix służy od odpytywania tzw. bazy whois zawierającej informacje o właścicielach i odpowiedzialnych za adresy IP oraz domeny. Uruchamiając należy podać adres IP lub domenę na temat której chcemy uzyskać

informację.

Komenda tcpdump

Komenda tcpdump dostępna w systemach *nix pozwala analizować ruch w sieci -- przeglądać informacje o przesyłanych pakietach. Dostępne są tylko informacje o pakietach które "widzi" zainstalowana w systemie karta sieciowa. Nie mniej jednak tcpdump jest w stanie dostarczyć bardzo użytecznych informacji, zwłaszcza gdy zostanie uruchomiony na ruterze przekazującym ruch pomiędzy sieciami. Często staje się nieocenionym narzędziem administratora sieci. Domyślnie program wypisuje jedynie informacje o nagłówkach przechwyconych pakietów, ale nawet to może spowodować że ilość danych będzie zbyt duża aby ją przeanalizować. Z tego względu program pozwala zarówno na zapis przechwyconych informacji do pliku, w celu późniejszej analizy za pomocą innych narzędzi (np. graficznych), jak i na zaawansowane filtrowanie przechwytywanych danych. Ta funkcjonalność jednak zdecydowanie wykracza poza ramy tego opracowania.

Windows

Pierwsza część ćwiczenia dotyczy komend dostępnych w systemie Windows, pozwalających wykonać diagnostykę sieci.

Sprawdzenie podstawowej konfiguracji

Wykonać komendę

```
ipconfig
```

Sprawdzić przydzielony adres IP, maskę podsieci, inne informacje. Porównać z informacjami uzyskanymi przez innych studentów na innych stacjach. Które parametry są takie same, a które są różne?

Sprawdzenie łączności sieciowej

- Poleceniem

```
ping <adres_ip>
```

używając adresu IP innej stacji uzyskanego od innego studenta. Sprawdzić, czy sieć pomiędzy poszczególnymi stacjami. Zapamiętać czasy odpowiedzi.

- Wykonać ping na adres www.google.com, sprawdzić jakie są czasy odpowiedzi, porównać z czasami uzyskanymi podczas poprzedniego zadania.
- Wykonać ping na nieistniejący adres IP (np. 10.1.1.5), jaki jest wynik komendy?

Sprawdzanie trasy w sieci

- Komendą

```
tracert
```

wyświetlić trasę do www.google.com, sprawdzić jakie są czasy poszczególnych przeskoków, porównać z uzyskanymi wcześniej czasami pingów do lokalnych stacji i zdalnych adresów. Ile jest przeskoków? Powtórzyć komendę kilkakrotnie, czy za każdym razem trasa jest taka sama?

- Wykonać traceroute do nieodpowiadającego/nieskonfigurowanego adresu IP (np. 10.1.1.5). Co pokazuje komenda? jak zinterpretować wyniki? Do której jakiej podsieci prowadzi trasa i na czym się kończy?

Sprawdzenie konfiguracji rutingu

Komendą

```
route
```

wyświetlić lokalną tablicę rutingu, odnaleźć trasy do bezpośrednio podłączonych sieci oraz trasę domyślną. Porównać z wynikami uzyskanymi z komendy traceroute.

Sprawdzenie stanu połączeń sieciowych

- Komendą

```
netstat
```

wyświetlić aktualne połączenia TCP. Podać adresy IP źródłowe i docelowe, oraz źródłowe i docelowe numery portów.

- Otworzyć za pomocą przeglądarki złożoną stronę internetową, np. http://www.wp.pl albo http://onet.pl po czym możliwie szybko (jeśli się uda to jeszcze w trakcie ładowania strony) uruchomić ponownie komendę netstat, sprawdzić adresy IP i porty, porównać z poprzednimi wynikami. Ile nowych połączeń nawiązano w celu otwarcia strony?

Sprawdzenie zewnętrznego adresu IP

- Serwis *What is My IP* podaje adres IP z jakim otwierający go komputer jest widoczny z Internetu. Otworzyć stronę http://www.whatismyip.com/. Jaki adres IP podano? Czy to jest ten adres, który wyświetliła komenda ipconfig na początku ćwiczenia? Wyjaśnić! Porównać z wynikami uzyskanymi przez innych studentów.

Linux

- Wystartować z płyty CD system Linux:
  - Umieścić płytę w napędzie i zrestartować komputer
  - Po uruchomieniu płyty wybrać opcję **Wypróbuj Ubuntu 10.04 LTS**

Konsola tekstowa

- Za pomocą kombinacji klawiszy `Ctrl-Alt-F1` przejść do konsoli tekstowej.
- W uruchomionym systemie brakuje komendy traceroute, żeby ją doinstalować należy wydać komendę:

```
sudo aptitude install traceroute
```

- Jeśli wyjście z jakiejś komendy nie zmieściło się na ekranie i "uciekło" do góry, można je obejrzeć przytrzymując klawisz *Shift* i przesuwając ekran w górę i w dół klawiszami *PgUp* i *PgDn*
- Za pomocą poniższych poleceń wykonać zadania wykonane wcześniej pod systemem Windows:
  - `ifconfig`
  - `ping`
  - `traceroute`
  - `route`
- Sprawdzić zewnętrzny adres IP korzystając z serwisu *What is My IP*

Porównać uzyskane informacje i wyniki z podanymi przez narzędzia windowsowe.

- Za pomocą komendy

```
host
```

    - Uzyskać adres IP na który rozwija się adres onet.pl
    - Sprawdzić na jaki adres symboliczny rozwija się uzyskany adres IP.
    - To samo wykonać dla adresu www.google.com.
    - Sprawdzić jaki jest adres IP i symboliczny serwera pocztowego obsługującego domenę onet.pl

- sprawdzić za pomocą komendy

```
whois
```

    - Kto zarejestrował domenę wp.pl i kiedy
    - Kiedy dokonano ostatniej zmiany wpisów
    - Do jakiej sieci (o jakim zakresie adresów) należy adres IP: 213.180.146.27
    - Kto jest właścicielem ww. adresu IP, w jakim kraju, pod jakim adresem pocztowym
    - Z jakim adresem mailowym należy się kontaktować w przypadku nadużycia pochodzącego z ww. adresu IP

Tryb graficzny

Za pomocą kombinacji klawiszy Ctrl-Alt-F7 lub Ctrl-Alt-F8 przejść do trybu graficznego.

- Włączyć program terminala znajdujący się w menu: *Programy -> Akcesoria -> Terminal*
- Analogicznie jak w Windowsie przetestować działanie komendy netstat dodając opcje -tu, żeby ograniczyć wyjście do połączeń TCP i portów UDP. Przeglądarkę można uruchomić klikając ikonę Firefoksa na pasku na górze.
- Oglądanie ruchu w sieci.
    - Zalogować się jako użytkownik root za pomocą komendy sudo bash
    - Uruchomić poniższą komendę na chwilę, wyłączyć po uzyskaniu kilkunastu linijek wyniku.

```
tcpdump -ne
```

    - Uruchomić poniższą komendę i za pomocą przeglądarki otworzyć dowolną stronę www

```
tcpdump -ne
```

Przeanalizować wyniki.