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

- ipconfig w Windows,
- ifconfig w systemach Linux.

Komendy te pozwalają sprawdzić oraz zmodyfikować (tylko ifconfig) konfigurację sieci. Podstawowe parametry konfiguracyjne jakie można uzyskać przy ich pomocy to:

- adres IP,
- maska podsieci,
- adres sprzętowy karty sieciowej MAC,
- adres domyślnej bramy (w Windows).

Komenda ping (Windows, Linux)

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 Linuksowe wersje programu ping pozwalając zorientować się co do 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

- tracert w Windows,
- traceroute w systemach Linux.

Komendy te 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 czasy odpowiedzi uzyskane od kolejnych węzłów (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 mtr (Linux)

Komenda mtr (My Traceroute) jest alternatywną wersją traceroute. Za jej pomocą możemy uzyskać informacje o procentowej ilości zgubionych pakietów dla każdego węzła trasy (kolumna Loss) oraz wartości statystyczne, takie jak średnia (Avg), odchylenie standardowe (StDev) czasów odpowiedzi, najlepsze (Best) i najgorsze (Worst) czasy. Program po uruchomieniu wykonuje się wielokrotnie, do momentu przerwania.

Komenda route (Windows, Linux)

Komenda route służy do wyświetlenia oraz modyfikacji tzw. tablicy trasowania (rutingu). Tablica trasowania 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 arp (Windows, Linux)

Komenda arp służy do wyświetlania i edytowania tablicy ARP (Address Resolution Protocol). Tablica ARP przechowuje adresy IP oraz sprzętowe (MAC) urządzeń, które w ostatnim czasie łączyły się z naszą siecią lokalną. Możemy wyświetlić listę wszystkich takich urządzeń (ich adresy IP oraz MAC) przy użyciu komendy arp z opcją -a.

Komenda netstat (Windows, Linux)

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 Linux warto wypróbować opcje:

- -t – wyświetla połączenia TCP;
- -u – wyświetla aktywne porty UDP;
- -p – wyświetla PID procesu, który korzysta z danego połączenia pozwalając identyfikować korzystający z niego uruchomiony program. Opcje można łączyć w jednym wywołaniu, np. netstat -utp.

Komenda host (Linux)

Komenda host dostępna jest w systemach Linux. Dzięki niej podając jako parametr adres symboliczny uzyskamy odpowiadający mu adres IP i odwrotnie. Komenda host odpytuje bazę DNS w celu uzyskania wyniku. 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 hostname (Windiws, Linux)

Komenda hostname umożliwia odczytanie lub ustawienie nazwy hosta danego urządzenia.

Komenda whois (Linux)

Komenda whois dostępna w systemach Linux służy od odpytywania tzw. bazy whois zawierającej informacje o właścicielach lub osobach odpowiedzialnych za adres IP oraz domenę. Uruchamiając należy podać adres IP lub domenę na temat której chcemy uzyskać informację.

Komenda wget (Windows (wymaga pobrania i instalacji), Linux)

Za pomocą komendy wget możemy pobrać dowolny plik z adresu podanego jako parametr bez użycia przeglądarki internetowej. Domyślnie plik pobiera się w bieżącym katalogu.

Komenda tcpdump (Linux)

Komenda tcpdump pozwala analizować ruch w sieci, tzn. przeglądać informację o pakietach przesyłanych do i ze wszystkich urządzeń połączonych z naszą siecią. Dostępne są tylko informacje o pakietach, które „widzi" zainstalowana w systemie karta sieciowa. Niemniej jednak tcpdump jest w stanie dostarczyć dużo 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 na zapis przechwyconych informacji do pliku w celu późniejszej analizy za pomocą innych narzędzi. Można również wykonywać zaawansowane filtrowanie przechwytywanych danych.

Informacje o pakietach uzyskane za pomocą polecenia tcpdump, to:

- czas przechwycenia pakietu,
- rodzaj pakietu i adresy IP (źródłowy i docelowy),
- flagi protokołu TCP,
- numer sekwencyjny i numer potwierdzenia,
- rozmiar okna w protokole TCP,
- dodatkowe opcje.

Zadania do wykonania w systemie Linux

Niektóre programy z poniższych zadań działają przez długi (lub nieograniczony) czas. Można je zakończyć skrótem klawiszowym Ctrl + C.

Sprawdzenie podstawowej konfiguracji

Wykonać komendę:

```
ifconfig
```

Sprawdzić przydzielony adres IP (inet), maskę podsieci (netmask), adres rozgłoszeniowy (broadcast), adres sprzętowy MAC (ether lub w starszych wersjach systemu - HWaddr) i inne informacje o interfejsie sieciowym naszego komputera oraz sieci lokalnej. Porównać z informacjami uzyskanymi przez innych studentów na innych stacjach. Które parametry są takie same, a które są różne?

Sprawdzenie zewnętrznego adresu IP

Serwis W*hatIsMyIp.com* podaje adres IP z jakim otwierający go komputer jest widoczny z Internetu. Otworzyć stronę: *https://www.whatismyip.com*. Jaki adres IP podano? Czy jest to ten adres, który wyświetliła komenda ifconfig? Wyjaśnić! Porównać z wynikami uzyskanymi przez innych studentów.

Sprawdzenie łączności sieciowej

Poleceniem:

```
ping <adres_ip>
```

- 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:

```
traceroute <adres>
```

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 jakiej podsieci prowadzi trasa i na czym się kończy?

Komendą:

```
mtr -b <adres>
```

Wyświetlić trasę do www.onet.pl. Sprawdzić, czy są jakieś węzły, przy których pakiet został zgubiony. Ile procentowo pakietów zostało zgubionych? Sprawdzić maksymalne, minimalne i średnie czasy odpowiedzi oraz ich odchylenie standardowe. Opcja -b powoduje, że oprócz nazw symbolicznych węzłów wyświetlają się również ich adresy IP.

Sprawdzenie konfiguracji rutingu

Komendą:

```
route
```

wyświetlić lokalną tablicę rutingu.

Uzyskiwanie adresu IP na podstawie adresu symbolicznego i na odwrót

Za pomocą komendy:

```
host <adres>
```

- uzyskać adres IP, na który rozwija się adres onet.pl;
- to samo wykonać dla adresu www.google.com;
- sprawdzić na jaki adres symboliczny rozwija się uzyskany adres IP 212.77.98.9;
- sprawdzić na jaki adres symboliczny rozwija się uzyskany adres IP 62.93.32.52.

Sprawdzanie nazwy hosta

Za pomocą komendy:

```
hostname
```

sprawdzić nazwę hosta swojego komputera.

Uzyskiwanie informacji o domenie

Sprawdzić za pomocą komendy:

```
whois <adres>
```

- Kto zarejestrował domenę wp.pl i kiedy.
- Kiedy dokonano ostatniej zmiany wpisów.
- Do jakiej sieci (o jakim zakresie adresów) należy ta domena.
- 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.

Jeśli program whois nie jest domyślnie zainstalowany w obsługiwanym systemie operacyjnym, należy go zainstalować za pomocą polecenia (wymagane będzie hasło do konta root, które poda prowadzący):

```
sudo apt install whois
```

Wyświetlanie listy urządzeń w sieci lokalnej

Komendą:

```
arp -a
```

wyświetlić adresy IP oraz MAC urządzeń w sieci lokalnej swojego komputera.

Następnie poprosić kolegę, aby wykonał ping na nasz adres i wywołać polecenie arp -a ponownie. Jeśli kolega nawiązał połączenie z naszym komputerem (albo my nawiązaliśmy połączenie z jego komputerem), to jego adres i nazwa hosta powinny tym razem pojawić się na liście.

Wyświetlanie aktywnych połączeń sieciowych

Komendą:

```
netstat
```

wyświetlić listę aktywnych połączeń sieciowych. Zwrócić uwagę, że połączenia mają różne typy, np. DGRAM – bezpołączeniowy tryb datagramów, STREAM – tryb połączeniowy (strumieniowany).

Pobranie pliku

Skopiować adres, z którego została pobrana niniejsza instrukcja. Następnie pobrać ją przy użyciu polecenia:

```
wget <adres>
```

Jeśli pliku nie uda się pobrać i pojawi się błąd weryfikacji certyfikatu, należy skorzystać z polecenia:

```
wget --no-check-certificate  <adres>
```

Spowoduje ono pominięcie sprawdzania certyfikatów SSL przed pobraniem pliku. Należy używać tej opcji tylko w przypadku, gdy jesteśmy pewni jaki plik znajduje się pod podanym adresem.

Plik pobierze się w katalogu bieżącym, którego ścieżkę możemy sprawdzić poleceniem `pwd`. Aby sprawdzić, czy plik udało się pobrać należy skorzystać z polecenia `ls` lub przejść do odpowiedniego katalogu w eksploratorze plików.

Analiza ruchu w sieci

Sprawdzić działanie polecenia:

```
sudo tcpdump
```

Na początku wpisujemy polecenie `sudo` oznaczające, że wykonujemy komendę posiadając uprawnienia administratora, które są wymagane do użycia `tcpdump`. Wymagane będzie hasło do konta root, które poda prowadzący.

Należy przeanalizować wyniki zgodnie z opisem teoretycznym na stronie 3.