

Sieci Komputerowe

LABORATORIUM 1

Komenda "ipconfig":

Komenda pozwalająca na wyświetlenie danych nt konfiguracji sieciowej komputera lub jej zmianę. Może one być użyta chociażby do sprawdzenia aktualnie przypisanego urządzeniu adresu IPv4. Na systemach UNIX jej odpowiednikiem jest *ifconfig*.

```
C:\>ipconfig

FastEthernet0 Connection: (default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::206:2AFF:FE56:CB43
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 10.0.0.1
    Subnet Mask . . . . .: 255.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                   0.0.0.0
```

Rysunek 1: Efekt skorzystania z komendy *ipconfig*.

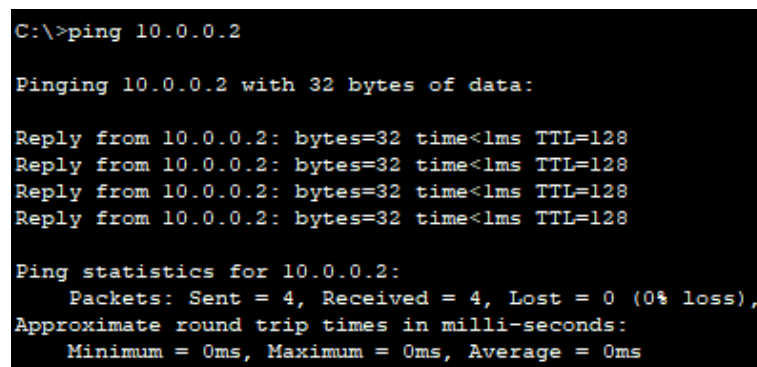
Do komendy *ipconfig* możemy dodać również parametry, zmieniające jej działanie:

- *brak parametru* - wyświetlenie skrótovej informacji nt konfiguracji sieciowej
- */all* - wyświetla szczegółowe informacje na temat konfiguracji sieciowej (w tym adres MAC)
- */release* - zwalnia wszystkie adresy IP przydzielone do karty sieciowej
- */renew* - pobiera nowe adresy IP dla karty sieciowej (wymaga aktywnego DHCP)
- */flushdns* - usuwa informacje na temat nazw domen z pamięci serwera DNS

- *displaydns* - wyświetla nazwy domen zawarte w pamięci serwera DNS
- *registerdns* - odświeża i aktualizuje informacje o nazwach domen w serwerze DNS

Komenda "ping":

Komenda pozwalająca na diagnozowanie połączenia sieciowego między dwoma urządzeniami w sieci. Badanie polega na przesłaniu kolejno 4 pakietów ICMP z jednego urządzenia i oczekiwanie na odpowiedź z drugiego. Czas między wysłaniem pakietu a otrzymaniem odpowiedzi nazywamy czasem odpowiedzi czy też czasem ping.



```
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128
Reply from 10.0.0.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Rysunek 2: Efekt skorzystania z komendy *ping*.

Za pomocą parametrów można dostosować ilość wysyłanych pakietów, czas oczekiwania na odpowiedź oraz rozmiar pakietów. Najczęściej używanymi są:

- *-n [ilość]* - ustala ilość pakietów które mają zostać przesłane
- *-l [ilość]* - ustala wielkość pakietów
- *-w [czas msek]* - określa maksymalny czas oczekiwania na odpowiedź
- *-a* - nastąpi próba identyfikacji nazwy z serwera DNS

Zamiast adresu IPv4 odbiorcy można wpisać nazwę hosta, która następnie zostanie rozpoznana przez DNS.

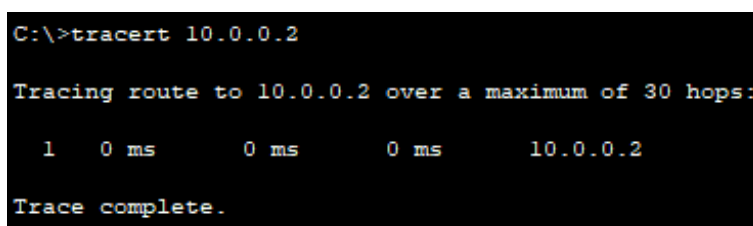
Protokół ICMP:

Protokół ICMP (Internet Control Message Protocol) to protokół warstwy sieciowej, który jest używany do przesyłania wiadomości diagnostycznych i sterujących w sieciach IP. Często jest stosowany w diagnozowaniu problemów

z siecią. Jego działanie polega na przesyłaniu wiadomości ICMP z między hostami, a następnie oczekiwaniu na odpowiedź.

Komenda "tracert":

Komenda pozwalająca na prześledzenie ścieżki pomiędzy hostami. Wyświetli ona informacje o wszystkich routerach przez które należy przejść, aby dotrzeć do hosta (pokaże dane o ścieżce do hosta). Jest to narzędzie oparte o wiadomości ICMP. Pozwala ono ustalić w łatwy sposób w którym punkcie ścieżki występuje problem z transmisją.



```
C:\>tracert 10.0.0.2

Tracing route to 10.0.0.2 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    10.0.0.2

Trace complete.
```

Rysunek 3: Efekt skorzystania z komendy *tracert*.

Do komendy *tracert* można dodać parametr zmieniający jej działanie:

- *-d* - wyłącza konwersję adresów na nazwy hostów (DNS).
- *-h [ilość]* - ustala maksymalną ilość skoków, z których ma składać się ścieżka

Host:

Każde urządzenie podłączone do sieci, które bierze bezpośredni udział w komunikacji sieciowej (jest urządzeniem końcowym). Każdy host obecny ma przypisany numer identyfikacyjny, adres IP (zgodny ze schematem adresowania protokołu IP).

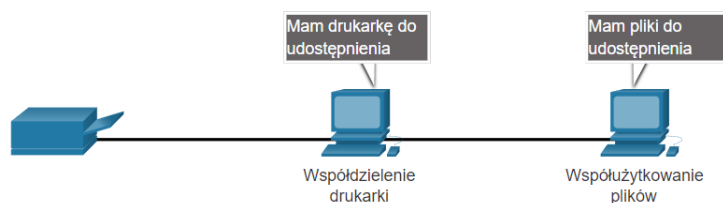
Serwery i klienci

Wśród hostów można wyróżnić urządzenia będące serwerami i klientami. Serwery posiadają oprogramowanie umożliwiające im dostarczanie informacji klientom danej usługi sieciowej. Urządzenia-klienci posiadają oprogramowanie do wysyłania żądań i wyświetlania danych przychodzących z serwerów. Oczywiście nic nie stoi na przeszkodzie, aby urządzenie było jednocześnie klientem jak i serwerem (choć zazwyczaj taka sytuacja nie występuje).

Sieć peer-to-peer:

O sieci peer-to-peer mówimy, gdy występujące w sieci hosty pełnią rolę za-

równie klienta jak i serwera. Tego typu sieci występują chociażby w domach czy małych firmach.



Rysunek 4: Schemat obrazujący sieć peer-to-peer.

Plusami sieci pper-to-peer są:

- Łatwa konfiguracja
- Mała złożoność
- Niższy koszt ze względu na brak wymogu zakupu dedykowanych urządzeń sieciowych i serwerów
- Duża użyteczność w wypadku prostych zadań jak współdzielenie plików i urządzeń wyjścia między urządzeniami

Minusami sieci peer-to-peer są:

- Brak scentralizowanej administracji (brak centralnego urządzenia-serwera).
- Mniejsze bezpieczeństwo
- Trudna skalowalność
- Zmniejszona wydajność ze względu na fakt, że każde urządzenie musi wykonywać zadania hosta i serwera

Urządzenia pośredniczące:

Urządzenia łączące poszczególne urządzenia końcowe z siecią. Ponadto mogą łączyć wiele pojedynczych sieci. Tworzą tym samym intersieć. Urządzenia pośredniczące używają adresy urządzeń końcowych oraz informacje nt połączeń wewnątrz sieci w celu określenia ścieżki, którą powinny obrać wiadomości transmitowane w sieci.

Odpowiedzialnością urządzeń pośredniczących jest:

- Regeneracje i retransmisja sygnałów komunikacyjnych (zawsze).
- Utrzymywanie danych nt istniejących w sieci ścieżkach transmisyjnych
- Powiadamianie innych urządzeń o błędach i awariach w komunikacji
- Przekierowywanie danych alternatywną ścieżką w wypadku awarii łącza
- Klasyfikacja i kierowanie wiadomościami zgodnie z priorytetami
- Blokowanie lub umożliwianie przepływu danych zgodnie z ustawieniami bezpieczeństwa

Urządzeniami pośredniczącymi są:

- Routery przewodowe lub bezprzewodowe
- Przełączniki (switch) sieci LAN
- Przełączniki wielowarstwowe
- Zapory ogniowe (firewall)

Medium sieciowe:

Komunikację między urządzeniami w sieci zapewniają media sieciowe. To właśnie one tworzą kanały, które służą do przesyłania wiadomości od źródła do celu. W nowoczesnych sieciach komunikacja odbywa się za pomocą mediów takich jak:

- *Przewody metalowe* - przesył danych w formie impulsów elektrycznych
- *Kable światłowodowe* - przesył danych w formie impulsów świetlnych
- *Transmisja bezprzewodowa* - przesył danych za pomocą fal elektromagnetycznych

Kryteria doboru medium sieciowego to:

- Odległość na jaką medium może poprawnie transmitować sygnał
- Otoczenie, w którym medium ma zostać zainstalowane
- Ilość danych, którą medium ma transmitować i prędkość tej transmisji

- Koszt danego medium i jego instalacji

Karta sieciowa:

Moduł umożliwiające fizyczne połączenie urządzenia końcowego z siecią.

Port fizyczny:

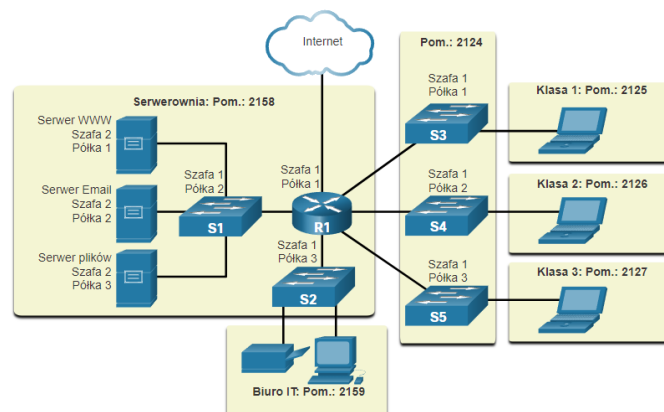
Wtyczka/gniazdo w urządzeniu sieciowym, do którego podłączone jest medium łączące to urządzenie z innym urządzeniem sieciowym.

Interfejs:

Specjalny port w urządzeniu sieciowym, który zapewnia połączenie z innymi sieciami. W routerach (urządzeniach służących do łączenia sieci) porty nazywamy interfejsami sieciowymi.

Schemat topologii fizycznej:

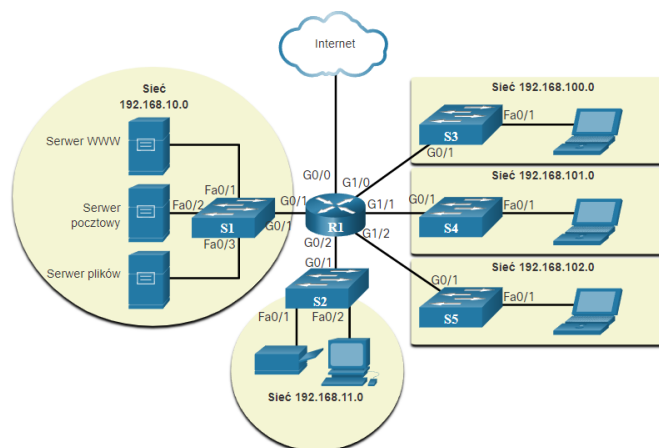
Schemat przedstawiający fizyczne położenie urządzeń i mediów w sieci.



Rysunek 5: Schemat przedstawiający topologię fizyczną sieci.

Schemat topologii logicznej:

Schemat przedstawiający urządzenia, porty i schemat adresowania sieci.



Rysunek 6: Schemat przedstawiający topologię logiczną sieci.

Sieć LAN:

Sieć lokalna (Local Area Network), rozpościerająca się na małym obszarze geograficznym. Może być to np. sieć łącząca urządzenia na obszarze jednego gospodarstwa domowego. Jest ona administrowana przez jedną organizację/osobę. Zapewnia ona wysoką przepustowość do wewnętrznych urządzeń sieciowych.

Sieć WAN:

Sieć Wide Area Network, rozpościerająca się na dużym obszarze geograficznym. Jest to sieć łącząca ze sobą poszczególne sieci LAN. Jest administrowana przez kilku usługodawców internetowych (ISP, Internet Service Provider). Typowo zapewniają wolne połączenie między połączonymi przez WAN sieciami LAN.

Internet:

Ogólnoświatowy zbiór połączonych ze sobą sieci. Może być zinterpretowany jako grupa połączony ze sobą sieci LAN i WAN. Internet nie jest niczyją własnością. Istnieją jednak organizacje, które zajmują się monitorowaniem struktury i standardów globalnej sieci.

Intranet:

Prywatne połączenie sieciowe należące do jakiejś organizacji. Dostępny tylko dla członków tej organizacji lub innych osób, które uzyskały autoryzację.

Ekstranet:

Siec wykorzystywana przez organizację w celu zapewnienia dostępu swoim współpracownikom czy też klientom do swoich danych. Przykładem jest ekstranet szpitala, który zapewnia dostęp do systemu rezerwacji wizyt online dla pacjentów.

Połączenie internetowe dla osób prywatnych i małych firm:

W wypadku gospodarstw domowych i małych firm połączenie z internetem odbywa się za pomocą:

- *Łącza kablowego* - połączenie przez kabel telewizji kablowej o wysokiej przepustowości i dostępności.
- *DSL (Digital Subscriber Line)* - połączenie przez linie telefoniczne o wysokiej przepustowości i dostępności. Często dostępne w formie ADSL, gdzie prędkość pobierania jest większa od prędkości przesyłu.
- *Sieci komórkowej* - połączenie bezprzewodowe uzależnione od dostępności sygnału sieci komórkowej.
- *Satelity* - połączenie bezprzewodowe poprzez sygnał satelitarny, wymagające bezpośredniej widoczności z satelitą.
- *Łącze telefoniczne dial-up* - tanie połączenie poprzez linie telefoniczną i modem o niskiej przepustowości.

Połączenie internetowe dla dużych organizacji:

Ze względu na większe wymagania co do przepustowości i dostępności pasma duże organizacje mają swoje własne metody połączenia z internetem:

- *Dedykowane łącza dzierżawione* - wynajmowane przez organizacje dedykowane obwody zapewniające połączenie między biurami.
- *Metro Ethernet* - połączenie przewodowe rozszerzające technologię dostępu LAN na sieci WAN.
- *Biznes DSL* - połączenie poprzez linie telefoniczne o wysokiej wydajności i dostępności o równych prędkościach przesyłu i pobierania (SDSL).
- *Satelita* - połączenie bezprzewodowe poprzez satelitę.

Sieci konwergentne:

Sieci będące w stanie transportować wiele usług (dane, wideo, audio itd) poprzez jedną i tą samą sieć. Każda z tych przesyłanych usług podlega pod te

same reguły, standardy i umowy.

Aspekty niezawodności sieci:

Nowoczesne sieci są projektowane z zachowaniem odpowiednich standardów, które zapewniają jej poprawne i wydajne funkcjonowanie. Architekci projektując sieć skupiają swoją uwagę na czterech aspektach:

- tolerancji błędów
- skalowalności
- jakości usług(QoS, Quality of Service)
- bezpieczeństwie

Tolerancja błędów:

Sieci powinny być odporne na awarie, czyli w stworzone w sposób ograniczający liczbę urządzeń, które zostaną dotknięte niedogodnościami w wypadku awarii. Muszą być zbudowane tak, aby w wypadku wystąpienia awarii istniał łatwy sposób na odzyskanie sprawności sieci. W tym celu korzystają one z tzw. ścieżek nadmiarowych, które mogą zastąpić uszkodzone ścieżki (sieci z nadmiarowością).

Routery są w stanie wykorzystywać nadmiarowość wykorzystując przełączanie pakietów. Każda wiadomość w sieci jest dzielona na części zwane pakietami, które oprócz właściwych danych zawierają dodatkowe informacje w swoim nagłówku. Następnie każdy pakiet jest osobno przesyłany do odbiorcy końcowego. Router przy każdym kolejnym pakiecie dynamicznie dobiera ścieżkę. Oznacza to, że każdy pakiet danej wiadomości może zostać de facto przesłany inną ścieżką.

Skalowalność:

Sieć musi być skalowalna, aby w prosty sposób móc obsługiwać coraz to nowych użytkowników i aplikacje. Skalowalność zakłada, że takie rozszerzenie odbywa się bez uszczerbku na wydajności już istniejących w sieci usług (inni użytkownicy nie mogą być poszkodowani tym, że podłączyliśmy nowe urządzenie). Skalowalność można osiągnąć przestrzegając przyjętych ogólnie standardów i protokołów.

Jakość usług:

Nowoczesne sieci są konwergentne, są w stanie przysyłać wiele różnych typów

informacji. W wypadku przepełnienia łącza w celu zapewnienia dobrej jakości usług sieciowych routery są w stanie priorytetyzować transport jednego typu danych nad drugim (np. przesył głosu ma priorytet nad przesyłem danych, bo niestabilna transmisja w połączeniu głosowym jest bardziej uciążliwa niż w wypadku chociażby otwierania stron WWW). Takie priorytety są ustalane w polityce jakości usług.

Bezpieczeństwo sieci:

Sieci powinny być także bezpieczne. Administratorzy w tym aspekcie muszą zwrócić uwagę na bezpieczeństwo infrastruktury sieciowej oraz bezpieczeństwo informacji.

Zabezpieczenie infrastruktury to fizyczne zabezpieczenie urządzeń zapewniających dostęp do sieci oraz zapobieganie dostępowi do nieautoryzowanego dostępu do ich oprogramowania zarządzającego.

Zabezpieczenie informacji zawartych w przesyłanych pakietach wymaga spełnienia trzech wymagań:

- *Poufności* - zapewnienie, że dane nie zostaną odczytane ani udostępnione osobom nieupoważnionym
- *Integralności* - zapewnienie, że dane nie ulegną zmianie podczas przesyłu
- *Dostępności* - zapewnienie terminowego i niezawodnego dostępu do danych uprawnionym użytkownikom

Zagrożenia bezpieczeństwa:

Obecnie wiele zagrożeń dla sieci pochodzi z Internetu. Są to zagrożenia zewnętrzne. (wektor zewnętrzny). Zaliczamy do nich:

- *Wirusy, robaki, konie trojańskie* - uruchamiające złośliwe oprogramowanie na zaatakowanym urządzeniu
- *Spyware i adware* - potajemnie zbierające informacje oprogramowanie
- *Ataki zero-day* - pojawiające się od razu po wykryciu podatności na atak
- *Ataki aktora zagrożeń* - działania złośliwej osoby

- *Odmowa usługi* - ataki mające na celu zmniejszenie wydajności działania aplikacji/sprzętu lub jej zatrzymanie
- *Przechwytywanie i kradzież danych*
- *Kradzież tożsamości* - atak polegający na kradzieży danych logowania

Istnieją również zagrożenia wewnętrzne, czyli pochodzące od urządzeń partycypujących w danej sieci. Mogą one być spowodowane zgubieniem urządzenia, celowym działaniem, przypadkowymi błędami użytkowników.

Elementy bezpieczeństwa sieci domowej:

Sieci domowe są chronione na bardzo podstawowym poziomie. Zabezpieczenia są wdrażane na urządzeniach końcowych oraz w punkcie łączenia sieci domowej z internetem. Często takie zabezpieczenia zapewnia sam dostawca usług internetowych. Są to chociażby:

- *Oprogramowanie antywirusowe i antyszpiegowskie* - chroniące urządzenie końcowe
- *Zapory filtrujące* - filtrujące nieautoryzowany dostęp do sieci oraz ruch z sieci do internetu. Zapory filtrujące mogą wystąpić na urządzeniach końcowych jak i na routerach.

Elementy bezpieczeństwa sieci korporacyjnych:

Sieci dużych firm wymagają bardziej dogłębnego monitorowania oraz kontrolowania ruchu. Ich systemy bezpieczeństwa składają się zazwyczaj z wielu współpracujących ze sobą komponentów. Takie sieci oczywiście także używają zapór filtrujących i oprogramowań antywirusowych ale korzystają również z:

- *Dedykowane systemy zapór* - systemy zapewniające bardziej zaawansowane funkcje zapory bardziej szczegółowo i wydajniej filtrujące ruch.
- *Listy kontroli dostępu (ACL)* - dodatkowo filtrujące dostęp i przekazywanie ruchu na bazie adresów IP i aplikacji
- *Systemy przeciwdziałania atakom (IPS)* - szybko identyfikujące ataki zero-day
- *Wirtualne sieci prywatne (VPN)* - zapewniające bezpieczny dostęp do organizacji dla pracowników zdalnych