Polecenie ipconfig

1. **Jakie informacje można uzyskać za pomocą polecenia ipconfig, które zostało wywołane bez dodatkowych opcji?**

Polecenie ipconfig, wywołane bez dodatkowych opcji, umożliwia uzyskanie podstawowych informacji na temat interfejsów sieciowych w systemie. Obejmuje to adresy IP, maski podsieci, bramy domyślne i status interfejsu sieciowego.

2. **Jakie informacje dodatkowe można uzyskać dzięki opcji /all?**

Opcja /all pozwala na uzyskanie bardziej szczegółowych informacji o interfejsach sieciowych. Obejmuje to również informacje o fizycznym adresie MAC, adresach DNS, serwerach DHCP, a także bardziej szczegółowe informacje o konfiguracji interfejsów sieciowych.

3. **Co to jest dzierżawa adresu IP i jak długo trwa?**

Dzierżawa adresu IP odnosi się do procesu przydzielania i czasowego przypisania adresu IP przez serwer DHCP (Dynamic Host Configuration Protocol). Czas trwania dzierżawy adresu IP może być skonfigurowany przez administratora sieci, ale zazwyczaj wynosi kilka godzin lub dni. Po upływie czasu dzierżawy, komputer musi odnowić dzierżawę adresu IP, w przeciwnym razie może stracić połączenie z siecią.

4. **Jakie informacje można uzyskać za pomocą polecenia ipconfig /displaydns**

Polecenie ipconfig /displaydns pozwala na wyświetlenie informacji dotyczących bufora DNS na komputerze. Można zobaczyć zapisane rekordy DNS, takie jak nazwy domenowe i odpowiadające im adresy IP, które zostały wcześniej rozwiązane i przechowywane w pamięci podręcznej.

5. **Czy za pomocą polecenia ipconfig można sprawdzić adres MAC karty sieciowej? Jeśli nie, to w jaki sposób można odczytać ten adres**

Polecenie ipconfig samo w sobie nie umożliwia bezpośredniego odczytu adresu MAC karty sieciowej. Jednak adres MAC można odczytać, używając polecenia ipconfig /all. W wynikach polecenia pojawi się sekcja "Adres fizyczny", która reprezentuje adres MAC danej karty sieciowej.

6. **Czy za pomocą polecenia ipconfig /all można uzyskać informacje o adresach IPv6? Czy adresy IPv4 i IPv6 różnią się? Jeśli tak, wymień różnice.**

Tak, polecenie ipconfig /all umożliwia uzyskanie informacji zarówno o adresach IPv4, jak i IPv6. Adresy IPv4 i IPv6 różnią się znacząco. Adresy IPv4 składają się z czterech sekcji liczb dziesiętnych, podczas gdy adresy IPv6 składają się z ośmiu sekcji szesnastkowych liczb. Adresy IPv6 są dłuższe i zawierają dwukropki między sekcjami. Ponadto, adresy IPv6 mają większą pojemność, co umożliwia obsługę większej liczby urządzeń i rozwiązuje problemy z brakiem adresów IPv4.

7. **Czym różni się adres IP (v4 i v6) od adresu MAC?**

Adres IP (zarówno IPv4, jak i IPv6) identyfikuje urządzenie w sieci. Adres IP jest nadawany przez sieć i może się zmieniać w zależności od konfiguracji sieciowej. Adres MAC (Media Access Control) jest unikalnym identyfikatorem przypisanym do karty sieci

Polecenie ping

1. **W jakich granicach zawierają się czasy odpowiedzi zdalnego komputera na wysyłane zapytania?**

Czasy odpowiedzi zdalnego komputera na wysyłane zapytania w poleceniu ping zawierają się w granicach czasu wyrażonego w milisekundach (ms). Zwykle, im niższy czas odpowiedzi, tym lepsze jest połączenie z danym hostem. Czasy odpowiedzi mogą różnić się w zależności od odległości fizycznej między komputerem a docelowym hostem, obciążenia sieci, jakości połączenia itp.

2. **Jakie informacje można uzyskać za pomocą polecenia ping?**

Polecenie ping umożliwia sprawdzenie dostępności i pomiar czasu odpowiedzi hosta w sieci. Informacje, które można uzyskać za pomocą polecenia ping, obejmują:

- Czas odpowiedzi hosta na wysłane zapytania ICMP (Ping)
- Procentowa strata pakietów (jeśli występuje)
- Statystyki dotyczące opóźnień, takie jak minimalny, maksymalny i średni czas odpowiedzi
- Adres IP hosta docelowego

3. **Działanie polecenia ping 127.0.0.1**

Polecenie ping 127.0.0.1 jest używane do testowania połączenia z lokalnym interfejsem sieciowym. Adres IP 127.0.0.1 jest specjalnym adresem loopback (pętli zwrotnej), który oznacza lokalny komputer. Wykonanie polecenia ping 127.0.0.1 służy do sprawdzenia, czy stos sieciowy na komputerze jest poprawnie skonfigurowany i czy interfejs sieciowy działa poprawnie.

4. **Jeśli korzystamy ze strony to skąd będą wysyłane wiadomości ICMP?**

Jeśli korzystamy ze strony internetowej, wiadomości ICMP będą wysyłane z naszego komputera do adresu IP docelowego strony. Po drodze wiadomości będą przechodziły przez różne routery i przełączniki sieciowe, aż dotrą do docelowego serwera. Wiadomości ICMP będą wysyłane z interfejsu sieciowego naszego komputera do interfejsu sieciowego docelowego serwera.

Polecenie tracert

1. **W jaki sposób przedstawiane są informacje o drodze pokonywanej przez pakiet?**

Polecenie tracert (lub traceroute w systemach Unix/Linux) służy do śledzenia trasy pakietu IP od komputera źródłowego do docelowego poprzez wysyłanie pakietów z coraz większymi wartościami TTL (Time to Live) i analizowanie odpowiedzi otrzymywanych od kolejnych węzłów sieciowych na tej trasie.

Informacje o drodze pokonywanej przez pakiet są przedstawiane w postaci listy węzłów sieciowych (routery) połączonych kolejno od komputera źródłowego do docelowego. Dla każdego węzła sieciowego na trasie polecenie tracert pokazuje:

- Numer skoku (hop count) - określa kolejność routera na trasie.
- Adres IP - adres IP routera na danej pozycji.
- Czas odpowiedzi - czas, który upłynął od wysłania pakietu do otrzymania odpowiedzi z danego routera. Pokazywany jest czas w milisekundach.

Dzięki tym informacjom można śledzić ścieżkę, jaką pokonują pakiety IP w drodze od źródła do celu. Można także zidentyfikować, które routery mogą generować opóźnienia lub przyczyniać się do utraty pakietów w trakcie transmisji danych.

Polecenie nslookup

1. **Z jakimi opcjami można wywoływać to polecenie, jakiego typu informacje można dzięki opcjom uzyskać?**

Polecenie nslookup służy do wykonywania zapytań DNS (Domain Name System) w celu uzyskania informacji dotyczących nazw domenowych i adresów IP. Polecenie nslookup może być wywoływane z różnymi opcjami, które umożliwiają uzyskanie różnych rodzajów informacji.

Oto niektóre z opcji, które można używać w poleceniu nslookup:

- querytype <typ> lub -q <typ>: Pozwala na określenie żądanego typu zapytania DNS. Możliwe wartości dla <typ> to np. A (adres IPv4), AAAA (adres IPv6), MX (rekordy poczty), NS (serwery nazw), CNAME (aliasy), itd.
- debug: Włącza tryb debugowania, który wyświetla szczegółowe informacje o przetwarzaniu zapytań DNS.
- server <adres_IP>: Określa serwer DNS, który ma być używany do wykonania zapytania. W przypadku pominięcia tej opcji, zostanie użyty domyślny serwer DNS skonfigurowany na komputerze.
- timeout <czas>: Określa czas oczekiwania na odpowiedź od serwera DNS, wyrażony w sekundach.
- all: Wyświetla wszystkie dostępne informacje na temat danego zapytania DNS, takie jak rekordy adresowe (A lub AAAA), rekordy MX, rekordy NS itp.
- queryclass <klasa>: Określa żądaną klasę zapytania DNS. Najczęściej używaną wartością jest IN (Internet), ale istnieją również inne klasy, takie jak CH (Chaosnet) czy HS (Hesiod).

Dzięki różnym opcjom polecenia nslookup można uzyskać szczegółowe informacje na temat rekordów DNS dla określonej domeny, przeprowadzić testy połączenia z serwerem DNS, zmienić serwer DNS, ustawić czas oczekiwania na odpowiedź oraz otrzymać dodatkowe szczegóły diagnostyczne w trybie debugowania.

Polecenie netstat

1. **Jakie informacje są możliwe do uzyskania za pomocą polecenia netstat?**

Polecenie netstat służy do wyświetlania różnych informacji o połączeniach sieciowych i statystykach sieciowych na komputerze. Oto niektóre z możliwych informacji, które można uzyskać za pomocą polecenia netstat:

- Połączenia sieciowe: Netstat może wyświetlić listę aktywnych połączeń sieciowych na komputerze, zarówno połączenia przychodzące, jak i wychodzące. Dla każdego połączenia można uzyskać informacje, takie jak adres IP i port lokalny, adres IP i port zdalny, stan połączenia (np. ESTABLISHED, LISTENING), itd.
- Statystyki protokołów: Netstat może pokazać statystyki dla różnych protokołów sieciowych, takich jak TCP (Transmission Control Protocol) i UDP (User Datagram Protocol). Statystyki te obejmują liczbę wysłanych i otrzymanych pakietów, liczbę błędów, liczby połączeń itp.
- Tablica trasowania (routing table): Netstat może wyświetlać informacje o tablicach trasowania, które zawierają informacje na temat dostępnych sieci, bram domyślnych i interfejsów sieciowych.
- Statystyki interfejsów sieciowych: Netstat może dostarczać informacje na temat statystyk dla poszczególnych interfejsów sieciowych, takich jak liczba wysłanych i otrzymanych pakietów, liczba błędów, prędkość transmisji itp.
- Połączenia w stanie nasłuchiwania (listening): Netstat może pokazać, które porty na komputerze są otwarte i nasłuchujących przychodzących połączeń sieciowych.
- Zawartość bufora: Netstat może pokazać zawartość bufora TCP/IP, który zawiera dane, które są gotowe do wysłania lub odbioru.

Polecenie netstat może być używane z różnymi opcjami, które pozwalają na dostosowanie wyświetlanych informacji. Opcje te mogą obejmować filtrowanie wyników na podstawie protokołu, interfejsu sieciowego, portu, itp.

Polecenie arp

Polecenie ARP (Address Resolution Protocol) służy do mapowania adresów IP na adresy MAC w lokalnej sieci. Protokół ARP jest używany w sieciach Ethernet lub Wi-Fi, aby znaleźć adres MAC dla określonego adresu IP.

1. Do czego służy protokół arp?

Protokół ARP służy do rozwiązania problemu znajdowania adresu MAC na podstawie adresu IP w sieci lokalnej. Gdy komputer chce wysłać pakiet do innego urządzenia w sieci, musi znać jego adres MAC, aby przekazać pakiet na właściwy interfejs sieciowy.

2. Jakie informacje można uzyskać za pomocą polecenia arp?

Za pomocą polecenia arp można uzyskać następujące informacje:

- Tablica ARP: Wyświetla tabelę ARP, która zawiera mapowanie adresów IP na adresy MAC dla urządzeń w lokalnej sieci.
- Adres MAC: Wyświetla adres MAC danego urządzenia w lokalnej sieci.
- Adres IP: Wyświetla adresy IP urządzeń w lokalnej sieci.

3. Jakie opcje są dostępne dla tego polecenia? (proszę podać 3-4).

Opcje dostępne dla polecenia arp to:

- arp -a: Wyświetla wszystkie wpisy w tablicy ARP.
- arp -d <adres_IP>: Usuwa wpis z tablicy ARP dla określonego adresu IP.
- arp -s <adres_IP> <adres_MAC>: Dodaje ręcznie wpis do tablicy ARP, mapując określony adres IP na adres MAC.
- arp -g: Wyświetla dynamiczne wpisy w tablicy ARP.

4. Czy informacje uzyskane za pomocą protokołu ARP są zapamiętywane w systemie operacyjnym?

Informacje uzyskane za pomocą protokołu ARP są tymczasowe i zazwyczaj są przechowywane w pamięci podręcznej systemu operacyjnego. Tablica ARP może być dynamicznie aktualizowana w zależności od aktywności w sieci, a wpisy mogą być usuwane po upływie pewnego czasu bezczynności lub po rozłączeniu urządzenia. Każde urządzenie w sieci może mieć swoją własną tablicę ARP.

Wireshark Ping

1. Ile wiadomości i jakiego typu wysłał komputer?

Polecenie ping wysyła wiadomości ICMP Echo Request do docelowego hosta. Domyślnie wysyłane są cztery takie wiadomości.

2. Ile wiadomości i jakiego typu otrzymał komputer?

Po wysłaniu wiadomości ICMP Echo Request, komputer oczekuje na odpowiedź ICMP Echo Reply od docelowego hosta. Jeśli host docelowy jest dostępny i skonfigurowany do odpowiadania na pakiety ping, komputer otrzyma cztery wiadomości ICMP Echo Reply.

3. Jakie są różnice pomiędzy adresem IPv4 i MAC?

Różnice między adresem IPv4 a adresem MAC zostały opisane wcześniej w odpowiedzi na wcześniejsze pytanie.

4. **Określić wartość parametru TTL.**

TTL (Time to Live) to parametr, który jest używany w pakietach IP. Określa maksymalną liczbę skoków (routingu) jakie pakiet może przejść, zanim zostanie odrzucony. Każdy router, przez który przechodzi pakiet, dekrementuje wartość TTL o 1. Jeśli wartość TTL osiągnie 0, pakiet jest odrzucany.

5. **Co to jest TTL i dlaczego jest ustawiany w pakietach IP?**

TTL jest ustawiany w pakietach IP, aby zapobiec nieskończonym pętlom pakietów w sieci. Działa jako mechanizm zapobiegający zbyt długiemu przetrzymywaniu pakietów w sieci, gdyż w przypadku awarii routera lub pętli w sieci, pakiety z TTL równym 0 są odrzucane.

6. **Czy pole o podobnym znaczeniu znajduje się w ramce Ethernetowej?**

W ramce Ethernetowej pole o podobnym znaczeniu to pole Length/Type, które określa długość ramki lub typ protokołu warstwy wyższej, jak IP. Nie ma jednak bezpośredniego pola TTL w ramce Ethernetowej.

Wireshark Tracert

1. **Ile wiadomości i jakiego typu wysłał komputer?**

Polecenie tracert wysyła wiadomości ICMP Echo Request (czasami nazywane Time Exceeded) z rosnącymi wartościami TTL. Liczba wysłanych wiadomości zależy od liczby routerów (hopów) między komputerem a docelowym adresem IP.

2. **Ile wiadomości i jakiego typu odebrał komputer?**

Komputer odbierze odpowiedzi ICMP Time Exceeded (czasami ICMP Echo Reply), które są generowane przez routery, gdy pakiet przekracza wartość TTL. Liczba odebranych wiadomości zależy od liczby routerów między komputerem a docelowym adresem IP oraz od konfiguracji tych routerów.

3. **Określić wartość parametru TTL w poszczególnych pakietach.**

Wartość parametru TTL w poszczególnych pakietach będzie rosnąca w miarę przesyłania ich przez routery. Każdy router dekrementuje wartość TTL o 1. Można śledzić wartość TTL w przechwyconych pakietach w programie Wireshark.

Wireshark Patchping

1. **Ile wiadomości i jakiego typu wysłał komputer?**

Polecenie pathping wysyła wiadomości ICMP Echo Request (ping) do docelowego hosta. Liczba wysłanych wiadomości zależy od ustawień domyślnych systemu operacyjnego, ale zazwyczaj są wysyłane trzy pakiety ICMP Echo Request na każdy router na ścieżce do docelowego hosta.

2. **Ile wiadomości i jakiego typu odebrał komputer?**

Komputer odbiera odpowiedzi ICMP Echo Reply od docelowego hosta oraz wiadomości ICMP Time Exceeded (czasami ICMP Echo Reply) generowane przez routery, gdy pakiet przekracza wartość TTL. Liczba odebranych wiadomości zależy od liczby routerów między komputerem a docelowym adresem IP oraz od konfiguracji tych routerów.

3. **Czy w wysyłanych (odbieranych) pakietach zmieniana jest wartość parametru TTL, jeśli tak to w jaki sposób?**

Wysyłane pakiety ICMP Echo Request mają wartość TTL zwiększaną o 1 na każdym hopie, czyli na każdym routerze na trasie do docelowego hosta. Odbierane pakiety mogą mieć różne wartości TTL, ponieważ są generowane przez routery i zależą od konfiguracji tych routerów.

4. **Na podstawie przechwyconych pakietów z wiadomościami protokołu ICMP przedstaw zasadę działania polecenia pathping.**

Polecenie pathping jest hybrydą polecenia ping i tracert. Wysyła ono pakiety ICMP Echo Request do docelowego hosta, jak w przypadku ping, ale jednocześnie analizuje odpowiedzi Time Exceeded (czasami ICMP Echo Reply) generowane przez routery, jak w przypadku tracert. Pathping śledzi ścieżkę pakietów i oblicza statystyki opóźnień i utraty pakietów na każdym hopie między komputerem a docelowym adresem IP.

Wireshark Telnet oraz SSH

Telnet

1. **Jakie informacje przedstawia program po wyborze opcji Follow TCP Stream?**

Po wybraniu opcji "Follow TCP Stream" w programie Wireshark, zostanie otwarte nowe okno, w którym wyświetlane są wszystkie przepływające pakiety TCP w ramach tego strumienia. W tym oknie można zobaczyć zarówno dane wysyłane przez klienta (np. polecenia, login, hasło) oraz dane otrzymywane z serwera (np. odpowiedzi, komunikaty).

2. **Co można powiedzieć o protokole telnet?**

Protokół telnet jest protokołem sieciowym używanym do zdalnego logowania na serwery. Umożliwia zdalny dostęp do wiersza poleceń na zdalnym hoście i przesyłanie danych tekstowych między klientem a serwerem. Protokół telnet działa na warstwie aplikacji modelu OSI i używa protokołu TCP do nawiązywania połączenia.

3. **W jaki sposób przesyłane są login i hasło?**

Login i hasło przesyłane są w formie niezaszyfrowanej (plain text) przez protokół telnet. Oznacza to, że dane są przesyłane w postaci zrozumiałej dla człowieka i mogą być odczytane przez osoby podsłuchujące ruch sieciowy. Dlatego korzystanie z protokołu telnet w sieciach publicznych lub niezaufanych jest niebezpieczne, ponieważ może prowadzić do przechwycenia poufnych informacji uwierzytelniających. W celu zapewnienia bezpieczeństwa przesyłanych danych, zaleca się stosowanie protokołu SSH (Secure Shell) zamiast telnetu, ponieważ SSH szyfruje dane i zapewnia bezpieczne zdalne logowanie i przesyłanie informacji.

SSH

1. **Jakie informacje przedstawia program po wyborze opcji Follow TCP Stream?**

Po wybraniu opcji "Follow TCP Stream" w programie Wireshark, zostanie otwarte nowe okno, w którym wyświetlane są wszystkie przepływające pakiety TCP w ramach tego strumienia. W tym oknie można zobaczyć dane wysyłane i otrzymywane między klientem a serwerem, w formacie zrozumiałym dla człowieka.

2. **Co można powiedzieć o protokole telnet**

Protokół SSH (Secure Shell) jest protokołem sieciowym, który zapewnia bezpieczne zdalne logowanie i przesyłanie danych. W przeciwieństwie do protokołu telnet, SSH używa szyfrowania, takiego jak asymetryczne szyfrowanie klucza publicznego, aby chronić poufne informacje

uwierzytelniające, takie jak login i hasło. SSH również zapewnia integralność i uwierzytelnianie serwera.

3. **W jaki sposób przesyłane są login i hasło?**

W protokole SSH login i hasło przesyłane są w formie zaszyfrowanej, co oznacza, że dane są nieczytelne dla osób podsłuchujących ruch sieciowy. Protokół SSH wykorzystuje protokoły kryptograficzne do nawiązywania bezpiecznego połączenia i wymiany kluczy kryptograficznych, a następnie szyfruje dane przesyłane między klientem a serwerem.

Który sposób łączenia się z serwerem jest bardziej bezpieczny?
Protokół SSH jest znacznie bardziej bezpieczny niż protokół telnet. Protokół SSH zapewnia uwierzytelnienie i szyfrowanie, co oznacza, że dane przesyłane przez SSH są chronione przed przechwyceniem i odczytaniem przez osoby nieuprawnione. W porównaniu, protokół telnet przesyła dane w formie niezaszyfrowanej, co sprawia, że są one podatne na przechwycenie i odczytanie przez osoby trzecie. W związku z tym zaleca się korzystanie z protokołu SSH zamiast telnetu, zwłaszcza w przypadku przesyłania poufnych informacji.

Wireshark FTP

Podczas analizy pakietów związanych z połączeniem FTP można zobaczyć, że dane uwierzytelniające, takie jak login i hasło, są przesyłane w postaci zrozumiałej dla człowieka (plain text). Protokół FTP nie zapewnia domyślnie szyfrowania danych ani uwierzytelniania serwera, co oznacza, że dane przesyłane za pomocą FTP są narażone na przechwycenie i odczytanie przez osoby trzecie.

W odniesieniu do pytania, czy istnieje bezpieczniejszy sposób przesyłania plików niż FTP, odpowiedź brzmi tak. Protokół FTP nie jest uważany za bezpieczny ze względu na brak szyfrowania i uwierzytelniania. Istnieje jednak wiele innych protokołów, które zapewniają bezpieczne przesyłanie plików, takie jak FTPS (FTP over SSL/TLS) i SFTP (SSH File Transfer Protocol).

FTPS to rozszerzenie protokołu FTP, które dodaje warstwę SSL/TLS do komunikacji FTP, umożliwiając szyfrowanie danych i uwierzytelnianie serwera. SFTP natomiast jest integralną częścią protokołu SSH i zapewnia bezpieczne przesyłanie plików poprzez szyfrowanie i uwierzytelnianie.

Wniosek: Jeśli chodzi o bezpieczeństwo przesyłania plików, FTP nie jest zalecanym protokołem ze względu na brak zabezpieczeń. Bezpieczniejsze opcje to korzystanie z FTPS lub SFTP, które oferują szyfrowanie i uwierzytelnianie.

Sieci LAN

1. **Jakie urządzenia są potrzebne aby komputery w sieci LAN mogły się ze sobą komunikować?**

Aby komputery w sieci LAN mogły się ze sobą komunikować, potrzebne są następujące urządzenia:

- Komputery: Są to urządzenia końcowe, które są podłączone do sieci LAN i mają możliwość komunikacji poprzez protokoły sieciowe, takie jak TCP/IP.
- Przełączniki (Switches): Przełączniki są wykorzystywane do połączenia różnych urządzeń w sieci LAN. Przełączniki odbierają dane z jednego portu i przesyłają je do odpowiedniego portu, aby dane dotarły do docelowego urządzenia w sieci.
- Kable sieciowe: Kable sieciowe są używane do połączenia komputerów i przełączników w sieci LAN. Najczęściej stosowanym kablem jest kabel Ethernet.

2. **Jakie adresy MAC oraz IP znajdują się w ramkach/pakietach z wiadomościami protokołu ICMP. Jak to wyjaśnić?**

Adresy MAC oraz IP znajdują się w ramkach/pakietach z wiadomościami protokołu ICMP w następujący sposób:

- Adres MAC: Adres MAC (Media Access Control) znajduje się w nagłówku ramki Ethernet, która przenosi pakiet ICMP. Adres MAC jest fizycznym adresem karty sieciowej urządzenia. Adres MAC jest wykorzystywany do bezpośredniego dostarczenia pakietów w obrębie sieci LAN.
- Adres IP: Adres IP (Internet Protocol) znajduje się w nagłówku pakietu ICMP. Adres IP identyfikuje źródłowy i docelowy komputer w sieci. Adres IP jest używany do dostarczania pakietów między różnymi sieciami, a także do routowania pakietów w sieci.

3. **Jaki jest zasięg adresów IP (OSI: W. sieci) oraz adresów MAC (OSI: W. Łącza danych)?**

Zasięg adresów IP (warstwa sieci w modelu OSI) obejmuje całą sieć, zarówno lokalną jak i rozległą. Adresy IP są unikalne w skali globalnej i służą do identyfikacji poszczególnych urządzeń w sieci. Adresy IP składają się z dwóch części: identyfikatora sieci i identyfikatora hosta, które są używane do określenia, do której sieci należy dany komputer i który konkretny komputer w tej sieci.

Zasięg adresów MAC (warstwa Łącza danych w modelu OSI) jest ograniczony do lokalnej sieci (LAN). Adresy MAC są unikalne w skali lokalnej sieci i są przypisane do kart sieciowych. Adres MAC jest używany do bezpośredniego dostarczenia danych między urządzeniami w tej samej sieci LAN, na podstawie fizycznego adresu karty sieciowej.

Protokół DNS

1. **Do czego służy protokół DNS?**

Protokół DNS (Domain Name System) służy do tłumaczenia nazw domenowych na adresy IP i odwrotnie. Głównym zadaniem protokołu DNS jest przekształcenie zrozumiałych dla ludzi nazw domenowych (np. www.example.com) na adresy IP, które są potrzebne do identyfikacji i komunikacji z konkretnym serwerem.

2. **Jakie wiadomości DNS zostały przechwycone przez program Wireshark?**

Program Wireshark może przechwytywać różne wiadomości DNS, takie jak zapytania DNS (DNS queries), odpowiedzi DNS (DNS responses), zapytania typu PTR (odwrotne przekształcenie), zapytania typu MX (rekordy poczty) itp. Wiadomości DNS związane z tłumaczeniem nazw domenowych na adresy IP i vice versa są przechwytywane przez Wireshark.

3. **Jaki protokół warstwy transportowej używany jest do przenoszenia wiadomości DNS?**

Protokół warstwy transportowej używany do przenoszenia wiadomości DNS to protokół UDP (User Datagram Protocol). DNS jest zazwyczaj realizowany przez UDP z uwagi na swoją prostotę i niższe opóźnienia w porównaniu do protokołu TCP (Transmission Control Protocol).

4. **Który port używany jest przez serwer DNS?**

Serwer DNS używa portu 53 jako port docelowy. Wiadomości DNS są wysyłane na ten port, aby nawiązać komunikację z serwerem DNS.

5. **Jaki numer portu używany jest przez lokalny komputer?**

Numer portu używany przez lokalny komputer zależy od konkretnego programu lub usługi korzystającej z protokołu DNS. Standardowy numer portu dla klienta DNS wynosi 53. Jednak lokalny komputer może używać różnych portów jako źródłowych w przypadku nawiązywania połączenia z serwerem DNS.

6. **Czy serwer DNS znajduje się w sieci lokalnej**

Serwer DNS może znajdować się zarówno w sieci lokalnej, jak i w sieci zewnętrznej. Istnieją publiczne serwery DNS, które są dostępne publicznie w Internecie i dostarczają informacji o domenach na całym świecie. Dodatkowo, w sieci lokalnej może istnieć serwer DNS, który obsługuje lokalne zapytania DNS dla urządzeń w tej sieci.

Routing

1. **Jaka jest składnia polecenia traceroute?**

Składnia polecenia traceroute: traceroute [opcje] [adres docelowy]

2. **Jaka jest składnia polecenia ipconfig?**

Składnia polecenia ipconfig: ipconfig [opcje]

3. **Jakie informacje można znaleźć w tablicy routingu?**

W tablicy routingu można znaleźć informacje dotyczące sieci docelowych, interfejsów sieciowych, bram domyślnych, metryk tras, typów protokołów routingu itp. Tablica routingu zawiera informacje, które są wykorzystywane do podejmowania decyzji o przesyłaniu pakietów w sieci.

4. **Które informacje są niezbędne do podjęcia decyzji o routingu?**

Do podjęcia decyzji o routingu niezbędne są informacje takie jak adres docelowy pakietu, tablica routingu zawierająca wpisy dotyczące dostępnych tras, metryki tras (koszt przesyłania), interfejsy sieciowe i adresy IP, a także typy protokołów routingu, które są aktywne w sieci.

5. **Jaki typ routingu został uruchomiony na routerze (statyczny/dynamiczny)?**

Typ routingu (statyczny lub dynamiczny) zależy od konfiguracji routera. Routery mogą być skonfigurowane do korzystania z routingu statycznego, w którym administrator ręcznie wprowadza wpisy do tablicy routingu, lub routingu dynamicznego, w którym routery wymieniają informacje o trasach za pomocą protokołów routingu i automatycznie aktualizują tablice routingu.

6. **Jaki protokół routingu został uruchomiony na routerze?**

Protokół routingu uruchomiony na routerze zależy od konfiguracji. Najpopularniejszymi protokołami routingu są OSPF (Open Shortest Path First), RIP (Routing Information Protocol), BGP (Border Gateway Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol) itp.

7. **Czy na podstawie tablicy routingu można narysować mapę sieci?**

Tablica routingu nie dostarcza wystarczających informacji do bezpośredniego narysowania mapy sieci. Mapa sieci obejmuje nie tylko informacje o trasach i adresach IP, ale także topologię fizyczną sieci, której nie można odtworzyć tylko na podstawie tablicy routingu.

8. **Informacje o jakich sieciach znajdują się w tablicy routingu (show ip route)?**

Tablica routingu (polecenie "show ip route") zawiera informacje o dostępnych trasach do różnych sieci. Można znaleźć informacje takie jak sieć docelowa, maska podsieci, brama domyślna, interfejs sieciowy, metryka trasy, typ protokołu routingu itp.

9. **Informacje o ilu sieciach zapisane są w tablicy routingu?**

Liczba sieci zapisanych w tablicy routingu może się różnić w zależności od konfiguracji routera i typu routingu. Tablica routingu może zawierać wpisy dla wielu sieci, zarówno lokalnych, jak i zdalnych.

10. W jaki sposób tablica routingu jest tworzona?

Tablica routingu jest tworzona na podstawie konfiguracji routera oraz informacji o trasach, które są gromadzone i wymieniane między routerami w sieci. Routery korzystają z różnych protokołów routingu (takich jak OSPF, RIP, BGP itp.) do komunikacji i aktualizacji tablic routingu, które umożliwiają im podejmowanie decyzji o przesyłaniu pakietów w sieci.

Dodatkowe

1. Z jakich pól składają się nagłówki (określ w bajtach długość każdego pola):

a) Ramka Ethernetowa:

- Adres MAC docelowego hosta: 6 bajtów
- Adres MAC źródłowy hosta: 6 bajtów
- Typ ramki (np. IPv4, ARP): 2 bajty

b) Pakiet IP:

- Wersja IP i długość nagłówka: 1 bajt
- Typ usługi: 1 bajt
- Długość całkowita pakietu: 2 bajty
- Identyfikator: 2 bajty
- Flagi i przesunięcie fragmentu: 2 bajty
- Czas życia (TTL): 1 bajt
- Protokół (np. TCP, UDP, ICMP): 1 bajt
- Suma kontrolna nagłówka: 2 bajty
- Adres IP źródła: 4 bajty
- Adres IP docelowy: 4 bajty

c) Segment TCP:

- Port źródłowy: 2 bajty
- Port docelowy: 2 bajty
- Numer sekwencyjny: 4 bajty
- Numer potwierdzenia: 4 bajty
- Długość nagłówka i flagi: 2 bajty
- Rozmiar okna: 2 bajty
- Suma kontrolna nagłówka: 2 bajty
- Wskaźnik priorytetu awaryjnego: 1 bajt

2. Z ilu bajtów składają się wiadomości protokołu DNS?

Wiadomości protokołu DNS różnią się w długości, ale zwykle mają od kilkudziesięciu do kilkuset bajtów, w zależności od rodzaju zapytania lub odpowiedzi.

3. Z ilu bajtów składają się wiadomości protokołu ARP?

Wiadomości protokołu ARP mają stałą długość i składają się z 28 bajtów.

4. Co znajduje się w polu danych wybranej wiadomości DNS, ARP i ICMP?

Pola danych w wiadomościach:

- Wiadomość DNS: Zawartość pola danych DNS różni się w zależności od rodzaju zapytania lub odpowiedzi. Na przykład, w zapytaniach DNS pole danych zawiera nazwę domeny, a w odpowiedziach zawiera adresy IP skojarzone z daną nazwą domeny.
- Wiadomość ARP: Pole danych w wiadomości ARP zawiera informacje o adresach MAC i IP hostów, które uczestniczą w żądaniu ARP lub odpowiedzi ARP.

- Wiadomość ICMP: Pole danych w wiadomości ICMP może zawierać różne informacje w zależności od typu komunikatu ICMP. Na przykład, w komunikacie "Echo Request" (ping) pole danych zawiera wartości używane do identyfikacji zapytania i odpowiedzi.

5. Ile pakietów musi wysłać komputer zanim zacznie się łączyć z serwerem WWW?

Liczba pakietów wysyłanych przez komputer zanim rozpocznie się łączenie z serwerem WWW zależy od protokołu komunikacyjnego używanego w warstwie transportowej. W przypadku protokołu TCP, które jest często używane przy połączeniach z serwerem WWW, jest to proces trzech kroków zwany "trójfazowym ustanawianiem połączenia". Obejmuje to wysłanie i odbiór trzech pakietów: SYN, SYN-ACK i ACK.