WYKŁAD 1

Co to jest protokół komunikacyjny? Dlaczego wprowadza się warstwy protokołów?

Protokół komunikacyjny to zbiór reguł i kroków postępowania, które są automatycznie wykonywane przez urządzenia komunikacyjne w celu nawiązania łączności i wymiany danych. Ustalany na stałe lub na czas danej sesji schemat postępowania. Określa on format danych i funkcję zmiany stanu. Na podstawie protokołu powinno dać się **jednoznacznie** skonstruować program komunikujący się.

Przesyłanie danych komputerowych to niezwykle trudny proces, dlatego rozdzielono go na kilka "etapów", czyli warstw. Warstwy oznaczają w istocie poszczególne funkcje spełniane przez sieć.

Wymień warstwy internetowego modelu warstwowego. Jakie są zadania każdej z nich?

Warstwy	Zadanie
7. aplikacji	Zajmuje się specyfikacją interfejsu, który wykorzystuje aplikacja do przesyłania danych w sieci. Odpowiada za protokoły użytkowników **(FTP, http, SMTP**).
6. prezentacji	**(tylko w modelu referencyjnym OSI)** Zadaniem jest przetworzenie danych od aplikacji do postaci kanonicznej zgodnej z reprezentacją OSI-RM. Odpowiada za kodowanie i konwersję danych oraz za kompresję/dekompresję; szyfrowanie/deszyfrowanie. Obsługuje np. MPEG, JPG, GIF.
5. sesji	**(tylko w modelu referencyjnym OSI)** Otrzymuje od różnych aplikacji dane, które muszą zostać odpowiednio zsynchronizowane. Synchronizacja zachodzi pomiędzy warstwami sesji systemu nadawcy i odbiorcy. Nadzoruje połączenie i wznawia je po przerwaniu.
4. transportowa	Segmentuje dane oraz składa je w tzw. strumień. Zapewnia całościowe połączenie między stacjami: źródłową oraz docelową, które obejmuje całą drogę transmisji. Następuje tutaj podział danych na części, które są kolejno numerowane i wysyłane do docelowej stacji. Wykorzystywane protokoły: **TCP i UDP.** Oba protokoły warstwy transportowej stosują kontrolę integralności pakietów, a pakiety zawierające błędy są odrzucane.
3. sieci	Routing. Jako jedyna dysponuje wiedzą dotyczącą topologii sieci. Jedyne zadanie – zapewnienie sprawnej łączności między bardzo odległymi punktami sieci. Protokoły warstwy sieci to: (**IPv4, IPv6, ICMP**, itp.).

2. łącza danych	Ma ona nadzorować jakość przekazywanych informacji (nadzór dotyczy wyłącznie warstwy niższej). Zajmuje się pakowaniem w ramki i wysyłaniem do warstwy fizycznej, tak aby obniżyć liczbę pojawiających się podczas przekazu błędów. Urządzenia działające w tej warstwie to: **most i przełącznik**.
1. fizyczna	Może wysyłać i odbierać pojedynczy bit (bez weryfikacji poprawności danych)

Czym różni się model odniesienia TCP/IP od OSI?

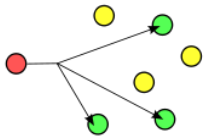
- TCP/IP łączy funkcje warstw prezentacji i sesji w warstwie aplikacji.
- TCP/IP łączy warstwy łącza danych i fizyczną modelu OSI w jednej warstwie (warstwa dostępu do sieci).
- TCP/IP wydaje się prostszy, ponieważ ma mniej warstw. Model odniesienia OSI jest mniej skomplikowany; ma więcej warstw, a to pozwala na szybszą współpracę i rozwiązywanie problemów.
- Protokół TCP/IP to standardy, na których oparty jest Internet, dlatego jest on bardziej wiarygodny. Sieci zazwyczaj nie są budowane w oparciu o protokoły modelu OSI, choć wykorzystuje się go jako przewodnika.

Wyjaśnij pojęcia: komunikacja simpleksowa, półdupleksowa, pełnodupleksowa.

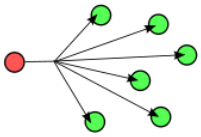
- **Simpleksowa**: nie jest możliwe przesyłanie informacji w dwóch kierunkach. Nadajnik i odbiornik nie mogą zamienić się funkcjami. Transmisja jest jednokierunkowa. Przełącznik jest mechaniczny (nie ma rozróżnienia częstotliwościowego), w stanie spoczynku nastawiony na odbiór blokuje nadawanie.
- **Półdupleksowa**: słabsza wersja komunikacji pełnodupleksowej, w której przesyłanie i odbieranie informacji odbywa się naprzemiennie, powodując spadek transferu.
- **Pełnodupleksowa**: informacje przesyłane są w obu kierunkach jednocześnie, bez spadku transferu

Czym różni się broadcast od multicastu?

- **Multicast** to sposób dystrybucji informacji, dla którego liczba odbiorców może być dowolna. Odbiorcy są widziani dla nadawcy jako pojedynczy grupowy odbiorca (*host group*) dostępny pod jednym adresem dla danej grupy multikastowej.



- **Broadcast** to rozsiewczy (rozgłoszeniowy) tryb transmisji danych polegający na wysyłaniu przez jeden port pakietów, które powinny być odebrane przez wszystkie pozostałe porty przyłączone do danej sieci (domeny broadcastowej).



Wyjaśnij pojęcie enkapsulacji.

Termin odnoszący się do struktury protokołu komunikacyjnego. Warstwa niższa opakowuje dane przekazane przez warstwę wyższą danego protokołu po stronie nadawczej we własne nagłówki i ew. stopki, które są wymagane do poprawnego przesyłania danych. Po stronie odbiorczej wykonywane jest działanie odwrotne prowadzące do wyodrębnienia danych z warstwy najwyższej przenoszącej dane użytkowe, zwanej warstwą aplikacji.

Co to jest interfejs sieciowy?

Najogólniej interfejsem sieciowym w systemach linux nazywamy urządzenia logiczne pozwalające na nawiązywanie połączeń różnego typu. Należy jednak pamiętać iż mówiąc interfejs sieciowy nie mamy zawsze na myśli **karty sieciowej**. Interfejsem sieciowym jest np. **pętla zwrotna** (lo). Mogą nim być też **tunele VPN** lub inne programy i urządzenia pozwalające na komunikację z lokalnym

lub zdalnym hostem. Czyli interfejs często jest reprezentacją sterownika karty sieciowej w systemie, ale może też być urządzeniem "wirtualnym" które realizuje programowo pewne zadania.

Po co w kablu UTP (skrętka nieekranowana) skręca się pary przewodów?

Poszczególne bity są przesyłane poprzez „puszczenie" przez kabel odpowiedniego napięcia. Skręcenie kabli pozwala zachować różnicę napięć między nimi (a to jest najistotniejsze), nawet gdy w pobliżu znajduję się silne źródło oddziaływujące na nasz kabel (np. magnes, lub inny kabel). Żyły skręca się w celu eliminacji wpływu **zakłóceń elektromagnetycznych** oraz zakłóceń wzajemnych, zwanych **przesłuchami**.

Dlaczego do przesyłania sygnału w skrętce wykorzystuje się parę przewodów a nie jeden?

Sumarycznie przesyłane jest zerowe napięcie, kabel generuje znikome pole elektromagnetyczne. Odbiornik mierzy tylko różnice między jednym a drugim, a zewnętrzne zakłócenie zazwyczaj zaburza jednakowo oba przewody różnica zostaje taka sama.

Kiedy stosujemy skrętkę zwykłą a kiedy z przeplotem?

Skrętka **zwykła** do połączenia: PC -> HUB,SWITCH
Skrętka **z przeplotem** do połączenia: PC -> PC, PC -> ROUTER.

Na czym polegają kodowania Manchester i 4B/5B?

- **Kodowanie Manchester** - kod liniowy sygnału cyfrowego. Na początku sygnał przyjmuje stan odpowiadający jego wartości binarnej, w środku czasu transmisji bitu następuje zmiana sygnału na przeciwny; dla zera z niskiego na wysoki, dla jedynki – z wysokiego na niski. Brak problemu długich ciągów zer i jedynek. Wadą jest **100% narzut**. Wykorzystywany głównie w **10 Mbitowych** wariantach.
- **Kodowanie 4B/5B** - dzieli przesyłane bity na porcje po 4 bity i koduje taką porcję deterministycznie na 5 bitach. Żaden z 5-bitowych kodów nie jest równy 00000 ani 11111, więc w wystarczający sposób eliminuje problem ze zliczaniem przez odbiornik długich ciągów zer/jedynek. **Narzut** wynosi **25%**. Wykorzystywany w **100 Mbitowych** wariantach.

WYKŁAD 2

Czym różni się koncentrator od przełącznika sieciowego?

Koncentrator nie może określić źródła ani miejsca docelowego odbieranych informacji, dlatego wysyła je do wszystkich połączonych z nim komputerów, w tym do komputera, z którego informację wysłano. Koncentrator może wysyłać i odbierać informacje, jednak nie jednocześnie. Z tego powodu koncentratory są wolniejsze od przełączników.
Przełącznik działają tak samo, jak koncentratory, jednak mogą identyfikować miejsce docelowe odbieranej informacji, dzięki czemu wysyłają ją tylko do komputerów, które daną informację mają odebrać. Przełączniki mogą jednocześnie wysyłać i odbierać informacje, dzięki czemu działają szybciej niż koncentratory.

Kiedy w sieci pojawiają się kolizje?

Kolizje powstają wtedy, kiedy dwa komputery usiłują wysłać pakiet przez łącze w tym samym czasie. Kolizja jest wykrywana automatycznie, komputery zaprzestają wtedy przesyłania. Po losowo wybranym czasie każdy z komputerów próbuje ponownie przesłać swój pakiet.

Co to jest czas propagacji?

Jest to maksymalny czas, który potrzebuje sygnał aby dotrzeć z jednego końca sieci na drugi.

Wyjaśnij skrót CSMA/CD.

Carrier Sense Multiple Access / with Collision Detection - protokół wielodostępu CSMA z badaniem stanu kanału i wykrywaniem kolizji.

Opisz budowę ramki ethernetowej. Po co jest preambuła ramki?

8	6	6	2	0–1500	0–46	4
Preambuła	Adres docelowy	Adres zrodlowy	Dług. / typ	Dane	Wypełnienie	Suma kontrolna

Preambuła zawiera bity synchronizacji przetwarzane przez kartę sieciową. Jest to naprzemienny ciąg bitów 1 i 0, informujący o nadchodzącej ramce. Najczęściej nie jest on włączany do wielkości ramki (nie widać go także w oknie WireSharka). Uznawany jest za część procesu komunikacji. Sekwencja wygląda następująco: 1010…10, co w zapisie szesnastkowym daje AAA…A. (7 bajtów)

SFD lub SOF - (Start of Frame Delimiter) - bajt kończący preambułę jest sekwencją 8 bitów o postaci: 10101011, zawsze jest zakończony dwoma bitami 1. W standardzie Ethernet bajt ten nie występuje, zastąpiony jest kolejnym bajtem preambuły (ostatni bit równy 0).

Co to jest adres MAC?

6-bajtowy (48-bitowy) ciąg zapisywany heksadecymalnie (np. **00:0A:E6:3E:FD:E1**) przypisany (teoretycznie) na stałe do karty sieciowej, który (teoretycznie) jednoznacznie ją określa. Pierwsze 24 bity oznaczają producenta karty, pozostałe 24 bity są unikatowym identyfikatorem danego egzemplarza karty. Adres **FF:FF:FF:FF:FF:FF** to adres broadcast.

Do czego służy tryb nasłuchu (*promiscuous mode*)?

Tryb pracy interfejsu sieciowego polegający na odbieraniu całego ruchu docierającego do karty sieciowej, nie tylko skierowanego na adres MAC karty sieciowej. Aby przestawić kartę sieciową w tryb promiscuous w systemie Linux należy wydać w terminalu polecenie: **ifconfig <karta_sieciowa> promisc**. Z trybu tego korzystają między innymi programy monitorujące ruch w sieci, tzw. sniffery.

Co to jest domena kolizyjna i domena broadcast?

- **Domena kolizyjna** - segment sieci, w którym transmisja musi być realizowana przez urządzenie w sposób wykluczający prowadzenie w tym czasie transmisji przez inne urządzenia (granicę stanowią porty urządzeń, most, przełącznik lub router). Wszystkie urządzenia podłączone do huba ethernetowego (lub hubów) tworzą jedną domenę kolizyjną, czyli rywalizują o dostęp do medium i współdzielą pasmo przepustowości. Przełączniki oddzielają domeny kolizyjne, koncentratory nie.
- **Domena broadcast (rozgłoszeniowa)** - jest segmentem sieci jaki pokonują pakiety typu broadcast (granicę stanowią routery i inne urządzenia pracujące w warstwie trzeciej).

Dlaczego w Ethernecie definiuje się minimalną długość ramki?

Minimalna długość ramki jest określona, aby w szybki sposób odróżniać „śmieci” od rzeczywistych informacji. Wysyłanie powinno trać co najmniej 2*α, gdzie α to czas propagacji sygnału. Daje to gwarancję, że nadawca dowie się o niepowodzeniu wysyłania (jeżeli takie nastąpi).

Jak działa algorytm obliczania sum kontrolnych CRC?

http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_13s/n2.pdf

WYKŁAD 3

Opisz sieci IP klasy A, B i C.

Klasa A: adresy przeznaczone do obsługi bardzo dużych sieci. Minimalne zapotrzebowanie na takie sieci, a więc architektura mocno ograniczała liczbę dopuszczalnych sieci klasy A, jednocześnie maksymalizując liczbę dopuszczalnych w nich stacji. Pierwszy bit zawsze równy **0**. Pierwszy bajt oznacza adres sieci, pozostałe trzy – adres stacji. Pierwszy bit równy 0 (dziesiętnie oznaczający 128) ogranicza największą liczbę sieci klasy A do 127. **Zakres adresów:** 1.0.0.0 – 126.255.255.255. 127.0.0.0 jest **zarezerwowany** do testowania stacji i **nie można** go przypisać żadnej sieci! Każda sieć klasy A może obsługiwać 16 777 214 stacji , 0.0.0.0 – identyfikacja sieci, 1.1.1.1 – broadcast.

Klasa B: adresy przeznaczone do obsługi sieci średnich i dużych. Pierwsze dwa bajty oznaczają numer sieci, a kolejne dwa numer stacji. Pierwsze dwa bity są równe **10**. Pierwszy bajt mieści się więc w zakresie 128 – 191. **Zakres adresów:** 128.1.0.0 do 191.255.255.255. Może obsłużyć co najwyżej 16 382 sieci) oraz 65 534 stacje $2^{16} - 2$).

Klasa C: adresy przeznaczone do obsługi dużej ilości małych sieci. Pierwsze trzy bajty określają sieć, pozostały jeden bajt - numer stacji. Pierwsze trzy bity równe są **110**. Zakres pierwszego bajtu: 192 – 223. **Zakres adresów:** 192.0.0.0 do 223.255.255.255. Może obsłużyć 2 097 150 sieci oraz 254 stacje.

Co to jest pętla lokalna (*loopback*)?

Sieć **127.0.0.0/8**. Interfejs `lo`. Łącząc się z dowolnym komputerem z tej sieci (zazwyczaj 127.0.0.1) łączymy się z samym sobą. Dzięki temu możemy pisać i testować aplikacje sieciowe nie posiadając połączenia z siecią.

Podaj jeden z zakresów adresów przeznaczonych do wykorzystania jako prywatne adresy IP.

10.0.0.0/8 (jedna siec klasy A), **172.16.0.0/12** (16 sieci klasy B), **192.168.0.0/16** (256 sieci klasy C)

Żeby takie adresy IP mogły się komunikować z Internetem (a właściwie, żeby Internet mógł komunikować się z nimi!), router łączący taką siec ze światem zewnętrznym musi specjalnie modyfikować przechodzące przez niego pakiety (NAT).

Jak działa polecenie ping? Jaki typ komunikatów ICMP wykorzystuje?

Polecenie ping pozwala na sprawdzenie czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji, zwanych lagami. Ping korzysta z protokołu ICMP, wysyła pakiety ***ICMP Echo Request*** i odbiera ***ICMP Echo Reply***.

Jak działa polecenie traceroute?

Działanie traceroute opiera się o protokoły komunikacyjne UDP oraz ICMP (na wykładzie podane, że ICMP). Wysyłane są pakiety z rosnącymi wartościami **pola TTL (Time to Live)**, na początku o wartości 1. Każdy router na trasie zmniejsza wartość o 1. Kiedy wartość spadnie do 0, router odrzuca pakiet i wysyła w odpowiedzi pakiet „Time Exceeded". Jeżeli pakiet dotrze w końcu do hosta docelowego, to najprawdopodobniej zostanie odesłany komunikat **ICMP "Port Unreachable"**. Dzieje się tak dlatego, że uniksowe implementacje programu **traceroute** świadomie wysyłają pakiety UDP z numerem portu powyżej 30000. Zazwyczaj na porcie o tak wysokim numerze nie działają żadne usługi, więc żaden proces w komputerze docelowym nie będzie chciał obsłużyć nadchodzącego pakietu. W tej sytuacji badanie trasy zostaje zakończone. Brak odpowiedzi na zadany pakiet sygnalizowany jest znakiem gwiazdki "*" i może wynikać z przeciążenia sieci, routera bądź z celowej konfiguracji urządzeń (ustawienia firewalla). Podobne narzędzia jak mtr oraz w systemach z rodziny Microsoft Windows program tracert są zaimplementowane nieco inaczej. Różnica polega na tym, że wysyłane pakiety to nie datagramy UDP, lecz komunikaty ICMP typu **"Echo Request"**. Jeżeli taki komunikat osiągnie swoje przeznaczenie, to zawsze zostanie odesłana odpowiedź **"Echo Reply"**. Dzięki temu nie trzeba polegać na założeniu związanym z wysokimi numerami portów dla datagramów UDP oraz można ominąć niektóre firewalle.

Do czego służą protokoły ARP i RARP?

ARP - Address Resolution Protocol (IP -> MAC). Służy on do identyfikacji adresu fizycznego (MAC) komputera na podstawie jego adresu IP. W tym celu wysyłane jest zapytanie *ARP Request* o treści: „kto ma dany adres IP?". Na zapytanie odpowiada tylko jeden komputer: „ja mam". Adres fizyczny zapisywany jest w tablicy ARP i parowany z adresem logicznym hosta docelowego, dzięki czemu nie będzie wymagane ponowne zapytanie o adres do momentu wyczyszczenia tablicy.

RARP - *Reverse Address Resolution Protocol* (MAC -> IP). Służy do ustalenia adresu IP na podstawie adresu MAC. Wysłane zostaje zapytanie: *„Jaki jest adres IP dla danego adresu MAC **aa:bb:cc:dd:ee:ff** ?"*. W odpowiedzi otrzymuje: *„Komputer mający adres MAC **aa:bb:cc:dd:ee:ff** ma adres IP **1.2.3.4***.

Na czym polega automatyczna konfiguracja interfejsu sieciowego? (chodzi m.in. o protokół APIPA)

Protokół, dzięki któremu klient DHCP może dokonać samokonfiguracji, jeżeli w sieci nie znajdzie serwera DHCP, z którego mógłby pobrać adres IP i inne parametry sieci. Usługa APIPA przydziela systemowi adres IP w przypadku, gdy komputer wyposażony jest w kartę sieciową, zostało zainstalowane oprogramowanie obsługi protokołów TCP/IP, karta sieciowa skonfigurowana jest do żądania przyznania adresu IP z serwera DHCP (ustawienie domyślne w Windows XP), a serwer DHCP w danym momencie jest nieosiągalny. Adres IP przydzielany jest z puli 169.254.0.1 - 169.254.255.254 z domyślną maską 255.255.0.0.

Co to jest MTU? Na czym polega technika wykrywania wartości MTU dla ścieżki?

MTU = Maximum Transmission Unit – jest to własność drugiej warstwy (maksymalna wielkość danych z warstwy trzeciej – **czyli maksymalny rozmiar pakietu**). Dla Ethernetu MTU wynosi **1500**, dla sieci bezprzewodowych **2312**. Technika wykrywania wartości MTU dla ścieżki polega na próbie wysłania pakietu z ustawionym bitem DT (don't fragment). Jeśli konieczna będzie fragmentacja, pakiet zostanie wyrzucony, a router odsyła z powrotem komunikat ICMP (destination unreachable, can't fragment). Znaczy że rozmiar pakietu jest zbyt duży i trzeba go zmniejszyć (informacja o prawidłowym rozmiarze pakietu zostanie przesłana przez router)

Czym różni się łączenie dwóch sieci za pomocą mostu od łączenia ich za pomocą routera?

Routery przesyłają informacje obwodami międzysieciowymi znacznie szybciej (routery usuwają zewnętrzne warstwy danych, zanim wyślą pakiet z jednej sieci lokalnej do drugiej) i skuteczniej niż mosty. Jeżeli dwie sieci używają tych samych segmentów sieci i protokołów kontroli dostępu np. Etherneth to można połączyć mostami każdą z nich. Jeśli jednak sieci są różne powiedzmy jedna wykonuje Etherneth, a druga token ring - najlepszym rozwiązaniem będą routery, ponieważ usuną one pakiety sformułowane dla IPX lub IP z ramki niższego poziomu.

WYKŁAD 4 i 5

Jak nazywają się jednostki danych przesyłane w kolejnych warstwach?

- Warstwa 1 (fizyczna): **strumień bitów**
- Warstwa 2 (łącza danych): **ramki**
- Warstwa 3 (sieci): **pakiety**
- Warstwa 4 (transportowa): **TPDU** (Transport Protocol Data Unit) – jednostka transportowa. **Segmenty** (TCP), **datagramy** (UDP)

Po co w warstwie 4 wprowadza się porty?

Porty wprowadza się, aby umożliwić rozróżnienie między jednoczesnymi transmisjami odbywającymi się między parą komputerów (komputer może nawiązać więcej niż jedno połączenie).

Co to jest gniazdo?

Reprezentuje dwukierunkowy punkt końcowy połączenia. Dwukierunkowość oznacza możliwość wysyłania i przyjmowania danych. Gniazdo posiada trzy główne właściwości: typ gniazda identyfikujący protokół wymiany danych, lokalny adres (np. adres IP), opcjonalny lokalny numer portu identyfikujący proces, który wymienia dane przez to gniazdo. Na czas trwania komunikacji może posiadać dodatkowe dwa atrybuty: adres zdalny (ponownie np. adres IP), opcjonalny numer portu identyfikujący zdalny proces (jeśli typ gniazda pozwala używać portów).

Adres IP wyznacza węzeł w sieci, numer portu określa proces w węźle, a typ gniazda determinuje sposób wymiany danych.

Czym różni się gniazdo nasłuchujące od gniazda połączonego? Czy w protokole UDP mamy gniazda połączone?

- Gniazdo nasłuchujące nie jest końcówką żadnego połączenia. Nie można przez nie przesyłać danych. Służą one do przyjmowania żądań połączenia, dlatego gniazdko takie nazywa się pasywnym (biernym) - nie robi ono nic, poza oczekiwaniem, aby zestawić połączenie.
- Gniazdo połączone - w momencie gdy przychodzi żądanie połączenia, na gnieździe nasłuchującym przeprowadzana jest operacja, która tworzy NOWE gniazdo połączone (może ono wysyłać i odbierać komunikaty), reprezentujące połączenie z klientem. Warto zauważyć, że gniazdo nasłuchujące nadal istnieje i oczekuje na połączenia.
- W protokole UDP istnieją gniazda połączone.

Czym różnią się protokoły UDP i TCP? Podaj zastosowania każdego z nich.

- TCP: połączeniowy, złożony, potwierdzenia, kontrola przepływu
- Gwarantuje, że wszystkie pakiety dotrą w odpowiedniej kolejności

Protokół TCP umożliwia kontrolę przeciążeń urządzeń znajdujących się pomiędzy komunikującymi się hostami. W przypadku, gdy następuje przeciążenie protokół TCP zmniejsza prędkość nadawania segmentów przez urządzenie nadawcze. Segmenty protokołu TCP są enkapsulowane w pakiety IP i przesyłane przy użyciu tego protokołu. Ze względu na właściwości IP polegające na przesyłaniu w sposób skuteczny pakietów wszelkimi możliwymi drogami, segmenty mogą dotrzeć do adresata w różnej kolejności. Mechanizm porządkowania segmentów umożliwia nadawanie im numerów sekwencyjnych, które następnie ułatwiają ponowne złożenie danych.
WYKORZYSTANIE: Aplikacje, w których zalety TCP przeważają nad wadami (większy koszt związany z utrzymaniem sesji TCP przez stos sieciowy), to m.in. programy używające protokołów warstwy aplikacji: HTTP, SSH, FTP czy SMTP/POP3 i IMAP4.

- UDP: bezpołączeniowy, prosty, zawodny

- Bez potwierdzeń
- Datagramy mogą się zgubić
- Datagramy mogą przyjść w innej kolejności
- DaTagramy mogą zostać zduplikowane
- Brak kontroli przepływu (szybki nadawca może zalać odbiorcę: po przepełnieniu buforu odbiorcy, datagramy są tracone) -> zalewający klient UDP

Protokół UDP został zaprojektowany w celu dostarczania użytkownikowi mechanizmów do przesyłania datagramów pomiędzy programami użytkowymi. Podobnie jak protokół niższej warstwy (IP) nie nawiązuje on połączenia w trakcie wysyłania danych. Host wysyłający segment UDP nie uzyskuje informacji zwrotnej o tym, czy dane dotarły do adresata. W samym protokole UDP nie ma również mechanizmów pozwalających na kontrolę przepływu. W związku z tym w przypadku, gdy host do którego mają dotrzeć segmenty nie jest w stanie ich obsłużyć, nie ma możliwości przesłać stosownej informacji. Mechanizm taki został zaimplementowany w protokole TCP. Do aplikacji wykorzystujących protokół UDP należą aplikacje komunikacji multimedialnej. Wszelkie programy wykorzystujące wideokonferencje, przesyłanie strumieniowe dźwięku wykorzystują szybkość tego protokołu.
WYKORZYSTANIE: UDP jest często używany w takich zastosowaniach jak wideokonferencje, strumienie dźwięku w Internecie i gry sieciowe, gdzie dane muszą być przesyłane możliwie szybko, a poprawianiem błędów zajmują się inne warstwy modelu OSI.

Do czego wykorzystywane są gniazda surowe?

Gniazda surowe posiadają pewne właściwości, których brakuje gniazdom TCP i UDP:

- Gniazda surowe pozwalają na wysyłanie i odbiór pakietów ICMP i IGMP.
- Za pomocą surowych gniazd można przetwarzać datagramy IP, których wartość pola oznaczającego typ protokołu jest nie obsługiwana przez jądro. Pozwala to na realizację obsługi własnego protokołu sieciowego na poziomie użytkownika.
- Przy pomocy gniazd surowych można utworzyć własny nagłówek IPv4, co pozwala na wysyłanie ręcznie spreparowanych pakietów TCP i UDP.

Co robią funkcję jądra bind(), listen(), accept(), connect()?

- **Bind():** służy do przypisania adresu (adresu węzła i numeru portu) do podanego gniazda. Funkcja ta musi być wywołana przez serwer zarówno w trybie połączeniowym jak i bezpołączeniowym. Może ją także wywołać klient jeśli chce używać do komunikacji konkretnego portu, a nie portu przydzielonego automatycznie przez system.

- **Listen():**sygnalizuje gotowość do przyjmowania żądań nawiązania połączenia, wysyłanych przez klientów.

- **Accept():** wywoływana w celu przyjęcia żądania nawiązania połączenia, zgłoszonego wcześniej (po wywołaniu funkcji listen()) i oczekującego w kolejce. Jeżeli żadne żądanie nie dotarło, serwer jest blokowany do momentu otrzymania żądania. Po przyjęciu żądania funkcja tworzy nowy deskryptor dla danego gniazda, który może być następnie wykorzystywany przez proces obsługi zgłoszenia.

- **Connect():** wywołana dla gniazda obsługiwanego przez połączeniowy protokół transportowy, podejmuje automatycznie próbę nawiązania połączenia, zgodnie z dowiązanym adresem. Może być ona jednak użyta również w trybie bezpołączeniowym. Wówczas, gdy dzięki wywołaniu connect() zostanie dowiązana struktura adresowa do

gniazda, przy wysyłaniu datagramu nie jest potrzebne podawanie adresu i można używać funkcji write() lub send() zamiast sendto().

Czym różni się otwarcie bierne od otwarcia aktywnego? Czy serwer może wykonać otwarcie aktywne?

- **Otwarcie bierne**:
  - serwer wykonuje otwarcie bierne tworząc gniazdo nasłuchujące
- **Otwarcie aktywne:**
  - klient wykonuje otwarcie aktywne wysyłając segment SYN zawierający numer początkowy
  - serwer potwierdza przyjęcie segmentu SYN i wysyła własny segment SYN zawierający początkowy numer danych, które będzie wysyłał przez to połączenie, wraz z segmentem ACK - segment SYN/ACK
  - klient sygnalizuje odebranie odpowiedzi wysyłając segment ACK

Do czego służą numery sekwencyjne w protokole TCP?

Numery sekwencyjne służą do numerowania kolejnych pakietów wysyłanych z danym połączeniu, co pozwala na zidentyfikowanie i odrzucenie zagubionych pakietów, które przyszły po czasie lub pakietów zduplikowanych. Zwiększają one także bezpieczeństwo.

Opisz trójstopniowe nawiązywanie połączenia w TCP. Jakie segmenty są przesyłane w trakcie takiego połączenia?

K1: strona wykonująca chcąca nawiązać połączenie wysyła segment SYN
K2: druga strona odsyła pakiet z ustawionymi flagami SYN oraz ACK
K3: strona inicjująca połączenie wysyła pakiet z ustawioną flagą ACK

Kto może wykonać zamknięcie aktywne połączenia? Jakie segmenty są wymieniane podczas modelowego zamykania połączenia w protokole TCP?

K1: dowolna ze stron wykonuje zamknięcie aktywne wysyłając segment FIN
K2: druga ze stron potwierdza odebranie tego komunikatu wysyłając segment ACK (zamknięcie bierne)
teraz mogą przepływać komunikaty od strony wykonującej zamknięcie bierne do strony wykonującej zamknięcie aktywne
K3: strona wykonująca zamknięcie bierne wysyła segment FIN
K4: druga strona wysyła segment ACK

Co zwraca funkcja read()/recv() wywołana na gnieździe połączonym w normalnym (blokującym) trybie? Kiedy zwraca 0 a kiedy blokuje?

`recv(_,_,_,0) = read(_,_,_). Przy UDP bylo recvfrom, przy TCP jest recv()`
`send(_,_,_,0) = write(_,_,_). Przy UDP bylo sendto, przy TCP jest send()`
Recv() – zwraca ilość otrzymanych bajtów (może być mniej, niż podane w argumencie *len* wywołania), -1 w przypadku błędu, 0 gdy połączenie po drugiej stronie zostało zamknięte.

Do czego służą flagi SYN, ACK, FIN i RST stosowane w protokole TCP?

- SYN - używana przy nawiązywaniu połączenia, ustala początkowy numer sekwencyjny (synchronizuje kolejne numery sekwencyjne)
- ACK - flaga mająca na celu potwierdzić odebranie odpowiednich danych (np. pakietu z flagą SYN lub FIN)
- FIN - flaga używana przy kończeniu połączenia
- RST - oznacza wystąpienie błędu, kończy połączenie. Wysyłana np. przy próbie połączenia z portem na którym nikt nie nasłuchuje (resetuje połączenie, wymagane ponowne uzgodnienie sekwencji)

Czy do stanu TIME_WAIT przechodzi strona, która wykonuje zamknięcie aktywne czy bierne? Dlaczego? Po co wprowadzono taki stan?

Strona wykonująca zamknięcie aktywne przechodzi do stanu TIME_WAIT, zaraz po otrzymaniu pakietu z ustaloną flagą FIN (na który to pakiet odpowiada pakietem z flagą ACK, lecz nie wie, czy pakiet ten dotarł do odbiorcy – stan TIME_WAIT). Stan ten utrzymuje się przez ok. 1-4min (2 x max. Czas życia segmentu).
Stan ten pozwala na dwukierunkowe zakończenie połączenia TCP w przypadku zagubienia ostatniego ACK (ponowne wysłanie pakietu z flagą FIN) oraz usunięcie starych duplikatów segmentów z sieci.

WYKŁAD 6

Po co istnieje system nazw DNS?

System nazw DNS istnieje aby ułatwić zapamiętywanie poszczególnych adresów. Ludziom łatwiej jest zapamiętać adres strony pl.wikipedia.org, niż jej adres IP: 145.97.39.135.

Rozwiń skrót TLD (kontekst: DNS), podaj parę przykładów.

TLD (Top Level Domain) - domena internetowa powyżej której nie istnieją żadne inne domeny w systemie DNS. Są one tworzone i zarządzane przez IANA i ICANN.

Każda domena w Internecie składa się z pewnej liczby nazw, oddzielonych kropkami. Ostatnia z tych nazw jest domeną najwyższego poziomu. Na przykład w "pl.wikipedia.org" domeną najwyższego poziomu jest "org".

Czym są strefy i delegacje DNS?

Strefa jest najmniejszą jednostką administracyjną DNS. Strefa to nazwa nadana hostom wewnątrz danej domeny z pominięciem wszystkich domen podrzędnych (np. w strefie uni.lodz.pl znajduje się host www.uni.lodz.pl, ale nie ftp.math.uni.lodz.pl). Za daną strefę odpowiada co najmniej jeden serwer nazw (w przypadku „.” Istnieje 13 serwerów głównych). Serwerami dla „pl” rządzi NASK.

Jest to spójny fragment poddrzewa, identyfikowany przez swój korzeń. Serwer nazw odpowiadający za daną strefę zna zawartość strefy oraz serwery nazw odpowiedzialne za strefy podrzędne (dzięki delegacjom).

Delegacje to krawędzie między poszczególnymi strefami.

Czym różni się rekurencyjne odpytywanie serwerów DNS od iteracyjnego?

Iteracyjne: klient przechodzi drzewo DNS zaczynając od korzenia.

Rekurencyjne: klient odpytuje serwer DNS, a on w naszym imieniu wykonuje odpytywanie.

- Windowsowy klient DNS i część systemów uniksowych wymaga takiego serwera
- Dla poprawy wydajności, serwer zapisuje sobie zwracane wyniki w pamięci podręcznej (odpowiedzi wyświetlane z pamięci podręcznej wyświetlane są jako non-authoritiative)

Jak działa odwrotny DNS? Jaką domenę wykorzystuje?

Polega na konwersji odwrotnej: adres IP -> nazwa domeny. Zamiast tworzyć kolejny protokół do tego celu, wykorzystuje się możliwości DNS, rekord PTR. Wykorzystuje on domenę `in-addr.arpa`, której poddomenami są klasy lub adresy IP. Przykładowo `222.111.in-addr.arpa` opisuje adresy sieci `111.222.0.0/16`.

Jakie znasz typy rekordów DNS? Co to jest rekord CNAME?

- **rekord A** lub **rekord adresu (ang. address record)** mapuje nazwę domeny DNS na jej 32-bitowy adres IPv4.

- **rekord AAAA** lub **rekord adresu IPv6 (ang. IPv6 address record)** mapuje nazwę domeny DNS na jej 128-bitowy adres IPv6.
- **rekord CNAME** lub **rekord nazwy kanonicznej (ang. canonical name record)** ustanawia alias nazwy domeny. Wszystkie wpisy DNS oraz poddomeny są poprawne także dla aliasu.
- **rekord MX** lub **rekord wymiany poczty (ang. mail exchange record)** mapuje nazwę domeny DNS na nazwę serwera poczty oraz jego priorytet.
- **rekord PTR** lub **rekord wskaźnika (ang. pointer record)** mapuje adres IPv4 lub IPv6 na nazwę kanoniczną hosta.
- **rekord NS** lub **rekord serwera nazw (ang. name server record)** mapuje nazwę domenową na listę serwerów DNS dla tej domeny.
- **rekord SOA** lub **rekord adresu startowego uwierzytelnienia (ang. start of authority record)** ustala serwer DNS dostarczający *autorytatywne* informacje o domenie internetowej, łącznie z jej parametrami (np. TTL).
- **rekord SRV** lub **rekord usługi (ang. service record)** pozwala na zawarcie dodatkowych informacji dotyczących lokalizacji danej usługi, którą udostępnia serwer wskazywany przez adres DNS.
- **TXT** – rekord ten pozwala dołączyć dowolny tekst do rekordu DNS. Rekord ten może być użyty np. do implementacji specyfikacji Sender Policy Framework.
-

Po co są rekordy sklejające (glue records)?

Serwery najwyższego poziomu z reguły posiadają tylko odwołania do odpowiednich serwerów DNS odpowiedzialnych za domeny niższego rzędu, np. serwery główne (obsługujące między innymi TLD .com) wiedzą, które serwery DNS odpowiedzialne są za domenę example.com. Serwery DNS zwracają nazwę serwerów odpowiedzialnych za domeny niższego rzędu. Możliwa jest sytuacja, że serwer główny odpowiada, że dane o domenie example.com posiada serwer dns.example.com. W celu uniknięcia zapętlenia w takiej sytuacji serwer główny do odpowiedzi dołącza specjalny rekord (tak zwany *glue record*) zawierający także adres IP serwera niższego rzędu (w tym przypadku dns.example.com).

Do czego służy plik /etc/hosts?

Plik hosts (/etc/hosts – ścieżka do pliku w systemach UNIXowych) jest jednym z modułów wielu systemów operacyjnych, który wspomaga adresowanie w sieciach komputerowych. Jego zadaniem jest tłumaczenie przyjaznych użytkownikom nazw domenowych (kanonicznych) na ich numeryczne odpowiedniki (adresy IP).

Jakie są wady i zalety częstotliwości 2,4 Ghz i 5 Ghz?

- 5Ghz:
  - wyższa częstotliwość - więcej bitów można przesłać ,
  - mało zatłoczone pasmo,
  - mały faktyczny zasięg: ok. 20 m,
  - fale bardzo pochłaniane przez ściany,
- 2.4Ghz
  - w tym paśmie działają również : Bluetooth, kuchenki mikrofalowe,
  - bezprzewodowe telefony, niektóre piloty do garażów, ...

- zasięg: ok. 50 m, lepsza penetracja ścian.

Przyporządkuj nazwy Bluetooth, Ethernet, WLAN do numerów standardów 802.3, 802.11, 802.15.

- 802.3 – Ethernet
- 802.11 – WLAN
- 802.15 - Bluetooth

Co to są interferencje? Jakie znasz inne problemy z warstwą fizyczną w sieciach bezprzewodowych?

- **interferencje** - wzajemne zakłócenia urządzeń pracujących z takimi samymi częstotliwościami (inne karty sieciowe, kuchenki mikrofalowe, ...)
- malejąca siła sygnału - sygnał rozpraszany, słabnie przy przechodzeniu przez ściany
- propagacja wielościeżkowa - ten sam sygnał wędruje do celu ścieżkami różnej długości
- półduplex - nie można jednocześnie nadawać i słuchać (tak jak w Ethernecie), nie wiemy czy wystąpiła kolizja (CSMA/CD bezużyteczne).

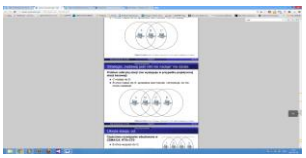
Dlaczego w sieciach bezprzewodowych nie stosuje się algorytmu CSMA/CD?

W sieciach bezprzewodowych nie ma możliwości wykrycia kolizji (jak to ma miejsce w Ethernecie).

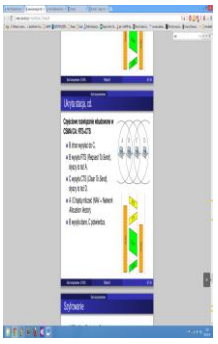
Wyjaśnij zjawisko ukrytej i odkrytej stacji.

Ukryta stacja – C nadaje do B; A chce nadać do B, sprawdza stan kanału i nic nie słyszy

Odkryta stacja (nie występuje w przypadku pojedynczej stacji bazowej) – C nadaje do D; B chce nadać do A, sprawdza stan kanału, wnioskuje, że nie może nadawać



Na czym polega rezerwowanie łącza za pomocą RTS i CTS? Jak pomaga rozwiązać problem ukrytej stacji?



- B chce wysłać do C
- B wysyła RTS (Request to send), słyszy to też A
- C wysyła CTS (Clear to send), słyszy to też D
- A i D będą milczeć (NAV - Network Allocation Vector)
- B wysyła dane, C potwierdza

Rozwiń skróty BSS i EBSS.

BSS – (Basic Service Set) to w sieciach bezprzewodowych standardu IEEE 802.11 grupa urządzeń bezprzewodowych logicznie ze sobą powiązanych. Zasięg ograniczony przez zasięg anteny punktu dostępowego.

EBSS – (Extended Basic Service Set) to wiele połączonych (zazwyczaj siecią kablową) punktów dostępowych.

Jakie znasz standardy szyfrowania w sieciach bezprzewodowych?

- WEP (Wired Equivalent Privacy) – słabe, obecnie do złamania w ciągu kilku minut (lub pasywna ataki działające w ciągu kilku godzin)
- WPA
- WPA2 (802.11i)

Na czym polega przeskakiwanie kanałów w sieci Bluetooth?

W czasie każdej sekundy wszystkie urządzenia Bluetooth w pikosieci 1600 razy zmieniają równocześnie używany kanał (tzw. przeskakiwanie częstotliwości). Sekwencja przeskakiwania jest obliczana niezależnie przez każde urządzenie w pikosieci, ale jako podstawa obliczeń wykorzystywany jest unikalny identyfikator mastera, dzięki czemu sieć pozostaje zsynchronizowana. Powoduje to unikanie interferencji z innymi sieciami Bluetooth, a także brak współpracy z WLAN (Bluetooth wygrywa).

Co to jest piconet?

Sieć utworzona na potrzeby standardu komunikacji Bluetooth, składająca się maksymalnie z ośmiu urządzeń (jedno urządzenie w trybie `master` i 7 w trybie `slave`).

WYKŁAD 7

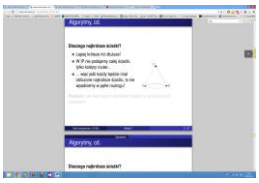
Co to jest RIB i FIB?

RIB (Routing Information Base) – informacje dotyczące routingu, trasy wpisane statycznie + „nauczone” od innych komputerów. Jest niezoptymalizowana, zawiera dodatkowe informacje, np. nieużywane ścieżki routingu, niezagregowane trasy. W Linkusie zaimplementowana w przestrzeni użytkownika .

FIB (Forwarding Information Base) - „skompilowana” tablica routingu używana do podejmowania decyzji o pakietach na podstawie najdłuższego pasującego prefiksu; zazwyczaj drzewa Patricia + optymalizacje + caching; zaimplementowana w jądrze (w urządzeniach czasem implementowana sprzętowo).

Dlaczego w algorytmach routingu dynamicznego obliczamy najkrótsze ścieżki?

- Lepsze krótsze niż dłuższe!
- W IP nie podajemy całej ścieżki, tylko kolejny router, więc jeśli każdy router będzie miał obliczone najkrótsze ścieżki, to nie wpadniemy w pętle routingu.



Czym różnią się algorytmy wektora odległości od algorytmów stanów łącz?

Algorytm wektora odległości to rozproszona implementacja algorytmu Bellmana-Forda. Jest prosta w implementacji, ale ma problemy z poprawnością. Komputery przesyłają całą tablicę routingu ale tylko do sąsiadów.

Algorytm stanów łącz to zalewanie + lokalny Dijkstra. Jest trudniejszy w implementacji, za to matematycznie prosty. Komputery przesyłają informacje o stanie swoich łącz do sąsiadów wszystkim wierzchołkom w sieci

Co to znaczy, że stan tablic routingu jest stabilny?

Stan tablic routingu określamy jako stabilny wtedy gdy wysyłanie tablic między komputerami nie wpływa na ich stan, tj. każdy ma już wszystkie interesujące go informacje.

Po co w algorytmach wektora odległości definiuje się największą odległość (16 w protokole RIP)?

Podczas usunięcia routera z sieci może powstać pętla. B przekuazyje swoją tablicę do C, następnie C przekazuje swoją tablicę do D, itd. Routery zwiększać będą znaną odległość do D średnio o 1 na turę -> problem zliczania do nieskończoności.

Jeśli odległość (w tym wypadku 16) przekroczy maksymalną wartość to uznajemy że straciliśmy połączenie do danego komputera. Problemem jest wolna zbieżność do stanu stablinego, ponieważ potrzeba około 16 tur, aby przekonać się, że router D jest nieosiągalny. Kolejnym minusem jest to, że maksymalna długość ścieżki może wynosić 15.

Na czym polega technika dzielenia horyzontu (split horizon) i dzielenia horyzontu z zatruwaniem ścieżki (split horizon with poison reverse)?

Dzielenie horyzontu – nie wysyłamy informacji o odległości do X do routera, który jest wpisany jako następny router na ścieżce do X.
Dzielenie horyzontu z zatruwaniem ścieżki – zamiast niewysyłania, wysyłamy „zatrutą ścieżkę”,tj. informację o tym, że do X mamy odległość nieskończoną.

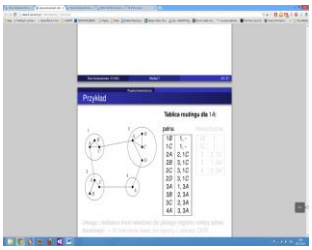
Po co stosuje się przyspieszone uaktualnienia (triggered updates)?

Komputer wysyła informacje o zepsuciu routera szybciej niż w swojej kolejce, dzięki czemu trudniej o uzyskanie sytuacji, w której dochodzi do tzw. „zliczania do nieskończoności". Stosowane w protokole RIP.

Rozwiń skrót LSA. Co oznacza?

LSA (Link State Advertisement) – stan pojedynczego łącza. Komunikat wykorzystywany w algorytmie stanu łączy, służy do propagowania informacji: na początku + przy zmianie + co jakiś czas (np. co 30 min) każdy komputer wysyła to, co się zmieniło (czyli komunikat LSA). Czas życia takiego komunikatu to około 1h, potem wyrzucane są z pamięci.

Na czym polega routing hierarchiczny? Po co się go stosuje?



Dzielimy routery na regiony (**systemy autonomiczne – AS**). Każdy router wie, co się dzieje w jego regionie i wie jak wysłać pakiet do innego regionu (ale nie wie jak wysłać pakiet do **konkretnego** komputera w regionie). Stosuje się go, ponieważ w internecie (składającym się z kilku milionów routerów) żadne z podejść (algorytm stanu łącz, algorytm wektora odległości) nie ma szans działać poprawnie.

Uwaga: nadawca musi wiedzieć do jakiego regionu należy adres docelowy! W Internecie łatwo, bo regiony = zakresy CIDR.

Co to jest default-free zone?

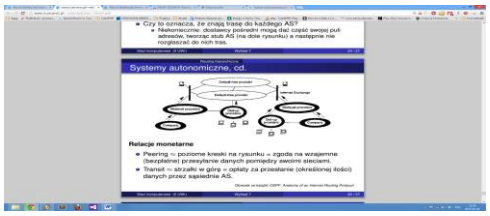
Default-free zones (DFZ) - routery z tych AS nie potrzebują wpisu bramy domyślnej, żeby wysłać pakiet w dowolne miejsce -> „Centrum Internetu".

Co to jest system autonomiczny? Jakie znasz typy AS? Co to jest peering?

System autonomiczny (*Autonomous System*, AS) to zbiór prefiksów (adresów sieci IP) pod wspólną administracyjną kontrolą, w którym utrzymywany jest spójny schemat trasowania (ang. *routing policy*). Każdy AS to określona klasa adresów IP – `whois`. AS to:

- Spójne zarządzanie,
- Spójna polityka wewnętrznego routing, zazwyczaj OSPF,
- Dla większych AS, OSPF umożliwia tworzenie dodatkowego poziomu hierarchii (AS dzielony jest na obszary)

Typy AS:



- Stub (tylko jedno połączenie na zewnątrz)
- Multithomed (wiele połączeń z innymi AS)
- Transit (j.w. + pozwala na routing przez siebie)

Peering jest to zgoda na wzajemne (bezpłatne) przesyłanie danych pomiędzy swoimi sieciami (poziome kreski na rysunku).

Transit (strzałki w górę) – opłaty za przesłanie (określonej ilości) danych przez sąsiednie AS.

WYKŁAD 8

Czym różni się tryb aktywny od pasywnego w połączeniach FTP? Który powoduje problem jeśli klient jest za routerem z NAT?

Tryb aktywny:

- Klient FTP wybiera port, informuje o nim serwer, po czym zaczyna na nim nasłuchiwać,
- Serwer FTP łączy się z tym portem i wysyła tam żądane dane
- Problem, jeśli klient jest za routerem z NAT

Tryb pasywny:

- Klient żąda, żeby serwer wybrał port,
- Serwer wybiera port, informuje o tym klienta, zaczyna nasłuchiwać,
- Klient łączy się z tym portem i pobiera stamtąd żądane dane.

Opisz budowę adresu URL. Opisz budowę adresu URL w przypadku schematu http.

Adres URL składa się z dwóch część oddzielonych dwukropkiem:

- Schemat (`http, ftp, mailto, file`…)
- Cześć zależna od rodzaju zasobu

URL w przypadku schematu http składa się z (część po dwukropku):

- //,
- Nazwa DNS serwera,
- Opcjonalnie `:port`,
- /,
- Identyfikator zasobu wewnątrz serwera,
- Przykład: `http://www.ii.uni.wroc.pl/~mbi/dyd/sieci_13s/.`

Uwaga! / w identyfikatorze wskazuje na hierarchię; identyfikator zasobu niekoniecznie jest ścieżką do pliku.

W jakim celu serwer WWW ustawia typ MIME dla wysyłanej zawartości? Podaj kilka przykładów typów MIME.

Internet media type, zwany także **typem MIME** oraz czasem **Content-Type** (po nazwie nagłówka kilku protokołów, którego wartość jest tego typu) jest dwuczęściowym identyfikatorem formatu plików w Internecie. Serwer www ustawia odpowiedni typ MIME w celu określenia rodzaju zasobu który jest przesyłany. Przykłady:

- Text/plain – plik tekstowy
- text/html – strona HTML
- image/jpeg – obrazek JPEG
- video/mpeg – film MPEG
- application/msword – dokument DOC
- application/pdf – dokument PDF
- application/octet-stream – ciag bajtów bez interpretacji

Wymień parę możliwych odpowiedzi HTTP wraz z ich znaczeniem.

- 200 OK – jest ok

- 301 Moved Permanently - zasób został trwale przeniesiony w inne miejsce
- 302 Found - plik został znaleziony, ale tymczasowo znajduje się w innej lokalizacji. Żądanie o zasób kończy się więc przekierowaniem.
- 304 Not Modified - zasób nie uległ zmianie patrząc pod kątem danych, które przekazano w żądaniu o ten zasób.
- 401 Unauthorized - strumień danych przesłanych przez klienta (np. przeglądarkę internetową) jest prawidłowy i serwer odczytał go poprawnie, lecz źródło URL wymaga autoryzacji danych użytkownika.
- 403 Forbidden – serwer został znaleziony, lecz jest brak dostępu
- 404 Not Found – zasobu nie znaleziono
- 500 Internal Server Error – wewnętrzny błąd serwera

Po co w nagłówku żądania HTTP/1.1 podaje się pole Host:?

Nagłówek host: służy do rozpoznania hosta, jeśli serwer na jednym IP obsługuje kilka VirtualHostów. Dla przykładowego żądania: `<http://www.w3.org/pub/WWW/>` pole host będzie zawierało: `www.w3.org`

Czy w jednym połączeniu TCP można pobrać wiele plików przez HTTP? Do czego służy opcja Connection: close w nagłówku HTTP?

Zazwyczaj przeglądarka pobiera wiele dokumentów naraz (np. strona WWW + obrazki). Opcja Connection: close służy do zamknięcia połączenia.

Kiedy serwer HTTP odpowiada komunikatem 304 Not Modified? Co oznaczają komunikaty 301 Moved Permanently i 302 Found?

- 304 Not Modified - zawartość zasobu nie podległa zmianie według warunku przekazanego przez klienta (np. data ostatniej wersji zasobu pobranej przez klienta - cache przeglądarki)
- 301 Moved Permanently - zasób został trwale przeniesiony w inne miejsce
- 302 Found - plik został znaleziony, ale tymczasowo znajduje się w innej lokalizacji. Żądanie o zasób kończy się więc przekierowaniem. Przyszłe odwołania do zasobu powinny być kierowane pod adres pierwotny

Do czego służą arkusze stylów CSS?

Arkusz stylów CSS to lista dyrektyw (tzw. reguł) ustalających w jaki sposób ma zostać wyświetlana przez przeglądarkę internetową zawartość wybranego elementu (lub elementów) (X)HTML lub XML.

Wymień parę możliwości uzyskiwania dynamicznych stron WWW.

- **Dynamika po stronie klienta**
  - **Javascript: prosty obiektowy interpretowany język, kod programu jest wbudowany w HTML.**
  - **Aplety Javy, aplikacje Flash, Silverlight (wykonanie realizowane przez odpowiednie wtyczki do przeglądarki)**
- **Dynamika po stronie serwera**
  - **URI może wskazywać na program, którego wynikiem działania jest HTML (+ ewentualnie nagłówek HTTP)**
    - **CGI (Common Gateway Interface): standard umożliwiający wykonanie dowolnego zewnętrznego programu**

- **Mechanizmy zintegrowane z serwerem WWW (PHP, JSP, ASP, mod_perl, ...)**
  - **Formularze, przekazywanie parametrów (metody GET i POST)**
  - **Cookies = utrzymywanie stanu sesji**

Co to jest CGI?

CGI (Common Gateway Interface): standard umożliwiający wykonanie dowolnego zewnętrznego programu. Znormalizowany interfejs, umożliwiający komunikację pomiędzy oprogramowaniem serwera WWW a innymi programami znajdującymi się na serwerze. Zazwyczaj program serwera WWW wysyła do przeglądarki statyczne dokumenty HTML. Za pomocą programów CGI można dynamicznie (na żądanie klienta) generować dokumenty HTML uzupełniając je np. treścią pobieraną z bazy danych.

Programy CGI są często pisane w językach interpretowalnych takich jak Perl, przez co nazywa się je także **skryptami CGI**.

Po co stosuje się metodę POST?

Metodą POST mamy do czynienia, gdy w URI nie widać żadnych parametrów. Dane metodą POST przesyłane są w obszarze danych pakietu i umieszczane w superglobalnej tablicy $_POST (tzn. można się od niej odwołać z dowolnego miejsca skryptu). Jako że użytkownik nie może podejrzeć przesłanych danych, tą metodą przesyłamy np. dane uwierzytelniające. Stosuje się ją także przy wgrywaniu plików.

Co to jest technologia REST?

REST (Representational State Transfer) - tworzenie usługi sieciowej wykorzystując metody (GET, PUT, POST, DELETE) protokołu HTTP. REST nie jest standardem, raczej filozofią. Łatwy do zautomatyzowania, czytelny dla człowieka. Zautomatyzowany dostęp do niektórych serwisów WWW (przykładowo do: eBay, Amazon, Twitter, Flickr, ...).

Jest wykorzystywany przez wiele frameworków aplikacji internetowych np. Ruby on Rails, Sinatra, Django, RESTlet, RESTeasy i wiele innych. Charakterystycznym elementem REST jest "restowy" (*RESTful*) interfejs usług webowych, w którym parametry wywołania danej usługi są umieszczane w ścieżce adresu URL, a nie w części przeznaczonej na parametry, jak w klasycznych wywołaniach GET lub POST.

Wywołanie klasyczne:

```
http://example.com/article?id=1234&format=print
```

Wywołanie RESTful

```
http://example.com/article/1234/print
```

Do czego służą serwery proxy?

- Ograniczanie ruchu do/z zewnętrznych stron WWW i przechowywanie zawartości stron w pamięci proxy.
- Kontrolowanie dostępu do zasobów WWW.

Uwaga: serwer proxy zazwyczaj oznacza serwer proxy WWW, ale można wyobrazić sobie proxy dla wielu innych usług (ARP, DNS, DHCP)

Kiedy serwer proxy decyduje się na wysłanie zapytania do serwera WWW, a kiedy obsługuje żądanie ze swojej pamięci podręcznej?

Działanie:

- Oczekuje na porcie 8080 lub 3128 (zazwyczaj),
- Jeśli w pamięci podręcznej (cache) nie ma żądanej strony lub jest nieaktualna, to proxy łączy się z żądaną stroną i zapamiętuje odpowiedź w pamięci podręcznej (cache).
- Proxy zwraca odpowiedź klientowi.

Jak serwer proxy decyduje, że strona jest nieaktualna:

- Serwer WWW ustawia pole `Expires`: w nagłówku odpowiedzi -> po tej dacie serwer proxy wyrzuca stronę z cache
- Serwer WWW może ustawić pole `Pragma: no-cache` lub/i `Cache-Control: no-cache` -> strona w ogóle nie będzie zapamiętywana na serwerze proxy
- Klient WWW może ustawić powyższe pole -> zawartość cache serwera zostanie pominięta
- W pozostałych przypadkach – heurystyki oparte np. na polu `Last-modified`:

<u>Jakie informacje dołączane są przez serwer proxy do zapytania?</u>

„Zwykły" serwer proxy dodaje do naszego żądania HTTP dodatkowe pola w nagłówku, m.in.

- `X-Forwarded-For`: (nasz adres IP)
- `Via`: (adres IP proxy)

(Istnieją tzw. anonimowe serwery proxy, które nie dodają tych nagłówków)

Anonimowy serwer proxy to:

Serwer pośredniczący, który funkcjonuje jako przekaźnik między użytkownikiem i serwisem internetowym oraz którego zadaniem jest ukrywanie adresu IP maszyny użytkownika, usuwanie niektórych elementów pozwalających na identyfikację użytkownika (ciasteczka, identyfikator używanej przeglądarki, itp.) i ewentualne szyfrowanie komunikacji, co ma na celu uczynienie użytkownika anonimowym.

WYKŁAD 9-10

Co to są szyfry monoalfabetyczne? Dlaczego łatwo je złamać?

Szyfr, w którym jednej literze alfabetu jawnego odpowiada dokładnie jedna litera alfabetu tajnego. Przykładowo funkcja E zmienia literę a na d, b na h itd. Szyfry takie stosowane były już w czasach Juliusza Cezara (wtedy E(a) = (a + 3) mod 26).
Łamanie szyfru: Policzyć rozkład statystyczny znaków w zaszyfrowanym tekście i porównać z rozkładem w dowolnym tekście jawnym z tego samego języka.

Na czym polegają ataki z wybranym tekstem jawnym i znanym tekstem jawnym?

Atak z wybranym tekstem jawnym: Atakujący ma możliwość wybrania tekstu jawnego do zaszyfrowania i zdobycia odpowiadającego mu szyfrogramu. Celem tego ataku jest zdobycie jakichkolwiek informacji na temat zaszyfrowanej wiadomości lub klucza szyfrującego.
Przykład: Adwersarz potrafi zmusić klienta, żeby wysłał wybrany przez adwersarza tekst, np.„ Pchnąć w tę łódź jeża lub ośm skrzyń fig".

Atak ze znanym tekstem jawnym: Zakłada, że kryptoanalityk dysponuje zarówno szyfrogramami jak i ich tekstami jawnymi, dzięki którym ma możliwość uzyskania klucza szyfrującego.
Przykład: Adwersarz potrafi podglądnąć kilka par (tekst jawny, szyfrogram).

W każdym przypadku szyfry są trywialne do złamania.

Czym szyfrowanie symetryczne różni się od asymetrycznego?

Szyfrowanie symetryczne: ten sam klucz jest stosowany do szyfrowania i deszyfrowania.
Szyfrowanie asymetryczne: klucz publiczny do szyfrowania i klucz prywatny do odszyfrowywania (powiązane ze sobą poprzez przekształcenia matematyczne).

Co to jest szyfrowanie one-time pad?

Szyfrowanie z kluczem jednorazowym - jest dużym zbiorem o niepowtarzalnych i przypadkowych sekwencjach znaków. Nadawca używa każdej litery z tego zbioru do zaszyfrowania jednego znaku tekstu jawnego. Szyfrowanie to dodanie modulo 26 jednego znaku tekstu jawnego i znaku jednorazowego klucza. W ogólnym przypadku: $E_K(m) = m \text{ xor } K$ (klucz musi być co najmniej tak długi jak tekst jawny).

Uwaga: W przypadku **one-time pad** mamy bezpieczeństwo teorioinformacyjne (nie da się odczytać szyfrogramu), w przypadku **szyfrowania asymetrycznego** mamy bezpieczeństwo kryptograficzne (odczytanie jest bardzo trudne obliczeniowo).

Czy w szyfrowaniu asymetrycznym szyfrujemy kluczem publicznym czy prywatnym? A jakim kluczem podpisujemy wiadomość?

Klucz publiczny do szyfrowania, prywatny do podpisywania.

Na czym polega podpisywanie wiadomości?

Liczony jest hasz wiadomości. Jest on następnie szyfrowany przez osobę uwierzytelniającą jej kluczem prywatnym i jako podpis elektroniczny dołączana do oryginalnej wiadomości.
Dowolna osoba posiadająca klucz publiczny może sprawdzić autentyczność podpisu, poprzez odszyfrowanie hasza za pomocą klucza publicznego nadawcy, oraz porównanie go z osobiście wyliczonym na podstawie wiadomości.

Co to są certyfikaty? Co to jest ścieżka certyfikacji?

Certyfikat klucza publicznego – informacja o kluczu publicznym podmiotu, która dzięki podpisaniu przez zaufaną trzecią stronę jest niemożliwa do podrobienia.
Przykład. Posiadamy:

- Klucz publiczny pewnej instytucji C,
- Wiarę w to, ze instytucja C świadomie wykorzystuje podpisy cyfrowe,
- Wiadomość „klucz publiczny osoby G to g" podpisaną przez instytucję C **<- to jest certyfikat**

Ścieżka certyfikacji – to nieprzerwany łańcuch zaufania do certyfikatów wydawanych przez zaufane urzędy certyfikacji, rozpoczynający się od konkretnego certyfikatu, a kończący się na głównym urzędzie w hierarchii certyfikacji.

Na czym polega bezpieczne połączenie za pomocą protokołu SSL? W jaki sposób następuje uwierzytelnienie serwera, z którym się łączymy?

- Serwer WWW wysyła certyfikat (klucz publiczny + dane o stronie) podpisany przez pewne CA,
- Przeglądarka sprawdza, czy posiada klucz publiczny tego CA, jeśli tak to sprawdza prawdziwość podpisu CA na certyfikacie,
- Przeglądarka sprawdza, czy dane o stronie opisują tę stronę, z którą zamierzamy się łączyć.

Lub bardziej szczegółowo:

- Użytkownik łączy się z witryną, wysyłając żądanie szyfrowanego połączenia,
- Serwer odpowiada automatycznie, wysyłając użytkownikowi swój certyfikat potwierdzający tożsamość,
- Przeglądarka użytkownika generuje unikalny klucz (ciąg znaków alfanumerycznych), który będzie użyty do szyfrowania komunikacji z witryną,
- Przeglądarka użytkownika szyfruje klucz sesji, kluczem publicznym witryny. Dzięki czemu tylko konkretna witryna może odczytać dane wysłane przez użytkownika,
- Bezpieczna, szyfrowana transmisja została ustanowiona. Od tej pory wszelkie dane wysyłane przez użytkownika bądź witrynę, mogą zostać odczytane tylko przez nich samych

Co to są klucze sesji? Po co się je stosuje?

Tymczasowy klucz szyfrujący uzyskiwany przez klienta od serwera dystrybucji kluczy w celu komunikacji z konkretnym serwerem.
Kiedy mamy uwierzytelniony serwer i możemy wysyłać do niego zaszyfrowane wiadomości pojawia się problem, ponieważ serwer także musi szyfrować dane wysyłane do nas. Moglibyśmy wysłać mu klucz publiczny, jednak szyfrowanie asymetryczne jest nieefektywne (RSA jest ok. 1000 wolniejszy niż AES). W takim wypadku przeglądarka generuje symetryczny klucz sesji, szyfruje go kluczem publicznym serwera WWW i wysyła go nie niego. Od tej pory komunikacja szyfrowana jest kluczem sesji.

Co to jest funkcja skrótu (fingerprint) danego klucza? Po co się ją stosuje?

Sytuacja kiedy pobieramy niepodpisany klucz publiczny. Aby go zweryfikować musimy skontaktować się z właścicielem klucz i poprosić o przedyktowanie go w celach weryfikacji (bez sesnu: po co pobieraliśmy go wcześniej, skoro teraz właściciel dyktuje go nam?).
Fingerprint klucza jest krótkim [kilkanaście znaków] kodem który identyfikuje [z dużym prawdopodobieństwem jednoznacznie] dany klucz. Własności:

- funkcja haszująca, szybko obliczalna, operuje na ci ¸agach bitów dowolnej długości, zwraca ciąg bitów o określonej długości m
- Przykładowo dla MD5 m = 160, dla SHA-2 m = 256.
- Funkcja ma dodatkową własność kryptograficzną: dla dowolnego x znalezienie y, takiego że $h(x) = h(y)$ jest obliczeniowo trudne.

Stosuje się go do weryfikacji poprawności klucza, jest praktyczny ponieważ jest dużo krótszy niż klucz faktyczny.

Jakie własności powinna mieć kryptograficzna funkcja skrótu?

- Brak praktycznej możliwości wygenerowania wiadomości o takim samym skrócie jak żądana wiadomość
- Brak praktycznej możliwości wygenerowanie dwóch wiadomości o takim samym skrócie
- Brak możliwości wnioskowania o wiadomości wejściowej na podstawie wartości skrótu (jednokierunkowość).

Na jaki atak narażone jest podejście, w którym wiadomość najpierw szyfrujemy a potem podpisujemy? A na jaki podejście, w którym wiadomość najpierw podpisujemy a potem szyfrujemy?

Szyfruj, potem podpisz: A wysyła do B wiadomość o treści: „mam genialny pomysł…". Oczywiście „świnia" przechwytuje wiadomość i wysyła własną. Osoba B myśli, że genialny pomysł miała świnia (świnia nawet nie wie jaki).
Rozwiązanie: Wystarczyłoby, żeby A zmienił wiadomość na: „To ja, A. Mój genialny pomysł ...". Automatyzacja: podpisz, zaszyfruj, podpisz.

Podpisz, potem szyfruj: A wysyła do B wiadomość m o treści: „mam genialny pomysł…". Tym razem B to świnia, wysyła $E_C(E_a(m))$ do swojego kumpla Charliego (dysponującego parą kluczy $(C;c)$).

Wykład 10

Do czego służy protokół SMTP a do czego POP3?

SMTP(Simple Mail Transfer Protocol) jest prostym **tekstowym** protokołem służącym do wysyłania wiadomości email. Jeśli wysyłamy wiadomość na adres email w domenie obsługiwanej przez dany serwer to zostaje ona zapisana na dysk. W przeciwnym przypadku serwer może przekazać ją dalej, stając się na chwilę klientem SMTP.

POP3 (Post Office Protocol version 3) to protokół internetowy z warstwy aplikacji pozwalający na odbiór poczty elektronicznej ze zdalnego serwera do lokalnego komputera poprzez połączenie TCP/IP.

Co to jest przekazywanie poczty (relaying)? Co to jest smarthost?

Jeśli wysyłamy wiadomość na adres email w domenie nie obsługiwanej przez dany serwer to może [nie musi] przekazać ją dalej. Czynność to relaying [denied]. Kiedyś był to domyślny sposób pracy serwerów pocztowych. Obecnie: aby serwer był skłonny do takiej operacji, email musi pochodzić z zaufanego źródła (np. klient SMTP musi się uprzednio autoryzować).
Podczas przekazywania wiadomości innemu serwerowi, przekazujący serwer SMTP staje się w danej transakcji zwykłym klientem SMTP. Przekazać może do docelowego serwera SMTP (rekord MX w DNS) lub do serwera SMTP (smarthost), który skłonny będzie przekazać ją dalej.

Jaki rekord DNS jest sprawdzany przed wysłaniem poczty do danej domeny?

Rekord MX.

Wymień parę popularnych pól w nagłówku maila. Do czego służą pola Received i Bcc?

- From
- To
- Cc (kopia)
- Bcc („ślepa” kopia)
- Date (data)
- Subject (temat)

Received - tracking information generated by mail servers that have previously handled a message)
Bcc - umożliwia wysłanie wiadomości poczty elektronicznej do wielu na raz odbiorców w taki sposób, że odbiorcy nie widzą wzajemnie swoich adresów.

Jakie pola w nagłówku są używane do ,,wątkowania'' wiadomości?

- References
- In-Reply-To

Co umożliwia standard MIME?

- Możliwość określenia `Content-Type:` (tak jak w HTTP) a w nim również kodowania.
- Pole `Content-Transfer-Encoding:` (np. 8bit, base64).
- `Content-Type: multipart/*:` możliwość wysyłania załączników (przykładowo wysyłania wiadomości jednocześnie w txt i html)

Co to jest spam? Jakie znasz metody walki ze spamem?

Są to niechciane wiadomości elektroniczne. Pierwszy raz wysłany prawdopodobnie 1 maja 1978 (reklama komputerów DEC).

Sposoby walki ze spamem:

- Blokowanie konkretnych tematów (wyrażenia regularne)
- Metody statystyczne (filtry bayesowskie)
- Blokowanie adresów (greylisting)
- SPF

Na czym polegają szare listy (greylisting)?

Początkowo wszyscy są na szarej liście, jeśli ktoś chce wysłać email na adres w danej domenie to proszony jest o ponowienie próby wysłania maila za jakiś czas, jeśli ponowi, to trafia na listę białą (zakładamy ze to nie spamer).

Na czym polega mechanizm SPF?

SPF (Sender Policy Framework) – niekomercyjny projekt mający na celu wprowadzenie zabezpieczenia serwerów SMTP przed przyjmowaniem poczty z niedozwolonych źródeł. Ma to pozytywnie wpłynąć na ograniczenie ilości spamu oraz zmniejszenie ilości rozsyłających się wirusów.

Rekord SPF w DNS dla danej domeny:

- `ii.uni.wroc.pl. TXT "v=spf1 ip4:156.17.4.0/24 mx:ii.uni.wroc.pl mx:gmail.com mx:google.com -all"`
- definiuje jakie komputery są uprawnione do wysyłania poczty z polem From: pochodzącym z domeny `ii.uni.wroc.pl`:
  - komputery z adresów 156.17.4.0/24
  - komputery obsługujące pocztę dla domen ii.uni.wroc.pl, gmail.com i google.com
- rekord sprawdzany przez odbiorcę
- Problemy przy przekazywaniu poczty (komputer przekazujący nie jest oryginalnym nadawcą wiadomości)

Serwer B zabezpieczony przez SPF sprawdza w DNS-ie, czy wysyłana do niego poczta pochodzi z serwera posiadającego „uprawnienia" do wysyłania poczty z danej domeny. Jeżeli tak, to poczta jest przyjmowana. Natomiast jeśli adres IP nie pasuje do danej domeny – połączenie jest odrzucane. Dzięki temu wiadomości wysyłane przez spamerów podszywających się pod cudze adresy e-mail lub przez wirusy typu Mydoom zostaną odrzucone.

Wykład 11

Co to jest pamięć CAM i gdzie się ją stosuje? Jak można ją przepełnić?

Jest to pamięć skojarzeniowa, używana między innymi w przełącznikach do przechowywania tablicy przełączania. Jest to rodzaj pamięci o krótkim czasie dostępu. Przełącznik ma sprzętową tablicę haszującą (CAM = content addressable memory) z wpisami „adres MAC - port". Zmieniając adres MAC można zalać CAM nowymi wpisami - przełącznik przejdzie w tryb uczenia się.

Opisz atak typu ARP spoofing; jak można go wykorzystać do podsłuchiwania komunikacji między dwoma komputerami podłączonymi do przełącznika sieciowego?

ARP spoofing to atak sieciowy w sieci Ethernet pozwalający atakującemu przechwytywać dane przesyłane w obrębie segmentu sieci lokalnej. Przeprowadzony tą metodą atak polega na rozsyłaniu w sieci LAN odpowiednio spreparowanych pakietów ARP zawierających fałszywe adresy MAC. W efekcie pakiety danych wysyłane przez inne komputery w sieci zamiast do adresata trafiają do osoby atakującej pozwalając jej na podsłuchiwanie komunikacji.

Co oznacza termin IP spoofing? Na czym polega metoda weryfikacji tak zmodyfikowanych pakietów (ingress filtering)?

IP spoofing - czyli fałszowanie adresu IP nadawcy.
Ingress Filtering (weryfikacja) - sprawdzanie czy przychodzące do nas pakiety rzeczywiście mogą pochodzić z sieci z którą dany interfejs jest połączony. Przykładowo z interfejsu sieciowego podłączonego do sieci `192.168.0.0/24` nie powinien nadejść pakiet ze źródłowym IP `200.200.200.200`.

Na czym polega atak RIP spoofing?

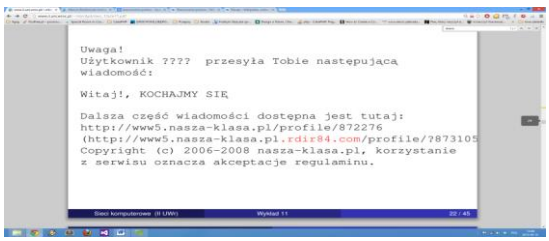
Opisz atak bazujący na zatruwaniu pamięci cache serwera DNS.

Przedstaw przykładowe ataki wykorzystujące brak sprawdzania poprawności wprowadzanych danych.

- Wprowadzenie dodatkowego, nowego polecenia, które zmodyfikuje zapytanie do bazy danych. (SQL injection),
- Wykorzystanie programu do wypisania zawartości plików systemu, które nie są przeznaczone dla zwykłego usera (../),
  przykład: `http://jakas.domena/skrypt?plik=../../etc/passwd?`
- Podanie na wejściu zbyt dużej ilości danych, przez co można nadpisać pamięć, które nie jest dla nas przeznaczona przykładowo adres powrotu (przepełnienie bufora)

Na czym polega phishing?

Phishing (*spoofing*) – wyłudzanie poufnych informacji osobistych (np. haseł lub szczegółów karty kredytowej) przez podszywanie się pod godną zaufania osobę lub instytucję, której te informacje są pilnie potrzebne. Jest to rodzaj ataku opartego na inżynierii społecznej.



Co to jest skanowanie portów? Po co się je wykonuje?

Skanowanie portów to wysyłanie pakietów do systemu w celu sprawdzenia otwartych portów i dostępnych serwisów. **nmap** - program komputerowy autorstwa Gordon'a Lyon'a, służący do skanowania portów i wykrywania usług w sieci.
Podczas skanowania można uzyskać informacje o:

- systemie operacyjnym,
- dostępnych usługach sieciowych,

- wersji programów obsługujących udostępnione usługi.

Przykładowo:

- `connect` scan
- `SYN` scan
- ustawianie różnych dziwnych flag (np. sama flaga `ACK`)

Co to są ataki DoS i DDoS?

Denial of service – celem jest wyczerpanie zasobów systemu operacyjnego albo zatkanie łącza. Możemy wyczerpać takie zasoby jak: moc obliczeniowa, limit jednoczesnych połączeń (`connet()`).

DDoS - rozproszony DoS (wykorzystanie wielu komputerów, np. uprzednio zainfekowanych robakiem internetowym).

Na czym polega atak typu odbity (reflected) DoS?

Wysyłamy do różnych komputerów komunikat z fałszywym adresem źródłowym (adres IP ofiary), przez co komputery odpowiadają ofierze. Komunikat to najczęściej `segment SYN`, `ICMP echo request (ping)` **Przykład:** smurf attack - wysyłamy ping na adres broadcast z podmienionym adresem IP ofiary (obecnie nie zadziała)

Na czym polegają ataki typu SYN flood?

SYN flood – wysyłanie samych segmentów SYN (zapełnienie tworzonej przez `listen()` kolejki połączeń oczekujących na nawiązanie).

Jak działa i do czego jest wykorzystywany ICMP Traceback?

Przed atakiem DDoS można się bronić tylko, jeśli atak pochodzi z jednego geograficznego obszaru. Problemem jest ustalenie źródła ataków (źródłowe adresy IP są podrobione. Po ustaleniu źródła, można zadzwonić do administratora.

ICMP Traceback: każdy router z małym prawdopodobieństwem (ok. 1⁄20000) dla przesyłanego pakietu wysyła również do odbiorcy dodatkowo komunikat ICMP, który zawiera informacje o przesyłanym właśnie przez router pakiecie, informacje o routerze, itp.

Opisz, jak wygląda uwierzytelnianie serwera SSH.

- Serwer wysyła klientowi swój klucz publiczny
- Klient generuje symetryczny klucz sesji (np. AES) i wysyła go
- szyfrując go kluczem publicznym serwera.
- Od tej pory połączenie szyfrowane jest kluczem sesji.
- Klient się uwierzytelnia podając swoje hasło.

Na czym polega uwierzytelnianie użytkownika przez SSH z wykorzystaniem kluczy RSA.

Podaj przykłady tunelowania.

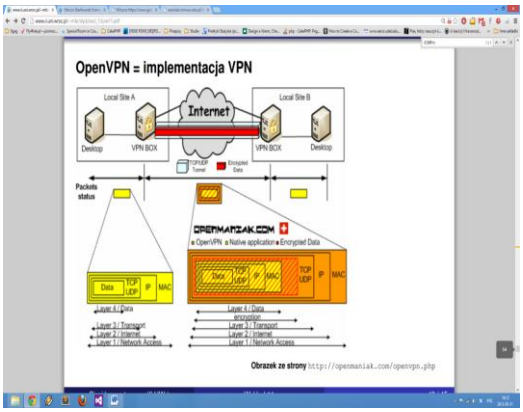
- **TCP w SSH**: Połączenia z portem 4025 na lokalnym komputerze będą przekazywane (i szyfrowane po drodze) do komputera `zdalny-serwer`, a tam przekazywane do portu 25:

  ```
  ssh -L 4025:localhost:25 user@zdalny-serwer
  ```

- Tunelowanie w POP3 i SMTP

Rozwiń skrót VPN. Do czego służy?

VPN (Virtual Private Network): Mamy dwie sieci połączone internetem i chcemy zrobić z nich jedną sieć logiczną. Transmisja wewnątrz każdej sieci jest bezpieczna, ale transmisja w internecie już nie. Przykład: dostęp do firmowej sieci z domu.



Zapisz adres IPv6 0321:0000:0000:0123:0000:0000:0000:0001 w najkrótszej możliwej postaci.

321:0:0:123::1

Wykład 12

Jakie są cechy charakterystyczne sieci peer-to-peer? Po co się je stosuje?

- Wszystkie komputery są jednocześnie klientami i serwerami,
- Każdy komputer może nawiązywać połączenia z innymi (bez pośrednictwa znanego serwera),
- Brak centralnego miejsca z danymi – niezawodność,
- Każdy wierzchołek sieci jest autonomiczny (brak administracji), ALE trudniejsze zagwarantowanie współpracy całości,
- Efektywne wykorzystanie zasobów klientów (dyskowych i obliczeniowych) - lepsza skalowalność.

Sieci p2p najczęściej stosowane są do współdzielenia i wymiany plików.

Co to jest sieć nakładkowa (overlay network)?

- logiczna sieć oparta o sieć bazową (Internet),
- bezpośrednie połączenia w sieci nakładkowej zazwyczaj nie są bezpośrednie w sieci bazowej,
- dobrze, jeśli struktura sieci nakładkowej odzwierciedla strukturę sieci bazowej

Jaka jest rola trackera w sieci Bittorrent?

Jest to komputer (serwer) będący nadzorcą działania sieci BitTorrent, czuwa niejako nad całym procesem wymiany plików, podłączają się do niego poszczególni klienci (programy które umożliwiaja nam wymianę plików) i ma on za zadanie między innymi przekazywać dane tj. adresy IP pomiędzy osobami pobierającymi plik. Sprawność jego działania poniekąd wpływa na szybkość z jaką możemy współdzielić pliki. Jego obecność jest konieczna do nawiązania połączenia z inną osobą i możliwości pobrania od tejże osoby jakiegokolwiek pliku.

Po co w plikach .torrent stosuje się funkcje skrótu?

Funkcja skrótu, inaczej: funkcja mieszająca lub funkcja haszująca – jest to funkcja, która przyporządkowuje dowolnie dużej liczbie krótką, zwykle posiadającą stały rozmiar, nie specyficzną, quasi-losową wartość, tzw. *skrót nieodwracalny*.

Info hash - 160-bitowa wartość pochodząca z funkcji skrótu SHA1. Funkcji tej jest podawana część metapliku `.torrent` zawierająca nazwy plików oraz hasze udostępnianych danych. Możliwa jest zmiana trackera oraz komentarza w pliku `.torrent` bez zmiany Info hasha.

Na czym polega NAT i po co się go stosuje?

Network Address Translation (Przekształcanie adresów sieciowych) - technika przesyłania ruchu sieciowego poprzez router, która wiąże się ze zmianą źródłowych lub docelowych adresów IP, zwykle również numerów portów TCP/UDP pakietów IP podczas ich przepływu. Zmieniane są także sumy kontrolne (zarówno w pakiecie IP jak i w segmencie TCP/UDP), aby potwierdzić wprowadzone zmiany. Większość systemów korzystających z NAT ma na celu umożliwienie dostępu wielu hostom w sieci prywatnej do internetu przy wykorzystaniu pojedynczego publicznego adresu IP. Niemniej NAT może spowodować komplikacje w komunikacji między hostami i może mieć pewien wpływ na osiągi.

Stosuje się go, ponieważ adresy IP się kończą (i są dość kosztowne) oraz chcemy ukrywać IP komputerów w sieci lokalnej przed światem zewnętrznym.

Wyjaśnij różnicę między źródłowym a docelowym NAT.

- **SNAT** (*Source Network Address Translation*) to technika polegająca na zmianie adresu źródłowego pakietu IP na jakiś inny. Stosowana często w przypadku podłączenia sieci dysponującej adresami prywatnymi do sieci Internet. Wtedy router, przez który podłączono sieć, podmienia adres źródłowy prywatny na adres publiczny (najczęściej swój własny).
- **SNAT** ma miejsce wtedy, gdy zmieniasz adres źródłowy pierwszego pakietu: tzn. kiedy zmieniasz adres maszyny z której inicjowane jest połączenie. SNAT wykonywany jest zawsze w fazie po routingu (post-routing), tuż przed tym zanim pakiet opuści maszynę po kablu. Masquerading jes specjalizowaną formą SNAT.
- **DNAT** (*Destination Network Address Translation*) to technika polegająca na zmianie adresu docelowego pakietu IP na jakiś inny. Stosowana często w przypadku, gdy serwer, który ma być dostępny z Internetu ma tylko adres prywatny. W tym przypadku router dokonuje translacji adresu docelowego pakietów IP z Internetu na adres tego serwera.
- **DNAT** ma miejsce wtedy, gdy zmieniasz adres docelowy pierwszego pakietu: tzn. kiedy zmieniasz adres maszyny do której ma dotrzeć połączenia. DNAT wykonywany jest zawsze przed routingiem (pre-routing), kiedy pakiet właśnie został odebrany z kabla. Przekazywanie portów, balansowanie obciążeniem i transparentne proxy to wszystko różne rodzaje DNAT

Opisz podobieństwa i różnice asymetrycznych (cone) NAT (pełnego, ograniczonego i ograniczonego portowo) i symetrycznych NAT.

Opisz technikę wybijania dziur (hole punching) w NAT. Po co konieczny jest serwer pośredniczący?

Porównaj wady i zalety filtrów pakietów: prostych, stanowych i działających w warstwie aplikacji.

Filtry proste

- Analizują tylko nagłówki IP,
- Szybkie, bardzo nieprecyzyjne.

Filtry stanowe

- Analizują nagłówki IP i TCP,
- Śledzą trójstanowe uzgodnienie, pamiętają stan połączenia,
- „Rozumieją” numery sekwencyjne - lepsza odporność na fałszowanie nagłówków.

Filtry działające w warstwie aplikacji

- Analizują zawartość segmentów i datagramów,
- Np. w przypadku FTP „rozumieją” ze trzeba otworzyć odpowiedni port na dane,
- To cos innego niż zapory aplikacji (które analizują wywołania systemowe aplikacji)

Do czego służą łańcuchy INPUT OUTPUT i FORWARD w zaporze Linuksa?

- **INPUT**: pakiety przychodzące z zewnątrz i konczące trasę na naszym komputerze
- **FORWARD**: pakiety przechodzące przez nasz komputer
- **OUTPUT**: pakiety tworzone lokalnie i opuszczające nasz komputer

Do czego służy klasyfikator -m state --state ESTABLISHED zapory?

W jakich łańcuchach zapory Linuksa wykonywany jest źródłowy a w jakich docelowy NAT?