Zastosowania sieci komputerowych

- współdzielenie zasobów, np. plików, drukarek
- komunikacja, np. poczta email, telefonia komórkowa, internetowa
- przypadek specjalny: Internet
  - wiele różnych nowych zastosowań: handel, usługi, reklama, gry on-line, *video on demand*, zdalne nauczanie, zdalne głosowanie, itd.
- zastosowania mobilne
  - podobne jak w poprzednich grupach, + dodatkowe, np. nawigacja
- sieci przemysłowe
  - zastosowania przemysłowe
    - w szczególności sieci bezprzewodowe
- sieci do zastosowań specjalnych
  - specjalne zastosowania komercyjne, np. systemy alarmowe
  - bezprzewodowe sieci czujników
  - zastosowania wojskowe

Klasy wielkości sieci komputerowych

- sieci osobiste PAN *Personal Area Network*

  Zasięg to często biurko lub pokój, ewentualnie dom i/lub ogród, należące do jednej osoby. Wiele typowych PAN to sieci bezprzewodowe, np. zrealizowane np. z wykorzystaniem technologii Bluetooth. Często podobną sieć zrealizowaną w technologii przewodowej określa się jako LAN.

- sieci lokalne LAN *Local Area Network*

  Zasięg do 1000 metrów, należące do jednej organizacji, z jednolitym zarządzaniem.

- sieci metropolitalne MAN *Metropolitan Area Network*

  Zasięg około 10 kilometrów, zwykle nie należą do jednej organizacji i często nie mają wspólnego zarządzania.

- sieci rozległe WAN *Wide Area Network*

  Zasięg może obejmować cały kraj, kontynent, lub więcej. Często, mianem WAN określa się nie rzeczywiste sieci komputerowe, ale **intersieci**, czyli sieci, które łączą różne sieci.

Systemy rozproszone

Systemem rozproszonym (*distributed system*) określa się sieciowy system komputerowy, który prezentuje użytkownikowi jednolity interfejs funkcji systemu, częściowo ukrywając jego sieciowy charakter.

Na przykład, sieć WWW prezentuje się jako pojedynczy dokument o strukturze drzewa. Możemy przechodzić między podstronami tego dokumentu, nie mając świadomości (albo nawet możliwości stwierdzenia), że poszczególne elementy są obsługiwane przez różne komputery, pod kontrolą różnych systemów operacyjnych, i zlokalizowane w różnych miejscach geograficznych.

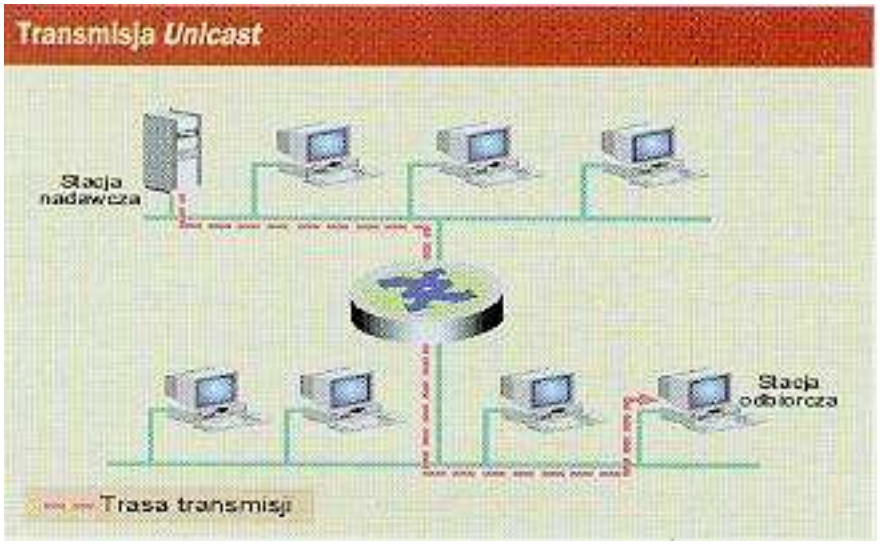
Innym przykładem może być system rezerwacji połączeń PKP lub lotniczych. Znajduje on połączenia realizowane przez różne składy/samloty, należące do różnych firm, a informacje o tych połączeniach i dostępności miejsc mogą znajdować się w różnych bazach danych.

W odróżnieniu, większość systemów operacyjnych prezentuje interfejs **sieciowego systemu operacyjnego** zmuszającego użytkownika do świadomej nawigacji pomiędzy elementami sieci komputerowej.

Typy transmisji sieciowych

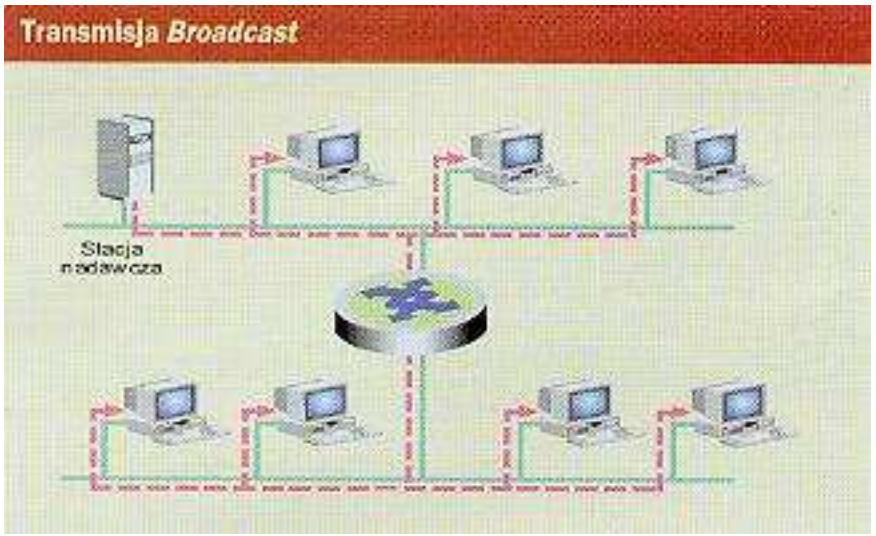
Komunikacja typu point-to-point (*unicast*)

np. połączenie telefoniczne drutowe (aparat końcowy do centrali)



Komunikacja typu *broadcast*

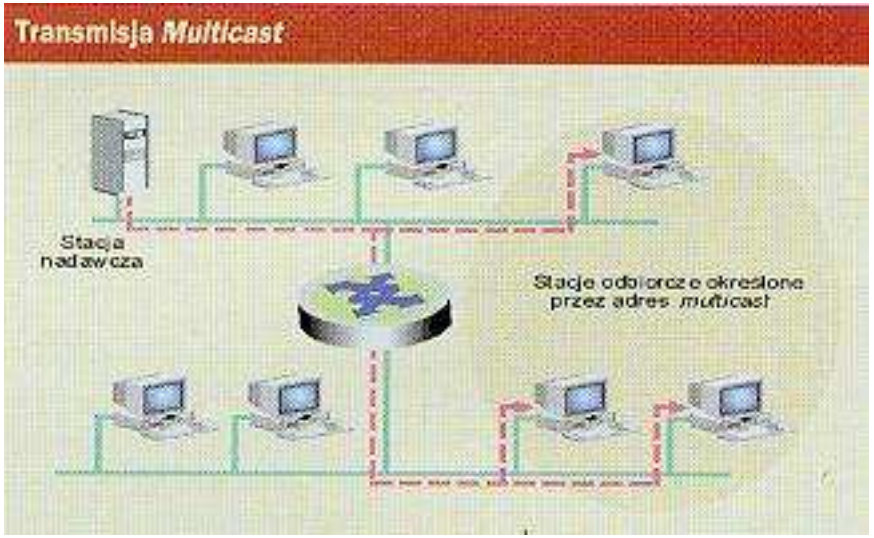
np. transmisja radiowa, satelitarna, itp.



Uwaga: transmisja typu *broadcast* może być adresowana do wybranych odbiorców, pomimo iż może używać pasma dostępnego dla wszystkich.

Typy transmisji sieciowych — multicast

Specjalna forma *broadcast*-u — *multicast*, oznacza jednoczesne nadawanie do grupy odbiorców. Należy odróżnić transmisję komunikatu *multicast* do określonej grupy (pojedynczy strumień danych) od transmisji jednego komunikatu wiele razy do grupy (zduplikowany strumień danych).



Technologie *multicast* nie są nowym wynalazkiem, ale dotychczas były mało popularne i rozwijane ze względu na komplikacje w niezbędnych technologiach i standardach. (Np. każdy router, nawet w małej sieci domowej lub osiedlowej, powinien być przystosowany do odebrania transmisji *mulicast*, zbadania adresu grupy *mulicast*, i zadecydowania, czy transmisję należy przekazywać do wnętrza sieci, i konkretnie do których jej części.

W kontekście nabierających popularności szerokopasmowych transmisji wideo te technologie jednak stają się coraz ważniejsze. Zamiast dublować strumień wideo, jak również wysyłać do wszystkich sieci (na świecie) lepiej kierować go do zdefiniowanej grupy.

Typy komunikacji — komunikacja połączeniowa

Wygodnie jest rozważać dwa zasadniczo różne modele komunikacji: połączeniowy i bezpołączeniowy.

Komunikacja połączeniowa jest oparta na zbudowaniu połączenia między stronami, połączenie inicjuje jedna strona, ale utrzymują je obie. Dopóki połączenie istnieje, każda ze stron może nadawać w dowolnym momencie, a druga strona odbiera tę transmisję. Po rozłączeniu, dalsza komunikacja jest niemożliwa do czasu ponownego nawiązania połączenia.

Dobrą analogią komunikacji połączeniowej jest rozmowa przez telefon. Strona inicjująca połączenie musi znać numer telefonu (adres) strony przyjmującej. Strona przyjmująca może nie mieć świadomości numeru dzwoniącego. (Czasami technologia sieci pozwala odbiorcy poznać ten numer, tzw. Caller-ID, ale nie jest to potrzebne do komunikacji.) Jednak po nawiązaniu połączenia żadna ze stron nie musi już pamiętać numeru telefonu drugiej strony.

Typowo w komunikacji połączeniowej strumień danych dochodzi w tej samej postaci w jakiej został nadany (nie ma zamiany kolejności), aczkolwiek przy zawodnym medium jest możliwe przekłamanie, albo utrata części danych.

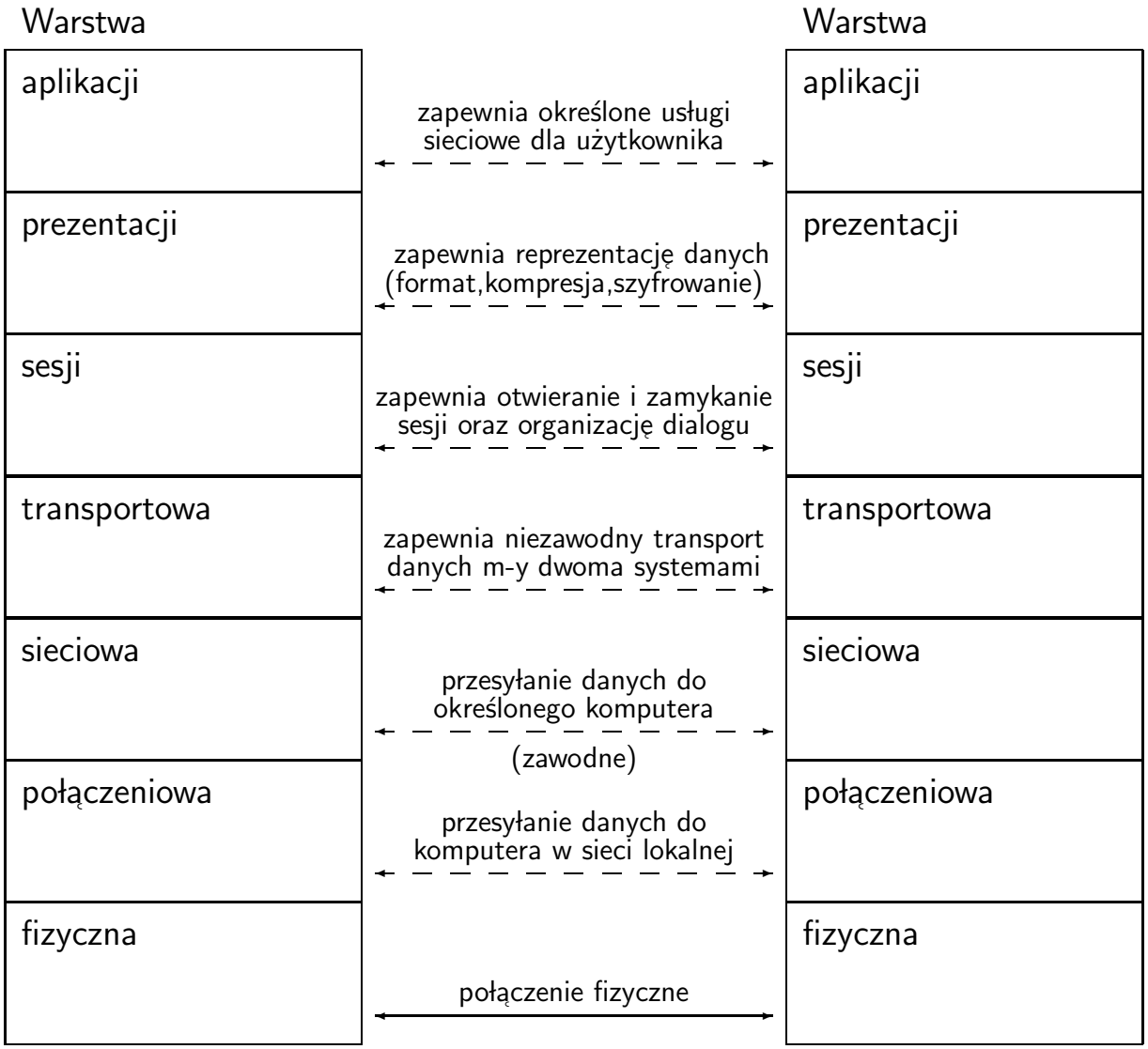
Typy komunikacji — komunikacja bezpołączeniowa

Komunikacja bezpołączeniowa jest oparta na wysyłaniu w pełni adresowanych pakietów danych, z których każdy może być niezależnie doręczony odbiorcy. W każdej chwili możemy wysłać odbiorcy pakiet danych, pod warunkiem, że znamy jego adres.

Podobną analogią komunikacji bezpołączeniowej jest korespondencja listowa. Aby wysłać komuś list trzeba znać jego adres, i żeby odbiorca mógł odpowiedzieć musi on znać adres nadawcy. Przesyłka może być doręczona z adresem nadawcy lub bez tego adresu. (Tradycyjna poczta nie oferuje usługi dostarczenia wraz z listem adresu nadawcy, ale w sieciowej komunikacji bezpołączeniowej takie możliwości zwykle istnieją.)

Typowo w komunikacji bezpołączeniowej możliwa jest zamiana kolejności niektórych pakietów (ich doręczenie w innej kolejności niż były nadane), bo trudno jest kontrolować media komunikacyjne aby tej kolejności przestrzegały. Przekłamania i gubienie przesyłek jest możliwe podobnie jak w komunikacji połączeniowej.

Warstwowy model sieci ISO-OSI



Zadania warstw modelu OSI/ISO

- Zadania warstwy fizycznej:
  - zapewnienie dostępu do danych
  - kodowanie strumienia danych
- Zadania warstwy łącza danych
  - dostęp do łącza,
  - formatowanie i transmisja ramek,
  - zapewnienie adresacji.
- Zadania warstwy sieciowej
  - dostarczenie logicznej adresacji
- Zadania warstwy transportowej
  - segmentacje danych w strumień i ponowne ich złożenie w punkcie docelowym

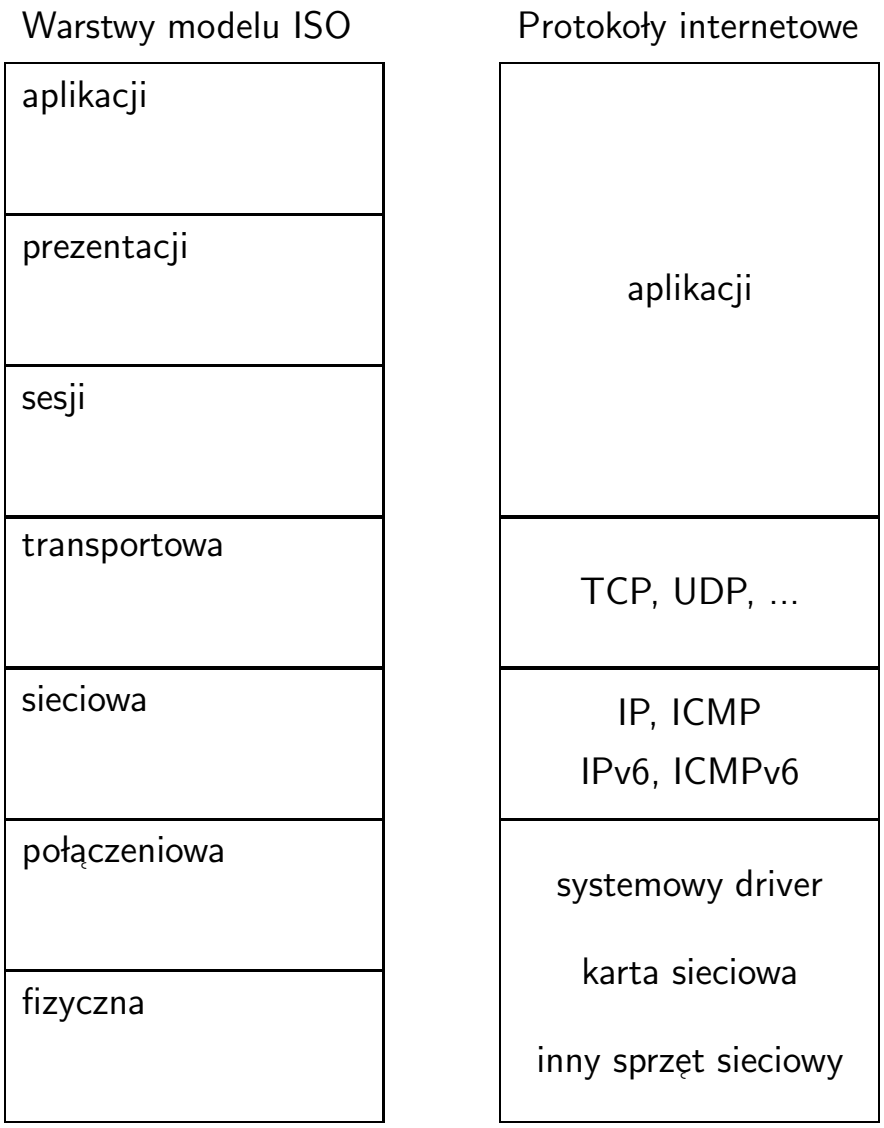
  - zapewnienie niezawodność przesyłu danych
  - zapewnienie parametrów jakości transmisji (QOS - Quality of Service)

- Zadania warstwy sesji
  - odpowiedzialna za sesje między dwoma procesami na różnych komputerach
  - implementowana jest przez system operacyjny
  - odpowiada za synchronizację danych między komputerami
  - określenie czy stacje mają uprawnienia do komunikacji przez sieć

- Zadania warstwy prezentacji
  - odpowiedzialna za reprezentacje danych
  - implementowana przez system operacyjny
  - konwersja między standardami kodowania znaków

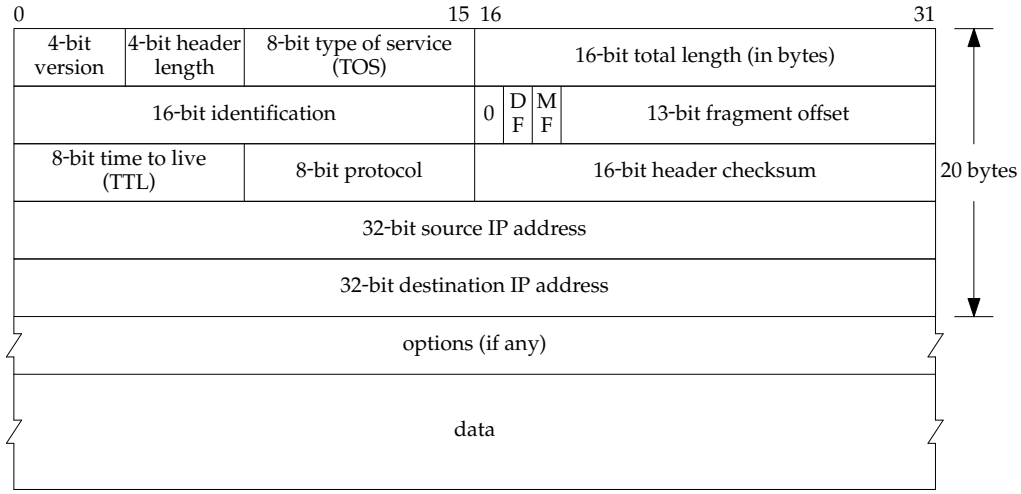
- Zadania warstwy aplikacji
  - najbliżej użytkownika
  - przeglądarka WWW, klient poczty elektronicznej, aplikacje konferencyjne, FTP

Model ISO a protokoły internetowe

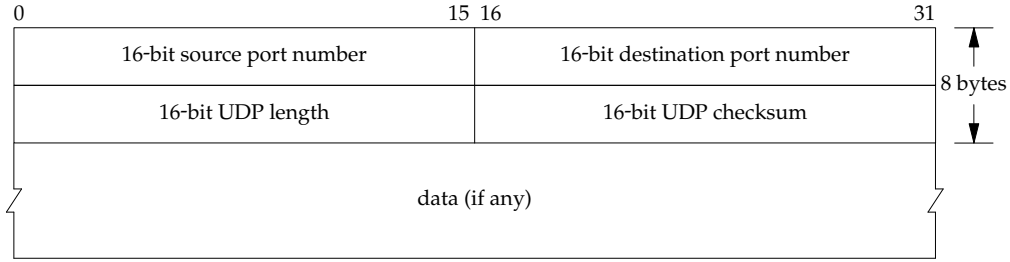


Nagłówki pakietów TCP, UDP i IP

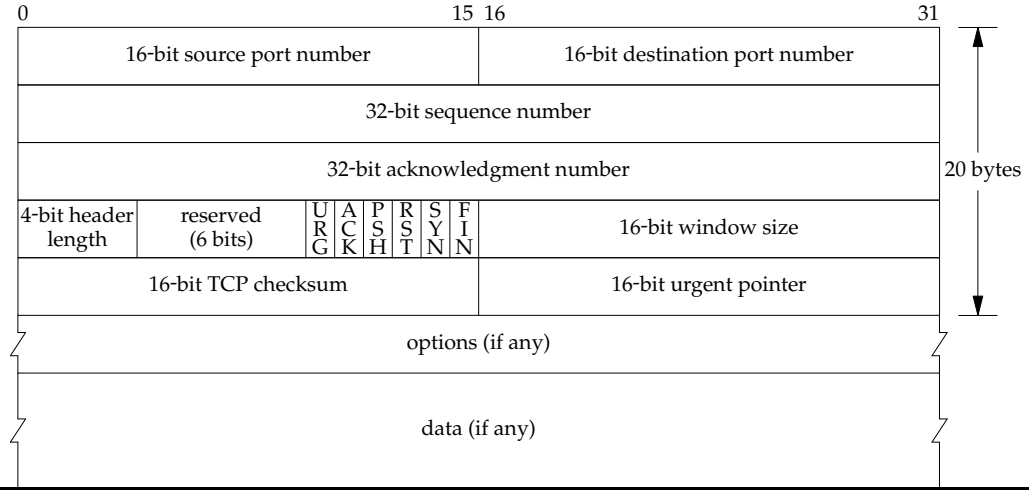
IP Header



UDP Header



TCP Header



Adresowanie w Internecie

32-bitowe (4-oktetowe) adresy IP wersji 4, stosowane od 1.I.1983

- klasa A: pierwszy oktet jest adresem sieci (a pozostałe trzy adresem komputera), z czego pierwszy bit jest zerem; możliwe 128 takich sieci (przedział 0-127) i 16 milionów komputerów w każdej
- klasa B: pierwsze dwa oktety są adresem sieci (a dwa adresem komputera), z czego pierwsze dwa bity są 10; możliwe 16 tysięcy adresów sieci (przedział 128-191) po 65 tysięcy komputerów
- klasa C: pierwsze trzy oktety są adresem sieci (a jeden adresem komputera), z czego pierwsze trzy bity są 110; możliwe dwa miliony takich sieci (przedział 192-223) i 256 komputerów w każdej
- klasa D: cały adres jest jednym adresem, ale cztery pierwsze bity muszą być 1110; adresy te stosuje się do komunikacji multicast
- adresy *broadcast*: same jedynki lub same zera w adresie komputera
- adresy prywatne:
  $10.0.0.0 - 10.255.255.255$
  $172.16.0.0 - 172.31.255.255$
  $192.168.0.0 - 192.168.255.255$

Sieci prywatne

W schemacie adresowania IPv4 trzy zakresy adresów zostały zarezerwowane jako „prywatne". Przeznaczone były do wykorzystania w sieciach LAN: domowych, biurowych, i firmowych, nie połączonych z Internetem. Korzystanie z tych adresów nie wymaga żadnych zezwoleń, uzgodnień, ani rejestracji:

- $10.0.0.0 - 10.255.255.255$
- $172.16.0.0 - 172.31.255.255$
- $192.168.0.0 - 192.168.255.255$

Oznacza to, że w takich sieciach można stosować oprogramowanie przeznaczone do Internetu, takie same urządzenia i konfiguracje, ale sieć nie będzie połączona z Internetem. Zapewnia to z jednej strony bezpieczeństwo infrastruktury firmy przed możliwymi atakami z Internetu, ale również brak zagrożenia możliwym wyciekiem danych przy okazji nieostrożnych poczynań pracowników. (Także zagrożenia marnowania czasu pracy przez browsowanie po Internecie.)

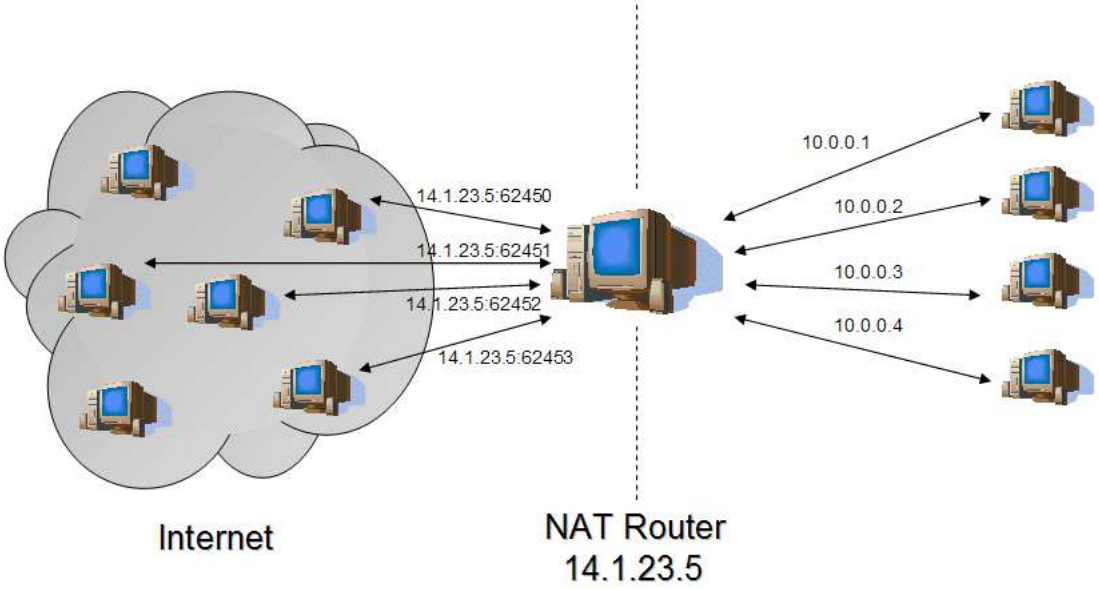
Prywatne zakresy adresowe okazały się niezwykle użyteczne ratując Internet przed wyczerpaniem zwykłych adresów.

Translacja adresów NAT

Przydzielanie adresów IP według schematu czterech klas jest nieefektywne; pomimo iż istnieje ponad 4 miliardy liczb 32-bitowych, ze względu na rewolucyjny rozwój Internetu, już w połowie lat 90-tych zaczęło brakować adresów IP. W związku z tym wdrażano różne zmiany, zwiększające elastyczność przydziału adresów (adresowanie bezklasowe), oraz trwały prace nad nowym standardem adresowania (system IPv6).

Jednak prace te posuwały się powoli i nie rokowały perspektywy szybkich zmian. W międzyczasie zaczęto oddolne, niewymagające globalnych zmian, wprowadzanie systemu NAT (*Network Address Translation*) polegające na wykorzystaniu adresowania sieci prywatnych, i łączeniu takich sieci z Internetem za pomocą routerów dokonujących zamiany adresów prywatnych w LAN na publiczny adres internetowy routera obsługującego sieć LAN, plus unikalnego numeru portu, identyfikującego połączenie.

Od strony Internetu wygląda to tak, jakby cały ruch z takiej sieci prywatnej pochodził z samego routera. Natomiast router zamienia adresy wychodzące z sieci lokalnej na swój własny adres, a adresy przychodzących odpowiedzi na właściwe adresy prywatne sieci LAN, na podstawie numeru portu.



NAT może wprowadzić na własny użytek małe biuro, gospodarstwo domowe, ale także całkiem duża firma, lub dostarczyciel usługi Internetu dla osiedla albo nawet całego miasta. NAT może być realizowany przez komputer zapewniający łączność sieci LAN z Internetem, może być zrealizowany przez router sprzętowy, a nawet aplikację na telefon komórkowy, tworzący prywatną sieć WiFi i łączący ją z Internetem przez sieć komórkową GSM.

Należy pamiętać, że NAT nie zapewnia pełnej łączności sieci LAN z Internetem, a jedynie połączenia wychodzące. Ogólnie nie jest możliwe umieszczenie serwera internetowego w sieci LAN z NAT, oraz nie jest to odpowiednie rozwiązanie dla pewnych typów komunikacji, jak np. telefonia internetowa VOIP.

Adresowanie bezklasowe CIDR

Jedną ze zmian wprowadzonych w celu rozwiązania (a raczej odsunięcia) problemu wyczerpywania się adresów IPv4 w internecie był system adresowania bezklasowego CIDR (*classless inter-domain routing*). Odrzuca on sztywny podział adresu na adres sieci i komputera wyznaczony przez klasę.

Obecnie dowolny adres IPv4 składa się z *prefixu* (pierwszej części) dowolnej długości, stanowiącego adres sieci, i reszty stanowiącej adres komputera. Dla wskazania długości prefixu stosuje się notację *x.y.z.t/p*. Na przykład, 156.17.9.0/25 oznacza adres sieci, w którym 25 bitów stanowi adres sieci, a pozostałych 7 adres komputera. Oznacza to, że może być 128 adresów w tej sieci, z których pierwszy (same zera w części adresu komputera) jest adresem sieci, a ostatni (same jedynki w części adresu komputera) jest adresem rozgłaszania (*broadcast*), co pozostawia 126 rzeczywistych adresów.

Adresowanie bezklasowe pozwala właścicielom bloków adresów efektywniej nimi gospodarować, co powoduje mniejsze marnowanie adresów w poszczególnych blokach. Jednak co równie ważne, pozwala ono administratorom sieci na definiowanie zagregowanych ścieżek routingu. Na przykład, pomimo iż istnieje wiele małych sieci o adresach zaczynających się na 156.17.x.x, to dla globalnego routera mogą one być reprezentowane jedną ścieżką 156.17/16.

Nowy protokół IPv6

System adresowania IPv4 jest wykorzystywany wraz z podstawowym protokołem komunikacyjnym Internetu IP od 1 stycznia 1983. Pozwolił on na poprawną pracę sieci od początku, kiedy istniało zaledwie kilkadziesiąt węzłów, aż do masowego wzrostu w latach 1990-tych, kiedy adresów IP zaczęło brakować.

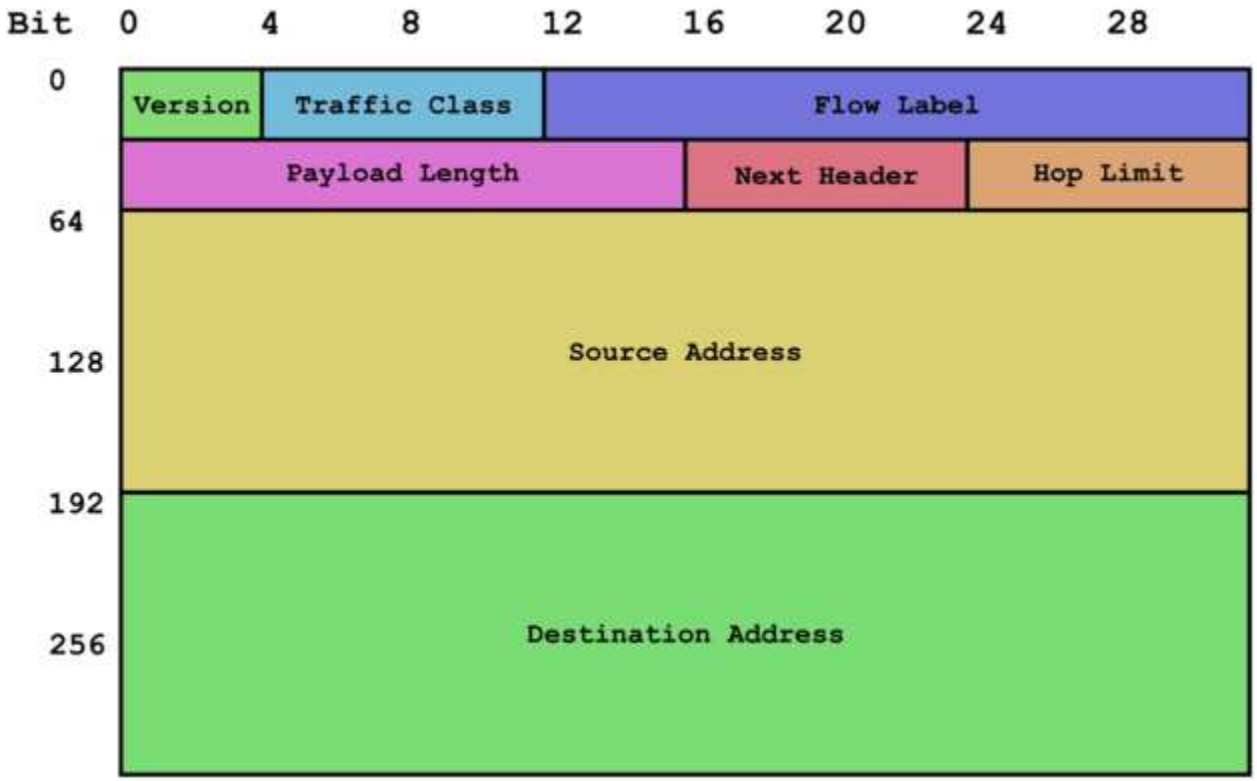
Ponadto, dowolność w przydzielaniu pojedynczych adresów sieci powodowała przeciążenie do granic fizycznych możliwości globalnych routerów internetowych. Wynikało to z faktu przydzielania różnym rozproszonym geograficznie jednostkom dowolnych adresów sieci, które musiały być routowane na poziomie globalnym.

Jednym z projektów zmiany systemu adresowania była koncepcja IPng (IP nowej generacji), która później rozwinęła się w standard IPv6. Niestety, ta koncepcja powstawała wolno i nie nadążała za potrzebami Internetu. Co gorsza, zatwierdzony ostatecznie w 1998 standard IPv6 nie zapewnia interoperacyjności z IPv4. W czasie gdy powstawał nie było jeszcze oczywiste, że w Internecie takiej drastycznej zmiany nie da się przeprowadzić.

Jednym z elementów standardu IPv6 jest nowy system adresowania.

System adresowania IPv6

Adresy IPv6 mają 128 bitów długości. Teoretycznie daje to około 10^{125} różnych adresów. Jednak celem tego systemu nie było wygenerowanie dużej liczby używalnych adresów. Raczej, przestrzeń adresowa ma zapewniać duży nadmiar, pozwalając zarówno na uproszczenie przetwarzanie adresu przez zewnętrzne routery, jak i umożliwienie autokonfiguracji własnych adresów przez komputery.



Routing (trasowanie?)

Routing jest czynnością określania lokalizacji sieci komputerowej na podstawie jej adresu.

Lokalizację rozumiemy tu w sensie połączeń, to znaczy znalezienie ścieżki sieciowej (szeregu połączonych routerów), prowadzącej do lokalizowanej sieci.

Realizacja tej czynności opiera się na związku prefixu adresu sieci z fizyczną lokalizacją sieci. Informacje wymieniane między komputerami znajdującymi ścieżki (routerami) pozwalają im na określanie tych ścieżek przez abstrakcję.

Algorytm routera: (1) jeśli adres jest w mojej podsieci to wysyłam pakiet do docelowego odbiorcy; (2) jeśli tak się składa, że mam w pamięci ścieżkę do podsieci odbiorcy pakietu, wraz z bramą lokalną (routerem) stanowiącą początek tej ścieżki, to przekazuję pakiet temu routerowi.

Szczególnym przypadkiem jest sytuacja, kiedy komputer posiada tzw. ścieżkę domyślną, określającą bramę dla wszystkich adresów, do których nie jest pamiętana indywidualna ścieżka. Jeśli komputer posiada zdefiniowaną taką ścieżkę to wie jak doręczyć wszystkie pakiety.

Routing — tablica ścieżek

Decyzja wyboru ścieżki sieciowej, do której należy wysłać dany pakiet sieciowy, jest podejmowana na podstawie docelowego adresu IP pakietu, i jej wynikiem jest wybór komputera w (jednej z) sieci lokalnej(ych), do której(ych) dany komputer jest podłączony. Routing jest czynnością wykonywaną w ramach protokołu IP (warstwy sieciowej, w nomenklaturze ISO).

Routing realizowany jest w sposób niezwykle prosty: system operacyjny posiada tablicę ścieżek sieciowych, określająca powiązania docelowych adresów IP komputerów i całych sieci, z bramami, czyli adresami IP komputerów w sieci lokalnej, czyli takich, do których przesłanie jest bezpośrednie.

Może istnieć wiele ścieżek w tej tablicy, i wybierana jest zawsze najlepiej dopasowana, to znaczy najbardziej szczegółowa ścieżka zgodna z danym adresem docelowym. W braku takiej ścieżki używana jest specjalna ścieżka domyślna, a gdy jej nie ma, pakietu nie da się wysłać do miejsca przeznaczenia, i routing kończy się niepowodzeniem. Pakiet zostaje zwyczajnie skasowany, natomiast do nadawcy może zostać wysłany komunikat informujący go o błędzie w jego tablicy ścieżek.

Adresy symboliczne

Dla wygody wprowadzono dualną przestrzeń adresów — adresy symboliczne. Są one zorganizowane w hierarchiczną strukturę tzw. domen adresowych. Struktura ta nie ma ograniczeń; domeny położone „niżej" w hierarchii są własnością różnych organizacji, które same dostarczają informacji o domenach w nich zawartych.

Np.: komputer `sequoia.iiar.pwr.edu.pl` (IP:156.17.9.3) należy do domeny `iiar.pwr.edu.pl`, która jest własnością Instytutu Informatyki, Automatyki i Robotyki Politechniki Wrocławskiej, i która otrzymała prawa do tej domeny od Politechniki Wrocławskiej, właściciela domeny `pwr.edu.pl`.

Przestrzeń adresów symbolicznych służy tylko wygodzie ludzkiej pamięci, i istnieje odwzorowanie adresów symbolicznych na adresy numeryczne. Do realizacji tego odwzorowania służy specjalny system DNS (*domain name system*) składający się z sieci serwerów wymieniających informacje o tych odwzorowaniach i serwujących te informacje na życzenie.

Translacja nazw symbolicznych — system DNS

- DNS (*Domain Name System*) — hierarchiczny, rozproszony system nazw symbolicznych w Internecie
- oparty na oddelegowaniu administracji domenami różnym instytucjom, korzystającym z własnych serwerów DNS, automatycznie wymieniającym między sobą informacje o administrowanych przez siebie domenach

  domena — poddrzewo hierarchicznego drzewa nazw
- własności: nadmiarowość, replikacja, buforowanie, duża niezawodność i tolerancja błędów, optymalizacja procesu uzyskiwania odpowiedzi w warunkach rzadkich zmian
- serwer DNS — program, którego zadaniem jest podawanie translacji adresu określonego w zapytaniu klienta, i komunikujący się z innymi serwerami DNS, w celu jej znalezienia
- serwery DNS mogą posiadać redundancję — dla danej domeny można wprowadzić oprócz serwera głównego (**primary**), równoważne serwery dodatkowe (**secondary**)

Serwery systemu DNS

- serwer DNS domyślnie jest **rekurencyjny**; w sytuacji gdy nie zna odpowiedzi na otrzymane zapytanie, sam kontaktuje się z innymi serwerami aby ją uzyskać, i udzielić pytającemu klientowi

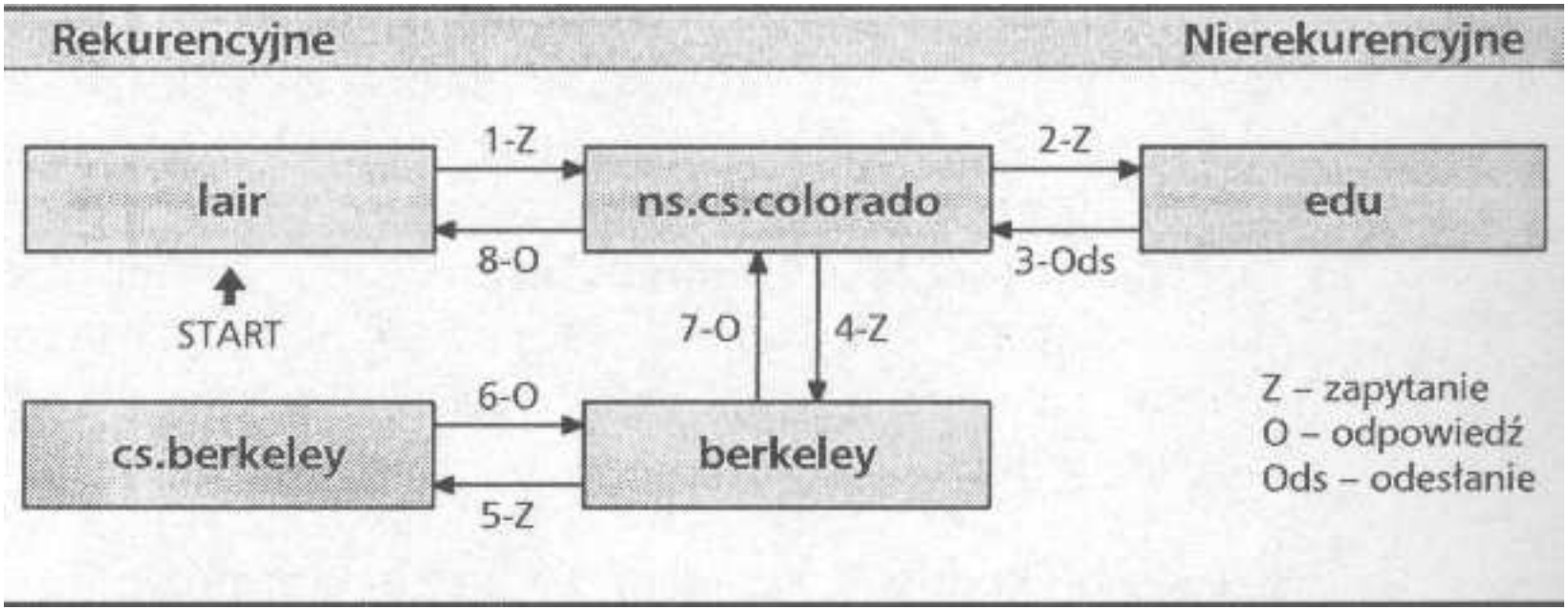
  rekurencyjny serwer jest właściwym rozwiązaniem dla sieci lokalnej, ponieważ pozwala klientom zawsze uzyskiwać odpowiedzi na swoje pytania, a ponadto może przechowywać uzyskane odpowiedzi, i udzielać ich potem kolejnym klientom bez ponownego odpytywania rekurencyjnego

- serwer DNS może być również **nierekurencyjny**; w przypadku nieznajomości odpowiedzi serwer taki nie pyta się innych serwerów, tylko odpowiada tzw. odsyłaczem (ang. *referral*), podającym adres innego, bardziej właściwego dla danej domeny serwera DNS

  serwery DNS wyższego poziomu w hierarchii Internetu (np. serwery główne takich domen jak .com albo .pl) są z zasady nierekurencyjne, więc tym bardziej nie przechowują informacji, które ich nie dotyczą

Dla domen pośrednich pomiędzy siecią lokalną a domeną główną Internetu musimy wybrać pomiędzy pracą rekurencyjną a nierekurencyjną serwera DNS. Jednak nierekurencyjny serwer nie może obsługiwać normalnych klientów, nieprzygotowanych na otrzymanie na swoje zapytanie odpowiedzi w postaci odsyłacza.

Przykład sekwencji odwołań do serwerów DNS dla zapytania o nazwę `mammoth.cs.berkeley.edu` wykonanego na komputerze `lair.cs.colorado.edu`:



Serwery DNS

primary — jest tylko jeden taki serwer dla strefy (ang. *zone*); strefa jest częścią domeny administrowaną przez serwer

secondary — takich może być dla danej strefy wiele, automatycznie aktualizują one swoje dane i ich odpowiedź jest równoważna odpowiedzi serwera *primary*

caching-only — nie jest właściwym źródłem informacji o żadnej strefie, nie posiada własnych informacji tylko realizuje funkcję rekurencyjnego odpytywania innych serwerów i przechowuje informacje przez dozwolony okres; można go uważać za rodzaj aktywnego klienta; jeśli nie chcemy zakładać w danym systemie serwera DNS, ale chcemy zaoszczędzić na ruchu sieciowym do zewnętrznych serwerów DNS, to możemy założyć właśnie serwer *caching-only*

Jeden serwer (uruchomiona instancja programu) może być serwerem primary dla jednej strefy (lub kilku), i serwerem secondary dla grupy innych stref, albo może być czystym serwerem caching-only.

System DNS zaprojektowany w połowie lat 1980-tych jest przykładem rozproszonego systemu o dużej niezawodności, poprawnie zabezpieczającego serwis translacji adresów symbolicznych w warunkach rozległego, niedeterministycznego Internetu. System poprawnie przetrwał rewolucyjny rozwój Internetu od początku lat 1990-tych, kiedy całkowicie zmieniły się technologie, prędkość, niezawodność, i wymagania stawiane Internetowi.

Jednej cechy, której nie przewidziano w tym systemie jest bezpieczeństwo. System powstał w czasie, gdy nie istniały ani obecne zagrożenia ani wymagania dotyczące bezpieczeństwa. Rozproszoność i redundancja tego systemu powoduje łatwość przeprowadzania ataków takich jak podszywanie się.

Bezpieczeństwo w środowisku sieciowym

Podstawowe zagadnienia i wymagania bezpieczeństwa:

poufność

Dotyczy zabezpieczenia treści przechowywanych i transmitowanych w sieci przed dostępem osób niepowołanych.

weryfikacja

Możliwość stwierdzenia czy zdalny partner w komunikacji sieciowej jest tym, za którego się powołuje, że otrzymany dokument jest na pewno wierną kopią dokumentu utworzonego przez zdalnego partnera

niezawodność

Gwarancja utrzymania komunikacji pomimo zakłóceń spowodowanych świadomie, lub nieświadomie (np. w wyniku czyjegoś błędu) przez czynniki trzecie, jak również przez awarie sprzętu i oprogramowania.

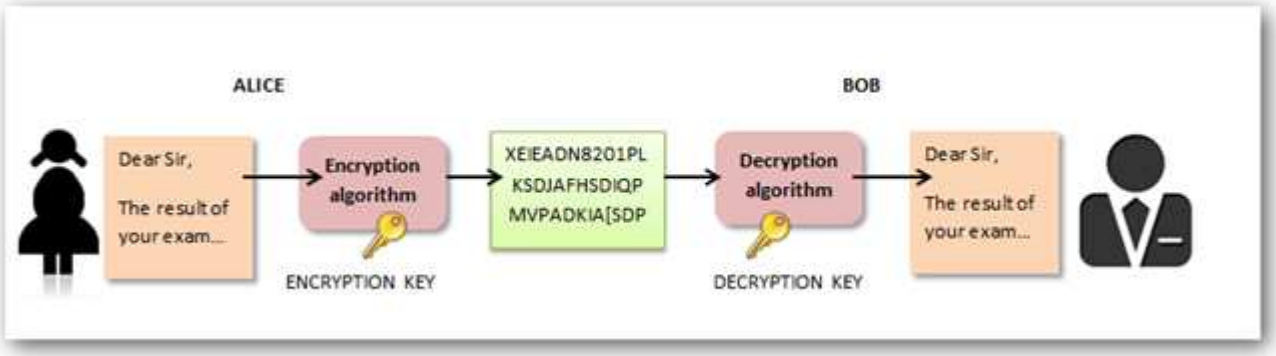
Zagrożenia i linie obrony

- zagrożenia:
  - włamania przez serwery sieciowe obsługujące połączenia z zewnątrz
  - włamania na konta użytkowników; do zwykłych zagrożeń polegających na groźbie zniszczenia danych wartościowych lub ujawnienia danych tajnych, dochodzi jeszcze stworzenie furtki do ataku na system
  - ataki typu DOS (*denial of service*)

- linie obrony:
  - monitorowanie połączeń sieciowych, wykrywanie dziur w systemie wykorzystanych w udanych atakach, zatykanie tych dziur
  - monitorowanie aktywności w systemie i poczynań użytkowników, pomaganie im w utrzymaniu bezpieczeństwa ich kont
  - prewencyjne blokowanie niektórych usług sieciowych (niepotrzebne serwisy, podejrzane adresy)
  - szyfrowanie połączeń
  - *firewalling* — zapory sieciowe
  - archiwizacja plików !!!

Szyfrowanie

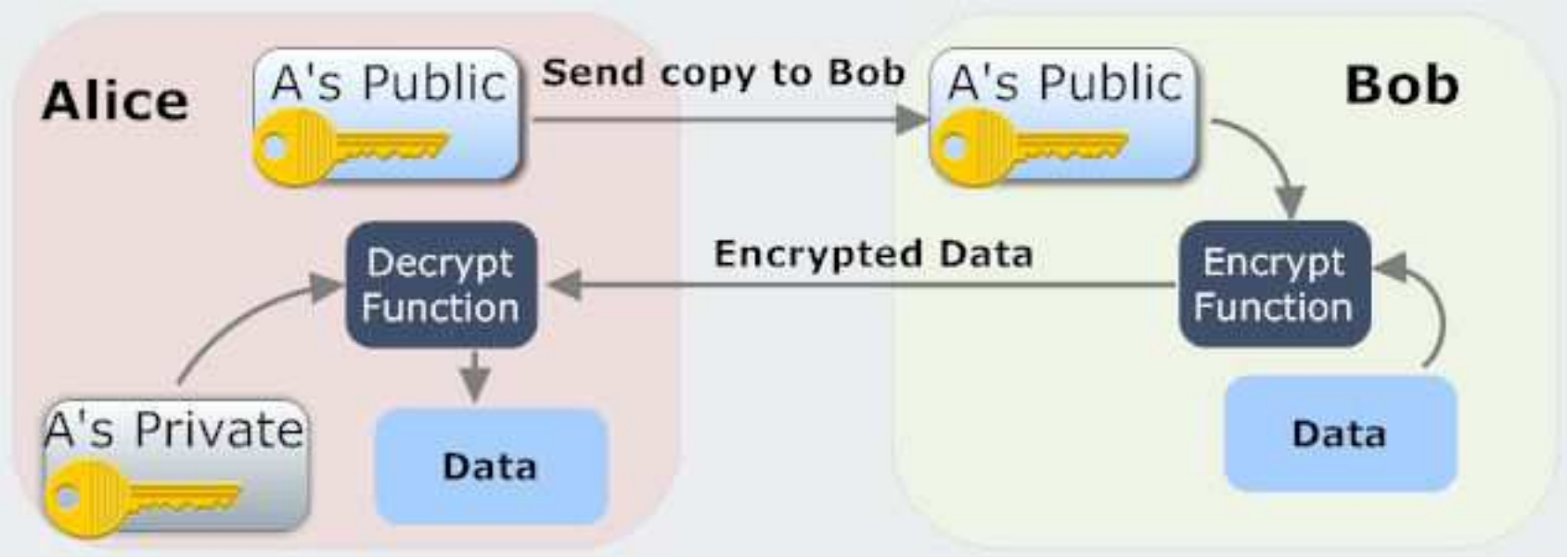
Jedną z najskuteczniejszych technologii stosowanych w celu utrzymania bezpieczeństwa współczesnych systemów sieciowych jest szyfrowanie. Jest ono stosowane w odniesieniu do pojedynczych dokumentów, jak i ciągłych transmisji sieciowych. Szyfrowanie umożliwia również stosowanie podpisów cyfrowych umożliwiając potwierdzanie integralności dokumentów oraz tożsamości partnera.



Tradycyjnie szyfrowanie, stosowane od starożytności, wykorzystywało technologie szyfrowania **symetrycznego**. Jego istotą jest identyczność kluczy (szyfrów) służących do szyfrowania i deszyfrowania. Bezpieczeństwo tego systemu opiera się na tajności kluczy, co stanowi zarazem jego podstawową słabość. W momencie gdy zachodzi konieczność wprowadzenia nowych kluczy, potrzebna jest metoda ich bezpiecznego przekazania sobie przez partnerów.

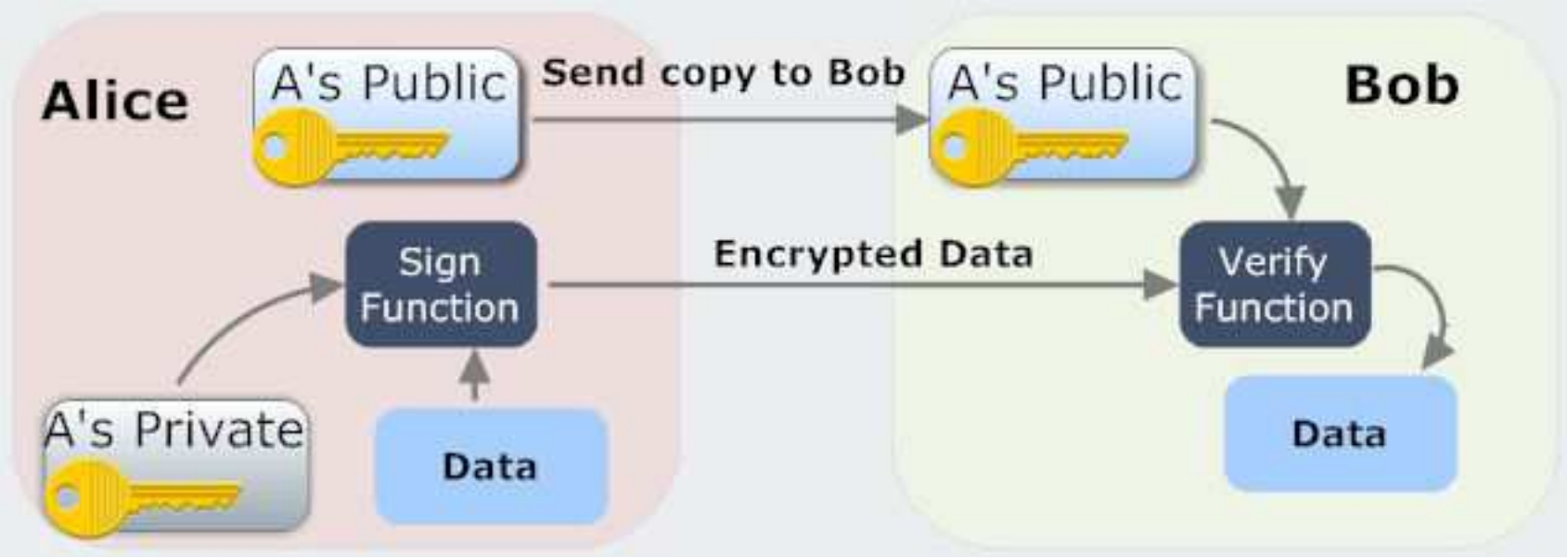
System klucza publicznego

Najważniejszą technologią szyfrowania stosowaną w systemach i sieciach komputerowych jest **szyfrowanie asymetryczne**, zwane również **systemem klucza publicznego**. Klucz szyfrowania każdej jednostki (osoby lub instytucji) składa się z dwóch części: **klucza publicznego**, który jest jawny i może być przesyłany otwartymi kanałami, oraz **klucza prywatnego**, który jest tajny i nigdzie nie wysyłany. Każdy może zaszyfrować wiadomość kluczem publicznym odbiorcy, ale odszyfrować ją będzie mógł tylko właściciel klucza znający jego część prywatną.



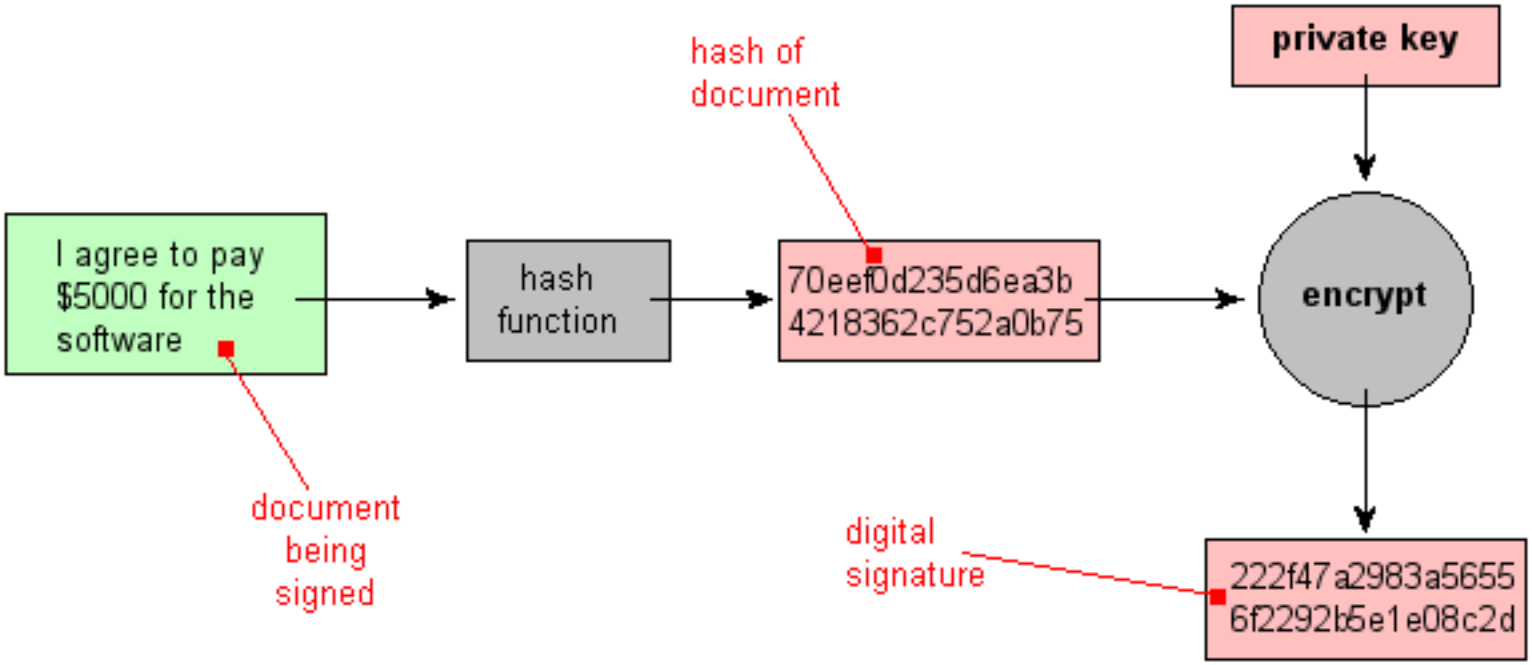
Podpisy cyfrowe

System klucza publicznego umożliwia łatwe wprowadzenie dodatkowej ważnej funkcji, jaką są **podpisy cyfrowe**. Polega ona na zaszyfrowaniu komunikatu przez nadawcę swoim własnym kluczem prywatnym. Taki komunikat może być odszyfrowany przez każdego, ale tylko kluczem publicznym nadawcy. Zgodność odszyfrowanego komunikatu z jego pełną otrzymaną wersją dowodzi, że to określona osoba zaszyfrowała wiadomość, oraz, że treść wiadomości jest nieprzekłamana.



Skróty kryptograficzne

Dodanie do wysyłanego komunikatu jego zaszyfrowanej wersji jako podpisu działa, ale niekoniecznie jest wygodne. Na przykład, dla długich komunikatów (takich jak film wideo) podpis byłby niepotrzebnie długi. Istnieją metody generowania **skrótów kryptograficznych** (ang. *digest* albo *hash*), które z dokumentu cyfrowego dowolnej długości tworzą krótki plik cyfrowy w taki sposób, że jest bardzo mało prawdopodobne, aby z innego sensownego dokumentu utworzyć identyczny skrót. Skrót kryptograficzny po zaszyfrowaniu własnym kluczem publicznym stanowi wygodniejszą wersję podpisu cyfrowego.



Skróty kryptograficzne (cd.)

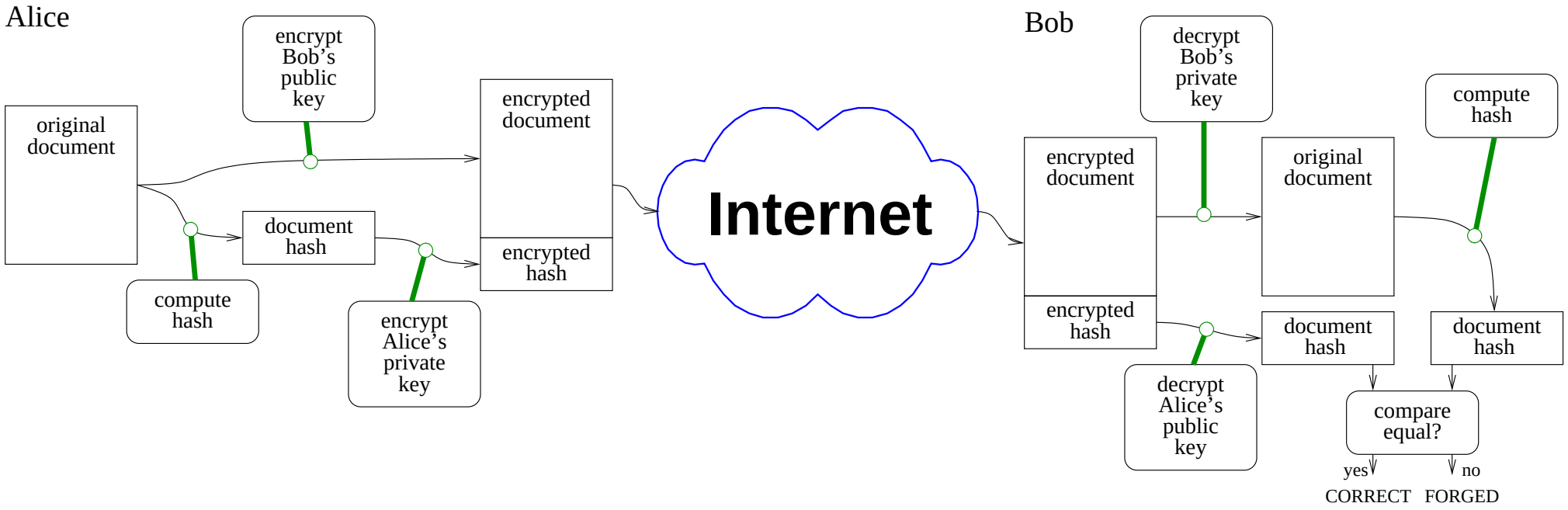
Zadaniem skrótu kryptograficznego jest utworzyć ciąg bitów, który będzie maksymalnie jednoznacznie związany z oryginalnym dokumentem, który z maksymalnym prawdopodobieństwem będzie różny dla różnych dokumentów, ale który będzie miał stałą długość. Algorytmy generacji takich skrótów nazywane są również funkcjami jednokierunkowymi albo mieszającymi.

Na przykład, popularny przez wiele lat algorytm skrótu kryptograficznego MD5 generuje ciągi 128-bitowe, często kodowane w postaci 32-znakowych napisów szesnastkowych (heksadecymalnych). Inny popularny algorytm SHA-1 generuje ciągi 16-bitowe, kodowane jako napisy heksadecymalne 40-znakowe.

Kryptografia silnie się rozwija. Istniejące algorytmy szyfrowania są intensywnie badane i nowe rozwijane. Na przykład, w 2011 opublikowano metodę ataku na algorytm SHA-1 pozwalający wygenerować kolizję (alternatywny ciąg bajtów dający tę samą wartość skrótu SHA-1). Metoda wymaga 2^{65} operacji i nikomu nie udało się jeszcze wygenerować takiej kolizji. Pomimo to główni producenci oprogramowania (Microsoft, Google, Mozilla) ogłosili, że od roku 2017 ich systemy nie będą akceptowały certyfikatów opartych na skrótach SHA-1. Istnieje jednak rodzina znacznie bezpieczniejszych algorytmów SHA-2.

Szyfrowanie i podpisywanie

Zastosowanie skrótów kryptograficznych jest zatem standardową i wygodną metodą podpisywania cyfrowego dokumentów. Poniżej przedstawiona jest pełna procedura szyfrowania dokumentu do bezpiecznej transmisji przez sieć, oraz generowania podpisu cyfrowego w celu sprawdzenia integralności dokumentu i wiarygodności jego autorstwa:



Dokładna zgodność obliczonego przez odbiorcę skrótu z wersją rozszyfrowaną z dokumentu świadczy o zgodności dokumentu z wersją wysłaną przez nadawcę.

System klucza publicznego (cd.)

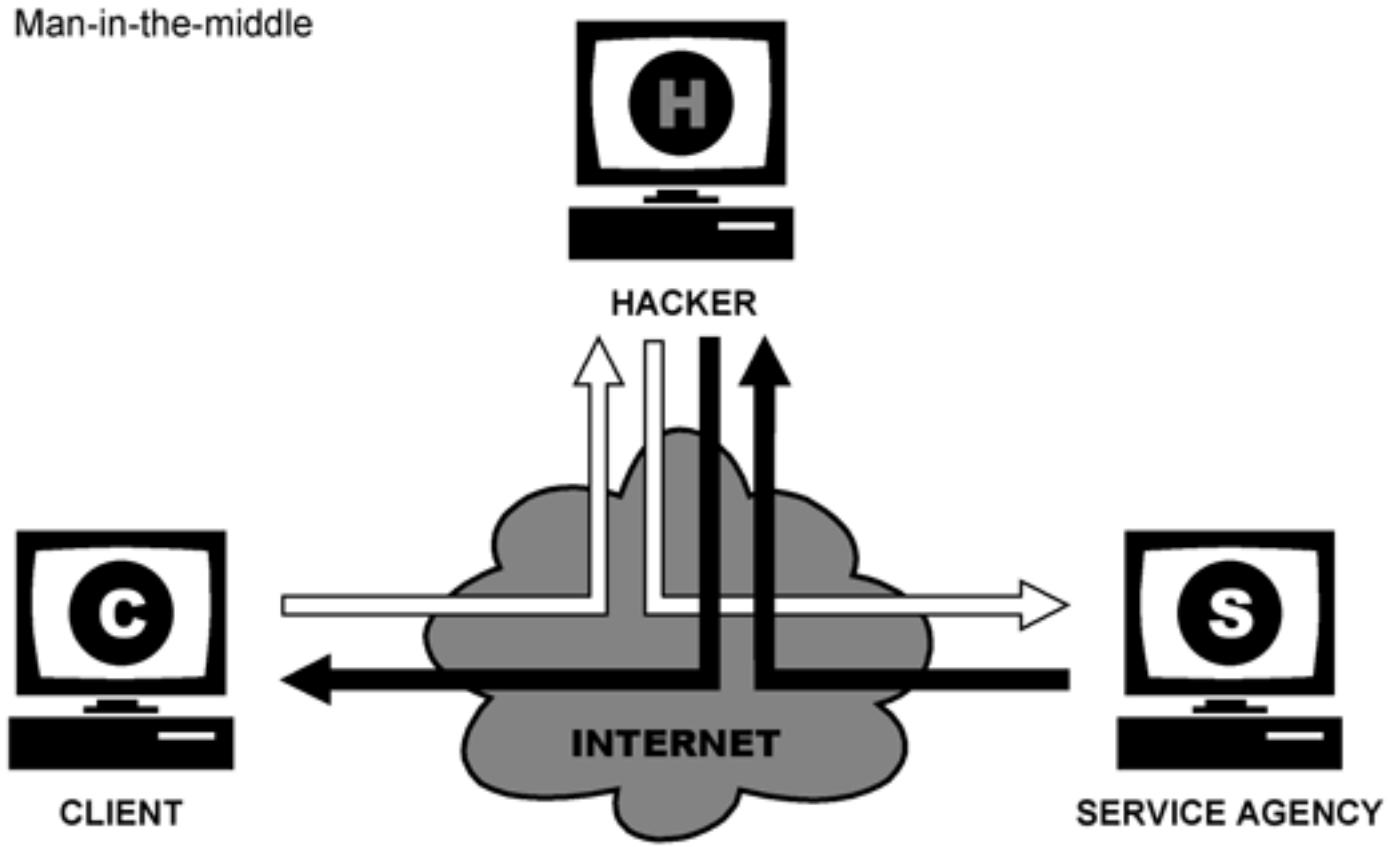
Podsumujmy wiadomości o systemie kluczy publicznych. Pozwala on na zaszyfrowanie komunikatu kluczem publicznym odbiorcy, i jednocześnie wygenerowanie podpisu cyfrowego dokumentu, czyli skrótu kryptograficznego oryginalnego dokumentu zaszyfrowanego kluczem prywatnym nadawcy. Odbiorca może odszyfrować wiadomość swoim kluczem prywatnym, następnie obliczyć jej skrót, i porównać go z otrzymanym od nadawcy skrótem, rozszyfrowanym kluczem publicznym nadawcy. W ten sposób oryginalna wiadomość była transmitowana w postaci zakodowanej, i odbiorca ma jednocześnie gwarancję, że wiadomość jest dokładnie zgodna z nadanym tekstem,

Teoretycznie technologia klucza publicznego rozwiązuje problem dystrybucji kluczy szyfrowania. Klucze można przesyłać jawnie otwartymi kanałami. Każdy może np. opublikować swój klucz na stronie internetowej, albo rozsyłać go elektronicznie bez obawy ujawnienia tajnych danych.

Jednak w masowym użyciu, z jakim mamy do czynienia we współczesnym Internecie, pojawiają się dodatkowe problemy. Klucze ulegają utraceniu i muszą być sprawnie unieważniane i rozsyłane nowe. Niezawodnie można przesłać klucz publiczny przyjacielowi (lub przyjaciółce), ale jak upewnić się, że klucz publiczny banku, firmy Paypal, albo urzędu skarbowego nie został przekłamany?

Atak pośrednika

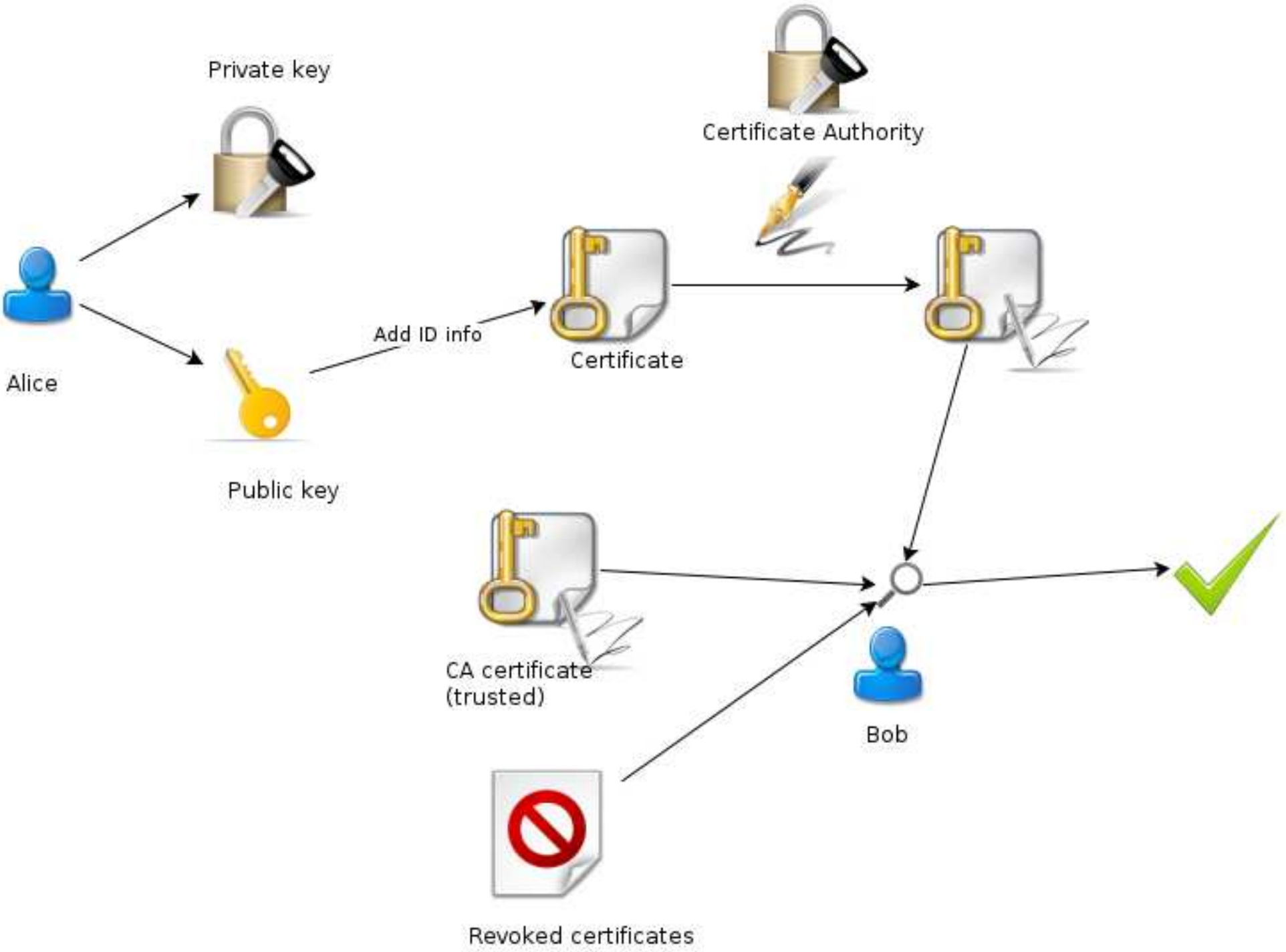
Niestety, w Internecie rozwinęły się liczne techniki ataków wykorzystujące dziury w zabezpieczeniach. Jeżeli komuś uda się przeprowadzić atak w chwili pobierania kluczy publicznych do komunikacji między dwoma partnerami, to może łatwo przechwycić, a nawet sfałszować, całą komunikację między nimi wykorzystując schemat zwany **atakiem pośrednika** (ang. *man-in-the-middle attack*).



Infrastruktura klucza publicznego (PKI)

Z powyższych względów system klucza publicznego został w Internecie rozbudowany do **Infrastruktury Klucza Publicznego** (PKI — *Public Key Infrastructure*). Wymaga ona stworzenia zaufanej instytucji zwanej Centrum (albo Urzędem) Certyfikacji CA (ang. *Certification Authority*). Jego rolą jest generowanie **certyfikatów** potwierdzających, że dany klucz publiczny jest rzeczywiście kluczem osoby lub instytucji, która podaje się za właściciela klucza. Ponieważ certyfikat jest podpisany przez Centrum, więc każdy może sprawdzić, że przesłany klucz publiczny innej jednostki jest właściwy.

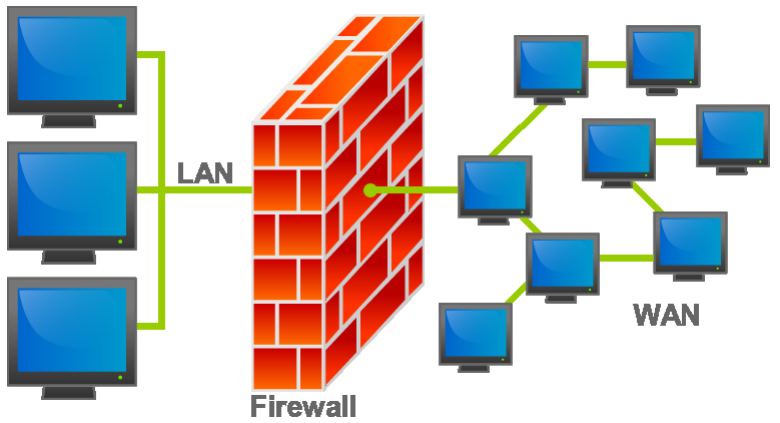
Jednocześnie Centrum przechowuje informacje o unieważnionych kluczach, i pełni szereg dalszych funkcji przydatnych w procesie szyfrowania i podpisywania dokumentów między partnerami w Internecie. Z tego powodu Centrum Certyfikacji musi samo być jednostką w pełni zaufaną, którego ani tożsamość, ani wiarygodność kluczy szyfrowania nie budzą wątpliwości. Na przykład, przeglądarki internetowe mają wbudowane w sobie listy istniejących na świecie Centrów Certyfikacji, i normalnie nie przyjmują certyfikatów podpisanych przez Centrum Certyfikacji spoza tej listy.


Private key
Certificate Authority
Alice
Add ID info
Certificate
Public key
CA certificate
(trusted)
Bob
Revoked certificates

Zapory sieciowe

W środowisku z wieloma komputerami i użytkownikami, zapewnienie im wszystkim indywidualnej ochrony i bezpieczeństwa może być przedsięwzięciem trudnym.

W takich sytuacjach, w konkretnej organizacji, bardziej ekonomiczne może być kontrolowanie dostępu do całej sieci danej organizacji w jednym punkcie połączenia ze światem, typowo bramie sieciowej lub routerze, zwanym wtedy zaporą sieciową (*firewall*).



Funkcje zapory sieciowej:

- filtrowanie ruchu wchodzącego i/lub wychodzącego,
- zapewnienie dostępu do wnętrza sieci autoryzowanym użytkownikom,
- monitorowanie i rejestrowanie połączeń.

Funkcjonowanie zapory sieciowej

- Zapora sieciowa pracująca jako filtr pakietów sprawdza każdy pakiet sieciowy i może:
  - przepuścić pakiet do odbiorcy w sieci wewnętrznej
  - odrzucić pakiet całkowicie
  - obsłużyć pakiet w ramach systemu zapory
- Zapora sieciowa może jednocześnie, albo alternatywnie, działać jako agent pośredni w protokołach, łącząc użytkownika sieci wewnętrznej ze światem zewnętrznym np. przekaźnik pocztowy (ang. *mail relay*), albo pośredni serwer WWW (ang. *web proxy*); zapora może:
  - implementować tylko „bezpieczny" podzbiór protokołu
  - dokonać kompleksowych sprawdzeń poprawności komunikacji
  - używać wyłącznie mechanizmów minimalizujących ryzyko
  - wykonywać swe operacje w specjalnie izolowanym środowisku
- Zapora sieciowa może również być wydzieloną maszyną do komunikacji z siecią zewnętrzną, dopuszczając połączenia zabronione w sieci wewnętrznej

Warianty zapory sieciowej

- Zapora poziomu sieciowego:
  - urządzenie przepuszczające lub blokujące pakiety zmierzające do wnętrza i na zewnątrz sieci chronionej, np. router
  - w najprostszym przypadku filtruje pakiety jedynie w oparciu o adres nadawcy, odbiorcy, i numer portu, zatem nie jest zdolny do rozpoznania dobrze zamaskowanych ataków
  - znacznie trudniejsze, choć teoretycznie możliwe, jest śledzenie stanu połączeń, przepływających danych, itp.
  - szybki, przeźroczysty dla użytkowników
- Zapora poziomu aplikacji:
  - zapewnia wewnątrz sieci chronionej możliwość pracy aplikacji sieciowych, tzn. łączenia się z serwerami na zewnątrz
  - realizacja może sprowadzać się do tzw. „serwera proxy" który pracuje na zaporze sieciowej i realizuje na zewnątrz żądania zgłaszane przez komputery wewnątrz sieci chronionej
  - umożliwia implementację precyzyjnych reguł dostępu i rejestrowania połączeń
  - zwykle nie są przeźroczyste dla użytkownika

Odpowiedzialność i etyka

Funkcjonowanie naszej cywilizacji coraz bardziej zależy od poprawnej pracy komputerów i sieci komputerowych. Dotyczy to w szczególności wszelkich komercyjnych sieci telekomunikacyjnych, infrastruktur medycznych i ratowniczych, meteorologicznych i geologicznych, nie wspominając o starym, poczciwym Internecie.

Zakłócenia w pracy tych sieci mogą prowadzić do katastrof, utraty życia, strat, przestępstw, itp. Dlatego studiowanie bezpieczeństwa sieci komputerowych jest ważnym działem nauki i techniki.

Ale nie tylko włamywanie się, zakłócanie pracy, niszczenie, i kradzieże są zagrożeniem. Są nim również wszelkie nadużycia wynikające z wykorzystania posiadanych uprawnień lub możliwości technicznych.

Rozważmy na przykład służby specjalne podsłuchujące prywatnych rozmów bez uzasadnienia, albo pracodawców odczytujących emaile przesyłane sobie przez pracowników, itp. Wydaje się to nadużyciem; zresztą jest zwykle niezgodne z prawem. Ale taki sam charakter ma ściąganie nielegalnych treści z Internetu (książek, filmów, muzyki, programów), albo co gorsza udostępnianie ich.