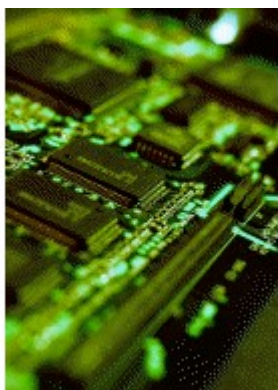




Systemy Operacyjne i Sieci Komputerowe



Sprzęt
komputerowy

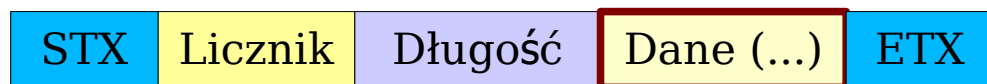
System Operacyjny
+
Programy

Łatwe
użytkowanie

Prowadzący: Robert Szmurło
szmurlor@iem.pw.edu.pl
GE 229



Zasada działania protokołu sieciowego – sieci pakietowe



Schematyczna
ramka pakietu.

- **Licznik** komunikatów - licznik używany aby zabezpieczyć systemy przed kilkukrotnym analizowaniem tych samych danych
- **Długość** danych - wskaźnik gdzie powinien wystąpić ETX w wiadomości
 - **STX** - bajt o wartości: 2 (znacznik początku pakietu)
 - **ETX** - bajt o wartości: 3 (znacznik końca pakietu)
 - **SYN** - bajt o wartości; 22
 - **ACK** - bajt o wartości: 6 - (wysyłany aby potwierdzić dotarcie wiadomości)
- Ramka przykładowego pakietu:
 - |STX|Licznik|Długosc|...tresc...|ETX



Scenariusz Komunikacji - Sukces

- Zakładamy pewien stan początkowy, czyli stan liczników.

STX	LICZNIK	DLUGOSC	treść pakietu	ETX
-----	---------	---------	---------------	-----

- Zakładamy stan licznika Nadawcy: 4

- Wiadomość wysłana, razem z ramką: "204LIPA3"

- Zakładamy, że wiadomość dociera,

- Jeżeli wartość licznika w wiadomości jest **większa lub równa** licznikowi odbiorcy wówczas odbiorca przyjmuje do analizy odebrane dane.

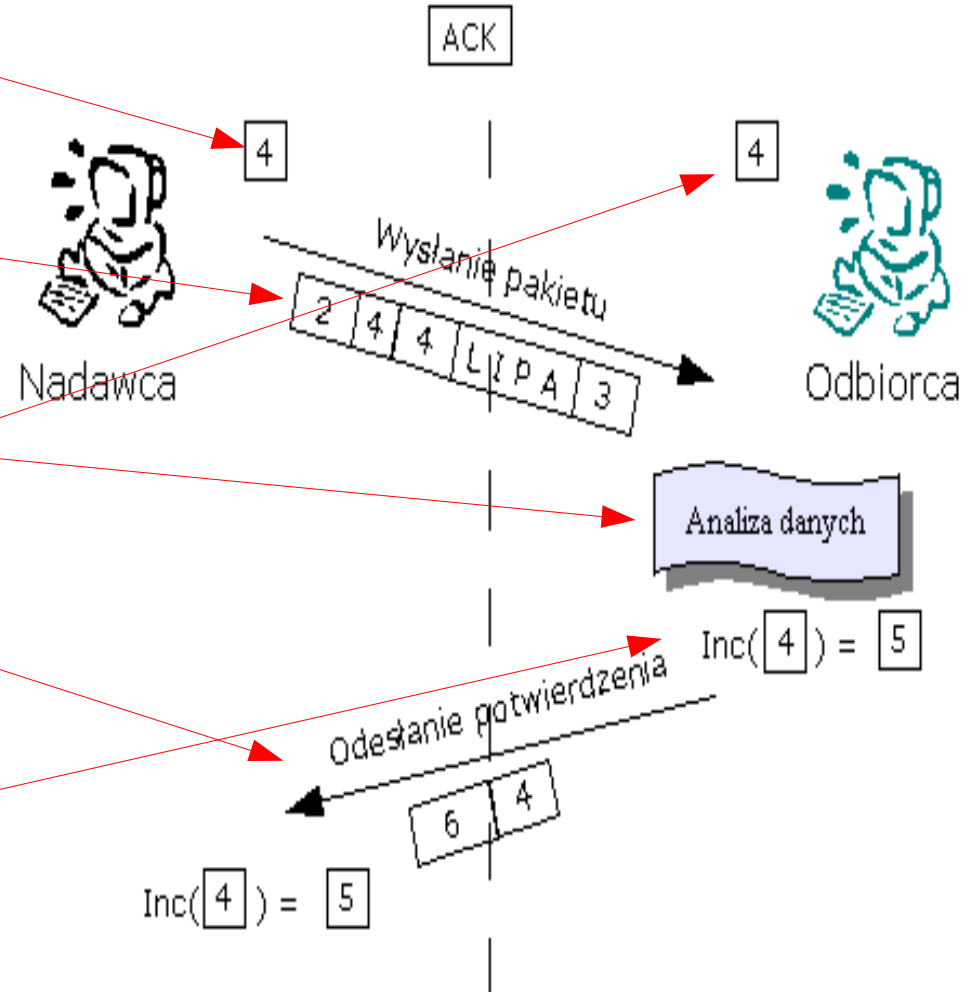
- Odbiorca wysyła potwierdzenie dołączając na końcu numer licznika który potwierdza, "64", cyfra 6 to po prostu ACK.

- Natychmiast po wysłaniu, Odbiorca inkrementuje swój licznik ($\text{inc}(4) = 5$),

- Zakładamy, że potwierdzenie dociera.

- Nadawca inkrementuje licznik ($\text{Inc}(4) = 5$).

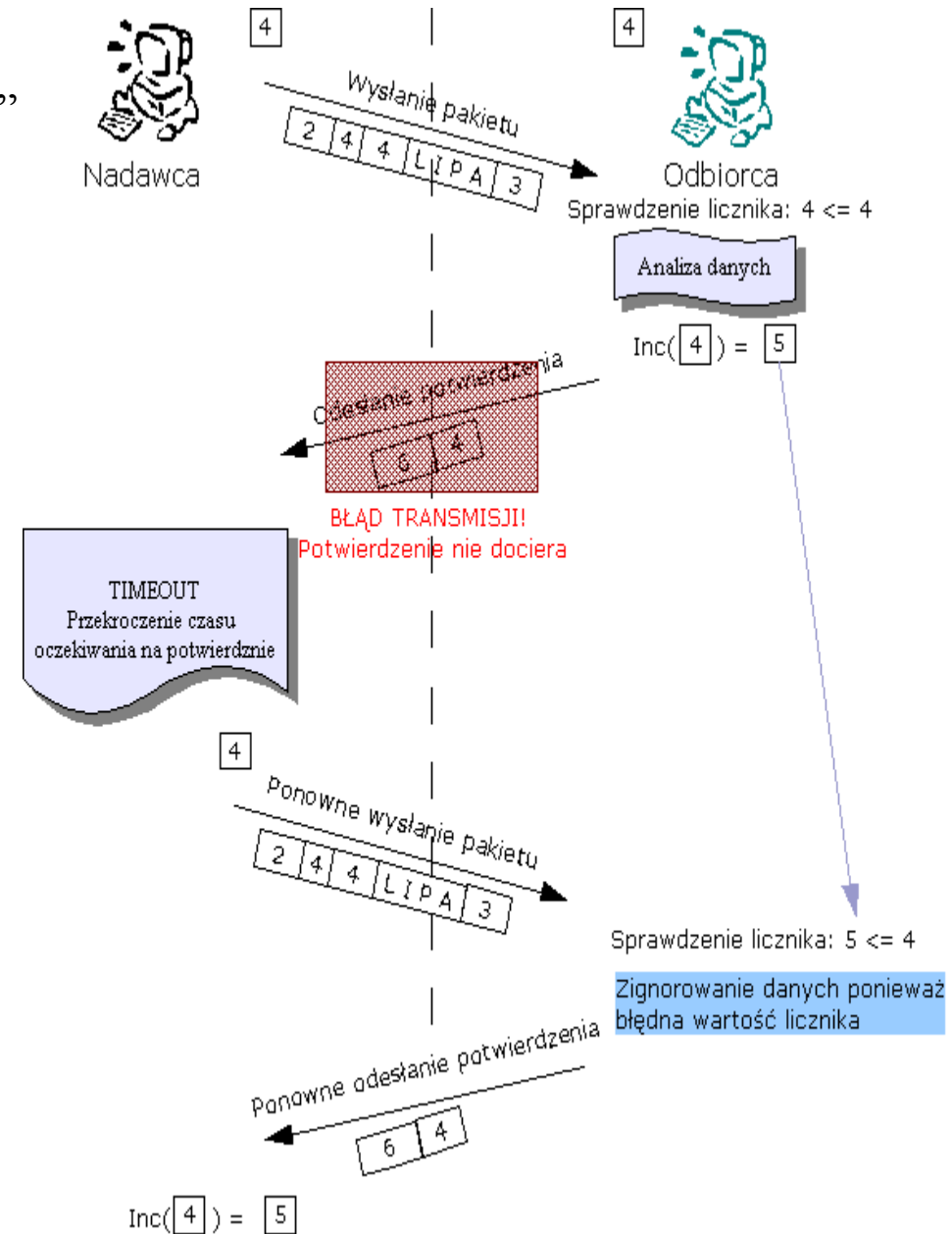
- Przy następnym pakiecie procedura przebiega analogicznie.





Scenariusz 2 – Błąd potwierdzenia

- Zakładamy stan licznika Nadawcy: 4
- Wiadomość wysłana, razem z ramką: “204LIPA3”
- Wiadomość dociera,
- Jeżeli wartość licznika w wiadomości jest \geq od licznika odbiorcy wówczas odbiorca przyjmuje dane do analizy.
- Odbiorca wysyła potwierdzenie dołączając na końcu numer licznika który potwierdza, (64)
- Odbiorca inkrementuje swój licznik ($\text{inc}(4) = 5$),
- Potwierdzenie nie dociera,
- (TIMEOUT) - przekroczenie czasu oczekiwania na potwierdzenie przez nadawcę.
- Wiadomość wysłana ponownie (z tym samym licznikiem == 4)
- Odbiorca sprawdza licznik i ignoruje wiadomość.
- Odbiorca wysyła potwierdzenie po raz drugi, (ze starą wartością licznika)
- Potwierdzenie dociera, Nadawca inkrementuje licznik ($\text{inc}(4) = 5$)





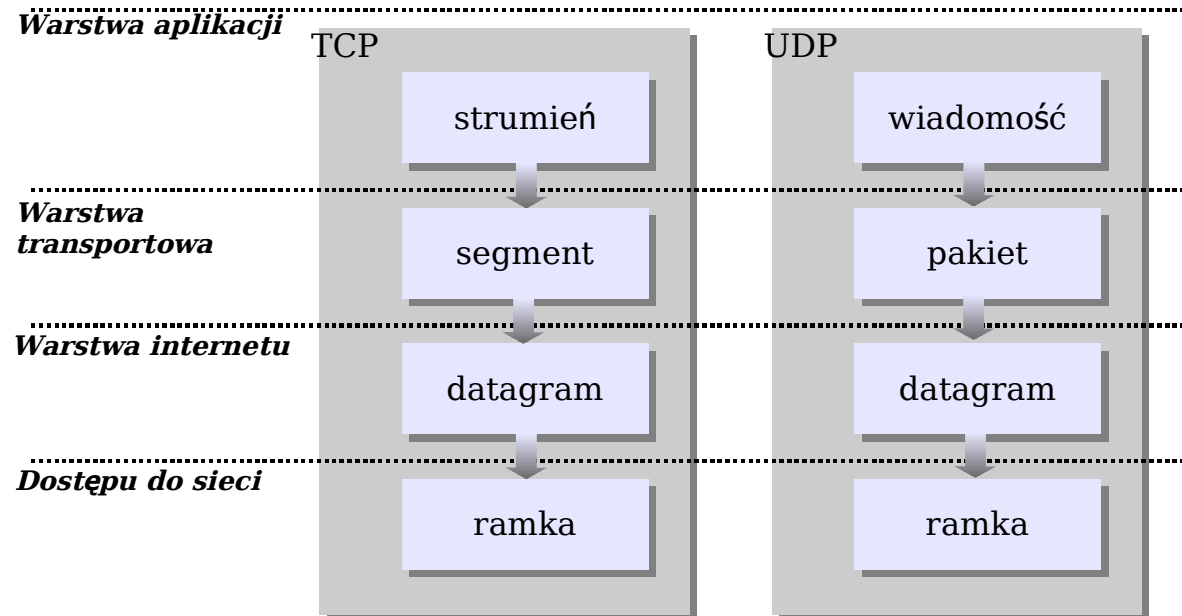
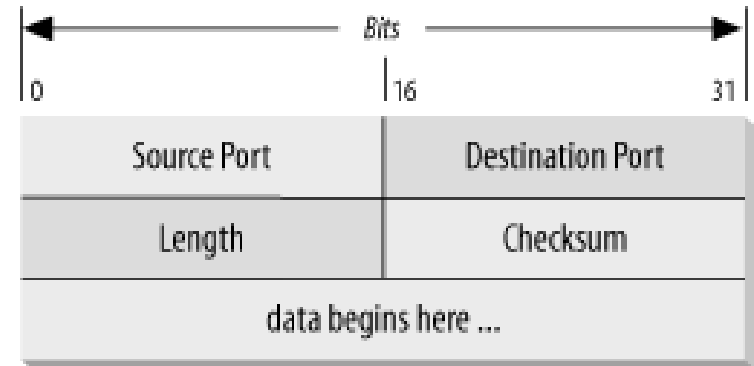
Scenariusz 3 – Błąd transmisji

- Wiadomość wysłana,
 - Wiadomość nie dociera,
 - (TIMEOUT) u nadawcy,
-
- Wiadomość wysłana,
 - Wiadomość nie dociera,
 - (TIMEOUT) u nadawcy,
-
- Wiadomość wysłana,
 - Wiadomość nie dociera,
 - (TIMEOUT) u nadawcy,
-
- KOMUNIKAT O BŁĘDZIE TRANSMISJI



TCP i UDP

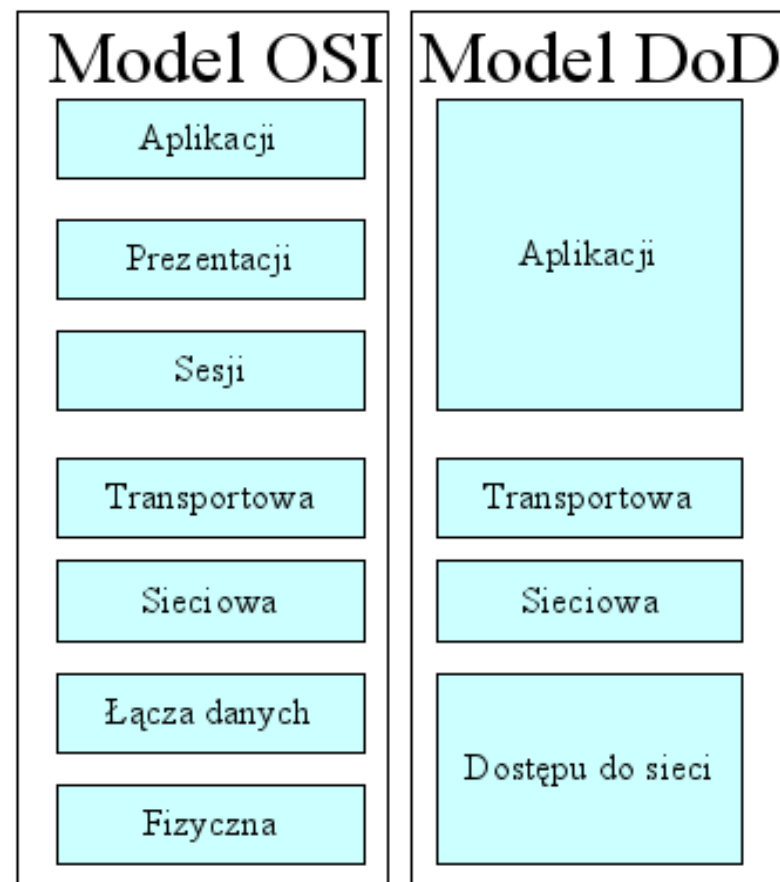
- **UDP**: User Datagram Protocol,
- **Prostszy i wydajniejszy** niż TCP,
- **Nie gwarantuje** dotarcia wiadomości,
- **Bezpołączeniowy** (nie ma sesji, każdy pakiet jest przesyłany osobno),
- Używany najczęściej przy komunikacji **Strumieniowej** (media, VoIP)





Protokoły sieciowe z podziałem na Warstwy w których pracują

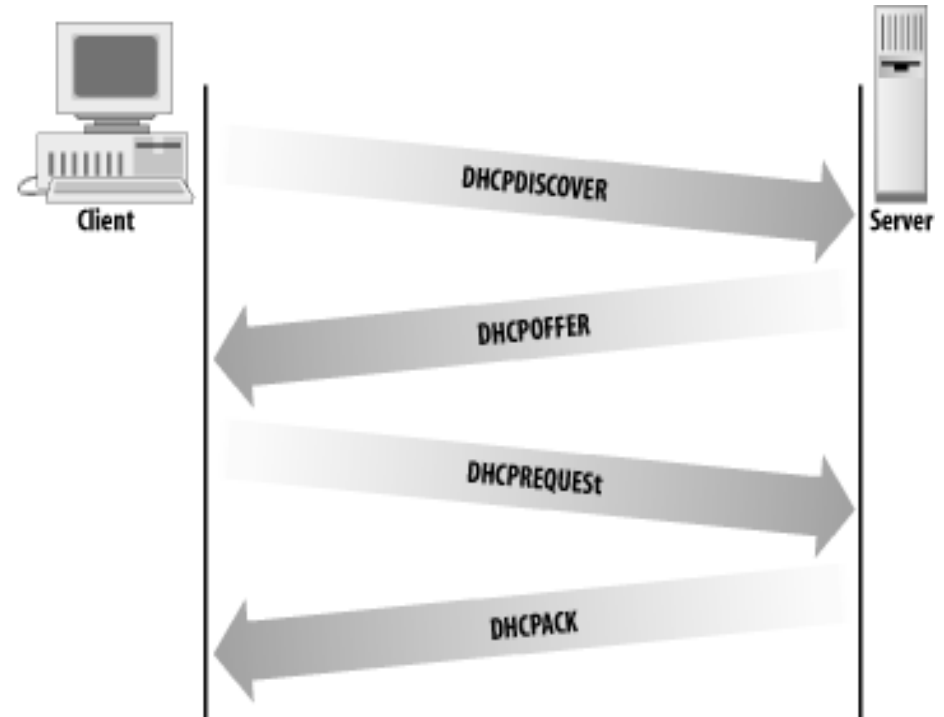
- **Warstwa aplikacji:** DNS, ED2K, FTP, HTTP, HTTPS, IMAP, IRC, NCP, NetBIOS, NWLink, NTP, POP3, RPC, SMTP, SMB, SSH, Telnet, X.500,
- **Warstwa transportowa:** NetBEUI, IPX, SSL, TCP, UDP,
- **Warstwa sieciowa:** ARP, IP, ICMP, IPsec, NAT
- **Warstwa dostępu do sieci:** 10BASE-T, 802.11b/g WiFi, ADSL, DHCP, Ethernet, ISDN, PPP, RS-232, SLIP, Token Ring





Warstwa Dostępu do Sieci: np.: DHCP

- DHCP (ang. Dynamic Host Configuration Protocol) to protokół komunikacyjny umożliwiający komputerom uzyskanie od serwera danych konfiguracyjnych, np. adresu IP hosta, adresu IP bramy sieciowej, adresu serwera DNS, maski sieci, i innych.
- Protokół **DHCP** opisuje trzy techniki przydzielania adresów IP:



- **przydzielanie ręczne** oparte na tablicy adresów MAC oraz odpowiednich dla nich adresów IP. Jest ona tworzona przez administratora serwera DHCP. W takiej sytuacji prawo do pracy w sieci mają tylko komputery zarejestrowane wcześniej przez obsługę systemu.
- **przydzielanie automatyczne**, gdzie wolne adresy IP z zakresu ustalonego przez administratora są przydzielane kolejnym zgłaszającym się po nie klientom.
- **przydzielanie dynamiczne**, pozwalające na ponowne użycie adresów IP. Administrator sieci nadaje zakres adresów IP do rozdzielania. Automatycznie pobierane adresy są udostępniane na **określony czas**: LEASE TIME PERIOD.



Przykład SMTP: Simple Mail Transfer Protocol

- **SMTP** (*ang. Simple Mail Transfer Protocol*) - protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w internecie.
- SMTP to względnie prosty, tekstowy protokół, w którym określa się **co najmniej jednego odbiorcę wiadomości** (w większości przypadków weryfikowane jest jego istnienie), a następnie przekazuje **treść wiadomości**. Łatwo przetestować serwer SMTP przy użyciu programu telnet.
- Protokół ten nie radził sobie dobrze z plikami binarnymi, ponieważ stworzony był w oparciu o czysty tekst ASCII. W celu kodowania plików binarnych do przesyłu przez SMTP stworzono standardy takie jak MIME.
(Przykład, który używaliśmy do opisu warstwy prezentacji)
- Przykład sesji SMTP:

```
→ 220 serwer ESMTX Exim 4.43 Wed, 12 Jan 2005 23:14:13 +0100
→ helo serwer.email.com
→ 250 uzytkownik.internet.com Hello uzytkownik at uzytkownik.internet.com [1.1.1.1]
→ mail from: <nadawca@domena.com>
→ 250 OK
→ rcpt to: <odbiorca@domena.com>
→ 250 Accepted
→ data
→ 354 Enter message, ending with "." on a line by itself
→ From: nadawca@domena.com
→ To: odbiorca@domena.com

→ tresc wiadomosci
→ .
→ 250 OK id=1Coql6-0003Qi-MP
→ quit
→ 221 serwer.email.com closing connection
```



POP – Post Office Protocol (POP3)

- Również protokół tekstowy. Przykładowa sesja:

```
% telnet volt.iem.pw.edu.pl 110
Trying 172.16.12.1 ...
Connected to volt.iem.pw.edu.pl.
Escape character is '^]'.
+OK volt POP3 Server Process 3.3(1) at Mon 8-Nov-2006 4:48PM-EDT
USER szmurlor
+OK User name (szmurlor) ok. Password, please.
PASS legia01
+OK 3 messages in folder NEWMAIL (V3.3 Rev B04)
STAT
+OK 3 459
RETR 1
+OK 146 octets
...Pełna treść pierwszej wiadomości...
DELE 1
+OK message # 1 deleted
RETR 2
+OK 155 octets
...Pełna treść drugiej wiadomości...
DELE 2
+OK message # 2 deleted
RETR 3
+OK 158 octets
...Pełna treść trzeciej wiadomości...
DELE 3
+OK message # 3 deleted
QUIT
+OK POP3 volt Server exiting (0 NEWMAIL messages left) Connection closed by foreign host.
```



Protokół HTTP

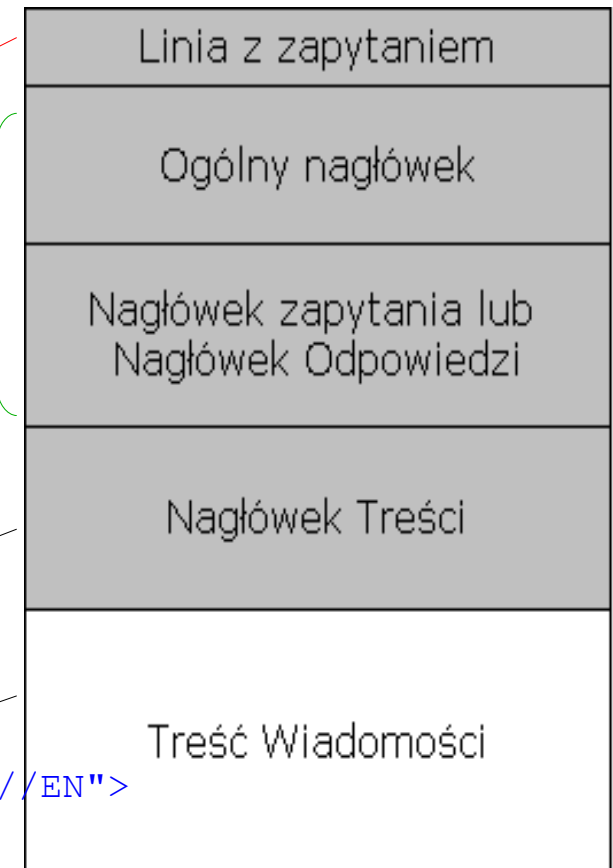
- Przykład:

```
szmurlor@max:~$ telnet www.ee.pw.edu.pl 80
Trying 194.29.144.6...
Connected to rose.ee.pw.edu.pl.
Escape character is '^]'.
GET http://www.ee.pw.edu.pl/index.html HTTP/1.0
```

```
HTTP/1.1 200 OK
Date: Wed, 21 Jan 2004 17:22:48 GMT
Server: Apache/1.3.27 (Unix) PHP/4.3.3
Last-Modified: Mon, 13 Oct 2003 09:56:00 GMT
ETag: "18284f-de-3f8a76b0"
Accept-Ranges: bytes
Content-Length: 222
Connection: close
Content-Type: text/html
X-Pad: avoid browser bug
```

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<!-- xxx -->
<head>
<meta http-equiv="refresh" content="0; URL=./index.php?strona=main" charset="iso-8859-2" />
</head>
<body></body>
</html>
```

```
Connection closed by foreign host.
szmurlor@max:~$
```





Bezpieczeństwo

- Stwierdzenie: „bezpieczeństwo jest zadaniem, które zaczyna się i kończy na administratorze“
- Nie ma bezpiecznych systemów w 100%. Bezpieczeństwo jest zawsze pewnym prawdopodobieństwem zaufania.
- Typowe formy ataków:
 - DOS – denial of service (odmowa obsługi)
 - Uzyskanie do kont zwykłych użytkowników
 - Zdobywanie uprawnień roota za pomocą dostępnych serwisów
 - Zdobywanie uprawnień roota za pomocą konta użytkownika
 - Backdoor - luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania



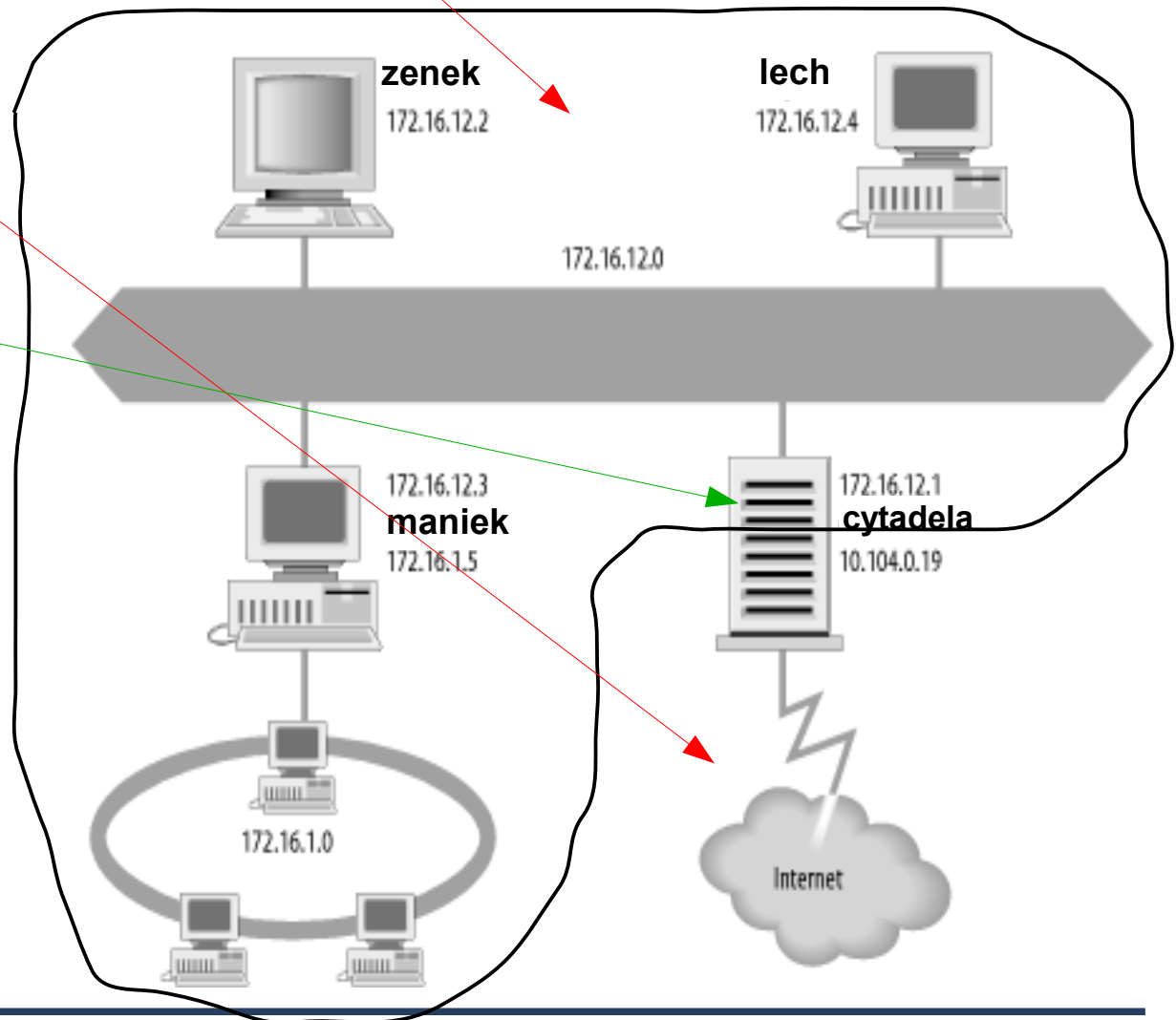
Bezpieczeństwo: Model „cebulki“

- Zabezpieczenie konta root i administratorów. (Nie zajmujemy się zabezpieczaniem kont administratorów, jeśli nie zabezpieczyliśmy wpieryw konta root.)
- Zabezpieczenie serwerów pracujących z uprawnieniami root oraz binarnych plików SUID/SGID. (Drobiazgowy administrator uruchamia tylko serwisy, które są niezbędne do pracy.)
- Zabezpieczenie kont użytkowników.
- Zabezpieczenie pliku z hasłami.
- Zabezpieczenie jądra systemu, urządzeń surowych i systemu plików. (Jeśli włamywacz uzyska prawa roota, to może praktycznie wszystko.)
- Szybkie wykrywanie niedopuszczalnych zmian dokonywanych w systemie.
- Paranoja. (Lekka paranoja jest potrzebna, ale nie może ona przeszkadzać w pracy.)



Przykładowa Topologia Sieci

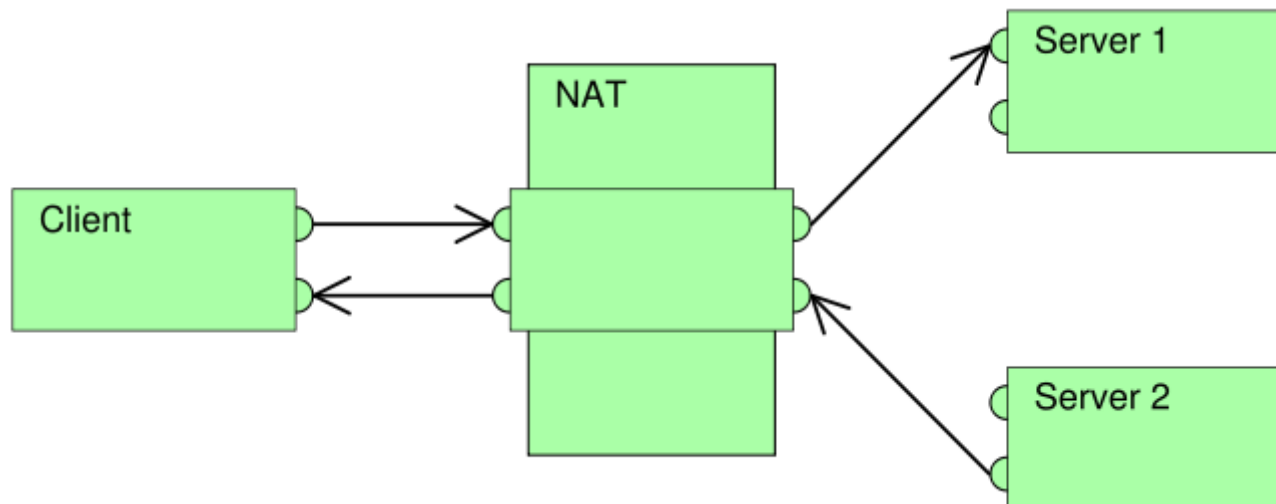
- DMZ – strefa zdemilitaryzowana
- WAN – sieć zewnętrzna
- Zabezpieczenia:
 - **Firewall:**
 - NAT
 - Proxy





NAT – Network Address Translation

- NAT: inaczej maskarada (*ang. Masquerading*) - technika translacji adresów sieciowych.
- Lokalne sieci komputerowe, korzystające z tzw. adresów prywatnych (specjalna pula adresów tylko dla sieci lokalnych), mogą zostać podłączone do Internetu przez jeden komputer (lub router), posiadający mniej adresów internetowych niż komputerów w tej sieci.
 - Wady: nie można na własnym komputerze uruchomić serwera dostępnego w Internecie bez zmian wymagających interwencji administratora, utrudnione korzystanie z programów P2P i bezpośredniego wysyłania plików, zachamował wprowadzenie IPv6.





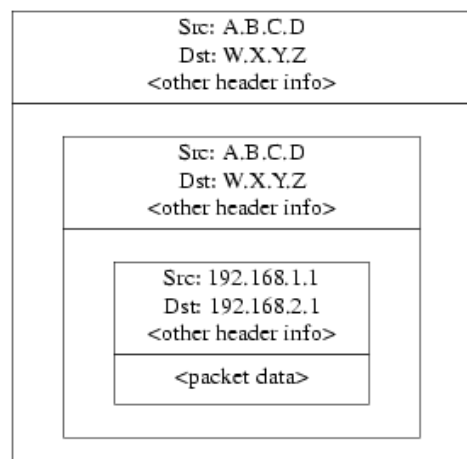
Serwer pośredniczący - Proxy

- Proxy - oprogramowanie lub serwer z odpowiednim oprogramowaniem, które dokonuje pewnych operacji (zwykle nawiązuje połączenia) w imieniu użytkownika. Często utożsamiany z pośrednikiem HTTP (HTTP proxy).
- Użytkownik zleca pośrednikowi zadania za pomocą odpowiedniego klienta. W wypadku usług FTP i HTTP jest to klient FTP i przeglądarka internetowa.
- Użycie pośrednika wprowadza w sieci element zabezpieczający, ponieważ jego praca realizowana jest w warstwie aplikacyjnej modeli ISO/OSI, i jako taka może analizować logiczną zawartość pakietów, a nie jedynie ich formalną zgodność ze standardem. Umożliwia to wykrywanie wirusów, lub nielegalnych tuneli danych.
- Podsumowując, dzięki proxy można uzyskać:
 - zmniejszenie czasu dostępu do danych z Internetu
 - zmniejszenie obciążenia łącz internetowych
 - większe bezpieczeństwo i anonimowość użytkowników
 - możliwość kontroli i wprowadzenia pewnych ograniczeń



VPN

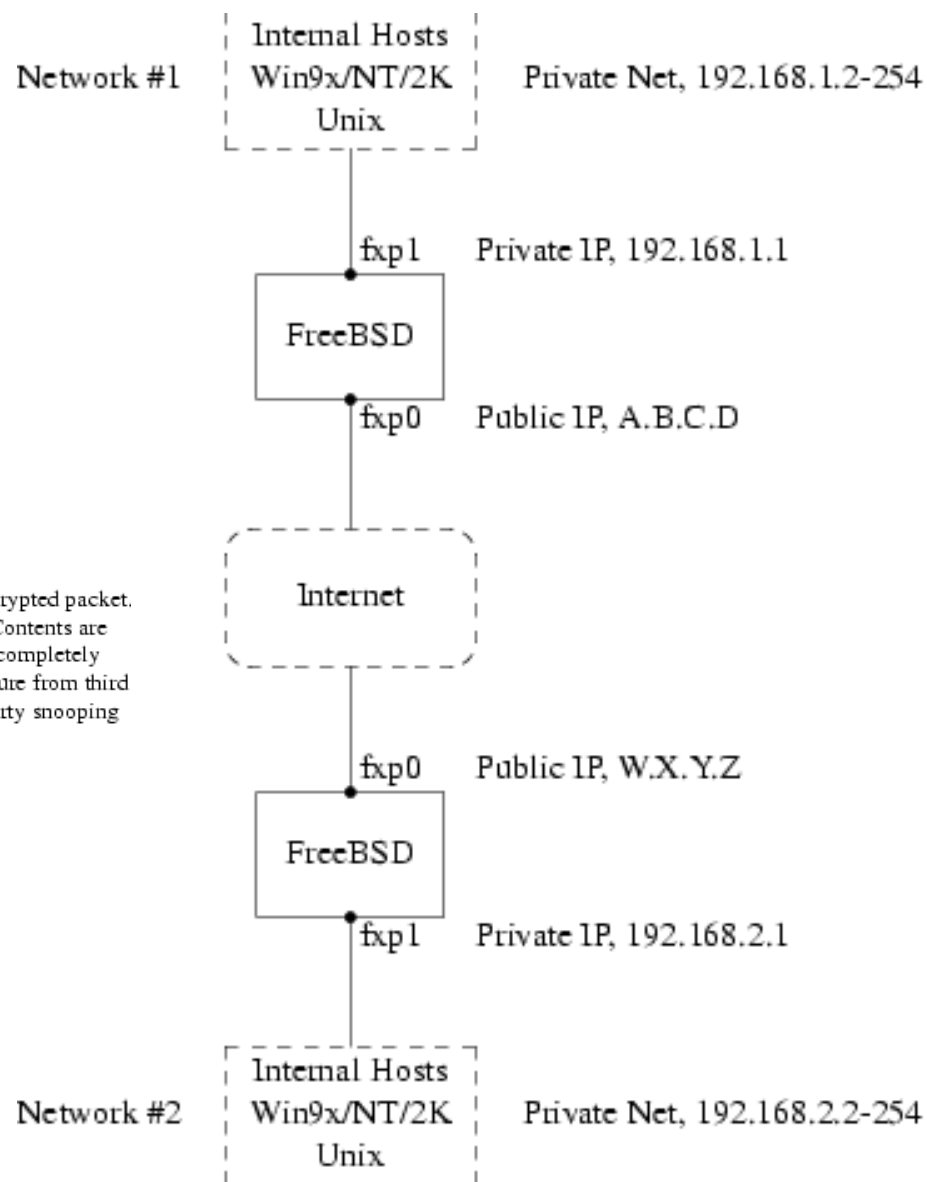
- VPN – Virtual Private Network



Original packet,
private IP addr

Encapsulated
packet,
with real IP addr

Encrypted packet.
Contents are
completely
secure from third
party snooping





OpenSSH

- Oparte na kluczach niesymetrycznych, podczas łączenia z serwerem musimy zaakceptować klucz serwera.
- Klient i serwer ssh
- Bezpieczne kopiowanie: scp
- Generacja kluczy do automatycznego logowania
- Tunelowanie ssh: (np.: bezpieczny dostęp do konta POP3, ominięcie rygorystycznego firewalla)





Współdzielenie Zasobów

- **Moc obliczeniowa** (**DCOM** – Dynamic Component Object Model, **RPC** – Remote Procedure Call, **MPI** - Message-Passing Interface, **SOAP** – Simple Object Access Protocol)
- **Pamięć dyskowa** (**NFS** – Network File System, Novell Netware, Windows Samba)
- **Drukarki** – serwery drukarek
- **Składnice danych** (data warehouse – bazy danych)
- **Serwery aplikacji** (architektura klient-serwer, **X Window**, **Windows Terminal Server** – remote desktop)
- **Autoryzacja użytkowników** (domena windows NT, XP Home Edition – brak możliwości autoryzacji w domenie, uproszczony system uprawnień do plików, serwer **NIS**, **LDAP** =?= **Active Directory**)



Terminologia...

- **DCOM** (Distributed Component Object Model - rozproszony obiektowy model komponentów) jest opracowanym przez Microsoft sposobem budowania komponentów programowych i zapewniania komunikacji między nimi w małej sieci komputerowej. Rozwinięty z COM jako odpowiedź na CORBA, stał się później częścią COM+. Został przez Microsoft uznany za przestarzały na rzecz platformy .NET.
- **RPC** (Remote Procedure Call) to protokół zdalnego wywoływania procedur, stworzony przez Suna i swego czasu dość popularny na Uniksach, obsługiwany w bibliotekach języka Java, a współcześnie wypierany przez bardziej rozbudowane protokoły takie jak CORBA czy XML-RPC.
- **MPI** (Interfejs Transmisji Wiadomości, ang. Message Passing Interfece) to protokół komunikacji pomiędzy komputerami. Tak naprawdę jest to standard komunikowania się działających na węzłach programów równoległych. MPI tworzą biblioteki, które można wywoływać w programach tworzonych w językach Fortran, C, C++ i Ada.



Terminologia...

- **SOAP** (Simple Object Access Protocol) to protokół wywoływania zdalnego dostępu do obiektów, wykorzystujący XML do kodowania wywołań i HTTP do ich przesyłania. Dokument SOAP składa się z trzech części: otoczki (envelope) która określa szkielet opisujący co znajduje się w komunikacie i jak go przetwarzać, zbioru reguł kodujących potrzebnych do rozszyfrowania typów danych (również złożonych) zdefiniowanych wewnątrz aplikacji, reguł dotyczących wywoływania zdalnych procedur i odczytu odpowiedzi.
- **NFS** (Network File System) to oparty o UDP protokół zdalnego udostępniania systemu plików. NFS jest de facto standardowym sieciowym systemem plików na Uniksach. Inne protokoły udostępniające taką usługę, jak np. Coda, nie zyskały dużej popularności. NFS został opracowany przez Sun Microsystems. Z NFS wiąże się wiele problemów - przede wszystkim bardzo trudno zapewnić że dana operacja została wykonana.



Terminologia...

- **LDAP** (Lightweight Directory Access Protocol). Jest to "lekki" protokół przeznaczony do dostępu do usług katalogowych. Bazuje na usługach katalogowych X.500. Wykorzystywany praktycznie w adresacji sieci Internet/Intranet w celu zapewnienia niezawodności, skalowalności i bezpieczeństwa danych. W odróżnieniu od X.500 nie potrzebuje ani szerokiego pasma (lightweight), ani dużej mocy obliczeniowej. LDAP pracuje w oparciu o protokół TCP/IP lub inne połączeniowe usługi transportu. Dane grupowane są w strukturze przypominającej drzewo katalogów. Każdy obiekt jest jednoznacznie identyfikowany poprzez swoje położenie na drzewie - tzw. distinguished name (DN).
- **NIS** (Network Information Service) Celem jego jest dostarczanie informacji, które muszą być dostępne w sieci (zwykle lokalnej) dla wszystkich komputerów. Informacje, które zwykle są dystrybuowane to: login/hasła/katalogi domowe, informacje o grupach. Jeśli na przykład informacja o twoim hasle jest zapisana w bazie haseł NIS, będziesz mógł się zalogować na wszystkich maszynach na sieci, które mają uruchomionego klienta NIS.



Terminologia...

- **Active Directory** to usługi katalogowe dla Windows 2003 Server oraz Windows 2000. Katalog przechowuje informacje o obiektach dostępnych w sieci – czy są to udziały sieciowe, drukarki, komputery, czy też wyspecjalizowane serwery bazodanowe czy inne oprogramowanie serwerowe. Dzięki Active Directory administrator ma potężne narzędzie pozwalające na wprowadzenie porządku i określonej, hierarchicznej struktury w sieci.
- Active Directory zarządza domenami Windows, które łączą się w hierarchiczną strukturę drzew domen i lasów domen. Są one zintegrowane z serwerami DNS.
- *„To allow Active Directory to gain popularity as an enterprise repository, Microsoft had to make an early commitment to LDAP. The Windows 2000 implementation of Active Directory is an LDAP-compliant directory supporting the core LDAP RFCs available at the time of its release. Currently, Windows 2000 Active Directory reaches LDAP compliance through support of the following RFCs.“*
(cytat z: *“Active Directory LDAP Compliance, Microsoft Corporation, Published: October 2003*)



System X Window jako Przykład Sieciowego Graficznego Interfejsu Użytkownika (GUI)

- Często oprócz X Window System stosuje się też nazwę X, X11 lub X11R6.
- Cechą charakterystyczną jest jego sieciowy charakter.
- System X tworzy okna, na których program może tworzyć obraz, oraz zajmuje się obsługą urządzeń wejściowych (myszki, klawiatury, tabletu). Serwer X może rysować tylko najprostsze obiekty (odcinki, wielokąty, elipsy, wyświetlać bitmapy, stawiać pojedyncze piksele), nie dostarcza natomiast żadnego interfejsu użytkownika, czyli przycisków, rozwijanych menu, pasków przewijania itp. Rysowaniem i obsługą tych elementów musi zająć się program, najczęściej jest to biblioteka widgetów. System X nie zajmuje się również obsługą okien, nie dostarcza żadnych wbudowanych mechanizmów do ich przesuwania, zmiany rozmiaru, zamykania i uruchamiania programów itd., nie rysuje także pasków tytułowych dla okien – tym wszystkim musi zająć się osobny program, tzw. menedżer okien (ang. window manager).

(wikipedia)



System X Window – Model Klient-Serwer

– X Server może być:

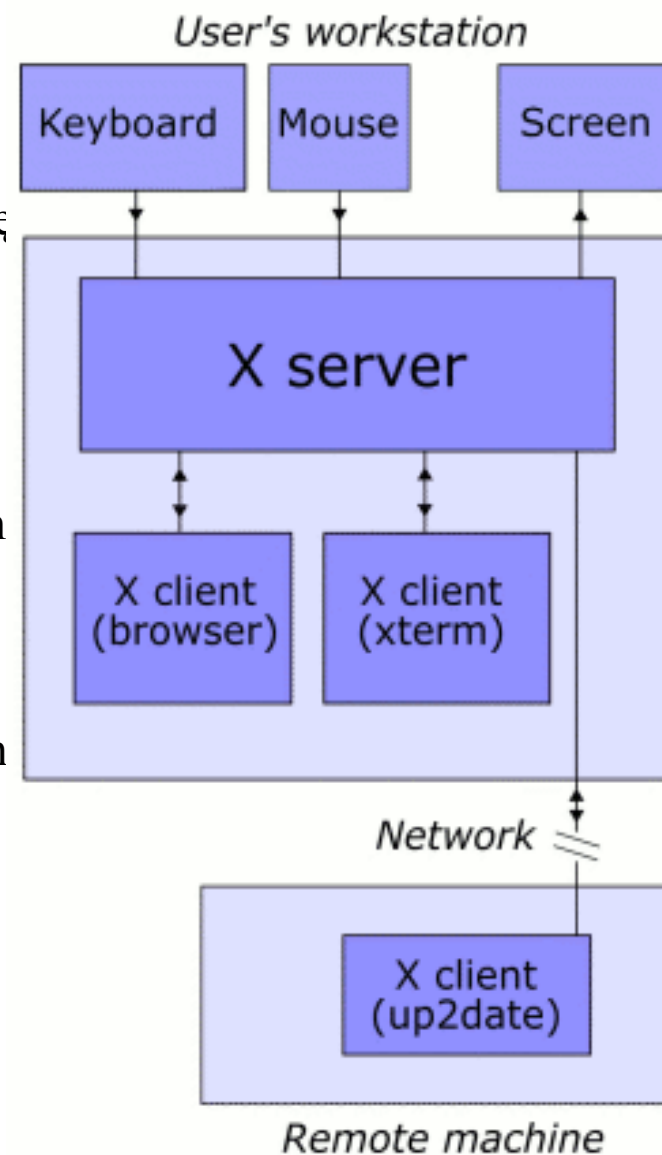
- Aplikacją rysującą w oknie znajdującym się w innym systemie graficznym (X Serwer z pakietu cygwin).
- Programem systemowym obsługującym bezpośrednio kartę graficzną danego PC.
- Zintegrowanym urządzeniem.

– Protokół komunikacyjny:

- Komunikacja między serwerem a klientami jest realizowana za pomocą wymiany pakietów przez połączenie sieciowe.

– Okna

- W Systemie X Window to co w innych systemach określan jest mianem okna (window), tutaj nazywa się top-level-window. W X okna znajdują się wewnątrz innych okien (okna potomne i macierzyste). Wszystkie elementy graficzne (przyciski, menu, suwaki itp) są realizowane w postaci okien potomnych.
- W X jest jedno okno korzeń (root window), które ma rozmiar ekranu. Wszystkie pozostałe okna są jego potomkami.





Jak to działa?

- Każdy X klient (czyli aplikacja graficzna) odczytuje wartość zmiennej środowiskowej DISPLAY, która definiuje z jakim X Serwerem ma się skontaktować. Typowe wartości to:
 - `export DISPLAY=localhost:1`
 - `export DISPLAY=localhost:2`
 - `export DISPLAY=server.iem.pw.edu.pl:1`
- Jak bezpiecznie przesyłać dane? Protokół komunikacyjny X Window jest nieszyfrowany!
 - Najłatwiej jest połączyć się konsolą tekstową i tunelować połączenie.



Przykład X Serwer w pakiecie Cygwin

The screenshot illustrates the process of running an X server in Cygwin and connecting to a remote machine. The terminal window shows the following steps:

1. Running `startx&` to start the X server. The terminal output includes:

```
robert@LAP-RS2 ~  
$ startx&  
[1] 1992  
  
robert@LAP-RS2 ~  
$  
Welcome to the XWin X server  
Vendor: The Cygwin/X Project  
Release: 6.8.99.901-4  
  
Contact: cygwin-xfree@cygwin.com  
  
XWin was started with the following command line:  
X :0 -multiwindow -clipboard  
  
_XSERVTransmkdir: Owner of /tmp/.X11-unix should  
winValidateArgs - g_iNumScreens: 1 iMaxConsecuti  
<II> XF86Config is not supported  
<II> See http://x.cygwin.com/docs/faq/cygwin-x-fa  
winDetectSupportedEngines - Windows NT/2000/XP  
winDetectSupportedEngines - DirectDraw installed  
winDetectSupportedEngines - DirectDraw4 installed  
winDetectSupportedEngines - Returning, supported
```
2. Closing the terminal window.
3. Running `ssh -Y szmurlor@max.iem.pw.edu.pl` to connect to a remote machine. The terminal output includes:

```
robert@LAP-RS2 ~  
$ ssh -Y szmurlor@max.iem.pw.edu.pl  
Password:  
Warning: No xauth data; using fake authentication data for X11 forwarding.  
Linux max.iem.pw.edu.pl 2.4.18-bf2.4 #1 Mon Apr 12 11:37:50 UTC 2004 i686 GNU/Li  
nux  
** zobacz: http://lop.iem.pw.edu.pl/  
**  
** serwer: max  
**  
You have mail.  
Last login: Wed Nov  8 15:02:33 2006 from robertd  
szmurlor@max:~$ xclock  
szmurlor@max:~$ kwr  
kurapper kwrite  
szmurlor@max:~$ kwr  
kurapper kwrite  
szmurlor@max:~$ kwrite  
Link points to /tmp/.ksocket-szmurlor"  
OPIxman: Cannot create a OPIxman when no GLIT is being used
```
4. Running `kwrite` on the remote machine to open a text editor.
5. The KWrite text editor window is shown, with the title bar displaying "Untitled - KWrite". The "About KWrite" dialog box is also visible, showing "KWrite 4.3 (Using KDE 3.3.2)".



Alternatywy dla X Window: VNC i NX

- **VNC** (ang. Virtual Network Computing) - system przekazywania obrazu z wirtualnego, bądź fizycznego środowiska graficznego.
 - Prosty pakiet serwer+klient jest dostępny pod najpopularniejsze systemy operacyjne z trybem graficznym, jak: Linux, Windows, BSD, MacOS, OS/2, Solaris, Amiga, SCO i wiele innych. Klienci VNC są dostępne nawet dla urządzeń typu PDA i niektórych telefonów komórkowych.
 - Jego wielką zaletą jest użycie licencji GPL, dzięki czemu VNC jest darmowe, bardzo rozwinięte, dostosowane do różnych potrzeb i bardzo wydajny.
 - <http://www.realvnc.com/>, <http://www.tightvnc.com/>
- Poważnym konkurentem staje się system **NX**, który działa z jeszcze większą wydajnością. - Jego autorem jest Gian Filippo Pinzari, który oparł NX o istniejący protokół X11, przykładając jednak znacznie większą wagę do kompresji danych przepływających między maszynami i uwzględniając charakterystykę współczesnych programów. W efekcie NX jest bardzo wydajny i działa skutecznie nawet przez łącza modemowe (czyli o przepustowości do 56,6 kb/s).
 - <http://www.nomachine.com/developers.php>,
<http://www.linuxjournal.com/article/8342>



Podsumowanie: podstawowe narzędzia sieciowe

- Warstwa sieciowa: ping, traceroute, tracert, ipconfig lub ipcfg (MS Windows), ifconfig (unix), route print, netstat -r, host (-mx), arp, tcpdump
- Warstwa aplikacji: telnet, ssh, scp, ftp, wget, lynx, putty,



Interakcja

- Jeżeli coś cię zainteresowało i chciałbyś aby na następnym wykładzie zostało rozszerzone, powtórzone, omówione dokładniej, to nie kępuj się i napisz maila:

szmurlor@iem.pw.edu.pl

- Jeżeli coś było nie jasne, napisz maila:

szmurlor@iem.pw.edu.pl

- Jeżeli coś cię znudziło, napisz maila:

szmurlor@iem.pw.edu.pl