

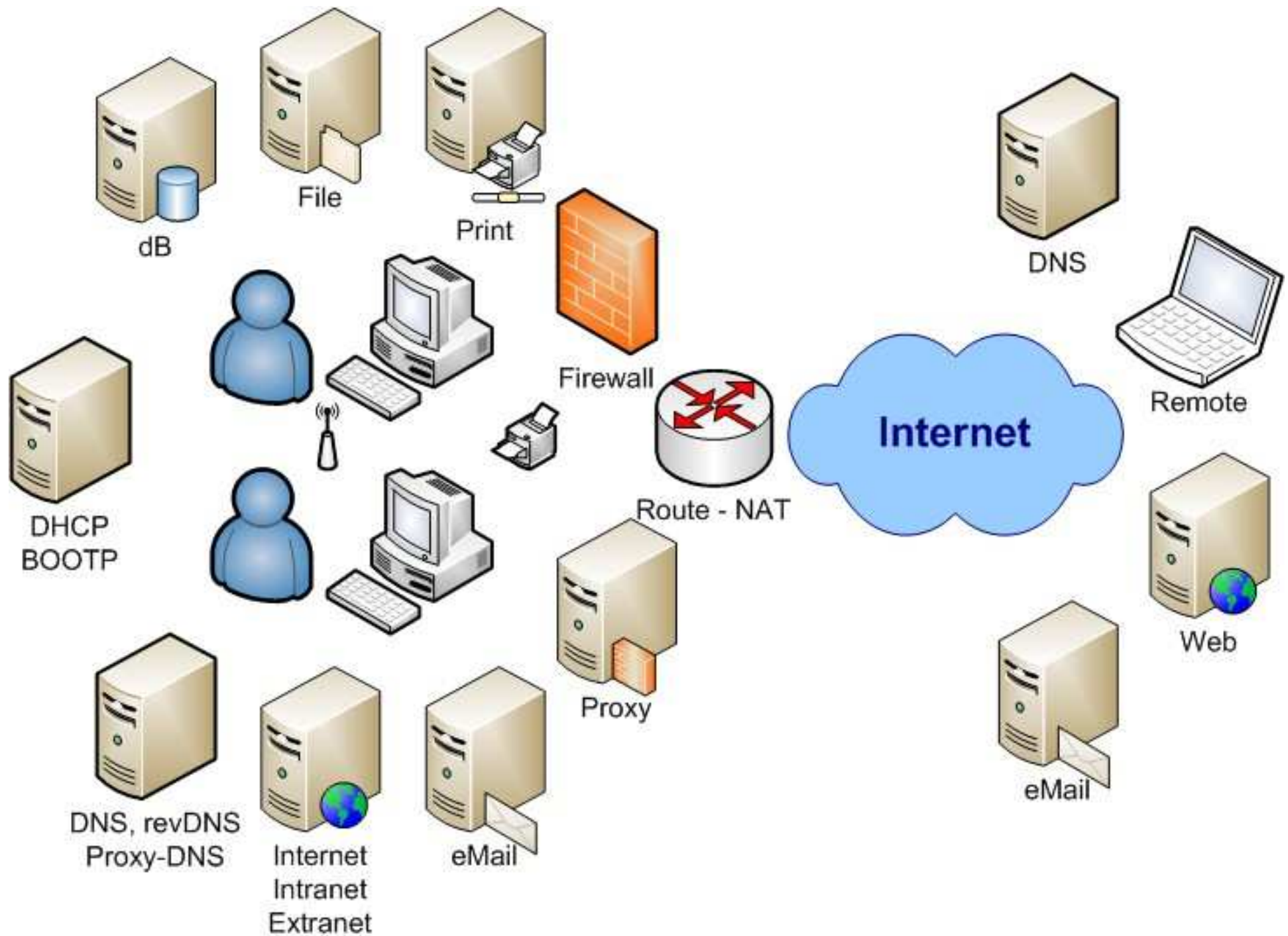


Sieciowe systemy operacyjne
Część 2. TCP/IP, IPv6 i konfiguracje
Autor Wojciech Gumiński



Ostrzeżenie:

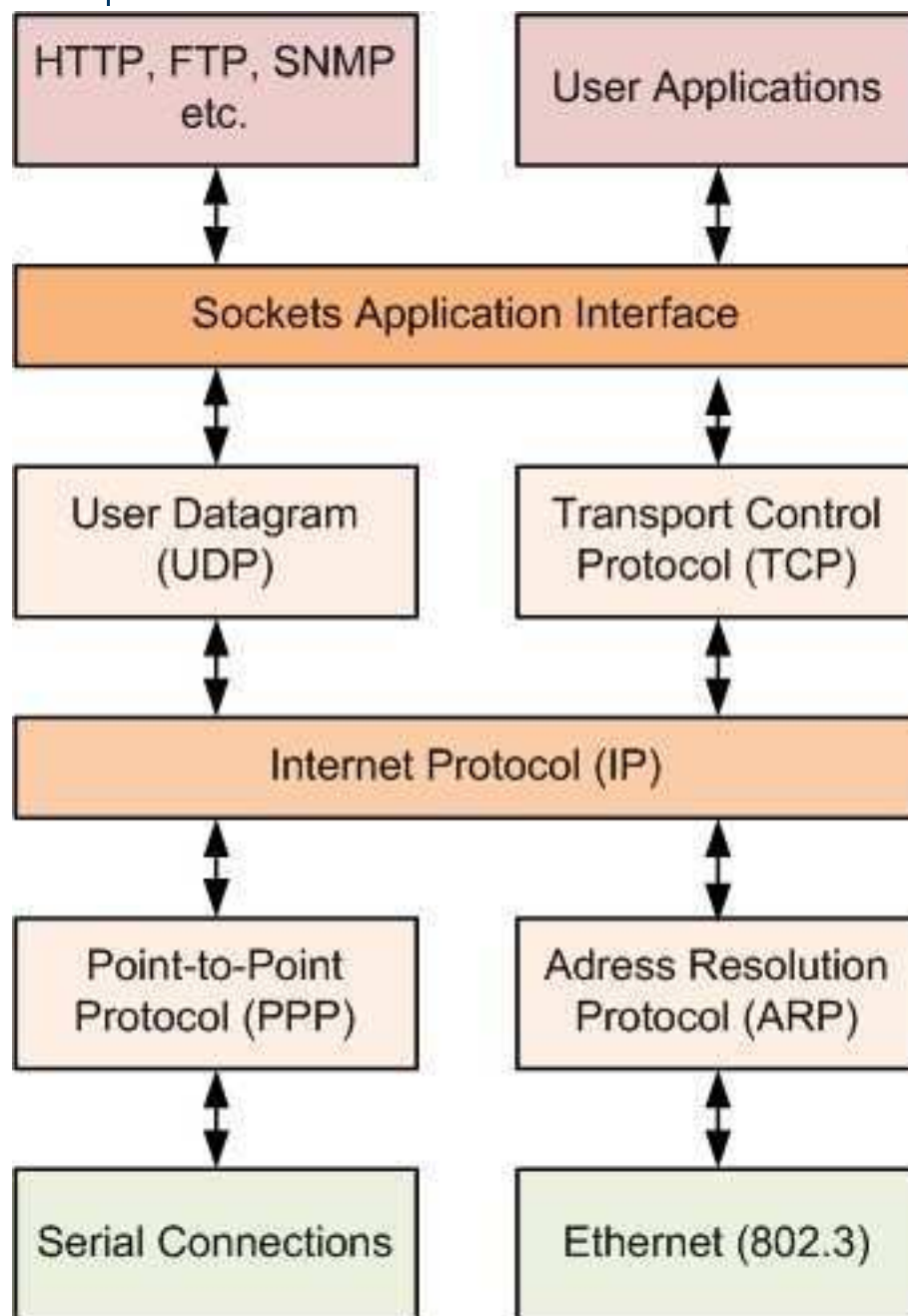
Informacje zawarte w tym dokumencie są materiałami pomocniczymi do prowadzenia wykładu. Nie zastąpią ani podręcznika, ani tym bardziej obecności na wykładach. Niektóre wpisy w przykładowych plikach konfiguracyjnych mogą być wzajemnie sprzeczne, ale ilustrują możliwości uzyskania określonych właściwości usług.

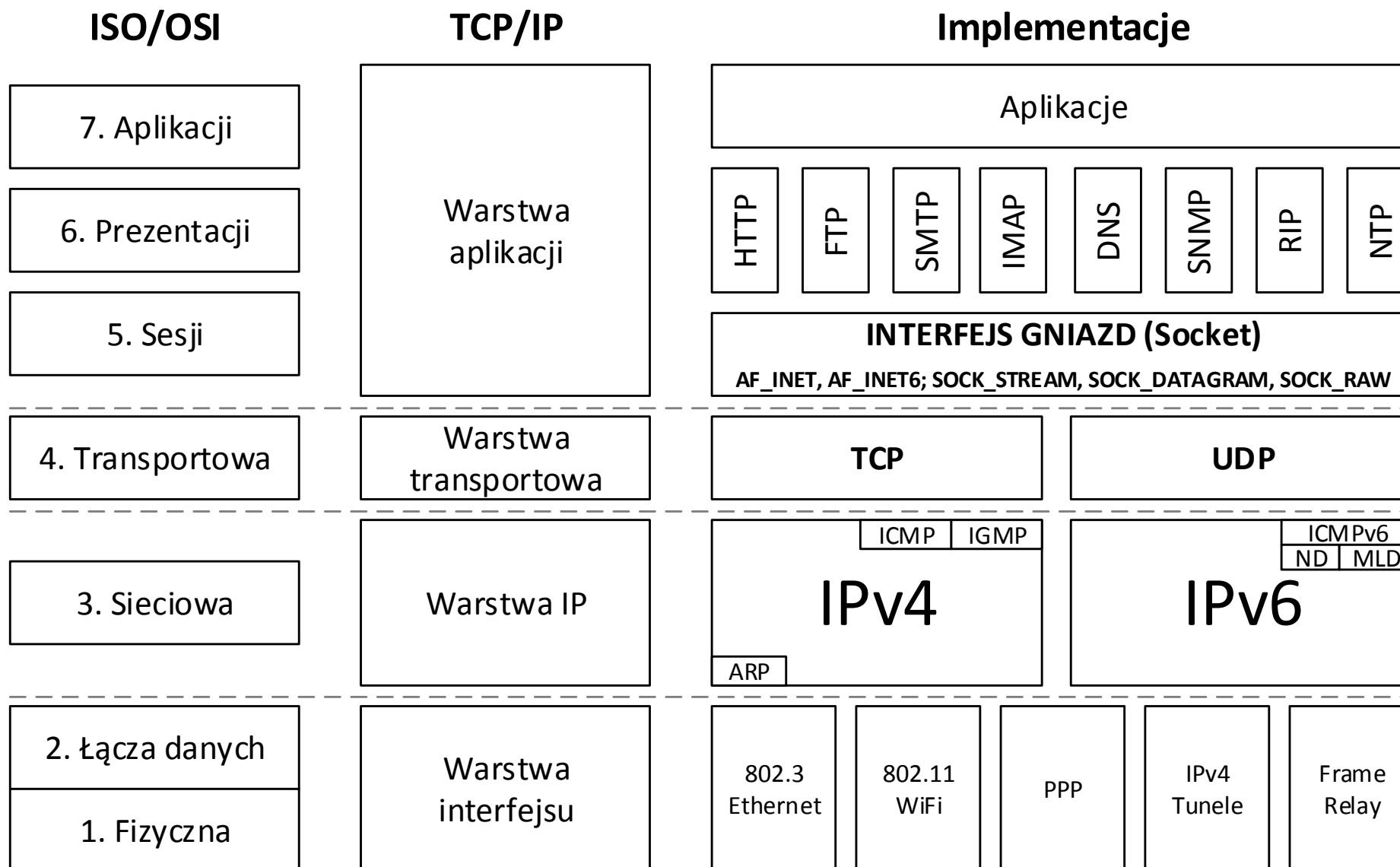


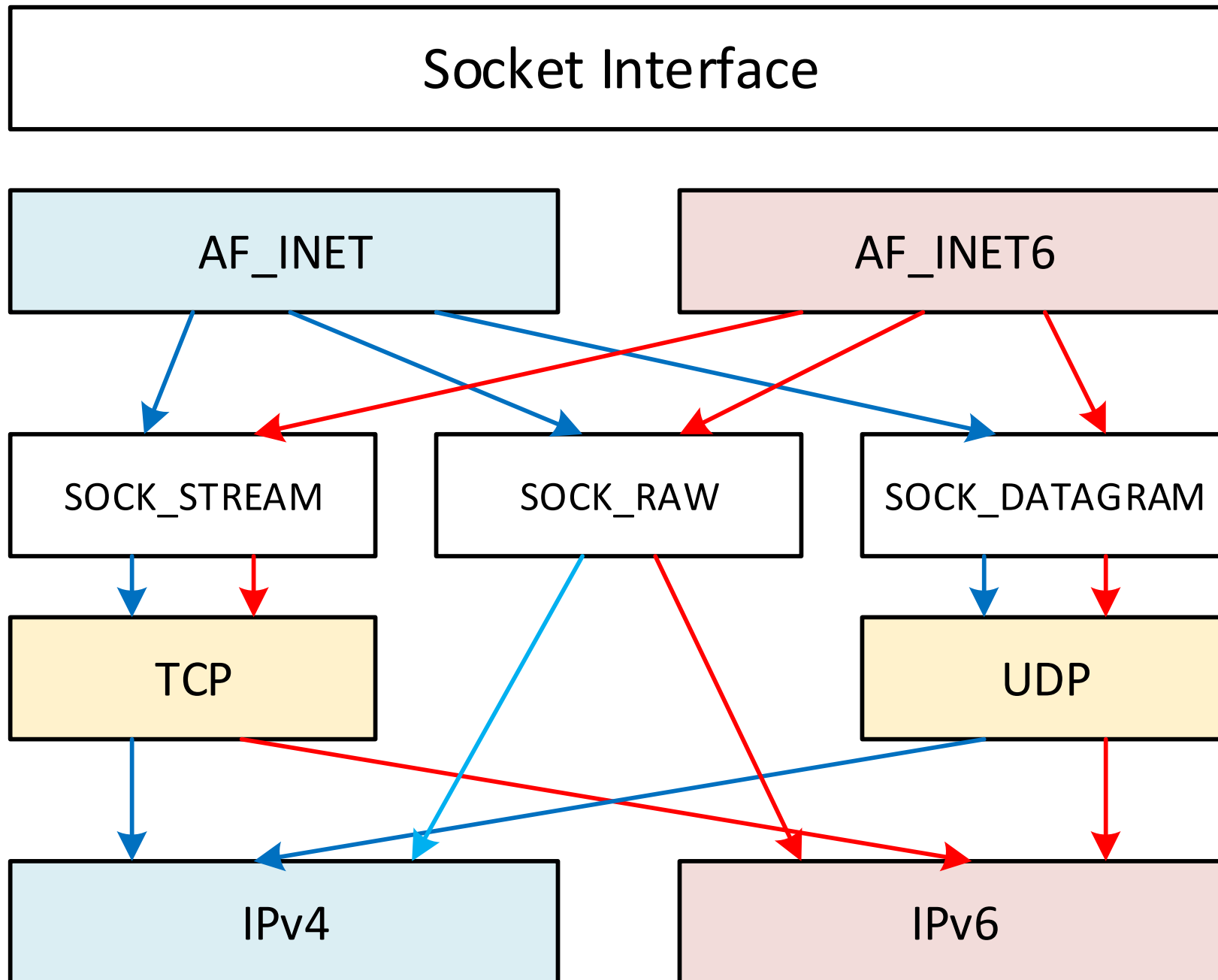


Wprowadzenie do TCP/IP

.

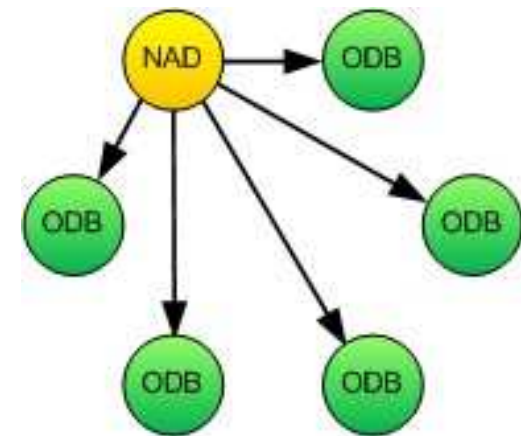
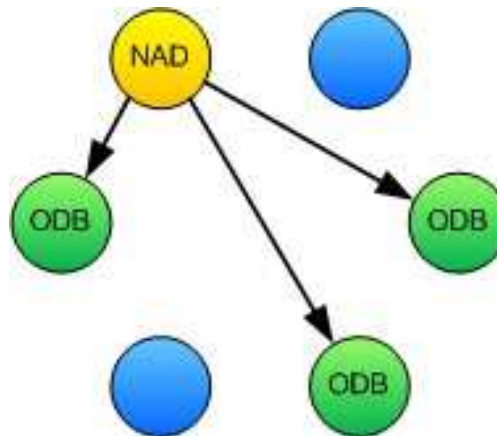
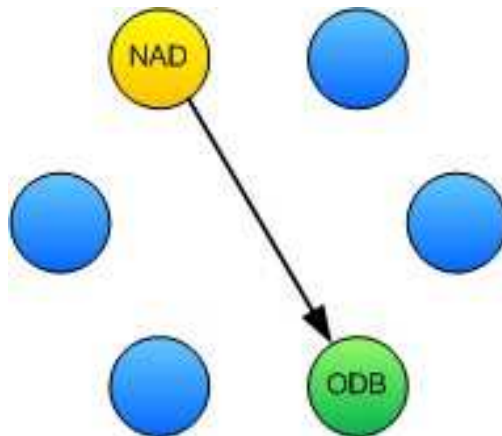






Rodzaje adresów ze względu na grupę odbiorców

- Pojedynczy adresat – unicast
- Grupa odbiorców – multicast
- Wszyscy odbiorcy – broadcast
- Najbliższy usługodawca - anycast



Adres IPv4

Przykład: 192.168.5.10

	Dziesiętnie	Binarnie
Adres IP	192.168.005.010	11000000.10101000.00000101.00001010
Maska sieci	255.255.255.000	11111111.11111111.11111111.00000000
Adres sieci	192.168.005.000	11000000.10101000.00000101.00000000
Adres rozgłoszeniowy	192.168.005.255	11000000.10101000.00000101.11111111

Adres_sieci = Adres_IP AND Maska_sieci

Adres rozgłoszeniowy = Adres_IP OR NOT Maska_sieci
= Adres_sieci OR NOT Maska_sieci



Klasy adresów

Klasa	Początkowe bity	Adres początkowy	Adres końcowy	Maska
A	0	0.0.0.0	127.255.255.255	255.000.000.000
B	10	128.0.0.0	191.255.255.255	255.255.000.000
C	110	192.0.0.0	223.255.255.255	255.255.255.000
D multikast	1110	224.0.0.0	239.255.255.255	255.255.255.240
E zarezerwowana	1111	240.0.0.0	255.255.255.255	

Specjalne adresy prywatne (nieroutowalne)

Klasa	Adres początkowy	Adres końcowy
1 x A	10.0.0.0	10.255.255.255
16 x B	172.16.0.0	172.31.255.255
256 x C	192.168.0.0	192.168.255.255
169.254.0.0/16	169.254.1.0	169.254.254.255

*Przydzielane pseudolosowo przy braku serwera DHCP w sieci lokalnej (RFC3927)

Adres łączy lokalnego (loopback) to 127.0.0.0/8
W szczególności 127.0.0.1/32 to localhost.



Adresowanie bezklasowe

(ang. *CIDR Classless Inter-Domain Routing*)

CIDR	Maska dziesiętnie	Liczba hostów*
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	2 (PPP)
/32	255.255.255.255	1

*Przy połączeniach międzysieciowych liczba hostów zmniejsza się o 1.



Przykłady adresów IP

10.11.12.13/8

Adres	00001010.00001011.00001100.00001101	10.11.12.13
Maska	11111111.00000000.00000000.00000000	255.0.0.0
Adres sieci	00001010.00000000.00000000.00000000	10.0.0.0
Broadcast	00001010.11111111.11111111.11111111	10.255.255.255

192.168.1.11/29

Adres	11000000.10101000.00000001.00001011	192.168.1.11
Maska	11111111.11111111.11111111.11111000	255.255.255.248
Adres sieci	11000000.10101000.00000001.00001000	192.168.1.8
Broadcast	11000000.10101000.00000001.00001111	192.168.1.15



Przykładowe podsieci dla maski 29-cio bitowej (32 podsieci – 160 hostów)

Adres sieci	Adres rozgłoszeniowy	Pierwszy adres hosta	Ostatni adres hosta
aa.bb.cc.0	aa.bb.cc.7	aa.bb.cc.1	aa.bb.cc.6
aa.bb.cc.8	aa.bb.cc.15	aa.bb.cc.9	aa.bb.cc.14
aa.bb.cc.16	aa.bb.cc.31	aa.bb.cc.17	aa.bb.cc.30
...
aa.bb.cc.232	aa.bb.cc.239	aa.bb.cc.233	aa.bb.cc.238
aa.bb.cc.240	aa.bb.cc.247	aa.bb.cc.241	aa.bb.cc.246
aa.bb.cc.248	aa.bb.cc.255	aa.bb.cc.249	aa.bb.cc.254



UDP User Datagram

Bajt	Bity 0-15	Bity 16-31
0	Port nadawcy	Port odbiorcy
4	Długość	Suma kontrolna
8	Dane	

UDP w IP4

Bajt	Bity 0-15	Bity 16-31
0	Adres nadawcy	
4	Adres odbiorcy	
8	Protokół, flagi	Długość UDP
12	Port nadawcy	Port odbiorcy
16	Długość	Suma kontrolna
20	Dane	

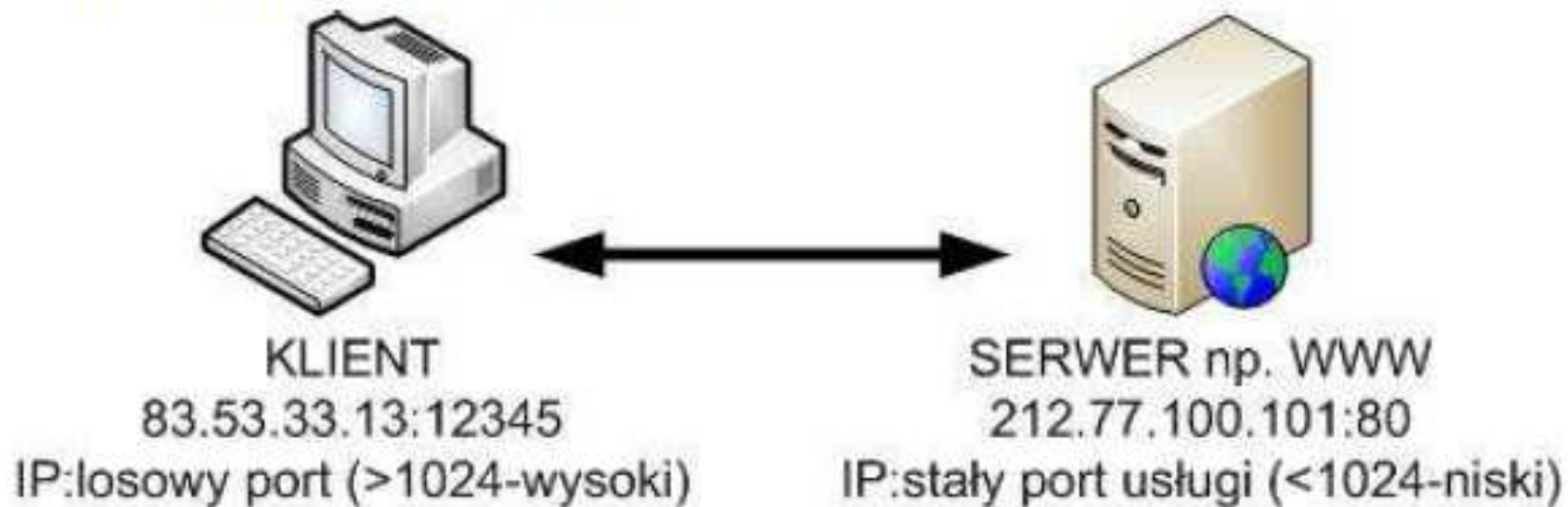


TCP Transport Control Protocol

Bajt	Bity 0-15	Bity 16-31
0	Port nadawcy	Port odbiorcy
4	Numer sekwencyjny	
8	Numer potwierdzenia	
12	Flagi	Szerokość okna
16	Suma kontrolna	Priorytet
20	Opcje (opcjonalnie)	
20/24	Dane	



Połączenie w TCP/IP





Klasyczna sekwencja nawiązywania połączenia TCP

(ang. *Three way handshake*)

1 klient -> serwer SYN

2 serwer -> klient SYN/ACK

3 klient -> serwer ACK

transmisja (ACK)



IPv6



IPv6 - zalety

- Większa przestrzeń adresowa (340×10^{36} vs $4,3 \times 10^9$)
- Bezstanowa autokonfiguracja węzłów (SLAAC)
- Multicasty
- Obligatoryjna obsługa IPSec
- Uproszczona obsługa przez routery
- Mobilność
- Opcjonalna rozszerzalność
- Jumbogramy (4GB vs 64KB)



IPv6 - wady

- Długie skomplikowane adresy
- Kłopotliwa i niejednoznaczna implementacja IPSec
- Minimalne MTU 1280
- Standardowe maski /64 /48
- (Nie)Bezpieczeństwo (globalna dostępność każdego hosta)
- Konieczność migracji aplikacji (zmiany w API)
- Długi okres wdrażania
- Słaba obsługa w systemach sprzed 2008 r.



IPv6 - krótko o zbyt długiej historii wdrażania

- 1996 – Linux kernel 2.1.6 obsługa IPv6 w fazie alfa
- 1996 – Uruchomienie sieci testowej 6bone
- 2000 – BSD, Sun Solaris
- 2001 – Cisco IOS, HP-OS, Compaq OpenVMS
- 2002 – Windows XP SP1, Windows 2003 Server
- 2003 – Apple Mac OS X 10.3 „Panther”
- 2007 – Windows Vista IPv6 protokołem domyślnym
- 2008 – Globalny DNS IPv6
- 2008 – <http://ipv6.google.com>, <http://ipv6.beijing2008.cn/en>
- 2009 – Google over IPv6
- 2010 – <http://www.v6.facebook.com>
- 2011 – koniec wolnych puli adresów IPv4
- 2012 – 8 czerwca, światowy dzień IPv6
- 2013 – 6 czerwca, światowy dzień IPv6 – włączenie IPv6 u „wielkich” na stałe
- 2013 – listopad, pierwszy z polskich dużych operatorów włącza IPv6 dla klientów indywidualnych



Adresy IPv6 (RFC4291- IPv6 Addressing Architecture)

- 2001:DB8::203:C0FF:FE12:3456
- 2001:0DB8:0000:0000:0203:C0FF:FE12:3456
- FE80::203:C0FF:FE12:3456
- FF02::1
- ::1
- ::192.0.2.33
- ::FFFF:192.0.2.33
- 2001:db8:122:344:c0:2:2100:: (192.0.2.33 w sieci /64)
- 64:FF9B::192.0.2.33 (IPv4 „well known” prefix RFC6052)
- FEC0:0:0:FFFF::1, FEC0:0:0:FFFF::2, FEC0:0:0:FFFF::3

Adresy IPv6

Typy adresów

- Nieokreślony `::/128`
- Loopback `::1/128`
- Multicast `FF00::/8`
- Link-local `FE80::/16`
- Global-unicast `2000::/3`
- Site-local `FEC0::/10 (deprecated)`

Adresy anycastowe są wybierane spośród adresów unicastowych i nie posiadają żadnego specjalnego wyróżnika.



Identyfikator interfejsu EUI-64 z adresu MAC

- MAC 00:12:34:56:78:9A
- EUI-64
 - ccccccUG:cccccccc:cccccccc:
 - 11111111:11111110:
 - pppppppp:pppppppp:pppppppp
- U to bit universal/local w adresie MAC zwykle 0 w EUI-64 zostaje zanegowany do 1
- G to bit individual/group zwykle 0
- EUI-64 0212:34:FF:FE56:789A

Pomimo tej procedury IPv6 nie wymaga kontroli znaczenia tych bitów.



Adresy specjalne

- Unique-local FC00::/7 (RFC4193)
 - FC00::/8 – zarezerwowane na przyszłość
 - FD00::/8 – do użycia z 40-bitowym losowym network ID
 - Nieroutowalne, prywatne
- Documentation 2001:DB8::/32
- 6to4 tunnel 2002::/16 (z IPv4 - 192.88.99.1/24)
- Teredo tunnel 2001:0::/32



Adresy multicastowe IPv6

- FF00::/16
- 11111111ORPTscop::
 - T=0 "well-known" assigned by IANA
 - T=1 "transient" or "dynamically" assigned
 - R (RFC3306), P (RFC3956) (do adresacji międzysieciowej)
 - scop - zasięg
 - 1 – interface-local scope
 - 2 – link-local scope
 - 4 – admin-local scope
 - 5 – site-local scope
 - 8 – organization-local scope
 - E – global scope



Adresy multicastowe IPv6

- FF02::1 – all nodes
- FF0X::2 – all routers
- FF05::1:3 – all DHCP servers
- FF02::1:2 – all DHCP servers and relays
- FF0X::C – SSDP (UPnP)
- FF0X:FB – mDNSv6
- FF0X:101 – NTP
- FF02::1:FF00:0000/104 - Solicited-Node Address



Adresy multicastowe IPv6 - obsługa obowiązkowa

- All nodes
 - FF01::1
 - FF02::1
- All routers
 - FF01::2
 - FF02::2
 - FF05::2
- Solicited-Node Address
 - FF02:0:0:0:0:1:FF00:0/104

Np. Dla adresu unicastowego 2001:db8::212:34FF:FE56:78:9A

Adresem multicastowym węzła będzie FF02:0:0:0:0:1:FF56:789A



Adresy URL IPv6

- Przykładowy adres IP:
 - 2001:db8::1
- Przykładowy URL:
 - http://[2001:db8::1]
- URL z podanym portem
 - https://[2001:db8::1]:443

Identyfikatory interfejsu w IPv6 (RFC4007 Zone-ID)

- FD80::1%3
- FD80::1%eth2

Adresy IPv6 w DNS

- DNS rekord typu AAAA
- revDNS domena ip6.arpa
 - Uwaga: revDNS stosuje notację bajt-kropka
 - Dla sieci 2001:db8::/64 będzie to:
0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa
- Dla kompatybilności adresów UNC w SO Windows, w których nie może występować dwukropek Microsoft stosuje domenę ip6-literal.net (DNS-hack)
 - 2001:db8::1
 - 2001-db8--1.ip6-literal.net
 - Np. \\2001-db8--1.ip6-literal.net\resource



Transmisja IPv6

- Natywna transmisja IPv6 w Ethernetie
 - Ethertype 86DD (IPv4 0800)
 - Multicast MAC Address 33-33-...
- Tunele 6in4
- Tunele 6to4
- Tunele Teredo
- Tunele 6rd
- Tunele ISATAP



Obsługa IPv6 w systemach operacyjnych **Windows**

W powszechnym użyciu są 3 rodzaje systemów z rodziny Windows.

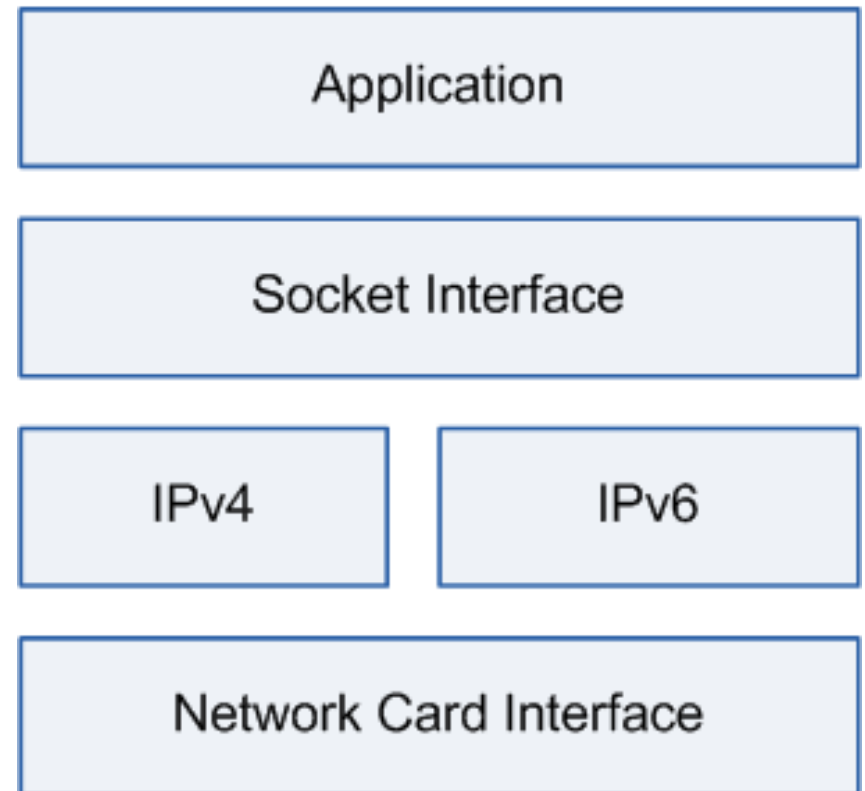
- NT 5.X – Windows 2000, Windows XP i Windows Server 2003
- NT 6.0 – Windows Vista i Windows Server 2008
- NT 6.1 – Windows 7 i Windows Server 2008 R2
- NT 6.2 – Windows 8 i Windows Server 2012
- NT 6.3 – Windows 8.1 i Windows Server 2012 R2

Rodzina NT 5.X wprowadziła obsługę IPv6 w bardzo ograniczonym zakresie (ręczna konfiguracja, wybrane usługi, niejednolita implementacja IPv4 i IPv6)



Dual Stack IPv4 i IPv6 w systemach NT 5.X

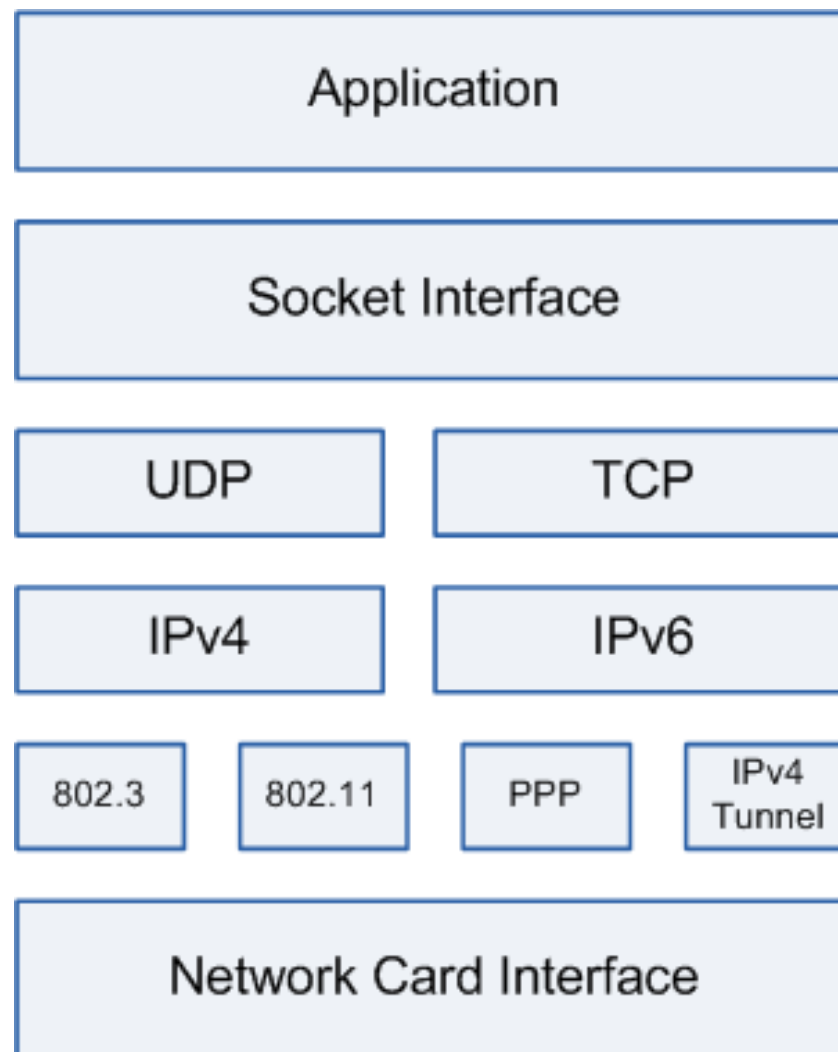
- Różna implementacja protokołów transportowych
- Brak rozszerzeń optymalizujących TCP/IP
- Obsługa tylko interfejsów Ethernet i FDDI (brak PPP)
- Rozdzielna implementacja IPSec uniemożliwia stosowanie wspólnych zasad uwierzytelniania
- Brak szyfrowania IPSec





Dual Stack IPv4 i IPv6 w systemach rodziny NT 6.X

- Domyślnie aktywna obsługa IPv6
- Jednolita implementacja protokołów transportowych
- Jednolite zasady zabezpieczeń w Active Directory





IPv6 w MS Windows

IPv6	Windows XP	Windows Server 2003	Windows 7/ Server 2008
Dual Stack IPv4/IPv6	YES	YES	YES
6to4 tunnel	Client only	Client only	YES
ISATAP	YES	YES	YES
Teredo tunnel	Client only	Client only	YES
IP-HTTPS tunnel	X	X	DirectAccess Only
LLMNR IPv6	NO	NO	YES
DNS (AAAA)	YES	YES	YES
DHCP	NO	NO	YES
Remote Desktop	NO	NO	YES
DirectAccess	X	X	YES
SNMP	MIB only	MIB only	YES (only NT6.X)
IPSec authentication	YES	YES	YES
IPSec encryption	NO	NO	YES



Konfiguracje do pracy w sieciach TCP/IP



Metody konfiguracji urządzeń w sieciach IP

- Manualne
 - Interfejs CLI
 - Interfejs GUI
 - Interfejs Webowy
 - Lokalne (konsola RS, konsola CLI i GUI)
 - Zdalne (Telnet, SSH, WWW)
- Automatyczne
 - DHCPv4 (RFC2131, RFC2132 dawniej RFC1541, RFC1533)
 - SLAAC IPv6 (RFC2462)
 - DHCPv6 (RFC3315)

Konfiguracja systemów MS Windows do pracy w sieci

Konfiguracja IP i DNS

Właściwości: Protokół internetowy (TCP/IP)

Ogólne Konfiguracja alternatywna

Przy odpowiedniej konfiguracji sieci możesz automatycznie uzyskać niezbędne ustawienia protokołu IP. W przeciwnym wypadku musisz uzyskać ustawienia protokołu IP od administratora sieci.

☒ Uzyskaj adres IP automatycznie

☐ Użyj następującego adresu IP:

Adres IP:

Maska podsieci:

Brama domyślna:

☒ Uzyskaj adres serwera DNS automatycznie

☐ Użyj następujących adresów serwerów DNS:

Preferowany serwer DNS:

Alternatywny serwer DNS:

Zaawansowane...

OK Anuluj

Właściwości: Protokół internetowy w wersji 6 (TCP/IPv6)

Ogólne

Ustawienia protokołu IPv6 mogą zostać przypisane automatycznie, jeśli używana sieć obsługuje taką możliwość. W przeciwnym razie należy skontaktować się z administratorem sieci, aby uzyskać odpowiednie ustawienia protokołu IPv6.

☒ Automatycznie uzyskaj adres IPv6

☐ Użyj następującego adresu IPv6:

Adres IPv6:

Długość prefiksu podsieci:

Brama domyślna:

☒ Uzyskaj adres serwera DNS automatycznie

☐ Użyj następujących adresów serwerów DNS:

Preferowany serwer DNS:

Alternatywny serwer DNS:

☐ Sprawdź przy zakończeniu poprawność ustawień

Zaawansowane...

OK Anuluj



Konfiguracja zapory

Dodawanie portu

Użyj tych ustawień, aby otworzyć port za pomocą Zapory systemu Windows. Aby znaleźć numer portu i protokół, zajrzyj do dokumentacji programu lub usługi, której chcesz użyć.

Nazwa:

Numer portu:

☒ TCP ☐ UDP

[Jakie ryzyko wiąże się z otwieraniem portu?](#)

Zmianianie zakresu

Aby określić zestaw komputerów, dla których ten port lub program jest odblokowany, kliknij opcję poniżej.

Aby określić listę niestandardową, wpisz rozdzielaną przecinkami listę adresów IP, podsieci lub obu.

☒ Dowolny komputer (łącznie z tymi w Internecie)

☐ Tylko moja sieć (podsieć)

☐ Lista niestandardowa:

Przykład: 192.168.114.201,192.168.114.201/255.255.255.0



Konfiguracja z wiersza poleceń

Konfiguracja IP i DNS z DHCP dla połączenia lokalnego

```
netsh interface ip set address "Połączenie lokalne" dhcp
```

```
netsh interface ip set dns "Połączenie lokalne" dhcp
```

```
netsh interface ip set wins "Połączenie lokalne" dhcp
```

Konfiguracja IP i DNS z DHCP dla połączenia o określonej nazwie

```
netsh interface ip set address "Połączenie sieci bezprzewodowej" dhcp
```

```
netsh interface ip set dns "Połączenie sieci bezprzewodowej" dhcp
```

```
netsh interface ip set wins "Połączenie sieci bezprzewodowej" dhcp
```

Uwaga: Do edycji skryptów zawierających znaki diakrytyczne należy używać programu EDIT, a nie NOTEPAD. System MS Windows stosuje różne kodowanie znaków diakrytycznych w konsoli (CP852) i w środowisku graficznym (Win1250).



Statyczna konfiguracja IP i DNS

```
netsh interface ip set address static "Połączenie lokalne" addr=192.0.2.10  
mask=255.255.255.0 gateway=192.0.2.254 gwmetric=1  
netsh interface ip set address static "Połączenie lokalne" 192.0.2.10 255.255.255.0  
192.0.2.254 1  
netsh interface ip add address static "Połączenie lokalne" 192.0.2.10 255.0.0.0  
netsh interface ip delete address "Połączenie lokalne" 192.0.2.10 ALL  
netsh interface ip set dns static "Połączenie lokalne" 192.0.2.1  
netsh interface ip add dns static "Połączenie lokalne" 192.0.2.100  
netsh interface ip set wins static "Połączenie lokalne" 192.0.2.1
```



Konfiguracja wyjątków zapory

```
netsh firewall add portopening TCP 80 WordWideWeb subnet
```

```
netsh firewall delete portopening TCP 80
```

```
netsh firewall set icmsetting 8 ENABLE
```

W ogólności:

netsh firewall add portopening

```
[ protocol = ] TCP|UDP|ALL
```

```
[ port = ] 1-65535
```

```
[ name = ] nazwa
```

```
[ [ mode = ] ENABLE|DISABLE
```

```
[ scope = ] ALL|SUBNET|CUSTOM
```

```
[ addresses = ] adresy
```

```
[ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

```
[ interface = ] nazwa ]
```

netsh firewall set icmpsetting

```
[ type = ] 2-5|8-9|11-13|17|ALL
```

```
[ [ mode = ] ENABLE|DISABLE
```

```
[ profile = ] CURRENT|DOMAIN|STANDARD|ALL
```

```
[ interface = ] nazwa ]
```



type - Typ protokołu ICMP.

2 - Zezwala na za duże pakiety wychodzące.

3 - Zezwala na nieosiągalność miejsca przeznaczenia danych wyjściowych.

4 - Zezwala na wygaszanie źródła wychodzącego.

5 - Zezwala na przekierowywanie.

8 - Zezwala na przychodzące żądanie echa.

9 - Zezwala na przychodzące żądanie routera.

11 - Zezwala na przekroczenie limitu czasu danych wyjściowych.

12 - Zezwala na problem z parametrem wychodzącym.

13 - Zezwala na przychodzące żądanie sygnatury czasowej.

17 - Zezwala na przychodzące żądanie maski.

ALL - Wszystkie typy.



Konfiguracja aplikacji dozwolonych dla zapory

```
netsh firewall add allowedprogram C:\www\wwwserv.exe wwwserv ENABLE
```

```
netsh firewall add allowedprogram C:\www\wwwserv.exe wwwserv ENABLE SUBNET
```

```
netsh firewall add allowedprogram C:\www\wwwserv.exe wwwserv ENABLE CUSTOM  
10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/24, LocalSubnet
```



Konfiguracja systemów Linux do pracy w sieci

Konfiguracja za pomocą DHCP

dhclient

#uruchomienie klienta dhcp

dhclient



Konfiguracja statyczna

```
ifconfig eth0 192.0.2.10 netmask 255.255.255.0 \
    broadcast 192.0.2.255
route add default gw 192.0.2.254
cat "nameserver 192.0.2.1" >/etc/resolv.conf
```

Dodatkowy adres IP (interfejs wirtualny)

```
ifconfig eth0:1 10.1.0.10 netmask 255.255.0.0
#wyłączenie
ifconfig eth0:1 down
#ponowne włączenie
ifconfig eth0:1 up
```



Konfiguracja statyczna za pomocą pakietu ip

#wylaczenie interfejsu

```
ip link set eth0 down
```

#wyczyszczenie poprzedniej konfiguracji

```
ip addr flush eth0
```

#ustawienie adresu

```
ip addr add 192.0.2.10/24 broadcast 192.0.2.255 dev eth0
```

```
ip -6 addr add 2001:db8:1::1/64 dev eth0
```

#włączenie

```
ip link set eth0 up
```

#routing

```
ip route add default via 192.0.2.254
```

```
ip -6 route add default via 2001:db8:1::FFFF
```