Computer Networks

Kamil NOWAK
Katedra Informatyki
Wydział Informatyki i Zarządzania Politechniki Wrocławskiej
kamil.nowak@pwr.edu.pl

Network layer of the ISO-OSI model
- IPv4 i IPv6 protocols
- Network addressing
- Subnetting with FLSM and VLSM method

Version 0.1-190325 transl. 191029

Keywords

IPv4, IPv6, adresacja IPv4, adresacja IPv6, maska, podsieć, adres sieci, adres hosta, adres broadcast, adres prywatny, adres publiczny, adres multicast, VLSM, CIDR, adresacja klasowa, adresacja bezklasowa

Introduction

Najbardziej powszechnym i podstawowym protokołem sieciowym występującym na świecie jest protokół IP (Internet Protocol). Protokół ten znajduje się w trzeciej warstwie modelu ISO-OSI lub drugiej modelu TCP/IP. Popularna nazwa globalnej sieci – Internet wywodzi się od nazwy tego protokołu. Pierwowzór sieci – sieć ARPANET powstał 1969r. na Uniwersytecie Kalifornijskim w Los Angeles (UCLA). Był to eksperymentalny projekt testowany dla potrzeb wojska, który miał funkcjonować pomimo uszkodzeń pewnej części sieci. Sieć testowa przekształciła się wkrótce w sieć użytkową. Do sieci dołączają się kolejne uniwersytety i użytkownicy. Stworzenie standardu prezentacji informacji html i serwerów WWW sprawiło, że sieć zaczęła się rozrastać w zaskakującym tempie. Początkowo sieć bazowała na adresacji klasowej. Szybko okazało się, że przewidziana z ogromnym nadmiarem pula adresów zaczyna się wyczerpywać. W celu lepszego zagospodarowania dostępnych adresów stworzono adresację bezklasową , adresy prywatne i usługę NAT. Dla coraz szybciej rozrastającego się Internetu było to niewystarczające, dlatego zaczęto opracowywać nową wersję tego protokołu. Obecna, stabilna wersja nosi nazwę IPv6. Protokół ten ma za zadanie zwiększyć pulę dostępnych adresów oraz zlikwidować wady poprzedniej wersji.

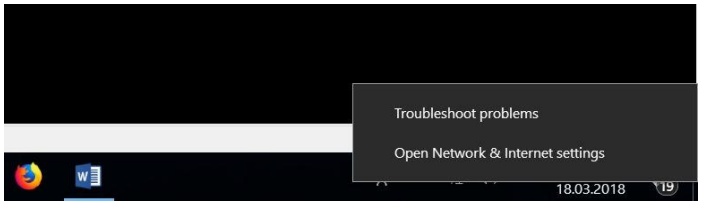
Spis treści

Konfiguracja adresu IP.

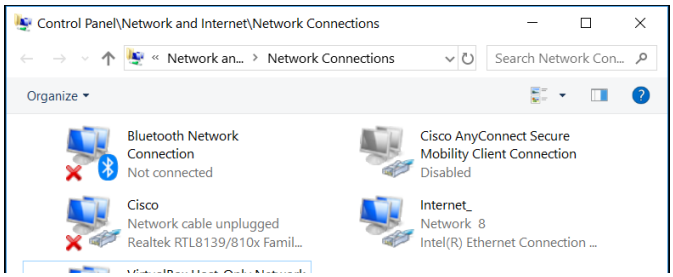
Konfiguracja IP w systemie Windows.

Konfiguracja w trybie GUI

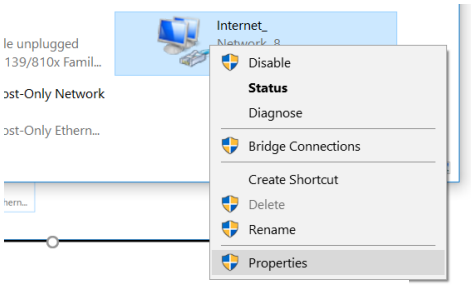
Poniższe obrazy przedstawiają proces ustawiania konfiguracji IPv4 i IPv6 w systemie Windows.



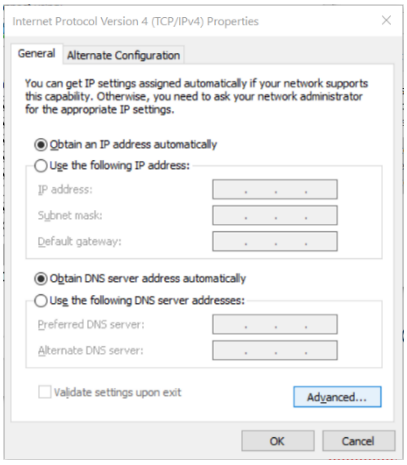
Rysunek 1 - Konfiguracja protokołu IP w systemie Windows. Szybkie dojście do opcji otwierającej konfigurację sieciową w Windows.



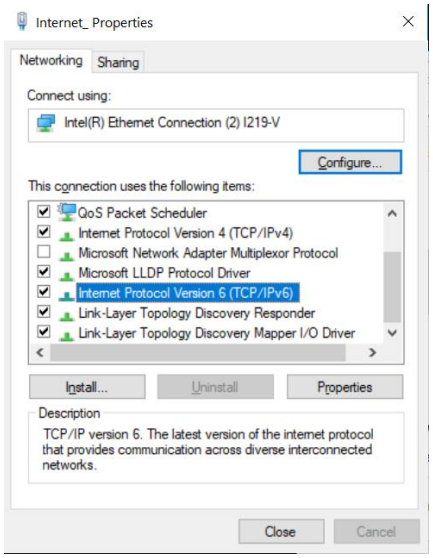
Rysunek 2 - - Konfiguracja protokołu IP w systemie Windows. Okono z interfejsami sieciowymi.



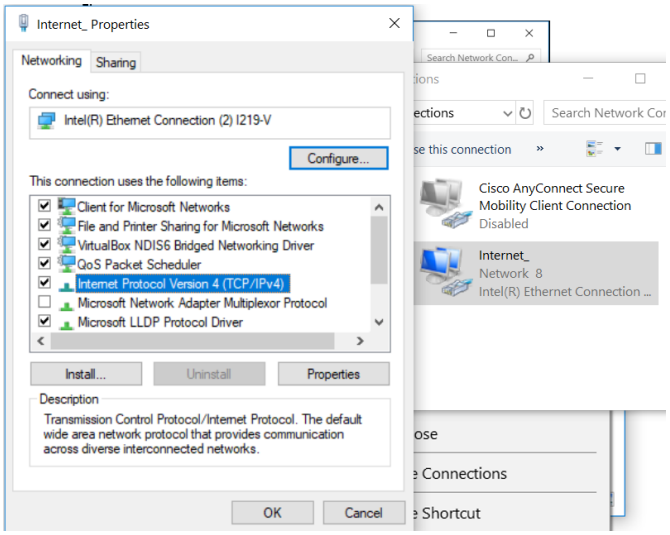
Rysunek 3 - - Konfiguracja protokołu IP w systemie Windows. Wybór właściwości karty sieciowej.



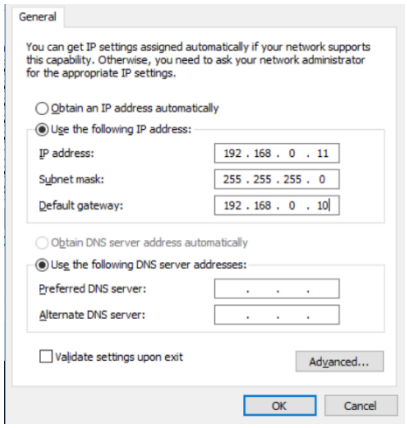
Rysunek 4 - Konfiguracja protokołu IP w systemie Windows. Wybór opcji automatycznej konfiguracji przez serwer DHCP.



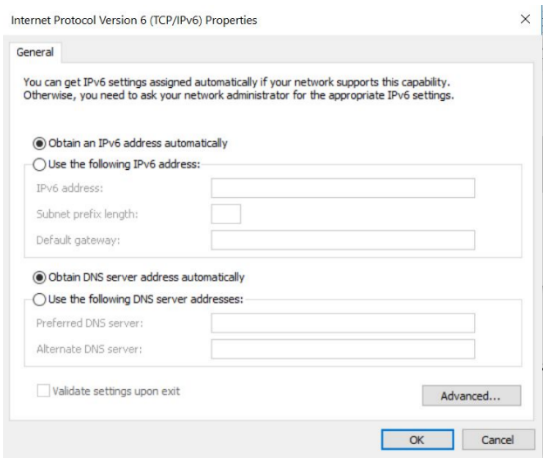
Rysunek 7 7 - Konfiguracja protokołu IP w systemie Windows. Wybór właściwości protokołu IPv6.



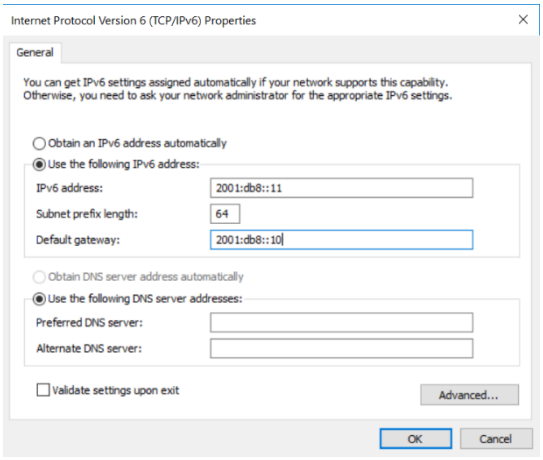
Rysunek 5 - Konfiguracja protokołu IP w systemie Windows. Wybór właściwości protokołu IPv4.



Rysunek 6 - Konfiguracja protokołu IP w systemie Windows. Konfiguracja ręczna adresu IPv4.



Rysunek 9 - Konfiguracja protokołu IP w systemie Windows. Wybór opcji automatycznej konfiguracji adresu.



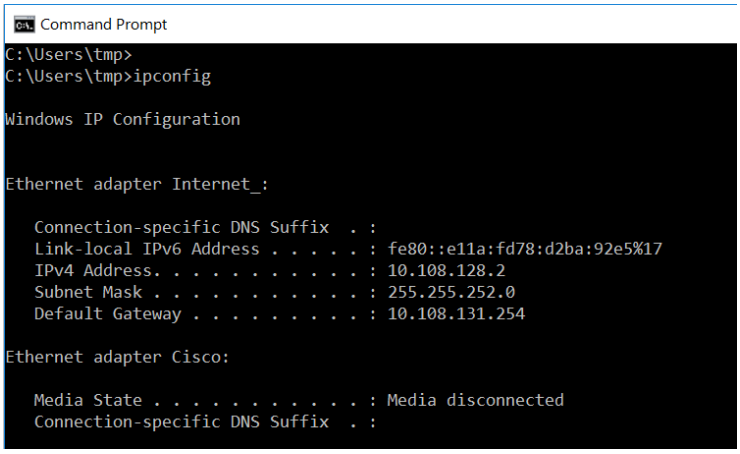
Rysunek 8 - Konfiguracja protokołu IP w systemie Windows. Konfiguracja ręczna adresu IPv6.

Aby sprawdzić poprawność konfiguracji protokołów IP w systemie Windows. Można skorzystać z interfejsu graficznego lub skorzystać z komendy `ipconfig` w oknie `cmd` (Command Line) Druga opcja jest pewniejsza, gdyż interfejs graficzny czasami może pokazać skonfigurowany adres, który w rzeczywistości nie zostanie przypisany do karty. Komendę można wykonać z dodatkowymi parametrami:

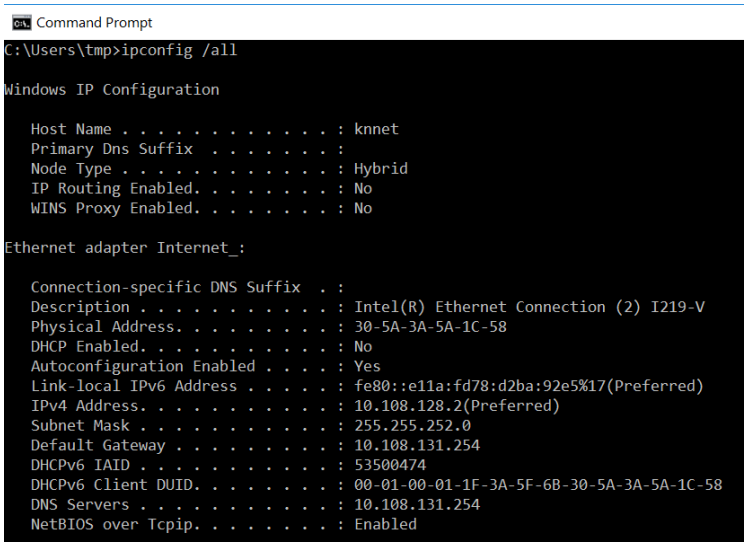
`ipconfig /all` - pokazuje dodatkowe informacje konfiguracyjne dotyczące np. adresu MAC, czy konfiguracji IPv6.

`ipconfig /release` – zwalnia adres IP przydzielony dynamicznie.

`ipconfig /renew` – ponownie pobiera adres IP na karcie skonfigurowanej dynamicznie.



Rysunek 10 - Konfiguracja protokołu IP w systemie Windows. Weryfikacja konfiguracji adresu IP komendą ipconfig.



Rysunek 11 - Konfiguracja protokołu IP w systemie Windows. Zawansowana weryfikacja konfiguracji karty sieciowej komendą ipconfig /all.

Konfiguracja w trybie CLI

W systemie Windows adres IP można ustawić również w oknie command line (cmd). Należy użyć narzędzia netsh. Można go używać w trybie wsadowym (wpisując wszystkie opcje w linii zaraz po polecniu netsh) lub jak shelu konfiguracyjnego (uruchamiamy netsh, a następnie poruszamy się po różnych poziomach tego skryptu).

Tryb interaktywny

```
netsh
netsh>/?
```

Tryb wsadowy

Konfiguracja adresu statycznego na karcie Cisco
Konfiguracja pełna

```
netsh interface ipv4 set address name="Cisco" source=static address=192.168.0.X1
mask=255.255.255.0 gateway=192.168.0.X0
```

Konfiguracja skrócona

```
netsh in ip set address "Cisco" static 192.168.0.X1 255.255.255.0 192.168.0.X0

netsh in ipv4 set dnsservers "Cisco" static 192.168.0.X0 primary

Konfiguracja adresu DHCP na karcie Internet
netsh in ipv4 set address name="Internet" dhcp
netsh in ip set dns "Internet" dhcp
```

Konfiguracja adresu IP w systemie Linux

Podobnie jak w systemie Windows, w systemie Linux można skonfigurować adres IP w trybie GUI lub CLI. Tryb graficzny nie jest polecany ze względu na różnorodność nakładek graficznych i ich nieprecyzyjne działanie. W trybie tekstowym wszystko powinno zadziałać poprawnie, jednak to również czekają na użytkownika niespodzianki. W różnych dystrybucjach Linuxa adres IP można konfigurować w różnych miejscach (różnych plikach). Poniżej podany jest przykład konfiguracji dla systemu Linux Debian. Konfigurację sieciową zmieniamy w pliku

```
/etc/network/interfaces
#Ustawienie adresu statycznego
auto eth0
```

```
iface eth0 inet static
address 192.168.0.X2
netmask 255.255.255.0
gateway 192.168.0.X0
dns-nameservers 156.17.5.2

#Ustawienie adresu dynamicznego
auto eth1
iface eth1 inet dhcp
```

Aktywowanie i sprawdzenie ustawień

```
ifdown eth0
ifup eth0
ifdown eth1
ifup eth1
ifconfig
```

Literatura

Materiały dydaktyczne Akademii Cisco CCNA 1

Laboratory tasks
- Network layer of the ISO-OSI model
- IPv4 and IPv6 addressing
- FLSM and VLSM subnetting

Variables and symbols used in the instruction

- X - the variable X corresponds to the device number, as well as the laboratory group number.
- Y – universal variable correspond to device number of any other group.

  K, L, M, N, ... - variables used interchangeably with the variables X and Y. Correspond to the devices and groups numbers.

  Note: The variables K, L, M, N, ... are used when the order of the connected devices is important. For example, when configuration on the R_K router differs from the R_L router configuration. The variable L should correspond to the number of the current device (current laboratory group number), variable K indicates the "left" device and M the "right" device.

  Variables X and Y are used when the order of the connected devices is not important. X means local device and Y means any remote device.
- A, B, C, ... - variables corresponding to the addresses of the networks created in the labs.
- [1.2.3.4] – the number of the CCNA lab corresponding to the current exercise.
- {Variable} - marks the required variable.
- [Variable] – marks an alternative variable.
- 2 points - task difficulty measure.
- COLORS - can be used to express some additional meaning:
  - **red - means extremely important things and obligatory tasks;**
  - orange - means additional/alternative tasks;
  - gray - means content that can be omitted in standard mode;
  - green – means additional information, explanations;
  - blue – means information to note to be checked by the instructor.
- FONT
  - **bold - highlighted information.**
  - `Courier New - configuration commands.`

IP addressing and device names used in the exercise

PCs

Name:		PC_X1
	Net:	LAN_X (Cisco)
	IP PC_L1:	192.168.X.X1/24
		fc00:X::X1/64
		fe80::X1
Gateway:		192.168.X.X0
		fc00:X::X0/64

Name:		PC_X2
	Net:	LAN_X (Cisco)

	IP PC_L2:	192.168.X.X2/24
		fc00:X::X2/64
		fe80::X2
Gateway:		192.168.X.X0
		fc00:X::X0/64

Switch

Name:		S_X
	Net:	LAN_X1
	Interface:	VLAN 1
	IP:	192.168.X.X9/24
		fc00:X::X9/64
		fe80::X9
Native VLAN:		VLAN 1
Gateway:		192.168.X.X0
		fc00:X::X0/64

Router

Name:		R_X
	Net:	LAN_X
	Interface:	Fa0/0 (Fa0/2/0, or another connected)
	IP:	192.168.X.X0/24
		fc00:X::X0/64
		fe80::X0
Gateway:		Loopback 1 (virtual interface)

X, L - the number of the current device.
K – the number of the previous device.
M – the number of the next device.
y – the number of the remote device.

Base topology of a single laboratory group

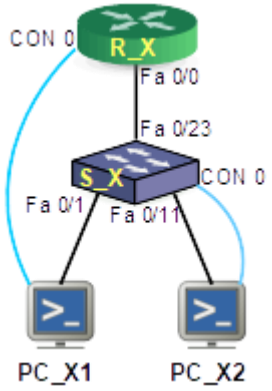


Figure 12 - Base topology of a single laboratory group.

The following connections have been configured in the base topology:

- PC_X1 intern NIC port - connected with a straight cable to S_X Fa 0/1 port.
- PC_X1 serial COM port - connected with a serial cable to R_X console port.
- PC_X2 intern NIC port - connected with a straight cable to S_X port Fa 0/11.

PC_X2 serial COM port - connected with a serial cable to S_X console port.
R_X port Fa 0/0 - connected with a straight cable to S_X Fa 0/23 port.

Lab topology

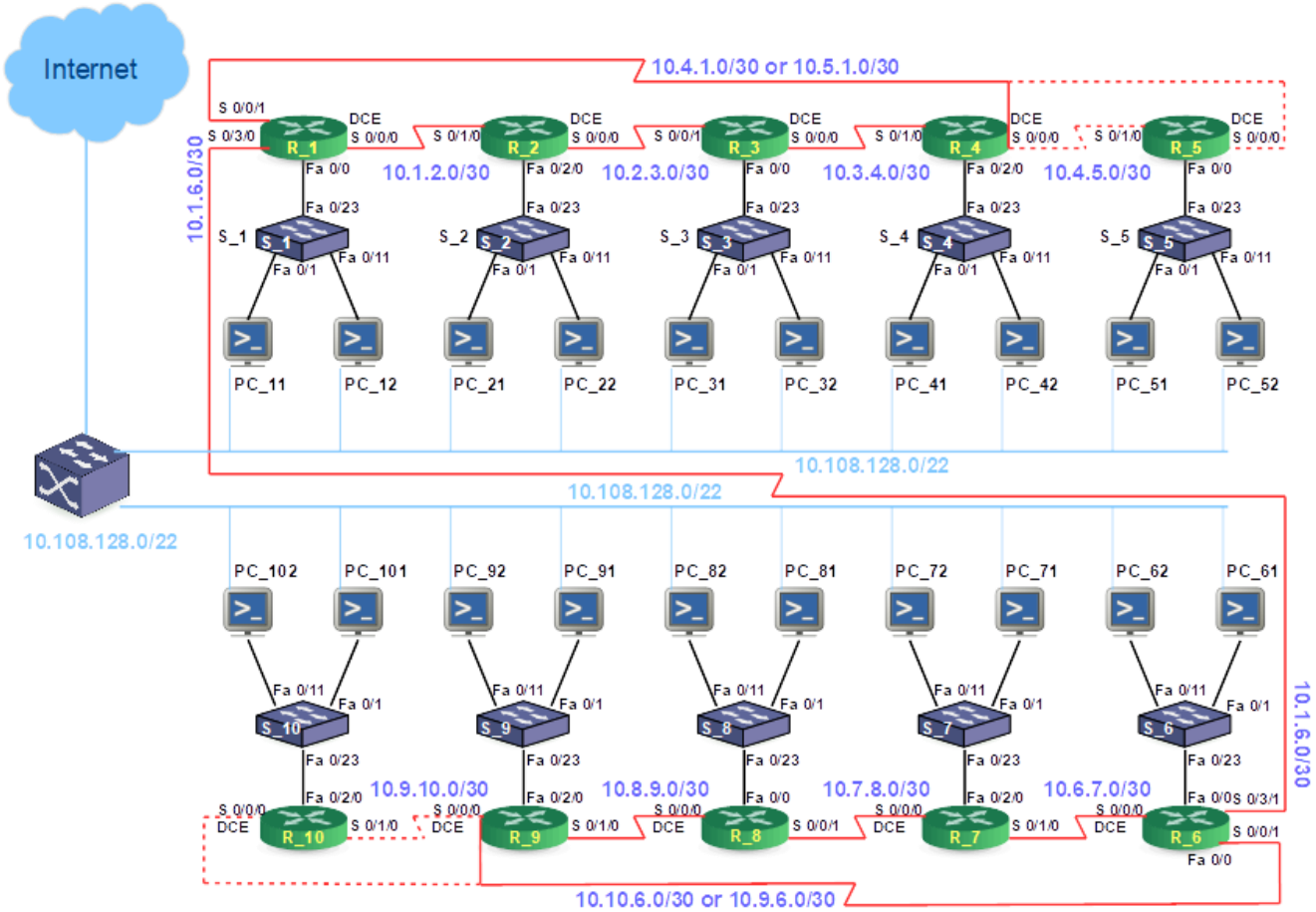


Figure 13 - Laboratory topology with double cabling.

Base PC configuration

Configure the computers using the IP addresses given in the instruction. Set the static IP address on the internal NIC (“Cisco”) that leads to the lab set. Set the dynamic IP address on the external NIC (“Internet”). Check the correctness of the configuration.

```
c:\>ipconfig
```

References to the CCNA 1 v. 6.0 labs

[7.1.2.9] - Converting IPv4 Addresses to Binary
[7.1.4.9] - Identifying IPv4 Addresses
[7.2.5.3] - Identifying IPv6 Addresses
[8.1.4.6] - Calculating IPv4 Subnets
[8.1.4.8] - Designing and Implementing a Subnetted IPv4 Addressing Scheme
[8.2.1.5] - Designing and Implementing a VLSM Addressing Scheme

References to the CCNA 1 v. 6.0 Packet Tracer scripts

[7.2.4.9] Packet Tracer - Configuring IPv6 Addressing
[7.3.2.5] Packet Tracer - Verifying IPv4 and IPv6 Addressing
[7.3.2.9] Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing
[8.1.4.7] Packet Tracer - Subnetting Scenario
[8.1.4.7] Packet Tracer - Subnetting Scenario 1

[8.2.1.4] Packet Tracer - Designing and Implementing a VLSM Addressing Scheme
[8.3.1.4] Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme

Note: tasks can be performed in two-person groups. Each task can be performed jointly or divided among group members.

Task 1 – Classful IPv4 network addressing (classes A, B, C, D, E)

Points: 1

Objectives

→ Familiarization with the classfull network addressing technique.
→ Differentiating addresses in terms of belonging to the selected class.
→ Differentiating addresses from special classes: multicast and reserved.
→ Documentation of network addressing.
→ Expert calculation of addresses:
- network,
- broadcast,
- the first and the last host address.

Practical task

The company network administrator should to analyze the addressing schema for invalid IP addresses. The company has addressing errors. In some places, forbidden addresses or addresses with incorrect masks are configured. One of the network segments still has RIP in its first version (classfull operation). Due to incorrectly selected classes of addresses, some of the networks are not routed.
nie są routowane.

Exercise scenario

1. Save the document in the user's home directory (eg: C:\cisco\users\user.name) and then open it to edit using Microsoft Word.
2. Complete the missing fields in the table. Try to not use the calculator.
3. Correct the wrong entries.

No	IP address	Fault Yes/No	Corrected host IP address or reason of fault	Class of address	Net bit number	Host bit number
1	1.100.200.30	No		A	8	24
2	144.61.72.83	No		B	16	16
3	220.91.122.23	No		C	24	8
4	230.31.32.33	Yes	**Designed for Multicasting**(D does not divide IPv4 into net-id and host-id.)	D	Non	Non
5	250.51.52.53	Yes	**Reserved for the Future Use** (The addresses in class E are not split into net-id and host-id)	E	Non	Non
6	11.255.255.255	Yes	Broadcast CLASS A	A	8	24

7	128.0.0.0	Yes	128.0.0.1	B	16	16
8	225.255.255.0	Yes	Subnet Mask C	D	Non	Non
9	224.0.0.3	Yes	**Designed for Multicasting**	D	Non	Non
10	254.255.5.6	Yes	**Reserved for the Future Use**	E	Non	Non

Table 1 - Classful IP addressing - calculation of mask length and class of address.

No		Binary format	Decimal format
		11111111.11111111.11111111.00000000	255.255.255.0
1	IP address	00000001.01100100.11001000.00011110	1.100.200.30
	Network mask	11111111.00000000.00000000.00000000	255.0.0.0
	Network address	00000001.00000000.00000000.00000000	1.0.0.0/8
	First host address	00000001.00000000.00000000.00000001	1.0.0.1
	Last host address	00000001.11111111.11111111.11111110	1.255.255.254
	Broadcast address	00000001.11111111.11111111.11111111	1.255.255.255
2	IP address	10010000.00111101.01001000.01010011	144.61.72.83
	Network mask	11111111.11111111.00000000.00000000	255.255.0.0
	Network address	10010000.00111101.00000000.00000000	144.61.0.0/16
	First host address	10010000.00111101.00000000.00000001	144.61.0.1
	Last host address	10010000.00111101.11111111.11111110	144.61.255.254
	Broadcast address	10010000.00111101.11111111.11111111	144.61.255.255
3	IP address	11011100.01011011.01111010.00010111	220.91.122.23
	Network mask	11111111.11111111.11111111.00000000	255.255.255.0
	Network address	11011100.01011011.01111010.00000000	220.91.122.0/24
	First host address	11011100.01011011.01111010.00000001	220.91.122.1
	Last host address	11011100.01011011.01111010.11111110	220.91.122.254
	Broadcast address	11011100.01011011.01111010.11111111	220.91.122.255

Table 2 - Classful IP addressing - calculation of the network address, broadcast of the first and last host. The binary form of the address.

4. After completing the exercise, make sure that the answers are saved.
5. You can continue to solve further tasks or ask the instructor to check the results.

Task 2 – Classless IPv4 network addressing

Points: 1

Objectives:

→ Familiarization with the classless network addressing technique.

→ Documentation of network addressing.

→ Expert calculation of classless addresses:

- network,

- broadcast,
- the first and the last host address.

Practical task

The administrator in the company was tasked with creating a classless addressing schema. Part of the old addresses should be corrected and some new addresses should be added.

Exercise scenario

1. Save the document in the user's home directory, and then open it in edit mode.
2. Verify the IPv4 network addressing in the table. Complete missing entries, correct any errors. Try to not use the calculator.

No	Host IP address	Fault Yes/No	Corrected IP address or reason of fault	Class of address	Subnet bits number (subnet mask – class mask)	Host bits number
1	1.100.200.30/12	No		A	12-8=4	32-12=20
2	144.61.72.83/20	No		B	20-16=4	32-20=12
3	220.91.122.23/28	No		C	28-24=4	32-28=4
4	30.31.255.255/16	Yes	4th Octet can be max 254	A	16-8=8	32-16=16
5	50.51.52.63/26	No		A	26-8=18	32-26=6
6	11.255.255.204/30	No		A	30-8=22	32-30=2
7	128.0.0.0/29	Yes	It stayed at the boundary	B	29-16=13	32-29=3
8	25.255.255.0/22	No		A	22-8=14	32-22=10
9	114.0.0.3/23	No		A	23-8=15	32-23=9
10	204.255.5.6/25	No		C	25-24=1	32-25=7

Table 3 - Classless IP addressing - calculation of the number of subnet and host bits.

Note: the number of subnet bits in the tables below should be calculated using the following formula:
Subnet bits = subnet mask bits – class mask bits

No		Binary format	Decimal format
		11111111.11111111.11111111.00000000	255.255.255.0
1	IP address	10010000.00111101.01001000.01010011	144.61.72.83/20
	Network mask	11111111.11111111.11110000.00000000	255.255.240.0
	Network address	10010000.00111101.01000000.00000000	144.61.64.0/20
	First host address	10010000.00111101.01000000.00000001	144.61.64.1
	Last host address	10010000.00111101.01001111.11111110	144.61.79.254
	Broadcast address	10010000.00111101.01001111.11111111	144.61.79.255
	Number of subnets	10000	2^4=16
	Hosts per subnet	111111111110	(2^12)-2=4094
2	IP address	11011100.01011011.01111010.00010111	220.91.122.23/28
	Network mask	11111111.11111111.11111111.11110000	255.255.255.240
	Network address	11011100.01011011.01111010.00010000	220.91.122.16/28
	First host address	11011100.01011011.01111010.00010001	220.91.122.17

	Last host address	11011100.01011011.01111010.00011110	220.91.122.30
	Broadcast address	11011100.01011011.01111010.00011111	220.91.122.31
	Number of subnets	10000	2^4=16
	Hosts per subnet	1110	(2^4)-2=14
3	IP address	11001100.11111111.00000101.00000110	204.255.5.6/25
	Network mask	11111111.11111111.11111111.10000000	255.255.255.128
	Network address	11001100.11111111.00000101.00000000	204.255.5.0/25
	First host address	11001100.11111111.00000101.00000001	204.255.5.1
	Last host address	11001100.11111111.00000101.01111110	204.255.5.126
	Broadcast address	11001100.11111111.00000101.01111111	204.255.5.127
	Number of subnets	10	2^1=2
	Hosts per subnet	1111110	(2^7)-2=126

Table 4 - Classless IP addressing - calculation of the network address, broadcast of the first and last host, number of subnets and number of hosts in the subnet. The binary form of the address.

3. After completing the exercise, make sure that the answers are saved.
4. You can continue to solve further tasks or ask the instructor to check the results.

Task 3 – Private, reserved and special addresses

Points: 1

Objectives:

→ Getting familiar with the private addresses used on the IP network.

→ Correct distinction non-routable private addresses.

→ Creation of addressing schema for the internal network (Intranet) without external access.

Practical task

The administrator in the company was asked to analyze the network address for invalid IP addresses. Private and public addresses have been incorrectly assigned in the company. Some network services are not available to external clients. Some protected resources have public addresses but should be accessible only from the Intranet. Some networks have already run out of public addresses. To enable access to an external network the private addressing and NAT service should be configured.

Exercise scenario

1. Save the document in the user's home directory, and then open it in edit mode.
2. Complete the missing fields in the table.
3. Correct the incorrect entries.

No	IP address	Class of address	Address public, private, other	Host IP address Yes/No	Type of address: host, network, broadcast, multicast, loopback, reserved, special	Subnet bits number (subnet mask – class mask)	Host bits number
1	127.1.2.3/8	A	Other	Yes	Loopback	8-8=0	32-8=24

2	10.61.72.83/20	A	Private	Yes	Network	20-8=12	32-1=20
3	172.20.122.23/28	B	Private	Yes	Network	28-16=12	32-28=4
4	192.168.0.255/18	C	Private	No	Network		
5	192.169.1.10/26	C	Public	Yes	Host	26-24=2	32-26=6
6	172.15.255.204/27	B	Public	Yes	Host	27-16=11	32-27=5
7	228.0.0.20/29	D	Other	Yes	Multicast	None	None
8	245.45.55.0/22	E	Other	Yes	Reserved	None	None
9	169.254.0.1/16	B	Other	Yes	Special	16-16=0	32-16=16
10	169.254.255.254/16	B	Other	Yes	Special	16-16=0	32-16=16

Table 5 – Private, reserved and special IPv4 addresses.

4. After completing the exercise, make sure that the answers are saved.
5. You can continue to solve further tasks or ask the instructor to check the results.

Task 4 – Verify the IPv6 network addressing in the table. Complete missing entries, correct any errors

Points: 1

Objectives:

→ Documentation of the IPv6 network addressing scheme.

→ Expert addresses calculation:

- Network;
- Broadcast;
- The first and the last host address.

→ Proper configuration of various types of IPv6 addresses.

→ Fluent calculation of IPv6 addresses compressed form.

Practical task

The company network administrator was tasked with creating an IPv6 address table. The company got the IPv6 network address and would like to have two protocols operating in parallel: IPv4 and IPv6. The administrator was also given the task of creating a local private addressing scheme enabling simple communication using short, private IPv6 addresses.

Exercise scenario

1. Save the document in the user's home and then open it to edit using Microsoft Word.
2. Complete the missing fields in the table.
3. Correct the wrong entries.

No		IPv6 hexadecimal format
1	IPv6 address	2000:3000:4000:5000:6000:7000:8000:9000/64
	Compressed IPv6 addres	2:3:4:5:6:7:8:9/64
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000

	Network address	2000:3000:4000:5000:0000:0000:0000:0000
	First host address	2000:3000:4000:5000:0000:0000:0000:0001
	Last host address	2000:3000:4000:5000:ffff:ffff:ffff:ffff
	Subnetwork ID	5
2	IPv6 address	3000:0003:0004:0005:0006:0007:0008:0009/64
	Compressed IPv6 addres	3000:3:4:5:6:7:8:9
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
	Network address	3000:0003:0004:0005:0000:0000:0000:0000
	First host address	3000:0003:0004:0005:0000:0000:0000:0001
	Last host address	3000:0003:0004:0005:ffff:ffff:ffff:ffff
	Subnetwork ID	5
3	IPv6 address	0002:0003:0004:0005:0006:0007:0008:0009
	Compressed IPv6 addres	2:3:4:5:6:7:8:9/64
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
	Network address	0002:0003:0004:0005:0000:0000:0000:0000
	First host address	0002:0003:0004:0005:0000:0000:0000:0001
	Last host address	0002:0003:0004:0005:ffff:ffff:ffff:ffff
	Subnetwork ID	5
4	IPv6 address	2000:0000:1234:0000:0000:0056:0000:0001/64
	Compressed IPv6 addres	2000:0:1234::56:0:1
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
	Network address	2000:0000:1234:0000:0000:0000:0000:0000
	First host address	2000:0000:1234:0000:0000:0000:0000:0001
	Last host address	2000:0000:1234:0000:ffff:ffff:ffff:ffff
	Subnetwork ID	56
5	IPv6 address	2222:0100:0200:0004:0000:0000:0000:fffe/64
	Compressed IPv6 addres	2222:100:200:x4::fffe
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
	Network address	2222:0100:0200:0004:0000:0000:0000:0000
	First host address	2222:0100:0200:0004:0000:0000:0000:0001
	Last host address	2222:0100:0200:0004:1111:1111:1111:1110
	Subnetwork ID	x4
6	IPv6 address	3232:0000:0000:1010:0001:0000:0000:0000
	Compressed IPv6 addres	3232::1010:1::/64
	Network mask	ffff:ffff:ffff:ffff:0000:0000:0000:0000
	Network address	3232:0000:0000:1010:0000:0000:0000
	First host address	3232:0000:0000:1010:0000:0000:0001
	Last host address	3232:0000:0000:1010:ffff:ffff:ffff:ffff
	Subnetwork ID	1010

Table 6 - IPv6 addressing - calculation of the network address, subnet ID, first and last host. A compressed form of the address.

No	IPv6 address	Address type; link-local, multicast, documentation, loopback, …
1	::/0	Default Route
2	::/128	Unspecified
3	::1/128	Loopback Address
4	fe80::10/64	Link-Local adress
5	ff02::1	Multicast adress
6	2001:db8:0:304::1/64	Documentation
7	3000:0000:0000:0128:1234:5678:aaaa:0029/64	Globally unicast
8	fc00:0:3:4::72/64	Unique local adress
9	fcff:0:10:6::1/64	Unique local adress
10	febf::2/64	Link-local adress

Table 7 IPv6 addressing - calculation of the network address, subnet ID, first and last host. A compressed form of the address.

4. After completing the exercise, make sure that the answers are saved.
5. You can continue to solve further tasks or ask the instructor to check the results.

Task 5 – Design of enterprise network addressing scheme using subnetworks with fixed mask length

Points: 1

Objectives:

→ Creation of FLSM address design for an enterprise network.

→ Expert adjustment of the mask length to create the right number of subnets.

→ Expert matching of mask length to create subnets with the right number of host addresses.

Practical task

The company has changed in the distribution and number of employees in individual departments. Another three-story building with an underground garage was attached to the company. The number of addresses and the division into subnets does not meet current needs.
The administrator was tasked with creating a new network addressing scheme. Due to the large address pool, the division is to be relatively simple and should to base on a fixed length subnet mask (FLSM).

Exercise scenario

1. Save the text document into the user's home directory, then open it to edit.
2. Following the requirements given below, design the enterprise network subnetting scheme using a fixed mask length method.

   Use the address 193.17.130.0/24.

The network administrator reviewed the enterprise demand and wrote down the following requirements for the number of subnets and the number of IP addresses in each subnet. The requirements are presented in the table below:

No	Group name	Demand for IP addresses
1	Designers	13
2	Accounting	14
3	Marketing	7
4	Security	9
5	Secretariat	6
6	Managemnt	12
7	Public wi-fi network	8
8	Point to point connections between routers – 8	2 per connection

Table 8 – Table of requirements for a computer network with a fixed mask length subnets.

3. Complete the appropriate document.

No	Name	Network details
1	Group name	Designers
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	13
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
2	Group name	Accounting
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	14
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
3	Group name	Marketing
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	7
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
4	Group name	Security
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	9
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24

5	Group name	Secretariat
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	6
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
6	Group name	Management
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	12
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
7	Group name	Public wi-fi network
	Network address	193.17.130.64/24
	Subnet bits number	26
	Required IP address count	8
	First host address	193.17.130.65/24
	Last host address	193.17.130.126/24
	Broadcast address	193.17.130.127/24
8	Group name	Point to point connections between routers
	Network address	193.17.130.64/24
	Subnet bits number	26
	Required IP address count	2 per
	First host address	193.17.130.65/24
	Last host address	193.17.130.126/24
	Broadcast address	193.17.130.127/24

Table 9 - Addressing table for a computer network with a fixed mask length subnets.

4. After completing the exercise, make sure that the answers are saved.
5. You can continue to solve further tasks or ask the instructor to check the results.

Task 6 – Design of enterprise network addressing scheme using subnetworks with variable length masks (VLSM)

Points: 1

Objectives:

→ Creation of an enterprise network addressing scheme using a variable length mask method (VLSM).

→ Expert adjustment of the mask length to the quantitative requirements in individual subnets.

→ Economical management of the available IP address pool.

Practical task

Due to the signing of an attractive contract, the company hired a large number of new employees. The existing network addressing model cannot allow everyone free access to resources. Service servers and computers of some employees lacked public IP addresses. The available company address pool theoretically allows to connect all network devices, but many addresses are wasted. Particularly high address losses occur in point-to-point connections.
The administrator was tasked with reworking the addressing scheme in order to increase the number of available addresses. The technique VLSM should be used.

Exercise scenario

1. Save the text document into the user's home directory, then open it to edit.
2. Following the requirements given below, design the enterprise network subnetting scheme using a variable length subnet mask.

   Use the address 193.17.130.0/24.

   The network administrator reviewed the enterprise demand and wrote down the following requirements for the number of subnets and the number of IP addresses in each subnet.
   The requirements are presented in the table below:

No	Group name	Demand for IP addresses
1	Designers	33
2	Accounting	16
3	Marketing	7
4	Security	9
5	Secretariat	6
6	Managemnt	12
7	Public wi-fi network	40
8	Point to point connections between routers – 8	2 per connection

Table 10 - Table of requirements for a computer network configured with variable length mask method.

3. Complete the appropriate document.

No	Name	Network details
1	Group name	Designers
	Network address	193.17.130.0/24
	Subnet bits number	26
	Required IP address count	33
	First host address	193.17.130.1/24
	Last host address	193.17.130.62/24
	Broadcast address	193.17.130.63/24
2	Group name	Accounting
	Network address	193.17.130.64/24

	Subnet bits number	27
	Required IP address count	16
	First host address	193.17.130.65/24
	Last host address	193.17.130.94/24
	Broadcast address	193.17.130.95/24
3	Group name	Marketing
	Network address	193.17.130.96/24
	Subnet bits number	28
	Required IP address count	7
	First host address	193.17.130.97/24
	Last host address	193.17.130.102/24
	Broadcast address	193.17.130.111/24
4	Group name	Security
	Network address	193.17.130.112/24
	Subnet bits number	28
	Required IP address count	9
	First host address	193.17.130.113/24
	Last host address	193.17.130.126/24
	Broadcast address	193.17.130.127/24
5	Group name	Secretariat
	Network address	193.17.130.128/24
	Subnet bits number	29
	Required IP address count	6
	First host address	193.17.130.129/24
	Last host address	193.17.130.134/24
	Broadcast address	193.17.130.135/24
6	Group name	Management
	Network address	193.17.130.136/24
	Subnet bits number	28
	Required IP address count	12
	First host address	193.17.130.137/24
	Last host address	193.17.130.150/24
	Broadcast address	193.17.130.151/24
7	Group name	Public wi-fi network
	Network address	193.17.130.152/24
	Subnet bits number	26
	Required IP address count	40
	First host address	193.17.130.153/24
	Last host address	193.17.130.214/24
	Broadcast address	193.17.130.215/24
8	Group name	Point to point connections between routers
	Network address	193.17.130.216/24
	Subnet bits number	28
	Required IP address count	2per(per taken 6)
	First host address	193.17.130.217/24
	Last host address	193.17.130.230/24

	Broadcast address	193.17.130.231/24

Table 11 - Addressing table for a computer network configured with variable mask lengths method.

4. After completing the exercise, make sure that the answers are saved.
5. You can continue to solve further tasks or ask the instructor to check the results.

Zadania laboratoryjne w środowisku wirtualnym. Symulator Packet Tracer.
Warstwa sieciowa modelu ISO-OSI.

Środowisko programu Packet Tracer umożliwia analizę działania i konfigurację różnych urządzeń sieciowych. Konfiguracja IP jest możliwa w wirtualnym środowisku na różne sposoby:

- Przy użyciu graficznego interfejsu użytkownika
- Przy użyciu interfejsu CLI (Command Line Interface)