Protokół IP

Protokół po raz pierwszy użyty w 1983 roku w sieci ARPANET. Zarządzaniem adresami IP zajmuje się IANA (*Internet Assigned Numbers Authority*), a przydziela je operator ICANN (*Internet Committee for Assigned Names and Numbers*).

Cechy protokołu:

a) bezpołączeniowość - przed wysłaniem danych, z odbiorcą nie jest ustanawiane żadne połączenie (odbiorca nie wie, że otrzyma dane);

b) dostarczenie pakietów nie jest gwarantowane (mogą być uszkodzone, dostarczone w innej kolejności lub w ogóle);

c) niezależność od mediów transmisji (światłowód, kabel miedziany, fale radiowe).

Ilość unikalnych adresów w Internecie

IPv4 → 2^{32} (4 294 967 296)

IPv6 → 2^{128} (340 282 366 920 938 463 463 374 607 431 768 211 456)

Rodzaje sieci

LAN (*Local Area Network*) - sieć o zasięgu lokalnym

WAN (*Wide Area Network*) - sieć rozległa

IP: **192.168.10.14**

Maska: **255.255.255.0**

Brama: **192.168.10.1**

Broadcast: **192.168.10.255**

Uwagi:

- Jeśli połączenie jest nawiązywane z maszyną w tej samej sieci LAN - router nie bierze udziału w połączeniu i brama domyślna nie jest konieczna.
- Broadcast występuje tylko w protokole IPv4.

Podział numeracji

Klasowa: podzielona umownie na klasy A, B, C (bez masek podsieci);

Bezklasowa (CIDR): wprowadzona w 1993 roku, z użyciem masek podsieci.

Publiczna numeracja IPv4

Historyczna numeracja klasowa (maski dodano w 1993 roku → CIDR)

Klasa **A**: 1.**xxx.xxx.xxx** - 126.**xxx.xxx.xxx**

(maska 16-bitowa: 255.**0.0.0**)

Klasa **B**: 128.sss.**xxx.xxx** - 191.sss.**xxx.xxx**

(maska 24-bitowa: 255.255.**0.0**)

Klasa **C**: 192.sss.sss.**xxx** - 223.sss.sss.**xxx**

(maska 32-bitowa: 255.255.255.**0**)

Także adresy edukacyjne TEST-NET (klasa D): 192.168.2.0 - 192.168.2.255 oraz multicastowe (np. protokoły routingu) 224.0.0.0 - 239.255.255.255; oraz adresy eksperymentalne (klasa E) 240.0.0.0 - 255.255.255.255.

Prywatna numeracja IPv4

Historyczna numeracja klasowa (maski dodano w 1993 roku → CIDR)

Prywatną numerację określa dokument RFC 1918 (“*Address Allocation for Private Internets*”). W przypadku IPv6 nie ma podziału na numerację publiczną i prywatną:

Klasa **A** (mało sieci, ale bardzo duże)

10.**0**.**0**.**0** - 10.**255**.**255**.**255**/8 (255.0.0.0)

Klasa **B**

172.**16**.**0**.**0** - 172.**31**.**255**.**255**/12 (255.240.0.0)

Klasa **C** (dużo sieci, ale bardzo małych)

192.168.**0**.**0** - 192.168.**255**.**255**/16 (255.255.0.0)

Wyjątkiem w klasie C jest grupa publicznych adresów edukacyjnych TEST-NET: 192.168.2.0 - 192.168.2.255.

Oktety

Adresy IPv4 zapisywane w systemie dziesiętnym, tak naprawdę mają postać oktetów (liczby binarne zgrupowane po osiem).
I tak, adres sieci (np. 192.168.0.**0**) ma rzeczywistą postać:

11000000.10101000.00000000.**00000000**

Adres rozgłoszeniowy w tej sieci (192.168.0.**255**) ma postać:

11000000.10101000.00000000.**11111111**

Dzielenie sieci

Po co dzielimy sieć?

1. Redukcja ruchu rozgłoszeniowego.

2. Podział logiczny (np. na działy: marketing, księgowość, produkcja, IT).

3. Redukcja kosztów w przypadków adresów publicznych.

Dzielenie sieci 192.168.0.0

1. Ilość adresów IP w dzielonych podsieciach **nie może** być dowolna (np. 200) i musi być zawsze jakąś potęgą liczby 2 (potęga = bity).

2. Podział zawsze zaczynamy od części z największą liczbą adresów.

3. Jeśli ilość adresów jest większa niż 128 (np. 150) to nie dzielimy takiej sieci.

4. Równy podział na podsieci to jednakowa maska dla każdej z nich. Może to jednak powodować marnotrawienie niewykorzystanych adresów IP.

5. Nierówny podział na podsieci (VLSM - *Variable Length Subnet Masking*) to różne maski dla każdej z nich. Równe podsieci dzielone są na pod-podsieci.

Notacja CIDR (*Classless Inter-Domain Routing*, 1993)

O przynależności do sieci nie decyduje już sam adres IP, lecz jego powiązanie z maską podsieci.

Adres sieci		*Maska*	*Wolne bity*	*Ilość adresów LAN*
192.168.12.0/**32**	→	255.255.255.**255**	2^0	1
192.168.12.0/**31**	→	255.255.255.**254**	2^1	2
192.168.12.0/**30**	→	255.255.255.**252**	2^2	4
192.168.12.0/**29**	→	255.255.255.**248**	2^3	8
192.168.12.0/**28**	→	255.255.255.**240**	2^4	16
192.168.12.0/**27**	→	255.255.255.**224**	2^5	32
192.168.12.0/**26**	→	255.255.255.**192**	2^6	64
192.168.12.0/**25**	→	255.255.255.**128**	2^7	128
192.168.12.0/**24**	→	255.255.255.**0**	2^8	256
192.168.12.0/**23**	→	255.255.**254**.**0**	2^9	512

Łączenie 2 sieci: 192.168.12.0/**23** = 192.168.12.0/**24** + 192.168.13.0/**24**

Notacja CIDR (*Classless Inter-Domain Routing*, 1993)

Adres sieci		*Maska*	*Wolne bity*	*Ilość adresów LAN*
192.168.12.0/**23**	→	255.255.**254**.**0**	2^{9}	512
192.168.12.0/**22**	→	255.255.**252**.**0**	2^{10}	1024
192.168.12.0/**21**	→	255.255.**248**.**0**	2^{11}	2048
192.168.12.0/**20**	→	255.255.**240**.**0**	2^{12}	4096
192.168.12.0/**19**	→	255.255.**224**.**0**	2^{13}	8192
192.168.12.0/**18**	→	255.255.**192**.**0**	2^{14}	16384
192.168.12.0/**17**	→	255.255.**128**.**0**	2^{15}	32768
192.168.12.0/**16**	→	255.255.**0**.**0**	2^{16}	65536
192.168.12.0/**15**	→	255.**254**.**0**.**0**	2^{17}	131072
192.168.12.0/**14**	→	255.**252**.**0**.**0**	2^{18}	262144
192.168.12.0/**13**	→	255.**248**.**0**.**0**	2^{19}	524288

Adres sieci		*Maska*	*Wolne bity*	*Ilość adresów LAN*
192.168.12.0/**12**	→	255.**240**.**0**.**0**	2^{20}	1048576
192.168.12.0/**11**	→	255.**224**.**0**.**0**	2^{21}	2097152
192.168.12.0/**10**	→	255.**192**.**0**.**0**	2^{22}	4194304
192.168.12.0/**9**	→	255.**128**.**0**.**0**	2^{23}	8388608
192.168.12.0/**8**	→	255.**0**.**0**.**0**	2^{24}	16777216
192.168.12.0/**7**	→	**254**.**0**.**0**.**0**	2^{25}	33554432
192.168.12.0/**6**	→	**252**.**0**.**0**.**0**	2^{26}	67108864
192.168.12.0/**5**	→	**248**.**0**.**0**.**0**	2^{27}	134217728
192.168.12.0/**4**	→	**240**.**0**.**0**.**0**	2^{28}	268435454
192.168.12.0/**3**	→	**224**.**0**.**0**.**0**	2^{29}	536870912
192.168.12.0/**2**	→	**192**.**0**.**0**.**0**	2^{30}	1073741824
192.168.12.0/**1**	→	**128**.**0**.**0**.**0**	2^{31}	2147483648
192.168.12.0/**0**	→	**0.0.0.0**	2^{32}	4 294 967 296

Uwaga!

Maska podsieci mówi tylko o tym, **ile** adresów IP może być użytych w danej podsieci. Nie określa jednak dokładnego **zakresu** tych adresów (początku i końca puli adresowej). O tym decyduje **adres podsieci** (wyznacza początek puli) oraz **broadcast** (wyznacza jej koniec). Routery nie przekazują broadcastu.

Notacja CIDR (*Classless Inter-Domain Routing*, 1993)

O przynależności do sieci nie decyduje już sam adres IP, lecz jego powiązanie z maską podsieci.

Adres sieci		*Maska w wersji bitowej (binarnej)*
192.168.12.0/**32**	→	11111111.11111111.11111111.11111111
192.168.12.0/**31**	→	11111111.11111111.11111111.1111111**0**
192.168.12.0/**30**	→	11111111.11111111.11111111.111111**00**
192.168.12.0/**29**	→	11111111.11111111.11111111.11111**000**
192.168.12.0/**28**	→	11111111.11111111.11111111.1111**0000**
192.168.12.0/**27**	→	11111111.11111111.11111111.111**00000**
192.168.12.0/**26**	→	11111111.11111111.11111111.11**000000**
192.168.12.0/**25**	→	11111111.11111111.11111111.1**0000000**
192.168.12.0/**24**	→	11111111.11111111.11111111.**00000000**
192.168.12.0/**23**	→	11111111.11111111.1111111**0.00000000**

Adres sieci		*Maska w wersji bitowej (binarnej)*
192.168.12.0/**22**	→	11111111.11111111.11111**00**.**00000000**
192.168.12.0/**21**	→	11111111.11111111.11111**000**.**00000000**
192.168.12.0/**20**	→	11111111.11111111.1111**0000**.**00000000**
192.168.12.0/**19**	→	11111111.11111111.111**00000**.**00000000**
192.168.12.0/**18**	→	11111111.11111111.11**000000**.**00000000**
192.168.12.0/**17**	→	11111111.11111111.1**0000000**.**00000000**
192.168.12.0/**16**	→	11111111.11111111.**00000000**.**00000000**
192.168.12.0/**15**	→	11111111.1111111**0**.**00000000**.**00000000**
192.168.12.0/**14**	→	11111111.111111**00**.**00000000**.**00000000**
192.168.12.0/**13**	→	11111111.11111**000**.**00000000**.**00000000**
192.168.12.0/**12**	→	11111111.1111**0000**.**00000000**.**00000000**
192.168.12.0/**11**	→	11111111.111**00000**.**00000000**.**00000000**
192.168.12.0/**10**	→	11111111.11**000000**.**00000000**.**00000000**

Adres sieci	*Maska w wersji bitowej (binarnej)*
192.168.12.0/**9** →	11111111.1**0000000**.**00000000**.**00000000**
192.168.12.0/**8** →	11111111.**00000000**.**00000000**.**00000000**
192.168.12.0/**7** →	1111111**0**.**00000000**.**00000000**.**00000000**
192.168.12.0/**6** →	111111**00**.**00000000**.**00000000**.**00000000**
192.168.12.0/**5** →	11111**000**.**00000000**.**00000000**.**00000000**
192.168.12.0/**4** →	1111**0000**.**00000000**.**00000000**.**00000000**
192.168.12.0/**3** →	111**00000**.**00000000**.**00000000**.**00000000**
192.168.12.0/**2** →	11**000000**.**00000000**.**00000000**.**00000000**
192.168.12.0/**1** →	1**0000000**.**00000000**.**00000000**.**00000000**
192.168.12.0/**0** →	**00000000**.**00000000**.**00000000**.**00000000**

Sumaryzacja IPv4 (agregacja)

Router ustanawia jedną trasę (o szerszej masce), która obejmuje swoim zasięgiem kilka sieci o węższych maskach (wszystkie muszą być podpięte do jednego interfejsu). Aby ustalić adres sumaryczny, należy zamienić adresy sieci na postać binarną i sprawdzić zgodność bitów zaczynając od lewej strony. Ilość tych bitów będzie oznaczać maskę sumaryczną.

172.20.0.0/16 10101100.00010100.00000000.00000000

172.21.0.0/16 10101100.00010101.00000000.00000000

172.22.0.0/16 10101100.00010110.00000000.00000000

172.23.0.0/16 10101100.00010111.00000000.00000000

Zgodnych jest 14 bitów, więc maska sumaryczna to /14 (255.252.0.0). Aby określić adres sumaryczny sieci, zachowujemy tylko zgodne bity, a resztę zamieniamy na 0.

10101100.000101**00**.00000000.00000000 → **172.20.0.0/14**

Sumaryzacja IPv6 (agregacja)

W tym przypadku, tylko różniącą się część adresu zamieniamy na postać binarną.

2001:0DB8:ACAD:0001::/64 → 2001:0DB8:ACAD:0000000000000001::/64

2001:0DB8:ACAD:0002::/64 → 2001:0DB8:ACAD:0000000000000010::/64

2001:0DB8:ACAD:0003::/64 → 2001:0DB8:ACAD:0000000000000011::/64

2001:0DB8:ACAD:0004::/64 → 2001:0DB8:ACAD:0000000000000100::/64

Zgodnych jest 61 bitów (16+16+16+13), więc maska sumaryczna to /61. Aby określić adres sumaryczny sieci, zachowujemy tylko zgodne bity, a resztę zamieniamy na 0.

2001:0DB8:ACAD:0000000000000**000**::/61 → 2001:0DB8:ACAD:0000::/61

w formie skróconej:

2001:DB8:ACAD::/61

Maski dziesiętne na binarne

Maski dziesiętne	Maski binarne	Ilość adresów IP
0	0000 0000	**255**
128	1000 0000	**128**
192	1100 0000	**64**
224	1110 0000	**32**
240	1111 0000	**16**
248	1111 1000	**8**
252	1111 1100	**4**
254	1111 1110	**2**
255	1111 1111	**0**

Wyznaczanie adresu sieci dla hosta

10.1.8.200/26

Zamiana na oktety z liczbami binarnymi:

00001010.00000001.00001000.11001000

Maska 26-bitowa:

11111111.11111111.11111111.11000000

Wynik operacji AND numeru hosta i jego maski (koniunkcja z algebry Boole’a):

00001010.00000001.00001000.11000000

Ponowna zamiana na liczby dziesiętne:

10.1.8.**192**

I to jest właśnie adres sieci dla hosta o numerze 10.1.8.200/26!

Ilość możliwych hostów

10.1.8.200/26

Zamiana na oktety z liczbami binarnymi:

00001010.00000001.00001000.11001000

Maska 26-bitowa:

11111111.11111111.11111111.11000000

Wynik operacji AND numeru hosta i jego maski (koniunkcja z algebry Boole'a):

00001010.00000001.00001000.11**000000**

Do wykorzystania mamy więc dostępnych 6 bitów:

$2^6-2=$**62**

(numery użyteczne w podsieci po odliczeniu numeru sieci i numeru *broadcast*)

Inny sposób (wynik koniunkcji z powrotem na system dziesiętny):

10.1.8.**192** → 256-192=64-2=**62**

Operacja AND wykorzystywana jest także do określenia, czy pakiet z danym IP jest skierowany do wewnętrznej sieci czy do zewnętrznej sieci.

Ilość możliwych podsieci

$$2^n = \text{ilość podsieci}$$

gdzie **n** to ilość **pożyczonych** bitów z części hosta dla części sieci, np.

11111111.11111111.11111111.**11**000000

Pożyczone są dwa bity z części hosta, więc maska to **/26**
(255.255.255.**192**), a ilość możliwych podsieci to:

$$2^2 = 4$$

Przykład podziału sieci

Dzielimy sieć 192.168.0.**0**/24 na 4 równe części

1. **Router nr 1**
Adres sieci: 192.168.0.**0**/26
Maska: 255.255.255.192
Brama: 192.168.0.**1**
Broadcast: 192.168.0.**63**
Dostępne adresy: 192.168.0.**2-62**

2. **Router nr 2**
Adres sieci: 192.168.0.**64**/26
Maska: 255.255.255.192
Brama: 192.168.0.**65**
Broadcast: 192.168.0.**127**
Dostępne adresy: 192.168.0.**66-126**

3. **Router nr 3**
Adres sieci: 192.168.0.**128**/26
Maska: 255.255.255.192
Brama: 192.168.0.**129**
Broadcast: 192.168.0.**191**
Dostępne adresy: 192.168.0.**130-190**

4. **Router nr 4**
Adres sieci: 192.168.0.**192**/26
Maska: 255.255.255.192
Brama: 192.168.0.**193**
Broadcast: 192.168.0.**255**
Dostępne adresy: 192.168.0.**193-254**

Przykład podziału sieci

Dzielimy sieć 10.**0**.**0**.**0**/8 na równe części (podział na sieci 10.0.**0**.**0**/16).

1. **Router nr 1**
Adres sieci: 10.1.**0**.**0**/16
Maska: 255.255.**0**.**0**
Brama: 10.1.**0**.**1**
Broadcast: 10.1.**255**.**254**
Dostępne adresy: **65535**

2. **Router nr 2**
Adres sieci: 10.2.**0**.**0**/16
Maska: 255.255.**0**.**0**
Brama: 10.2.**0**.**1**
Broadcast: 10.2.**255**.**254**
Dostępne adresy: **65535**

3. **Router nr 3**
Adres sieci: 10.3.**0**.**0**/16
Maska: 255.255.**0**.**0**
Brama: 10.3.**0**.**1**
Broadcast: 10.3.**255**.**254**
Dostępne adresy: **65535**

4. **Router nr 4**
Adres sieci: 10.4.**0**.**0**/16
Maska: 255.255.**0**.**0**
Brama: 10.4.**0**.**1**
Broadcast: 10.4.**255**.**254**
Dostępne adresy: **65535**

...itd. aż do 256 podsieci.

Przykład podziału nierównego

Dzielimy sieć 192.168.0.**0**/24 na 3 nierówne części
(*VLSM - Variable Length Subnet Mask*)

1. **Router nr 1**
Adres sieci: 192.168.0.**0**/25
Maska: 255.255.255.128
Brama: 192.168.0.**1**
Broadcast: 192.168.0.**127**
Dostępne adresy: 192.168.0.2-126

2. **Router nr 2**
Adres sieci: 192.168.0.**128**/26
Maska: 255.255.255.192
Brama: 192.168.0.**129**
Broadcast: 192.168.0.**191**
Dostępne adresy: 192.168.0.130-190

3. **Router nr 3**
Adres sieci: 192.168.0.**192**/26
Maska: 255.255.255.192
Brama: 192.168.0.**193**
Broadcast: 192.168.0.**255**
Dostępne adresy: 192.168.0.194-254

Inne tabele podziałów

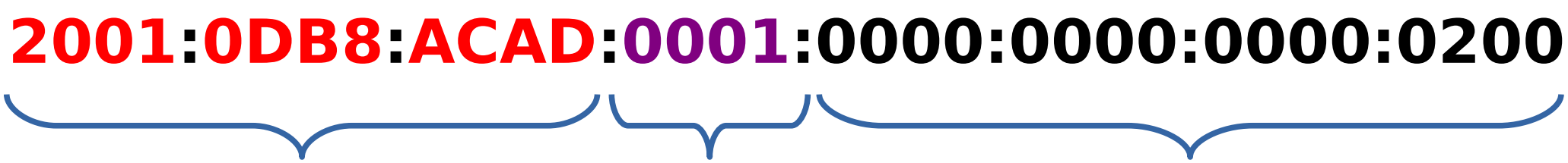
Podział dla **4 adresów** (*/**30**, 255.255.255.**252**):
0-3, 4-7, 8-11, 12-15, 16-19, 20-23, 24-27, 28-31, 32-35, 36-39, 40-43, 44-47, 48-51, 52-55, 56-59, 60-63, 64-67, 68-71, 72-75, 76-79, 80-83, 84-87, 88-91, 92-95, 96-99, 100-103, 104-107, 108-111, 112-115, 116-119, 120-123, 124-127, 128-131, 132-135, 136-139, 140-143, 144-147, 148-151, 152-155, 156-159, 160-163, 164-167, 168-171, 172-175, 176-179, 180-183, 184-187, 188-191, 192-195, 196-199, 200-203, 204-207, 208-211, 212-215, 216-219, 220-223, 224-227, 228-231, 232-235, 236-239, 240-243, 244-247, 248-251, 252-255.

Podział dla **8 adresów** (*/**29**, 255.255.255.**248**):
0-7, 8-15, 16-23, 24-31, 32-39, 40-47, 48-55, 56-63, 64-71, 72-79, 80-87, 88-95, 96-103, 104-111, 112-119, 120-127, 128-135, 136-143, 144-151, 152-159, 160-167, 168-175, 176-183, 184-191, 192-199, 200-207, 208-215, 216-223, 224-231, 232-239, 240-247, 248-255.

Podział dla **16 adresów** (*/**28**, 255.255.255.**240**):
0-15, 16-31, 32-47, 48-63, 64-79, 80-95, 96-111, 112-127, 128-143, 144-159, 160-175, 176-191, 192-207, 208-223, 224-239, 240-255.

Protokół IPv6

1. Nie ma tu już tradycyjnego podziału na pule adresów prywatnych i adresów publicznych. Każde urządzenie może (choć nie musi) posiadać adres globalny (pula adresów obecnie będąca w użyciu zaczyna się na 2000::/3) i możliwość połączeń *End-To-End* w sieci Internet. Na jednym interfejsie host może posiadać kilka adresów globalnych IPv6 (statycznych i dynamicznych jednocześnie), podobnie może posiadać kilka adresów bramy domyślnej. Dla celów demonstracyjnych używa się adresów zaczynających się na 2001:0DB8::/32. Adres składa się z 8 hextetów i w praktyce najczęściej ma prefiks /48 (3 pierwsze hextety identyfikują sieć). Przy tworzeniu podsieci nie ma konieczności pożyczania bitów ani z części globalnej ani z części hostów (możliwe jest stworzenie 65536 podsieci → od 0000 do FFFF). Nie ma także konieczności przeliczania na system binarny:



prefix globalny (sieć)
48-bit

ID podsieci (klient)
16-bit

ID hosta (karty sieciowej)
64-bit

Protokół IPv6 a ICMPv6

Ma również wygenerowany adres lokalny (*Link-Local,* zaczynający się na **FE80::/10**), utworzony przez mechanizm **SLAAC** (*Stateless Address Autoconfiguration*), który jest odpowiednikiem APIPA do połączeń lokalnych (jest on konieczny). Host może go wygenerować bez zapytania DHCPv6, jedynie w oparciu o odebrane komunikaty routera typu ICMPv6, czyli ogłoszenia „*Router Advertisment*” wysyłane przez router co 200 sekund do wszystkich maszyn z IPv6 (*multicast*). Ogłoszenia wysyłane są z adresu *Link-Local* routera i zawierają *Link-Local* dla hosta, bramę domyślną, DNS. Router może przekazać hostowi tylko część informacji prosząc go, aby resztę uzyskał od DHCPv6.

Host może wymusić na routerach IPv6 takie zapytanie wysyłając do niego komunikat „*Router Solicitation*”. Może także zignorować RA routera i poprosić o informacje DHCPv6. Może także wysłać zapytanie do innych hostów (*Neighbor Solicitation*), czy aby nie mają tego samego IPv6 (DAD [*Duplicate Address Detection*]; w tym przypadku host wygeneruje sobie nowy). Mogą także pytać o ich adres MAC. Hosty mu odpowiadają (*Neighbor Advertisment*).

Protokół IPv6

Link-Local może być także ustawiony statycznie. Identyfikuje go pierwsze 10 bitów, następnie 54 bity oznaczają sieć (są zmienne), po czym występuje 64 bity identyfikujące hosta.

W przypadku, gdy router nie posiada adresu globalnego, jego *Link-Local* będzie adresem bramy dla lokalnej sieci (choć nie jest ten adres routowalny). Router może posiadać adres globalny na swoim interfejsie LAN, jak i WAN.

Urządzenie może także posiadać adres „*unikalny lokalnie*” w zakresie **FC00::/7** do **FDFF::/7**.

Protokół IPv6

2. Nie ma już konieczności stosowania NAT. Zaleca się, aby każde urządzenie było dostępne w sieci Internet.

3. Nie ma tradycyjnych masek podsieci, są jedynie prefiksy (np. numer/64), które pełnią podobną funkcję.

Protokół IPv6

4. Nie ma już adresów rozgłoszeniowych (*broadcast*). Funkcjonują natomiast adresy *multicast* (**FF00::/8**, w tym **FF02::1** dla „wszystkie węzły” [odpowiednik *broadcast*] oraz **FF02::2** dla „wszystkie routery”), które odbierane mogą być przez wszystkie urządzenia z włączonym protokołem IPv6.

5. Nie ma już adresów sieci (w routingu).

6. Mogą występować w postaci skompresowanej: a) zera wiodące (na początku) mogą być pomijane, b) zera występujące w ciągu (np. 0000:0000:0000) można **jednokrotnie** zamienić na **::** . Na przykład, w przypadku odpowiednika pętli zwrotnej:

127.0.0.1 = **::1/128**

= 0000:0000:0000:0000:0000:0000:0000:0001

Protokół IPv6

Adres IPv6 może być 128-bitowy, ale typowa sieć LAN ma adres 64-bitowy, np.:

2001:0DB8:000A::/64

czyli

2001:0DB8:000A:0000:0000:0000:0000:0000

Część sieciowa

identyfikator interfejsu (host)

Protokół IPv6 a MAC

1. Zamiast adresów MAC 48-bitowych (EUI-48), używa się adresów 64-bitowych (EUI-64; *Extended Unique Identifier*), w których pierwsze 24 bity identyfikują producenta (OUI, *Organizationally Unique Identifier*), a następne 40 bitów identyfikują dane urządzenia (NIC). W **nowych** adresach dodaje się 00:00 do środka adresu. Gdy chcemy stary adres przekonwertować na EUI-64, dodajemy FF:FE do środka adresu, np.:

EUI-48: ac:ee:9e:3c:c7:ee

EUI-64: ac:ee:9e:**00:00**:3c:c7:ee

EUI-64 (kompatybilny z EUI-48): ac:ee:9e:**ff:fe**:3c:c7:ee

2. Jeśli pierwszy oktet MAC zamienimy na postać binarną, i przedostatnia wartość będzie wynosić 1 - jest to adres lokalny. Jeśli wartość wynosi 0 - jest to adres uniwersalny (globalny). Czyli: AC = 101011**0**0 (jest to adres globalny).

Protokół IPv6 a MAC

3. Specjalne adresy MAC:

FF:FF:FF:FF:FF:FF - odpowiednik adresu broadcastowego IP (np. 192.168.0.255); adres wykorzystywany podczas zapytań ARP (który host ma dane IP; odpowiedź jest typu *unicast*); przełącznik, który odebrał zapytanie ARP, rozgłasza je do wszystkich aktywnych portów za wyjątkiem portu nadawcy);

01:00:5E:0A:00:02 - adres typu *multicast* dostępny dla określonej grupy hostów (odpowiednik adresu IP 224.139.34.56 w warstwie 3);

Usługi i protokoły

Protokół to zbiór zasad dotyczący formatu danych przesyłanych przez sieć komputerową.

TCP/IP (*Transmission Control Protocol/Internet Protocol*) - niezależny od systemu operacyjnego, nie ma portu;

NetBIOS - używa portów 137, 138 (UDP) oraz 139 (TCP); *NetBIOS over TCP/IP* używa portu 445;

FTP (*File Transfer Protocol*) - standardowy port 20 (dane) i 21 (komunikaty sterujące);

Telnet - standardowy port 23;

SSH (*Secure Shell*) - standardowy port 22;

SMTP (*Simple Mail Transfer Protocol*) - poczta wychodząca; standardowy port 25;

DNS (*Domain Name Service*) - standardowy port 53;

POP3 (*Post Office Protocol*) - odbieranie poczty; standardowy port 110;

IMAP (*Internet Message Access Protocol*) - nowsze rozwiązanie w stosunku do POP3; standardowy port 143;

HTTP (*Hyper Text Transfer Protocol*) - przesyłanie danych hipertekstowych; standardowy port 80;

HTTPS (*HTTP over TLS/SSL*) - wykorzystywany w czasie bezpiecznego logowania się na konta, połączenie jest wtedy szyfrowane; standardowy port 443;

GG - komunikator; standardowy port 1550;

eMule - klient P2P; standardowy port 4662 i 4672;

DHCP - klienty wyszukują w sieci serwera DHCP na zasadzie rozgłoszenia (rozgłoszenie ograniczone);

OSPF - routery wymieniają między sobą informacje o swoich sieciach za pomocą pakietów LSA (*Link-State Advertisment*) na adres multicast 224.0.0.5 lub 224.0.0.6 (lub IPv6: FF02::5 → wszystkie routery z protokołem OSPF); za pomocą pakietu „*Hello*” (co 10 sekund) wykrywają swoich sąsiadów; ustala trasy na podstawie „kosztów połączenia” (przepustowość oparta o szerokość pasma);

SNMP (*Simple Network Management Protocol*) - protokół warstwy 7, monitorowanie stanu urządzeń sieciowych i ich poszczególnych komponentów, powiadamianie administratora o awariach; wykorzystywany jest protokół UDP (porty 161 / 162; możliwe jest także wykorzystanie TCP), program składa się z zarządcy (*Manager*) oraz licznych agentów na urządzeniach sieciowych (na drukarkach, routerach, switchach, komputerach, itp.). Agenci udostępniają zarządcy takie informacje jak: temperatura procesora, ilość miejsca na dysku, zalogowani użytkownicy, itp. Agent może wysyłać zarządcy alarmy (*trap*), jeśli zostanie przekroczona jakaś wartość. Zarządca przedstawia te informacje w czytelny sposób, np. wizualizuje topologię sieci, trendy, anomalie, powiadamianie za pomocą SMS.

W systemie *Windows 10*, agent SNMP funkcjonuje jako „*Usługa SNMP*” (można ją skonfigurować klikając w nią: zakładka *„Pułapki” / „Nazwa społeczności”*). Jeśli taka usługa nie istnieje, należy ją dodać: *Ustawenia / Aplikacje / Funkcje opcjonalne / Protokół SNMP.*

SNMP v1 - brak szyfrowania, 32-bit, UDP; łatwo przechwycić jawne hasło (*community-string*) i zmienić konfigurację urządzenia;
SNMP v2 - brak szyfrowania, 64-bit, UDP;
SNMP v3 - szyfrowanie (trzeba wygenerować klucze), TCP; trzy tryby: noauthnopriv (bez zabezpieczeń, kompatybilny z wersją 1), authnopriv (nieszyfrowana, ale zabezpieczona hasłem i użytkownikiem), authpriv (szyfrowana i autoryzowana)
Info: Ze względu na problemu z bezpieczeństwem, Microsoft rezygnuje powoli z tego protokołu.

Agent SNMP dla Gentoo Linux

emerge -vp net-snmp

nano /etc/snmp/snmpd.conf *(nie należy nigdy używać domyślnych nazw communities, tj.* ***public*** *[tylko odczyt] oraz* ***private*** *[także zapis])*

/etc/init.d/snmpd start
netstat -tulpen | grep 161 *(sprawdzamy czy agent działa)*

Testujemy działanie:
$ **snmpwalk -v2c -c** *nazwaCommunity* **192.168.7.25**
$ **snmpwalk -Os -c** *nazwaCommunity* **-v 1 127.0.0.1 system**

Narzędzie graficzne:
emerge -vp mrtg *(Przeglądanie wykresów sieciowych: http://127.0.0.1/mrtg)*
emerge -vp net-analyzer/nagios

Komunikacja SNMP w szczegółach

Menadżer wysyła do agenta komunikaty:
SNMP GET (pobieranie parametrów od klienta za pomocą UDP 161)
SNMP SET (modyfikuje parametry klienta)

Agent wysyła do menadżera:
SNMP TRAP/INFORM (gdy nastąpiła zmiana wartości danego parametru urządzenia, UDP 162 lub TCP 162 w SNMPv3)

Inne ciekawe informacje

1. Wysłanie wydruku do drukarki znajdującej się w innym LAN.

Rozwiązanie: Ustawiamy na naszym komputerze drugi numer IP z tego samego zakresu, co drukarka (w ustawieniach protokołu IPv4 klikamy w „*Dodaj...*”).

2. Przełączniki (switche) nie muszą mieć własnego numeru IP. Jeśli go mają, to jego jedyną funkcją jest możliwość zdalnego zarządzania.

3. Każdy producent sprzętu musi zarejestrować się w IEEE, w wyniku czego otrzymuje adresację MAC dla swoich urządzeń (pierwsze 24 bity to identyfikator producenta).

4. Adres sieci w routingu można określić za pomocą adresu IPv4 **0.0.0.0** (*default*) lub IPv6 **::/0**, który oznacza „każdy inny cel” (który nie może być osiągnięty za pomocą innych wpisów w routingu). Cele znajdujące się w tej samej sieci, system określa jako „*On-Link*” (nie potrzebna jest wtedy brama).

Przełączniki - podział fizyczny

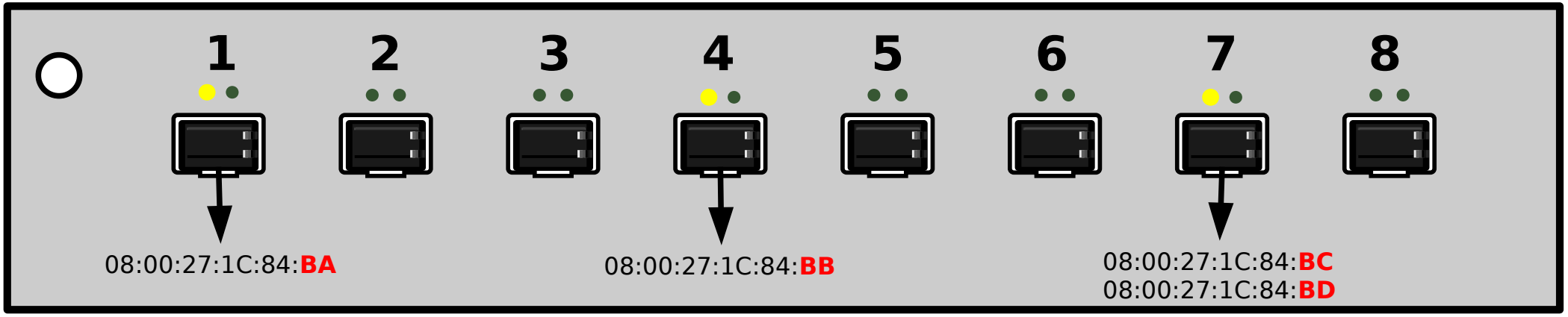
1. Przełączniki o **stałej konfiguracji** - ilość portów fizycznych jest stała i określona, mniejsza liczba szybkich portów.

2. Przełączniki o **modułowej konfiguracji** - do urządzenia można dodać dodatkowe moduły zawierające określone porty. Rozwiązanie droższe niż w przypadku stałej konfiguracji.

3. Przełączniki o **konfiguracji stosu** (*stackable*) - kilka przełączników można połączyć za pomocą dedykowanych do tego celu portów i kabli tworząc w ten sposób jedno urządzenie zestawione w wieżę (stos). W takiej konfiguracji, cała wieża jest zasilana zbiorczo za pomocą jednego kabla (*StackPower*). Rozwiązanie ekonomiczne.

Przełącznik - zasada działania

Przełączniki posiadają w swojej pamięci tablicę wiążącą swoje porty fizyczne z **adresami MAC** podpiętych urządzeń. Tablica przetrzymywana jest w szybkiej pamięci **CAM** (*Content Addressable Memory*) i budowana jest poprzez zapisanie MAC źródłowego, a następnie wysyłanie ramki na wszystkie porty (tzw. „*zalewanie portów*”) i nasłuchiwaniu odpowiedzi typu *unicast* od właściwego adresata. Dzięki temu wiedzą, na którym porcie jest adresat i przez który port w przyszłości wysłać otrzymaną ramkę Ethernet. Adresy w tablicy odświeżane są co 5 minut. Urządzenie działa w **warstwie 2** modelu OSI.



Przełącznik - metody przesyłania

1. ***Store-and-Forward*** (przechowaj i przekaż) - przełącznik najpierw otrzymuje i składuje całą ramkę (buforowanie), sprawdza błędy (CRC: porównuje sumę kontrolną **FCS** [*Frame Check Sequence*] z ramki), a następnie ją wysyła do odbiorcy. Jeśli wykryje błąd - porzuca ramkę. Metoda stosowana, gdy prędkość przesyłu na wejściu i wyjściu jest różna (np. wejście 100Mb/s, a wyjście 1Gb/s). Stosowana domyślnie w urządzeniach *Cisco*.

2. ***Cut-through*** (przełączanie w locie) - przełącznik od razu przesyła ramkę w części, gdy tylko odczyta adres MAC odbiorcy (czyli po odebraniu 14 bajtów). Nie sprawdza błędów. Dzięki temu uzyskuje dużą wydajność. Jeśli jednak pojawią się błędy, przepustowość łącza spadnie, a docelowa karta sieciowa odrzuci uszkodzone ramki.

3. **Fragment free** - przed przesłaniem ramki przełącznik musi odebrać 64 bajty (okno kolizji), aby sprawdzić, czy nie wystąpiła fragmentacja.

Przełącznik - domeny

1. **Domena kolizyjna** - segment sieci, w której pasmo jest współdzielone przez urządzenia (tak jest w przypadku koncentratorów); w tym samym czasie, tylko jedno urządzenie może nadawać sygnał, inaczej dochodzi do kolizji. Przełączniki i routery działają inaczej: dzielą sieć na **mikrosegmenty** (każdy port fizyczny przełącznika jest wyizolowany od pozostałych i stanowi osobną domenę kolizyjną). Przełączniki zapewniają na porcie pełne pasmo oraz pełny duplex (jednoczesne wysyłanie i odbieranie sygnału). W mikrosegmentach nie dochodzi do kolizji, a gdy włączony jest pełny duplex, mechanizm sprawdzania kolizji jest w ogóle wyłączony.

2. **Domena rozgłoszeniowa** - rozgłoszenie wysyłane jest na adres MAC: FF:FF:FF:FF:FF:FF (same binarne jedynki). Dociera do wszystkich urządzeń podłączonych do przełącznika (oprócz urządzenia wysyłającego). Jeśli urządzeniem odbierającym jest inny przełącznik, on również wysyła rozgłoszenie na wszystkie swoje porty. W przypadku routerów, każdy port jest osobną domeną rozgłoszeniową.