Internet Society
Ukraine Chapter

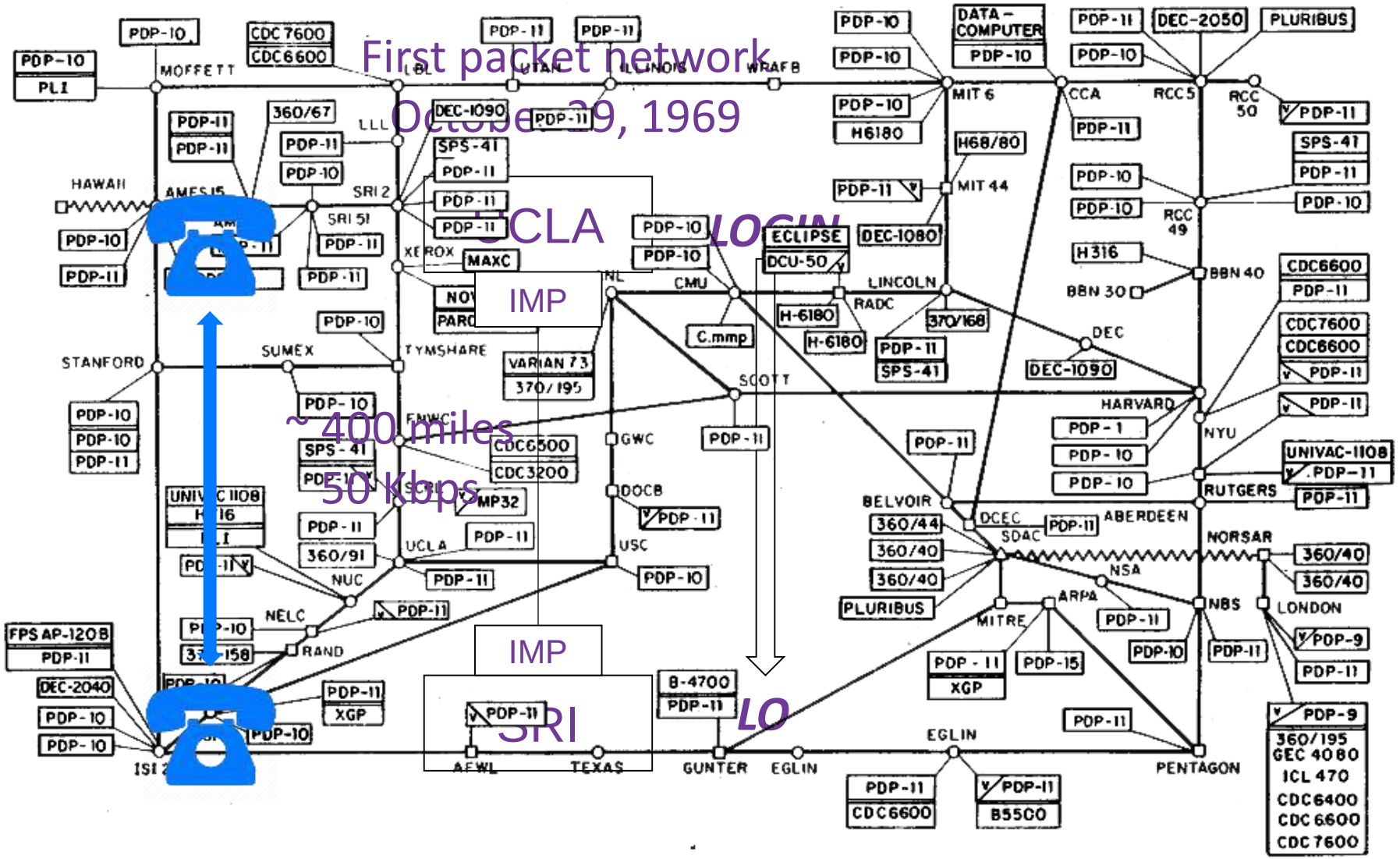
Сезонна школа: 2023

Internet Governance
Управління Інтернет

Як нам облаштувати Інтернет?

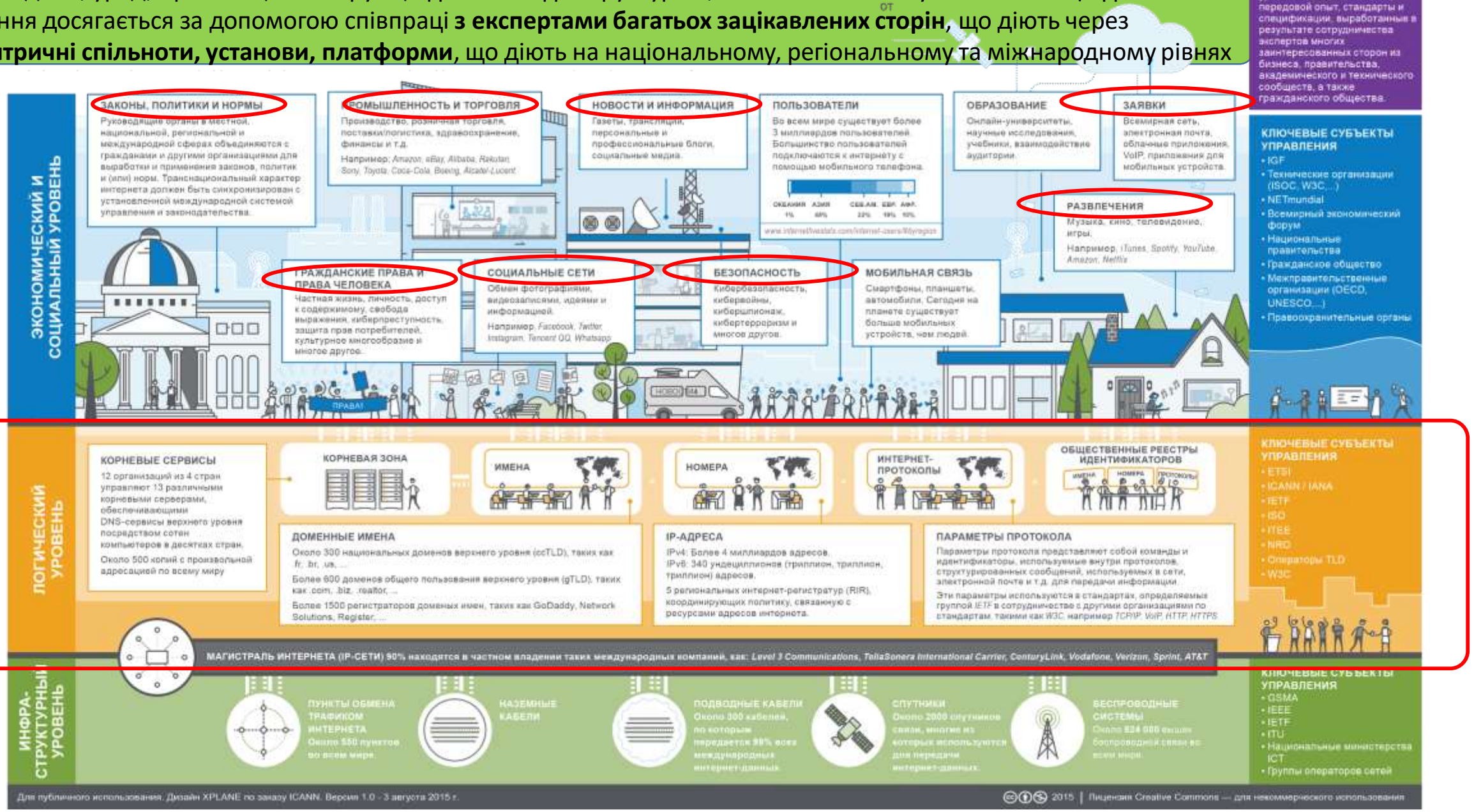
First steps

ARPANET LOGICAL MAP, MARCH, 1977



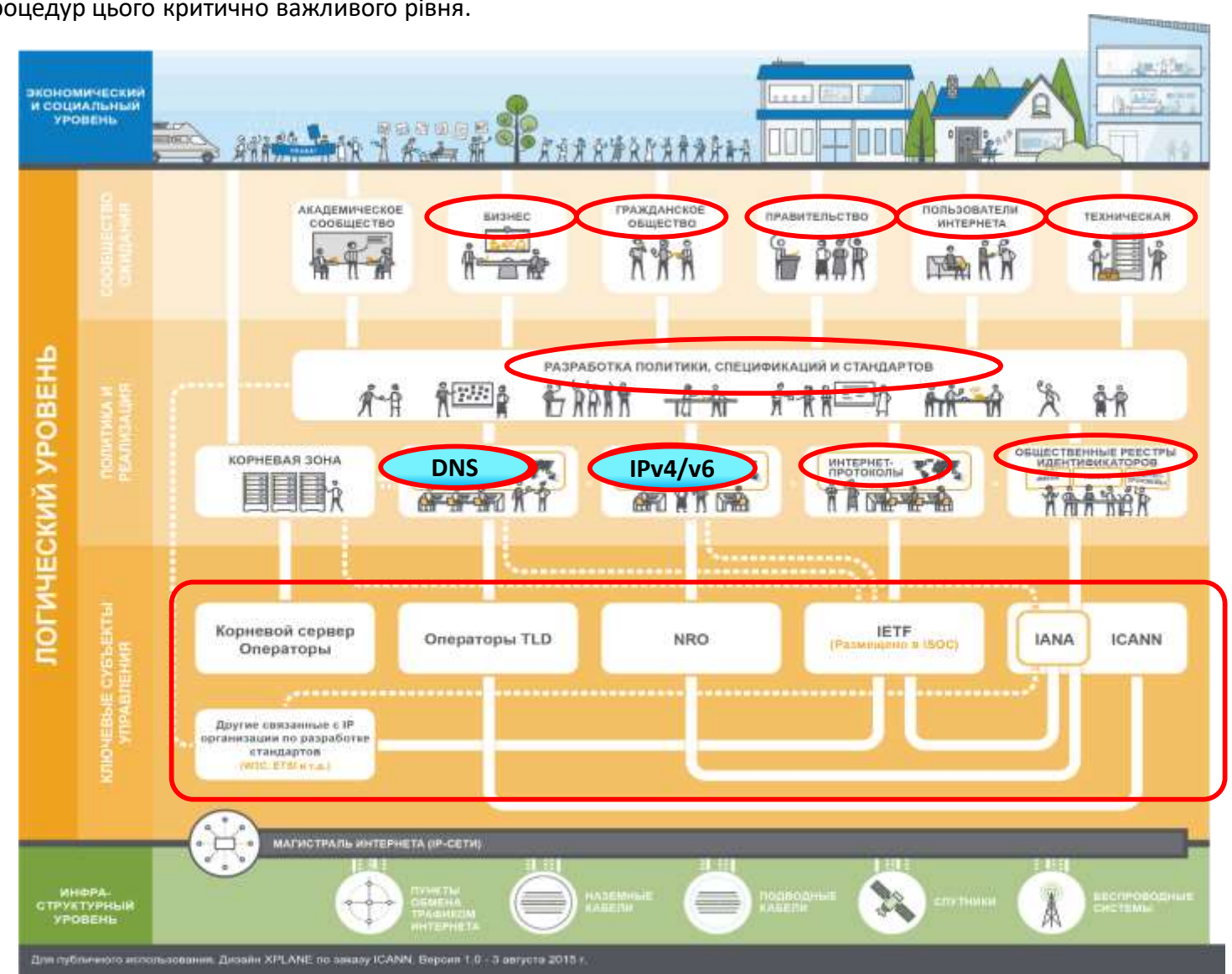
Три рівня цифрового управління *(за схемою ICANN)*

Жодна людина, уряд, організація не керує цифровою інфраструктурою, економікою або суспільством. Цифрове управління досягається за допомогою співпраці **з експертами багатьох зацікавлених сторін**, що діють через **поліцентричні спільноти, установи, платформи**, що діють на національному, регіональному та міжнародному рівнях



Логічний рівень цифрового управління *(за схемою ICANN)*

Мета - забезпечення управління єдиного Інтернет за рахунок унікальних ідентифікаторів (адрес, доменних імен, номерів). ICANN координує управління цим рівнем у партнерстві з іншими професійними і технічними спільнотами, наприклад, ITU, GSMA, 3GPP, для забезпечення безпеки, стабільності, відмовостійкості і цілісності при роботі процедур цього критично важливого рівня.



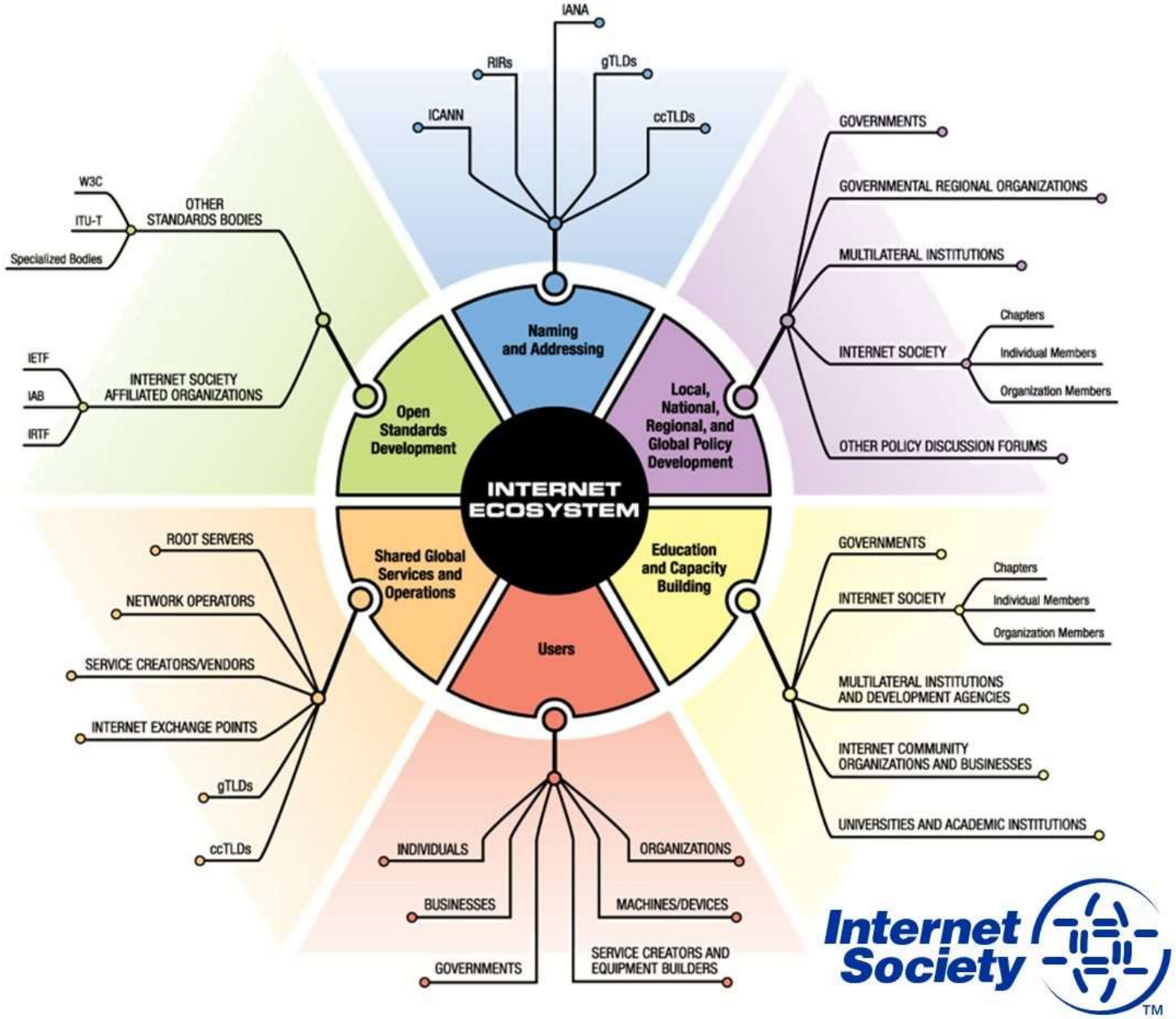
ТЕХНІЧНІ ОПЕРАЦІЇ

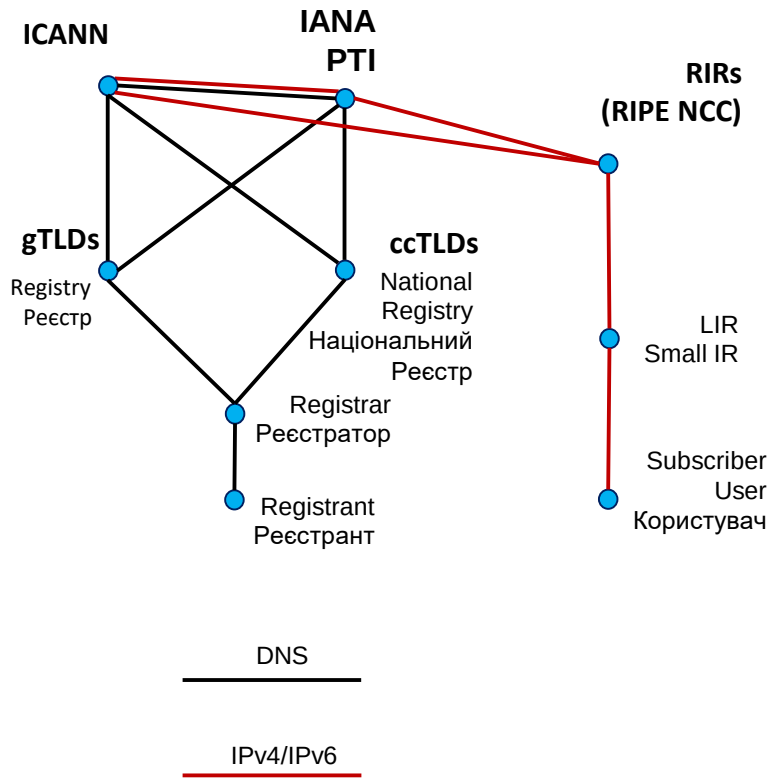
Технічне спільнота складається з декількох незалежних суб'єктів, об'єднаних спільними принципами і взаємними зобов'язаннями, які забезпечують безпеку і стабільність інфраструктури інтернету. Спільнота кожного з цих суб'єктів виробляє політики і стандарти з використанням відкритого, всебічного і заснованого на консенсусі підходу.

СПІЛЬНОТА ЗАЦІКАВЛЕНИХ СТОРІН

Наукове співтовариство
Вищі навчальні заклади
Лідери академічної думки
Викладачі та студенти
Неурядові організації
Некомерційні організації
Дослідницькі центри
Бізнес
Приватні компанії з різних галузей
Промислові і торговельні асоціації
Громадянське суспільство
Міжнародні організації
Уряд
Національні уряди
Окремі економіки, визнані на міжнародній арені
Міжнародні урядові та договірні організації
Міжурядові організації
Державні органи
(З безпосереднім інтересом в міжнародному управлінні інтернетом)
Користувачі інтернету
Окремі громадяни, зацікавлені в регіональному або міжнародному управлінні інтернетом
Технічне спільнота
Інтернет-інженери
Комп'ютерні інженери
Розробники програмного забезпечення
Мережеві оператори

Internet Governance. Naming and Addressing



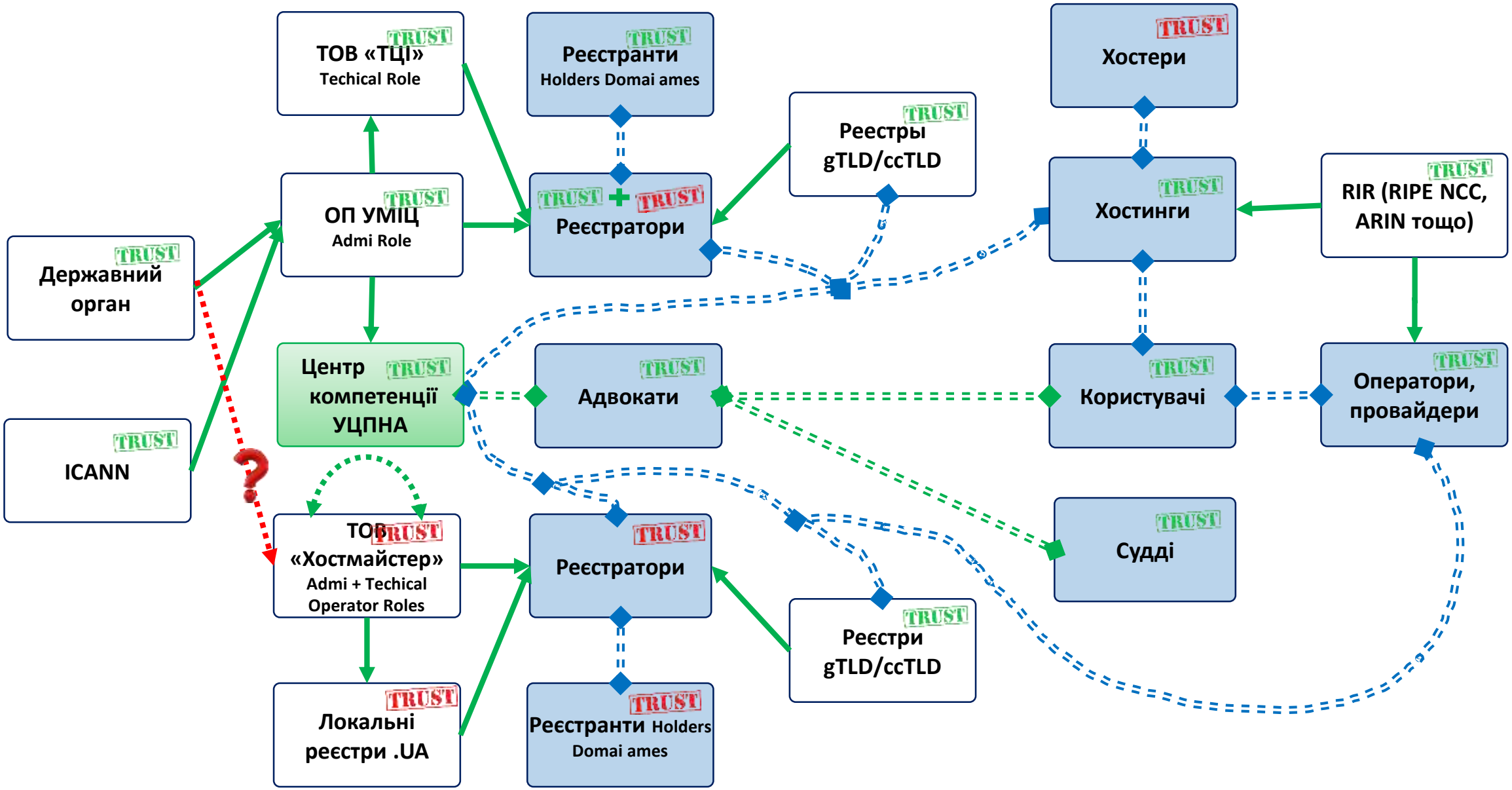


Модель Internet Governance

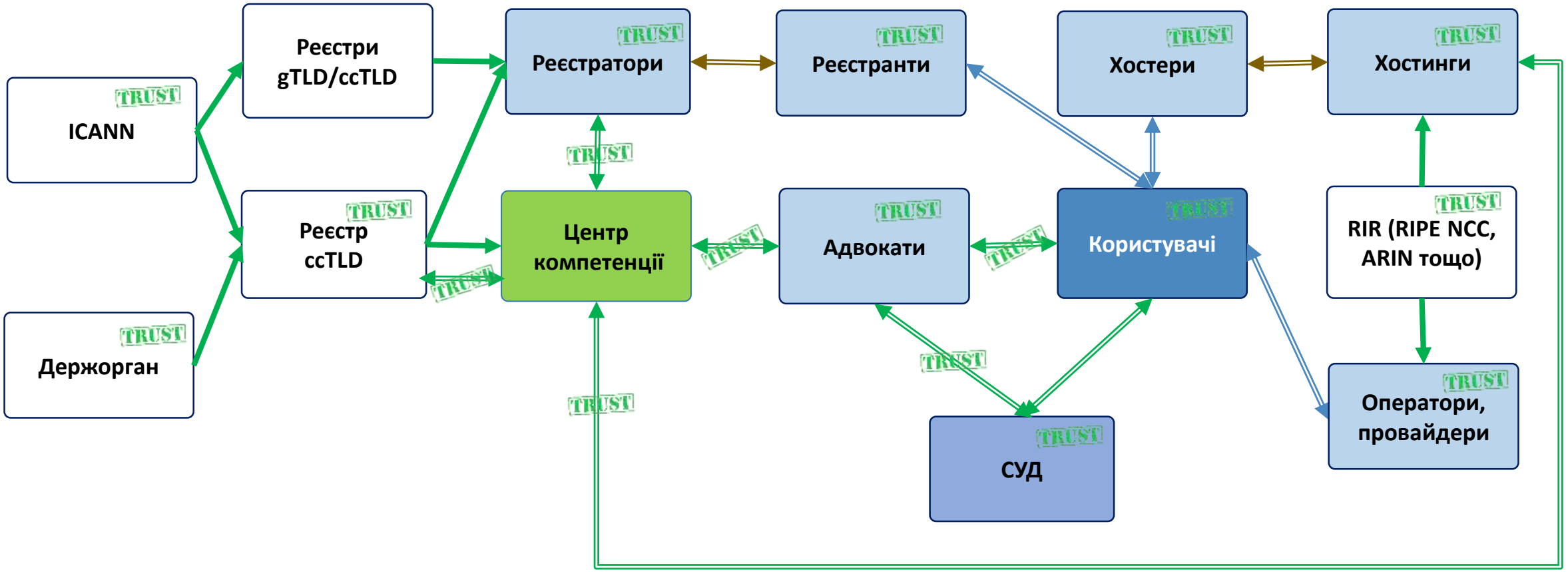
Internet Governance:

- Stakeholder and Actors
- Multistakeholders
- Multistakeholderism
- Trust
- Internet Resources
- Resources Governance
- Policies, Standards and BCP

Архітектура системи довіри на доменному ринку України

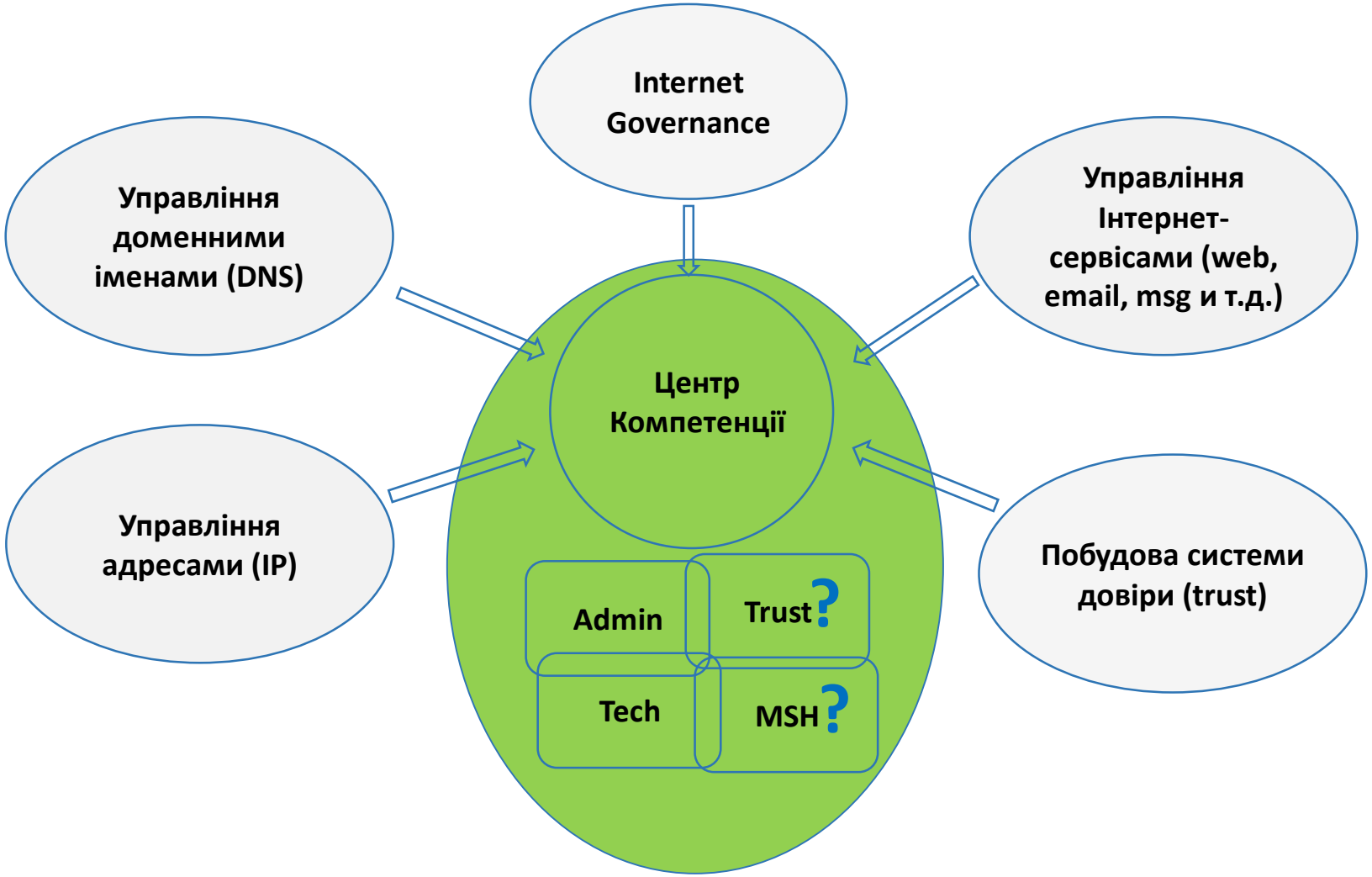


Архітектура системи багатосторонньої довіри. Ідеальна схема



Центр Компетенції. Виникнення поняття TRUST.

Центр Компетенції повинен об'єднувати функціональність адміністрування та управління як адміністративними, організаційними і юридичними аспектами ринку, так і технічними і технологічними, а також вирішувати завдання формування трастового середовища для всіх сторін, що залучені і беруть участь в процесах прийняття рішень.



Доменні імена та IP-адреси

Система доменних імен – DNS. Поняття.

DNS (система доменних імен) – це “телефонна книга” Інтернету. Як номер телефону в ній виступає IP-адреса, а як найменування контактів - домени. У таку книгу можна внести не лише «телефонний номер», а й додаткову інформацію про контакт (e-mail, місце роботи тощо).

Інформація про домен зберігається на серверах DNS. Щоб внести їх у систему DNS, потрібно прописати ресурсні записи. За допомогою їх сервери діляться відомостями про домени з іншими серверами. Поки не прописані ресурсні записи для домену, його немає у «телефонній книзі» Інтернету. Отже, робота сайту чи пошти на ньому неможлива. Перш ніж братися до вказівки ресурсних записів, потрібно зареэструвати та делегувати домен, тобто прописати йому DNS-серверы.

Домен верхнього рівня – логічний вузол у дереві імен. Право адмініструвати зону може бути передано третім особам, рахунок чого забезпечується розподіленість бази даних.

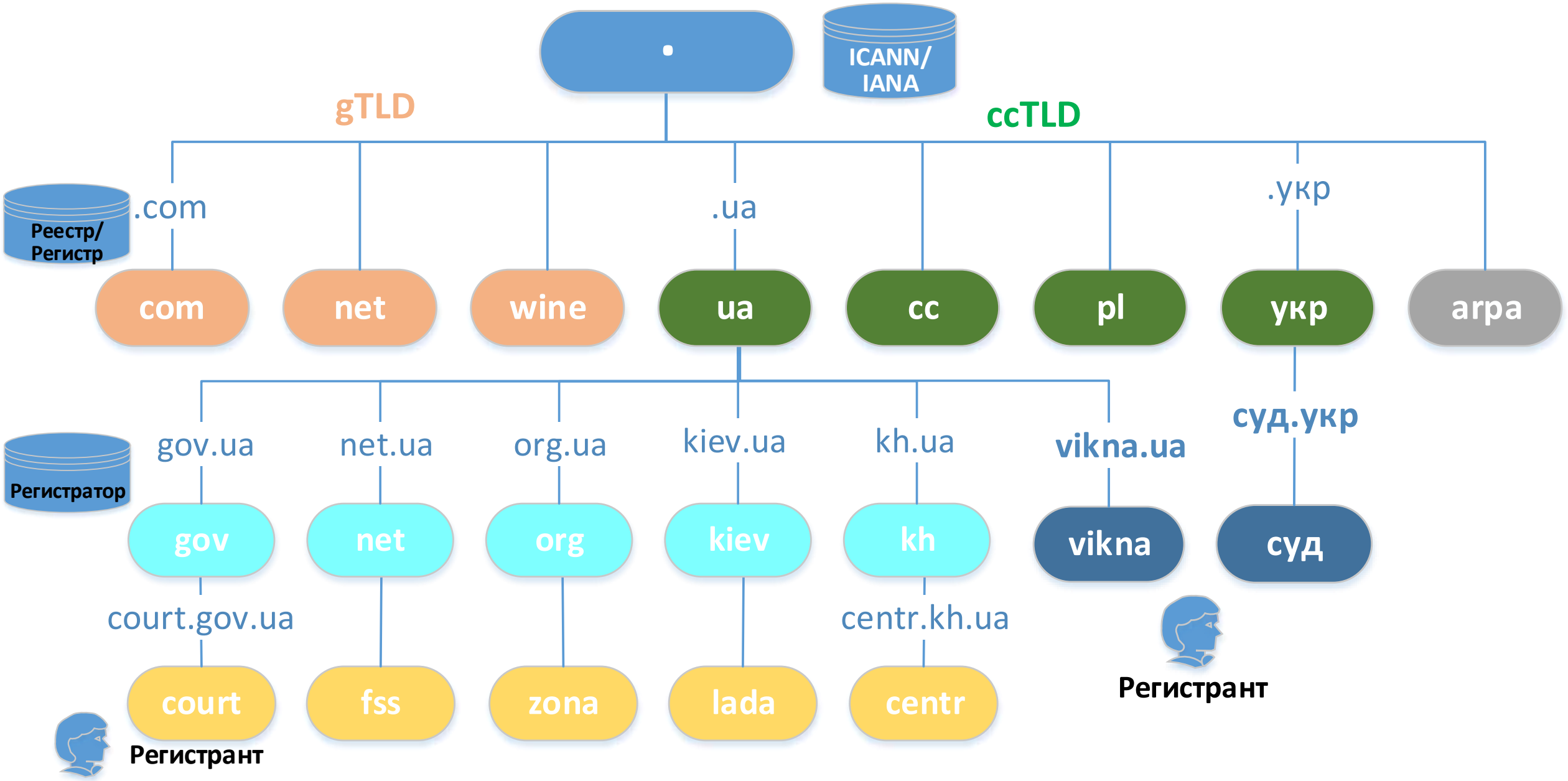
Доменне ім’я — це унікальна назва, що ідентифікує домен та складається з символьного позначення, що використовується в адресному просторі мережі Інтернет, виділеної будь-якій юридичної, або физичної особі, або для інших цілей. Структура доменного імені відбиває порядок проходження домену в ієрархічному вигляді.

Піддомен - ім'я підлеглого доменного імені. Такий поділ може досягати глибини 127 рівнів, а кожна мітка може містити до 63 символів, доки загальна довжина разом з точками не досягне 254 символів.

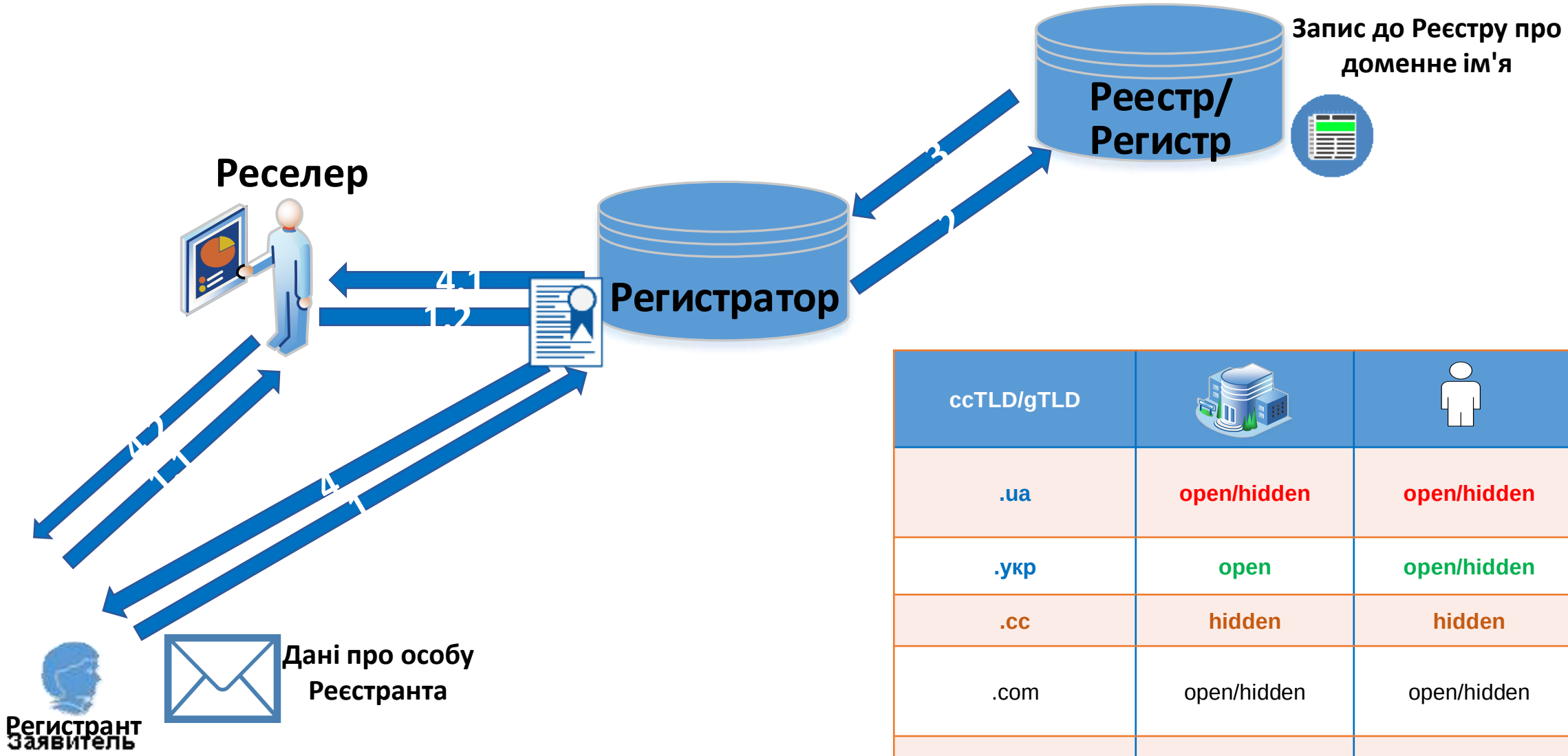
DNS-сервер — спеціалізоване програмне забезпечення для обслуговування DNS. DNS-сервер може бути авторитативним (репрезентативним) за деякі зони та/або може перенаправляти запити вищим серверам.

DNS-клієнт – спеціалізована для роботи з DNS. У ряді випадків DNS-сервер виступає у ролі DNS-клієнта.

Що таке доменні імена?

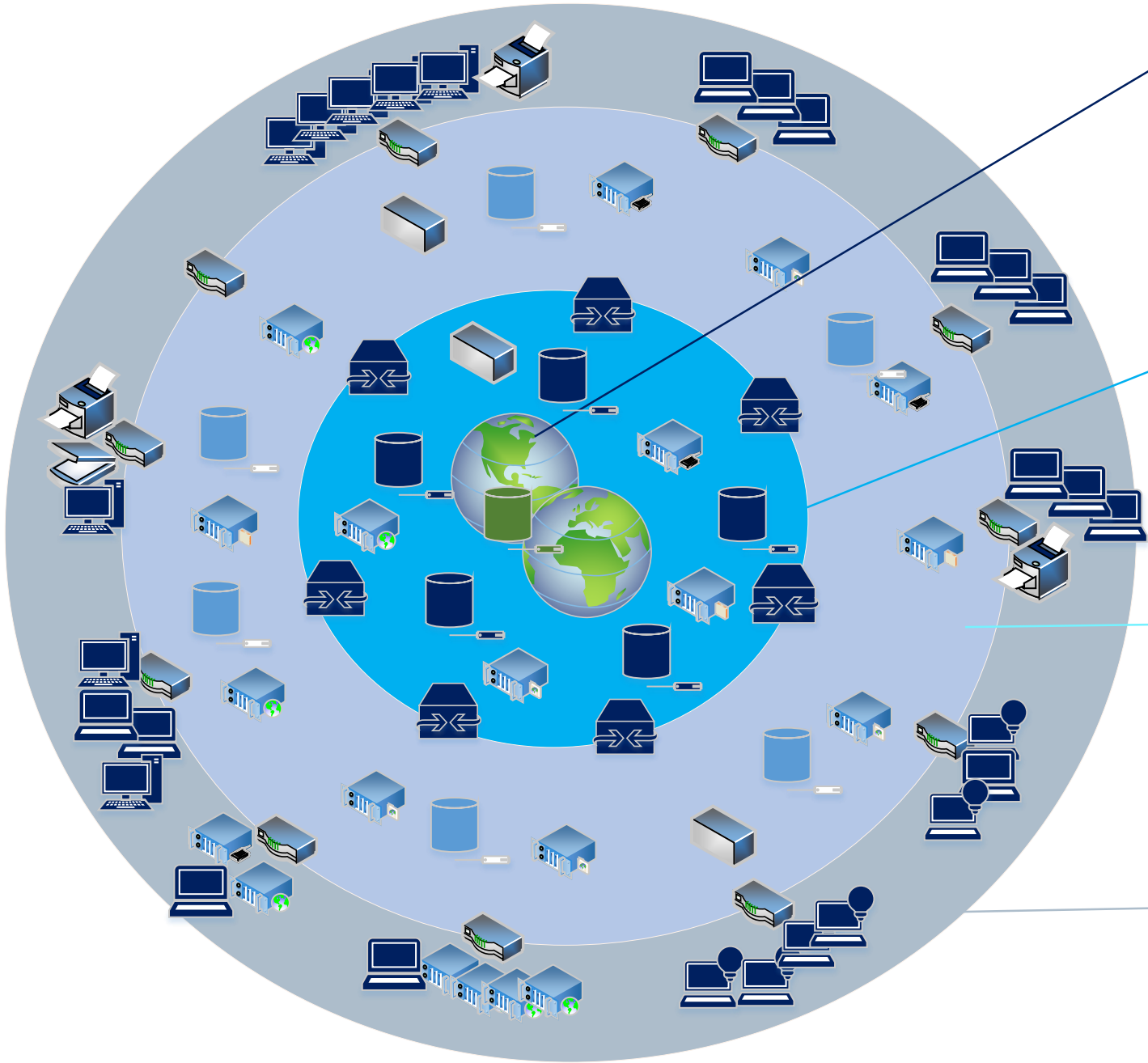


Як відбувається реєстрація доменного імені?



ccTLD/gTLD		
.ua	open/hidden	open/hidden
.укр	open	open/hidden
.cc	hidden	hidden
.com	open/hidden	open/hidden
.eu	open (exactly ad strictly)	open/hidden

Що таке IP-адреси?



ICANN
IANA

Всесвітній план IP

RIPE NCC
ARIN
APNIC
LACNIC
AfriNIC

Діапазони IP зовнішніх / публічних адрес, що розподілені по регіонах світу

LIR
ISP

Діапазони IP зовнішніх / публічних адрес, що розподілені по операторам в регіоні

Користувачі

IP зовнішні / публічні
+
IP внутрішні / «сірі»

4. Управління доменними іменами

Як відбувається управління доменним ім'ям?

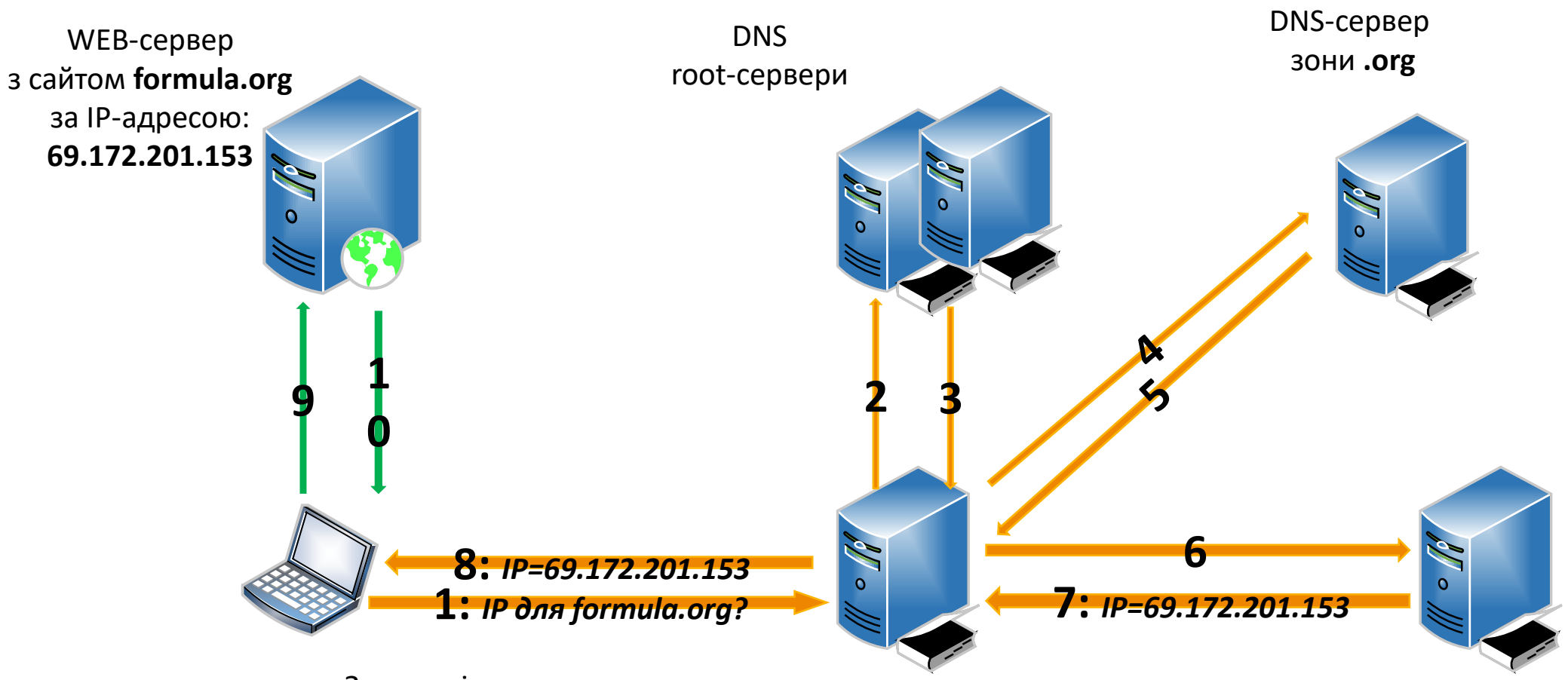
Обліковий запис

IP-адреса, що зіставляється певного сервісу, пов'язаного з доменним ім'ям

IP-адреса, що зіставляється web-сервісу, пов'язаного з доменним ім'ям

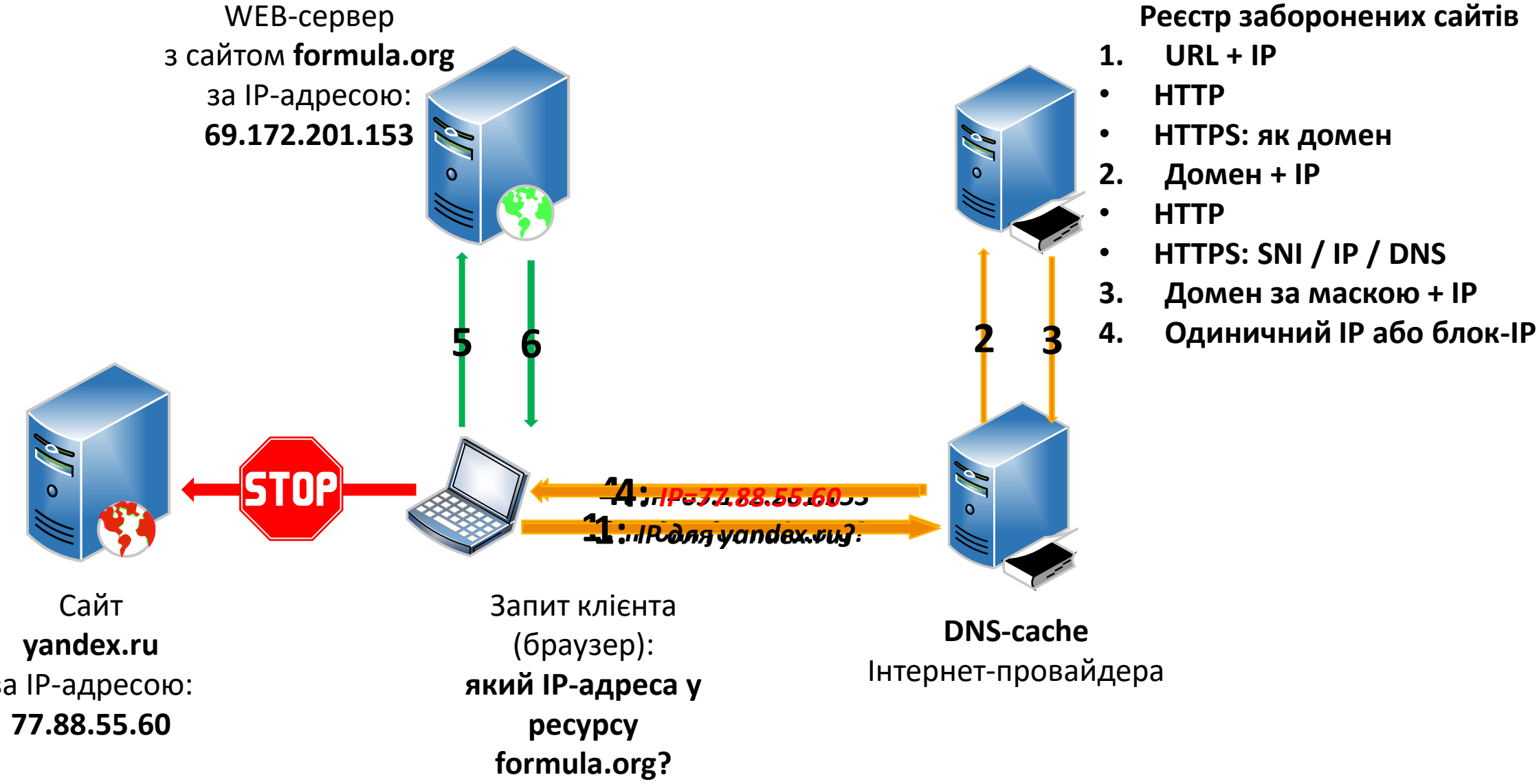
Доменная запись	Тип	Значение
ftp	A	93.190.40.29
localhost	A	127.0.0.1
mail	A	93.190.40.29
pop	A	93.190.40.29
smtp	A	93.190.40.29
test-domen.ua.	A	93.190.40.29
www	A	93.190.40.29
test-domen.ua.	NS	ns1.ukrdomen.com.
test-domen.ua.	NS	ns2.ukrdomen.com.
mx.ukrdomen.com.	MX	10
mx2.uh.com.ua.	MX	5
test-domen.ua.	TXT	"v=spf1 a mx ip4:93.190.40.15 ~all"

Навіщо потрібні доменні імена?



a) How does a DNS server work?

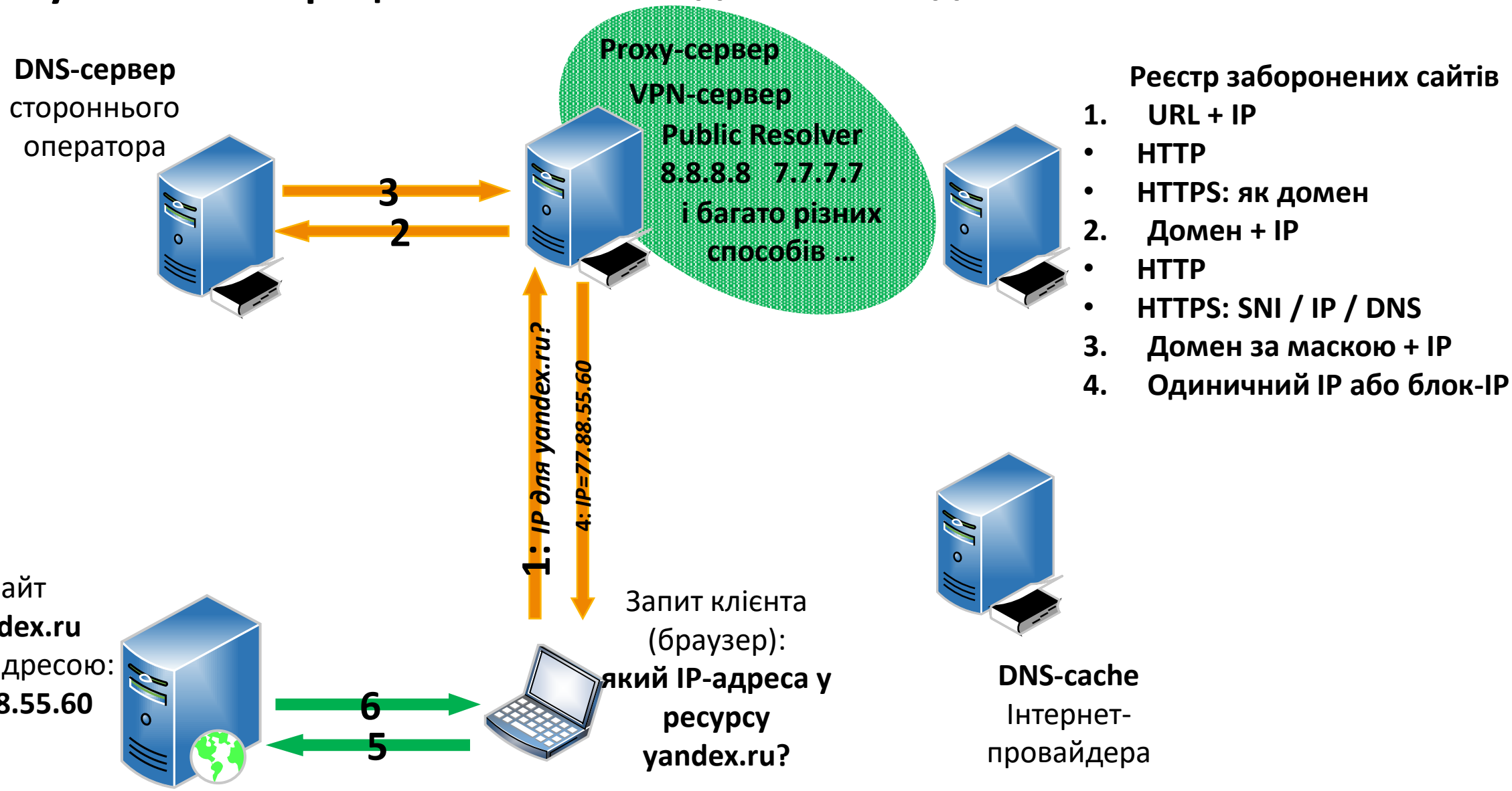
Блокування.



Реєстр заборонених сайтів

1. **URL + IP**
   - **HTTP**
   - **HTTPS: як домен**
2. **Домен + IP**
   - **HTTP**
   - **HTTPS: SNI / IP / DNS**
3. **Домен за маскою + IP**
4. **Одиничний IP або блок-IP**

Блокування. Не працюють… Іноді або завжди?



IPv4 адреси

IP-адрес - це унікальний числовий ідентифікатор пристрою в комп'ютерній мережі, що працює за протоколами **TCP/IP** або **UDP/IP**
У мережі Інтернет потрібна глобальна унікальність адреси; у разі роботи в локальній мережі потрібна унікальність адреси в межах мережі. Існують дві версії протоколу для IP-адрес :

1) **IPv4** адреса має довжину 4 байта і записується у вигляді чотирьох десяткових чисел, розділених крапками

<decimal1>.<decimal2>.<decimal3>.<decimal4>,

кожне з яких може набувати значення від 0 до 255, наприклад,

186.3.12.54

- Максимальна кількість **IPv4** обчислюється виходячи з формули $2^{(4*8)}$.
- Особливості.
  - Адреси IP, що використовуються в локальних мережах, відносять до адрес Intranet: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
  - Адреси IP, що використовуються для комунікацій усередині хоста (localhost): 127.0.0.0/8 - використовується (див. localhost)
  - Адреси IP, що використовуються для автоматичного налаштування мережного інтерфейсу у разі відсутності DHCP: блок з 169.254.1.0 до 169.254.254.255, тобто підмережа 169.254.0.0/16 за винятком підмереж 169.254.0.0/24 и 169.254.255.0/24

a) What is an IP address?

IPv6 адреси

2) **IPv6** адреса має довжину 16 байт і записується у вигляді восьми чотиризначних шістнадцяткових чисел (еквівалентні восьми 16-бітним числам), розділених двокрапками

<hex1>:<hex2>:<hex3>:<hex4>:<hex5>:<hex6>:<hex7>:<hex8>

кожен розряд якого може набувати значення від 0 до F, наприклад,

2001:0db8:85a3:0000:0000:8a2e:0c70:7f34

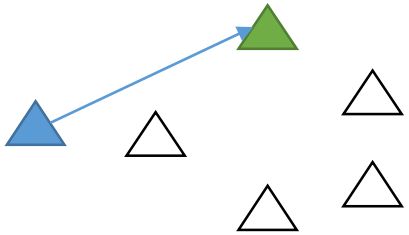
- Максимальна кількість IPv6 обчислюється виходячи з формули $\mathbf{2^{(8*16)}}$.
- Типи адрес IPv6:
  - одноадресні (**Unicast**), призначені для односпрямованої передачі даних, що має на увазі під собою передачу пакетів єдиному адресату, коли адреса належить в мережі лише одному єдиному кінцевому пристрою.
  - групові (**Anycast**), призначені для розсилки пакетів, дозволяють пристрої посилати дані найближчому з групи одержувачів, при цьому при отриманні анонсу маршрутів з двох і більше точок, буде обраний найкоротший, який не обов'язково буде до найближчої географічної точки.
  - багатоадресні (**Multicast**), призначені передачі потокового відео, коли необхідно доставити відео-контент необмеженому числу абонентів, не перевантажуючи мережу. Це тип передачі даних, що найчастіше використовується в IPTV мережах, коли одну і ту ж програму дивляться велика кількість абонентів.

a) IPv6 Addresses Explained

Типи IPv6 адрес

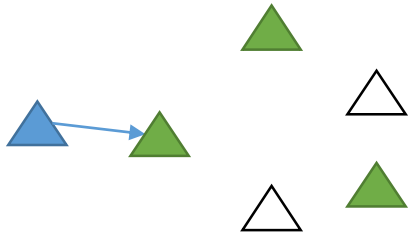
Моделі доставки контенту

Unicast



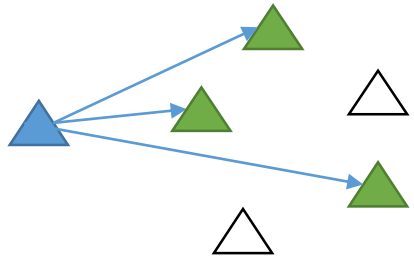
один к одному

Anycast



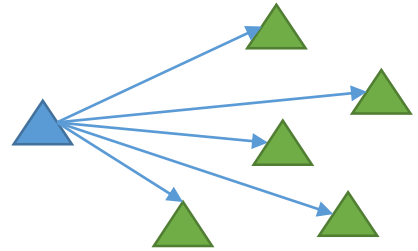
один к найближчему одному

Multicast



один к багатьом

Broadcast

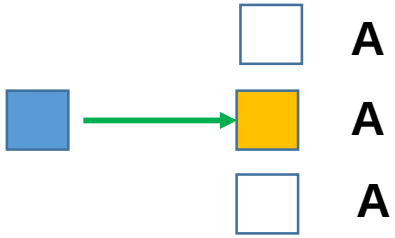


один до всіх

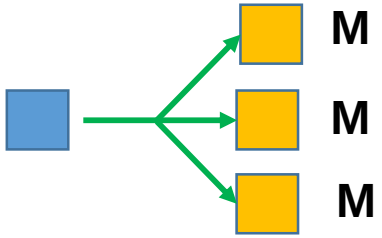
Типы IPv6 адресов

Unicast

Anycast



Multicast



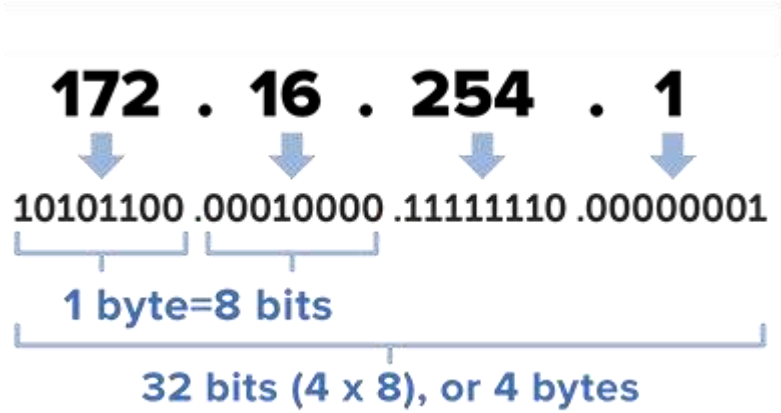
Anycast адреси - це адреси, які можуть бути більш ніж одного інтерфейсу, тобто. різним пристроям, і кілька пристроїв можуть мати ту саму довільну адресу.
Пакет, надісланий на довільну адресу, направляється на «найближчий» інтерфейс, що має цю адресу, відповідно до таблиці маршрутизації маршрутизатора.

IPv6 Address Types

Мережі і IP-адреси

Для з'єднання мережевих пристроїв (маршрутизатор, комутатор і т.д.) в Інтернеті використовується набір комунікаційних протоколів.
IP-адреса, маска підмережі та стандартний шлюз є необхідними елементами конфігурації комунікаційних протоколів.
IP-мережі адресуються та діляться на мережі та підмережі.

IP-адреса - це логічна числова адреса, що присвоюється кожному комп'ютеру, принтеру, маршрутизатору або будь-якому іншому пристрої в IP-мережі, причому кожна з них має унікальну IP-адресу. IP-адреси налаштовуються або вручну (статична IP-адреса), або DHCP-сервером. IP-адреса складається з 4 байт даних. Байт складається з 8 біт (біт-це одна цифра, і це може бути тільки 1 або 0), тому у нас є в цілому 32 біти для кожної IP-адреси. Це приклад IP-адреси у двійковому форматі: 10101100. 00010000. 11111110.00000001. Щоб спростити справу, десяткове уявлення зазвичай використовується для створення IP-адреси таким чином: 172. 16. 254. 1



IP-адреси поділяються на публічні та приватні.
Для приватних адрес зарезервовано три блоки IP-адрес:
10.0.0.0 – 10.255.255.255/8 (16777216 хостів)
172.16.0.0 – 172.31.255.255/12 (1048576 хостів)
192.168.0.0 – 192.168.255.255/16 (65536 хостів)

Приватні IP-адреси, також звані внутрішніми, внутрішньомережевими, локальними або сірими, будь-яка організація має право використовувати на свій розсуд без будь-якої реєстрації у будь-якої організації.

Мережі і IP-адреси

Підсітка та маска підмережі

Щоб працювати в Інтернет потрібна публічна IP-адреса, яка «маскуватиме» 1 або кілька приватних IP-адрес.Таким чином, вся приватна мережа може підключатися до Інтернету через одну публічну IP-адресу (або пул адрес), надану провайдером. В результаті ресурс глобальних адрес витрачається набагато економніше.

Підсіти-це процес поділу більшої мережі на дрібніші підмережі. Ми завжди резервуємо IP-адресу для ідентифікації підмережі та ще одну для ідентифікації широкомовної адреси всередині підмережі. Підмережі розбивають великі мережі на дрібні частини, що є більш ефективним та дозволить зберегти велику кількість адрес. Тому менші мережі створювали меншу широкомовну передачу, яка генерувала менший широкомовний трафік. Крім того, підсіть також спрощує усунення несправностей, ізолюючи мережеві проблеми аж до їхнього конкретного існування.

Маска підмережі – це 32- або 128-розрядне число, яке сегментує існуючу IP-адресу в мережі TCP/IP. Він використовується протоколом TCP/IP для визначення того, чи знаходиться хост у локальній підмережі або у віддаленій мережі. Маска підмережі ділить IP-адресу на мережеву адресу та адресу хоста, таким чином, щоб визначити, яка частина IP-адреси зарезервована для мережі та яка частина доступна для використання хостом. Після того, як задана IP-адреса та її маска підмережі, можна визначити мережну адресу (підмережа) хоста. Зазвичай калькулятори підмереж легко доступні в інтернеті, які допомагають розділити IP-мережу на підмережі..

CIDR	Остання IP-адреса в підмережі	Маска підмережі	Кількість адрес в підмережі	Кількість хостів в підмережі	Клас підмережі
a.b.c.d**/32**	0.0.0.0	255.255.255.255	1	1*	1/256 C
a.b.c.d**/31**	0.0.0.1	255.255.255.254	2	2*	1/128 C
a.b.c.d**/30**	0.0.0.3	255.255.255.252	4	2	1/64 C
a.b.c.d**/29**	0.0.0.7	255.255.255.248	8	6	1/32 C
a.b.c.d**/28**	0.0.0.15	255.255.255.240	16	14	1/16 C
a.b.c.d**/27**	0.0.0.31	255.255.255.224	32	30	1/8 C
a.b.c.d**/26**	0.0.0.63	255.255.255.192	64	62	1/4 C
a.b.c.d**/25**	0.0.0.127	255.255.255.128	128	126	1/2 C
a.b.c.0**/24**	0.0.0.255	255.255.255.000	256	254	1 C
a.b.c.0**/23**	0.0.1.255	255.255.254.000	512	510	2 C
a.b.c.0**/22**	0.0.3.255	255.255.252.000	1024	1022	4 C
a.b.c.0**/21**	0.0.7.255	255.255.248.000	2048	2046	8 C
a.b.c.0**/20**	0.0.15.255	255.255.240.000	4096	4094	16 C
a.b.c.0**/19**	0.0.31.255	255.255.224.000	8192	8190	32 C
a.b.c.0**/18**	0.0.63.255	255.255.192.000	16 384	16 382	64 C
a.b.c.0**/17**	0.0.127.255	255.255.128.000	32 768	32 766	128 C
a.b.0.0**/16**	0.0.255.255	255.255.000.000	65 536	65 534	256 C = 1 B
a.b.0.0**/15**	0.1.255.255	255.254.000.000	131 072	131 070	2 B
a.b.0.0**/14**	0.3.255.255	255.252.000.000	262 144	262 142	4 B
a.b.0.0**/13**	0.7.255.255	255.248.000.000	524 288	524 286	8 B
a.b.0.0**/12**	0.15.255.255	255.240.000.000	1 048 576	1 048 574	16 B
a.b.0.0**/11**	0.31.255.255	255.224.000.000	2 097 152	2 097 150	32 B
a.b.0.0**/10**	0.63.255.255	255.192.000.000	4 194 304	4 194 302	64 B
a.b.0.0**/9**	0.127.255.255	255.128.000.000	8 388 608	8 388 606	128 B
a.0.0.0**/8**	0.255.255.255	255.000.000.000	16 777 216	16 777 214	256 B = 1 A
a.0.0.0**/7**	1.255.255.255	254.000.000.000	33 554 432	33 554 430	2 A
a.0.0.0**/6**	3.255.255.255	252.000.000.000	67 108 864	67 108 862	4 A
a.0.0.0**/5**	7.255.255.255	248.000.000.000	134 217 728	134 217 726	8 A
a.0.0.0**/4**	15.255.255.255	240.000.000.000	268 435 456	268 435 454	16 A
a.0.0.0**/3**	31.255.255.255	224.000.000.000	536 870 912	536 870 910	32 A
a.0.0.0**/2**	63.255.255.255	192.000.000.000	1 073 741 824	1 073 741 822	64 A
a.0.0.0**/1**	127.255.255.255	128.000.000.000	2 147 483 648	2 147 483 646	128 A
0.0.0.0**/0**	255.255.255.255	000.000.000.000	4 294 967 296	4 294 967 294	256 A

Network Address Translation (NAT)

Швидке рішення для усунення нестачі адрес IPv4 при отриманні….

A. Переваг:

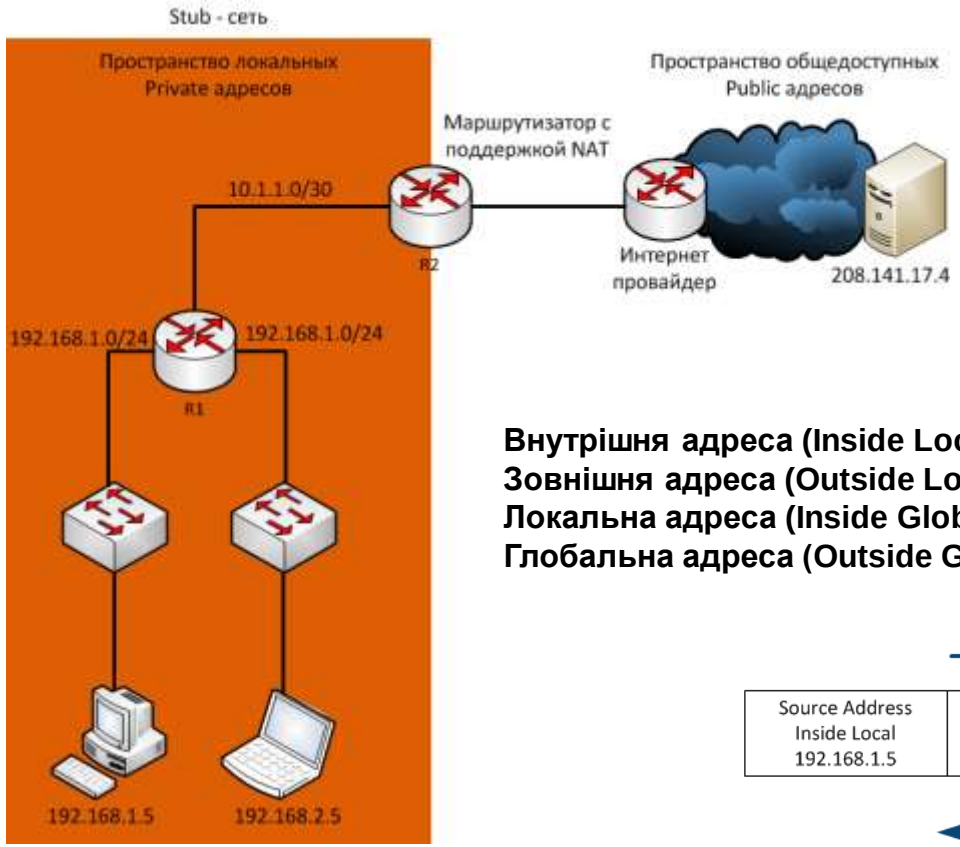
1) NAT зберігає зареєстровану схему адресації, дозволяючи приватизацію мереж Інтранет. Внутрішні хости можуть спільно використовувати одну загальнодоступну IPv4-адресу для всіх зовнішніх комунікацій. В цьому випадку потрібно мало зовнішніх адрес для підтримки багатьох внутрішніх хостів;
2) NAT підвищує гнучкість з'єднань із загальнодоступною мережею;
3) NAT забезпечує узгодженість для внутрішніх схем адресації мережі. Це означає, що організація-клієнт може змінювати провайдерів, і їй не потрібно змінювати конфігурацію своєї внутрішньої мережі;
4) NAT забезпечує безпеку мережі. Інтранет мережі не анонсують назовні свої адреси або внутрішню топологію, вони залишаються достатньо надійними при використанні у поєднанні з NAT для отримання зовнішнього доступу, що контролюється. Важливо – NAT не замінює фаєрволи (брандмауери).

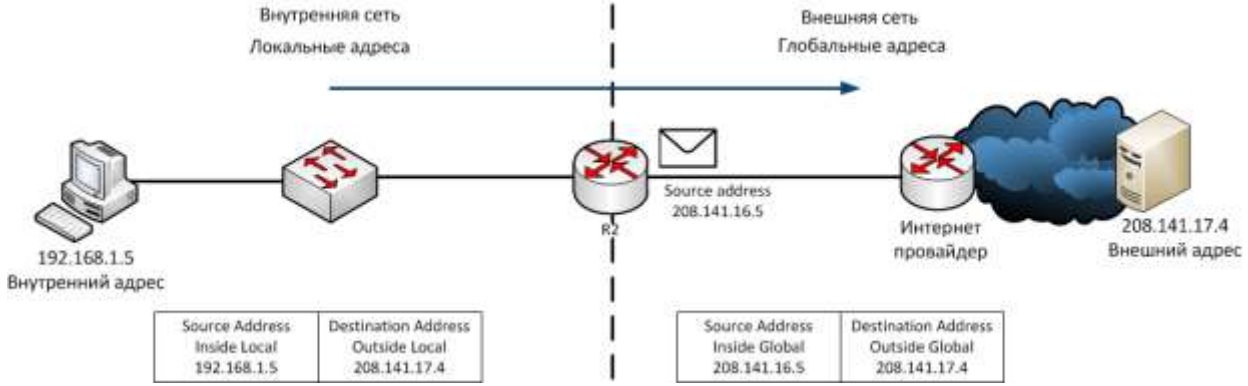
B. Недоліків:

1) NAT збільшує затримки перемикання, тому що переклад кожної IPv4 адреси в заголовках пакетів вимагає часу. Тому продуктивність мережі падає, що може зашкодити працездатності протоколів реального часу;
2) Втрата наскрізної адресації, яку вимагають деякі інтернет-протоколи та додатки, які використовують фізичні адреси, а не Fully Qualified Domain Name (певне ім'я домену);
3) Втрата наскрізного трасування пакетів, які зазнають численних змін адрес пакетів протягом декількох NAT-переходів, що ускладнює пошук та усунення неполадок;
4) Використання NAT ускладнює використання протоколів тунелювання, такі як IPsec, оскільки NAT змінює значення в заголовках, які заважають перевіркам цілісності, що виконуються IPsec та іншими протоколами тунелювання;
5) Служби, що вимагають ініціювання TCP-з'єднань із зовнішньої мережі, або stateless протоколи, наприклад, що використовують UDP, можуть бути порушені. Якщо маршрутизатор NAT не налаштований для підтримки таких протоколів, вхідні пакети не можуть досягти свого адресата.

How does NAT work?

Network Address Translation (NAT)



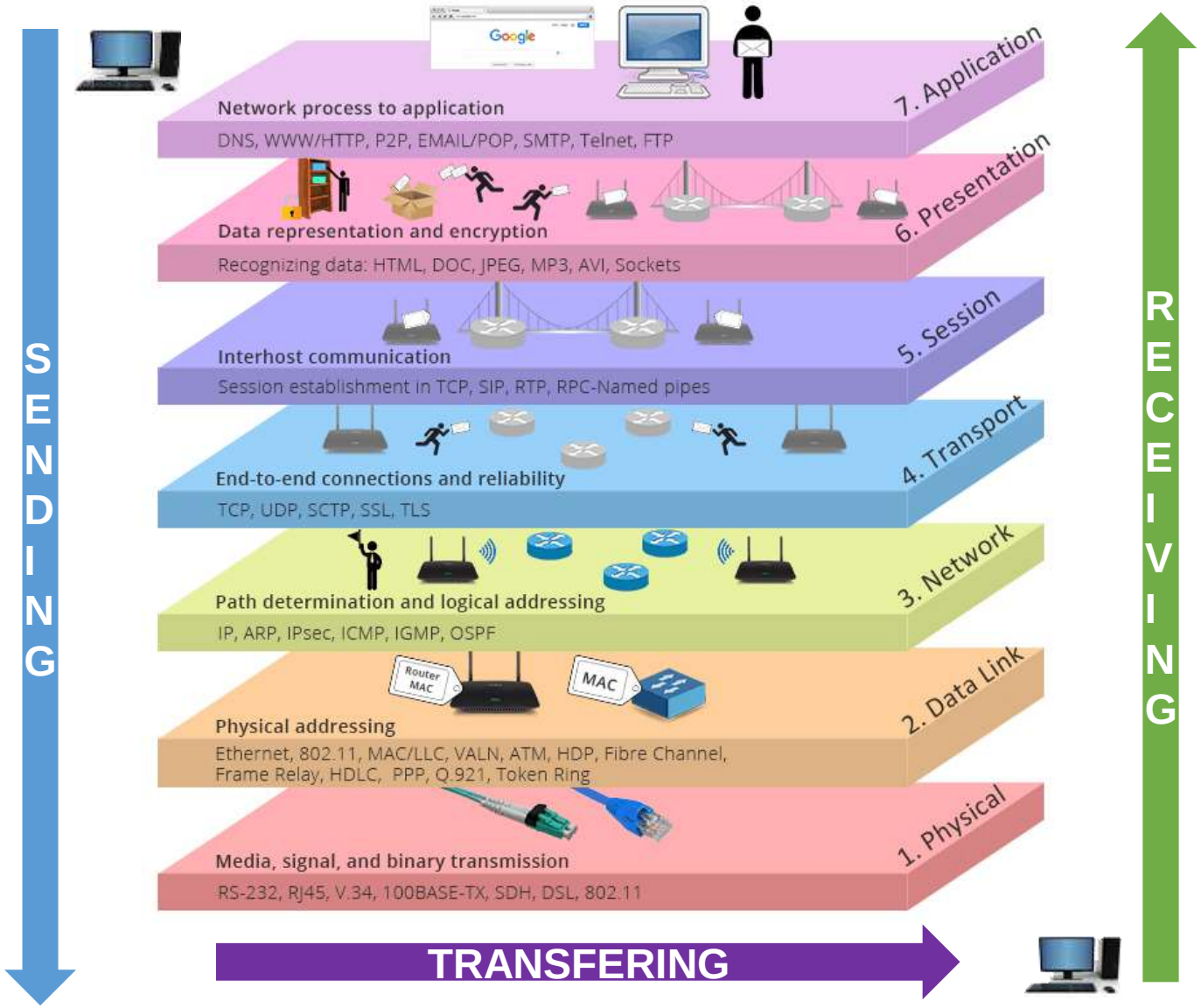


Внутрішня адреса (Inside Local address) - адреса пристрою, який транслюється NAT;
Зовнішня адреса (Outside Local address) - адреса пристрою призначення;
Локальна адреса (Inside Global address) - це будь-яка адреса, яка відображається у внутрішній частині мережі;
Глобальна адреса (Outside Global address) - це будь-яка адреса, яка відображається в зовнішній частині мережі;

NAT таблица маршрутизатора			
ПК		Веб-сервер	
Inside Global	Inside Local	Outside Local	Outside Global
208.141.17.4	192.168.1.5	208.141.16.5	208.141.16.5

a) Types of NAT

Модель OSI та навіщо вона потрібна?

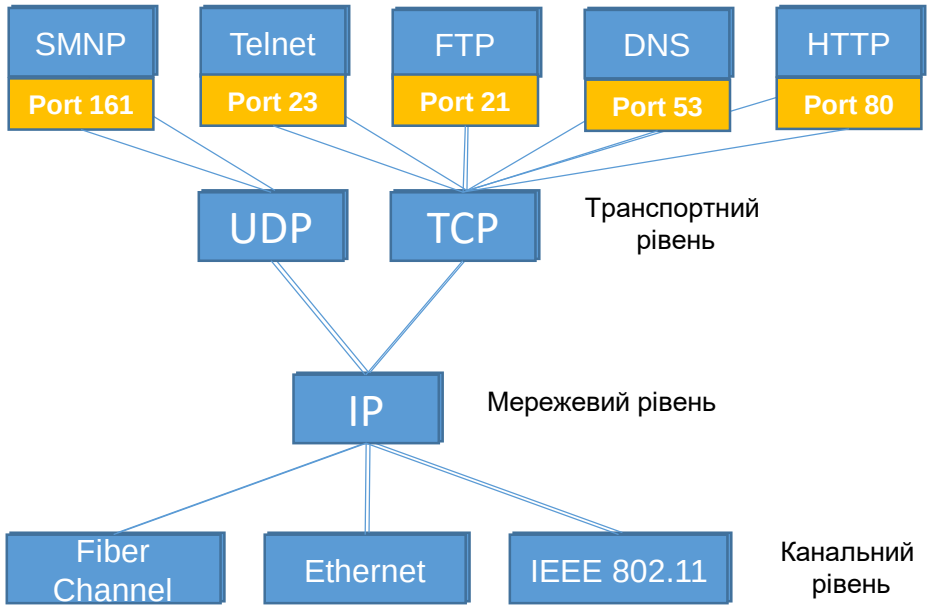


Мережева модель OSI (The Open Systems Interconnection model) — мережева модель стеку (магазину) мережевих протоколів OSI/ISO. За допомогою цієї моделі різні мережні пристрої можуть взаємодіяти один з одним. Модель визначає різні рівні взаємодії систем. Кожен рівень виконує певні функції за такої взаємодії.

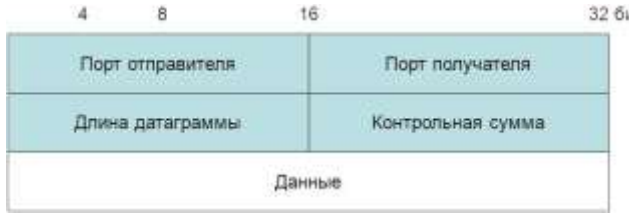
a) What is OSI Model?
b) Network Protocols
c) TCP/UDP and their place in the OSI

Протоколи TCP і UDP

Транспортний рівень мережевої моделі OSI призначений для доставки даних. При цьому не має значення, які дані передаються, звідки й куди. Блоки даних поділяються на фрагменти, розміри яких залежить від використовуваного протоколу. Протоколи цього рівня призначені взаємодії типу точка-точка.
Існує безліч класів протоколів транспортного рівня, починаючи від протоколів, що надають лише основні транспортні функції, наприклад, функції передачі даних без підтвердження прийому, і закінчуючи протоколами, які гарантують доставку до пункту призначення декількох пакетів даних у належній послідовності, мультиплексують кілька потоків даних, забезпечують механізм управління потоками даних та гарантують достовірність прийнятих даних.
Два основні протоколи: **TCP** (RFC 9293) і **UDP** (RFC 768) .



Структура заголовку UDP



Структура заголовку TCP

Пояснення моделі TCP IP
Протоколи або навіщо потрібна IP адресація?

Протоколи TCP і UDP. Порти.

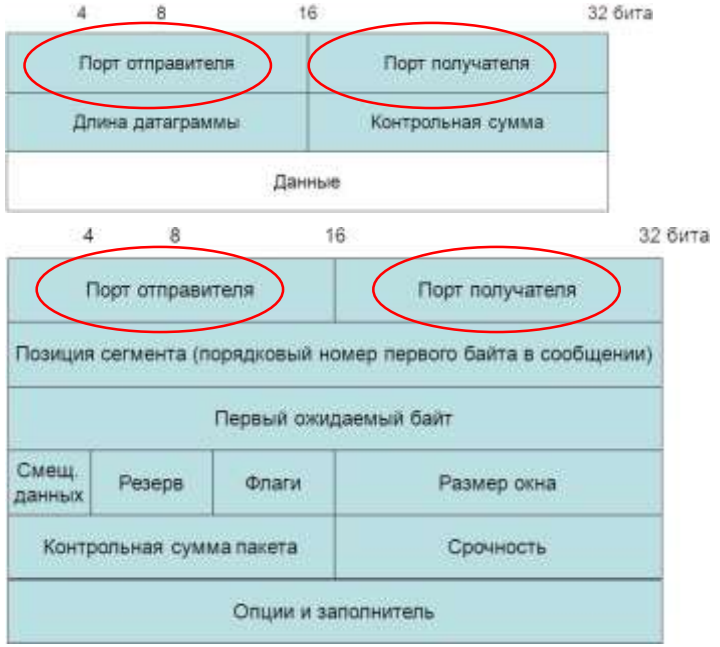
Мережеві порти (https://iana.org) дають інформацію про програми, які звертаються до мережних пристроїв. Знаючи програми, які використовують мережу, та відповідні мережеві порти, можна скласти точні правила для брандмауера, і налаштувати хости таким чином, щоб вони пропускали лише корисний трафік.

У протоколах TCP і UDP **порт** — ідентифікований номером системний ресурс, що виділяється додатку, що виконується на деякому мережевому хості, для зв'язку з додатками, що виконуються на інших мережевих хостах (а також з іншими додатками на цьому ж хості).

Основні правила необхідні розуміння роботи порту:

1) Порт може бути зайнятий лише однією програмою і в цей момент не може використовуватись іншою.
2) Всі програми для зв'язку між собою за допомогою мережі використовують порти.

Для кожного з протоколів TCP та UDP стандарт визначає можливість одночасного виділення на хості до 65536 унікальних портів з номерами від 0 до 65535. При передачі по мережі номер порту в заголовку пакета використовується (разом з IP-адресою хоста) для адресації конкретної програми (і конкретного мережного з'єднання, що йому належить).



Приклади портів:

443: HTTP Secure (HTTPS)
21: File Transfer Protocol (FTP)
22: Secure Shell (SSH)
25: Простой протокол передачи почты (SMTP)
53: Система доменных имен (DNS)
80: Протокол передачи гипертекста (HTTP)
110: Post Office Protocol Version 3 (POP3)
123: Протокол сетевого времени (NTP)
143: Internet Message Access Protocol (IMAP)
161: Простой протокол управления сетью (SNMP)1
94: Internet Relay Chat (IRC)
5060: Session Initiation Protocol (SIP)
5061: Session Initiation Protocol (SIP)

Протоколи TCP і UDP. Порти.

Порт - це умовне число від 0 до 65535, що дозволяють різним програмам, виконуваним одному хості, отримувати дані незалежно друг від друга (надають так звані мережеві сервіси). Кожна програма обробляє дані, що надходять на певний порт (іноді говорять, що програма слухає цей номер порту).Зазвичай за деякими поширеними мережевими протоколами закріплені стандартні номери портів (наприклад, веб-сервери зазвичай приймають дані протоколу TCP-порт 80), хоча у більшості випадків програма може використовувати будь-який порт. Порт - це умовне число від 0 до 65535, що дозволяють різним програмам, виконуваним одному хості, отримувати дані незалежно друг від друга (надають звані мережеві сервіси). Кожна програма обробляє дані, що надходять на певний порт (іноді говорять, що програма слухає цей номер порту).Зазвичай за деякими поширеними мережевими протоколами закріплені стандартні номери портів (наприклад, веб-сервери зазвичай приймають дані протоколу TCP-порт 80), хоча у більшості випадків програма може використовувати будь-який порт.

TCP- або UDP-пакети завжди містять два поля номера порту: відправника та одержувача.

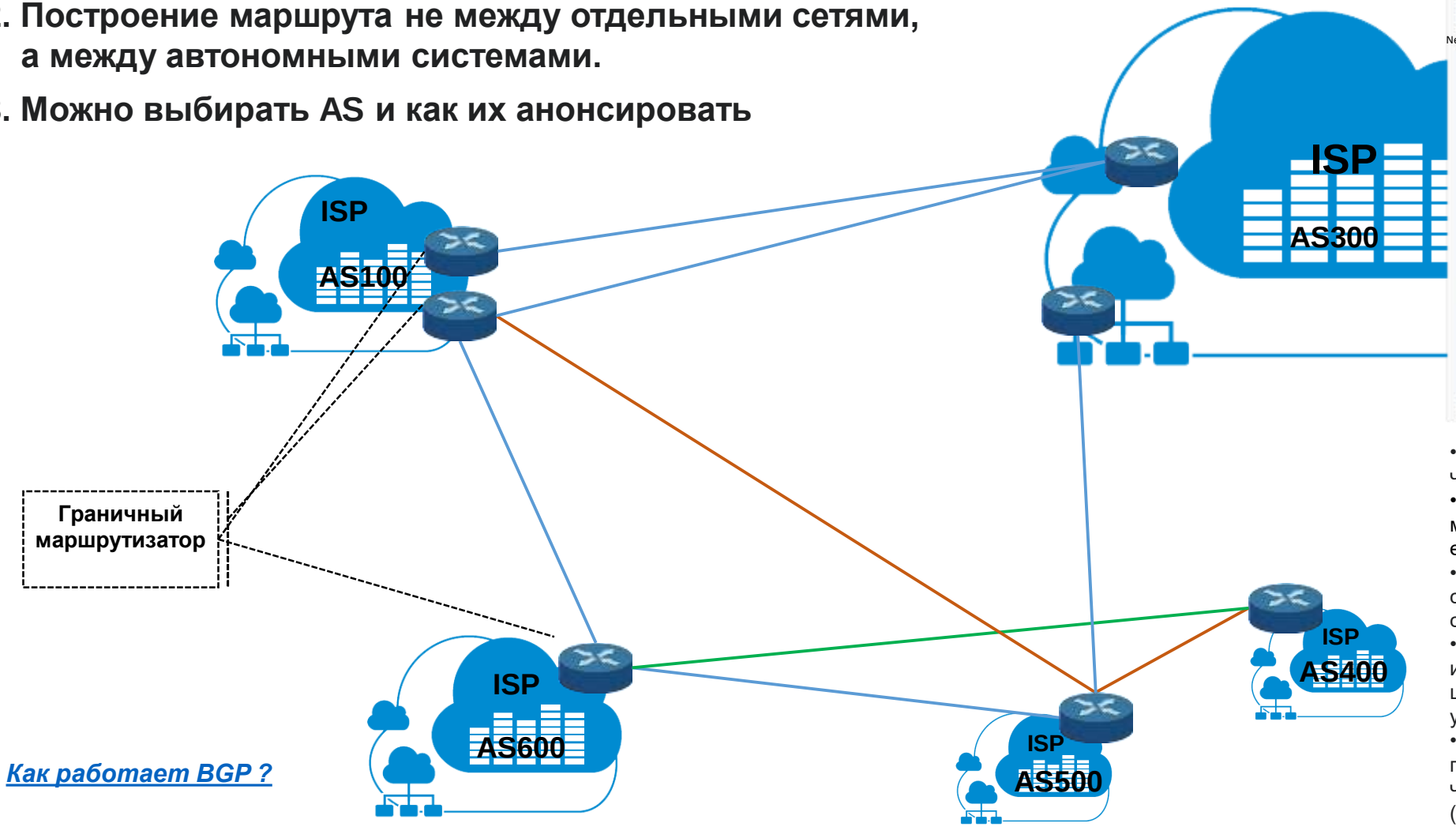
Тип **обслуговуючої програми** визначається портом одержувача запитів, що надходять, і цей же номер є портом відправника відповідей. «Зворотний» порт (порт відправника запитів, він порт одержувача відповідей) при підключенні по TCP визначається клієнтом довільно (хоча номери менше 1024 і вже зайнятих портів не призначаються), і користувача інтересу не представляє. Використання зворотних номерів портів UDP залежить від реалізації.

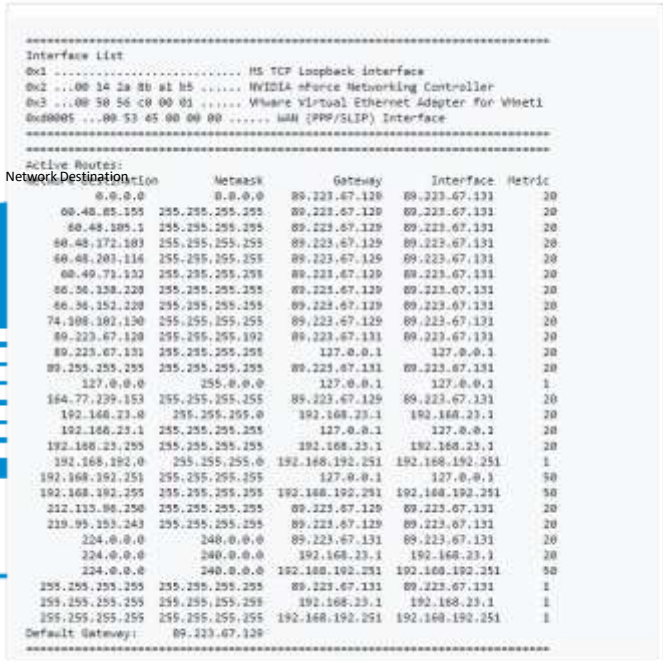
Номери портів

Протокол BGP

BGP предназначен для обмена информацией о маршрутизации и доступности между **автономными системами (AS)** в Интернете. Передача данных – используется протокол TCP, порт 179

1. **Внешняя маршрутизация**
2. **Построение маршрута не между отдельными сетями, а между автономными системами.**
3. **Можно выбирать AS и как их анонсировать**

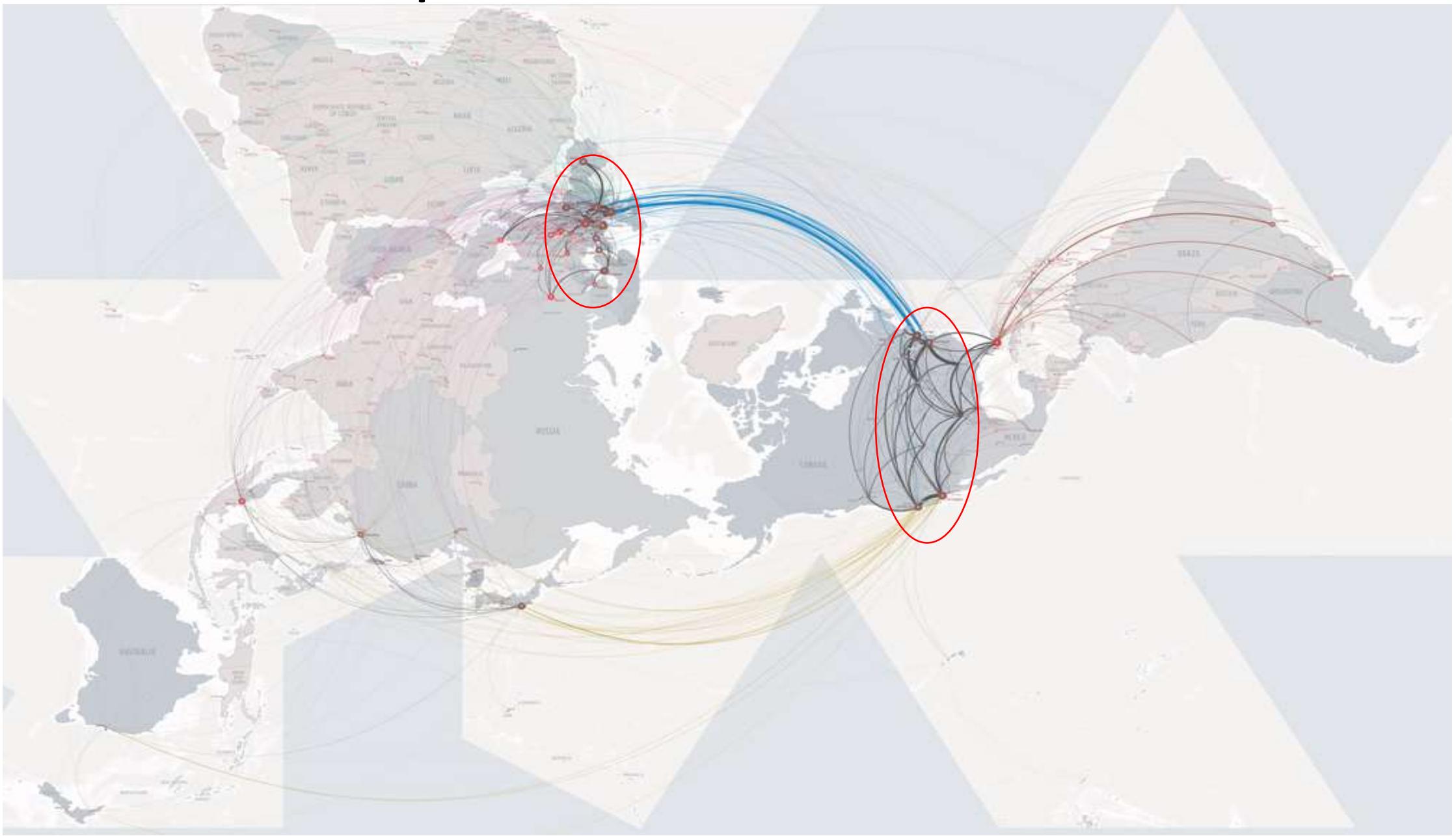


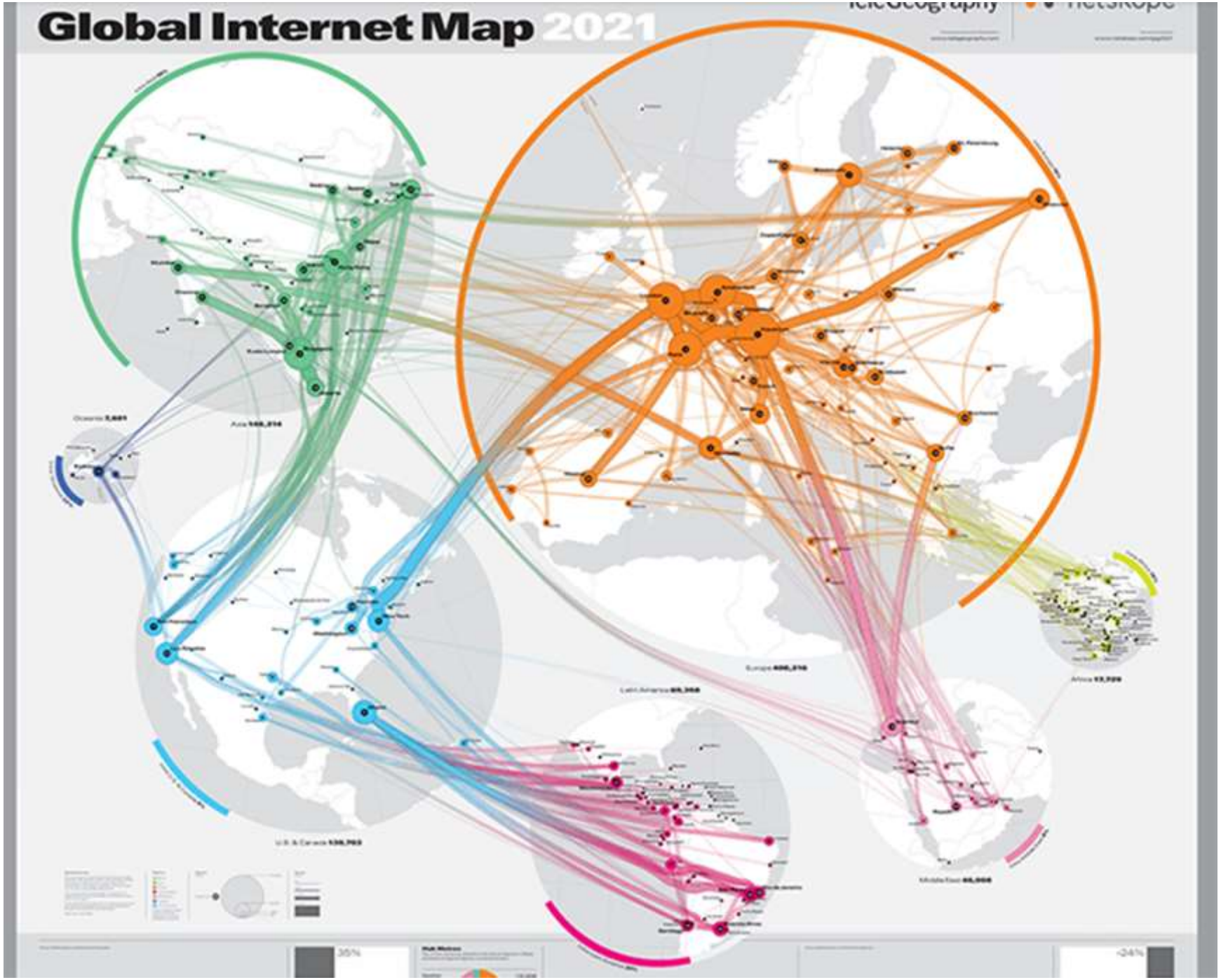


•**адрес сети или узла назначения**, либо указание, что маршрут является *маршрутом по умолчанию*
•**маска сети назначения** (для IPv4-сетей маска /32 (255.255.255.255) позволяет указать единичный узел сети)
•**шлюз**, обозначающий адрес маршрутизатора в сети, на который необходимо отправить пакет, следующий до указанного адреса назначения
•**интерфейс**, через который доступен шлюз; интерфейс может быть отличен от шлюза, если шлюз доступен через дополнительное сетевое устройство, например, сетевую карту
•**метрика** — числовой показатель, задающий предпочтительность маршрута. Чем меньше число, тем более предпочтителен маршрут (интуитивно представляется как расстояние).

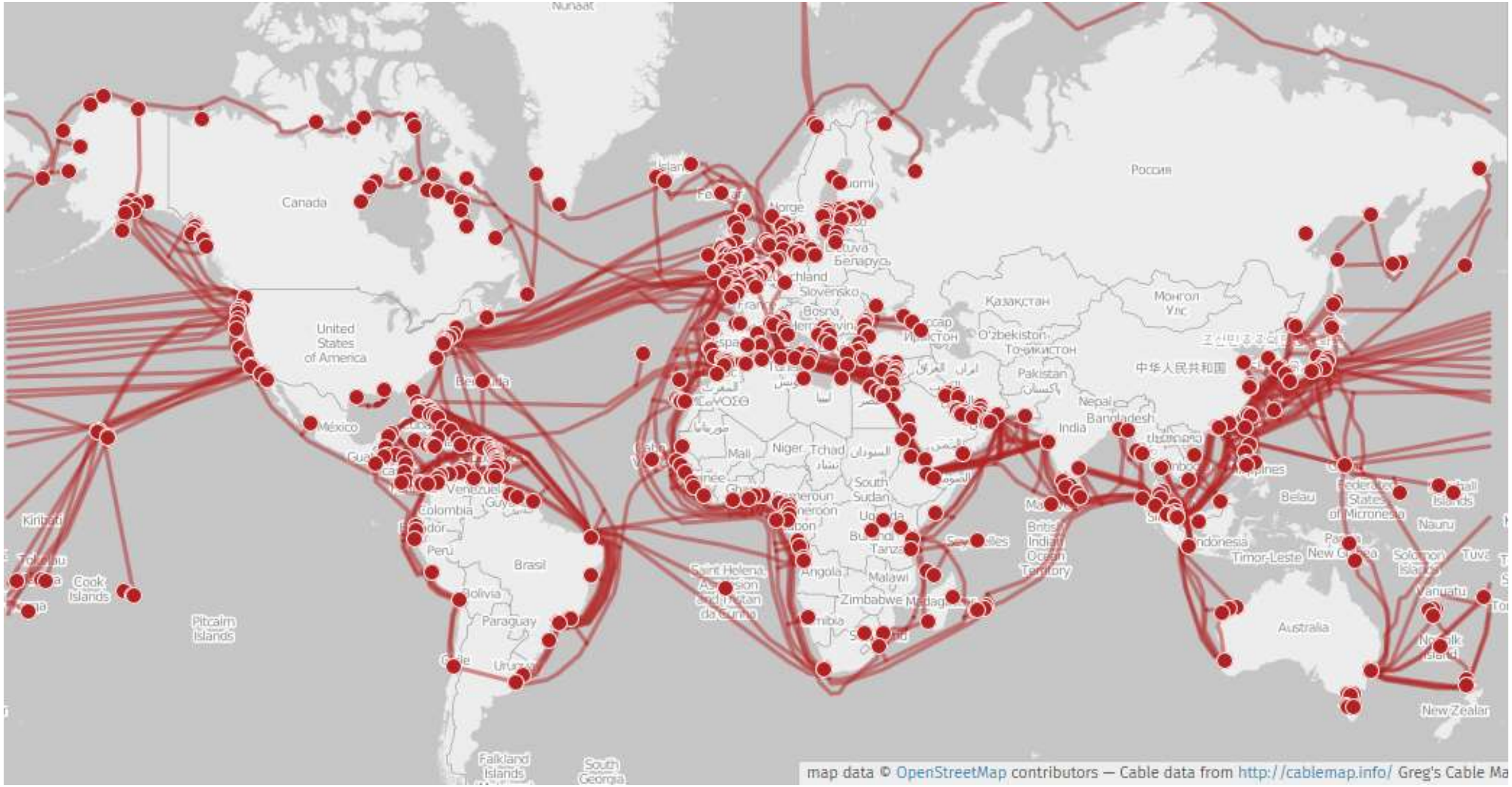
Как работает BGP ?

Global Internet Map 2012




Global Internet Map 2021

Global Internet Backbone



Internet Backbone

Опорна мережа Інтернету (англ. Internet backbone) — головні магістралі передачі між величезними, стратегічно взаємопов'язаними мережами і основними маршрутизаторами в Інтернеті.

Ці магістралі передачі даних контролюються комерційними, державними, науковими та іншими високопродуктивними центрами, точками обміну трафіком та точками доступу до мережі, які обмінюються інтернет-трафіком між країнами та континентами. Інтернет-провайдери (часто Tier-1-оператори) беруть участь в обміні трафіком опорної мережі Інтернету за допомогою приватно укладених угод про з'єднання мереж, головним чином за принципом пірингу.

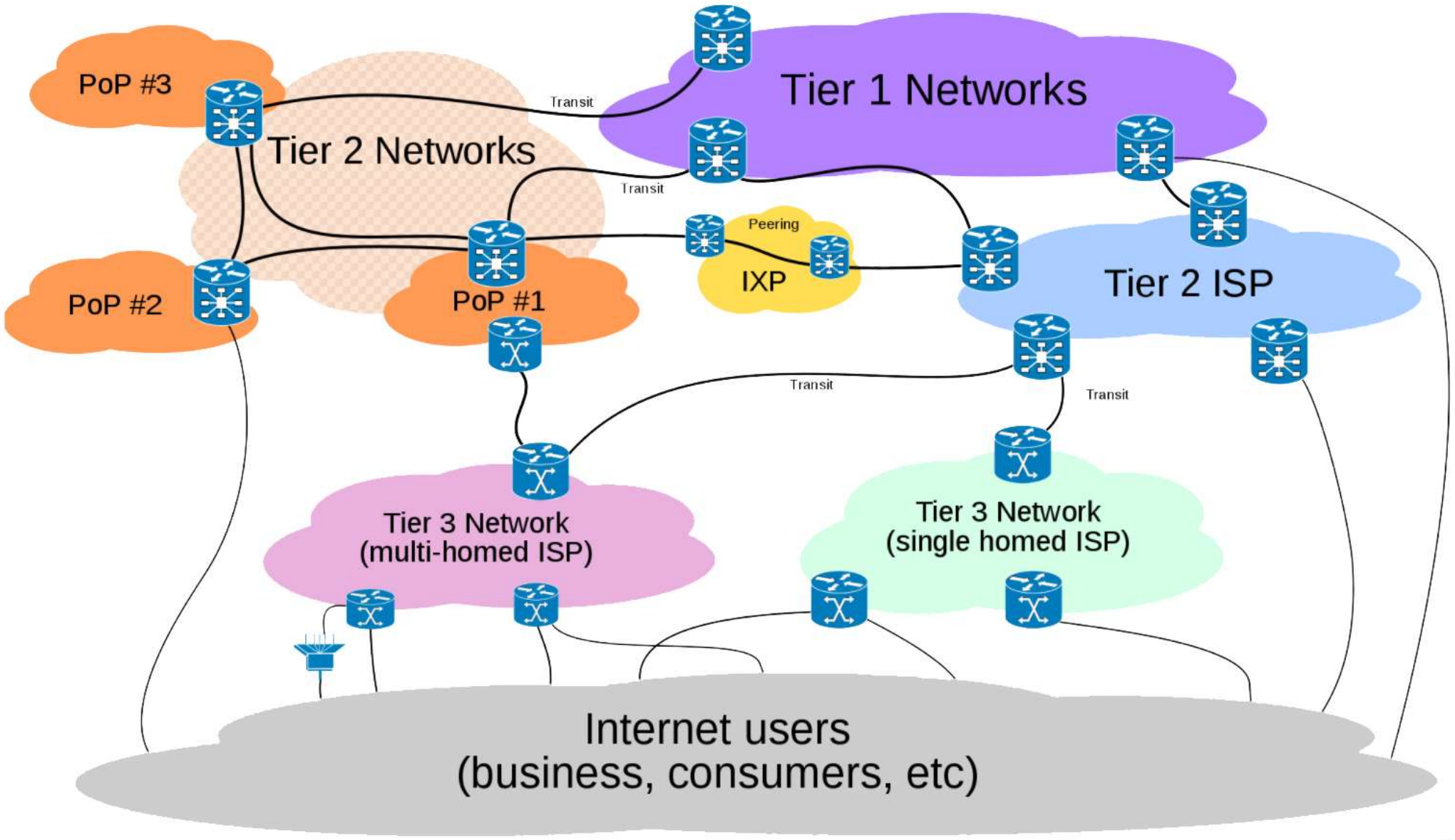
Магістральна мережа зв'язку – транспортна телекомунікаційна інфраструктура для надання послуг зв'язку. Як правило, магістральна мережа зв'язку шикується на власних або орендованих волоконно-оптичних лініях з використанням високошвидкісного або низькошвидкісного канального обладнання зв'язку.

Levels of Internet Infrastructure

What is the Internet backbone?

Рівні технічно інфраструктури Інтернет

Network architecture of different levels on the Internet



ISPs Tier1, Tier2 and Tier3

Network architecture of different levels on the Internet

Tier-1 — оператор, который имеет доступ к сети Интернет исключительно через пиринговые соединения.

- Операторы Tier-1 ближе к «ядру (центру) Интернета».
- Операторы Tier-1 предоставляют лучшее соединение с Интернетом.

Tier-2 — оператор, который имеет доступ к части сети Интернет через пиринговые соединения, но покупает транзит IP-трафика для доступа к остальной части Интернета.

- Операторы Tier-2 являются посредниками в продаже Интернета от Tier-1.
- Многие Tier-2 основную часть Интернета видят через паритетные каналы, и лишь небольшую оставшуюся часть — через платный IP-транзит.
- Некоторые Tier-2 значительно больше некоторых Tier-1, и могут предоставлять соединение лучшего качества или более скоростное.

Tier-3 — оператор, который для доступа к сети Интернет использует исключительно каналы, которые покупает у других операторов.

Опорная сеть Интернета (англ. Internet backbone) — главные магистрали передачи данных между огромными, стратегически взаимосвязанными сетями и основными маршрутизаторами[en] в Интернете. Эти магистрали передачи данных контролируются коммерческими, государственными, научными и другими высокопроизводительными центрами, точками обмена трафиком и точками доступа к сети[en], которые обмениваются интернет-трафиком между странами и континентами. Интернет-провайдеры (часто Tier-1-операторы) участвуют в обмене трафиком опорной сети Интернета с помощью частным образом заключённых соглашений о соединениях сетей, главным образом по принципу пиринга.

Рівні операторів Інтернет мереж

Tier-1 - оператор, який має доступ до мережі Інтернет виключно через безплатні пірингові з'єднання;
Tier-2 - оператор, який має доступ до частини мережі Інтернет через пірингові з'єднання, але купує транзит IP-трафіку для доступу до решти Інтернету;
Tier-3 - оператор, який для доступу до мережі Інтернет використовує виключно канали, які купує в інших операторів.

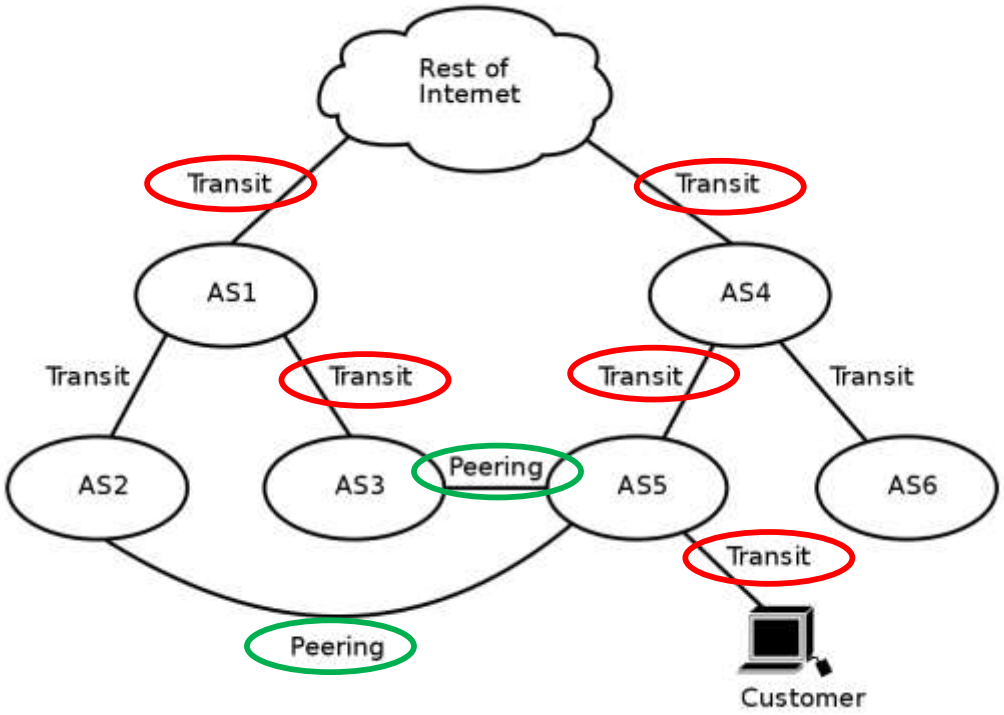
Відносини між різними рівнями інтернет-провайдерів

Мережа рівня 1 — це мережа Інтернет, яка може підключатися до будь-якої іншої Інтернету виключно через міжз'єднання без розрахунків. Це називається піринг без розрахунків. Мережі рівня 1 можуть обмінюватися трафіком з іншими мережами рівня 1 без сплати будь-яких комісій за обмін трафіком у будь-якому напрямку. Мережі рівня 2 і всі мережі 3 повинні платити за передачу трафіку в інші мережі.
Немає органу, визначального рівні мереж, що у Інтернеті. Найбільш поширене та загальноприйняте визначення мережі рівня 1 – це мережа, яка може підключатися до будь-якої іншої мережі в Інтернеті без покупки IP-транзиту або оплати пірингу.
Відповідно до цього визначення, мережа рівня 1 повинна бути мережею без купівлі послуг транзиту, яка безкоштовно взаємодіє з будь-якою іншою мережею рівня 1 і може підключатися до всіх основних мереж в Інтернеті. Не всі мережі без транзиту є мережами рівня 1, оскільки можна стати вільним від транзиту, заплативши за піринг, а також можна обійтися без транзиту без доступу до всіх основних мереж в Інтернеті.
Спільнота пірінгу в Інтернеті — це набір координаторів пірінгу, присутніх у точках обміну даними в Інтернеті більш ніж на одному континенті.
Загальні визначення мереж рівня 2 та рівня 3:
Мережа рівня 2: Мережа, яка безкоштовно зв'язується з деякими мережами, але при цьому купує IP-транзит або платить за піринг, щоб отримати доступ до якоїсь частини Інтернету.
Мережа рівня 3: Мережа, яка купує транзит/піринг виключно в інших мережах для участі в Інтернеті.

Пиринг

Пиринг (peering — соседствование) — соглашение интернет-операторов об обмене трафиком между своими сетями, а также техническое взаимодействие, реализующее данное соглашение: соединение сетей и обмен информацией о сетевых маршрутах по протоколу BGP, содержащее три элемента:

- **физическое соединение сетей;**
- **техническое взаимодействие между сетями, обмен маршрутами;**
- **коммерческие и договорные пиринговые соглашения**.

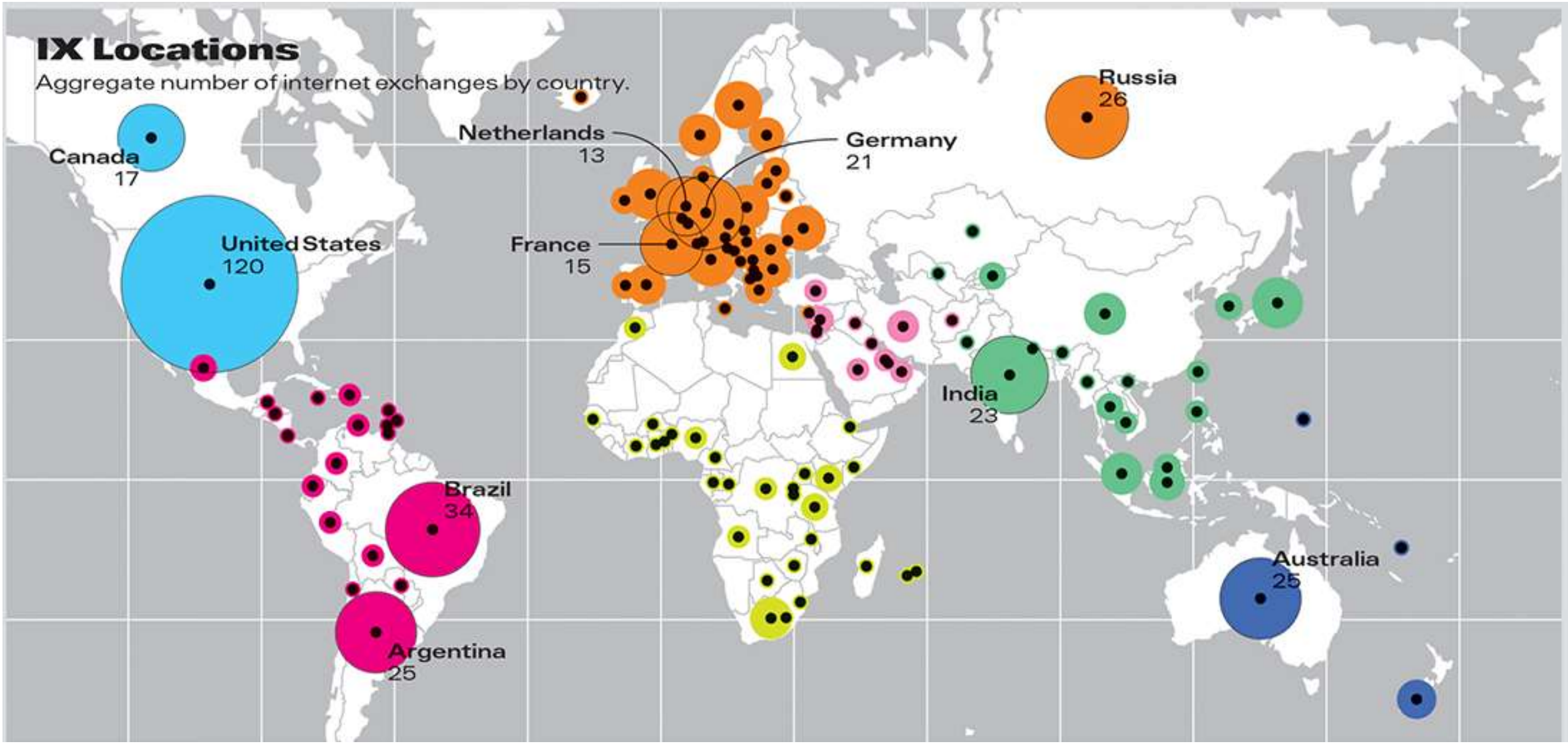


Пиринг предполагает объединение двух сетей для свободного обмена трафиком друг с другом для взаимной выгоды. Эта «взаимная выгода» чаще всего является мотивацией пиринга, которая часто описывается исключительно как «снижение затрат на услуги транзита». Другие менее ощутимые мотивы могут включать:

- повышенную избыточность (за счет снижения зависимости от одного или нескольких транзитных провайдеров),
- повышенную пропускная способность для чрезвычайно больших объемов трафика (распределение трафика по множеству сетей),
- повышенный контроль маршрутизации трафика,
- повышенную производительность (попытка обойти потенциальные узкие места с помощью «прямого» пути),
- улучшение восприятия своей сети (возможность претендовать на «более высокий уровень»),
- Легкость обращения за неотложной помощью (от дружественных AS).

How Network Peering Works?

Internet Exchange Points (IXP)



Ukranian Internet Backbone