



УКРАЇНА

(19) **UA** (11) **92153** (13) **C2**
(51) **МПК (2009)**
H04L 29/06
H04L 12/28

МІНІСТЕРСТВО ОСВІТИ
І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ

ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(54) ШВИДКЕ ВСТАНОВЛЕННЯ З'ЄДНАННЯ ДЛЯ ДОСТУПУ ДО МЕРЕЖІ

1

(21) a200702124
(22) 29.07.2005
(24) 11.10.2010
(86) PCT/US2005/027069, 29.07.2005
(31) 11/193,068
(32) 28.07.2005
(33) US
(31) 60/592,470
(32) 30.07.2004
(33) US
(46) 11.10.2010, Бюл.№ 19, 2010 р.
(72) ЛІОЙ МАРЧЕЛЛО, US, ВАН ЦЗЮНЬ, US, СІ-РОТА МАСАКАЗУ, JP, ХСУ РЕЙМОНД ТАХ-ШЕНГ, US, ВЕСРЕПАЛЛІ СІВАРАМАКРІШНА, US
(73) КВЕЛКОММ ІНКОРПОРЕЙТЕД, US
(56) EP 1434404 A; 30.06.2004
(57) 1. Спосіб сеансу зв'язку для доступу до мережі через вузол (46) доступу до мережі, що містить етапи, на яких:
встановлюють у першому вузлі (44) фізичний канал зв'язку зі згаданим вузлом (46) доступу до мережі;
приймають у першому вузлі (44) від згаданого вузла (46) доступу до мережі через згаданий фізичний канал зв'язку перше повідомлення (56), яке включає в себе запит аутентифікації;
надають у першому вузлі (44) перший набір варіантів параметрів для відповіді на згаданий запит аутентифікації, конфігурації каналу зв'язку і доступу до мережі в другому повідомленні (58);
відправляють зі згаданого першого вузла (44) згадане друге повідомлення (58) згаданому вузлу (46) доступу до мережі через згаданий фізичний канал зв'язку;
приймають у згаданому першому вузлі (44) від згаданого вузла (46) доступу до мережі через згаданий фізичний канал зв'язку третє повідомлення (60), яке включає в себе вибір згаданого першого набору варіантів параметрів згаданого другого повідомлення (58); і
починають у згаданому першому вузлі (44) згаданий доступ до мережі через згаданий фізичний канал зв'язку, коли згаданий вибір згаданого першого набору варіантів параметрів задовольняє порогове значення.
2. Спосіб за п. 1, причому згаданий спосіб додатково містить етап, на якому відправляють зі згада-

2

ного першого вузла (44) четверте повідомлення, яке має другий набір варіантів параметрів, відмінний від згаданого першого набору варіантів параметрів, згаданому вузлу (46) доступу до мережі, коли згаданий вибір згаданого першого набору варіантів параметрів не задовольняє порогове значення.

3. Спосіб за п. 1, у якому, якщо перед наданням згаданим першим вузлом (44) згаданого набору варіантів параметрів згаданий перший вузол (44) приймає PPP-повідомлення (протокол точка-точка) від згаданого вузла (46) доступу до мережі, згаданий спосіб додатково включає в себе етап, на якому згаданий перший вузол (44) негайно приступає до здійснення зв'язку зі згаданим вузлом (46) доступу до мережі, відправляючи інше PPP-повідомлення у відповідь на згадане PPP-повідомлення.

4. Спосіб за п. 3, який додатково містить етап, на якому у згаданому першому вузлі (44) надають пакет даних для згаданого повідомлення, що має формат пакета даних, по суті подібний до відповідного формату пакета даних згаданих PPP-повідомлень.

5. Спосіб за п. 1, який додатково містить етап, на якому згаданий перший вузол (44) обмінюється луна-повідомленнями зі згаданим вузлом (46) доступу до мережі після попередньо визначеного періоду бездіяльного зв'язку зі згаданим вузлом (46) доступу до мережі.

6. Спосіб за п. 1, який додатково включає в себе етапи, на яких згаданий перший вузол (44) обмінюється користувацькими даними для згаданого доступу до мережі зі згаданим вузлом (46) доступу до мережі, і приймає повідомлення аутентифікації від згаданого вузла (46) доступу до мережі в процесі згаданого доступу до мережі.

7. Спосіб за п. 1, у якому система зв'язку підтримує IP (Інтернет-протокол).

8. Спосіб сеансу зв'язку з першим вузлом (44), який намагається здійснити доступ до мережі, у системі зв'язку, що містить етапи, на яких:

відправляють у вузлі (46) доступу до мережі перше повідомлення (56), яке включає в себе запит аутентифікації від згаданого першого вузла (44) при встановленні фізичного каналу зв'язку зі згаданим першим вузлом (44);

(13) **C2**

(11) **92153**

(19) **UA**

приймають у вузлі (46) доступу до мережі від згаданого першого вузла (44) через згаданий фізичний канал зв'язку друге повідомлення (58), яке включає в себе перший набір варіантів параметрів для відповіді на згаданий запит аутентифікації, конфігурації каналу зв'язку і доступу до мережі; відправляють у вузлі (46) доступу до мережі через згаданий фізичний канал зв'язку третє повідомлення (60), яке включає в себе вибір згаданого першого набору варіантів параметрів згаданого другого повідомлення (58); і

приймають у вузлі (46) доступу до мережі дані для згаданого доступу до мережі від згаданого першого вузла (44) через згаданий фізичний канал зв'язку, коли згаданий перший вузол (44) визнає, що згаданий вибір згаданого першого набору варіантів параметрів задовольняє порогове значення.

9. Спосіб за п. 8, причому згаданий спосіб додатково включає в себе етап, на якому приймають у згаданому вузлі (46) доступу до мережі зі згаданого першого вузла (44) четверте повідомлення, що включає в себе другий набір варіантів параметрів, відмінний від згаданого першого набору варіантів параметрів, коли згаданий вибір згаданого першого набору варіантів параметрів не задовольняє згадане порогове значення.

10. Спосіб за п. 8, у якому, якщо після згаданого встановлення згаданого фізичного каналу зв'язку згаданий вузол (46) доступу до мережі приймає PPP-повідомлення (протокол точка-точка) від згаданого першого вузла (44), згаданий спосіб додатково включає в себе етап, на якому згаданий вузол (46) доступу до мережі негайно приступає до здійснення зв'язку зі згаданим першим вузлом (44), відправляючи інше PPP-повідомлення у відповідь на згадане PPP-повідомлення.

11. Спосіб за п. 10, що додатково містить етап, на якому надають пакет даних для згаданого повідомлення, що має формат пакета даних, по суті подібний до відповідного формату пакета даних згаданих PPP-повідомлень.

12. Спосіб за п. 8, що додатково включає в себе етап, на якому згаданий вузол (46) доступу до мережі обмінюється луна-повідомленнями зі згаданим першим вузлом (44) після попередньо визначеного періоду бездіяльного зв'язку зі згаданим вузлом.

13. Спосіб за п. 8, що додатково включає в себе етапи, на яких згаданий вузол (46) доступу до мережі обмінюється користувацькими даними для згаданого доступу до мережі зі згаданим першим вузлом (44) і відправляє повідомлення аутентифікації згаданому першому вузлу в процесі згаданого доступу до мережі.

14. Спосіб за п. 8, у якому система зв'язку підтримує IP (Інтернет-протокол).

15. Пристрій для доступу до мережі через вузол доступу до мережі в системі зв'язку, що містить: засіб, у першому вузлі (44), для встановлення фізичного каналу зв'язку зі згаданим вузлом (46) доступу до мережі;

засіб, у першому вузлі (44), для прийому від згаданого вузла (46) доступу до мережі через згаданий фізичний канал зв'язку першого повідомлення (56), яке включає в себе запит аутентифікації;

засіб, у першому вузлі (44), для надання першого набору варіантів параметрів для відповіді на згаданий запит аутентифікації, конфігурації каналу зв'язку і доступу до мережі в другому повідомленні (58);

засіб, у першому вузлі (44), для відправлення згаданого другого повідомлення (58) згаданому вузлу (46) доступу до мережі через згаданий фізичний канал зв'язку;

засіб, у згаданому першому вузлі (44), для прийому від згаданого вузла (46) доступу до мережі через згаданий фізичний канал зв'язку третього повідомлення (60), яке включає в себе вибір згаданого першого набору варіантів параметрів згаданого другого повідомлення (58); і

засіб, у згаданому першому вузлі (44), для початку згаданого доступу до мережі через згаданий фізичний канал зв'язку, коли згаданий вибір згаданого першого набору варіантів параметрів задовольняє порогове значення.

16. Пристрій за п. 15, що додатково містить засіб, у згаданому першому вузлі (44), для відправлення через згаданий фізичний канал зв'язку четвертого повідомлення, що має другий набір варіантів параметрів, відмінний від згаданого першого набору варіантів параметрів, згаданому вузлу (46) доступу до мережі, коли згаданий вибір згаданого першого набору варіантів параметрів не задовольняє згадане порогове значення.

17. Пристрій за п. 15, у якому, якщо перед згаданим першим набором варіантів параметрів, наданим згаданим надавальним засобом, згаданий перший вузол (44) приймає PPP-повідомлення (протокол точка-точка) від згаданого вузла (46) доступу до мережі, згаданий пристрій додатково містить засіб, у згаданому першому вузлі (44), для негайного здійснення зв'язку зі згаданим вузлом (46) доступу до мережі шляхом відправлення іншого PPP-повідомлення у відповідь на згадане PPP-повідомлення.

18. Пристрій за п. 17, що додатково містить засіб, у згаданому першому вузлі (44), для надання пакета даних для згаданого повідомлення, що має формат пакета даних, по суті подібний до відповідного формату пакета даних згаданих PPP-повідомлень.

19. Пристрій за п. 15, що додатково включає в себе засіб, у згаданому першому вузлі (44), для обміну луна-повідомленнями зі згаданим вузлом (46) доступу до мережі після попередньо визначеного періоду бездіяльного зв'язку зі згаданим вузлом (46) доступу до мережі.

20. Пристрій за п. 15, що додатково включає в себе засіб, у згаданому першому вузлі (44), для обміну користувацькими даними для згаданого доступу до мережі зі згаданим вузлом (46) доступу до мережі і засіб, у згаданому першому вузлі (44), для прийому повідомлення аутентифікації від згаданого вузла (46) доступу до мережі в процесі згаданого доступу до мережі.

21. Пристрій за п. 15, причому система зв'язку підтримує IP (Інтернет-протокол).

22. Пристрій для сеансу зв'язку з першим вузлом (44), що намагається здійснити доступ до мережі, у системі зв'язку, що містить:

засіб, у вузлі (46) доступу до мережі, для відправлення першого повідомлення (56), яке включає в себе запит аутентифікації від згаданого першого вузла (44) при встановленні фізичного каналу зв'язку зі згаданим першим вузлом (44);

засіб, у вузлі (46) доступу до мережі, для прийому від згаданого першого вузла (44) через згаданий фізичний канал зв'язку другого повідомлення (58), яке включає в себе перший набір варіантів параметрів для відповіді на згаданий запит аутентифікації, конфігурації каналу зв'язку і доступу до мережі;

засіб, у вузлі (46) доступу до мережі, для відправлення через згаданий фізичний канал зв'язку третього повідомлення (60), яке включає в себе вибір згаданого першого набору варіантів параметрів згаданого другого повідомлення (58); і

засіб, у вузлі (46) доступу до мережі, для прийому даних для згаданого доступу до мережі від згаданого першого вузла (44) через згаданий фізичний канал зв'язку, коли згаданий перший вузол (44) визнає, що згаданий вибір згаданого першого набору варіантів параметрів задовольняє порогове значення.

23. Пристрій за п. 22, що додатково містить: засіб, у вузлі (46) доступу до мережі, для прийому зі згаданого першого вузла (44) через згаданий фізичний канал зв'язку четвертого повідомлення, що має другий набір варіантів параметрів, відмінний від згаданого першого набору варіантів параметрів, коли згаданий перший вузол (44) не визнає, що згаданий вибір згаданого першого набору варіантів параметрів задовольняє порогове значення.

24. Пристрій за п. 23, у якому, якщо після згаданого встановлення згаданого фізичного каналу зв'язку згаданий вузол (46) доступу до мережі приймає

PPP-повідомлення (протокол точка-точка) від згаданого першого вузла (44), згаданий пристрій додатково містить засіб, у згаданому вузлі (46) доступу до мережі, для того, щоб негайно приступити до здійснення зв'язку зі згаданим першим вузлом (44), відправляючи інше PPP-повідомлення у відповідь на згадане PPP-повідомлення.

25. Пристрій за п. 24, що додатково містить засіб, у згаданому вузлі (46) доступу до мережі, для надання пакета даних для згаданого повідомлення, що має формат пакета даних, по суті подібний до відповідного формату пакета даних згаданих PPP-повідомлень.

26. Пристрій за п. 22, що додатково включає в себе засіб, у згаданому вузлі (46) доступу до мережі, для обміну луна-повідомленнями зі згаданим першим вузлом (44) після попередньо визначеного періоду бездіяльного зв'язку зі згаданим вузлом.

27. Пристрій за п. 22, що додатково включає в себе засіб, у згаданому вузлі (46) доступу до мережі, для обміну користувацькими даними для згаданого доступу до мережі зі згаданим першим вузлом (44) і засіб для відправлення повідомлення аутентифікації згаданому першому вузлу (44) у процесі згаданого доступу до мережі.

28. Пристрій за п. 22, причому система зв'язку підтримує IP (Інтернет-протокол).

29. Пристрій для сеансу зв'язку для вузла доступу до мережі в системі зв'язку, що містить:

модуль пам'яті, що включає в себе машиночитані інструкції, який, коли виконується підходящим комп'ютерним обладнанням, спонукає обладнання виконувати етапи способу згідно з будь-яким з пунктів 1-14.

30. Пристрій за п. 29, причому система зв'язку підтримує IP (Інтернет-протокол).

Заявка про пріоритет 35 U.S.C. §119

Дана Заявка на патент заявляє пріоритет Попередньої заявки США № 60/592 470, озаглавленої "Method and Apparatus for Fast Packet Data Session Establishment", зареєстрованої 30 липня 2004 року і призначеної правонаступнику цієї заявки, і таким чином явно міститься в даному документі за допомогою посилання.

I. Галузь техніки, до якої належить винахід

Даний винахід, загалом, належить до передачі пакетів даних, а більш конкретно, до первинних сеансів зв'язку перед встановленням з'єднання передачі пакетних даних для доступу до мережі.

II. Попередній рівень техніки

Глобальна взаємодія мереж дозволяє інформації бути швидко доступною незалежно від географічних відстаней. Фіг.1 показує спрощене схематичне креслення глобального з'єднання мереж, що звичайно іменується як Інтернет, позначений посиланням з номером 20. Інтернет 20 є, по суті, багатьма мережами з різними рівнями ієрархії, сполученими разом. Інтернет 20 працює по IP (протоколу Інтернету), опублікованому IETF (інже-

нерною проблемною групою Інтернет). Деталі IP можуть бути знайдені в RFC (Запити на коментарі) 791, опубліковані IETF.

Приєднаними до Інтернету 20 є різні окремі мережі, іноді звані LAN (локальні обчислювальні мережі) або WAN (глобальні обчислювальні мережі) в залежності від розмірів мережі. Показані на Фіг.1 є деякими з таких мереж 22, 24 і 26.

У кожній з мереж 22, 24 і 26 можуть бути різні частини обладнання, сполучені з і у взаємодії один з одним. Прикладами є комп'ютери, принтери і сервери, якщо назвати тільки деякі, які звичайно називаються вузлами. Коли вузол здійснює зв'язок за межами своєї власної мережі через Інтернет 20, вузлу повинна бути призначена IP-адреса. Призначення IP-адреси може бути ручним або автоматичним. Ручне призначення IP-адреси може бути виконане, наприклад, мережним адміністратором. Більш часто, IP-адреса призначається автоматично, наприклад, виділеним сервером в LAN.

Візьмемо приклад для ілюстрації. Передбачимо, що вузол 30 в мережі 22 намагається відправити пакет даних іншому вузлу 34 в мережі 24. Під

керуванням IP кожний пакет даних повинен мати адресу джерела і адресу одержувача. У цьому випадку адреса джерела - це адреса вузла 30 в мережі 22. Адреса одержувача - це адреса вузла 34 в мережі 24.

Дуже часто потрібні з'єднання вузол-вузол перед доступом до мережі, такої як Інтернет 20. Наприклад, передбачимо, що вузол 30 в мережі 22 є портативним комп'ютером. Вузол 30 портативного комп'ютера не має прямого доступу до мережі 22. Проте, вузол 30 портативного комп'ютера може зв'язатися з NAS (сервером доступу до мережі) 32 в мережі 22 через деякі інші засоби, наприклад, за допомогою комутованого виклику провідного модему через телефонну лінію. У цьому випадку, вузол 30 типово встановлює сеанс PPP (протокол точка-точка) з NAS (сервером доступу до мережі) 32 в мережі 22. Передачі пакетів даних після того, як встановлені між вузлом 30 і мережею 22 або будь-якими іншими мережами через Інтернет 20, будуть проходити через провідний модем і телефонну лінію. Якщо модем передає і приймає сигнали послідовно і асинхронно через телефонну лінію, пакети даних, що передаються по телефонній лінії, також повинні бути відповідно розбиті на кадри, щоб задовольняти вимогам послідовної і асинхронної модемної лінії зв'язку.

Прихід безпроводних технологій дозволяє вузлам переміщатися із своєї спочатку зареєстрованої мережі в іншу мережу. Наприклад, звертаючись знову до Фіг.1, вузол 30 замість постійно сполученого проводом з мережею 22 може бути безпроводним пристроєм, таким як PDA (персональний цифровий помічник), стільниковим телефоном або мобільним комп'ютером. Безпроводний вузол 30 може переміщуватися за межі своєї домашньої мережі 22. Таким чином, вузол 30 може пересуватися далеко від своєї домашньої мережі 22 в чужу мережу 26. Щоб одержати доступ до мережі 26 або бути сполученим з іншими мережами через Інтернет 20, вузол 30 також типово встановлює PPP-сеанс з NAS (сервером доступу до мережі) 33 в мережі 26. Зв'язок між вузлом 30 і NAS 33 в цьому випадку існує через радіоканал. З іншого боку, пакети даних, що передаються між вузлом 30 і безпроводною мережею, також повинні бути розбиті на кадри, щоб уміститися в формат, який встановлений під час PPP-сеансу між вузлом 30 і NAS 33 через радіоканал.

Основна частина PPP описується в RFC 1661 і 1662, опублікованих IETF. PPP є протоколом взаємодії рівноправних систем, в якому обидва вузли є рівноправними. Тобто, ні один не приймає на себе роль ні клієнта, ні сервера. Кожна сторона може запитати дії або виконати дії по відношенню до іншої. По суті, PPP є дослідницьким і сеансом, що домовляється між вузлами, під час якого вузли дізнаються про ресурси один одного в термінах можливостей і доступності і остаточно наближаються до того, щоб встановити взаємно прийнятні варіанти параметрів, перед яким-небудь потоком мережного трафіку.

Фіг.2 показує блок-схему послідовності зразкового PPP-сеансу 34 зв'язку, в якому вузол 30 в мережі 26 намагається встановити канал зв'язку

(прим: з'єднання, канал зв'язку - будь-який вид комунікаційного шляху між двома комп'ютерами (одержувачем і відправником даних)) з NAS 32 для одержання доступу до Інтернету 20.

PPP має ряд компонентів протоколу. У зразковому PPP-сеансі, показаному на Фіг.2, PPP має LCP (протокол керування з'єднанням) 36, CHAP (протокол аутентифікації за методом "виклик-привітання") 38 і IPCP (протокол конфігурації протоколу Інтернету) 40 як компоненти.

Спочатку, після завершення встановлення фізичного каналу зв'язку, тобто, вузол 30 і NAS 33 здатні зв'язатися один з одним на апаратному рівні, наприклад, є необхідність пройти через LCP 36. LCP 36 служить меті встановлення основного каналу зв'язку між вузлом 30 і NAS 33. У час LCP 36 вузол 30 і NAS 33 обмінюються і обговорюють необхідні варіанти параметрів зв'язку один з одним. Варіанти можуть включати в себе максимальний розмір пакета даних в каналі зв'язку, параметри, що належать до керування якістю, схему стиснення поля, що використовується HDLC (високорівневий протокол керування каналом передачі даних) заголовка і чи готовий рівноправний учасник мережі бути аутентифікованим.

Процеси для LCP 36 більш або менш працюють за етикетом "рукостискання" (квітування запитів). Спочатку, запитуюча сторона пропонує один або більше параметрів, відправляючи повідомлення запиту конфігурації. Якщо який-небудь параметр не розпізнається приймаючою стороною, приймаюча сторона відповідає зворотно за допомогою повідомлення відхилення конфігурації. Якщо знехтуваний параметр є критичним для шуканого каналу зв'язку, запитуюча сторона тоді повинна припинити PPP-сеанс.

З іншого боку, якщо параметр розпізнається, але варіант, що належить до параметра, неприйнятний, відповідаюча сторона відправляє зворотне повідомлення про відсутність підтвердження прийому конфігурації. Запитуюча сторона знов може або завершити PPP-сеанс, або відправити інше повідомлення запиту конфігурації з іншим варіантом для того ж параметра.

Як згадано раніше, PPP є протоколом взаємодії рівноправних систем. Або вузол 30, або NAS 33 може бути запитуючою стороною. Те ж саме вважається істинним для ролі відповідаючої сторони. Всі параметри з асоціативно зв'язаними варіантами повинні бути обговорені і відрегульовані таким чином, як описано вище. Можуть бути потрібними декілька циклів узгодження, як показано на Фіг.2. Загальна схема узгодження в своїй основі є одностороннім процесом. Якщо запитуюча сторона визначає, що всі необхідні параметри є прийнятними для відповідаючої сторони, запитуюча сторона відправляє фінальне повідомлення про підтвердження прийому конфігурації відповідаючій стороні. Після того, як обидві сторони відправили повідомлення підтвердження прийому конфігурації, вони потім переходять до фази аутентифікації.

Щоб гарантувати, що сторони авторизовані, повинна бути виконана аутентифікація. Одним способом виконати аутентифікацію є використати інший PPP-компонент CHAP 38. Це типово NAS

33, який ініціює CHAP 38, щоб перевірити ідентичність вузла 30. У час CHAP 38 NAS 33 відправляє повідомлення, зване повідомленням виклику, вузлу 30. Під керуванням CHAP, існує спільно використовуваний секрет, який використовується разом з повідомленням виклику, який використовується, щоб обчислити повідомлення у відповідь з використанням попередньо узгодженого алгоритму. Вузол 30 потім відправляє повідомлення у відповідь, генероване секретним алгоритмом, до NAS 33. NAS 33 після цього порівнює прийняте повідомлення у відповідь з повідомленням, обчисленим самим NAS 33. Якщо порівняння вказує збіг, вузлу 30 говориться перейти до CHAP 38, в якому NAS 33 відправляє повідомлення про успіх CHAP вузлу 30. Інакше сервером NAS 33 відправляється повідомлення про невдачу CHAP.

Альтернативно, замість CHAP 38, аутентифікація може бути виконана за допомогою проходження через PAP (протокол аутентифікації по паролі). У PAP вузол просто відправляє NAS 33 ім'я користувача і пароль для перевірки. Якщо підтверджено, вузлу 30 говориться перейти до PAP.

Якщо вузлу 30 потрібен IP-доступ, інформація, що належить до IP, знову повинна бути передана і узгоджена. Наприклад, серед іншого, вузлу 30 може бути необхідно мати призначення IP-адреси для того, щоб одержати доступ до Інтернет 20 (Fig.1) відповідно до IP. Щоб досягнути цієї мети, починається узгодження і обмін варіантів параметрів по IPCP 40. У зразковому PPP-сеансі 34 вузол 30 спочатку запитує IP-адресу 0.0.0.0 у NAS 33. У відповідь NAS 33 відправляє повідомлення про відсутність підтвердження прийому конфігурації, пропонуючи вузлу 30 використати IP-адресу a.b.c.d. Якщо прийнято, вузол 30 підтверджує використання IP-адреси a.b.c.d, відправляючи NAS 33 інше повідомлення для підтвердження прийому.

Зрештою, коли вузол 30 узгоджує всі параметри, обговорені у час IPCP 40, вузол 30 відправляє повідомлення про підтвердження прийому до NAS 33. Надалі передаються користувацькі дані сеансу доступу до мережі. IP-пакети даних мережного трафіку інкапсулюються в PPP-кадри з параметрами і узгоджуються у час LCP 36 раніше.

У кінці доступу до мережі або вузол 30, або NAS 33 може відправити повідомлення запиту завершення іншому, який після цього відповідає зворотно повідомленням підтвердження завершення і закінчує сеанс зв'язку.

Як може бути видно на Fig.2 і описано вище, дійсно існує ряд повідомлень, які передаються між вузлом 30 і NAS 33 під час PPP-сеансу 34. По суті, затрачується значна тривалість часу. Це особливо вірно, якщо PPP-сеанс 34 узгоджується по повільному каналу зв'язку з високою латентністю даних.

Відповідно, існує необхідність надати більш швидкий і більш ефективний спосіб встановлення первинних каналів зв'язку перед будь-якими наступними рівнями трафіку даних.

Суть винаходу

Сеанс зв'язку між вузлом, який шукає доступ до мережі, і NAS (сервером доступу до мережі) встановлюється за допомогою проходження через

обміни тільки декількома повідомленнями. Спочатку, при установленні фізичного каналу зв'язку між вузлом і NAS, NAS негайно відправляє повідомлення запиту аутентифікації вузлу. У відповідь, вузол відправляє повідомлення запиту, яке включає в себе, на доповнення до відповіді аутентифікації, всі інші варіанти параметрів для конфігурації каналу зв'язку і керування доступом до мережі. NAS потім відбирає і вибирає набір варіантів параметрів з множини і після цього відправляє назад вузлу вибрані варіанти в повідомленні у відповідь. Якщо вибрані варіанти в повідомленні у відповідь задовольняють пороговій величині, вузол просто передає користувацькі дані для доступу до мережі через NAS.

Крім того, можуть бути здійснені можливості обробки відмови, при яких, якщо сеанс зв'язку відповідно до зразкового варіанта здійснення винаходу не може бути встановлений, може бути прийнятий традиційний PPP (протокол точка-точка), щоб продовжити сеанс зв'язку.

Відповідно до одного аспекту винаходу розкрите є способом, пристроєм і носієм, в яких вузол, який намагається одержати доступ до мережі, містить етапи або засоби надання набору варіантів параметрів для аутентифікації, конфігурації каналу зв'язку і доступу до мережі в повідомленні, і відправлення цього повідомлення вузлу доступу до мережі.

Відповідно до іншого аспекту винаходу, розкрите є іншим способом, пристроєм і носієм для вузла доступу до мережі, які містять етапи або засоби прийому від вузла, який намагається одержати доступ до мережі, повідомлення, що включає в себе набір варіантів параметрів для аутентифікації, конфігурації каналу зв'язку і доступу до мережі, і відправлення вузлу, який добивається доступу до мережі, іншого повідомлення, яке стосується авторизації набору варіантів параметрів.

Ці і інші ознаки і переваги будуть очевидні фахівцям в даній галузі техніки з подальшого детального опису, що використовується разом з супроводжувальними кресленнями, на яких однакові номери посилань посилаються на аналогічні частини.

Короткий опис креслень

Fig.1 - схематичне креслення глобального з'єднання мереж;

Fig.2 - схема послідовності з'єднання сеансу зв'язку традиційного протоколу;

Fig.3 - схематичне креслення вузлів, обговорених в зразковому варіанті здійснення винаходу;

Fig.4 - схематичне креслення, яке показує стек протоколів в ієрархічному порядку;

Fig.5 - схема послідовності з'єднання сеансу зв'язку відповідно до зразкового варіанта здійснення винаходу;

Fig.6 - блок-схема, яка показує етапи, які мають на увазі, відповідно до зразкового варіанта здійснення винаходу;

Fig.7 - схема послідовності з'єднання, яка показує зразковий варіант здійснення, виконаний з

можливостями обробки відмови по відношенню до традиційного протоколу;

Фіг.8 - відповідна блок-схема для схеми послідовності з'єднання на Фіг.7;

Фіг.9 - схема іншої послідовності зв'язку, яка показує зразковий варіант здійснення, виконаний з іншою можливістю обробки відмови по відношенню до традиційного протоколу;

Фіг.10 - відповідна блок-схема для схеми послідовності з'єднання на Фіг.9;

Фіг.11 - схематичне креслення частини схеми вузла, який намагається одержати доступ до мережі, відповідно до зразкового варіанта здійснення;

Фіг.12 - схема послідовності з'єднання сеансу зв'язку на Фіг.1, здійсненого з додатковими типами повідомлень;

Фіг.13 - схематичне креслення частини схеми вузла, який намагається одержати доступ до мережі, відповідно до зразкового варіанта здійснення; і

Фіг.14 - схематичне креслення частини схеми вузла доступу до мережі відповідно до зразкового варіанта здійснення.

Докладний опис варіантів винаходу

Подальший опис наданий для того, щоб дозволити будь-якому фахівцеві в даній галузі техніки реалізувати і використати винахід. Деталі викладені в подальшому описі з метою пояснення. Повинно бути оцінено, що звичайний фахівець в даній галузі техніки зрозуміє, що винахід може бути застосований на практиці без використання цих конкретних деталей. У інших випадках добре відомі структури і процеси не розробляються в деталях для того, щоб не захащувати опис винаходу зайвими деталями. Таким чином, даний винахід не призначений, щоб бути обмеженим показаними варіантами здійснення, а повинен узгоджуватися з самою широкою галуззю застосування, узгодженою з принципами і ознаками, розкритими в даному документі.

Фіг.3 показує спрощене схематичне креслення вузлів, порушених в зразковому варіанті здійснення винаходу. Загальна система зв'язку позначається посиланням з номером 42. У цьому варіанті здійснення система 42 зв'язку включає в себе мережу 48, сполучену з базовою мережею 50, яка може бути інтранетом або Інтернетом. У мережі 48 розташовується NAS (сервер доступу до мережі), який служить як шлюз між мережею 48 і будь-яким вузлом, який намагається одержати доступ до мережі. У системі 42 передбачається, що існує такий вузол 44, який шукає доступ або до мережі 48, або до інших мереж (не показані) через базову мережу 50. Вузол 44 зв'язується з NAS 46 через канал 45 зв'язку.

Канал 44 зв'язку може мати різні форми. Назвемо тільки декілька, наприклад: канал 44 зв'язку може бути провідним каналом зв'язку, таким як традиційне телефонне провідне з'єднання, каналом зв'язку по коаксіальному кабелю або каналом зв'язку по оптичному кабелю. Крім того, канал 45 зв'язку може також бути безпровідним каналом зв'язку. У цьому випадку канал 45 зв'язку є радіоінтерфейсом.

У цьому варіанті здійснення передбачається, що канал 45 зв'язку є радіоінтерфейсом. Вузол 44 є мобільним пристроєм, який зв'язується з NAS 46 безпровідним чином. Мережа 48 підтримує безпровідні технології, такі як стандарти cdma2000, як викладено TIA/EIA (Асоціацією виготівників засобів зв'язку/асоціацією електронної промисловості). NAS 46 в цьому випадку є PDSN (вузлом обслуговування передачі пакетних даних), сполученим з RAN (мережа радіодоступу), яка здійснює зв'язок з вузлом 44 через RF (радіочастотні) сигнали по радіоканалу 45. PDSN і RAN відомі в даній галузі техніки і не показані на Фіг.3 з міркувань ясності і стислості.

Перед описом операційних деталей системи 42 зв'язку пояснимо спочатку різні типи протоколів з різними рівнями ієрархії і їх взаємними відношеннями.

У галузі мережних комунікацій, протоколи розташовуються в ієрархії відповідно до OSI-моделі (взаємодія відкритих систем), як викладено ISO (Міжнародною організацією по стандартизації) і ITU-T (Сектором по стандартизації Міжнародного союзу електрозв'язку). Метою є полегшити взаємодію обладнання від різних постачальників. Тобто, кожний рівень ієрархії протоколів має свої власні специфікації. По суті, поки специфікації окремого рівня ієрархії задовольняються, гарантується, що розробки продуктів на цьому рівні повинні бути сумісні з іншими продуктами на інших рівнях.

Передбачається, що система 42 на Фіг.3 підтримує IP (протокол Інтернету). Фіг.4 схематично показує стек протоколів в ієрархічному порядку, що звичайно іменується як "стек протоколів" і загалом позначається посиланням з номером 52. Стек 52 IP-протоколів структурований відповідно до IETF (інженерна проблемна група Інтернет) моделі, яка схожа, але не точно така ж, що і модель OSI. Відповідно до IETF-моделі стек 52 протоколів IP має п'ять рівнів, починаючи з рівня 1 до рівня 5. Таким чином, пакет даних, відправлений вузлом, таким як вузол 44 або 46, показаний на Фіг.3, повинен бути оброблений стеком 52 протоколів. Стек протоколів 52 створюється у вузлі в формі програмного або апаратного забезпечення або їх комбінації. Також, пакет даних, прийнятий тим же вузлом, повинен бути оброблений стеком 52 протоколів, але в зворотному порядку.

Візьмемо приклад для ілюстрації. Передбачається, що пакет даних обробляється для того, щоб бути відправленим з вузла, такого як вузол 44 або 46 (Фіг.3), пакет даних спочатку створюється відповідно до одного з протоколів на рівні додатків, тобто, рівні 5. Рівень 5 включає в себе HTTP (протокол передачі гіпертексту), SMTP (простий протокол пересилки електронної пошти), FTP (протокол передачі файлів) і RTP (транспортний протокол реального часу). Додатково передбачається, що пакет даних є продуктом VoIP (передача голосу по протоколу Інтернет) сеансу. Пакет даних, таким чином, повинен бути відформатований відповідно до RTP на рівні 5.

Чутливі до часу пакети даних, такі як пакети даних, одержані в результаті з протоколу RTP на

рівні 5, повинні бути оброблені в реальному часі. Конкретно, пошкоджені пакети звичайно не пересялаються, а замість цього просто пропускаються, так, щоб не утрудняти передачі інших вихідних пакетів даних. RTP пакети даних тому звичайно передаються через UDP (протокол користувацьких дейтаграм) на рівні 4, транспортному рівні. Відповідно, пакет даних з RTP на рівні 5 далі повинен бути сформульований відповідно до UDP на рівні 4.

З іншого боку, якщо пакет даних створюється з інших протоколів на рівні 5, таких як FTP, пакет даних звичайно відправляється через TCP (протокол керування передачею) на рівні 4. Під керуванням TCP важливе значення має точна доставка пакета даних. По суті, пошкоджені пакети завжди пересилаються, хоч, можливо, сповільнюють загальний процес передачі даних.

Пакети даних після проходження через цей транспортний рівень, рівень 4, доповнюються інформацією, такою як номери портів джерела і одержувача.

Пакет даних після проходження через транспортний рівень, рівень 4, потім відправляється мережному рівню, рівню 3, для обробки. У цьому окремому випадку, результуючий пакет даних з рівня 4 повинен бути знову відформатований відповідно до IP, наприклад, з доданими адресами джерела і одержувача пакета даних.

Повинно бути зазначено, що з міркувань стислості на рівні 3 показаний тільки IP на Фіг.4. Існують інші протоколи, які виконують додаткові до IP функції, також існуючі на рівні 3. Прикладом є ICMP (протокол керуючих повідомлень мережі Інтернет), який служить для відправлення повідомлень про помилки для недоставлених пакетів даних.

Після цього, пакет даних повинен бути розбитий на кадри, щоб уміститися в будь-який протокол, який застосовується на рівні мережного інтерфейсу, рівні 2. PPP (протокол точка-точка), описаний раніше, класифікується як протокол рівня 2. Сеанс протоколу зв'язку перед доступом до мережі відповідно до зразкового варіанта здійснення винаходу також стосується рівня мережного інтерфейсу.

Найнижчий рівень стека 52 протоколу на Фіг.4 - це фізичний рівень, рівень 1, який має справу з фізичним здійсненням передачі пакета даних. Наприклад, якщо канал 45 зв'язку (Фіг.3) є традиційним провідним каналом зв'язку, фізичний рівень, рівень 1, стосується апаратної схеми в обох вузлах 44 і 46 (Фіг.3), яка збуджує сигнали через проводи, які складають канал 45 зв'язку. Якщо канал 45 зв'язку представлений радіоінтерфейсом, фізичний рівень, рівень 1, належить до повітряного простору і апаратної схеми в обох вузлах 44 і 46 (Фіг.3), яка приймає і передає сигнали по повітряному простору.

Що стосується пакета даних, прийнятого вузлом, таким як вузол 44 і 46 (Фіг.3), пакет даних повинен бути оброблений таким же стеком 52 протоколів, але в зворотному порядку, тобто, від рівня 1 до рівня 5.

Тепер посилання повертається до Фіг.3. У цьому прикладі передбачається, що вузол 44 намагається одержати доступ до мережі через NAS 46. Перед яким-небудь обміном повідомленнями фізичний канал 45 зв'язку повинен бути готовий передавати сигнали. Виражаючись інакше, фізичний рівень, рівень 1, вузлів 44 і 45 повинен фізично бути присутнім і бути встановленим.

У цьому варіанті здійснення, як згадувалося раніше, канал 45 зв'язку є радіоінтерфейсом, а безпроводною технологією, що підтримується мережею 48, є cdma2000. Фізичний рівень має справу з безпроводною схемою у вузлі 44 і RAN в NAS 46. RAN може включати в себе щонайменше один BSC (контролер базової станції) і множину BS (базових станцій). RAN, BSC і BS не показані на Фіг.3.

Відповідно до цього варіанта здійснення, після того, як фізичний рівень, рівень 1, встановлений, тобто, обидва вузли 44 і 46 виявили взаємну фізичну присутність один одного, NAS 46 негайно відправляє перше повідомлення вузлу 44.

Фіг.5 є блок-схемою, яка показує послідовність передачі повідомлень між вузлом 44 і NAS 46. Загальний потік процесу позначається посиланням з номером 54.

Перше повідомлення називається повідомленням синхронізації і позначається посиланням з номером 56. Повідомлення 56 синхронізації включає в себе всі можливі варіанти аутентифікації для вузла 44, щоб вибрати з них. Варіанти можуть включати в себе повідомлення виклику по СНАР (протоколу аутентифікації по методу "виклик-привітання") і запит пароля і імені користувача, яких вимагає протокол PAP (протокол аутентифікації по паролю). У повідомлення 56 синхронізації також повинні бути включені відмінні від СНАР і PAP інші протоколи аутентифікації, які визначені і підтримуються в PPP.

Після прийому повідомлення 56 синхронізації вузол 44 відповідає повідомленням 58 запиту, як показано на Фіг.5.

У повідомлення 58 запиту вузол 44 включає необхідну інформацію аутентифікації у відповідь на запити, як викладено в повідомленні 56 синхронізації. Крім того, вузол 44 також включає в повідомлення 58 запиту всі варіанти параметрів, необхідні для встановлення каналу зв'язку вузла 44 для подальшого доступу до мережі через NAS 46. Не робиться відмінність, чи належать параметри з асоціативно зв'язаними варіантами до конфігурації каналу зв'язку, аутентифікації або контролю доступу до мережі. Тобто, замість класифікації параметрів згідно з функціями компонентів протоколу, таких як LCP (протокол керування каналом зв'язку), СНАР (протокол аутентифікації по методу "виклик-привітання") і IPCP (протокол керування протоколом Інтернету), як описано раніше по відношенню до PPP, в повідомленні 58 запиту цього варіанта здійснення всі параметри з варіантами включаються незалежно від функцій. Більш конкретно, параметри з варіантами в повідомленні 58 запиту можуть включати в себе відповідь на повідомлення виклику, або ім'я користувача і пароль, якщо застосовно, параметри конфігурації каналу 45 зв'язку, такі як розмір дейтаграми і схему стис-

нення поля HDLC-заголовка (високорівневий протокол керування каналом передачі даних), також як і всі параметри для доступу до мережі, такі як IP-адресу, конфігурацію DNS (доменна система імен) і протокол стиснення IP-заголовка, якщо застосовно, і так далі.

Повинно бути зазначено, що повідомлення 58 запиту переважно формується з навмисною надмірністю в термінах вибору, так, щоб дозволити NAS 46 вибрати варіанти, які підтримуються обома вузлами 30 і 46, таким чином дозволяючи обом вузлам 44 і 46 швидко закінчити загальний процес первинного встановлення каналу зв'язку. З різноманітності альтернатив NAS 46 може вибірково виділити параметри з асоціативно зв'язаними варіантами, які очевидно підтримуються, з метою збільшення імовірності успішного каналу зв'язку, таким чином скорочуючи час установлення. Виражаючись інакше, повідомлення 58 запиту по суті діє як повідомлення оголошення зі всіма доступними варіантами параметрів, що підтримуються вузлом 44, в якому вибір піднабору варіантів за допомогою NAS 46 повинен дозволити здійснення процесу з'єднання.

Відповідно, як показано на Фіг.5, NAS 46 відповідає повідомленням 60 відповіді після прийому повідомлення 58 запиту. У повідомленні 60 відповіді NAS 46 вибирає варіанти з різних альтернатив. Повідомлення 60 відповіді включає в себе вибрані варіанти параметрів з їх асоціативно зв'язаними значеннями конфігурації. Дуже часто повідомлення 60 відповіді є останнім повідомленням, необхідним перед початком мережного трафіку від вузла 44.

На відміну від способів інших протоколів, таких як PPP-протокол точка-точка, описаний раніше, відповідно до цього варіанта здійснення немає необхідності в яких-небудь повідомленнях підтвердження, щоб підтверджувати прийом або не підтверджувати прийом. По суті, у відповідь на будь-яке повідомлення, будь це повідомлення 56 синхронізації, повідомлення 58 запиту або повідомлення 60 відповіді, ні Аск-, ні Нак-повідомлення не потрібні. Відповідаючий вузол просто переходить до наступного етапу. Відсутність відповіді на будь-який окремих запитаний елемент має на увазі, що такий елемент недоступний або не підтримується.

Повертаючись назад до Фіг.5, після прийому повідомлення 60 відповіді, якщо варіанти, вибрані за допомогою NAS 46, задовольняють визначеному пороговому значенню, наприклад, всі вибрані варіанти дозволяють вузлу 44 встановити канал зв'язку для доступу до мережі, вузол 44 переходить прямо до передачі користувацьких даних 62 до NAS 46. Знову ж, повідомлення підтвердження прийому не відправляється вузлом 44.

По закінченні доступу до мережі або вузол 44, або NAS 46 може відправити повідомлення 64 запиту завершення іншому, який після цього відповідає зворотно повідомленням 66 підтвердження завершення і закінчує сеанс зв'язку.

У обставинах, що менш часто зустрічаються, може бути недостатньо варіантів конфігурації в повідомленні 58 запиту для NAS 46 для того, щоб встановити канал зв'язку для доступу до мережі,

якого добивається вузол 44. Тобто, варіанти, вибрані за допомогою NAS 46, в повідомленні 60 відповіді можуть бути недостатніми, щоб задовольнити пороговому значенню для вузла 44, щоб встановити канал зв'язку для доступу до мережі. NAS 46, однак, відправляє повідомлення 58 відповіді тільки з прийнятими варіантами, а неприйняті варіанти пропускаються. Знов, немає необхідності в Нак-повідомленні. Як згадано раніше, запропоновані варіанти, включені до складу повідомлення 58 запиту, але пропущені в повідомленні 60 відповіді, непрямим чином вказують відсутність підтримки пропущених варіантів. У цьому випадку NAS 46 не може встановити мережний трафік і чекає, поки вузол 44 не відправить нове повідомлення запиту.

Що стосується вузла 44, якщо він вибирає з'єднання, незважаючи на пропущені варіанти параметрів через відсутність підтримки в повідомленні 60 відповіді, наприклад, пропущені варіанти є некритичними, вузол 44 може почати передачу мережного трафіку. З іншого боку, якщо пропущені параметри абсолютно необхідні, щоб встановити з'єднання для доступу до мережі, наприклад, IP-адреса, що запитується вузлом 44, пропущена в повідомленні 60 відповіді, мережний трафік не може бути встановлений, і говориться, що з'єднання не вдалося.

Загальний процес 54 також показаний в блок-схемі на Фіг.6.

Процес встановлення з'єднання згідно з винаходом також конфігурується, щоб мати можливості обробки відмови для інших протоколів зв'язку. У цьому варіанті здійснення, якщо процес 54 з'єднання, показаний на Фіг.5 і 6, не підтримується або у вузлі 44, або в NAS 46 (Фіг.3), традиційний PPP задіюється як протокол переходу на аварійний режим, щоб продовжити процес з'єднання, що приводить до можливого доступу до мережі, якого добивається вузол 44.

По суті, можуть бути дві можливості, відповідно описані нижче в даному документі.

Перший сценарій виникає, коли вузол 44 підтримує процес 54 з'єднання, а NAS 46 - ні. Посилання тепер направлене на Фіг.7 в поєднанні з Фіг.3. Фіг.7 є блок-схемою, яка показує послдовність передачі повідомлень між вузлом 44 і NAS 46 в цьому сценарії. Загальний потік повідомлень позначений посиланням з номером 68. Оскільки передбачається, що вузол 44 підтримує процес 54 з'єднання, при встановленні фізичного рівня, рівня 1, між вузлами 44 і 46 вузол 44 чекає повідомлення 56 синхронізації. Однак, NAS 46 не має повідомлення 56 синхронізації, для відправлення, тому що також передбачається, що NAS 46 не підтримує процес 54 з'єднання. Замість цього NAS 46 відправляє повідомлення 70 запиту конфігурації LCP по протоколу PPP вузлу 44.

Після прийому повідомлення 70 запиту конфігурації LCP вузол 44 негайно дізнається, що NAS 46 не підтримує процес 54 з'єднання, і швидко здійснює дії, щоб зв'язатися з NAS 46 через традиційний PPP. Конкретно, у відповідь на повідомлення 70 запиту конфігурації LCP вузол 44 відправляє повідомлення 72 підтвердження прийому

конфігурації LCP, як показано на Фіг.7. Альтернативно, вузол може відправити повідомлення про відсутність підтвердження прийому конфігурації, якщо запропоновані варіанти LCP в повідомленні 70 запиту конфігурації є небажаними, подібним до традиційного PPP чином.

Повинно бути зазначено, що в цьому варіанті здійснення або вузол 44, або вузол 46 розпізнає, чи є прийняте повідомлення PPP-повідомленням або неPPP-повідомленням. Як буде описано пізніше, формат кадру даних, що використовується в цьому варіанті здійснення, є таким же, що і використовуваний для PPP, таким чином дозволяючи швидке розпізнавання і розрізнення повідомлень.

Перерва в процесі по суті схожа на процес 34, показаний на Фіг.2. Тобто, після успішного з'єднання трафік 74 даних встановлюється між вузлом 44 і NAS 46. По закінченні доступу до мережі або вузол 44, або NAS 46 може відправити повідомлення 76 запиту завершення іншому, який після цього відповідає зворотно повідомленням 78 підтвердження завершення і завершує сеанс 68 зв'язку.

Відповідна блок-схема процесу 68 показана на Фіг.8. Етапи традиційного PPP не показані на Фіг.8 заради стислості.

Другий сценарій відбувається, коли NAS 46 підтримує процес 54 з'єднання, а вузол 44 - ні. Посилання тепер направлено на Фіг.9 в сполученні з Фіг.3. Фіг.9 є блок-схемою, яка показує послідовність передачі повідомлень між вузлом 44 і NAS 46 в цьому сценарії. Повний потік повідомлень позначається посиланням з номером 70. Оскільки передбачається, що NAS 46 підтримує процес 54 з'єднання, після установа фізичного рівня, рівня 1, між вузлами 44 і 46 NAS 46 негайно відправляє повідомлення 56 синхронізації вузлу 44. Оскільки також передбачається, що вузол 44 не підтримує процес 54 з'єднання, після прийому повідомлення 56 синхронізації вузол 44 не розпізнає повідомлення 56 синхронізації. Як згадано раніше і буде додатково пояснено нижче, вузол 44 може відрізнити PPP-повідомлення від неPPP-повідомлення. Таким чином, з нерозпізнаним повідомленням 56 синхронізації, вузол 44 відкидає нерозпізнане повідомлення 56 синхронізації, використовуючи стандартні PPP-процедури. Замість цього, вузол 44 відправляє повідомлення 72 запиту конфігурації LCP по фізичному каналу зв'язку, встановленому між вузлом 44 і NAS 46.

Якщо NAS 46 приймає повідомлення 72 запиту конфігурації LCP або PPP-відхилення повідомлення 56 синхронізації, NAS 46 негайно відмінює всі функції, що належать до процесу 54 з'єднання (Фіг.5 і 6) і йде через традиційний PPP-процес 34, як показано на Фіг.2 і описано раніше.

Після успішного з'єднання може бути здійснений обмін трафіком 74 даних між вузлом 44 і NAS 46. По закінченні доступу до мережі або вузол 44, або NAS 46 може відправити повідомлення 76 запиту завершення іншому, який після цього відповідає зворотно повідомленням 78 підтвердження завершення і завершує сеанс 70 зв'язку.

Фіг.10 показує відповідну блок-схему процесу 70. Етапи традиційного PPP не показані на Фіг.10 з міркувань стислості і ясності.

Фіг.11 показує формат кадру даних, що використовується в потоці процесу 54 (Фіг.5). Шаблон кадру для пакета даних процесу 54 позначається посиланням з номером 80. По суті, шаблон 80 схожий на відповідний шаблон пакета даних, використовуваний PPP, як викладено в RFC 1662. Зокрема, кадр 80 даних включає в себе поле 82 прапора, поле 84 адреси, керуюче поле 86, поле 88 номера протоколу, поле 90 даних і поле 92 FCS (контрольна послідовність кадру).

Поле 82 прапора має одинбайтову довжину і вказує початок кадру пакета даних. Поле 82 прапора завжди приймає шістнадцяткове значення 7E і є таким же значенням, що використовується для процесу 54 з'єднання і PPP, як потрібно по RFC 1662.

Поле 84 адреси також має одинбайтову довжину і завжди встановлюється в шістнадцяткове значення, рівне FF, як також викладено в RFC 1662.

Керуюче поле 86 має одинбайтову довжину і фіксоване з шістнадцятковим значенням, рівним 03, як також описано в RFC 1662.

У полі 88 номера протоколу, значення в цьому полі вказує, що пакет 80 даних присутній. Поле 88 номера протоколу є двобайтовим по довжині. Наприклад, як визначено в RFC 1661 і 1662, кожне з LCP-повідомлень, таких як повідомлення 70 запиту конфігурації, має шістнадцяткове значення, рівне C021. У цьому варіанті здійснення кожне з повідомлень, таких як повідомлення 56 синхронізації, повідомлення 58 запиту або повідомлення 60 відповіді, що використовуються в процесі 54 з'єднання (Фіг.5), має унікальне значення протоколу, відмінне від будь-якого із значень протоколу, що використовуються в PPP. По суті, легко може бути розпізнано, чи є пакет 80 даних PPP-пакетом або неPPP-пакетом.

Поле 90 даних має довжину, яка змінюється від нуля до більше байтів, корисного навантаження, яка містить або дані, або керуючу інформацію. Наприклад, якщо значення в полі 88 номера протоколу зі значенням, яке вказує, що пакет 80 даних - це повідомлення 58 запиту, поле даних включає в себе всю інформацію, що належить до варіантів параметрів, як згадано вище. Як інший приклад, якщо значення в полі 88 номера протоколу має значення, яке вказує, що пакет 80 даних є користувацькими даними 62 (Фіг.5), IP-пакет даних, генерований на рівні 3, повністю інкапсулюється в полі 90 даних.

FCS-поле 92 змінюється від двох до чотирьох байтів по довжині і містить коди, такі як CRC (циклічний надмірний код), для кадру 80, щоб надати основний захист проти помилок під час передачі.

У доповнення до повідомлення 56 синхронізації, повідомлення 58 запиту, повідомлення 60 відповіді, запиту 64 завершення і повідомлення підтвердження завершення, як згадано вище (наприклад, див. Фіг.5), інші типи повідомлень можуть також бути здійснені в процесі 54 встанов-

лення каналу зв'язку. Фіг.12 показує декілька прикладів.

Посилання тепер направлене на Фіг.3 в сполучанні з Фіг.12. Наприклад, після продовженого періоду недіючого зв'язку, позначеного посиланням з номером 94 на Фіг.12, або вузол 44, або NAS 46 може відправити повідомлення 96 луна-запиту іншій стороні, щоб довідатися про стан сторони або каналу 45 зв'язку. Наприклад, якщо не існує фізичного каналу зв'язку, встановленого для каналу 45 зв'язку через збій живлення, відправляюча сторона не прийме відповідь на повідомлення 45 луна-запиту. Відповідно, відправляюча сторона може захотіти завершити сеанс 54 зв'язку. З іншого боку, якщо канал 45 зв'язку ще фізично діючий, приймаюча сторона може відповісти на повідомлення 96 луна-запиту, відправляючи повідомлення 98 луна-відповіді. Відправляюча сторона може після цього відмовитися від рішення завершити сеанс 54 зв'язку. Тривалість періоду 94 часу може бути попередньо визначена.

Між обмінами користувацькими даними 62 NAS 46 може відправити повідомлення 98 аутентифікації вузлу 44, яке запитує інформацію для подальшої аутентифікації. Наприклад, під час звичайного трафіку даних вузол 44 може потребувати доступу до важливої інформації, до якої можуть одержати доступ тільки деякі користувачі. По суті, NAS 46 може відправити повідомлення 99 аутентифікації вузлу 44 для подальшої аутентифікації. На доповнення до протоколів аутентифікації, таких як PAP і CHAP, як згадано вище, також можуть використовуватися інші більш складні схеми протоколів, відомі в даній галузі техніки. Прикладом може бути EAP (розширений протокол аутентифікації), що застосовує зовнішній сервер, такий як AAA (аутентифікація, авторизація і облік) сервер, розташований або всередині, або за межами мережі 48, для аутентифікації.

Фіг.13 схематично показує частину апаратної реалізації пристрою, такого як вузол 44, показаний на Фіг.3, позначеного посиланням з номером 100, відповідно до зразкового варіанта здійснення винаходу. Пристрій 100 може бути побудований і інтегрований в різні форми, такі як, наприклад, портативний комп'ютер, PDA (персональний цифровий секретар) або стільниковий телефон.

Пристрій 100 містить центральну шину 102 даних, яка зв'язує декілька схем разом. Схеми включають в себе CPU (центральний процесор) або контролер 104, схему 106 прийому, схему 108 передачі і модуль 110 пам'яті.

Якщо пристрій 100 є безпроводним пристроєм, схеми 106 і 108 прийому і передачі можуть бути сполучені з RF-схемою (радіочастотною), непоказаною на кресленні. Схема 106 прийому обробляє і буферизує прийняті сигнали перед відправленням на шину 102 даних. З іншого боку, схема 108 передачі обробляє і буферизує дані від шини 102 даних перед відправленням з пристрою 100. CPU/контролер 104 виконує функцію керування даними шини 102 даних і додатково функцію загальної обробки даних, що включає в себе виконання керуючого вмісту модуля 110 пам'яті.

Замість окремого розміщення, як показано на Фіг.13, як альтернатива, схема 108 передачі і схема 106 прийому можуть бути частинами CPU/контролера 104.

Модуль 110 пам'яті включає в себе набір інструкцій, що звичайно позначаються посиланням з номером 112. У цьому варіанті здійснення інструкції включають в себе, серед іншого, частини, такі як функція 114 стека протоколів, клієнт 116 встановлення каналу зв'язку, PPP-функція 118. Функція 114 стека протоколів запускає стек протоколів, подібний стеку 52, як показано і описано на Фіг.4 раніше. Клієнт 116 встановлення каналу зв'язку включає в себе набори інструкцій відповідно до процесу, такого як процеси, описані на Фіг.5-10, наведених вище. PPP-функція 118 включає в себе набори інструкцій для того, щоб дати можливість пристрою 102 виконати PPP-процес. PPP-функція 118 може використовуватися незалежно або при переході на аварійний режим з клієнта 116 встановлення каналу зв'язку, як також описано раніше.

У цьому варіанті здійснення модулем 110 пам'яті є схема RAM (оперативний запам'ятовуючий пристрій). Зразкові частини 114, 116 і 118 інструкцій є програмними процедурами або модулями. Модуль 110 пам'яті може бути сполучений з іншою схемою пам'яті (не показана), яка може бути або енергозалежного, або енергонезалежного типу. Як альтернатива, модуль 110 пам'яті може бути виконаний з інших типів схем, таких як EEPROM (електрично стираний програмований постійний запам'ятовуючий пристрій), EPROM (електрично програмований постійний запам'ятовуючий пристрій), ROM (постійний запам'ятовуючий пристрій), ASIC (спеціалізована інтегральна мікросхема), магнітний диск, оптичний диск і інші, добре відомі в даній галузі техніки.

Фіг.14 схематично показує частину апаратної реалізації іншого пристрою, такого як NAS 46, показаного на Фіг.3 відповідно до винаходу і позначеного посиланням з номером 120. Пристрій 120 містить центральну шину 122 даних яка зв'язує декілька схем разом. Схеми включають в себе CPU (центральний процесор) або контролер 124, схему 126 приймача, схему 128 передавача і модуль 130 пам'яті.

Схеми 126 і 128 прийому і передачі можуть бути сполучені з мережною шиною даних (не показана), з якою сполучений пристрій 120. Схема 126 прийому обробляє і буферизує прийняті сигнали від мережної шини даних (не показана) перед маршрутизацією до внутрішньої шини 122 даних. Схема 128 передачі обробляє і буферизує дані від шини 122 даних перед відправленням з пристрою 120. CPU/контролер 124 виконує роботу з керування даними шини 122 даних і функцію загальної обробки даних, що включає в себе виконання керуючого вмісту модуля 130 пам'яті.

Знову ж, замість окремого розміщення, як показано на Фіг.14, схема 128 передачі і схема 126 прийому можуть бути частинами CPU/контролера 124.

Модуль 130 пам'яті включає в себе набір інструкцій, загалом, позначених посиланням з номером 134. У цьому варіанті здійснення інструкції

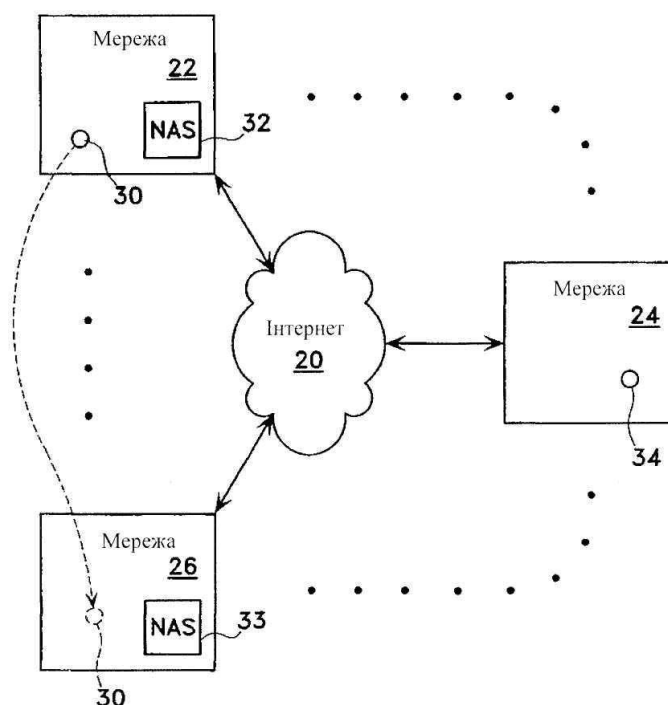
включають в себе частини, серед іншого, функції 136 стека протоколів, сервера 138 встановлення з'єднання, PPP-функцію 130. Функція 136 стека протоколів запускає стек протоколів, подібний стеку 52, як показано і описано на Фіг.4 раніше. Сервер 138 встановлення з'єднання включає в себе набори інструкцій відповідно до процесу, такого як процеси, описані на Фіг.5-10, і як описано вище. PPP-функція 140 включає в себе набори інструкцій, що дозволяють пристрою 120 виконати PPP-процес. PPP-функція 140 може виконуватися незалежно або як перехід на аварійний режим з сервера 138 встановлення з'єднання, як також описано раніше.

Модуль 130 пам'яті може бути зроблений з типів схем пам'яті, як згадано вище і додатково не повторюється.

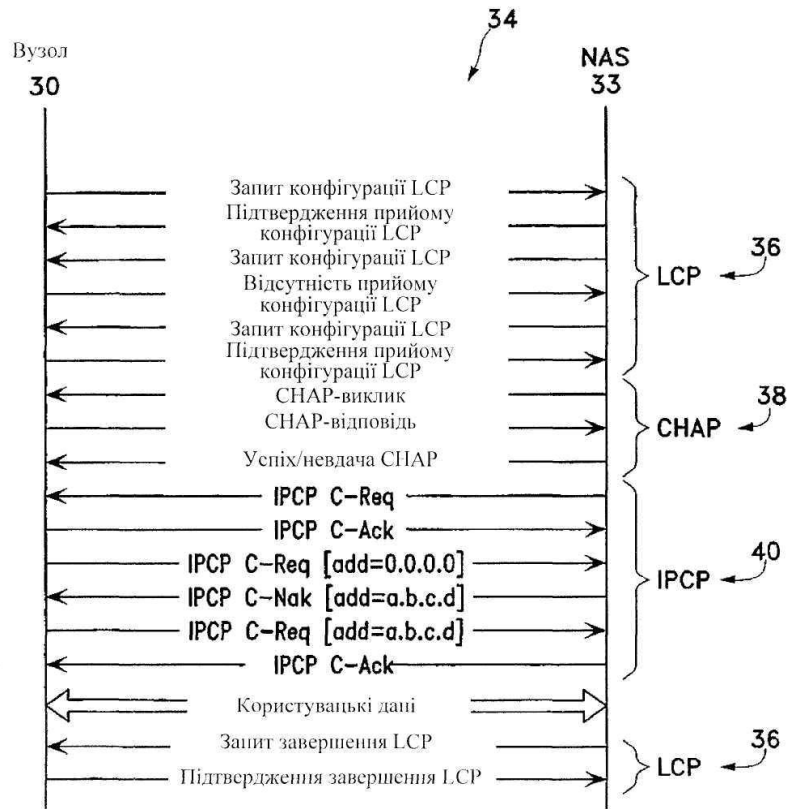
Також повинно бути зазначено, що процеси 54, 68 і 70, як описано і показано на Фіг.5-10, можуть також бути збережені і передаватися на будь-якому машиночитаному носії, відомому в даній галузі техніки. У цій специфікації і прикладений формулі винаходу термін "машиночитаний носій" посилається на будь-який носій, який бере участь в наданні інструкцій CPU/контролеру 104 і 124, відповідно до показаних і описаних на Фіг.12 і 13, для виконання. Такий машиночитаний носій, якщо він має тип сховища, може приймати форму енергозалежного або енергонезалежного носія даних, подібного типам схем для модулів 110 і 130 пам'я-

ті, як також описано раніше. Такий машиночитаний носій, якщо він передавального типу, може включати в себе коаксіальний кабель, металевий провід, оптичний кабель або радіоінтерфейс, що передає звукові або електромагнітні хвилі, здатні передавати сигнали, наприклад, що читаються машинами або комп'ютерами.

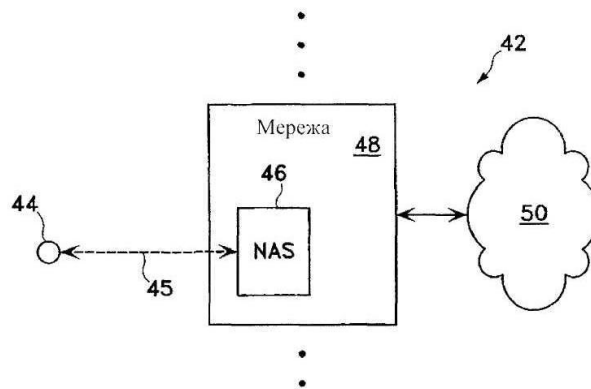
На закінчення, описаний у варіанті здійснення протокол рівня 3 описується як IP. IP може бути різних версій, таких як IPv4 (протокол Інтернету версії 4) і IPv6 (протокол Інтернету версії 6). Крім того, повинно бути зазначено, що протоколи рівня 3 є однаково застосовними. Наприклад, протоколом рівня 3 може бути IPX (протокол міжмережного обміну пакетами), Apple-Talk і різні інші мережні протоколи різних версій. Крім того, в зразковому варіанті здійснення вузол 44 зображується як мобільний пристрій, що зв'язується з NAS 46 безпроводним чином. Повинно бути оцінено, що вузол 60 може бути стаціонарним. Крім того, не потрібно, щоб канал 45 зв'язку був радіоканалом. Замість цього, канал 45 зв'язку може бути провідним каналом зв'язку. Крім того, будь-які логічні блоки, схеми і етапи алгоритму, описані разом з варіантом здійснення, можуть бути виконані в апаратних, програмних, апаратно-програмних засобах або їх комбінаціях. Фахівцям в даній галузі техніки буде зрозуміло, що ці і інші зміни в формі і деталях можуть бути зроблені тут без відступу від мети і духу винаходу.



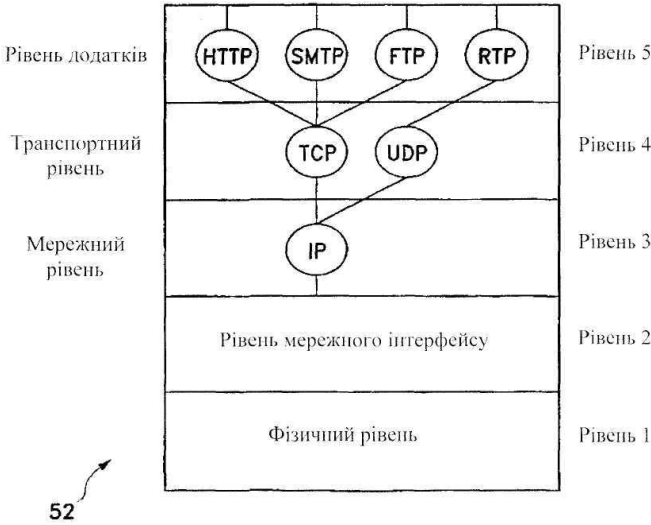
Фіг.1



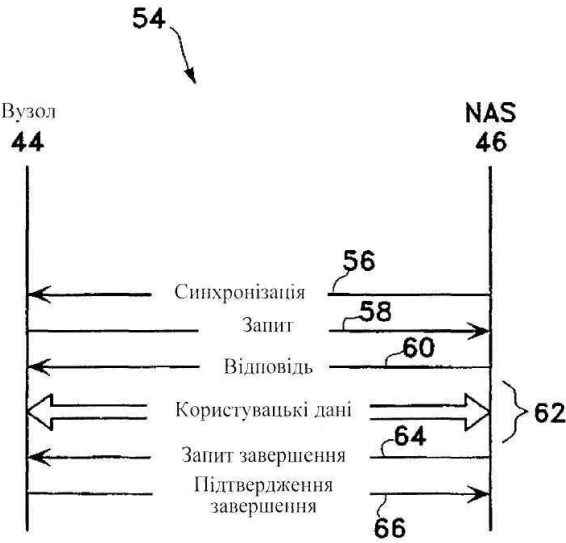
Фиг.2



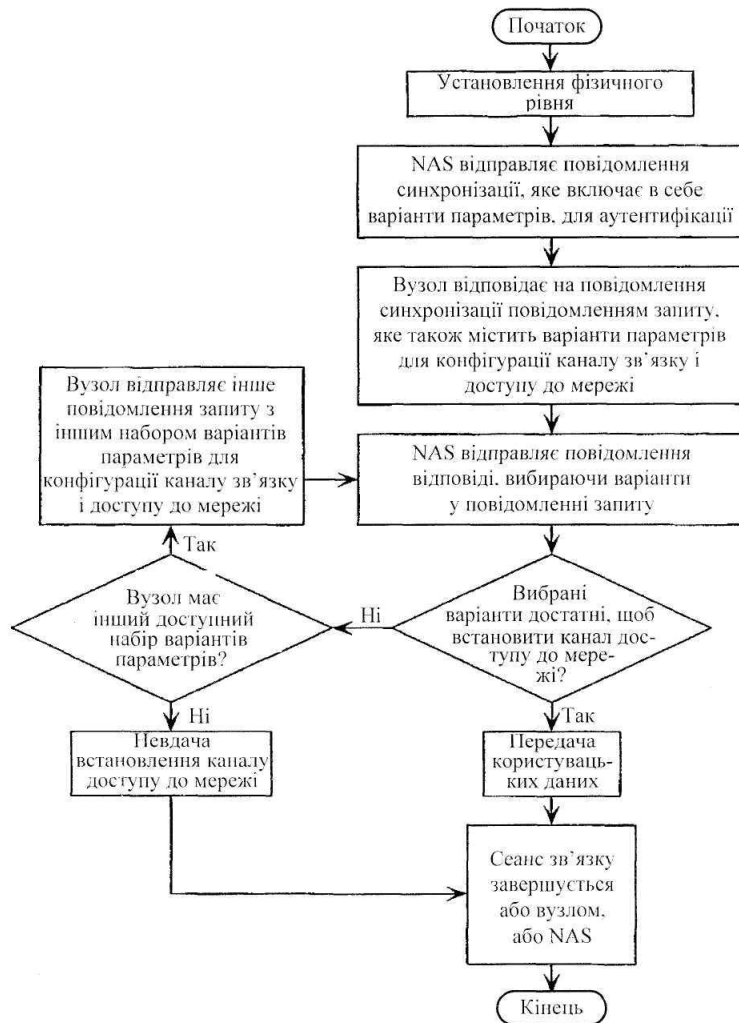
Фиг.3



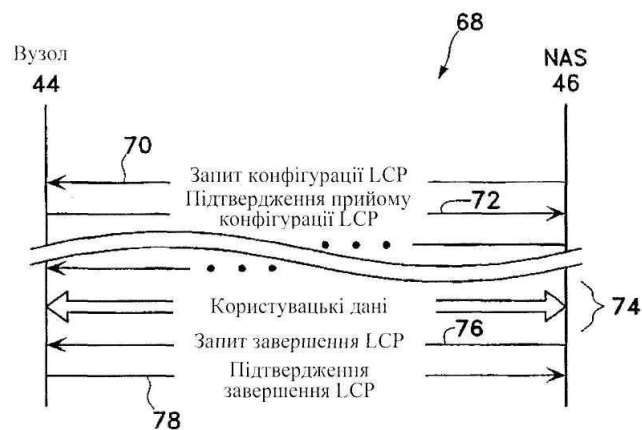
Фіг.4



Фіг.5



Фіг.6



Фіг.7

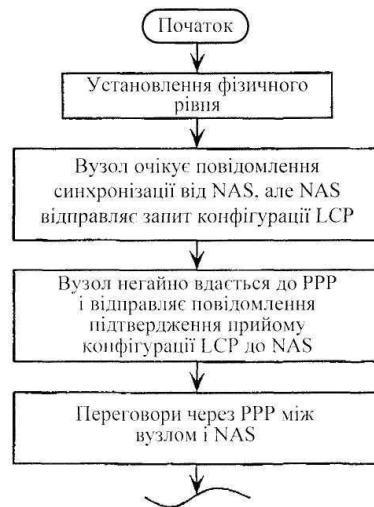


Fig. 8

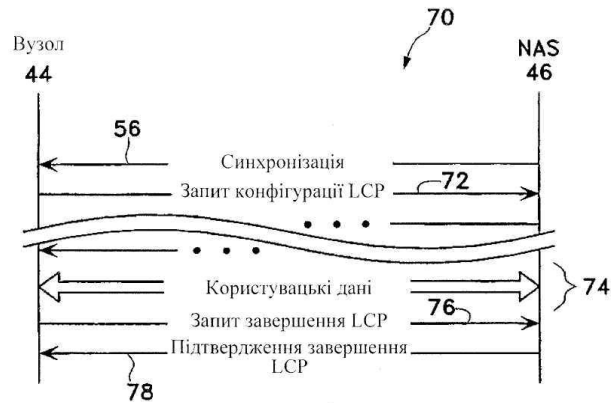


Fig. 9

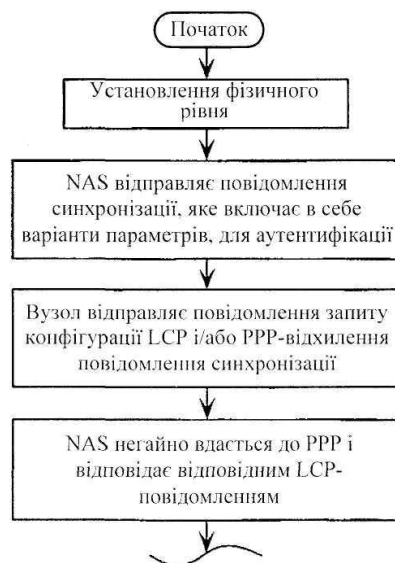
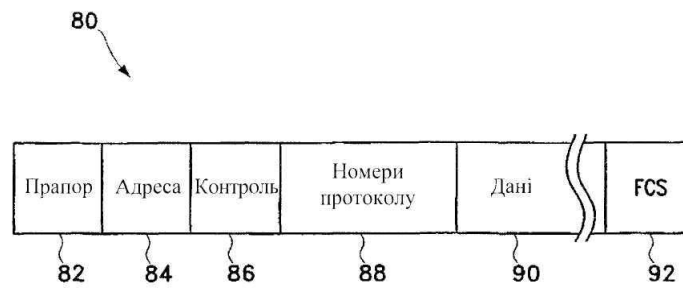
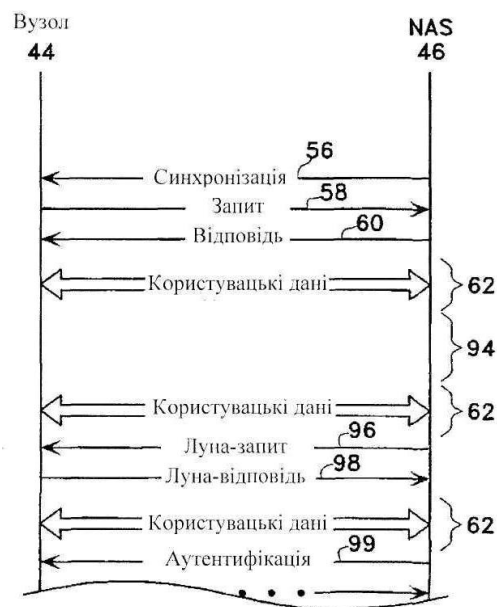


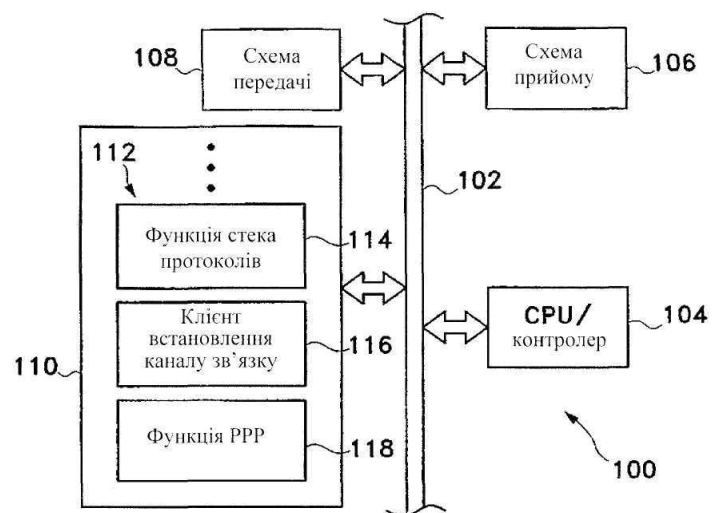
Fig. 10



Фиг. 11



Фиг. 12



Фиг. 13

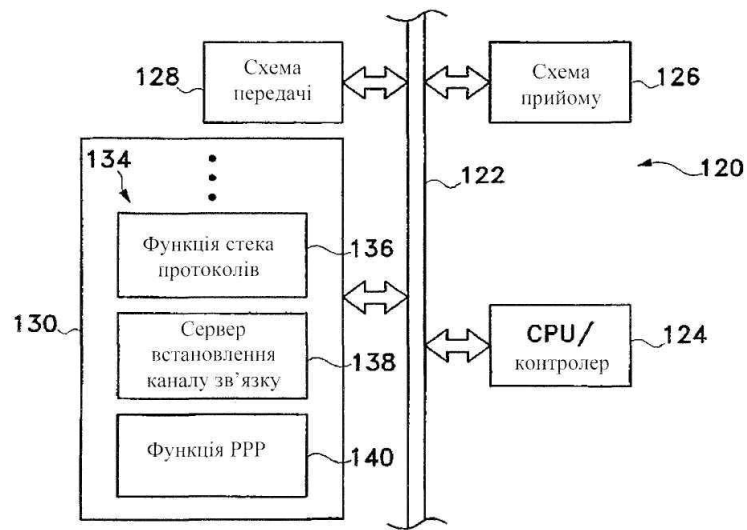


Fig. 14