Лабораторна робота № 5

Сервіс доступу до файлів SMB/CIFS

1. Короткі теоретичні відомості.

1.1. Сервіси SMB/CIFS.

Управління сесіями. Створення, підтримка і розрив логічного каналу між робочою станцією і мережними ресурсами файлового сервера.

Файловий доступ. Робоча станція може звернутися до файл-серверу з запитами на виконання типових файлових операцій (відкриття файлу, читання даних і т.п.).

Сервіс друку. Робоча станція може ставити файли в чергу для друку на сервері і отримувати інформацію про чергу друку.

Сервіс повідомлень. SMB підтримує просту передачу адресних і широкомовних повідомлень по локальній мережі.

1.2. Місце в стеку протоколів TCP/IP.

Рівні ISO OSI	**Протоколи SMB**
Прикладний	SMB
Представлення	
Сеансовий	NetBIOS
Транспортний	UDP/TCP
Мережний	IP
Канальний	IEEE 802.3
Фізичний	

1.3. Версії протоколу SMB.

У 1983 році компанія IBM (Баррі Фейгенбаум) розробила протокол SMB.

IBM розробила API для мережної взаємодії між вузлами в локальній мережі - NetBIOS API.

У поєднанні з транспортним протоколом, який повинен називатися NetBEUI - NetBIOS.

У 1988 році Microsoft і Intel змінили протокол під назвою «Базовий протокол», який використовував NetBIOS API для доставки пакетів протоколу CIFS.

У 1996 році SMB був перейменований в CIFS з новими функціями.

SMB/CIFS - NetBIOS поверх TCP, використовувався Microsoft до Windows 2000.

У Windows Vista з'явилася нова версія протоколу - SMB 2.0. Протокол був значно спрощений (у SMB було понад 100 команд, а в SMB 2 - всього 19).

У Windows 8 з'явилася нова версія протоколу - SMB 3.0.

SMB 3.0.2 був представлений з Windows 8.1 та Windows Server 2012 R2; у цих та пізніших випусках попередню версію SMB 1 можна відключити для підвищення безпеки.

SMB 3.1.1 був представлений з Windows 10 та Windows Server 2016. Ця версія підтримує шифрування AES-128 GCM на додаток до шифрування CCM AES-128, доданого в SMB3, та реалізує перевірку цілісності перед автентифікацією за допомогою хешу SHA-512. SMB 3.1.1 також робить безпечні переговори обов'язковими при підключенні до клієнтів за допомогою SMB 2.x і вище.

1.4. Протокол NetBIOS.

NetBIOS працює поверх безлічі транспортних протоколів, але на сьогодні основні реалізації працюють поверх стеку TCP/IP.

Документи RFC1001 і RFC1002 описують роботу NetBIOS поверх TCP/UDP (NBT). RFC1001 описує концепцію і методи. RFC1002 містить детальну специфікацію. У цих документах описані 3 основних служби:

- імен;
- сесій;
- датаграм.

1.5. Служба імен.

Складається з реєстрації і запитів імен. NetBIOS-ім'я - зрозумілий для людини ідентифікатор комп'ютера. Також як і в системі імен DNS NetBIOS-ім'я повинне бути зареєстроване в базі і має перетворюватися в IP-адресу для транспортування пакетів. DNS-імена і IP-адреси статично закріплені за комп'ютером, тоді як NetBIOS-імена реєструються динамічно під час завантаження операційної системи. Працює з використанням широкомовлення або сервера імен NetBIOS (NBNS або WINS). Комп'ютери для реєстрації та перегляду імен можуть використовувати:

- b-node;
- p-node;
- m-node;
- h-node.

1.6. Типи комп’ютерів NetBIOS.

Роль	Значення
b-node	Використовує лише широкомовну реєстрацію та перегляд імен.
p-node	Використовує тільки реєстрацію точка-точка і перегляд імен.
m-node	Використовує широкомовну реєстрацію. Якщо вона успішна, він повідомляє про це сервер NBNS. Використовує широкомовний метод для перегляду імен; використовує NBNS сервер, якщо метод широкомовних запитів невдалий.
h-node (гібрид)	Використовує NBNS сервер для реєстрації та перегляду імен; використовує широкомовні запити, якщо сервер NBNS не доступний.

1.7. Правила використання NetBIOS-імен.

NetBIOS-ім'я може використовуватися одним комп'ютером (unique name) або декількома комп'ютерами. В останньому випадку ім'я належить до групи комп'ютерів (group name).

NetBIOS імена утворюють плоский простір імен без ієрархії, як в системі DNS. Це означає, що кожен комп'ютер повинен використовувати унікальну послідовність символів, що утворюють

його ім'я. На відміну від системи DNS, де 2 і більше імені можуть збігатися, якщо вони знаходяться в різних доменах.

NetBIOS-імена повинні складатися тільки з наступних символів:

```
a-z
A-Z
0-9
! @ # $ % ^ & ( ) - ' { } . ~
```

NetBIOS-ім'я може складатися максимум з 15 символів для ідентифікації ресурсу, 16-й символ показує тип ресурсу.

1.8. Типи ресурсів NetBIOS.

Ім’я ресурсу	**Значення в полі тип**
Standard Workstation Service	00
Messenger Service (WinPopup)	03
RAS Server Service	06
Domain Master Browser Service (associated with primary domain controller)	1B
Master Browser name	1D
Fileserver (including printer server)	20
Network Monitor Agent	BE

1.9. Служба сесій.

Сесія забезпечує відмовостійкий зі збереженням послідовності відправки обмін повідомленнями між парою NetBIOS застосунків. Використовується 139 порт протоколу TCP для емуляції функціонування сесії. SMB використає цю службу для відправки команд, наприклад, для роботи з файлами або принтерами.

1.10. Служба датаграм.

Для роботи SMB досить тільки служб сесій і імен, але для пошуку комп'ютерів в мережі (функція перегляду) необхідна служба датаграм. Функція перегляду мережі не є частиною протоколу SMB. Служба датаграм забезпечує ненадійний, без збереження порядку надходження і без встановлення з'єднання сервіс обміну повідомленнями. Для роботи служби датаграм використовується порт 138 протоколу UDP. SMB можуть працювати поверх TCP без NetBIOS. DNS і доменні імена можуть використовуватися для забезпечення сервісу імен, служба сесій може працювати прямо поверх TCP, служба датаграм - прямо поверх UDP.

2. Завдання на роботу.

2.1. Встановити та налаштувати файловий сервер, який реалізує протоколи SMB/CIFS та відповідає наступним вимогам:

- створені користувачі з іменами, доступом та правами, які відповідають варіанту завдання;
- гостьовий доступ (без проходження автентифікації) до каталогів з правами, які відповідають варіанту завдання;

- доступ до домашнього каталогу для автентифікованого користувача з правами, які відповідають варіанту завдання;

- доступ до прихованого каталогу (невидимий при перегляді списку спільних ресурсів штатними засобами) з правами, які відповідають варіанту завдання.

2.3. Виконати аналіз протокольного обміну між клієнтом та сервером під час автентифікації та пересилки файлів.

2.4. Рекомендується використовувати наступне програмне забезпечення:

- SMB-сервер: samba;
- SMB-клієнт: smbclient.

2.5. Для перевірки роботи файлового серверу та аналізу протокольного обміну рекомендується використовувати утиліти: nbtscan, nmblookup, smbtree, nmap.

Варіант	**Ім'я користувача**	**Права доступу до каталогів**			
		Прихований	**Домашній**	**public**	**incoming**
1	alpha	R	RW	R	RW
	beta	RW	RW	R	-
	gamma	-	R	R	RW
	гість	R	-	R	RW
2	mercury	-	RW	-	-
	venus	RW	R	R	RW
	saturn	R	RW	R	RW
	гість	RW	-	-	RW
3	tiger	RW	RW	R	RW
	lion	-	RW	-	RW
	lynx	R	-	R	-
	гість	-	-	R	-
4	rose	R	R	R	RW
	gerbera	RW	RW	-	-
	aster	-	R	-	RW
	гість	R	-	R	-
5	ubuntu	R	RW	R	RW
	debian	RW	RW	R	-
	centos	-	R	R	RW
	гість	R	-	-	RW

Варіант	Ім'я користувача	Права доступу до каталогів			
		Прихований	Домашній	public	incoming
6	red	RW	RW	R	RW
	green	-	RW	-	RW
	blue	R	-	R	-
	гість	RW	-	R	RW
7	gold	R	RW	R	RW
	silver	RW	RW	R	-
	iron	-	R	R	RW
	гість	RW	-	-	-
8	london	R	R	R	RW
	tokyo	RW	RW	-	-
	paris	-	R	-	RW
	гість	-	-	-	RW
9	dollar	R	RW	R	RW
	dinar	RW	RW	R	-
	lira	-	R	R	RW
	гість	RW	-	R	-
10	nile	-	RW	-	-
	amazon	RW	R	R	RW
	congo	R	RW	R	RW
	гість	RW	-	R	-
11	apple	RW	RW	R	RW
	orange	-	RW	-	RW
	grape	R	-	R	-
	гість	R	-	-	-
12	one	R	R	R	RW
	two	RW	RW	-	-
	three	-	R	-	RW
	гість	-	-	R	RW
13	march	R	RW	R	RW
	april	RW	RW	R	-
	may	-	R	R	RW
	гість	RW	-	-	RW

Варіант	Ім'я користувача	Права доступу до каталогів			
		Прихований	Домашній	public	incoming
14	maria	-	RW	-	-
	tomas	RW	R	R	RW
	tereza	R	RW	R	RW
	гість	R	-	R	-
15	france	RW	RW	R	RW
	spain	-	RW	-	RW
	italy	R	-	R	-
	гість	RW	-	R	RW

3. Контрольні питання.

3.1. Стек NetBIOS/SMB.

3.2. NetBIOS імена та типи ресурсів.

3.3. Сервіс імен NetBIOS. Реєстрація та перегляд імен NetBIOS. Типи комп'ютерів NetBIOS.

3.4. Вибори головного переглядача.

3.5. Служби датаграм та сесій.

4. Література.

RFC1001 https://tools.ietf.org/html/rfc1001
RFC1002 https://tools.ietf.org/html/rfc1002
[MS-CIFS] http://msdn.microsoft.com/en-us/library/ee442092.aspx
[MS-SMB] http://msdn.microsoft.com/en-us/library/cc246231.aspx
[MS-SMB2] http://msdn.microsoft.com/en-us/library/cc246482.aspx