ДОДАТОК А

Графічний матеріал атестаційної роботи

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДОЕЛЕКТРОНІКИ

Кафедра Електронних обчислювальних машин

Метод дистанційного керування науковими інструментами з віртуалізацією інтерфейсів

Виконав:
студент гр. СПзм-18-2
Онацький Р.С.

Керівник:
к.т.н., ст. викладач
Ткачов В.М.

МЕТА ВИКОНАННЯ АТЕСТАЦІЙНОЇ РОБОТИ І ПОСТАНОВКА ЗАДАЧІ

Метою атестаційної роботи є аналіз існуючих та розробка нового методу дистанційного керування науковими інструментами з віртуалізацією інтерфейсів з відмовостійкою мережною складовою на платформі віртуальних (оверлейних) комп'ютерних мереж.

Задача атестаційної роботи полягає у розробці методу дистанційного керування науковими інструментами, які підключені до обчислювальних станцій, шляхом віртуалізації інтерфейсів та організації віртуальних каналів зв'язку для доступу до них.

Реалізовану технічну систему за таким методом функціонування необхідно дослідити на предмет встановлення залежності його відмовостійкості від стану каналів зв'язку.

СУЧАСНИЙ СТАН ЗАДАЧІ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ДОСТУПУ ДО ВІДДАЛЕНИХ ПРИСТРОЇВ. ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ

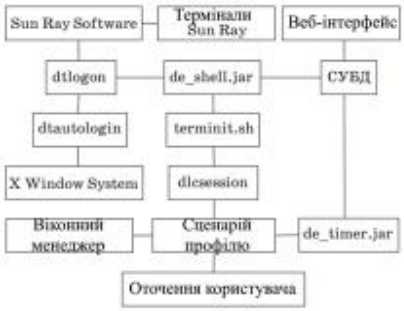


Схема взаємодії компонентів системи управління терміналами

Логіка роботи систем, що реалізують дистанційний доступ до віддалених пристроїв, будується на таких основних правилах:

- для кожного користувача за графіком роботи встановлюється ліміт часу роботи з дистанційною системою, в рамках якого він може подати заявку через інтерфейс системи на зручні день і час;
- одночасно з одним віддаленим пристроєм може працювати один користувач;
- канал зв'язку має резервуватися та дублюватися шляхом створення віртуальної надбудови (оверлейної мережі);
- доступ до інтерфейсів віддалених пристроїв має здійснюватися авторизованими користувачами;
- доступ до обладнання через термінальні інтерфейсні станції має бути авторизованим.

3

СУЧАСНИЙ СТАН ЗАДАЧІ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ДОСТУПУ ДО ВІДДАЛЕНИХ ПРИСТРОЇВ. АНАЛІЗ ВІДОМИХ МЕТОДІВ ОРГАНІЗАЦІЇ ДИСТАНЦІЙНОГО ДОСТУПУ

Сервіси для організації віддаленого доступу до операційної системи

- TELNET
- SSH
- Virtual Network Computing
- TeamViewer
- LiteManager
- UltraVNC

Сервіси організації термінального доступу

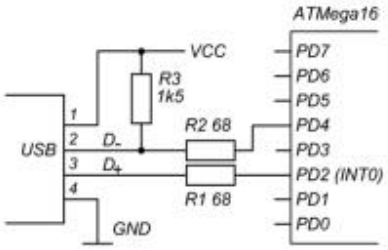
- Citrix
- Microsoft
- X Window System

VDI і VDS сервіси

- інфраструктура віртуальних робочих столів
- служби віддалених робочих столів або термінальні сервіси
- дистанційна фізична робоча станція
- віртуалізація додатків

4

ВІРТУАЛІЗАЦІЯ USB-ІНТЕРФЕЙСУ В МЕРЕЖІ (ЕМУЛЯЦІЯ)



Варіант підключення мікроконтролера до шини USB

Візуалізація підключення в диспетчері пристроїв операційної системи

Трансляція пристрою для комп'ютерної мережі

5

ВІРТУАЛІЗАЦІЯ МЕРЕЖНОЇ СКЛАДОВОЇ

Крок 1. Необхідно здійснити настройку видачі/отримання реальної IP-адреси шляхом організації VPN-сервера.

Крок 2. У комп'ютерній мережі наукового інструменту на комп'ютері, який має доступ до мережі Інтернет через низькошвидкісний канал зв'язку (3G-модем), встановлюється клієнтська частина VPN-тунелю.

Крок 3. Тепер на (n+1)-комп'ютері налаштовуємо свій власний VPN-сервер.

Крок 4. З боку клієнта необхідно налаштувати клієнтську частину VPN-тунелю.

$$\Psi = D\ell(2S + (2i-1)\sum_{i=1}^{log_2 S} 2^{i-1}$$

Загальна пропускна здатність тунелю окремо взятого підключення до комп'ютерної мережі наукового інструменту через VPN-тунель

$$\Psi' = D(1 + log_2 S + \sum_{i=1}^{log_2 S} 2^i + \ell S)$$

Загальна пропускна здатність VPN-сервера при віртуалізації USB-портів (1 порт для 1 підключення)

$$\theta = D(\ell S - YW)$$

Значення пропускної здатності, яка не ефективно використовується під час передачі від кожного з абонентів VPN мережі команд управління на USB-порт

6

ПРИКЛАД РЕАЛІЗАЦІЇ КОМУНІКАЦІЙ

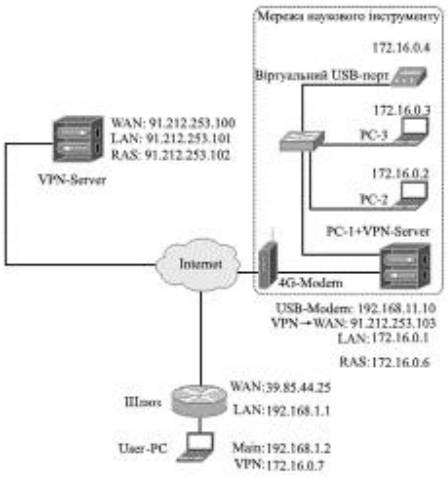


Схема мережної взаємодії при наявності пулу реальних IP-адрес

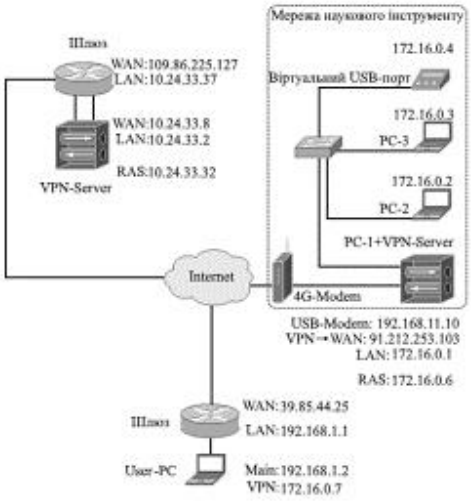
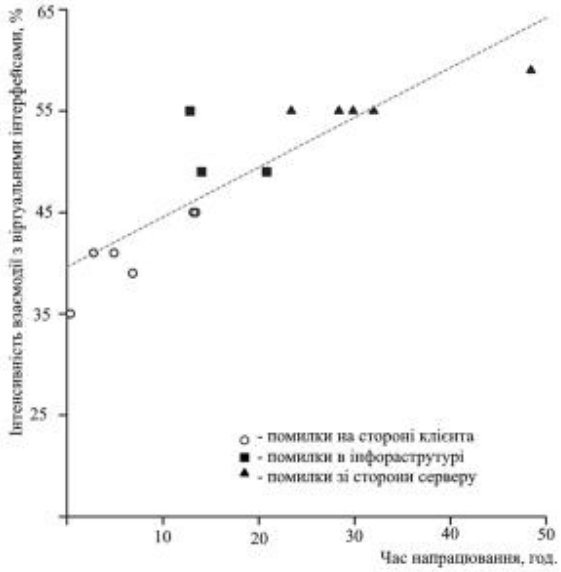


Схема мережної взаємодії при відсутності пулу реальних IP-адрес

7

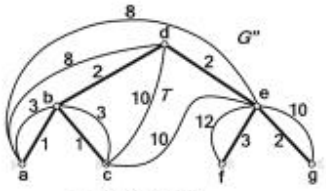
ДОСЛІДЖЕННЯ КЛІЄНТ-СЕРВЕРНОЇ ВЗАЄМОДІЇ

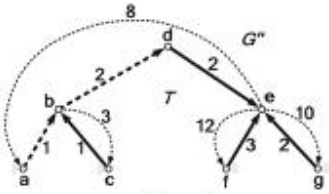


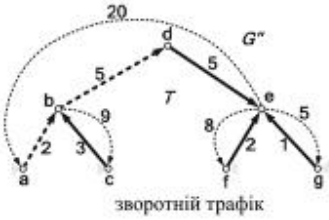
Частота виявлень помилок при взаємодії компонентів клієнт-серверної моделі в залежності від інтенсивності взаємодії компонентів

8

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ВІДМОВОСТІЙКОСТІ ВІРТУАЛЬНОЇ МЕРЕЖІ







Графи G'' для вихідного та вхідного трафіку

Оптимальна аугментація A''

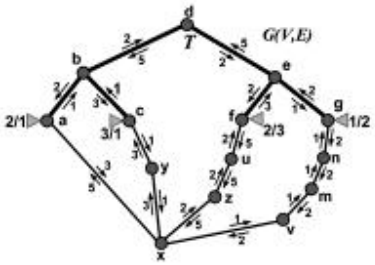
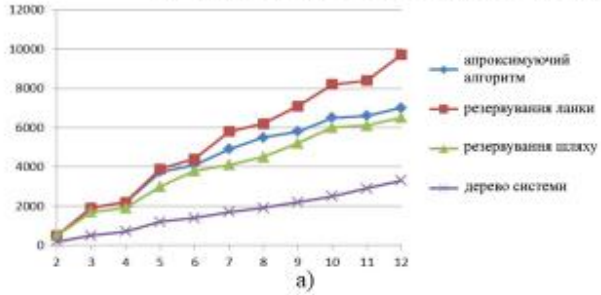
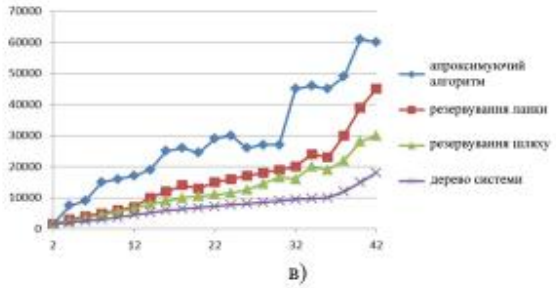


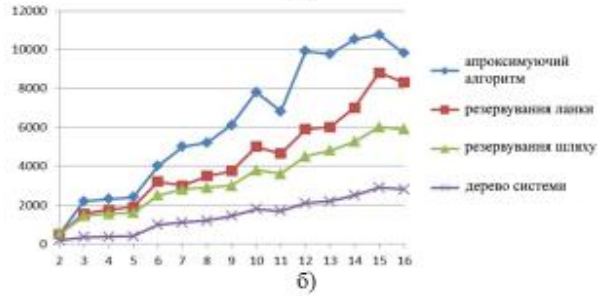
Схема запасної смуги пропускання, отримана за результатами дослідження

9

ОЦІНКА ЕФЕКТИВНОСТІ ВІДМОВОСТІЙКОСТІ СИСТЕМИ ДИСТАНЦІЙНОГО ДОСТУПУ ДО ВІДДАЛЕНИХ ПРИСТРОЇВ







Оцінка відмовостійкості системи дистанційного керування науковими інструментами з віртуалізацією інтерфейсів: а) для топології 12-node Ring; б) для топології NSFNET16; в) для топології Euroring

10

АПРОБАЦІЯ РЕЗУЛЬТАТІВ

Результати роботи апробовані на Міжнародній науковій інтернет-конференції "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" 12 травня 2020 року.

Отримана публікація:

Tomonova K.O., Onatskiy R.S. Organization of remote access to USB devices on computer network with terminal clients / Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 48) – У друці.

11

ВИСНОВКИ

В результаті виконання атестаційної роботи поставлена і успішно вирішена задача розробки методу дистанційного керування науковими інструментами з віртуалізацією інтерфейсів.

Зокрема:

- сформульована задача з формалізацією необхідних технічних вимог до розроблюваної оверлейної комп'ютерної мережі та особливостей віртуалізації USB-інтерфейсів;
- запропоноване рішення мережної складової задачі, засноване на використанні множинних VPN-тунелів;
- запропонований спосіб клієнт-серверної взаємодії при віртуалізації USB-інтерфейсів.

Необхідно відзначити, що об'єднання VPN-тунелів в каскадні схеми випадковим чином є не ефективним для побудови великих оверлейних мережевих інфраструктур для організації дистанційного доступу до наукових інструментів. Незважаючи на те, що пропускна здатність залежить від виду топології мережі, необхідно проводити аналіз розподілу VPN-підмереж для підвищення надійності процесу передачі даних. Таким чином, можна зробити висновок, що аналіз загальної пропускної здатності VPN-тунелів мереж багато в чому залежить від правильної організації розподіленої системи. Це також в деякій мірі пов'язано з маршрутизацією даних і правилами призначення шлюзів для комп'ютерів обсерваторії і клієнтів в якості основних для уникнення можливих неефективних маршрутів передачі інформації.

12

ДОДАТОК Б

Системні файли VPN-серверу

```
# Perform a TLS loopback test -- server side.
#
# This test performs a TLS negotiation once every 10 seconds,
# and will terminate after 2 minutes.
#
# From the root directory of the OpenVPN distribution,
# after openvpn has been built, run:
#
#    ./openvpn  --config  sample-config-files/loopback-client    (In  one
window)
#          ./openvpn     --config     sample-config-files/loopback-server
(Simultaneously in another window)

rport 16001
lport 16000
remote localhost
local localhost
dev null
verb 3
reneg-sec 10
tls-server
dh sample-keys/dh2048.pem
ca sample-keys/ca.crt
key sample-keys/server.key
cert sample-keys/server.crt
tls-auth sample-keys/ta.key 0
cipher AES-256-GCM
ping 1
inactive 120 10000000
```

Приклад Б.1 – Вміст файлу cloopback-server

```
# Perform a TLS loopback test -- client side.
#
# This test performs a TLS negotiation once every 10 seconds,
# and will terminate after 2 minutes.
#
# From the root directory of the OpenVPN distribution,
# after openvpn has been built, run:
#
#    ./openvpn  --config  sample-config-files/loopback-client    (In  one
window)
#          ./openvpn     --config     sample-config-files/loopback-server
(Simultaneously in another window)

rport 16000
lport 16001
remote localhost
local localhost
dev null
verb 3
reneg-sec 10
```

```
tls-client
remote-cert-tls server
ca sample-keys/ca.crt
key sample-keys/client.key
cert sample-keys/client.crt
tls-auth sample-keys/ta.key 1
cipher AES-256-GCM
ping 1
inactive 120 10000000
```

Приклад Б.2 – Вміст файлу cloopback-client

```
#!/bin/sh

# A Sample OpenVPN-aware firewall.

# eth0 is connected to the internet.
# eth1 is connected to a private subnet.

# Change this subnet to correspond to your private
# ethernet subnet.  Home will use HOME_NET/24 and
# Office will use OFFICE_NET/24.
PRIVATE=10.0.0.0/24

# Loopback address
LOOP=127.0.0.1

# Delete old iptables rules
# and temporarily block all traffic.
iptables -P OUTPUT DROP
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -F

# Set default policies
iptables -P OUTPUT ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD DROP

# Prevent external packets from using loopback addr
iptables -A INPUT -i eth0 -s $LOOP -j DROP
iptables -A FORWARD -i eth0 -s $LOOP -j DROP
iptables -A INPUT -i eth0 -d $LOOP -j DROP
iptables -A FORWARD -i eth0 -d $LOOP -j DROP

# Anything coming from the Internet should have a real Internet address
iptables -A FORWARD -i eth0 -s 192.168.0.0/16 -j DROP
iptables -A FORWARD -i eth0 -s 172.16.0.0/12 -j DROP
iptables -A FORWARD -i eth0 -s 10.0.0.0/8 -j DROP
iptables -A INPUT -i eth0 -s 192.168.0.0/16 -j DROP
iptables -A INPUT -i eth0 -s 172.16.0.0/12 -j DROP
iptables -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP

# Block outgoing NetBios (if you have windows machines running
# on the private subnet).  This will not affect any NetBios
# traffic that flows over the VPN tunnel, but it will stop
# local windows machines from broadcasting themselves to
# the internet.
iptables -A FORWARD -p tcp --sport 137:139 -o eth0 -j DROP
iptables -A FORWARD -p udp --sport 137:139 -o eth0 -j DROP
iptables -A OUTPUT -p tcp --sport 137:139 -o eth0 -j DROP
iptables -A OUTPUT -p udp --sport 137:139 -o eth0 -j DROP
```

```
# Check source address validity on packets going out to internet
iptables -A FORWARD -s ! $PRIVATE -i eth1 -j DROP

# Allow local loopback
iptables -A INPUT -s $LOOP -j ACCEPT
iptables -A INPUT -d $LOOP -j ACCEPT

# Allow incoming pings (can be disabled)
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

# Allow services such as www and ssh (can be disabled)
iptables -A INPUT -p tcp --dport http -j ACCEPT
iptables -A INPUT -p tcp --dport ssh -j ACCEPT

# Allow incoming OpenVPN packets
# Duplicate the line below for each
# OpenVPN tunnel, changing --dport n
# to match the OpenVPN UDP port.
#
# In OpenVPN, the port number is
# controlled by the --port n option.
# If you put this option in the config
# file, you can remove the leading '--'
#
# If you taking the stateful firewall
# approach (see the OpenVPN HOWTO),
# then comment out the line below.

iptables -A INPUT -p udp --dport 1194 -j ACCEPT

# Allow packets from TUN/TAP devices.
# When OpenVPN is run in a secure mode,
# it will authenticate packets prior
# to their arriving on a tun or tap
# interface.  Therefore, it is not
# necessary to add any filters here,
# unless you want to restrict the
# type of packets which can flow over
# the tunnel.

iptables -A INPUT -i tun+ -j ACCEPT
iptables -A FORWARD -i tun+ -j ACCEPT
iptables -A INPUT -i tap+ -j ACCEPT
iptables -A FORWARD -i tap+ -j ACCEPT

# Allow packets from private subnets
iptables -A INPUT -i eth1 -j ACCEPT
iptables -A FORWARD -i eth1 -j ACCEPT

# Keep state of connections from local machine and private subnets
iptables -A OUTPUT -m state --state NEW -o eth0 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state NEW -o eth0 -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

# Masquerade local subnet
iptables -t nat -A POSTROUTING -s $PRIVATE -o eth0 -j MASQUERADE
```

Приклад Б.3 – Вміст файлу sample-config-files