
Specyfikacja wymagań

dla FiberOrca

Marta Kurzych

m.kurzych.649@studms.ug.edu.pl

Konrad Kreczko

k.kreczko.813@studms.ug.edu.pl



Wydział Matematyki, Fizyki i Informatyki
Uniwersytet Gdański
Rok akademicki 2024-2025
20.11.2024

Spis treści

1	Wprowadzenie	2
1.1	Cel dokumentu	2
1.2	Zakres produktu	2
2	Opis ogólny	2
2.1	Perspektywa produktu	2
2.2	Funkcje produktu	2
2.3	Ograniczenia	3
3	Model procesów biznesowych	3
3.1	Aktorzy i charakterystyka użytkowników	3
3.2	Obiekty biznesowe	3
4	Wymagania funkcjonalne	4
5	Charakterystyka interfejsów	7
5.1	Interfejs użytkownika	7
5.2	Interfejsy zewnętrzne	7
6	Wymagania pozafunkcjonalne	8

Wprowadzenie

Cel dokumentu

Dokument stanowi jedyne źródło wymagań aplikacji FiberOrca. Stanowi podstawę dla specyfikacji oprogramowania. Dokument przeznaczony głównie dla zespołu deweloperskiego zajmującego się wytwarzaniem oprogramowania FiberOrca.

Zakres produktu

Celem projektu jest utworzenie systemu informatycznego umożliwiającego monitorowanie i analizę ruchu sieciowego przez Command Line Interface. System będzie umożliwiał analizę pojedynczego pakietu, analizę ruchu sieciowego w czasie, zbieranie danych w tle oraz eksport danych do najpopularniejszych formatów. System będzie pozwalał na wizualizację danych w celu ułatwienia analizy.

Opis ogólny

Perspektywa produktu

System będzie narzędziem terminalowym, działającym w środowisku Unix-podobnym. Będzie zapewniał interfejs tekstowy do interakcji z użytkownikiem. Program będzie mógł działać w trybie interaktywnym oraz wsadowym.

Funkcje produktu

Podstawowe funkcjonalności:
<ul style="list-style-type: none">• Przechwytywanie pakietów w czasie rzeczywistym• Analiza protokołów sieciowych (IP, TCP, UDP)• Filtrowanie pakietów według różnych kryteriów• Zapisywanie przechwyconych pakietów do pliku• Odczytywanie pakietów z zapisanego pliku• Wyświetlanie statystyk ruchu sieciowego w postaci wykresów

Tabela 1: Funkcje produktu

System wymaga:
<ul style="list-style-type: none">• System operacyjny: Linux (kernel 4.0 lub nowszy)• Minimum 512MB RAM• Procesor x86 z co najmniej 2 rdzeniami

Tabela 2: Ograniczenia systemu

Model procesów biznesowych

Aktorzy i charakterystyka użytkowników

ID:	USER
Nazwa:	Użytkownik
Opis:	Użytkownik może odczytywać pakiety, filtrować je oraz zapisywać do pliku.

Tabela 3: Charakterystyka użytkowników

Obiekty biznesowe

Obiekty biznesowe	
Nazwa:	Pakiet
Opis:	Podstawowa jednostka danych przechwytywanych przez system. Zawiera dane nagłówka oraz zawartość pakietu.
Nazwa:	Filtr
Opis:	Zestaw reguł określających, które pakiety mają być przechwytywane lub wyświetlane.
Nazwa:	Sesja
Opis:	Reprezentuje pojedynczą sesję przechwytywania pakietów z określonymi parametrami.

Tabela 4: Obiekty biznesowe systemu

Wymagania funkcjonalne

Wymagania funkcjonalne zostały przedstawione na diagramie przypadków użycia.

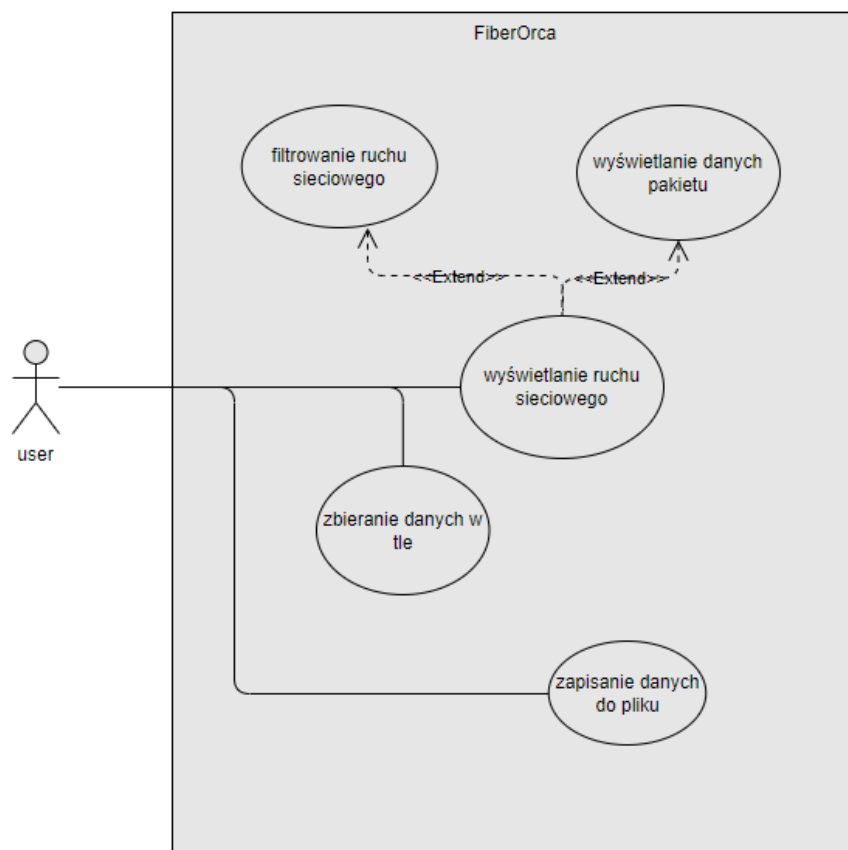


Tabela 5: Specyfikacja przypadku użycia: Analiza pakietów

ID:	PacketAnalysis
Nazwa:	Analiza pakietów sieciowych
Aktorzy główni:	User
Aktorzy pomocniczy:	Brak
Poziom:	Podstawowy
Priorytet:	P0
Opis:	System analizuje zawartość przechwyconych pakietów, dekoduje nagłówki i wyświetla szczegółowe informacje.
Wyzwalacze:	<ol style="list-style-type: none">1. Pakiet jest dostępny w buforze.2. Użytkownik wybiera pakiet do szczegółowej analizy.

Warunki początkowe:	<ol style="list-style-type: none"> 1. Pakiety są dostępne w buforze lub pliku. 2. System posiada informacje o protokołach.
Warunki końcowe:	<ol style="list-style-type: none"> 1. Pakiet jest zdekodowany. 2. Informacje o pakiecie są wyświetlone. 3. Statystyki są zaktualizowane.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. System pobiera pakiet z bufora. 2. System analizuje nagłówek Ethernet: <ol style="list-style-type: none"> (a) Adresy MAC (b) Typ protokołu 3. System analizuje nagłówek IP: <ol style="list-style-type: none"> (a) Adresy IP (b) Protokół wyższej warstwy (c) Flagi i fragmentację 4. System analizuje protokoły wyższych warstw: <ol style="list-style-type: none"> (a) TCP/UDP porty i flagi (b) Dane aplikacyjne 5. System wyświetla zdekodowane informacje. 6. System aktualizuje statystyki ruchu.
Scenariusze alternatywne:	<ol style="list-style-type: none"> 1. Analiza protokołów specyficznych dla aplikacji. 2. Generowanie raportów statystycznych.
Wyjątki:	<ul style="list-style-type: none"> • Nieznany protokół. • Uszkodzony pakiet. • Niekompletny pakiet. • Błąd dekodowania.
Dodatkowe wymagania:	System musi analizować pakiety w czasie rzeczywistym. Analiza powinna obejmować podstawowe protokoły sieciowe (Ethernet, IP, TCP, UDP, ICMP).

Tabela 6: Specyfikacja przypadku użycia: Przechwytywanie pakietów

ID:	PacketCapture
Nazwa:	Przechwytywanie pakietów sieciowych
Aktorzy główni:	User
Aktorzy pomocniczy:	Brak
Poziom:	Podstawowy
Priorytet:	P0
Opis:	System przechwytuje pakiety sieciowe na wybranym interfejsie z możliwością zastosowania filtrów.
Wyzwalacze:	<ol style="list-style-type: none"> 1. Użytkownik uruchamia polecenie rozpoczęcia przechwytywania. 2. Użytkownik wskazuje interfejs sieciowy.
Warunki początkowe:	<ol style="list-style-type: none"> 1. Program uruchomiony z uprawnieniami administratora. 2. Interfejs sieciowy jest dostępny. 3. Biblioteka libpcap jest poprawnie zainicjalizowana.
Warunki końcowe:	<ol style="list-style-type: none"> 1. Pakiety są przechwytywane z sieci. 2. Pakiety są buforowane w pamięci. 3. Opcjonalnie pakiety są zapisywane do pliku.
Scenariusz Główny:	<ol style="list-style-type: none"> 1. Użytkownik wybiera interfejs sieciowy. 2. Użytkownik określa parametry przechwytywania: <ol style="list-style-type: none"> (a) Rozmiar bufora (b) Tryb promiscuous (c) Maksymalny rozmiar pakietu 3. Użytkownik opcjonalnie definiuje filtry BPF. 4. System rozpoczyna nasłuchiwanie na interfejsie. 5. System przechwytuje pakiety. 6. System zapisuje pakiety do bufora.
Scenariusze alternatywne:	<ol style="list-style-type: none"> 1. Zapis przechwyconych pakietów do pliku. 2. Rotacja plików logów przy długim przechwytywaniu.

Wyjątki:	<ul style="list-style-type: none"> • Brak uprawnień root. • Interfejs jest niedostępny. • Błąd inicjalizacji libpcap. • Przepełnienie bufora.
Dodatkowe wymagania:	System musi obsługiwać tryb promiscuous. Przechwytywanie musi działać bez gubienia pakietów przy standardowym obciążeniu sieci.

Charakterystyka interfejsów

Interfejs użytkownika

ID	Wymaganie	Priorytet
1	Interfejs musi umożliwiać filtrowanie i sortowanie wyników analizy według pól (np. IP, port).	P1

ID	Wymaganie	Priorytet
2	System powinien weryfikować poprawność danych wejściowych, np. poprawność adresu IP, portu lub zakresu czasowego.	P0

ID	Wymaganie	Priorytet
3	Użytkownik powinien mieć możliwość wizualizacji analizy w różnych trybach (pojedynczy pakiet, ruch w czasie).	P0

ID	Wymaganie	Priorytet
4	System musi oferować możliwość eksportu wyników analizy do plików w formacie CSV za pomocą poleceń CLI.	P1

Interfejsy zewnętrzne

ID	Wymaganie	Priorytet
1	Backend musi przetwarzać dane w czasie rzeczywistym i udostępniać wyniki do wizualizacji w interfejsie CLI.	P0

ID	Wymaganie	Priorytet
2	System musi obsługiwać filtrowanie danych na poziomie backendu, zgodnie z poleceniami przekazanymi przez UI (np. filtr IP lub protokołu).	P1

Wymagania pozafunkcjonalne

ID:	SECURITY
Nazwa:	Ograniczenie dostępu i bezpieczne przechowywanie plików
Priorytet:	P0
Opis:	System jest zabezpieczony przed nieautoryzowanym użyciem narzędzia do działań niezgodnych z polityką bezpieczeństwa oraz zebrane dane powinny być zapisywane w katalogach chronionych przed nieautoryzowanym dostępem.

ID:	MEMORY
Nazwa:	Zarządzanie pamięcią
Priorytet:	P0
Opis:	System musi działać z minimalnymi wymaganymi uprawnieniami i nie może zapisywać wrażliwych danych w postaci niezaszyfrowanej. Backend powinien unikać wycieków pamięci, stosując odpowiednią kontrolę alokacji oraz dealokacji zasobów.

ID:	AVAILABILITY
Nazwa:	Dostępność
Priorytet:	P2
Opis:	System powinien być udostępniony do pobrania i instalacji przez popularne menagery pakietów, takie jak apt i dnf.

ID:	PERFORMANCE
Nazwa:	Wydajność
Priorytet:	P0
Opis:	System powinien być zoptymalizowany pod względem prędkości działania i działać współbieżnie, by być w stanie monitorować ruch sieciowy nawet na najstarszych urządzeniach

ID:	RELIABILITY
Nazwa:	Niezawodność
Priorytet:	P1
Opis:	System musi działać stabilnie przez długi czas, obsługiwać błędy oraz przepełnienie bufora.