DOBIERANIE OPROGRAMOWANIA UŻYTKOWEGO DO REALIZACJI OKREŚLONYCH ZADAŃ W KONFIGURACJI I MONITORINGU SIECIOWEGO.

Dobieranie oprogramowania użytkowego służącego do konfiguracji i monitoringu sieci komputerowych jest bardzo istotne z punktu widzenia administracyjnego, w tym wykrywania przyczyn występujących w sieciach problemów technicznych.
Prawidłowa konfiguracja urządzeń sieciowych pozwala skutecznie wyeliminować występowanie problemów takich jak na przykład błędne kierowanie ruchu, nieautoryzowany dostęp do sieci, konflikty w sieci , nieprawidłowa adresacja urządzeń itp.
Podstawowym urządzeniem sieciowym, dzięki któremu można zbudować sieć komputerową jest **router.**
Można go wykorzystać do połączenia dwóch sieci lokalnych LAN lub połączenia sieci lokalnej do Internetu. Może on być traktowany jako wyspecjalizowany komputer, posiadający swój własny procesor, pamięć, system operacyjny i inne podzespoły. Router musi posiadać minimum dwa interfejsy - po jednym dla każdej z sieci. System operacyjny routera umożliwia uruchomienie protokołu routingu, a bardziej zaawansowane routery pozwalają na uruchomienie różnych protokołów routingu, o czym decyduje administrator podczas konfiguracji routera.
W zaawansowanych routerach można również uruchomić dodatkowe usługi, takie jak translacja adresów NAT, filtrowanie pakietów za pomocą kontroli list dostępu.
Ciągłe monitorowanie sieci komputerowej, to jedno z głównych zadań każdego administratora.
Aby ułatwić monitorowanie sieci powstało wiele aplikacji wspomagających prace administratora.
Oprogramowanie do monitorowania sieci służy również do rozwiązywania problemów występujących w sieciach komputerowych. Dzięki nim można przeskanować sieć i zobaczyć które komputery w sieci w danej chwili pracują, jakie mają przydzielone adresy IP oraz jakie posiadają adresy MAC.
Przykładami takich programów są **Angry IP Scanner** (skanuje adresy IP i adresy MAC urządzeń pracujących w sieci), **Network Scanner Application** (skanuje adresy IP i adresy MAC urządzeń pracujących w sieci, prezentuje nazwy urządzeń), **Wireshark** (analizuje ruch sieciowy, transmisję pakietów, itp.), **inSSIDer** (analizuje sieci WiFi, moc sygnału, kanały, na których pracują sieci, itp.), **Network Mapper - Nmap** (skanuje i prezentuje pracujące komputery w sieci, ich adresy IP, adresy MAC, wykorzystywany do audytu bezpieczeństwa) , **Ntop** (służący do zbierania informacji statystycznych dotyczących ruchu sieciowego). Niektóre z tych programów (np. Wireshark) analizują ruch sieciowy wykrywając błędy transmisji danych, konflikty IP itp. Można dzięki niemu wykryć wiele występujących w sieci problemów związanych z ruchem sieciowym.

W systemie Windows standardowo zaimplementowano narzędzia umożliwiające monitorowanie komputera w sieci. Statystyki interfejsu można wyświetlić za pomocą polecenia **netstat** uruchamianego z wiersza poleceń. Polecenie z opcją -e (**netstat -e**) wyświetla liczbę wysyłanych i odebranych pakietów. Polecenie **nbtstat** wyświetla statystykę protokołu NetBIOS.

DOBIERANIE OPROGRAMOWANIA UŻYTKOWEGO DO REALIZACJI OKREŚLONYCH ZADAŃ W KONFIGURACJI I MONITORINGU SIECIOWEGO.

Ćwiczenie 1.

Wykorzystując wiersz poleceń i polecenia dotyczące statystyk w sieci komputerowej, wyświetl możliwie najwięcej informacji sieciowych i krótko opisz czego dotyczą.

Ćwiczenie 2.

Pobierz i zainstaluj program Network Scanner Application, a następnie przeskanuj lokalną sieć komputerową w szkole lub w domu i na przykładzie jednego urządzenia w sieci komputerowej wypisz uzyskane informacje.