



**UNIWERSYTET OPOLSKI**  
**WYDZIAŁ MATEMATYKI, FIZYKI I INFORMATYKI**

**Informatyka**

**PRACA INŻYNIERSKA**

**Przemysław Krzysztof Pyda**

**Projekt sieci komputerowej z usługami serwerowymi**  
**Windows Server**  
**Project of computer network with Windows Server services**

Praca napisana pod kierunkiem  
**dr Jolanty Tańculi**

**Opole 2023**

## **Streszczenie**

Niniejsza praca dyplomowa dotyczy opracowania i wdrożenia projektu na rzeczywistych urządzeniach sieciowych klasy korporacyjnej. Praca dedykowana jest dla małej firmy informatycznej, specjalizującej się w wytwarzaniu oprogramowania oraz projektów graficznych. Projekt zostanie zrealizowany na fizycznych urządzeniach sieciowych firmy Cisco oraz na wirtualnym serwerze Windows Server 2016. Sieć powinna zapewnić niezawodny dostęp do programów i zasobów sprzętowych. Niezawodność infrastruktury sieci realizowana będzie poprzez skalowalność i redundancję, co w przyszłości przyczyni się do łatwej jej rozbudowy.

**Słowa kluczowe:** projekt sieci, redundancja, Cisco, Windows Server

## **Abstract**

The diploma thesis concerns the development and implementation of the project on real enterprise-class network devices. The work is dedicated for a small IT company specializing in software development and graphic design. The project will be implemented on physical Cisco network devices and on a virtual Windows Server 2016 server. The network should provide reliable access to programs and hardware resources. Reliability of the network infrastructure will be implemented through scalability and redundancy, which will contribute to its easy expansion in the future.

**Keywords:** network design, redundancy, Cisco, Windows Server

## Spis treści

Wstęp.....	5
1. Cel i założenia pracy .....	6
1.1. Założenia ogólne.....	6
1.2. Założenia Windows Server.....	7
1.3. Założenia sieciowe .....	7
2. Infrastruktura sieciowa .....	9
2.1. Sprzętowa infrastruktura.....	9
2.2. Rzuty budynku oraz umiejscowienie urządzeń .....	11
2.3. Projekt logiczny sieci komputerowej .....	13
2.4. Technologie i protokoły wykorzystane w infrastrukturze sieciowej.....	15
3. Adresacja i podłączenia sieciowe.....	20
3.1. Adresy sieciowe.....	20
3.2. Sieci Virtual LAN (VLAN).....	21
3.3. Fizyczne podłączenia urządzeń sieciowych .....	22
4. Wybrane technologie sieciowe i metody zabezpieczania sieci w warstwie 2.....	26
4.1. Technologia stackowania przełączników .....	26
4.2. Technologia logicznej agregacji łączy .....	27
4.3. Port Security .....	28
4.4. DHCP Snooping .....	29
4.5. Dynamic ARP Inspection (DAI) .....	30
5. Mechanizmy i protokoły Windows Server.....	31
5.1. Serwery lokalne Windows Server .....	31
5.2. Redundancja kart sieciowych w Windows Server .....	32
5.3. Struktura organizacyjna firmy CyberCode.com – Grupy i Użytkownicy .....	34
5.4. Profile mobilne użytkowników .....	39
5.5. Redundancja usług serwerowych Windows Server – Active Directory.....	43
5.6. Serwer DHCP – Wdrożenie w konfiguracji redundantnej .....	45
5.7. Wewnętrzna strona internetowa firmy .....	49
5.8. Wykorzystanie GPO do zautomatyzowania instalacji oprogramowania Google Chrome wraz z dedykowaną konfiguracją ADM.....	52
5.9. Ustawienia polityki haseł.....	55
5.10. Ustawienie banneru logowania .....	57
5.11. Blokada dostępu do panelu sterowania.....	57
5.12. Mapowanie dysków sieciowych .....	58
6. Proces i testy użytkownika zasobów z perspektywy użytkownika domenowego.....	63
6.1. Proces logowania użytkownika .....	63

6.2.	Testy połączeń sieciowych – Windows 10.....	71
6.3.	Komputer administracyjny .....	73
6.4.	Komunikacja SSH z komputera administracyjnego .....	75
7.	Bezpieczeństwo infrastruktury .....	77
7.1.	Bezpieczeństwo budynku .....	77
7.2.	Bezpieczeństwo dostępu administracyjnego .....	77
7.3.	Bezpieczeństwo sieciowe .....	78
7.4.	Bezpieczeństwo Windows Server .....	79
	Podsumowanie .....	80
	Bibliografia.....	81
	Opis zawartości APD .....	82
	Spis tabel .....	82
	Spis rysunków .....	83
	Spis listingów .....	86

## Wstęp

W dzisiejszych czasach bezawaryjny i wydajny dostęp do zasobów sieci Internet i intranet jest na wagę złota. W wielkich firmach nawet kilkuminutowe przestoje w dostępie do usług mogą generować milionowe straty. Wszelkich tego typu zagrożeń należy za wszelką cenę unikać. Obecnie projektanci sieci muszą zmierzyć się z kilkoma, niezwykle ważnymi zadaniami. Projektowana sieć musi zapewniać szybki i łatwy dostęp do zasobów przez użytkowników końcowych. Powinna zapewniać bezpieczeństwo transmitowanego ruchu sieciowego, a przede wszystkim być wysoce bezawaryjna. Kluczowe elementy infrastruktury sieciowej powinny posiadać mechanizmy wykrywania awarii oraz jasno określone procedury, które wykonywane są w momencie uszkodzenia jej newralgicznych elementów. Nadmiarowość może być realizowana zarówno poprzez warstwę fizyczną (np. Link Aggregation, nadmiarowy switch/router) bądź poprzez warstwę programową (np. tracking w protokole HSRP, protokoły routingu dynamicznego). Kolejnym wymaganiem stawianym przed projektantem jest utrzymanie możliwego współczynnika ceny do jakości. W idealnym scenariuszu, gdy cena na wydaną instalację sieciową nie grałaby roli, nic nie stałoby na przeszkodzie, aby użyć najwyższych dostępnych możliwych modeli urządzeń sieciowych. Niestety, realia większości projektów są takie, iż im taniej, tym lepiej i nie jest potrzebny specjalistyczny, nowoczesny sprzęt. W naszym projekcie będziemy dążyć do osiągnięcia złotego środka czyli efektu dającego możliwie wysoką wydajność, bezpieczeństwo i odporność na awarię z w miarę niskim budżetem oczywiście na odpowiednim poziomie.

W przypadku tej pracy inżynierskiej środowiskiem laboratoryjnym jest sala laboratoryjna w Instytucie Informatyki Uniwersytetu Opolskiego. Do realizacji założeń wykorzystywany jest sprzęt dostępny w sali oraz sprzęt prywatny studenta.

## **1. Cel i założenia pracy**

Celem pracy jest wykonanie projektu sieci komputerowej i konfiguracja urządzeń wchodzących w jej skład. Praca opierać się będzie na fikcyjnej firmie o nazwie „CyberCode”, która specjalizuje się w wytwarzaniu oprogramowania przez zespół programistów oraz realizacji projektów graficznych przez dział grafików. Projekt zostanie zrealizowany na fizycznych urządzeniach sieciowych firmy Cisco oraz na wirtualnym serwerze Windows Server 2016. Infrastruktura sieci i techniki niezawodności zapewnione będą poprzez jej skalowalność i redundancję. Sieć powinna też posiadać odpowiednio wysoki poziom przyszłej rozbudowy.

W firmie poza działem informatycznym oraz graficznym znajduje się dział zarządczy, dział sprzedaży oraz dział Human Resources. Zdecydowana większość pracowników pracuje w dziale ICT (dziale informatycznym). Siedzibą firmy jest budynek złożony z piętra oraz parteru. Na kondygnacji dolnej znajdują się: pomieszczenie pracowników informatycznych, dział HR, dział graficzny, główna serwerownia oraz dwie toalety. Na kondygnacji górnej znajdują się kolejne dwa pomieszczenia z przeznaczeniem dla pracowników informatycznych, biuro kadry zarządczej, biuro kierowników realizowanych projektów oraz dział sprzedaży. Dodatkowo na piętrze znajdziemy małą kuchnię przeznaczoną dla pracowników firmy oraz 2 toalety. Dodatkowo na dolnej i górnej kondygnacji znajduje się ogólnodostępna drukarka sieciowa. Celem pracy jest opracowanie projektu logicznego sieci wraz z wdrożeniem, bez projektu okablowania budynku czy pomieszczeń.

### **1.1. Założenia ogólne**

- Ilość pracowników poszczególnych działów może wzrosnąć w miarę rozwoju firmy, dlatego zagospodarowanie budynku powinno zakładać możliwość zwiększenia pracowników. Dodatkowo pomieszczenia pracownicze posiadają odpowiednio większą kubaturę w celu przyszłej rozbudowy stanowisk pracy;
- Sieć powinna być w pełni skalowalna oraz redundantna. Za wszelką cenę powinno się unikać punktów „single point of failure”, czyli pojedynczych punktów awarii, wpływających krytycznie na działanie całej sieci;
- Sprzęt serwerowy, zarówno w serwerowni jak i szafie rack podwieszanej na piętrze, powinien być niedostępny dla osób nieuprawnionych;

- Główna szafa serwerowo-sieciowa znajduje się w klimatyzowanej serwerowni. Infrastruktura powinna być odporna na chwilowe zaniki prądu. W realizacji tego zadania zostanie użyty UPS;
- Do specjalnego komputera, przeznaczonego do awaryjnego administrowania siecią komputerową możliwość logowania powinni mieć jedynie uprawnieni administratorzy. Komputer znajduje się w serwerowni.

## **1.2.Założenia Windows Server**

- Użytkownicy posiadają własne konta w domenie CyberCode.com;
- Użytkownicy synchronizują swoje pliki przy użyciu profili mobilnych z dyskiem podłączonym pod serwer w celu synchronizacji plików pomiędzy urządzeniami;
- Użytkownicy mają narzuconą politykę tworzenia bezpiecznych haseł – minimum 10 znaków, hasło spełnia wymogi złożoności, 24 ostatnio użyte hasła są zapisywane;
- Użytkownik przy pierwszym logowaniu będzie musiał zmienić domyślne hasło na unikalne;
- Odpowiednie działy posiadają odpowiednio zmapowane dyski sieciowe – według założonych uprawnień i potrzeb;
- Serwer powinien posiadać 2 karty sieciowe działające w trybie NIC Teaming Mode;
- Serwery powinny działać redundantnie i przejmować kluczowe usługi takie jak Active Directory czy role serwera DHCP w wypadku awarii jednego z dwóch serwerów;
- Użytkownicy powinni mieć dostęp do intranetu i dwóch stron dostępnych dla wszystkich autoryzowanych użytkowników – strona informacyjna cybercode.local oraz portal pracowniczy portal.cybercode.local;
- Administracja warstwy serwerowej powinna w razie możliwości być prowadzona w języku angielskim.

## **1.3. Założenia sieciowe**

- Pracownicy poszczególnych działów grupowani są w odpowiadające sobie sieci VLAN (Virtual LAN) w celu logicznego odseparowania od innych działów;
- Użytkownicy nie mogą przynosić swoich urządzeń bez wiedzy administratora;
- Użytkownicy nie będą łączyć się zdalnie, poprzez VPN, do zasobów sieci firmowej;

- Poszczególne sieci VLAN powinny mieć dostęp do serwerów DHCP. Nie powinno zachodzić wycinanie ruchu rozgłoszeniowego potrzebnego do otrzymania automatycznej adresacji IPv4;
- Administratorzy powinni mieć dostęp do urządzeń sieciowych przy pomocy szyfrowanego połączenia SSH po poprawnym procesie autoryzacji.



## 2. Infrastruktura sieciowa

Rozdział ten dotyczy projektu infrastruktury sieciowej, użytych urządzeń, oprogramowania, architektury budynku, topologii sieci.

### 2.1. Sprzętowa infrastruktura

Projekt opiera się na założeniach utrzymania kampusowej sieci LAN, które hierarchiczność możemy przedstawić w dwóch lub trzech warstwach. Ze względu na mało rozbudowany projekt wykorzystano model dwuwarstwowy:

- Warstwa rdzenia (ang. Core) - kluczowa warstwa, w której podejmowane są najważniejsze działania dotyczące routingu i przełączania. Do warstwy rdzenia zaliczamy 2 routery pracujące w protokole redundancji GLBP, 2 najwydajniejsze, wzajemnie zestackowane switchy L3 będące mostem głównym STP oraz łącznikami pomiędzy routerami oraz serwerem Windows. Urządzenia warstwy najwyższej powinny mieć najwyższą możliwą odporność na awarie. Urządzenia w tej warstwie posiadają redundantne zasilanie działające w trybie Hot Plug;
- Warstwa dostępową (ang. Access) - najniższa warstwa, w której do przełączników L2 podpinane są urządzenia końcowe, takie jak komputery, VoIP czy drukarki. Warstwa z założenia z najniższym współczynnikiem ochrony przed awarią. Awaria pojedynczego połączenia kablowego od przełącznika do komputera nie jest awarią krytyczną.

Wykorzystane urządzenia w infrastrukturze sieciowej:

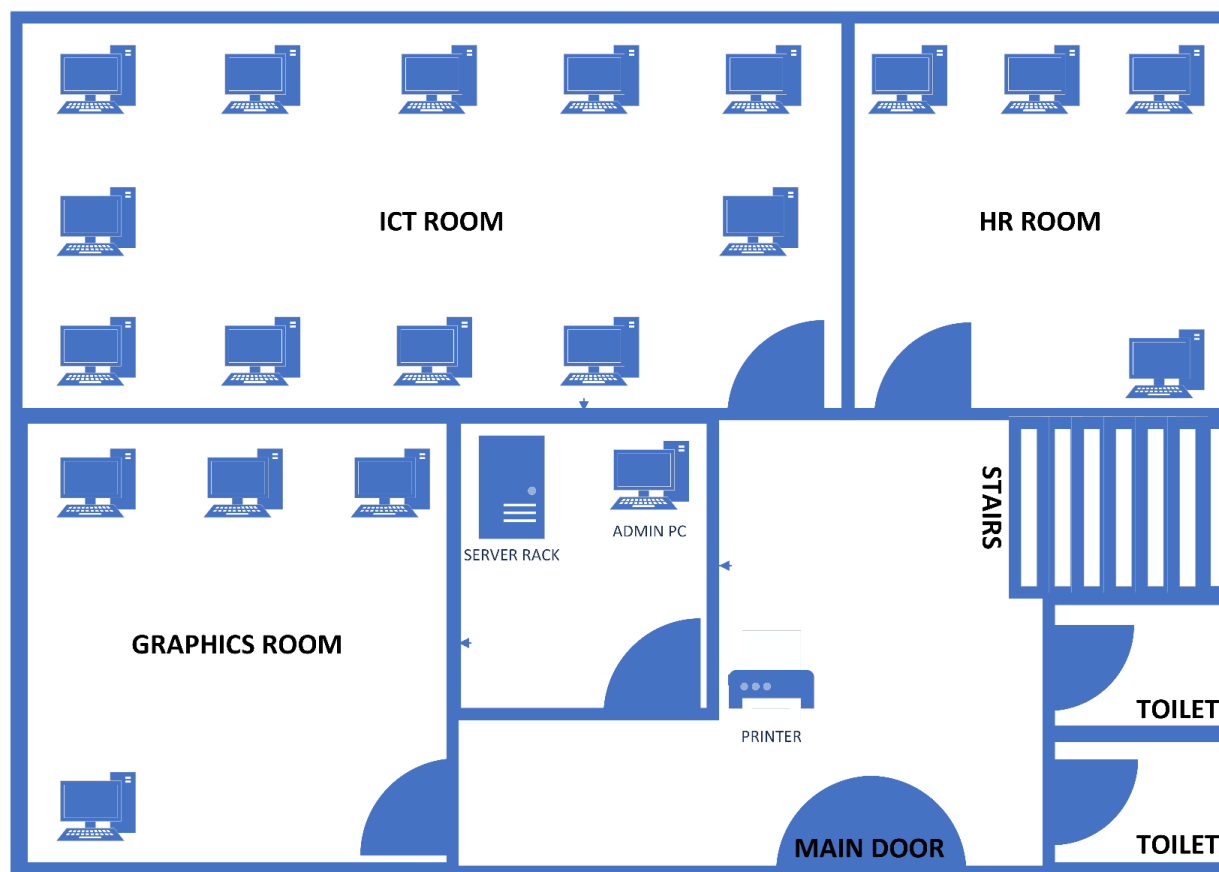
- 1x router Cisco 1841. Router symulujący w celach projektowych dostawcę ISP oraz połączenia z siecią Internet;
- 2x router Cisco 1841. Podstawowy, prosty router marki Cisco wystarczający do realizowania podstawowych zadań związanych z realizacją routingu pomiędzy siecią wewnętrzną LAN z światem zewnętrznym. Są to routery brzegowe infrastruktury sieciowej firmy;
- 2x Cisco Catalyst 3750G z systemem IOS C3750-IPSERVICESK9-M w wersji 12.2(55)SE12. 24 portowa odmiana przełączników serii 3750 pozwalająca na przełączanie pakietów w warstwie 3 (Switch L3). Przełączniki te znajdują się w warstwie rdzenia i realizują zadania mostu głównego mechanizmu STP

oraz odpowiadają za routing pomiędzy oddzielnymi sieciami VLAN (inter-vlan routing). Dodatkowo w celu zwiększenia bezawaryjności urządzenia pracują w trybie stack, będąc połączone ze sobą specjalnym okablowaniem, dzięki czemu przepustowość pomiędzy przełącznikami w warstwie rdzenia wynosi 32Gb/s;

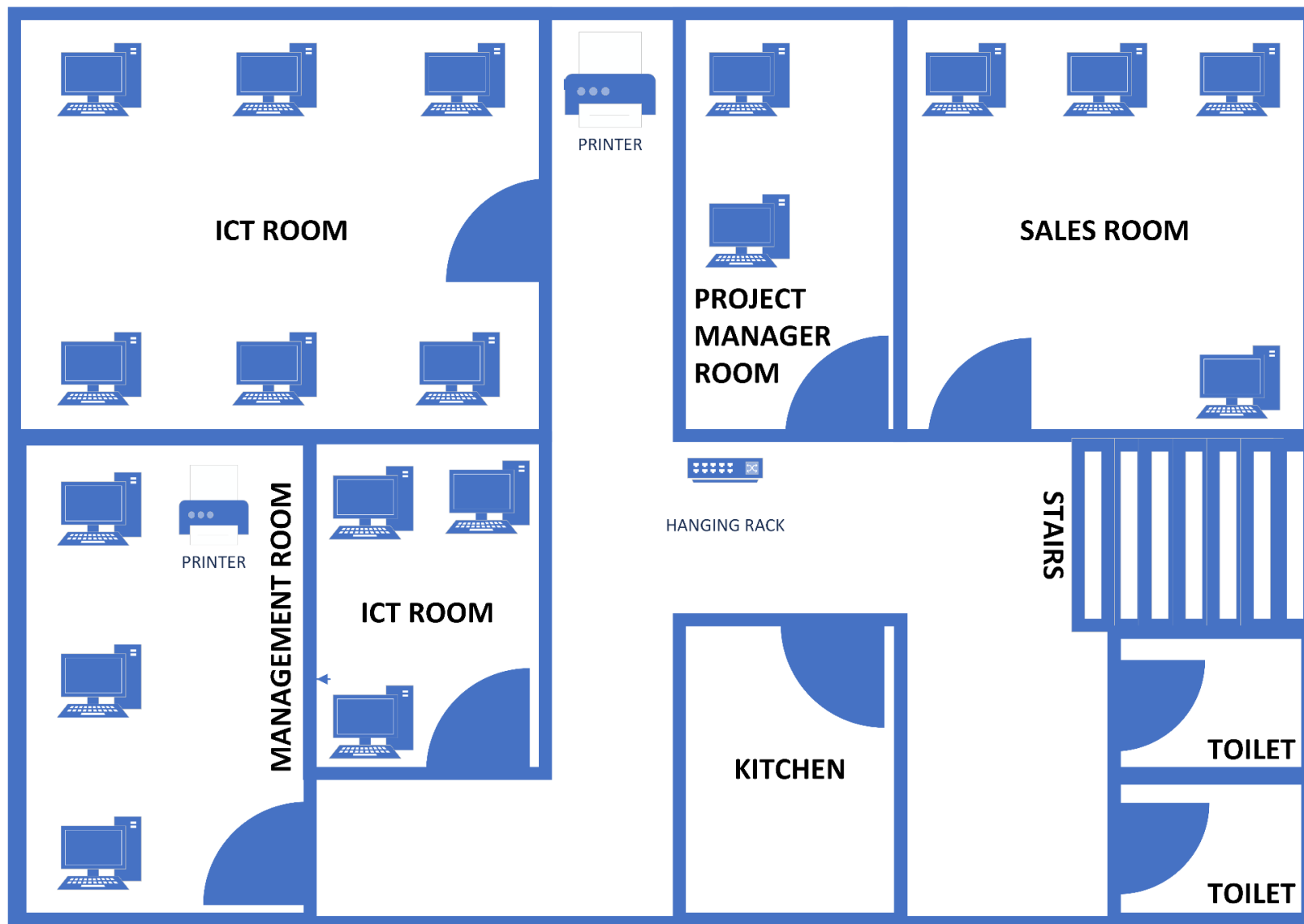
- 2x Cisco Catalyst 2960 z systemem IOS 2960-LANBASEK9-M w wersji 12.2(50)SE3. 24 portowa odmiana przełączników z serii 2960 w infrastrukturze sieciowej pełni rolę przełączników dostępowych, do których podłączane są urządzenia końcowe. Przełączanie w tym modelu odbywa się wyłącznie na podstawie warstwy drugiej, a więc adresów MAC kart sieciowych urządzeń w topologii. Na każdej z kondygnacji znajduje się pojedynczy przełącznik w zabezpieczonym miejscu, niedostępny dla osób nieuprawnionych;
- Wirtualizowane oprogramowanie serwerowe Windows Server 2016 odpowiadające za usługi domenowe w infrastrukturze sieciowej. Oprogramowanie zaimplementowane jest na urządzeniu klasy Personal Computer przy użyciu oprogramowania Oracle VM VirtualBox . Za część sprzętową odpowiada procesor Intel Core i3-4170, wspierany przez 12GB pamięci operacyjnej oraz szybki dysk HDD;
- Fizyczne komputery klienckie klasy Personal Computer, podłączone do przełączników dostępowych przy pomocy okablowania miedzianego.

## 2.2. Rzuty budynku oraz umiejscowienie urządzeń

Wedle założeń projektu siedzibą firmy jest budynek o dwóch kondygnacjach opisany na stronie 5. Na podstawie dostępnych pomieszczeń i charakterystyki budynku określono poniższy rozkład i umiejscowienie urządzeń.

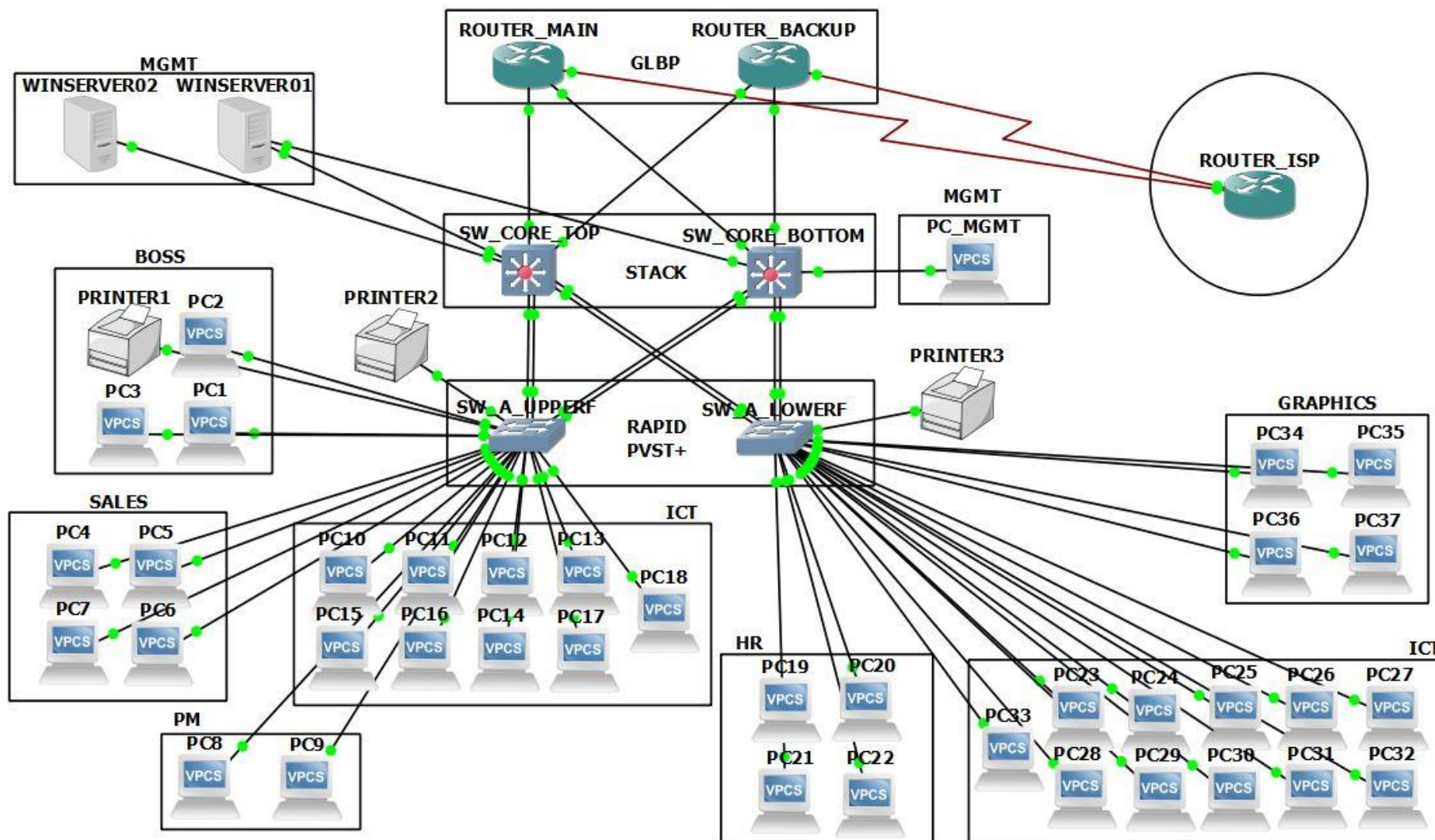


Rysunek 2.2.1 Rzut budynku - parter. Opracowanie własne



Rysunek 2.2.2 Rzut budynku - piętro. Opracowanie własne

### 2.3. Projekt logiczny sieci komputerowej



Rysunek 2.3.1 Logiczna perspektywa sieci komputerowej. Opracowanie własne

Pliki konfiguracyjne poszczególnych urządzeń sieciowych znajdują się w listingach na końcu pracy inżynierskiej:

- Konfiguracja ROUTER\_ISP znajduje się w Listing 1 - ROUTER\_ISP;
- Konfiguracja ROUTER\_MAIN znajduje się Listing 2 - ROUTER\_MAIN;
- Konfiguracja ROUTER\_BACKUP znajduje się w Listing 3 - ROUTER\_BACKUP;
- Konfiguracja SW\_CORE znajduje się w Listing 4 - SW\_CORE;
- Konfiguracja SW\_A\_UPPERF znajduje się Listing 5 - SW\_A\_UPPERF;
- Konfiguracja SW\_A\_LOWERF znajduje się Listing 6 – SW\_A\_LOWERF;

## **2.4.Technologie i protokoły wykorzystane w infrastrukturze sieciowej**

Podczas wdrażania projektu wykorzystano wiele współcześnie wykorzystywanych technologii sieci komputerowych. Poniżej omówione zostaną kluczowe z nich. Zdecydowana większość omówionych technologii zawiera się w zakresie certyfikacyjnym Cisco Certified Network Associate.

- Virtual Local Area Network (VLAN) to wirtualna sieć lokalna, która umożliwia podzielenie fizycznej sieci LAN na kilka logicznych sieci VLAN. Każda VLAN jest traktowana jako osobna sieć LAN. VLAN pozwala na zwiększenie wydajności sieci poprzez lepsze zarządzanie ruchem sieciowym oraz zapewnia lepsze bezpieczeństwo poprzez ograniczenie dostępu do pewnych zasobów sieciowych tylko dla uprawnionych użytkowników. Jest to szczególnie przydatne w dużych sieciach korporacyjnych, gdzie istnieje wiele oddzielnych grup użytkowników, które potrzebują dostępu do różnych zasobów sieciowych. Dodatkowo rozdzielanie urządzeń pomiędzy różne sieci VLAN wpływa na zmniejszenie ruchu rozgłoszeniowego;
- Inter-VLAN Routing (ang. routing między VLAN) to technologia sieciowa, która umożliwia komunikację pomiędzy różnymi VLAN w sieci LAN (ang. Local Area Network) przy wykorzystaniu routera bądź przełącznika wielkowarstwowego (przełącznika posiadającego zdolność do routingu pakietów). Router lub przełącznik bramowy pełni funkcję mostu pomiędzy różnymi VLAN, umożliwiając im wymianę danych. Realizacja routingu pomiędzy sieciami VLAN może odbywać się na kilka sposobów, lecz do najpopularniejszych zalicza się wykorzystanie interfejsów SVI (Switched Virtual Interface) w przełącznikach oraz metoda Router on a stick, w której to router przy pomocy tagowania dot1Q pozwala na komunikację ze sobą z założenia oddzielnych sieci wirtualnych;
- Gateway Load Balancing Protocol (GLBP) to protokół sieciowy, który służy do zwiększenia wydajności i niezawodności sieci poprzez równoważenie obciążenia między kilkoma routerami lub przełącznikami bramowymi (ang. gateway). Dzięki GLBP sieć może skorzystać z kilku niezależnych ścieżek dostępu do Internetu lub innych sieci, co pozwala na zwiększenie przepustowości oraz zmniejszenie ryzyka awarii sieci. GLBP działa na poziomie warstwy 3 sieciowej (ang. network layer) i umożliwia przydzielenie każdemu hostowi w sieci adresu IP wirtualnej bramy (ang. virtual IP address, VIP), który jest używany do komunikacji

z zewnętrzną siecią. Każdy router lub przełącznik bramowy w sieci GLBP ma przydzielony unikalny adres MAC wirtualnej bramy (ang. virtual MAC address, VMAC). Dzięki temu GLBP jest w stanie przekazywać ruch sieciowy między poszczególnymi urządzeniami w sposób dynamiczny, tak aby zapewnić równomierne rozłożenie obciążenia. Alternatywnymi protokołami, umożliwiającymi redundancję routingu, są protokoły HSRP oraz VRPP. Opracowanie własne na podstawie [1];

- EtherChannel to technologia sieciowa, która umożliwia łączenie kilku niezależnych interfejsów sieciowych w jeden wirtualny interfejs, co pozwala na zwiększenie przepustowości i niezawodności sieci. EtherChannel jest stosowany głównie w sieciach LAN (ang. Local Area Network) i WAN (ang. Wide Area Network) i może być wykorzystywany zarówno w sieciach opartych o przełączniki, jak i routery. EtherChannel umożliwia łączenie kilku fizycznych interfejsów sieciowych w jeden wirtualny interfejs, co pozwala na zwiększenie przepustowości sieci. W przypadku, gdy jedno z połączonych interfejsów ulegnie awarii, ruch sieciowy automatycznie jest przekierowywany przez pozostałe interfejsy, co zapewnia wysoką niezawodność sieci. EtherChannel wymaga odpowiedniego sprzętu sieciowego, takiego jak przełączniki lub routery, które są zdolne do obsługi tej technologii. W celu skonfigurowania EtherChannel należy skonfigurować odpowiednie interfejsy sieciowe oraz skonfigurować protokół komunikacyjny, taki jak Port Aggregation Protocol (PAgP) lub Link Aggregation Control Protocol (LACP). Opracowanie własne na podstawie [6];
- SSH (ang. Secure Shell) to protokół sieciowy służący do bezpiecznej komunikacji między komputerami za pośrednictwem sieci. SSH umożliwia zdalne zarządzanie komputerami poprzez udostępnienie dostępu do konsoli systemu operacyjnego zdalnego komputera. SSH jest często używany do zdalnego zarządzania serwerami oraz do zabezpieczania połączeń sieciowych przed nieupoważnionym dostępem. SSH używa mechanizmu szyfrowania danych, co pozwala na bezpieczną komunikację nawet w przypadku, gdy dane są przesyłane przez niezabezpieczone sieci. SSH umożliwia również uwierzytelnianie użytkowników za pomocą haseł lub kluczy publicznych, co zapewnia dodatkową ochronę przed nieupoważnionym dostępem do komputera;
- OSPF (ang. Open Shortest Path First) to protokół routingu wewnętrznego (ang. Interior Gateway Protocol, IGP), który służy do wymiany informacji o topologii sieci pomiędzy routerami w celu umożliwienia im podejmowania optymalnych decyzji dotyczących



przekazywania ruchu sieciowego. OSPF jest szczególnie przydatny w dużych sieciach, gdzie istnieje wiele różnych ścieżek między poszczególnymi urządzeniami sieciowymi. OSPF działa na poziomie warstwy 3 sieciowej (ang. network layer) i umożliwia routerom wymianę informacji o topologii sieci za pomocą specjalnych wiadomości routingu. Router OSPF może wymieniać te wiadomości z innymi routerami OSPF lub z hostami, które są skonfigurowane do obsługi OSPF. OSPF umożliwia routerom wybieranie optymalnych ścieżek dostępu do innych sieci za pomocą algorytmu Dijkstry, który uwzględnia koszty przekazywania ruchu sieciowego przez poszczególne interfejsy sieciowe. Dzięki temu OSPF jest w stanie zapewnić wysoką wydajność sieci oraz zmniejszyć ryzyko utraty ruchu sieciowego w przypadku awarii jednej z ścieżek dostępu. Routery, na których został uruchomiony protokół typu link state (np. OSPF, IS-IS), mają informacje nie tylko o swoich najbliższych sąsiadach, lecz również o stanie łącza sąsiadów i innych routerów w sieci. Każdy z routerów posiada więc pełną bazę informacji. Protokoły te wysyłają podczas aktualizacji dane dotyczące jedynie zmian, co ma znaczący wpływ na ilość przesyłanych danych, a co za tym idzie – na szybkość. Protokoły link state budują pełną topologię sieci, a więc routery wymieniają się konkretniejszymi i bardziej regularnymi informacjami;

- Rapid PVST (ang. Rapid Per VLAN Spanning Tree) to implementacja protokołu Spanning Tree Protocol (STP), która umożliwia zarządzanie topologią sieci LAN (ang. Local Area Network) i zapobiega występowaniu pętli sieciowych. Rapid PVST jest szczególnie przydatny w sieciach, gdzie istnieje wiele przełączników sieciowych i konieczne jest zapobieganie pętli sieciowych poprzez selektywne blokowanie niektórych interfejsów sieciowych. Rapid PVST działa na poziomie warstwy 2 sieciowej (ang. data link layer) i umożliwia przełącznikom sieciowym wymianę informacji o topologii sieci za pomocą specjalnych wiadomości STP. Dzięki temu przełączniki są w stanie wybrać optymalną ścieżkę dostępu do innych urządzeń sieciowych i zapobiec występowaniu pętli sieciowych poprzez blokowanie niektórych interfejsów. Rapid PVST tworzy osobne instancje dla różnych sieci VLAN na jednym przełączniku sieciowym. Dzięki temu przełącznik jest w stanie przekazywać ruch sieciowy pomiędzy różnymi VLAN za pomocą jednego interfejsu sieciowego, co pozwala na zwiększenie wydajności sieci. Opracowanie własne na podstawie [2].
- Spanning Tree Portfast to funkcja, która jest częścią protokołu Spanning Tree Protocol (STP) i umożliwia skrócenie czasu uruchamiania interfejsu sieciowego w przełączniku sieciowym. Kiedy interfejs sieciowy jest uruchamiany za pomocą Portfast, STP pomija

proces weryfikacji topologii sieci, który jest zazwyczaj wymagany dla interfejsów sieciowych. Dzięki temu interfejs jest gotowy do pracy znacznie szybciej niż w przypadku standardowego uruchamiania interfejsu. Funkcja PortFast powinna być uruchamiana jedynie na portach urządzeń końcowych w przełącznikach dostępowych;

- Spanning Tree BPDU Guard to funkcja, która jest częścią protokołu Spanning Tree Protocol (STP) i służy do ochrony interfejsów sieciowych przed nieautoryzowanymi wiadomościami STP (ang. BPDU, Bridge Protocol Data Units). Kiedy BPDU Guard jest włączony na interfejsie sieciowym, STP blokuje przychodzące wiadomości STP, które nie są autoryzowane przez administratora sieci. Dzięki temu możliwe jest zabezpieczenie interfejsów sieciowych przed nieautoryzowanymi zmianami topologii sieci, które mogą być spowodowane przez ataki hakerskie lub błędy konfiguracyjne;
- Switched Virtual Interface (SVI) to interfejs wirtualny, który służy do komunikacji pomiędzy różnymi urządzeniami sieciowymi znajdującymi się w tej samej podsieci sieci LAN (ang. Local Area Network). SVI jest tworzony przez przełącznik sieciowy i służy jako punkt końcowy dla ruchu sieciowego w danej podsieci. Dzięki temu możliwe jest przesyłanie ruchu sieciowego pomiędzy różnymi urządzeniami znajdującymi się w tej samej podsieci, nawet jeśli są one połączone z różnymi portami przełącznika sieciowego;
- Technologia stackowania switchy (ang. switch stacking) to sposób połączenia kilku przełączników sieciowych w jeden wirtualny przełącznik, który jest zarządzany jako jedno urządzenie. Stackowanie switchy umożliwia łączenie kilku przełączników sieciowych za pomocą specjalnych kabli stackowych i zarządzanie nimi jako jednym urządzeniem za pomocą jednego adresu IP. Wykorzystanie tej funkcjonalności w połączeniu z nadmiarowymi połączeniami i technologii Etherchannel pozwala skutecznie zabezpieczyć rdzeń sieci przed awarią jednego z urządzeń w stosie;
- Interfejs Loopback to wirtualny interfejs sieciowy, który może być tworzony na urządzeniach sieciowych bądź w systemach operacyjnych. Interfejsom Loopback na routerze można przypisać adresację sieciową oraz wykorzystywać je do symulacji rzeczywistej sieci Internet;
- DHCP (ang. Dynamic Host Configuration Protocol) to protokół sieciowy, który służy do automatycznego przydzielania adresów IP oraz innych parametrów sieciowych dla urządzeń podłączonych do sieci LAN (ang. Local Area Network). DHCP umożliwia urządzeniom sieciowym otrzymywanie adresu IP i innych parametrów sieciowych

od specjalnego serwera DHCP, zamiast ręcznego konfigurowania tych ustawień przez administratora sieci. DHCP działa w następujący sposób: urządzenie sieciowe oczekujące przydziału do sieci wysyła do serwera DHCP specjalne zapytanie o adres IP i inne parametry sieciowe. Serwer DHCP następnie przydziela adres IP i inne parametry sieciowe dla tego urządzenia i wysyła je z powrotem do urządzenia. Dzięki temu urządzenie jest w stanie automatycznie skonfigurować swoje parametry sieciowe i rozpocząć pracę w sieci. Do komunikacji serwer DHCP wykorzystuje port 67 UDP, zaś klient – port 68 UDP. Opracowanie własne na podstawie [3].

- Windows Active Directory (AD) to rozwiązanie firmy Windows oparte na protokole LDAP. Active Directory umożliwia tworzenie i zarządzanie użytkownikami, grupami i innymi obiektami sieciowymi za pomocą specjalnej bazy danych, która jest dostępna dla wszystkich urządzeń w sieci. Dzięki temu możliwe jest łatwe zarządzanie uprawnieniami dostępu do zasobów sieciowych i kontrola dostępu do nich przez poszczególnych użytkowników. Active Directory umożliwia również integrację z innymi usługami i rozwiązaniami sieciowymi, takimi jak DHCP (ang. Dynamic Host Configuration Protocol) czy DNS (ang. Domain Name System). Dzięki temu możliwe jest zarządzanie różnymi aspektami sieci w sposób centralny i uproszczony. Active Directory jest często używane w środowiskach serwerowych i służy do centralizowania zarządzania i kontroli dostępu do zasobów sieciowych, takich jak pliki, drukarki czy aplikacje. Z reguły protokół LDAP wykorzystuje port TCP/UDP o numerze 389;
- Obiekt Grupy Zasad (GPO)(ang. Group Policy Object) to zbiór ustawień kontrolujących konfigurację sieci. GPO są używane do zdefiniowania ustawień dla określonej grupy użytkowników lub komputerów w organizacji. Można ich użyć do konfiguracji szerokiego zakresu ustawień, w tym kontroli bezpieczeństwa i dostępu, instalacji i utrzymania oprogramowania oraz konfiguracji systemów i sieci.

GPO są przechowywane w centralnym miejscu, nazywanym kontenerem Grupy Zasad, który jest strukturą logiczną w usłudze Active Directory. GPO to ważne narzędzie dla administratorów do zarządzania i utrzymywania konfiguracji sieci. Pozwalają one administratorom na centralizację zarządzania ustawieniami i zmniejszenie czasu i wysiłku potrzebnego do ich utrzymania i aktualizacji;

### 3. Adresacja i podłączenia sieciowe

#### 3.1. Adresy sieciowe

Tabela 3.1.1 Adresy sieciowe. Opracowanie własne

Adres IP	Adres sieci	Maska podsieci	Podłączone urządzenie	Port urządzenia	Opis
12.73.61.1	12.73.61.0	/30	ROUTER_ISP	Serial0/0/0	Link ROUTER_MAIN
12.73.62.1	12.73.62.0	/30	ROUTER_ISP	Serial0/0/1	Link ROUTER_BACKUP
12.73.61.2	12.73.61.0	/30	ROUTER_MAIN	Serial0/0/0	Link ROUTER_ISP
12.73.62.2	12.73.61.0	/30	ROUTER_BACKUP	Serial0/0/0	Link ROUTER_ISP
3.3.3.3	3.0.0.0	/8	ROUTER_ISP	Loopback0	Symulowana sieć
4.4.4.4	4.0.0.0	/8	ROUTER_ISP	Loopback1	Symulowana sieć
10.5.1.1	10.5.1.0	/24	---	---	GLBP 5
10.5.1.2	10.5.1.0	/24	ROUTER_MAIN	FastEthernet0/0	GLBP 5
10.5.1.3	10.5.1.0	/24	ROUTER_BACKUP	FastEthernet0/0	GLBP 5
10.5.1.5	10.5.1.0	/24	SW_CORE_STACK	VLAN5	SVI VLAN GLBP 5
10.5.1.10	10.5.1.0	/24	ADMIN PC	GigabitEthernet1/0/7	Management PC
10.6.1.1	10.6.1.0	/24	---	---	GLBP 6
10.6.1.2	10.6.1.0	/24	ROUTER_MAIN	FastEthernet0/1	GLBP 6
10.6.1.3	10.6.1.0	/24	ROUTER_BACKUP	FastEthernet0/1	GLBP 6
10.6.1.5	10.6.1.0	/24	SW_CORE_STACK	VLAN6	SVI VLAN GLBP 6
192.168.7.1	192.168.7.0	/28	SW_CORE_STACK	VLAN7	SVI VLAN SERVERS
192.168.7.10	192.168.7.0	/28	WINSRV01	VLAN7	Windows Server 2016
192.168.7.12	192.168.7.0	/28	WINSRV02	VLAN7	Windows Server 2016
192.168.10.1	192.168.10.0	/29	SW_CORE_STACK	VLAN10	SVI VLAN BOSS
192.168.20.1	192.168.20.0	/24	SW_CORE_STACK	VLAN20	SVI VLAN SALES
192.168.30.1	192.168.30.0	/24	SW_CORE_STACK	VLAN30	SVI VLAN PM
192.168.40.1	192.168.40.0	/24	SW_CORE_STACK	VLAN40	SVI VLAN HR
192.168.50.1	192.168.50.0	/24	SW_CORE_STACK	VLAN50	SVI VLAN ICT
192.168.60.1	192.168.60.0	/28	SW_CORE_STACK	VLAN60	SVI VLAN PRINTERS
192.168.70.1	192.168.70.0	/24	SW_CORE_STACK	VLAN70	SVI VLAN GRAPHICS
192.168.119.3	192.168.119.0	/24	SW_CORE_STACK	VLAN119	Zdalne połączenie SSH
192.168.119.4	192.168.119.0	/24	SW_A_UPPERF	VLAN119	Zdalne połączenie SSH
192.168.119.5	192.168.119.0	/24	SW_A_LOWERF	VLAN119	Zdalne połączenie SSH

### 3.2. Sieci Virtual LAN (VLAN)

W celu odseparowania od siebie działów oraz zmniejszenia ilości pakietów rozgłoszeniowych zostały wykorzystane sieci VLAN. Nadanie odpowiednim podsięciom adresacji na podstawie ich numeru VLAN pozwala osiągnąć przejrzystość i zwiększyć szybkość pracy. Tabela podziałów sieci znajduje się poniżej.

Tabela 3.2.1 Wykorzystywane sieci VLAN. Opracowanie własne

Numer VLAN	Nazwa	Przeznaczenie
5	GLBP5	Komunikacja core switch z routerami
6	GLBP6	Komunikacja core switch z routerami
7	SERVERS	Urządzenia serwerowe i monitorujące
10	BOSS	Dział zarządczy i kierowniczy
20	SALES	Dział sprzedaży i marketingu
30	PM	Dział Project Managera
40	HR	Dział Human Resources
50	ICT	Dział informatyczny
60	PRINTERS	Drukarki
70	GRAPHICS	Dział grafiki komputerowej i animacji
100	GUEST	Odizolowana sieć gościnna
127	---	Natywna sieć vlan
999	DUMMY	Sieć "czarna dziura"
119	SSH	Do podłączenia zdalnego przez SSH

### 3.3. Fizyczne podłączenia urządzeń sieciowych

Tabela 3.3.1 Fizyczne podłączenia - ROUTER\_ISP. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
FastEthernet0/0	---	---	---
FastEthernet0/1	---	---	---
FastEthernet0/1/0	---	---	---
FastEthernet0/1/1	---	---	---
FastEthernet0/1/2	---	---	---
FastEthernet0/1/3	---	---	---
Serial0/0/0	---	ROUTER_MAIN	---
Serial0/0/1	---	ROUTER_BACKUP	---
Loopback0	---	---	Symulowana sieć
Loopback1	---	---	Symulowana sieć

Tabela 3.3.2 Fizyczne podłączenia - ROUTER\_MAIN. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
FastEthernet0/0	5	SW_CORE_TOP	GLBP 5
FastEthernet0/1	6	SW_CORE_BOTTOM	GLBP 6
FastEthernet0/1/0		---	---
FastEthernet0/1/1		---	---
FastEthernet0/1/2		---	---
FastEthernet0/1/3		---	---
Serial0/0/0		ROUTER_ISP	---
Serial0/0/1		---	---

Tabela 3.3.3 Fizyczne podłączenia - ROUTER\_BACKUP. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
FastEthernet0/0	5	SW_CORE_TOP	GLBP 5
FastEthernet0/1	6	SW_CORE_BOTTOM	GLBP 6
FastEthernet0/1/0		---	---
FastEthernet0/1/1		---	---
FastEthernet0/1/2		---	---
FastEthernet0/1/3		---	---
Serial0/0/0		ROUTER_ISP	---
Serial0/0/1		---	---

Tabela 3.3.4 Fizyczne podłączenia - SW\_CORE. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
GigabitEthernet1/0/1	6	ROUTER_MAIN	---
GigabitEthernet1/0/2	6	ROUTER_BACKUP	---
GigabitEthernet1/0/3	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/4	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/5	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/6	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/7	5	ADMIN PC	Management PC
GigabitEthernet1/0/8	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/9	trunk	SW_A_UPPERF	Etherchannel 2
GigabitEthernet1/0/10	trunk	SW_A_UPPERF	Etherchannel 2
GigabitEthernet1/0/11	trunk	SW_A_LOWERF	Etherchannel 3
GigabitEthernet1/0/12	trunk	SW_A_LOWERF	Etherchannel 3
GigabitEthernet1/0/13	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/14	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/15	7	WIN-SERVER01	NIC Teaming - LACP - Etherchannel 4
GigabitEthernet1/0/16	7	WIN-SERVER02	NIC Teaming - LACP - Etherchannel 5
GigabitEthernet1/0/17	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/18	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/19	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/20	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/21	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/22	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/23	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet1/0/24	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/1	5	ROUTER_MAIN	---
GigabitEthernet2/0/2	5	ROUTER_BACKUP	---
GigabitEthernet2/0/3	---	---	---
GigabitEthernet2/0/4	---	---	---
GigabitEthernet2/0/5	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/6	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/7	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/8	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/9	trunk	SW_A_UPPERF	Etherchannel 2
GigabitEthernet2/0/10	trunk	SW_A_UPPERF	Etherchannel 2
GigabitEthernet2/0/11	trunk	SW_A_LOWERF	Etherchannel 3
GigabitEthernet2/0/12	trunk	SW_A_LOWERF	Etherchannel 3
GigabitEthernet2/0/13	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/14	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/15	7	WIN-SERVER01	NIC Teaming - LACP - Etherchannel 4
GigabitEthernet2/0/16	7	WIN-SERVER02	NIC Teaming - LACP - Etherchannel 5
GigabitEthernet2/0/17	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/18	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/19	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/20	---	---	Zarezerwowane na potrzeby rozwoju

GigabitEthernet2/0/21	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/22	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/23	---	---	Zarezerwowane na potrzeby rozwoju
GigabitEthernet2/0/24	---	---	Zarezerwowane na potrzeby rozwoju

Tabela 3.3.5 Fizyczne połączenia - SW\_A\_UPPERF. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
FastEthernet0/1	trunk	SW_CORE_STACK	Etherchannel 2
FastEthernet0/2	trunk	SW_CORE_STACK	Etherchannel 2
FastEthernet0/3	trunk	SW_CORE_STACK	Etherchannel 2
FastEthernet0/4	trunk	SW_CORE_STACK	Etherchannel 2
FastEthernet0/5	10	Urządzenie końcowe	BOSS
FastEthernet0/6	10	Urządzenie końcowe	BOSS
FastEthernet0/7	10	Urządzenie końcowe	BOSS
FastEthernet0/8	60	Drukarka	---
FastEthernet0/9	20	Urządzenie końcowe	SALES
FastEthernet0/10	20	Urządzenie końcowe	SALES
FastEthernet0/11	20	Urządzenie końcowe	SALES
FastEthernet0/12	20	Urządzenie końcowe	SALES
FastEthernet0/13	30	Urządzenie końcowe	PM
FastEthernet0/14	30	Urządzenie końcowe	PM
FastEthernet0/15	50	Urządzenie końcowe	ICT
FastEthernet0/16	50	Urządzenie końcowe	ICT
FastEthernet0/17	50	Urządzenie końcowe	ICT
FastEthernet0/18	50	Urządzenie końcowe	ICT
FastEthernet0/19	50	Urządzenie końcowe	ICT
FastEthernet0/20	50	Urządzenie końcowe	ICT
FastEthernet0/21	50	Urządzenie końcowe	ICT
FastEthernet0/22	50	Urządzenie końcowe	ICT
FastEthernet0/23	50	Urządzenie końcowe	ICT
FastEthernet0/24	60	Drukarka	---



Tabela 3.3.6 Fizyczne połączenia - SW\_A\_LOWERF. Opracowanie własne

Port	VLAN	Podłączone urządzenie	Opis
FastEthernet0/1	trunk	SW_CORE_STACK	Etherchannel 3
FastEthernet0/2	trunk	SW_CORE_STACK	Etherchannel 3
FastEthernet0/3	trunk	SW_CORE_STACK	Etherchannel 3
FastEthernet0/4	trunk	SW_CORE_STACK	Etherchannel 3
FastEthernet0/5	40	Urządzenie końcowe	HR
FastEthernet0/6	40	Urządzenie końcowe	HR
FastEthernet0/7	40	Urządzenie końcowe	HR
FastEthernet0/8	40	Urządzenie końcowe	HR
FastEthernet0/9	50	Urządzenie końcowe	ICT
FastEthernet0/10	50	Urządzenie końcowe	ICT
FastEthernet0/11	50	Urządzenie końcowe	ICT
FastEthernet0/12	50	Urządzenie końcowe	ICT
FastEthernet0/13	50	Urządzenie końcowe	ICT
FastEthernet0/14	50	Urządzenie końcowe	ICT
FastEthernet0/15	50	Urządzenie końcowe	ICT
FastEthernet0/16	50	Urządzenie końcowe	ICT
FastEthernet0/17	50	Urządzenie końcowe	ICT
FastEthernet0/18	50	Urządzenie końcowe	ICT
FastEthernet0/19	50	Urządzenie końcowe	ICT
FastEthernet0/20	70	Urządzenie końcowe	GRAPHICS
FastEthernet0/21	70	Urządzenie końcowe	GRAPHICS
FastEthernet0/22	70	Urządzenie końcowe	GRAPHICS
FastEthernet0/23	70	Urządzenie końcowe	GRAPHICS
FastEthernet0/24	60	Drukarka	---

## 4. Wybrane technologie sieciowe i metody zabezpieczania sieci w warstwie 2

### 4.1. Technologia stackowania przełączników

Technika łączenia kluczowych elementów sieci we wszelakiego rodzaju stosy czy klastry jest szeroko wykorzystywana. W obecnych sieciach za wszelką cenę należy unikać sytuacji braku dostępności do usług. W przełącznikach Cisco od serii 3750 wzwyż istnieje możliwość połączenia przełączników specjalnym okablowaniem, co pozwala na wzajemne zwiększenie przepustowości, zaś wszystkie przełączniki podłączone szeregowo kablem konsolowym pracują logicznie jako jedno urządzenie. Ułatwia to konfigurację oraz wpływa pozytywnie na ilość dostępnych fizycznych portów w przełączniku, gdyż przełączniki warstwy rdzenia nie muszą być ze sobą połączone okablowaniem w trybie trunk.

W stos można łączyć maksymalnie 9 urządzeń, o ile posiadają specjalny port oraz urządzenia pracują pod kontrolą tego samego systemu operacyjnego IOS.

```
SW_CORE#sh switch stack-ports summary
```

Switch#/Port#	Stack Port Status	Neighbor	Cable Length	Link OK	Link Active	Sync OK	# Changes To LinkOK	In Loopback
1/1	OK	2	50 cm	Yes	Yes	Yes	1	No
1/2	OK	2	50 cm	Yes	Yes	Yes	1	No
2/1	OK	1	50 cm	Yes	Yes	Yes	1	No
2/2	OK	1	50 cm	Yes	Yes	Yes	1	No

```
SW_CORE#sh switch stack-ring speed
SW_CORE#sh switch stack-ring speed

Stack Ring Speed      : 32G
Stack Ring Configuration: Full
Stack Ring Protocol    : StackWise
SW_CORE#sh switch stack-ring ac

Sw  Frames sent to stack ring (approximate)
-----
1      203773
2      250558

Total frames sent to stack ring : 454331

Note: these counts do not include frames sent to the ring
by certain output features, such as output SPAN and output
ACLs.

SW_CORE#sh switch
Switch/Stack Mac Address : 0016.47af.5600
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
1	Member	0011.bb7e.5700	1	0	Ready
*2	Master	0016.47af.5600	12	0	Ready

Rysunek 4.1.1 Widok stosu przełączników SW\_CORE. Opracowanie własne

## 4.2. Technologia logicznej agregacji łączy

Technologia łączenia portów została szerzej opisana w rozdziale „Technologie i protokoły wykorzystane w infrastrukturze sieciowej”. Wartym przypomnienia są tryby agregacji łączy:

- PAgP – protokół własnościowy firmy Cisco
- LACP – protokół otwarty, szeroko wykorzystywany i implementowany

Etherchannel jest nazewnictwem wykorzystywanym w nomenklaturze Cisco i oznacza dokładnie to samo co LAG (Link aggregation). LAG zezwala na łączne zwiększenie przepustowości, dzięki czemu 4 interfejsy spięte w PAgP/LACP pracujące w trybie Full-Duplex FastEthernet, osiągną prędkość 400mbps, zamiast standardowych 100mbps.

Etherchannel może pracować w kilku trybach, które zostały opisane w tabeli poniżej.

Tabela 4.2.1 Możliwe ustawienia EtherChannel. Opracowanie własne na podstawie [6]

Tryby działania interfejsów w EtherChannel		
Tryb	Protokół	Opis
Auto	PAgP	Interfejs nie negocjuje aktywnie wymiany pakietów PaGP
Desirable	PAgP	Interfejs aktywnie dąży do wymiany pakietów PaGP
On	EtherChannel	Nie następuje negocjacja. Wymusza włączenie połączeń
Active	LACP	Interfejs aktywnie dąży do wymiany pakietów LACP
Passive	LACP	Interfejs nie negocjuje aktywnie wymiany pakietów LACP

```
SW_CORE#sh etherchannel summary
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

Number of channel-groups in use: 4
Number of aggregators:          4

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
2      Po2 (SU)      LACP        Gi1/0/9 (P) Gi1/0/10 (P) Gi2/0/9 (P)
                          Gi2/0/10 (P)
3      Po3 (SU)      LACP        Gi1/0/11 (P) Gi1/0/12 (P) Gi2/0/11 (P)
                          Gi2/0/12 (P)
4      Po4 (SD)      LACP        Gi1/0/15 (D) Gi2/0/15 (I)
5      Po5 (SD)      LACP        Gi1/0/16 (I) Gi2/0/16 (D)
```

Rysunek 4.2.1 Podsumowanie agregacji LAG dla SW\_CORE. Opracowanie własne

### 4.3. Port Security

Technologia Port Security jest mechanizmem bezpieczeństwa opierającym się na dopuszczaniu lub blokowaniu ruchu dla urządzeń. Mechanizm uruchamia się na portach przeznaczonych głównie dla urządzeń końcowych w celu ograniczenia możliwości podłączenia urządzenia nieuprawnionego. Port Security umożliwia określenie adresów MAC, w sposób statyczny lub dynamiczny, które mogą komunikować się na danym interfejsie przełącznika. Przy użyciu odpowiednich komend można dostosować wiele parametrów dotyczących mechanizmu „Port Security”. W przypadku wdrożenia dla firmy zostały zastosowane następujące ustawienia:

- Na interfejsie zapisywane są maksymalnie 3 adresy MAC dopuszczone do komunikacji;
- Ustawienie „aging time” wynosi 30 minut;
- Odliczanie „aging time” rozpoczyna się w momencie wykrycia nieaktywności na interfejsie;
- Adresy mogą być przypisywane dynamicznie;
- W przypadku naruszenia klauzuli bezpieczeństwa następuje blokada portu, zaś zdarzenie zostanie zarejestrowane w logach.

Dodatkowym, użytecznym mechanizmem bezpieczeństwa, wykorzystywanym często wraz z instancjami mechanizmów STP (ang. Spanning-Tree Protocol) oraz Port Security jest zabezpieczenie BPDU Guard. W momencie otrzymania ramki BPDU na nieuprawnionym porcie (komenda spanning-tree bpduguard enable) port przechodzi w tryb err-disable. Ramki BPDU generowane są poprzez przełączniki w związku z działaniem protokołu STP, dlatego mechanizm ten powinien zablokować nielegalnie podłączone przełączniki bądź urządzenia udające te urządzenia.

#### 4.4. DHCP Snooping

DHCP Snooping jest mechanizmem obrony przed DHCP Spoofing. DHCP Spoofing może być wykorzystywany przez nieuczciwe serwery DHCP do podawania klientom maszyny atakującego jako fałszywej bramy domyślnej w celu przekierowania ich ruchu przez atakującego (Man-in-the-middle attack, MITM). Może być również wykorzystany jako atak typu Denial of Service w celu nadania klientom nieprawidłowych ustawień adresów IP. Może to być zrobione złośliwie przez atakującego, może też łatwo zdarzyć się przypadkowo, jeśli do sieci zostanie dodane jakiegokolwiek urządzenie obsługujące usługi DHCP.

W implementacji mechanizmu obronnego dla Cisco administrator ma za zadanie określić interfejsy sieciowe jako zaufane lub niezaufane.

Porty podłączone do serwerów DHCP, oraz porty łączące przełączniki ze sobą (w celu umożliwienia przejścia ruchu między klientami a serwerem DHCP) powinny być skonfigurowane jako zaufane.

- Na portach zaufanych wiadomości DHCP nie są filtrowane;
- na portach niezaufanych wiadomości od serwerów DHCP są zawsze odrzucane;
- na portach niezaufanych wiadomości od klientów DHCP są monitorowane pod kątem potencjalnych ataków.

Wiadomości DISCOVER i REQUEST są sprawdzane pod kątem zgodności adresów MAC pomiędzy ramką Ethernet a wiadomością DHCP, zaś wiadomości RELEASE i DECLINE są sprawdzane w tabeli wiązań DHCP Snooping pod kątem zgodności adresu IP i interfejsu. Jeśli host zażądał adresu IP przez jeden interfejs, a później przełącznik otrzyma wiadomość RELEASE/DECLINE dla tego samego adresu IP, ale na innym interfejsie, przefiltruje tę ostatnią wiadomość, ponieważ jest ona prawdopodobnie od złośliwego hosta, który próbuje oszukać serwer DHCP, aby zakończyć dzierżawę adresu IP dla legalnego hosta.

Dodatkowo DHCP Snooping może stosunkowo mocno obciążać procesor urządzeń aktywnych, dlatego zaleca się ograniczenie ilości przychodzących wiadomości DHCP na interfejs, aby zapobiec atakom DoS. W wypadku przekroczenia określonego limitu port przechodzi w stan err-disabled.

#### **4.5. Dynamic ARP Inspection (DAI)**

DAI jest mechanizmem obrony przed atakami ARP Poisoning. W przypadku ataków ARP Poisoning, atakujący oszukuje hosty, aby uwierzyły, że adres IP jest powiązany z adresem MAC atakującego, a nie legalnym adresem MAC celu. Może to być wykorzystane jako atak typu Man-In-The-Middle lub Denial of Service. Atakujący wysyła niepotrzebne wiadomości ARP z własnym adresem MAC i adresem IP ofiary. Jeśli atak się powiedzie, inne hosty będą wysyłać ruch przeznaczony dla ofiary do atakującego zamiast niego. DAI wykorzystuje tablicę wiązań DHCP tworzoną przez DHCP Snooping, która posiada listę, jaki adres IP został przypisany do jakiego adresu MAC przez DHCP. Dla hostów nie korzystających z DHCP można dodać wpisy statyczne.

Jeśli dany host wysłał wiadomości DHCP na jeden port, to powinien tam pozostać i wszystkie wiadomości ARP powinny iść przez ten sam port. Wiadomości ARP idące przez inne porty są odrzucane, chyba że porty te są zaufane.

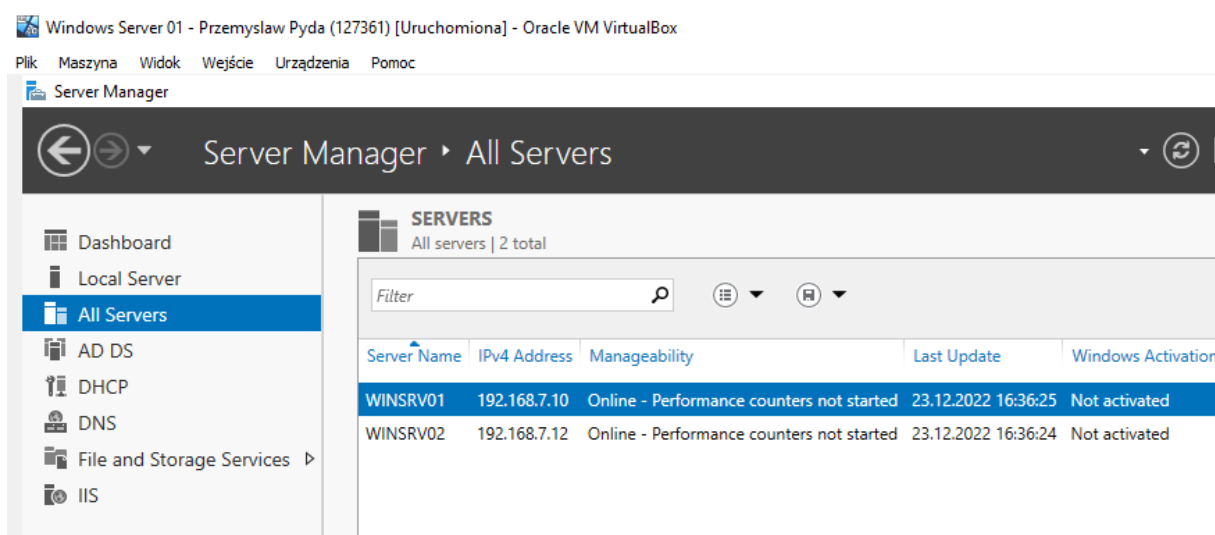
Podobnie jak w przypadku mechanizmu DHCP Snooping, funkcjonalność DAI może być obciążająca dla urządzenia, dlatego sugerowane jest wykorzystanie limitu operacji „arp inspection”. Dodatkowo DAI sprawdza wszystkie ramki ARP w celu weryfikacji ich poprawności i odrzuca niepoprawne lub potencjalnie niebezpieczne ramki.

## 5. Mechanizmy i protokoły Windows Server

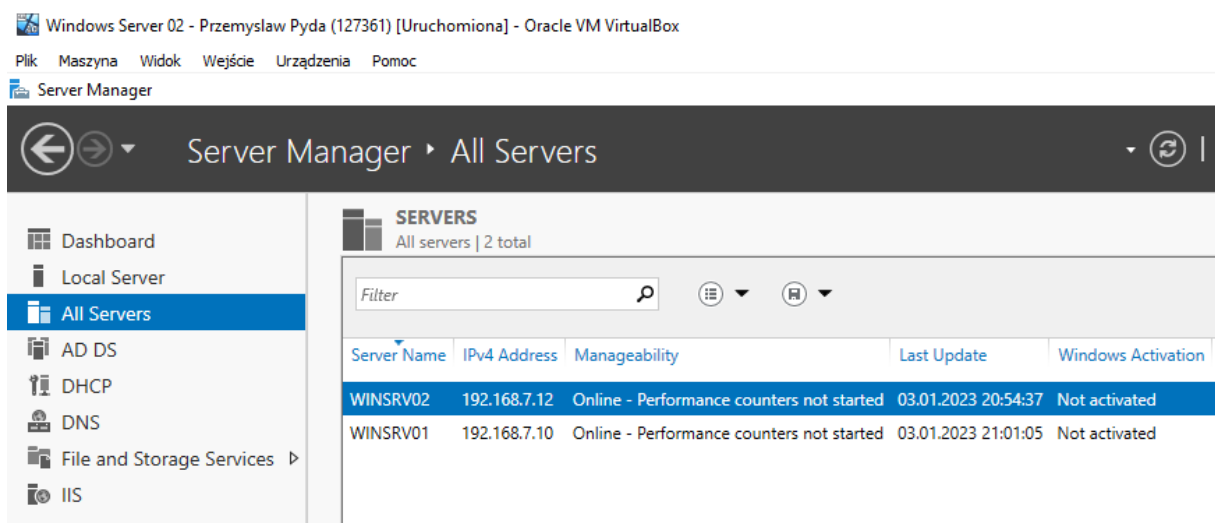
### 5.1. Serwery lokalne Windows Server

W infrastrukturze za zadania serwerowe odpowiedzialne są dwa fizyczne, niezależne sprzętowo komputery pracujące pod systemem Windows Server 2016 Standard. Komputery te są wirtualizowane przy pomocy hipernadzorcy (ang. Hypervisor) typu drugiego, jakim jest oprogramowanie Oracle VM VirtualBox w wersji 7.0.4.

Każda z maszyn wirtualnych ma przypisane 4GB pamięci operacyjnej, 2 wirtualne rdzenie procesora oraz 30GB dynamicznie alokowanego miejsca na dysku twardym. 2 wirtualne karty sieciowe działają w trybie mostka (ang. Bridge), co pozwala jej na fizyczny dostęp do karty sieciowej zamontowanej w komputerze w Sali 108INF.



Rysunek 5.1.1 Widok "All Servers" dla maszyny WINSRV01. Opracowanie własne

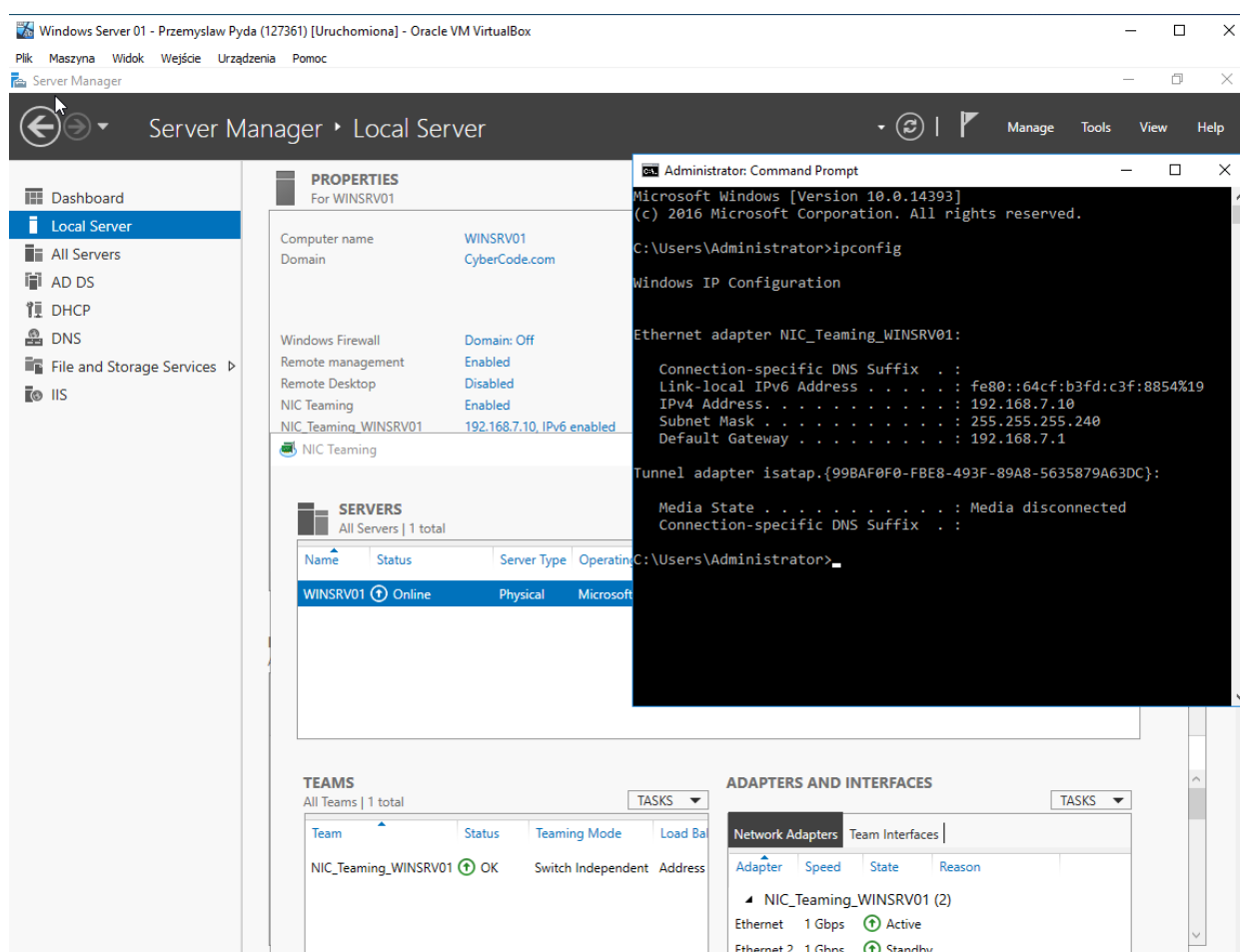


Rysunek 5.1.2 Widok "All Servers" dla maszyny WINSRV02. Opracowanie własne

## 5.2.Redundancja kart sieciowych w Windows Server

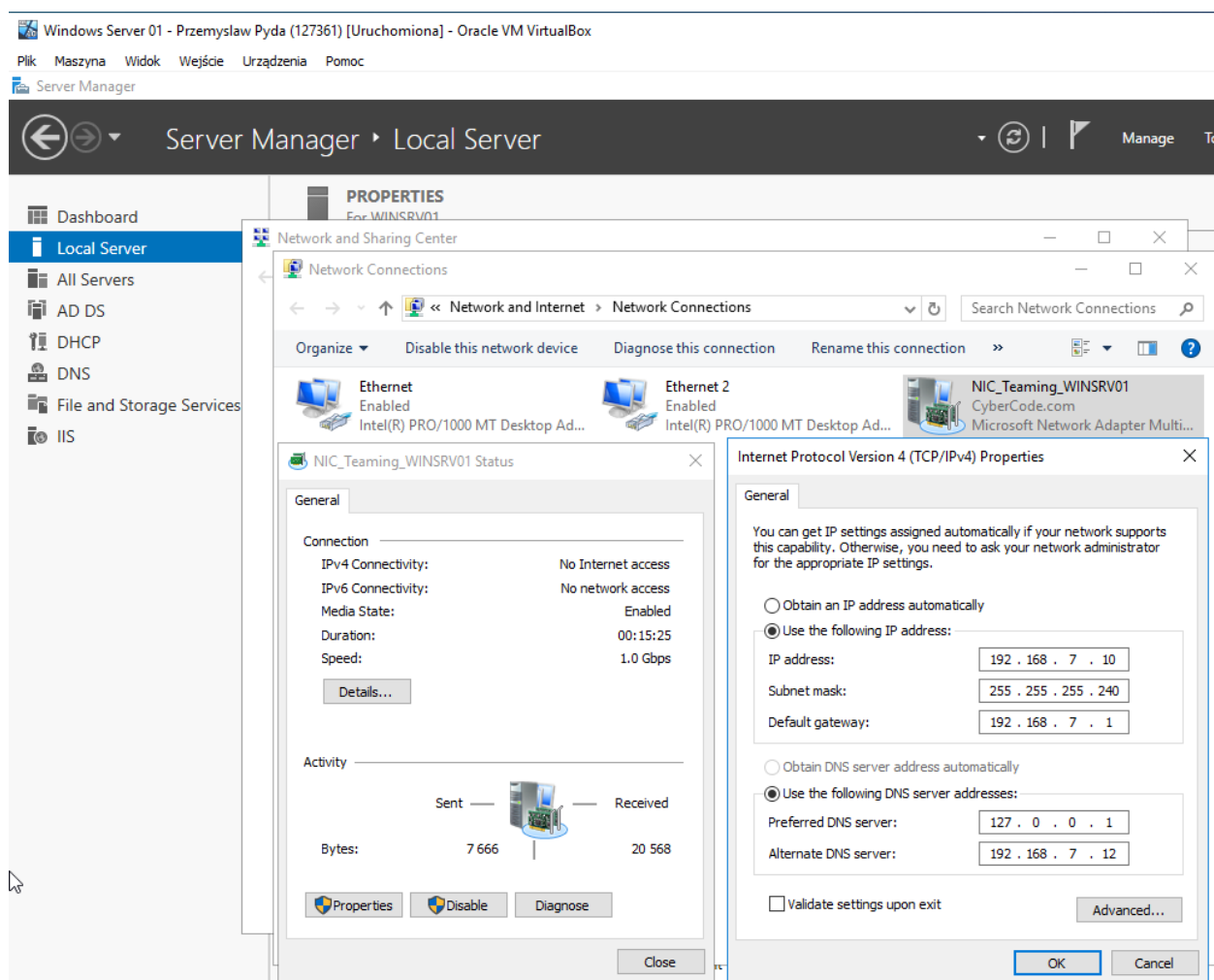
W celu zmniejszenia awaryjności i zwiększenia redundancji karty sieciowej Windows Server bądź jednego członka ze stacku przełączników warstwy core wykorzystana jest funkcjonalność grupowania kart sieciowych w trybie NIC Teaming.

Karty działają w trybie „Switch Independent”, gdzie karta sieciowa podłączona do górnego przełącznika SW\_CORE pracuje w trybie „Active”, zaś druga karta sieciowa, będąca podłączoną do drugiego, dolnego przełącznika SW\_CORE, działa w trybie „Standby”. W wypadku awarii preferowanej karty sieciowej bądź górnego członka stacku następuje przełączenie ruchu sieciowego na zapasową kartę sieciową. Podczas korzystania z wirtualnych kart sieciowych w środowisku Oracle VM VirtualBox nie można zastosować kart sieciowych działających w trybie równoważenia obciążenia lub LACP. Podczas fizycznie instalowanego oprogramowania Windows Server preferowane ustawienia powinny różnić się od tych zaprezentowanych na poniższych zrzutach ekranu.



Rysunek 5.2.1 Konfiguracja nadmiarowych kart sieciowych. Opracowanie własne

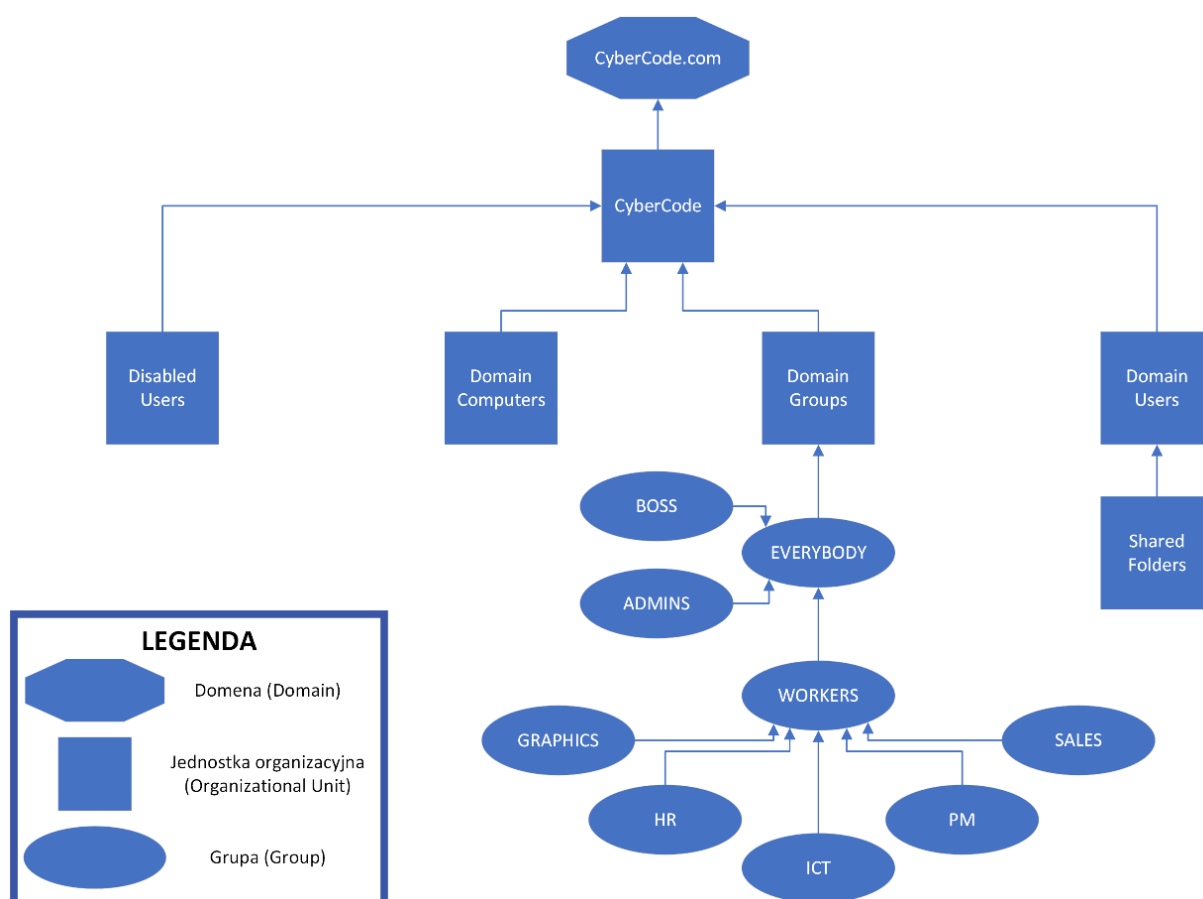




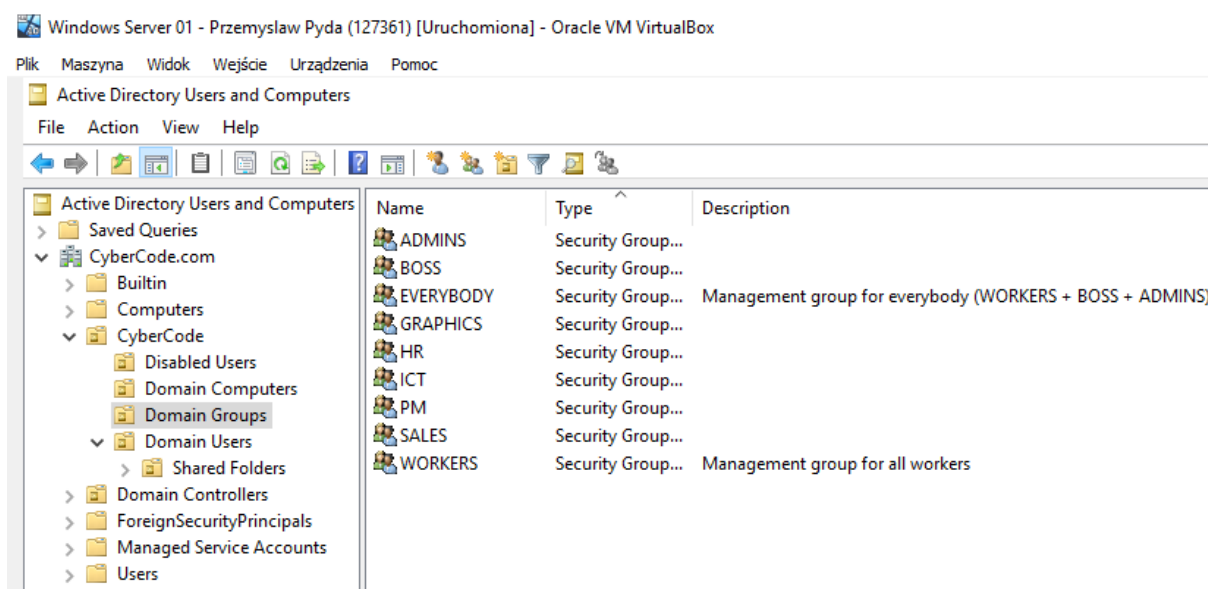
Rysunek 5.2.2 Konfiguracja adresu NIC Teaming. Opracowanie własne

### 5.3. Struktura organizacyjna firmy CyberCode.com – Grupy i Użytkownicy

W celu zarządzania firmą poprzez środowisko serwerowe Windows Server 2016 konieczne było zorganizowanie poszczególnych grup, użytkowników i komputerów w konkretne logiczne jednostki. Struktura przedstawiona jest na zrzucie ekranu poniżej ze szczególnym uwzględnieniem grup, będących odpowiednikiem działów w firmie. Każda utworzona grupa jest grupą bezpieczeństwa, dzięki czemu będzie można przypisywać do niej Obiekty Zasad Grupy (ang. GPO – Group Policy Object).



Rysunek 5.3.1 Struktura organizacyjna firmy CyberCode. Opracowanie własne



Rysunek 5.3.2 Widok "Domain Groups". Opracowanie własne

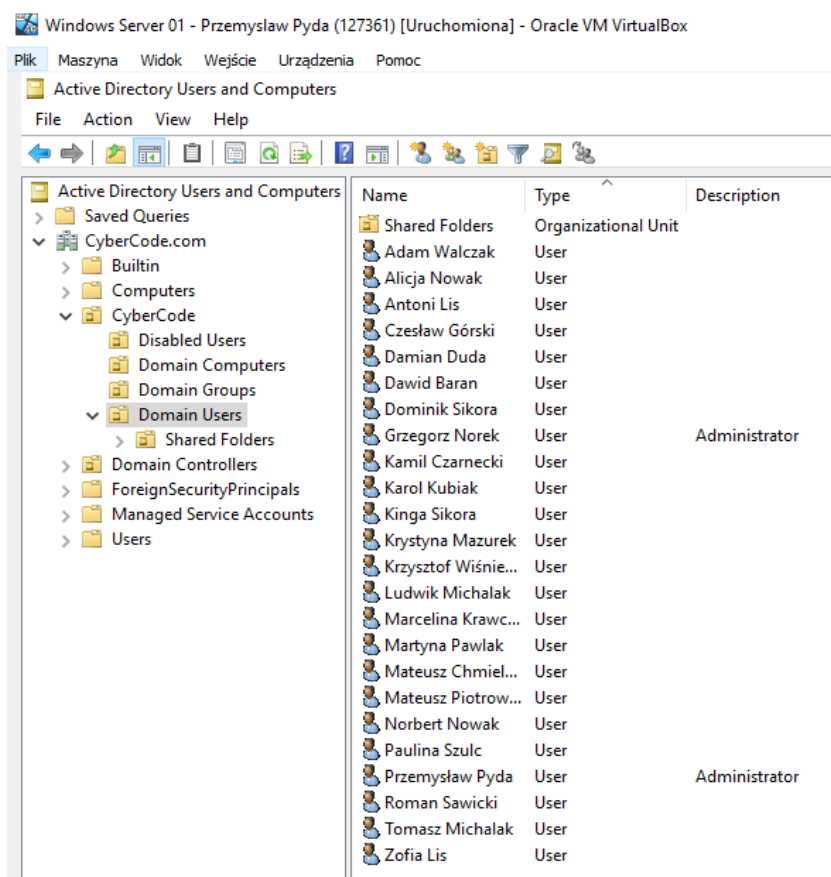
Administratorzy systemu utworzyli konta użytkowników w jednostce organizacyjnej Domain Users i przypisali ich do odpowiadającej im grupy w jednostce organizacyjnej Domain Groups. Przy pierwszym logowaniu na konto, istnieje wymóg zmiany domyślnego hasła CberC@de na inne hasło, spełniające wymogi polityki bezpiecznych haseł.

Dla każdego użytkownika na podstawie jego imienia i nazwiska tworzony zostaje identyfikator konta według następującego szablonu: Nazwisko.Imię z pominięciem polskich znaków, czyli dla użytkownika Czesław Górski utworzona nazwa użytkownika to Gorski.Czeslaw. Nazwy użytkowników muszą być unikalne i z założenia niezmiennie.

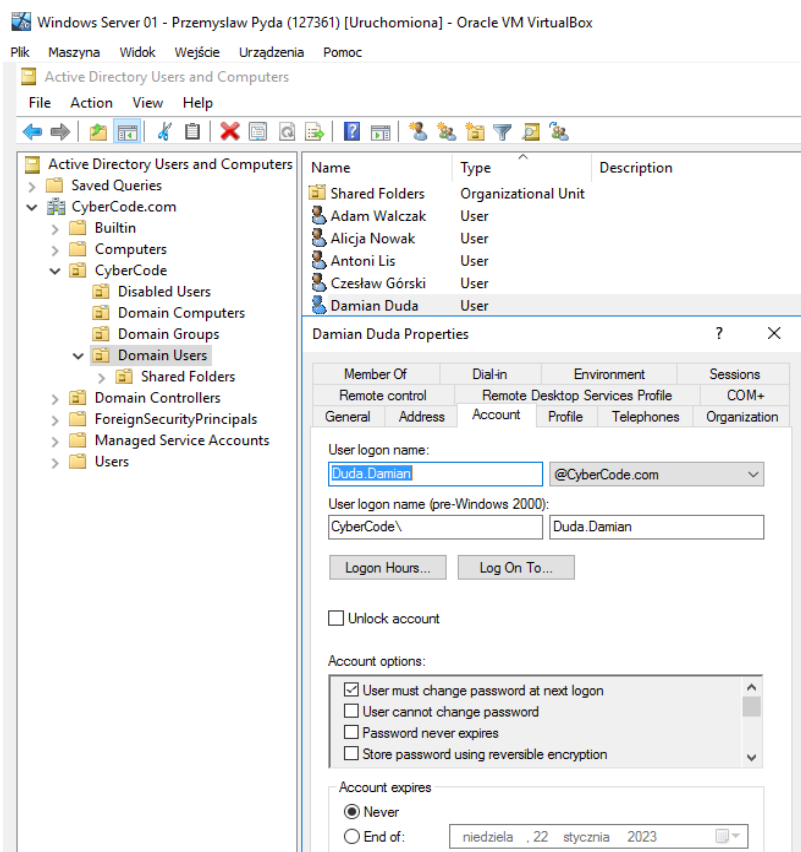
Lista użytkowników wraz z uwzględnieniem grupy, do której należą, znajduje się poniżej.

Tabela 5.3.1 Użytkownicy domenowi. Opracowanie własne

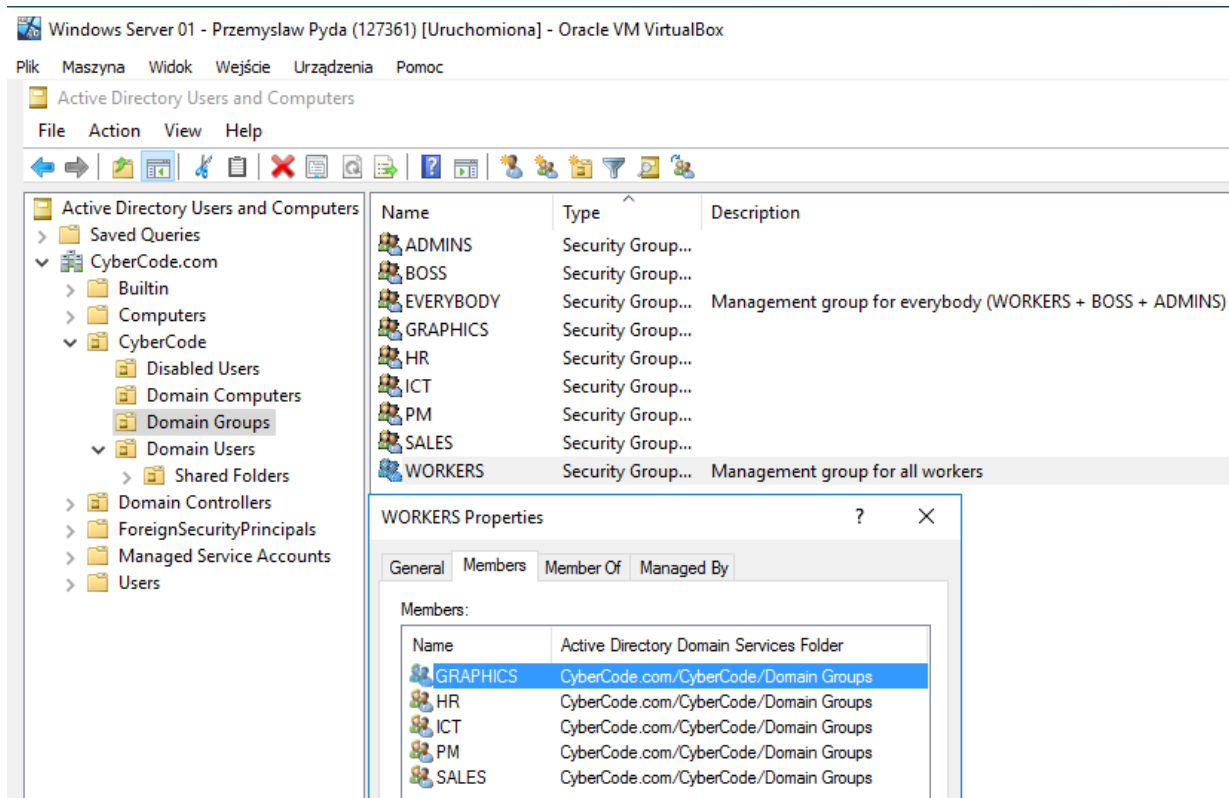
Imię i nazwisko	Hasło	Nazwa logowania	Grupa
Przemysław Pyda	\$InzPydzik00	Pyda.Przemyslaw	ADMINS
Grzegorz Norek	\$InzN0rek005	Norek.Grzegorz	ADMINS
Mateusz Chmielewski	CberC@de	Chmielewski.Mateusz	BOSS
Mateusz Piotrowski	CberC@de	Piotrowski.Mateusz	BOSS
Dominik Sikora	CberC@de	Sikora.Dominik	ICT
Krzysztof Wiśniewski	CberC@de	Wisniewski.Krzysztof	ICT
Karol Kubiak	CberC@de	Kubiak.Karol	ICT
Czesław Górski	CberC@de	Gorski.Czeslaw	ICT
Roman Sawicki	CberC@de	Sawicki.Roman	ICT
Antoni Lis	CberC@de	Lis.Antoni	GRAPHICS
Kamil Czarnecki	CberC@de	Czarnecki.Kamil	GRAPHICS
Damian Duda	CberC@de	Duda.Damian	SALES
Dawid Baran	CberC@de	Baran.Dawid	SALES
Ludwik Michalak	CberC@de	Michalak.Ludwik	SALES
Adam Walczak	CberC@de	Walczak.Adam	SALES
Norbert Nowak	CberC@de	Nowak.Norbert	PM
Marcelina Krawczyk	CberC@de	Krawczyk.Marcelina	PM
Alicja Nowak	CberC@de	Nowak.Alicja	BOSS
Paulina Szulc	CberC@de	Szulc.Paulina	HR
Kinga Sikora	CberC@de	Sikora.Kinga	HR
Krystyna Mazurek	CberC@de	Mazurek.Krystyna	HR
Martyna Pawlak	CberC@de	Pawlak.Martyna	HR
Zofia Lis	CberC@de	Lis.Zofia	GRAPHICS
Tomasz Michalak	CberC@de	Michalak.Tomasz	ICT



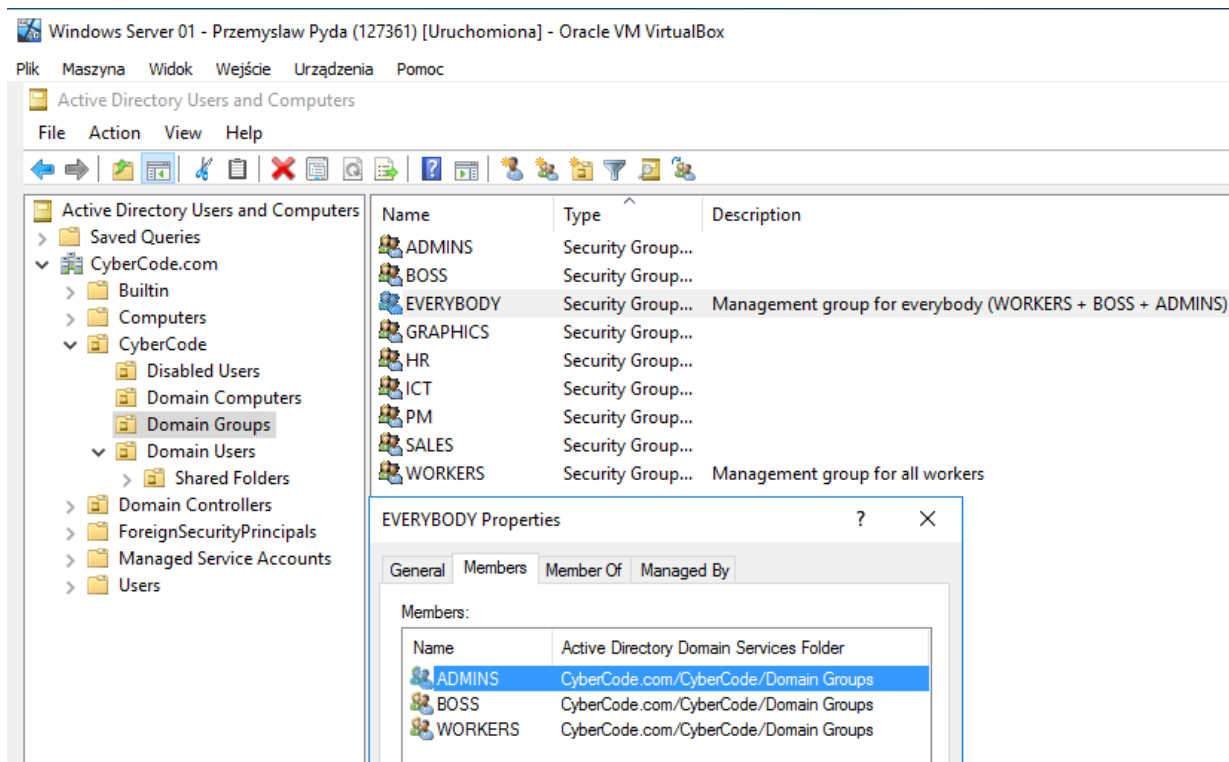
Rysunek 5.3.3. Widok "Domain Users". Opracowanie własne



Rysunek 5.3.4 Widok właściwości dla użytkownika domenowego. Opracowanie własne



Rysunek 5.3.5 Widok właściwości członków grupy WORKERS. Opracowanie własne



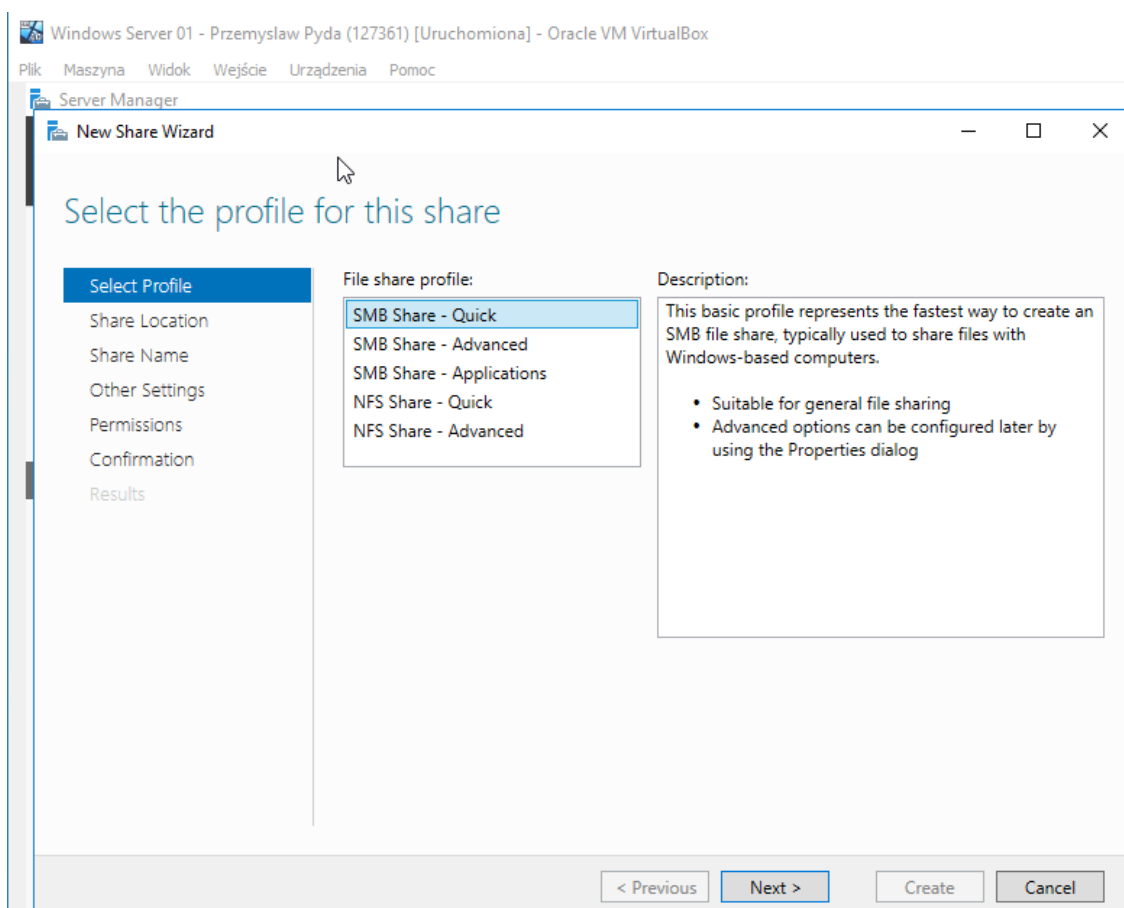
Rysunek 5.3.6 Widok właściwości członków grupy EVERYBODY. Opracowanie własne

## 5.4. Profile mobilne użytkowników

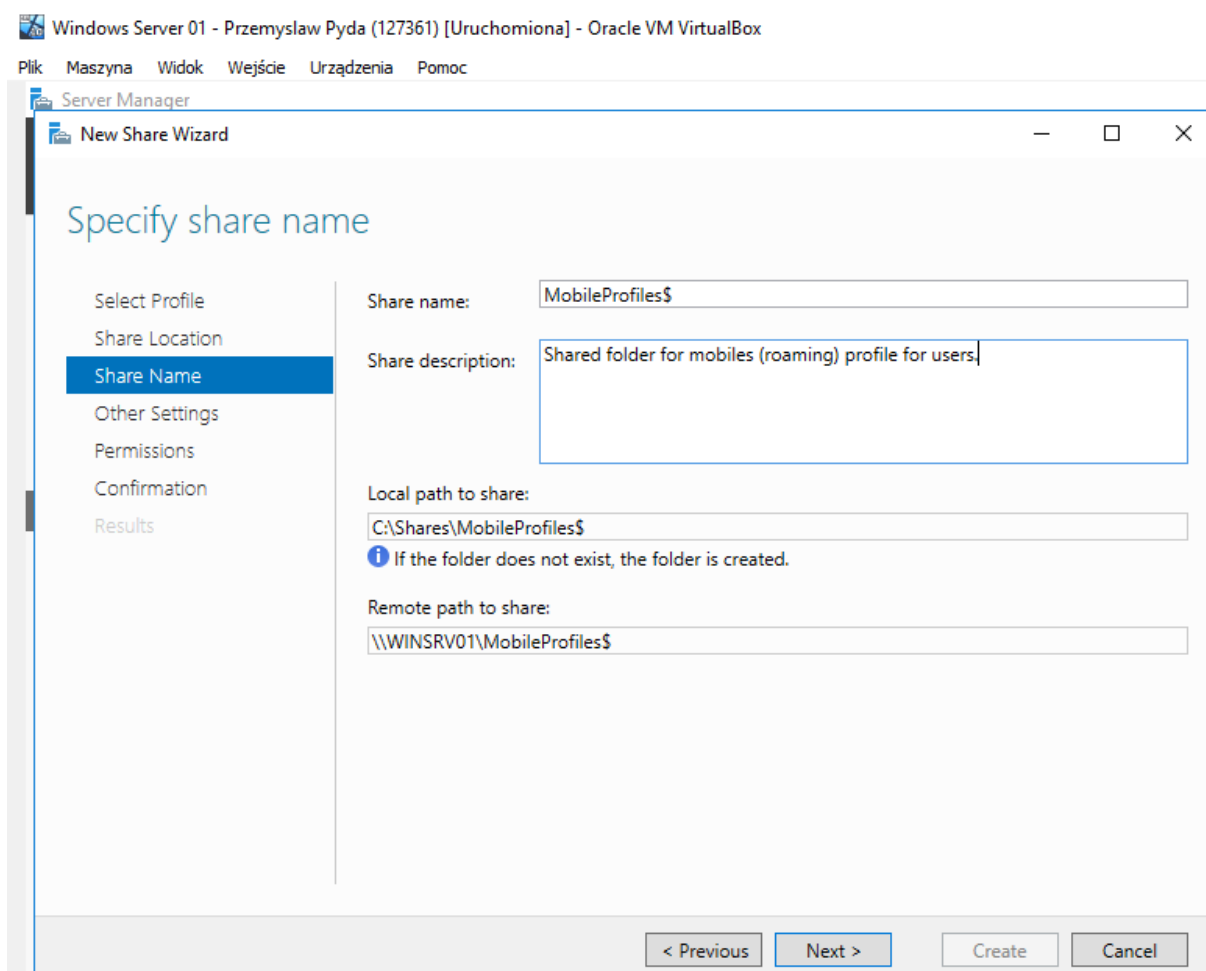
Każdy z użytkowników w domenie CyberCode posiada do swojego konta domenowego przypisaną funkcjonalność profilu mobilnego (ang. Roaming User Profile). Pozwala to użytkownikowi na przechowywanie jego profilu użytkownika na serwerze sieciowym, nie zaś na komputerze lokalnym, co pozwala synchronizować pliki użytkownika podczas jego pracy na różnych komputerach dołączonych do domeny.

Kiedy użytkownik loguje się do komputera z profilem mobilnym, profil jest pobierany z serwera i przechowywany lokalnie na komputerze. Wszelkie zmiany wprowadzone do profilu podczas logowania użytkownika są zapisywane lokalnie, a następnie przesyłane z powrotem na serwer podczas wylogowania użytkownika. To pozwala użytkownikowi uzyskać dostęp do swoich osobistych ustawień i preferencji z dowolnego komputera, pod warunkiem posiadania dostępu do sieci i swojego profilu mobilnego.

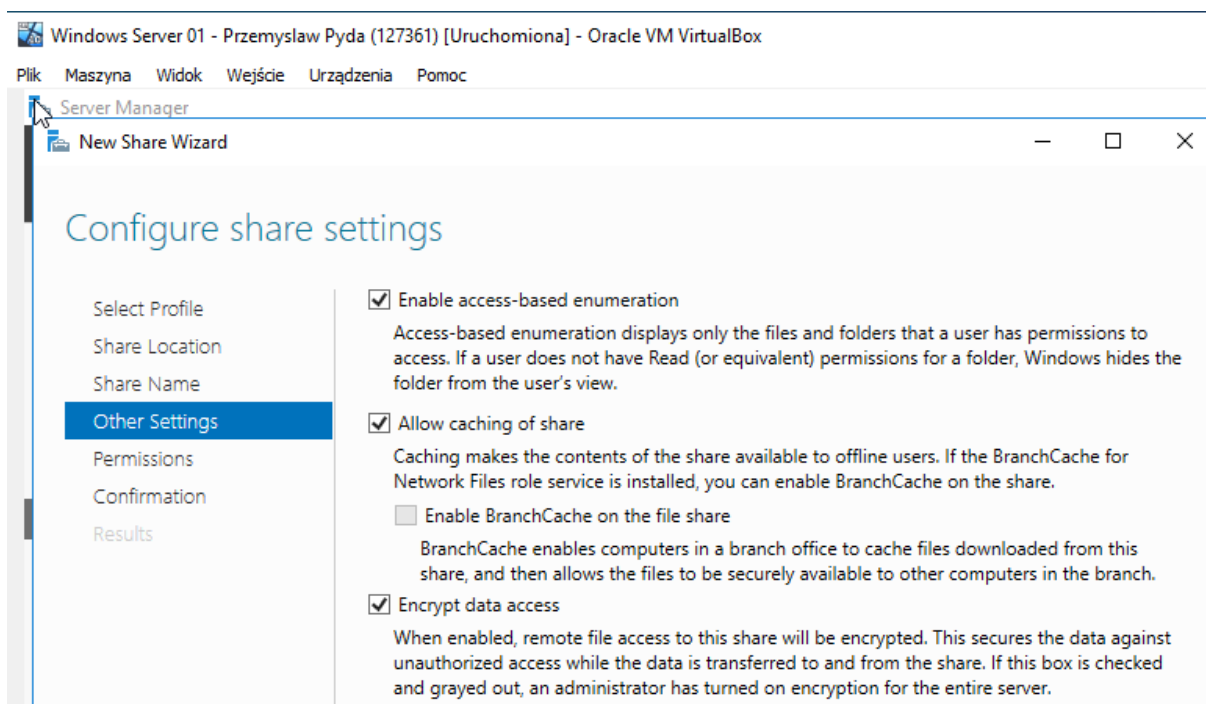
Poniżej przy pomocy zrzutów ekranu pokazany jest proces konfiguracji i wdrożenia profili mobilnych dla użytkowników z poziomu Windows Server 2016.



Rysunek 5.4.1 Profil mobilny - wybór zasobu udostępnionego. Opracowanie własne

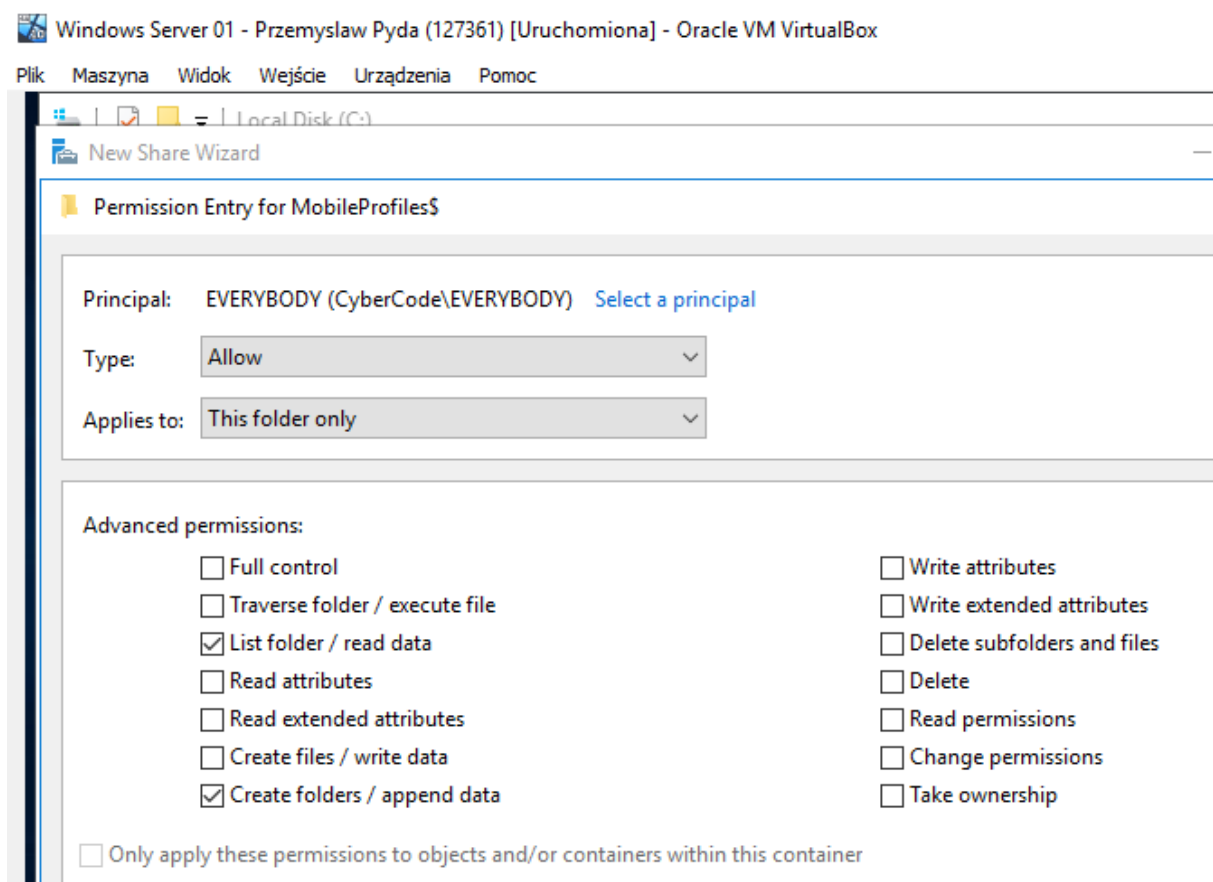


Rysunek 5.4.2 Profil mobilny - tworzenie zasobu udostępnionego. Opracowanie własne

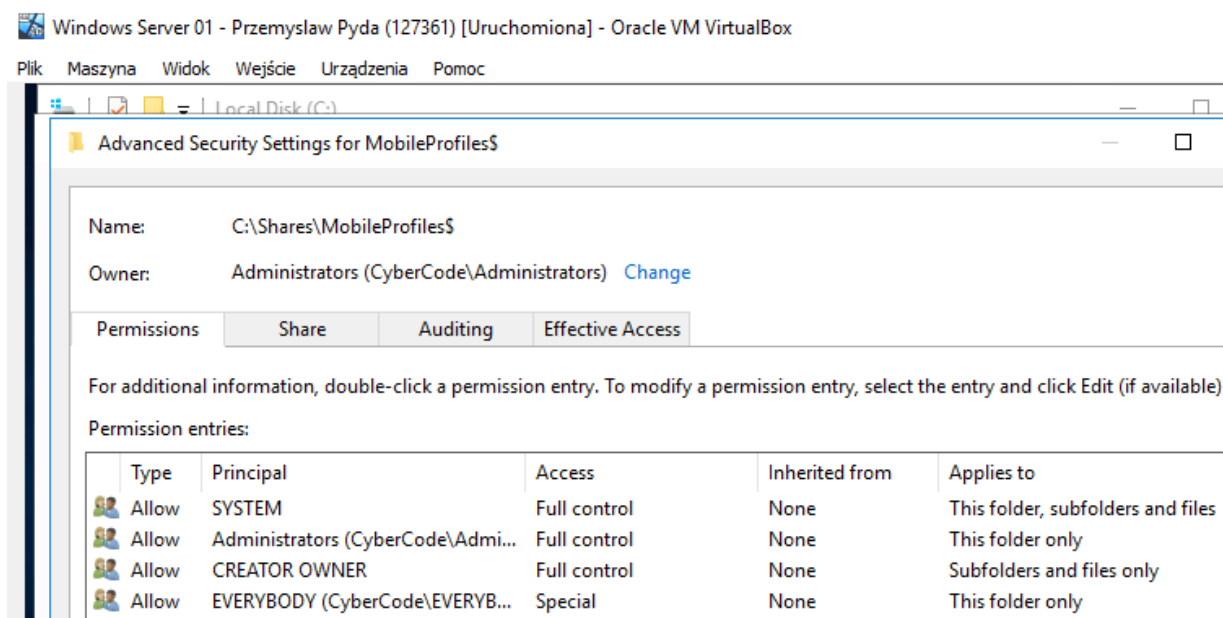


Rysunek 5.4.3 Profil mobilny - właściwości zasobu. Opracowanie własne

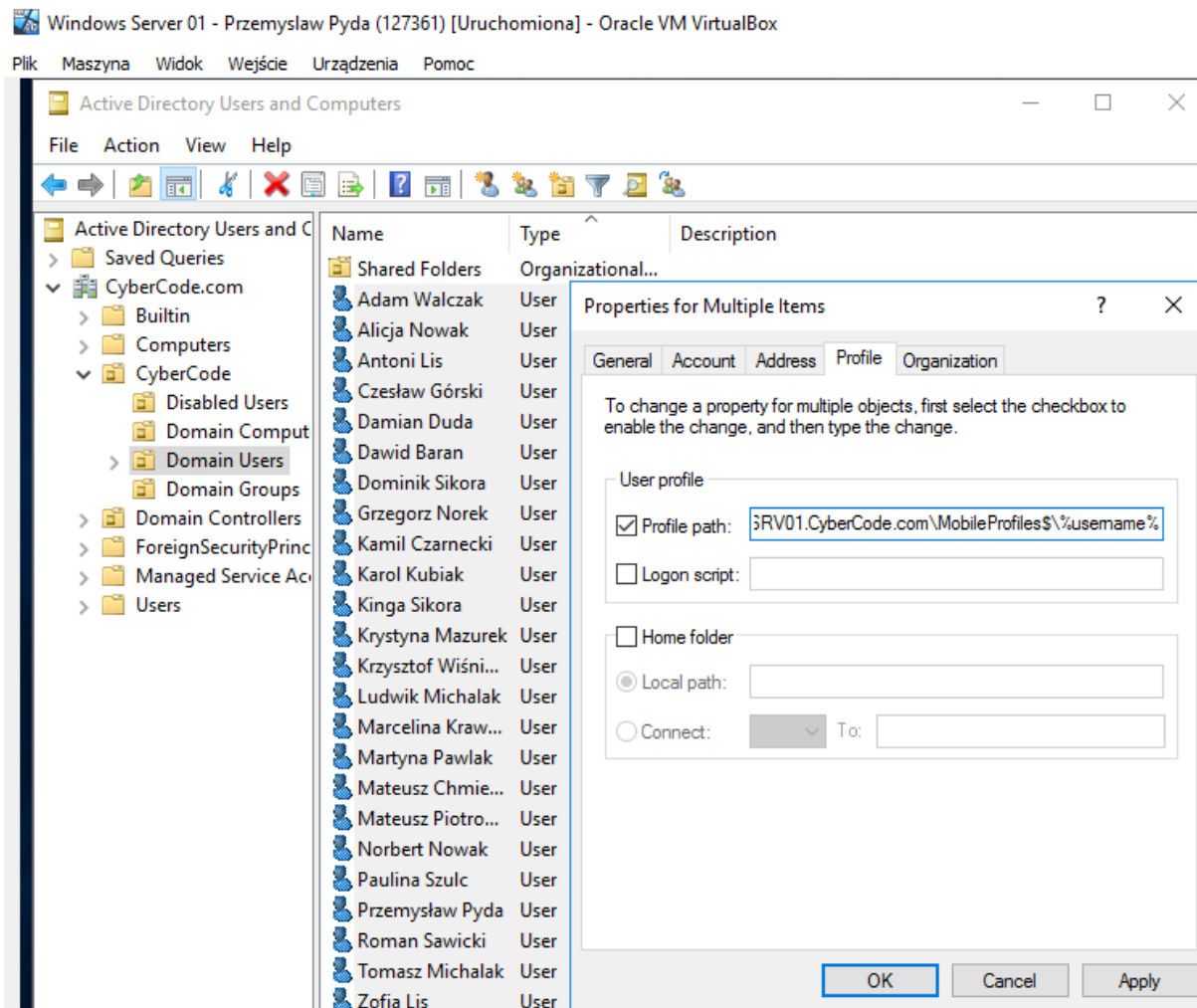




Rysunek 5.4.4 Ustawienia uprawnień do zasobu. Opracowanie własne

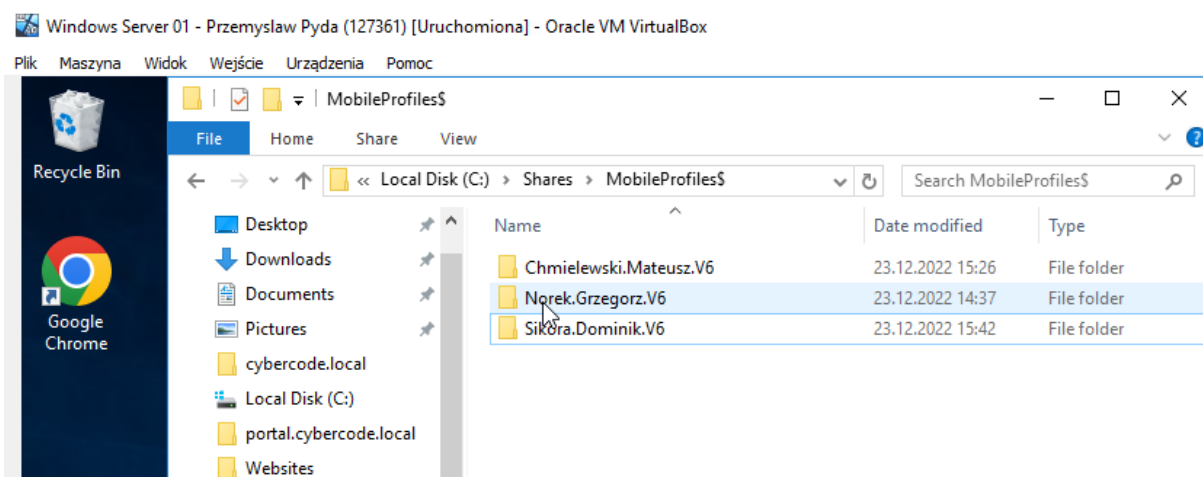


Rysunek 5.4.5 Profil mobilny - Ustawienia bezpieczeństwa folderu. Opracowanie własne



Rysunek 5.4.6 Profil mobilne – Zmienna globalna w ścieżce. Opracowanie własne

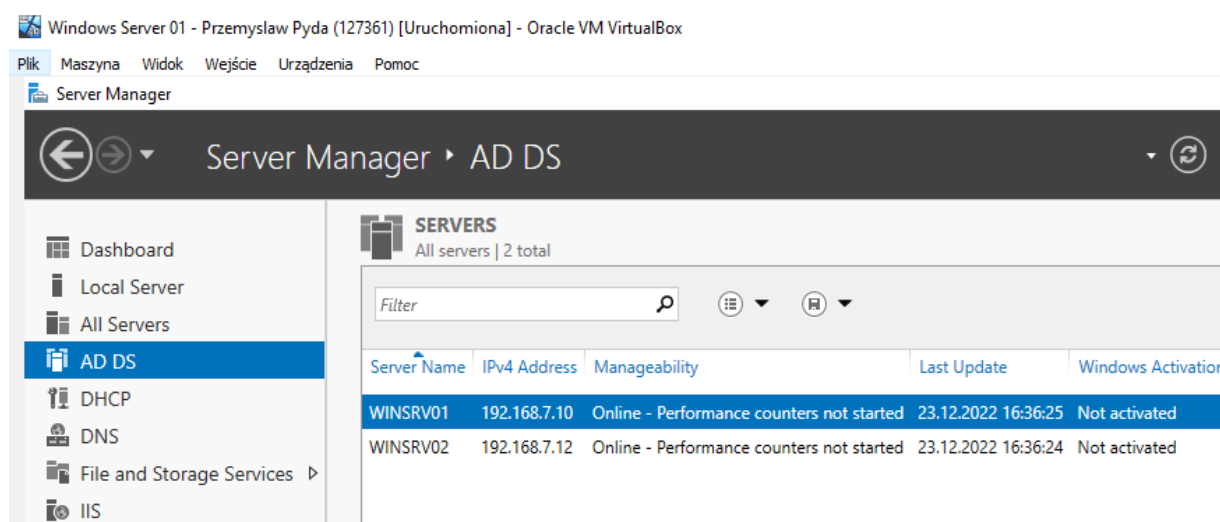
Po wdrożeniu funkcjonalności profili mobilnych w momencie pierwszego zalogowania się użytkownika do domeny tworzony jest profil mobilny w określonej lokalizacji.



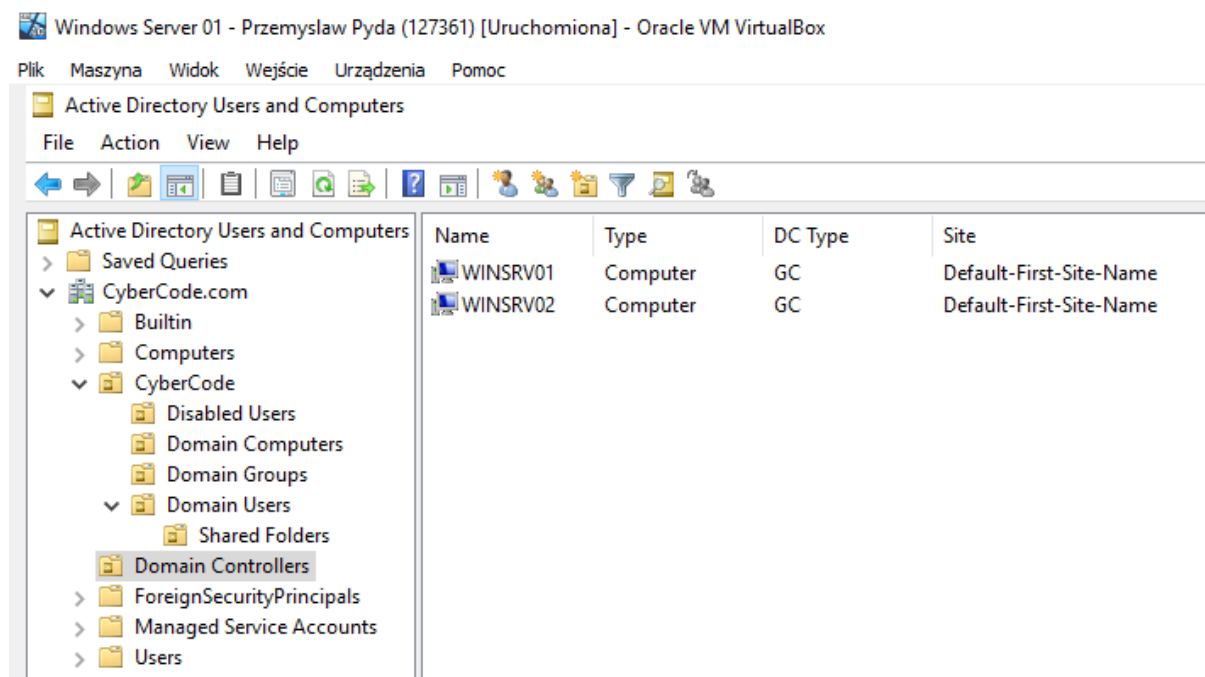
Rysunek 5.4.7 Profil mobilny - Wygenerowane profile mobilne. Opracowanie własne

## 5.5. Redundancja usług serwerowych Windows Server – Active Directory

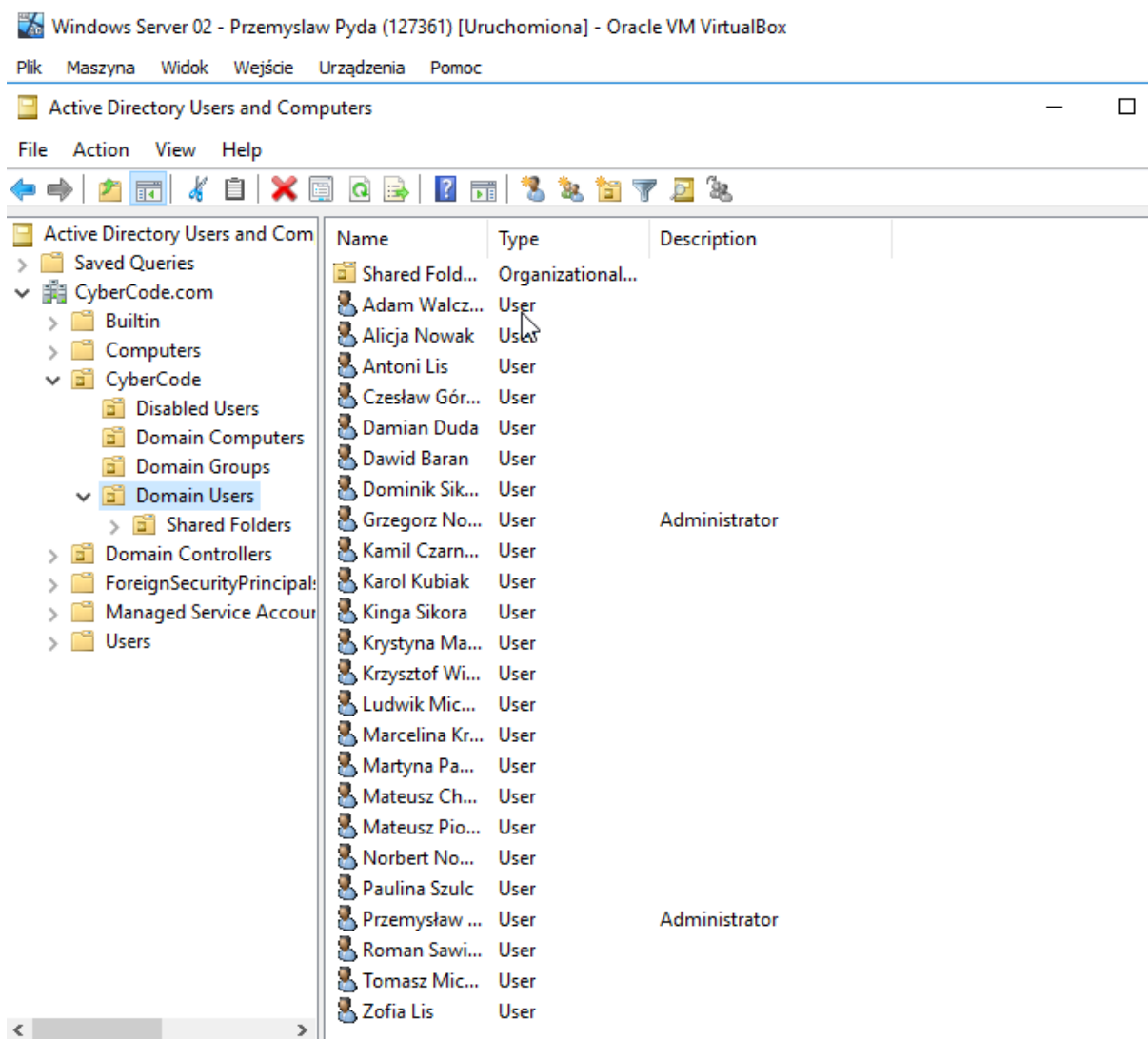
W celu minimalizowania ryzyka związanego z krytyczną awarią systemu teleinformatycznego, jaką niewątpliwie jest brak możliwości zalogowania na komputery domenowe, wykorzystano drugi, fizyczny komputer działający pod systemem Windows Server. Dołączając go do tego samego lasu domenowego co pierwotny kontroler domeny osiąga się pełną zgodność baz LDAP oraz ich synchronizację w czasie rzeczywistym. W wypadku awarii jednego z urządzeń dalej użytkownicy będą mieli możliwość dostępu do zasobów AD.



Rysunek 5.5.1 Widok nadmiarowych kontrolerów domeny AD. Opracowanie własne



Rysunek 5.5.2 Kontrolery AD w aplikacji AD Users and Computers. Opracowanie własne



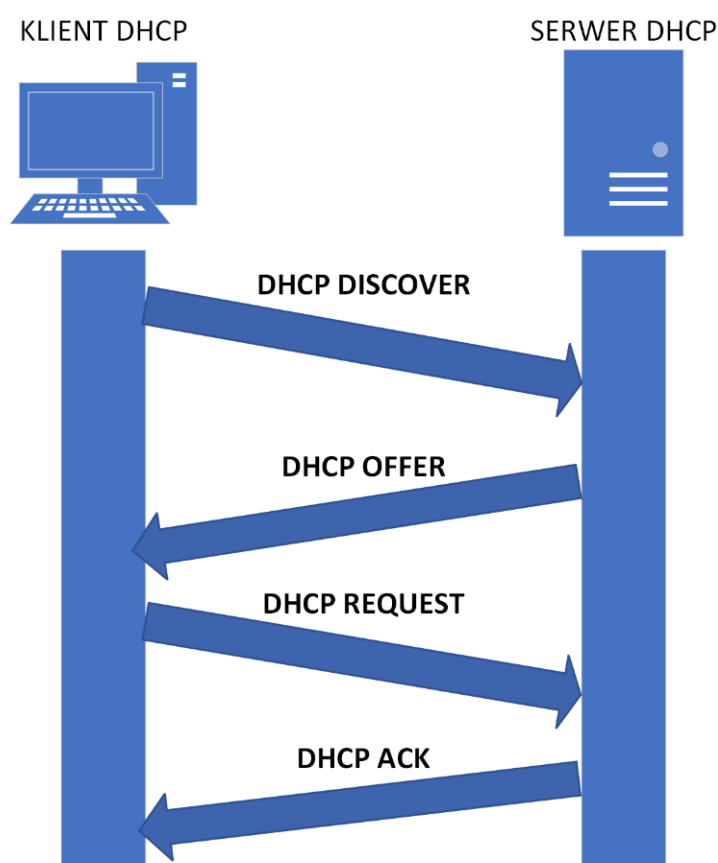
Rysunek 5.5.3 Powielenie ustawień AD na WINSRV02. Opracowanie własne

Jak widać na powyższym zrzucie ekranu ustawienia synchronizują się pomiędzy kontrolerami domeny. Jakakolwiek wprowadzona zmiana w strukturze zostanie zsynchronizowana z pozostałymi kontrolerami, co pozwala zachować aktualną strukturę domeny i bezproblemowe jej wykorzystywanie, gdyby nastąpiła awaria głównego serwera, pełniącego rolę kontrolera domeny WINSRV01.

## 5.6. Serwer DHCP – Wdrożenie w konfiguracji redundantnej

Serwer DHCP służy do automatycznego, dynamicznego przydzielania adresów IP dla urządzeń końcowych. W firmie CyberCode zadania serwera DHCP są realizowane poprzez Windows Server dzięki 2 urządzeniom serwerowym WINSRV01 i WINSRV02 działającym w trybie failover ze skonfigurowanym trybem dzielenia obciążania (ang. Load-balancing) w proporcji 60/40, czyli 60% zapytań DHCP trafia do urządzenia WINSRV01, zaś pozostałe 40% zapytań DHCP trafia do urządzenia WINSRV02. W razie awarii którejkolwiek ze stron partnerstwa dostępny serwer przejmuje 100% zapytań DHCP.

Proces przydzielania adresu IP prezentuje poniższy schemat.

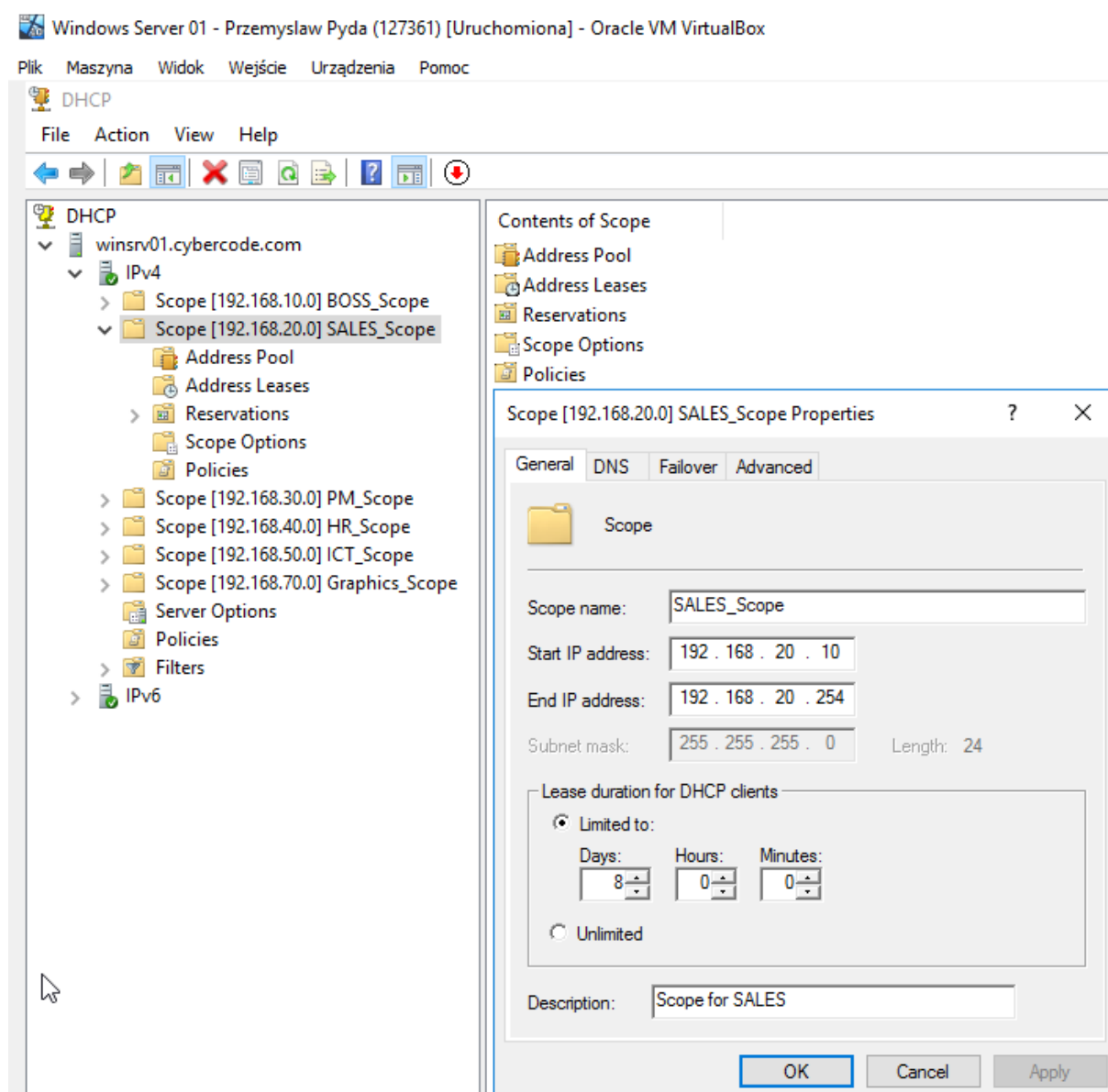


Rysunek 5.6.1 Przydzielanie adresu IP przez DHCP. Opracowanie własne na podstawie [4]

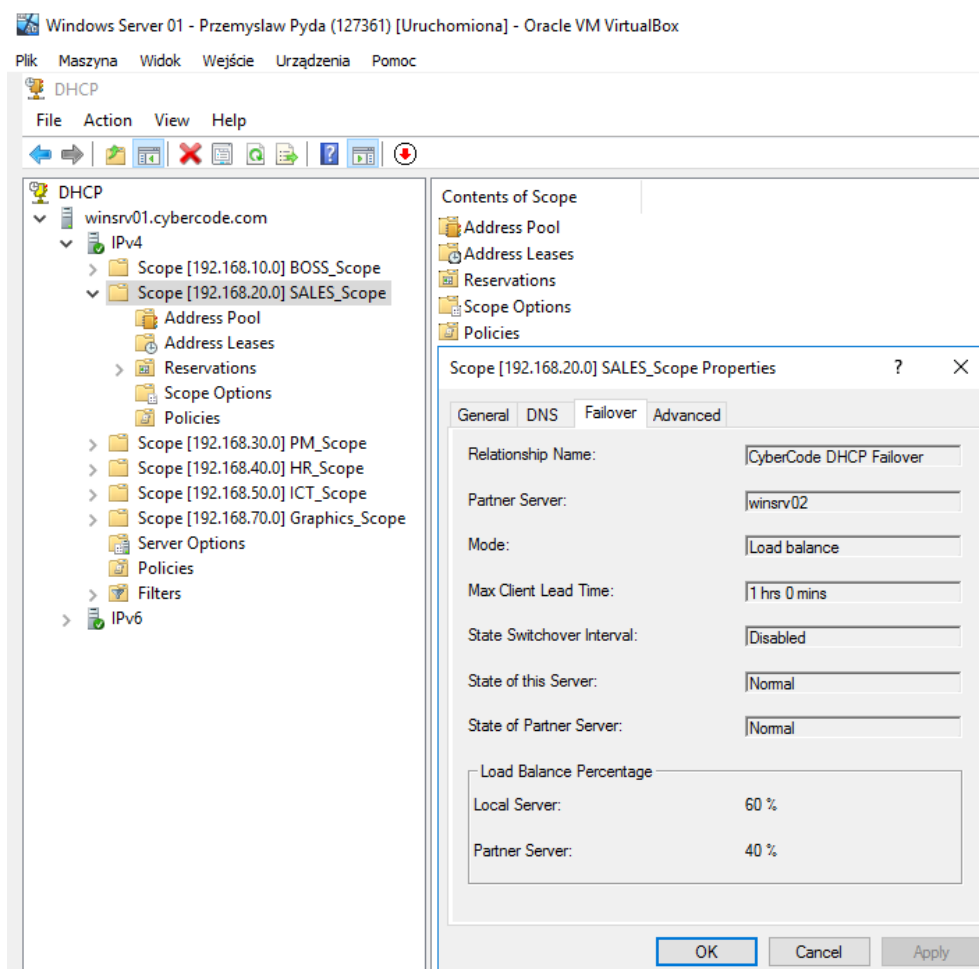
Analizując powyższy schemat widać, że to klient wysyła komunikat broadcastowy DHCP Discover w celu zlokalizowania serwera DHCP. Komunikaty rozgłoszeniowe nie opuszczają lokalnej podsieci, a więc urządzenia nie znajdujące się w tej samej podsieci co serwer nie będą mogły osiągnąć oferty DHCP, nawet pomimo możliwości pomyślnego wykonania echo request protokołu ICMP w kierunku serwera DHCP. Dopiero skonfigurowanie

przekazywania pakietów DHCP na przełącznikach sieciowych pozwoli na uzyskanie oczekiwanego efektu.

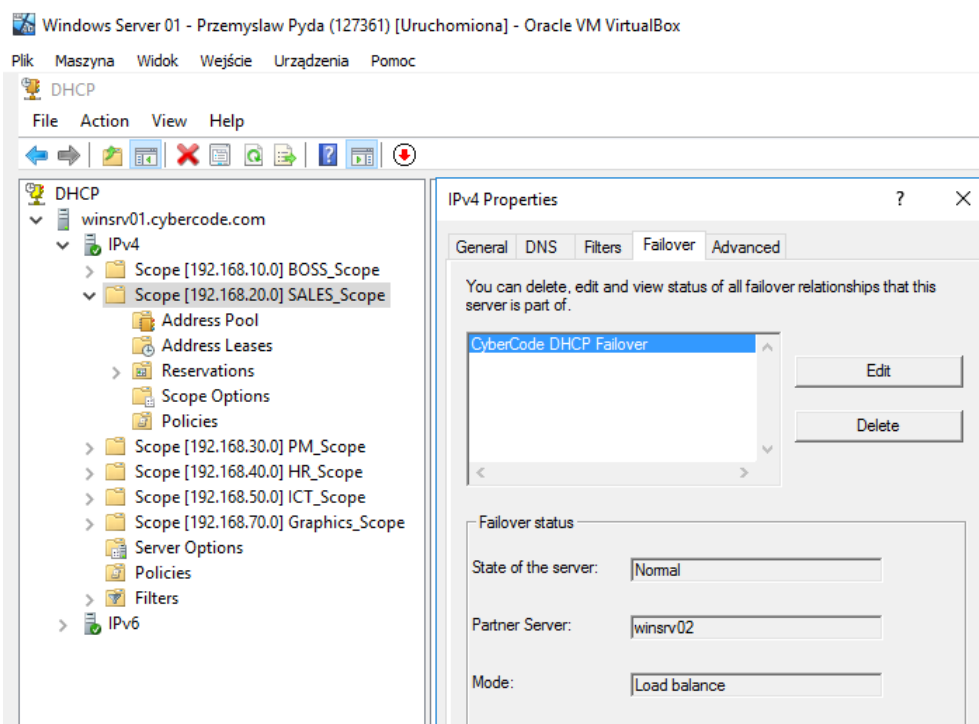
Poniższe zrzuty ekranu prezentują przystawkę DHCP i jej konfigurację dla oddziału sprzedażowego. Pozostałe pule tworzone są analogicznie, w zależności od określonej adresacji sieciowej.



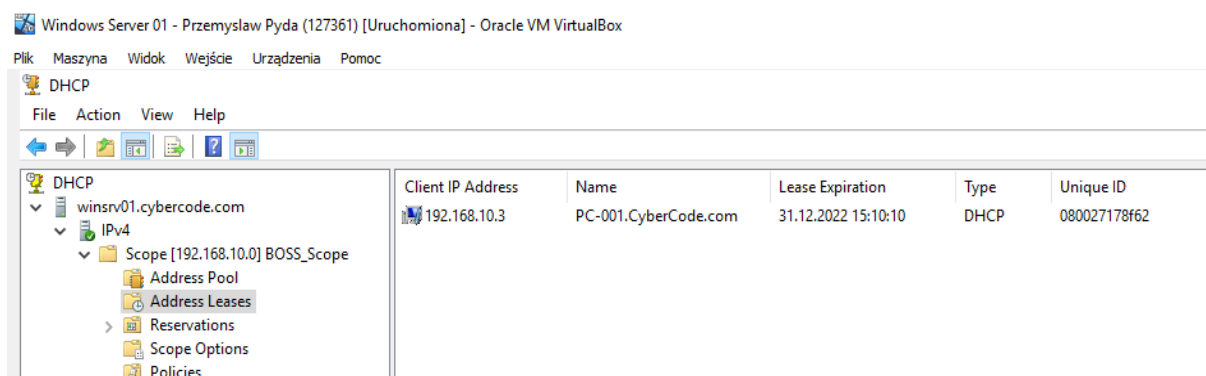
Rysunek 5.6.2 DHCP - Utworzenie pól adresów. Opracowanie własne



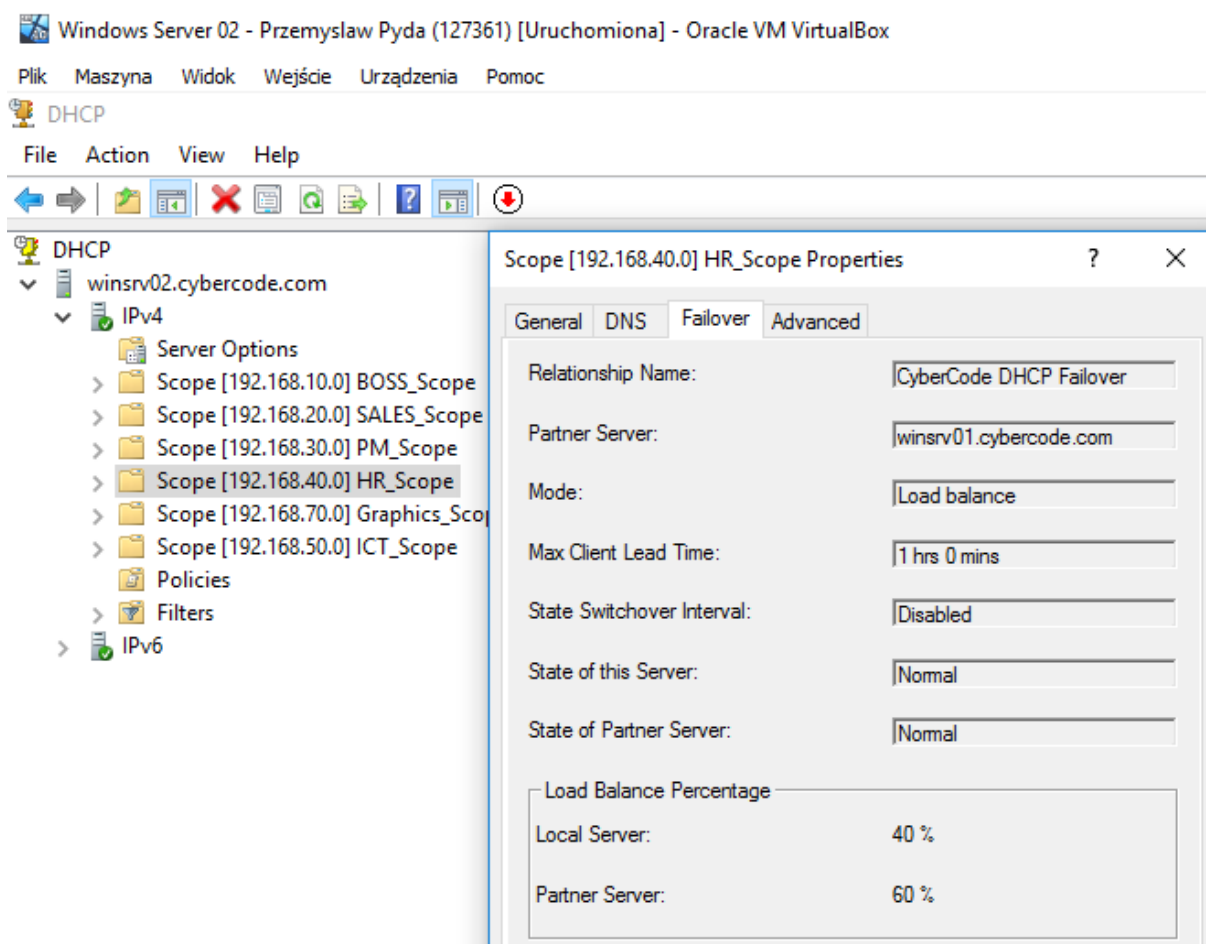
Rysunek 5.6.3 DHCP - Widok zakładki "Failover" dla WINSRV01. Opracowanie własne



Rysunek 5.6.4 DHCP - Relacja sąsiedztwa w trybie "Failover". Opracowanie własne



Rysunek 5.6.5 DHCP - Widok "Adress Leases" dla DHCP. Opracowanie własne



Rysunek 5.6.6 DHCP - Relacja sąsiedztwa dla WINSRV02. Opracowanie własne



## 5.7. Wewnętrzna strona internetowa firmy

Kadra zarządcza oczekiwała wdrożenie strony internetowej dostępnej jedynie w sieci lokalnej, będącej alternatywą dla mapowanego dysku sieciowego „Ogłoszenia”.

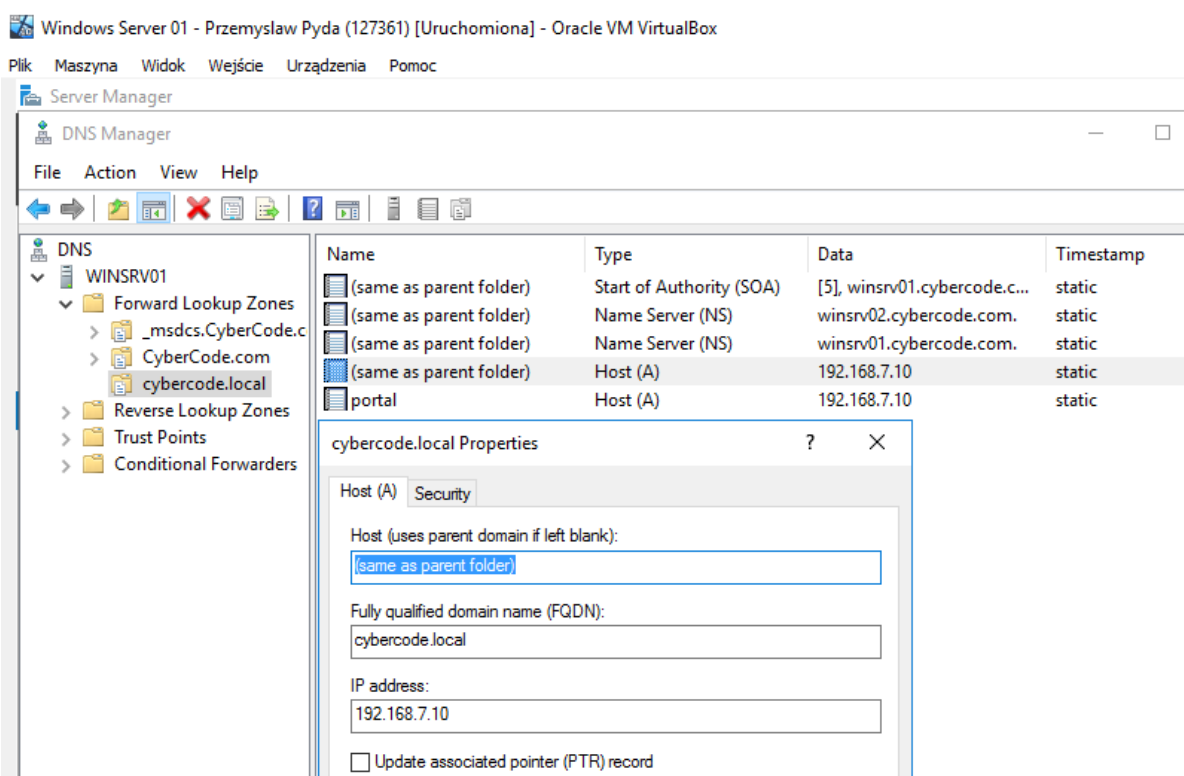
Strona internetowa powinna być dostępna przez przeglądarki internetowe po wpisaniu następujących adresów internetowych:

- cybercode.local – strona główna z informacjami
- portal.cybercode.local – portal pracowniczy

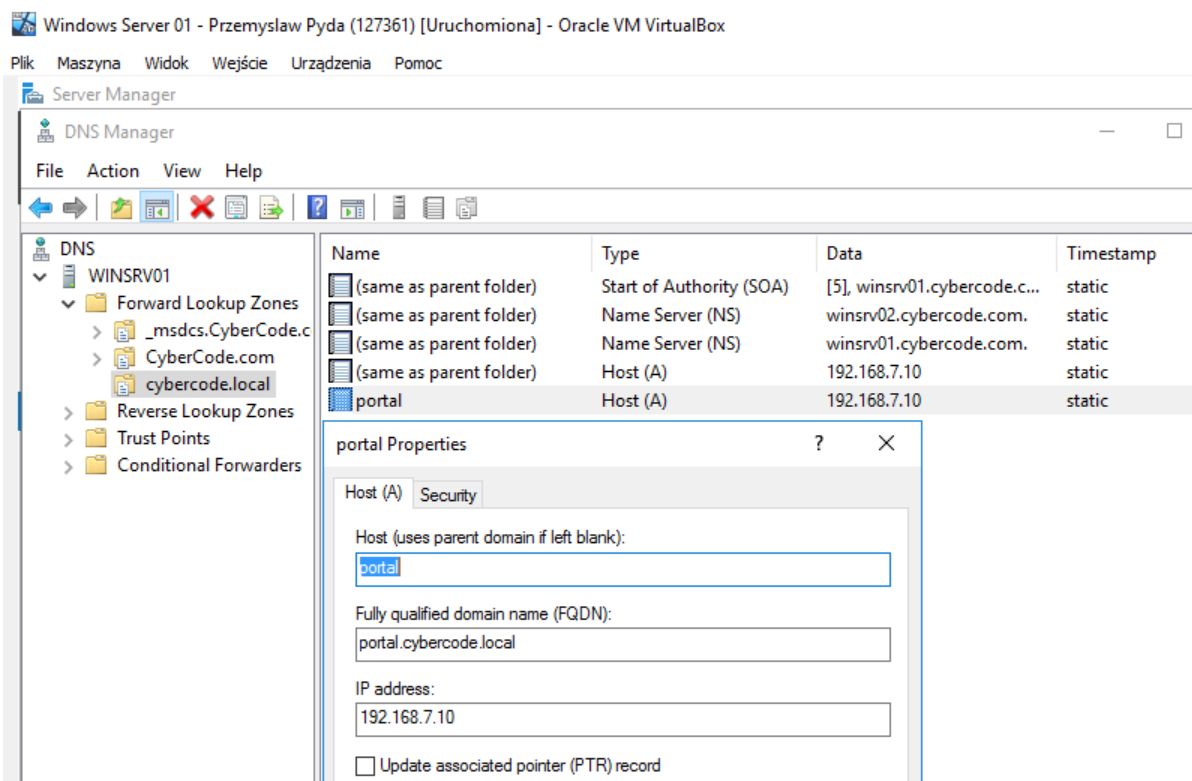
W celu wdrożenia tego założenia zostały stworzone 2 foldery na dysku lokalnym urządzenia WINSRV01 w lokalizacji C:\Websites\cybercode.local i C:\Websites\portal.cybercode.local.

W powyższych folderach utworzono plik index.html. Celem pracy inżynierskiej nie było stworzenie strony internetowej, dlatego efekt jest surowy.

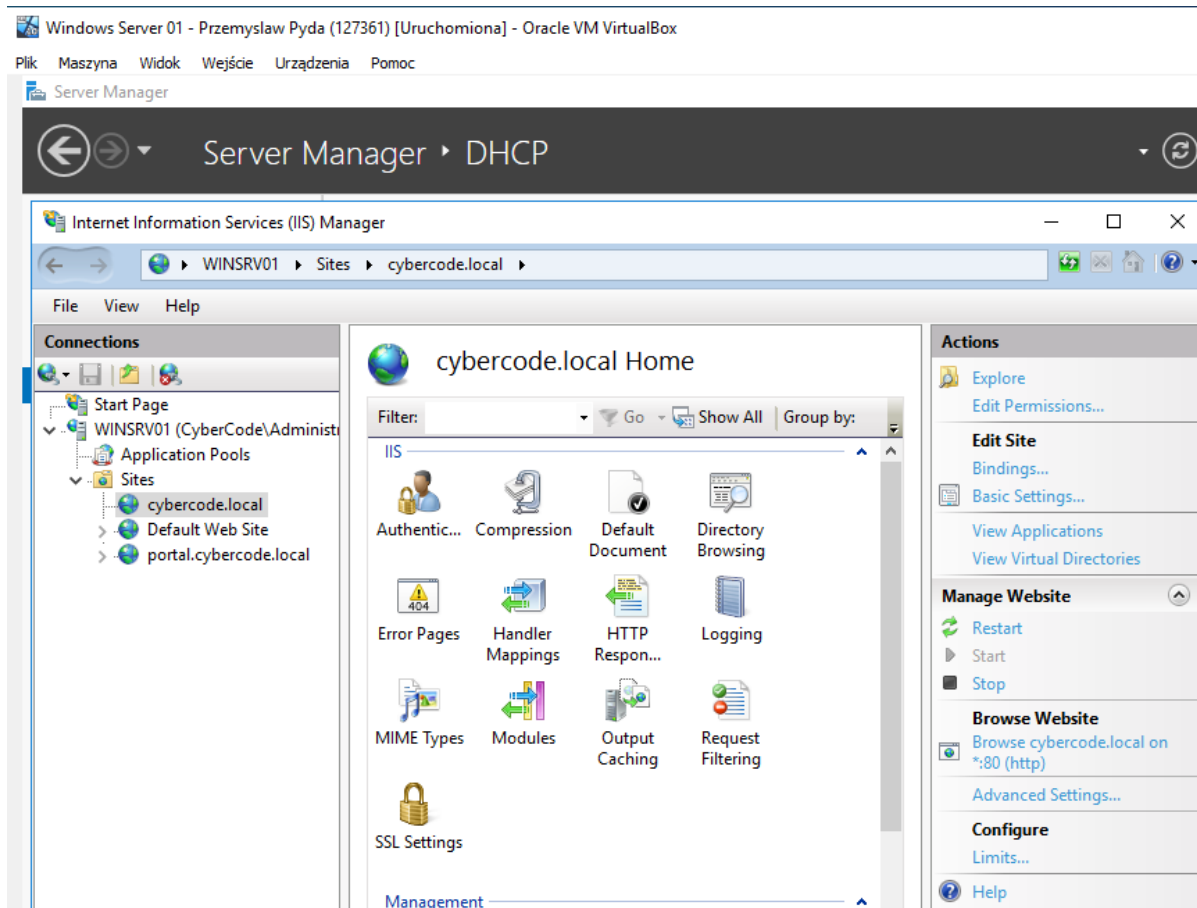
Ważnym krokiem było utworzenie nowej strefy i dodanie wpisów w DNS w Forward Lookup Zones oraz powiązanie adresu FQDN do adresu IP serwera IIS, świadczącego usługi webowe. W innym wypadku strona nie byłaby dostępna po wpisaniu nazwy mnemonicznej.



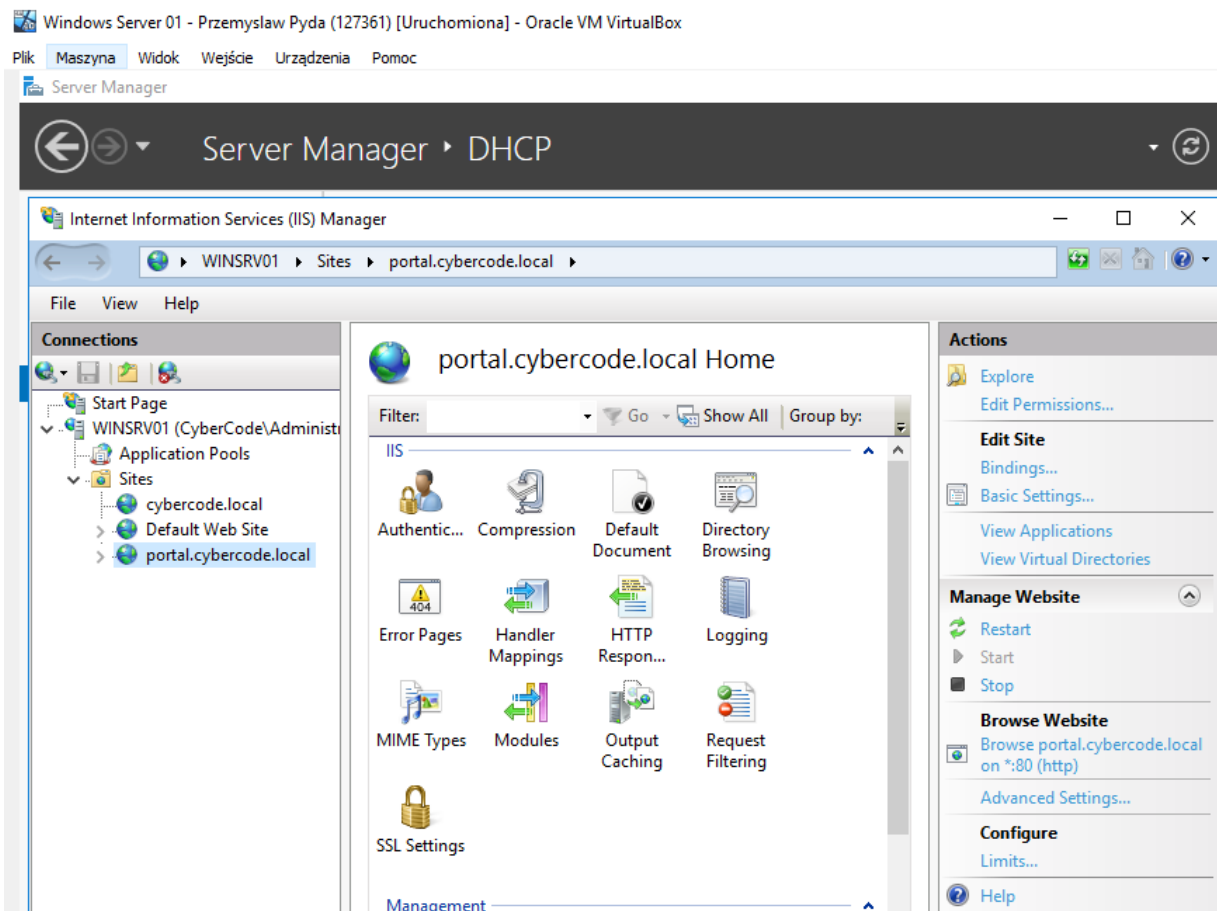
Rysunek 5.7.1 Utworzenie wpisów w Forward Lookup Zones. Opracowanie własne



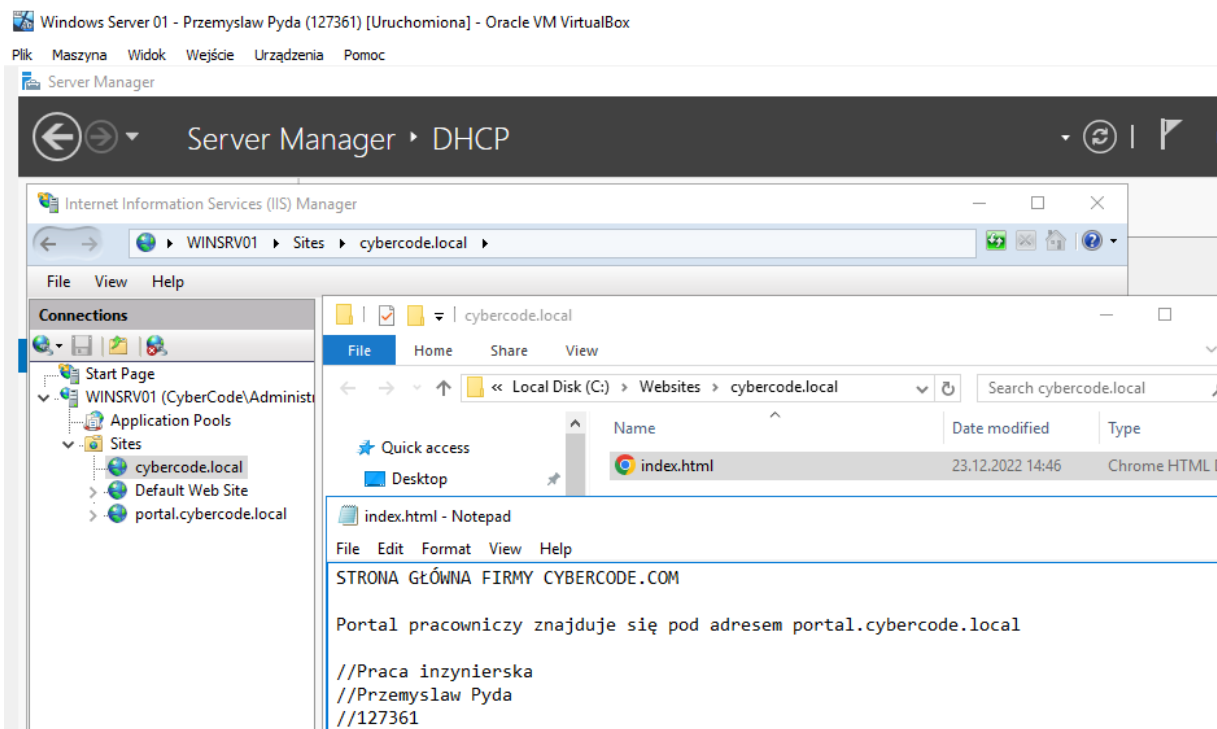
Rysunek 5.7.2 Utworzenie wpisów w Forward Lookup Zones - portal. Opracowanie własne



Rysunek 5.7.3 Manager IIS - cybercode.local. Opracowanie własne



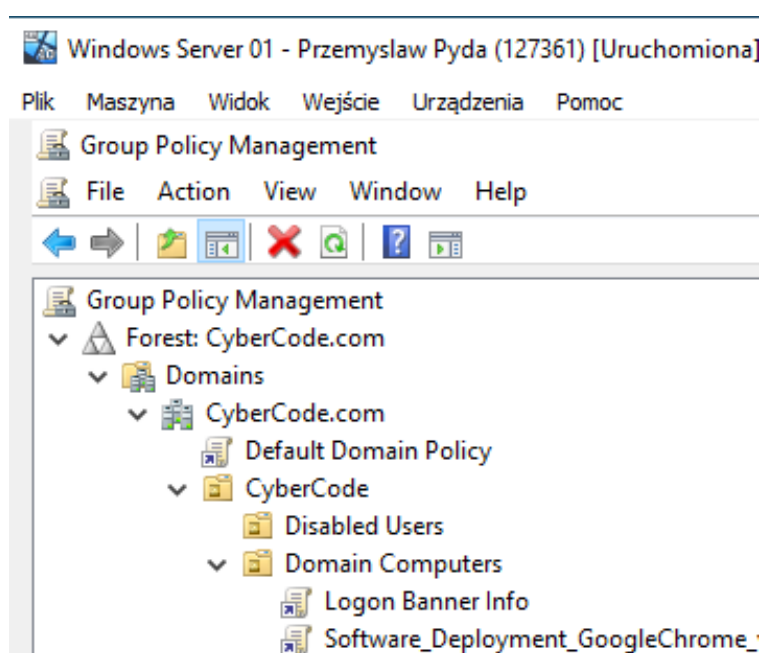
Rysunek 5.7.4 Manager IIS - portal.cybercode.local. Opracowanie własne



Rysunek 5.7.5 Plik strony internetowej cybercode.local. Opracowanie własne

## 5.8. Wykorzystanie GPO do zautomatyzowania instalacji oprogramowania Google Chrome wraz z dedykowaną konfiguracją ADM

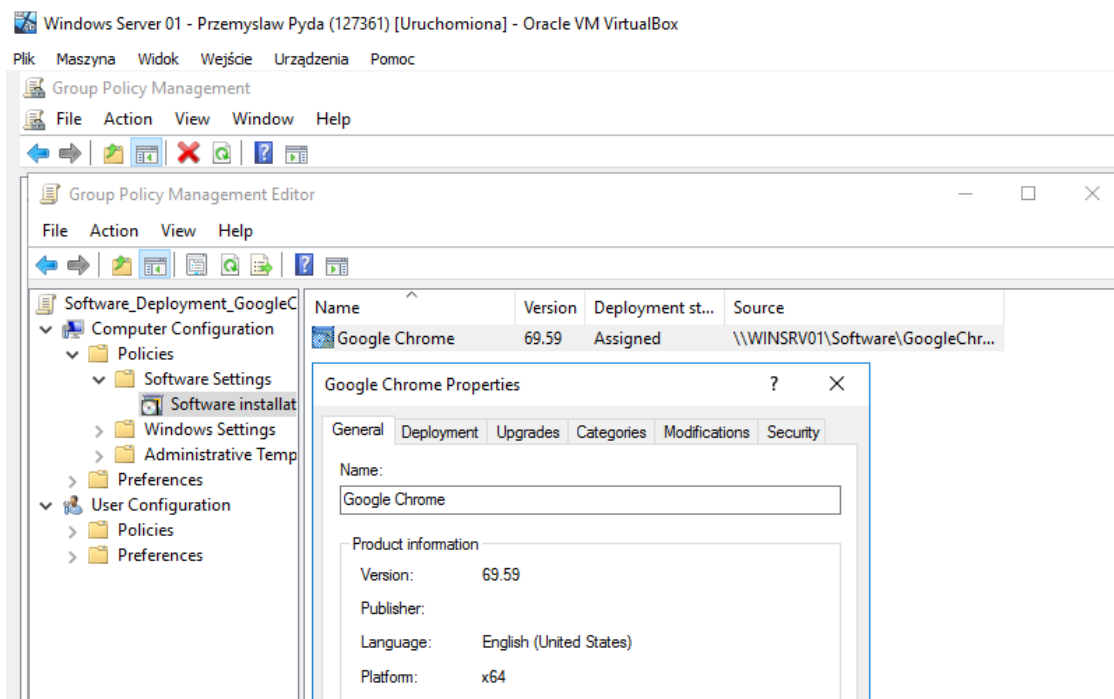
Każdy z komputerów w domenie powinien posiadać przeglądarkę internetową zdolną do wykorzystania nowoczesnych technologii i łatwą w użytkowaniu dla użytkownika końcowego. Wybór padł na znaną i powszechnie stosowaną przeglądarkę Google Chrome w wersji 108.0.5359.125. Pobierając pakiet Chrome Enterprise Bundle 64-bit mamy dostęp zarówno do dokumentacji, plików instalacyjnych (w tym ważnego instalatora paczki \*.msi) jak i plików konfiguracyjnych adm/admx służących do zarządzania ustawieniami.



Rysunek 5.8.1 Utworzenie GPO dla wdrożenia Google Chrome. Opracowanie własne

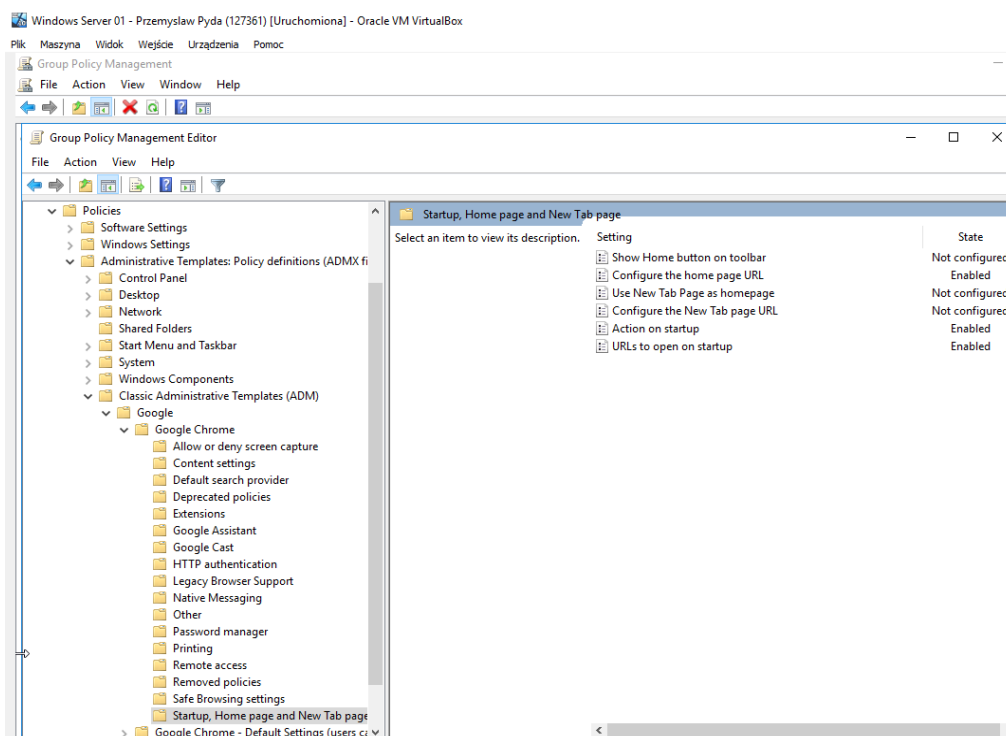
Pierwszym krokiem w celu wdrożenia aplikacji było utworzenie GPO dla jednostki organizacyjnej „Domain Computers”, gdyż konfigurowane ustawienie w tym wypadku dotyczy konfiguracji komputerów, nie zaś użytkowników.

W zakładce „Software installation” naszym celem jest określenie lokalizacji paczki GoogleChromeStandaloneEnterprise64.msi oraz potwierdzenie ustawień wdrożenia. Po odpowiedniej konfiguracji na każdym komputerze dołączonym do domeny, w sposób automatyczny, przeglądarka Google Chrome zostanie zainstalowana, zaś jej skrót zostanie umiejscowiony na pulpicie użytkownika.



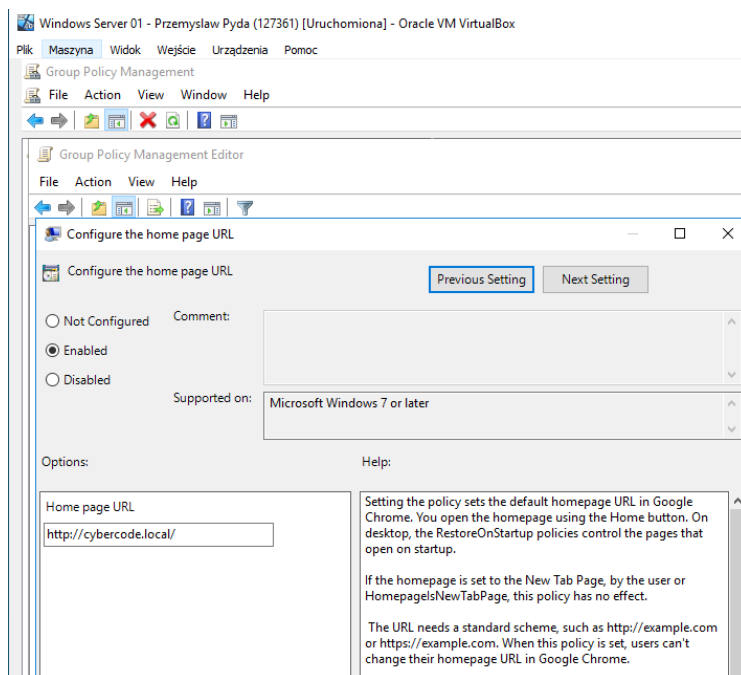
Rysunek 5.8.2 Wdrożona paczka instalacyjna Google Chrome. Opracowanie własne

Kolejnym krokiem jest import pliku chrome.adm w polityce szablonów administracyjnych. Po pomyślnym imporcie administrator uzyskuje możliwość personalizacji przeglądarki dla użytkowników domenowych.

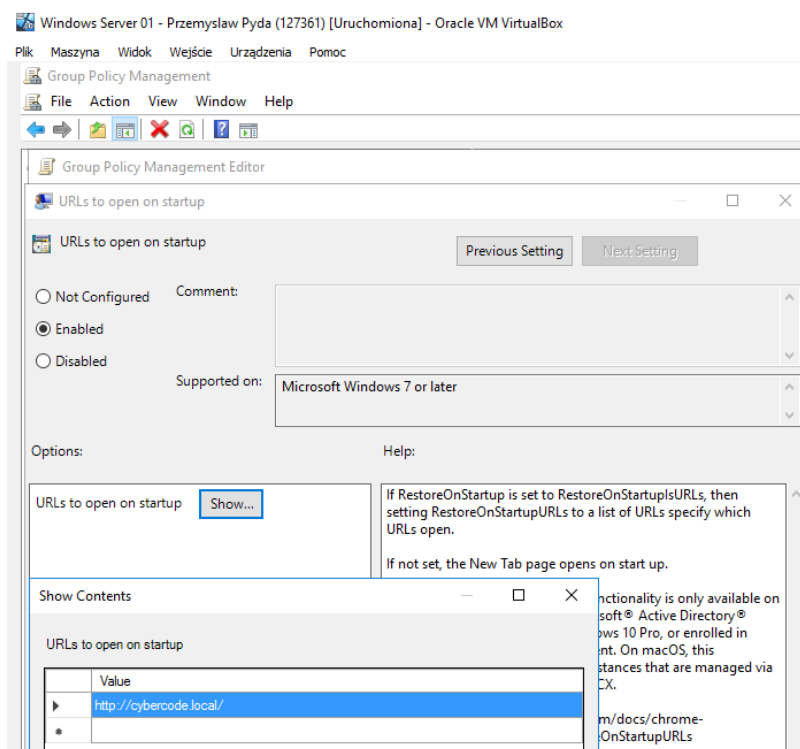


Rysunek 5.8.3 Ustawienia szablonów ADM dla Google Chrome. Opracowanie własne

Według założeń stroną startową, powinna być strona cybercode.local i powinna być ona uruchamiana za każdym razem w nowej karcie, przy starcie przeglądarki. Konfiguracja znajduje się na poniższych zrzutach ekranu.



Rysunek 5.8.4 Ustawienie strony startowej. Opracowanie własne

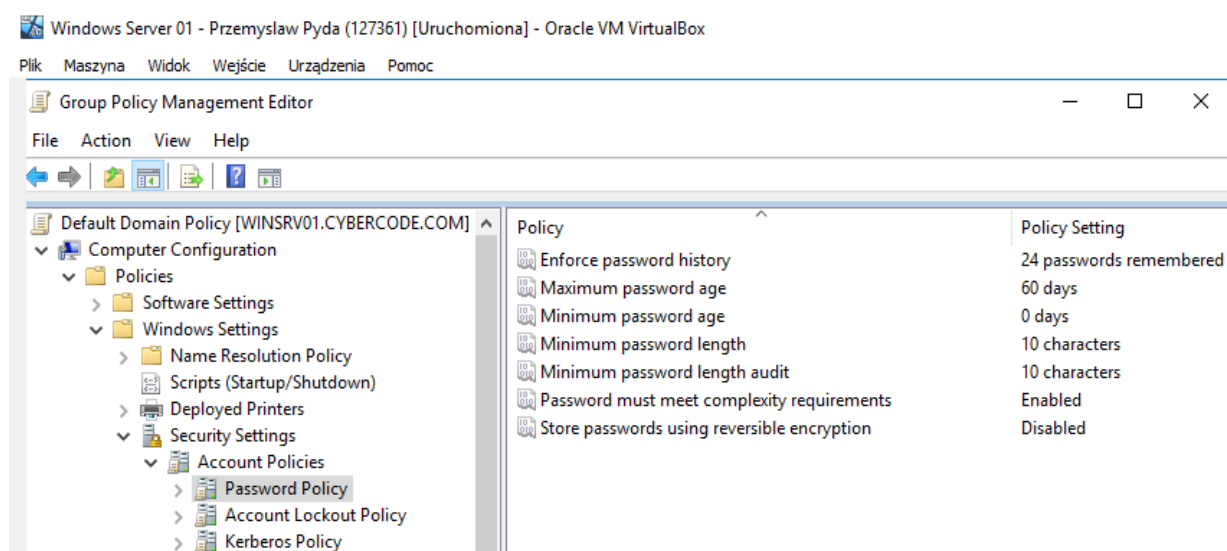


Rysunek 5.8.5 Ustawienie strony zawsze uruchamianej przy starcie. Opracowanie własne

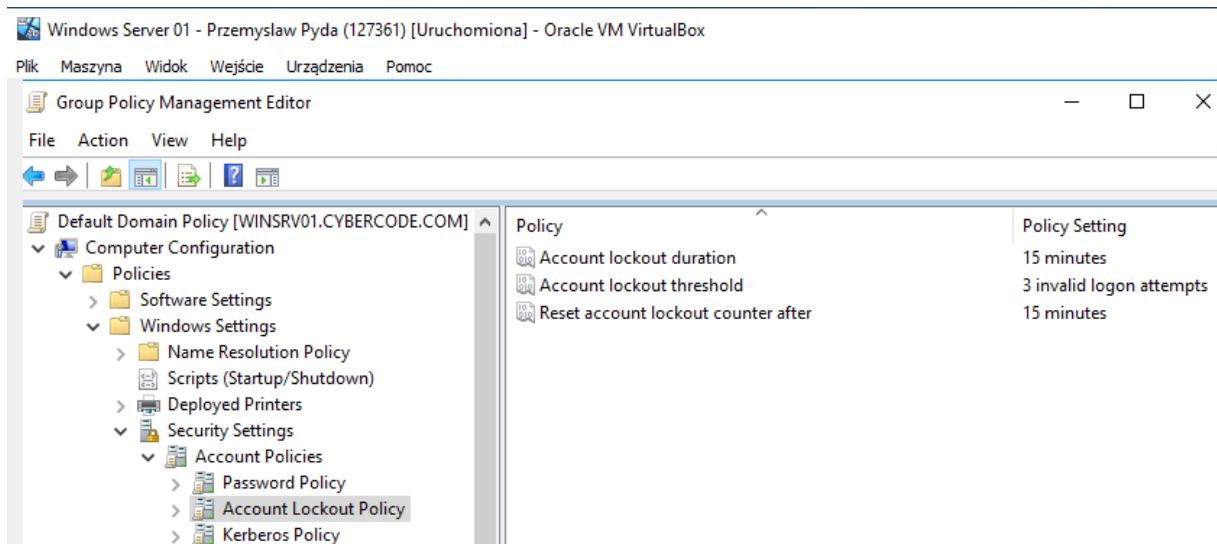
## 5.9. Ustawienia polityki haseł

Ustawienia polityki haseł określają, jakie hasła użytkownicy mogą przypisywać do swoich kont domenowych oraz jak zdefiniowane zostały zasady i reagowania w przypadku próby utworzenia niedozwolonego hasła. Polityka bezpieczeństwa dla haseł określona jest w domyślnym GPO dla komputerów w domenie.

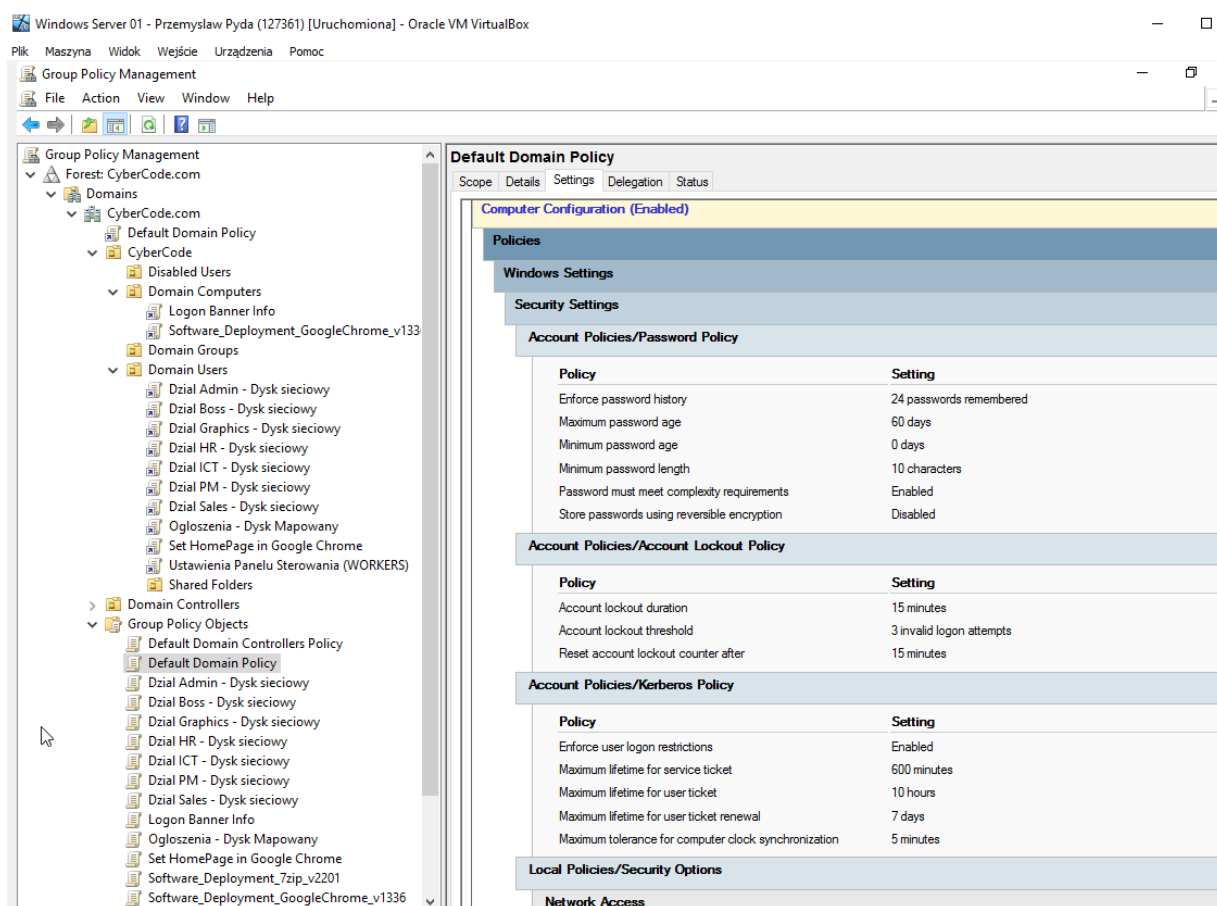
Według założeń hasło powinno spełniać warunki złożoności (co najmniej 3 z 4 z kategorii muszą występować w hasle: mała litera, wielka litera, cyfra, znak specjalny), nie może zawierać nazwy użytkownika ani części imienia i nazwiska użytkownika przekraczających dwa kolejne znaki. Hasło musi być co najmniej 10 znakowe, a liczba haseł niemogących się powtórzyć wynosi 24. Dodatkowo wymuszona jest zmiana hasła co 60 dni. Po 3 błędnych próbach logowania konto zostaje zablokowane na 15 minut. Tylko administrator może zdjąć blokadę konta szybciej lub manualnie zrestartować hasło.



Rysunek 5.9.1 Ustawienia polityki haseł dla bazowego GPO. Opracowanie własne



Rysunek 5.9.2 Ustawienia blokowania konta dla bazowego GPO. Opracowanie własne

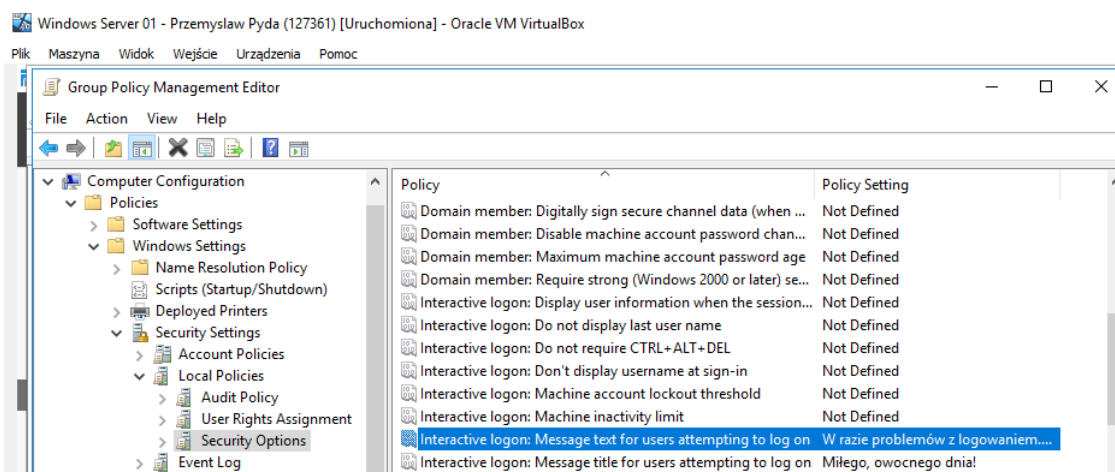


Rysunek 5.9.3 Sumaryczny widok polityk haseł. Opracowanie własne



## 5.10. Ustawienie banneru logowania

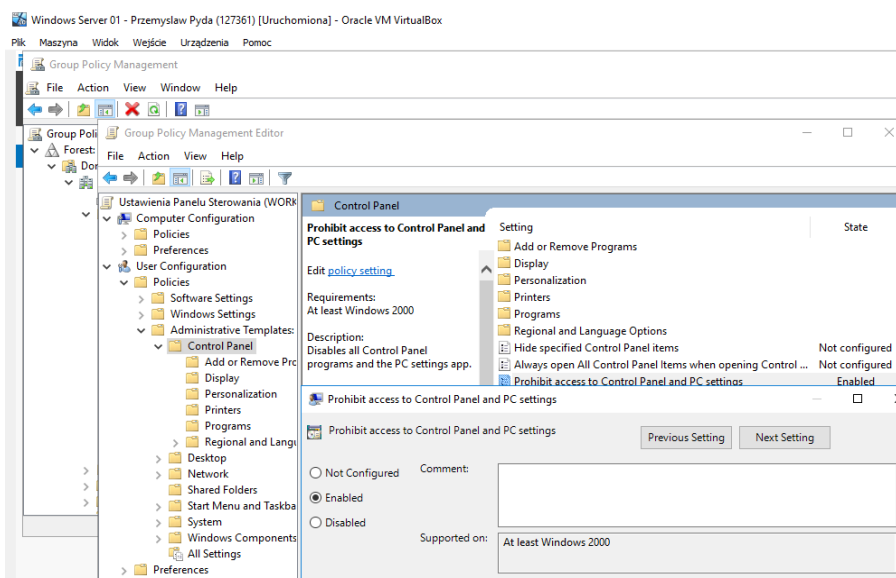
Przed procesem logowania do domeny przed użytkownikiem pojawia się ekran informujący o danych kontaktowych do administratora. Dane te mogą zostać wykorzystane w przypadku problemów z logowaniem bądź dostępem do jakiegokolwiek usługi. Konfiguracja opiera się na stworzeniu GPO i ustawieniach bezpieczeństwa dla lokalnych polityk komputera.



Rysunek 5.10.1 Ustawienie banneru logowania. Opracowanie własne

## 5.11. Blokada dostępu do panelu sterowania

Użytkownicy z grupy „Workers” nie powinni mieć dostępu do panelu sterowania. Konfiguracja opiera się na stworzeniu GPO i ustawieniu panelu sterowania w szablonach administracyjnych użytkownika domenowego. Dodatkowo wymagane jest określenie filtra Security Filtering na określoną grupę użytkowników „Workers”.



Rysunek 5.11.1 Blokada Panelu Sterowania dla użytkowników. Opracowanie własne

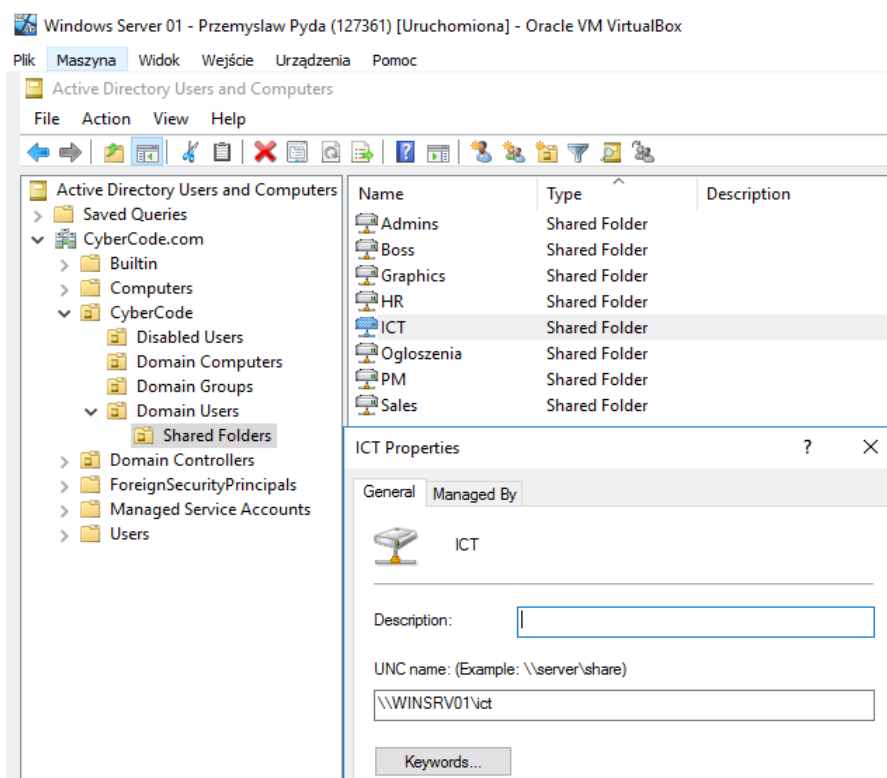
## **5.12. Mapowanie dysków sieciowych**

Każdy z użytkowników powinien mieć dostęp, w oparciu o reguły, do następujących folderów działających jako zmapowane dyski sieciowe:

- Ogłoszenia – litera dysku O: - Dysk z ogłoszeniami i informacjami dostępny dla wszystkich autoryzowanych użytkowników domenowych. Dodawanie plików i prawo do ich edycji posiadają jedynie użytkownicy grupy BOSS oraz HR, użytkownicy pozostałych grup mają uprawnienia jedynie do odczytu plików, bez możliwości ich edycji;
- Folder działowy – litera dysku Z: - Dysk przeznaczony z założenia tylko dla danej grupy użytkowników, reprezentującą dany oddział firmy. Pełne prawa do folderu posiada jedynie dany oddział firmy, zaś dodatkowo dział ADMINS posiada wgląd w foldery działów GRAPHICS ICT, PM i SALES w ramach potencjalnego wsparcia. Użytkownicy grupy ADMINS nie mają dostępu do plików działu BOSS oraz HR. Tylko autoryzowany użytkownik tego działu ma prawo do dostępu do zasobów.

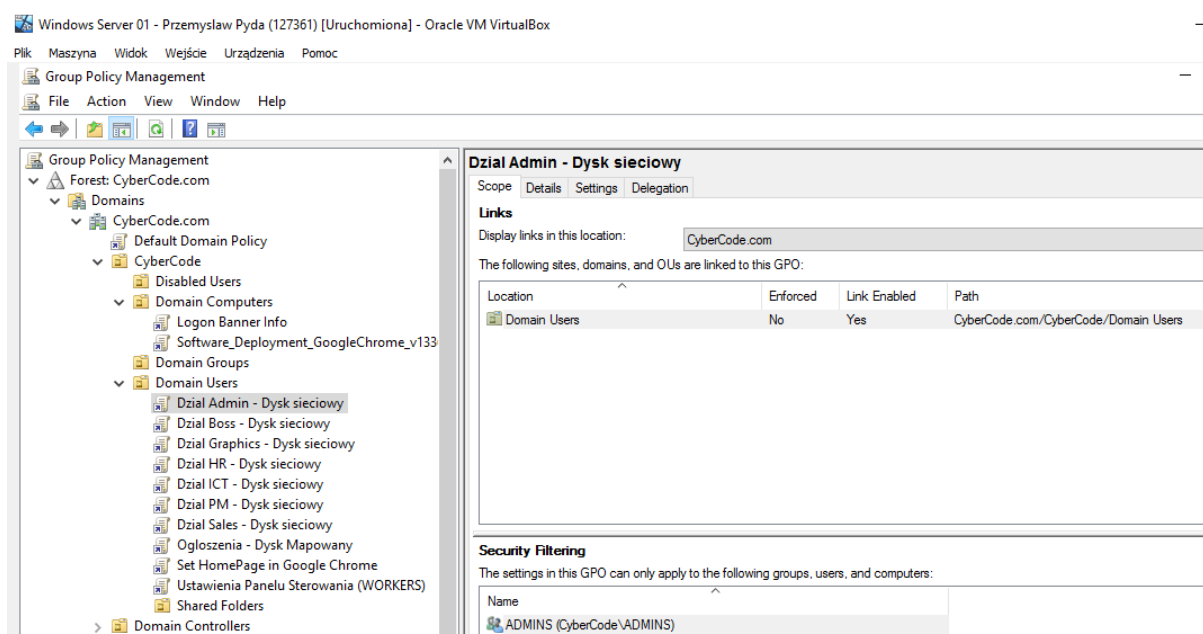
Mapowanie dysków sieciowych odbywa się za pomocą GPO. Jest to skalowalna metoda, zdecydowanie bardziej praktyczna niż przypisywanie folderów udostępnionych w profilach użytkowników. Jest również bezpieczna ze względu na wykorzystanie funkcjonalności „Security Filtering” oraz „Item-level targeting”.

Dla łatwiejszej konfiguracji, w przypadku wielu folderów udostępnianych, można wspomagać się wpisami typu „Shared Folder” w jednostce organizacyjnej „Shared Folders”.

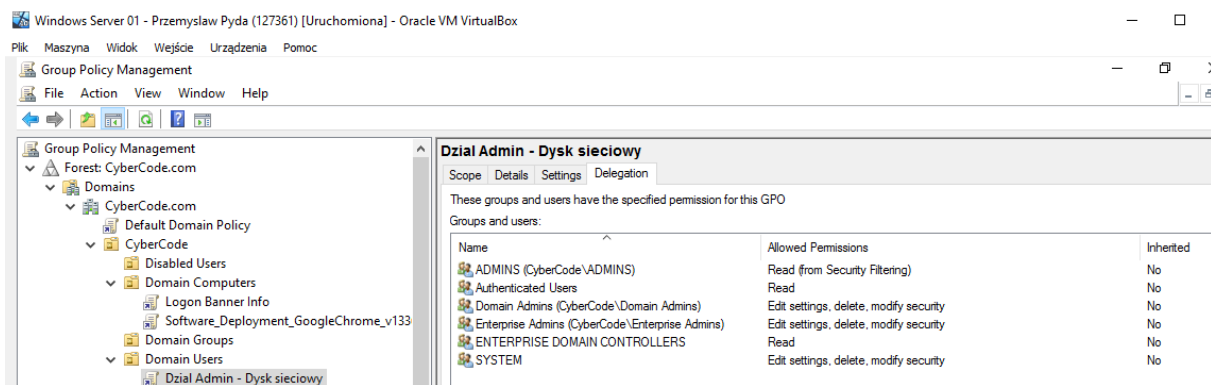


Rysunek 5.12.1 Utworzenie obiektów "Shared Folders". Opracowanie własne

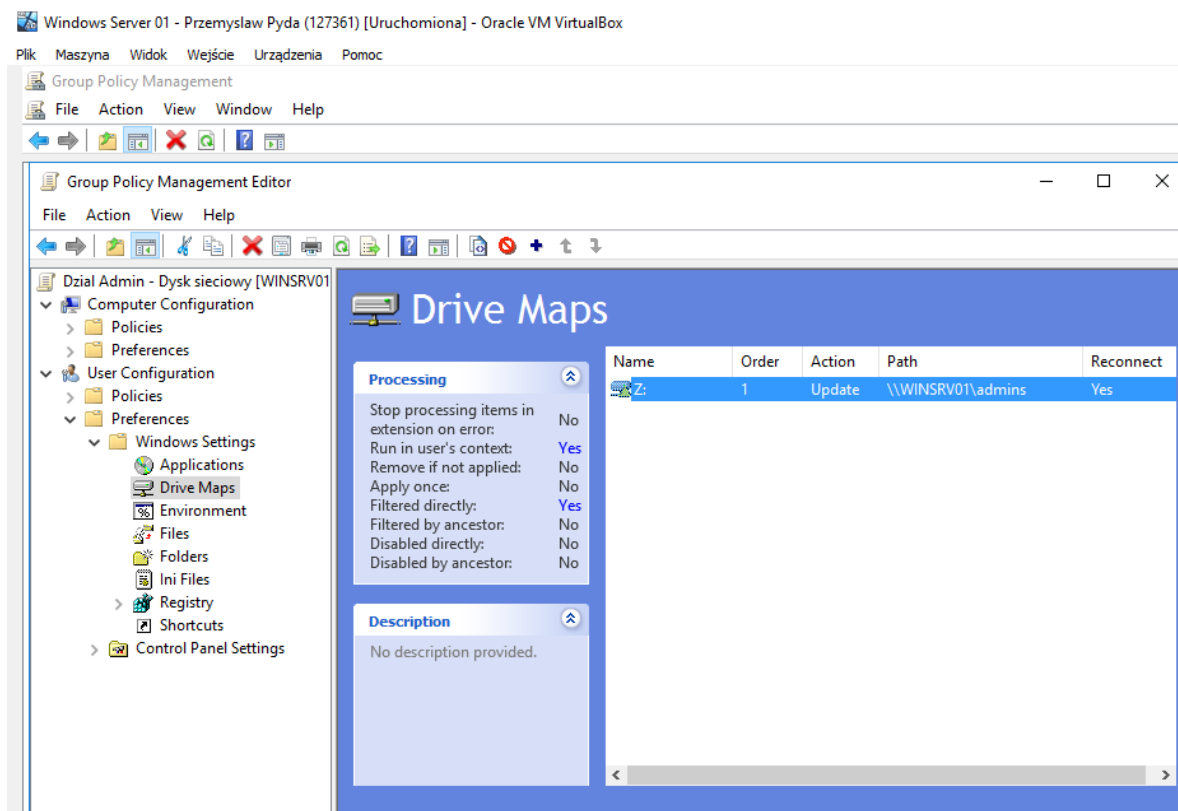
Proces mapowania dysków sieciowych na przykładzie folderu działowego przeznaczonego dla grupy ADMINS oraz folderu z ogłoszeniami znajdują się na zrzutach ekranu poniżej. W przypadku folderów działowych konfiguracja dla innych oddziałów jest analogiczna, dlatego nie zostanie zaprezentowana na zrzutach ekranu.



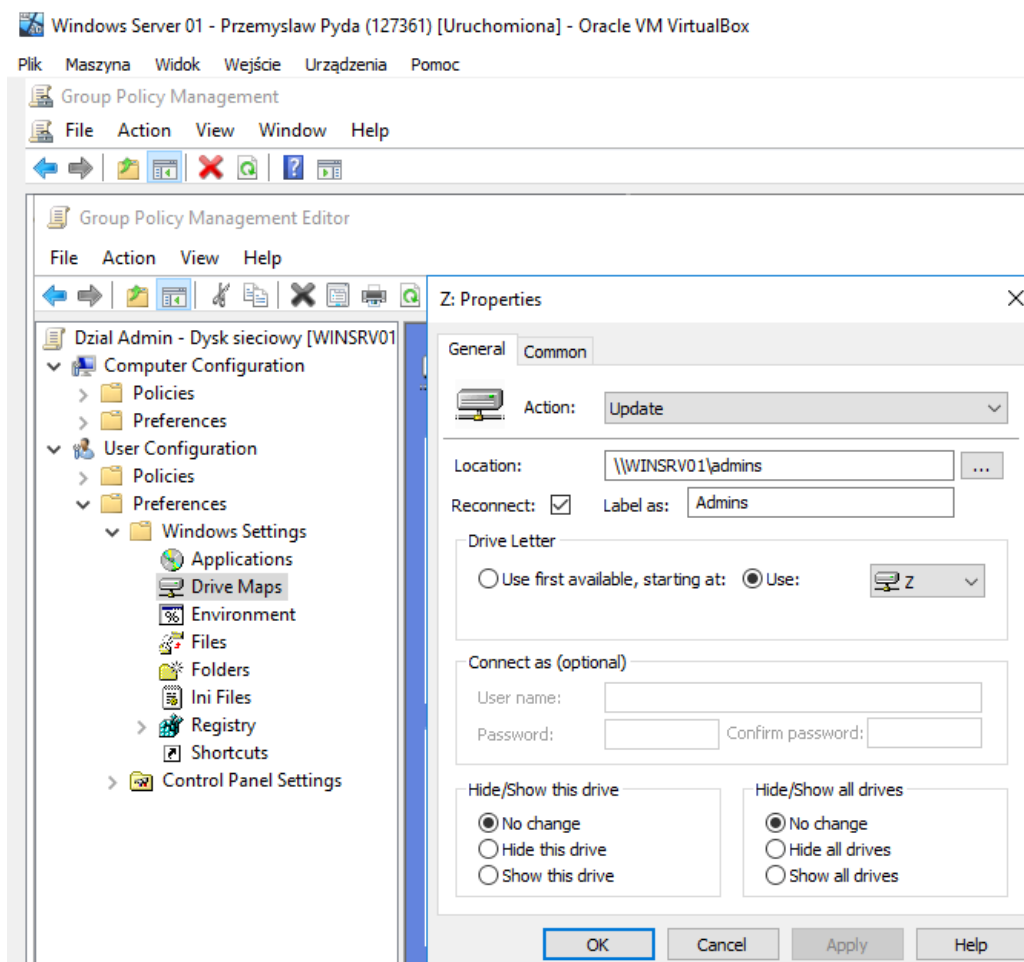
Rysunek 5.12.2 Security Filtering dla GPO. Opracowanie własne



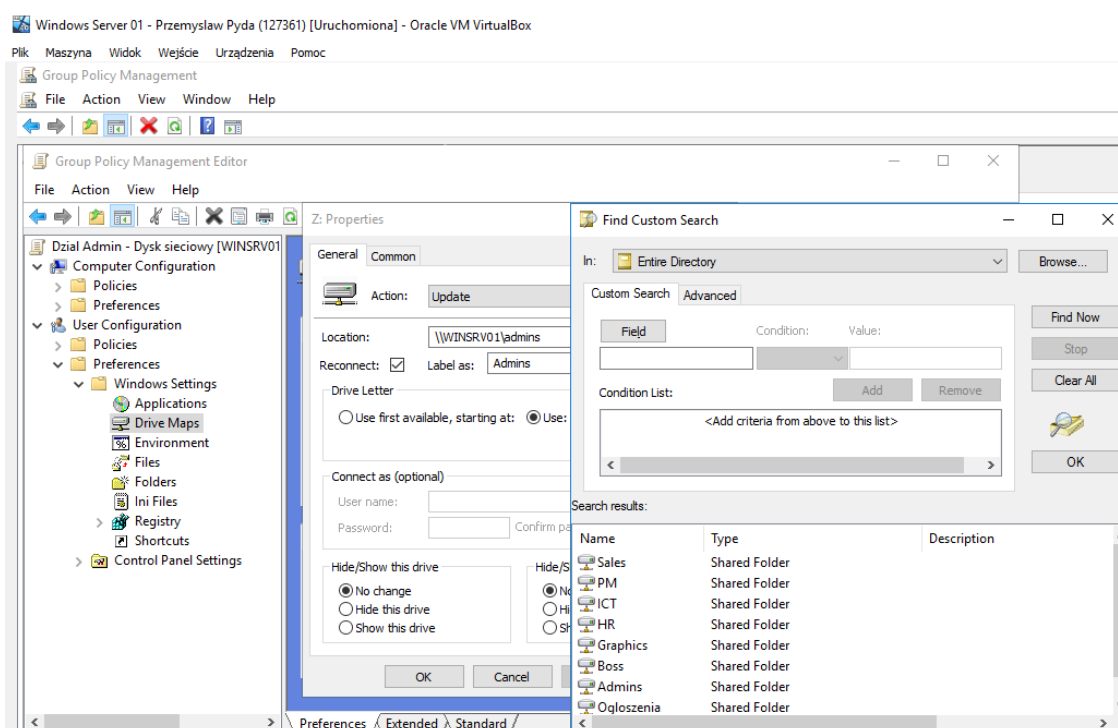
Rysunek 5.12.3 Ustawienia delegacji dla GPO. Opracowanie własne



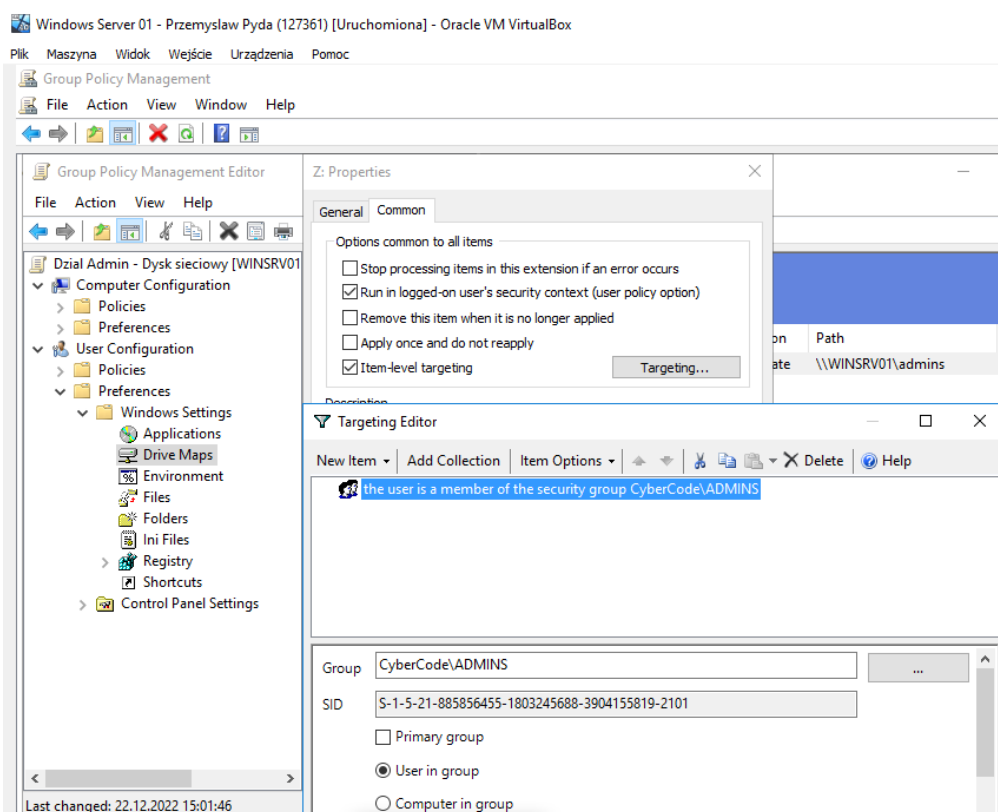
Rysunek 5.12.4 Przypisanie dysku mapowanego dla GPO. Opracowanie własne



Rysunek 5.12.5 Widok "General" dla udostępnionego dysku. Opracowanie własne

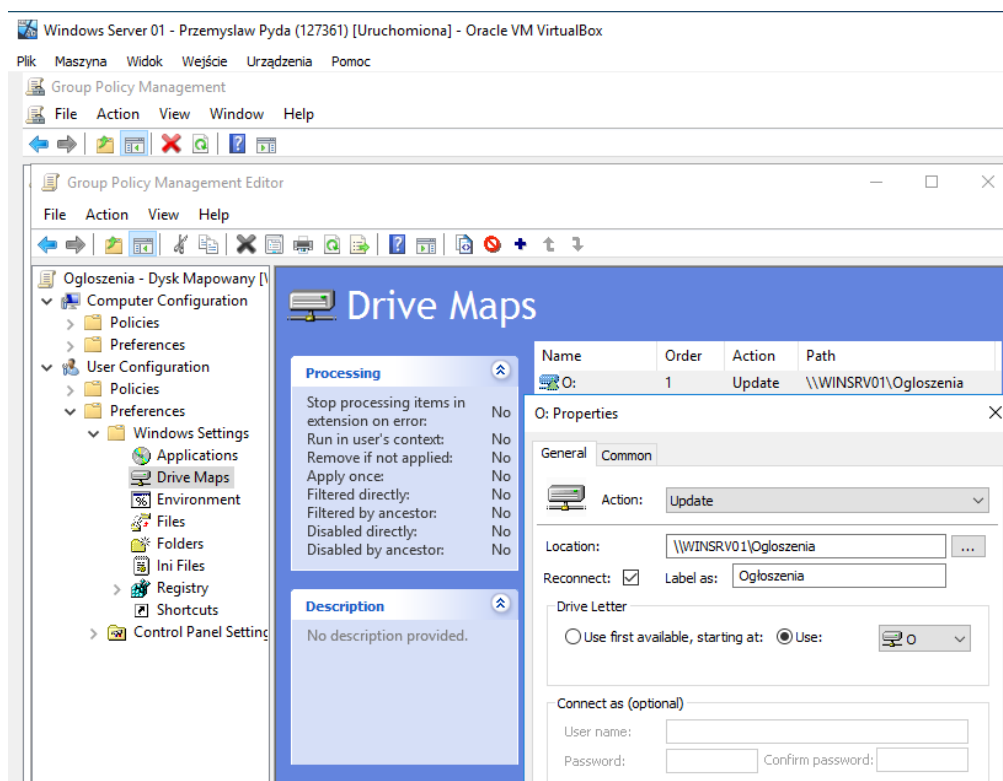


Rysunek 5.12.6 Przypisanie "Shared Folders" mapowanych dysków. Opracowanie własne



Rysunek 5.12.7 Widok "Common". Item-level targeting grupy. Opracowanie własne

W przypadku dysku sieciowego Ogłoszenia, który z założenia jest dostępny dla zautoryzowanych użytkowników, nie są potrzebne żadne dodatkowe ustawienia.



Rysunek 5.12.8 Mapowanie dysku sieciowego "Ogłoszenia". Opracowanie własne

## 6. Proces i testy użytkowania zasobów z perspektywy użytkownika domenowego

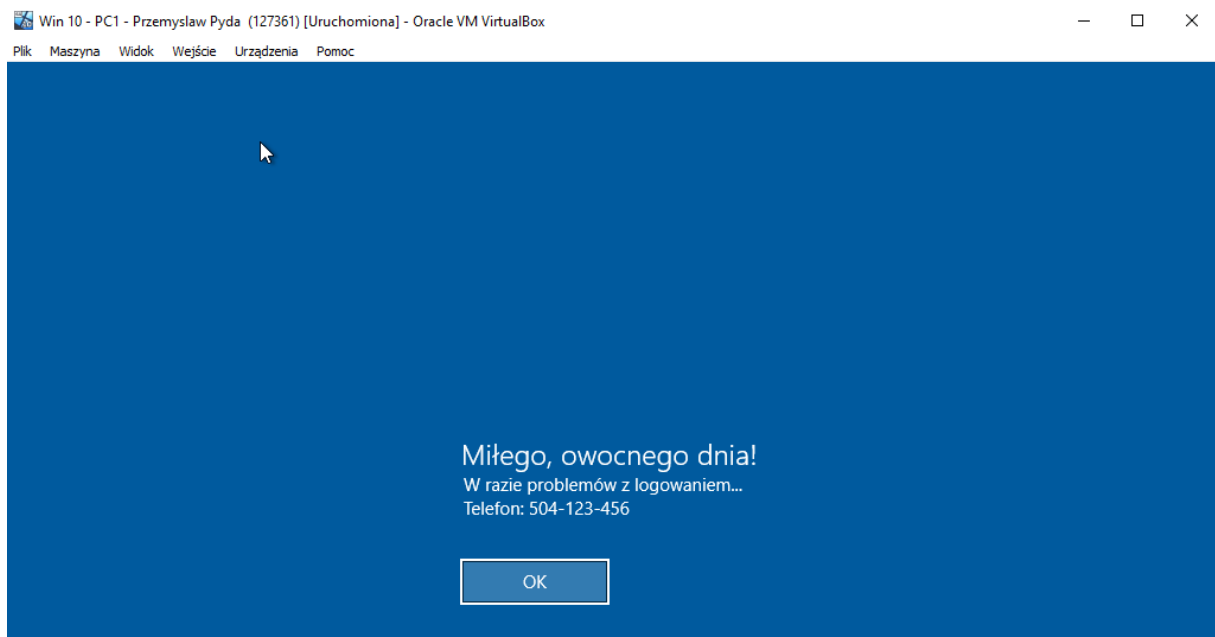
### 6.1. Proces logowania użytkownika

W celu weryfikacji poprawności wdrożeń i konfiguracji, realizowanych przy pomocy Windows Server 2016 oraz fizycznego sprzętu sieciowego Cisco, wykorzystano dwa fizyczne komputery w Sali 108INF i zainstalowano na nich poprzez oprogramowanie Oracle VM VirtualBox systemy klienckie Windows 10, które następnie podłączono do domeny CyberCode.com. Maszynom wirtualnym oraz nazwom komputerów zainstalowanych na tych maszynach wirtualnych nadano odpowiednie nazwy.

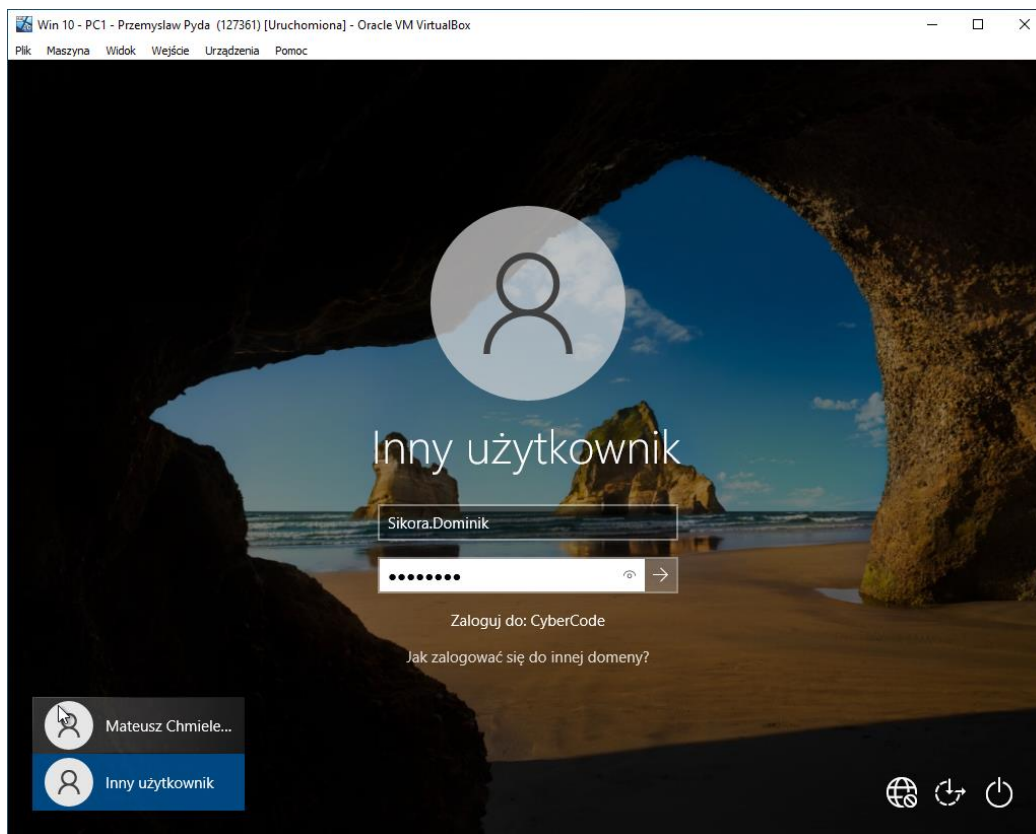
Testy użytkowania zasobów domenowych przeprowadzono na komputerze wirtualizowanym o nadanej nazwie systemowej PC-001.

Podczas testów będziemy wykorzystywać konta dwóch użytkowników domenowych:

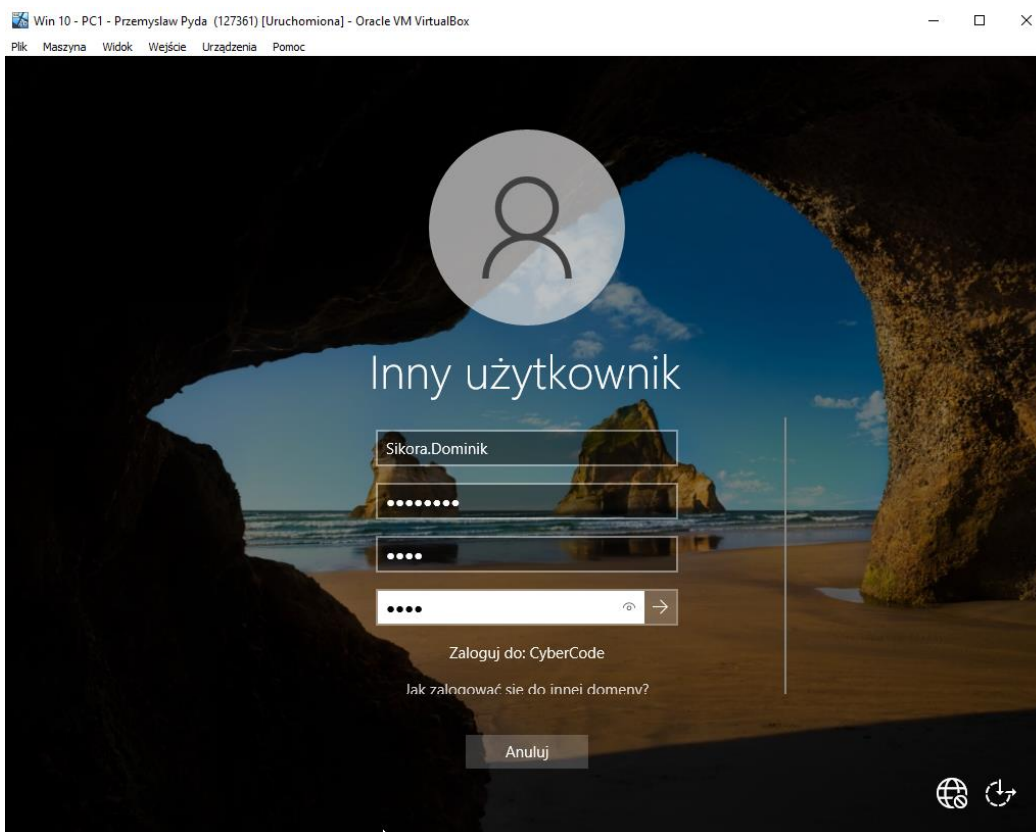
- Dominik Sikora – pracownik grupy ICT
- Mateusz Chmielewski – kadra zarządcza – grupy BOSS



Rysunek 6.1.1 Banner logowania na systemie Windows 10. Opracowanie własne

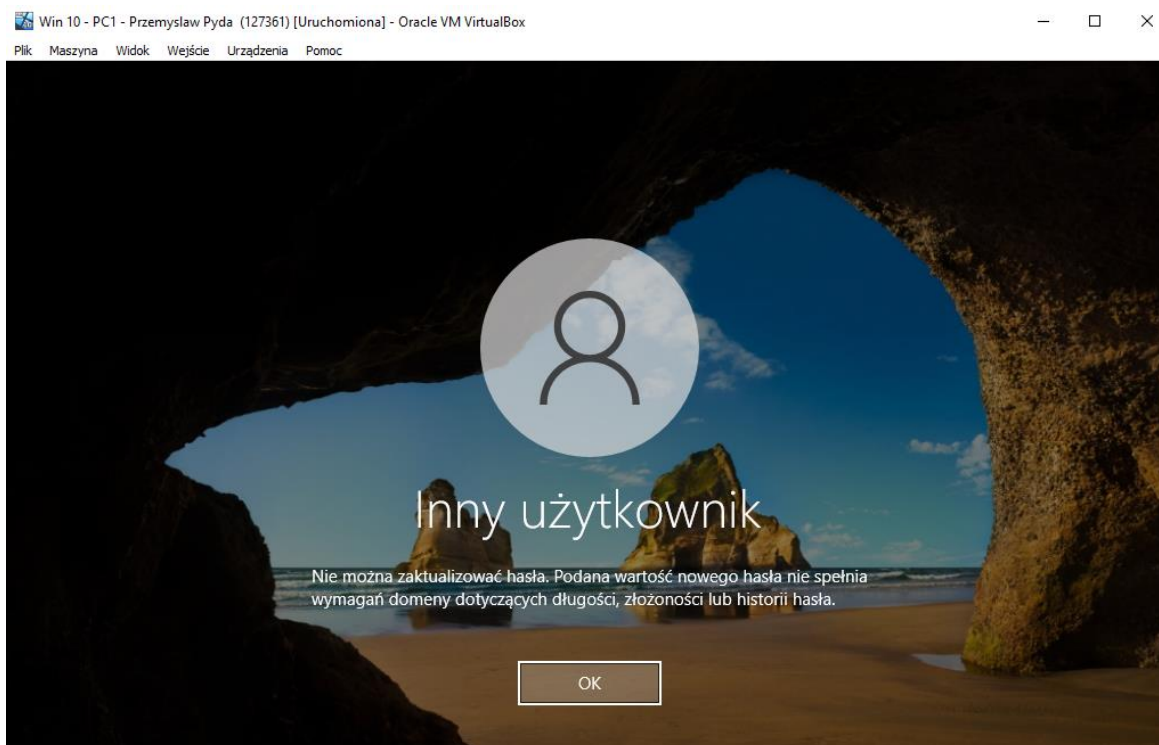


Rysunek 6.1.2 Pierwsze logowanie użytkownika. Opracowanie własne

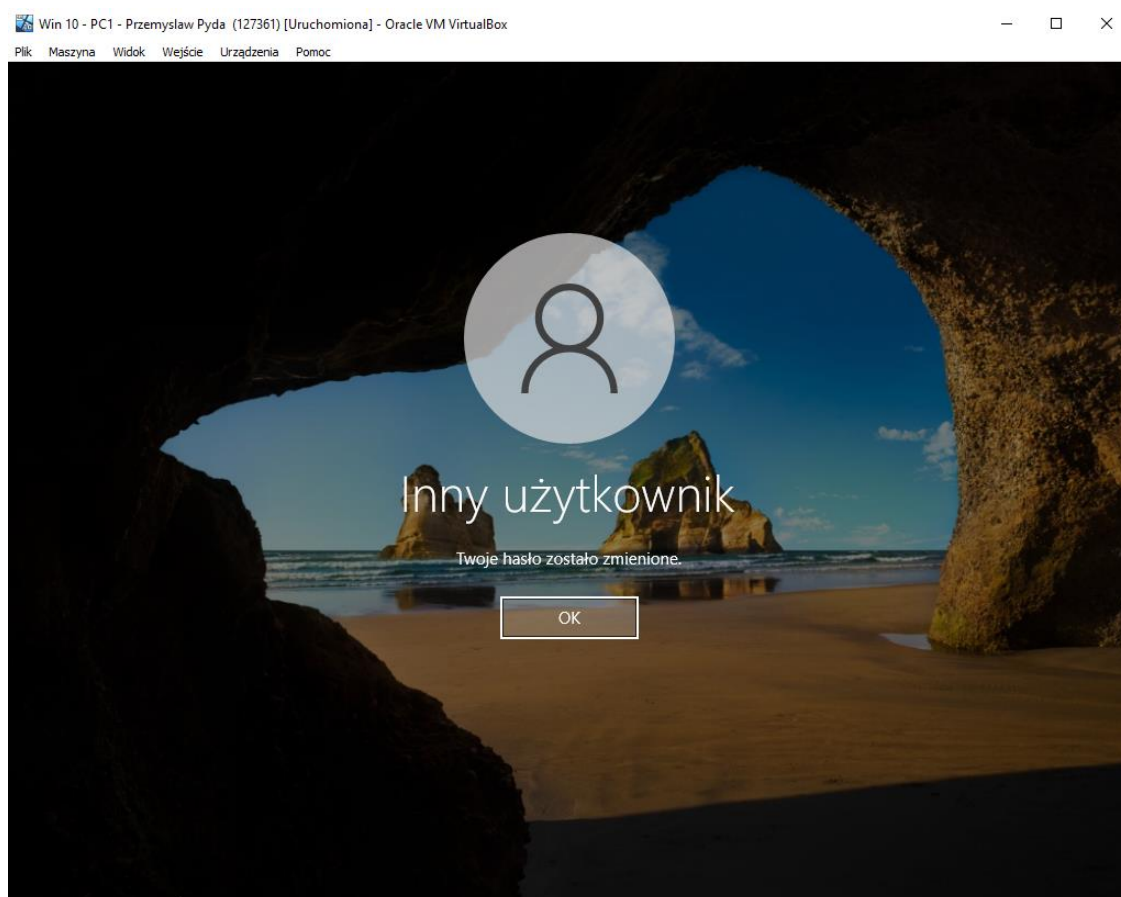


Rysunek 6.1.3 Wymuszona zmiana hasła przy pierwszym logowaniu. Opracowanie własne

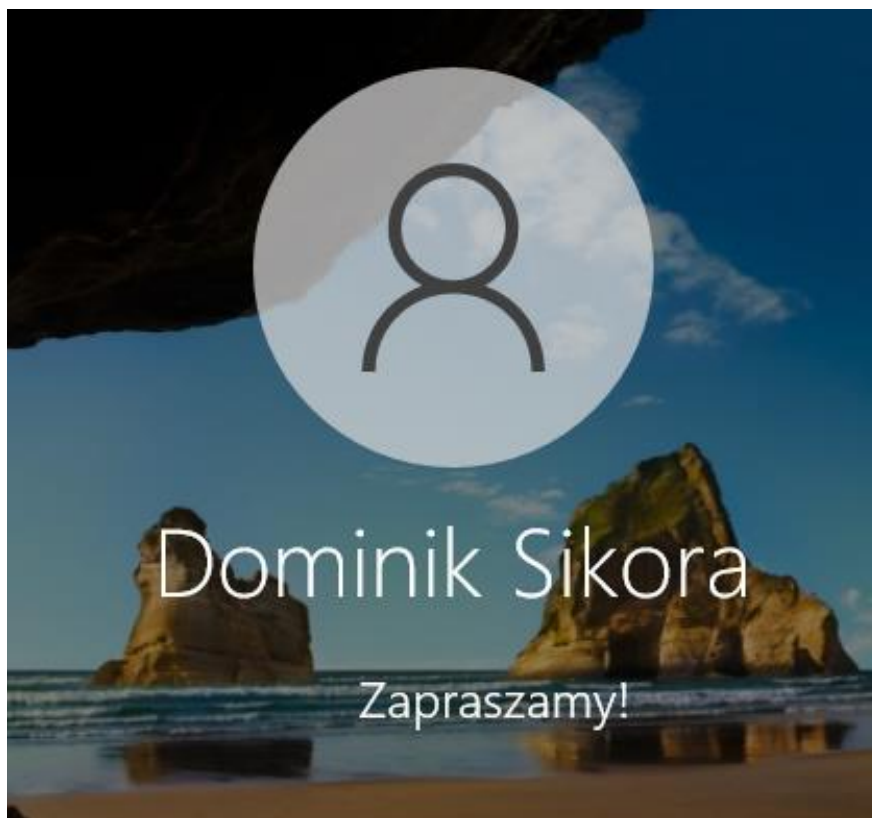




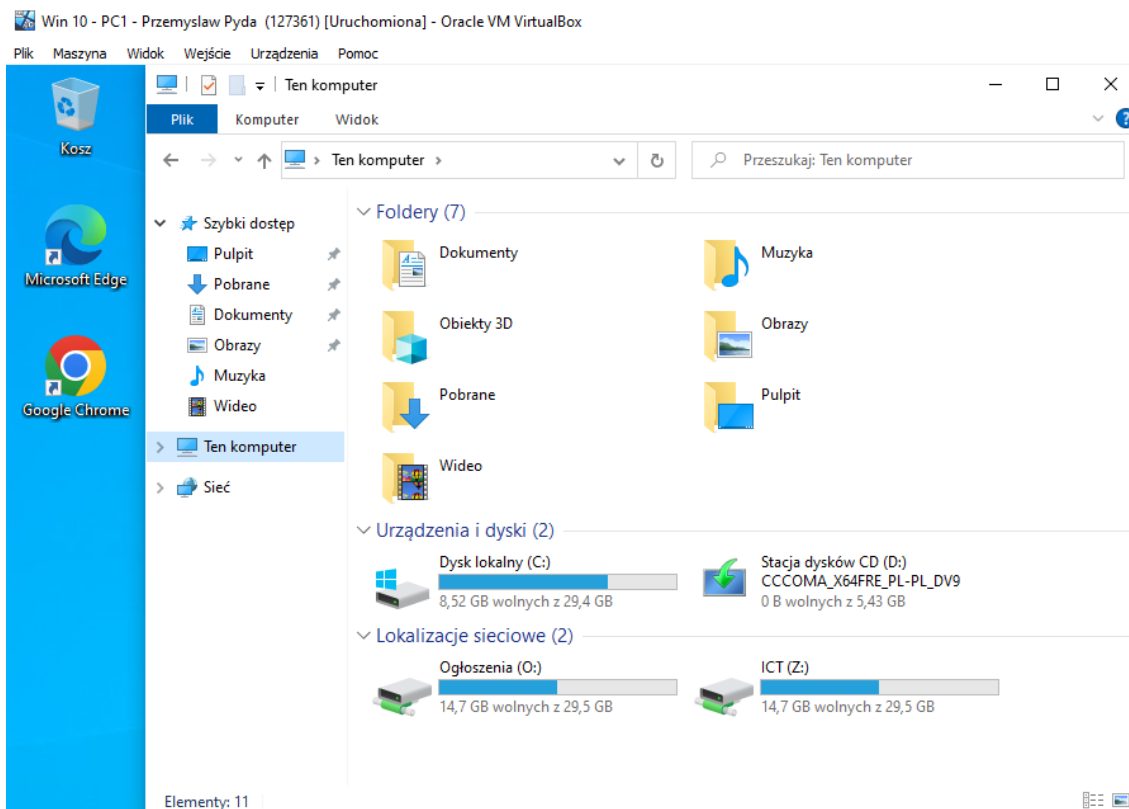
Rysunek 6.1.4 Hasło 4-znakowe nie spełnia wymogów. Opracowanie własne



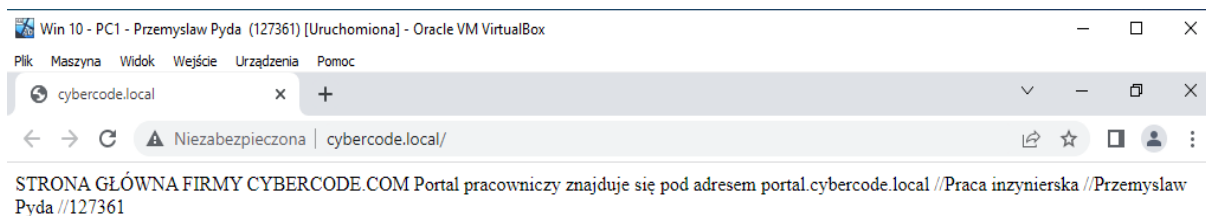
Rysunek 6.1.5 Ustawienie hasła spełniającego wymogi. Opracowanie własne



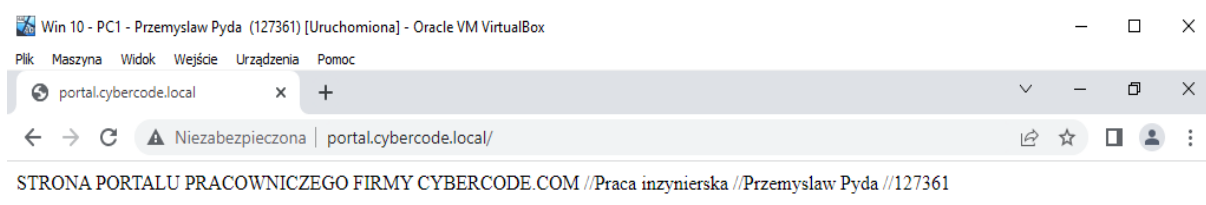
Rysunek 6.1.6 Pomyślne pierwsze logowanie użytkownika. Opracowanie własne



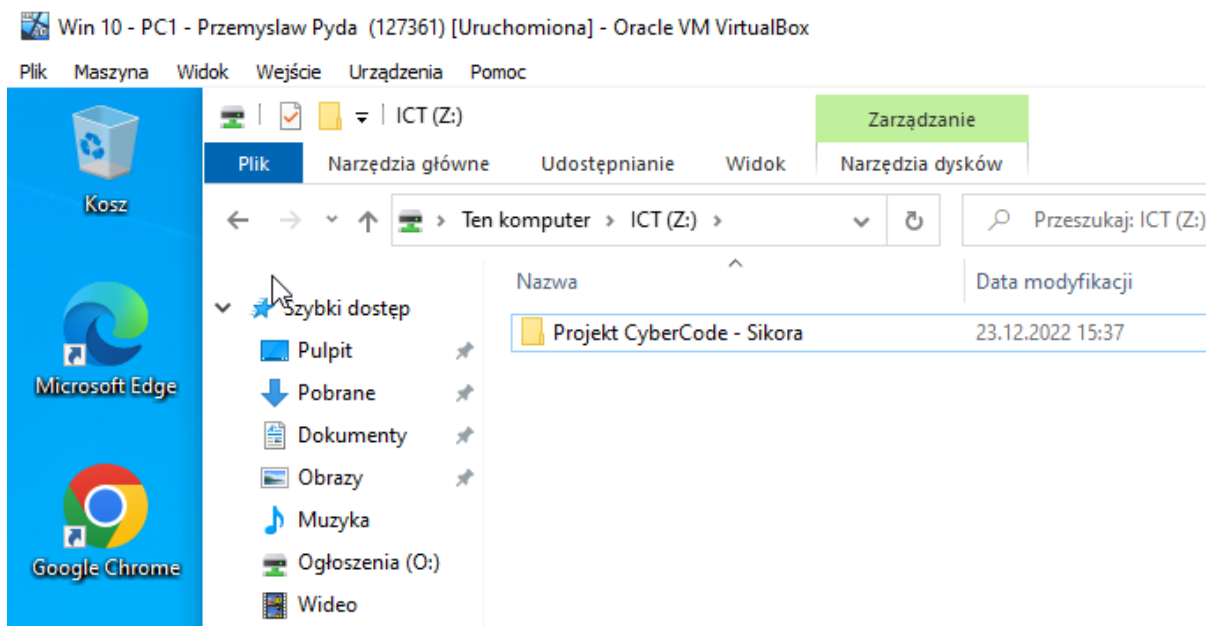
Rysunek 6.1.7 Widok Eksploratora dla grupy ICT. Opracowanie własne



Rysunek 6.1.8 Strona główna cybercode.local. Opracowanie własne

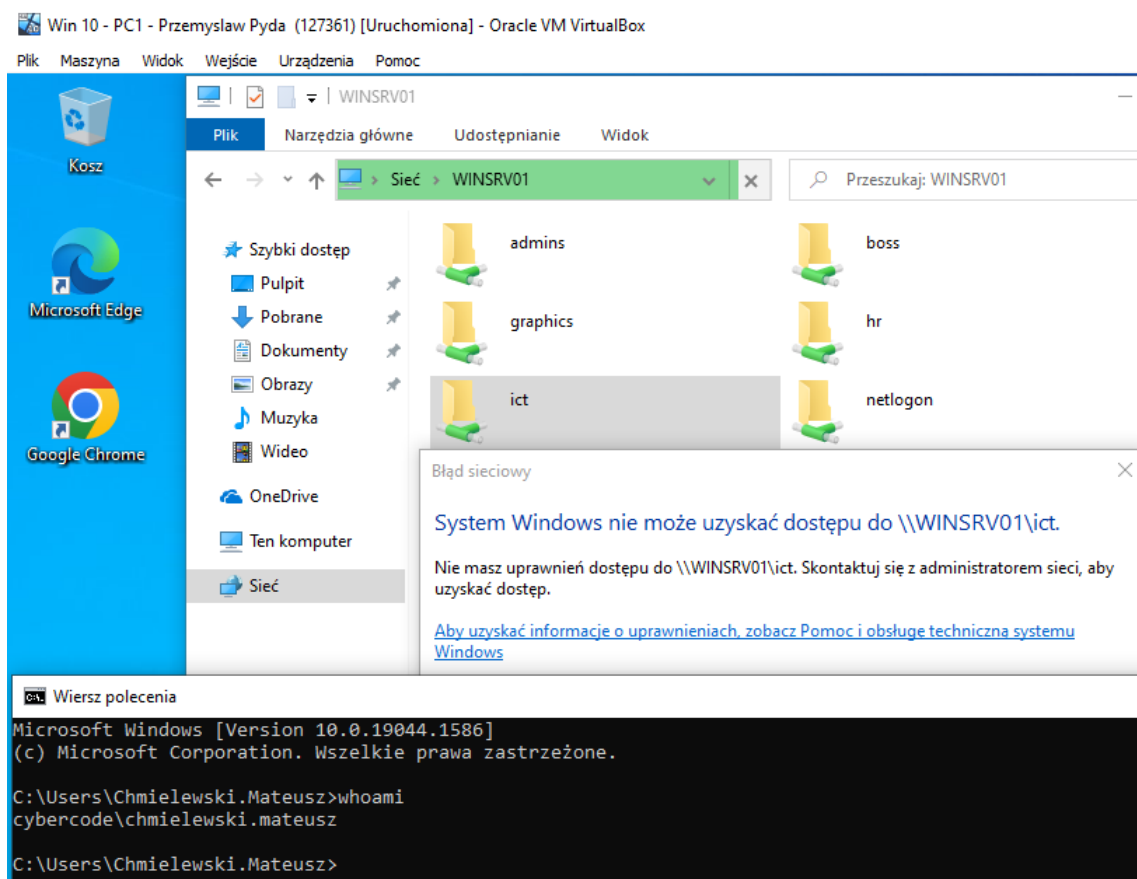


Rysunek 6.1.9 Strona portalu pracowniczego portal.cybercode.local.. Opracowanie własne



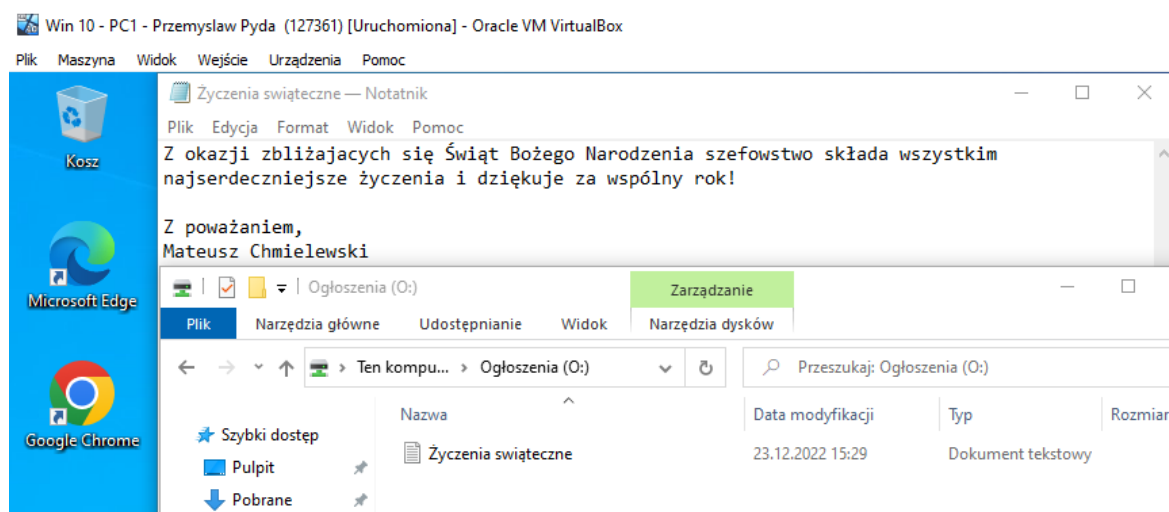
Rysunek 6.1.10 Edycja folderu sieciowego przez konto uprawnione. Opracowanie własne

Kontynuujemy testowanie, zmieniając aktywnego użytkownika na Mateusza Chmielewskiego. Jak widać, nawet użytkownik z grupy BOSS nie ma dostępu do folderów udostępnionych dla innych działów, nawet odwołując się bezpośrednio do lokalizacji sieciowej \\WINSRV01.



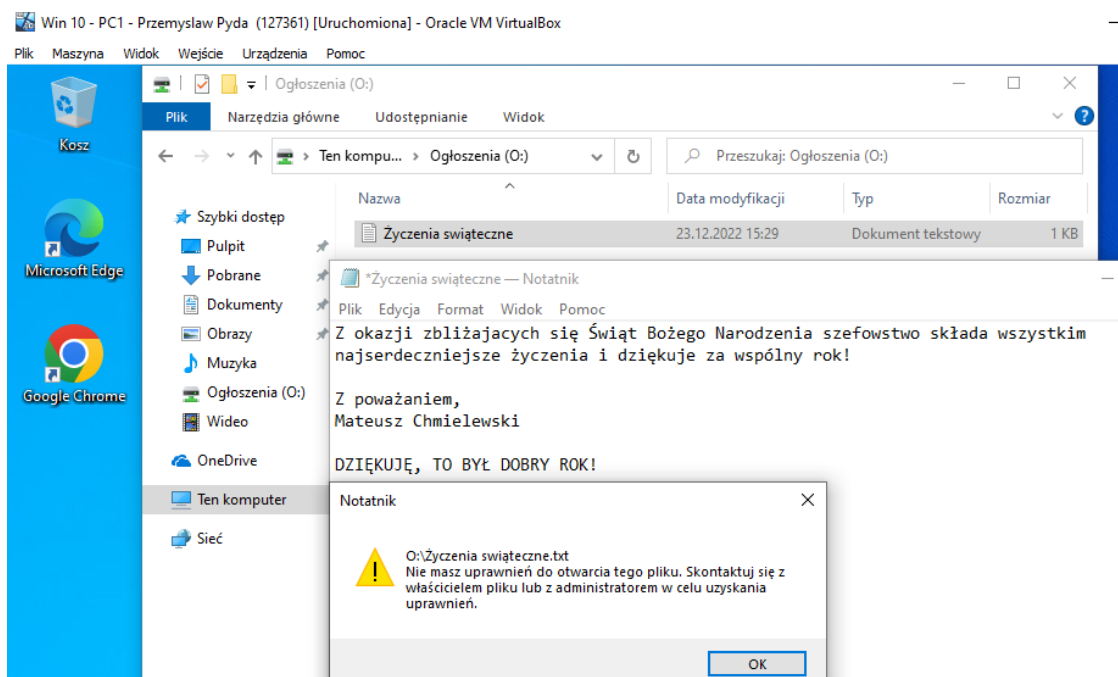
Rysunek 6.1.11 Próba dostępu do nieuprawnionego zasobu. Opracowanie własne

Kolejnym testem jest utworzenie pliku w ogólnodostępnym folderze Ogłoszenia. Tylko użytkownicy grup BOSS i HR mają prawa do modyfikacji zawartości. Jak widać, użytkownik Mateusz Chmielewski jest w stanie utworzyć plik i go modyfikować.



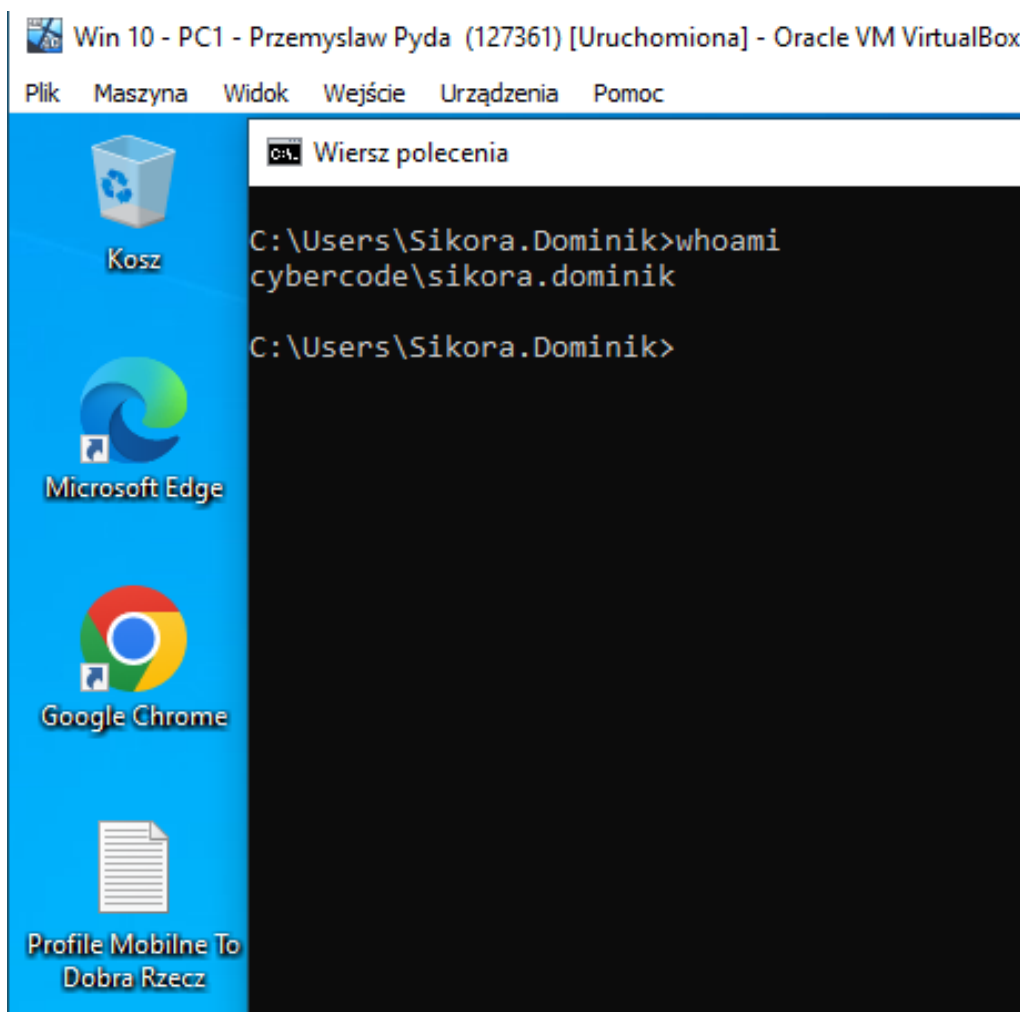
Rysunek 6.1.12 Utworzenie ogłoszenia przez członka grupy BOSS. Opracowanie własne

Wracamy do użytkownika Dominika Sikory. Na rysunku 67 można zobaczyć, że ma on dostęp do folderu z ogłoszeniami, potrafi również otworzyć plik utworzony przez użytkownika z grupy BOSS, jednak nie może wprowadzić żadnych zmian w strukturze pliku – przy próbie zapisu pliku następuje błąd.



Rysunek 6.1.13 Zakaz edycji pliku przez nieuprawnione konto. Opracowanie własne

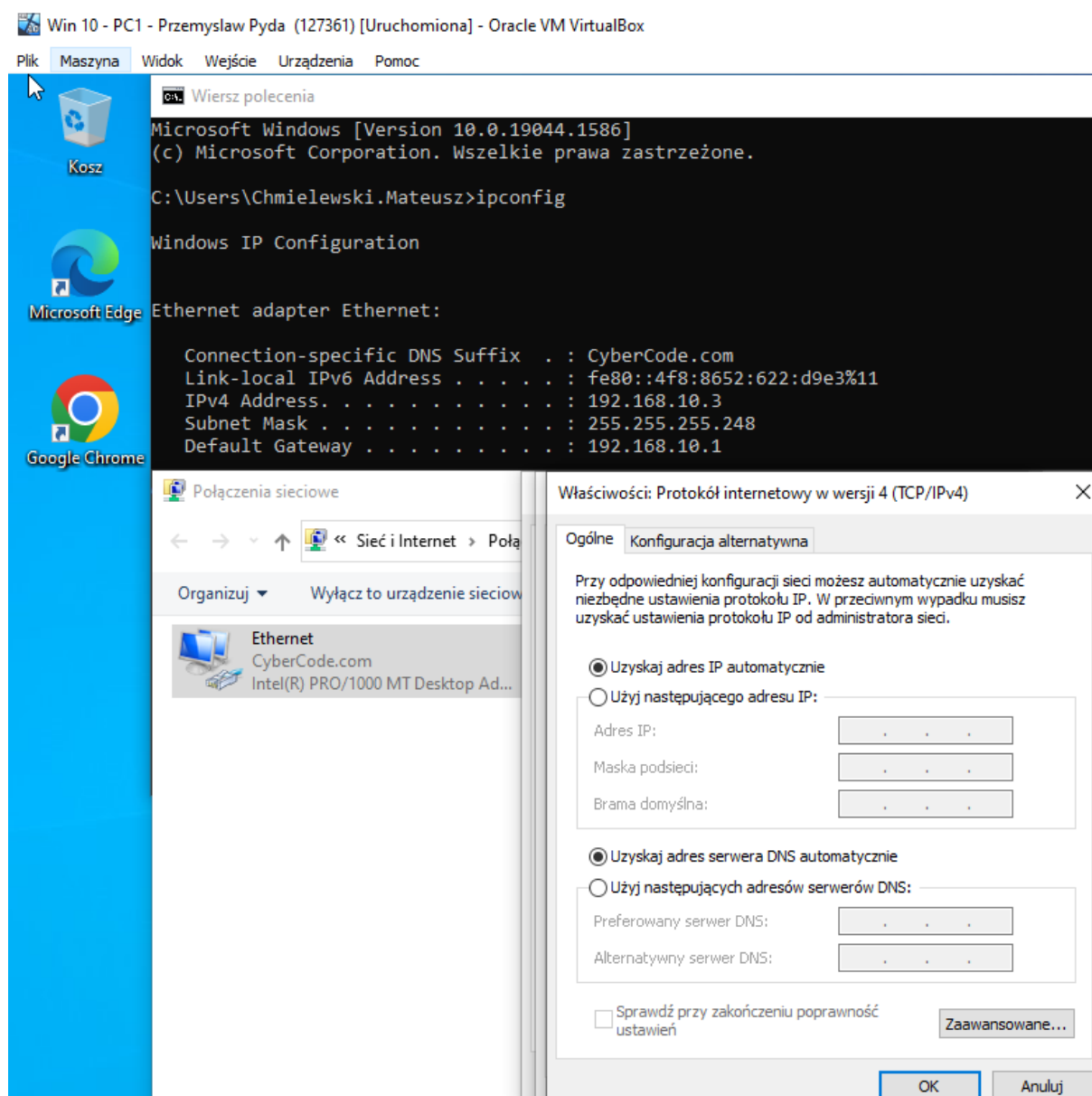
Poniższy zrzut ekranu prezentuje utworzenie pliku na pulpicie. Dzięki funkcjonalności profilu mobilnego plik ten będzie dostępny dla użytkownika, nawet jeżeli zaloguje się na innym komputerze domenowym.



Rysunek 6.1.14 Plik synchronizowany profilem mobilnym

## 6.2. Testy połączeń sieciowych – Windows 10

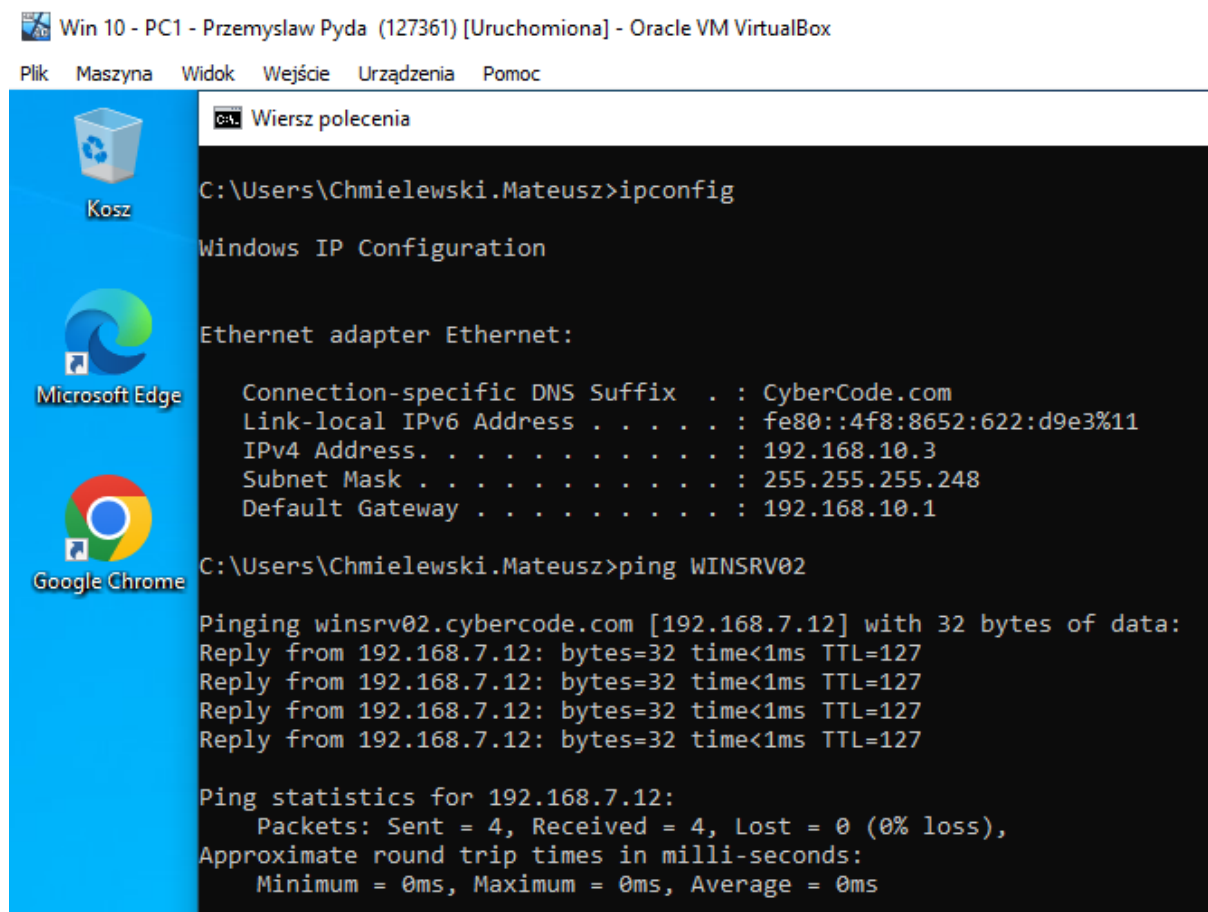
Poniższy zrzut ekranu pokazuje ustawienia karty sieciowej w komputerze domenowym. Jak widać, proces uzyskania automatycznie adresacji IP przebiegł pomyślnie. W poniższym przykładzie użytkownikiem jest Mateusz Chmielewski, którego komputer należy do sieci VLAN o numerze 10 (adresacja 192.168.10.0/29) oraz korzysta z puli DHCP BOSS\_Scope.



Rysunek 6.2.1 Tryb automatyczny TCP/IPv4. Klient DHCP. Opracowanie własne



Na poniższym zrzucie ekranu wykonujemy test usługi DNS. Komputer potrafi rozwiązać nazwę urządzenia WINSRV02 i przetłumaczyć ją na adres IPv4 192.168.7.12. Usługa DNS działa prawidłowo. Dodatkowo przedstawiono działający routing pomiędzy różnymi sieciami VLAN (Inter-VLAN Routing). Podsieć przeznaczona na serwery posiada inną adresację niż podsieć przeznaczona dla członków grupy BOSS.



```
Win 10 - PC1 - Przemyslaw Pyda (127361) [Uruchomiona] - Oracle VM VirtualBox
Plik Maszyna Widok Wejście Urządzenia Pomoc

Wiersz polecenia

C:\Users\Chmielewski.Mateusz>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : CyberCode.com
    Link-local IPv6 Address . . . . . : fe80::4f8:8652:622:d9e3%11
    IPv4 Address. . . . . : 192.168.10.3
    Subnet Mask . . . . . : 255.255.255.248
    Default Gateway . . . . . : 192.168.10.1

C:\Users\Chmielewski.Mateusz>ping WINSRV02

Pinging winsrv02.cybercode.com [192.168.7.12] with 32 bytes of data:
Reply from 192.168.7.12: bytes=32 time<1ms TTL=127
Reply from 192.168.7.12: bytes=32 time<1ms TTL=127
Reply from 192.168.7.12: bytes=32 time<1ms TTL=127
Reply from 192.168.7.12: bytes=32 time<1ms TTL=127

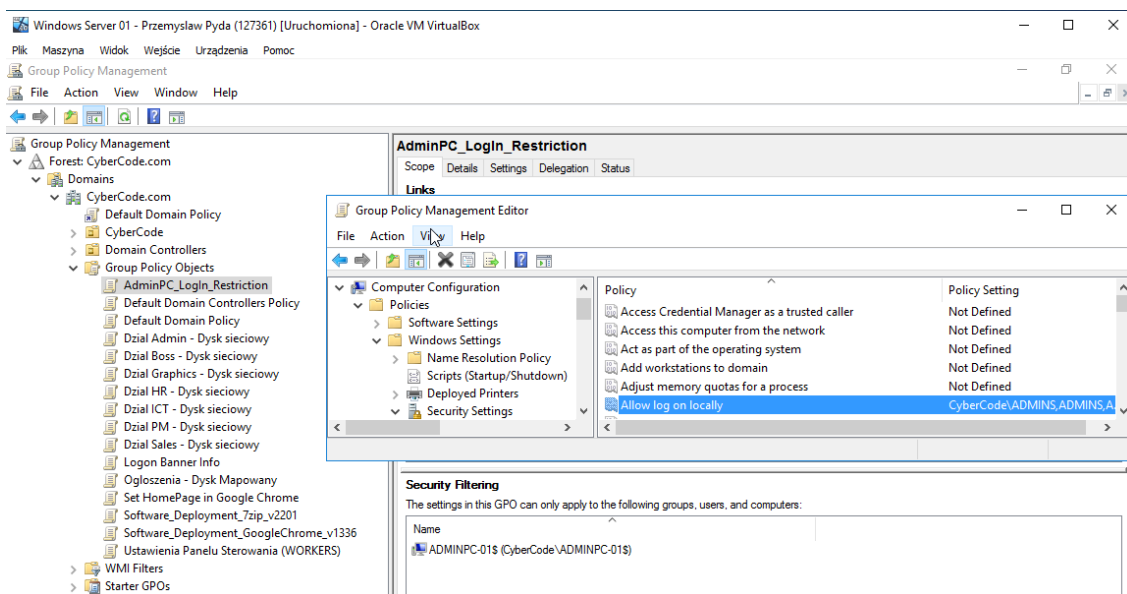
Ping statistics for 192.168.7.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Rysunek 6.2.2 Test połączenia sieciowego z wykorzystaniem DNS. Opracowanie własne

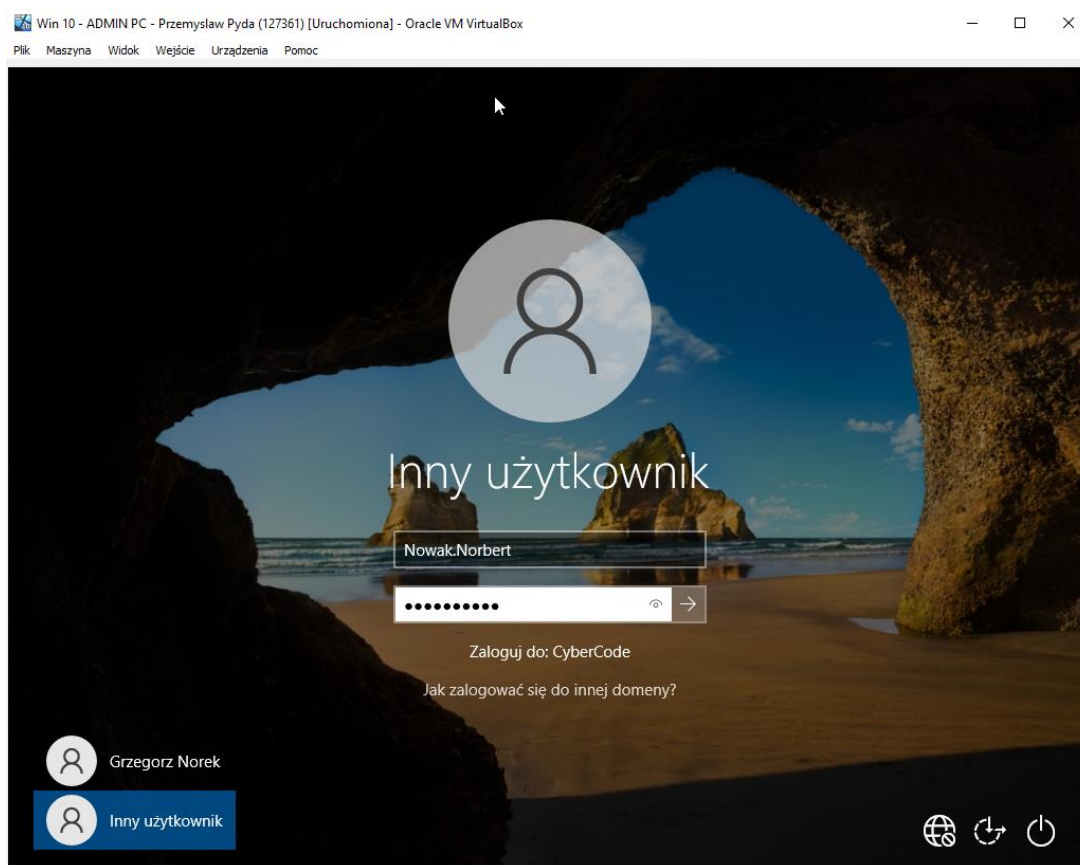


### 6.3. Komputer administracyjny

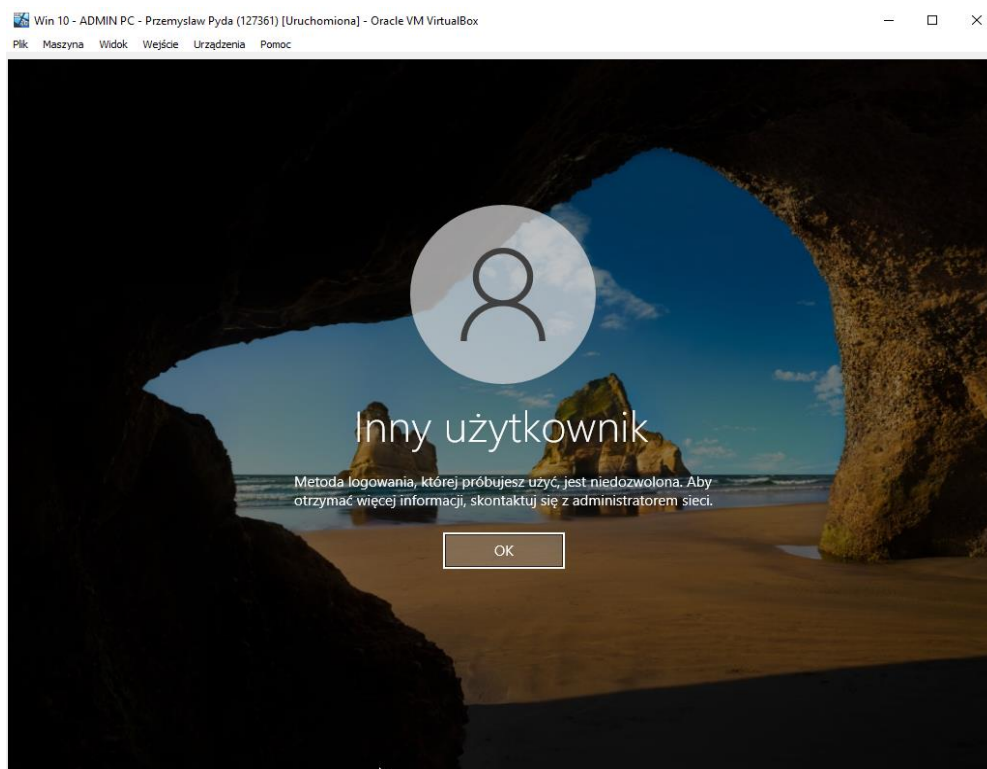
Użytkownicy grupy ADMINS powinni mieć dostęp do komputera administracyjnego, który znajduje się w zamkniętej serwerowni. Inni użytkownicy nie powinni posiadać uprawnień do logowania domenowego na komputerze w serwerowni.



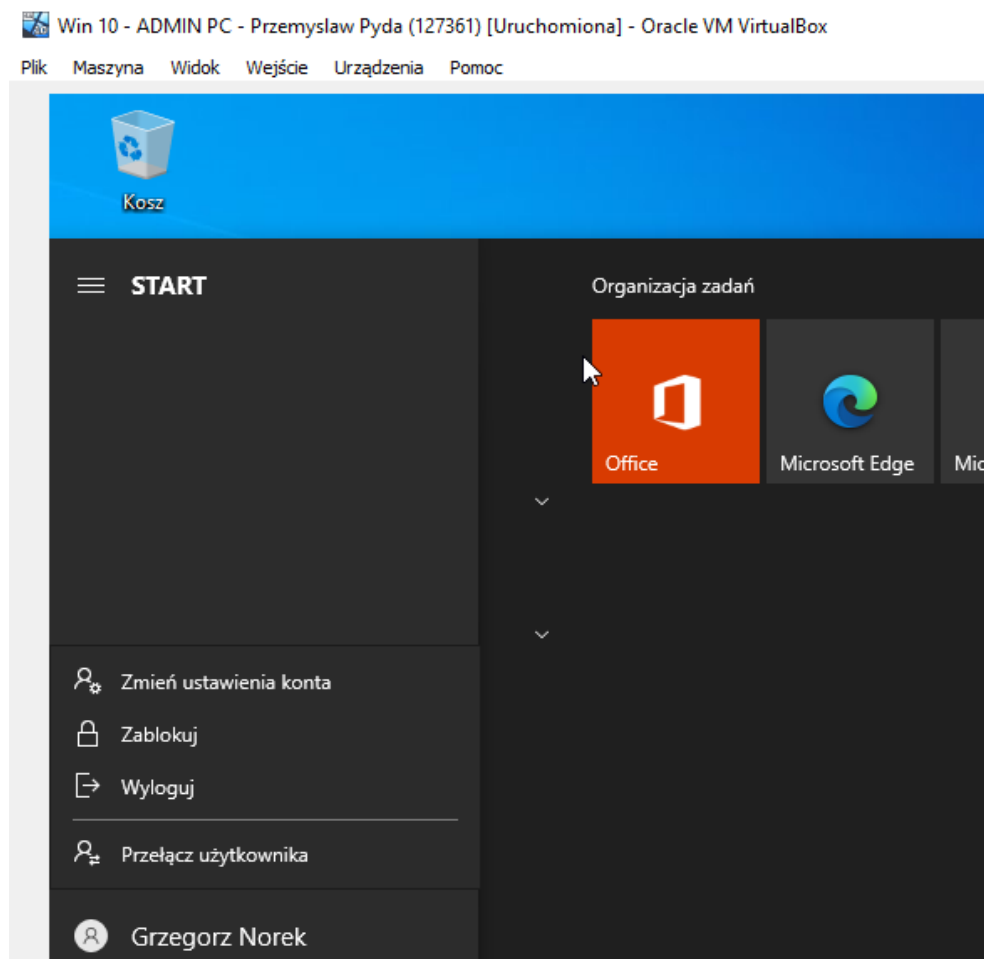
Rysunek 6.3.1 Definiowanie kont uprawnionych do logowania. Opracowanie własne



Rysunek 6.3.2 Próba logowania nieuprawnionego użytkownika. Opracowanie własne



Rysunek 6.3.3 Powiadomienie o niemożliwości zalogowania. Opracowanie własne



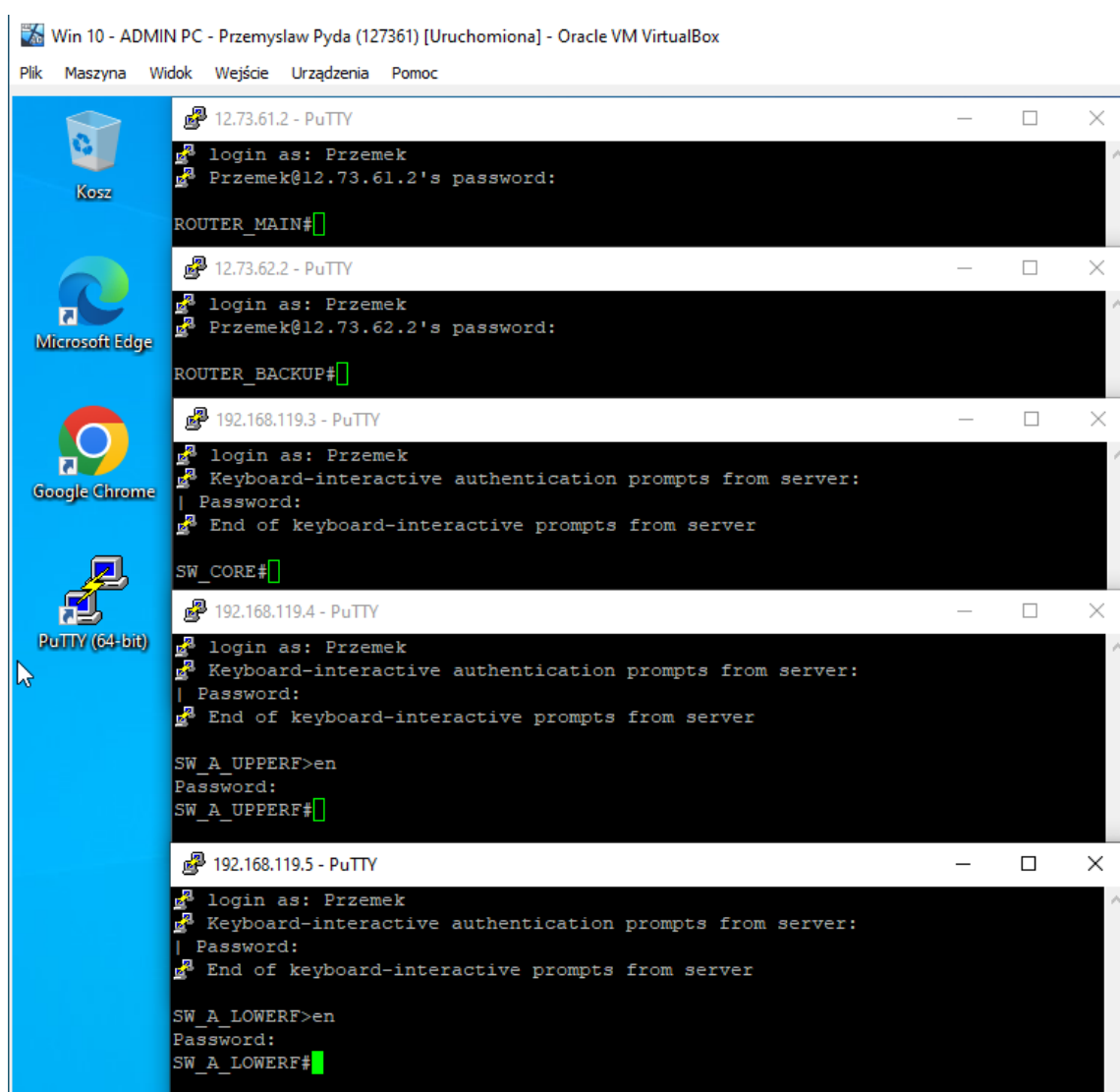
Rysunek 6.3.4 Pomyślnie zalogowany użytkownik grupy ADMINS. Opracowanie własne

## 6.4. Komunikacja SSH z komputera administracyjnego

Zgodnie z założeniami polityki bezpieczeństwa administratorzy powinni mieć możliwość łączenia się do urządzeń sieciowych za pomocą protokołu SSH. Administratorzy powinni móc zdalnie konfigurować urządzenia w bezpieczny, szyfrowany sposób.

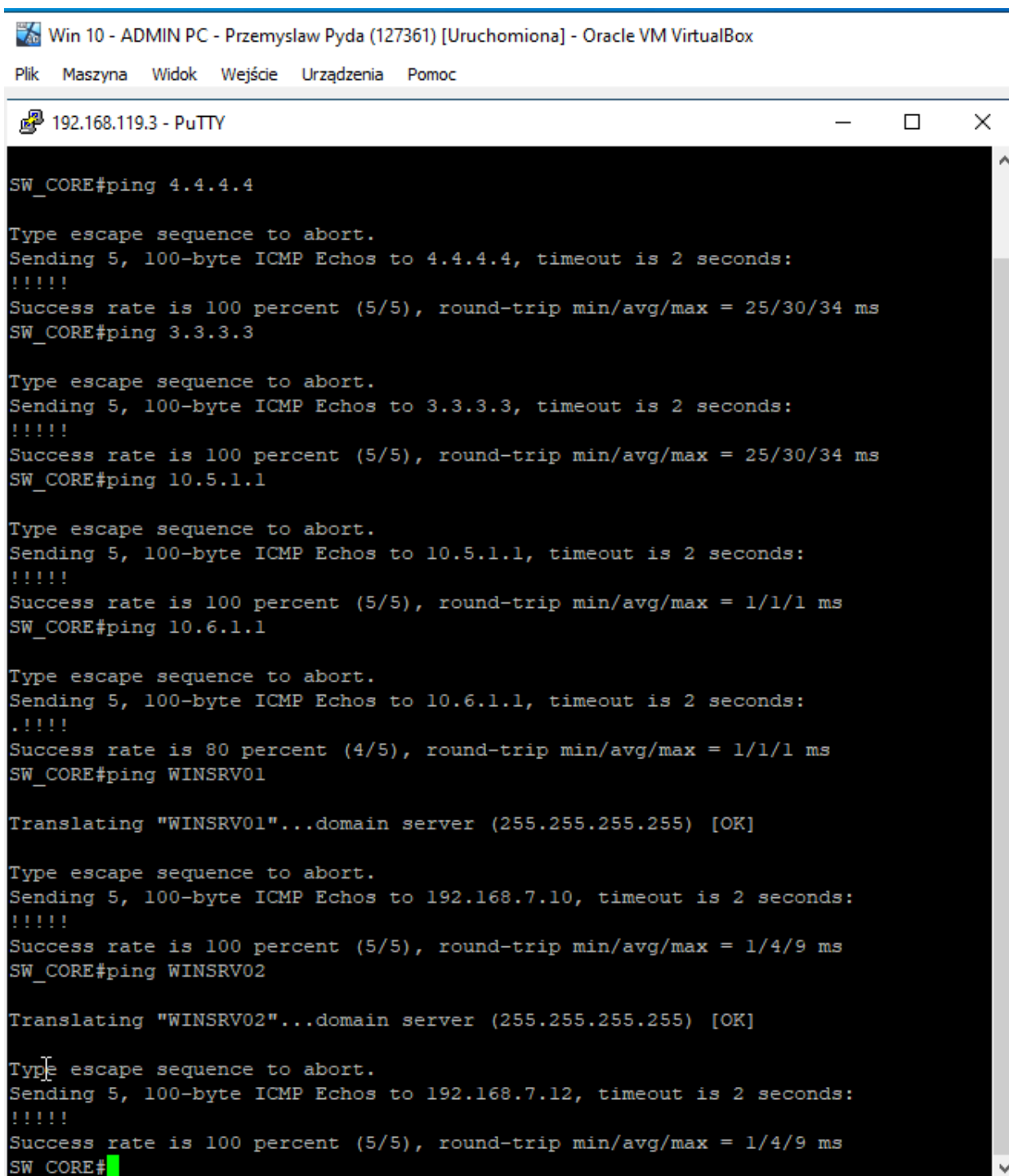
Na urządzeniach sieciowych Cisco zostały spełnione warunki do połączenia SSH – została nadana nazwa domenowa, wygenerowane zostały klucze RSA o złożoności 1024 bitów oraz utworzony użytkownik do logowania przy użyciu protokołu SSH o odpowiednich uprawnieniach. Administrator nie ma możliwości zdalnego logowania się przy użyciu podatnego, nieszyfrowanego protokołu Telnet.

Do testów połączeń wykorzystane zostało darmowe oprogramowanie PuTTY.



Rysunek 6.4.1 Połączenie protokołem SSH do urządzeń sieciowych. Opracowanie własne

Dodatkowo z poziomu SSH zostały wykonane testy połączeń sieciowych z sieciami symulującymi zewnętrzną sieć Internet (interfejsy Loopback w urządzeniu ROUTER\_ISP), z aktywnymi bramami protokołu GLBP oraz serwerami Windows Server przy użyciu nazw mnemonicznych, co jednocześnie sprawdza działanie serwera DNS.



The screenshot shows a PuTTY terminal window titled "192.168.119.3 - PuTTY". The terminal output shows a series of ping commands and their results from a device named SW\_CORE. The tests include pinging IP addresses 4.4.4.4, 3.3.3.3, 10.5.1.1, 10.6.1.1, and WINSRV01, WINSRV02, as well as loopback addresses 192.168.7.10 and 192.168.7.12. The results show success rates of 100% for most tests, except for 10.6.1.1 which has an 80% success rate. The terminal also shows DNS translation for WINSRV01 and WINSRV02 to the IP address 255.255.255.255.

```
SW_CORE#ping 4.4.4.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/30/34 ms
SW_CORE#ping 3.3.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 3.3.3.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 25/30/34 ms
SW_CORE#ping 10.5.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.5.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
SW_CORE#ping 10.6.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.6.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
SW_CORE#ping WINSRV01
Translating "WINSRV01"...domain server (255.255.255.255) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
SW_CORE#ping WINSRV02
Translating "WINSRV02"...domain server (255.255.255.255) [OK]
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.12, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/9 ms
SW_CORE#
```

Rysunek 6.4.2 Symulowana sieć Internet, testy sieciowe. Opracowanie własne

## **7. Bezpieczeństwo infrastruktury**

Zachowanie odpowiedniego poziomu bezpieczeństwa powinno znajdować się w gestii administratorów, odpowiedzialnych za koordynowaną infrastrukturę. Dodatkowo w kwestiach bezpieczeństwa należy zachować balans pomiędzy zdrowym rozsądkiem a praktycznymi aspektami bezpieczeństwa. Wprowadzenie wymogu 18 znakowego hasła, z wymogiem jego zmiany co 2 tygodnie, jest w teorii wyjątkowo bezpieczne, jednakże w praktyce użytkownicy nie korzystający z menedżerów haseł nie będą mieli możliwości ich zapamiętania. Może to przełożyć się, prawdopodobnie, na zapisywanie haseł na karteczkach przyklepanych do biurka czy monitora, co niweczy szczere starania administratorów, gdyż trzeba mieć na uwadze ochronę przez zagrożeniami zarówno z zewnątrz, jak i wewnątrz.

Dodatkowo sieć powinna być możliwie wysoce bezawaryjna, zaś kluczowe urządzenia w infrastrukturze powinny pracować redundantnie, by zwiększyć odporność na awarie. Kwestia bezpieczeństwa infrastruktury sieciowej została wymieniona i opisana w powyższych rozdziałach. Grupując poprzednie rozdziały opisujące podjęte działania w aspekcie bezpieczeństwa zewnętrznego i wewnętrznego, można do nich zaliczyć:

### **7.1. Bezpieczeństwo budynku**

- Zamykane na klucz szafy serwerowe w głównym punkcie dystrybucyjnym (serwerownia) oraz w lokalnym punkcie dystrybucyjnym (podwieszana szafa serwerowa na piętrze). Dostęp do szaf rackowych mają jedynie administratorzy;
- W przyszłości zaimplementowany zostanie system kontroli dostępu, opierający się na wykorzystaniu kart magnetycznych.

### **7.2. Bezpieczeństwo dostępu administracyjnego**

- Do komputera przeznaczonego do zarządzania siecią logować domenowo mogą się jedynie administratorzy;
- Do zdalnego zarządzania urządzeniami sieciowymi wykorzystywany jest bezpieczny i szyfrowany protokół SSH. Logowanie przy pomocy protokołu TELNET jest zabronione;
- Hasło użytkownika do logowania SSH jest tajne i spełnia wymogi złożoności;
- Wykorzystywany jest protokół SSH w wersji 2, zaś czas wylogowania dla połączeń zdalnych wynosi 90 minut.

### 7.3. Bezpieczeństwo sieciowe

- Routery brzegowe pracują z wykorzystaniem protokołu GLBP, który rozwiązuje problem redundancji, a dodatkowo równoważy obciążenie. Dodatkowo instancja protokołu GLBP zabezpieczona jest hasłem, by uniknąć podłączenie nieuprawnionego routera;
- Wykorzystywany jest protokół OSPF pomiędzy routerami brzegowymi sieci a routerem dostawcy usług internetowych. Instancja protokołu OSPF zabezpieczona jest hasłem;
- Przełączniki działają w trybie „vtp transparent”, co zabezpiecza je przed nadpisaniem konfiguracji pliku vlan.dat poprzez podłączenie przełącznika o wyższym numerze rewizji;
- Na urządzeniach sieciowych wygenerowany został certyfikat RSA o wielkości 1024 bitów. Certyfikat ten jest z założenia nieeksportowalny;
- Most główny protokołu STP został statycznie ustawiony. Zadania mostu realizuje stos przełączników w warstwie rdzenia;
- Skonfigurowano i wdrożono mechanizm Port Security;
- Skonfigurowano i wdrożono mechanizm DHCP Snooping;
- Skonfigurowano i wdrożono mechanizm DAI;
- Wdrożono mechanizm BPDU Guard;
- Wykorzystano wirtualne sieci LAN w celu separacji urządzeń;
- Nieużywane porty sieciowe są administracyjnie wyłączone ;
- Na urządzeniach zostały wprowadzone odpowiednie hasła dostępu do trybu uprzywilejowanego oraz konfiguracji globalnej;
- Administrator zostanie automatycznie wylogowany z urządzeń sieciowych po 5 minutach nieaktywności;
- Na urządzeniach sieciowych włączona jest funkcjonalność szyfrowania haseł;
- Logowanie na urządzeniach sieciowych jest blokowane na określony czas po 3 błędnych próbach w ciągu określonego czasu. Wszelkie logowania znajdują się w logu systemowym;
- Interfejsy posiadają na sztywno przypisanie trybu access/trunk.

#### **7.4. Bezpieczeństwo Windows Server**

- Użytkownicy autoryzują się poprzez indywidualne, jasno identyfikujące użytkownika konta domenowe w usłudze LACP Windows Server Active Directory;
- Wprowadzona jest odpowiednia polityka haseł;
- Konta użytkowników przechowywane są jako profile mobilne na serwerze, co daje możliwości tworzenia kopii zapasowych plików globalnie dla wszystkich użytkowników z jednego folderu;
- Wdrożono odpowiednie zasady grupy GPO w Windows Server;
- Dla folderów udostępnionych zastosowano odpowiednią politykę bezpieczeństwa, uwzględniającą odpowiedni poziom uprawnień do udostępnionych zasobów;
- Dyski działowe posiadają odpowiednie poziomy zabezpieczeń ze względu na ustawienia filtrowania i item-targetowania w GPO;
- Przeglądarka internetowa jest wdrażana zdalnie przez administratorów, dlatego mogą oni w nagłej potrzebie zmienić program będący przeglądarką internetową lub wykonać odpowiednią zmianę wersji, bez ingerencji użytkownika końcowego;
- W przypadku trzykrotnego, niepoprawnego logowania domenowego konto jest czasowo blokowane.

Dodatkowo administratorzy powinni dołożyć wszelkich starań w kwestii regularnego monitorowania urządzeń sieciowych, serwerowych oraz klienckich. Powinni oni regularnie instalować aktualizacje i łatki bezpieczeństwa.

## Podsumowanie

Celem pracy było stworzenie projektu, dokumentacji i konfiguracji sieci komputerowej z usługami serwerowymi Windows Server. Projekt wdrożono i przetestowano na sprzęcie sieciowym i komputerowym, znajdującym się w Sali 108, w Instytucie Informatyki Uniwersytetu Opolskiego. W pracy przedstawiono szczegółową topologię sieci, urządzenia i oprogramowanie do zarządzania siecią, usługi i protokoły sieciowe, opracowano zabezpieczenia sieci, w tym podział na VLAN-y, redundancję i skalowalność.

Przez cały tok realizacji pracy inżynierskiej autor poszerzył swoje umiejętności praktyczne oraz poznał nowe protokoły i mechanizmy wykorzystywane w sieciach komputerowych. Cel pracy został osiągnięty.

Oczywiście, projekt można dalej rozwijać. Pomysłami, które można by wdrożyć jest wykorzystanie PAT (Port Address Translation), wdrożenie środowiska do monitorowania sieci (np. LibreNMS) oraz utworzenie klastrów Windows Server, aby zwiększyć odporność na awarię. Idąc dalej – można wdrożyć zapory ogniowe Firewall, zarówno typu sprzętowego, jak FortiGate 100F czy Cisco ISA albo oprogramowanie, np. OPNsense. W przypadku realnego rozwoju infrastruktury logicznym, narzucającym się krokiem jest wdrożenie połączeń bezprzewodowych przy użyciu kontrolera WLC oraz punktów AP.

Autor pracy jest przekonany, iż godziny spędzone nad realizacją projektu i analiza zagadnień w procesie tworzenia powyższej pracy inżynierskiej będą dobrym prognostykiem na przyszłość i rozwój kariery zawodowej.



## **Bibliografia**

### **Literatura**

- [1] Adam Józefiok: CCNA 200-301. Zostań administratorem sieci komputerowych. Helion, 2020-11-02
- [2] Gary A. Donahue: Wojownik sieci. Wydanie II. Helion, 2012-04-16
- [3] Joe Casad: TCP/IP w 24 godziny. Wydanie VI. Helion, 2017-12-01

### **Zasoby internetowe**

- [4] Dokument RFC 2131 „Dynamic Host Configuration Protocol” z oficjalnej strony ietf.org (data dostępu: 02.11.2022).
- [5] Zasoby internetowe strony *nastykusieci.pl* (data dostępu: 03.12.2022)
- [6] Zasoby internetowe strony *study-ccna.com* (data dostępu: 03.12.2022)

## Opis zawartości APD

Pliki umieszczone w Archiwum Prac Dyplomowych jako „Praca praktyczna”:

- Dokument Pyda\_PrzemysławKrzysztof\_2023.pdf

## Spis tabel

Tabela 3.1.1 Adresy sieciowe. Opracowanie własne .....	20
Tabela 3.2.1 Wykorzystywane sieci VLAN. Opracowanie własne .....	21
Tabela 3.3.1 Fizyczne połączenia - ROUTER_ISP. Opracowanie własne .....	22
Tabela 3.3.2 Fizyczne połączenia - ROUTER_MAIN. Opracowanie własne .....	22
Tabela 3.3.3 Fizyczne połączenia - ROUTER_BACKUP. Opracowanie własne.....	22
Tabela 3.3.4 Fizyczne połączenia - SW_CORE. Opracowanie własne .....	23
Tabela 3.3.5 Fizyczne połączenia - SW_A_UPPERF. Opracowanie własne .....	24
Tabela 3.3.6 Fizyczne połączenia - SW_A_LOWERF. Opracowanie własne .....	25
Tabela 4.2.1 Możliwe ustawienia EtherChannel. Opracowanie własne na podstawie [6].....	27
Tabela 5.3.1 Użytkownicy domenowi. Opracowanie własne .....	36

## Spis rysunków

Rysunek 2.2.1 Rzut budynku - parter. Opracowanie własne .....	11
Rysunek 2.2.2 Rzut budynku - piętro. Opracowanie własne .....	12
Rysunek 2.3.1 Logiczna perspektywa sieci komputerowej. Opracowanie własne .....	13
Rysunek 4.1.1 Widok stosu przełączników SW_CORE. Opracowanie własne .....	26
Rysunek 4.2.1 Podsumowanie agregacji LAG dla SW_CORE. Opracowanie własne.....	27
Rysunek 5.1.1 Widok "All Servers" dla maszyny WINSRV01. Opracowanie własne .....	31
Rysunek 5.1.2 Widok "All Servers" dla maszyny WINSRV02. Opracowanie własne .....	31
Rysunek 5.2.1 Konfiguracja nadmiarowych kart sieciowych. Opracowanie własne .....	32
Rysunek 5.2.2 Konfiguracja adresu NIC Teaming. Opracowanie własne .....	33
Rysunek 5.3.1 Struktura organizacyjna firmy CyberCode. Opracowanie własne .....	34
Rysunek 5.3.2 Widok "Domain Groups". Opracowanie własne.....	35
Rysunek 5.3.3. Widok "Domain Users". Opracowanie własne .....	37
Rysunek 5.3.4 Widok właściwości dla użytkownika domenowego. Opracowanie własne .....	37
Rysunek 5.3.5 Widok właściwości członków grupy WORKERS. Opracowanie własne.....	38
Rysunek 5.3.6 Widok właściwości członków grupy EVERYBODY. Opracowanie własne ..	38
Rysunek 5.4.1 Profil mobilny - wybór zasobu udostępnionego. Opracowanie własne .....	39
Rysunek 5.4.2 Profil mobilny - tworzenie zasobu udostępnionego. Opracowanie własne .....	40
Rysunek 5.4.3 Profil mobilny - właściwości zasobu. Opracowanie własne .....	40
Rysunek 5.4.4 Ustawienia uprawnień do zasobu. Opracowanie własne .....	41
Rysunek 5.4.6 Profil mobilne – Zmienna globalna w ścieżce. Opracowanie własne.....	42
Rysunek 5.4.7 Profil mobilny - Wygenerowane profile mobilne. Opracowanie własne.....	42
Rysunek 5.5.1 Widok nadmiarowych kontrolerów domeny AD. Opracowanie własne.....	43
Rysunek 5.5.2 Kontrolery AD w aplecie AD Users and Computers. Opracowanie własne....	43
Rysunek 5.5.3 Powielenie ustawień AD na WINSRV02. Opracowanie własne .....	44
Rysunek 5.6.1 Przydzielanie adresu IP przez DHCP. Opracowanie własne na podstawie [4]	45
Rysunek 5.6.2 DHCP - Utworzenie pól adresów. Opracowanie własne .....	46
Rysunek 5.6.3 DHCP - Widok zakładki "Failover" dla WINSRV01. Opracowanie własne...	47
Rysunek 5.6.4 DHCP - Relacja sąsiedztwa w trybie "Failover". Opracowanie własne .....	47
Rysunek 5.6.5 DHCP - Widok "Adress Leases" dla DHCP. Opracowanie własne.....	48
Rysunek 5.6.6 DHCP - Relacja sąsiedztwa dla WINSRV02. Opracowanie własne .....	48
Rysunek 5.7.1 Utworzenie wpisów w Forward Lookup Zones. Opracowanie własne.....	49
Rysunek 5.7.2 Utworzenie wpisów w Forward Lookup Zones - portal. Opracowanie własne	50

Rysunek 5.7.3 Manager IIS - cybercode.local. Opracowanie własne .....	50
Rysunek 5.7.4 Manager IIS - portal.cybercode.local. Opracowanie własne .....	51
Rysunek 5.7.5 Plik strony internetowej cybercode.local. Opracowanie własne .....	51
Rysunek 5.8.1 Utworzenie GPO dla wdrożenia Google Chrome. Opracowanie własne .....	52
Rysunek 5.8.2 Wdrożona paczka instalacyjna Google Chrome. Opracowanie własne .....	53
Rysunek 5.8.3 Ustawienia szablonów ADM dla Google Chrome. Opracowanie własne .....	53
Rysunek 5.8.4 Ustawienie strony startowej. Opracowanie własne .....	54
Rysunek 5.8.5 Ustawienie strony zawsze uruchamianej przy starcie. Opracowanie własne ..	54
Rysunek 5.9.1 Ustawienia polityki haseł dla bazowego GPO. Opracowanie własne .....	55
Rysunek 5.9.2 Ustawienia blokowania konta dla bazowego GPO. Opracowanie własne .....	56
Rysunek 5.9.3 Sumaryczny widok polityk haseł. Opracowanie własne .....	56
Rysunek 5.10.1 Ustawienie banneru logowania. Opracowanie własne .....	57
Rysunek 5.11.1 Blokada Panelu Sterowania dla użytkowników. Opracowanie własne .....	57
Rysunek 5.12.1 Utworzenie obiektów "Shared Folders". Opracowanie własne .....	59
Rysunek 5.12.2 Security Filtering dla GPO. Opracowanie własne .....	59
Rysunek 5.12.3 Ustawienia delegacji dla GPO. Opracowanie własne .....	60
Rysunek 5.12.4 Przypisanie dysku mapowanego dla GPO. Opracowanie własne .....	60
Rysunek 5.12.5 Widok "General" dla udostępnionego dysku. Opracowanie własne .....	61
Rysunek 5.12.6 Przypisanie "Shared Folders" mapowanych dysków. Opracowanie własne ..	61
Rysunek 5.12.7 Widok "Common". Item-level targeting grupy. Opracowanie własne .....	62
Rysunek 5.12.8 Mapowanie dysku sieciowego "Ogłoszenia". Opracowanie własne .....	62
Rysunek 6.1.1 Banner logowania na systemie Windows 10. Opracowanie własne .....	63
Rysunek 6.1.2 Pierwsze logowanie użytkownika. Opracowanie własne .....	64
Rysunek 6.1.3 Wymuszona zmiana hasła przy pierwszym logowaniu. Opracowanie własne	64
Rysunek 6.1.4 Hasło 4-znakowe nie spełnia wymogów. Opracowanie własne .....	65
Rysunek 6.1.5 Ustawienie hasła spełniającego wymogi. Opracowanie własne .....	65
Rysunek 6.1.6 Pomyślne pierwsze logowanie użytkownika. Opracowanie własne .....	66
Rysunek 6.1.7 Widok Eksploratora dla grupy ICT. Opracowanie własne .....	66
Rysunek 6.1.8 Strona główna cybercode.local. Opracowanie własne .....	67
Rysunek 6.1.9 Strona portalu pracowniczego portal.cybercode.local.. Opracowanie własne .	67
Rysunek 6.1.10 Edycja folderu sieciowego przez konto uprawnione. Opracowanie własne ..	67
Rysunek 6.1.11 Próba dostępu do nieuprawnionego zasobu. Opracowanie własne .....	68
Rysunek 6.1.12 Utworzenie ogłoszenia przez członka grupy BOSS. Opracowanie własne ...	69
Rysunek 6.1.13 Zakaz edycji pliku przez nieuprawnione konto. Opracowanie własne .....	69

Rysunek 6.1.14 Plik synchronizowany profilem mobilnym .....	70
Rysunek 6.2.1 Tryb automatyczny TCP/IPv4. Klient DHCP. Opracowanie własne.....	71
Rysunek 6.2.2 Test połączenia sieciowego z wykorzystaniem DNS. Opracowanie własne ...	72
Rysunek 6.3.1 Definiowanie kont uprawnionych do logowania. Opracowanie własne .....	73
Rysunek 6.3.2 Próba logowania nieuprawnionego użytkownika. Opracowanie własne .....	73
Rysunek 6.3.3 Powiadomienie o niemożliwości zalogowania. Opracowanie własne .....	74
Rysunek 6.3.4 Pomyślnie zalogowany użytkownik grupy ADMINS. Opracowanie własne ..	74
Rysunek 6.4.1 Połączenie protokołem SSH do urządzeń sieciowych. Opracowanie własne ..	75
Rysunek 6.4.2 Symulowana sieć Internet, testy sieciowe. Opracowanie własne .....	76

## Spis listingów

Listing 1 - ROUTER_ISP .....	86
Listing 2 - ROUTER_MAIN.....	89
Listing 3 - ROUTER_BACKUP .....	92
Listing 4 - SW_CORE.....	95
Listing 5 - SW_A_UPPERF.....	104
Listing 6 – SW_A_LOWERF .....	114

### Listing 1 - ROUTER\_ISP

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname ROUTER_ISP  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
!  
resource policy  
!  
ip cef  
!  
!  
!  
!  
ip domain name BestISP.net  
ip ssh version 2  
!  
!  
!  
username Przemek privilege 15 secret 5 $1$kBe2$XZpk6iS/oZC3N.3xYN/290  
!  
!  
!  
!  
!  
!  
interface Loopback0
```

```
ip address 3.3.3.3 255.0.0.0
!
interface Loopback1
ip address 4.4.4.4 255.0.0.0
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1/0
switchport mode trunk
shutdown
!
interface FastEthernet0/1/1
switchport mode trunk
shutdown
!
interface FastEthernet0/1/2
switchport mode trunk
shutdown
!
interface FastEthernet0/1/3
switchport mode trunk
shutdown
!
interface Serial0/0/0
bandwidth 64
ip address 12.73.61.1 255.255.255.252
clock rate 64000
!
interface Serial0/0/1
bandwidth 64
ip address 12.73.62.1 255.255.255.252
clock rate 64000
!
interface Vlan1
no ip address
!
router ospf 1
router-id 3.3.3.3
log-adjacency-changes
network 3.0.0.0 0.255.255.255 area 0
```

```
network 4.0.0.0 0.255.255.255 area 0
network 12.73.61.0 0.0.0.3 area 0
network 12.73.62.0 0.0.0.3 area 0
!
!
!
ip http server
no ip http secure-server
!
!
!
!
!
!
!
control-plane
!
!
!
line con 0
  logging synchronous
line aux 0
  logging synchronous
line vty 0
  logging synchronous
  login local
  transport input ssh
line vty 1 4
  login local
  transport input ssh
line vty 5 15
  login local
  transport input ssh
!
scheduler allocate 20000 1000
!
webvpn context Default_context
  ssl authenticate verify all
!
no inservice
!
end
```



Listing 2 - ROUTER\_MAIN

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname ROUTER_MAIN  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$N8Rg$kw4K858MqoBYtOG8YOGp70  
!  
no aaa new-model  
!  
resource policy  
!  
ip cef  
!  
!  
!  
!  
no ip domain lookup  
ip domain name CyberCode.com  
ip ssh time-out 90  
ip ssh version 2  
login block-for 60 attempts 3 within 45  
login on-failure log every 3  
login on-success log  
!  
!  
!  
username Przemek privilege 15 password 7 062F013B7C570D18  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 10.5.1.2 255.255.255.0  
duplex auto  
speed auto  
glbp 5 ip 10.5.1.1  
glbp 5 priority 150  
glbp 5 preempt  
glbp 5 authentication md5 key-string 7 100A00171F4222120824  
!  
interface FastEthernet0/1
```

```

ip address 10.6.1.2 255.255.255.0
duplex auto
speed auto
glbp 6 ip 10.6.1.1
glbp 6 priority 150
glbp 6 preempt
glbp 6 authentication md5 key-string 7 054F0F013B1A7E101D25
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Serial0/0/0
description Link ROUTER_ISP (OSPF)
bandwidth 64
ip address 12.73.61.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 09654013291C1313243F340C
no fair-queue
!
interface Serial0/0/1
no ip address
shutdown
clock rate 64000
!
interface Vlan1
no ip address
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0
network 12.73.61.0 0.0.0.3 area 0
network 192.168.0.0 0.0.255.255 area 0
!
ip route 192.168.0.0 255.255.0.0 10.5.1.5
ip route 192.168.0.0 255.255.0.0 10.6.1.5
!
!
ip http server
no ip http secure-server
!
!
!
!
!
!

```

```
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
  exec-timeout 5 0  
  password 7 022F0A413B1F0B206741070A0A1B13  
  logging synchronous  
  login  
line aux 0  
  logging synchronous  
line vty 0 4  
  exec-timeout 5 0  
  logging synchronous  
  login local  
  transport input ssh  
line vty 5 15  
  exec-timeout 5 0  
  login local  
  transport input ssh  
!  
scheduler allocate 20000 1000  
!  
webvpn context Default_context  
  ssl authenticate verify all  
!  
no inservice  
!  
end
```

Listing 3 - ROUTER\_BACKUP

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname ROUTER_BACKUP  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$euEQ$snd8A5dTofax2exSGBK3E/  
!  
no aaa new-model  
!  
resource policy  
!  
ip cef  
!  
!  
!  
!  
ip domain name CyberCode.com  
ip ssh time-out 90  
ip ssh version 2  
login block-for 60 attempts 3 within 45  
login on-failure log every 3  
login on-success log  
!  
!  
!  
username Przemek privilege 15 secret 5 $1$n6BN$konEUbwbNOP0mJ43zgenn.  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/0  
ip address 10.5.1.3 255.255.255.0  
duplex auto  
speed auto  
glbp 5 ip 10.5.1.1  
glbp 5 authentication md5 key-string 7 155602021E7F1B3D2C13  
!  
interface FastEthernet0/1  
ip address 10.6.1.3 255.255.255.0  
duplex auto  
speed auto
```

```

glbp 6 ip 10.6.1.1
glbp 6 authentication md5 key-string 7 074B2842545F291C1332
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Serial0/0/0
description Link ROUTER_ISP (OSPF)
bandwidth 64
ip address 12.73.62.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 7 002D1D1C34420F0720127C68
no fair-queue
!
interface Serial0/0/1
no ip address
shutdown
clock rate 64000
!
interface Vlan1
no ip address
!
router ospf 1
router-id 2.2.2.2
log-adjacency-changes
network 10.0.0.0 0.255.255.255 area 0
network 12.73.62.0 0.0.0.3 area 0
network 192.168.0.0 0.0.255.255 area 0
!
ip route 192.168.0.0 255.255.0.0 10.5.1.5
ip route 192.168.0.0 255.255.0.0 10.6.1.5
!
!
ip http server
no ip http secure-server
!
!
!
!
!
!
!
!
control-plane
!

```

```
!  
!  
line con 0  
  exec-timeout 5 0  
  password 7 013A081E6B12020E0A43401A160916  
  logging synchronous  
  login  
line aux 0  
  logging synchronous  
line vty 0  
  exec-timeout 5 0  
  logging synchronous  
  login local  
  transport input ssh  
line vty 1 4  
  exec-timeout 5 0  
  login local  
  transport input ssh  
line vty 5 15  
  exec-timeout 5 0  
  login local  
  transport input ssh  
!  
scheduler allocate 20000 1000  
!  
webvpn context Default_context  
  ssl authenticate verify all  
!  
no inservice  
!  
end
```

Listing 4 - SW\_CORE

```
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname SW_CORE  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$DCuq$/Vi8bdZ2Hy9239chgrD6R/  
!  
username Przemek privilege 15 secret 5 $1$GRg8$dO7U439ySrbDlzEQeXSIZ.  
!  
!  
no aaa new-model  
switch 1 provision ws-c3750g-24ts  
switch 2 provision ws-c3750g-24ts-1u  
system mtu routing 1500  
ip routing  
ip domain-name CyberCode.com  
!  
!  
ip dhcp snooping vlan 10,20,30,40,50,60,70,80  
no ip dhcp snooping information option  
ip dhcp snooping  
ip arp inspection vlan 10,20,30,40,50,60,70,80  
login block-for 60 attempts 3 within 45  
login on-failure log every 3  
login on-success log  
!  
!  
crypto pki trustpoint TP-self-signed-1202673152  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-1202673152  
revocation-check none  
rsa-keypair TP-self-signed-1202673152  
!  
!  
crypto pki certificate chain TP-self-signed-1202673152  
certificate self-signed 01  
3082024D 308201B6 A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274  
69666963 6174652D 31323032 36373331 3532301E 170D3933 30333031 30303032  
35355A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649  
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 32303236  
37333135 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
```

```

8100DDCF 623FD39C A55134C0 A780D012 A11EAFAA A4DDFE63 92B5DB9A
5F825CA2
492CD1C3 94375339 13F686F9 69E596D9 5AC3CBFE 2FE278F4 F6E8C7CA
3B1570A8
8BB549DD C9AC40B0 D6E68FD3 BC44E56B 59352275 E41E7319 A39B2289
1665A27A
25F62BF6 D506950A 98828A17 00CF2AEB 7D8209F6 F0784022 6A2C19F8
1FCABD0A
CC2D0203 010001A3 75307330 0F060355 1D130101 FF040530 030101FF 30200603
551D1104 19301782 1553575F 434F5245 2E437962 6572436F 64652E63 6F6D301F
0603551D 23041830 16801495 AA979A83 D46C186F AD52E5A3 8A6241C7
95D2ED30
1D060355 1D0E0416 041495AA 979A83D4 6C186FAD 52E5A38A 6241C795
D2ED300D
06092A86 4886F70D 01010405 00038181 00808589 2E96D324 5A01DEBF 86F7D6FA
376E2C0F A612B9A6 A5A08110 59282DA8 BB12F5C2 0B63BC68 6F48D6B2
6FBFD45E
A14602EC 82EB1AF7 29221F6E F4FD8328 566D888B 0CD6B036 A13C01CC
38B747AB
A18B9452 BE2C0E18 7CEB3A9D DA260D49 7AED0EF7 8E0C89B1 4390C56A
2E6FFA13
EF904AD8 E8DB46E1 471DA8A3 4C4F6E1F 69
quit
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 1-4094 priority 24576
!
vlan internal allocation policy ascending
!
ip ssh time-out 90
ip ssh version 2
!
!
!
interface Port-channel2
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
ip dhcp snooping trust
!
interface Port-channel3
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk

```



```
switchport nonegotiate
ip arp inspection trust
ip dhcp snooping trust
!
interface Port-channel4
!
interface Port-channel5
!
interface GigabitEthernet1/0/1
switchport access vlan 6
switchport mode access
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet1/0/2
switchport access vlan 6
switchport mode access
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet1/0/3
switchport mode access
!
interface GigabitEthernet1/0/4
switchport mode access
!
interface GigabitEthernet1/0/5
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
switchport access vlan 5
!
interface GigabitEthernet1/0/8
shutdown
!
interface GigabitEthernet1/0/9
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 2 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/10
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
```

```
ip arp inspection trust
channel-group 2 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/11
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 3 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/12
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 3 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/13
!
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
switchport access vlan 7
switchport mode access
channel-group 4 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/16
switchport access vlan 7
switchport mode access
channel-group 5 mode active
ip dhcp snooping trust
!
interface GigabitEthernet1/0/17
shutdown
!
interface GigabitEthernet1/0/18
shutdown
!
interface GigabitEthernet1/0/19
shutdown
!
interface GigabitEthernet1/0/20
shutdown
!
```

```
interface GigabitEthernet1/0/21
shutdown
!
interface GigabitEthernet1/0/22
shutdown
!
interface GigabitEthernet1/0/23
shutdown
!
interface GigabitEthernet1/0/24
shutdown
!
interface GigabitEthernet1/0/25
shutdown
!
interface GigabitEthernet1/0/26
shutdown
!
interface GigabitEthernet1/0/27
shutdown
!
interface GigabitEthernet1/0/28
shutdown
!
interface GigabitEthernet2/0/1
switchport access vlan 5
switchport mode access
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet2/0/2
switchport access vlan 5
switchport mode access
ip arp inspection trust
ip dhcp snooping trust
!
interface GigabitEthernet2/0/3
switchport mode access
shutdown
!
interface GigabitEthernet2/0/4
switchport mode access
shutdown
!
interface GigabitEthernet2/0/5
shutdown
!
interface GigabitEthernet2/0/6
shutdown
!
```

```
interface GigabitEthernet2/0/7
switchport access vlan 5
!
interface GigabitEthernet2/0/8
shutdown
!
interface GigabitEthernet2/0/9
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 2 mode active
ip dhcp snooping trust
!
interface GigabitEthernet2/0/10
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 2 mode active
ip dhcp snooping trust
!
interface GigabitEthernet2/0/11
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 3 mode active
ip dhcp snooping trust
!
interface GigabitEthernet2/0/12
switchport trunk encapsulation dot1q
switchport trunk native vlan 127
switchport mode trunk
switchport nonegotiate
ip arp inspection trust
channel-group 3 mode active
ip dhcp snooping trust
!
interface GigabitEthernet2/0/13
!
interface GigabitEthernet2/0/14
!
interface GigabitEthernet2/0/15
switchport access vlan 7
switchport mode access
channel-group 4 mode active
```

```
ip dhcp snooping trust
!
interface GigabitEthernet2/0/16
switchport access vlan 7
switchport mode access
channel-group 5 mode active
ip dhcp snooping trust
!
interface GigabitEthernet2/0/17
shutdown
!
interface GigabitEthernet2/0/18
shutdown
!
interface GigabitEthernet2/0/19
shutdown
!
interface GigabitEthernet2/0/20
shutdown
!
interface GigabitEthernet2/0/21
shutdown
!
interface GigabitEthernet2/0/22
shutdown
!
interface GigabitEthernet2/0/23
shutdown
!
interface GigabitEthernet2/0/24
shutdown
!
interface GigabitEthernet2/0/25
shutdown
!
interface GigabitEthernet2/0/26
shutdown
!
interface GigabitEthernet2/0/27
shutdown
!
interface GigabitEthernet2/0/28
shutdown
!
interface Vlan1
no ip address
!
interface Vlan5
ip address 10.5.1.5 255.255.255.0
!
```

```
interface Vlan6
ip address 10.6.1.5 255.255.255.0
!
interface Vlan7
ip address 192.168.7.1 255.255.255.240
!
interface Vlan10
ip address 192.168.10.1 255.255.255.248
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan20
ip address 192.168.20.1 255.255.255.0
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan30
ip address 192.168.30.1 255.255.255.0
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan40
ip address 192.168.40.1 255.255.255.0
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan50
ip address 192.168.50.1 255.255.255.0
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan60
ip address 192.168.60.1 255.255.255.240
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan70
ip address 192.168.70.1 255.255.255.0
ip helper-address 192.168.7.10
ip helper-address 192.168.7.12
!
interface Vlan100
ip address 192.168.100.1 255.255.255.0
!
interface Vlan119
ip address 192.168.119.3 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.5.1.1 10
ip route 0.0.0.0 0.0.0.0 10.6.1.1 20
```

```
ip http server
ip http secure-server
!
!
!
ip sla enable reaction-alerts
!
!
vstack
!
line con 0
exec-timeout 5 0
password 7 09654013291C131320030A39242829
logging synchronous
login
speed 115200
line vty 0 4
exec-timeout 5 0
logging synchronous
login local
transport input ssh
line vty 5 15
exec-timeout 5 0
logging synchronous
login local
transport input ssh
!
end
```

Listing 5 - SW\_A\_UPPERF

```
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname SW_A_UPPERF  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$iqQC$okYwkhRkqn683MNcKKgTq1  
!  
username Przemek secret 5 $1$Nz1O$R3jM9AOWtrRovbXBpqJnC/  
no aaa new-model  
system mtu routing 1500  
vtp mode transparent  
ip subnet-zero  
!  
!  
ip dhcp snooping  
no ip domain-lookup  
ip domain-name CyberCode.com  
ip arp inspection vlan 20,30,40,50,70,80  
!  
!  
crypto pki trustpoint TP-self-signed-458638464  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-458638464  
revocation-check none  
rsa-keypair TP-self-signed-458638464  
!  
!  
crypto pki certificate chain TP-self-signed-458638464  
certificate self-signed 01  
3082024F 308201B8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274  
69666963 6174652D 34353836 33383436 34301E17 0D393330 33303130 30303035  
315A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F  
532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3435 38363338  
34363430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100  
CB8C6AA3 54F629B2 8DF1EEDA DBBE1F68 9B5D7371 620EBC83 21C36FCD  
897C4F66  
C894EF78 AF3CB058 7EFEE00B 44BDE434 E32B1BB7 21B88302 D289A47E  
F77FE294  
6D757528 3FD0EAAB 310A6A5F 55CF9329 142C1FC2 9D720379 A2E4BA82  
B45D0EF4
```



```

FC78A4AD AA18704C 1CE1C455 BC59243B 0439329F 6577D9E3 EB32D55F
F2F25C93
02030100 01A37930 77300F06 03551D13 0101FF04 05300301 01FF3024 0603551D
11041D30 1B821953 575F415F 55505045 52462E43 79626572 436F6465 2E636F6D
301F0603 551D2304 18301680 142CF7F9 7CE8D701 93F7065D 10C7B660 F29C9BAA
7E301D06 03551D0E 04160414 2CF7F97C E8D70193 F7065D10 C7B660F2 9C9BAA7E
300D0609 2A864886 F70D0101 04050003 81810040 C06BD1E6 D43396B0 D198A06F
DBA00F36 18994121 7EE3232C A07254C4 303A7593 A6CF7616 0AD39690
47CDC2E5
F69D81D4 D8B2CC24 D564B114 5B48ECF0 BE5946E0 2FBDCE87 E378DFDC
0873824C
A5565CE8 1D87D1A5 12EC31C4 04F09353 57002B98 18DDF1E7 87413758 20E5F59F
834D0923 A45F5A96 9B17A34B 2B44C77B F46B95
quit
!
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 90
ip ssh version 2
!
vlan 10
name BOSS
!
vlan 20
name SALES
!
vlan 30
name PM
!
vlan 40
name HR
!
vlan 50
name ICT
!
vlan 60
name PRINTERS
!
vlan 70
name GRAPHICS
!

```

```
vlan 99
 name GUEST_PRIMARY
!
vlan 100
 name GUEST
!
vlan 119
 name SSH
!
vlan 999
 name DUMMY
!
ip ssh version 2
!
!
interface Port-channel2
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface FastEthernet0/1
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 2 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 2 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/3
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 2 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/4
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
```

```
ip arp inspection trust
channel-group 2 mode passive
ip dhcp snooping trust
!
interface FastEthernet0/5
description PC
switchport access vlan 10
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/6
description PC
switchport access vlan 10
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
switchport port-security mac-address sticky 0013.4630.e096
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/7
description PC
switchport access vlan 10
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
```

```

interface FastEthernet0/8
description Printer
switchport access vlan 60
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/9
description PC
switchport access vlan 20
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/10
description PC
switchport access vlan 20
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/11
description PC
switchport access vlan 20
switchport mode access
switchport port-security maximum 3

```

```

switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/12
description PC
switchport access vlan 20
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/13
description PC
switchport access vlan 30
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/14
description PC
switchport access vlan 30
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky

```

```
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/15
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/16
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/17
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
```

```
interface FastEthernet0/18
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/19
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/20
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/21
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
```

```

switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/22
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/23
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/24
description Printer
switchport access vlan 60
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky

```



```
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan119
ip address 192.168.119.4 255.255.255.0
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 5 0
logging synchronous
line vty 0
exec-timeout 5 0
logging synchronous
login local
transport input ssh
line vty 1 4
exec-timeout 5 0
login local
transport input ssh
line vty 5 15
exec-timeout 5 0
login local
transport input ssh
!
end
```

Listing 6 – SW\_A\_LOWERF

```
!  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname SW_A_LOWERF  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$OJJ8$CX/vp/728eBkamAVQneHK.  
!  
username Przemek secret 5 $1$1JsZ$OzBUfZLIPesC68kFP1nJI0  
no aaa new-model  
system mtu routing 1500  
vtp mode transparent  
ip subnet-zero  
!  
!  
ip dhcp snooping vlan 10,20,30,40,50,60,70,80  
no ip dhcp snooping information option  
ip dhcp snooping  
no ip domain-lookup  
ip domain-name CyberCode.com  
ip arp inspection vlan 10,20,30,40,50,60,70,80  
!  
!  
crypto pki trustpoint TP-self-signed-2449269760  
enrollment selfsigned  
subject-name cn=IOS-Self-Signed-Certificate-2449269760  
revocation-check none  
rsa-keypair TP-self-signed-2449269760  
!  
!  
crypto pki certificate chain TP-self-signed-2449269760  
certificate self-signed 01  
30820251 308201BA A0030201 02020101 300D0609 2A864886 F70D0101 04050030  
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274  
69666963 6174652D 32343439 32363937 3630301E 170D3933 30333031 30303030  
35325A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649  
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34343932  
36393736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281  
8100D140 13C2FBED 96E22019 1DAF9770 E6E74297 E9154C3C E635BEA4  
F9C228FA  
EBBE44F2 EBCB554E 6C8DA6D0 5849E9E9 911A61AE 40E1AEED 21FD4ABE  
6AB41BD9
```

```

2E424E3D BD5A543B E027F2B5 B32961F7 0EE67959 8DEC2C0D B852B72A
CACE08DE
DCAD8A4C 7506A1F1 25B6B088 E93CB0A8 277F5F7E 48243F06 28AE25BA
42FBF0E6
40C90203 010001A3 79307730 0F060355 1D130101 FF040530 030101FF 30240603
551D1104 1D301B82 1953575F 415F4C4F 57455246 2E437962 6572436F 64652E63
6F6D301F 0603551D 23041830 16801421 E63A72AE A468E9AC 079D0369 8C7517B1
E8A34830 1D060355 1D0E0416 041421E6 3A72AEA4 68E9AC07 9D03698C 7517B1E8
A348300D 06092A86 4886F70D 01010405 00038181 00B4CE63 AF256D61 F2BB24F2
3FD10B39 8EE67795 44FA114B 6870842F D039652C 6B8D05C0 89ED8EB8
B2F1C319
D6A0C00E 93631423 D53A84BA 5A0CD1F3 1BE12C0A 4169A383 3B70D12C
D8F99F7F
02FEFC25 8CBF684E 00F7C317 010DFD8D F0783F8B AEA6B335 1CCFD50C
8CFDC091
61648BA5 4734C296 D2923C18 BF030D79 DB18893D F8
quit
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 10
name BOSS
!
vlan 20
name SALES
!
vlan 30
name PM
!
vlan 40
name HR
!
vlan 50
name ICT
!
vlan 60
name PRINTERS
!
vlan 70
name GRAPHICS
!

```

```
vlan 99
 name GUEST_PRIMARY
!
vlan 100
 name GUEST
!
vlan 119
 name SSH
!
vlan 999
 name DUMMY
!
ip ssh version 2
!
!
interface Port-channel3
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface FastEthernet0/1
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 3 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/2
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 3 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/3
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 channel-group 3 mode passive
 ip dhcp snooping trust
!
interface FastEthernet0/4
 switchport trunk native vlan 127
 switchport mode trunk
 switchport nonegotiate
```

```
ip arp inspection trust
channel-group 3 mode passive
ip dhcp snooping trust
!
interface FastEthernet0/5
description PC
switchport access vlan 40
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/6
description PC
switchport access vlan 40
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/7
description PC
switchport access vlan 40
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/8
```

```

description PC
switchport access vlan 40
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/9
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/10
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/11
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security

```

```

switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/12
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/13
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/14
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12

```

```

spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/15
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/16
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/17
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/18

```



```

description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/19
description PC
switchport access vlan 50
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/20
description PC
switchport access vlan 70
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/21
description PC
switchport access vlan 70
switchport mode access
switchport port-security maximum 3
switchport port-security

```

```

switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/22
description PC
switchport access vlan 70
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/23
description PC
switchport access vlan 70
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface FastEthernet0/24
description Printer
switchport access vlan 60
switchport mode access
switchport port-security maximum 3
switchport port-security
switchport port-security aging time 30
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 12

```

```
spanning-tree portfast
spanning-tree bpduguard enable
ip dhcp snooping limit rate 15
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
no ip address
no ip route-cache
!
interface Vlan119
ip address 192.168.119.5 255.255.255.0
no ip route-cache
!
ip http server
ip http secure-server
!
control-plane
!
!
line con 0
exec-timeout 5 0
logging synchronous
line vty 0 4
exec-timeout 5 0
login local
transport input ssh
line vty 5 15
exec-timeout 5 0
login local
transport input ssh
!
end
```