Wyższa Szkoła

Ekonomii i Informatyki

W Krakowie

JAKUB NOWICKI

Numer albumu 11506

MARCIN DZIEDZIC

Numer albumu 11461

Implementacja AAA w sieci LAN dostępu do urządzeń sieciowych

Kraków 2020

**Spis treści**

[**Wstęp** 3](#_Toc32613543)

[**1.** **Środowisko techniczne** 4](#_Toc32613544)

[**1.1** **Cisco Internetworking Operating System (IOS)** 4](#_Toc32613545)

[**1.2 Cisco IOS XR** 6](#_Toc32613546)

[**1.3 Cisco IOS XE** 8](#_Toc32613547)

[**1.4 Cisco Identity Services Engine (ISE)** 9](#_Toc32613548)

[**1.5 Terminal Access Controller Access-Control System Plus (TACACS+)** 10](#_Toc32613549)

[**1.6 Uwierzytelnianie (ang. *Authentication*)** 11](#_Toc32613550)

[**1.7 Autoryzacja (ang. *Authorization*)** 12](#_Toc32613551)

[**1.8 Accounting** 13](#_Toc32613552)

[**1.9 Wirtualizacja (ang. *Virtualization*)** 13](#_Toc32613553)

[**1.10 Microsoft Hyper-V** 15](#_Toc32613554)

[**1.11 Router** 16](#_Toc32613555)

[**1.12 Network Switch** 17](#_Toc32613556)

[**2.** **Projekt Sieci** 19](#_Toc32613557)

[**2.1 Wykorzystane rozwiązania** 19](#_Toc32613558)

[**3.** **Wnioski** 22](#_Toc32613559)

[**4.** **Bibliografia** 23](#_Toc32613560)

[**Netografia** 23](#_Toc32613561)

[**Spis Tabel** 24](#_Toc32613562)

Wstęp

Przedmiotem niniejszej pracy inżynierskiej jest implementacja authentication, authorization and accounting (AAA) w urządzeniach sieciowych. Obecnie jest to najpopularniejsza metoda, która pozwala na szeroki zakres kontroli dostępu do urządzeń, które znajdują się w naszej sieci lokalnej.

Celem pracy jest zaimplementowanie w pełni działającego systemu na realnych urządzeniach sieciowych firmy Cisco z wykorzystaniem różnych protokołów uwierzytelniających za pomocą platformy Cisco Identity Services Engine (ISE) oraz protokołu TACACS+.

W pierwszym rozdziale znajduje się szeroki opis działania używanego sprzętu oraz oprogramowania w niniejszej pracy.

W drugim rozdziale znajduje się szczegółowo opisany projekt sieci oraz jakie dodatkowe technologie oprócz implementacji AAA będą używane w celu zapewnienia redundancji.

1. **Środowisko techniczne**

## **Cisco Internetworking Operating System (IOS)**

IOS został opracowany w latach 80-tych, kiedy routery miały ograniczoną pamięć (256 Kb) oraz małą moc procesora. Modułowość w architekturze systemu pozwoliła mu się rozwijać wraz z rosnącymi możliwościami sprzętowymi i wykorzystywać coraz to nowsze funkcje sieciowe, które były wymagane przez klientów Cisco[[1]](#footnote-1).

IOS został stworzony w oparciu o model monolitycznego jądra, dzięki któremu cechuje się wyższą wydajnością niż systemy bazujące na mikro jądrach. Różnica w wydajności polega na tym, że cały system operacyjny ładowany jest do kernel space, dzięki czemu wszystkie komponenty mają bezpośredni dostęp do sprzętu i oszczędzają czas na przetwarzaniu. Używanie monolitycznego jądra niesie ze sobą również negatywne skutki takie jak brak stabilności, gdzie jeden źle napisany program jest w stanie unieruchomić cały system.

IOS dzieli procesy ze względu na ich priorytet i traktuje każdy proces, jako pojedynczy wątek. Procesy, którym system przydzielił wysoki priorytet są uruchamiane przed procesami z niższym priorytetem, ale proces o wysokim priorytecie nie może zabrać już przydzielonej mocy procesora innemu wątkowi z niższym priorytetem. IOS uruchamia procesy zgodnie z harmonogramem, przez co jedna instrukcja musi się wykonać zanim kolejna instrukcja zostanie wykonana, co przekłada się na większą wydajność, ponieważ procesor nie musi się przełączać między zadaniami i ponownie ładować informacji o nich do pamięci.

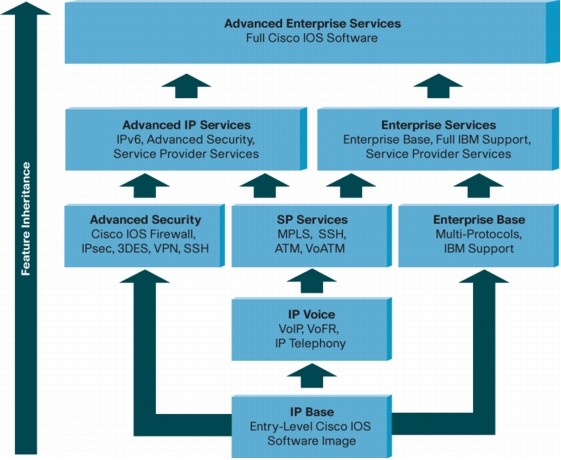
Zarządzanie pamięcią w Cisco IOS jest maksymalnie uproszczone, system mapuje całą dostępną pamięć fizyczną do jednej płaskiej wirtualnej przestrzeni adresowej, w której wszystkie procesy dzielą tą przestrzeń wspólnie. Takie podejście, mimo iż zmniejsza nagłówek i zwiększa wydajność to system jest bardziej skomplikowany. Dodatkowo niesie ze sobą niebezpieczeństwo gdzie jeden wadliwy proces może siać spustoszenie w innych działających poprawnie procesach.

Obrazy systemu IOS są pakowane w unikalne pliki dla każdej platformy. Dla jednej platformy istnieje, co najmniej kilka obrazów, w którym każdy zawiera różne funkcje. Podstawową paczką z funkcjami jest IP Base, który zawiera wszystkie podstawowe funkcje dla routera lub switcha takie jak:

* Quality of Service (QoS)
* Access Control Lists (ACL)
* Statyczny routing
* Dynamiczny routing
* IEEE 802.1Q

Ograniczeniem, jaki zestaw funkcji możemy pobrać nakłada na nas licencja, którą posiadamy. Gdy potrzebujemy bardziej rozbudowanego pakietu musimy wykupić odpowiednią licencje, która jest droższa od podstawowej IP Base.

Rysunek 1. Pakiety funkcji w systemie Cisco IOS



Źródło: Cisco, <https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/ios-packaging/prod_bulletin09186a00801af451.html>

Na rysunku powyżej mamy przedstawione wszystkie dostępne pakiety na platformie IOS. Widać również zależności między nimi i to, jakie najważniejsze funkcje posiadają.

Dodatkowym ograniczeniem związanym z używaniem bardziej rozbudowanego pakietu funkcji jest dostępna ilość pamięci Flash oraz DRAM na naszym urządzeniu sieciowym. W przypadku podstawowego pakietu takiego jak IP Base zapotrzebowanie na pamięć Flash i DRAM może być nawet dwukrotnie niższe niż w przypadku najbardziej rozbudowanego pakietu takiego jak Advanced Enterprise Services.

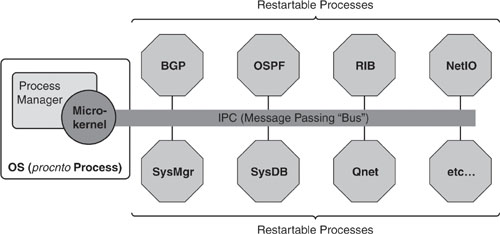
Należy również pamiętać, że nie wszystkie paczki są dostępne na wszystkich platformach sprzętowych na przykład router Cisco 1721 posiada tylko 3 paczki (IP Base, Advanced Security oraz Enterprise Base).

## **1.2 Cisco IOS XR**

Zapowiedziany w 2004 roku przez Cisco system IOS XR miał być odpowiedzią dla rosnących wymagań klientów, którzy potrzebowali wysokiej niezawodności i dostępności sieci[[2]](#footnote-2).

W odróżnieniu od Ciso IOS nowy system IOS XR działa na mikro jądrze real-time operating system (RTOS) od firmy QNX Software Systems.

Rysunek 2. Architektura mikro jądra w systemie IOS XR



Źródło: Tahir, Ghattas, Birhanu, Nawaz, 2009, s. 10

W jądrze systemu działa tylko menadżer procesów, wszystkie inne procesy są wyrzucone poza jądro, co jest zobrazowane na Rysunku 2. Dzięki takiemu podejściu możemy zrestartować pojedynczy proces na przykład SysDB bez potrzeby restartowania całego systemu.

IOS XR pozwala na wielozadaniowość[[3]](#footnote-3). Tak jak w przypadku Cisco IOS procesy z wyższym priorytetem są wykonywane przed procesami z niższym priorytetem natomiast procesy z wyższym priorytetem mogą tymczasowo usuwać procesy z niższym priorytetem z procesora by uzyskać dodatkowe zasoby czasu procesora.

System przydziela równe wartości czasu dla procesów o tym samym priorytecie, dzięki czemu można uniknąć sytuacji, w której jeden zapętlony proces zabiera ciągle całą moc obliczeniową procesora w efekcie zawieszając go.

IOS XR ma również wbudowane zabezpieczenia, które sprawdzają czy wszystkie procesy działają i odpowiadają. Jeżeli jakiś proces nie odpowiada system zbiera informacje, które ten proces przechowuje w pamięci, następnie zostaje on automatycznie zrestartowany, a pamięć, która została zebrana przez checkpoint service zostaje ona udostępniona procesowi po restarcie by ten mógł odzyskać wszystkie dane, które mógł utracić.

Wszystkie aplikacje, które są uruchomione na IOS XR działają na wirtualnej pamięci zamiast bezpośrednio na fizycznej. Pozwala to na przydzielenie każdemu procesowi jego części wirtualnej pamięci, którą tylko on zajmuje. Dzięki takiemu podzieleniu pamięci jedna aplikacja nie jest w stanie uszkodzić lub nadpisać innej części pamięci, z której korzysta inna aplikacja. Dodatkową korzyścią korzystania z wirtualnej pamięci jest możliwość jest rozszerzenia na inne media takie jak dyski twarde.

IOS XR używa bibliotek łączonych dynamicznie (ang. *Dynamik Link Libraries* (DLLs)) zamiast pakietu z funkcjami znanych z Cisco IOS[[4]](#footnote-4). Wykorzystywanie bibliotek zamiast paczek z funkcjami jest lepsze wykorzystanie pamięci, ponieważ gdy nie potrzebujemy już jakiejś biblioteki na przykład BGP możemy ją wyłączyć, dzięki czemu otrzymamy więcej wolnego miejsca na pamięci operacyjnej. Dodawanie nowych DLL lub usuwanie ich możemy wykonywać bez restartu urządzenia czy przerw w jego działaniu.

Package installation envelopes (PIEs) są to paczki, które zawierają różne funkcje tak jak w przypadku feature set znanego z IOS. W PIEs wyróżnia się paczkę: mini, która zawiera wszystkie niezbędne komponenty do odpalenia urządzenia sieciowego oraz jego podstawowe funkcje jak routing i switching. Dodatkowe funkcje takie jak na przykład MPLS mogą zostać dodane odpowiednimi pakietami PIE.

## **1.3 Cisco IOS XE**

IOS XE trafił na rynek podczas premiery routerów Cisco z serii ASR 1000. System ten, pomimo że jest niemal identyczny pod względem komend używanych w command line interface (CLI) posiada szereg usprawnień względem systemu IOS.

IOS XE w odróżnieniu od IOS bazuje na jądrze Linuxa i dodaje warstwę abstrakcji, dzięki czemu system może pracować stabilniej. Bezpośredni dostęp do sprzętu mają tylko sterowniki oraz samo jądro Linuxa. Aplikacje, które chciałby by uzyskać dostęp do sprzętu muszą używać Application programming interface (API).

Cały system IOS XE działa, jako aplikacja uruchomiona na Linuxie, dzięki takiemu podejściu oprócz samego systemu możemy uruchomić inne programy na urządzeniu sieciowym, na przykład do analizy ruchu sieciowego jak. Taka architektura systemu pozwala procesom na działanie na kilku procesorach lub rdzeniach jednocześnie, natomiast aplikacje z wyższym priorytetem nie są w stanie zawiesić czy usunąć tymczasowo innych procesów by wywłaszczyć przydzielone im zasoby sprzętowe.

Jądro Linuxa pozwala nam na obsługę wirtualnej pamięci większej niż 4 GB poprzez swoją 64-bitową architekturę. W IOS XE to jądro przydziela wirtualną pamięć aplikacjom, ponieważ nie ma tu zaimplementowanego sprzętowego kontrolera, który by się tym zajmował. Ochrona pamięci, która ma zapobiec uszkodzeniu pamięci jednego procesu przez drugi jest zaimplementowana w IOSd.

IOS XE w odróżnieniu od innych systemów Cisco posiada jeden uniwersalny obraz, w którym już znajdują się różne paczki funkcji znane z systemu IOS. Każda z tych paczek może być włączona poprzez aktywowanie odpowiedniej licencji na urządzeniu. Istnieje również możliwość przetestowania danej paczki z funkcjami za darmo przez 90 dni, po tym czasie należy paczkę wyłączyć lub aktywować kupioną licencję.

Tabela 1. Porównanie systemów operacyjnych Cisco

|  |  |  |  |
| --- | --- | --- | --- |
| System | Jądro | Zarządzanie pamięcią | Dodatkowe funkcje |
| IOS | Monolityczne | Brak wsparcia wirtualnej pamięci | Każdy pakiet funkcji skompilowany, jako osobny plik dla osobnej platformy |
| IOS XE | Jądro Linuxa | Wsparcie 64-bitowej pamięci wirtualnej | Uniwersalny obraz, który zawiera wszystkie pakiety funkcji znane z IOS |
| IOX XR | Mikro jądro | Wsparcie wirtualnej pamięci z dedykowanym kontrolerem sprzętowym | Dodatkowe funkcje są dodawane poprzez osobne pliki PIE |

Źródło: opracowanie własne na podstawie (Edgeworth, 2015)

W tabeli 1 zostało przedstawione porównanie pomiędzy systemami Cisco gdzie widać, że każdy system różni się pomiędzy sobą czy to w zarządzaniu pamięcią czy w użytym jądrze.

## **1.4 Cisco Identity Services Engine (ISE)**

Cisco ISE ukazał się w 2011 roku i był pierwszym produktem firmy Cisco zbudowanym od zera by dostarczyć klientom scentralizowany system zarządzający dostępem do sieci LAN. W miarę upływu czasu firma rozbudowywała ISE by posiadał więcej funkcji oraz nowe rozwiązania techniczne, co zaowocowało tym, że Cisco ISE jest jednym z najbardziej rozbudowanych produktów do zarządzania bezpieczeństwem sieci na rynku[[5]](#footnote-5).

ISE posiada wiele funkcjonalności a najważniejsze z nich to:

* Scentralizowana kontrola dostępu do sieci
* Uproszczone przeprowadzanie audytów bezpieczeństwa
* Uproszczony dostęp do sieci dla gości
* Automatyczna reakcja na zagrożenia występujące w sieci lokalnej
* Administracja urządzeniami sieciowymi poprzez protokół TACAS+

Identity Service Engine jest przygotowany do pracy bezpośrednio na fizycznych urządzeniach, może też działać na narzędziach do zarządzania procesami wirtualizacji takimi jak: VMware, Linux KVM czy Microsoft Hyper-V. Dzięki możliwości uruchomienia platformy na wirtualnej maszynie możemy ją łatwo skalować dokładając kolejne serwery i zyskać redundancje na wypadek awarii jednego z serwerów.

Pomimo głównego zadania dla ISE, jakim jest kontrola dostępu do sieci posiada również rozbudowany moduł AAA. Moduł ten dzięki wykorzystaniu autorskiego protokołu uwierzytelniania Cisco zwanego Terminal Access Controller Access-Control System Plus (TACACS+) zapewnia bezpieczną metodę logowania do urządzeń sieciowych oraz rozbudowaną kontrole przywilejów.

## **1.5 Terminal Access Controller Access-Control System Plus (TACACS+)**

Opracowany przez Cisco w 1993 roku protokół TACACS+ i jest jednym z dwóch najpopularniejszych protokołów, które oferują scentralizowaną usługę AAA. Protokół ten został opracowany, jako następca XTACACS, z którym nie jest kompatybilny.

Cisco opracował go, jako lepszą i bezpieczniejszą alternatywę dla istniejącego już protokołu Remote Authentication Dial-In User Service (RADIUS).

Tabela 2. Porównanie pomiędzy TACACS+ i RADIUS

|  |  |  |
| --- | --- | --- |
| Cechy | TACACS+ | RADIUS |
| Najczęściej używane dla | Urządzenia sieciowe | Użytkownicy |
| Protokół transportowy | TCP | UDP |
| Używane port(y) do uwierzytelnienia | 49 | 1645, 1812 |
| Protokół szyfruje hasła | Tak | Tak |
| Cechy | TACACS+ | RADIUS |
| Protokół Szyfruje cały pakiet | Tak | Nie |
| Wspiera funkcje autoryzacji konkretnych komend dla użytkowników | Tak | Nie |
| Zdefiniowany przez | Cisco | RFC 2865, 2866 |

Źródło: opracowanie własne na podstawie (Odom, 2017)

W tabeli drugiej jest przedstawione porównanie pomiędzy dwoma najpopularniejszymi protokołami uwierzytelniającymi gdzie widocznym jest, że protokół TACACS+ jest bezpieczniejszy niż RADIUS oraz daje o wiele większe możliwości konfiguracji dostępu na urządzeniach sieciowych.

Ze względu na duże korzyści wynikające z używania autorskiego protokołu, Cisco zaleca używanie TACACS+, jako protokół do uwierzytelniania przy logowaniu na urządzeniach sieciowych.

Przy próbie logowania się do urządzenia sieciowego, na którym jest ustawione logowanie za pomocą tego protokołu użytkownik wprowadza login i hasło, a urządzenie sieciowe na przykład router przekazuje zaszyfrowany pakiet z tymi danymi do zewnętrznego serwera TACACS+ (najczęściej jest to serwer Cisco ISE). Serwer AAA odpowiada jedną z dwóch wiadomości, albo wysyła kod ACCEPT, czyli podane dane do logowania były poprawne lub serwer wysyła kod REJECT odrzucając podaną kombinacje loginu i hasła, jako nieprawidłową[[6]](#footnote-6).

## **1.6 Uwierzytelnianie (ang. *Authentication*)**

Authentication jest to proces mający za zadanie potwierdzić naszą tożsamość na podstawie, co najmniej jednego z trzech elementów:

* Coś, co mamy
* Coś, co wiemy
* Czymś jesteśmy

Uwierzytelnianie nie musi ograniczać się tylko do jednego elementu wymienionego powyżej by potwierdzić naszą tożsamość. Możemy używać uwierzytelniania dwuskładnikowego (ang. *Two Factor Authentication* (2FA)), dzięki czemu zwiększamy poziom bezpieczeństwa, ponieważ podania oprócz na przykład czegoś, co wiemy jak login i hasło musimy użyć tokenu, czyli coś, co mamy.

Authentication jest pierwszym krokiem w AAA i występuje w różnych programach za każdym razem, gdy musimy podać na przykład login i hasło.

Uwierzytelnianie na urządzeniach sieciowych może zostać przeprowadzone za pomocą różnych protokołów takich jak TACACS+ czy RADIUS. Authentication może też zostać przeprowadzone lokalnie gdzie urządzenie sieciowe sprawdzi lokalnie czy użytkownik podaje prawidłowy login i hasło. Lokalne uwierzytelnianie na urządzeniu sieciowym jest niezalecane ze względu na możliwość podejrzenia danych do logowania w konfiguracji urządzenia oraz przy większej liczbie urządzeń zmiana hasła dla jednego z użytkowników może być bardzo czasochłonna[[7]](#footnote-7).

## **1.7 Autoryzacja (ang. *Authorization*)**

Autoryzacja jest drugim modułem w strukturze AAA, który ma za zadanie przyznania użytkownikowi praw dostępu, które posiada. Uprawnienia mogą zostać nadane dla pewnej grupy lub indywidualnie użytkownikowi z tym, że przywileje nadane użytkownikowi bezpośrednio są ważniejsze niż przywileje, które otrzymuje za pośrednictwem uczestnictwa w grupie.

Autoryzacja klienta następuje tylko po poprawnym przejściu etapu uwierzytelniania, czyli klient musi podać poprawne dane w procesie autentykacji i po ich weryfikacji następuje etap autoryzacji[[8]](#footnote-8).

Proces autoryzacji najłatwiej jest dostrzec w środowisku firmowym, gdy próbujemy uruchomić aplikację, która wymaga praw administratora, gdy takowych nie posiadamy. Pomimo podania poprawnych danych logowania naszego konta aplikacja nie uruchomi się a my otrzymamy błąd, w którym zostaniemy poinformowani, że nie mamy wystarczających uprawnień do wykonania tej operacji.

Autoryzacja może zostać przeprowadzana lokalnie natomiast takie rozwiązanie nie skaluje się dobrze i najczęściej proces ten przebiega na zdalnym serwerze AAA.

Na urządzeniach sieciowych Cisco istnieje 16 stopni przywilejów (od 0 do 15, gdzie 0 to najniższy stopień przywilejów, a 15 najwyższy)[[9]](#footnote-9). Podczas autoryzacji urządzenie sieciowe sprawdza lokalnie lub na zdalnym serwerze AAA, jaki poziom przywilejów ma użytkownik, który podał określony login i hasło i na tej podstawie Cisco IOS uprawnia użytkownika do używania określonych komand.

## **1.8 Accounting**

Accounting polega na zapisywaniu zdarzeń na serwerze AAA lub innym przeznaczonym tylko do tego serwerze (na przykład SYSLOG server). Jest to ostatni moduł w strukturze AAA, który umożliwia śledzenie zdarzeń, które dzieją się w chwili obecnej lub takich, które już się wydarzyły.

Logi, które są zapisywane pozwalają na monitorowanie, na przykład, do jakich treści użytkownik uzyskał lub próbował uzyskać dostęp. Urządzenia sieciowe również mogą zbierać logi lub je wysyłać na zewnętrzny serwer o tym, co się dzieje na danym urządzeniu. Dzięki użyciu takich protokołów jak TACACS+ jesteśmy w stanie sprawdzić, jakich komend użył użytkownik na danym urządzeniu[[10]](#footnote-10).

Zebrane logi możemy eksportować do plików CSV lub Open Database Connectivity (ODBC) w celu łatwiejszego ich przeglądania.

## **1.9 Wirtualizacja (ang. *Virtualization*)**

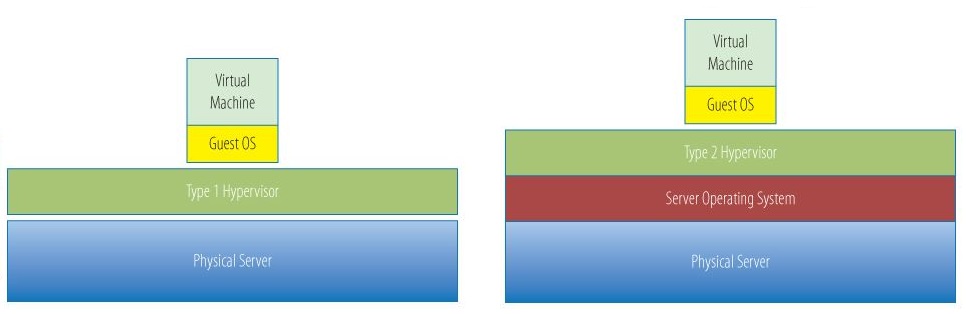
Wirtualizacja często jest określana warstwą abstrakcji nałożonej na sprzęt fizyczny by ten stał się obiektem logicznym. Dzięki takiemu zabiegowi jesteśmy w stanie lepiej kontrolować zasoby, które są przypisane do wirtualnej maszyny (ang. virtual machine).

Gdy posiadamy fizyczny serwer zmiana jego zasobów sprzętowych takich jak płyta główna (ang. motherboard) czy central processing unit (CPU) często sprawia, że system, który jest już na nim zainstalowany i skonfigurowany przestanie się uruchamiać, przez co będziemy musieli go zainstalować i skonfigurować ponownie. Wirtualizacja w takich przypadkach oszczędza bardzo wiele czasu, ponieważ możemy bez potrzeby instalowania i konfigurowania systemu na nowo powiększyć na przykład ilość dostępnych rdzeni procesora.

Wirtualizacja ułatwia nam lepsze wykorzystanie zasobów, a co za tym idzie oszczędność pieniędzy, ponieważ lepiej wykorzystując nasze zasoby możemy posiadać mniej serwerów. W wirtualnym środowisku zasoby przypisane do maszyn wirtualnych mogą się zmieniać w czasie rzeczywistym. Takie podejście pozwala by maszyna wirtualna, która w danej chwili nie potrzebuje dużej ilości zasobów systemowych może je udostępnić maszynie, która w danej chwili ich potrzebuje.

Kiedyś do wirtualizacji wykorzystywane był Virtual Machine Monitor (VMM) natomiast z biegiem czasu ewoluował w trochę inny rodzaj oprogramowania pełniący więcej zadań, którego nazywamy teraz hypervisorem. Jest to oprogramowanie, które rozdziela fizyczne zasoby serwera pomiędzy wirtualne maszyny, które działają na danym serwerze.

Rysunek 3 Porównanie hypervisorów Typu 1 i 2



Źródło: opracowanie własne na podstawie [Portnoy, 2016]

Na rysunku czwartym zostało przedstawione porównanie dwóch typów hypervisorów, wyróżniamy typ pierwszy oraz typ drugi. W typie 1 hypervisor znajduje się bezpośrednio na fizycznym serwerze, jest to implementacja tak zwana bare-metal, czyli nic nie dzieli hypervisora oraz sprzętu serwera. Implementacja typu pierwszego wyróżnia się lepszą wydajnością, ponieważ między hypervisorem, a fizycznym sprzętem nie ma dodatkowej warstwy, jaką jest system operacyjny. Kolejną zaletą takiego rozwiązania jest lepsze bezpieczeństwo, ponieważ systemy operacyjne mogą posiadać dziury bezpieczeństwa, w tym wypadku, gdy takiego systemu nie ma i jest tylko hypervisor atakujący może, co najwyżej unieruchomić nam tylko jedną maszynę wirtualną, gdy inne będą pracowały bez problemu[[11]](#footnote-11). Jednym z najpopularniejszych hypervisorów typu 1 są: Hyper-V, VMware ESX i ESXi.

Hypervisor typu drugiego posiada dodatkową warstwę, która jest widoczna na rysunku 4. Ta dodatkowa warstwa, jaką jest system operacyjny, na którym działa hypervisor sprawia, że są one mniej wydajne, mniej stabilne oraz mniej bezpieczne. Pomimo swoich znaczących wad są one bardzo popularne wśród zwykłych użytkowników, ponieważ są o wiele prostsze w instalacji i użytkowaniu niż hypervisory typu pierwszego. Jednym z najpopularniejszych hypervisorów typu 2 są: VirtualBox, VMware Workstation, VMware Player.

## **1.10 Microsoft Hyper-V**

Hyper-V ukazał się wraz z premierą Windows Server 2008 zastępując poprzednie narzędzie do wirtualizacji od Microsoftu. Windows Virtual PC, którego zastąpił Hyper‑V był hypervisorem typu 2, który nie przyjął się dobrze na rynku i nie był szeroko wykorzystywany.

W przeciwieństwie do poprzedniego hypervisora Hyper-V jest typem 1, czyli bazuje bezpośrednio na sprzęcie. Wiele osób odnosi błędne wrażenie jakoby był on typem 2, ponieważ Hyper-V w systemie operacyjnym włącza się, jako funkcję i pojawia się on po ponownym restarcie komputera, jako program w systemie. Pomimo że można odnieść wrażenie, że jest on hypervisorem typu 2 jest on typem 1, ponieważ po włączeniu funkcjonalności hiper-v podczas restartu komputera dokonywane są zmiany i nasz system operacyjny działa, jako specjalna maszyna wirtualna[[12]](#footnote-12).

Dzięki takiemu podejściu użytkownik otrzymał wydajny hypervisor, który jest bardzo prosty w instalacji oraz użytkowaniu. Stał się on również bardzo popularny i jest wykorzystywany w środowiskach domowych oraz serwerowych gdzie na równi rywalizuje z hypervisorami typu 1 oraz 2.

Microsoft intensywnie rozwija Hyper-V i od czasu swojej premiery z Windows Server 2008 doszło dużo nowych funkcji takich jak:

* Zagnieżdżona wirtualizacja
* Rozszerzalny wirtualny switch
* Backup w chmurze
* Dzielone dyski wirtualne
* Automatyczna aktywacja maszyn wirtualnych

To tylko niektóre nowe funkcje, które dodał Microsoft na przestrzeni lat czyniąc Hyper-V jednym z najbardziej rozbudowanych hypervisorów na rynku.

Pomimo licznych zalet tego hypervisora posiada również on swoje ograniczenia takie jak:

* Brak wirtualizacji sprzętu audio
* Przed Windowsem 8.1 oraz Windows Server 2012 R2 problem ten można było obejść poprzez podłączenie się Remote Desktop Connection do maszyny wirtualnej
* Problemy z grafiką na maszynach wirtualnych
* Występuje on na procesorach nieposiadających Second Level Address Translation (SLAT)
* Grupowanie kart sieciowych
* Nie jest wspierane, jeżeli producent karty nie dostarcza sterowników

## **1.11 Router**

Router jest urządzeniem sieciowym, który przekazuje pakiety danych pomiędzy sieciami komputerowymi. Routery pełnią funkcję kierowania ruchu w Internecie. Dane wysłane przez Internet takie jak strona internetowa czy email są pakietami danych. Pakiety najczęściej są przesyłane z jednego routera do innego routera w innej sieci i tak w kółko aż pakiet dotrze do celu.

Router jest połączony do dwóch lub więcej sieci. Kiedy pakiet przychodzi z jednej sieci router sprawdza adres sieciowy w pakiecie wykorzystując tablice routingu decyduje gdzie dalej przekazać pakiet[[13]](#footnote-13).

Najczęściej spotykany typ routera są domowe lub dla małych biur, które mają ograniczone funkcje i najczęściej tylko przekazują pakiety dalej do sieci Internet. Jako przykładem może być digital subsribers line (DSL) router, który umożliwia połączenie poprzez dostawcę Internetu. Bardziej zaawansowane routery klasy biznesowej łącza duże przedsiębiorstwa bezpośrednio do routerów corowych dostawców Internetu by przesyłać dane z dużą przepustowością przez łącza światłowodowe.

Router posiada 2 typy elementów sieciowych, które nazywają się płaszczyznami przetwarzania:

* control plane: router utrzymuje tablice routingu, która zawiera informacje gdzie pakiet z danym adresem IP powinien zostać przekazany. Tablica wypełnia się poprzez statyczne drogi dodawane manualnie przez użytkownika lub używając dynamicznego protokołu routingu, który dodaje takie drogi do tablicy.
* forwarding plane: router przekazuje pakiety pomiędzy interfejsami wchodzącymi a wychodzącymi. Przekazuje je do poprawnych sieci używając informacji zawartych w nagłówkach pakietów, które dopasowuje do informacji zawartych w tablicy routingu.

Wyróżniamy routery dostępowe, corowe oraz dystrybucyjne. Routery dostępowe włączając w to małe routery dla domowych biur są najczęściej zlokalizowane w domu lub w biurze, które nie potrzebują hierarchicznego routing. Najczęściej są one zoptymalizowane pod minimalne koszty, przez co posiadają niewiele funkcji. Dystrybucyjne to routery, które agregują ruch z wielu routerów dostępowych. Routery dystrybucyjne są często odpowiedzialne za wymuszanie quality of service (QoS) w sieci WAN, przez co są wydajniejsze i posiadają więcej pamięci by obsługiwać wiele połączeń. W dużych przedsiębiorstwach routery corowe najczęściej łączą kilka routerów dystrybucyjnych z różnych budynków przedsiębiorstwa. Optymalizowane są pod maksymalną wydajność i przepustowość by sprostać dużemu ruchowi sieciowemu.

Routery często są rozróżniane są ze względu na to, w jakiej sieci działają. Routery działające w sieci lokalnej lub wewnątrz organizacji nazywane są routerami wewnętrznymi. Kolejnym typem routerów są routery, które działają na sieci szkieletowej Internetu, one opisywane są, jako routery zewnętrzne. Ostatnim typem routerów często spotykanych w domach są routery graniczne lub inaczej zwane bramami domyślnymi, łączą one sieci wewnętrzne z sieciami wide area network (WAN).

## **1.12 Network Switch**

Przełącznik sieciowy (ang. Network Switch) jest sieciowym urządzeniem, które łączy komputery w sieci lokalnej. Switch wysyła i odbiera pakiety przekazujące je do urządzeń docelowych. Switch zawiera o wiele więcej portów niż router, ponieważ jego zadanie jest trochę inne gdyż on ma zapewniać połączenie w sieci lokalnej, a nie poza siecią lokalną.

Switch najczęściej przekazuje ramki bazując na adresie MAC zawartym w nagłówku, to dotyczy tylko podstawowych switchy. Oprócz przełączników drugiej warstwy są switche warstwy, 3 które przekazują pakiety na podstawie adresu MAC lub adresu IP[[14]](#footnote-14).

Przełączniki sieciowe zostały wprowadzone, jako następcy hubów, dzięki temu ramki przestały być ciągle wysyłane na wszystkie porty tak jak to było w przypadku hubów, które nie były świadome drugiej warstwy i po prostu przekazywały ramki dalej. Switche rozprzestrzeniają ramki tylko, podczas gdy nie posiadają w tablicy MAC adres, do którego ma zostać dostarczona ramka, gdy proces uczenia się adresów zakończy się wtedy switche przekazują ramki bezpośrednio do odpowiednich portów.

Switche pełnią ważną rolę w rozdzielaniu ruchu na warstwie drugiej za sprawą virtual local area network (VLAN), dzięki której są w stanie rozdzielić ruch pomiędzy różnymi VLANami zapewniając większe bezpieczeństwo i możliwość udostępnienia konkretnych zasobów sieciowych. Dzięki takiemu podziałowi większa domena rozgłoszeniowa staje się mniejsza i dzięki temu zmniejsza się ilość pakietów rozgłoszeniowych (ang. broadcast), które krążą po sieci zużywając przepustowość łączy.

Switch pełni ważną rolę we wszystkich nowoczesnych sieciach lokalnych. Firmy mające siedzibę mieszczącą się w pokoju najczęściej posiadają wbudowany switch w router, który pełni rolę połączenia do Internetu. Większe przedsiębiorstwa mogą posiadać od kilku do nawet kilku tysięcy zarządzanych switchy.

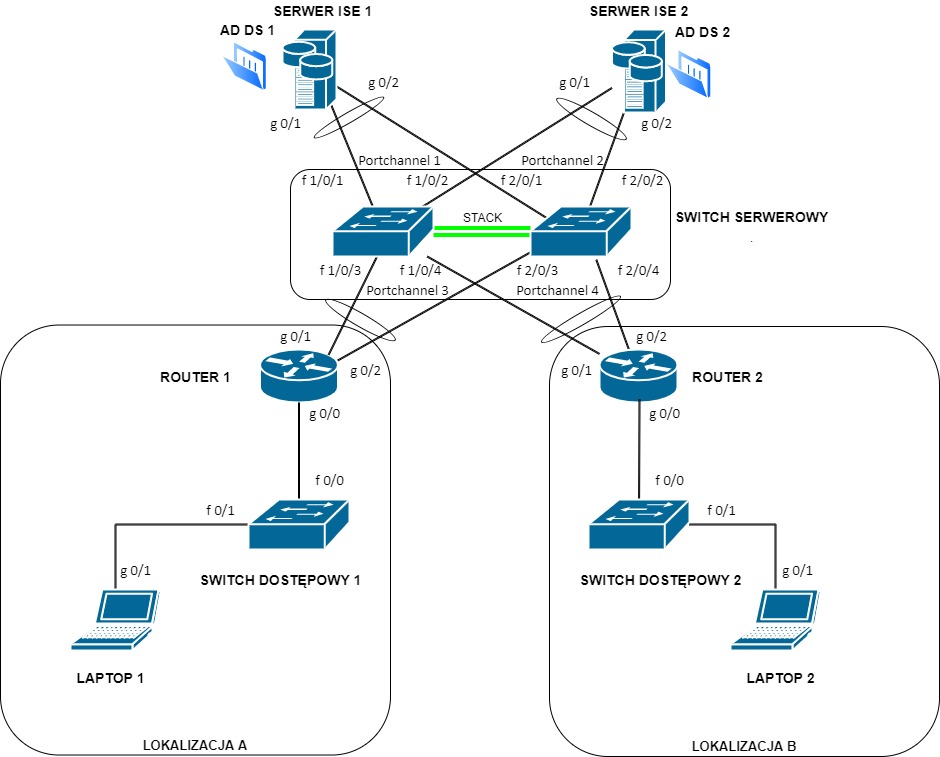
Switche dostępowe są używane na skraju sieci i pełni funkcję punktu połączenia dla urządzeń użytkowników. Kolejnym typem switchy są switche dystrybucyjne, które łączą wiele switchy dostępowych, bardzo często dystrybucyjne switche są przełącznikami warstwy, 3 ponieważ są one wydajniejsze przy routingu pomiędzy VLANami. Switche corowe łączą przełączniki dystrybucyjne oraz routery corowe, które przekazują ramki do routerów a te dalej do sieci Internet.

Wyróżniamy 3 typt switchy:

* Zarządzalne: jesteśmy w stanie podłączyć się do urządzenia po porcie szeregowym lub porcie USB i za pomocą konsoli jesteśmy w stanie wprowadzać komendy, dzięki którym możemy zmienić zachowanie i działanie switcha
* Nie zarządzalne: są to switche, którymi nie możemy zarządzać, są to proste tanie urządzenia nadające się do małych firm lub gospodarstw domowych
* Inteligentne: jesteśmy w stanie zarządzać switchem w ograniczony sposób przez na przykład interfejs webowy

# **Projekt Sieci**

Rysunek 4 Schemat sieci



Źródło: opracowanie własne

## **2.1 Wykorzystane rozwiązania**

- Kontroler domeny - Active Directory Domian Services (AD DS.)jest usługą służącą do zarządzania tożsamością, nadawania dostępu do zasobów sieciowych lub usług w sieci. Pozwala zabezpieczyć i zarządzać infrastrukturą, użytkownikami i zasobami. AD DS. jest miejscem do przechowywania i zarządzania informacjami o zasobach sieciowych, zapewnia wsparcie dla aplikacji korzystających z katalogu , takich jak Microsoft Exchange Server oraz umożliwia scentralizowane zarządzanie.

- EtherChannel:, Aby można było wykorzystać większą ilość połączeń, możemy albo wyłączyć protokół STP, co jest bardzo ryzykowne, bo może doprowadzić do paraliżu całe sieci, albo możemy wykorzystać funkcjonalność LAG (ang. Link Aggregation Port), zwaną w technologii CISCO kanałem ethernetowym (ang. EtherChannel) i połączyć klika fizycznych interfejsów w jeden logiczny. Dzięki czemu rozwiązujemy problem niebezpieczeństwa w razie wystąpienia awarii związanego z wykorzystaniem tylko jednego przewodu łączącego urządzenia, a przy okazji nie będziemy zmuszeni wyłączyć STP na przełącznikach.

EtherChannel to technologia, która umożliwia wykorzystanie nadmiarowości w bardziej efektywny sposób. Pozwala, bowiem na połączenie kilku fizycznych połączeń w jedno logiczne.

- VLAN (ang. Virtual LAN) to wirtualna sieć wyodrębniona z sieci fizycznej. Oznacza to, że urządzenia fizycznie podłączone są do jednego przełącznika, ale poprzez zastosowanie technologii oznaczania ramek (tagowania) można je oznaczyć tak, że będą dla siebie niewidoczne. Będą częścią innych zbiorów.

Tabela 3Adresacja w sieci

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Urządzenie | Interfejs | Adres IP | Maska | | Brama domyślna | |
| Serwer ISE 1 | gigabitethernet 0/1 | Portchannel 1 | | | | |
| Serwer ISE 1 | gigabitethernet 0/2 |
| Serwer ISE 1 | Portchannel 1 | 192.168.100.1 | 255.255.255.0 | | 192.168.100.254 | |
| Serwer ISE 2 | gigabitethernet 0/1 | Portchannel 2 | | | | |
| Serwer ISE 2 | gigabitethernet 0/2 |
| Serwer ISE 2 | Portchannel 2 | 192.168.100.2 | | 255.255.255.0 | | 192.168.100.254 |
| AD DS 1 | Portchannel 1 | 192.168.100.3 | | 255.255.255.0 | | 192.168.100.254 |
| AD DS 2 | Portchannel 2 | 192.168.100.4 | | 255.255.255.0 | | 192.168.100.254 |
| Switch serwerowy | fastethernet 1/0/1 | Portchannel 1 | | | | |
| Switch serwerowy | fastethernet 1/0/2 | Portchannel 2 | | | | |
| Switch serwerowy | fastethernet 1/0/3 | Portchannel 3 | | | | |
| Switch serwerowy | fastethernet 1/0/4 | Portchannel 4 | | | | |
| Switch serwerowy | fastethernet 2/0/1 | Portchannel 1 | | | | |
| Switch serwerowy | fastethernet 2/0/2 | Portchannel 2 | | | | |
| Switch serwerowy | fastethernet 2/0/3 | Portchannel 3 | | | | |
| Switch serwerowy | fastethernet 2/0/4 | Portchannel 4 | | | | |
| Switch serwerowy | Portchannel 1 | - | - | | - | |
| Switch serwerowy | Portchannel 2 | - | - | | - | |
| Switch serwerowy | Portchannel 3 | - | - | | - | |
| Urządzenie | Interfejs | Adres IP | Maska | | Brama domyślna | |
| Switch serwerowy | Portchannel 4 | - | - | | - | |
| Router 1 | gigabitethernet 0/0 | 10.10.10.254 | 255.255.255.0 | | - | |
| Router 1 | gigabitethernet 0/1 | Portchannel 3 | | | | |
| Router 1 | gigabitethernet 0/2 |
| Router 1 | Portchannel 3 | 192.168.100.252 | 255.255.255.0 | | - | |
| Router 2 | gigabitethernet 0/0 | 10.10.20.254 | 255.255.255.0 | | - | |
| Router 2 | gigabitethernet 0/1 | Portchannel 4 | | | | |
| Router 2 | gigabitethernet 0/2 |
| Router 2 | Portchannel 4 | 192.168.100.253 | 255.255.255.0 | | - | |
| Switch dostępowy 1 | fastethernet 0/1 | - | - | | - | |
| Switch dostępowy 1 | fastethernet 0/2 | - | - | | - | |
| Switch dostępowy 2 | fastethernet 0/1 | - | - | | - | |
| Switch dostępowy 2 | fastethernet 0/2 | - | - | | - | |
| Laptop 1 | gigabitethernet 0/1 | 10.10.10.1 | 255.255.255.0 | | 10.10.10.254 | |
| Laptop 2 | gigabitethernet 0/1 | 10.10.20.2 | 255.255.255.0 | | 10.10.20.254 | |
| HSRP |  | 192.168.100.254 | 255.255.255.0 | |  | |

Źródło: opracowanie własne

Weryfikacja poprawności działania projektu

1. Test Serwera ISE
   1. Awaria Serwera ISE 1
   2. Awaria Serwera ISE 2
   3. Awaria obu serwerów jednocześnie
   4. Awaria jednego połączenia etherchannel
2. Test warstwy L3
   1. Awaria Routera 1
   2. Awaria Routera 2
   3. Awaria jednego ze switchy serwerowych
3. Dostęp do urządzeń sieciowych
   1. Próba logowania do Routera 1

Logowanie i poziomy dostępu jako :

* + - Administrator
    - Audytor
    - Użytkownik
  1. Próba logowania do Routera 2

Logowanie i poziomy dostępu jako :

* + - Administrator
    - Audytor
    - Użytkownik
  1. Próba logowania do Switch 1
  2. Próba logowania do Switch 2
  3. Próba logowania do Switch serwerowy

# **Wnioski**

Przedstawiony model sieci gwarantuje bardzo dobry nadzór nad dostępem do urządzeń w sieci. Projekt zapewnia weryfikacje dostępu w pierwszej kolejności przez serwer ISE który bazuje na kontach użytkowników w AD DS., a w przypadku awarii ISE można się nadal zalogować do urządzeń poprzez konta lokalne na poszczególnych urządzeniach.

Kolejnym etapem usprawniania kontroli dostępu może być wprowadzenie systemu SD-Access który bazuje na wprowadzonym w tym projekcie systemie ISE.

Usługi Cisco SD-Access pozwalają na pełna automatyzacje procesów związanych z dostępem do urządzeń, oferują proaktywne monitorowanie i zarządzanie sieci.

# **Bibliografia**

1. Akin T., Hardening Cisco Routers, O’Reilly Media, Sebastopol, 2002, s. 38
2. Carroll B., Cisco Access Control Security: AAA Administrative Services, Cisco Press, Indianapolis, 2004, s. 3, 5
3. Carroll B., Banga P., Santuka V., AAA Identity Management Security, Cisco Press, Indianapolis, 2010, s. 6
4. Edgeworth B., Foss A., Rios R., IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols, Cisco Press, Indianapolis, 2015, s. 2, 6
5. Heary J., Cisco ISE for BYOD and Secure Unified Access Second Edition, Cisco Press, Indianapolis, 2017, s. 23
6. Morimoto R., Shapiro J., Yardeni G., Droubi O., Noel M., Abbate A., Amaris C., Windows Server 2016 Unleashed, Pearson Education, USA, 2017 s. 3
7. Odom W., CCNA 200-301 Official Cert Guide Volume 1, Cisco Press, Indianapolis, 2019 s. 43
8. Odom W., CCNA 200-301 Official Cert Guide Volume 2, Cisco Press, Indianapolis, 2019 s. 32
9. Portnoy M., Virtualization Essentials 2nd Edition, Sybex, Indianapolis, 2016 s. 3
10. Santos O., Stuppi J., CCNA Security 210-260 Official Cert Guide, Cisco Press, Indianapolis, 2015, s. 39
11. Savill J., Mastering Windows Server 2016 Hyper-V, Sybex, Indianapolis, 2016, s. 21
12. Singh D., Vinod M., Anandh V., CCNA Security 210-260 Certification Guide, Pack Publishing, Brimingham, 2018, s. 14, 23
13. Tahir M., Ghattas M., Birhanu D., Nawaz S., Cisco IOS XR Fundamentals, Cisco Press, Indianapolis, 2009, s. 9

## **Netografia**

*Wallace K., Comparing Cisco IOS, NX-OS, and IOS-XR*, 2017, zasoby

Internetu: <https://kwallaceccie.mykajabi.com/blog/comparing-cisco-ios-nx-os-and-ios-xr>, dostęp: 29.12.2019

## **Spis Tabel**

Tabela 1. Porównanie systemów operacyjnych Cisco 9

Tabela 2. Porównanie pomiędzy TACACS+ i RADIUS 10

Tabela 3. Adresacja w sieci 20

**Spis Rysunków**

Rysunek 1. Pakiety funkcji w systemie Cisco IOS 5

Rysunek 2. Architektura mikro jądra w systemie IOS XR 6

Rysunek 3. Porównanie hypervisorów Typu 1 i 2 14

Rysunek 4. Schemat sieci 19

1. Edgeworth B., Foss A., Rios R., *IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols*, Cisco Press, Indianapolis, 2015, s. 2 [↑](#footnote-ref-1)
2. Tahir M., Ghattas M., Birhanu D., Nawaz S., *Cisco IOS XR Fundamentals*, Cisco Press, Indianapolis, 2009, s. 9 [↑](#footnote-ref-2)
3. <https://kwallaceccie.mykajabi.com/blog/comparing-cisco-ios-nx-os-and-ios-xr>, [dostęp: 29.12.2019] [↑](#footnote-ref-3)
4. Edgeworth B., Foss A., Rios R., *IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols*, Cisco Press, Indianapolis, 2015, s. 6 [↑](#footnote-ref-4)
5. Heary J., *Cisco ISE for BYOD and Secure Unified Access Second Edition*, Cisco Press, Indianapolis, 2017, s. 23 [↑](#footnote-ref-5)
6. Singh D., Vinod M., Anandh V., *CCNA Security 210-260 Certification Guide*, Pack Publishing, Brimingham, 2018, s. 14 [↑](#footnote-ref-6)
7. Carroll B., *Cisco Access Control Security: AAA Administrative Services*, Cisco Press, Indianapolis, 2004, s. 3 [↑](#footnote-ref-7)
8. Carroll B., *Cisco Access Control Security: AAA Administrative Services*, Cisco Press, Indianapolis, 2004, s. 5 [↑](#footnote-ref-8)
9. Akin T., *Hardening Cisco Routers*, O’Reilly Media, Sebastopol, 2002, s. 38 [↑](#footnote-ref-9)
10. Carroll B., Banga P., Santuka V., *AAA Identity Management Security*, Cisco Press, Indianapolis, 2010, s. 6 [↑](#footnote-ref-10)
11. Portnoy M., *Virtualization Essentials 2nd Edition*, Sybex, Indianapolis, 2016 s. 3 [↑](#footnote-ref-11)
12. Savill J., *Mastering Windows Server 2016 Hyper-V*, Sybex, Indianapolis, 2016, s. 21 [↑](#footnote-ref-12)
13. Odom W., *CCNA 200-301 Official Cert Guide Volume 1*, Cisco Press, Indianapolis, 2019 s. 43 [↑](#footnote-ref-13)
14. Odom W., *CCNA 200-301 Official Cert Guide Volume 2*, Cisco Press, Indianapolis, 2019 s. 32 [↑](#footnote-ref-14)