Zapewnienie gwarantowanej jakości i dostępności usług transmisji danych przy wykorzystaniu radiokomunikacji satelitarnej

Praca spełnia wymagania stawiane pracom dyplomowym na studiach pierwszego stopnia.

Wstęp

Motywacją do napisania niniejszej pracy było udokumentowanie, zbudowanej przez autora sieci satelitarnej oraz przedstawienie łączności satelitarnej jako dziedziny teleinformatyki. Praca zawiera praktyczne przykłady oraz symulacje takiej sieci, gdyż wynajęcie pasma satelitarnego wyłącznie na potrzeby pomiarów i testów jest wysoko nieopłacalne. Łączność satelitarna w dzisiejszych czasach jest wykorzystywana głównie jako łącze zapasowe lub przeznaczone do dedykowanych transmisji, dlatego projekt sieci przedstawionej w pracy skupia się głównie na jej specyfice działania oraz konfiguracji urządzeń do zastosowania w takich sieciach.

Treść pracy jest podzielona na sekcje tematyczne. W pierwszej sekcji omówione są podstawy łączności satelitarnej. Następnie w kolejnych dwóch sekcjach opisane zostają technologie zastosowane do wykonania sieci, pomiarów oraz symulacji. Wszystkie kolejne sekcje dotyczą specyfiki działania, projektu oraz rozwiązań technicznych zastosowanych w pracy. W ostatnich rozdziałach przedstawione są możliwości rozbudowy oraz przyszłe kierunki rozwoju prezentowanej sieci.

Wszystkie opisy w tej pracy dotyczą satelit komunikacyjnych; żaden z opisów ani żadna instalacja lub konfiguracja nie odnosi się do satelit pozycjonowania lub obrazowania. Dotyczy to również prezentowanych anten oraz terminali – są one przeznaczone wyłącznie do teleinformatycznych sieci satelitarnych, a nie do transmisji telewizji czy sygnałów audiowizualnych odbieranych za pomocą dekoderów telewizji satelitarnej.

Cel realizacji pracy

Celem niniejszej pracy jest:

- Przedstawienie podstaw łączności satelitarnej,
- Ukazanie zasady działania urządzeń wykorzystywanych w tej dziedzinie,
- Opis rodzajów satelit komunikacyjnych oraz pasm satelitarnych,
- Prezentacja technologii wykorzystanych w pracy,
- Zbadanie narzędzia TC jako środka do symulacji parametrów sieci satelitarnych,
- Szczegółowe opisanie specyfiki działania sieci satelitarnych oraz krok po kroku przedstawienie konfiguracji takiej sieci.

Zadania do realizacji

Poniżej wymienione są główne zadania niezbędne do spełnienia wymagań postawionych we wstępie:

1. Przygotowanie sekcji wyjaśniającej podstawy łączności satelitarnej.
2. Wyjaśnienie oraz przedstawienie technologii satelitarnych wykorzystanych w pracy.
3. Przeprowadzenie testu narzędzia TC pod systemem Linux.
4. Wyjaśnienie oraz przedstawienie technologii sieciowych wykorzystanych w pracy.
5. Przedstawienie wymagań funkcjonalnych oraz niefunkcjonalnych sieci satelitarnej.
6. Implementacja oraz konfiguracja urządzeń – opis krok po kroku.
7. Wymienienie fizycznych urządzeń zastosowanych do wdrożenia.
8. Przyszłe drogi badań lub ścieżki rozbudowy.
9. Podsumowanie uzyskanych wyników oraz wniosków.

Wstęp do łączności satelitarnej

Antena satelitarna


Antena

satelitarna, Raisting Niemcy. CC BY-SA 2.5
Źródło: https://pl.wikipedia.org/wiki/Plik:Erdfunkstelle_Raisting_2.jpg

Antena satelitarna to niezbędna część traktu satelitarnego, bez której nie może działać ani część nadawcza jak i również część odbiorcza. Jest to element służący do nadawania lub odbioru sygnału radiowego, najczęściej z satelitów telekomunikacyjnych. Stosowane często w gospodarstwach domowych do odbioru telewizji satelitarnej.

Na powyższym rysunku 1 przedstawiono antenę satelitarną (średnicy 28.5m) stosowaną w transmisji przez europejskie teleporty. Ateny takie w dzisiejszych czasach są już rzadko stosowane gdyż technologia półprzewodnikowa umożliwiła budowę wzmacniaczy wysokiej mocy przy optymalizacji kosztów takiego wzmacniacza. W nowych instalacjach stosuje się maksymalnie anteny o średnicy nie większej niż 10 metrów.

Wygląd anteny wynika z tego że przy częstotliwościach EHF (30-300 GHz), zjawiska falowe uwidaczniają się zdecydowanie bardziej niż przy niższych częstotliwościach. Atena satelitarna przypomina zdecydowanie bardziej swoim działaniem zwierciadło paraboliczne niż klasyczną antenę bazującą na zasadzie dipola pół falowego. Konsekwencją tego jest również to że możemy w łatwy sposób obliczyć zysk takiej anteny.

$$G = \frac{4 \pi A}{\lambda^2}e_A = (\frac{\pi d}{\lambda})^2 e_A \label{eq:antenna_gain}$$

- A: pole powierzchni apertury anteny. Rozmiar otworu przez który przechodzą fale elektromagnetyczne.
- d: Średnica anteny jeżeli antena jest okrągła.
- λ: Długość fali elektromagnetycznej.
- e_A: Parametr wydajności apertury, pomiędzy 0 a 1.

Z tego wzoru możemy wywnioskować że im większa średnica anteny tym większy jej zysk. Dlatego w starszych instalacjach z lat 90 stosowano bardzo duże anteny, ponieważ wzmacniacze dużych mocy na wysokie pasmo były bardzo nie wydajane energetycznie oraz kosztowo.

Budowa sztucznego satelity ziemskiego

Makieta ERS 2 – sztucznego satelity Ziemi
Źródło: https://commons.wikimedia.org/wiki/File:ERS_2.jpg

Sztuczny satelita ziemski to każdy obiekt wykonany przez człowieka który porusza się po pewnej orbicie wokół ziemi. Pierwszym tego rodzaju obiektem był Sputnik 1, wystrzelony na orbitę przez ZSRR w 1957 roku. W tym rozdziale są opisane główne części które są odpowiedzialne za działanie takiego satelity. Poniższe sekcje skupiają się głównie na kwestiach elektroniki oraz teleinformatyki, kwestie mechaniczne są omówione mniej obszernie.

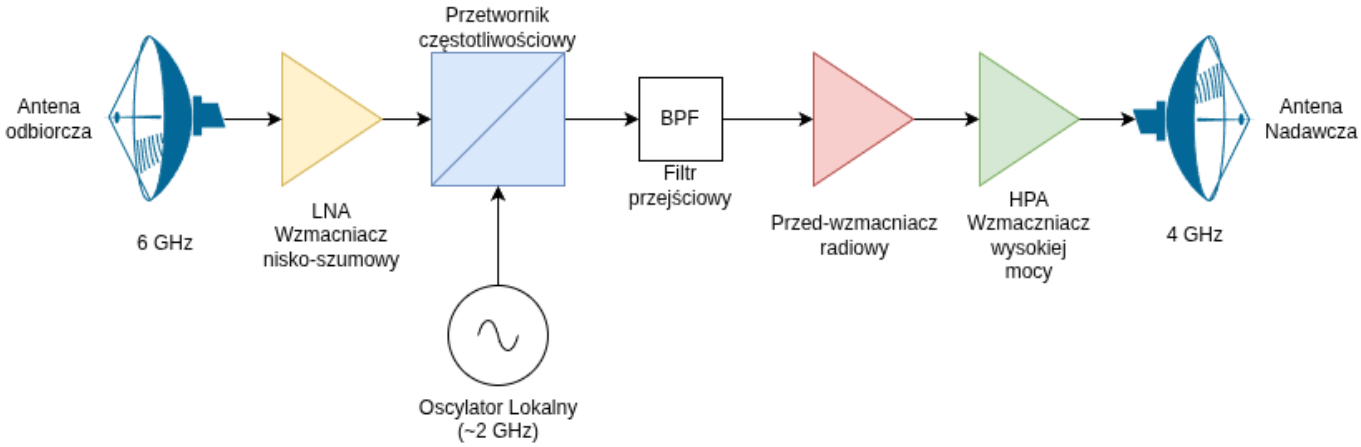
Pozycjonowanie oraz kontrola orbitalna satelity

Każdy z satelit stworzonych przez ludzi, nie miał dostatecznie dużo czasu (Miliardów lat) żeby ustabilizować swoją orbitę, więc potrzebuje on kompensacji, która pozwoli mu utrzymać się na jego wyznaczonej pozycji. Pozycje satelitów geostacjonarnych są oznaczane ze względu na odchylenie na wschód oraz na zachód od południka zerowego. Na przykład satelita wysunięty nad równikiem na

wschód o 7 stopni od południka zerowego będzie nazwany „E7”, w dzisiejszych czasach z racji dużej zajętości pozycji czasami wysyła się kilka satelit na jedną pozycję powoduje to wtedy że nazewnictwo wygląda np. „E7A”, „E7B”, „E7C”.

Sama kompensacja pozycji satelity jest realizowana poprzez silniki odrzutowe, wyrzucają one mieszankę gazu która pozwala kompensować ruchy około orbitalne satelity. Ilość paliwa jest zwykle ograniczona co powoduje że satelity mają ograniczoną żywotność np. satelita Eutelsat 7B wysłany na obitę w 2013 roku jest przeznaczony do działania około 15 lat, co oznacza że w roku 2028 prawdopodobnie skończy mu się paliwo do przeprowadzania kompensacji. Rozwiązaniem w takich sytuacjach jest zastosowanie anteny nadawczo-odbiorczych z śledzeniem satelity, pozwala to wtedy na wykorzystanie satelity jeszcze przez kilka lat po zakończeniu się jego daty przydatności.

Transponder



Schemat przykładowego transpondera [Opracowanie własne]

Transponder satelitarny to kluczowy element systemów komunikacyjnych, odpowiedzialny za odbieranie, wzmacnianie i retransmisję sygnałów. Jego budowa obejmuje kilka kluczowych komponentów:

- **Antena odbiorcza:** Odbiera sygnały z Ziemi.
- **Wzmacniacz nisko-szumowy (LNA):** Wzmacnia słabe sygnały, aby zredukować szumy i zwiększyć ich moc.
- **Przetwornik częstotliwościowy (i lokalny oscylator):** Konwertuje częstość odbieranego sygnału na inną częstość, wymagającą do nadawania.
- **Filtr przejściowy (BPF):** Odrzuca niepożądane częstotliwości, pozwalając tylko na przejście oczekiwanego sygnału.
- **Przed wzmacniacz radiowy:** Dalsze zwiększanie mocy sygnału przed jego nadawaniem.
- **Wzmacniacz radiowy wysokiej mocy (HPA):** Ostatecznie wzmacnia sygnał do poziomu, który może być skutecznie retransmitowany z powrotem na Ziemię.
- **Antena nadawcza:** Emisja sygnału w kierunku stacji odbiorczej na Ziemi.

Pasma satelitarne i zależność dostępności usług

Pasma częstotliwości wykorzystywane w łączności satelitarnej determinują nie tylko charakter oferowanych usług, ale także ich dostępność geograficzną, odporność na zakłócenia atmosferyczne oraz wymogi regulacyjne. Poniżej przedstawiono najważniejsze pasma, ich typowe zastosowania oraz

czynniki wpływające na dostępność usług w poszczególnych regionach.

Pasmo L (1-2 GHz)

- **Zastosowania**: systemy nawigacji satelitarnej (GPS, GLONASS, Galileo), łączność mobilna w warunkach niskiego SNR, niektóre systemy telemetrii.
- **Zalety**: duża odporność na opady atmosferyczne (deszcz, śnieg) oraz zakłócenia jonosferyczne; stosunkowo niewielka utrata mocy sygnału przy długich odległościach.
- **Ograniczenia**: ograniczona przepustowość w porównaniu z wyższymi pasmami; konieczność stosowania większych anten w celu uzyskania wysokiego zysku.
- **Dostępność**: szeroko dostępne globalnie, ponieważ pasmo L jest przydzielone do usług publicznych i nie wymaga kosztownych licencji.

Pasmo S (2-4GHz)

- **Zastosowania**: radary pogodowe, monitorowanie atmosfery, niektóre systemy łączności awaryjnej, satelity obserwacyjne.
- **Zalety**: umiarkowana wrażliwość na opady; możliwość uzyskania średniej przepustowości przy relatywnie niewielkich antenach.
- **Ograniczenia**: pasmo jest częściowo zajęte przez systemy wojskowe i naukowe, co może ograniczać dostępność w niektórych krajach.
- **Dostępność**: dostępne w większości regionów, ale wymaga koordynacji z organami regulacyjnymi w celu uniknięcia interferencji.

Pasmo C (4-8 GHz)

- **Zastosowania**: telewizja satelitarna (DTH), transmisje danych w sieciach korporacyjnych, łącza back-haul.
- **Zalety**: dobre pokrycie geograficzne przy umiarkowanej wielkości anten; stosunkowo niska podatność na deszcz w porównaniu z wyższymi pasmami.
- **Ograniczenia**: wymaga większych anten niż pasma Ku/Ka; pasmo jest silnie zagospodarowane, co może prowadzić do zatłoczenia spektrum.
- **Dostępność**: szeroko wykorzystywane w Europie i Ameryce Północnej; w niektórych regionach Azji i Afryki dostępność może być ograniczona ze względu na przydziały narodowe.

Pasmo X (8-12 GHz)

- **Zastosowania**: komunikacja wojskowa, radary śledzące, łącza satelitarne w trudnych warunkach atmosferycznych.
- **Zalety**: wysoka precyzja i możliwość uzyskania dużej przepustowości; lepsza odporność na zakłócenia jonosferyczne niż niższe pasma.
- **Ograniczenia**: silna absorpcja przy intensywnych opadach deszczu (tzw. *rain fade*); wymaga precyzyjnego ukierunkowania anten.
- **Dostępność**: ograniczona do użytkowników posiadających odpowiednie licencje wojskowe lub rządowe; w niektórych krajach dostępna jedynie w ramach programów badawczych.

Pasmo Ku (12-18GHz)

- **Zastosowania**: transpondery telewizyjne, szerokopasmowy Internet satelitarny, łącza VSAT.
- **Zalety**: stosunkowo wysoka przepustowość przy umiarkowanej wielkości anten; dobra równowaga między zasięgiem a podatnością na *rain fade*.
- **Ograniczenia**: wymaga precyzyjnego ustawienia anteny; w rejonach o intensywnych opadach deszczu jakość usługi może się obniżać.
- **Dostępność**: szeroko dostępne w Europie, Ameryce Północnej i części Azji; w niektórych regionach wymaga uzyskania licencji od lokalnych regulatorów.

Pasmo Ka (26,5-40GHz)

- **Zastosowania**: wysokoprzepustowe łącza satelitarne, 5G back-haul, transmisje wideo w jakości 4K/8K, systemy IoT o dużej przepustowości.
- **Zalety**: bardzo duża przepustowość, umożliwiająca transmisję gigabitowych strumieni danych; małe anteny ze względu na krótszą długość fali.
- **Ograniczenia**: silna podatność na *rain fade* i inne zjawiska atmosferyczne; wymaga zaawansowanych technik korekcji błędów i adaptacyjnego przydziału mocy.
- **Dostępność**: rośnie w miarę wprowadzania nowych regulacji; w niektórych krajach dostępne dopiero w ramach pilotowych projektów.

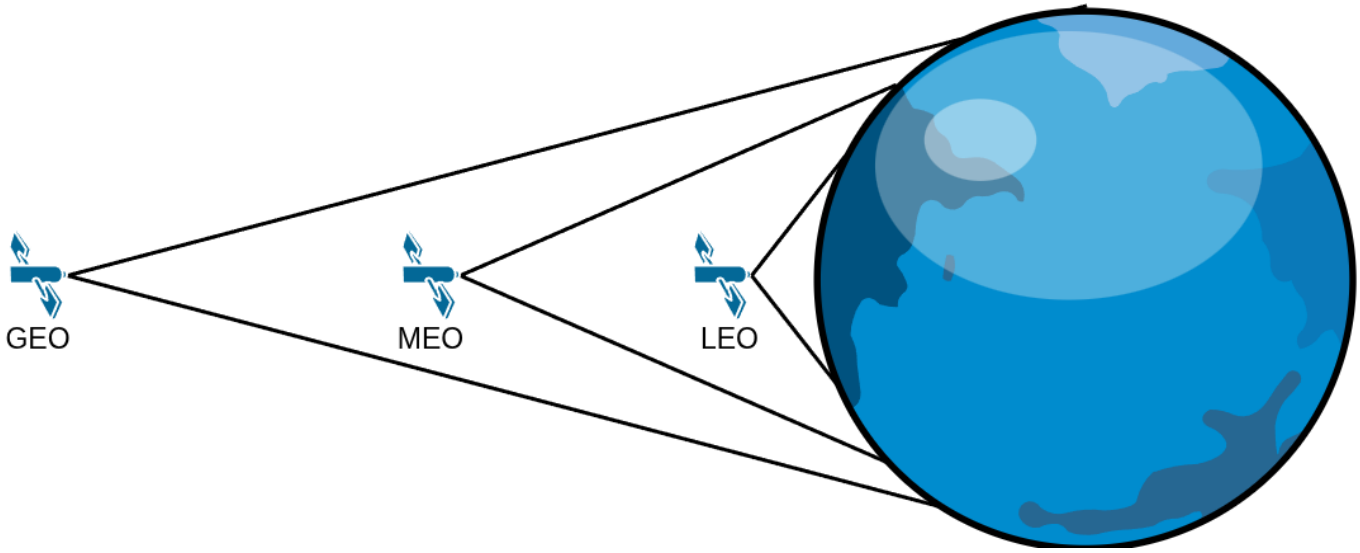
Pasmo V (40-75 GHz)

- **Zastosowania**: eksperymentalne systemy łączności satelitarnej, badania nad transmisją danych w bardzo wysokich częstotliwościach, prototypy sieci satelitarnych dla 6G.
- **Zalety**: ekstremalnie duża przepustowość (kilkadziesiąt gigabitów na sekundę); możliwość wykorzystania bardzo małych anten i układów elektronicznych.
- **Ograniczenia**: bardzo silna absorpcja przez atmosferę (głównie woda i tlen); wymaga precyzyjnego sterowania wiązką oraz zaawansowanych technik modulacji.
- **Dostępność**: obecnie ograniczona do laboratoriów badawczych i projektów demonstracyjnych; regulacje dopuszczające komercyjne wykorzystanie dopiero w fazie opracowywania.

Podsumowanie zależności dostępności usług

- **Czynniki geograficzne**: w regionach o wysokich opadach (np. tropikalne) pasma wyższe (Ku, Ka, V) mogą wymagać dodatkowych technik mitigacji *rain fade*, co podnosi koszty wdrożenia.
- **Regulacje i licencje**: niektóre pasma (X, V) są zarezerwowane dla zastosowań wojskowych lub badawczych, co ogranicza ich dostępność dla sektora komercyjnego.
- **Wymagania przepustowości**: aplikacje wymagające dużej przepustowości (np. transmisje wideo 4K, back-haul 5G) skłaniają się ku pasmom Ka i Ku, natomiast systemy o krytycznym znaczeniu i niskiej przepustowości (np. nawigacja) korzystają z pasma L.
- **Koszty infrastruktury**: niższe częstotliwości (L, S) wymagają większych anten, co zwiększa koszty instalacji, podczas gdy wyższe częstotliwości (Ka, V) pozwalają na mniejsze anteny, ale zwiększają koszty związane z korekcją zakłóceń.

Rodzaje sztucznych satelit ziemskich



Schemat ideowy orbit satelit komunikacyjnych [Opracowanie własne]

LEO (Low Earth Orbit)

Satelity na niskiej orbicie (160-2000 km) charakteryzują się:

- **Niskim opóźnieniem** (20–40ms) – korzystne dla aplikacji czasu rzeczywistego (VoIP, aplikacje online, telekonferencje).
- **Wysoką rozdzielczością obrazów** – umożliwiają szczegółowe obserwacje Ziemi, monitorowanie zmian środowiskowych.
- **Krótkim okresem orbitalnym** (90–120min) – wymaga dużej liczby satelit w konstelacji, aby zapewnić ciągłość pokrycia.

Typowe zastosowania: konstelacje broadbandowe (Starlink, OneWeb), systemy obserwacji Ziemi (Sentinel-2, Landsat), misje badawcze i edukacyjne.

MEO (Medium Earth Orbit)

Orbita średnia (2000–35786km) jest wykorzystywana głównie przez systemy nawigacyjne:

- **Stała wysokość około 20200km** – optymalny kompromis między zasięgiem a opóźnieniem (ok. 70ms).
- **Stała liczba satelit** (np. 24 w GPS) zapewnia globalne pokrycie przy umiarkowanej liczbie jednostek.
- **Stabilność orbitalna** – mniejsze wpływy atmosferyczne niż w LEO, co zmniejsza potrzebę korekt orbitalnych.

Przykłady: GPS, GLONASS, Galileo, BeiDou.

GEO (Geostationary Orbit)

Satellity geostacjonarne (35786km) poruszają się z prędkością kątową równą rotacji Ziemi, co daje:

- **Stałą pozycję względem powierzchni** – jedna antena naziemna może obsługiwać cały obszar widoczny z jednego punktu.
- **Duży zasięg** – pojedynczy satelita pokrywa ok. $\frac{1}{3}$ powierzchni Ziemi.
- **Wyższe opóźnienie** (ok. 250ms) – mniej korzystne dla aplikacji wymagających niskiego RTT, ale akceptowalne dla transmisji wideo i telekomunikacji.

Zastosowania: transmisje telewizyjne, szerokopasmowy Internet satelitarny, meteorologia, łączność awaryjna.

Wnioski projektowe

Wybór orbity powinien być uzależniony od wymagań aplikacji:

niskie opóźnienie → LEO;

globalna dostępność przy minimalnej liczbie satelit → MEO;

szeroki zasięg przy jednej jednostce → GEO.

Koszty uruchomienia i eksploatacji rosną wraz z wysokością orbity (większe wymagania napędowe, dłuższy czas życia satelity, droższe systemy napędowe).

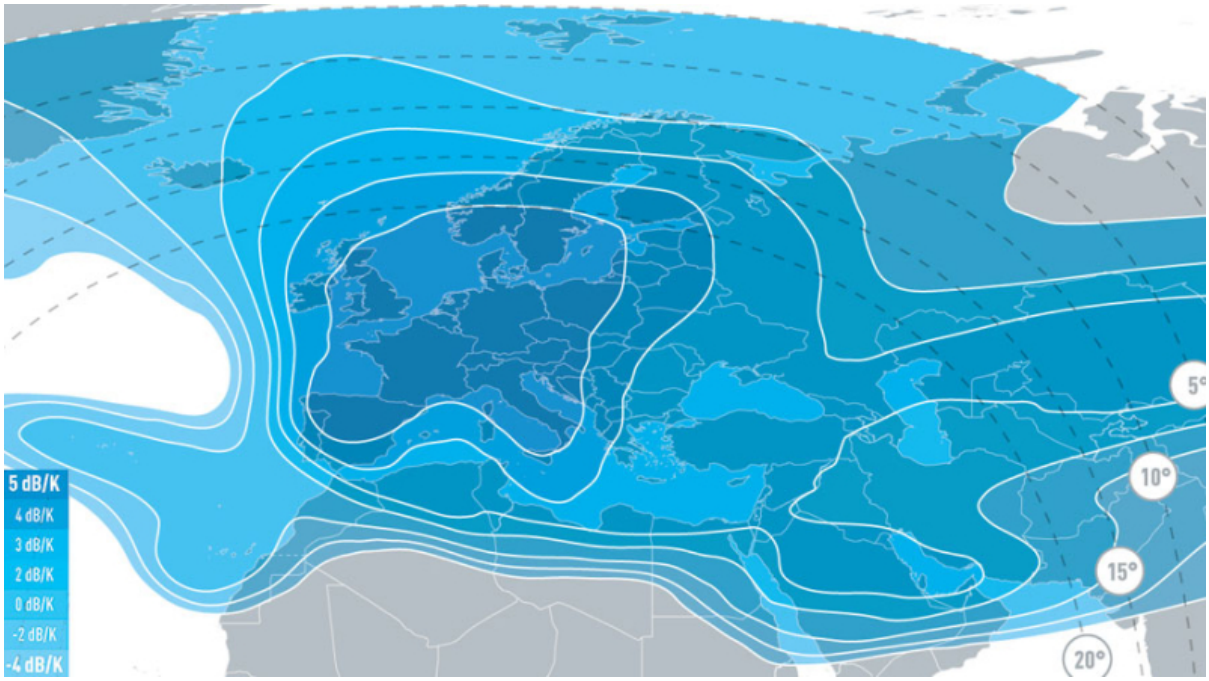
Zarządzanie interferencjami wymaga uwzględnienia przydziału pasm oraz współpracy międzynarodowej, szczególnie w pasmach Ku/Ka, które są intensywnie wykorzystywane.

Redundancja i niezawodność – konstelacje LEO i HEO zapewniają naturalną redundancję dzięki dużej liczbie satelit; w GEO redundancja wymaga uruchomienia zapasowych satelit w tej samej pozycji orbitalnej.

Pokrycie planety przez sygnał satelitarny

Sygnał satelitarny pokrywa obszary planety za pomocą różnych metod transmisji, co pozwala na dostarczanie usług telekomunikacyjnych i danych na dużą skalę.

Mapa odbiorcza: Przedstawia zasięg, w jakim sygnał z satelity może być odbierany na powierzchni Ziemi. W przypadku Eutelssatelliteat 7B, sygnał pokrrackywa znaczną część Europy, Bliskiego Wschodu oraz części Afryki.



Mapa nadawcza (z ziemi) satelity Eutelsat 7B
Źródło: https://www.eutelsat.com/satellite-network/GEO-fleet/eutelsat-7-east

Mapa nadawcza: Ukazuje zasięg obszarów, z których sygnał może być wysyłany do satelity. W przypadku Eutelsat 7B, użytkownicy muszą znajdować się w odpowiednich strefach, aby skutecznie korzystać z usług nadawczych.

Pokrycie sygnałem satelitarnym jest kluczowe dla zapewnienia szerokopasmowego dostępu do internetu, transmisji telewizyjnej oraz komunikacji w trudno dostępnych regionach, gdzie infrastruktura lądowa nie jest rozwinięta.

Technologie satelitarne wykorzystane w

pracy

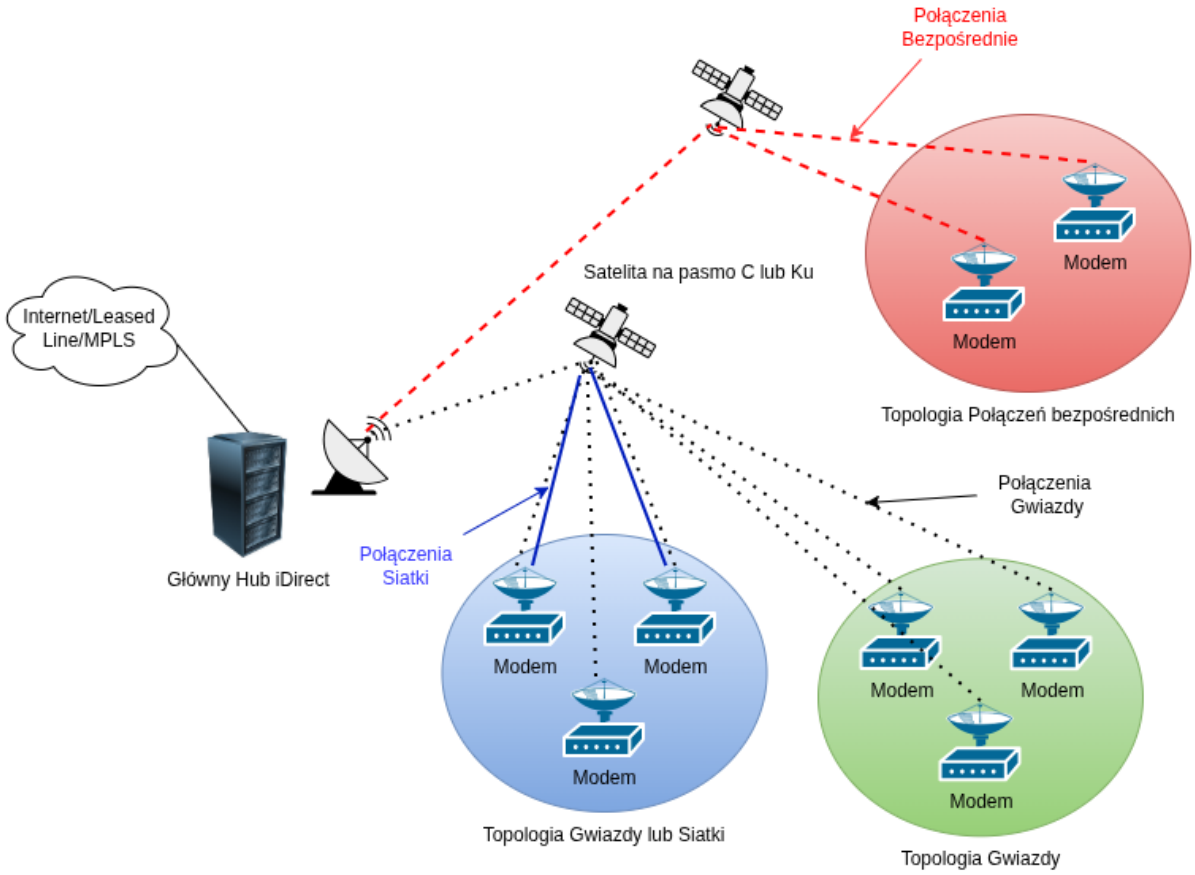
W poniższej sekcji omówimy technologie satelitarne, które są kluczowe dla budowy sieci obsługującej terminale satelitarne. Takie sieci odgrywają istotną rolę w transmisji danych IP, co czyni je niezbędnymi w sytuacjach, gdy tradycyjne łącza, takie jak przewodowe połączenia internetowe, są niedostępne.

Sieci satelitarne są niezwykle cenne w obszarach, gdzie infrastruktura telekomunikacyjna jest ograniczona. Przykładem mogą być lokalizacje wiejskie lub odległe tereny, w których brak jest dostępu do kabli światłowodowych lub łączy radiowych, takich jak sieci komórkowe 4G/LTE. W takich przypadkach, technologie satelitarne oferują elastyczne rozwiązania, które umożliwiają użytkownikom uzyskanie stabilnego i szybkiego dostępu do internetu.

Satelitarna łączność geostacjonarna

Z racji popularności i łatwości implementacji w pracy została zastosowana łączność geostacjonarna, ponieważ orbita GEO zapewnia stałą pozycję satelity względem punktu naziemnego, co eliminuje konieczność skomplikowanego śledzenia anteną i znacząco upraszcza konfigurację sieci w warunkach polowych. Symulacje oraz wszystkie powiązane konfiguracje zostały opracowane z myślą o paśmie Ku, które jest najczęściej wykorzystywanym pasmem do transmisji danych IP w sieciach satelitarnych ze względu na korzystny stosunek przepustowości do podatności na zjawisko *rain fade*. Pasmo Ku (12–18GHz) oferuje wystarczającą szerokość pasma, aby obsłużyć protokoły transportowe (TCP/UDP) oraz techniki adaptacyjnego kodowania i modulacji (ACM), co pozwala na dynamiczne dostosowywanie parametrów transmisji do aktualnych warunków atmosferycznych. Dodatkowo, pasmo to jest szeroko wspierane przez liczne platformy satelitarne, w tym rozwiązania iDirect, które dostarczają gotowe terminale, oprogramowanie zarządzające pasmem oraz narzędzia diagnostyczne, co znacząco skraca czas wdrożenia i redukuje koszty operacyjne. Dzięki temu połączenie GEO-Ku stanowi optymalne rozwiązanie zarówno dla łączności zapasowej, jak i jako główne łącze internetowe w lokalizacjach pozbawionych dostępnych łączy przewodowych lub radiowych (np. 4G/LTE).

Platforma iDirect



Schemat sieci satelitarnej na bazie platformy iDirect [Opracowanie własne]

W realizacji projektu sieci wykorzystano platformę satelitarną iDirect. W poniższym porównaniu wykorzystano pojęcie przeskoku satelitarnego. Przeskok satelitarny to przesłanie sygnału z miejsca nadawania i następnie odebranie go w miejscu odbioru, w poniższym porównaniu wykorzystano pojęcie pojedynczego skoku oraz podwójnego skoku. Poniżej wyjaśnienie tych pojęć. *Pojedynczy skok satelitarny* następuje w momencie w którym, nadawany sygnał jest przetwarzany tylko raz przez satelitę. Czyli na przykład w sytuacji w której dwa terminale komunikują się razem poprzez pasmo satelitarne. Sygnał jest najpierw nadawany przez jeden terminal potem odbierany przez drugi. *Podwójny skok satelitarny* następuje w momencie w którym sygnał jest przetwarzany przez satelitę podwójnie. Kiedy np. terminal chce dostać się do internetu i musi przejść przez punkt główny czyli huba. Terminal wykonuje polecenie `ping 8.8.8.8`, pakiet najpierw jest przesyłany do huba, hub następnie rozkodowuje pakiet satelitarny i przesyła go na adres docelowy `8.8.8.8`, czeka na odpowiedź `ECHO REPLY` w momencie otrzymania odpowiedzi, zakodowuje ją w pakiet satelitarny, wysyła na satelitę i następnie terminal go otrzymuje. W taki sposób zachodzi tzw. podwójny skok. Platforma iDirect pozwala na realizację sieci satelitarnych w poniższych trybach konfiguracji:

- Topologia gwiazdy lub siatki
  - Pozwala na połączenie każdego terminala z każdym (po podwójnym przeskoku)
  - Dodatkowo pozwala na definiowanie połączeń między terminalami (po pojedynczym przeskoku)
- Topologia gwiazdy
  - Pozwala na połączenie każdego terminala z każdym (po podwójnym przeskoku)
  - Nie pozwala na połączenia siatkowe między terminalami (bez podwójnego

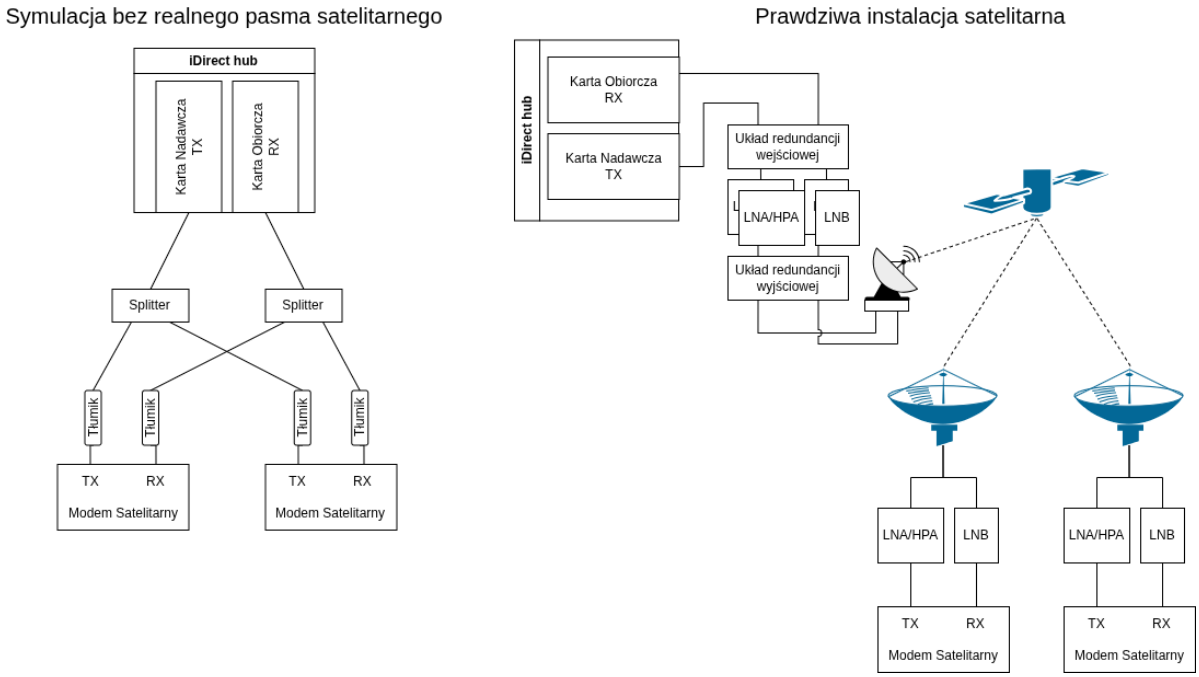
skoku)

- Topologia połączeń bezpośrednich
  - Pozwala tylko i wyłącznie na połączenia bezpośrednie między dwoma lub więcej terminalami satelitarnymi na dedykowanym, przeznaczonym tylko i wyłącznie do tego paśmie tzw. jeden kanał na nośną (eng. SCPC single channel per carrier)

W tej pracy sieć oraz platforma satelitarna były skonfigurowane pod działanie sieci w trybie „Topologia gwiazdy”. Konsekwencją tego jest to że cały ruch sieciowy jaki zachodzi, między terminalami albo do internetu musi przejść przez punkt centralny (tzw. hub).

Wykorzystanie pętli TX-RX do symulacji łącza satelitarnego

Podczas testów przed uruchomieniem sieci satelitarnej, trzeba przeprowadzić testy funkcjonalne. Z racji tego że pasmo satelitarne jest usługą o wysokiej cenie, powoduje to szukanie i opracowywanie rozwiązań które pozwalają przetestować działanie sieci bez pasma satelitarnego. Na rysunku 8 możemy zaobserwować, porównanie tego jakie są najważniejsze komponenty prawdziwej sieci satelitarnej, oraz jak możemy to uprościć w celu przetestowania sieci bez pasma satelitarnego.



Schemat symulacji pętli TXRX oraz porównanie z realną instalacją [Opracowanie własne]

Sieć satelitarna podczas zastosowania prawdziwego pasma satelitarnego wymaga od nas zastosowania pełnych traktów odbiorczych i nadawczych dla strony terminala jak i również huba. Trakt nadawczy powinien być również redundantny, więc potrzebujemy zastosować podwójnie sprzęt nadawczy i odbiorczy po stronie huba.

Natomiast przy testach funkcjonalnych wystarczy zastosować dzielniki do których możemy podłączyć stronę nadawczą i odbiorczą terminali, i po uprzednim stłumieniu sygnału do odpowiedniego poziomu, możemy tak przygotowane sygnały podłączyć do

terminali. Pozwoli to na podłączenie i uwierzytelnienie się w sieci satelitarnej bez uprzedniego wynajmowania pasma satelitarnego.

Testy wykonane w taki sposób nie pozwalają na zbadanie opóźnienia i ograniczeń pasma wynikających z pasma satelitarnego. Dlatego w następnym rozdziale przedstawiono metodę badania i symulacji takich warunków za pomocą otwarto źródłowego oprogramowania.

Wykorzystanie narzędzia TC do symulacji charakterystyki łącza satelitarnego

Pasmo satelitarne jest usługą która jest stosunkowo droga. Powoduje to że w niektórych analizach może być potrzebne symulowanie warunków takiej sieci. W poprzednich sekcjach przedstawiono jak za-symulować sieć satelitarną na platformie satelitarnej, natomiast takie symulacje nie mają odpowiedniego ograniczenia pasma, ani również opóźnienia. Tutaj natomiast skupiamy się na symulacji opóźnień oraz ograniczeń pasma.

Narzędzie Traffic Control

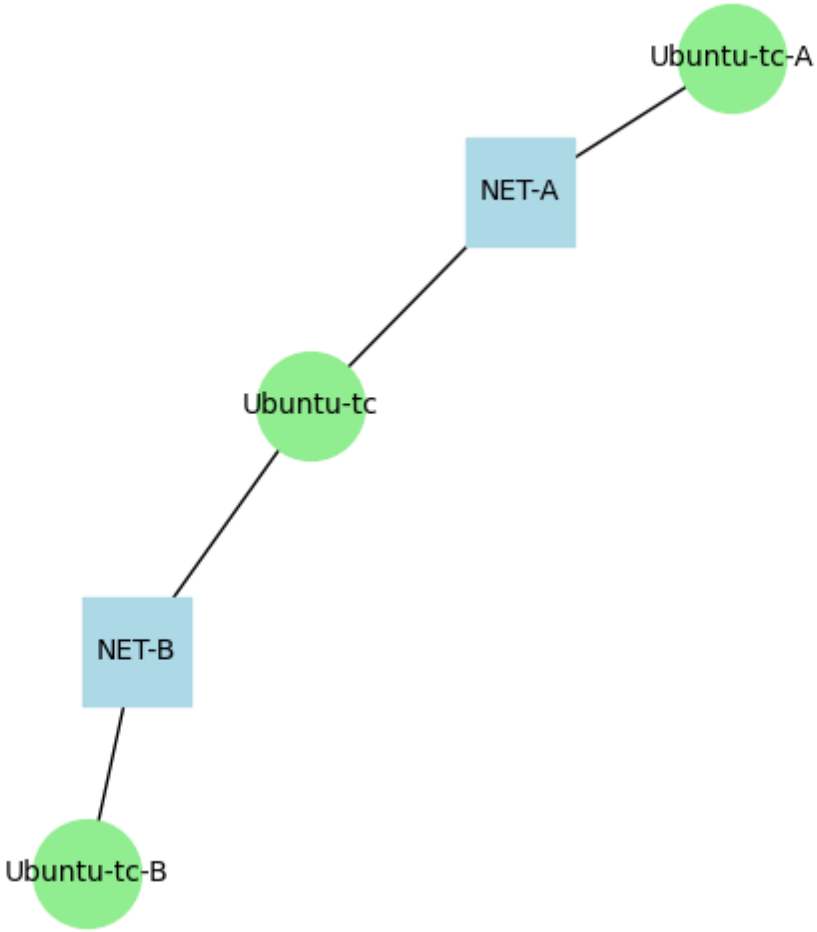
Narzędzie Traffic Control (TC) w systemie Linux jest kluczowe w zarządzaniu ruchem sieciowym, pozwalając na emulację różnych warunków sieciowych, takich jak opóźnienia czy ograniczenia pasma. Dzięki TC można precyzyjnie kontrolować, jak dane przepływają przez sieć, co jest niezbędne do skutecznej symulacji zachowań łącza satelitarnego.

Wymagania funkcjonalne środowiska testowego

Środowisko którego implementację przedstawiono w tej sekcji powinno skutecznie symulować warunki sieciowe zgodnie z zadanymi parametrami. Środowisko powinno być zdolne do zachowania zadanych parametrów. Jeżeli ustawione parametry to np. opóźnienie 100ms, ograniczenie pasma 20Mbps oraz starty 1%, to środowisko powinno zachować te parametry i pozostać w tym samym rzędzie wielkości żeby pomiar oraz zastosowanie symulacji miały sens implementacji.

Konfiguracja środowiska testowego

Aby przeprowadzić symulację, konieczne było skonfigurowanie odpowiedniego środowiska testowego. Na poniższej ilustracji przedstawiono schemat maszyn wirtualnych, które zostały użyte do symulacji.



Schemat maszyn wirtualnych zastosowanych do symulacji [Opracowanie własne]

Tabela konfiguracji sieci [Opracowanie własne]

Nazwa maszyny	Interfejs	Adres IP	Brama	Sieć
ubuntu-tc	eth0	192.168.1.1/24	X	NET-A
ubuntu-tc	eth1	192.168.2.1/24	X	NET-B
ubuntu-tc-A	eth0	192.168.1.10/24	192.168.1.1/24	NET-A
ubuntu-tc-B	eth0	192.168.2.10/24	192.168.2.1/24	NET-B

W konfiguracji sieci opisanej w Tabeli 1 użyto maszyn z wieloma interfejsami, co pozwoliło na testowanie różnych scenariuszy.

Konfiguracja maszyny Ubuntu-tc

Na maszynie głównej (ubuntu-tc) włączono forwarding dla IPv4, co pozwoliło na przesyłanie ruchu między interfejsami. Poniżej przedstawiono polecenia umożliwiające aktywację tej funkcji:

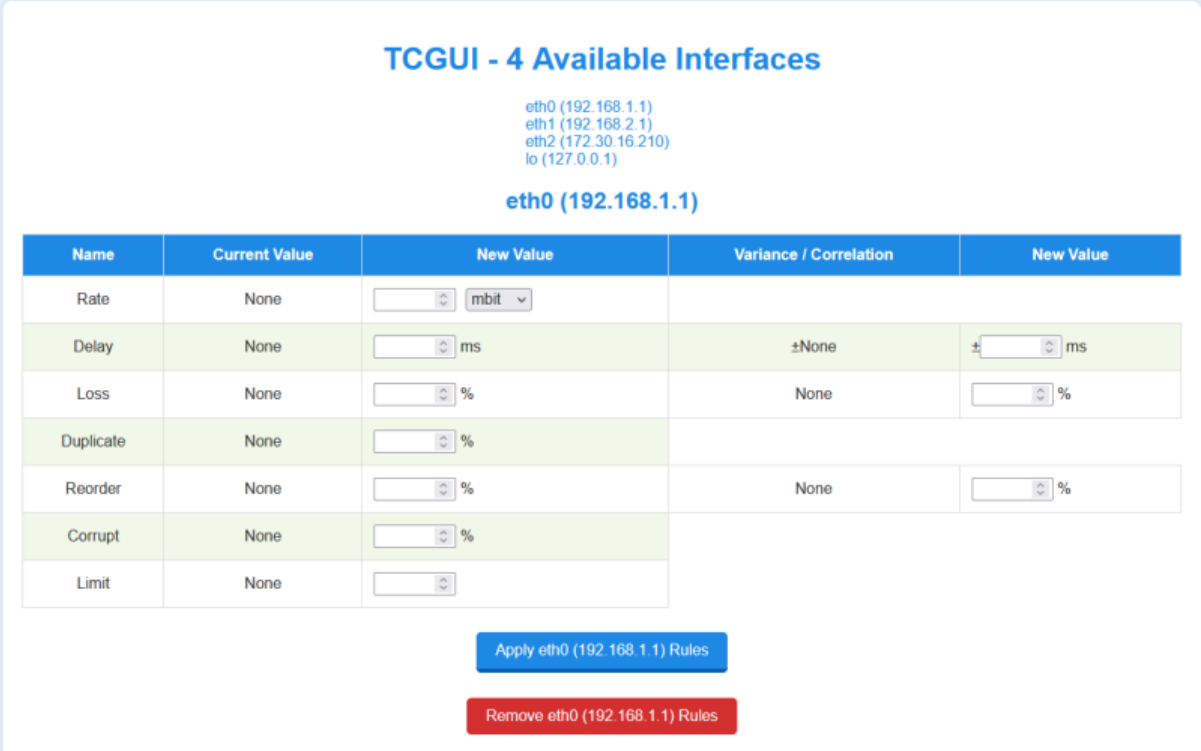
```
echo "net.ipv4.ip_forward=1" | sudo tee -a /etc/sysctl.conf
```

Następnie należało zrestartować interfejsy sieciowe, a także skopiować i uruchomić

narzędzie TC GUI (narzędzie autorstwa użytkownika TUM-LKN publikowane na licencji MIT):

```
sudo apt install git
    git clone https://github.com/tum-lkn/tcgui
    cd tcgui
    sudo python3 main.py --ip 127.0.0.1
```

W przeglądarce możemy otworzyć narzędzie do konfiguracji TC poprzez interfejs webowy pod url http://127.0.0.1:5000.



Interfejs webowy do sterowania narzędziem TC

Ustawienia na reszcie maszyn

Inne maszyny musiały zostać przygotowane poprzez zainstalowanie iperf3, co można zrealizować za pomocą następującego polecenia:

```
sudo apt-get update
    sudo apt-get install iperf3
```

Musimy je jeszcze zaadresować statycznie za pomocą GUI albo za pomocą netplan

Analiza wyników

Testy rozwiązania mają na celu sprawdzenie na ile miarodajne jest narzędzie TC do symulacji parametrów sieci satelitarnych. Przy rozpatrywaniu wyników pomiarów brano pod uwagę ustawione parametry do parametrów zmierzonych. Jeżeli wyniki są

odbiegająca od siebie to znaczy że narzędzie TC nie jest w stanie symulować zmian tego parametru sieciowego.

Wyniki pomiarów

W poniższej tabeli przedstawiono opis parametrów ustawionych w interfejsie `tc-gui` oraz realny pomiar w kolumnie obok.

Wyniki testów opóźnień, pasma UDP i TCP, oraz inne testy [Opracowanie własne]

Opis ograniczeń	**Protokół**	**Straty**	**Pasmo**	**Opóźnienie [ms]**
Testy opóźnień				
Test bez dodanego opóźnienia	ICMP	0%	—	1,131
Test z dodanym opóźnieniem 10ms wynik z 100 pomiarów	ICMP	0%	—	11,020
Test z dodanym opóźnieniem 100ms wynik z 100 pomiarów	ICMP	0%	—	101,071
Test z dodanym opóźnieniem 1000ms wynik z 100 pomiarów	ICMP	0%	—	1000,911
Testy pasma UDP				
Test bez ograniczenia 30s (UDP 1Gbps iperf)	UDP	—	998 Mbps	—
Ograniczenie pasma do 300Mbps 30s (UDP iperf)	UDP	72%	282 Mbps	—
Ograniczenie pasma do 100Mbps 30s (UDP iperf)	UDP	91%	94,3 Mbps	—
Ograniczenie pasma do 10Mbps 30s (UDP iperf)	UDP	99%	9,72 Mbps	—
Ograniczenie pasma do 1Mbps 30s (UDP iperf)	UDP	100%	972 kbps	—
Testy pasma TCP				
Test bez ograniczenia 30s (TCP iperf)	TCP	2	10,3 Gbps	—
Ograniczenie pasma do 300Mbps 30s (TCP iperf)	TCP	0	282 Mbps	—
Ograniczenie pasma do 100Mbps 30s (TCP iperf)	TCP	0	94,3 Mbps	—
Ograniczenie pasma do 10Mbps 30s (TCP iperf)	TCP	152	9,72 Mbps	—
Ograniczenie pasma do 1Mbps 30s (TCP iperf)	TCP	0	972 kbps	—
Testy w obie strony tzw. zapętlone, oraz z wieloma parametrami ograniczeń				
10Mbps, opóźnienie 2000ms, utrata 3%, uszkodzone 10%	ICMP	24%	—	4001,69
10Mbps, opóźnienie 600ms, utrata 3%, uszkodzone 10% (TCP iperf)	TCP	23	82 kbps	—
10Mbps, opóźnienie 600ms, utrata 3%, uszkodzone 10% (UDP iperf)	UDP	99%	7,79 kbps	—

Opis ograniczeń	Protokół	Straty	Pasmo	Opóźnienie [ms]
60Mbps, opóźnienie 600ms, utrata 5% (UDP iperf)	UDP	98%	14,7 Mbps	—

Analiza wyników symulacji

Analizując wyniki testów przeprowadzonych w ramach symulacji, można zauważyć, że narzędzie Traffic Control (TC) wykazuje dużą lecz nie idealną precyzję w realizacji ustawionych parametrów. Oto kluczowe wnioski dotyczące jego dokładności i efektywności:

- *Dokładność ustawień pasma:* TC z powodzeniem ograniczało pasmo do zadanych wartości, co potwierdzają wyniki testów. Obserwowane wartości pasma były zbliżone do tych, które zostały skonfigurowane, co świadczy o efektywności narzędzia w zarządzaniu przesyłem danych.
- *Emulacja opóźnień:* Narzędzie TC precyzyjnie odwzorowuje dodane opóźnienia, które miały miejsce w rzeczywistych warunkach. Ustawione opóźnienia odpowiadały uzyskanym wartościom, co potwierdza jego zdolność do symulacji rzeczywistych warunków sieciowych.
- *Straty pakietów:* TC pozwoliło na kontrolowanie strat pakietów w różnych scenariuszach. Wyniki pokazują, że narzędzie skutecznie różnicowało sytuacje, w których występowały straty, co jest kluczowe dla analizy jakości łącza.
- *Wydajność pod dużym obciążeniem:* Pomimo dodanych ograniczeń pasma i opóźnień, TC nie potrafiło utrzymać względnie stabilnej wydajności, jeżeli chodzi o symulacje wymagające większej ilości parametrów. Co powoduje że lepiej symulować opóźnienie ale bez jednoczesnego symulowania ograniczeń w transmisji.
- *Praktyczne zastosowanie:* Zważywszy na osiągnięte wyniki, narzędzie TC ujawnia swój potencjał w symulacji sieci o wysokim opóźnieniu i małej przepustowości, jednak nie przy jednoczesnym symulowania obydwu parametrów jednocześnie, zwłaszcza w kontekście platform satelitarnych, gdzie pasmo oraz opóznienie mają konkretne wartości.

Podsumowując, Traffic Control (TC) okazało się skutecznym narzędziem do emulacji i symulowaniem parametrami sieciowymi, z wysoką dokładnością w dostosowywaniu się do zadanych wartości. Jednak nie pozwala na jednoczesną miarodajną symulację ograniczenia pasma oraz opóźnienia. Jego wykorzystanie w analizach i symulacjach sieci satelitarnych może pozwolić na testy rozwiązań i ich odporności na starty pakietów, ograniczenia pasma lub opóźnienie.

Technologie sieciowe wykorzystane w pracy

W tej sekcji przedstawione zostaną kluczowe technologie sieciowe, które zostały wykorzystane w niniejszej pracy. Omówione zostaną zarówno urządzenia, jak i protokoły, które pozwalają na efektywne zarządzanie sieciami.

Urządzenia MikroTik – charakterystyka i zastosowanie

Urządzenia MikroTik to popularne rozwiązanie w zakresie sprzętu sieciowego, oferujące elastyczność i rozmaite możliwości konfiguracji. Charakteryzują się intuicyjnym interfejsem, co sprawia, że są idealne zarówno dla małych, jak i dużych sieci. MikroTik stosuje system RouterOS, który umożliwia zarządzanie ruchami, QoS, VPN oraz innymi funkcjami związanymi z bezpieczeństwem.

Protokół VRRP – zasada działania i implementacja

Protokół VRRP (Virtual Router Redundancy Protocol) służy do zwiększenia dostępności bramy sieciowej. W ramach VRRP kilka routerów współpracuje, aby zapewnić, że jeden z nich działa jako „wirtualny router”. Dzięki temu, w przypadku awarii jednego z routerów, pozostałe mogą przejąć odpowiedzialność, co minimalizuje przestoje sieci.

Protokół RIP – mechanizmy routingu dynamicznego

Protokół RIP (Routing Information Protocol) to jeden z najstarszych protokołów routingu dynamicznego, wykorzystujący algorytm wektora odległości. RIP umożliwia routerom wymianę informacji o trasach w sieci, co pozwala na dynamiczne dostosowanie tras w odpowiedzi na zmiany w topologii. Chociaż prosty w implementacji, jego zastosowanie jest ograniczone w dużych sieciach ze względu na maksymalną liczbę 15 przeskoków.

Co ważne, protokół RIP jest szczególnie wymagany do działania platform satelitarnych, ponieważ wciąż jest szeroko wykorzystywany w tych systemach.

Redundancja i przełączanie awaryjne w sieciach IP

Redundancja i przełączanie awaryjne są kluczowymi elementami w projektowaniu niezawodnych sieci IP. Poprzez zastosowanie VRRP, sieci mogą zapewnić ciągłość działania nawet w przypadku awarii komponentów. Właściwe planowanie i implementacja tych technologii są niezbędne dla utrzymania stabilności i dostępności usług sieciowych.

Projekt sieci komputerowej do obsługi łączności satelitarnej

Wymagania

Wymagania funkcjonalne

- **Dekodowanie protokołów własnościowych iDirect** – serwery PP muszą odbierać sygnał satelitarny, rozkodowywać go do pakietów IP i przekazywać dalej w sieci IP.
- **Dynamiczna wymiana informacji o trasach** – protokół RIP musi być uruchomiony na routerach brzegowych oraz na serwerach PP, aby automatycznie propagować informacje o sieciach tunelowych i lokalnych sieciach klientów.
- **Obsługa dwóch odrębnych domen adresowych** – sieć musi być podzielona na VLAN UPSTREAM (przetworzone dane IP) i VLAN TUNNEL (surowe dane satelitarne) przy użyciu przełącznika warstwy drugiej.
- **Redundancja kluczowych elementów** – routery brzegowe muszą pracować w trybie aktywno-pasywnym (VRRP) i mieć skonfigurowane dwie ścieżki WAN z publicznymi adresami IP.
- **Zarządzanie i monitorowanie** – serwer NMS musi mieć dostęp do bazy danych konfiguracji iDirect oraz zapewniać interfejs do zdalnego monitoringu i aktualizacji konfiguracji.
- **Obsługa wielu terminali satelitarnych** – każdy terminal satelitarny (modem) musi być w stanie zarejestrować swoją sieć lokalną (np. `172.16.32.0/24`) i przekazać tę informację serwerowi PP, który rozgłasza ją do routerów brzegowych.
- **Obsługa NAT i translacji adresów** – routery brzegowe muszą wykonywać NAT dla ruchu wychodzącego do Internetu, zachowując jednocześnie możliwość zwrotu ruchu do odpowiednich terminali satelitarnych.

Wymagania niefunkcjonalne

1. **Wysoka dostępność** – projekt musi zapewniać jak nawiększą niezawodność działania dzięki redundancji serwerów PP, NMS oraz routerów (VRRP, podwójne połączenia WAN).
2. **Skalowalność** – architektura powinna umożliwiać dodanie kolejnych serwerów PP i terminali satelitarnych bez konieczności przebudowy istniejącej infrastruktury; każdy nowy serwer PP wymaga jedynie podłączenia dwóch portów do przełącznika.
3. **Wydajność** – przełącznik warstwy drugiej musi obsługiwać co najmniej 1Gbps na każdy port VLAN przy jednoczesnym wsparciu 802.1Q trunkingu.
4. **Zarządzalność** – konfiguracja przełącznika i routerów musi być możliwa poprzez połączenie SSH lub serial do urządzeń.
5. **Kompatybilność sprzętowa** – wszystkie użyte urządzenia (Cisco Catalyst, MikroTik RouterBOARD, serwery PP) muszą wspierać protokół RIP, VLAN 802.1Q oraz VRRP w wersji 3.
6. **Odporność na awarie zasilania** – kluczowe elementy (routery, przełącznik, serwery PP) wyposażone w zasilacze UPS o przynajmniej 30minutowej autonomii. Wymaganie nie omawiane w tej pracy, natomiast zostało zapewnione przez środowisko w którym sieć była implementowana.

Projekt sieci oraz przepływu danych

Platforma iDirect ma stosunkowo specyficzne wymagania co do sieci komputerowej jaka

ma być zastosowana do obsługi ruchu sieciowego wytwarzanego przez terminale satelitarne. Aby przedstawić te wymagania musimy najpierw zapoznać się z najważniejszymi komponentami takiej sieci.

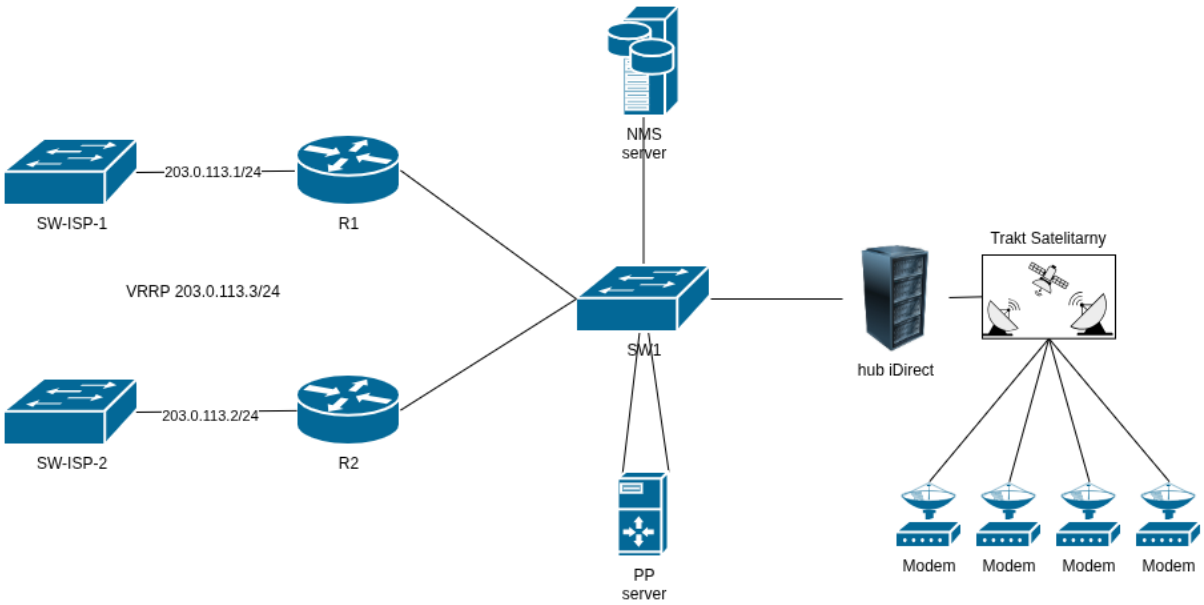
Główne elementy platformy iDirect

Serwer PP (ang. Protocol processor). Platforma satelitarna używa własnościowych protokołów które nie są kompatybilne z sieciami ogólnego przeznaczenia, aby ten ruch sieciowy mógł zostać poprawnie obsłużony przez sieci IP musi być najpierw rozkodowany do postaci pakietów IP, zadanie to należy do serwera PP który jest podłączony do takiej sieci poprzez dwa porty i na jednym z nich otrzymuje dane do rozkodowania i następnie przesyła je na drugi port, do sieci w której mogą te dane być przetworzone przez normalne routery IP. Ilość tych serwerów jest zależna od wielkości sieci.

Serwer NMS (ang. Network managment system). To jest serwer którego nie wpływa na działanie sieci ale jest kluczowym komponentem, zawiera on bazę danych w której przechowywane są informację na temat konfiguracji sieci oraz kart w systemie iDirect. Serwer ten zwykle instaluję się w dwóch egzemplarzach oraz ustawia się na nich replikację bazy danych, w celu zachowania redundancji.

Router krańcowy (ang. Edge). Jest to urządzenie które obsługuje ruch w całej sieci. Platforma iDirect wykorzystuję routing dynamiczny RIP do komunikacji z modemami satelitarnymi oraz wykorzystuje dwie sieci które oddzielają dane przed przetwarzaniem przez serwery PP oraz po przetwarzaniu przez serwery PP. Sieć która zawiera dane przed przetwarzaniem nazywa się „tunnel” a sieć po przetworzeniu danych nazywa się „upstream”.

Rdzeń sieci iDirect



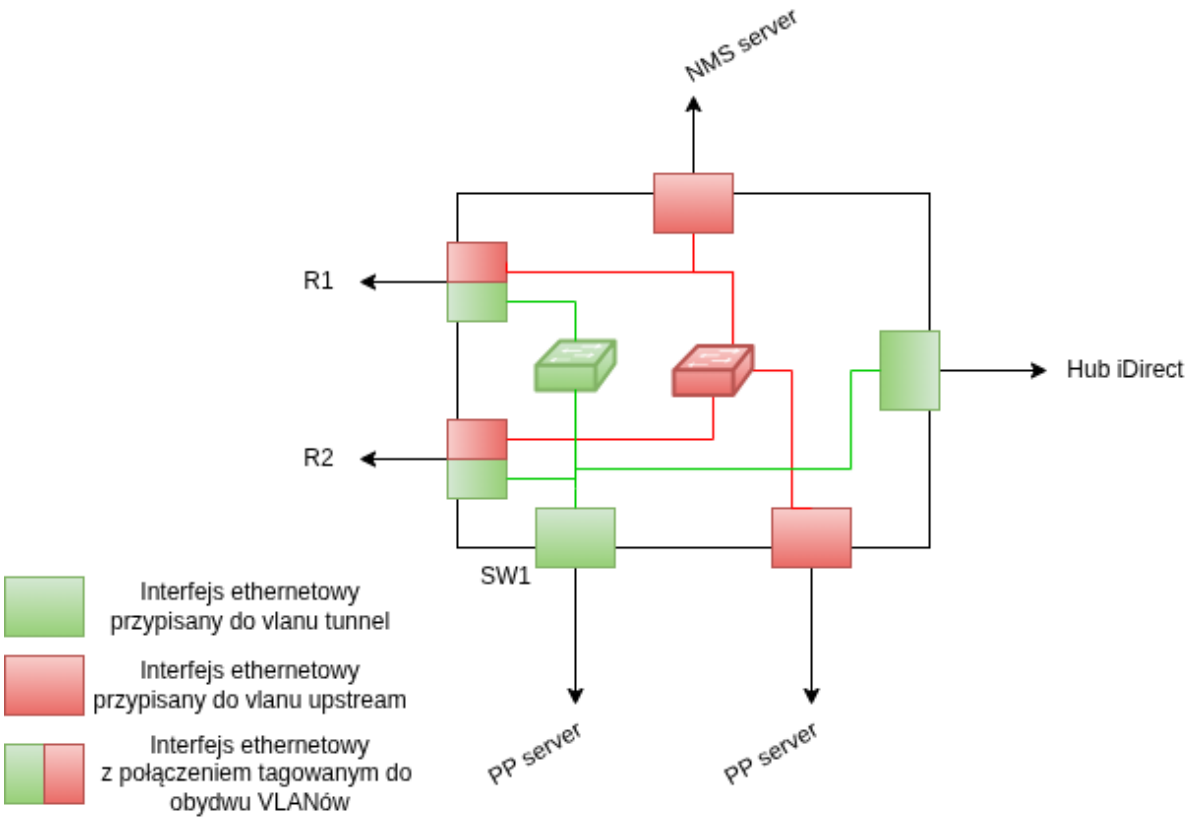
Uproszczony schemat sieci komputerowej do obsługi platformy iDirect [Opracowanie własne]

Na uproszczonym rysunku 11 możemy zaobserwować jak wygląda rdzeń sieci

komputerowej do obsługi platformy. Struktura infrastruktury serwerowej oraz sama platforma iDirect ma jedną sporą wadę nie pozwala w żaden łatwy sposób zrobić redundancji dla switcha przez który przechodzi cały ruch sieciowy, bez przełączania fizycznie połączeń między dwoma switchami. Wynika to z tego że w momencie podłączenia się do sieci satelitarnej modemy zostają przypisane do jednego z serwerów PP i nie można dynamicznie tego serwera zmienić po podłączeniu się do sieci.

Schemat pozwala natomiast na obserwację tego w jaki sposób komponenty są połączone w sieć. Serwer NMS jest podłączony do sieci upstream przechowuje on tylko konfigurację więc nie zmienia przepływu danych w sieci. Serwer PP jest podłączony dwoma portami do switcha, co oznacza że jest podłączony do sieci tunnel i jednocześnie do sieci upstream, podział tych sieci na switchu SW1 jest realizowany za pomocą sieci VLAN. Routery działają jako routery dostępowe do sieci internet. Od strony WAN są podłączone dwoma łączami do internetu oraz mają przydzielone dwa adresy publiczne oraz jeden wirtualny dla technologii VRRP.

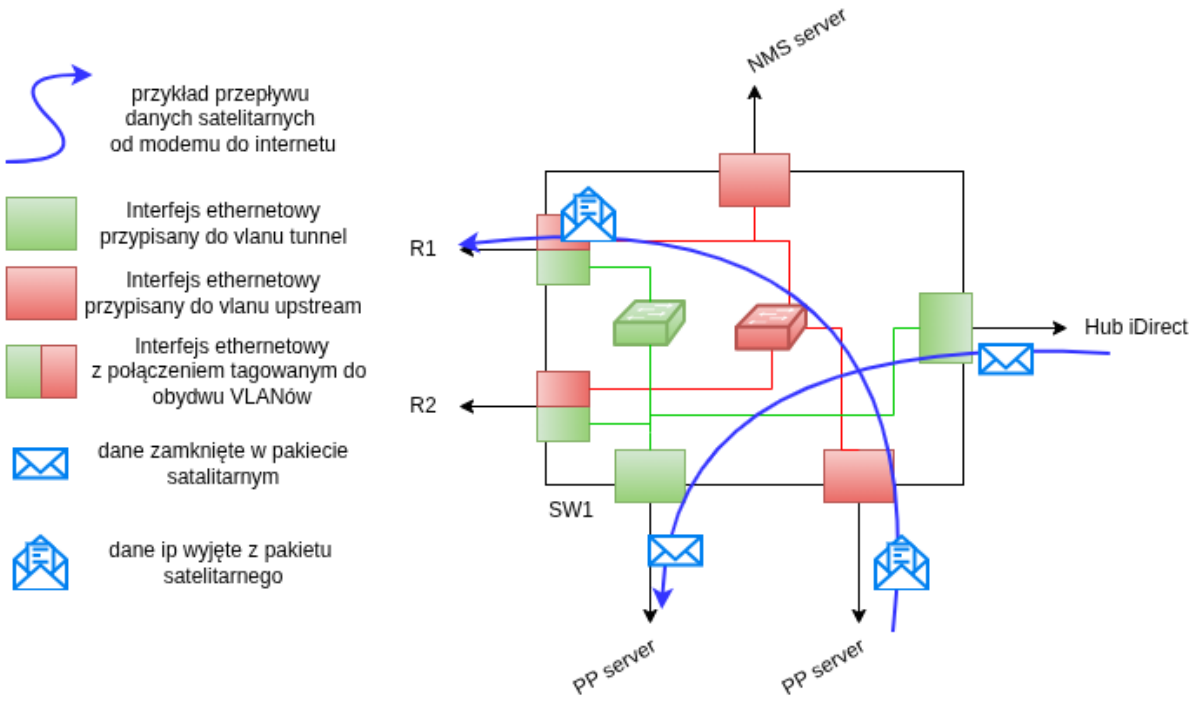
Przepływ danych w warstwie 2



Schemat konfiguracji switcha SW1 [Opracowanie własne]

Schemat przedstawiony na rysunku12 ilustruje szczegółową konfigurację przełącznika warstwy drugiej, który stanowi serce całej infrastruktury iDirect. Na poziomie fizycznym przełącznik jest podzielony na dwa odrębne segmenty logiczne, realizowane przy pomocy VLAN-ów: VLAN10 (oznaczony jako UPSTREAM) oraz VLAN20 (oznaczony jako TUNNEL). VLAN20 służy wyłącznie do transportu surowych, jeszcze niezdekodowanych danych satelitarnych, które po przybyciu do serwera PP są przekształcane w standardowe pakiety IP. Dzięki temu ruch w tej części sieci pozostaje odizolowany od wszelkich operacji

przetwarzania i nie jest narażony na niepotrzebne ingerencje. Z kolei VLAN10, czyli UPSTREAM, obsługuje wszystkie funkcje zarządzania i monitoringu – w tej sieci znajdują się serwery NMS, które przechowują konfiguracje iDirect, a także interfejsy serwera PP po przetworzeniu danych. Dzięki temu ruch zarządzający i ruch użytkowników końcowych (przetworzone pakiety IP) są rozdzielone, co zwiększa zarówno bezpieczeństwo, jak i przejrzystość operacyjną. Dodatkowo przełącznik wykorzystuje trunking 802.1Q na portach łączących się z routerami brzegowymi (R1 i R2), co umożliwia jednoczesne przenoszenie obu VLAN-ów przez jedno fizyczne łączę, a jednocześnie zapewnia pełną separację logiczną. Taki podział pozwala na łatwe skalowanie – wystarczy dodać kolejne serwery PP lub terminale satelitarne, podłączając je do odpowiednich portów VLAN, bez konieczności przebudowy istniejącej topologii. W rezultacie przełącznik zapewnia nie tylko wydajny przepływ danych, ale także elastyczność niezbędną do utrzymania wysokiej dostępności i prostego zarządzania całym systemem iDirect.



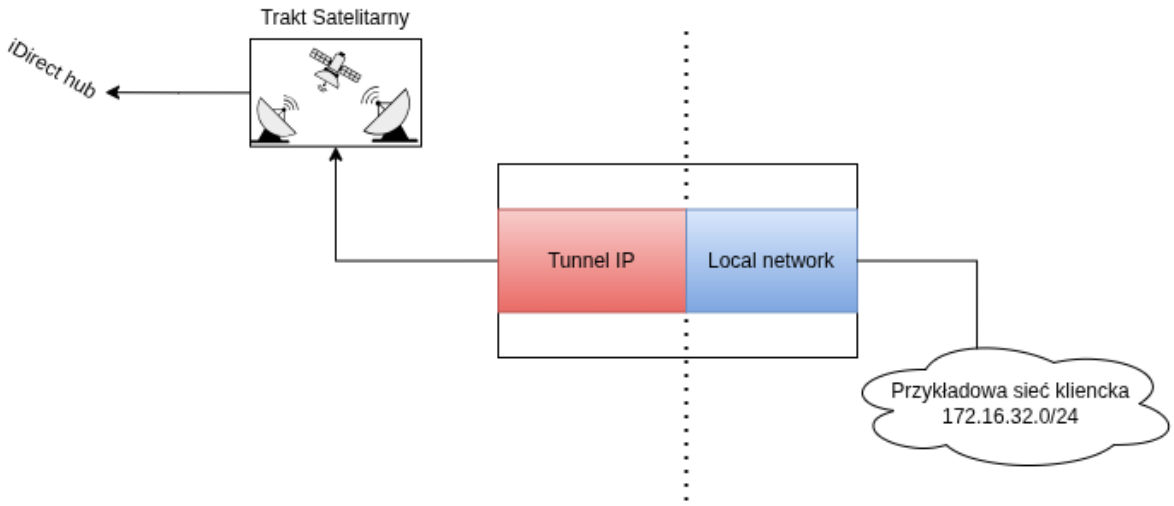
Schemat przepływu danych z platformy satelitarnej do routerów [Opracowanie własne]

Schemat zamieszczony w rysunku13 obrazuje szczegółowy przebieg danych satelitarnych w obrębie przełącznika, ukazując jednocześnie, że w każdej sieci komputerowej ruch jest dwukierunkowy – każdy pakiet, który przemieszcza się w jedną stronę, musi po drodze odbyć równie istotny proces powrotu w odwrotnej kolejności. W kontekście platformy iDirect oznacza to, że po przyjęciu surowego pakietu satelitarnego przez port VLAN20 (TUNNEL), przełącznik kieruje go do serwera PP, który pełni rolę pośrednika dekodującego własnościowy protokół iDirect na standardowe pakiety IP. Po przetworzeniu, pakiet trafia do VLAN10 (UPSTREAM), skąd może zostać skierowany do routera brzegowego lub serwera NMS w zależności od przeznaczenia.

Kluczowym elementem tej architektury jest fakt, że router krańcowy (Edge) nie ma bezpośredniego dostępu do terminali satelitarnych znajdujących się w sieci TUNNEL. Zamiast tego, router musi polegać na serwerze PP, który poprzez dynamiczny protokół routingu RIP rozgłasza informacje o wszystkich adresach modemów satelitarnych. Dzięki temu router posiada w swojej tablicy routingu wpisy wskazujące, że określone sieci lokalne (np. `172.16.32.0/24`) są osiągalne poprzez adres serwera PP.

Warto podkreślić, że każdy terminal satelitarny zachowuje się jak odrębny router – posiada własną sieć lokalną, którą udostępnia klientowi podłączonemu do portu Ethernet. Ta sieć lokalna jest rejestrowana w systemie iDirect i przekazywana do serwera PP, a następnie rozgłaszana do routera brzegowego. W praktyce oznacza to, że gdy pakiet przychodzi z Internetu do routera, zostaje skierowany do serwera PP, który na podstawie swojej tablicy routingu odsyła go do odpowiedniego terminala satelitarnego poprzez sieć TUNNEL. Po dotarciu do terminala, pakiet jest dalej przekazywany do urządzenia końcowego w sieci lokalnej klienta. Ten proces – od terminala do PP, dalej do routera, do Internetu i z powrotem – zapewnia pełną kontrolę nad ruchem, umożliwia monitorowanie i zarządzanie oraz gwarantuje, że wszystkie elementy sieci pozostają ze sobą spójnie powiązane, mimo fizycznej separacji dwóch domen adresowych.

Podział sieci na terminalu satelitarnym



Schemat podziału sieci na terminalu satelitarnym [Opracowanie własne]

Na dotychczas opisanych etapach nie zachodzi żadna translacja adresów – wszystkie segmenty sieci (tunnel, upstream oraz lokalne sieci terminali) muszą ze sobą bezpośrednio wymieniać pakiety, co wymusza pełną koordynację adresową pomiędzy nimi. Analizując schemat przedstawiony na rysunku14, można zauważyć, że router brzegowy nie zna szczegółów struktury sieci lokalnych (local network) podłączonych do poszczególnych modemów satelitarnych. Informacje te są dostarczane w sposób dynamiczny dzięki protokołowi RIP, którego rozgłoszeniami zarządza serwer PP. Każdy modem satelitarny po uruchomieniu rejestruje się w platformie iDirect, przekazując informację o swojej własnej sieci lokalnej (np. `172.16.32.0/24`) oraz o adresie tunelowym, pod którym jest dostępny (np. `192.168.20.10`). Platforma informuje o tym serwer PP, który w konsekwencji aktualizuje swoją tablicę routingu i rozgłasza nowy wpis do routera krańcowego. W tablicy routera pojawia się rekord wskazujący, że docelowa sieć lokalna jest osiągalna poprzez adres IP serwera PP w sieci upstream (np. `192.168.10.111`). Jednocześnie serwer PP zachowuje w swojej własnej bazie informację, że podany adres upstream odpowiada konkretnemu adresowi tunelowemu modemu, co pozwala mu w przyszłości skierować przychodzące pakiety z powrotem do właściwego terminala. Dzięki temu mechanizmowi router zawsze wie, przez który serwer PP ma przesłać ruch, aby dotrzeć do określonej sieci lokalnej, a serwer PP z kolei zna dokładny adres tunelowy modemu, który umożliwia finalne dostarczenie pakietu do urządzenia końcowego w sieci klienta. Ten dwustopniowy proces – najpierw informacja o sieci lokalnej

przekazywana z modemu do PP, a następnie od PP do routera – eliminuje potrzebę ręcznej konfiguracji tras i zapewnia automatyczną, skalowalną wymianę routingu w całej infrastrukturze iDirect.

Studium przypadku, przykład przepływu danych

Żeby bardziej rozjaśnić zasadę działania przepływu danych w sieci iDirect, rozpatrzmy przykład transmisji pakietu w sieci gdzie terminal satelitarny wyśle pakiet ICMP. Poniżej spis adresów wykorzystanych do takiego przypadku.

1. `8.8.8.8` - przykładowy adres dostępny w internecie
2. `192.168.10.0/24` - podsieć dla VLANu upstream
3. `192.168.20.0/24` - podsieć dla VLANu tunnel
4. `192.168.10.1` - adres R1 w VLANie upstream
5. `192.168.20.1` - adres R1 w VLANie tunnel
6. `192.168.10.2` - adres R2 w VLANie upstream
7. `192.168.20.2` - adres R2 w VLANie tunnel
8. `192.168.10.3` - adres VRRP w VLANie upstream
9. `192.168.20.3` - adres VRRP w VLANie tunnel
10. `192.168.10.111` - interfejs serwera PP w VLANie upstream
11. `192.168.20.111` - interfejs serwera PP w VLANie tunnel
12. `172.16.32.0/24` - podsieć kliencka
13. `172.16.32.1` - adres local network modemu
14. `192.168.20.10` - adres tunnel ip modemu
15. `172.16.32.254` - adres klienta (np. komputera podłączonego do terminala satelitarnego)

Przeanalizujmy sytuację w której klient podłączony do terminala satelitarnego wysyła pakiet ICMP do adresu `8.8.8.8`.

Komputer wysyła pakiet icmp na adres `8.8.8.8`

Adres źródłowy	Adres docelowy
172.16.32.254	8.8.8.8

Modem odbiera ten pakiet, nie zna sieci docelowej więc przekazuje ten pakiet na swoją bramę czyli na serwer PP, `192.168.20.111`.

Adres źródłowy	Adres docelowy
172.16.32.254	8.8.8.8

Serwer PP odbiera pakiet (w sieci tunnel) rozkodowuje go z pakietu satelitarnego na pakiet IP. Następnie sprawdza w tablicy routingu sieć docelową, nie zna jej więc przekazuje go na swoją bramę czyli adres VRRP (w sieci upstream) `192.168.10.3`.

Adres źródłowy	Adres docelowy
172.16.32.254	8.8.8.8

Routery R1 i R2 odbierają pakiet (w sieci upstream) sprawdzają sieć docelową która jest w internecie, przekazują pakiet do swojej bramy w sieci publicznej maskując swój adres. W tym miejscu na potrzeby tej analizy pominiemy fragment przechodzenia pakietu przez sieć internet i przejdziemy od razu do etapu powrotu pakietu. Serwer `8.8.8.8` zwraca pakiet na adres publiczny routerów routery odbierają go i następnie podmieniają z powrotem adresy z tabeli połączeń przechodzących przez NAT.

Adres źródłowy	Adres docelowy
8.8.8.8	172.16.32.254

Router w tabeli routingu RIP ma wpis (rozgłoszony przez serwer PP) który mówi że do sieci **172.16.32.0/24** ma dostać się przez serwer PP **192.168.10.111**. Więc router przekazuje to z powrotem na serwer PP.

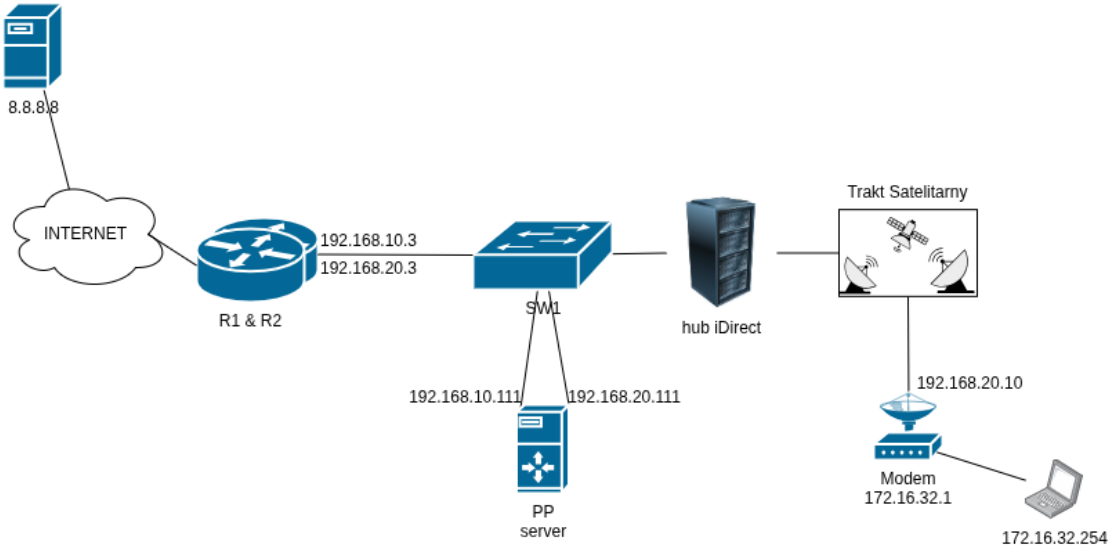
Serwer PP odbiera pakiet i zgodnie z tabelą routingu RIP ma trasę która pokazuje że do sieci `172.16.32.0/24` ma dostać się przez adres tunnel ip modemu `192.168.20.10`.

Adres źródłowy	Adres docelowy
8.8.8.8	172.16.32.254

Modem otrzymuje pakiet i zgodnie z wspisem w tabli przekazuje go na sieć która jest do niego bezpośrednio podłączona.

Adres źródłowy	Adres docelowy
8.8.8.8	172.16.32.254

Powyżej wyjaśniony proces można zaobserwować na rysunku 15. Na wymienionym rysunku przedstawiono wszystkie urządzenia wymienione w procesie oraz umieszczono obok nich przypisy z odpowiednimi adresami w celu łatwiejszej wizualizacji tego procesu.



Schemat sieci satelitarnej wraz z adresacją [Opracowanie własne]

Implementacja konfiguracji zgodnej z wymaganiami

Konfiguracja switcha dla platformy iDirect

W poprzednich sekcjach omówiliśmy specyfikę działania platformy oraz przepływ danych. W tej sekcji omówimy jak skonfigurować switch platformy iDirect tak żeby umożliwić jego działanie w sieci, służącej do obsługi tej platformy.

Poniżej analiza konfiguracji switcha na przykładzie platformy Cisco Catalyst. Wymieniono poszczególne etapy konfiguracji takiego urządzenia wykonane w trybie konfiguracji globalnej (przy uprzednim wykonaniu poleceń `enable` a nastepnie `configure terminal`)

1. Dodanie VLANów dla sieci upstream oraz tunnel.

```
vlan 10
name UPSTREAM
exit

vlan 20
name TUNNEL
exit
```

1. Ustawienie portów dla routerów R1 i R2.

```
interface GigabitEthernet1/0/1
description R1
switchport mode trunk
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
exit
```

```
interface GigabitEthernet1/0/2
description R2
switchport mode trunk
switchport trunk allowed vlan 10,20
switchport trunk encapsulation dot1q
exit
```

1. Przykład konfiguracji portów dla serwera NMS oraz PP

```
interface GigabitEthernet1/0/3
description NMS
switchport mode access
switchport access vlan 10
exit

interface GigabitEthernet1/0/4
description PP tunnel
switchport mode access
switchport access vlan 10
exit

interface GigabitEthernet1/0/5
description PP upstream
switchport mode access
switchport access vlan 20
exit
```

Konfiguracja routera do obsługi platformy iDirect

W poprzedniej sekcji omówiona została konfiguracja urządzenia warstwy drugiej, w tej sekcji omówimy konfigurację routera do obsługi platformy iDirect. Do wdrożenia tej sieci została wybrana platforma sprzętowa MikroTik bazująca na systemie RouterOS.

Poniżej analiza krok po kroku konfiguracji przeprowadzonej na routerach R1 oraz R2. Fragmenty konfiguracji nie różniące się pomiędzy routerami zostały wymienione tylko na przykładzie routera R1, natomiast fragmenty konfiguracji różniące się miedzy routerami zostały wymienione podwójnie z wyjaśnieniem różnic. Polecania zostały wykonane z standardowego terminala dostępnego w systemie RouterOS.

Zmiana nazw interfejsów.

```
/interface ethernet
set [ find default-name=ether1 ] name=ether1-WAN
set [ find default-name=ether2 ] name=ether2-iDX
```

Interfejs o nazwie `ether1-WAN` jest podłączony do sieci internet. Interfejs o nazwie `ether2-iDX` jest podłączony do switcha SW1

Dodanie wirtualnych interfejsów na porcie `ether2-iDX` do obsługi sieci VLAN.

```
/interface vlan
add interface=ether2-iDX name=VLAN10-Upstream vlan-id=10
add interface=ether2-iDX name=VLAN20-Tunnel vlan-id=20
```

Konfiguracja VRRP na interfejsach.

Konfiguracja na routerze R1, który jest routerem głównym.

```
/interface vrrp
add group-authority=self interface=VLAN10-Upstream
name=VRRP1-VLAN10-Upstream \
priority=200 vrid=10
add group-authority=VRRP1-VLAN10-Upstream
interface=VLAN20-Tunnel name=\
VRRP2-VLAN20-Tunnel priority=200 vrid=20
add group-authority=VRRP1-VLAN10-Upstream
interface=ether1-WAN name=VRRP3-WAN \
priority=200 vrid=40
```

Konfiguracja na routerze R2, który jest routerem zapasowym.

```
/interface vrrp
add group-authority=VRRP1-VLAN10-Upstream
interface=VLAN10-Upstream name=VRRP1-VLAN10-Upstream \
priority=100 vrid=10
add group-authority=VRRP1-VLAN10-Upstream
interface=VLAN20-Tunnel name=\
VRRP2-VLAN20-Tunnel priority=100 vrid=20
add group-authority=VRRP1-VLAN10-Upstream
interface=ether1-WAN name=VRRP3-WAN \
priority=100 vrid=40
```

Wyżej wymieniona konfigurcja składa się z trzech interfejsów VRRP.

`VRRP1-VLAN10-Upstream`

`VRRP2-VLAN20-Tunnel`

`VRRP3-WAN`

Każdy z tych interfejsów jest skonfigurowany tak że parametr group-authority to interfejs `VRRP1-VLAN10-Upstream`. Oznacza to że w przypadku kiedy urządzenia przestaną się ze sobą komunikować poprzez sieć upstream to VRRP automatycznie przełączy się na router zapasowy. Interfejs `VRRP2-VLAN20-Tunnel` nie był konieczny do skonfigurowania gdyż nie ma wymagania bramy dla sieci tunnel, nastomiast jest to przydatne podczas konfigurowania kart w hubie iDirect. Ostatni interfejs to `VRRP3-WAN` jest on wykorzystywany głównie do wychodzenia do internetu poprzez jeden wirtualny adres interfejsu VRRP i w przypadku przełączenia awaryjnego adres publiczny się nie zmienia.

Włączenie routingu dynamicznego RIP na routerze, na odpowiednich interfejsach.

```
/routing rip instance
add disabled=no name=rip-instance-1 routing-
table=main
/routing rip interface-template
add disabled=no instance=rip-instance-1 interfaces=\
VRRP1-VLAN40-Upstream,VRRP2-VLAN50-Tunnel
```

Stworzenie list interfejsów oraz dodanie interfejsów do tych list.

```
/interface list
add name=WAN
add name=LAN
```

```
/interface list member
add interface=ether1-WAN list=WAN
add interface=VLAN10-Upstream list=LAN
add interface=VLAN20-Tunnel list=LAN
add interface=VRRP1-VLAN10-Upstream list=LAN
add interface=VRRP2-VLAN20-Tunnel list=LAN
add interface=VRRP3-WAN list=WAN
add interface=ether2-iDX list=LAN
```

Interfejsy zostały dodane do grup w poniższy sposób:
WAN: ether1-WAN, VRRP3-WAN
LAN: VRRP1-VLAN10-Upstream, VRRP2-VLAN20-Tunnel, ether2-iDX, VLAN10-Upstream, VLAN20-Upstream
Interfejsy zostały przydzielone w ten sposób gdyż chcemy żeby wszystkie były rozpatrywane jako interfejsy od strony lokalnej lub od strony publicznej, w zasadach w firewallu, nie zależnie od tego czy są to interfejsy wirtualne czy fizyczne.

Zaadresowanie interfejsów Konfiguracja R1:

```
/ip address
add address=192.168.10.1/24 interface=VLAN10-Upstream
network=192.168.10.0
add address=192.168.20.1/24 interface=VLAN20-Tunnel
network=192.168.20.1
add address=192.168.10.3/24 interface=VRRP1-VLAN10-
Upstream network=192.168.10.0
add address=192.168.20.3/24 interface=VRRP2-VLAN20-
Tunnel network=192.168.20.0
add address=203.0.113.1/27 interface=ether1-WAN
network=203.0.113.0
add address=203.0.113.3/27 interface=VRRP4-WAN
network=203.0.113.0
```

Konfiguracja R2 to samo co powyżej oraz zmiany wymienione niżej:

```
/ip address
add address=192.168.10.2/24 interface=VLAN10-Upstream
network=192.168.10.0
add address=192.168.20.2/24 interface=VLAN20-Tunnel
network=192.168.20.1
add address=192.168.10.3/24 interface=VRRP1-VLAN10-
```

```
Upstream network=192.168.10.0
add address=192.168.20.3/24 interface=VRRP2-VLAN20-
Tunnel network=192.168.20.0
add address=203.0.113.2/27 interface=ether1-WAN
network=203.0.113.0
add address=203.0.113.3/27 interface=VRRP4-WAN
network=203.0.113.0
```

Tabela adresacji routerów [Opracowanie własne]

Router	**Interfejs**	**Adres**
R1	VLAN10-Upstream	192.168.10.1
R1	VLAN20-Tunnel	192.168.20.1
R1	VRRP1-VLAN10-Upstream	192.168.10.3
R1	VRRP2-VLAN20-Tunnel	192.168.20.3
R1	ether1-WAN	203.0.113.1
R1	VRRP4-WAN	203.0.113.3
R2	VLAN10-Upstream	192.168.10.2
R2	VLAN20-Tunnel	192.168.20.2
R2	VRRP1-VLAN10-Upstream	192.168.10.3
R2	VRRP2-VLAN20-Tunnel	192.168.20.3
R2	ether1-WAN	203.0.113.2
R2	VRRP4-WAN	203.0.113.3

Włączenie funkcji przekazywania zapytań DNS

Włączenie tej funkcji pozwala na ustawienie serwera DNS na adres routera, dla klientów. Router działa wtedy jak rekursywny DNS z własną pamięcią cache dla częstych zapytań oraz można zdefiniować własne statyczne wpisy DNS.

```
/ip dns
set allow-remote-requests=yes servers=8.8.8.8
```

Ustawienie zasad filtrowania na firewallu

```
/ip firewall filter
add action=accept chain=input comment="accept
established,related" \
connection-state=established,related
add action=drop chain=input comment="drop invalid"
```

```
connection-state=invalid
add action=accept chain=input comment="accept icmp"
protocol=icmp
add action=drop chain=input comment="drop all not
coming from lan" \
in-interface-list=!LAN
add action=accept chain=forward comment="accept in
ipsec policy" \
ipsec-policy=in,ipsec
add action=accept chain=forward comment="accept out
ipsec policy" \
ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward
comment=fasttrack \
connection-state=established,related hw-offload=yes
add action=drop chain=forward comment="drop forward
invalid" \
connection-state=invalid
add action=drop chain=forward comment="drop all from
WAN not DSTNATed" \
connection-nat-state=!dstnat connection-state=new in-
interface-list=WAN
add action=accept chain=forward comment=\
"accept established,related, untracked" connection-
state=\
established,related,untracked
```

Poniżej wyjaśnienie poszczególnych zasad, w kolejności ich występowania listingu.

accept established,related - zasada pozwalająca na przepuszczenie pakietów które należą do połączeń które zostały już zestawione lub są kontynuowane.

drop invalid - zasada która odrzuca połączenie które mają stan połączenia jako invalid.

accept icmp - zasada pozwalająca na ruch ICMP kierowany do routera.

drop all not coming from lan - zasada blokująca cały ruch który ma źródło poza interfejsami na liście LAN a jest skierowany do routera.

accept in/out ipsec policy - dwie zasady które zgodnie z dokumentacją MikroTika powinny być zaimplementowane aby klienci którzy są podłączeni do sieci LAN routera mogli zestawiać tunele ipsec.

fasttrack - zasada która zgodnie z dokumentacją MikroTika ma odciążyć procesor routera dla pakietów które są już przypisane do istniejących połączeń.

drop forward invalid - zasada która ma nie pozwolić routerowi przekazać dalej pakietów których stan połączenia to invalid.

drop all from WAN not DSTNATed - zasada która ma odrzucić wszystkie nowe połączenia które nie zostały dodane do przekierowań portów (translacji adresów docelowych DNAT).

Konfiguracja translacji adresów źródłowych.

Router został skonfigurowany tak że wszystkie pakiety wychodzące przez interfejsy na liście WAN, mają zamaskowany adres źródłowy publicznym adresem VRRP.

```
/ip firewall nat
add action=src-nat chain=srcnat log-prefix=NAT
out-interface-list=WAN \
to-addresses=203.0.113.3
```

Ustawienie trasy domyślnej.

Adres `203.0.113.254` to adres bramy dla publicznej podsieci.

```
/ip route
add check-gateway=ping disabled=no distance=1
dst-address=0.0.0.0/0 gateway=\
203.0.113.254 routing-table=main scope=30
suppress-hw-offload=yes \
target-scope=10
```

Konfiguracja usług, strefy czasowej, nazwy routera oraz NTP.

```
/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set ssh address=192.168.0.0/16
set api disabled=yes
set api-ssl disabled=yes
/system clock
set time-zone-name=Europe/Warsaw
/system identity
set name=IDIRECT-MIKROTIK-X
/system ntp client
set enabled=yes
/system ntp server
set broadcast=yes enabled=yes multicast=yes
/system ntp client servers
add address=tempus1.gum.gov.pl
add address=tempus2.gum.gov.pl
```

Poniżej wymienione procesy wykonane w konfiguracji:

Wyłączenie nie używanych usług na routerze takich jak: telnet, ftp, www, api. Ograniczenie połączeń ssh do routera tylko z sieci lokalnych.

Ustawienie strefy czasowej na strefę Europe/Warsaw.

Ustawienie nazwy routera na IDIRECT-MIKROTIK-X gdzie X to 1 dla R1 oraz 2 dla R2

Włączenie usługi ntp client oraz ntp server.

Skonfigurowanie klienta ntp i ustawienie serwerów na główny urząd miar.

Zastosowane urządzenia

Urządzenie wykorzystane do wdrożenia wcześniej wymienionych konfiguracji to:

1. Platforma iDirect Evolution series 15100, razem z wymaganymi kartami nadawczymi i odbiorczymi.
2. Modem/Terminal satelitarny iDirect Evolution X3
3. Serwery Dell poweredge R440
4. Switch Cisco Catalyst C9300-24P-M

Wybór platformy satelitarnej padł na platformę iDirect gdyż jest to jedna z najlepiej wspieranych i najlepiej udokumentowanych platform służących do wdrożeń sieci satelitarnych.

Router został wybrany jako MikroTik gdyż posiada on wszystkie funkcje wymagane do obsługi platformy oraz pozwoli na ewentualną rozbudowę sieci o tunele VPN lub redystrybucję tras w przyszłości. Łatwość konfiguracji oraz znajomość platformy przez autora też były nieuwzględnione podczas wyboru tej platformy.

Switch nie pełni tutaj żadnej innej funkcji poza dzieleniem domeny rozgłoszeniowej na dwie podsieci tunnel oraz upstream. Platforma Catalyst została wybrana z racji znajomości tej platformy.

Platforma iDirect

Platforma Satelitarna iDirect Evolution series 15100
Źródło: https://www.idirect.net/

Najważniejsze cechy platformy:

- Seria 15100 może pomieścić do 20 uniwersalnych lub obronnych kart liniowych (ULC, DLC)
- Obsługuje do pięciu satelitów
- Obsługuje DVB-S2/DVB-S2X ACM z modulacją od QPSK do 256APSK
- Karty liniowe obsługują do 119 Msps DVB-S2X forward carriers i Adaptive TDMA na powrocie
- 48-portowy interfejs Gigabit Ethernet LAN obsługuje wysokie szybkości symboli nośnych
- Wysoki poziom nadmiarowości dzięki łańcuchowemu połączeniu hubów i nadmiarowości geograficznej
- Umożliwia konfigurację operatora sieci hosta (HNO) i operatora sieci wirtualnej (VNO)
- Współpracuje z wysokowydajnymi procesorami protokołów i serwerami NMS w celu inteligentnego routingu IP i równoważenia obciążenia

Terminal Satelitarny

Modem/Terminal satelitarny iDirect Evolution X3
Źródło: https://www.idirect.net/

Maksymalne parametry osiągane dla modemu iDirect Evolution X3:

- Downstream DVB-S2 Upstream TDMA Upstream SCPC Return
- Modulation QPSK, 8PSK, 16APSK BPSK, QPSK, 8PSK BPSK, QPSK, 8PSK
- Max. Symbol Rate 45 Msps 7.5 Msps 15 Msps
- Max. Info Rate 150 Mbps1 12.8 Mbps 24 Mbps
- Max. Line Card IP Data Rate 149 Mbps1 11.1 Mbps2 18.2 Mbps3
- Max. Remote IP Data Rate 29 Mbps1 7.8 Mbps2 11.8 Mbps31

Serwery PP oraz NMS

Serwer Dell poweredge R440
Źródło: https://www.dell.com/

Switch

Switch Cisco Catalyst C9300-24P-M
Źródło: https://www.cisco.com/

Routery

Router Mikrotik RB1100AHx4
Źródło: https://mikrotik.com/

Podsumowanie i wnioski

Projekt sieci przedstawionej w pracy to minimalne wymagania funkcjonale co do sieci która musi być wdrożona aby obsłużyć podstawowe funkcje platformy iDirect. Sieć ta jest już aktualnie wdrożona podczas pisania tej pracy i obsługuję kilka stacji satelitarnych.

Środowiska testowe oraz konfiguracje przedstawione w tej pracy miały na celu rozjaśnienie działania sieci satelitarnych oraz przedstawienie tego w jaki sposób takie sieci się implementuje. Cel ten został zrealizowany na przykładzie projektu sieci satelitarnej zawierającej wymaganą ilość komponentów do obsługi takiej sieci.

Kierunki przyszłych badań

Platforma iDirect to zaawansowane rozwiązanie, które zapewnia wyjątkową elastyczność w zakresie konfiguracji sieci. Dzięki tej platformie możliwe jest zestawienie infrastruktury telekomunikacyjnej w taki sposób, aby dostawca satelitarny był połączony z główną lokalizacją klienta za pomocą dedykowanego łącza światłowodowego, podczas gdy wszystkie biura podległe są integrowane poprzez łącza satelitarne. Ta unikalna architektura pozwala

na wdrożenie innowacyjnych rozwiązań i lepsze zarządzanie zasobami, co stanowi doskonałą bazę do przyszłych badań i rozwoju.

Na podstawie wyników osiągniętych w niniejszej pracy, istnieje możliwość rozbudowy lub prowadzenia dalszych badań, które mogą obejmować następujące obszary.

Rozbudowa infrastruktury zabezpieczeń

Przewiduje się wprowadzenie dodatkowych zabezpieczeń oparciu o technologie tuneli VPN. Tunelowanie VPN pozwala na bezpieczne połączenia między zdalnymi lokalizacjami a centralą, co jest kluczowe w kontekście ochrony danych wrażliwych i komunikacji. Współczesne potrzeby biznesowe oraz intensyfikacja cyberataków sprawiają, że wzmocnienie zabezpieczeń sieciowych przy użyciu technologii VPN staje się priorytetem, szczególnie w sytuacjach, gdy pracownicy pracują zdalnie.

Zastosowanie adresacji publicznej

Kolejnym kierunkiem rozwoju jest zastosowanie adresacji publicznej na urządzeniach klienckich oraz redystrybucja tras protokołu RIP do BGP. Implementacja takich rozwiązań może przynieść korzyści dla klientów, którzy przy takiej strukturze sieci mogą mieć przydzielony publiczny adres IP.

Opracowanie symulacji obciążenia sieci

Ostatnim, ale nie mniej istotnym kierunkiem badań, jest opracowanie dodatkowych symulacji obciążenia sieci. Stworzenie modeli symulacyjnych pozwoli na lepsze zrozumienie reakcji systemu pod różnymi obciążeniami, zwłaszcza w kontekście wzrastającej liczby użytkowników i urządzeń podłączonych do sieci. Dzięki tym badaniom można będzie identyfikować potencjalne wąskie gardła i optymalizować infrastrukturę, co wpłynie na jakość świadczonych usług oraz zadowolenie końcowych użytkowników.

Podsumowanie

Przyszłość badań w zakresie technologii satelitarnej i lądowej infrastruktury sieciowej składa się z wielu,

różnorodnych elementów, które razem tworzą kompleksową sieć usług telekomunikacyjnych. Zastosowanie innowacyjnych rozwiązań w zakresie bezpieczeństwa, routing oraz symulacji obciążenia może przyczynić się do znacznej poprawy wydajności i bezpieczeństwa sieci. Dalsze badania powinny skupić się na integracji tych technologii w sposób, który zaspokoi rosnące potrzeby użytkowników oraz przyczyni się do zrównoważonego rozwoju infrastruktury telekomunikacyjnej.