Network: Projekt sieci SATCOM

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.

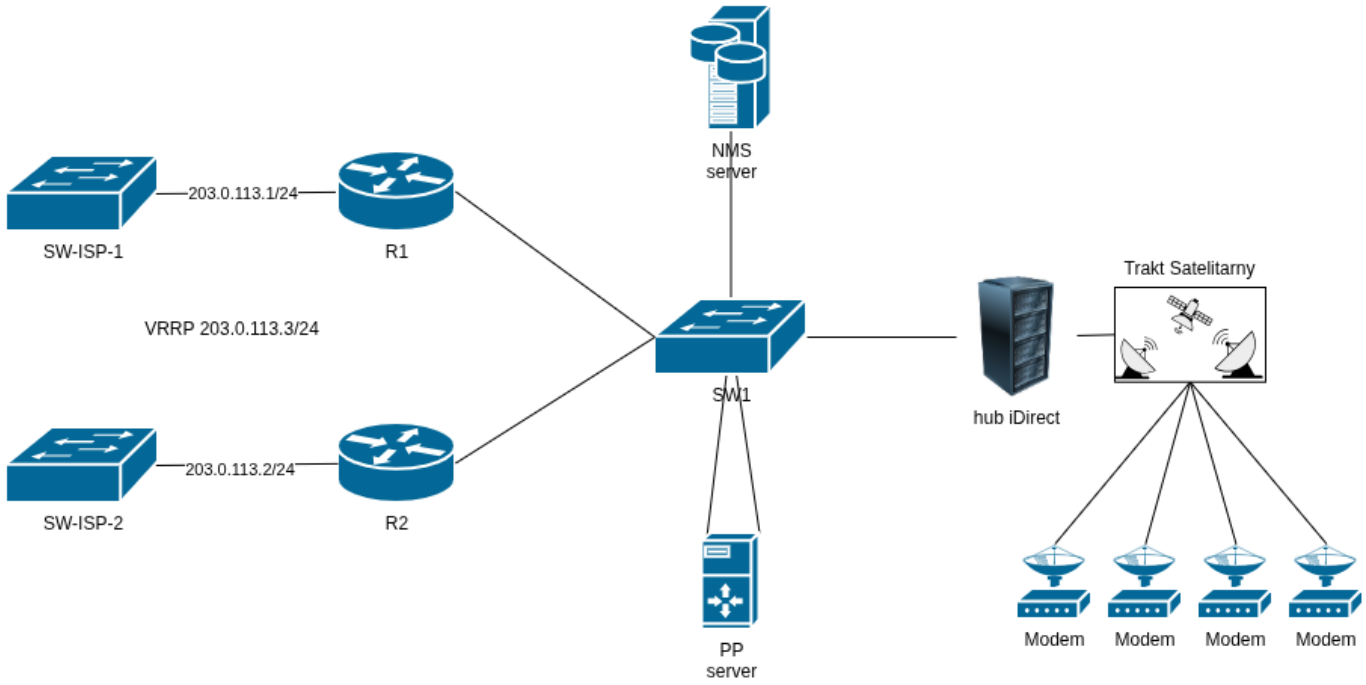
Główne elementy platformy iDirect

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

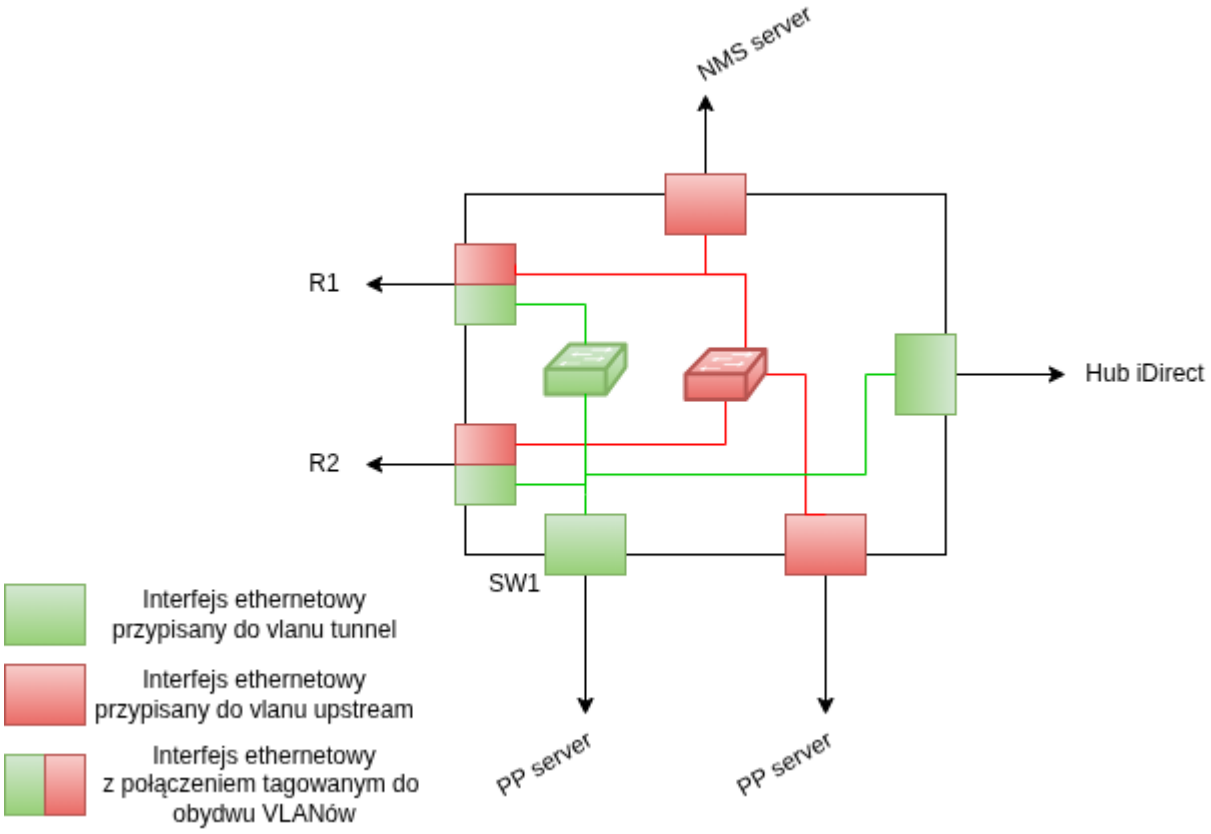


Uproszczony schemat sieci komputerowej do obsługi platformy iDirect [Opracowanie własne]

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.

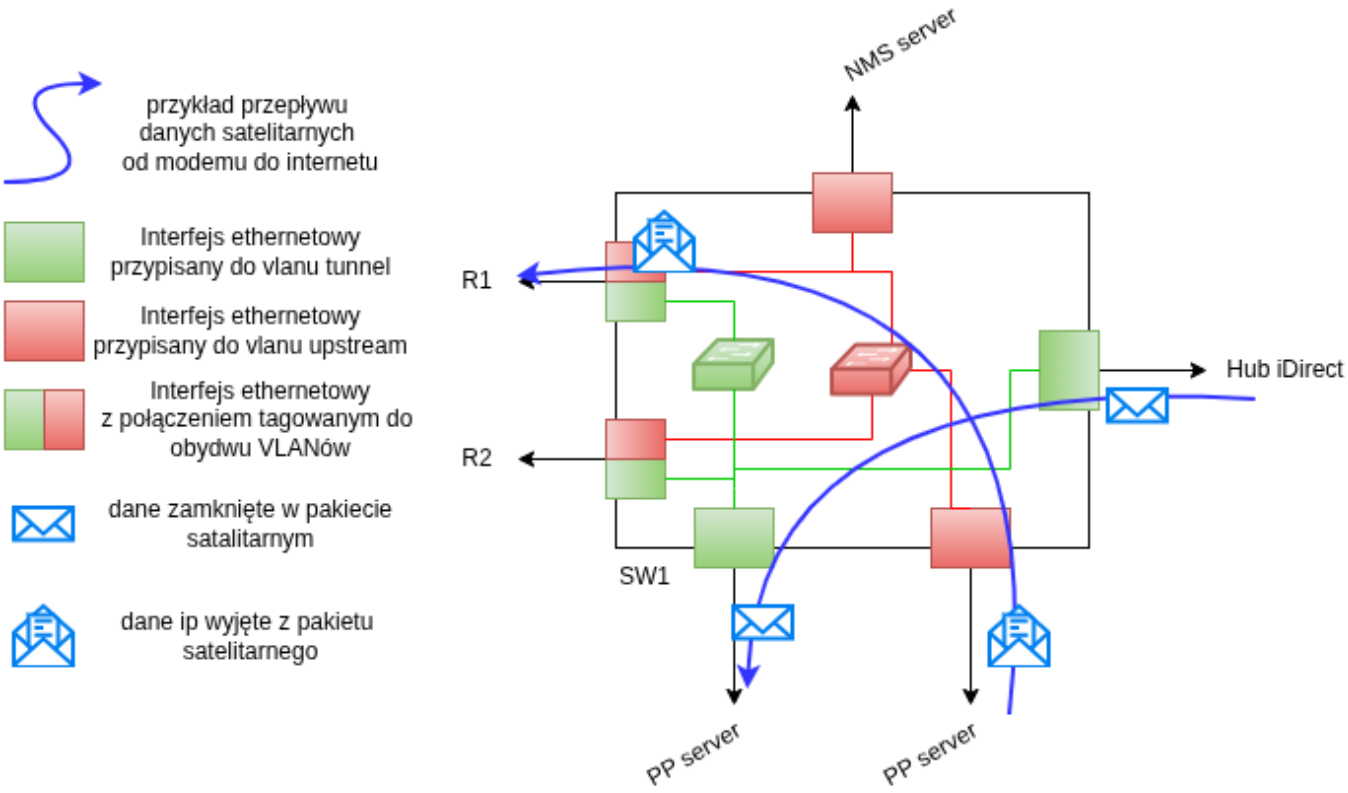
Przepływ danych w warstwie 2



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]

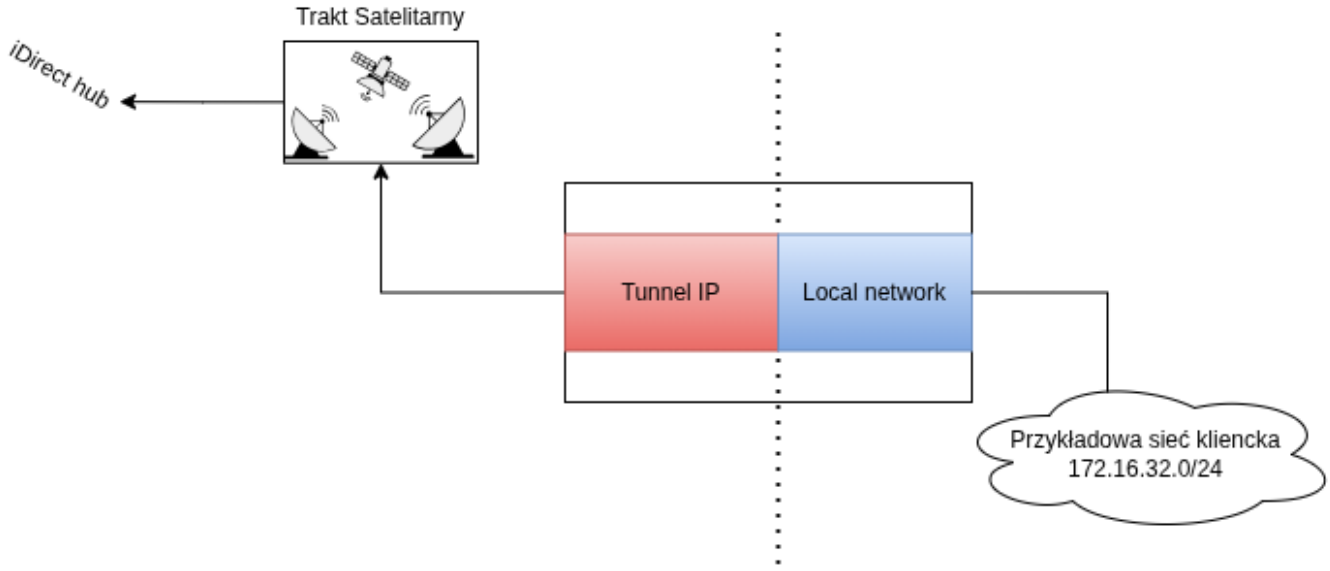
Schemat zamieszczony w rysunku13 obrazuje szczegółowy przebieg danych satelitarnych w obrębie przełącznika, ukazując jednocześnie, że w każdej sieci komputerowej ruch jest dwukierunkowy – każdy pakiet, który przemieszcza się w jedną stronę, musi po drodze odbyć równie istotny proces powrotu w odwrotnej 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`.

1. **Komputer** wysyła pakiet icmp na adres `8.8.8.8`

Adres źródłowy	Adres docelowy
172.16.32.254	8.8.8.8

2. **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

3. **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

4. **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.

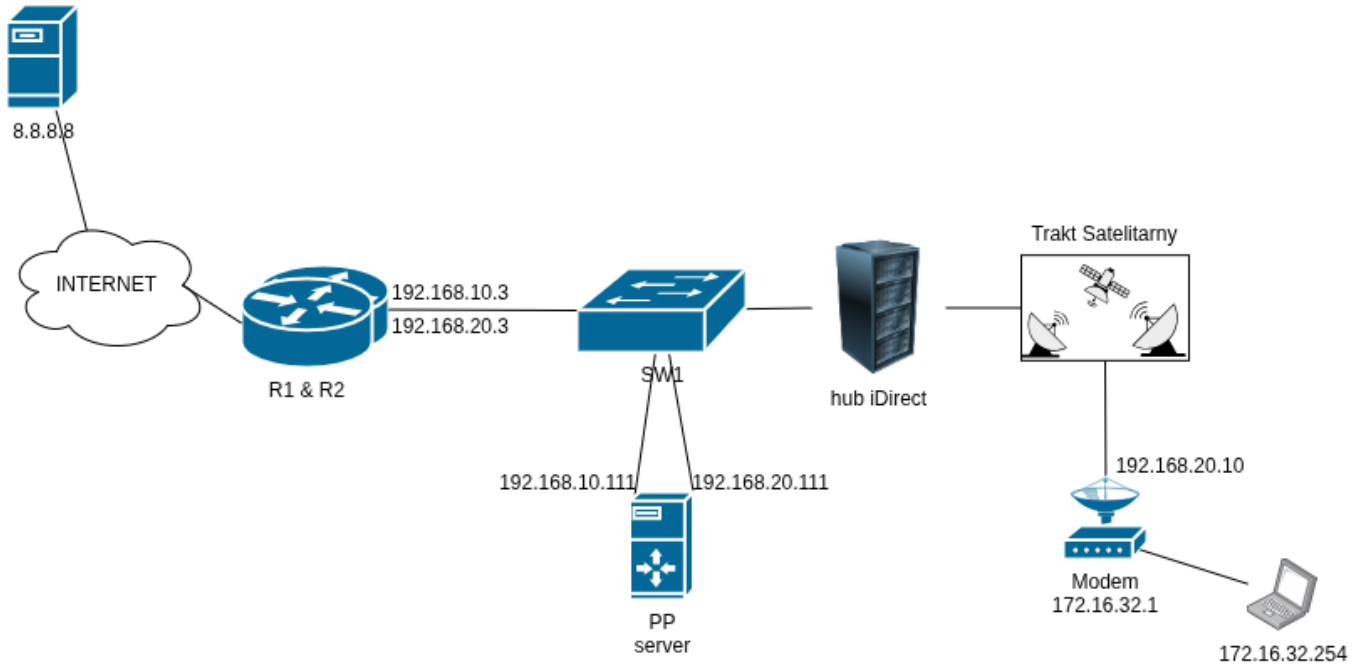
5. **Serwer PP** odbiera pakiet i zgodnie z tabelą routingu RIP ma trasę która pokazuje że do sieci `172.16.32.0/24` ma dostać się przez adres tunnel ip modemu `192.168.20.10`.

Adres źródłowy	Adres docelowy
8.8.8.8	172.16.32.254

6. **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.

1. 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

2. 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
```

1. 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.

2. 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
```

1. 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.

2. 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

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
```

4. 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).

5. 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
```

6. 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
```

7. 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

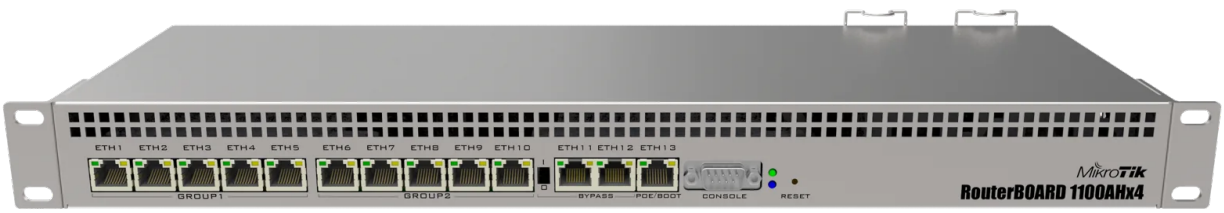
Serwery PP oraz NMS

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.