Network: SATCOM network project

Network technologies used in the work

This section will outline the key network technologies used in this thesis. Both devices and protocols will be discussed that allow for effective management of networks.

MikroTik devices - characteristics and applications

MikroTik devices are a popular networking equipment solution, offering flexibility and a variety of configuration options. They feature an intuitive interface, which makes them ideal for both small and large networks. MikroTik uses RouterOS to manage traffic, QoS, VPN and other security-related features.

VRRP protocol - operating principle and implementation

The Virtual Router Redundancy Protocol (VRRP) is used to increase the availability of a network gateway. Under VRRP, several routers work together to ensure that one of them acts as a 'virtual router'. This way, if one router fails, the others can take over responsibility, minimising network downtime.

RIP protocol - dynamic routing mechanisms

The Routing Information Protocol (RIP) is one of the oldest dynamic routing protocols, using a distance vector algorithm. RIP allows routers to exchange routing information on the network, allowing routes to be dynamically adjusted in response to changes in topology. Although simple to implement, its use is limited in large networks due to the maximum number of 15 hops.

Importantly, the RIP protocol is particularly required for the operation of satellite platforms, as it is still widely used in these systems.

Redundancy and failover in IP networks

Redundancy and failover are key elements in the design of reliable IP networks. Through the use of VRRP, networks can ensure business continuity even in the event of component failure. Proper planning and implementation of these technologies are essential to maintain the stability and availability of network services.

Computer network design for satellite communications

Requirements

Functional requirements

- **Decoding of iDirect proprietary protocols** - PP servers must receive the satellite signal, decode it into IP packets and forward it over the IP network.
- **Dynamic routing information exchange** - the RIP protocol must be running on the edge routers and PP servers to automatically propagate information about tunnel networks and local client networks.
- **Support for two separate address domains** - the network must be divided into VLANs UPSTREAM (processed IP data) and VLAN TUNNEL (raw satellite data) using a Layer 2 switch.
- **Redundancy of key components** - The edge routers must operate in active-passive mode (VRRP) and have two WAN paths configured with public IP addresses.
- **Management and monitoring** - the NMS server must have access to the iDirect configuration database and provide an interface for remote monitoring and configuration updates.
- **Support for multiple satellite terminals** - each satellite terminal (modem) must be able to register its local network (e.g. `172.16.32.0/24`) and pass this information to the PP server, which broadcasts it to the edge routers.
- **NAT and address translation support** - edge routers must perform NAT for outgoing traffic to the Internet, while retaining the ability to return traffic to the appropriate satellite terminals.

Non-functional requirements

1. **High availability** - The design must ensure the highest possible operational reliability through redundancy of the PP servers, NMS and routers (VRRP, dual WAN connections).
2. **Scalability .** - the architecture should allow additional PP servers and satellite terminals to be added without having to rebuild the existing infrastructure; each new PP server only requires two ports to be connected to the switch.
3. **Performance** - the Layer 2 switch must support at least 1Gbps per port VLAN while supporting 802.1Q trunking.
4. **Manageability** - configuration of the switch and routers must be possible via SSH or serial connection to the devices.
5. **Hardware compatibility** - all devices used (Cisco Catalyst, MikroTik RouterBOARD, PP servers) must support RIP, VLAN 802.1Q and VRRP version 3.
6. **Resistance to power failures** - key components (routers, switch, PP servers) equipped with UPS with at least 30 minutes autonomy. A requirement not discussed in this thesis, but was provided by the environment in which the network was implemented.

Network and data flow design

The iDirect platform has relatively specific requirements for the computer network to be used to

handle the network traffic generated by the satellite terminals. In order to present these requirements, we must first review the most important components of such a network.

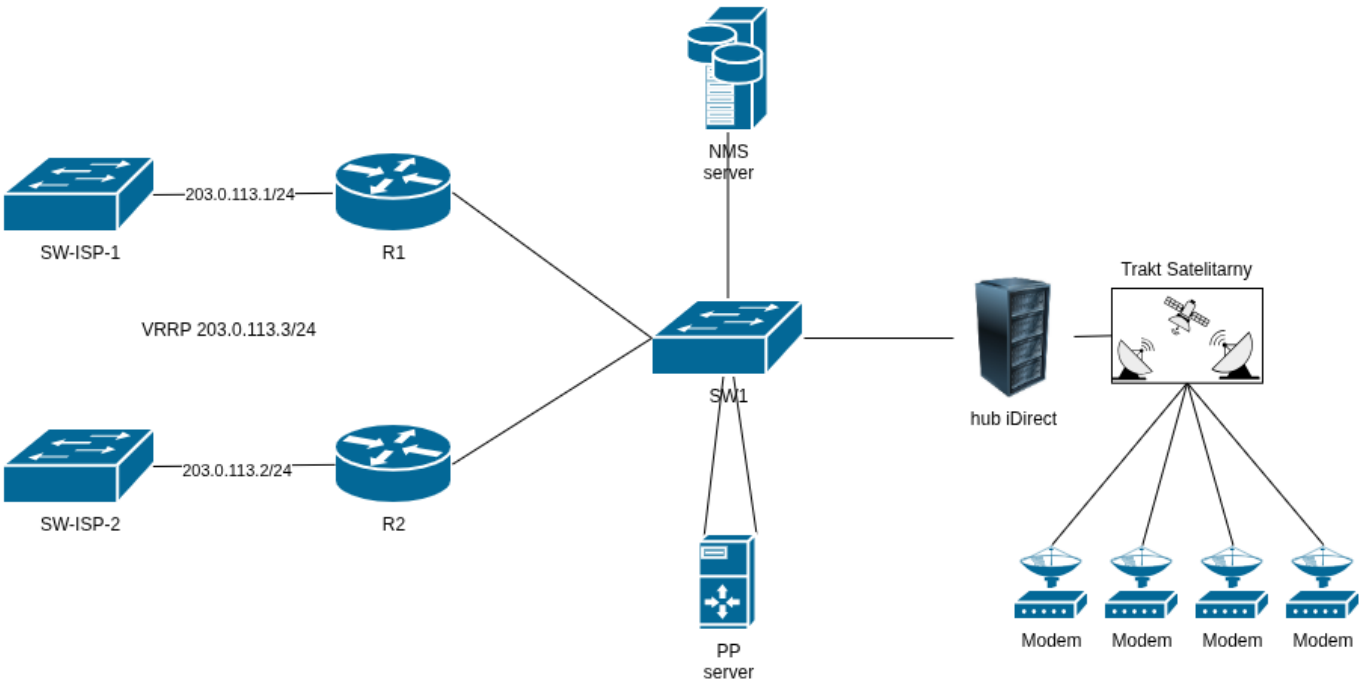
The main components of the iDirect platform

PP (protocol processor) server. The satellite platform uses proprietary protocols that are not compatible with general-purpose networks, so in order for this network traffic to be properly handled by IP networks, it must first be decoded into IP packets, this task belongs to the PP server which is connected to such a network via two ports and on one of them it receives the data to be decoded and then sends it to the other port, to the network where this data can be processed by normal IP routers. The number of these servers depends on the size of the network.

Network management system (NMS) server. This is a server which does not affect the operation of the network, but is a key component, containing a database which stores information about the network configuration and cards in the iDirect system. This server is usually installed in duplicate and replication of the database is set up to maintain redundancy.

Edge router. This is the device that handles traffic across the network. The iDirect platform uses dynamic RIP routing to communicate with the satellite modems and uses two networks that separate the data before processing by the PP servers and after processing by the PP servers. The network that contains the data before processing is called 'tunnel' and the network after processing is called 'upstream'.

The core of the iDirect network



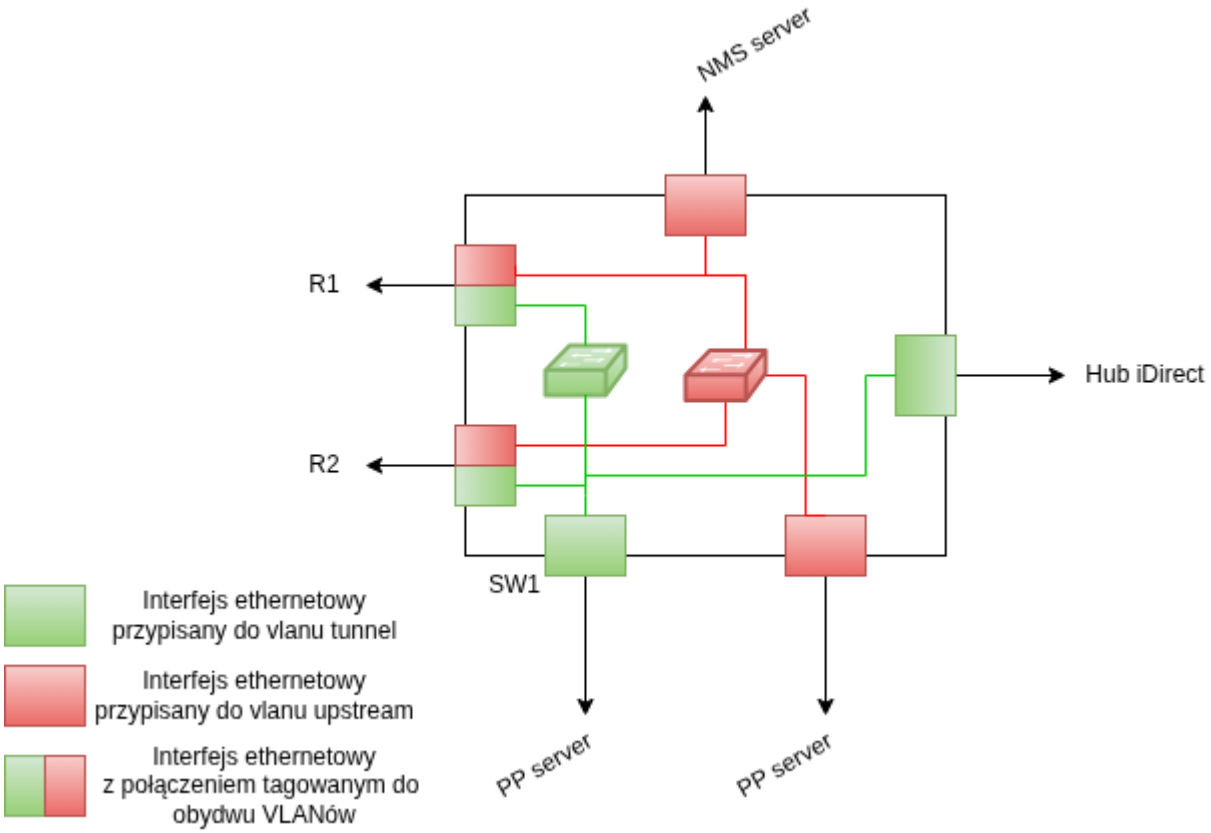
Simplified diagram of the computer network for the iDirect platform [Own elaboration].

In the simplified drawing 11 we can see what the core of the computer network to support the platform looks like. The structure of the server infrastructure and the iDirect platform itself has one significant drawback: it does not allow in any easy way to make redundancy for the switch through which all network traffic passes, without physically switching the connections between two switches.

This is because when you connect to the satellite network, the modems are assigned to one of the PP servers and you cannot dynamically change this server once you are connected to the network.

Instead, the diagram allows you to observe how the components are networked. The NMS server is connected to the upstream network it only stores the configuration so it does not change the data flow in the network. The PP server is connected with two ports to the switch, which means that it is connected to the tunnel network and at the same time to the upstream network, the division of these networks on switch SW1 is realised using VLANs. The routers act as access routers to the Internet. On the WAN side, they are connected with two links to the Internet and are assigned two public addresses and one virtual address for VRRP technology.

Layer 2 data flow



SW1 switch configuration diagram [own elaboration].

The diagram shown in Figure12 illustrates the detailed configuration of the Layer 2 switch, which is the heart of the entire iDirect infrastructure. At the physical level, the switch is divided into two distinct logical segments, implemented using VLANs: VLAN10 (labelled UPSTREAM) and VLAN20 (labelled TUNNEL). VLAN20 is used exclusively for the transport of raw, not yet decoded satellite data, which is converted into standard IP packets on arrival at the PP server. This ensures that traffic in this part of the network remains isolated from any processing operations and is not subject to unnecessary interference. VLAN10, or UPSTREAM, on the other hand, handles all management and monitoring functions - this network houses the NMS servers that store iDirect configurations, as well as the PP server interfaces after processing. This keeps management traffic and end-user traffic (processed IP packets) separate, increasing both security and operational transparency. In addition, the switch uses 802.1Q trunking on the ports connecting to the edge routers (R1 and R2), allowing both VLANs to be carried simultaneously over a single physical link, while providing full logical

separation. This separation allows for easy scaling - simply add more PP servers or satellite terminals by connecting them to the appropriate VLAN ports, without having to rebuild the existing topology. As a result, the switch provides not only efficient data flow, but also the flexibility needed to maintain high availability and simple management of the entire iDirect system.

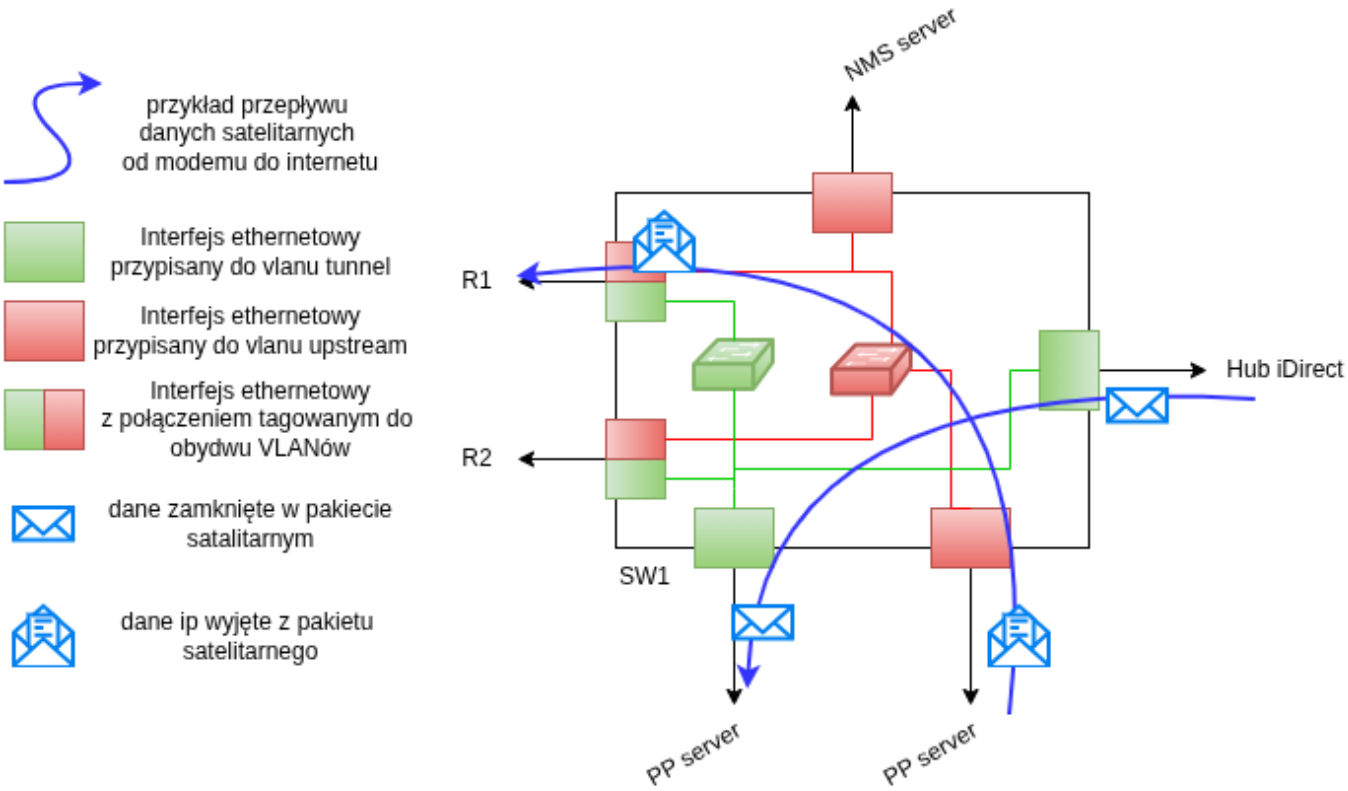


Diagram of the data flow from the satellite platform to the routers [Own elaboration].

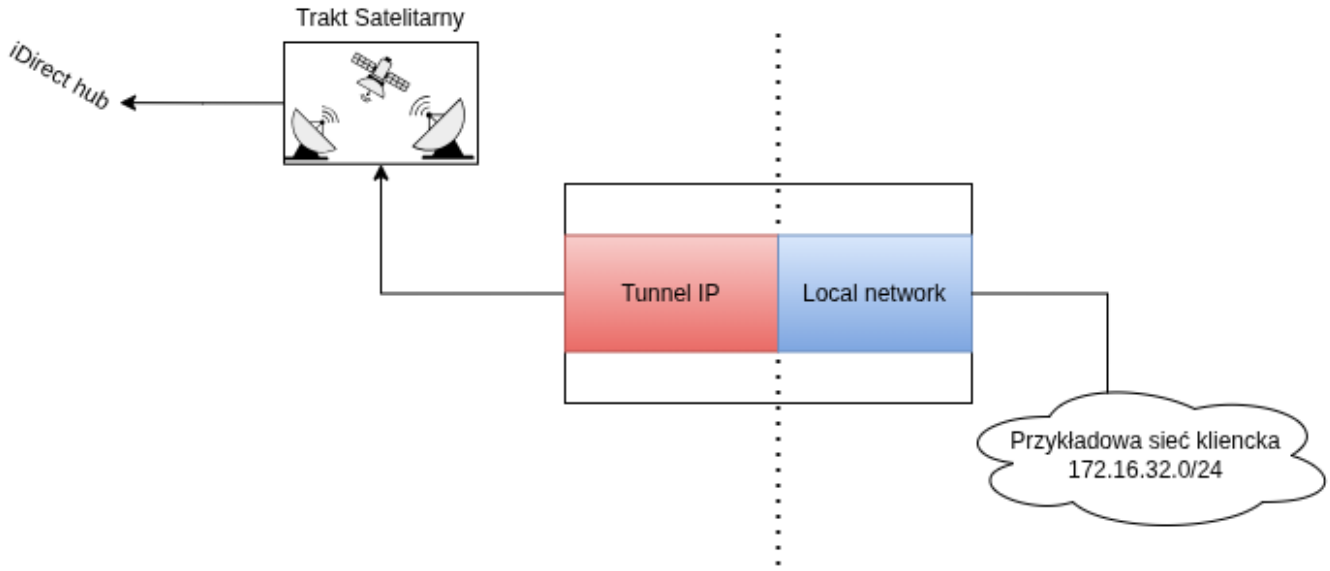
The diagram in Figure13 illustrates the detailed flow of satellite data within the switch, while also showing that in any computer network, traffic is bidirectional - any packet that travels one way must undergo the equally important process of returning in reverse along the way. In the context of the iDirect platform, this means that once a raw satellite packet is received by a VLAN20 (TUNNEL) port, the switch routes it to a PP server, which acts as an intermediary decoding the proprietary iDirect protocol into standard IP packets. Once processed, the packet goes to VLAN10 (UPSTREAM), from where it can be routed to an edge router or NMS server depending on its destination.

A key element of this architecture is that the edge router (Edge) does not have direct access to the satellite terminals located in the TUNNEL network. Instead, the router has to rely on a PP server that broadcasts information about all satellite modem addresses via the dynamic routing protocol RIP. This ensures that the router has entries in its routing table indicating that specific local networks (e.g. `172.16.32.0/24`) are reachable via the address of the PP server.

It is worth noting that each satellite terminal behaves like a separate router - it has its own local network, which it makes available to a client connected to the Ethernet port. This local network is registered with iDirect and forwarded to the PP server and then broadcast to the edge router. In practice, this means that when a packet arrives from the Internet at the router, it is routed to the PP server, which, based on its routing table, sends it to the appropriate satellite terminal via the TUNNEL network. Once it reaches the terminal, the packet is further forwarded to a terminal device on the customer's local network. This process - from the terminal to the PP, on to the router, to the Internet and back again - provides full control over the traffic, enables monitoring and management, and ensures that all network elements remain coherently interconnected despite the physical separation

of the two address domains.

Network partitioning at the satellite terminal



Schematic of network partitioning at a satellite terminal [Own elaboration].

At the stages described so far, there is no address translation - all network segments (tunnel, upstream and local terminal networks) have to exchange packets directly with each other, which enforces full address coordination between them. Analysing the diagram shown in Figure14, it can be seen that the edge router does not know the details of the structure of the local networks connected to the individual satellite modems. This information is provided dynamically through the RIP protocol, whose broadcasts are managed by the PP server. Each satellite modem registers with the iDirect platform on start-up, providing information about its own local network (e.g. `172.16.32.0/24`) and the tunnel address at which it is available (e.g. `192.168.20.10`). The platform informs the PP server, which consequently updates its routing table and broadcasts the new entry to the edge router. A record appears in the router table indicating that the target local network is reachable via the IP address of the PP server on the upstream network (e.g. `192.168.10.111`). At the same time, the PP server retains the information in its own database that the specified upstream address corresponds to a specific tunnel address of the modem, which allows it to route incoming packets back to the correct terminal in the future. Thanks to this mechanism, the router always knows which PP server it needs to send traffic through to reach a specific local network, and the PP server in turn knows the exact tunnel address of the modem that enables the final delivery of the packet to the terminal device on the customer's network. This two-step process - first the local network information passed from the modem to the PP and then from the PP to the router - eliminates the need for manual route configuration and provides automatic, scalable routing exchange across the iDirect infrastructure.

Case study, data flow example

To further illuminate the principle of how data flow works in an iDirect network, let's consider an example of a packet transmission in a network where a satellite terminal will send an ICMP packet. Below is a list of the addresses used for such a case.

1. `8.8.8.8` - example address available on the Internet
2. `192.168.10.0/24` - subnet for upstream VLAN

3. `192.168.20.0/24` - subnet for tunnel VLAN
4. `192.168.10.1` - R1 address in the upstream VLAN
5. `192.168.20.1` - R1 address in the tunnel VLAN
6. `192.168.10.2` - R2 address in upstream VLAN
7. `192.168.20.2` - R2 address in the tunnel VLAN
8. `192.168.10.3` - VRRP address in the upstream VLAN
9. `192.168.20.3` - VRRP address in the tunnel VLAN
10. `192.168.10.111` - PP server interface in the upstream VLAN
11. `192.168.20.111` - PP server interface in the tunnel VLAN
12. `172.16.32.0/24` - client subnet
13. `172.16.32.1` - modem local network address
14. `192.168.20.10` - modem tunnel ip address
15. `172.16.32.254` - client address (e.g. computer connected to satellite terminal)

Let us analyse a situation in which a client connected to a satellite terminal sends an ICMP packet to the address `8.8.8.8`.

1. **The computer** sends an icmp packet to `8.8.8.8`

Source address	Destination address
172.16.32.254	8.8.8.8

2. **Modem** receives this packet, it does not know the destination network so it forwards the packet to its gateway, i.e. the PP server, `192.168.20.111`.

Source address	Destination address
172.16.32.254	8.8.8.8

3. **PP server** receives the packet (in the tunnel network) decodes it from a satellite packet into an IP packet. It then checks the destination network in the routing table, does not know it, so forwards it to its gateway, i.e. the VRRP address (in the upstream network) `192.168.10.3`.

Source address	Destination address
172.16.32.254	8.8.8.8

4. **Routers R1 and R2** receive the packet (in the upstream network) check the destination network which is in the internet, forward the packet to their gateway in the public network masking their address. At this point, for the purposes of this analysis, we will skip the part of the packet passing through the internet and go straight to the packet return stage. Server `8.8.8.8` returns the packet to the public address of the routers, the routers receive it and then swap the addresses back from the connection table passing through NAT.

Source address	Destination address
8.8.8.8	172.16.32.254

   The router has an entry in the RIP routing table (propagated by the PP server) that says that to the network **172.16.32.0/24** is to be accessed by the PP server **192.168.10.111**. So the router passes this back to the PP server.

5. **PP server** receives the packet and according to the RIP routing table has a route that shows

that to the network `172.16.32.0/24` is to be reached via the tunnel ip address of the modem `192.168.20.10`.

Source address	Destination address
8.8.8.8	172.16.32.254

6. **Modem** receives the packet and, according to the table, forwards it to the network that is directly connected to it.

Source address	Destination address
8.8.8.8	172.16.32.254

The above-explained process can be observed in figure 15. In the mentioned figure, all the devices mentioned in the process are shown and annotated next to them with the corresponding addresses in order to visualise the process more easily.

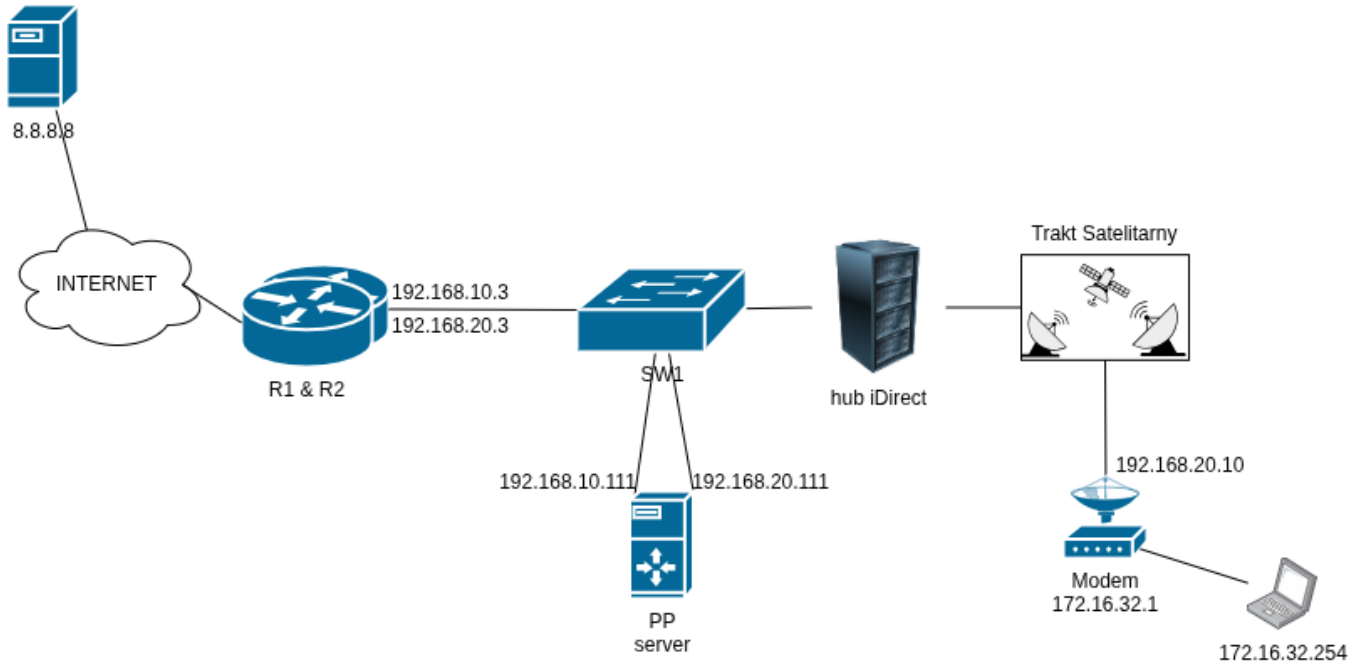


Diagram of the satellite network with addressing [Own elaboration].

Implementation of a compliant configuration

Switch configuration for the iDirect platform

In the previous sections, we discussed the specifics of the platform and data flow. In this section, we will discuss how to configure the iDirect platform switch to allow it to operate on the network used to support the platform.

Below is an analysis of how to configure a switch using the Cisco Catalyst platform as an example. We list the various steps to configure such a device performed in global configuration mode (with prior execution of the commands `enable` and then `configure terminal`)

1. Adding VLANs for upstream and tunnel networks.

```
vlan 10
name UPSTREAM
exit

vlan 20
name TUNNEL
exit
```

1. Setting ports for routers R1 and 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. Example of port configuration for NMS server and 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
```

Router configuration for the iDirect platform

The previous section discussed the configuration of a Layer 2 device, in this section we will discuss the configuration of a router to support the iDirect platform. A MikroTik hardware platform based on RouterOS was chosen to implement this network.

Below is a step-by-step analysis of the configuration performed on routers R1 and R2. Sections of the configuration that do not differ between routers are listed only on the example of router R1, while sections of the configuration that differ between routers are listed twice with an explanation of the differences. Commands were made from a standard terminal available in RouterOS.

1. Renaming interfaces.

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

   Interface named `ether1-WAN` is connected to the Internet. The interface named `ether2-iDX` is connected to switch SW1

2. Adding virtual interfaces on a port `ether2-iDX` for VLAN support.

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

1. VRRP configuration on the interfaces. Configuration on router R1, which is the master router.

```
/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
```

   Configuration on router R2, which is the backup router.

```
/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
```

   The aforementioned configuration consists of three VRRP interfaces.

   - `VRRP1-VLAN10-Upstream`
   - `VRRP2-VLAN20-Tunnel`

- VRRP3-WAN

Each of these interfaces is configured so that the group-authority parameter is the interface VRRP1-VLAN10-Upstream. This means that if the devices stop communicating with each other via the upstream network, VRRP automatically switches to the backup router. Interface VRRP2-VLAN20-Tunnel was not necessary to configure, as there is no gateway requirement for the tunnel network, but it is useful when configuring cards in the iDirect hub. The last interface is VRRP3-WAN this is mainly used to go to the internet via one virtual address of the VRRP interface and in the event of a failover the public address does not change.

2. Enable dynamic RIP routing on the router, on the relevant interfaces.

```
/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. Creating lists of interfaces and adding interfaces to these lists.

```
/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
```

Interfaces were added to groups as follows:
WAN: ether1-WAN, VRRP3-WAN
LAN: VRRP1-VLAN10-Upstream, VRRP2-VLAN20-Tunnel, ether2-iDX, VLAN10-Upstream, VLAN20-Upstream
The interfaces have been allocated in this way because we want them all to be considered as interfaces on the local side or on the public side, in the rules in the firewall, regardless of whether they are virtual or physical interfaces.

2. Addressing interfaces Configuration 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
```

R2 configuration same as above plus the changes listed below:

```
/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
```

Router addressing table [Own elaboration].

Router	**Interface**	**Address**
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. Enabling DNS query forwarding Enabling this function allows you to set the DNS server to the address of the router, for clients. The router then acts as a recursive DNS with its own cache for frequent queries and you can define your own static DNS entries.

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

4. Setting up filtering rules on the firewall

```
/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
```

Below is an explanation of the individual rules, in the order in which they appear in the listings.

- **accept established,related** - rule allowing packets that belong to connections that have already been established or are continuing to be established to pass.
- **drop invalid** - a rule that drops connections that have a connection status of invalid.
- **accept icmp** - a rule that allows ICMP traffic directed to the router.
- **drop all not coming from lan** - rule that blocks all traffic that has a source outside the interfaces on the LAN list and is directed to the router.
- **accept in/out ipsec policy** - two rules which, according to MikroTik documentation, should be implemented so that clients who are connected to the router's LAN can establish ipsec tunnels.
- **fasttrack** - a policy that, according to MikroTik documentation, should be implemented to relieve the router's CPU of packets that are already assigned to existing connections.
- **drop forward invalid** - a rule which is supposed to prevent the router from forwarding packets whose connection status is invalid.
- **drop all from WAN not DSTNATed** - a rule to drop all new connections that have not been added to the port forwarding (DNAT destination translation).

5. Source address translation configuration. The router has been configured so that all packets going out through the interfaces in the WAN list, have their source address masked with a public VRRP address.

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

6. Setting the default route. Address `203.0.113.254` is the gateway address for the public subnet.

```
/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. Configuration of services, time zone, router name and 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
```

The following listed processes performed in the configuration:

- Disabling unused services on the router such as telnet, ftp, www, api. Restricting ssh connections to the router from local networks only.
- Setting the time zone to Europe/Warsaw.
- Setting the router name to IDIRECT-MIKROTIK-X where X is 1 for R1 and 2 for R2.
- Enabling ntp client and ntp server.
- Configuring the ntp client and setting the servers to the main office of measurement.

Equipment used

The equipment used to implement the previously mentioned configurations is:

1. iDirect Evolution series 15100 platform, together with the required transmit and receive cards.
2. iDirect Evolution X3 satellite modem/terminal
3. Dell poweredge R440 servers
4. Cisco Catalyst C9300-24P-M switch

The choice of satellite platform fell on iDirect as it is one of the best supported and best documented platforms for satellite network deployments.

The router was chosen as MikroTik as it has all the features required to support the platform and will allow for possible future expansion of the network with VPN tunnels or route redistribution. Ease of configuration and the author's familiarity with the platform were also not taken into account when selecting this platform.

The switch has no function here other than to split the broadcast domain into two subnets tunnel and upstream. The Catalyst platform was chosen because of its familiarity.

iDirect platform

Evolution series 15100 satellite platform
Source: https://www.idirect.net/

Platform highlights:

- 15100 series can accommodate up to 20 universal or defensive line cards (ULC, DLC).
- Supports up to five satellites
- Supports DVB-S2/DVB-S2X ACM with modulation from QPSK to 256APSK.
- Line cards support up to 119 Msps DVB-S2X forward carriers and Adaptive TDMA on return.
- 48-port Gigabit Ethernet LAN interface supports high carrier symbol rates.
- High levels of redundancy through hub chaining and geographic redundancy.
- Enables host network operator (HNO) and virtual network operator (VNO) configuration.
- Works with high-performance protocol processors and NMS servers for intelligent IP routing and load balancing.

Satellite terminal

iDirect Evolution X3 satellite modem/terminal
Source: https://www.idirect.net/

Maximum performance achieved for the iDirect Evolution X3 modem:

- 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

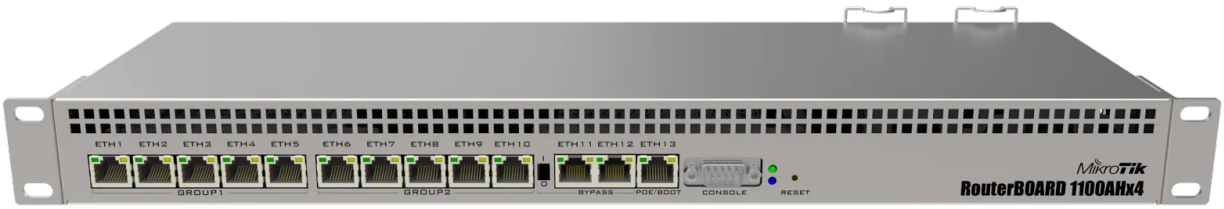
PP and NMS servers

Dell poweredge R440 server
Source: https://www.dell.com/

Switch

Cisco Catalyst C9300-24P-M switch
Source: https://www.cisco.com/

Routers



Mikrotik RB1100AHx4 router
Source: https://mikrotik.com/

Summary and conclusions

The network design presented in this thesis is the minimum functional requirements for the network that needs to be deployed to support the basic functions of the iDirect platform. This network is already in place at the time of writing and supports several satellite stations.

The test environments and configurations presented in this thesis were intended to illuminate the operation of satellite networks and show how such networks are implemented. This objective has been realised using the example of a satellite network design containing the required number of components to support such a network.

Directions for future research

The iDirect platform is an advanced solution that provides exceptional flexibility in terms of network configuration. With this platform, it is possible to set up the telecommunications infrastructure in such a way that the satellite provider is connected to the customer's main location via a dedicated fibre link, while all subordinate offices are integrated via satellite links. This unique architecture allows for the implementation of innovative solutions and better management of resources, providing an excellent basis for future research and development.

Based on the results achieved in this thesis, there is scope for expansion or further research, which could include the following areas.

Expansion of the security infrastructure

Additional security measures based on VPN tunneling technologies are envisaged. VPN tunneling allows for secure connections between remote locations and the head office, which is crucial for the protection of sensitive data and communications. Today's business needs and the intensification of cyber attacks make strengthening network security using VPN technology a priority, especially in situations where employees work remotely.

The use of public addressing

Another development is the use of public addressing on client devices and the redistribution of RIP protocol routes to BGP. The implementation of such solutions can benefit customers who can be assigned a public IP address with this network structure.

Development of network load simulation

Last, but not least, is the development of additional network load simulations. The creation of simulation models will allow a better understanding of the system response under different loads, especially in the context of the increasing number of users and devices connected to the network. Through this research, it will be possible to identify potential bottlenecks and optimise the infrastructure, which will have an impact on the quality of services provided and end-user satisfaction.

Summary

The future of satellite technology research and terrestrial network infrastructure is made up of many, diverse elements that together form a comprehensive network of telecommunications services. The use of innovative security, routing and load simulation solutions can significantly improve network performance and security. Further research should focus on integrating these technologies in a way that meets the growing needs of users and contributes to the sustainability of the telecommunications infrastructure.