JURNAL ILMIAH MERPATI VOL. 12, NO. 3 DECEMBER 2024 p-ISSN: 2252-3006
e-ISSN: 2685-2411

Design and Implementation of Point to Point Wireless Network with VPN IPSec and GRE Security for Internet Network Distribution in Sulangai Village

Agus Budiman Wiranata[a1], Gusti Made Arya Sasmita[a2], I Made Sunia Raharja[a3]
[a]Information Technology Department, Faculty of Engineering, Udayana University, Bali, Indonesia
e-mail: [1]agusbudiman186@gmail.com, [2]aryasasmita@unud.ac.id, [3]sunia.raharja@unud.ac.id

Abstrak

Desa Sulangai menghadapi keterbatasan akses internet akibat kondisi geografisnya di wilayah pegunungan, yang membuat infrastruktur kabel seperti fiber optik sulit diterapkan. Solusi yang diusulkan adalah jaringan wireless point-to-point dengan metode Network Development Life Cycle (NDLC), meliputi analisis, desain, simulasi, implementasi, monitoring, dan manajemen. Hasil pengujian menunjukkan kekuatan sinyal -69 dBm pada Base Station dan Client Station, kategori sangat baik. Setelah implementasi keamanan menggunakan VPN IPsec dan GRE, performa jaringan tetap stabil dengan throughput pagi 53373 Kbps dan siang 57520 Kbps, packet loss 0,16%, delay 0,14 ms, dan jitter 0,14 ms, semuanya masuk kategori sangat baik. Analisis QoS menunjukkan peningkatan signifikan, dengan indeks kualitas layanan mencapai 4 (sangat memuaskan) membuktikan bahwa solusi ini efektif dalam menyediakan akses internet yang aman dan handal.

Kata kunci: *GRE, Internet, Jaringan Wireless Point-to-Point, Network Development Life Cycle, Quality of Service, VPN IPSec*

Abstract

Sulangai Village faces limited internet access due to its geographical conditions in the mountainous area, which makes it difficult to implement cable infrastructure such as fiber optics. The proposed solution is a point-to-point wireless network with the Network Development Life Cycle (NDLC) method, including analysis, design, simulation, implementation, monitoring, and management. The test results showed a signal strength of -69 dBm at the Base Station and Client Station, a very good category. After implementing security using VPN IPsec and GRE, network performance remained stable with a morning throughput of 53373 Kbps and an afternoon of 57520 Kbps, packet loss of 0.16%, delay of 0.14 ms, and jitter of 0.14 ms, all in the very good category. QoS analysis showed a significant improvement, with a service quality index reaching 4 (very satisfactory) proving that this solution is effective in providing secure and reliable internet access.

Keyword: *GRE, Internet, IPSec VPN, Network Development Life Cycle, Point-to-point wireless network, Quality of Service*

1. Introduction

The Indonesian Internet Service Providers Association (APJII) shows that Indonesian internet users in 2024 will reach 221,563,479 people out of a total population of 278,696,200 Indonesians in 2023. A total of 57,132,71 Indonesians are not yet connected to the internet [1]. This obstacle is felt in areas classified as underdeveloped, frontier and outermost which can be called 3T. Sulangai Village is in Petang District, Badung Regency, located in a mountainous area with an altitude of ± 600 meters above sea level, facing similar challenges as those experienced by other 3T areas. The point-to-point wireless network is a solution to overcome the problem of limited internet access in Sulangai Village. Sulangai village has geographical conditions in a mountainous area so that the implementation of network infrastructure in cable media is very difficult, because it does not have adequate facilities. Point to point wireless network technology service providers can build internet network infrastructure with wireless links or wireless can reach areas that experience problems in computer network cable infrastructure such as fiber optics or the absence of internet infrastructure.

The point-to-point wireless network is a solution to overcome the problem of limited internet access in Sulangai Village. Sulangai village has geographical conditions in a mountainous area so that the implementation of network infrastructure in cable media is very difficult, because it does not have adequate facilities. Point to point wireless network technology service providers can build internet network infrastructure with wireless links or wireless can reach areas that experience problems in computer network cable infrastructure such as fiber optics or the absence of internet infrastructure. A point-to-point wireless network is a condition where two points are connected directly wirelessly and allows two LAN lines to be connected in bridge mode without carrying out the routing process [2].

Point-to-point wireless networks are vulnerable to various cyber attacks, including Denial of Service, malware, Man in the Middle, Stream Attack, and Spoofing. Computer network security has an important role in the computer network environment, network security has an important foundation in protecting information, systems and network infrastructure from various threats and risks of cyber attacks. Network security is a set of practices to prevent damage, threats and unauthorized access to computer networks. The aim of computer network security is to ensure that information sent over the network can only be accessed by authorized parties and to maintain the integrity of the information by ensuring that the information is not changed and protecting the computer network from attacks [3]. There are several network security practices that can be applied to point-to-point wireless networks, especially Virtual Private Network – Internet Protocol Security and Generic Routing Encapsulation. Virtual Private Network – Internet Protocol Security is a computer network security technology for securing network communications by creating encrypted tunneling on the internet. Generic Routing Encapsulation is a computer network security technology with tunneling to send information between two points in the network [4].

Research in 2017 study at the State University of Jakarta addressed the problem of the absence of fault tolerance on backbone lines that are susceptible to overload, which can be detrimental to institutions. The solution was to build a point-to-point wireless network as a preventive measure. The test results showed good performance with 0% packet loss, a signal strength of -64.75 dBm, and a throughput of 11.15 Mbps [2].

Research on point-to-point network security optimization using VPN IPSec and GRE through GNS3 simulation. The results show that IPSec has higher security with a throughput of 0.878 Mbps and an average ping of 75 ms, while GRE is simpler with a throughput of 1.060 Mbps and an average ping of 78 ms. Both support stable connections without request time out (RTO). IPSec is suitable for high security, while GRE is more flexible for simple network needs [4].

Research in 2020 in Trimodadi Village addressed the difficulty of internet access due to the inaccessibility of fiber optic cables and expensive cellular packages during the COVID-19 pandemic. The solution is a point-to-point wireless network that provides fast and affordable internet. Measurement results showed good signal quality (-73 dBm) and an average bandwidth of 9.3 Mbps out of a total of 10 Mbps, with 90% efficiency [5].

Research on the implementation of point-to-point wireless networks at PT. Sinar Mulia Plasindo Lestari to overcome communication difficulties and share data between the head office and branches 800 meters away without an internet connection. The test results showed an average transfer bandwidth of 17.6 Mbps, receive 10.6 Mbps, average Ping Speed 26.8 Mbps, 500 ms interval of 2.9 Mbps, and Tx/Rx signal strength -70/-69 dBm [6].

Research on the implementation of point-to-point wireless networks at SMA UNKLAB to overcome the constraints of pulling cables to the NOC. The results show a signal quality of AirMax Quality 96% and AirMax Capacity 88%. Connectivity testing shows stable ping to the gateway and the internet, with PCQ implementation to divide bandwidth evenly to clients [7].

A 2020 study analyzed the quality of point-to-point wireless networks at PT. Bukit Asam TBK Tanjung Enim to support data processing and information exchange. Measurements in the MCC area showed the highest download percentage at the Watrik Container during peak hours

(50.2%) and the lowest during off-peak hours (25.9%). The highest average delay reached 85 ms (very good category), and the highest packet loss of 6% occurred at the Watrik Container during peak hours (09:00-11:00) [8].

2. Research Method / Proposed Method

The research method used in this research is the Network Development Life Cycle (NDLC) method. Network Development Life Cycle is a research method as a guide for developing and designing computer networks [9].

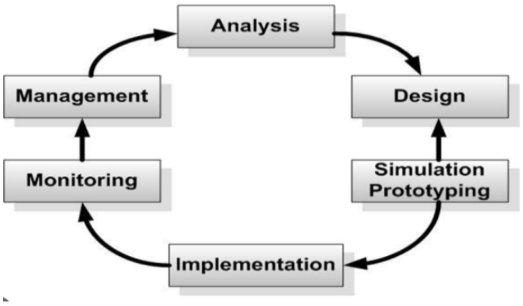


Figure 1. Research Method Network Development Life Cycle

Figure 1 is an image of the stages of the NDLC model used in this research. The stages of the NDLC research method consist of 6 stages, namely analysis, design, simulation prototyping, implementation, monitoring, and management. The six stages are interrelated because they have a sequential flow and steps.

2.1 Network Topology

The network topology design will show the network design that will be used in Sulangai Village. Topology design will describe how each computer network device is connected to each other. The following is a physical network topology design that will be used in Sulangai Village.

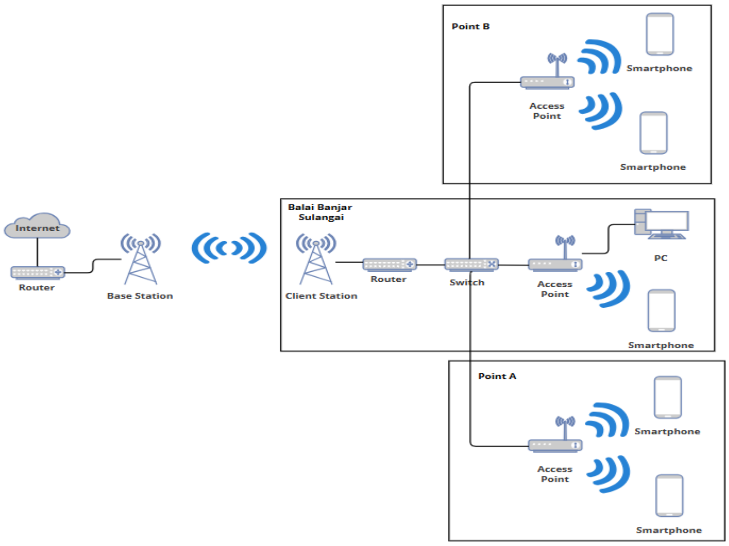


Figure 2. Network Topology Sulangai Village

Figure 2 shows the physical network topology design in Sulangai Village. The base station on the left side sends internet to Balai Banjar Sulangai as a client station. The client station is connected to the router, then distributed via switch to three access points at Balai Banjar, Point A, and Point B. The network distribution mapping is shown in the image below.

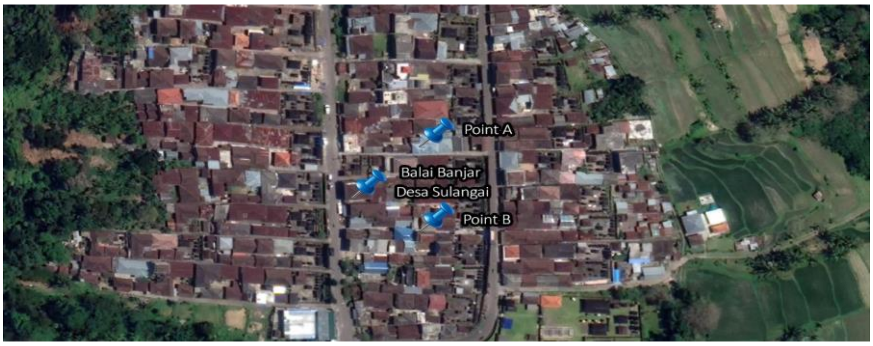
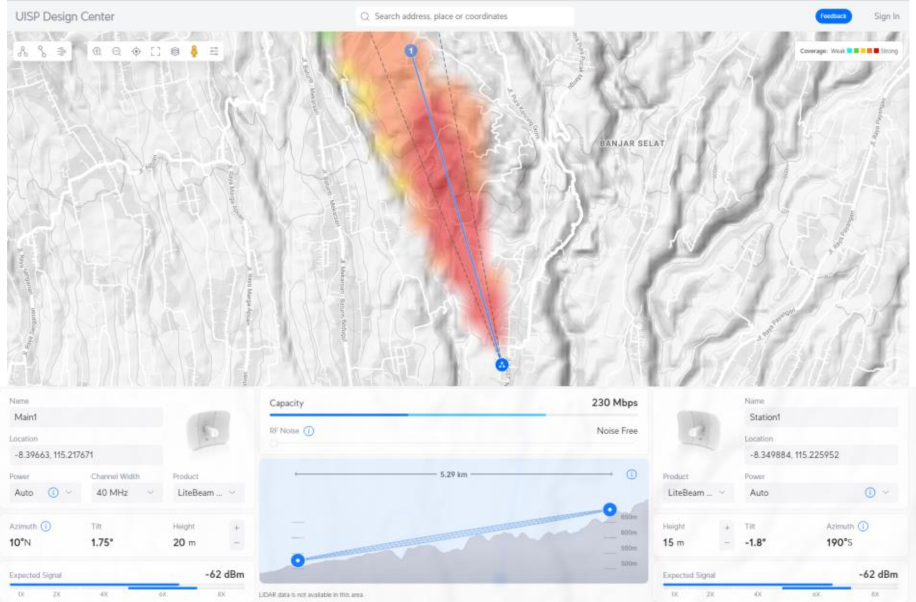


Figure 3. Illustration of Network Distribution Mapping

Figure 3 depicts the network distribution mapping in Sulangai Village with three main points, Balai Banjar Sulangai, Point A, and Point B. Balai Banjar functions as a client station to receive signals from the base station as well as being the location of routers, switches and access points. Access points at Point A and Point B help expand network coverage in Sulangai Village. Internet network distribution in Sulangai village is carried out using the voucher method with bandwidth limits of 2 types, namely 1 Mbps and 2 Mbps.

2.2 Wireless Point to Point Simulation

Point-to-point wireless network simulation is a crucial step in designing and implementing efficient wireless communication systems. This process involves modeling various network elements, including hardware, operating frequencies, and environmental conditions.



Name: Main1
Location: -8.39663, 115.217671
Power: Auto
Channel Width: 40 MHz
Product: LiteBeam ...
Azimuth: 10°N
Tilt: 1.75°
Height: 20 m
Expected Signal: -62 dBm

Capacity: 230 Mbps
RF Noise: Noise Free
5.29 km

Name: Station1
Location: -8.349884, 115.225952
Product: LiteBeam ...
Power: Auto
Height: 15 m
Tilt: -1.8°
Azimuth: 190°S
Expected Signal: -62 dBm

Figure 4. Wireless Point to Point Simulation

Figure 4 shows a point-to-point wireless simulation using the Airlink UBNT application. The simulation determines the location of the base station at the Petang Subdistrict Office and the client station at Balai Banjar Sulangai (2 floors), with a distance of ±5.29 km. The base station uses a 20 meter high pole, while the client station has a total height of 15 meters (5 meter pole and 10 meter building). The antenna device used is the LiteBeam 5ac, whose specifications are similar to the LHG 5nD. The simulation aims to ensure the feasibility of infrastructure at the location and adapt to the geographical conditions of Sulangai Village which is in the mountains (600 meters above sea level). The simulation results show an expected signal of -62 dBm, so that the implementation of a point-to-point wireless network is very possible.

3. Literature Study

Literature study is a way to solve problems by tracing written sources that have been written before. Study literature is obtained from journals, books, the internet and data sheets to create ideas and concepts in research.

3.1 Point to Point

Point-to-point is a condition where there is a direct connection between two nodes without involving intermediaries or other nodes. Point-to-point networks allow direct connection between two Local Area Network lines using bridge mode without the need to go through a routing process [2]. Point-to-point wireless networks use radio links to create a connection between two locations.

3.2 IPSec

Internet Protocol Security, abbreviated as IPSec, is a computer network security protocol with the aim of protecting datagram transmission in a TCP/IP-based network. IPsec uses tunneling technology to encrypt data at a level parallel to the IP protocol ensuring secure delivery of information over the internet or intranet. IPSec utilizes three protocols in the form of Header Authentication (HA), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE). These three protocols aim to provide encryption, authentication and key exchange management functions [10].

3.3 Generic Routing Encapsulation

Generic Routing Encapsulation is a tunneling protocol that has the ability to carry more than one type of communication addressing protocol. Generic Routing Encapsulation process by wrapping or encapsulating all packets into one package with the Internet Protocol addressing system. The packet is sent via a tunnel system that works on the Internet Protocol communication protocol. Generic Routing Encapsulation does not have a data encryption system so it is necessary to add a more secure protocol to protect data [11].

3.4 Line of Sight

Line of Sight is a method of sending information where there are no obstacles between connected terminals, so the signal can go directly from the sender to the receiver. Application in line of sight conditions is very rare, there are several factors that influence line of sight communication including fading, free space attenuation, reflections, and atmospheric conditions [12].

3.5 Signal Strength Measurement

Signal quality is based on a number of factors, including output power from the transmitter, sensitivity of the receiver, path loss from the transmitter to the receiver. Signal strength is expressed in decibels (dB), due to the low power level, and free space attenuation. The following is a level scale for signal strength based on the Received Signal Strength Indicator (RSSI) and Key Perfomance Indicator (KPI) [13],[14].

Table 1. Signal Strength Rating Scale

Signal Strength Value (dBm)	Category	Index
>-60	Very Good	5
-60 s/d -70	Good	4
-71 s/d -80	Average	3
-81 s/d -90	Bad	2
<-90	Very Bad	1

Table 2. Signal to Noise Scale

Value dB	Category
<30 - >15	Very Good
<15 - >0	Good
<0 - >-5	Average
<-5- >-11	Bad
<-11 - >20	Very Bad

3.6 Quality of Service

Quality of Service is a measurement method used to evaluate how well a network performs and defines the characteristics and properties of certain services. . Some Quality of Service parameters that are generally used are delay, jitter, packet loss, and throughput. The following are TIPHON standards for Quality of Service [15].

Table 3. QoS Percentage and Value

Value	Precentage (%)	Index
3,8 - 4	95 - 100	Very Satisfactory
3 - 3,79	75 - 95,75	Satisfying
2 - 2,99	50 - 74,75	Less Satisfactory
1 - 1,99	25 - 49,75	Not Satisfactory

3.6.1 Throughput

Throughput is a level of achievement that can be calculated from bandwidth, where the higher the bandwidth value, the greater the resulting throughput. Throughput can be thought of as the effective speed of data transfer, measured in bits per second (bps) [15].

Table 4. Category Throughput

Category Throughput	Throughput (kbps)	Index
Very Good	>2100 Kbps	4
Good	700-2100 Kbps	3
Average	338 – 700 Kbps	2
Bad	0 – 338 Kbps	1

3.6.2 Packet Loss

Packet loss is a packet that has a time limit. Packages that have passed the time limit must be discarded. Packet loss is an indicator that reflects a situation where packet loss occurs due to collisions and congestion in the network [15].

Table 5. Category Packet Loss

Category Packet Loss	Packet Loss	Indeks
Very Good	0% - 2%	4
Good	3% - 14%	3
Average	15% -24%	2
Bad	>25%	1

3.6.3 Delay

Delay is the time required for a data or information packet to be sent from source to destination. Factors that influence delay include distance, transfer media, and processing time to the destination [15].

Table 6. Category Delay

Category Delay	Delay (ms)	Index
Very Good	< 150	4
Good	150 – 300	3
Average	300 – 450	2
Bad	>450	1

3.6.4 Jitter

Jitter is a variation of delay time and includes the difference between the delay and the next delay. The higher the traffic volume in the network will cause congestion, so the jitter value will also increase [15].

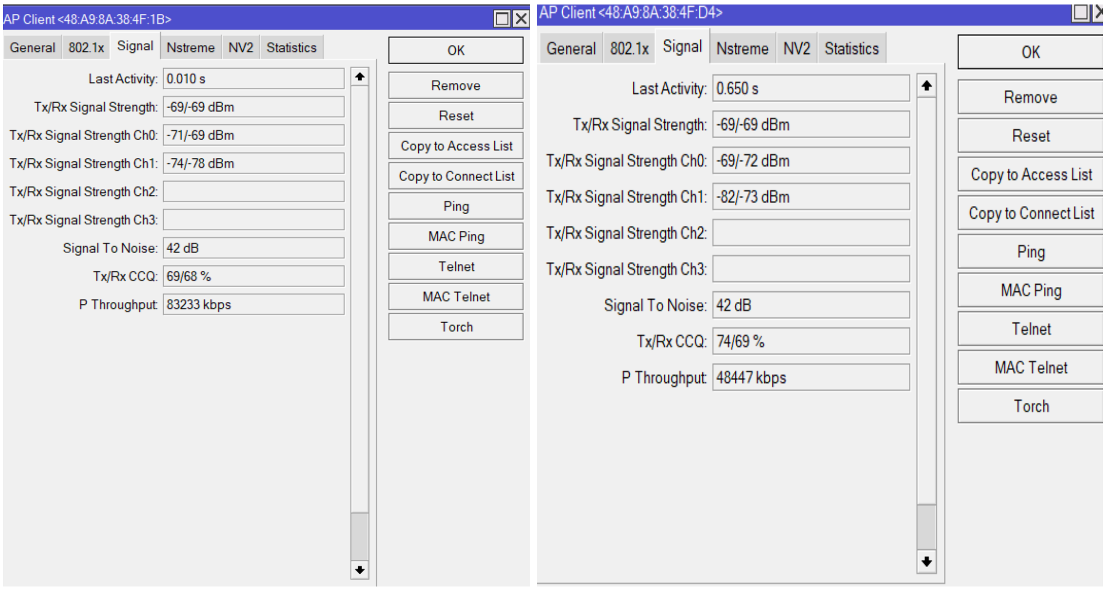
Table 7. Category Jiiter

Category Jitter	Jitter (ms)	Index
Very Good	0	4
Good	1 – 75	3
Average	76 – 125	2
Bad	>125	1

4. Result and Discussion

4.1 Test Signal Strength

Testing signal strength in implementing a point to point wireless network is a crucial process in determining whether wireless performance is reliable or not. The stronger the signal received, the better and more reliable the connectivity.



AP Client <48:A9:8A:38:4F:1B>

Last Activity: 0.010 s
Tx/Rx Signal Strength: -69/-69 dBm
Tx/Rx Signal Strength Ch0: -71/-69 dBm
Tx/Rx Signal Strength Ch1: -74/-78 dBm
Tx/Rx Signal Strength Ch2:
Tx/Rx Signal Strength Ch3:
Signal To Noise: 42 dB
Tx/Rx CCQ: 69/68 %
P Throughput: 83233 kbps

AP Client <48:A9:8A:38:4F:D4>

Last Activity: 0.650 s
Tx/Rx Signal Strength: -69/-69 dBm
Tx/Rx Signal Strength Ch0: -69/-72 dBm
Tx/Rx Signal Strength Ch1: -82/-73 dBm
Tx/Rx Signal Strength Ch2:
Tx/Rx Signal Strength Ch3:
Signal To Noise: 42 dB
Tx/Rx CCQ: 74/69 %
P Throughput: 48447 kbps

Figure 5. Signal Strength Base Station and Client Station

Figure 5 shows the signal measurement results from the LHG 5nD device at the Client Station, with a signal strength of -69 dBm, signal-to-noise ratio (SNR) 42 dB, and Tx/Rx CCQ 74/69%. The higher the CCQ, the better the connection quality.

Table 8. Signal Strength Results

Station	Signal Value (dBm)	Category	Index
Base Station	-69 dBm	Good	4
Client Station	-69 dBm	Good	4

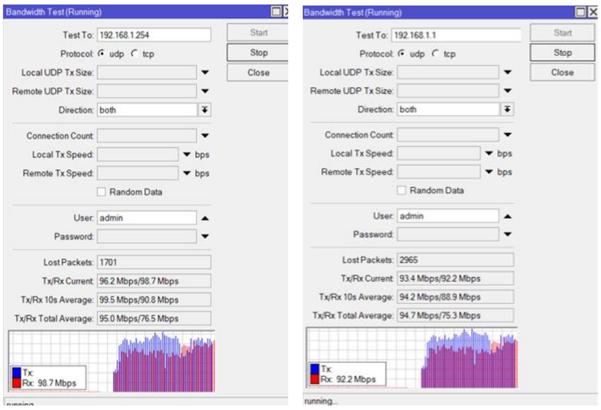
Table 9. Signal To Noise Results

Station	Signal Noise (dB)	Category
Base Station	42 dB	Very Good
Client Station	42 dB	VeryGood

Table 8 shows the signal strength of point-to-point wireless networks with a value of -69 dBm for Base Station and Client Station, including the good category according to RSSI, supporting stable data transmission. Table 9 shows the network signal-to-noise with a value of 42 dB for the Base Station and Client Station, including the very good category according to the KPI.

4.2 Bandwidth Speed Testing

Bandwidth testing is carried out with the aim of assessing the maximum capacity that can be handled by a point-to-point wireless network. This is important to ensure that the network can handle the expected network traffic load.



Bandwidth Test (Running)

Test To: 192.168.1.254
Protocol: ● udp ○ tcp
Local UDP Tx Size:
Remote UDP Tx Size:
Direction: both
Connection Count:
Local Tx Speed: bps
Remote Tx Speed: bps
□ Random Data
User: admin
Password:
Lost Packets: 1701
Tx/Rx Current: 96.2 Mbps/98.7 Mbps
Tx/Rx 10s Average: 99.5 Mbps/90.8 Mbps
Tx/Rx Total Average: 95.0 Mbps/76.5 Mbps

Bandwidth Test (Running)

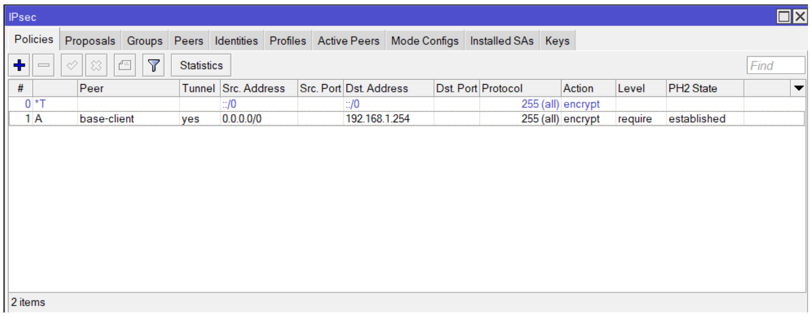
Test To: 192.168.1.1
Protocol: ● udp ○ tcp
Local UDP Tx Size:
Remote UDP Tx Size:
Direction: both
Connection Count:
Local Tx Speed: bps
Remote Tx Speed: bps
□ Random Data
User: admin
Password:
Lost Packets: 2965
Tx/Rx Current: 93.4 Mbps/92.2 Mbps
Tx/Rx 10s Average: 94.2 Mbps/88.9 Mbps
Tx/Rx Total Average: 94.7 Mbps/75.3 Mbps

Figure 6.Speed Test Base Stattion and Client Station

Figure 6 shows the results of bandwidth testing on the Base Station and client station after implementing security using the Mikrotik Bandwidth Test. Base station Tx/Rx speeds currently reach 96.2 Mbps and 98.1 Mbps, with 10-second averages of 99.5 Mbps and 90.8 Mbps, and total averages of 95.9 Mbps and 76.5 Mbps. Client station Tx/Rx speeds are currently recorded at 93.4 Mbps and 92.2 Mbps, with a 10 second average of 94.2 Mbps and 88.9 Mbps, and a total average of 94.7 Mbps and 75.3 Mbps. The stability of network performance can be seen from the uniformity of results without significant fluctuations. These results show stable and consistent network performance without significant fluctuations.

4.3 IPSEC VPN Security Testing

IPsec (Internet Protocol Security) VPN security testing is a critical process to ensure that a private virtual network using the IPsec protocol can provide the expected level of security.

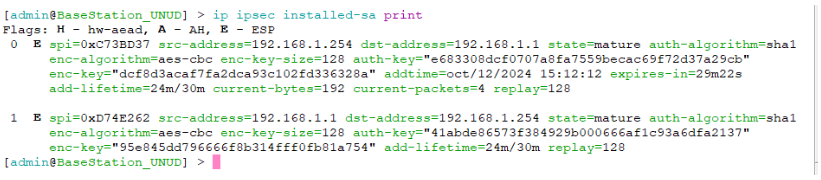


#		Peer	Tunnel	Src. Address	Src. Port	Dst. Address	Dst. Port	Protocol	Action	Level	PH2 State
0	*T			::/0		::/0		255 (all)	encrypt		
1	A	base-client	yes	0.0.0.0/0		192.168.1.254		255 (all)	encrypt	require	established

2 items

Figure 7. PH2 State Testing IPSec VPN Security

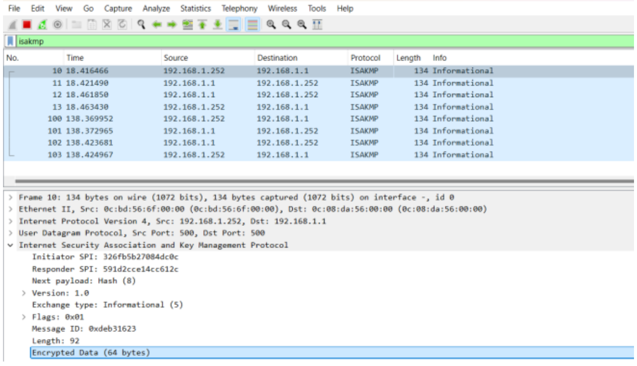
Figure 7 shows an IPsec VPN security test with the status PH2 State established, indicating a successful connection and encrypted network traffic. Column Src. Address (0.0.0.0) indicates all encrypted source addresses, while Dst. Address (192.168.1.254) is the encrypted destination address. This result confirms the success of the IPsec VPN connection between the Base station and Client station.



```
[admin@BaseStation_UNUD] > ip ipsec installed-sa print
Flags: H - hw-aead, A - AH, E - ESP
 0  E spi=0xC73BD37 src-address=192.168.1.254 dst-address=192.168.1.1 state=mature auth-algorithm=sha1
      enc-algorithm=aes-cbc enc-key-size=128 auth-key="e683308dcf0707a8fa7559becac69f72d37a29cb"
      enc-key="dcf8d3acaf7fa2dca93c102fd336328a" addtime=oct/12/2024 15:12:12 expires-in=29m22s
      add-lifetime=24m/30m current-bytes=192 current-packets=4 replay=128

 1  E spi=0xD74E262 src-address=192.168.1.1 dst-address=192.168.1.254 state=mature auth-algorithm=sha1
      enc-algorithm=aes-cbc enc-key-size=128 auth-key="41abde86573f384929b000666af1c93a6dfa2137"
      enc-key="95e845dd796666f8b314fff0fb81a754" add-lifetime=24m/30m replay=128
[admin@BaseStation_UNUD] >
```

Figure 8. Security Associations Output Testing

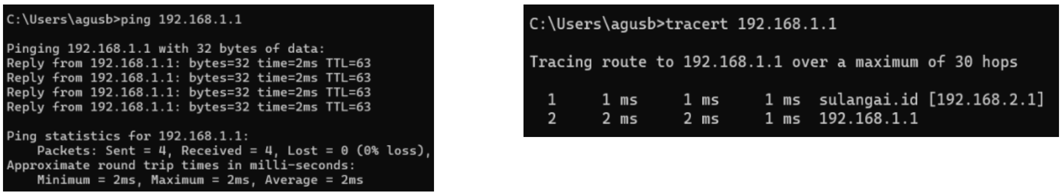
Figure 8 shows an IPsec VPN security test with the Security Association (SA) list installed. The connection between the Base station and Client station was successfully established with security active. The mature status indicates the SA is active and ready to encrypt network traffic.



```
isakmp

No.      Time         Source          Destination     Protocol  Length Info
      10 18.416466    192.168.1.252   192.168.1.1     ISAKMP       134 Informational
      11 18.421490    192.168.1.1     192.168.1.252   ISAKMP       134 Informational
      12 18.461850    192.168.1.1     192.168.1.252   ISAKMP       134 Informational
      13 18.463430    192.168.1.252   192.168.1.1     ISAKMP       134 Informational
     100 138.369952   192.168.1.252   192.168.1.1     ISAKMP       134 Informational
     101 138.372965   192.168.1.1     192.168.1.252   ISAKMP       134 Informational
     102 138.423681   192.168.1.1     192.168.1.252   ISAKMP       134 Informational
     103 138.424967   192.168.1.252   192.168.1.1     ISAKMP       134 Informational

> Frame 10: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface -, id 0
> Ethernet II, Src: 0c:bd:56:6f:00:00 (0c:bd:56:6f:00:00), Dst: 0c:08:da:56:00:00 (0c:08:da:56:00:00)
> Internet Protocol Version 4, Src: 192.168.1.252, Dst: 192.168.1.1
> User Datagram Protocol, Src Port: 500, Dst Port: 500
v Internet Security Association and Key Management Protocol
    Initiator SPI: 326fb5b27084dc0c
    Responder SPI: 591d2cce14cc612c
    Next payload: Hash (8)
  > Version: 1.0
    Exchange type: Informational (5)
  > Flags: 0x01
    Message ID: 0xdeb31623
    Length: 92
    Encrypted Data (64 bytes)
```

Figure 9. Wireshark ISAKMP Protocol Capture Results

Figure 9 is the result of capturing the ISAKMP protocol with the Wireshark application The end of the data capture shows Encrypted data, indicating the package has been secured with an encryption algorithm. Package specific contents cannot be accessed without the encryption key.



```
C:\Users\agusb>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

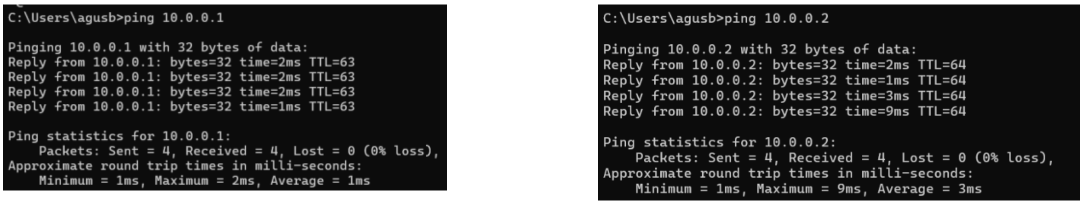
```
C:\Users\agusb>tracert 192.168.1.1

Tracing route to 192.168.1.1 over a maximum of 30 hops

  1     1 ms     1 ms     1 ms  sulangai.id [192.168.2.1]
  2     2 ms     2 ms     1 ms  192.168.1.1
```

Figure 10. Traceroute ang Ping Testing Results

Figure 10 shows IPsec VPN security testing using traceroute and ping from the client to the Base station gateway. The results show that all packets run smoothly, with the base station responding to messages from the client, indicating that the point-to-point wireless network is functioning normally after implementing IPsec VPN security.

4.4 GRE Security Testing

GRE (Generic Routing Encapsulation) security testing is an important process in ensuring that the protocol can secure the data transmitted over the network. The use of GRE is not only to carry out the encapsulation process, but the use of GRE is to support multicast communication which cannot be done by an IPSec VPN which only supports unicast communication.

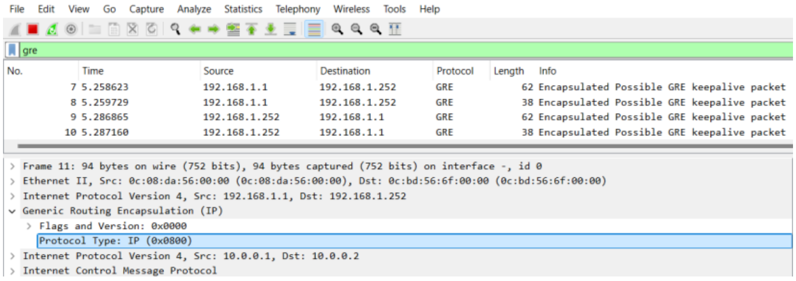


```
C:\Users\agusb>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=63
Reply from 10.0.0.1: bytes=32 time=2ms TTL=63
Reply from 10.0.0.1: bytes=32 time=2ms TTL=63
Reply from 10.0.0.1: bytes=32 time=1ms TTL=63

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
C:\Users\agusb>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=2ms TTL=64
Reply from 10.0.0.2: bytes=32 time=1ms TTL=64
Reply from 10.0.0.2: bytes=32 time=3ms TTL=64
Reply from 10.0.0.2: bytes=32 time=9ms TTL=64

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms
```

Figure 11. Ping GRE Testing Results

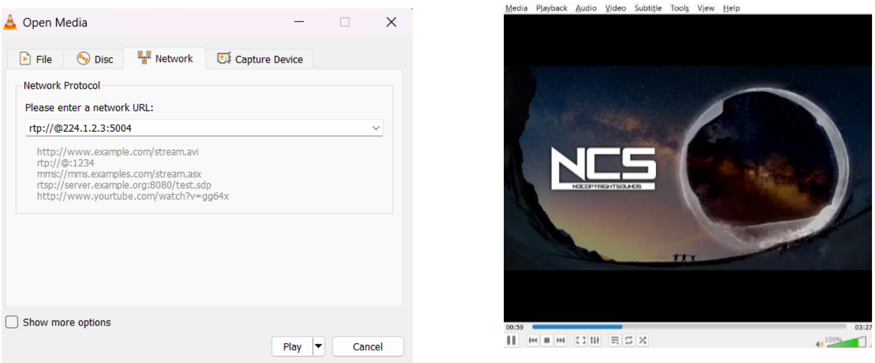
Figure 11 shows GRE security testing by pinging the IP Address of the GRE interface on the Base Station and Client Station. The results show that the client can communicate with the Base Station and Client Station.



```
gre
No.   Time      Source         Destination    Protocol  Length  Info
   7 5.258623  192.168.1.1    192.168.1.252  GRE           62 Encapsulated Possible GRE keepalive packet
   8 5.259729  192.168.1.1    192.168.1.252  GRE           38 Encapsulated Possible GRE keepalive packet
   9 5.286865  192.168.1.252  192.168.1.1    GRE           62 Encapsulated Possible GRE keepalive packet
  10 5.287160  192.168.1.252  192.168.1.1    GRE           38 Encapsulated Possible GRE keepalive packet

> Frame 11: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface -, id 0
> Ethernet II, Src: 0c:08:da:56:00:00 (0c:08:da:56:00:00), Dst: 0c:bd:56:6f:00:00 (0c:bd:56:6f:00:00)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.252
v Generic Routing Encapsulation (IP)
  > Flags and Version: 0x0000
    Protocol Type: IP (0x0800)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 10.0.0.2
> Internet Control Message Protocol
```

Figure 12. GRE Protocol Capture Results

Figure 12 shows the results of capturing the GRE protocol using Wireshark, which displays the GRE protocol active and operating in network traffic. Protocol type IP (0x0800) indicates IPv4 packet encapsulated in GRE. Packets with source IP 10.0.0.1 and destination IP 10.0.0.2 are encapsulated in the GRE tunnel between 192.168.1.1 and 192.168.1.252. GRE allows multicast communications, complementing IPsec VPNs that only support unicast communications.



Network Protocol

Please enter a network URL:

rtp://@224.1.2.3:5004

http://www.example.com/stream.avi
rtp://@:1234
mms://mms.examples.com/stream.asx
rtsp://server.example.org:8080/test.sdp
http://www.yourtube.com/watch?v=gg64x

□ Show more options

Figure 13. Stream Video From Client

Figure 13 shows the VLC Stream Client configuration for accessing video on the client side. Access is carried out by entering network URL in the form of a multicast group IP, for example: rtp://@224.1.2.3:5004. Displays the video stream results on the client side, proving that GRE supports multicast communications. The client successfully received a 24 MB 720p resolution video sent by the server via GRE. All clients in a multicast group can receive the same stream, indicating successful multicast communication.

4.5 QoS Analysis Results Before Security Implementation

Prior to security implementations such as IPsec VPN or GRE, QoS (Quality of Service) measurements aim to ensure network performance, such as speed, latency, jitter, and packet loss rate, meets application or user needs. At this stage, the main focus is to analyze network performance under normal conditions without any overhead from security mechanisms. The QoS testing was conducted in two sessions, namely in the morning and in the afternoon, on weekdays from Monday to Friday.

Table 10. QoS Analysis Results in the Morning Without Bandwidth Limitation Before Security Implementation

Parameter	Value	Index	Category
Throughput (Kbps)	50851 Kbps	4	Very Good
Packet Loss (%)	0,07 %	4	Very Good
Delay (ms)	0,15 ms	4	Very Good
Jitter (ms)	0,15 ms	4	Very Good
Quality of Service		4	Very Satisfactory

Table 11. QoS Analysis Results in the Afternoon Without Bandwidth Limitation Before Security Implementation

Parameter	Value	Index	Category
Throughput (Kbps)	50861 Kbps	4	Very Good
Packet Loss (%)	0,14 %	4	Very Good
Delay (ms)	0.14 ms	4	Very Good
Jitter (ms)	0.14 ms	4	Very Good
Quality of Service		4	Very Satisfactory

4.6 QoS Analysis Results After Security Implementation

Once security is implemented, such as VPN encryption or GRE encapsulation, QoS is measured again to ensure the network continues to provide optimal performance despite additional processes such as encryption or encapsulation. It is important to evaluate the impact of security implementations on latency, throughput, jitter, and packet loss rates. The QoS testing was conducted in two sessions, namely in the morning and in the afternoon, on weekdays from Monday to Friday.

Table 12. QoS Analysis Results in the Morning Without Bandwidth Limitation After Security Implementation

Parameter	Value	Indeks	Category
Throughput (Kbps)	53373 Kbps	4	Very Good
Packet Loss (%)	0,16 %	4	Very Good
Delay (ms)	0.14 ms	4	Very Good
Jitter (ms)	0.14 ms	4	Very Good
Quality of Service		4	Very Satisfactor

Table 13. QoS Analysis Results in the Afternoon Without Bandwidth Limitation After Security Implementation

Parameter	Value	Indeks	Category
Throughput (Kbps)	57520 Kbps	4	Very Good
Packet Loss (%)	0,16 %	4	Very Good
Delay (ms)	0,13 ms	4	Very Good
Jitter (ms)	0,13 ms	4	Very Good
Quality of Service		4	Very Satisfactor

4.7 Qos Comparison After and Before Security Implementation

QoS comparisons are carried out to determine the effect of network quality on various parameters, namely throughput, packet loss, delay and jitter. By comparing the results after and before implementing security, the aim is to show whether implementing security has a significant impact on network performance or not.

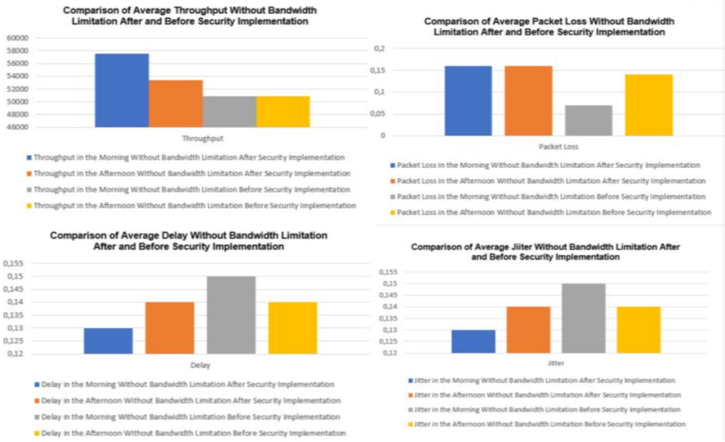


Figure 14. Comparison QoS Without Bandwidth Limitation After and Before Security Implementation

Figure 14 show the average throughput is higher after the security implementation, with 57,520 Kbps in the morning and 53,373 Kbps in the afternoon, compared to before the implementation. The packet loss in the morning and afternoon increased to 0.16% after the security implementation, but it remains in the very good category. The delay in the morning decreased to 0.13 ms after the implementation, while it remained stable at 0.14 ms in the afternoon. The jitter in the morning decreased to 0.13 ms after the implementation, with the afternoon remaining stable at 0.14 ms.

5. Conclusion

Based on the results obtained, the Design and Implementation of Point-to-Point Wireless Network with IPSec Security and GRE VPN for Internet Network Distribution in Sulangai Village showed satisfactory results. Sulangai Village, which is located in the mountains at an altitude of ±600 meters, faces limited telecommunications infrastructure due to uneven topography, thus hampering internet access and the development of a digital society. The network implementation successfully reached a distance of 5.29 km from the base station at the Petang District Office to the client station at the Sulangai Banjar Hall. Measurements showed a signal strength of -69 dBm, which is included in the good category, so that it is able to provide stable internet connectivity. QoS testing without bandwidth limitation shows throughput of 50851–57520 Kbps, packet loss of 0.07–0.16%, delay of 0.13–0.15 ms, and jitter of 0.13–0.15 ms with index 4 (very good category). In addition, IPSec VPN is applied to protect unicast communications with encryption, while GRE is used to support multicast transmission. Multicast video streaming testing showed that the network remained stable without interruption even though the security features were active. In general, high-quality hardware can provide higher throughput, improve connection stability, and extend range by several kilometers compared to standard hardware.

References

[1] APJII, “APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang,” apjii.or.id. Accessed: Nov. 26, 2024. [Online]. Available: https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

[2] M. F. Duskarnaen and F. Nurfalah, “Analisis, Perancangan, Dan Implementasi Jaringan Wireless Point To Point Antara Kampus A Dan Kampus B Universitas Negeri Jakarta,” *PINTER J. Pendidik. Tek. Inform. dan Komput.*, vol. 1, no. 2, pp. 134–141, 2017, doi: 10.21009/pinter.1.2.6.

[3] R. Permana, D. Ramadhani, and I. Lestari, “Proteksi Keamanan Jaringan Komputer di Sekolah Menengah Kejuran Al-Madani Pontianak,” *Int. J. Nat. Sci. Eng.*, vol. 3, no. 1, p. 37, 2019, doi: 10.23887/ijnse.v3i1.22175.

[4] Nana and D. Iskandar Mulyana, “Optimasi Keamanan Jaringan Point to Point Menggunakan VPN IPSec dan GRE,” *J. Jupiter*, vol. 14, pp. 297–305, 2022.

[5] A. Wibowo and Ristyo, “PERANCANGAN DAN IMPLEMENTASI JARINGAN WIRELESS POINT TO POINT UNTUK WARGA DESA TRIMODADI KEC ABUNG SELATAN,” *J. Sist. dan Teknol. Inf.*, vol. 1 No 2, pp. 54–63, 2020, [Online]. Available: https://doi.org/10.47637/sienna.v1i2.348

[6] D. Ichsan and H. Suhendi, “Implementasi Jaringan Wireless Point To Point Antara Kantor Pusat Dan Kantor Cabang Di Pt. Sinar Mulia Plasindo Lestari …,” *eProsiding Tek. Inform. …*, vol. 2, no. 1, pp. 28–36, 2021.

[7] J. Moedjahedy, “Implementasi Point to Point Jaringan Internet Nirkabel di SMA Universitas Klabat,” *CogITo Smart J.*, vol. 2, no. 2, p. 240, 2016, doi: 10.31154/cogito.v2i2.33.240-249.

[8] Y. Fitrisia and M. A. Setianto, “Implementasi GRE Over IPSec Tunnel VPN menggunakan Fortigate,” *J. Komput. Terap.*, vol. 9, no. 2, pp. 212–223, 2023, doi: 10.35143/jkt.v9i2.6097.

[9] Nurfadilah Fitria Fatayana and A. H. Mustika, “Pengembangan Keamanan Jaringan Hotspot Berbasis Mikrotik Menggunakan Otentikasi Pengguna (User) Di Smp Negeri 7 Metro,” *J. Mhs. Ilmu Komput.*, vol. 3, no. 2, pp. 376–384, 2022, [Online]. Available: https://scholar.ummetro.ac.id/index.php/IlmuKomputer/article/view/2838

[10] cisco, “Understand IPsec IKEv1 Protocol,” 2024, [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.pdf

[11] Cisco, “Hardware Compatibility Matrix for Cisco cBR Series Routers,” pp. 1–24, 2024.

[12] I. Campbell Scientific, “Application Note: Line of Sight Obstruction,” *Appl. Note 3RF-E*, p. 18, 2016, [Online]. Available: https://s.campbellsci.com/documents/au/technical-papers/line-of-sight-obstruction.pdf

[13] Veries Industries, “Veris Aerospond Wireless Sensors : Received Signal Strength Indicator (RSSI),” *Vwp* , p. 1, 2018.

[14] J. Petrovitch, “Understand Noise with WiFi SNR,” netally. Accessed: Nov. 17, 2024. [Online]. Available: https://www.netally.com/tech-tips/understand-noise-with-wi-fi-snr/

[15] ETSI, “Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); General aspects of Quality of Service (QoS),” *Etsi Tr 101 329 V2.1.1*, vol. 1, pp. 1–37, 2020.