Indonesian Journal of Interdisciplinary Research in Science and Technology (MARCOPOLO)
Vol. 2, No. 4, 2024 : 415 - 436

Multicast Radar Data Transmission Using the Tunnel in Tunnel Method and IGMP (Internet Group Management Protocol) Filtering by Utilizing the Internet Network

Ekky Widha Atmaka[1]*, Adhitya Wisnu Hartoko[2]
[1]Perum LPPNPI Cabang Manado
[2]Perum LPPNPI Cabang Halim
Corresponding Author: Ekky Widha Atmaka ekkyatmaka01@yahoo.com

A R T I C L E I N F O

Keywords : Transmisi Data, Radar Multicast, IGMP

Received : 03 March
Revised : 18 March
Accepted: 20 April

©2024 Atmaka, Hartoko: This is an open-access article distributed under the terms of the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

This research proposes the implementation of multicast radar data transmission using the tunnel in tunnel method by utilizing the installed IP VPN network. The background of this study is the failure in radar data transmission resulting in a change of service from surveillance to procedural service, as well as the impact of the Covid-19 pandemic on aviation organizations. The purpose of this implementation is to enhance flight safety while achieving cost efficiency for the company. Objectives include changing transmission methods, budget efficiency, improving operational safety, compliance with international standards, and support for the concept of flight information management. Advantages of multicast radar data transmission include centralized IP base, ease of monitoring, and the use of FO converters for surge protection. Implementation is based on aviation regulations, international standards, and partnership contracts. Contingency plans cover network and device failure scenarios. Cost benefit analysis shows significant financial gains from this implementation. It is hoped that this research will make a positive contribution to improving efficiency and operational safety in aviation.

DOI: https://doi.org/10.55927/marcopolo.v2i4.8836
E-ISSN : 2986-8009
https://journal.formosapublisher.org/index.php/marcopolo

Transmisi Multicast Data Radar Menggunakan Metode Tunnel in Tunnel dan IGMP (Internet Group Management Protocol) Filtering dengan Pemanfaatan Jaringan Internet

Ekky Widha Atmaka[1]*, Adhitya Wisnu Hartoko[2]
[1]Perum LPPNPI Cabang Manado
[2]Perum LPPNPI Cabang Halim
Corresponding Author: Ekky Widha Atmaka ekkyatmaka01@yahoo.com

A R T I C L E I N F O

Kata Kunci: Transmisi Data, Radar Multicast, IGMP

Received : 03 Maret
Revised : 18 Maret
Accepted: 20 April

©2024 Atmaka, Hartoko: This is an open-access article distributed under the terms of the Creative Commons Atribusi 4.0 Internasional.

A B S T R A K

Penelitian ini mengusulkan implementasi transmisi data radar multicast menggunakan metode tunnel in tunnel dengan memanfaatkan jaringan IP VPN yang telah terinstalasi. Latar belakang studi ini adalah kegagalan dalam transmisi data radar yang mengakibatkan perubahan layanan dari surveilans menjadi layanan prosedural, serta dampak pandemi Covid-19 terhadap organisasi penerbangan. Maksud dari implementasi ini adalah meningkatkan keselamatan penerbangan sambil mencapai efisiensi anggaran perusahaan. Tujuan meliputi perubahan metode transmisi, efisiensi anggaran, peningkatan keselamatan operasional, kepatuhan terhadap standar internasional, dan dukungan terhadap konsep manajemen informasi penerbangan. Kelebihan transmisi data radar multicast mencakup sentralisasi IP base, kemudahan pemantauan, dan penggunaan coverter FO untuk proteksi lonjakan tegangan. Dasar pelaksanaan mencakup regulasi penerbangan, standar internasional, dan kontrak kerja sama. Rencana kontingensi mencakup skenario kegagalan jaringan dan perangkat. Analisis cost benefit menunjukkan keuntungan finansial yang signifikan dari implementasi ini. Diharapkan penelitian ini memberikan kontribusi positif dalam meningkatkan efisiensi dan keselamatan operasional penerbangan.

PENDAHULUAN

Sebuah program peningkatan pelayanan berbasis surveillance telah diimplementasikan dalam wilayah tertentu oleh Perusahaan Umum Lembaga Penyelenggara Navigasi Penerbangan Indonesia (Perum LPPNPI) atau yang lebih dikenal dengan AirNav Indonesia, dimana pelayanan ini diberikan oleh suatu lembaga atau organisasi yang relevan. Program ini bertujuan untuk meningkatkan efisiensi dan keamanan dalam pemanduan lalu lintas penerbangan dengan mentransmisikan data radar dari satu lokasi ke lokasi lainnya menggunakan teknologi VSAT. Namun, dalam beberapa kasus, terjadi kegagalan dalam transmisi data radar yang mengakibatkan perubahan dalam pelayanan dari layanan surveilans menjadi layanan prosedural. Kegagalan ini umumnya disebabkan oleh gangguan pada sistem transmisi VSAT, yang menghasilkan perubahan yang signifikan dalam layanan selama jangka waktu tertentu.

VSAT adalah singkatan dari "*Very Small Aperture Terminal*". Ini adalah teknologi komunikasi satelit yang digunakan untuk menghubungkan titik-titik terpencil atau jarak jauh dengan jaringan komunikasi global. VSAT menggunakan terminal kecil dengan antena parabola yang biasanya berdiameter antara 75 cm hingga 2,4 meter. Terminal ini dipasang di lokasi pengguna, seperti di gedung, kapal, atau stasiun bumi, dan dihubungkan dengan satelit komunikasi. Berikut adalah beberapa komponen utama dari sistem VSAT:

1. Antena, dimana hal ini merupakan sebuah antena parabola kecil digunakan untuk mengirim dan menerima sinyal dari dan ke satelit. Ukuran antena dapat bervariasi tergantung pada aplikasi dan lokasi pengguna.
2. Transceiver, kata transceiver ini adalah perangkat elektronik yang terdiri dari transmitter dan receiver. Ini mengubah sinyal radio dari data digital yang dihasilkan oleh komputer atau perangkat lain menjadi sinyal radio analog untuk transmisi melalui antena, dan sebaliknya.
3. Modem, yang mana modem ini digunakan untuk mengonversi sinyal digital dari komputer atau perangkat lain menjadi sinyal yang cocok untuk transmisi melalui antena. Ini juga melakukan fungsi modulasi dan demodulasi untuk mentransfer data secara efisien melalui saluran komunikasi.
4. Satelit, yang sebagaimana dimaksud adalah VSAT menggunakan satelit komunikasi yang melayani jangkauan geografis tertentu untuk mentransfer data antara terminal pengguna dan pusat jaringan. Satelit-satelit ini biasanya ditempatkan di orbit geostasioner atau orbit bumi rendah.
5. Pusat Jaringan, juga dikenal sebagai "hub", merupakan pusat kontrol untuk jaringan VSAT. Ini mengelola semua terminal pengguna, mengarahkan lalu lintas data antara terminal, dan menghubungkan jaringan VSAT dengan jaringan telekomunikasi lainnya, seperti internet atau jaringan pribadi perusahaan.

Keuntungan utama dari teknologi VSAT termasuk kemampuannya untuk menyediakan konektivitas yang andal dan cepat di daerah terpencil atau sulit dijangkau, fleksibilitas dalam skala implementasi dari beberapa terminal hingga ribuan terminal, serta kemampuannya untuk mendukung berbagai aplikasi, termasuk telekomunikasi, internet, dan jaringan perusahaan. Namun, biaya awal dan keterbatasan bandwidth seringkali menjadi tantangan dalam penerapan teknologi ini.

Sebagai tambahan, situasi pandemi Covid-19 telah memberikan dampak yang luas dan serius, baik secara sosial maupun ekonomi, tidak hanya pada individu tetapi juga pada organisasi yang terlibat dalam penyediaan layanan penerbangan. Dalam menghadapi tantangan ini, diperlukan upaya untuk mengurangi beban finansial organisasi tanpa mengorbankan standar keselamatan operasi penerbangan. Oleh karena itu, diperlukan inovasi-inovasi baru yang dapat membantu meminimalkan biaya operasional sambil tetap memastikan tingkat keselamatan yang optimal.

Salah satu solusi yang diusulkan untuk mengatasi masalah kegagalan dalam transmisi data radar adalah dengan mengimplementasikan sistem transmisi data multicast menggunakan metode tunnel in tunnel melalui jalur *Virtual Private Network* (VPN) yang tersedia.

Transmisi data multicast adalah metode pengiriman data di jaringan komputer di mana satu sumber data mengirimkan informasi ke beberapa tujuan sekaligus. Ini berbeda dengan transmisi unicast, di mana data hanya dikirimkan ke satu tujuan, dan transmisi broadcast, di mana data dikirimkan ke semua perangkat dalam jaringan. Berikut adalah detail tentang transmisi data multicast:

1. Sumber Data, dimana Transmisi data multicast dimulai dengan sumber data, yang bisa berupa server, router, atau perangkat lain yang memiliki informasi yang ingin dibagikan kepada beberapa penerima.
2. Alamat Multicast yang ada di dalam jaringan, setiap grup penerima memiliki alamat multicast unik yang digunakan untuk mengidentifikasi mereka. Alamat ini adalah alamat IPv4 atau IPv6 yang khusus digunakan untuk multicast. Dalam IPv4, alamat multicast dimulai dengan angka 224.x.x.x hingga 239.x.x.x. Dalam IPv6, alamat multicast dimulai dengan "ff".
3. Penerima, yang dimaksud penerima adalah perangkat atau aplikasi yang ingin menerima data yang dikirimkan oleh sumber multicast. Penerima dapat berada di satu atau lebih jaringan yang terhubung ke jaringan sumber.
4. Protokol Multicast, yaitu untuk mengatur pengiriman dan pengelolaan data multicast, protokol khusus digunakan. Salah satu yang paling umum digunakan adalah Internet Group Management Protocol (IGMP) untuk IPv4 dan Multicast Listener Discovery (MLD) untuk IPv6. Protokol ini memungkinkan penerima untuk bergabung dengan atau meninggalkan grup multicast sesuai kebutuhan.
5. Pengiriman Data dimana sumber data mengirimkan paket data ke alamat multicast yang ditentukan. Router dalam jaringan kemudian menggunakan informasi dari protokol multicast untuk menentukan jalur

yang tepat untuk mengirimkan paket ke grup multicast yang sesuai. Ini memastikan bahwa hanya perangkat yang tertarik dengan data yang menerima dan memprosesnya.

6. Scalability, yang merupakan salah satu keuntungan utama dari transmisi data multicast adalah skalabilitasnya. Daripada mengirimkan salinan data terpisah untuk setiap penerima (seperti dalam transmisi unicast), sumber hanya perlu mengirim satu salinan data, yang kemudian dapat disalurkan ke beberapa penerima oleh router di jaringan.
7. Efisiensi, yaitu dengan mengirimkan data hanya kepada penerima yang membutuhkannya, transmisi data multicast mengurangi lalu lintas jaringan yang tidak perlu. Hal ini dapat mengurangi beban pada jaringan dan meningkatkan efisiensi penggunaan sumber daya.
8. Keamanan, dimana meskipun ada protokol keamanan yang tersedia untuk transmisi data multicast, seperti Secure Real-time Transport Protocol (SRTP) untuk audio dan video, transmisi multicast terbuka terhadap penyalahgunaan oleh penerima yang tidak sah. Oleh karena itu, perlu dilakukan pengaturan keamanan yang cermat saat mengimplementasikan transmisi multicast dalam lingkungan jaringan.

Dengan menggunakan transmisi data multicast, organisasi dapat menyediakan layanan streaming, distribusi konten, aplikasi kolaborasi yang efisien dan scalable serta dapat mentransmisikan data radar/surveillance dalam kaitannya terhadap operasional navigasi penerbangan di dalam jaringan mereka. Sedangkan VPN adalah singkatan dari Virtual Private Network. Ini adalah teknologi yang memungkinkan untuk membuat koneksi aman melalui jaringan publik, seperti internet. VPN bekerja dengan mengenkripsi data yang kirim melalui koneksi internet, sehingga membuatnya sulit bagi pihak luar untuk memata-matai atau mencuri informasi. Berikut adalah beberapa komponen penting dari VPN:

1. Enkripsi, dimana sebuah VPN menggunakan enkripsi untuk melindungi data yang dikirim antara perangkat dan server VPN. Ini berarti bahwa informasi yang kirimkan melalui koneksi VPN diacak, sehingga bahkan jika seseorang mencuri data tersebut, mereka tidak akan bisa membacanya tanpa kunci enkripsi yang benar.
2. Tunneling, dimana disini VPN menciptakan "tunnel" yang aman melalui internet. Ini berarti bahwa datadikirim melalui jalur aman dari perangkatke server VPN, sehingga tidak bisa diakses oleh pihak ketiga yang mungkin mencoba memata-matai atau memanipulasi koneksi.
3. IP Address Masking, pada saat terhubung ke VPN, alamat IPyang asli disembunyikan dan digantikan oleh alamat IP dari server VPN. Ini membantuuntuk menjaga privasi online, karena situs web dan layanan online hanya melihat alamat IP server VPN, bukan alamat IPyang sebenarnya.
4. Bypassing Geographical Restrictions adalah salah satu kegunaan paling umum dari VPN adalah untuk mengakses konten yang mungkin dibatasi berdasarkan lokasi geografis. Dengan terhubung ke server VPN di negara

lain,dapat membuatnya tampak seolah-olahmengakses internet dari negara tersebut, memungkinkanuntuk mengakses konten yang mungkin tidak tersedia di wilayah.

5. Keamanan Wi-Fi Publik saat terhubung ke Wi-Fi publik, seperti di kafe atau bandara, seringkali ada risiko keamanan yang meningkat. VPN dapat membantu melindungi informasi sensitifdari serangan seperti pencurian data atau serangan man-in-the-middle saat menggunakan Wi-Fi publik.
6. Meskipun VPN menyediakan banyak manfaat, penting untuk diingat bahwa tidak semua VPN diciptakan sama. Penting untuk memilih penyedia VPN yang tepercaya dan dapat dipercaya, karena beberapa VPN mungkin memonitor atau menyimpan log aktivitas pengguna mereka. Selain itu, kinerja dan kecepatan koneksi juga dapat bervariasi tergantung pada penyedia VPN yangpilih.

Dengan memanfaatkan teknologi ini, diharapkan dapat meningkatkan keandalan dan keamanan dalam mentransmisikan data radar, sambil juga meningkatkan efisiensi pengeluaran organisasi. Teknologi multicast memungkinkan untuk mengirimkan data kepada sekelompok komputer yang tergabung dalam suatu grup tertentu dengan hanya satu pengiriman, sedangkan teknologi tunnel in tunnel memastikan koneksi poin ke poin yang lebih aman dan terlindungi melalui jaringan internet atau publik. Dengan demikian, diharapkan dapat tercipta efisiensi yang lebih besar dalam pengeluaran dan keuangan organisasi, sambil tetap memastikan kelancaran dan keselamatan operasi penerbangan.

Maksud dan Tujuan

1. Maksud dari transmisi data radar multicast menggunakan metode tunnel in tunnel adalah untuk meningkatkan keselamatan penerbangan dengan memastikan kehandalan transmisi data radar dan memanfaatkan infrastruktur jaringan yang sudah ada. Hal ini bertujuan untuk mencapai efisiensi anggaran perusahaan sambil tetap menjaga keselamatan operasional penerbangan.
2. Tujuan dari implementasi ini adalah sebagai berikut:

a. Mengubah metode transmisi data radar dari VSAT menjadi Internet Protocol and Suites (IPS) guna meningkatkan keamanan dan keandalan data radar serta mengurangi risiko kegagalan sistem transmisi VSAT.
b. Mencapai efisiensi anggaran perusahaan dengan memanfaatkan infrastruktur jaringan yang sudah tersedia, yang lebih ekonomis daripada menggunakan fasilitas VSAT.
c. Menjadi pendukung dalam sistem pemanduan lalu lintas udara (ATC) dengan mengurangi risiko kegagalan transmisi data radar, yang dapat mengakibatkan penurunan layanan dari surveilans menjadi layanan prosedural.
d. Mematuhi standar SARPs yang telah ditetapkan oleh International Civil Aviation Organization (ICAO).

e. Mendukung konsep System Wide Information Management (SWIM) dan Integrated Management of Aeronautical Services (IMANS) dalam pengelolaan informasi penerbangan yang terintegrasi dan terkoordinasi.

Kelebihan Transmisi Data Radar Multicast

a. Sentralisasi IP Base, dimana hal ini memungkinkan untuk mengirimkan/transmisi data radar ke provider lain, dengan cara ini dapat mengurangi *corrupt data radar* pada proses *converting* dari data serial menjadi IP dan dapat dilakukan pengetesan data menggunakan aplikasi AST Modos atau aplikasi Wireshark sebelum melakukan konfigurasi.
b. Memungkinkan untuk melakukan *plug and play cable main/standby* ataupun menggunakan metode *fail-over* pada *router* yang tersedia.
c. Perangkat transmisi data IP dapat termonitor melalui aplikasi ERR-Robot yang dikembangkan oleh penulis.
d. Mudah melakukan pengecekan apabila data radar tidak tertampil pada ATC System dengan menggunakan *tools torch* pada *router* aplikasi wirehark ataupun aplikasi AST Modos, sedangkan untuk converter serial harus menggunakan alat tambahan, misalkan osiloskop.
e. Di dalam router sudah tersedia fitur graphing traffic sehingga dapat dengan mudah mengidentifikasi masalah apabila terjadi kegagalan transmisi.
f. Transmisi data berbasis IP memungkinkan menggunakan coverter FO (*Fiber Optic*) dan *Arrester Port* antara *switch* radar / ATC System menuju *router* untuk proteksi lonjakan tegangan akibat sambaran petir.

TINJAUAN PUSTAKA

Annex 11 – Air Traffic Services menjelaskan sebagai berikut:

Performance-based surveillance (PBS) operations

1. Dalam menerapkan operasi PBS, spesifikasi RSP harus ditetapkan oleh Negara-negara. Bila berlaku, spesifikasi RSP tersebut harus ditetapkan berdasarkan kesepakatan navigasi udara regional.
2. Spesifikasi RSP yang ditetapkan harus sesuai dengan layanan lalu lintas udara yang disediakan.
3. Ketika suatu spesifikasi RSP telah ditetapkan oleh Negara-negara untuk pemantauan berbasis kinerja, unit ATS harus dilengkapi dengan peralatan yang mampu memberikan kinerja yang konsisten dengan spesifikasi RSP yang ditetapkan.

ICAO Doc. 9869 – PBCS Manual menjelaskan sebagai berikut:

Aeronautical telecommunication network (ATN) adalah Sebuah arsitektur internetwork global yang memungkinkan jaringan data darat, udara-darat, dan avionik untuk bertukar data digital untuk keamanan navigasi udara serta untuk operasi lalu lintas udara yang teratur, efisien, dan ekonomis.

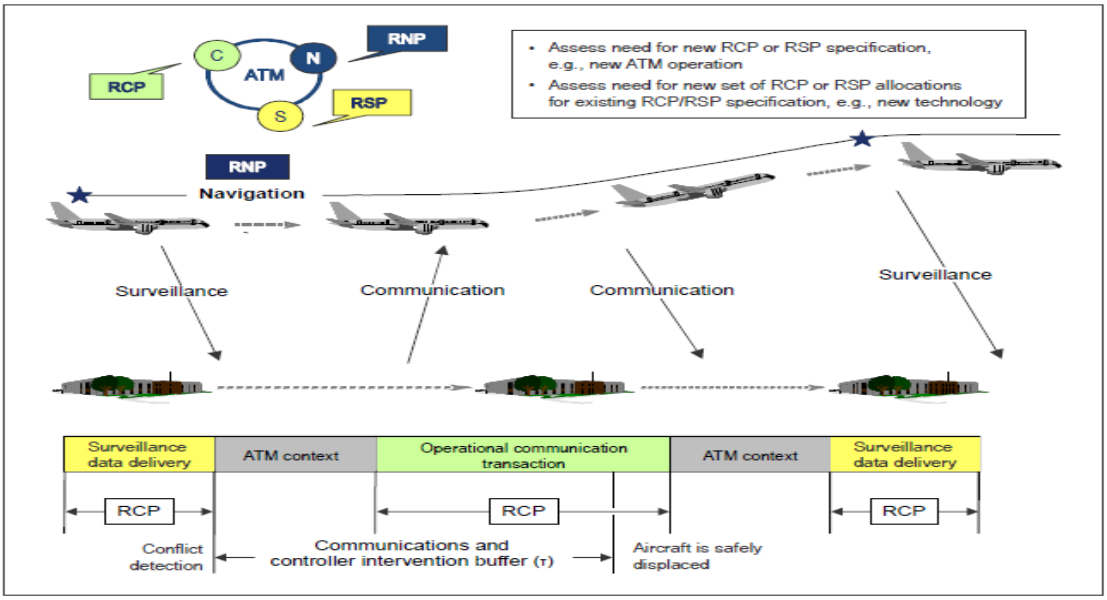
Performance-based surveillance (PBS) adalah Pemantauan yang didasarkan pada spesifikasi kinerja yang diterapkan pada penyediaan layanan lalu lintas udara.

Catatan.— Spesifikasi RSP mencakup persyaratan kinerja pemantauan yang dialokasikan ke komponen sistem dalam hal pemantauan yang akan disediakan dan waktu pengiriman data yang terkait, kontinuitas, ketersediaan, integritas, akurasi data pemantauan, keselamatan, dan fungsionalitas yang diperlukan untuk operasi yang diusulkan dalam konteks konsep ruang udara tertentu.

Spesifikasi Required surveillance performance (RSP) adalah Seperangkat persyaratan untuk penyediaan layanan lalu lintas udara dan peralatan darat yang terkait, kemampuan pesawat, dan operasi yang diperlukan untuk mendukung pemantauan berbasis kinerja.

Tabel 1. Hubungan antara RCP dan RSP *Specification*

Communication and controller intervention buffer, τ, parameter (Appendix 5)	*Normal communication and surveillance*	*Non-normal communication*	*Non-normal surveillance*
Not considered part of τ. The time for the system to deliver the surveillance data to the ATS unit.	Consideration for RSP specification.	Consideration for RCP specification.	Consideration for RSP specification.
The time for the controller to recognize the potential conflict and to devise an alternative means of separation (assumed to be achieved by a change of level in procedurally controlled airspace).	Not considered in RSP or RCP specification.	Not considered in RCP specification.	No time allocated for RSP specification. (Overdue position report.)
The time taken to communicate the instructions to the pilot via normal means of communication. In the case of an overdue position report, the time taken to obtain the report via normal means of surveillance.	Consideration for RCP specification.	Consideration for RCP specification.	Consideration for RSP specification. (Time after which the controller initiates first attempt to obtain overdue position report.)
The time taken to communicate the instructions to the pilot via alternative means of communication. In the case of a first attempt to obtain overdue position report fails, the time taken for a second attempt via alternative means of surveillance.	Not applicable.	Consideration for RCP specification.	Consideration for RSP specification. (Time after which the controller initiates second attempt to obtain overdue position report. If no response received, the controller would have initiated communication with other aircraft.)
The time for the pilot to react and initiate an appropriate manoeuvre and the time for the aircraft to achieve a change of trajectory sufficient to ensure that a collision will be averted.	Not applicable.	Not applicable.	Not applicable.
Not considered part of τ. Communication time for the PORT and WILCO responses to the ATC instruction, which may be concurrent with manoeuvring the aircraft.	Consideration for RCP specification.	Consideration for RCP specification.	Not applicable.



Gambar 1. Konteks Operasional Kapabilitas dan Performansi Komunikasi dan *Surveillance*

Persyaratan operasional dari suatu spesifikasi RSP berlaku untuk layanan pemantauan dan menentukan nilai parameter untuk waktu transit data pemantauan, kontinuitas RSP, ketersediaan RSP, dan integritas RSP, serta nilai yang dialokasikan (misalnya, required surveillance monitored performance (RSMP), required surveillance technical performance (RSTP), dan, bila berlaku, kinerja manusia). Ketika menerapkan RSP, diasumsikan bahwa komponen sistem pendukung kompatibel dan interoperabel, sesuai dengan standar interoperabilitas.

Suatu spesifikasi RSP diidentifikasi dengan suatu penunjuk (misalnya, RSP 180) untuk menyederhanakan konvensi penamaan penunjuk dan membuat waktu pengiriman data pemantauan yang diperlukan dengan jelas terlihat bagi perencana ruang udara, produsen pesawat, dan operator. Penunjuk mewakili nilai waktu pengiriman data pemantauan ketika pengiriman data pemantauan dianggap terlambat.

Kinerja aktual terkait dengan pengiriman data pemantauan dari waktu yang terkait dengan posisi pesawat yang diberikan dengan data, hingga waktu ketika unit ATS menerima data tersebut (disebut sebagai actual (operational) surveillance performance (ASP)). Pemantauan pasca-implementasi terus menilai ASP.

Tabel 2. Spesifikasi RSP

RSP specification	*RSP delivery time (seconds)*	*RSP continuity (probability)*	*RSP availability (probability)*	*RSP integrity (acceptable rate/flight hour)*
RSP 180	180	0.999	0.999 0.9999 (efficiency) (see Note 3)	FOM = navigation specification Time at position accuracy = +/- 1 sec Data integrity (malfunction) = 10^{-5}
RSP 400	400	0.999	0.999	FOM = Navigation specification Time at position accuracy = +/- 30 sec Data integrity (malfunction) = 10^{-5}

ICAO Doc. 9896 Part III Chapter 1 – Manual on the ATN using IPS Standards and Protocols menjelaskan sebagai berikut:
Multicast

1. Kebutuhan untuk mengirim informasi yang sama ke beberapa penerima adalah salah satu persyaratan utama distribusi data surveilans. Persyaratan ini dapat didukung oleh layanan multicast IPv4 dan IPv6. Teknik jaringan lain yang mencapai tujuan multicast yang sama tidak lagi dipertimbangkan dalam lingkup dokumen ini.
2. Sejumlah terbatas negara Kontraktor ICAO telah menerapkan layanan multicast IPv4 nasional untuk distribusi data surveilans. Namun, rentang terbatas ruang alamat multicast IPv4 dan ketiadaan gateway antara IPv4 dan IPv6 menghambat penyebaran yang dapat diskalakan untuk ATN/IPS.
3. Dalam beberapa tahun terakhir, kemajuan teknis yang signifikan telah dicapai dalam bidang multicast IP, yaitu sourcespecific multicast (SSM). Berbeda dengan implementasi yang ada berdasarkan PIM-SM (Protocol Independent Multicast- Sparse Mode), SSM memberikan kesederhanaan dan ketahanan tambahan terhadap routing lalu lintas multicast IP dan juga sangat cocok untuk kebutuhan surveilans. Penggunaannya melalui IPv6 direkomendasikan dalam panduan EUROCONTROL yang berjudul "EUROCONTROL Guidelines for Implementation Support (EGIS), Bagian 5: Spesifikasi Komunikasi & Navigasi, Bab 12, Daftar Kebutuhan Profil Distribusi Surveilans melalui IP Multicast (Profile Requirement List-PRL)".
4. Saluran data sourcespecific multicast (SSM) didefinisikan oleh kombinasi alamat multicast tujuan dan alamat unicast sumber. Ini sesuai dengan aliran data surveilans tunggal yang tersedia dari sumber tertentu dalam ATN/IPS.

METODOLOGI

Metode : deskripsi kuantitatif
Analisa : uji reliabilitas dan uji regresi
Sampel : pengukuran terhadap waktu saat pelayanan air traffic service diberikan pada sebuah bandara

HASIL PENELITIAN DAN PEMBAHASAN

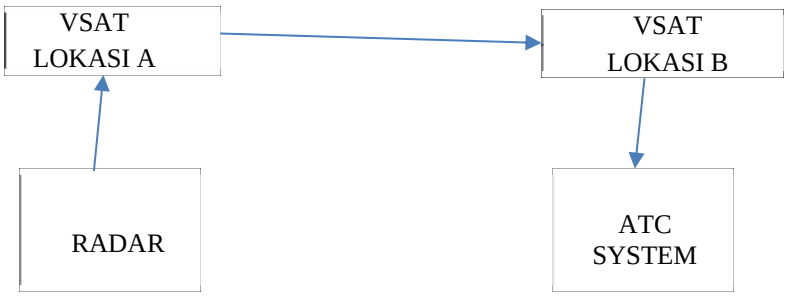
Transmisi Data Radar Saat Ini

Kondisi saat ini transmisi data radar antara kedua lokasi masih menggunakan layanan VPN (*Virtual Private Network*) VSAT. VSAT (*Very Small Aperture Terminal*) adalah sistem komunikasi satelit yang menggunakan antena kecil untuk mentransmisikan data melalui satelit. Dalam konteks ini, jika kedua lokasi menggunakan layanan VSAT untuk transmisi data radar, berikut adalah beberapa kondisi yang mungkin terjadi:

1. Latensi, hal ini dikarenakan data harus melakukan perjalanan ke luar angkasa ke satelit dan kembali ke bumi, akan ada latensi (penundaan) dalam transmisi data. Latensi ini dapat bervariasi tergantung pada jarak

antara terminal VSAT dan satelit, serta kondisi atmosfer dan kepadatan lalu lintas di satelit.

2. Kualitas Sinyal, dimana kualitas sinyal dapat dipengaruhi oleh berbagai faktor, termasuk kondisi cuaca, interferensi elektromagnetik, dan penutupan oleh bangunan atau struktur lainnya. Jika ada gangguan dalam sinyal, hal ini dapat mengakibatkan gangguan atau penurunan kualitas transmisi data.
3. Kecepatan Transmisi data dapat dipengaruhi oleh sejumlah faktor, termasuk bandwidth yang tersedia pada layanan VSAT yang digunakan, kondisi jaringan satelit, dan jumlah pengguna yang bersamaan menggunakan layanan tersebut. Beberapa layanan VSAT mungkin menawarkan kecepatan transfer data yang lebih tinggi daripada yang lain, tergantung pada paket layanan yangpilih.
4. Biaya, yang mana penggunaan layanan VSAT biasanya melibatkan biaya langganan bulanan serta biaya berdasarkan pemakaian data. Biaya ini dapat bervariasi tergantung pada penyedia layanan dan jenis layanan yangpilih. Beberapa layanan VSAT mungkin memiliki batasan kuota data bulanan, sementara yang lain mungkin menawarkan paket tanpa batasan kuota data.
5. Keamanan, hal ini dikarenakan data yang ditransmisikan melalui layanan VSAT melakukan perjalanan melalui satelit, ada potensi keamanan yang perlu dipertimbangkan. Meskipun data yang ditransmisikan biasanya dienkripsi, ada risiko bahwa sinyal dapat diintersep atau diretas oleh pihak yang tidak sah. Oleh karena itu, penting untuk menggunakan protokol keamanan yang kuat dan memastikan bahwa sistem VSATterlindungi dengan baik.



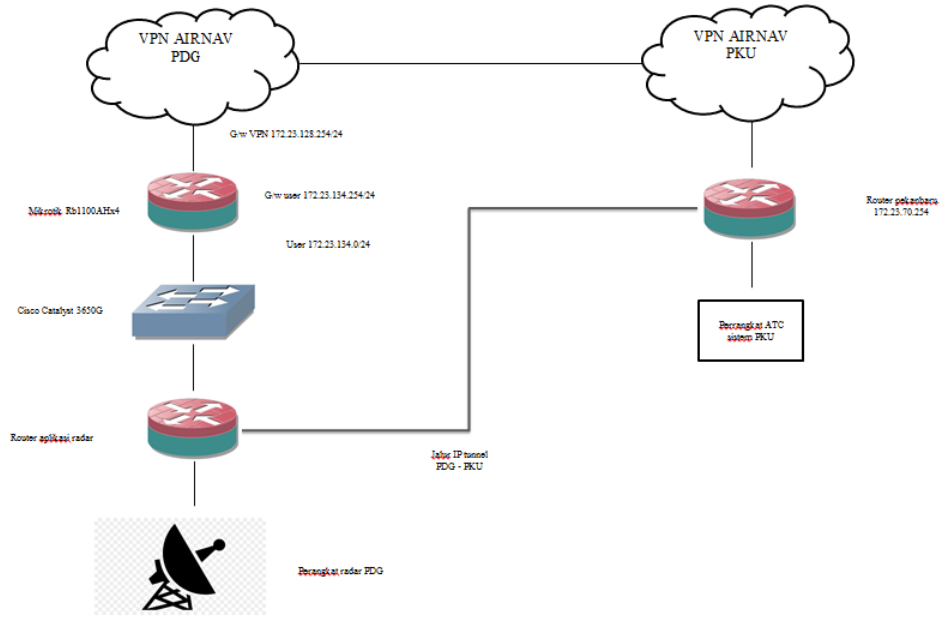
Gambar 2. Topologi Transmisi Data Radar saat Menggunakan VSAT

Transmisi Data Radar Multicast

Dengan adanya jaringan VPN (*Virtual Private Network*) yang telah terinstalasi di lokasi tertentu sehingga dapat dimanfaatkan untuk membuat system tunneling yang kedepanya dapat menjadi backup ataupun pengganti transmisi data yang selama ini disediakan oleh VSAT.

Tunneling IP (*Internet Protocol*) merupakan suatu system yang dapat membungkus suatu data yang kemudian ditansmisikan menuju suatu alamat tanpa mengurangi ataupun menambah besar kecilnya suatu data serta dapat meningkatkan keamanan sebuah data yang melewati sebuah jaringan.

Sebuah tunnel dapat dijadikan suatu metode transmisi didalam sebuah jaringan tanpa mengganggu lalu lintas packet data yang melewati sebuah sistem,sehingga dapat dijadikan salah satu metode untuk mentransmisikan data radar dari satu lokasi ke lokasi lain. Berikut contoh topologi antara dua lokasi yaitu antara padang dan pekanbaru mengenai transmisi multicast data radar menggunakan metode tunnel in tunnel.



Gambar 3.Topologi Transmisi Data Radar Multicast

Dari blok diagram diatas penggunaan metode tunnel in tunnel sangat efektif dalam penggunaanya dimana di site radar padang hanya membutuhkan sebuah router dikarenakan bandwith yang dibutuhkan untuk mentransmisikan data radar padang relative kecil hanya 10 kbps sehingga sangat lebih efisien dalam penggunaanya.

Filter IGMP

IGMP adalah singkatan dari Internet Group Management Protocol. Ini adalah protokol komunikasi yang digunakan oleh host IP dan router multicast yang berdekatan untuk menetapkan keanggotaan grup multicast. Secara sederhana, IGMP memungkinkan host untuk memberi tahu router multicast lokalnya bahwa ia ingin menerima lalu lintas multicast untuk grup tertentu, dan memungkinkan router untuk mengirimkan lalu lintas multicast secara efisien hanya ke segmen-segmen jaringan di mana itu diperlukan.

Sekarang, filter IGMP umumnya merujuk pada fitur dalam perangkat jaringan seperti router atau switch yang memungkinkan administrator untuk mengontrol lalu lintas multicast yang mengalir melalui jaringan dengan memfilter pesan IGMP. Dengan filter IGMP, dapat menentukan grup-multicast mana yang diizinkan atau ditolak dalam segmen jaringan, membantu mengelola bandwidth dan mengoptimalkan kinerja jaringan. Fitur ini sangat berguna dalam skenario di mana ingin mengontrol aliran lalu lintas multicast dan mencegah paket multicast yang tidak perlu membanjiri bagian-bagian tertentu dari jaringan.

Filter IGMP adalah fitur yang ada di perangkat jaringan seperti router atau switch yang memungkinkan pengguna untuk mengontrol lalu lintas data multicast di jaringan. Dengan filter IGMP, pengguna dapat menentukan grup-multicast mana yang diizinkan atau diblokir untuk melewati segmen-segmen tertentu dari jaringan. Ini membantu dalam mengelola penggunaan bandwidth dan meningkatkan efisiensi jaringan dengan mengurangi lalu lintas yang tidak perlu. Dengan kata lain, filter IGMP memungkinkan pengguna untuk mengontrol dan mengarahkan secara tepat lalu lintas multicast yang diterima dan dikirimkan dalam jaringan.

IGMP (Internet Group Management Protocol) filtering adalah sebuah fitur yang digunakan pada perangkat jaringan seperti switch atau router untuk mengontrol dan mengelola lalu lintas multicast dalam jaringan. Ini penting karena multicast memungkinkan pengiriman data dari satu sumber ke beberapa penerima secara bersamaan, yang sering digunakan dalam aplikasi streaming video, konferensi video serta digunakan dalam pengiriman data stream seperti halnya data radar.

Berikut adalah beberapa analisa tentang IGMP filtering:

1. Pengelolaan Lalu Lintas, yang mana IGMP filtering memungkinkan administrator jaringan untuk mengelola lalu lintas multicast dengan lebih efektif. Dengan memfilter lalu lintas IGMP, administrator dapat membatasi jumlah penerima multicast dalam jaringan, mengoptimalkan penggunaan bandwidth, dan mengurangi beban jaringan yang tidak perlu.
2. Keamanan, dimana IGMP filtering juga dapat digunakan sebagai alat keamanan dalam jaringan. Dengan membatasi alamat multicast yang diterima oleh switch atau router, administrator dapat mencegah serangan seperti flood attack, di mana seorang penyerang mengirimkan banyak permintaan join group ke grup multicast yang tidak valid untuk menghabiskan sumber daya jaringan.
3. Pengoptimalan Jaringan dalam jaringan yang besar atau kompleks, penggunaan IGMP filtering dapat membantu mengoptimalkan kinerja jaringan dengan mengurangi jumlah lalu lintas multicast yang tidak perlu disebarkan ke seluruh jaringan. Ini dapat mengurangi beban pada perangkat jaringan dan meningkatkan responsivitas jaringan secara keseluruhan.
4. Pemecahan Masalah Jaringan, yaitu IGMP filtering dapat membantu dalam pemecahan masalah jaringan terkait multicast. Dengan kemampuan untuk membatasi dan mengisolasi lalu lintas multicast, administrator dapat dengan lebih mudah mengidentifikasi masalah, seperti loop multicast atau konfigurasi yang salah, dan mengambil tindakan korektif.

Namun demikian, penggunaan IGMP filtering juga perlu dilakukan dengan hati-hati. Jika tidak dikonfigurasi dengan benar, dapat menyebabkan gangguan pada layanan yang membutuhkan multicast, atau bahkan mengakibatkan isolasi penerima yang sah dari grup multicast yang diinginkan.

Oleh karena itu, pemahaman yang baik tentang konfigurasi dan penggunaan IGMP filtering sangat penting bagi administrator jaringan.

Kebutuhan Fasilitas untuk Implementasi Transmisi Data Radar Multicast

Untuk implementasi transmisi data radar multicast, beberapa fasilitas diperlukan:

1) Jaringan Komunikasi: Jaringan komunikasi yang dapat mendukung layanan multicast diperlukan untuk mengirimkan data radar ke penerima yang dituju. Jaringan ini harus memiliki kapasitas yang memadai dan ketersediaan yang tinggi untuk memastikan transmisi data yang lancar.
2) Perangkat Jaringan: Router dan perangkat jaringan lainnya yang mendukung multicast perlu dipasang dan dikonfigurasi dengan benar. Ini termasuk perangkat keras dan perangkat lunak yang mampu mengelola aliran data multicast dengan efisien.
3) Sumber Data Radar: Sistem radar yang menghasilkan data harus dihubungkan ke jaringan komunikasi. Data radar ini akan menjadi sumber data untuk transmisi multicast.
4) Protokol Multicast: Protokol multicast seperti Protocol Independent Multicast (PIM) atau Source-Specific Multicast (SSM) mungkin diperlukan tergantung pada kebutuhan spesifik implementasi. Protokol ini membantu dalam manajemen dan routing data multicast.
5) Keamanan: Langkah-langkah keamanan harus diterapkan untuk melindungi data radar yang ditransmisikan dari ancaman keamanan. Ini termasuk enkripsi data dan akses kontrol yang tepat.
6) Monitoring dan Manajemen: Fasilitas untuk memantau dan mengelola kinerja transmisi data multicast diperlukan. Ini meliputi alat pemantauan jaringan dan sistem manajemen jaringan untuk mendeteksi dan mengatasi masalah yang mungkin timbul.
7) Ketersediaan Backup: Rencana cadangan harus disiapkan untuk mengatasi kegagalan sistem utama. Ini dapat mencakup jalur komunikasi backup dan sistem penggantian otomatis untuk memastikan kelangsungan operasi.
8) Router mikrotik.

   Router MikroTik adalah perangkat keras jaringan yang dirancang dan diproduksi oleh perusahaan MikroTik. Perangkat ini berfungsi sebagai router, switch, firewall, dan juga dapat berperan sebagai server untuk berbagai layanan jaringan seperti DHCP, DNS, VPN, dan lainnya. Router MikroTik biasanya menjalankan sistem operasi RouterOS, yang merupakan perangkat lunak berbasis Linux yang dikembangkan oleh MikroTik.

   Router MikroTik dikenal karena kemampuannya yang kuat dan fleksibel dalam mengelola jaringan, serta menyediakan berbagai fitur yang dapat disesuaikan sesuai dengan kebutuhan pengguna. Mereka sering digunakan dalam berbagai skenario jaringan, mulai dari rumah tangga hingga perusahaan besar, penyedia layanan Internet, dan penyedia

layanan telekomunikasi. Beberapa fitur utama dari Router MikroTik termasuk:

a. Routing: Memungkinkan pengaturan dan manajemen rute jaringan, termasuk rute statis dan dinamis menggunakan protokol seperti OSPF, RIP, dan BGP.
b. Firewall: Menyediakan firewall yang kuat untuk melindungi jaringan dari serangan dan mengatur lalu lintas jaringan sesuai kebijakan keamanan.
c. Switching: Memiliki kemampuan switching yang memungkinkan untuk membuat VLAN, mengatur port switch, dan mengelola lalu lintas jaringan lokal.
d. Wireless: Dapat berfungsi sebagai pengontrol akses titik akses wireless (wireless access point) atau memperluas jaringan nirkabel melalui fitur WDS (Wireless Distribution System).
e. VPN: Mendukung berbagai protokol VPN termasuk PPTP, L2TP, IPsec, dan OpenVPN, yang memungkinkan pengaturan koneksi aman antara lokasi jarak jauh.
f. Manajemen Jaringan: Menyediakan berbagai alat untuk pemantauan dan manajemen jaringan, termasuk antarmuka grafis dan baris perintah yang kuat.

9) Internet Protocol (IP) Virtual Private Network (VPN).

I P VPN adalah singkatan dari "Internet Protocol Virtual Private Network". Ini adalah jenis jaringan pribadi virtual (VPN) yang menggunakan protokol Internet Protocol (IP) untuk mengirimkan data secara aman melalui jaringan publik, seperti Internet. IP VPN memungkinkan organisasi atau individu untuk terhubung ke jaringan pribadi mereka melalui koneksi yang aman dan terenkripsi di atas infrastruktur jaringan publik. Berikut adalah beberapa fitur dan karakteristik utama dari IP VPN:

a. Keamanan: IP VPN menggunakan teknologi enkripsi dan protokol keamanan seperti IPsec (Internet Protocol Security) untuk menyediakan lapisan keamanan tambahan saat mentransmisikan data melalui jaringan publik. Ini memastikan bahwa data yang ditransmisikan tetap aman dan terlindungi dari akses yang tidak sah.
b. Privasi: Dengan menggunakan IP VPN, pengguna dapat mengakses sumber daya jaringan pribadi atau aplikasi organisasi dari jarak jauh tanpa mengorbankan privasi. Semua data yang ditransmisikan melalui VPN terenkripsi, sehingga tidak dapat diakses oleh pihak yang tidak sah.
c. Akses Jarak Jauh: IP VPN memungkinkan pengguna untuk terhubung ke jaringan pribadi mereka dari lokasi yang jauh atau dari perangkat yang tidak terhubung secara fisik ke jaringan lokal, seperti saat bepergian atau bekerja dari rumah.
d. Skalabilitas: IP VPN dapat disesuaikan dengan kebutuhan organisasi, baik itu untuk skala kecil, menengah, atau besar. Hal ini

memungkinkan perusahaan untuk menyesuaikan ukuran jaringan VPN mereka sesuai dengan pertumbuhan bisnis atau perubahan kebutuhan.

e. Fleksibilitas: IP VPN dapat digunakan untuk berbagai keperluan, termasuk koneksi cabang ke kantor pusat, akses jarak jauh untuk karyawan, pengamanan koneksi internet publik, dan lain-lain. Ini memberikan fleksibilitas dalam penggunaan dan penerapan.

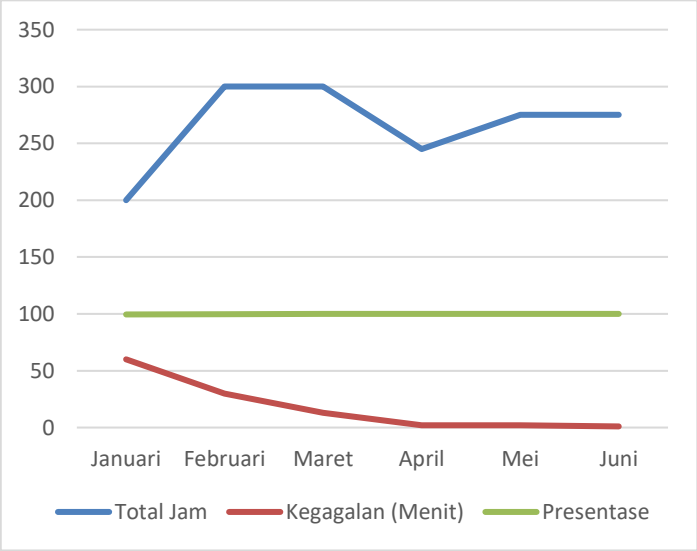
Uji Reliabilitas

a. Fase Uji Coba

Fase uji coba dilaksanakan selama 6 (enam) bulan yaitu dari bulan Januari 2023 s/d Juni 2023, pada fase uji coba ini hanya untuk identifikasi pesawat dan integrasi data radar display, dengan hasil sebagai berikut:

Tabel 3.Fase Uji Coba

No.	Bulan	Total Jam	Kegagalan (menit)	Presentase
1.	Januari	200	60	99.5%
2.	Februari	300	30	99.83%
3.	Maret	300	13	99.92%
4.	April	245	2	99.98%
5.	Mei	275	2	99.98%
6.	Juni	275	1	99.98%
Total		1045	105	99.87%



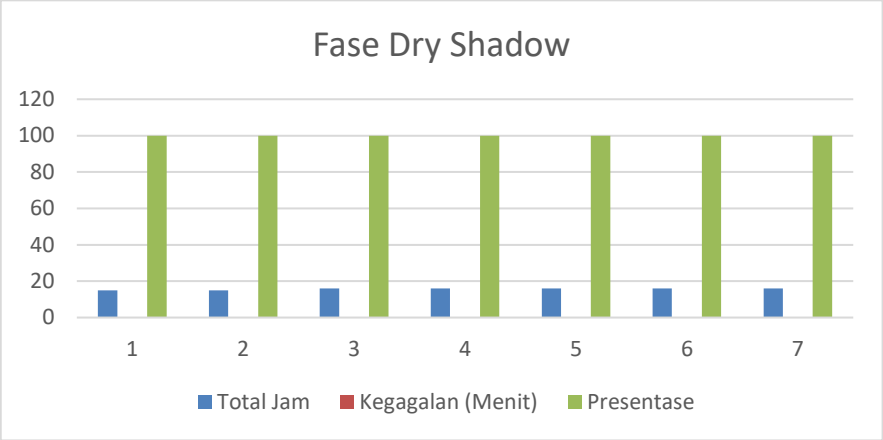
Gambar 4. Diagram Fase Uji Coba

b. Fase *Dry Shadow*

Fase *Dry Shadow* dilaksanakan selama 7 (tujuh) hari, transmisi data radar yang terintegrasi dengan sistem VSAT menjadi *main*, sedangkan transmisi data radar multicast dengan metode tunnel in tunnel menjadi *standby*. Hasil dari fase *Dry Shadow*, adalah:

Tabel 4. Fase *Dry Shadow*

No.	Bulan	Total Jam	Kegagalan (menit)	Presentase
1.	01 – 07 Juli 2023	110	0	100%
Total		110	0	100%



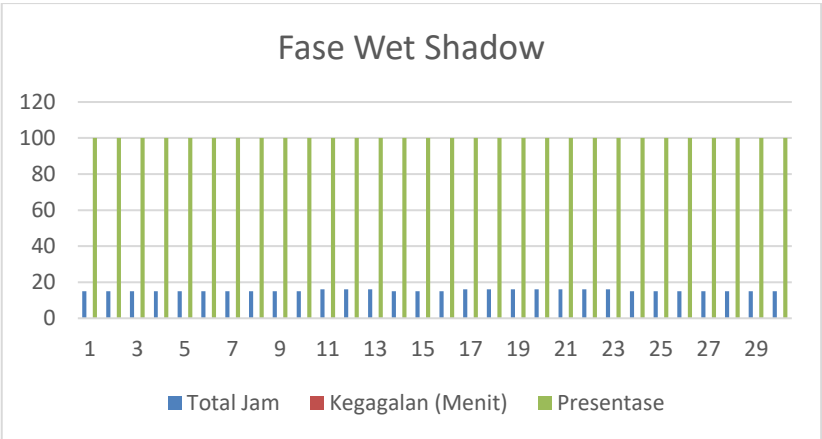
Gambar 5. Diagram Fase Dry Shadow

c. Fase *Wet Shadow*

Fase *Wet Shadow* dilaksanakan selama 1 (satu) bulan, transmisi data radar multicast dengan metode tunnel in tunnel menjadi *main* dan transmisi data radar yang terintegrasi dengan sistem VSAT menjadi *standby*. Hasil dari fase *Wet Shadow*, adalah:

Tabel 5. Tabel fase *Wet Shadow*

No.	Bulan	Total Jam	Kegagalan (menit)	Presentase
1.	8 Juli – 8 Agustus 2023	460	0	100%
Total		460	0	100%



Gambar 6. Diagram Fase Wet Shadow

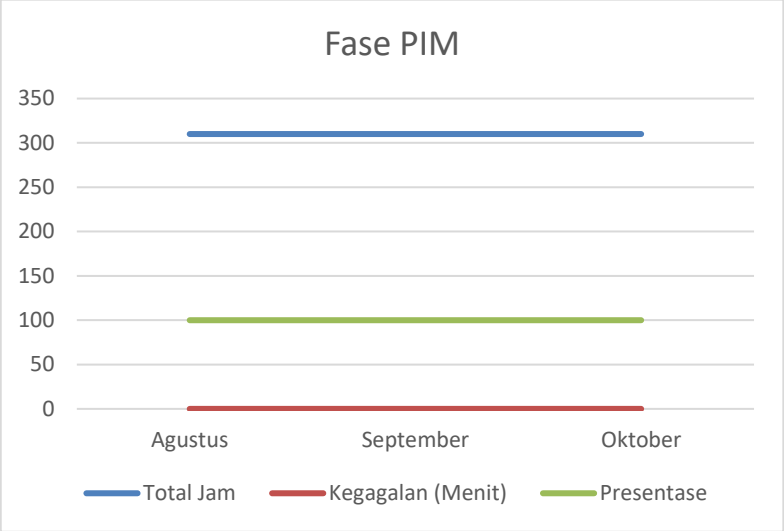
d. Fase *Full Implementation and Post Monitoring*

Fase *Full Implementation and Post Monitoring* dilaksanakan selama 3 (tiga) bulan, dimana pada fase ini transmisi data radar multicast dengan metode tunnel in tunnel digunakan sebagai fasilitas *main*, sedangkan transmisi data radar yang

terintegrasi dengan sistem VSAT tidak digunakan lagi. Hasil dari fase *Full Implementation and Post Monitoring*, adalah:

Tabel 6. Fase *Full Implementation and Post Monitoring*

No.	Bulan	Total Jam	Kegagalan (menit)	Presentase
1.	Agustus	310	0	100%
2.	September	310	0	100%
3.	Oktober	310	0	100%
Total		930	0	100%



Gambar 7.Diagram Fase Full Implementation And Post Monitoring

e. Hasil Regresi Linear

Tabel 8. Hasil Regresi Linear

Regression Statistics	
Multiple R	0,81066541
R Square	0,657178407
Adjusted R Square	0,619087119
Standard Error	0,032520035
Observations	11

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	1	0,018245662	0,018245662	17,25272208	0,002470969
Residual	9	0,009517974	0,001057553		
Total	10	0,027763636			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95,0%*	*Upper 95,0%*
Intercept	99,70637698	0,064653526	1542,164574	1,03202E-25	99,56012054	99,85263341	99,56012054	99,85263341
200	0,00075254	0,000181176	4,153639619	0,002470969	0,000342691	0,001162388	0,000342691	0,001162388

Tabel 9. Residual Output

Observation	*Predicted 99,7*	*Residuals*
1	99,89451185	-0,064511851
2	99,93213883	-0,012138826
3	99,93966422	0,040335779
4	99,93966422	0,040335779
5	99,93966422	0,040335779
6	100,0073928	-0,007392777
7	100,0073928	-0,007392777
8	100,0073928	-0,007392777
9	100,0073928	-0,007392777
10	100,0073928	-0,007392777
11	100,0073928	-0,007392777

Gambar 8. Diagram Linear Regression

Contingency Plan Transmisi Data Radar Multicast

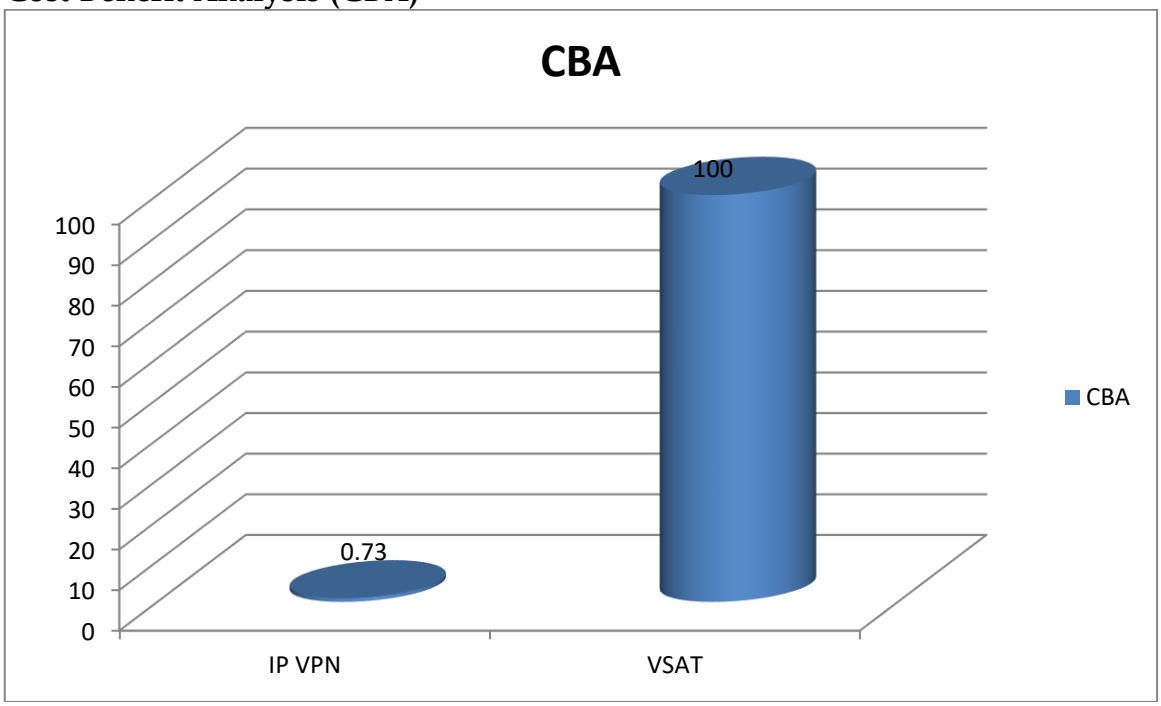
Rencana kontingensi yang dibuat terhadap kemungkinan terjadinya gangguan/kegagalan transmisi data radar multicast dengan metode tunnel in tunnel dengan mempertimbangkan beberapa kemungkinan kondisi yang dapat terjadi antara lain:

1. Jaringan/VPN mengalami kegagalan/*malfunction*/*error*.
   - Memberikan pelayanan *procedural services*.
   - Menggunakan Aplikasi ERR-Robot sebagai pendeteksi kegagalan jaringan AirnavNet, untuk mempercepat proses perbaikan.
2. *Router* mengalami kegagalan/*malfunction*/*error*.
   - Menggunakan metode *Virtual Router Redundancy Protocol* (VRRP).
3. Transmisi data radar multicast dengan metode tunnel in tunnel mengalami kegagalan/*malfunction*/*error*.
   - Memberikan pelayanan *procedural services*.

- Melakukan *plug and play cable.*
- Menggunakan metode *fail-over* pada *router.*

.

Cost Benefit Analysis (CBA)



Gambar 9. Diagram Cost Benefit Analysis (CBA)

KESIMPULAN DAN REKOMENDASI

Kesimpulan

Kesimpulan dari penelitian ini secara umum adalah bahwa implementasi transmisi data radar multicast menggunakan metode tunnel in tunnel melalui jaringan IP VPN menawarkan solusi yang lebih efektif dan efisien daripada menggunakan layanan VSAT. Dengan memanfaatkan teknologi multicast dan tunneling, efisiensi bandwidth dapat ditingkatkan, keandalan transmisi meningkat, dan biaya operasional dapat dikurangi. Dukungan yang tepat dari infrastruktur jaringan, protokol multicast, dan rencana kontingensi juga penting untuk keberhasilan implementasi. Analisis biaya dan manfaat menunjukkan bahwa pendekatan ini memiliki potensi keuntungan yang lebih besar dalam jangka panjang. Oleh karena itu, transisi menuju transmisi data radar multicast adalah langkah yang dapat meningkatkan layanan surveilans penerbangan secara keseluruhan.

Saran

Saran singkat dari hasil penelitian jurnal ini adalah:

1. Evaluasi secara rutin latensi dan kualitas sinyal VSAT, serta pertimbangkan penyesuaian infrastruktur jika diperlukan.
2. Pastikan layanan VSAT dapat memenuhi kebutuhan bandwidth yang diperlukan untuk transmisi data radar.
3. Monitor dan kelola penggunaan data secara efisien untuk mengontrol biaya yang tidak perlu.

4. Prioritaskan keamanan data dengan menerapkan protokol keamanan yang kuat pada sistem VSAT.
5. Implementasikan filter IGMP untuk mengontrol lalu lintas data multicast secara efektif.
6. Siapkan semua fasilitas yang diperlukan untuk implementasi transmisi data radar multicast dengan baik.
7. Pertimbangkan penggunaan router MikroTik yang fleksibel untuk mendukung infrastruktur jaringan yang dibutuhkan.
8. Manfaatkan IP VPN untuk konektivitas yang aman antara lokasi radar.
9. Buat rencana kontingensi yang komprehensif untuk mengatasi kemungkinan gangguan dalam transmisi data radar multicast.
10. Lakukan analisis cost benefit secara berkelanjutan untuk membandingkan biaya dan manfaat antara layanan VSAT dan transmisi data radar multicast.

PENELITIAN LANJUTAN

Dalam penulisan artikel ini peneliti menyadari masih banyak kekurangan baik dari segi bahasa, penulisan, dan bentuk penyajian mengingat keterbatasan pengetahuan dan kemampuan dari peneliti sendiri. Oleh karena itu, untuk kesempurnaan artikel, peneliti mengharapkan kritik dan saran yang membangun dari berbagai pihak.

DAFTAR PUSTAKA

Annex 11 – Air Traffic Services

Autor, A. B., & Brasileiro, F. V. (2015). "IGMP Filtering for Multicast Security". Journal of Computer Networks and Communications, 2015, 1-9.

Aviation System Block Upgrade (ASBU);

Bansal, P., & Rai, R. (2019). "Managing Multicast Traffic Using IGMP Filtering: A Comprehensive Study". International Journal of Computer Applications, 181(37), 30-35.

Chandra, A., & Gupta, S. (2017). "Optimizing Network Performance through IGMP Filtering: A Case Study". International Journal of Computer Science and Network Security, 17(8), 65-72.

Deering, S. E., & Cheriton, D. R. (1990). "Multicast Routing in Datagram Internetworks and Extended LANs". ACM Transactions on Computer Systems (TOCS), 8(2), 85-110.

Dubey, R., & Singh, V. (2018). "Enhancing Network Efficiency with IGMP Filtering: An Analysis". Journal of Network Management, 8(2), 45-52.

Huitema, C. (1996). "Multicast Routing in the Internet". IEEE Internet Computing, 12(2), 70-77.

ICAO Doc. 9869 – *Performance-Based Communication and Surveillance (PBCS) Manual;*

ICAO Doc. 9896 – *Manual on The Aeronautical Telecommunication Network* (ATN) *using Internet Protocol Suites* (IPS) *Standards and Protoco.*

Indonesia Modernization Air Navigation Systems (IMANS).

Kumar, S., & Sharma, M. (2020). "IGMP Filtering: A Review of Applications and Challenges". International Journal of Advanced Research in Computer Science, 11(5), 128-135.

Patel, H., & Shah, D. (2016). "Troubleshooting Multicast Issues Using IGMP Filtering: A Practical Approach". Journal of Networking and Telecommunications, 6(3), 78-85.

Peraturan Direksi Perum Lembaga Penyelenggara Pelayanan Navigasi Penerbangan Indonesia Nomor PER.033/LPPNPI/IX/2015 tentang Safety Assessment Pelayanan Navigasi Penerbangan;

Peraturan Menteri Perhubungan Nomor PM 9 Tahun 2022 tentang Perubahan atas Peraturan Menteri Perhubungan Nomor PM 55 Tahun 2016 tentang Tatanan Navigasi Penerbangan Nasional;

Peraturan Menteri Perhubungan Nomor PM. 10 Tahun 2022 tentang Perubahan Atas Peraturan Menteri Perhubungan Nomor PM 65 Tahun 2017 tentang Peraturan Keselamatan Penerbangan Sipil bagian 170 (*Civil Aviation Safety Regulation Part 170*) tentang Peraturan Lalu Lintas Udara (*Air Traffic Rules*)

Peraturan Menteri Perhubungan Nomor PM. 29 Tahun 2021 tentang Peraturan Keselamatan Penerbangan Sipil Bagian 172 Tentang Penyelenggara Pelayanan Manajemen Lalu Lintas Dan Telekomunikasi Penerbangan

Peraturan Menteri Perhubungan Nomor PM. 62 Tahun 2017 tentang Peraturan Keselamatan Penerbangan Sipil Bagian 19 Tentang Sistem Manajemen Keselamatan

System Wide Information Management (SWIM)

Undang-Undang Nomor 1 Tahun 2009 tentang Penerbangan