UNIVERSITAS
MERCU BUANA

IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

TUGAS AKHIR

Aditya Fauziyanto
41516110035

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Tugas Akhir

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:
Aditya Fauziyanto
41516110035

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2020

LEMBAR PERNYATAAN ORISINALITAS

Yang bertanda tangan dibawah ini:

NIM	: 41516110035
Nama	: Aditya Fauziyanto
Judul Tugas Akhir	: IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 09 Februari 2021

Aditya Fauziyanto

SURAT PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Aditya Fauziyanto
NIM	:	41516110035
Judul Tugas Akhir	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Dengan ini memberikan izin dan menyetujui untuk memberikan kepada Universitas Mercu Buana **Hak Bebas Royalti Noneksklusif** (*None-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul diatas beserta perangkat yang ada (jika diperlukan).

Dengan Hak Bebas Royalti/Noncksklusif ini Universitas Mercu Buana berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat dan mempublikasikan tugas akhir saya.

Selain itu, demi pengembangan ilmu pengetahuan di lingkungan Universitas Mercu Buana, saya memberikan izin kepada Peneliti di Lab Riset Fakultas Ilmu Komputer, Universitas Mercu Buana untuk menggunakan dan mengembangkan hasil riset yang ada dalam tugas akhir untuk kepentingan riset dan publikasi selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Jakarta, 09 Februari 2020

Aditya Fauziyanto

SURAT PERNYATAAN LUARAN TUGAS AKHIR

Sebagai mahasiswa Universitas Mercu Buana, saya yang bertanda tangan di bawah ini :

Nama Mahasiswa	:	Aditya Fauziyanto
NIM	:	41516110035
Judul Tugas Akhir	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Menyatakan bahwa :

1. Luaran Tugas Akhir saya adalah sebagai berikut :

No	Luaran	Jenis			Status	
1	Publikasi Ilmiah	Jurnal Nasional Tidak Terakreditasi			Diajukan	✓
		Jurnal Nasional Terakreditasi	✓			
		Jurnal International Tidak Bereputasi			Diterima	
		Jurnal International Bereputasi				
	Disubmit/dipublikasikan di :	Nama Jurnal	: Jurnal Edukasi Dan Penelitian Informatika			
		ISSN	: 2548-9364			
		Link Jurnal	: Jurnal.untan.ac.id			
		Link File Jurnal Jika Sudah di Publish	:			

2. Bersedia untuk menyelesaikan seluruh proses publikasi artikel mulai dari submit, revisi artikel sampai dengan dinyatakan dapat diterbitkan pada jurnal yang dituju.
3. Diminta untuk melampirkan scan KTP dan Surat Pernyataan (Lihat Lampiran Dokumen HKI), untuk kepentingan pendaftaran HKI apabila diperlukan

Demikian pernyataan ini saya buat dengan sebenarnya.

Mengetahui
Dosen Pembimbing TA

Desi Ramayanti, S.Kom, MT

Jakarta, 09 Februari 2021

Aditya Fauziyanto

LEMBAR PERSETUJUAN PENGUJI

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110035
Nama	:	Aditya Fauziyanto
Judul Tugas Akhir	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 9 Februari 2021

(Harni Kusniyati, ST.,MKom)

LEMBAR PERSETUJUAN PENGUJI

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110035
Nama	:	Aditya Fauziyanto
Judul Tugas Akhir	:	Implementasi Traversal Server Menggunakan Traversal Relay Arounds Nat (TURN) pada Jaringan Voip Studi Kasus PT Aplikanusa Lintasarta

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 25 Februari 2021

(Dr. Leonard Goeirmanto)

LEMBAR PERSETUJUAN PENGUJI

LEMBAR PERSETUJUAN PENGUJI

NIM	:	41516110035
Nama	:	Aditya Fauziyanto
Judul Tugas Akhir	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 9 Februari 2021

(Sri Dianing, Asri, ST, M.Kom)
Dosen Penguji 3

LEMBAR PENGESAHAN

LEMBAR PENGESAHAN

IM	:	41516110035
ama	:	Aditya Fauziyanto
dul Tugas Akhir	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Tugas Akhir ini telah diperiksa dan disidangkan sebagai salah satu persyaratan untuk memperoleh gelar Sarjana pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Jakarta, 9 Februari 2021

Menyetujui,

(Desi Ramayanti, S.Kom, MT)
Dosen Pembimbing

Mengetahui,

(Diky Firdaus, S.Kom, MM)	(Desi Ramayanti, S.Kom, MT)
Koord. Tugas Akhir Teknik Informatika	Ka. Prodi Teknik Informatika

ABSTRAK

Nama	:	Aditya Fauziyanto
NIM	:	41516110035
Pembimbing TA	:	Desi Ramayanti, S.Kom, MT
Judul	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

PT Aplikanusa lintasarta merupakan perusahaan yang bergerak dibidang *internet service provider*. Lintasarta sudah memiliki jaringan voip sebelumnya namun memiliki permasalahan yaitu belum terjamin nya Quality of service dari layanan VoIP dan juga belum adanya *server* yang berfungsi untuk melakukan *blocking* SIP *domain* dengan menambahkan pattern terntetu agar terhindar dari *Toll fraud*. Keterbatasan *bandiwdth* saat ini bisa menyebabkan terjadinya beban berlebih pada sebuah *traffic* jaringan. IETF (*Internet Engineering Task Force*) memiliki suatu *standard* untuk memnuhi kebutuhan QoS yaitu Diffserv yang mampu mengklasifikasi packet sesuai kebutuhan. namun diffserv saja tidak cukup, ketika terjadi penumpukan packet maka packet yang menumpuk tersebut akan didrop oleh karena itu penambahan WRED sebagai solusi dari *dropping* tersebut dengan menerapkan sistem *treshold*. algoritma WRED mampu memberikan pengaruh yang baik, hasil pengujian layanan VoIP dengan menambahkan WRED mampu mengurangi *packet loss* sekitar 15% dan delay 10% Diffserv-WRED juga bisa memaksimalkan *Throughput* yaitu 2% dibanding diffserv dan juga mengurangi *jitter* sekitar 8% dibandingkan jika hanya menerapkan diffserv saja dan juga penerapan TURN-*Server* dengan *call policy* pattern mampu memblock panggilan yang berpotensi *toll fraud* yang melakukan panggilan terus menerus maupun dengan domain terntetu, hal ini mampu menjaga kondisi dari *resource* VoIP seperti *call manager* agar ketersediaanya terjaga dikarenakan terhindar dari exploitasi.

Kata kunci:
Qos,VoIP,Diffserv,TURN,SIP

ABSTRACT

Name	:	Aditya Fauziyanto
Student Number	:	41516110035
Counsellor	:	Desi Ramayanti, S.Kom, MT
Title	:	IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

.

PT Aplikanusa Lintasarta is a company engaged in the internet service provider. Lintasarta already has a voip network before but has problems, namely the quality of service of VoIP services is not guaranteed and there is also no server that functions to block SIP domains by adding certain patterns to avoid Toll fraud. Current bandwidth limitations can cause network traffic to overload. IETF (Internet Engineering Task Force) has a standard to meet QoS needs, namely Diffserv which is able to classify packets according to needs. However, diffserv alone is not enough, when there is an accumulation of packets, the packets that accumulate will be dropped, therefore the addition of WRED as a solution to the dropping is by applying the threshold system. The WRED algorithm is able to provide a good effect, the test results of VoIP services by adding WRED can reduce packet loss by about 15% and delay 10% Diffserv-WRED can also maximize throughput, which is 2% compared to diffserv and also reduce jitter by about 8% compared to only applying diffserv. only and also the application of the TURN-Server with a call policy pattern is able to block calls that have the potential to toll fraud that make calls continuously or with certain domains, this is able to maintain the condition of VoIP resources such as call managers so that their availability is maintained due to avoidance of exploitation.

Key words:
research, guidance, computer science, universitas mercu buana

KATA PENGANTAR

Puji syukur kita panjatkan kepada Allah S.W.T, karena berkat rahmat-Nya penulis bisa menyelesaikan penelitian ini.

Penulis menyadari bahwa tanpa bantuan dan bimbingan Ibu Desi Ramayanti, S.Kom., MT dan rekan-rekan yang telah membantu saya dalam menyelesaikan penelitian saya mungkin saya tidak dapat menyelesaikan penelitian ini tepat waktu, Oleh karena itu, penulis mengucapkan terima kasih kepada:

1. Ibu Desi Ramayanti, S.Kom., MT selaku Dosen Pembimbing Tugas Akhir Teknik Informatika.
2. Ibu Desi Ramayanti, S.Kom., MT selaku Ketua Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Mercu Buana.
3. Bapak Diky Firdaus, S.Kom, MM selaku Koordinator Tugas Akhir Teknik Informatika.
4. Orang tua yang telah memberikan dukungan doa dan semangat.
5. Vici Ramadhani yang telah membantu menjaga kesehatan mental, doa dan semangat
6. Teman-teman rekan mahasiswa Universitas Mercubuana yang tidak bisa disebut satu persatu yang yang turut membantu memberikan support dan dukungan kepada penulis selama proses penelitian ini.

Akhir kata, penulis menyadari terdapat ketidaksempurnaan dan kekurangan dalam penelitian tugas akhir ini.Penulis berharap semoga penelitian tugas akhir ini dapat memberikan manfaat.

Jakarta, 20 Desember 2020
Penulis

DAFTAR ISI

JEPIN

(Jurnal Edukasi dan Penelitian Informatika)

ISSN(e): 2548-9364 / ISSN(p) : 2460-0741

Vol. x
No. y
mm yy

NASKAH JURNAL

IMPLEMENTASI TRAVERSAL SERVER MENGGUNAKAN TRAVERSAL RELAY AROUNDS NAT (TURN) PADA JARINGAN VOIP STUDI KASUS PT APLIKANUSA LINTASARTA

Aditya Fauziyanto[#1], Desi Ramayanti[*2]

[#]*Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana*
Meruya, Jakarta barat
[1]Adityafauziyanto@gmail.com

[*]*Informatika, Universitas Mercubuana*
Meruya, Jakarta barat
[2]Desi.ramayanti@mercubuana.ac.id

***Abstrak*— PT Aplikanusa lintasarta merupakan perusahaan yang bergerak dibidang *internet service provider*. Lintasarta sudah memiliki jaringan voip sebelumnya namun memiliki permasalahan yaitu belum terjamin nya Quality of service dari layanan VoIP dan juga belum adanya *server* yang berfungsi untuk melakukan *blocking* SIP *domain* agar terhindar dari *Toll fraud*. Keterbatasan *bandiwdth* saat ini bisa menyebabkan terjadinya beban berlebih pada sebuah *traffic* jaringan. IETF (*Internet Engineering Task Force*) memiliki suatu *standard* untuk memnuhi kebutuhan QoS yaitu Diffserv yang mampu mengklasifikasi packet sesuai kebutuhan. namun diffserv saja tidak cukup, ketika terjadi penumpukan packet maka packet yang menumpuk tersebut akan didrop oleh karena itu penambahan WRED sebagai solusi dari *dropping* tersebut dengan menerapkan sistem *treshold*. algoritma WRED mampu memberikan pengaruh yang baik, hasil pengujian layanan VoIP dengan menambahkan WRED mampu mengurangi *packet loss* sekitar 15% dan delay 10% Diffserv-WRED juga bisa memaksimalkan *Throughput* yaitu 2% dibanding diffserv dan juga mengurangi *jitter* sekitar 8% dibandingkan jika hanya menerapkan diffserv saja dan juga penerapan TURN-*Server* dengan *call policy* mampu memblock panggilan yang berpotensi toll fraud yang melakukan panggilan terus menerus maupun dengan domain terntetu, hal ini mampu menjaga kondisi dari *resource* VoIP seperti *call manager* agar ketersediaanya terjaga dikarenakan terhindar dari exploitasi.**

***Kata kunci*— Qos,VoIP,Diffserv,TURN,SIP**

PENDAHULUAN

Sistem komunikasi adalah sistem dimana mengirim informasi dari satu tempat ke tempat lain melalui sebuah media transmisi [1]. Dalam komunikasi pun ada beberapa elemen seperti sumber informasi, penyebar, penerima, tujuan. Sistem komunikasi saat ini sudah banyak berkembang seperti telepon analog berbasis PSTN, Sistem telepon analog berbasis PABX dan IP Phone berbasis internet dengan VoIP. masing masing teknologi memiliki kekurangan dan kelebihan masing masing seperti telepon PSTN biaya telepon yang lebih mahal namun memiliki kelebihan tidak perlu adanya sistem admin karena semua sudah ada di sentral. sistem PABX juga memiliki kelebihan yaitu semua *user* bisa berkomunikasi dengan nomor ekstensi, menghemat biaya penggunaan telepon dalam satu *line* kekurangan nya tidak bisa melakukan komunikasi diluar *line* secara bersamaan. sistem VoIP pun memiliki kelebihan yaitu Biaya yang lebih murah jika melakukan panggilan interlokal karena hanya membutuhkan *Domain* dan internet saja namun VoIP memiliki kekurangan yaitu keamanan dan kualitas suara yang tidak bagus jika tidak menggunakan *traversal server*[2].

Saat ini teknologi telepon yang paling efisien dan banyak digunakan adalah telepon berbasis VoIP. VoIP adalah sebuah teknologi yang bisa menggunakan *internet protocols* sebagai media transmisi suara, suara ditransmisikan menggunakan *packet* pada sirkuit *line* [1]. VoIP juga memiliki beberapa protokol yaitu *Session Initiate Protocol* (SIP) dan H.323. SIP adalah protokol lapisan aplikasi yang digunakan untuk VOIP (*Voice over Internet Protocol*). SIP digunakan untuk mengendalikan sesi komunikasi multimedia selain itu SIP dapat digunakan untuk sesi multimedia lainnya seperti pesan instan, konferensi *video*, *game online*, faks melalui IP, dan bahkan untuk *transfer file* [3]. Implementasi VOIP menggunakan protokol SIP pernah dilakukan pada penelitian Mohammad risnandar dkk. Penelitian ini membahas mengenai implementasi VoIP berbasis SIP pada fakultas teknik di UIKA bogor. Sebelumnya fakultas teknik UIKA bogor tidak memiliki jaringan untuk voice lalu mohammad risnandar dkk melakukan penelitian berbasis SIP untuk diimplementasikan di lingkungan fakultas teknik UIKA bogor. Hasilnya setelah dilakukan implementasi jaringan VoIP berbasis SIP mendapatkan rata rata *delay* 20 *millisecond*, 0,23 *milisecond* pada *jitter* dan 0,06% pada *packet loss*[4].

Protokol VOIP selain SIP adalah H.323, merupakan protokol standar VoIP tertua yang direkomendasikan oleh ITU-T yang mendefinisikan komunikasi multimedia *real-time* dan konferensi melalui jaringan *packet-based*. Jaringan berbasis paket tersebut antara lain *internet Protocol* (IP), *internet Packet Exchange* (IPX), *Local Area Network* (LAN), *Enterprise Network* (EN), *Metropolitan Area Network* (MAN), dan *Wide Area Network* (WAN)[5]. Penelitian tentang H.323 dilakukan oleh Lola Yorita Astrid dkk membahas mengenai QoS pada jaringan VoIP local dengan menggunakan H.323 . Pada penelitian ini menggunakan beberapa macam *codec* dan hasilnya ada beberapa variasi QoS

yang terjadi. hasilnya adalah dengan *codec* G.729 menghasilkan *jitter* 33 *millisecond, delay* 79,21 *millisecond* dan *packet loss* sebesar 1.83%. sedangkan dengan *codec* G.723 didapatkan hasil *jitter* 10,09 *millisecond*, *delay* 46,10 *millisecond* dan *packet loss* sebesar 0.89%[6].

Lintasarta merupakan sebuah perusahaan yang bergerak dibidang *internet service provider* yang berfokus pada jaringan dan SD-wan yang didirikan tahun 1988. Lintasarta bermarkas di Jakarta tepatnya di Jl M.H Thamrin. Sistem komunikasi yang berjalan saat ini di perusahaan lintasarta adalah menggunakan sistem telepon IP PBX. Sistem telepon IP PBX yang ada mampu melakukan panggilan ekstensi ke 100 lebih pengguna telepon. IP PBX merupakan suatu perangkat yang fungsinya melakukan *switching* komunikasi telepon berbasis analog maupun berbasis IP. IP PBX mampu mengelola ekstensi berbasis analog ataupun IP.[7].

Jaringan VoIP rentan terkena masalah keamanan *cyber* yaitu *toll-fraud*. IP PBX *existing* perusahaan tidak bisa melakukan *blocking* pada *domain* yang masuk dan rentan terkena *toll-fraud. Toll-fraud* akan menggunakan *resources* VoIP yang diserang dan akan digunakan orang lain untuk melakukan panggilan baik kedalam maupun keluar negeri. Hal tersebut sangat akan merugikan perusahaan dikarenakan biaya untuk panggilan akan dibebankan kepada pemilik jaringan VoIP yang diserang. *Toll-Fraud* bisa diatasi dengan *blocking domain* yaitu dengan melakukan *blacklist pattern domain* SIP. *domain* yang mencurigakan akan dimasukan *pattern* kedalam *turn server* setelah itu jika terdapat panggilan dari *domain* yang sebelumnya sudah di *blacklist* panggilan akan langsung diputus oleh TURN *server* dan tidak akan sampai kedalam *Call manager, data recording* ataupun *resources* IP *endpoint* yang ada di *call manager* akan aman dan tidak akan tampil. Jaringan VoIP juga memerlukan *Quality Of services* yang stabil, namun pada ip pbx *existing* milik perusahaan tidak bisa melakukan perubahan *codec* yang digunakan, ip pbx hanya bisa menggunakan *codec default* yaitu G.711 dengan *bandwidth* 64Kbps. Codec tersebut terlalu besar dibanding *codec* terbaru saat ini yaitu G.729 yang berukuran 8Kbps. *Codec* akan mempengaruhi *Quality Of Services* dari suatu jaringan VoIP oleh karena itu biasanya digunakan mekanisme pengatur QoS yaitu Diffserv. Dengan metode diffserv paket bisa diklasifikasikan sesuai kebutuhan dan bisa melakukan mekanisme *dropping* jika terjadi penumpukan *packet* pada umumnya mekanisme *dropping* diatur berdasarkan *Differentiated Service Code Point* (DSCP) pada Diffserv, paket paket yang sudah diprioritaskan sebelumnya bisa diatasi dengan *Weighted Random Early Detection* (WRED).

Terbatasnya Ip *address* versi 4 saat ini banyak sekali yang menggunakan metode *symmetric* NAT untuk mentranslate ip *address*. Untuk melewati sebuah perangkat NAT dibutuhkan suatu metode yang bisa melakukan *relay* NAT, karena *system* VoIP berbasis SIP haruslah *Peer to Peer*[8]. Oleh karena itu pada penelitian sebelumnya F alamsyah dkk melakukan implementasi webRTC menggunakan TURN *server* sebagai *server* untuk membangun koneksi *Peer to peer* pada webRTC[9]. *Traversal relay around* NAT (TURN) adalah suatu metode yang digunakan dalam suatu jaringan VoIP berbasis SIP yang fungsinya untuk merelay IP *address* yang di NAT. *Symmetric* NAT biasa digunakan agar sebuah jaringan tidak bisa melakukan koneksi *Peer to peer* secara langsung, oleh karena itu TURN digunakan untuk merelay permintaan ke *symmetric* NAT dari ip luar jaringan agar bisa melakukan koneksi *peer to peer* ke dalam jaringan VoIP berbasis SIP [10]. Pada jaringan VoIP berbasis SIP TURN biasa dikombinasikan oleh teknik lain agar lebih menjamin kualitas QoS pada jaringan VoIP. Yaitu dengan metode *differentiated service,* TURN-Diffserv dan TURN-Diffserv-WRED[11].

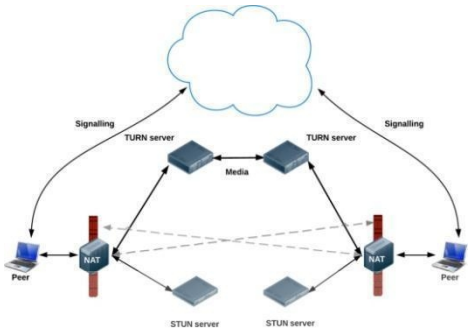
Tujuan dari penelitian ini adalah untuk mengetahui efektifitas implementasi TURN *server* pada jaringan VoIP menggunakan *bandwidth* seminimal mungkin namun tetap menjaga kualitas dari QoS pada jaringan VoIP dengan menerapkan teknik *differentiated service*. Oleh karena itu penulis memilih sistem VoIP dengan *traversal server* sebagai solusi dari permasalahan terkait jaringan VoIP yang sensitif dengan QoS.

DASAR TEORI

Traversal Relay Arounds NAT (TURN)

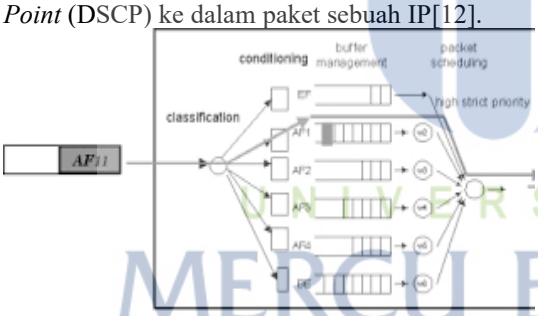
Traversal using relays around NAT (TURN) adalah salah satu metode untuk mengatur penerimaan data melalui koneksi *Transmission control protocol* (TCP) atau *User Datagram Protocol* (UDP) yang beroperasi di belakang sebuah *Network address translation* (NAT). *Server* TURN merelay paket dari Internet protokol eksternal ke perangkat internal. TURN bisa mengatur klien untuk menyampaikan paket ke dan dari *host* lain (*peer*) dan dapat mengontrol bagaimana *relay* dilakukan. Lalu klien akan

memperoleh alamat IP dan *port* yang disebut *relayed-transport-address*.
Ketika transmisi data secara langsung/*peer-to-peer* gagal dilakukan, transmisi data secara *Relay* umum nya dijadikan sebagai alternatif. *Traversal Using Relay* NAT (TURN) Server bekerja dengan meneruskan data / *Relay* ke komputer tujuan mirip seperti *Proxy*[10].
.



Gambar 1 cara kerja TURN Server

Differentiated Services
Differentiated service merupakan suatu teknik dalam implementasi QoS dalam jaringan berbasis IP. *Differentiated services* akan memberikan perbedaan melalui pembagian kelas pada sebuah *traffic*. Identifikasi kelas pada diffserv menggunakan Diffserv *Code Point* (DSCP) ke dalam paket sebuah IP[12].

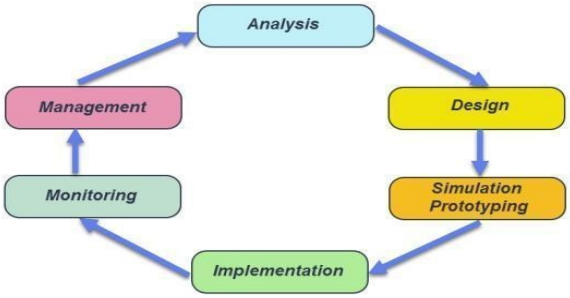


Gambar 2 Alur kerja Diffserv [13]

Dalam diffserv dikenal pula teknik *Weighted Random Early Access* atau disebut WRED adalah sebuah metode yang akan melakukan *dropping packet* jika terjadi penumpukan pada antrian dan hanya memprioritaskan paket yang sudah di definisikan besaran maksimal bandwidthnya[13]

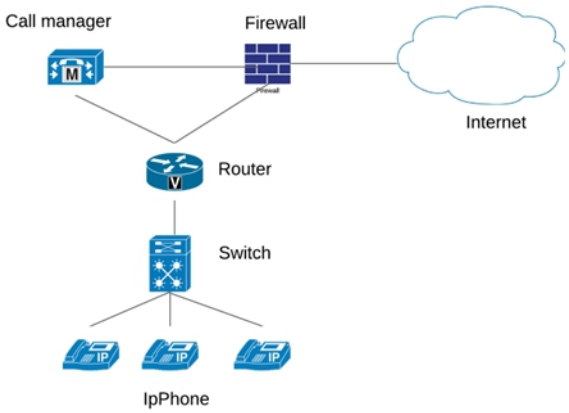
METODE PENELITIAN

Penelitian ini menggunakan metode *Network Development Life Cycle* (NDLC), dimana metode ini melakukan pendekatan terhadap proses komunikasi data berorientasi *network* yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi bisnis, daur hidup, pengembangan aplikasi dan analisis pendistribusian data. Tahapan pada metode NDLC adalah *analysis, design, simulation prototyping, implementation, monitoring* serta tahapan terakhir adalah *management*. Untuk mendukung percobaan pada jaringan voip sangat dibutuhkan beberapa tahap untuk mengidentifikasi *packet packet* yang lewat[14]



Gambar 3 *network development life cycle* (NDLC) [15]

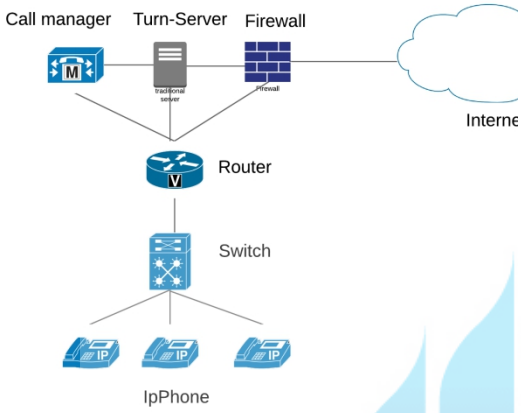
a. Tahapan *Analysis*
Pada tahap ini, dilakukan *survey* dan wawancara untuk mendapatkan informasi terkait dengan permasalahan yang ada. *Survey* dilakukan di lingkungan lintasarta dan wawancara terhadap *Senior engineer collaboration and security*. Berdasarkan hasil *survey* dan wawancara yang dilakukan terungkap bahwa sistem komunikasi IP PBX *existing* perusahaan saat ini tidak bisa melakukan *blocking* pada *domain* yang masuk dan rentan terkena *toll-fraud*. sehingga diperlukan penambahan fungsi keamanan mengatasi masalah tersebut. Topologi sebelum adanya *Turn-Server* terdapat pada gambar 5 dimana belum adanya *Turn-Server* dan juga *firewall* tidak bisa melakukan *blocking port* SIP dan juga domain SIP karena *Firewall* tidak bisa melakukan penambahan *pattern call policy*.



Gambar 4 Topologi sebelum adanya *Turn-Server*

b. Tahapan Design

Pada tahapan ini, dilakukan perancangan terhadap topologi jaringan WAN dengan implementasi VoIP PT aplikanusa Lintasarta dengan menambahkan TURN *server*. Dimana *Turn Server* akan melakukan *relay* NAT baik dari dalam maupun dari luar jaringan menuju ke internet dari *router*.



Gambar 5 *Design* jaringan

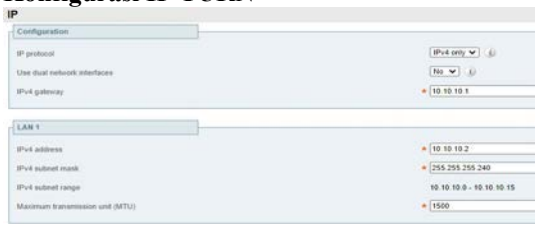
Penambahan *Turn-Server* berada di posisi sebelum *call manager, Turn-Server* akan melakukan *blocking* panggilan panggilan asing dari luar untuk menjaga ketersediaan dari *call manager* agar tidak tereksploitasi.

c. Simulation prototyping

Pada penelitian ini simulasi tidak bisa dilakukan dengan *software cisco packet tracer* tetapi menggunakan *software* dan *trial license* dari *cisco* dan diimplementasikan menggunakan *Virtual machine*. Untuk tahapan simulasi terdapat beberapa tahapan yang dilakukan

a. Melakukan instalasi *Call manager* dan TURN *Server* di *virtual*.
b. Melakukan Konfigurasi berikut pada *Turn Server*
c. Melakukan Simulasi protipe

Konfigurasi IP TURN



Gambar 6 Konfigurasi IP TURN

Gambar 6 menunjukan konfigurasi IP *address* yang berfungsi untuk membuka *portal web admin server*.

Konfigurasi SIP dan UDP Port

Gambar 7 Konfigurasi SIP dan UDP Port

Gambar 7 menunjukan konfigurasi mode pada *server* yang harus di *enable* yaitu SIP,TCP,UDP dan TLS. UDP Port memiliki *port default* yaitu 5060 begitu pula dengan TCP. Untuk TLS memiliki *port default* 5061.

Konfigurasi *Search Rule*

Gambar 8 Konfigurasi *Search Rule*

Gambar 8 menunjukan konfigurasi *search rule*. Konfigurasi ini bertujuan memberikan *Pattern domain* agar *server* tidak menerima banyak *call exploit* yang bisa membuat *server* menjadi lambat.

Konfigurasi Diffserv

```
TBS-R1(config)#access-list 101 permit
udp any any range 40000 45000
TBS-R1(config)#access-list 102 permit
udp any any range 537 7000
TBS-R1(config)#class-map VOIP
TBS-R1(config-cmap)# match access-group
102
TBS-R1(config)#policy-map DSCP_DIFFSERV
TBS-R1(config-pmap)#class VOIP
TBS-R1(config-pmap-c)#bandwidth 128
TBS-R1(config-pmap-c)#set dscp ef
```

Gambar 9 Konfigurasi Diffserv

Gambar 9 merupakan kode konfigurasi Diffserv pada *router cisco, access list* adalah salah satu metode untuk melakukan seleksi terhadap paket yang memiliki kriteria dan sudah di *permit* [jurnal jett]. Untuk voip ditentukan dengan *bandwidth minimal* 128kbps dan diatur dengan marking DSCP EF (*expedited forwarding*).

Konfigurasi WRED

```
TBS-R1(config)#class-map m_cs4
TBS-R1(config-cmap)#match dscp cs4
TBS-R1(config)#class-map m_ef
TBS-R1(config-cmap)#match dscp ef
TBS-R1(config)#policy-map WRED
TBS-R1(config-pmap)#class m_ef
TBS-R1(config-pmap-c)#bandwidth 128
TBS-R1(config-pmap-c)#random-detect
dscp-based
TBS-R1(config-pmap-c)#random-detect dscp
46 30 50 10
TBS-R1(config-pmap)#class m_cs4
```

Gambar 10 Konfigurasi WRED

Konfigurasi WRED pada DSCP *field di Policy-map* tujuannya untuk mengaktifkan random detect berdasarkan dscp-*based*. Nilai *threshold* yang diatur adalah 30 batas antrian minimal paket yang masuk dan nilai maksimal 50.

Berikut adalah hasil simulasi *toll fraud* yaitu meng-*Intercept* panggilan asing yang masuk

```
2020-09-20T11:49:26.738+07:00 tvcs: Event="Call Attempted" Service="SIP" Src-
Src-port="37008" Src-alias-type="SIP" Src-alias="sip:1000@lintasarta.co.id"
Dst-alias-type="SIP" Dst-alias="sip:*810484222886955@lintasarta.co.id"
Call-serial-number="46d3317d-1f66-4b6e-bce1-0435c11d42a6"
Tag="ad486749-7ac3-45df-8525-003826c3f795" Protocol="TLS"
Auth="NO" Level="1" UTCTime="2020-09-20 04:49:26,737"
```

Gambar 11 *call attempt*

Pertama penyusup mencoba melakukan panggilan menggunakan *domain* 1000@lintas.xxx lalu mencoba memanggil dengan tujuan *8198xx@lintas.xxx

```
2020-09-20T11:49:26.738+07:00 tvcs: Event="Search Attempted" Service="SIP" Src-alias-type="SIP" Src-ali
Dst-alias-type="SIP" Dst-alias="sip:*810484222886955@lintasarta.co.id"
Call-serial-number="46d3317d-1f66-4b6e-bce1-0435c11d42a6" Tag="ad486749-7ac3-45df-8525-003826c3f795"
Detail="searchtype:INVITE" Level="1" UTCTime="2020-09-20 04:49:26,738"
```

Gambar 12 search attempted

Lalu *domain* melakukan penelusuran dari luar untuk mencoba memasuki kedalam *resource* voip yaitu *call manager* untuk melakukan panggilan

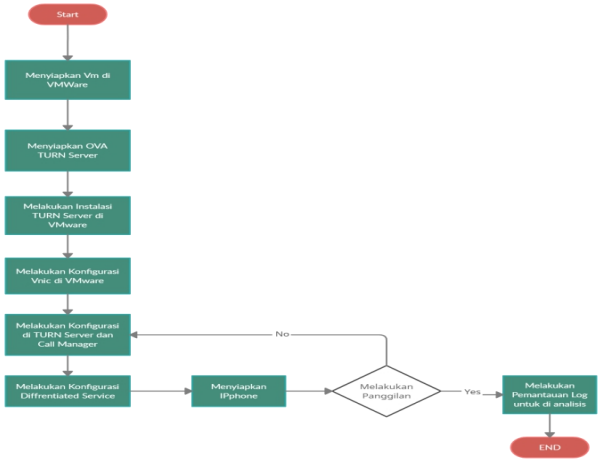
```
2020-09-20T11:49:58.797+07:00 tvcs: Event="Call Rejected" Service="SIP" Src-ip="195.154.169.163" Src-port="3708
alias="sip:1000@lintasarta.co.id"
Dst-alias-type="SIP" Dst-alias="sip:*810484222886955@lintasarta.co.id"
Call-serial-number="46d3317d-1f66-4b6e-bce1-0435c11d42a6"
Tag="ad486749-7ac3-45df-8525-003826c3f795"
Detail="Forbidden" Protocol="TLS" Response-code="404" Level="1" UTCTime="2021-01-25 04:49:58,797"
```

Gambar 13 Hasil *intercept*

Namun belum memasuki ke *call manager* penelusuran sudah di *intercept* oleh TURN server yaitu ditandai dengan call "*Rejected*" dan dengan detail "*Forbidden*". Hal tersebut menandakan bahwa call dari penyusup berhasil direject dan tidak bisa masuk ke *resources* VoIP.

d. *Implementation*

Pada tahapan ini dilakukan implementasi jaringan VoIP PT. Aplikanusa Lintasarta berdasarkan topologi yang sudah dirancang. Pada proses ini peneliti menambahkan *pattern domain* SIP pada TURN *server* dan *call manager* untuk menghindari *toll fraud* dan juga *differentiated service* pada jaringan VoIP untuk mendapatkan jaminan QoS yang lebih baik.

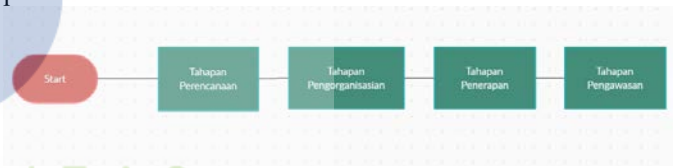


Gambar 14 Proses Implementasi

e. *Monitoring*

Tahapan ini dilakukan proses monitoring untuk menjaga ketersediaan server agar bisa digunakan dan Monitoring dilakukan terhadap log dan domain panggilan yang masuk ke jaringan VoIP

f. *Management* : Pada tahap ini adalah tahapan untuk melaksanakan pemeliharaan hasil penelitian yang sudah di implementasi, tahap ini dilakukan oleh *staff* terkait perusahaan.

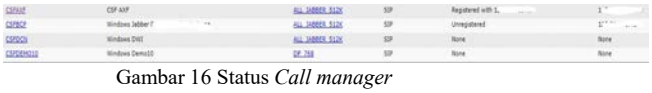


Gambar 15

Tahapan perencanaan di operasional untuk melakukan perencanaan *improvement* terkait jaringan Voip. Tahapan pengorganisasian yaitu penentuan orang yang akan memegang operasional jaringan voip oleh *manager* terkait. Tahapan penerapan yaitu untuk menerapkan hasil dari perencanaan *improvement* diawal. Tahapan pengawasan yaitu untuk menghawasi dan evaluasi tahapan management agar berjalan sesuai dengan tahapan *management* diawal.

HASIL DAN PEMBAHASAN

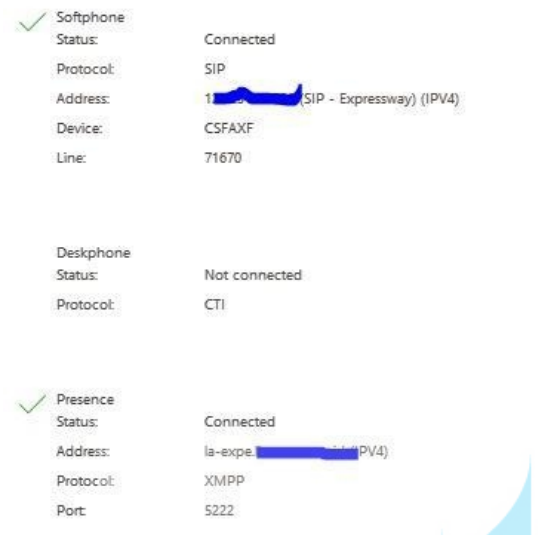
PENGUJIAN PANGGILAN



Gambar 16 Status *Call manager*

Gambar 16 adalah hasil implementasi terlihat *user* CSF AXP berhasil teregister ke TURN *server* dengan tanda "*Registered*". *Registered* adalah bahwa Ipphone berhasil teregister ke

TURN *server* dan akan membawa alamat IP *Turn Server* jika melakukan panggilan yang berbeda IP atau *domain*.



Gambar 17 Informasi di IPphone

Gambar 17 merupakan informasi pada IpPhone yang berhasil teregister di TURN *server* dengan ditandai dengan adanya *address* pada bagian *softphone* dan juga *address* namun berisi *domain* pada bagian *presence*

2020-08-11T12:53:17.934+07:00 tvcs: Event="Search Completed" Service="SIP" type="SIP" Src-alias="sip:71670@1.4.3.1" Dst-alias-type="SIP" Dst-alias="sip Call-serial-number="b12dff94-af52-4a6a-b2d3-6bc765d9e8c0" Tag="88bfac05-09d0 b249856b7e33" Detail="found:true, searchtype:INVITE" Call-routed="YES" Level -08-12 05:53:17,793"

2020-08-12T12:53:17.924+07:00 tvcs: Event="Call Connected" Service="SIP" Sr Src-port="22790" Src-alias-type="SIP" Src-alias="sip:71670@1.4.3.1" Dst-alia alias="sip:apo@10.5.2.1" Call-serial-number="b12dff94-af52-4a6a-b2d3-6bc765d Tag="88bfac05-09d0-4322-8e08-b249856b7e33" Protocol="TLS" Call-routed="YES" UTCTime="2020-08-12 05:53:17,793"

Gambar 18 detail panggilan proses panggilan SIP

Gambar 18 merupakan detail panggilan proses sip dimana berisi seperti *source address* yaitu 1.4.3.1 dan juga *extension* 71670 (*user* axp). dan juga berisi detail dari *destination* yaitu *user* apo@10.5.2.1 dan juga berisi seperti *port* dan juga *search rule* yang berhasil yang ditandai dengan "*Search Completed*"

Pengujian TURN-Server

Berikut adalah hasil uji TURN-Server. Yang pertama adalah mem*block* panggilan panggilan asing yang ingin menyerang *Resource* VoIP

Gambar 19 Percobaan *toll fraud*

Pada gambar 19 pada *log* TURN *server* terjadi percobaan *toll-fraud* yaitu sumber 100xxx@lintasarta.co.id menuju 000xxx@lintasarta.co.id.

Gambar 20 *Call policy*

Call policy merupakan konfigurasi yang berguna untuk memasukan *pattern* yang ingin di*block*. Pada *call policy* ketika ada nomor panggilan dengan awalan angka 0 sampai dengan 9 atau tanda *(bintang) dan menggunakan *domain local* contoh *0213@lintasarta.co.id maka akan dilakukan reject call.

tvcs: Event="Call Attempted" Service="SIP" Src-ip="188.161.105.104" Src-port="52988" Src-alias-type="SIP" Src-alias="sip:1001000000000000s@la-expe.lintasarta.co.id" Dst-alias-type="SIP" Dst-alias="sip:601146812410181@la-expe.lintasarta.co.id" Call-serial-number="d4e5e2df-35aa-4593-9cac-f5e2761cd450" Tag="d1b91d66-a26b-430f-a8ef-348db1a9474a" Protocol="TCP" Auth="NO" Level="1"

Gambar 21 Detail Toll fraud

Pada gambar 21 merupakan *call detail record* pada panggilan yang berpotensi *fraud*. Sumber mencoba melakukan panggilan ke *domain* @lintasarta.co.id

tvcs: Event="Search Attempted" Service="SIP" Src-alias-type="SIP" Src-alias="1001000000000000s@la-expe.lintasarta.co.id" Dst-alias-type="SIP" Dst-alias="sip:601146812410181@la-expe.lintasarta.co.id" Call-serial-number="d4e5e2df-35aa-4593-9cac-f5e2761cd450" Tag="d1b91d66-a26b-430f-a8ef-348db1a9474a" Detail="searchtype:INVITE" Level="1"

Gambar 22 Detail toll fraud

Pada gambar 22 ketika panggilan sudah dicoba maka akan terjadi proses traversal yaitu pencarian dari jaringan luar menuju jaringan internal dengan mencoba melakukan INVITE ke TURN server agar bisa terigester dengan domain @lintasarta.co.id.

tvcs: Event="Search Completed" Reason="Forbidden" Service="SIP" Src-alias-type="SIP" Src-alias="1001000000000000s@la-expe.lintasarta.co.id" Dst-alias-type="SIP" Dst-alias="sip:601146812410181@la-expe.lintasarta.co.id" Call-serial-number="d4e5e2df-35aa-4593-9cac-f5e2761cd450" Tag="d1b91d66-a26b-430f-a8ef-348db1a9474a" Detail="found:false, searchtype:INVITE, Info:Policy Response" Level="1"

Gambar 23 Detail toll fraud

Pada gambar 23 ketika proses traversal sudah selesai namun TURN-*Server* melakukan pemberitahuan bahwa nomor tersebut adalah *pattern*-nomor yang sudah di *block* pada *call policy* sehingga TURN-*Server* tidak melakukan registrasi ke nomor tersebut dengan alasan "*Forbidden*".

tvcs: Event="Call Rejected" Service="SIP" Src-ip="188.161.105.104" Src-port="52988" Src-alias-type="SIP" Src-alias="sip:1001000000000000s@la-expe.lintasarta.co.id" Dst-alias-type="SIP" Dst-alias="sip:601146812410181@la-expe.lintasarta.co.id" Call-serial-number="d4e5e2df-35aa-4593-9cac-f5e2761cd450" Tag="d1b91d66-a26b-430f-a8ef-348db1a9474a" Detail="Forbidden" Protocol="TCP" Response-code="403" Level="1"

Gambar 24 detail *toll fraud*

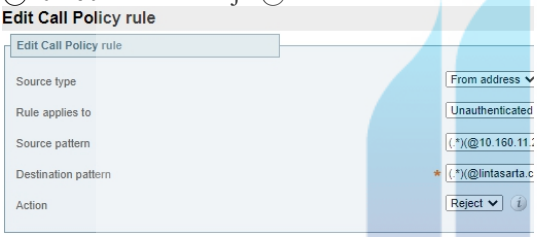
Pada gambar xx terlihat panggilan tidak direspon yaitu dengan status "*Call rejected*" dan dengan detail "*Forbidden*" hal ini menunjukan bahwa serangan *toll fraud* dengan *pattern* yang sudah dimasukan pada *call policy* sebelumnya sudah berhasil melakukan *blocking* dan tidak terregister ke TURN-*Server*.

Pengujian TURN-*Server* Dengan *Pattern* Tertentu

Berikut adalah pengujian dengan *blocking pattern* tertentu. Jika terjadi sebuah *toll fraud* dengan sumber menggunakan *pattern* terntentu

Gambar 25 *Log blocking* IP

Pada gambar 25 terjadi pangilan dari *domain* @10.160.11.21 menuju @lintasarta.co.id



Gambar 26 *Call Policy*

Pada gambar 26 merupakan *call policy* dengan *rules* mem*block* panggilan yang masuk dari *domain* @10.160.11.21 menuju @lintasarta.co.id.

```
tvcs: Event="Call Attempted" Service="SIP" Src-ip="182.23.65.1
Src-port="5061" Src-alias-type="SIP" Src-alias="sip:7771@10.16
Dst-alias-type="SIP" Dst-alias="sip:71670@lintasarta.co.id"
Call-serial-number="1c8775b8-6fb7-4692-a549-3666f8e16ad5"
Tag="960b0f12-24cc-4924-9281-49e3bce09eaf" Protocol="TLS" Auth
```

Gambar 27 Detail Panggilan

Pada gambar 27 merupakan proses percobaan pemanggilan dari *domain* @10.160.11.21 menuju *domain* @lintasarta.co.id

```
tvcs: Event="Search Attempted" Service="SIP" Src-alias-type="SIP"
Src-alias="7771@10.160.11.21" Dst-alias-type="SIP" Dst-alias="sip:71670
Call-serial-number="1c8775b8-6fb7-4692-a549-3666f8e16ad5"
Tag="960b0f12-24cc-4924-9281-49e3bce09eaf"
Detail="searchtype:INVITE" Level="1"
```

Gambar 28 Detail panggilan

Pada gambar 28 merupakan proses percobaan pencarian dari *domain* @10.160.22 21 menuju kedalam jaringan @lintasarta.co.id melalui TURN-Server.

```
tvcs: Event="Search Completed" Reason="Forbidden" S
Src-alias-type="SIP" Src-alias="7771@10.160.11.21"
Dst-alias-type="SIP" Dst-alias="sip:71670@lintasart
Call-serial-number="1c8775b8-6fb7-4692-a549-3666f8e
Tag="960b0f12-24cc-4924-9281-49e3bce09eaf" Detail="
searchtype:INVITE, Info:Policy Response" Level="1"
```

Gambar 29 Detail Panggilan

Pada gambar 29 merupakan proses setelah pencarian selesai namun TURN-*Server* memberikan notifikasi dengan alasan "*Forbidden*"

```
tvcs: Event="Call Rejected" Service="SIP" Src-ip="182.23.65.174" Src-port="5061"
Src-alias-type="SIP" Src-alias="sip:7771@10.160.11.21" Dst-alias-type="SIP"
Dst-alias="sip:71670@lintasarta.co.id"
Call-serial-number="1c8775b8-6fb7-4692-a549-3666f8e16ad5"
Tag="960b0f12-24cc-4924-9281-49e3bce09eaf"
Detail="Forbidden" Protocol="TLS" Response-code="403" Level="1"
```

Gambar 30 Detail Panggilan

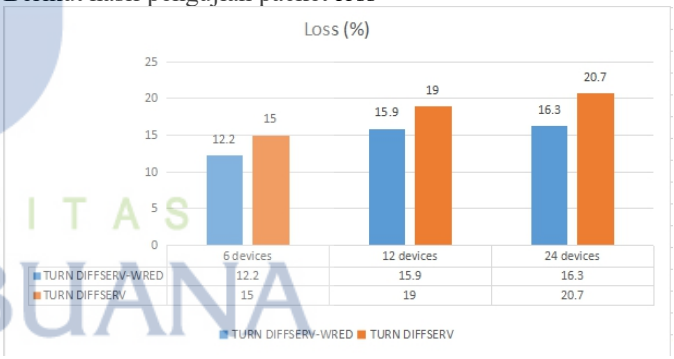
Pada gambar 30 terlihat panggilan tidak direspon yaitu dengan status "*Call rejected*" dan dengan detail "*Forbidden*" hal ini menunjukan bahwa serangan *toll fraud* dengan *domain pattern* tertentu yang sudah dimasukan pada *call policy* sebelumnya sudah berhasil melakukan *blocking* dengan *pattern* tertentu dan tidak terregister ke TURN-*Server*.

Pengujian Diffrentiated Services

Berikut adalah hasil dari pengujian dengan melakukan panggilan secara bersama yaitu sebanyak 6,12,dan 24 devices. Telah dilakukan analisis terkait pengaruh diffrentiated services terhadap kualitas jaringan dari VoIP.

Packet Loss

Berikut hasil pengujian packet loss

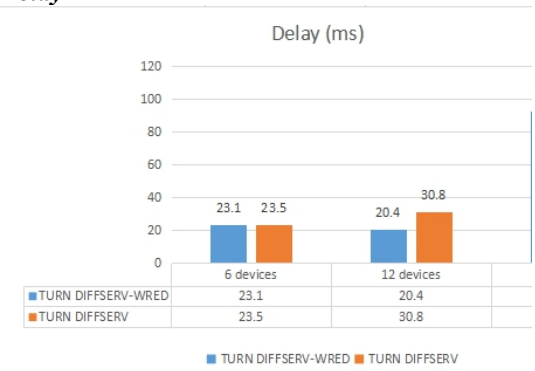


Gambar 31 hasil pengujian *packet loss*

Pada gambar 31 *packet loss* yang didapat dengan diffserv-wred tergolong bagus menurut *standard* tiphon yaitu dengan rata-rata 15% dan diffserv dengan kategori sedang dengan rata-rata 21%, namun pada kapasitas maksimal baik kedua metode tidak mengalami kenaikan yang signifikan yaitu 16.3% pada diffserv-wred dan 20.7% pada diffserv. Hal tersebut terjadi karena proses *marking* VoIP dengan DSCP *field* EF hanya dikonfigurasi oleh salah satu *router* saja namun hal tersebut bisa diatasi dengan menambahkan *Weighted random early access* karena penumpukan paket bisa dihindari dengan melakukan *dropping packet* saat pengiriman. dengan

menambahkan WRED bisa memperbaiki sekitar 20% *loss* daripada hanya menggunakan diffserv.

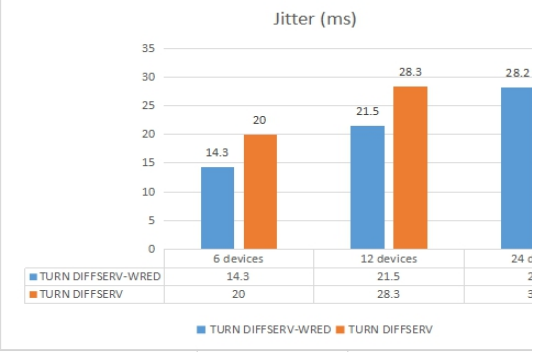
Delay



Gambar 32 hasil pengujian *delay*

pada gambar 32 *delay* yang didapat pada layanan VoIP dengan semua skenario tergolong sangat bagus yaitu diffserv - wred dengan rata-rata 23.1ms di 6 devices dan 20.4ms di 12 devices sedangkan diffserv dengan rata-rata 23.5ms di 6 *devices*. Sedangkan pada kapasitas maksimal 24 *devices*, diffserv-WRED mendapatkan rata rata 92.5ms dan 100.8ms pada diffserv, pada kapasitas maksimal masih dalam kategori bagus menurut *standard* tiphon yaitu <150ms. hal ini terjadi karena pada saat diffserv VoIP melewati jaringan MPLS tidak ada adanya *marking* paket yang menyebabkan paket tidak di prioritaskan dan terjadi delay yang tinggi namun hal tersebut bisa diatasi dengan dengan WRED dikarenakan semakin *packet* dikirim dengan adanya marking DSCP *field* yang memungkinkan *packet* untuk diprioritaskan sampai ke tujuan.

Jitter

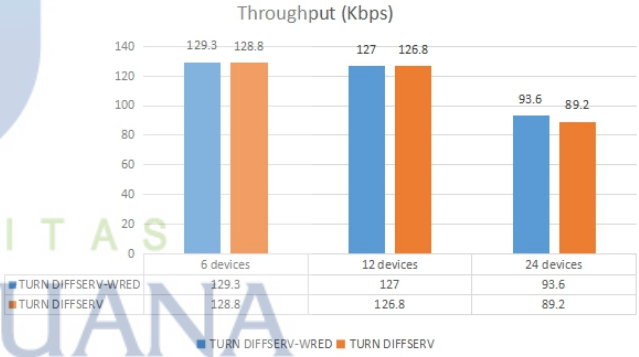


Gambar 33 hasil pengujian *jitter*

Gambar 33 adalah hasil pengujian *jitter* pada layanan VoIP dilihat dari hasil pengujian pada layanan VoIP disemua metode mempunyai selisih yang sedikit dan tidak signifikan. pada percobaan 6 *devices* didapat *jitter* 14.3ms pada metode TURN Diffserv-WRED dan 23.5ms pada metode TURN Diffserv, pada 12 *devices* *jitter* xx pada metode a dan xx pada metode b, dan pada 24 *devices* didapat *jitter* 92.5 pada metode Diffserv-WRED dan 100.8ms pada metode TURN Diffserv. Semakin banyak dilakukan percobaan hasil *jitter* semakin naik, nilai *jitter* tersebut menurut *standard* tiphon masuk kategori bagus pada 6 *devices* dan 12 *devices* yaitu <75ms dan kaetgori sedang pada 24 *devices* dengan standard <125ms. Namun perbedaannya tidak terlalu signfikan di setiap percobaan. pada TURN diffserv-WRED menunjukan jika proses *marking* atau pemberian prioritas pada pengiriman paket dapat mengurangi tingginya *jitter* yang timbul karena antrian paket di *router* meskipun ada *router* yang tidak dikonfigurasi serupa, namun lain halnya dengan TURN Diffserv proses *marking packet* tidak lagi terjadi saat melewati *router* yang tidak dikonfigurasi sehingga menyebabkan *jitter* menjadi tinggi.

Thorughput

Berikut hasil pengujian *Throughput*



Gambar 34 hasil pengujian *throughput*

Gambar 34 adalah hasil pengujian *throughput* pada layanan VoIP. Pada percobaan 6 *devices* terlihat penggunaan *throughput* 100% pada 12 *devices* juga masih 100% dan pada 24 *devices* terlihat penurunan *throughput* yang signifikan yaitu sekitar 70% *throughput* pada kedua metode. penurunan pada 24 *devices* sangat wajar dikarenakan adanya keterbatasan *bandwidth* sebesar 1Mbps namun menurut *standard* tiphon *throughput* 70% masuk kategori sedang dan masih *reliable* untuk melakukan panggilan VoIP. Penggunaan *thorughput* yang masih baik jika semakin banyak *devices* terjadi karna adanya *policy-map bandwidth* sebesar 128Kbps dan juga pada VoIP menggunakan DSCP *field* EF yang

mana besaran *bandwidth* akan diprioritaskan untuk jaringan VoIP.

KESIMPULAN

Berdasarkan hasil penelitian dan pengujian pada dengan semua parameter yaitu baik *toll fraud* secara *random* maupun dengan *pattern* tertentu, berfungsi dengan sangat baik. Pengujian dengan *pattern* tertentu, TURN-*Server* mampu melakukan *blocking pattern* tersebut karena sudah dimasukan *pattern* sebelumnya pada *call policy*. Dan Pengujian *Toll-fraud random* berfungsi dengan baik dikarenakan TURN-*Server* bisa memblocking banyaknya *toll fraud* yang ada dikarenakan *behavior hacker* yang memanfaatkan local *domain* dan nomor dengan *pattern* 0 sampa 9 dan *. Dan juga pengujian kualitas jaringan DIffserv-WRED mampu menjaga QoS dari komunikasi VoIP, namun untuk rata-rata di semua percobaan dan semua parameter QoS dengan Diffserv-WRED memiliki kemampuan yang lebih baik dibanding diffserv, karena diffserv-WRED mampu mengurangi *packet loss* sekitar 15% dan *delay* 10% Diffserv-WRED juga bisa memaksimalkan *Throughput* yaitu 2% dibanding diffserv dan juga mengurangi *jitter* sekitar 8%

UCAPAN TERIMA KASIH / *ACKNOWLEDGMENT*

Terimakasih kepada Dosen Pembimbing yang sudah mau membimbing dengan sabar dalam penyusunan jurnal ini. Terimakasih juga kepada diri saya sendiri karena sudah mampu menyelesaikan jurnal ini.

REFERENSI

[1] T. Chakraborty and I. Saha, *VoIP Technology : Applications and Challenges*. 2018.

[2] V. Mayor, R. Estepa, A. Estepa, and G. Madinabeitia, "Unified call admission control in corporate domains," *Comput. Commun.*, vol. 150, pp. 589–602, 2020, doi: 10.1016/j.comcom.2019.11.041.

[3] R. Handayani, "Voice over Internet Protocol (VOIP) Pada Jaringan Nirkabel Berbasis Raspberry Pi," *Kinetik*, vol. 2, no. 2, p. 82, 2017, doi: 10.22219/kinetik.v2i2.146.

[4] G. A. Risnandar Mohammad, Hendrawan Ade Hendri, Prakosha Bayu Adhi, "Implementasi Voice over Internet Protocol (VoIP) Berbasis Session Initiation Protocol (SIP) Berbantuan Briker versi 1.4 Untuk Pengukuran Quality of Services Pada Jaringan Komputer di Fakultas Teknik UIKA Bogor," *J. UMJ*, no. November, pp. 1–8, 2016.

[5] M. Hariyadi and N. Abidin, "Implementasi Dan Analisa Quality of Service Wireless Voip Berbasis Sip Pada Mobile Adhoc Network Berbasis Openwrt," *NJCA (Nusantara J. Comput. Its Appl.*, vol. 3, no. 2, pp. 135–145, 2018, doi: 10.36564/njca.v3i2.73.

[6] D. P. P. H and L. Y. Astri, "SISTEM MONITORING PARAMETER QOS JARINGAN VoIP LOKAL," vol. 8, no. 2, pp. 29–34, 2013.

[7] A. Najihi, I. M. Wayan, Widyawan, and E. Najwaini, "Analisis Kinerja IP PBX Server pada Single Board Circuit Raspberry PI," *J. POSITIF, Vol. I, No.2, Mei 2016 16 - 24*, vol. I, no. 2, pp. 16–24, 2016.

[8] F. Alamsyah, D. P. Kartikasari, and F. A. Bakhtiar, "Implementasi WebRTC Pada Sistem Broadcast Pembelajaran Untuk Menampilkan Bahasa Isyarat," vol. 3, no. 10, pp. 10331–10336, 2019.

[9] Y. Jung and R. Agulto, "Integrated management of network address translation, mobility and security on the blockchain control plane," *Sensors (Switzerland)*, vol. 20, no. 1, 2020, doi: 10.3390/s20010069.

[10] E. Kfoury and D. Khoury, "Securing natted iot devices using ethereum blockchain and distributed turn servers," *2018 10th Int. Conf. Adv. Infocomm Technol. ICAIT 2018*, no. 1, pp. 115–121, 2018, doi: 10.1109/ICAIT.2018.8686623.

[11] Mitra Unik, S. Soni, and Randra Aguslan Pratama, "Penerapan Metode Htb Dan Diffserv Guna Peningkatan Qos Pada Layanan Video Streaming," *J. Fasilkom*, vol. 9, no. 3, pp. 35–40, 2019, doi: 10.37859/jf.v9i3.1665.

[12] F. Wulansari, R. Munadi, and R. Mayasari, "Analisis Jaringan MPLS-TE Fast Reroute Menggunakan Metode QoS Diffserv Berbasis Server OpenIMSCore," vol. 2016, no. Sentika, pp. 18–19, 2016.

[13] L. D. D. Saputra and W. Sulistyo, "Analisis QoS Differentiated Service pada Jaringan MPLS Menggunakan Algoritma Threshold," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 4, p. 227, 2017, doi: 10.25126/jtiik.201744427.

[14] R. Novrianda, "Implementasi authentication Captive Portal pada Wireless Local Area Network PT. Rikku Mitra Sriwijaya," *Regist. J. Ilm. Teknol. Sist. Inf.*, vol. 4, no. 2, p. 67, 2018, doi: 10.26594/register.v4i2.1245.

[15] W. Efendi and R. Yusuf, "Implementation of Dynamic Routing OSPF and Loopback IP for Failover IBGP Connections," *Int. J. Comput. Appl.*, vol. 178, no. 37, pp. 31–37, 2019, doi: 10.5120/ijca2019919245.

KERTAS KERJA

Ringkasan

Kertas kerja ini merupakan material kelengkapan artikel jurnal dengan judul di atas. Kertas kerja berisi semua material hasil penelitan Tugas Akhir yang tidak dimuat/atau disertakan di artikel jurnal. Di dalam kertas kerja ini disajikan: literature review, dataset yang digunakan, source code, dan hasil eksperimen secara keseluruhan