SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK IV - Surabaya, 27 April 2024
Ruang Seminar Gedung A, Kampus Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2024.5925

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Implementasi Keamanan ACL dan Pembatasan Porsi Host pada Wifi Router untuk Layanan FTTH Jaringan Indihome

Anggoro Arie Dewanto, Shah Khadafi, Dimas Bima Bagaskara, Resa Uttungga

Institut Teknologi Adhi Tama Surabaya
e-mail: khadafi@itats.ac.id

ABSTRACT – Font 10

the hierarchical structure of a computer network that can be developed into an internet network is very dependent on the development and reliability of the supporting infrastructure within it. The increasingly widespread use of computer network access using internet access, and the increasing number of devices connected to the internet network, unknowingly results in some users who are not authorized or unable to disrupt the internet network, which results in misuse of customer access security. PT Telkomsel Indonesia (Persero) Tbk, as the internet network provider, has very high speed services using fiber optic or Fiber To The Home (FTTH) known as IndiHome. For users who have registered and used IndiHome products, supporting devices such as fiber optic cables and communication devices such as OLT, ONT, ONU, and UTP cables and Wi-Fi Router devices have been previously provided. Internet network access security is very necessary for users who use IndiHome services. The router's role is most important when sending electromagnetic signals to computers, laptops and smartphones owned by users, sometimes devices owned by other people who cannot also get internet access or are called unauthorized users. This research implements the IP address subnetting technique to limit access to Router devices used as internet network gateways, and the Media Access Control (MAC) Access Control List (ACL) technique to record the MAC addresses of devices owned by users who access the internet. The results of this research show that by implementing IP subnets you can limit users through predetermined host portion limits of 5 so that they get reject status, and MAC ACLs that can record MAC addresses so that they get permission to use internet access.

Keywords: subnetting IP address; ACL; wifi router; IndiHome internet; network computer.

ABSTRAK

Struktur hirarki jaringan komputer yang dapat dikembangkan menjadi jaringan internet sangat bergantung terhadap pengembangan dan keandalan infrastruktur pendukung di dalamnya. Semakin luas akses jaringan komputer menggunakan yang menggunakan akses internet, dan semakin banyak perangkat-perangkat yang terkoneksi jaringan internet, tanpa disadari mengakibatkan beberapa pengguna yang tidak berhak atau tidak diizinkan dapat mengganggu jaringan internet, yang berakibat pada keamanan akses pelanggan yang disalahgunakan. PT Telkomsel Indonesia (Persero) Tbk, selaku *provider* jaringan internet memiliki layanan kecepatan yang sangat tinggi menggunakan fiber optic atau *Fiber To The Home* (FTTH) yang dikenal dengan IndiHome. Bagi pengguna yang telah mendaftar dan menggunakan produk IndiHome, telah disediakan sebelumnya perangkat pendukung seperti kabel fiber optic beserta perangkat komunikasinya seperti OLT, ONT, ONU, dan kabel UTP beserta perangkat Wi-Fi Router. Keamanan akses jaringan internet sangat diperlukan bagi pengguna yang memanfaatkan layanan IndiHome. Peranti Router paling penting ketika mengirimkan sinyal elektromagnetik bagi komputer, Laptop, dan SmartPhone yang dimiliki pengguna, terkadang perangkat yang dimiliki oleh orang lain yang tidak berhak juga dapat mendapatkan akses internet atau disebut dengan unauthorized user. Penelitian ini mengimplementasikan teknik subnetting IP *address* untuk membatasi akses perangkat Router yang digunakan sebagai gateway jaringan internet, dan teknik *Media Access Control* (MAC) *Access Control List* (ACL) untuk melakukan perekaman MAC *address* perangkat-perangkat yang dimiliki pengguna melakukan akses internet. Hasil dari penelitian ini menunjukkan bahwa dengan mengimplementasikan *subnet* IP dapat membatasi pengguna melalui batasan porsi host sebanyak 5 saja yang telah ditentukan sehingga mendapatkan status *deny*, dan MAC ACL yang dapat merekam MAC address sehingga mendapatkan *permit* menggunakan akses internet.

Kata kunci: subnetting IP address; ACL; wifi router; IndiHome internet; jaringan komputer.

PENDAHULUAN

Jaringan komputer memiliki struktur hirarki yang berjenjang yang terdiri dari komputer, infrastruktur jaringan, dan *software* yang terintegrasi, yang menyediakan sebuah layanan yang telah ditentukan bagi *end user* [1]. Setiap perangkat yang terhubung dengan jaringan komputer mengakses layanan jaringan secara *online* yang menggunakan infrastruktur jaringan komputer [2]. Infrastruktur jaringan diantaranya, Wi-Fi Router, Switch, kabel Fiber Optik dan kabel *Unshielded Twisted Pair* (UTP). Peranti *Router* merupakan perangkat yang dapat dengan mudah diatur untuk melakukan manajemen *user*, membatasi pemakaian bandwidth, mengatur *inbond* dan *outbond* trafik jaringan, dan juga mengatur keamanan jaringan.

Untuk dapat bertukar informasi atau mengirimkan data, jaringan internet menggunakan standar *protocol* jaringan komunikasi yaitu *Transmision Control Protocol* dan *Internet Protocol* yang disingkat TCP/IP. Protokol TCP/IP memberikan kemudahan akses jaringan melalui pengalamatan *host* yaitu IP *address* beserta *subnetmask*. Penggunaan IP dan *subnetmask* diimplementasikan pada setiap perangkat yang terhubung dengan jaringan, sehingga masing-masing perangkat memiliki IP address yang unik yang berbeda dengan komputer *host* yang lain. Penggunaan IP *address* yang sembarangan, dan pemetaan IP yang tidak terencana dengan baik, menyebabkan penyalahgunaan dari sisi *user* dan sering terjadinya celah bagi *intruder* atau penyusup untuk melakukan aktivitas *intrusion system* [3]. Jaringan yang tidak memiliki monitoring atau pengawasan dan pencegahan terhadap adanya penyusup yang berstatus *authorized user*, lebih mudah masukmya serangan atau ancaman yang dilakukan oleh *intruder* [4].

Perusahaan-perusahaan penyedia jasa internet diharuskan dan diwajikan untuk melakukan pengamanan terhadap koneksi jaringan internet yang disediakan ke seluruh pelanggannya. Peraturan tersebut berdasarkan Undang-undang No.36 tahun 1999 yang digagas oleh Kementerian KOMINFO (Komunikasi dan Informatika) [5]. Pemerintah melalui KOMINFO mengantisipasi maraknya kejadian-kejadian serangan *cyber* yang dilakukan oleh penyusup yang dapat mengeksplotasi kelemahan jaringan, yang masuk melalui perangkat

jaringan yang dapat menyebabkan *vulnerability* [6], atau kelemahan yang dimiliki sistem jaringan [7]. Dengan adanya kejadian tersebut, sering terjadinya eksploitasi bidang keamanan komputer di dalamnya. Diperlukan keamanan yang dapat mendeteksi dan mengetahui adanya aktivitas adanya serangan *cyber*.

PT. Telkom Indonesia (Persero) Tbk, sebagai perusahaan *Internet Service Provider* (ISP) dan penyedia jaringan telekomunikasi secara lengkap di Indonesia, memiliki salah satu layanan yang sangat digemari yaitu Indonesia Digital Home disingkat IndiHome adalah salah satu layanan dari PT. Telkom Indonesia berupa paket layanan komunikasi dan data dengan kecepatan yang sangat tinggi yang disebut dengan *Fiber To The Home* (FTTH). Fitur-fitur yang dimiliki oleh IndiHome diantaranya *Voice over Internet Protocol* (VOIP), jaringan internet (*Internet on Fiber atau High Speed Internet*), dan televisi interaktif (UseeTV Cable, IPTV) [8]. Selain itu, pelanggan juga mendapatkan tayangan TV berbayar dan juga saluran telepon rumah. Perangkat FTTH pada jaringan rumahan yaitu Wi-Fi Router, Switch, kabel Fiber Optik dan kabel *Unshielded Twisted Pair* (UTP). Akses jaringan internet melalui FTTH yang menggunakan kabel jaringan fiber optic menggunakan serat silica, infra merah atau berbasiskan cahaya, yang instalasinya harus direncanakan dengan baik sehingga dapat melakukan transmisi data, dan dapat memenuhi kebutuhan pengguna melakukan akses internet [9]. Dengan berbagai metode akses tersebut, memungkinkan pelanggan mengakses internet dari jarak jangkauan yang diizinkan perangkat yang digunakan tanpa adanya batasan pengguna.

Permasalahan-permasalahan yang sering dihadapi pada jaringan IndiHome selaku penyedia jasa internet, terutama perangkat Wi-Fi *Router* yang menyebarkan sinyal elektromagnetik yang membawa trafik jaringan internet. Wi-FI Router yang digunakan oleh IndiHome terkadang belum dapat melakukan pembatasan akses jaringan internet untuk orang lain dan yang tidak diizinkan, masih bisa mendapatkan akses internet atau disebut dengan *unauthorized user*. Permasalahan pendistribusian/peminjaman IP *address* oleh Wi-Fi Router tidak terstruktur dengan baik, yang mengakibatkan *unauthorized user* masih mendapatkan IP *address* yang mengakibatkan orang lain di luar rumah masih dapat mengakses internet. Penelitian ini bertujuan untuk mengimplementasikan keamanan pada layanan Wi-Fi IndiHome pada perangkat Wi-Fi Router yang menggunakan teknik keamanan *Media Access Control* (MAC) *Access Control List* (ACL) [10] [11], yang dapat melakukan akses penolakan atau penerimaan akses memanfaatkan informasi *header* pada MAC address yang terdapat lapisan Data Link pada protokol OSI [12]. Untuk melakukan pembatasan *host* yang akan melakukan akses terhadap jaringan internet, maka penelitian ini juga melakukan subnetting IP *address* terhadap di dalam perangkat router yang bertindak selaku Router gateway, sehingga dapat memberikan batasan jumlah porsi host yang dapat mengakses jaringan internet dengan memanfaatkan layanan dari IndiHome.

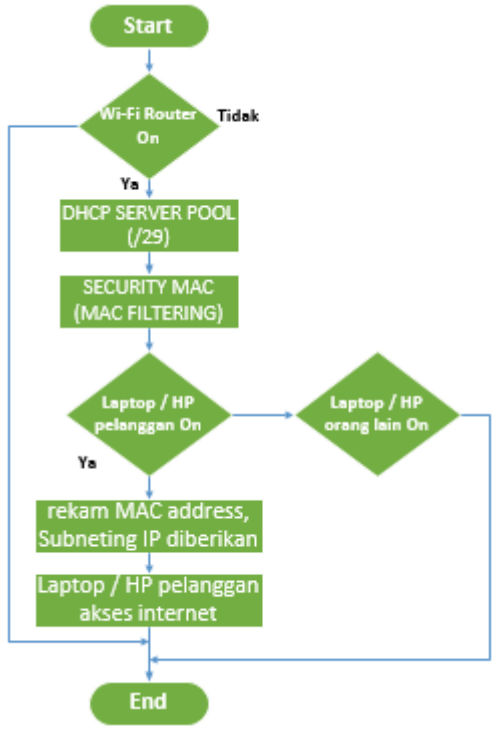
METODE

Metode Penelitian

Rancangan keamanan akses jaringan internet terhadap perangkat Wi-Fi Router ini dengan memanfaatkan beberapa fitur yang dimiliki oleh Wi-Fi *Router*, yaitu fitur IP *address* menggunakan teknik subnetting IP *address* dan juga fitur ACL (*access control list*). *Subnetting* IP yang digunakan untuk penelitian ini, yaitu prefiks ("/") 29. Penggunaan prefiks /29 sebagai pembatas jumlah *host* yang terhubung dengan perangkat Wi-Fi Router untuk koneksi dengan jaringan internet, sesuai dengan jumlah perangkat di rumah sebanyak 5 perangkat, yang terdiri dari Laptop dan HandPhone (spesifikasi subnet IP pada Tabel 2).

Metode penelitian disajikan dalam bentuk diagram alir atau *flowchart*. *Flowchart* rancangan keamanan pada jaringan IndiHome nampak pada Gambar 1. Ketika perangkat Wi-Fi Router sudah menyala (On), kemudian diatur IP address pada fitur DHCP servernya untuk mengimplementasikan IP subnet. Selanjutnya, melakukan pengaturan keamanan MAC address melalui fitur MAC Filtering. Maka, ketika semua perangkat Laptop atau HP dalam keadaan

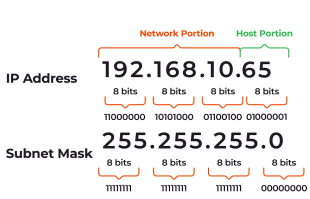
menyala dan ingin koneksi dengan jaringan internet, Laptop atau HP tersebut melakukan *request* IP *address* kepada Wi-Fi *Router*, Ketika IP *address* telah *acknowledged* (disetujui) dan diberikan ke perangkat, selanjutnya fitur ACL dalam Wi-Fi *Router* menyimpan MAC *address* dan diberikan status ***permit*** untuk melakukan akses jaringan Internet. Bila terdapat perangkat orang lain yang berusaha melakukan akses internet melalui Wi-Fi Router, maka statusnya ***deny***, dikarenakan Subnetting IP *address* sudah melebihi porsi dan MAC *address* tidak terekam di dalam fitur ACL.



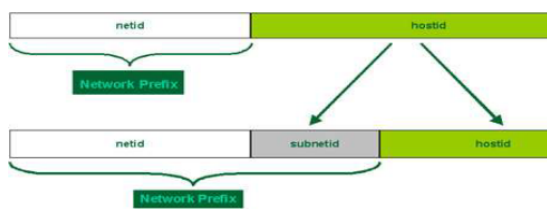
Gambar1. *Flowchart* Keamanan Jaringan Internet Wi-FI IndiHome.

Subnetting IP

Tujuan dilakukan *subnetting* IP adalah untuk membatasi *request* IP *address* yang dilakukan oleh semua perangkat rumahan yang berjumlah 5 unit perangkat. Subnetting adalah teknik yang digunakan untuk menentukan porsi jaringan ataupun porsi *host* yang akan digunakan seperti yang nampak pada Gambar 2, khususnya IP address berbasiskan panjang biner 32-bit. Teknik subnetting biasanya memperluas *mask* bernilai "1" pada sebagian bit porsi *host*.



(a)



(b)

Gambar 2. (a) Ilustrasi Notasi Biner IP address dan Subnet Mask, (b) Blok Network dan Subnetwork Pada IP Address

Untuk menentukan porsi jumlah *subnetwork* dalam sebuah jaringan lokal menggunakan Persamaan 1, sedangkan untuk menentukan porsi jumlah *subnetwork* dalam sebuah jaringan lokal menggunakan Persamaan 2.

$$jumlah\ subnet\ =\ 2\hat{}n \qquad \text{Persamaan 1}$$

Keterangan:
n : jumlah bit yang dipinjam

$$jumlah\ host\ per\ subnet\ =\ (2\hat{}h)\ -\ 2 \qquad \text{Persamaan 2}$$

Keterangan:
n : jumlah bit tersisa yang tidak dipinjam

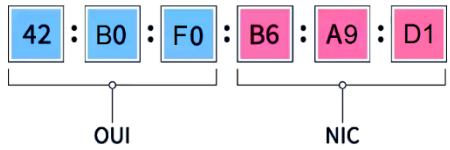
Tabel 1. Spesifikasi Pembagian *Subnetting* pada IP *Address*

Desimal Subnet mask	/	Biner Subnet Mask	Jumlah	
			Host /subnet	Subnet
255.255.255.128	/25	11111111.11111111.11111111.10000000	126	2
255.255.255.192	/26	11111111.11111111.11111111.11000000	62	4
255.255.255.224	/27	11111111.11111111.11111111.11100000	30	8
255.255.255.240	/28	11111111.11111111.11111111.11110000	14	16
255.255.255.248	/29	11111111.11111111.11111111.11111000	6	32
255.255.255.252	/30	11111111.11111111.11111111.11111100	2	64

Hasil perhitungan jumlah *subnet* dan *host per subnet* pada masing-masing "/" (prefix) yaitu /25, /26, /27, /28, /29, dan /30 pada Tabel 1, menunjukkan bahwa semakin banyak biner dipinjam pada porsi *host* yang mask bernilai "1", maka semakin sedikit jumlah *host per subnet* dan semakin banyak subnet yang dimiliki.

MAC ACL

Media Access Control (MAC) *address* merupakan alamat identitas sebuah peranti network (*Ethernet card*) yang terdapat pada komputer, laptop ataupun perangkat SmartPhone/HP. Gambar 3 mengilustrasikan format penomoran MAC *address* berdasarkan dari kombinasi bilangan decimal dan heksadesimal yang terdiri dari 6 set karakter berpasangan, masing-masing pasangan dipisahkan dengan titik dua (":"). Singkatan OUI kepanjangan dari *Organizationally Unique Identifier* yang merupakan keterangan dari pembuat perangkat atau manufaktur perangkat jaringan, sedangkan NIC kepajangan dari *Network Interface Card*.



Gambar 3. Ilustrasi Notasi Bilangan Heksadesimal MAC Address

Access Control List (ACL) terinstall di dalam Router melakukan kontrol terhadap trafik *network* data *inbond* ataupun *outbond* yang melintasi perangkat Router. ACL yang menyimpan nomor alamat *source* MAC dapat ***permit*** atau ***deny*** menolak akses ke lalu lintas yang menggunakan informasi lapisan nomor 2 yaitu *Datalink*. Implementasi MAC ACL sebagai keamanan akses internet pada jaringan IndiHome terutama untuk mengontrol host atau perangkat

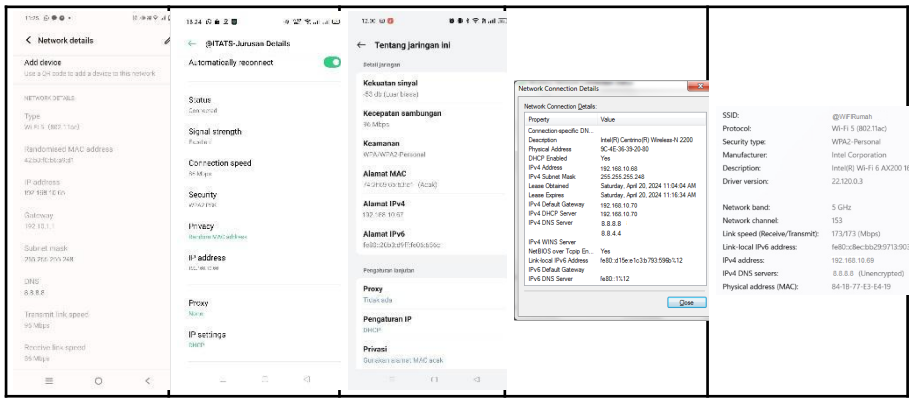
mana saja yang dapat atau tidak dapat mengakses jaringan rumah. Dengan MAC ACL sebagai *permit* (mengizinkan) atau *deny* (menolak) sinyal elektromagnetik dari Wi-FI Router.

HASIL DAN PEMBAHASAN

Hasil Implementasi Keamanan Wi-FI Router Jaringan FTTH

Sebagai objek penelitian pada rumah pelanggan Wi-FI IndiHome, terdiri dari 5 unit perangkat, yaitu HandPhone sebanyak 3 unit, dan Laptop sebanyak 2 unit. Dimana semua perangkat tersebut terhubung dengan sebuah Wi-Fi *Router* dengan fitur Router *management*. Sedangkan sebuah perangkat yang lain, dalam hal ini sebagai perangkat *guest* (HP *guest*) yang digunakan oleh orang lain yang bukan bagian dari daftar *user* di rumah tersebut. Implementasi keamanan jaringan FTTH untuk akses internet ini menggunakan fitur yang dimiliki oleh perangkat Router Wi-Fi, yaitu IP *Subnetting* dan *Media Access Control* (MAC) *Access Control List* (ACL).

Hasil mengimplementasikan teknik keamanan pada jaringan FTTH IndiHome menggunakan subnetting IP *address* dan MAC ACL, dimana semua perangkat yang ada di rumah melakukan akses jaringan internet. Perangkat Wi-Fi Router dengan SSID "**@WiFiRumah**", memberikan *subnet* IP *address* prefix /29 ke semua perangkat rumah. Hasilnya ditunjukkan pada tangkapan layar pada masing-masing perangkat, pada menu *Network Properties* yang nampak pada Gambar 4. Gambar 4 (a) tampilan menu *Network Properties* HP 1 (IP: 192.168.10.65, *subnet mask*: 255.255.255.248), Gambar 4 (b) tampilan menu *Network Properties* HP 2 (IP: 192.168.10.66, *subnet mask*: 255.255.255.248), Gambar 4 (c) tampilan menu *Network Properties* HP 3 (IP: 192.168.10.67, *subnet mask*: 255.255.255.248), Gambar 4 (d) tampilan menu *Network Properties* Laptop 1 (IP: 192.168.10.68, *subnet mask*: 255.255.255.248), dan Gambar 4 (e) tampilan menu *Network Properties* Laptop 2 (IP: 192.168.10.69, *subnet mask*: 255.255.255.248).



(a) (b) (c) (d) (e)

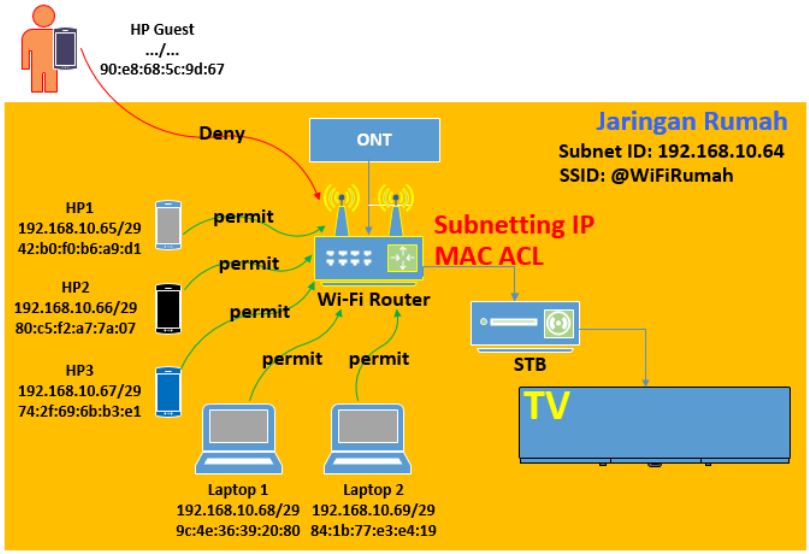
Gambar 4. Hasil *Request* IP *address* Dari Perangkat Di Dalam Jaringan Rumah

Pembahasan Data

Keadaan perangkat Laptop atau HP yang ada di rumah terhadap koneksi internet diilustrasikan seperti pada Gambar 5. Perangkat-perangkat yang digunakan oleh pelanggan terdiri dari Laptop (2 unit) dan SmartPhone (3 unit) mendapatkan akses jaringan IndiHome berkat layanan DHCP *server* yang sudah *include* di dalam fitur Wi-Fi *Router*. IP *address* yang diberikan oleh Wi-Fi Router melalui proses DHCP *request* yang dilakukan oleh perangkat Laptop dan SmartPhone. Selanjutnya *Router* memberikan jawaban persetujuan melalui proses DHCP

acknowledge. Sehingga masing-masing perangkat rumah dapat akses jaringan internet dengan subnet IP menggunakan subnet IP 192.168.1.64/29.

Fitur MAC *address filtering* pada perangkat Wi-Fi *Router* melakukan perekaman nomor MAC *address* yang dimiliki masing-masing perangkat di rumah pelanggan, terutama setelah melakukan koneksi ke jaringan internet. Nomor-nomor MAC address tersebut disimpan ke dalam database sistem Wi-Fi Router yang terinstall di dalam perangkat, dan selanjutnya nomor MAC tersebut diberikan status akses "***permit***" yang berarti diizinkan koneksi ke jaringan internet. Untuk perangkat yang lain yaitu perangkat *guest* (HP *guest*) yang bukan bagian dari daftar *user* di rumah tersebut, nomor MAC address tidak direkan, dan diberikan status akses "***deny***" yang berarti tidak diizinkan koneksi ke jaringan internet.



Gambar 5. Topologi Star Untuk FTTh IndiHome

Hasil Subnetting IP dan MAC ACL

Daftar subnet IP *address* dan MAC *address* beserta spesifik informasi mengenai akses jaringan internet pada masing-masing perangkat di rumah, disajikan pada Tabel 2. Semua perangkat Laptop dan HandPhone yang dimiliki oleh pelanggan, telah berhasil mendapatkan subnet IP address yang masing-masing perangkat berada pada prefix /29 dengan batasan porsi host sebanyak 5 unit. Perangkat Wi-Fi Router dapat menyimpan informasi MAC *address* melalui ACL dan memberikan status ***permit*** mengakses internet kepada masing-masing perangkat milik pelanggan IndiHome. Sedangkan pengguna lain (bukan pelanggan) atau disebut dengan *user Guest* yang memiliki MAC *address* yang tidak termasuk dalam ACL, memberikan status ***deny*** akses internet, sehingga tidak mendapatkan jatah porsi subnet IP *address*.

Tabel 2. Spesifikasi dan Status SmartPhone dan Laptop Terkoneksi Wi-Fi Router

Unit	Merk & Sitem	Address		Status
		IP Subnet	MAC	
HP 1	VIVO, Android	192.168.1.65/29	42:b0:f0:b6:a9:d1	Permit
HP 2	OPPO, Android	192.168.1.66/29	80:c5:f2:a7:7a:07	Permit

HP 3	SAMSUNG, Android	192.168.1.67/29	74:2f:69:6b:b3:e1	Permit
Laptop 1	TOSHIBA, Windows	192.168.1.68/29	9c:4e:36:39:20:80	Permit
Laptop 2	ASUS, Windows	192.168.1.69/29	84:1b:77:e3:e4:19	Permit
HPguest	-		-	Deny

KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa:

1. Jaringan FTTH fiber optic pada IndiHome memiliki kecepatan sangat tinggi, namun tidak memiliki keamanan akses jaringan internet.
2. Implementasi keamanan pembatasan porsi host sebanyak 5 perangkat yang dimiliki oleh pelanggan menggunakan subnet IP address atau prefiks /29.
3. Implementasi keamanan MAC LAC dapat mencegah (*deny*) perangkat lain yang bukan pelanggan untuk mengakses jaringan internet IndiHome.

DAFTAR PUSTAKA

[1] A. S. Y. Irawan *et al.*, *PENGENALAN JARINGAN KOMPUTER*. Get Press Indonesia, 2023.

[2] F. A. Muthahari, S. Khadafi, I. T. Adhi, and T. Surabaya, "SNESTIK Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika Implementasi VPS Pada Cloud Infrastructure Untuk Layanan Mail Server Personal PT.Garuda Voucher Indonesia," in *Seminar Nasional Sistem Informasi Indonesia*, 2022, p. 239. [Online]. Available: https://ejurnal.itats.ac.id/snestikdanhttps://snestik.itats.ac.id

[3] S. Khadafi, B. D. Meilani, and S. Arifin, "Sistem Keamanan Open Cloud Computing Menggunakan Ids (Intrusion Detection System) Dan Ips (Intrusion Prevention System)," *J. IPTEK*, vol. 21, no. 2, p. 67, 2017, doi: 10.31284/j.iptek.2017.v21i2.207.

[4] S. Khadafi, Y. D. Pratiwi, and E. Alfianto, "Keamanan Ftp Server Berbasiskan IDS Dan IPS Menggunakan Sistem Operasi Linux Ubuntu," *Netw. Eng. Res. Oper.*, vol. 6, no. 1, p. 11, 2021, doi: 10.21107/nero.v6i1.190.

[5] K. P. I. dan H. K. Kominfo, "Kewajiban Pengamanan Jaringan Bagi Seluruh Penyelenggara Internet Service Provider (ISP)/ Network Access Provider (NAP)," *KOMINFO*, 2015. https://www.kominfo.go.id/content/detail/4603/siaran-pers-no-18pihkominfo32015-tentang-kewajiban-pengamanan-jaringan-bagi-seluruh-penyelenggara-internet-service-provider-isp-network-access-provider-nap/0/siaran_pers

[6] G. A. Herdiana and M. Sudarma, "Audit Configuration and Vulnerability Router on Diskominfos of Bali Province," *Ojs.Unud.Ac.Id*, vol. 6, no. 2, pp. 100–104, 2021, [Online]. Available: https://ojs.unud.ac.id/index.php/ijeet/article/download/IJEET.2021.v06.i01.p17/39912

[7] H. Fardiansyah *et al.*, *Cyber Crime Paling Populer pada Era Digital*. Media Sains Indonesia, 2022.

[8] Telkomsel, "Pilihan Paket IndiHome Internet UnlimitedNo Title," *Telkomsel*, 2024. https://indihome.co.id/paket/daftar (accessed Mar. 15, 2024).

[9] A. Pratama, Muhammad Rizki Kusuma; Khadafi, Shah; Pakarbudi, "Implementasi Manajemen Proyek Dengan Metode CPM (Critical Path Method) Tentang Optimalisasi Durasi Proyek Pemasangan Fiber Optik Diperusahaan XYZ," *Implementasi Manaj. Proy. Dengan Metod. CPM (Critical Path Method) Tentang Optim. Durasi Proy. Pemasangan*

Fiber Opt. Diperusahaan XYZ, pp. 233–240, 2021.

[10] S. N. M. P. Simamora, N. Hendrarini, and L. E. Sitepu, "Metode Access Control List sebagai Solusi Alternatif Seleksi Permintaan Layanan Data Pada Koneksi Internet," *J. Teknol. Inf. Politek. Telkom*, vol. 1, no. 1, pp. 15–19, 2011.

[11] A. T. Laksono and M. A. H. Nasution, "Implementasi Keamanan Jaringan Komputer Local Area Network Menggunakan Access Control List pada Perusahaan X," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 83, 2020, doi: 10.30865/json.v1i2.1920.

[12] S. Khadafi, S. Nurmuslimah, and F. K. Anggakusuma, "Implementasi Firewall Dan Port Knocking Sebagai Keamanan Data Transfer Pada Ftp Server Berbasiskan Linux Ubuntu Server," *J. Ilm. NERO*, vol. 4, no. 3, pp. 181–188, 2019, [Online]. Available: https://nero.trunojoyo.ac.id/index.php/nero/article/view/137/127