



## Perancangan *Backup Link* Menggunakan Metode HSRP (*Hot Standby Router Protocol*) Dalam Penyediaan *Layer-3* Redundansi

Tommy Elco Geraldi, Moh.Iwan Wahyuddin, Andri Aningsih

Fakultas Teknologi Komunikasi dan Informatika, Informatika, Universitas Nasional, Jakarta, Indonesia

Email: [tommyelco@gmail.com](mailto:tommyelco@gmail.com), [iwan\\_wyd@yahoo.com](mailto:iwan_wyd@yahoo.com), [andrianingsih@civitas.unas.ac.id](mailto:andrianingsih@civitas.unas.ac.id)

**Abstrak**—Dengan bertambahnya pengguna jaringan internet saat ini jika hanya memiliki satu router, apabila router tersebut mengalami gangguan (*down*), maka internet tidak akan bisa digunakan. Berdasarkan penelitian terdahulu, penerapan metode HSRP (*Hot Standby Router Protocol*) dengan membuat satu *active link* dan satu *backup link* dapat mengatasi hal tersebut. Pada penelitian ini akan menggunakan metode HSRP, VTP (*Vlan Trunking Protocol*), InterVLAN, dan VLAN (*Virtual Local Area Network*) sebagai pembanding. pengujian pada penelitian ini akan menggunakan parameter *packet loss* dan *throughput*. Dari hasil pengujian yang telah dilakukan menunjukkan bahwa dengan penerapan metode HSRP dapat memberikan ketersediaan jaringan dengan *packet loss* hanya 0,32%, serta *throughput* sebesar 1,159Mb/s (95,58%) dari penggunaan sebanyak 100 PC.

**Kata Kunci:** Redundancy, Link, HSRP, Metode, Failover

**Abstract**—With the increase of internet user today, if it only has one router, when the router experiencing a network failure, then the internet cannot be used. To overcome this problem, the HSRP (*Hot Standby Router Protocol*) method by creating one active link and one backup link has been applied in the previous research. In this research will be applying the HSRP, VTP (*Vlan Trunking Protocol*), InterVLAN, and VLAN (*Virtual Local Area Network*) as a comparison. The testing parameter in this research will be using *packet loss* and *throughput*. From the result of testing that has been done, it shows that by applying the HSRP method, it gives a network availability with the *packet loss* of only 0,32%, and *throughput* of 1,159Mb/s (95,58%) from using 100 PC.

**Keywords:** Redundancy, Link, HSRP, Method, Failover

### 1. PENDAHULUAN

Dengan bertambahnya pengguna jaringan internet saat ini jika hanya memiliki satu *router*, apabila *router* tersebut mengalami gangguan (*down*), maka internet tidak akan bisa digunakan. Untuk menanggulangi permasalahan yang ada, maka dapat diterapkan konsep metode HSRP (*Hot Standby Router Protocol*), yaitu suatu metode dimana terdapat satu *active link* yang berguna sebagai *link* utama untuk melanjutkan *packet* dan satu *standby link* yang berguna sebagai *backup link* untuk melanjutkan *packet* ketika *link* utama mengalami gangguan dan apabila *link* utama kembali normal, maka *backup link* tersebut akan kembali menjadi *standby* (tidak aktif)[1]-[2].

Sebelumnya dilakukan penelitian oleh Ala Mohamed Ali Mohamed dkk menguji metode HSRP tanpa mengkombinasikan dengan penambahan metode VTP (*Vlan Trunking Protocol*), InterVLAN, dan VLAN (*Virtual Local Area Network*) adalah pilihan terbaik dalam membuat *layer-3* redundansi[3]. Penelitian yang dilakukan oleh Wisnu Purwanto dkk tanpa mengkombinasikan dengan penambahan metode VTP (*Vlan Trunking Protocol*), InterVLAN, dan VLAN (*Virtual Local Area Network*) mengatakan bahwa dengan penerapan metode HSRP dapat memberikan redundansi pada *layer-3* yang handal[4].

Berdasarkan penelitian tersebut, pada penelitian kali ini akan menerapkan metode HSRP (*Hot Standby Router Protocol*) dikombinasikan penambahan metode VLAN (*Virtual Local Area Network*), InterVLAN, dan VTP (*Vlan Trunking Protocol*) yang diharapkan bisa mendapatkan hasil lebih baik.

### 2. METODE PENELITIAN

#### 2.1 HSRP (*Hot Standby Router Protocol*)

HSRP merupakan suatu metode yang diterapkan pada perangkat jaringan Cisco, dimana konsep yang digunakan adalah dengan membuat satu *virtual gateway* IP address pada dua perangkat, sehingga dua perangkat tersebut memiliki *virtual gateway* yang sama satu dengan yang lainnya[5]. HSRP memiliki satu *active link* dan satu *standby link*, dimana *active link* adalah *interface* utama yang bekerja untuk melanjutkan *packet* yang keluar dan masuk, sedangkan *standby link* adalah *interface* kedua (*backup link*) yang akan langsung bekerja secara langsung jika jalur utama mengalami *link down*[6]-[7].

#### 2.2 InterVLAN Routing

InterVLAN Routing adalah metode untuk melakukan *routing* antar VLAN atau untuk meneruskan *traffic* antar VLAN yang telah didaftarkan agar tetap bisa saling terhubung, meskipun memiliki VLAN yang berbeda atau *network* yang tidak berada dalam satu segmen yang sama.

#### 2.3 VTP (*Vlan Trunking Protocol*)

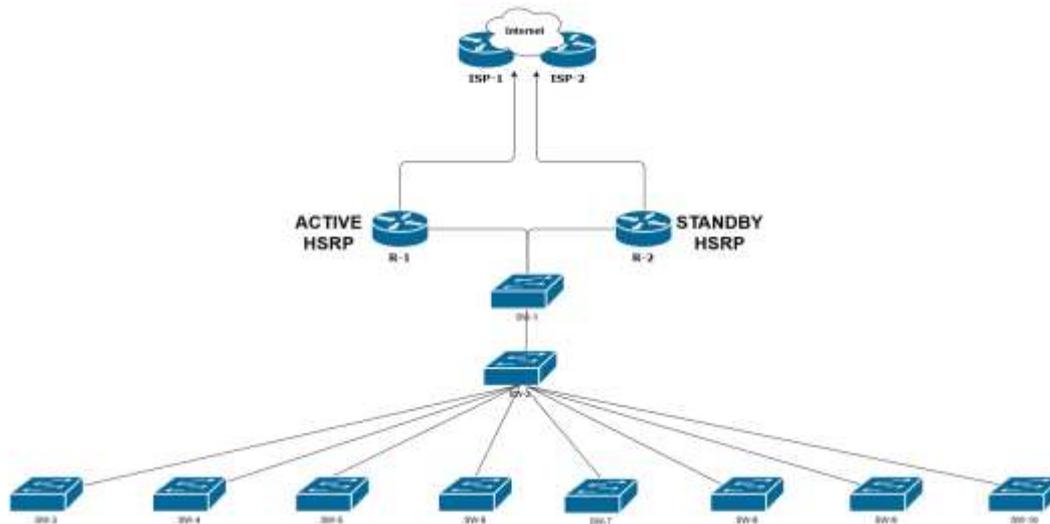


VLAN digunakan untuk membuat beberapa segmen *network* berbeda, namun tetap bisa saling terhubung satu sama lainnya. VTP digunakan untuk metode *trunking* milik Cisco yang berfungsi untuk menyederhanakan pembuatan VLAN pada *switch*, sehingga proses pembuatan VLAN tidak harus dilakukan pada semua *switch*.

Semua konfigurasi akan dilakukan melalui CLI (*Command Line Interface*) menggunakan aplikasi *terminal* SecureCRT pada perangkat Cisco yang akan disimulasikan menggunakan aplikasi GNS3 (*Graphical Network Simulator 3*). SecureCRT adalah aplikasi *terminal emulator* yang berguna untuk melakukan SSH, TELNET, dan juga mengkonfigurasi perangkat jaringan. GNS3 (*Graphical Network Simulator 3*) merupakan aplikasi simulasi jaringan komputer berbasis GUI yang bersifat *open source*. GNS3 dapat mensimulasikan jaringan yang kompleks dan memiliki berbagai fitur yang dapat digunakan untuk keperluan seperti *design, testing, training*, dan juga penelitian menggunakan Cisco IOS (*Cisco Internetwork Operating System*) dari *router* dan *switch* asli.

### 2.4 Kerangka Penelitian

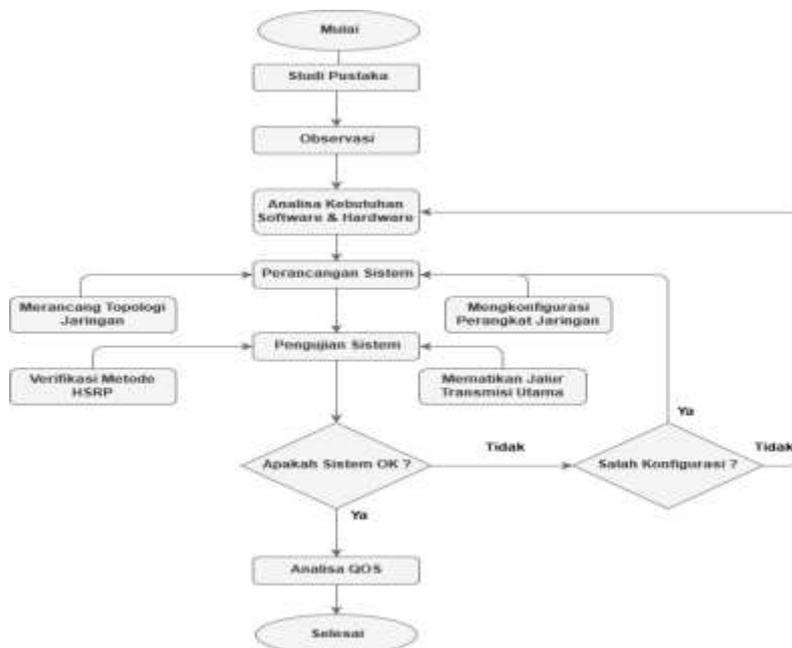
Penelitian ini menerapkan metode HSRP (*Hot Standby Router Protocol*) dalam perancangan jaringan yang dibuat dan disimulasikan menggunakan aplikasi GNS-3 (*Graphical Network Simulator-3*)



Gambar 1. Desain Topologi

Gambar 1 merupakan desain topologi yang akan diterapkan dalam proses perancangan jaringan pada penelitian ini, dengan mengimplementasikan metode HSRP (*Hot Standby Router Protocol*), sehingga terdapat backup link pada jaringan layer-3 network.

Bagan alur (*Flowchart*) proses perancangan jaringan yang akan menerapkan metode Hot Standby Router Protocol dimulai dari proses studi pustaka sampai dengan analisa QOS dapat dilihat pada gambar dibawah ini.



Gambar 2. Flowchart Perancangan Jaringan Metode HSRP



- Berdasarkan flowchart yang telah dibuat dapat dijelaskan secara ringkas sebagai berikut :
- Mencari jurnal sebagai bahan referensi penelitian.
- Melakukan pengamatan terhadap object yang akan diteliti.
- Meneliti kebutuhan software dan hardware yang akan digunakan dalam melakukan penelitian ini.
- Merancang topologi jaringan serta melakukan konfigurasi pada setiap perangkat jaringan.
- Melakukan pengujian terhadap sistem, apakah sistem hasil rancangan OK. Jika terdapat kesalahan pada konfigurasi jaringan, maka akan kembali ke point d. Jika bukan dari konfigurasi maka kembali pada point c.
- Menganalisa QOS pada jaringan yang telah dibuat dan berjalan dengan benar

**2.5 Kebutuhan Hardware dan Software**

Dalam melakukan penelitian ini dibutuhkan alat pendukung perangkat keras dan lunak, diantaranya adalah :

**2.5.1 Spesifikasi Perangkat Keras**

Tabel dibawah ini adalah spesifikasi perangkat keras yang digunakan dalam melakukan penelitian ini.

**Tabel 1.** Spesifikasi Perangkat Keras

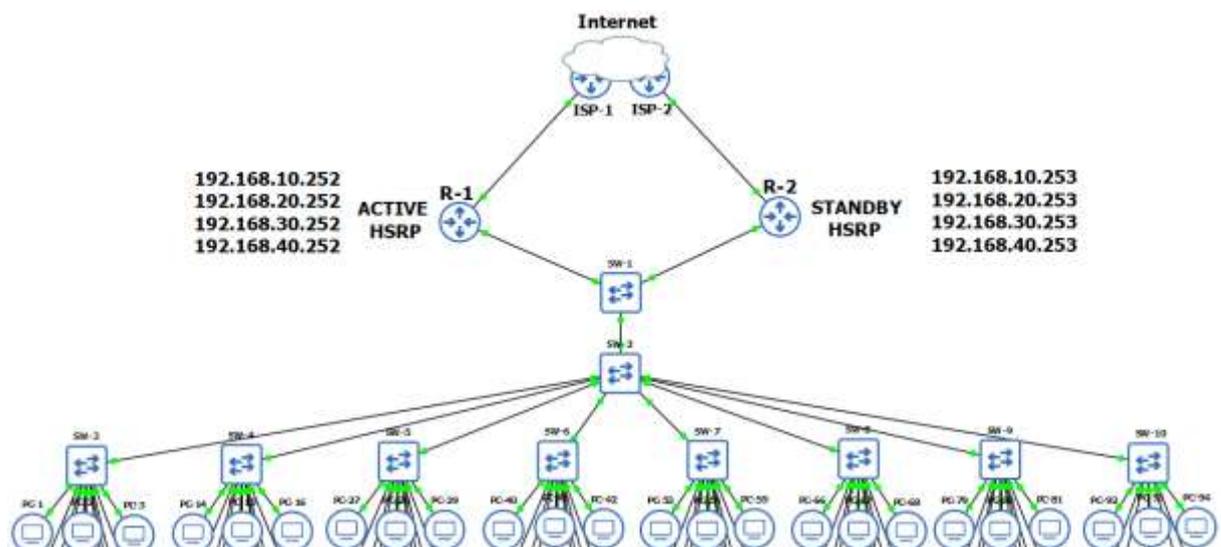
Perangkat	Spesifikasi Perangkat
Processor	Intel i5-8250u 1.60GHz – 3.40GHz
Memory	DDR4 16GB
Storage	SSD 512GB + Harddisk 1TB
VGA	Nvidia Geforce MX150
Monitor	LG-MK600 24 Inch
OS	Windows 10 Pro

**2.5.2 Software**

Dibawah ini adalah software yang digunakan dalam melakukan penelitian ini.

- GNS3**, Software ini digunakan untuk melakukan simulasi jaringan yang telah dirancang.
- VMware**, VMware digunakan sebagai server untuk aplikasi GNS3, yang gunanya untuk memperingan kinerja memori.
- SecureCRT**, SecureCRT ini digunakan sebagai terminal cli untuk mengkonfigurasi perangkat jaringan seperti *router* dan *switch*.
- Wireshark**, Software Wireshark digunakan untuk membantu melakukan analisa pada penelitian ini.
- IOSv**, IOSv digunakan sebagai *virtual OS* pada *router* dan *switch*.

**3. HASIL DAN PEMBAHASAN**



**Gambar 3.** Topologi Jaringan Metode HSRP

Topologi pada Gambar 3. Pada saat PC mengakses internet, user tidak perlu khawatir akan terjadi kegagalan dalam mengirim *packet* jika terjadi *link down* pada jalur transmisi kabel utama, karena secara otomatis *router* akan menggunakan *backup link*. Dalam topologi ini, *router* telah dikonfigurasi metode *Hot Standby Router Protocol*, sehingga dengan adanya metode HSRP maka akan memiliki *backup link*, karena fungsi dari HSRP adalah untuk membuat redundansi pada *layer 3*.



## 3.1 Pengujian Metode *Hot Standby Router Protocol*

Pada tahap ini, akan dilakukan ping dari PC-1 ke IP 8.8.8.8 (google.com) yang bertujuan untuk memastikan bahwa pengiriman *packet* berjalan dengan baik, *trace route* yang bertujuan untuk melihat *hop* yang dilalui dari PC-1 ke alamat IP 8.8.8.8 (google.com) guna memastikan apakah proses *failover* berjalan dengan benar, serta menggunakan *command show standby* pada terminal SecureCRT guna mengetahui status dari HSRP, lalu menguji dengan cara membuat *link down* dengan sengaja pada jalur kabel transmisi utama guna mengetahui apakah perpindahan *link* dari jalur transmisi utama ke *backup link* berlangsung secara otomatis. Hal ini penting untuk menjamin ketersediaan *backup link* ke jaringan secara utuh tanpa perlu adanya pemindahan secara manual yang dapat meningkatkan *down time*. Pada pengujian ini akan secara bertahap menggunakan semua PC yang ada pada topologi jaringan diatas, namun sebagai contoh untuk mengetahui alur kerja dari metode HSRP, pada gambar dibawah ini akan diwakili menggunakan PC-1 sebagai contoh.

### 3.1.1 Pemutusan *Link* dan Proses *Failover*

```
State is Active
1 state change, last state change 00:00:09
Virtual IP address is 192.168.10.254
Active virtual MAC address is 0000.0c07.ac0a
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 2 sec, hold time 3 sec
Next hello sent in 0.192 secs
Preemption enabled
Active router is local
Standby router is 192.168.10.253, priority 160 (expires in 2.336 sec)
Priority 200 (configured 200)
```

**Gambar 4.** Status HSRP Pada R-1 Sebelum Terjadi *Failover*

Pada Gambar 4, bisa dilihat bahwa status *interface* pada R-1 masih dalam keadaan *State is Active*, yang berarti bahwa belum terjadi *failover*, sehingga *packet* yang akan dikirim keluar akan tetap melalui *link* utama, yaitu R-1 seperti yang dapat dilihat pada Gambar 3.

```
PC-1> ping 8.8.8.8 -c 10
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=37.912 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=47.416 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=254 time=34.759 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=254 time=30.106 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=254 time=49.758 ms
84 bytes from 8.8.8.8 icmp_seq=6 ttl=254 time=31.517 ms
84 bytes from 8.8.8.8 icmp_seq=7 ttl=254 time=31.516 ms
84 bytes from 8.8.8.8 icmp_seq=8 ttl=254 time=24.109 ms
84 bytes from 8.8.8.8 icmp_seq=9 ttl=254 time=28.957 ms
84 bytes from 8.8.8.8 icmp_seq=10 ttl=254 time=53.298 ms
```

**Gambar 5.** Kondisi PC-1 Sebelum Terjadi *Failover*

Pada Gambar 5 dilakukan ping dari PC-1 ke alamat IP 8.8.8.8 (google.com) dengan sukses melalui jalur kabel transmisi utama sebelum terjadinya *failover*, yaitu R-1.

```
State is Init (interface down)
2 state changes, last state change 00:00:12
Virtual IP address is 192.168.10.254
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac0a (v1 default)
Hello time 2 sec, hold time 3 sec
Preemption enabled
Active router is unknown
Standby router is unknown
Priority 200 (configured 200)
```

**Gambar 6.** Status HSRP Pada R-1 Setelah Terjadi *Failover*

Pada Gambar 6, terlihat bahwa setelah dengan sengaja dilakukan *link down* pada jalur transmisi utama, status *interface* telah berubah dari *active* menjadi *init* (Tidak aktif lagi), dimana itu berarti proses *backup link* telah terjadi, sehingga sekarang jika ada *packet* yang akan dikirim keluar, maka *packet* tersebut akan melewati *backup link* yang berada pada R-2 seperti yang dapat dilihat pada gambar 3.



```
PC-1> ping 8.8.8.8 -c 10
84 bytes from 8.8.8.8 icmp_seq=1 ttl=254 time=36.380 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=254 time=35.063 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=254 time=32.121 ms
8.8.8.8 icmp_seq=4 timeout
84 bytes from 8.8.8.8 icmp_seq=5 ttl=254 time=23.294 ms
84 bytes from 8.8.8.8 icmp_seq=6 ttl=254 time=22.804 ms
84 bytes from 8.8.8.8 icmp_seq=7 ttl=254 time=22.193 ms
84 bytes from 8.8.8.8 icmp_seq=8 ttl=254 time=18.745 ms
84 bytes from 8.8.8.8 icmp_seq=9 ttl=254 time=15.129 ms
84 bytes from 8.8.8.8 icmp_seq=10 ttl=254 time=45.671 ms
```

**Gambar 7.** Kondisi PC-1 Saat Proses *Failover* ke *Backup Link*

Gambar 7 menunjukkan bahwa pada saat pengiriman *packet* dari PC-1 ke IP 8.8.8.8 (google.com) terjadi *link down* yang dilakukan dengan sengaja, sehingga pada gambar 7 terdapat 1 *packet* yang tidak dapat terkirim. Pada gambar 7 terbukti bahwa *failover* dari *link* utama ke *backup link* berhasil dilakukan, sehingga proses pengiriman *packet* terus berlanjut melalui *backup link*, yaitu melalui R-2 seperti yang dapat dilihat pada gambar 3.

```
PC-1> trace 8.8.8.8 -P 6
trace to 8.8.8.8, 8 hops max (TCP), press Ctrl+C to stop
 1 192.168.10.252 3.562 ms 3.606 ms 3.033 ms
 2 192.11.11.1 6.283 ms 9.282 ms 9.327 ms
 3 8.8.8.8 25.379 ms 20.365 ms 9.473 ms
PC-1>
```

**Gambar 8.** *Trace Route* Sebelum *Failover*

Pada Gambar 8 dilakukan *trace route* dari PC-1 ke alamat IP 8.8.8.8 (google.com) menggunakan *link* utama, terbukti dengan *output* alamat IP 192.168.10.252 pada gambar diatas, yaitu alamat IP address *link* utama pada R-1 seperti yang dapat dilihat pada gambar 3.

```
PC-1> trace 8.8.8.8 -P 6
trace to 8.8.8.8, 8 hops max (TCP), press Ctrl+C to stop
 1 192.168.10.253 4.637 ms 3.066 ms 3.825 ms
 2 192.11.10.5 12.005 ms 10.206 ms 9.273 ms
 3 8.8.8.8 19.847 ms 21.236 ms 19.215 ms
PC-1>
```

**Gambar 9.** *Trace Route* Setelah *Failover*

Pada Gambar 9 setelah proses *failover* dilakukan *trace route* dari PC-1 ke alamat IP 8.8.8.8 (google.com) menggunakan *backup link*, terbukti pada gambar diatas memiliki *output* dengan alamat ip 192.168.10.253, dimana itu adalah IP address milik *backup link* pada R-2 seperti yang terlihat pada gambar 3.

### 3.2 Parameter QOS (*Quality Of Service*)

Parameter pengujian yang dilakukan untuk melihat kinerja dari penerapan metode HSRP akan berfokus pada dua parameter, yaitu *packet loss* dan *throughput*.

#### 3.2.1 *Packet Loss*

*Packet Loss* merupakan suatu parameter dalam menentukan jumlah *packet* yang tidak terkirim atau hilang. Penyebab *packet loss* bisa dikarenakan terjadinya gangguan pada jalur transmisi kabel.

**Tabel 2.** Standarisasi *Packet Loss* Berdasarkan ITU-T

Kategori Degradasi	<i>Packet Loss</i> (%)
Sangat Bagus	0-2
Bagus	3-14
Sedang	15-24
Buruk	> 25



ITU-T (*International Telecommunication Union Telecommunication*) merupakan sebuah badan internasional yang merancang standar tingkat dunia untuk peralatan dan sistem telekomunikasi. Pada penelitian ini, peneliti menggunakan ITU-T sebagai acuan hasil *packet loss* yang telah diteliti.

### 3.2.2 Throughput

*Throughput* adalah suatu parameter kemampuan dari suatu jaringan dalam melakukan pengiriman data.

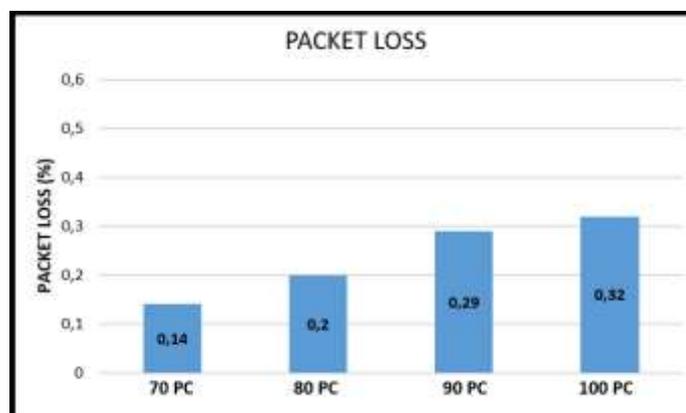
**Tabel 3.** Standarisasi *Throughput* Berdasarkan TIPHON

Kategori <i>Throughput</i>	Nilai (%)
Sangat Bagus	76-100
Bagus	51-75
Sedang	26-50
Buruk	< 25

TIPHON (*Telecommunications and Internet Protocol Harmonization Over Networks*) adalah sebuah badan internasional yang merancang standar QOS (*Quality Of Service*). Pada penelitian ini, TIPHON digunakan oleh peneliti sebagai acuan hasil *throughput* yang telah diteliti.

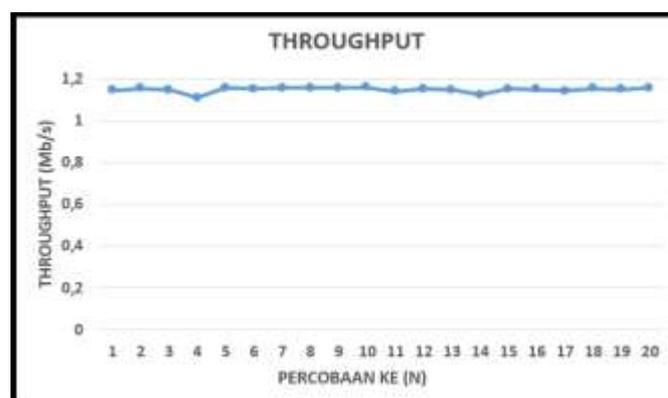
### 3.3. Grafik Hasil Pengujian *Packet Loss* dan *Throughput*

Pengujian *packet loss* akan dilakukan sebanyak 4 kali, yang mana pengujian pertama menggunakan 70 PC, pengujian kedua dilakukan menggunakan 80 PC, pengujian ketiga menggunakan 90 PC, dan pengujian ke empat menggunakan 100 PC, sedangkan pengujian *throughput* dilakukan dengan cara memberikan beban *traffic* sebesar 1,2Mb pada jaringan, lalu pada waktu tertentu koneksi pada jalur transmisi utama yang berada pada R-1 seperti yang dapat dilihat pada Gambar 3 diputus secara sengaja.



**Gambar 10.** Grafik Hasil Pengujian *Packet Loss* Metode HSRP

Dari Gambar 10 dapat dilihat bahwa hasil pengujian *packet loss* menggunakan 70 PC, 80 PC, 90 PC, dan 100 PC tidak ada yang melebihi 1%. Jika merujuk pada ITU-T, maka hasil pengujian *packet loss* yang telah dilakukan termasuk kedalam kategori yang Sangat Bagus, karena dari hasil pengujian *packet loss* yang telah dilakukan terdapat hasil terkecil dari pengujian 70 PC sebesar 0,14% dan hasil terbesar dari pengujian 100 PC sebesar 0,32%, sehingga dengan penerapan metode HSRP dapat disimpulkan dapat meningkatkan ketersediaan jaringan yang terjamin



**Gambar 11.** Grafik Hasil Pengujian *Throughput* Metode HSRP



Pada Gambar 11 terlihat bahwa saat memberikan *traffic* sebesar 1,2Mb pada jaringan dan kemudian dilakukan pemutusan secara sengaja terdapat *throughput* terendah sebesar 1,108Mb/s (92,33%), *throughput* tertinggi sebesar 1,159Mb/s (96,58%), serta jika dirata-ratakan, maka *throughput* dari penerapan metode HSRP adalah sebesar 1,147Mb/s (95,58%). Jika dilihat pada Tabel 3 yang merujuk pada TIPHON, maka hasil pengujian *throughput* termasuk kedalam kategori Sangat Bagus.

## 4. KESIMPULAN

Berdasarkan hasil pengujian dengan memanfaatkan metode HSRP, ketersediaan jaringan pada *layer 3 network* terjamin karena adanya *active link* dan *backup link* dari penerapan metode *Hot Standby Router Protocol*, terbukti dari pengujian yang telah dilakukan dengan penggunaan sebanyak 100 PC hanya terdapat 0,32% *packet loss*, sedangkan untuk *throughput* terdapat hasil yang berbeda-beda ketika dilakukan *link down*, namun *throughput* tetap terjaga karena adanya penerapan metode HSRP. Hal ini berguna jika HSRP diterapkan pada perusahaan yang memiliki banyak user dan tidak ingin terjadi *link down* pada *layer 3* ketika terjadi masalah pada jalur transmisi kabel utama, karena dengan menggunakan metode HSRP ini, ketika jalur transmisi utama mengalami *link down*, maka secara otomatis akan langsung menggunakan *backup link*, sehingga ketersediaannya terjamin.

## REFERENCES

- [1] C. V. Ravikumar, Y. M. Srikanth, P. Sairam, M. Sundeeep, K. P. Bagadi, and V. Annepu, "Performance analysis of HSRP in provisioning layer-3 gateway redundancy for corporate networks," *Indian J. Sci. Technol.*, vol. 9, no. 20, pp. 2–6, 2016.
- [2] A. K. Singh and A. Kothari, "HSRP (Hot Stand by Routing Protocol) reliability issues over the Internet service provider's network," *Orient. J. Comput. Sci. Technol.*, vol. 4, no. 2, 2011.
- [3] A. M. A. Mohamed, J. N. P. Soon, W. S. Wan, P. K. Yuen, and L. E. Heng, "Hot Standby Router Protocol for a Private University in Malaysia," *Int. J. Sci. Eng. Technol.*, vol. 4, no. 3, pp. 172–174, 2015.
- [4] W. Purwanto and S. Risnanto, "Implementasi Metode HSRP Pada Bank Jawa Barat dan Banten Kantor Wilayah I dan KCP Simpang Dago," vol. 3, no. 1, 2018.
- [5] W. H. Pamungkas and E. Prayitno, "Perancangan Jaringan Redundancy Link Menggunakan Konsep HSRP dan Etherchannel (Studi Kasus PT. Telkom Area Palangkaraya)," *Metik*, vol. 2, no. 1, pp. 75–82, 2018.
- [6] B. I. D. Kumar and G. Vasanth, "Performance Evaluation of HSRP based reliable Multihomed Network for two Different Applications," vol. 6, no. 8, pp. 92–99, 2017.
- [7] P. Kaur, H. Kaur, and J. Kaur, "Hot Standby Routing Protocol ( HSRP )," vol. 3, no. 1, pp. 2110–2112, 2017.