

Praktikum 4

IF2230 Jaringan Komputer

DNS, SSH, Network Access Control List, dan IPv6

Dipersiapkan oleh:

妹ラボラトリー

(Asisten Laboratorium Sistem Terdistribusi)

Sister; **L**ab²²

*“Licht wird uns an die richtige Stelle bringen, weitermachen,
weiter auf der Straße”*

Pernyataan Hak Cipta

© Laboratorium Sistem Terdistribusi 2025

Seluruh teks soal praktikum ini dilindungi oleh undang-undang hak cipta dan hanya boleh disimpan atau didistribusikan atas izin eksplisit dari para penulis.

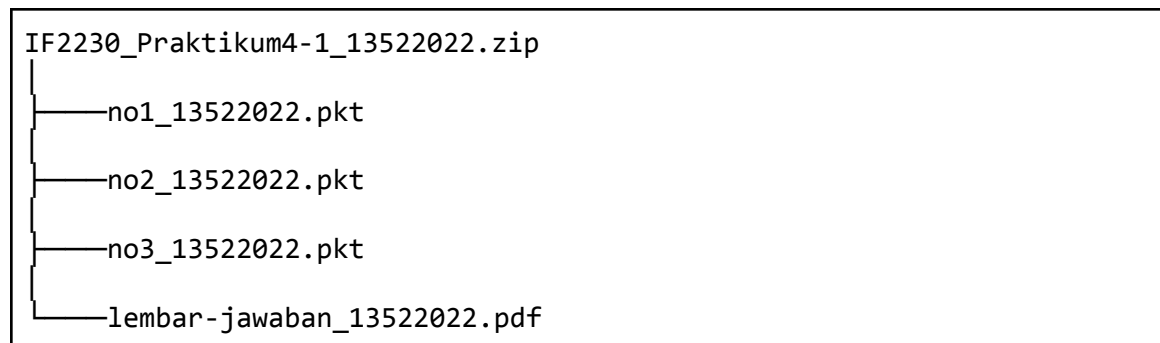
Hak cipta ini berlaku hingga 1 Juni 2025. Setelah tanggal tersebut, semua hak atas dokumen ini dilepaskan oleh penulis, dan seluruh isi dan materi dapat digunakan, dimodifikasi, serta didistribusikan secara bebas untuk tujuan apapun tanpa batasan.

Instruksi

Kerjakan dan kumpulkan tugas ini dengan mengikuti semua ketentuan berikut.

1. Buatlah salinan dari dokumen ini dengan **File -> Make a copy**, kemudian kerjakan soal-soal pada salinan dokumen Anda.
2. Format *file* pengumpulan adalah sebagai berikut.
 - Simpan dokumen ini dengan nama **lembar-jawaban_[NIM].pdf**.
 - Simpan semua *deliverables* **.pkt** dengan format nama **no[X]_[NIM].pkt** (dengan X adalah nomor yang bersangkutan dengan *file* itu).
 - Kemudian zip semua *file*, dan namakan **IF2230_Praktikum4-1_[NIM].zip**. Kumpulkanlah *file* zip ini pada *link* form yang diberikan.

Contoh struktur zip sebagai berikut.



3. Lakukan pengumpulan melalui [form ini](#). Form akan ditutup tepat pukul 14.50 dan **tidak ada toleransi untuk pengumpulan yang telat**.
4. Praktikum bersifat **individual**, Anda dilarang bekerja sama.
5. Praktikum bersifat **closed book**. Namun, Anda **diperbolehkan** untuk membuka dan membaca dokumentasi resmi berikut (dan *cheat sheet*) selama praktikum.
 - [Cheat Sheet](#)
6. Jangan lupa untuk isi [pernyataan integritas](#).

Pernyataan Integritas

Salin dan ketiklah pernyataan ini **secara manual** pada kolom biru di bawahnya. Gantilah <NAMA> dan <NIM> sesuai dengan identitas Anda.

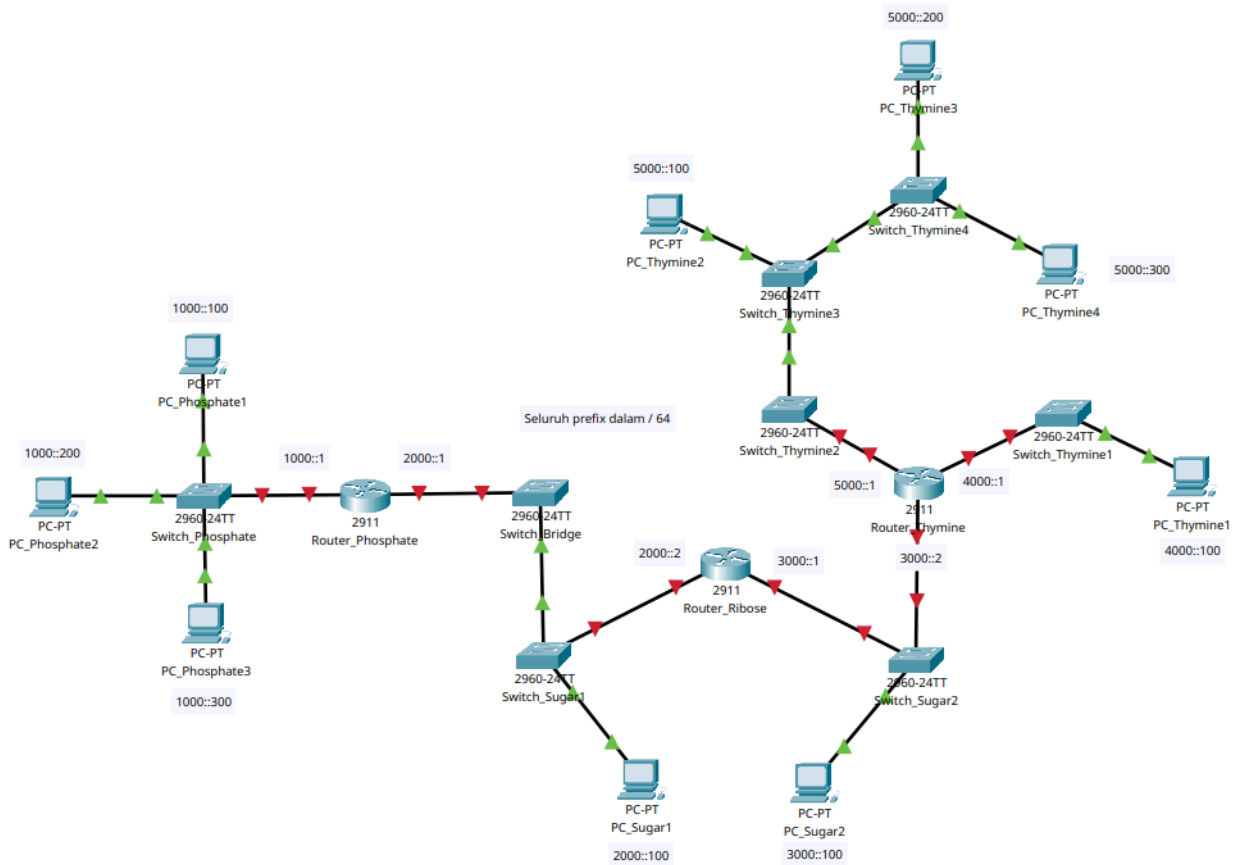
Dengan ini saya, <NAMA> dengan NIM <NIM> menyatakan bahwa saya akan mengerjakan praktikum ini dengan sejujur-jujurnya. Saya setuju bahwa jika saya dengan sengaja melakukan kecurangan, maka saya telah gagal untuk menghormati kerja keras orang lain dan pantas untuk menerima konsekuensi terberat untuk mata kuliah ini.

Dengan ini saya, Muhammad Iqbal Haidar dengan NIM 13523111 menyatakan bahwa saya akan mengerjakan praktikum ini dengan sejujur-jujurnya. Saya setuju bahwa jika saya dengan sengaja melakukan kecurangan, maka saya telah gagal untuk menghormati kerja keras orang lain dan pantas untuk menerima konsekuensi terberat untuk mata kuliah ini.

Soal

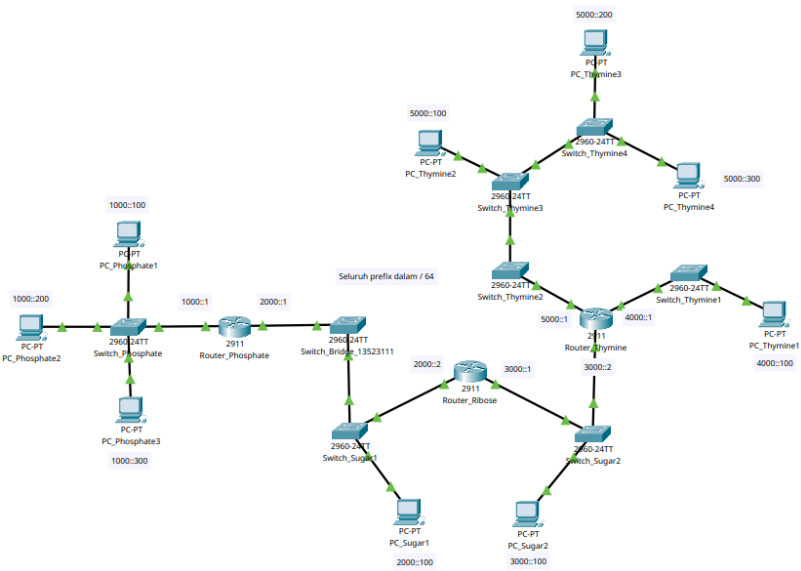
Nomor 1

Unduh *file .pkt* pada tautan berikut: [Template Topologi](#). Simpan file dengan format nama: `no1_[NIM].pkt`



Tip: Unduh filenya.

a.	<p>Buka file .pkt, lalu lakukan hal-hal berikut:</p> <ul style="list-style-type: none">• Konfigurasi IPv6 address dan default gateway untuk seluruh PC, sesuai dengan label. Jika sebuah PC tersambung pada > 1 router, pilih salah satu sebagai default gateway.• Konfigurasi IPv6 address untuk seluruh interface pada masing-masing router.• Ubah <code>display name</code> Switch_Bridge menjadi Switch_Bridge_[NIM]. <p>Lampirkan <i>screenshot</i> topologi setelah seluruh <i>link</i> sudah menjadi hijau.</p>
----	---

	
b.	<p>Konfigurasi <i>IPv6 static routing</i> pada seluruh <i>router</i>.</p> <p><i>Tip: Untuk mempercepat proses, dapat menggunakan ::/0 seperti yang ditulis pada cheat sheet.</i></p> <p>Berikan hasil <i>copy-paste</i> atau <i>screenshot</i> perintah untuk masing-masing <i>router</i>.</p> <div> <div>i. Router_Phosphate</div> <div> Router_Phosphate(config)#ipv6 unicast-routing Router_Phosphate(config)#ipv6 route ::/0 2000::2 </div> </div> <div> <div>ii. Router_Ribose</div> <div> Router_Ribose(config)#ipv6 unicast-routing Router_Ribose(config)#ipv6 route ::/0 2000::1 Router_Ribose(config)#ipv6 route ::/0 3000::2 </div> </div> <div> <div>iii. Router_Thymine</div> <div> Router_Thymine(config)#ipv6 unicast-routing Router_Thymine(config)#ipv6 route ::/0 3000::1 </div> </div>
c.	<p>Lampirkan <i>screenshot</i> untuk hasil-hasil <i>ping</i> berikut.</p> <div> <div>i. PC_Phosphate1 → PC_Thymine2</div> </div>

PC_Phosphate1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 5000::100

Pinging 5000::100 with 32 bytes of data:

Reply from 5000::100: bytes=32 time=17ms TTL=125
Reply from 5000::100: bytes=32 time=1ms TTL=125
Reply from 5000::100: bytes=32 time=7ms TTL=125
Reply from 5000::100: bytes=32 time<1ms TTL=125

Ping statistics for 5000::100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 17ms, Average = 6ms
```

ii. PC_Sugar1 → PC_Thymine1

PC_Sugar1

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 4000::100

Pinging 4000::100 with 32 bytes of data:

Reply from 4000::100: bytes=32 time<1ms TTL=126
Reply from 4000::100: bytes=32 time=1ms TTL=126
Reply from 4000::100: bytes=32 time<1ms TTL=126
Reply from 4000::100: bytes=32 time<1ms TTL=126

Ping statistics for 4000::100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

iii. PC_Sugar2 → PC_Phosphate2

PC_Sugar2

Physical Config Desktop Programming Attributes

Command Prompt

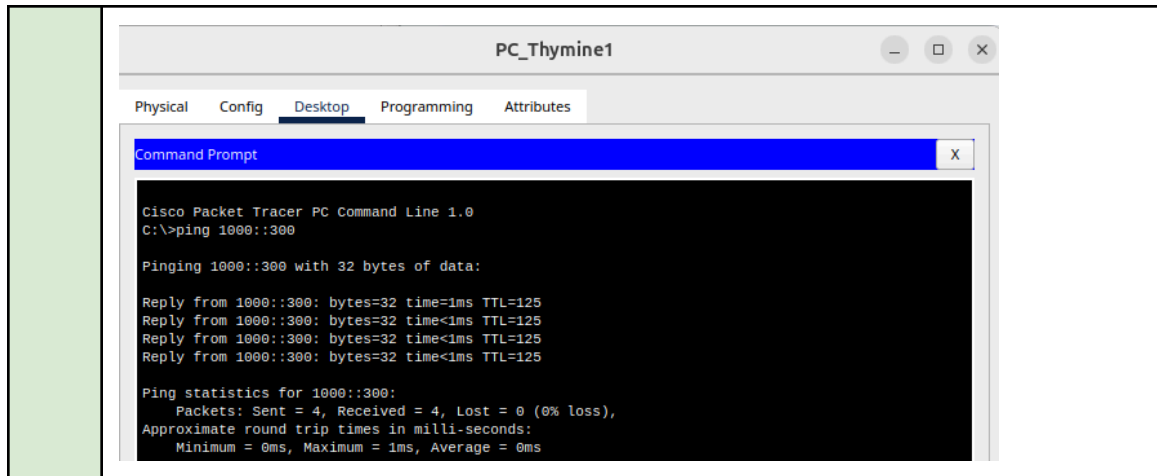
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 1000::200

Pinging 1000::200 with 32 bytes of data:

Reply from 1000::200: bytes=32 time=10ms TTL=126
Reply from 1000::200: bytes=32 time<1ms TTL=126
Reply from 1000::200: bytes=32 time<1ms TTL=126
Reply from 1000::200: bytes=32 time<1ms TTL=126

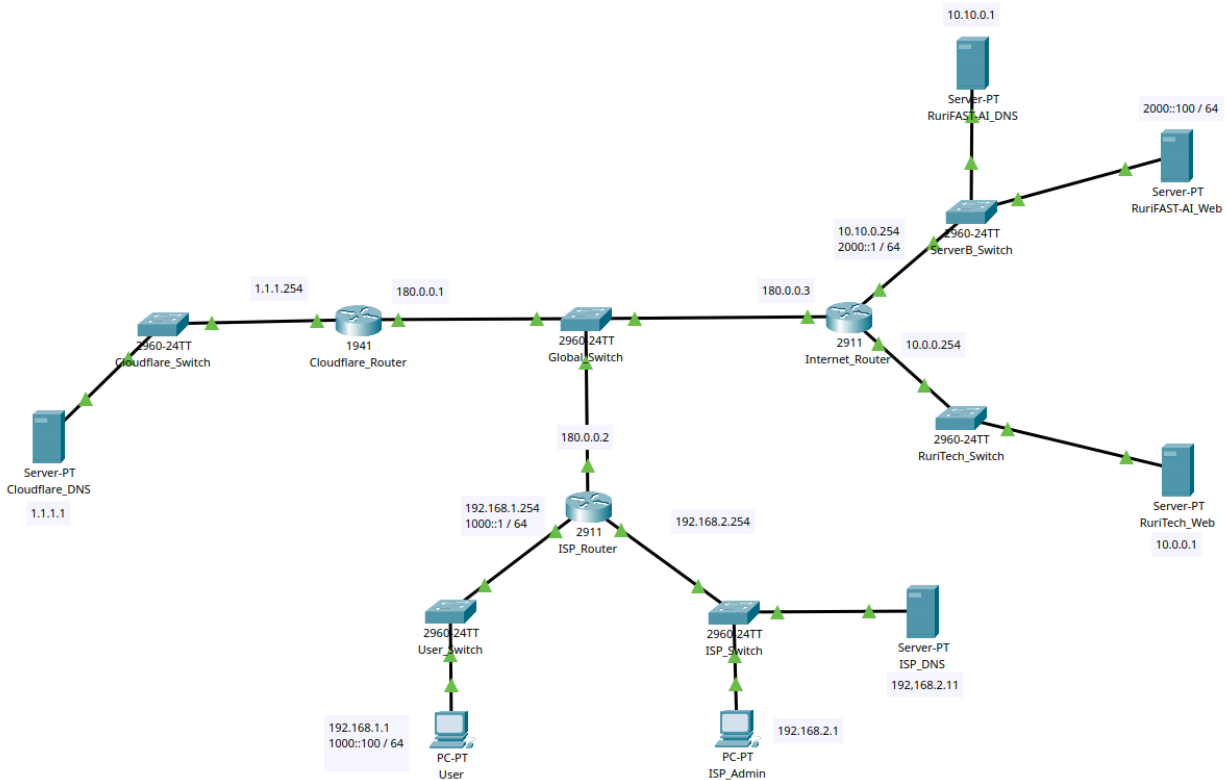
Ping statistics for 1000::200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

iv. PC_Thymine1 → PC_Phosphate3



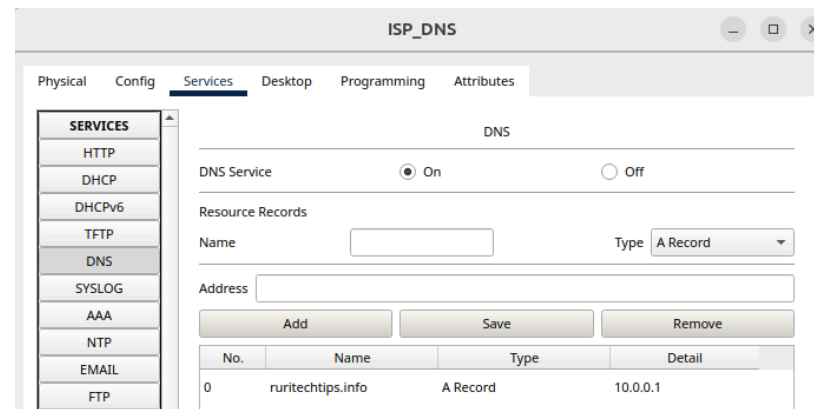
Nomor 2

Unduh **file .pkt** pada tautan berikut: [Template Topologi](#). Simpan file dengan format nama: no2_[NIM].pkt



Tip: Unduh filenya.

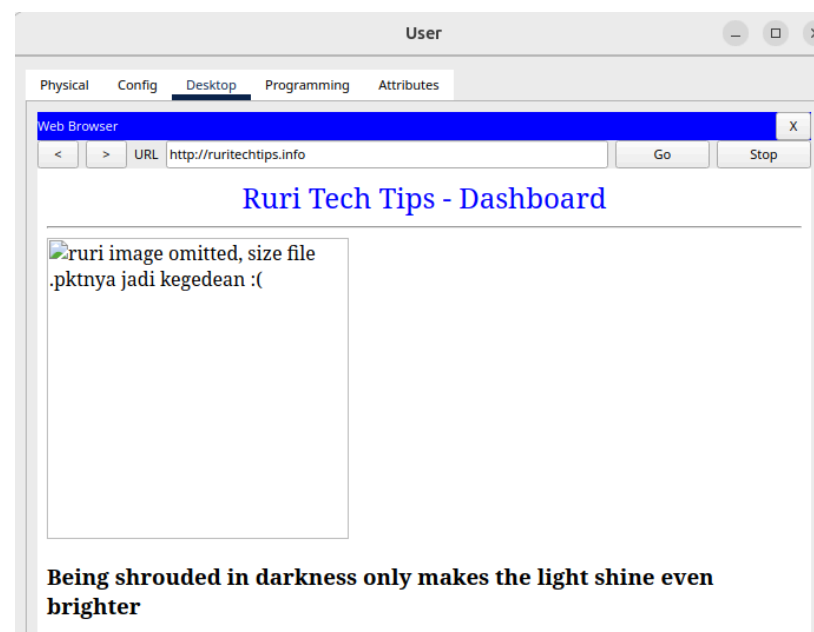
a.	<p>Sebuah <i>internet service provider (ISP)</i> merupakan sebuah perusahaan yang menyediakan layanan akses ke internet bagi pelanggannya, umumnya dengan memberikan <i>public IP address</i> sehingga perangkat pelanggan dapat berkomunikasi dengan jaringan luar.</p> <p>Selain itu, agar dapat mengakses situs-situs di Internet tanpa perlu menghafal <i>ip address</i>, perusahaan ISP umumnya menyediakan <i>DNS server</i> untuk melakukan <i>domain name translation</i> bagi para pelanggan.</p> <p>i. Tambahkan <i>DNS record</i> pada server ISP_DNS sehingga PC User dapat mengakses RuriTech_Web melalui <i>domain</i> ruritechtips.info (10.0.0.1)!</p> <p>Lampirkan <i>screenshot</i> perubahan yang dilakukan dan jelaskan secara singkat.</p>
----	---



Dilakukan penambahan DNS record bertipe A dengan domain ruritech.info dan IPv4 10.0.0.1 ke dalam ISP_DNS Server

ii. Pada **PC User**, akses situs **ruritechtips.info** melalui *web browser*.

Lampirkan *screenshot* hasilnya, cukup bagian atas website dan *browser* saja yang menunjukkan website sudah berhasil di-load.



b. Melalui inspeksi paket, pihak ISP menyadari bahwa Anda telah memanfaatkan layanan DNS mereka untuk mengakses situs yang mereka anggap *suspicious* atau tidak bermanfaat (padahal sebenarnya aman-aman saja).

Melihat hal tersebut, mereka memutuskan untuk menggunakan kekuasaan mereka (secara wajar dan sama sekali bukan merupakan

penyalahgunaan) untuk memblokir akses Anda ke layanan DNS mereka.

Namun mereka tidak ingin melakukan perubahan di *router* secara langsung setiap ada perubahan konfigurasi, karena lokasinya yang jauh dari kantor mereka, sehingga mereka memutuskan untuk **memasang SSH sehingga konfigurasi router ISP dapat diubah dari PC Administrator.**

(Untuk soal (i) – (iii) dan (v) – (vi) berikan copy-paste atau screenshot perintah yang dijalankan)

i. Lakukan **setup awal pemasangan SSH** pada **ISP_Router** dengan mengatur *hostname* dan *domain-name* dengan nama **ISP**, dan membuat sebuah akun dengan kredensial:

- **Username: admin**
- **Privilege: 15**
- **Secret: admin**

```
ISP_Router(config)#hostname ISP
ISP(config)#ip domain-name ISP
ISP(config)#username admin privilege 15 secret admin
```

ii. Lakukan *key generation* dengan algoritma RSA.

```
ISP(config)#crypto key generate rsa
The name for the keys will be: ISP.ISP
Choose the size of the key modulus in the range of
360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater
than 512 may take
a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be
non-exportable...[OK]
```

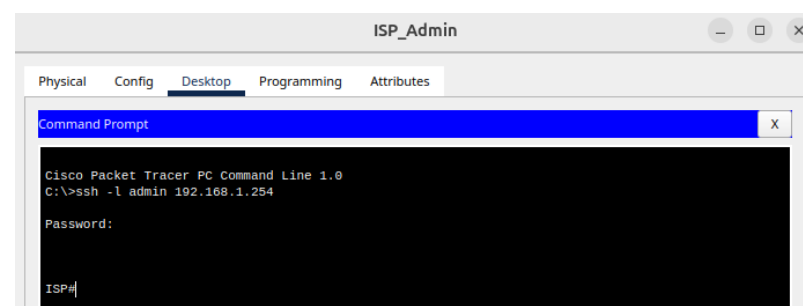
iii. Lakukan *setup virtual line (vty)* dari 0-15 dan pasang mekanisme *login* secara lokal.

```
ISP(config)#line vty 0 15
*Mar 1 0:8:53.263: %SSH-5-ENABLED: SSH 1.99 has been
enabled
ISP(config-line)#login local
```

ISP(config-line)#transport input ssh

iv. Akses SSH **ISP_Router** dari **PC ISP_Admin**.

Lampirkan *screenshot* hasilnya.



v. Masih di *interface* SSH, definisikan *access-list* yang memblokir seluruh paket dari **PC User**.

ISP(config)#ip access-list standard 1

ISP(config-std-nacl)#10 deny 192.168.1.1 0.0.0.0

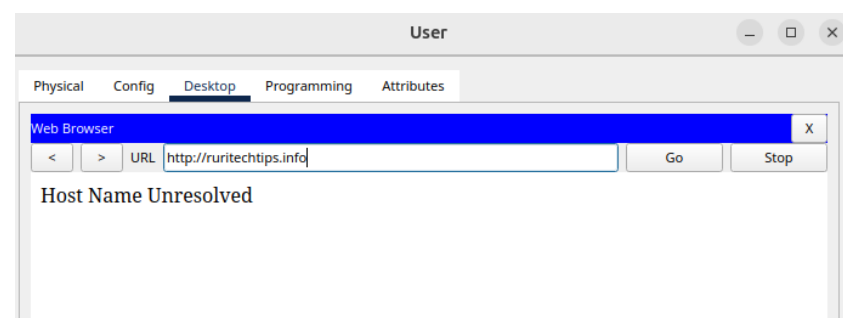
vi. Aplikasikan *access-list* tersebut ke paket-paket yang **keluar** dari *interface* **GigabitEthernet0/1** pada **ISP_Router**.

ISP(config)#int gi 0/1

ISP(config-if)#ip access-group 1 out

vii. Sekarang akses lagi situs **ruritechtips.info** melalui *web browser* milik **PC User**.

Lampirkan *screenshot* hasilnya.



c. Lirili Larila (Pengguna PC User) merasa kesal atas hak dasarnya untuk mengakses internet menggunakan layanan DNS telah ditarik seenak-enaknya oleh perusahaan ISP.

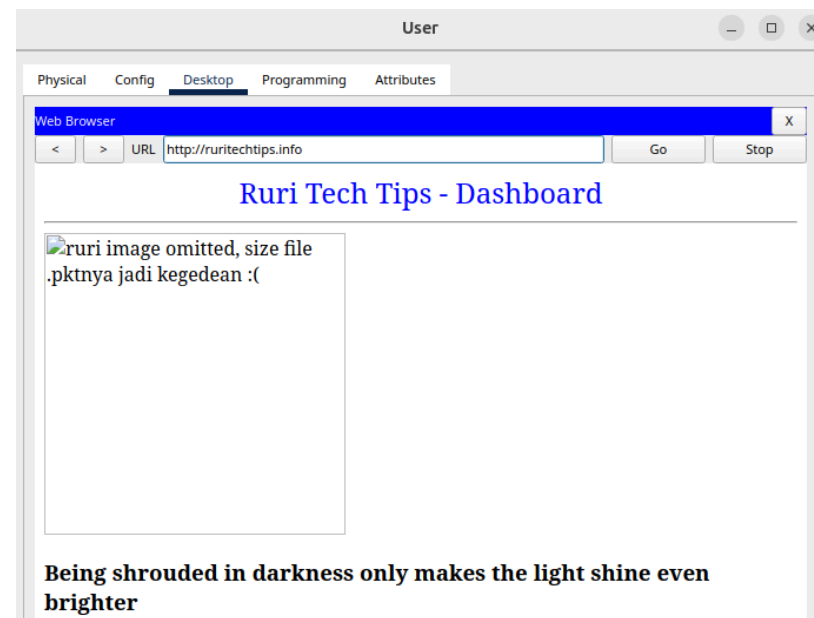
Untungnya, Lirili Larila telah lulus IF2230 Jaringan Komputer dan menyadari bahwa ia hanya perlu mengganti server DNS-nya agar dapat kembali mengakses situs informasi teknologi kesukaannya.

Lakukan hal-hal tersebut:

- Ubah *DNS server* milik **PC User** untuk mengarah ke **Cloudflare_DNS**.
- Konfigurasi **Cloudflare_DNS** untuk memiliki *DNS record* yang mengarah ke **RuriTech_Web** melalui *domain* **ruritechtips.info** (sama seperti untuk *ISP_DNS*).

Pada **PC User**, akses situs **ruritechtips.info** melalui *web browser*.

Lampirkan *screenshot* hasilnya.



d. Akibat inovasinya di bidang teknologi informasi dan komputasi, RuriTech menjadi salah satu perusahaan teknologi yang paling cepat berkembang di zaman modern dan memutuskan untuk mendirikan *startup* turunan Ruri FAST-AI (*Feedforward-Attention Transformer System*) yang berfokus pada perkembangan teknologi AI.

Ruri FAST-AI memutuskan untuk memulai bisnis dengan mendirikan sebuah *website*. Sebagai perusahaan teknologi, mereka menyadari atas keterbatasan alamat IPv4, dan mengintegrasikan alamat IPv4 dan IPv6 pada jaringan mereka.

Akan tetapi, beberapa jaringan ISP masih belum mengimplementasikan *tunneling* untuk IPv6 sehingga belum bisa mengakses jaringan mereka.

Bantulah perkembangan bisnis Ruri FAST-AI dengan mengimplementasikan **IPv6 Tunneling** antara jaringan **ISP_Router** dan **Internet_Router**!

Catatan: Alamat IPv6 sudah terkonfigurasi untuk perangkat dan router sesuai dengan label pada file template, sehingga hanya perlu mengkonfigurasi tunnel dan routing saja.

i. **Konfigurasi** *tunneling* pada interface **Tunnel0** untuk **ISP_Router**, dengan **alamat IPv6 3000::1/64**.

Copy-paste atau screenshot perintahnya pada kotak dibawah ini.

```
ISP(config)#int tunnel 0
ISP(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to
up

ISP(config-if)#ipv6 en
ISP(config-if)#ipv6 add 3000::1/64
ISP(config-if)#tunnel source gi 0/0
ISP(config-if)#tunnel dest 180.0.0.3
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to up

ISP(config-if)#tunnel mode ipv6ip
```

ii. **Konfigurasi** *tunneling* pada interface **Tunnel0** untuk **Internet_Router**, dengan **alamat IPv6 3000::2/64**.

Copy-paste atau screenshot perintahnya pada kotak dibawah ini.

```
Internet_Router(config)#int tunnel 0
Internet_Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to
up

Internet_Router(config-if)#ipv6 en
Internet_Router(config-if)#ipv6 add 3000::2/64
```

```
Internet_Router(config-if)#tunnel source gi 0/0
Internet_Router(config-if)#tunnel dest 180.0.0.2
Internet_Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Tunnel0, changed state to up

Internet_Router(config-if)#tunnel mode ipv6ip
```

iii. **Konfigurasi**kan *RIP routing* untuk **Tunnel0** dan **interface yang tersambung ke PC User** pada **ISP_Router**.

Copy-paste atau screenshot perintahnya pada kotak dibawah ini.

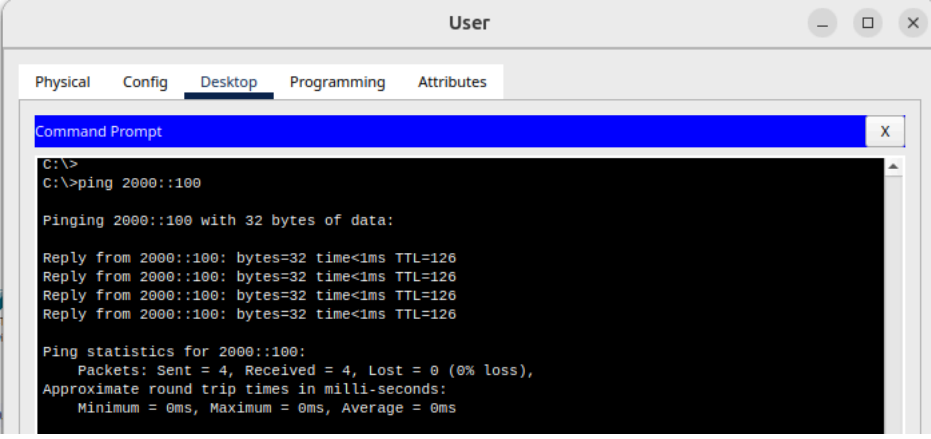
```
ISP(config)#ipv6 unicast-routing
ISP(config)#ipv6 router rip RIP0
ISP(config-rtr)#ex
ISP(config)#int tunnel 0
ISP(config-if)#ipv6 rip RIP0 en
ISP(config-if)#ex
ISP(config)#int gi 0/0
ISP(config-if)#ipv6 rip RIP0 en
ISP(config-if)#ex
```

iv. **Konfigurasi**kan *RIP routing* untuk **Tunnel0** dan **interface yang tersambung ke RuriFAST-AI_Web** pada **Internet_Router**.

Copy-paste atau screenshot perintahnya pada kotak dibawah ini.

```
Internet_Router(config)#ipv6 unicast-routing
Internet_Router(config)#ipv6 router rip RIP1
Internet_Router(config-rtr)#ex
Internet_Router(config)#int tunnel 0
Internet_Router(config-if)#ipv6 rip RIP1 en
Internet_Router(config-if)#ex
Internet_Router(config)#int gi 0/0
Internet_Router(config-if)#ipv6 rip RIP1 en
Internet_Router(config-if)#ex
```

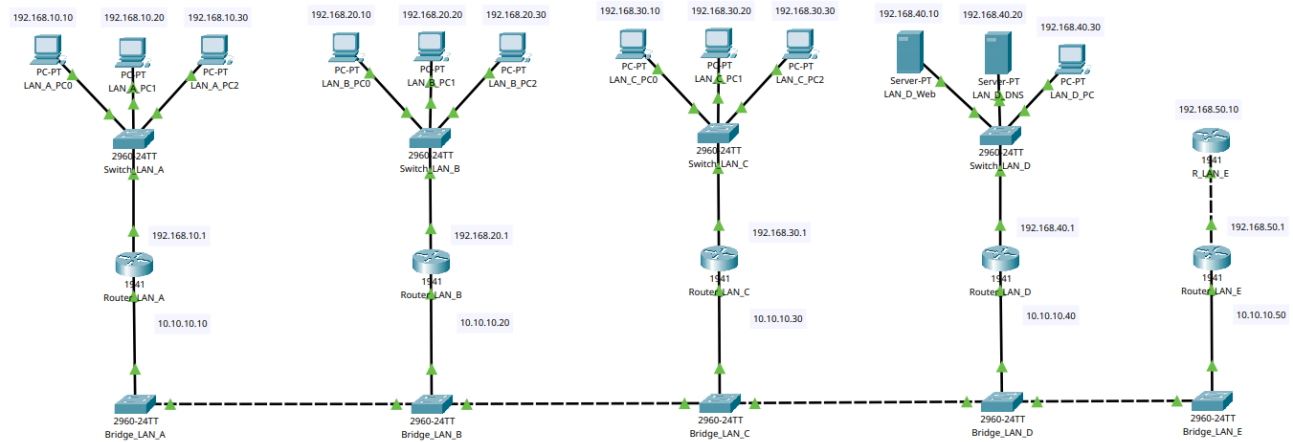
v. Dari **PC User**, lakukan *ping* terhadap **RuriFAST-AI_Web**. Lampirkan *screenshot* hasilnya.

	
e.	<p>Setelah mengimplementasikan <i>tunneling</i>, masuk ke <i>simulation mode</i> dan lakukan <i>ping</i> lagi dari PC User ke RuriFAST-AI_Web.</p> <p>Inspeksi paketnya ketika masuk ke ISP_Router. Bandingkan format paketnya pada halaman <i>Inbound PDU Details</i> dan <i>Outbound PDU Details</i>.</p> <p>Berdasarkan kedua format paket tersebut, jelaskan bagaimana <i>IPv6 tunneling</i> bekerja dan memungkinkan paket IPv6 untuk melalui jaringan IPv4!</p> <p>SRC IP saat Inbound PDU berupa 1000::100 sedangkan pada Outbound PDU 180.0.0.2. DST IP berubah dari 2000::100 menjadi 180.0.0.3</p> <p>Tunneling IPv6 bekerja dengan mengenkapsulasi SRC dan DST IPv6 menjadi sebuah IPv4 Header dengan protocol field di set menjadi 41 sehingga paket tetap bisa melewati jaringan IPv4 meskipun sudah pengguna menggunakan IPv6</p>
f.	<p>[Bonus]</p> <p>Ruri FAST-AI ingin seluruh <i>website</i> dan layanan mereka dapat diakses publik melalui domain .ruri.</p> <p>Konfigurasi Cloudflare_DNS untuk melakukan <i>DNS resolution</i> terhadap domain fast.ai.ruri dengan alur sebagai berikut:</p> <ul style="list-style-type: none"> • Pengguna (PC User) mengirim <i>query</i> untuk fast.ai.ruri ke Cloudflare_DNS. • Cloudflare_DNS mem-<i>forward</i> seluruh <i>query</i> untuk domain .ruri ke RuriFAST-AI_DNS.

	<ul style="list-style-type: none"> • Pada RuriFAST-AI_DNS terdapat <i>DNS record</i> untuk fast.ai.ruri, yang mengarah ke RuriFAST-AI_Web. Hasil ini akan dikembalikan ke Cloudflare_DNS dan nantinya ke pengguna yang mengirimkan <i>query</i>. <p>Yang perlu diperhatikan: Cloudflare_DNS <i>tidak</i> memiliki <i>record</i> yang langsung mengarah ke RuriFAST-AI_Web.</p> <p>i. Implementasikan alur tersebut dengan menambahkan sejumlah <i>DNS record</i> yang sesuai untuk masing-masing server DNS.</p> <p>Pastikan implementasi Anda cukup sesuai dengan bagaimana <i>DNS resolution</i> umumnya diimplementasikan di dunia asli dengan menambahkan tipe-tipe <i>record</i> yang sesuai.</p> <p>Berikan <i>screenshot DNS record</i> yang Anda tambahkan, dan jelaskan secara singkat masing-masing <i>record</i>.</p> <p>[Jawaban / <i>Screenshot</i>]</p>
	<p>ii. Pada PC User, akses situs fast.ai.ruri melalui <i>web browser</i>.</p> <p>Lampirkan <i>screenshot</i> hasil.</p> <p>[<i>Screenshot</i>]</p>
g.	<p>[Bonus]</p> <p>Jelaskan proses <i>DNS resolution</i> ketika seorang pengguna mengakses situs six.itb.ac.id.</p> <p>[Jawaban]</p>

Nomor 3

Unduh **file .pkt** pada tautan berikut: [Template Topologi](#). Simpan file dengan format nama: no3_[NIM].pkt



Tip: Unduh filenya.

Keterangan: Jika pada soal diberikan instruksi untuk permit/deny **LAN_X** (bukan **LAN_X_PCY**, misalkan), gunakan *subnet* dari LAN tersebut pada *access-list*. Permit/deny akses LAN dengan menggunakan alamat PC-nya satu per satu tidak akan dinilai.

a.	<p>Pada Router_LAN_A, definisikan <i>access-list</i> untuk memblokir LAN_B_PC0, namun masih mengizinkan sumber lainnya, dengan perintah berikut:</p> <pre>access-list 1 deny host 192.168.20.10</pre> <p>Terapkan <i>access-list</i> tersebut pada paket yang masuk ke <i>interface</i> luar Router_LAN_A.</p> <p>Sekarang, coba lakukan beberapa hal berikut:</p> <ul style="list-style-type: none">• Lakukan <i>ping</i> dari LAN_B_PC0 → LAN_A_PC0• Lakukan <i>ping</i> dari LAN_B_PC2 → LAN_A_PC0 <p>Apakah <i>access-list</i> sudah bekerja sesuai yang diharapkan? Jika belum, jelaskan mengapa <i>access-list</i> belum bekerja dengan benar, dan berikan solusi untuk memperbaiki kesalahan tersebut!</p> <p>Tambahkan solusi tersebut ke <i>access-list</i> Router_LAN_A.</p>
----	--

	<p>Menambahkan aturan baru pada access list yakni menerima tanpa batasan dengan prioritas dibawah aturan pertama.</p> <pre>Router_LAN_A(config)#ip access-list standard 1 Router_LAN_A(config-std-nacl)#11 permit any</pre>
b.	<p>Pada Router_LAN_B, definisikan <i>access-list</i> untuk:</p> <ul style="list-style-type: none"> • Memblokir <i>host LAN_A_PC0</i> • Memblokir keseluruhan LAN_C • Mengizinkan seluruh sumber lain <p>Terapkan <i>access-list</i> pada paket yang masuk ke <i>interface</i> luar Router_LAN_B.</p> <p>Berikan <i>copy-paste</i> atau <i>screenshot</i> perintah yang Anda lakukan.</p> <pre>Router_LAN_B(config)#ip access-list standard 1 Router_LAN_B(config-std-nacl)#15 permit any Router_LAN_B(config-std-nacl)#10 deny 192.168.30.0 0.0.0.255 Router_LAN_B(config-std-nacl)#5 deny host 192.168.10.10 Router_LAN_B(config-if)#ip access-group 1 in</pre>
c.	<p>Jalankan show access-lists di Router_LAN_C.</p> <p>Sudah didefinisikan <i>access-list</i> untuk:</p> <ul style="list-style-type: none"> • Memblokir keseluruhan LAN_A, kecuali LAN_A_PC0 yang masih diberikan akses • Mengizinkan seluruh sumber lainnya <p>Sekarang, coba lakukan beberapa hal berikut:</p> <ul style="list-style-type: none"> • Lakukan <i>ping</i> dari LAN_A_PC2 → LAN_C_PC0 • Lakukan <i>ping</i> dari LAN_A_PC0 → LAN_C_PC0 <p>Apakah <i>access-list</i> sudah bekerja sesuai yang diharapkan? Jika belum, jelaskan mengapa <i>access-list</i> belum bekerja dengan benar, dan berikan solusi untuk memperbaiki kesalahan tersebut! (tidak perlu diterapkan pada konfigurasi)</p> <p>Belum, karena aturan permit LAN_A_PC0 memiliki nomor prioritas di bawah aturan deny semua LAN_A. Solusinya ubah nomor prioritas permit LAN_A_PC0 sehingga berada diatas aturan deny semua LAN_A</p>

d.	<p>Pada Router_LAN_D, definisikan <i>access-list</i> untuk:</p> <ul style="list-style-type: none"> • Mengizinkan akses dari seluruh sumber ke LAN_D_PC • Memberikan akses <i>ping</i> dari LAN_C_PC2 ke keseluruhan LAN_D, namun memblokir akses lainnya (termasuk HTTPS dan DNS) • Mengizinkan akses ke layanan HTTPS milik LAN_D_Web untuk seluruh sumber • Mengizinkan akses ke layanan DNS milik LAN_D_DNS untuk seluruh sumber • Memblokir seluruh akses lainnya <p><i>Pengetesan DNS dan HTTPS dapat menggunakan domain ruri.info.</i></p> <p>Terapkan <i>access-list</i> pada paket yang masuk ke <i>interface</i> luar Router_LAN_D.</p> <p>Jalankan show access-lists, lalu berikan <i>copy-paste</i> atau <i>screenshot</i> ACL yang telah dibuat.</p> <pre> Router_LAN_D(config)#ip access-list extended 101 Router_LAN_D(config-ext-nacl)#10 permit ip any 192.168.40.30 0.0.0.0 Router_LAN_D(config-ext-nacl)#20 permit icmp 192.168.30.30 0.0.0.0 any Router_LAN_D(config-ext-nacl)#30 permit tcp any 192.168.40.10 0.0.0.0 eq 443 Router_LAN_D(config-ext-nacl)#40 permit udp any 192.168.40.20 0.0.0.0 eq 53 Router_LAN_D(config-ext-nacl)#50 deny ip any any Router_LAN_D(config)#int gi 0/1 Router_LAN_D(config-if)#ip access-group 101 in Extended IP access list 101 10 permit ip any host 192.168.40.30 20 permit icmp host 192.168.30.30 any 30 permit tcp any host 192.168.40.10 eq 443 40 permit udp any host 192.168.40.20 eq domain 50 deny ip any any </pre>
e.	<p>[Bonus]</p> <p>Perhatikan: Untuk soal ini, terapkan <i>access-list</i> pada paket yang masuk ke <u><i>interface</i></u> dalam Router_LAN_E (paket yang berasal dari R_LAN_E).</p>

Pada **Router_LAN_E**, definisikan *access-list* untuk layanan dari **R_LAN_E** sebagai berikut:

- Mengizinkan akses seluruh paket ke **LAN_D_PC**, kecuali SSH
- Hanya mengizinkan *ping* ke **LAN_A**
- Hanya mengizinkan layanan *telnet* ke **LAN_B**, kecuali ke **LAN_B_PC0**
- Mengizinkan layanan SSH ke seluruh tujuan, kecuali untuk **LAN_C** (pengecualian untuk **LAN_C_PC0** yang masih boleh mengakses SSH)
- Memblokir seluruh paket lainnya

*Catatan: Seluruh entri ACL didefinisikan dari **R_LAN_E** → [destination], namun untuk testing **ping, telnet, dan SSH** tetap dari luar → **R_LAN_E**.*

*Pengetesan telnet dapat menggunakan perintah **telnet ruri.router** dengan **username ruri** dan **password ruri**.*

*Pengetesan SSH dapat menggunakan perintah **ssh -l ruri ruri.router** dengan **password ruri**.*

Jalankan **show access-lists**, lalu berikan *copy-paste* atau *screenshot* ACL yang telah dibuat.

[Perintah]