LKS SMK TINGKAT PROPINSI NTB 2021

INFORMATION TECHNOLOGY NETWORK SYSTEM ADMINISTRATION (ITNSA)

SOAL CISCO PACKET TRACER NETWORK ACTUAL + FUTURE NETWORK

(WAKTU PENYELESAIAN 120 MENIT)

Oleh I Putu Hariyadi (putu.hariyadi@universitasbumigora.ac.id)

Terdapat perusahaan fiktif dengan nama **PT. Mandalika** yang memiliki kantor pusat atau **HeadQuarter (HQ)** di **Mataram** dan kantor cabang (**BRANCH**) di **Sumbawa**. Masing-masing kantor terkoneksi ke *Internet* melalui **Internet Service Provider (ISP)**. Pada kantor pusat (**HQ**) **Mataram** terdapat 3 (tiga) **Virtual Local Area Network (VLAN)** yaitu **VLAN 11 HRD**, **VLAN 12 MARKETING** dan **VLAN 13 NATIVE**. Komunikasi antar **VLAN (InterVLAN Routing)** dilakukan melalui **router HQ** dengan konfigurasi **router-on-stick** yang menerapkan protokol enkapsulasi **IEEE 802.1Q** pada **subinterface GigabitEthernet0/0**. **HQ Mataram** menerapkan **Wireless Controller (WLC)** dan **LeighWeight Access Point (LWAP)** untuk manajemen **Wireless Local Area Network (WLAN)**. Selain itu **WLAN** juga menggunakan **server Radius** dan **WPA2-Enterprise** untuk mengotentikasi pengguna nirkabel. Pengaturan **DHCP Server** dipusatkan pada **router HQ** untuk mendistribusikan pengalamatan IP secara dinamis bagi **End Device** seperti **Laptop** yang tersebar di **VLAN HRD** dan **MARKETING** serta **LWAP** di **VLAN NATIVE**. **Network Address Translation (NAT)** dikonfigurasi pada **router HQ** untuk melakukan *sharing* koneksi *Internet* ke *Client* di **VLAN** yang terdapat pada **HQ Mataram** dan menjembatani pengaksesan **Server HQ** dari *Internet*.

Koneksi *Internet* pada kantor cabang **Sumbawa (BRANCH)** dikelola oleh **router BRANCH** sehingga dapat dibagi pakai oleh **PC** di **VLAN Sales** dan **Tablet** yang terhubung baik pada jaringan nirkabel **WLAN ENGINEER**. **Switch** pada kantor cabang

dikonfigurasi dengan pengamanan **802.1x** untuk mengotentikasi koneksi dari PC-PC pada **VLAN Sales**. Otentikasi **AAA (Authentication, Authorization and Accounting)** untuk **802.1x** menggunakan **server BRANCH** sebagai **Radius**. Untuk mengamankan akses pada **WLAN ENGINEER** maka juga diterapkan **WPA2-Enterprise** berbasis **Radius** pada **Wireless Router WRT_BRANCH**.

Site-to-Site Virtual Private Network (VPN) menggunakan **Internet Protocol Security (IPSec)** dan **Generic Routing Encapsulation (GRE)** atau **GRE over IPSec** dibangun untuk menghubungkan antara kantor cabang dengan pusat dari **PT. MANDALIKA**. VPN memfasilitasi kebutuhan jalur komunikasi antar lokasi kantor yang terpisah secara geografis dan akses sumber daya di *Server Intranet* yang terdapat di kantor pusat dari kantor cabang dan sebaliknya. *Routing* protokol **Open Shortest Path First (OSPF)** dengan desain **single area** digunakan untuk merutekan paket antar jaringan kantor pusat dan cabang tersebut. Konfigurasi **OSPF** dilakukan pada **router HQ** dan **BRANCH**.

Terdapat **20 (dua puluh) tugas** yang harus diselesaikan.

Tugas 1: Konfigurasi Server HQ MATARAM dari PT. Mandalika

1. Mengatur pengalamatan **IP** dan **default gateway** serta **DNS** pada **Server HQ** dengan ketentuan sebagai berikut:
    a. **IP Address**: alamat **IP kedua** dari **subnet 10.0.14.0/30**.
    b. **Default Gateway**: alamat **IP pertama** dari **subnet 10.0.14.0/30**.
    c. **Server DNS**: **192.0.2.1**
2. Mengaktifkan layanan **HTTP** dan **HTTPS**.
3. Mengaktifkan layanan **AAA** dan mengatur **Network Configuration** dengan jenis **Server Radius** serta **User Setup**, seperti terlihat pada tabel berikut:
    a. **Network Configuration**

Client Name	Client IP	Key

WLC_HQ	**IP ke-empat** dari **subnet 10.0.13.0/24**	SMKHebat2021
HQ	**IP pertama** dari **subnet 10.0.14.0/30**	NTBJawara2021

b. **User Setup**

Username	Password
hrd1	hrd1
hrd2	hrd2
mkt1	mkt1
mkt2	mkt2
adminHQ	LksNTB2021
supportHQ	mandalika

Tugas 2: Konfigurasi Router HQ MATARAM dari PT. MANDALIKA

1. Mengatur **hostname** dari **Router** dengan nama "**HQ**".
2. Mengatur protokol enkapsulasi pada **interface Serial0/0/0** yang terhubung ke router ISP dengan **PPP** dan menerapkan otentikasi PPP menggunakan **CHAP** dengan sandi "**LksNTB**".
3. Mengatur pengalamatan IP pada **interface Serial0/0/0** yang terhubung ke router ISP menggunakan alamat **IP kedua** dari alamat **subnet HQ-ISP 192.0.2.16/29**.
4. Mengatur pengalamatan IP pada **interface GigabitEthernet0/1** yang terhubung ke Server HQ menggunakan alamat **IP pertama** dari **subnet 10.0.14.0/30**.
5. Mengatur **router-on-stick** untuk komunikasi antar VLAN dengan membuat **subinterface** pada **interface GigabitEthernet0/0** yang menerapkan protokol enkapsulasi **IEEE 802.1Q**. Alokasi pengalamatan IP pada setiap *subinterface* menggunakan ketentuan berikut:
    a. **Subinterface GigabitEthernet0/0.11** untuk **VLAN 11 HRD** dengan alamat **IP pertama** dari alamat **subnet 10.0.11.0/24**.

b. **Subinterface GigabitEthernet0/0.12** untuk **VLAN 12 MARKETING** dengan alamat **IP pertama** dari alamat **subnet 10.0.12.0/24**.
c. **Subinterface GigabitEthernet0/0.13** untuk **VLAN 13 NATIVE** dan diatur sebagai **native VLAN** serta menggunakan alamat **IP pertama** dari alamat **subnet 10.0.13.0/24**.

6. Membuat **DHCP Server**
   a. Membuat **Pool**
      - Nama **Pool "HRD"** untuk **VLAN 11** dengan alamat **subnet 10.0.11.0/24**.
      - Nama **Pool "MARKETING"** untuk **VLAN 12** dengan alamat **subnet 10.0.12.0/24**.
      - Nama **Pool "NATIVE"** untuk **VLAN 13** dengan alamat **subnet 10.0.13.0/24**.
      - Parameter TCP/IP yang diatur pada setiap *pool* adalah:
        - **Default gateway** yang diperoleh DHCP Client menggunakan alamat **IP pertama** dari masing-masing **subnet dari setiap VLAN**.
        - Alamat IP dari **server DNS** untuk **seluruh pool** menggunakan alamat IP dari **Server Root DNS** yaitu **192.0.2.1**.
      - Khusus untuk **pool "NATIVE"** juga dilakukan distribusi parameter alamat IP dari **Wireless Controller WLC_HQ** yang menggunakan alamat **IP ke-empat** dari **subnet 10.0.13.0/24** sehingga **LeighWeight Access Point (LWAP)** dapat melakukan registrasi secara otomatis.
   b. Mengatur alamat IP yang tidak disewakan ke *DHCP Client* untuk masing-masing pool.
      - Alamat **IP pertama** dari alamat **subnet VLAN 11 HRD** dan **VLAN 12 MARKETING**.

- Alamat **IP pertama** sampai dengan **ke-empat** dari alamat **subnet VLAN 13 NATIVE**.

7. Mengatur **default route** ke **ISP** menggunakan **gateway** berupa alamat **IP pertama** dari alamat **subnet HQ-ISP 192.0.2.16/29** yang digunakan oleh **interface Serial0/0/0** dari **router ISP**.
8. Membuat **Extended Named ACL** dengan nama "**ALLOW-INTERNET**" dan memiliki ketentuan sebagai berikut:
    a. Mengijinkan **query** ke **server DNS** dengan alamat IP Publik 192.0.2.1 dari sumber manapun untuk memetakan nama domain ke alamat IP dan sebaliknya.
    b. Mengijinkan akses *Internet* **HANYA** ke layanan **email** yang disediakan oleh **gmail.com** dengan alamat **IP Publik 192.0.2.5** bagi seluruh *host* yang terdapat pada **VLAN 11 HRD** yang memiliki alamat **subnet 10.0.11.0/2**4. Pastikan *host-host* pada VLAN tersebut hanya dapat mengirim dan mengunduh email dari **gmail.com**.
    c. Mengijinkan akses *Internet* bagi seluruh *host* pada **VLAN 12 MARKETING** dengan alamat **subnet 10.0.12.0/24** dan **VLAN 13 NATIVE** dengan alamat **subnet 10.0.13.0/24**.
9. Mengatur **NAT Overload** atau **Port Address Translation (PAT)** untuk **Standard Named ACL "ALLOW-INTERNET"**.
10. Mengatur **static NAT** agar **HANYA** layanan **HTTP** dan **HTTPS** pada **server HQ** dengan alamat **IP Private 10.0.14.2** ditranslasi ke alamat **IP Publik 192.0.2.19**.
11. Mengatur agar **router HQ** melakukan sinkronisasi waktu dengan **Server NTP** yang memiliki alamat **IP 192.0.2.2** dan menggunakan otentikasi pesan **md5** dengan **key 46** serta **password "NTBHebat2021"**.
12. Mengatur **password privilege mode** dengan **secret "LksNTB2021"**.
13. Mengatur **server DNS** dari **router HQ** dengan alamat **IP 192.0.2.1**.
14. Mengaktifkan **SSH versi 2** pada **router HQ** dengan nama **domain "mandalika.id"** dan membuat **RSA keys** dengan **modulus 1024**.

15. Membuat akun otentikasi lokal di **router HQ** dengan **username "admin"** dan sandi "**LksNTB2021**". Akun ini digunakan sebagai cadangan ketika otentikasi ke *server Radius* mengalami permasalahan.
16. Mengaktifkan fitur **AAA** pada **router HQ** dan mengatur agar otentikasi *default* menggunakan "**local**" **database**.
17. Membuat list otentikasi **login** pengguna dengan nama "**SERVER-AAA**" yang menggunakan metode otentikasi **Radius** terlebih dahulu dan dilanjutkan dengan "**local**".
18. Koneksi ke **Server Radius** dengan alamat **IP kedua** dari **subnet 10.0.14.0/30** dan menggunakan **secret "NTBJawara2021"**.
19. Mengatur agar **router HQ** hanya menerima **remote access** melalui **SSH** dengan jumlah sesi maksimal untuk **5 (lima)** pengguna dalam satu waktu dan menggunakan *list* otentikasi "**SERVER-AAA**".
20. Mengatur agar akses **console** ke *router* juga menggunakan *list* otentikasi "**SERVER-AAA**".
21. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 3: Konfigurasi Switch SW_HQ_L1 pada HQ MATARAM dari PT. MANDALIKA

1. Mengatur **hostname** dari **Switch** dengan nama "**SW_HQ_L1**".
2. Mengatur **VTP** dengan nama **domain** "**MANDALIKA**" dan sandi menggunakan "**LksNTB**".
3. Membuat **VLAN baru** antara lain:
    a. **VLAN 11** dengan nama **HRD**.
    b. **VLAN 12** dengan nama **MARKETING**.
    c. **VLAN 13** dengan nama **NATIVE**.
4. Mengatur pengalamatan IP pada **interface VLAN 13** dengan alamat **IP kedua** dari alamat **subnet 10.0.13.0/24**.

5. Mengatur **default gateway** menggunakan alamat **IP pertama** dari alamat **subnet 10.0.13.0/24** yang merupakan salah satu alamat IP di router HQ agar dapat berkomunikasi dengan beda network.
6. Mengatur **port FastEthernet0/1** menjadi anggota **VLAN 13**.
7. Mengaktifkan mode port menjadi **trunk** untuk **interface FastEthernet0/10**, **FastEthernet0/11** dan **GigabitEthernet0/1** serta **GigabitEthernet0/2**.
   Catatan: VLAN 13 difungsikan sebagai **native VLA**N.
8. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 4: Konfigurasi Switch SW_HQ_L2 pada HQ MATARAM dari PT. MANDALIKA

1. Mengatur **hostname** dari **Switch** dengan nama "**SW_HQ_L2**".
2. Mengatur **VTP** dengan mode **Client** dan nama **domain "MANDALIKA"** serta sandi menggunakan "**LksNTB**".
3. Mengatur pengalamatan **IP** pada **interface VLAN 13** dengan alamat **IP ketiga** dari alamat **subnet 10.0.13.0/24**.
4. Mengatur **default gateway** menggunakan alamat **IP pertama** dari alamat **subnet 10.0.13.0/24** yang merupakan salah satu alamat **IP** di **router HQ** agar dapat berkomunikasi dengan beda network.
5. Mengaktifkan **mode port** menjadi **trunk** untuk **interface FastEthernet0/20** dan **GigabitEthernet0/2**.
   Catatan: VLAN 13 difungsikan sebagai native VLAN.
6. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 5 Konfigurasi dan Verifikasi PC Admin2 pada HQ MATARAM dari PT. Mandalika

1. Mengatur **DHCP Client** pada **PC Admin2** yang terdapat di kantor pusat (**HQ**) **MATARAM** dari **PT. MANDALIKA**. Pastikan PC tersebut telah berhasil memperoleh pengalamatan IP secara dinamis dari **DHCP Server**.
2. Verifikasi koneksi dari **PC Admin2** ke **Switch SW_HQ_L1** dan **Router HQ** menggunakan **Simple PDU**. Pastikan koneksi berhasil dilakukan.

Tugas 6: Konfigurasi Wireless Controller (WLC) pada HQ MATARAM dari PT. MANDALIKA

1. Lakukan konfigurasi awal (**initial setup**) pada **WLC_HQ** menggunakan **browser** dari **desktop PC_Admin1** dengan mengakses alamat **IP** dari **WLC** yaitu **http://192.168.1.1**.
2. Konfigurasi **akun baru** untuk administrasi dengan **username "admin"** dan **sandi "LksNTB2021"**.
3. Konfigurasi **Controller** dengan ketentuan sebagai berikut:
    a. **System Name: WLC_HQ**
    b. **Management IP Address**: menggunakan alamat **IP ke-empat** dari **subnet 10.0.13.0/24**
    c. **Default Gateway**: menggunakan alamat **IP pertama** dari **subnet 10.0.13.0/24**
    d. **Management VLAN ID: 1**
    e. Konfigurasi **WLAN** dengan **Network Name "TEST"** dan **Passphrase "LksNTB2021"**.
4. Setelah **initial setup** selesai dilakukan maka konfigurasi **WLC_HQ** dapat dilakukan melalui **browser** dari **desktop PC_Admin2** dengan mengakses alamat **IP** dari **WLC** melalui **HTTPS** yaitu **https://10.0.13.4**. Login menggunakan **username "admin"** dan **sandi "LksNTB2021"**.
5. Hapus **WLAN** dengan **Network Name "TEST"**.
6. Mengatur **interface VLAN baru** pada **WLC** dengan ketentuan sebagai berikut:

Interface Name	VLAN ID	Port Number	IP Address	Gateway

INT-WLAN-11	11	1	10.0.11.254/24	10.0.11.1
INT-WLAN-12	12	1	10.0.12.254/24	10.0.12.1

7. Mengatur **WLC** agar menggunakan **server RADIUS** dengan alamat **IP kedua** dari **subnet 10.0.14.0/30** dan **shared secret "SMKHebat2021"** untuk mengotentikasi pengguna WLAN.
8. Mengatur **WLAN baru** pada WLC dengan ketentuan sebagai berikut:

Profile Name	SSID	ID	Interface	FlexConnect
PROF-WLAN-11-HRD	HRD-MANDALIKA	1	INT-WLAN-11	Local Switching & Local Auth
PROF-WLAN-12-MARKETING	MARKETING-MANDALIKA	2	INT-WLAN-12	Local Switching & Local Auth

9. Mengamankan setiap WLAN dengan **WPA2-Enterprise**.

Tugas 7: Konfigurasi LeighWeight Access Point (LWAP) pada HQ MATARAM dari PT. MANDALIKA

1. Mengatur pengalamatan **IP** secara dinamis atau sebagai **DHCP Client** pada **LWAP_HQ_L1** dan **LWAP_HQ_L2**.
2. Verifikasi konfigurasi yang telah dilakukan untuk memastikan setiap **LWAP** telah memperoleh pengalamatan IP secara dinamis dari **Server DHCP**.
3. Pastikan pula **CWAP Status** dari setiap **LWAP** tersebut menginformasikan bahwa telah berhasil terkoneksi ke alamat **IP** dari **WLC_HQ** dan menyediakan 2 (dua) **WLAN** yaitu **HRD-MANDALIKA** dan **MARKETING-MANDALIKA**.

Tugas 8: Konfigurasi dan Verifikasi End Device pada VLAN HRD dan MARKETING di HQ dari PT. MANDALIKA

1. Mengatur **DHCP Client** pada **interface Wireless0** dari setiap **End Device** pada **VLAN**

HRD dan **MARKETING** yaitu **Laptop_HRD1**, **Laptop_HRD2** dan **Laptop_MKT1** serta **Laptop_MKT2** agar memperoleh pengalamatan IP secara dinamis dari **DHCP Server**.

2. Mengkoneksikan **Laptop_HRD1** dan **Laptop HRD2** yang terdapat di **VLAN HRD** ke **LWAP** dengan **SSID "HRD-MANDALIKA"** dengan pengaturan **Wireless Security WPA2-Enterprise**. Gunakan akun otentikasi, seperti terlihat pada tabel berikut:

Login Name	Password	Device Name
hrd1	hrd1	Laptop_HRD1
hrd2	hrd2	Laptop_HRD2

3. Mengkoneksikan **Laptop_MKT1** dan **Laptop MKT2** yang terdapat di **VLAN MARKETING** ke **LWAP** dengan **SSID "MARKETING-MANDALIKA"** dengan pengaturan **Wireless Security WPA2-Enterprise**. Gunakan akun otentikasi berikut:

Login Name	Password	Device Name
mkt1	mkt1	Laptop_MKT1
mkt2	mkt2	Laptop_MKT2

4. Verifikasi koneksi dari setiap **Laptop** ke **Laptop** lainnya yang terdapat di kantor pusat **(HQ) MATARAM** menggunakan **Simple PDU**. Pastikan koneksi berhasil dilakukan.
5. Verifikasi koneksi *Internet* dari **Laptop_HRD1** dan **Laptop_HRD2** yang terdapat di **VLAN MARKETING** menggunakan **email** dengan tujuan **external@gmail.com**. Subjek dan pesan *email* yang digunakan untuk ujicoba dapat ditentukan secara mandiri. Pastikan *email* berhasil dikirim dari **Laptop_HRD1** dan **Laptop_HRD2**.

6. Melalui **PC Client_Internet** yang terdapat di **subnet Internet** lakukan verifikasi bahwa **email** yang dikirim dari **Laptop_HRD1** dan **Laptop_HRD2** berhasil diterima. Lakukan tindak lanjut dengan membalas setiap *email* tersebut.
7. Pastikan email berhasil diunduh dari **Laptop_HRD1** dan **Laptop_HRD2**.
8. Verifikasi koneksi Internet dari **Laptop_MKT1** dan **Laptop_MKT2** yang terdapat di **VLAN MARKETING** menggunakan **browser** dengan mengakses **Server ntbprov.go.id**, **ditpsmk.net** dan **gmail.com** serta **universitasbumigora.ac.id**. Pastikan koneksi berhasil dilakukan.

Tugas 9: Konfigurasi Server BRANCH SUMBAWA dari PT. Mandalika

1. Mengatur pengalamatan **IP** dan **default gateway** serta **DNS** pada **Server BRANCH** dengan ketentuan sebagai berikut:
   a. **IP Address** : alamat **IP ke-empat** dari **subnet 10.0.15.0/29**.
   b. **Default Gateway** : alamat **IP pertama** dari **subnet 10.0.15.0/29**.
   c. **Server DNS** : **192.0.2.1**
2. Mengaktifkan layanan **HTTP** dan **HTTPS**.
3. Mengaktifkan layanan **AAA** dan mengatur **Network Configuration** dengan jenis **Server Radius** serta **User Setup**, seperti terlihat pada tabel berikut:
   a. **Network Configuration**

Client Name	Client IP	Key
BRANCH	IP Pertama dari subnet 10.0.15.0/29	NTBJawara2021
SW_BRANCH	IP Kedua dari subnet 10.0.15.0/29	NTBHebat2021
WRT_BRANCH	IP Ketiga dari subnet 10.0.15.0/29	SMKBisa2021

   b. **User Setup**

Username	Password
sales1	sales1

sales2	sales2
engineer1	engineer1
engineer2	engineer2
adminBRANCH	LksNTB2021
helpdeskBRANCH	mandalika

Tugas 10: Konfigurasi Router BRANCH SUMBAWA dari PT. MANDALIKA

1. Mengatur **hostname** dari **Router** dengan nama "**BRANCH**".
2. Mengatur protokol enkapsulasi pada **interface Serial0/0/1** yang terhubung ke **router ISP** dengan **PPP** dan menerapkan otentikasi PPP menggunakan **CHAP** dengan sandi "**LksNTB**".
3. Mengatur pengalamatan **IP** pada **interface Serial0/0/1** yang terhubung ke **router ISP** menggunakan alamat **IP kedua** dari alamat **subnet ISP-BRANCH 192.0.2.24/29**.
4. Mengatur **router-on-stick** untuk komunikasi antar **VLAN** dengan membuat **subinterface** pada **interface GigabitEthernet0/0** yang menerapkan protokol enkapsulasi **IEEE 802.1Q**.
5. Alokasi pengalamatan IP pada setiap **subinterface** menggunakan ketentuan berikut:
    a. **Subinterface GigabitEthernet0/0.1** untuk **VLAN 1** dengan alamat **IP pertama** dari alamat **subnet 10.0.15.0/29**.
    b. **Subinterface GigabitEthernet0/0.2** untuk **VLAN 2 SALES** dengan alamat **IP pertama** dari alamat **subnet 10.0.15.16/28**.
6. Membuat **DHCP Server** untuk mendistribusikan pengalamatan IP secara dinamis menggunakan alamat **subnet 10.0.15.16/28** untuk PC-PC di **VLAN 2** dengan nama **pool** "**SALES**". Parameter TCP/IP yang diatur untuk *pool* tersebut meliputi **default gateway** menggunakan alamat **IP pertama** dari **subnet 10.0.15.16/28** dan **server DNS** menggunakan **192.0.2.1**.

Mengatur agar alamat **IP pertama** dari **subnet 10.0.15.16/28** tidak disewakan ke **DHCP Client**.

7. Mengatur **default route** ke **ISP** menggunakan **gateway** berupa alamat **IP pertama** dari alamat **subnet ISP-BRANCH 192.0.2.24/29** yang digunakan oleh **interface Serial0/0/1** dari **router ISP**.
8. Membuat **Standard Named ACL** dengan nama "**ALLOW-INTERNET**" yang mengijinkan akses *Internet* bagi seluruh *host* pada alamat **subnet 10.0.15.0/29** dan **10.0.15.16/28**.
9. Mengatur **NAT Overload** atau **Port Address Translation (PAT)** untuk **Standard Named ACL "ALLOW-INTERNET"**.
10. Mengatur **static NAT** agar **HANYA** layanan **HTTP** dan **HTTPS** pada **server BRANCH** dengan alamat **IP Private 10.0.15.4** ditranslasi ke alamat **IP Publik 192.0.2.27**.
11. Mengatur agar **router BRANCH** melakukan sinkronisasi waktu dengan **Server NTP** yang memiliki alamat **IP 192.0.2.2** dan menggunakan otentikasi pesan **md5** dengan **key 46** serta **password "NTBHebat2021"**.
12. Mengatur **password privilege mode** dengan **secret** "**LksNTB2021**".
13. Mengatur **server DNS** dari **router BRANCH** dengan alamat **IP 192.0.2.1**.
14. Mengaktifkan **SSH versi 2** pada **router BRANCH** dengan nama **domain "branch.mandalika.id"** dan membuat **RSA keys** dengan **modulus 1024**.
15. Membuat akun otentikasi lokal di **router BRANCH** dengan **username "admin"** dan **sandi "LksNTB2021"**. Akun ini digunakan sebagai cadangan ketika otentikasi ke **server Radius** mengalami permasalahan.
16. Mengaktifkan fitur **AAA** pada **router BRANCH** dan mengatur agar otentikasi default menggunakan "**local**" database.
17. Membuat list otentikasi **login** pengguna dengan nama "**SERVER-AAA**" yang menggunakan metode otentikasi **Radius** terlebih dahulu dan dilanjutkan dengan "**local**".
18. Koneksi ke **Server Radius** dengan alamat **IP ke-empat** dari **subnet 10.0.15.0/29** dan menggunakan **secret "NTBJawara2021"**.

19. Mengatur agar **router BRANCH** hanya menerima **remote access** melalui **SSH** dengan jumlah sesi maksimal untuk 5 (lima) pengguna dalam satu waktu dan menggunakan list otentikasi "**SERVER-AAA**".
20. Mengatur agar akses **console** ke **router** juga menggunakan list otentikasi "**SERVER-AAA**".
21. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 11: Konfigurasi Switch SW_BRANCH pada BRANCH SUMBAWA dari PT. MANDALIKA

1. Mengatur **hostname** dari **Switch** dengan nama "**SW_BRANCH**".
2. Mengatur pengalamatan **IP** pada interface **VLAN 1** dengan alamat **IP kedua** dari alamat **subnet 10.0.15.0/29**.
3. Mengatur **default gateway** menggunakan alamat **IP pertama** dari alamat **subnet 10.0.15.0/29** yang merupakan salah satu alamat **IP** di **router BRANCH SUMBAWA** sehingga dapat berkomunikasi ke beda jaringan.
4. Mengatur otentikasi untuk **802.1x** agar secara **default** menggunakan **server AAA Radius** dengan alamat **IP ke-empat** dari **subnet 10.0.15.0/29** dan **port 1645** serta **secret "NTBHebat2021"**.
5. Membuat **VLAN** baru dengan **ID 2** yang memiliki nama **SALES**.
6. Mengatur agar **port FastEthernet0/1** dan **FastEthernet0/2** menjadi anggota dari **VLAN 2**.
7. Mengatur agar **interface FastEthernet0/1** dan **FastEthernet0/2** menjalankan **EAPoL (802.1x)**.
8. Mengaktifkan **mode port** menjadi **trunk** untuk **interface GigabitEthernet0/2** yang terhubung ke **router BRANCH SUMBAWA**.
9. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 12: Konfigurasi DHCP Client dan Verifikasi Koneksi Internet pada PC VLAN 2 SALES dari BRANCH SUMBAWA PT. MANDALIKA

1. Mengatur setiap PC di **VLAN 2 SALES** kantor cabang **Sumbawa (BRANCH)** sebagai **DHCP Client** dan mengaktifkan fitur keamanan **802.1x** dengan akun otentikasi, seperti terlihat pada tabel berikut:

PC	User	Password
PC_Sales1	sales1	sales1
PC_Sales2	sales2	sales3

2. Pastikan masing-masing PC pada setiap **VLAN** telah berhasil memperoleh pengalamatan **IP** secara dinamis dari **DHCP Server**.
3. Verifikasi koneksi dari **PC_SALES1** ke **PC_SALES2** dan ke **router BRANCH SUMBAWA** menggunakan **Simple PDU**. Pastikan koneksi berhasil dilakukan.
4. Verifikasi koneksi *Internet* dari setiap PC yang terdapat di **VLAN 2 SALES** menggunakan *browser* dengan mengakses **Server ntbprov.go.id**, **ditpsmk.net** dan **gmail.com** serta **universitasbumigora.ac.id**. Pastikan koneksi berhasil dilakukan.
5. Apabila konfigurasi **NAT** pada **router HQ MATARAM** telah diselesaikan maka verifikasi akses ke **Server HQ** dari **PT. MANDALIKA** juga dapat dilakukan dengan mengakses "**mandalika.id**". Pastikan koneksi berhasil dilakukan.

Tugas 13: Konfigurasi Wireless Router WRT_BRANCH pada BRANCH Sumbawa dari PT. MANDALIKA

1. Mengatur pengalamatan **IP** secara statik atau **manual** pada **Internet Setup** dengan ketentuan sebagai berikut:
   a. Menggunakan alamat **IP ketig**a dari **subnet 10.0.15.0/29.**
   b. **Default gateway** menggunakan alamat **IP pertama** dari **subnet 10.0.15.0/29.**
   c. **Server DNS** menggunakan **192.0.2.1.**
2. Mengatur pengalamatan **IP** secara statik atau **manual** pada **Network Setup** dengan nilai berupa alamat **IP pertama** dari **subnet 10.0.15.128/25**.

3. Mengaktifkan fitur **DHCP Server** dan mengatur alamat IP yang didistribusikan secara dinamis ke *DHCP Client* mulai dari alamat **IP pertama** dari **subnet 10.0.15.128/25** untuk **maksimum 100 pengguna**. Parameter **Server DNS** menggunakan **192.0.2.1**.
4. Mengatur fitur **Wireless** dengan ketentuan sebagai berikut:
    a. **Network mode "Wireless-G Only"**.
    b. Nama pengenal jaringan nirkabel atau **SSID "ENGINEER-MANDALIKA"**.
    c. **Channel 6**.
    d. Mengaktifkan fitur **SSID Broadcast**.
    e. Mode pengamanan menggunakan **WPA2 Enterprise** dengan enkripsi **AES**.
    f. **Radius Server** menggunakan alamat **IP ke-empat** dari **subnet 10.0.15.0/29** dengan **shared secret "SMKBisa2021"**.

Tugas 14: Konfigurasi dan Verifikasi End Device pada WLAN ENGINEER BRANCH SUMBAWA

1. Mengatur **DHCP Client** pada **interface Wireless0** dari setiap **End Device** pada **subnet WLAN ENGINEER** yaitu **Tablet_ENGINEER1** dan **Tablet_ENGINEER2** agar memperoleh pengalamatan IP secara dinamis dari **DHCP Server**.
2. Mengkoneksikan setiap Tablet yang terdapat di **subnet WLAN ENGINEER** ke **Wireless Access Point (AP)** dengan **SSID "ENGINEER-MANDALIKA"** dengan pengaturan **Wireless Security WPA2-Enterprise**. Gunakan akun otentikasi berikut:

Device	Login Name	Password
Tablet_ENGINEER1	engineer1	engineer1
Tablet_ENGINEER2	engineer2	engineer2

Tugas 15: Konfigurasi VPN menggunakan GRE over IPSec dan OSPF pada router HQ MATARAM dari PT. MANDALIKA

1. Membuat **Extended Named ACL** dengan nama "**INTERESTING-TRAFFIC**" untuk:
    a. Mengijinkan trafik **GRE** dari alamat **IP sumber 192.0.2.18** ke alamat **IP tujuan 192.0.2.26**.
    b. Mengidentifikasi trafik **IP** dari **Server HQ MATARAM** yaitu **10.0.14.2** ke **VLAN 2 SALES** pada **router BRANCH SUMBAWA** dengan alamat **subnet 10.0.15.0/29** ke alamat IP dari sebagai *interesting traffic*.
    c. Mengidentifikasi trafik **IP** dari **VLAN 11 HRD** dengan alamat **subnet 10.0.11.0/24** yang terdapat di kantor pusat (**HQ**) dari **PT. Mandalika** ke **Server BRANCH** dengan alamat **10.0.15.4** sebagai *interesting traffic*.
    d. Mengidentifikasi trafik **IP** dari **VLAN 12 MARKETING** dengan alamat **subnet 10.0.12.0/24** yang terdapat di kantor pusat (**HQ**) dari **PT. Mandalika** ke **Server BRANCH** dengan alamat **10.0.15.4** sebagai *interesting traffic*.
2. Mengkonfigurasi **IKE Phase 1 ISAKMP policy** dengan **priority 46** dan **IKE Phase 2 IPSec policy** dengan **sequence 46** pada **router HQ MATARAM** dengan ketentuan, seperti terlihat pada tabel A dan B berikut:

Tabel A. Parameter ISAKMP Phase 1 Policy		
Parameter	**Router HQ MATARAM**	**Router BRANCH SUMBAWA**
Key Distribution Method	ISAKMP	ISAKMP
Encryption Algorithm	AES 256	AES 256
Hash Algorithm	SHA-1	SHA-1
Authentication Method	pre-share	pre-share
Key Exchange	DH 5	DH 5

ISAKMP Key	Mandalika	Mandalika

Tabel B. Parameter IPSec Phase 2 Policy

Parameter	Router HQ MATARAM	Router BRANCH SUMBAWA
Transform Set Name	HQ-SET	BRANCH-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	192.0.2.26	192.0.2.18
Traffic to be Encrypted	Extended Named ACL "INTERESTING-TRAFFIC"	Extended Named ACL "INTERESTING-TRAFFIC"
Crypto Map Name	HQ-MAP	BRANCH-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

4. Mengatur crypto map pada **outgoing Serial0/0/0 interface**.
5. Mengatur **GRE Tunnel** melalui **IPSec** dengan ketentuan sebagai berikut:
    a. Mengatur alamat **IP** dari **interface tunnel 46** menggunakan alamat **IP pertama** dari **subnet 10.0.14.4/30**.
    b. Mengatur **interface Serial0/0/0** sebagai **sumber** dan alamat **IP 192.0.2.26** sebagai tujuan untuk titik akhir dari **interface tunnel 46**.
6. Menambahkan alamat **subnet 10.0.14.0/30, 10.0.14.5/30** dan **10.0.11.0/24** serta **10.0.12.0/24** menggunakan **wildcard mask subnet** sebagai bagian dari jaringan **OSPF area 0** pada **routing protocol OSPF process-id 46**.
7. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 16: Konfigurasi VPN menggunakan GRE over IPSec dan OSPF pada router BRANCH SUMBAWA dari PT. MANDALIKA

1. Membuat **Extended Named ACL** dengan nama "**INTERESTING-TRAFFIC**" untuk:
    a. Mengijinkan trafik **GRE** dari alamat **IP sumber 192.0.2.26** ke alamat **IP tujuan 192.0.2.18**.
    b. Mengidentifikasi trafik **IP** dari **VLAN 2 SALES** pada **router BRANCH SUMBAWA** dengan alamat **subnet 10.0.15.0/29** ke alamat **IP dari Server HQ MATARAM** yaitu **10.0.14.2** sebagai *interesting traffic*.
    c. Mengidentifikasi trafik **IP** dari **Server BRANCH** dengan alamat **10.0.15.4** ke **VLAN 11 HRD** dengan alamat **subnet 10.0.11.0/24** yang terdapat di kantor pusat (**HQ**) **MATARAM** dari **PT. Mandalika** ke sebagai *interesting traffic*.
    d. Mengidentifikasi trafik **IP** dari **Server BRANCH** dengan alamat **10.0.15.4** ke **VLAN 12 MARKETING** dengan alamat subnet **10.0.12.0/24** yang terdapat di kantor pusat (**HQ**) **MATARAM** dari PT. Mandalika ke sebagai *interesting traffic*.
2. Mengkonfigurasi **IKE Phase 1 ISAKMP policy** dengan **priority 46** dan **IKE Phase 2 IPSec policy** dengan sequence **46** pada **router BRANCH SUMBAWA** dengan ketentuan, seperti terlihat pada tabel A dan B berikut:

Tabel A. Parameter ISAKMP Phase 1 Policy		
Parameter	**Router HQ MATARAM**	**Router BRANCH SUMBAWA**
Key Distribution Method	ISAKMP	ISAKMP
Encryption Algorithm	AES 256	AES 256
Hash Algorithm	SHA-1	SHA-1
Authentication Method	pre-share	pre-share
Key Exchange	DH 5	DH 5

ISAKMP Key	Mandalika	Mandalika

Tabel B. Parameter IPSec Phase 2 Policy

Parameter	Router HQ MATARAM	Router BRANCH SUMBAWA
Transform Set Name	HQ-SET	BRANCH-SET
ESP Transform Encryption	esp-aes	esp-aes
ESP Transform Authentication	esp-sha-hmac	esp-sha-hmac
Peer IP Address	192.0.2.26	192.0.2.18
Traffic to be Encrypted	Extended Named ACL "INTERESTING-TRAFFIC"	Extended Named ACL "INTERESTING-TRAFFIC"
Crypto Map Name	HQ-MAP	BRANCH-MAP
SA Establishment	ipsec-isakmp	ipsec-isakmp

4. Mengatur **crypto map** pada **outgoing Serial0/0/1 interface**.
5. Mengatur **GRE Tunnel** melalui **IPSec** dengan ketentuan sebagai berikut:
    a. Mengatur alamat **IP** dari **interface tunnel 46** menggunakan alamat **IP kedua** dari **subnet 10.0.14.4/30**.
    b. Mengatur **interface Serial0/0/1** sebagai **sumber** dan **alamat IP 192.0.2.18** sebagai tujuan untuk titik akhir dari **interface tunnel 46**.
6. Menambahkan alamat **subnet 10.0.14.4/30** dan **10.0.15.0/29** serta **10.0.15.16/28** menggunakan **wildcard mask subnet** sebagai bagian dari jaringan **OSPF area 0** pada **routing protocol OSPF process-id 46**.
7. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 17: Verifikasi Koneksi VPN dari End Device pada HQ MATARAM

1. Verifikasi koneksi menggunakan **Simple PDU** dari **End Device** yang terdapat pada **VLAN HRD** dan **MARKETING** di kantor pusat (**HQ**) **MATARAM** ke **VLAN SALES** dan **WLAN ENGINEER** pada kantor cabang (**BRANCH**) **SUMBAWA**. Pastikan koneksi berhasil dilakukan.
2. Verifikasi akses layanan **HTTP** dan **HTTPS** yang terdapat di **Server BRANCH SUMBAWA** menggunakan **browser** dengan mengakses alamat **http://10.0.15.4** dan **https://10.0.15.4** dari **End Device** yang terdapat pada **VLAN HRD** dan **MARKETING** dari kantor pusat (**HQ**) **MATARAM**. Pastikan layanan HTTP dan HTTPS dapat terakses.
3. Verifikasi akses layanan **FTP** yang terdapat di **Server BRANCH** menggunakan **FTP Client** dengan mengakses alamat **10.0.15.4** dari **End Device** yang terdapat pada **VLAN HRD** dan **MARKETING** dari kantor pusat (**HQ**) **MATARAM**. **User** untuk otentikasi FTP adalah "**lks**" dengan **password** "**ntb**". Pastikan layanan FTP dapat terakses.

Tugas 18: Verifikasi Koneksi VPN dari End Device pada BRANCH SUMBAWA

1. Verifikasi koneksi menggunakan **Simple PDU** dari **End Device** yang terdapat pada **VLAN SALES** dan **WLAN ENGINEER** dari kantor cabang (**BRANCH**) **SUMBAWA** ke **End Device** yang terdapat pada **VLAN HRD** dan **MARKETING** di kantor pusat (**HQ**) **MATARAM**. Pastikan koneksi berhasil dilakukan.
2. Verifikasi akses layanan **HTTP** dan **HTTPS** yang terdapat di **Server HQ MATARAM** menggunakan **browser** dengan mengakses alamat **http://10.0.14.2** dan **https://10.0.14.2** dari **End Device** yang terdapat pada **VLAN SALES** dan **WLAN ENGINEER** dari kantor cabang (**BRANCH**) **SUMBAWA**. Pastikan layanan HTTP dan HTTPS dapat terakses.
3. Verifikasi akses layanan **FTP** yang terdapat di **Server HQ** menggunakan **FTP Client** dengan mengakses alamat **10.0.14.2** dari **End Device** yang terdapat

pada **VLAN SALES** dan **WLAN ENGINEER** dari kantor cabang (**BRANCH**) **SUMBAWA**. **User** untuk otentikasi FTP adalah "**lks**" dengan **password** "**ntb**". Pastikan layanan FTP dapat terakses.

Tugas 19: Konfigurasi Roled Based Access Control (RBAC) pada router HQ MATARAM

1. Membuat **view** dengan nama "**support**" dan mengatur sandi dari *view* tersebut dengan nilai "**mandalika**".
2. Mengatur agar *view* yang dibuat hanya dapat mengeksekusi perintah "**ping**" dan perintah "**traceroute**" serta seluruh perintah yang diawali dengan "**show**".
3. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.

Tugas 20: Konfigurasi Roled Based Access Control (RBAC) pada router BRANCH SUMBAWA

1. Membuat **view** dengan nama "**helpdesk**" dan mengatur sandi dari *view* tersebut dengan nilai "**mandalika**".
2. Mengatur agar *view* yang dibuat hanya dapat mengeksekusi perintah "**show ip protocols**", "**show ip route**", "**show ip interface brief**" dan "**ping**" serta "**traceroute**".
3. Verifikasi konfigurasi yang telah dilakukan untuk memastikan telah sesuai dengan ketentuan.