**LAPORAN PRAKTIKUM**

**TEKNOLOGI WAN**

**PERTEMUAN 2**

**PPP, PAP, CHAP, dan OSPF**

****

Disusun oleh :

Alexsander Niko Dian 22084417

Damianus Yudha Christyawan 22084422

Brigitta Celna F 22084454

Catharina Nariswari 22084494

Adi Atmaja 22084511

**PROGRAM STUDI TEKNIK INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS KRISTEN DUTA WACANA**

**2011**

1. **LANDASAN TEORI**
2. PPP (Point–to-Point)

PPP merupakan sebuah protocol yang digunakan untuk melakukan hubungan antara client dengan server secara Point-to-Point. Enkapsulasi PPP digunakan untuk menghubungkan Router Cisco dan Router Non-Cisco. PPP mengenkapsulasi data frame untuk pengiriman melalui jalur fisik, dengan menggunakansambungan kabel serial, kabel telepon, dan lain-lain.

PPP mendukung otentikasi PAP (Password Authentication Protocol) dan CHAP (Challenge Handshake Authentication Protocol).

Tiga komponen utama pada PPP:

1. Menggunakan protocol HDLC sebagai dasar untuk mengenkapsulasi datagram melalui hubungan Point-to-Point.
2. Menggunakan versi tambahan dari Link Control Protocol (LCP) untuk membuat, mengkonfigurasi, dan menguji koneksi data.
3. Masih memiliki hubungan dengan Network Control Protokol (NCP) untuk membuat dan mengkonfigurasi network-layer protocol yang berbeda. NCP yang lebih umum adalah Internet Prottocol Contorl Protocol, Apple Talk Control Protocol, Novell IPX Control Protocol,Cisco Systems Control Protocol, SNA Control Protocol,and Compression Control Protocol.

Kelebihan PPP dibandingkan dengan HDLC:

1. Fitur untuk memantau manajemen kualitas link, juka terlalu banyak kesalahan yang terdeteksi, maka PPP akan mamatikan link tersebut.
2. PPP mendukung PAP dan CHAP.

PPP dapat dikonfigurasi pada beberapa tipe interface:

* Asynchronous serial
* Synchronous serial
* High-Speed Serial Interface (HSSI)
* Integrated Services Digital Network (ISDN)

Cara untuk mengkonfigurasi PPP, dimana menggunakan interface serial 0/0/0:

R3#configure terminal

R3(config)#interface serial 0/0/0

R3(config-if)#encapsulation ppp

1. PAP (Password Authentication Protocol)

PAP merupakan otentikasi yang ada di PPP. PAP adalah proses two-way dimana tidak terjadi enkripsi terhadap username dan password, yang dikirimkan adalah berupa plain text. Jika accepted, maka koneksi akan diizinkan untuk terjadi.

PAP mentransmisikan username dan password melalui jariringan lalu kemudian dicocokkan pada table username dan password yang ada. Otentikasi ini biasanya digunakan pada protocol HTTP. Kelemahan PAP adalah username dan password dapat dikirim tanpa dienkripsi terlebih dahulu.





Konfigurasi PAP pada Router R1:

R1(config)#username R2 password passR2

R1(config)#inteface serial2/0

R1(config-if)#encapsulation PPP

R1(config-f)#ppp pap sent-username R1 password passR1

R1(config-if)#no shutdown

R1(config-if)#clock rate 64000

R1(config-if)#ppp authentication pap

Konfigurasi PAP pada Router R2:

R2(config)#username R1 password passR1

R2(config)#inteface serial2/0

R2(config-if)#encapsulation PPP

R2(config-f)#ppp pap sent-username R2 password passR2

R2(config-if)#no shutdown

R2(config-if)#ppp authentication pap

1. CHAP (Challenge Handshake Authentication Protocol)

CHAP juga otentikasi yang ada pada PPP, tetapi CHAP lebih aman dibandingkan PAP. Ia menggunakan three-way dalam proses saling menukar *shared secret*. 3 tahap di CHAP:

1. Setelah fase LCP selesai, dan CHAP telah bernegosiasi dengan kedua device, authenticator mengirim *challenge message* ke peer.
2. Peer memberi respon dengan menghitung nilai menggunakan *one-way hash function.*
3. Authenthicator mengecek kembali respon tersebut dan mencocokakan dengan nilai hashnya. Jika nilainya sama, maka *authentication* berhasil. Jika tidak, koneksi akan dihentikan.





Konfigurasi CHAP pada Router R1:

R1(config)#username R2 password pass

R1(config)#inteface serial2/0

R1(config-if)#encapsulation PPP

R1(config-if)#no shutdown

R1(config-if)#clock rate 64000

R1(config-if)#ppp authentication chap

Konfigurasi CHAP pada Router R2:

R2(config)#username R1 password pass

R2(config)#inteface serial2/0

R2(config-if)#encapsulation PPP

R2(config-if)#no shutdown

R2(config-if)#ppp authentication chap

1. OSPF

OSPF merupakan sebuah routing protokol berjenis IGP yang hanya dapat bekerja dalam jaringan internal. OSPF juga merupakan *routing* protocol yang bukan ciptaan dari vendor manapun. Dengan demikian, siapapun dapat menggunakannya, perangkat manapun dapat kompatibel dengannya, dan di manapun routing protokol ini dapat diimplementasikan.

Langkah pertama yang harus dilakukan sebuah router OSPF adalah harus membentuk hubungan dengan *neighbor router*. Router OSPF mempunyai sebuah mekanisme untuk dapat menemukan router tetangganya dan dapat membuka hubungan. Mekanisme tersebut disebut dengan istilah Hello protocol. Dalam membentuk hubungan dengan tetangganya, router OSPF akan mengirimkan sebuah paket berukuran kecil secara periodik ke dalam jaringan atau ke sebuah perangkat yang terhubung langsung dengannya. Paket kecil tersebut dinamai dengan istilah Hello packet. Pada kondisi standar, Hello packet dikirimkan berkala setiap 10 detik sekali (dalam media broadcast multiaccess) dan 30 detik sekali dalam media Point-to-Point. Hello packet berisikan informasi seputar pernak-pernik yang ada pada router pengirim. Hello packet pada umumnya dikirim dengan menggunakan *multicast address* untuk menuju ke semua router yang menjalankan OSPF (IP multicast 224.0.0.5). Semua router yang menjalankan OSPF pasti akan mendengarkan protocol hello ini dan juga akan mengirimkan hello packet-nya secara berkala. Cara kerja dari Hello protocol dan pembentukan neighbour router terdiri dari beberapa jenis, tergantung dari jenis media di mana router OSPF berjalan.

Kelebihan OSPF adalah kecepatan konvergen yang handal dan skalabilitas ke network yang labih besar. Namun, karena setiap router bekerja dengan menggunakan database link state, ini akan menyebabkan hardware router bekerja semakin berat.

1. **CAPTURE TOPOLOGI**

****

1. **CAPTURE HASIL PRAKTIKKUM**
2. **SWITCH**

#################### SHOW RUN ####################

Switch#sh running-config

Building configuration...

Current configuration : 1262 bytes

!

version 12.1

no service pad

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname Switch

!

!

ip subnet-zero

!

ip ssh time-out 120

ip ssh authentication-retries 3

!

spanning-tree mode pvst

no spanning-tree optimize bpdu transmission

spanning-tree extend system-id

!

!

!

 --More-- !

interface FastEthernet0/1

 switchport mode trunk

!

interface FastEthernet0/2

 switchport access vlan 10

 switchport mode access

!

interface FastEthernet0/3

 switchport access vlan 10

 switchport mode access

!

interface FastEthernet0/4

!

interface FastEthernet0/5

!

interface FastEthernet0/6

!

interface FastEthernet0/7

!

interface FastEthernet0/8

!

interface FastEthernet0/9

 --More-- !

interface FastEthernet0/10

!

interface FastEthernet0/11

!

interface FastEthernet0/12

!

interface FastEthernet0/13

!

interface FastEthernet0/14

!

interface FastEthernet0/15

!

interface FastEthernet0/16

!

interface FastEthernet0/17

!

interface FastEthernet0/18

!

interface FastEthernet0/19

!

interface FastEthernet0/20

!

 --More-- interface FastEthernet0/21

!

interface FastEthernet0/22

!

interface FastEthernet0/23

!

interface FastEthernet0/24

!

interface Vlan1

 no ip address

 no ip route-cache

 shutdown

!

ip http server

!

line con 0

 speed 115200

line vty 5 15

!

!

end

#################### SHOW INT BR ####################

Switch#sh int br

Interface IP-Address OK? Method Status Protocol

Vlan1 unassigned YES unset administratively down down

FastEthernet0/1 unassigned YES unset up up

FastEthernet0/2 unassigned YES unset up up

FastEthernet0/3 unassigned YES unset up up

FastEthernet0/4 unassigned YES unset down down

FastEthernet0/5 unassigned YES unset down down

FastEthernet0/6 unassigned YES unset down down

FastEthernet0/7 unassigned YES unset down down

FastEthernet0/8 unassigned YES unset down down

FastEthernet0/9 unassigned YES unset down down

FastEthernet0/10 unassigned YES unset down down

 --More-- FastEthernet0/11 unassigned YES unset down down

FastEthernet0/12 unassigned YES unset down down

FastEthernet0/13 unassigned YES unset down down

FastEthernet0/14 unassigned YES unset down down

FastEthernet0/15 unassigned YES unset down down

FastEthernet0/16 unassigned YES unset down down

FastEthernet0/17 unassigned YES unset down down

FastEthernet0/18 unassigned YES unset down down

FastEthernet0/19 unassigned YES unset down down

FastEthernet0/20 unassigned YES unset down down

FastEthernet0/21 unassigned YES unset down down

FastEthernet0/22 unassigned YES unset down down

 --More-- FastEthernet0/23 unassigned YES unset down down

FastEthernet0/24 unassigned YES unset down down

#################### SHOW VLAN BR ####################

Switch# sh sh i vlan br

VLAN Name Status Ports

---- -------------------------------- --------- -------------------------------

1 default active Fa0/4, Fa0/5, Fa0/6, Fa0/7

 Fa0/8, Fa0/9, Fa0/10, Fa0/11

 Fa0/12, Fa0/13, Fa0/14, Fa0/15

 Fa0/16, Fa0/17, Fa0/18, Fa0/19

 Fa0/20, Fa0/21, Fa0/22, Fa0/23

 Fa0/24

10 A active Fa0/2, Fa0/3

20 B active

30 C active

40 D active

50 11 active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup

1. **ROUTER**

R1(config-if)#show ip int brie end

R1#sho

\*Mar 1 01:05:53.707: %SYS-5-CONFIG\_I: Configured from console by console

R1#show ip int brie

Interface IP-Address OK? Method Status Protocol

FastEthernet0 192.168.0.129 YES manual up up

FastEthernet0.1 unassigned YES unset up up

FastEthernet0.10 unassigned YES unset deleted down

Serial0 192.168.0.169 YES manual up up

Serial1 192.168.0.165 YES manual up up

R1#show run

Building configuration...

Current configuration : 940 bytes

!

version 12.3

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname R1

!

boot-start-marker

boot-end-marker

!

!

memory-size iomem 25

no aaa new-model

ip subnet-zero

!

!

!

ip cef

!

username R3 password 0 cisco

 --More-- username RB password 0 cisco

!

!

!

interface FastEthernet0

 ip address 192.168.0.129 255.255.255.224

 speed auto

!

interface FastEthernet0.1

!

interface Serial0

 ip address 192.168.0.169 255.255.255.252

 encapsulation ppp

 ppp authentication pap

 ppp pap sent-username R1 password 0 cisco

!

interface Serial1

 ip address 192.168.0.165 255.255.255.252

 encapsulation ppp

 clock rate 64000

 ppp authentication chap

!

router ospf 1

 --More-- log-adjacency-changes

 network 192.168.0.128 0.0.0.31 area 0

 network 192.168.0.164 0.0.0.3 area 0

 network 192.168.0.168 0.0.0.3 area 0

!

ip classless

no ip http server

!

!

line con 0

 logging synchronous

line aux 0

line vty 0 4

!

end

R1# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

 E1 - OSPF external type 1, E2 - OSPF external type 2

 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

 ia - IS-IS inter area, \* - candidate default, U - per-user static route

 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 192.168.0.0/24 is variably subnetted, 10 subnets, 4 masks

O 192.168.0.96/27 [110/782] via 192.168.0.166, 00:03:11, Serial1

O 192.168.0.64/27 [110/1563] via 192.168.0.170, 00:03:11, Serial0

O 192.168.0.0/26 [110/782] via 192.168.0.170, 00:03:11, Serial0

C 192.168.0.168/30 is directly connected, Serial0

C 192.168.0.170/32 is directly connected, Serial0

O 192.168.0.172/30 [110/1562] via 192.168.0.170, 00:03:11, Serial0

O 192.168.0.160/30 [110/782] via 192.168.0.166, 00:03:12, Serial1

 [110/782] via 192.168.0.170, 00:03:12, Serial0

C 192.168.0.164/30 is directly connected, Serial1

C 192.168.0.166/32 is directly connected, Serial1

C 192.168.0.128/27 is directly connected, FastEthernet0

R1#ping show ip route int s 0

Serial0 is up, line protocol is up

 Hardware is PowerQUICC Serial

 Internet address is 192.168.0.169/30

 MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,

 reliability 255/255, txload 1/255, rxload 1/255

 Encapsulation PPP, LCP Open

 Open: CDPCP, IPCP, loopback not set

 Keepalive set (10 sec)

 Last input 00:00:00, output 00:00:00, output hang never

 Last clearing of "show interface" counters 00:21:38

 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

 Queueing strategy: weighted fair

 Output queue: 0/1000/64/0 (size/max total/threshold/drops)

 Conversations 0/3/32 (active/max active/max total)

 Reserved Conversations 0/0 (allocated/max allocated)

 Available Bandwidth 96 kilobits/sec

 5 minute input rate 0 bits/sec, 0 packets/sec

 5 minute output rate 0 bits/sec, 0 packets/sec

 2374 packets input, 47305 bytes, 0 no buffer

 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

 115 input errors, 0 CRC, 115 frame, 0 overrun, 0 ignored, 0 abort

 2388 packets output, 56530 bytes, 0 underruns

 0 output errors, 0 collisions, 176 interface resets

 --More-- 0 output buffer failures, 0 output buffers swapped out

 66 carrier transitions

 DCD=up DSR=down DTR=up RTS=up CTS=up

R1#sho show int s 0 1

Serial1 is up, line protocol is up

 Hardware is PowerQUICC Serial

 Internet address is 192.168.0.165/30

 MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,

 reliability 255/255, txload 1/255, rxload 1/255

 Encapsulation PPP, LCP Open

 Open: CDPCP, IPCP, loopback not set

 Keepalive set (10 sec)

 Last input 00:00:03, output 00:00:03, output hang never

 Last clearing of "show interface" counters 00:21:28

 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

 Queueing strategy: weighted fair

 Output queue: 0/1000/64/0 (size/max total/threshold/drops)

 Conversations 0/1/32 (active/max active/max total)

 Reserved Conversations 0/0 (allocated/max allocated)

 Available Bandwidth 96 kilobits/sec

 5 minute input rate 0 bits/sec, 0 packets/sec

 5 minute output rate 0 bits/sec, 0 packets/sec

 1109 packets input, 37528 bytes, 0 no buffer

 Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

 72 input errors, 0 CRC, 71 frame, 0 overrun, 0 ignored, 0 abort

 886 packets output, 29917 bytes, 0 underruns

 0 output errors, 0 collisions, 146 interface resets

 --More-- 0 output buffer failures, 0 output buffers swapped out

 296 carrier transitions

 DCD=up DSR=up DTR=up RTS=up CTS=up

R1#show int s 1 fa 0

FastEthernet0 is up, line protocol is up

 Hardware is PQUICC\_FEC, address is 0002.1762.1ec0 (bia 0002.1762.1ec0)

 Internet address is 192.168.0.129/27

 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,

 reliability 255/255, txload 1/255, rxload 1/255

 Encapsulation ARPA, loopback not set

 Keepalive set (10 sec)

 Full-duplex, 100Mb/s, 100BaseTX/FX

 ARP type: ARPA, ARP Timeout 04:00:00

 Last input 00:00:04, output 00:00:02, output hang never

 Last clearing of "show interface" counters never

 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

 Queueing strategy: fifo

 Output queue: 0/40 (size/max)

 5 minute input rate 0 bits/sec, 0 packets/sec

 5 minute output rate 0 bits/sec, 0 packets/sec

 571 packets input, 76221 bytes

 Received 406 broadcasts, 0 runts, 0 giants, 0 throttles

 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

 0 watchdog

 0 input packets with dribble condition detected

 877 packets output, 100414 bytes, 0 underruns

 4 output errors, 0 collisions, 6 interface resets

 --More-- 0 babbles, 0 late collision, 0 deferred

 4 lost carrier, 0 no carrier

 0 output buffer failures, 0 output buffers swapped out

R1#ping 192.168.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R1#ping 192.168.0.1 66

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.66, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

R1#ping 192.168.0.66 19 72 3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.173, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R1#ping 192.168.0.173 0

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.170, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

R1#ping 192.168.0.170 8

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.178, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

R1#ping 192.168.0.178 4

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.174, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms

R1#ping 192.168.0.174 7

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.177, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms

R1#ping 192.168.0.177 66

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.166, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

R1#ping 192.168.0.166 30

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.130, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

R1#ping 192.168.0.130 66

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.166, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

R1#ping 192.168.0.166 1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.0.161, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

R1#show controler

R1#show controllers

Interface FastEthernet0

Hardware is PQUICC MPC860T ADDR: 810BBBA8, FASTSEND: 8003A880

DIST ROUTE ENABLED: 0

Route Cache Flag: 11

 ADDR\_LOW =0x00021762, ADDR\_HIGH =0x00001EC0, HASH\_HIGH =0x00800100, HASH\_LOW =0x00020000

 R\_DES\_ST =0x01917540, X\_DES\_ST =0x01917680, R\_BUFF\_SIZ=0x00000600, ECNTRL =0xF0000002

 IEVENT =0x00000000, IMASK =0x0A000000, IVEC =0xC0000000, R\_DES\_ACT=0x01000000

 X\_DES\_ACT=0x00000000, MII\_DATA =0x50821000, MII\_SPEED =0x00000014, R\_BOUND =0x00000600

 R\_FSTART =0x00000500, X\_FSTART =0x00000440, FUN\_CODE =0x7F000000, R\_CNTRL =0x00000004

 R\_HASH =0x3F000000

 X\_CNTRL =0x00000004

 HW filtering information:

 Promiscuous Mode Disabled

 Software MAC address filter(hash:length/addr/mask/hits):

 pquicc\_fec\_instance=0x810BDFE0

 rx ring entries=32, tx ring entries=32

 rxring=0x1917540, rxr shadow=0x810BE220, rx\_head=12, rx\_tail=0

 txring=0x1917680, txr shadow=0x81181E48, tx\_head=29, tx\_tail=29, tx\_count=0

 --More--

RX\_RING\_ENTRIES

 status 8000, len 79, buf\_ptr 191D140

 status 8000, len DE, buf\_ptr 191AB00

 status 8000, len 67, buf\_ptr 191B7C0

 status 8000, len A2, buf\_ptr 1920440

 status 8000, len C6, buf\_ptr 191C480

 status 8000, len 79, buf\_ptr 1918B20

 status 8000, len DE, buf\_ptr 1922A80

 status 8000, len 67, buf\_ptr 191CAE0

 status 8000, len 4E, buf\_ptr 19184C0

 status 8000, len A2, buf\_ptr 191EAC0

 status 8000, len C6, buf\_ptr 1924A60

 status 8000, len 79, buf\_ptr 191F120

 status 8000, len DE, buf\_ptr 191F780

 status 8000, len 67, buf\_ptr 191FDE0

 status 8000, len A2, buf\_ptr 1921760

 status 8000, len C6, buf\_ptr 191B160

 status 8000, len 79, buf\_ptr 1920AA0

 status 8000, len B6, buf\_ptr 1921DC0

 status 8000, len 122, buf\_ptr 1921100

 status 8000, len BE, buf\_ptr 1917E60

 status 8000, len 67, buf\_ptr 1922420

 --More-- status 8000, len 4E, buf\_ptr 191BE20

 status 8000, len 40, buf\_ptr 19230E0

 status 8000, len 4E, buf\_ptr 1919180

 status 8000, len 108, buf\_ptr 1923740

 status 8000, len 140, buf\_ptr 1923DA0

 status 8000, len 4E, buf\_ptr 1917800

 status 8000, len 79, buf\_ptr 1924400

 status 8000, len DE, buf\_ptr 191DE00

 status 8000, len 67, buf\_ptr 19197E0

 status 8000, len A2, buf\_ptr 1919E40

 status A000, len C6, buf\_ptr 191A4A0

TX\_RING\_ENTRIES

 status 0, len C1, buf\_ptr 194BA3A

 status 0, len 69, buf\_ptr 194B3BA

 status 0, len BA, buf\_ptr 194AD3A

 status 0, len A2, buf\_ptr 194BA3A

 status 0, len A2, buf\_ptr 194B3BA

 status 0, len A2, buf\_ptr 194AD3A

 status 0, len 5D, buf\_ptr 194BA3A

 status 0, len 4A, buf\_ptr 194B3BA

 status 0, len 4A, buf\_ptr 194AD3A

 status 0, len 5A, buf\_ptr 180020A

 --More-- status 0, len 12B, buf\_ptr 194BA3A

 status 0, len AF, buf\_ptr 194AD3A

 status 0, len 72, buf\_ptr 194BA3A

 status 0, len 78, buf\_ptr 194B3BA

 status 0, len 9E, buf\_ptr 194AD3A

 status 0, len 1C6, buf\_ptr 194BA3A

 status 0, len 5D, buf\_ptr 194B3BA

 status 0, len 5D, buf\_ptr 194AD3A

 status 0, len C1, buf\_ptr 194BA3A

 status 0, len 7E, buf\_ptr 194B3BA

 status 0, len 36, buf\_ptr 194AD3A

 status 0, len C1, buf\_ptr 194BA3A

 status 0, len 69, buf\_ptr 194B3BA

 status 0, len BA, buf\_ptr 194AD3A

 status 0, len E6, buf\_ptr 194BA3A

 status 0, len 5D, buf\_ptr 194B3BA

 status 0, len 5D, buf\_ptr 194B3BA

 status 0, len C1, buf\_ptr 194AD3A

 status 0, len 69, buf\_ptr 194BA3A

 status 0, len BA, buf\_ptr 194B3BA

 status 0, len E6, buf\_ptr 194AD3A

 status 2000, len 5D, buf\_ptr 194AD3A

 throttled=0, enabled=0, disabled=0

 --More-- rx\_framing\_err=0, rx\_overflow\_err=0, rx\_buffer\_err=0

 rx\_no\_enp=0, rx\_discard=0

 tx\_one\_col\_err=0, tx\_more\_col\_err=0, tx\_no\_enp=0, tx\_deferred\_err=0

 tx\_underrun\_err=0, tx\_late\_collision\_err=0, tx\_loss\_carrier\_err=4

 tx\_exc\_collision\_err=0, tx\_buff\_err=0, fatal\_tx\_err=0

 PHY registers:

 Register 00 1000

 Register 01 782D

 Register 02 7810

 Register 03 0003

 Register 04 01E1

 Register 05 41E1

 Register 06 0001

 Register 16 0000

 Register 17 0000

 Register 18 4000

 Register 19 0800

 Register 20 38C8

 --More-- Interface Serial0

Hardware is PowerQUICC MPC860

DTE V.35 TX and RX clocks detected.

idb at 0x811AA960, driver data structure at 0x811ACBC4

SCC Registers:

General [GSMR]=0x2:0x00000030, Protocol-specific [PSMR]=0x8

Events [SCCE]=0x0000, Mask [SCCM]=0x001F, Status [SCCS]=0x06

Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E

Interrupt Registers:

Config [CICR]=0x00365F80, Pending [CIPR]=0x04000A00

Mask [CIMR]=0x30200440, In-srv [CISR]=0x00000000

Command register [CR]=0x640

Port A [PADIR]=0x4000, [PAPAR]=0x663C

 [PAODR]=0x0000, [PADAT]=0xFFF3

Port B [PBDIR]=0x0600F, [PBPAR]=0x0900E

 [PBODR]=0x00000, [PBDAT]=0x00CEC

Port C [PCDIR]=0x00C, [PCPAR]=0x000

 [PCSO]=0x280, [PCDAT]=0xC30, [PCINT]=0x000

Receive Ring

 rmd(FF002530): status 9000 length 12 address 193DD04

 rmd(FF002538): status B000 length 12 address 193E384

Transmit Ring

 tmd(FF0025B0): status 5C00 length 10 address 1800994

 --More--

1. **HOST**



 ***Ping***



 ***Hasil Share File***

1. **PEMBAHASAN**
2. **SWITCH**

Pada kegiatan praktikum kali ini kelompok kami menggunakan 1 Router dan 1 Switch dan 3 komputer (1 untuk konfigurasi router, 1 untuk konfigurasi switch, 1 sebagai user sebuah vlan). Kabel yang dibutuhkan adalah kabel serial yang menghubungkan antar router. Kemudian kabel straight untuk menghubungkan router ke switch dan komputer ke switch.

 Pada Switch port fa0/1 untuk menghubungkan ke router . Port Fa0/2 ke switch kelompok lain dan port fa0/3 ke komputer untuk konfigurasi dan 1 lagi tambahan fa 0/4 untuk user(telnet).

 Hal pertama yang kami lakukan dalam kegiatan praktikum ini adalah menghubungkan semua hardware yang digunakan (router, switch, komputer, kabel, dll). Kemudian setelah semua selesai terpasang kami memulai konfigurasi.

 Konfigurasi dimulai dengan menjadikan switch kelompok kami sebagai server. Kemudian kami mensetting vtp domain CISCO dan vtp password CISCO, sebagai nama dan password. Kemudian kami membuat vlan dan menentukan namanya. Vlan 10 dengan nama A, vlan 20 dengan nama B, vlan 30 dengan nama C, vlan 40 dengan nama D, dan terakhir vlan 50 dengan nama 11.

 kemudian mensetting interface fa 0/1 (menuju router) dengan mode trunk, interface fa0/2 , fa0/3, dan fa0/4 dengan mode access vlan 10. karena area kelompok A menggunakan Vlan 10.

Switch S1

pada topologi diatas, Switch S1 dilakukan konfigurasi sebagai berikut :

* **setting vtp**

vtp mode

Switch kelompok A menjadi server dari switch- switch kelompok lain

Konfigurasi : Vtp mode SERVER

vtp domain

memberikan nama vtp

Konfigurasi : vtp domain CISCO

vtp password

memberikan password vtp

Konfigurasi : vtp password CISCO

* **setting vlan**

di switch Kel-A dibuat :

vlan 10 yang bernama A

* + - * + vlan 10
				+ name A

vlan 20 yang bernama B

* + - * + vlan 20
				+ name B

vlan 30 yang bernama C

* + - * + vlan 30
				+ name C

vlan 40 yang bernama D

* + - * + vlan 40
				+ name D

vlan 50 yang bernama 11

* + - * vlan 50
			* name 11
* **Port**

dari switch Kelompok A, harus ada pengkonfigurasian vlan yang telah dibuat tadi melewati port mana dari switch tersebut :

untuk vlan 10 port yang aktif adalah fa 0/2 , fa0/3 dan fa 0/4(telnet)

 untuk fa0/2

* + - * + int fa 0/2
				+ switchport mode access
				+ switchport access vlan 10

 untuk fa0/3

* + - * + int fa 0/3
				+ switchport mode access
				+ switchport access vlan 10

untuk fa0/4

* + - * + int fa 0/4
				+ switchport mode access
				+ switchport access vlan 10

untuk vlan 20,30,40,50 port yang aktif adalah Switch dari kelompok lain

1. **ROUTER**

Pada Topologi, kelompok kami mendapat tugas untuk mengkonfigurasi router R1. Pada router tersebut, pertama-tama kita melakukan pengalamatan, Serial 1 dengan IP address 192.168.0.165/30 untuk menghubungkan dengan R3, kemudian Serial 0 dengan IP Address 192.168.0.169/30 untuk network yang menghubungkan router dengan R2, dan fast ethernet 0/1 dengan IP address 192.168.0.129/27 untuk LAN A yang terhubung dengan switch.

 Selain itu kita juga mensetting router OSPF dengan memasukkan network yang terhubung langsung.

 R1(config)#router ospf 1

 R1(config-router)#network 192.168.0.164 0.0.0.3 area 0

 R1(config-router)#network 192.168.0.168 0.0.0.3 area 0

 R1(config-router)#network 192.168.0.128 0.0.0.31 area 0

Dan tinggal menunggu tabel routing konvergens, maka didapat tabel routing sbb :

R1# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

 E1 - OSPF external type 1, E2 - OSPF external type 2

 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

 ia - IS-IS inter area, \* - candidate default, U - per-user static route

 o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

 192.168.0.0/24 is variably subnetted, 10 subnets, 4 masks

O 192.168.0.96/27 [110/782] via 192.168.0.166, 00:03:11, Serial1

O 192.168.0.64/27 [110/1563] via 192.168.0.170, 00:03:11, Serial0

O 192.168.0.0/26 [110/782] via 192.168.0.170, 00:03:11, Serial0

C 192.168.0.168/30 is directly connected, Serial0

C 192.168.0.170/32 is directly connected, Serial0

O 192.168.0.172/30 [110/1562] via 192.168.0.170, 00:03:11, Serial0

O 192.168.0.160/30 [110/782] via 192.168.0.166, 00:03:12, Serial1

 [110/782] via 192.168.0.170, 00:03:12, Serial0

C 192.168.0.164/30 is directly connected, Serial1

C 192.168.0.166/32 is directly connected, Serial1

C 192.168.0.128/27 is directly connected, FastEthernet0

Sesudah tabel routing konvergence, maka saatnya mengkonfigurasi autentikasi untuk PAP dan CHAP. PAP akan digunakan untuk autentikasi dengan R2, maka pertama kali kita mendaftarkan username dan password untuk Router R2

R1(config)#username RB password cisco

Setelah mendaftarkan username, yang kita lakukan adalah mengubah enkapsulasi HDLC pada serial 0 dengan enkapsulasi PPP

R1(config)#inteface serial 0

R1(config-if)#encapsulation PPP

Kemudian kita mengirimkan username dan password R1 kepada router R2

R1(config-if)#ppp authentication pap

R1(config-if)#ppp pap sent-username R1 password cisco

Setelah itu kita verifikasi dengan Show Interface serial 0, akan terlihat bahwa encapsulasi akan berubah ke PPP, dan LCP Open, ini menunjukkan bahwa autentikasi berhasil dan Router bisa saling berkomunikasi lagi. Ketika LCP Closed, maka ini menunjukkan bahwa autentikasi belum berhasil, ini mungkin bisa saja dari kesalahan dalam menuliskan username dan password, atau kesalahan fisik, pada saat LCP closed, Tabel routing yang didapat dari interface serial tersebut akan hilang, dan akan muncul kembali jika LCP Open.

Ketika sudah di verifikasi untuk autentikasi PAP, maka saatnya mengkonfigurasi autentikasi CHAP untuk serial 1 yang terhubung ke R3. Pertama-tama, kita mendaftarkan username dan password untuk R3

R1(config)#username R3 password cisco

Sesudah itu, yang kita lakukan adalah mensetting enkapsulasi untuk serial 1 menjadi PPP.

R1(config)#inteface serial 1

R1(config-if)#encapsulation PPP

Sesudah demikian, yang perlu kita lakukan hanya mensetting autentikasinya menjadi CHAP

R1(config-if)#ppp authentication chap

Sesudah itu, kita melakukan verifikasi lagi dengan show interface serial 1, apabila enkapsulasi sudah berganti ke PPP dan LCP open, maka autentikasi sukses.

1. **KENDALA YANG DIHADAPI**

Kendala yang terjadi adalah ketika username untuk CHAP harus sesuai dengan hostname router tetangga. Kelompok kami sempat mencoba dengan host yang berbeda. Ketika kita cek di **show ip interface brief**, line protocol ke serial 1 masih **up**. Ini menunjukkan bahwa koneksi masih bisa dilakukan, namun, ketika serial kita shutdown, kemudian no shutdown lagi, line protocol down. Dan koneksi tidak terjadi. Ini dikarenakan LCP sudah terbentuk terlebih dahulu dan ketika kita mengganti username dan password tanpa shutdown dan no shutdown, maka hal itu tidak berpengaruh. Dan username dan hostname untuk CHAP harus **sama.**

1. **KESIMPULAN**

Praktkum saat itu menggunakan OSPF routing agar setiap router kelompok A, B, C, D dapat saling berhubungan. Selain itu pada praktikun tersebut juga diterapkan keamanan antar serial, yaitu Password Authentication Protocol (PAP) dan Challenge Handshake Authentication Protocol (CHAP) . Dengan PAP password dikirimkan dalam bentuk clear text(teks biasa) sehingga tidak aman, karena password dikirim secara clear text, pasangan user name dan password dikirim berkali-kali sampai authentikasi tercapai atau koneksi terputus. Sedangkan CHAP menggunakan metode hashing dan MD5 untuk mengencrypt password sehingga lebih aman, selain itu protokol ini digunakan pada start-up awal dari datalink dan pada saat checkup periodik pada link untuk memastikan bahwa router masih berkomunikasi dengan host yang sama.

Sedangkan untuk switch: switch kelompok A di setting sebagai VTP server dengan domain CISCO dan password CISCO, sehingga switch kelompok B, C, D, E di setting sebagai VTP client dengan domain dan password yang sama dengan VTP servernya. Setelah itu maka di trunk dan setiap switch yang di setting sebagai VTP client mendapat update vlan dari switch yang di setting sebagai VTP server.

Dengan topologi dan konfigurasi yang dilakukan seperti di atas, praktikum tersebut dapat berjalan dengan sukses. Setting PAP dan CHAP untuk masing-masing router A, B, C, D tidak mengalami kendala. Setiap kelompok dapat saling berkomunikasi dan dapat melakukan ping pada alamat IP yang terjauh, selain itu setiap router pada masing-masing kelompok mendapatkan semua IP yang terhubung melalui OSPF routing.

1. **TABEL PEMBAGIAN TUGAS**

|  |  |  |
| --- | --- | --- |
| **NIM** | **NAMA** | **PEMBAGIAN TUGAS** |
| **LAPORAN** | **PRAKTIKKUM** |
| 22084417 | Alexsander Niko Dian | Kesimpulan, kendala | Dokumentasi, Setting switch |
| 22084422 | Damianus Yudha Christyawan | Pembahasan router, Capture hasil switch, router | Mengkonfigurasi Router |
| 22084454 | Brigitta Celna F | Landasan teori | Setting Router  |
| 22084494 | Catharina Nariswari | Pembahasan Switch | Mengkonfigurasi Switch |
| 22084511 | Adi Atmaja | Capture host | Dokumentasi topologi, setting host |