2016

**LABORATORIUM PRIDE**

**KELOMPOK KEAHLIAN PROGRAMMING**

**FAKULTAS ILMU TERAPAN**

**UNIVERSITAS TELKOM**



Modul Praktikum Instalasi Jaringan Komputer

**Hanya dipergunakan di lingkungan Fakultas Ilmu Terapan**

## DAFTAR PENYUSUN

Hariandi Maulid, S.T., M.Sc

M. Yusril Helmi Setyawan, M. Kom

Diperbaiki Oleh

Hariandi Maulid, S.T., M.Sc

## LEMBAR REVISI

|  |  |  |
| --- | --- | --- |
| No | Keterangan Revisi | Tanggal Revisi Terakhir |
| 1 | Revisi Bagian Pertama | 15 Agustus 2016 |
|  |  |  |
|  |  |  |

## LEMBAR PERNYATAAN

Saya yang bertanggung jawab di bawah ini:

Nama : Hariandi Maulid, S.T., M.Sc

NIP : 15781201-4

Dosen PJMP : Instalasi Jaringan Komputer

Kelompok Keahlian : Programming

Menerangkan dengan sesungguhnya bahwa modul ini telah diteview dan akan digunakan untuk pelaksanaan praktikum di Semester Genap Tahun Ajaran 2016/2017 di Laboratorium pride Fakultas Ilmu Terapan Universitas Telkom

Bandung, Agustus 2016

Mengetahui,

Ketua Kelompok Keahlian Dosen PJMP

Hariandi Maulid, M.Sc. Hariandi Maulid, M.Sc.

NIP 15781201-4 NIP 15781201-4

# DAFTAR ISI

[DAFTAR PENYUSUN 1](#_Toc459448056)

[LEMBAR REVISI 2](#_Toc459448057)

[LEMBAR PERNYATAAN 3](#_Toc459448058)

[DAFTAR ISI 4](#_Toc459448059)

[DAFTAR GAMBAR 5](#_Toc459448060)

[DAFTAR PROGRAM 7](#_Toc459448061)

[DAFTAR TABEL 8](#_Toc459448062)

[Modul 0 : Running Modul 9](#_Toc459448063)

[0.1 Tujuan 9](#_Toc459448064)

[0.2 Peraturan Praktikum 9](#_Toc459448065)

[0.3 Penilaian Praktikum 10](#_Toc459448066)

[Modul 1 : Basic Network 11](#_Toc459448067)

[1.1 Tujuan 11](#_Toc459448068)

[1.2 Alat & Bahan 11](#_Toc459448069)

[1.3 Dasar Teori 11](#_Toc459448070)

[1.3.1 Network Route 11](#_Toc459448071)

[1.3.2 Topology Orientation and Building a Small Network 13](#_Toc459448072)

[1.4 Latihan 15](#_Toc459448073)

# DAFTAR GAMBAR

[Gambar 2‑1 Output Pointer **Error! Bookmark not defined.**](#_Toc408777776)

[Gambar 2‑2 Elemen Single Linked List **Error! Bookmark not defined.**](#_Toc408777777)

[Gambar 2‑3 Single Linked List dengan Elemen Kosong **Error! Bookmark not defined.**](#_Toc408777778)

[Gambar 2‑4 Single Linked List dengan 3 Elemen **Error! Bookmark not defined.**](#_Toc408777779)

[Gambar 2‑5 Circular Single Linked List **Error! Bookmark not defined.**](#_Toc408777780)

[Gambar 2‑7Single Linked List Insert First 2 **Error! Bookmark not defined.**](#_Toc408777781)

[Gambar 2‑8Single Linked List Insert First 3 **Error! Bookmark not defined.**](#_Toc408777782)

[Gambar 2‑9Single Linked List Insert Last 1 **Error! Bookmark not defined.**](#_Toc408777783)

[Gambar 2‑10Single Linked List Insert Last 2 **Error! Bookmark not defined.**](#_Toc408777784)

[Gambar 2‑11Single Linked List Insert Last 3 **Error! Bookmark not defined.**](#_Toc408777785)

[Gambar 2‑12Single Linked List Insert After 1 **Error! Bookmark not defined.**](#_Toc408777786)

[Gambar 2‑13Single Linked List Insert After 2 **Error! Bookmark not defined.**](#_Toc408777787)

[Gambar 2‑14Single Linked List Insert After 3 **Error! Bookmark not defined.**](#_Toc408777788)

[Gambar 2‑15 Single Linked List Delete First I **Error! Bookmark not defined.**](#_Toc408777789)

[Gambar 2‑16Single Linked List Delete First 2 **Error! Bookmark not defined.**](#_Toc408777790)

[Gambar 2‑17Single Linked List Delete First 3 **Error! Bookmark not defined.**](#_Toc408777791)

[Gambar 2‑18Single Linked List Delete Last 1 **Error! Bookmark not defined.**](#_Toc408777792)

[Gambar 2‑19Single Linked List Delete Last 2 **Error! Bookmark not defined.**](#_Toc408777793)

[Gambar 2‑20Single Linked List Delete Last 3 **Error! Bookmark not defined.**](#_Toc408777794)

[Gambar 2‑21Single Linked List Delete After 1 **Error! Bookmark not defined.**](#_Toc408777795)

[Gambar 2‑22Single Linked List Delete After 2 **Error! Bookmark not defined.**](#_Toc408777796)

[Gambar 2‑23Single Linked List Delete After 3 **Error! Bookmark not defined.**](#_Toc408777797)

[Gambar 3‑1Double Linked List dengan Elemen Kosong **Error! Bookmark not defined.**](#_Toc408777798)

[Gambar 3‑3 Circular Double Linked List **Error! Bookmark not defined.**](#_Toc408777800)

[Gambar 3‑5 Double Linked List Insert First 2 **Error! Bookmark not defined.**](#_Toc408777801)

[Gambar 3‑6 Double Linked List Insert First 3 **Error! Bookmark not defined.**](#_Toc408777802)

[Gambar 3‑7 Double Linked List Insert First 4 **Error! Bookmark not defined.**](#_Toc408777803)

[Gambar 3‑9 Double Linked List Insert Last 2 **Error! Bookmark not defined.**](#_Toc408777804)

[Gambar 3‑10Double Linked List Insert Last 3 **Error! Bookmark not defined.**](#_Toc408777805)

[Gambar 3‑11 Double Linked List Insert Last 4 **Error! Bookmark not defined.**](#_Toc408777806)

[Gambar 2‑10 Double Linked List Insert After 1 **Error! Bookmark not defined.**](#_Toc408777807)

[Gambar 3‑13 Double Linked List Insert After 2 **Error! Bookmark not defined.**](#_Toc408777808)

[Gambar 3‑14 Double Linked List Insert After 3 **Error! Bookmark not defined.**](#_Toc408777809)

[Gambar 3‑15 Double Linked List Delete First 1 **Error! Bookmark not defined.**](#_Toc408777810)

[Gambar 3‑16 Double Linked List Delete First 2 **Error! Bookmark not defined.**](#_Toc408777811)

[Gambar 3‑17 Double Linked List Delete First 3 **Error! Bookmark not defined.**](#_Toc408777812)

[Gambar 3‑18 Double Linked List Delete Last 1 **Error! Bookmark not defined.**](#_Toc408777813)

[Gambar 3‑19 Double Linked List Delete Last 2 **Error! Bookmark not defined.**](#_Toc408777814)

[Gambar 3‑20 Double Linked List Delete Last 3 **Error! Bookmark not defined.**](#_Toc408777815)

[Gambar 3‑21 Double Linked List Delete After 1 **Error! Bookmark not defined.**](#_Toc408777816)

[Gambar 3‑22 Double Linked List Delete After 2 **Error! Bookmark not defined.**](#_Toc408777817)

[Gambar 3‑23 Double Linked List Delete After 3 **Error! Bookmark not defined.**](#_Toc408777818)

[Gambar 4‑1 Muti Linked List **Error! Bookmark not defined.**](#_Toc408777819)

[Gambar 4‑2 Multi Linked List Insert Anak 1 **Error! Bookmark not defined.**](#_Toc408777820)

[Gambar 4‑3 Multi Linked List Insert Anak 2 **Error! Bookmark not defined.**](#_Toc408777821)

[Gambar 4‑4 Multi Linked List Delete Anak 1 **Error! Bookmark not defined.**](#_Toc408777822)

[Gambar 4‑5 Multi Linked List Delete Anak 2 **Error! Bookmark not defined.**](#_Toc408777823)

[Gambar 4‑6 Multi Linked List Delete Induk 1 **Error! Bookmark not defined.**](#_Toc408777824)

[Gambar 5‑1Stack dengan 3 Elemen **Error! Bookmark not defined.**](#_Toc408777825)

[Gambar 5‑2 Stack Push 1 **Error! Bookmark not defined.**](#_Toc408777826)

[Gambar 5‑3 Stack Push 2 **Error! Bookmark not defined.**](#_Toc408777827)

[Gambar 5‑4 Stack Push 4 **Error! Bookmark not defined.**](#_Toc408777828)

[Gambar 5‑5 Stack Pop 1 **Error! Bookmark not defined.**](#_Toc408777829)

[Gambar 5‑6 Stack Pop 2 **Error! Bookmark not defined.**](#_Toc408777830)

[Gambar 5‑7 Stack Pop 3 **Error! Bookmark not defined.**](#_Toc408777831)

[Gambar 6‑2 Queue Insert 1 **Error! Bookmark not defined.**](#_Toc408777833)

[Gambar 6‑3 Queue Insert 2 **Error! Bookmark not defined.**](#_Toc408777834)

[Gambar 6‑4 Queue Insert 3 **Error! Bookmark not defined.**](#_Toc408777835)

[Gambar 6‑5 Queue Delete 1 **Error! Bookmark not defined.**](#_Toc408777836)

[Gambar 6‑6 Queue Delete 2 **Error! Bookmark not defined.**](#_Toc408777837)

[Gambar 6‑7 Queue Delete 3 **Error! Bookmark not defined.**](#_Toc408777838)

[Gambar 7‑1 arrayQueue.h **Error! Bookmark not defined.**](#_Toc408777839)

[Gambar 8‑1 Heap Tree **Error! Bookmark not defined.**](#_Toc408777840)

[Gambar 8‑2 Binary Search Tree Insert **Error! Bookmark not defined.**](#_Toc408777841)

[Gambar 8‑3 Binary Search Tree sebelum di-Delete **Error! Bookmark not defined.**](#_Toc408777842)

[Gambar 8‑4 Binary Search Tree setelah di-Delete **Error! Bookmark not defined.**](#_Toc408777843)

[Gambar 8‑5 Traversal pada Binary Tree 1 **Error! Bookmark not defined.**](#_Toc408777844)

[Gambar 8‑6 traversal pada Binary Tree 2 **Error! Bookmark not defined.**](#_Toc408777845)

[Gambar 9‑1 Graph Kost dan Common Lab **Error! Bookmark not defined.**](#_Toc408777846)

[Gambar 9‑2 Graph Tidak Berarah (Undirected Graph) **Error! Bookmark not defined.**](#_Toc408777847)

[Gambar 9‑3 Graph **Error! Bookmark not defined.**](#_Toc408777848)

[Gambar 9‑4 Representasi Graph Array 2 Dimensi **Error! Bookmark not defined.**](#_Toc408777849)

[Gambar 9.5 Representasi Graph Multi Linked List **Error! Bookmark not defined.**](#_Toc408777850)

[Gambar 9‑5 Graph Jarak Antar kota **Error! Bookmark not defined.**](#_Toc408777851)

[Gambar 9‑6 Graph Breadth First Search (BFS) **Error! Bookmark not defined.**](#_Toc408777852)

[Gambar 9‑7 Graph Depth First Search (DFS) **Error! Bookmark not defined.**](#_Toc408777853)

[Gambar 10‑1 Graph Berarah (Directed Graph) **Error! Bookmark not defined.**](#_Toc408777854)

[Gambar 10‑2 Graph Berarah 2 **Error! Bookmark not defined.**](#_Toc408777855)

[Gambar 10‑3 Ilustrasi Topological Sort **Error! Bookmark not defined.**](#_Toc408777856)

# DAFTAR PROGRAM

[Program 1‑1 Fungsi 1](#_Toc378324154)

[Program 1‑2 Pemanggilan dengan Nilai (call by value) 1](#_Toc378324155)

[Program 1‑3 Pemeanggilan dengan Referensi (call by reference) 1](#_Toc378324156)

[Program 1‑4 Prosedur 1](#_Toc378324157)

[Program 1‑5 Rekursif 1](#_Toc378324158)

[Program 1‑6 Copy String dengan Array 1 1](#_Toc378324159)

[Program 1‑7 Copy String dengan Array 2 1](#_Toc378324160)

[Program 2‑1 Pointer **Error! Bookmark not defined.**](#_Toc378324161)

[Program 3‑1 Deklarasi Struktur Data Double Linked List **Error! Bookmark not defined.**](#_Toc378324162)

[Program 4‑1 multilist.h **Error! Bookmark not defined.**](#_Toc378324163)

[Program 4‑2 adtmulti.h **Error! Bookmark not defined.**](#_Toc378324164)

[Program 5‑1 Deklarasi Struktur Data Stack **Error! Bookmark not defined.**](#_Toc378324165)

[Program 5‑2 Stack Representasi Tabel **Error! Bookmark not defined.**](#_Toc378324166)

[Program 5‑3 Hanoi.h **Error! Bookmark not defined.**](#_Toc378324167)

[Program 6‑1 Deklarasi Struktur Data Queue **Error! Bookmark not defined.**](#_Toc378324168)

[Program 6‑2 Queue.h **Error! Bookmark not defined.**](#_Toc378324169)

[Program 6‑3 queuebarang.h **Error! Bookmark not defined.**](#_Toc378324170)

[Program 8‑1 tree.h **Error! Bookmark not defined.**](#_Toc378324171)

[Program 9‑1 Deklarasi Struktur Data Graph dengan Representasi Array 2 Dimensi **Error! Bookmark not defined.**](#_Toc378324172)

[Program 9‑2 graph.h **Error! Bookmark not defined.**](#_Toc378324173)

[Program 10‑1 topological.h **Error! Bookmark not defined.**](#_Toc378324174)

# DAFTAR TABEL

[Tabel 1‑1 Ilustrasi Array Dua Dimensi 1](#_Toc378324175)

[Tabel 9‑1 Container Queue BFS **Error! Bookmark not defined.**](#_Toc378324176)

[Tabel 9‑2 Container Stack DFS **Error! Bookmark not defined.**](#_Toc378324177)

# Running Modul

## Tujuan

Setelah mengikuti Running Modul mahasiswa diharapkan dapat:

1. Memahami peraturan kegiatan praktikum.
2. Memahami Hak dan Kewajiban praktikan dalam kegiatan praktikum.
3. Memhami komponen penilaian kegiatan praktikum.

## Peraturan Praktikum

1. Praktikum diampu oleh **Dosen Kelas** dan dibantu oleh **Asisten Laboratorium** dan **Asisten Praktikum**.
2. Praktikum dilaksanakan di Gedung FIT lantai 2 (**PRIDE LAB**) sesuai jadwal yang ditentukan.
3. Praktikan wajib membawa **modul praktikum, kartu praktikum, dan alat tulis**.
4. Praktikan wajib mengisi **daftar hadir** dan **BAP praktikum** dengan bolpoin **bertinta hitam**.
5. Durasi kegiatan praktikum **D3 = 4 jam (200 menit)**.
6. 15 menit untuk pengerjaan Tes Awal atau wawancara Tugas Pendahuluan
7. 60 menit untuk penyampaian materi
8. 125 menit untuk pengerjaan jurnal dan tes akhir
9. Jumlah **pertemuan praktikum**:
   * 10 kali di lab (praktikum rutin)
   * 3 kali di luar lab (terkait Tugas Besar dan/atau UAS)
   * 1 kali berupa presentasi Tugas Besar dan/atau pelaksanaan UAS
10. Praktikan **wajib hadir minimal 75%** dari seluruh pertemuan praktikum di lab.Jika total kehadiran kurang dari 75% maka nilai UAS/ Tugas Besar = 0.
11. Praktikan yang datang terlambat :

* <= 30 menit : diperbolehkan mengikuti praktikum tanpa tambahan waktu Tes Awal
* > 30 menit : tidak diperbolehkan mengikuti praktikum

1. Saat praktikum berlangsung, asisten praktikum dan praktikan:
   * Wajib menggunakan **seragam** sesuai aturan Institusi.
   * Wajib mematikan/ men-silent semua **alat komunikasi**(smartphone, tab, iPad, dsb).
   * Dilarang membuka **aplikasi yang tidak berhubungan** dengan praktikum yang berlangsung.
   * Dilarang mengubah **setting software maupun hardware** komputer tanpa ijin.
   * Dilarang **membawa makanan maupun minuman** di ruang praktikum.
   * Dilarang **memberikan jawaban ke praktikan lain** (pre-test, TP, jurnal, dan post-test).
   * Dilarang **menyebarkan soal pre-test, jurnal, dan post-test**.
   * Dilarang**membuang sampah/sesuatu apapun** di ruangan praktikum.
2. Setiap praktikan dapat mengikuti praktikum susulan maksimal 2 modul untuk satu praktikum.
   * Praktikan yang dapat mengikuti praktikum susulan hanyalah praktikan yang memenuhi syarat sesuai ketentuan Institusi, yaitu rawat inap di Rumah Sakit (menunjukkan bukti rawat inap dan resep obat dari RS), tugas dari Institusi (menunjukkan surat dinas dari Institusi), atau mendapat musibah (menunjukkan surat keterangan dari orangtua/ wali mahasiswa).
   * Persyaratan untuk praktikum susulan diserahkan sesegera mungkin ke Asisten Praktikum untuk keperluan administrasi.
3. Pelanggaran terhadap peraturan praktikum ini akan ditindak secara tegas secara berjenjang di lingkup Kelas, Laboratorium, Program Studi, Fakultas, hingga Institusi.

## Penilaian Praktikum

1. Komponen penilaian praktikum:

**60%** nilai permodul dan **40%** nilai Tugas Besar (atau UAS praktek)

1. Seluruh komponen penilaian beserta pembobotannya ditentukan oleh dosen **PJMP**
2. Penilaian permodul dilakukan oleh **asisten praktikum**, sedangkan nilai Tugas Besar/ UAS diserahkan kepada **dosen kelas,** dilaporkan ke **PJMP.**
3. Baik praktikan maupun asisten tidak diperkenankan meminta atau memberikan **tugas tambahan** untuk perbaikan nilai.
4. Standar **indeks dan range nilai** ditentukan oleh dosen PJMP atas sepengetahuan Ketua Kelompok Keahlian

# Basic Network and Topology

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Menggunakan tracert dan NeoTrace untuk menelusuri rute jaringan dari PC ke Remote Server
2. Merancang topologi jaringan skala kecil peer-to-peer dan jaringan berbasis switch menggunakan Packet Tracer dasar.

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software tracert, NeoTrace, dan Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Route

Route Tracing Computer Software merupakan sebuah utilitas yang dapat menampilkan arus data jaringan dari komputer pengguna asal menuju perangkat komputer tujuan yang terletak di jaringan lain.

Adapun syntax yang biasa digunakan biasanyaseperti ini:

**traceroute** <destination network name or end device address>

(Unix and similiar systems)

or

**tracert** <destination network name or end device address>

(MS Windows systems)

Dua perintah tersebut diatas biasanya digunakan untuk network troubleshooting. Pengguna dapat mengidentifikasi jalur yang dilintasi untuk mencapai perangkat tujuan tertentu dalam sebuah jaringan ataupun antar jaringan yang berbeda. Setiap router merupakan sebuah titik dimana sebuah network terhubung ke network yang lain dan sebuah paket diteruskan (*forwarded*) ke router lain atau perangkat tujuan. Jumlah dari keseluruhan router disebut dengan jumlah “**hop**” yang dilintasi data dari sumber ke tujuan. Daftar jumlah hop ini dapat digunakan untuk mengidentifikasi masalah alir data ketika seorang user mencoba untuk mengakses sebuah layanan seperti website. Selain itu, juga dapat digunakan ketika seseorang mengunduh data. Ketika ada sejumlah website (mirrors) yang menyediakan file yang sama untuk diunduh, kita dapat melakukan terceroute setiap mirror tersebut untuk menentukan website mana yang menyediakan data lebih cepat.

#### Skenario

Anda akan menggunakan dua routing tracing software untuk menganalisa jalut Internet dari sumber ke tujuan. Aktifitas ini harus dilakukan dengan sebuah komputer yang terhubung ke Internet juga menyediakan akses ke command line. Pertama, anda akan menggunakan tracert berbasis windows. Selanjutnya akan menggunakan tool NeoTrace. Praktikum ini mengasumsikan bahwa NeoTrace sudah terinstall. Jika komputer yang anda gunakan belum mempunyai NeoTrace, silahkan unduh disini:

http://www.softpedia.com/get/Network-Tools/Traceroute-Whois-Tools/McAfee-NeoTrace-

Professional.shtml

Task 1: Trace Route to Remote Server

* + - 1. Buka command prompt, ketik tracert [www.cisco.com](http://www.cisco.com)

Output baris pertama menunjukkan Fully Qualified Domain Name (FQDN) yangdiikuti dengan IP address.

Domain Name Service (DNS) Server dari kampus harus dapat me-resolve (menerjemahkan) nama domain ke IP address. Tanpa name resolution ini, perintah tracert akan gagal. Karena tool ini berjalan di atas TCP/IP layer yang hanya memahami IP address.

Jika DNS tidak tersedia, Ip address dari perangkat atau komputer tujuan harus dimasukkan setelah perintah tracert.

* + - 1. Pelajari output yang ditampilkan

Berapa banyak hop antara perangkat sumber dan perangkat tujuan?\_\_\_\_\_\_\_\_\_\_\_

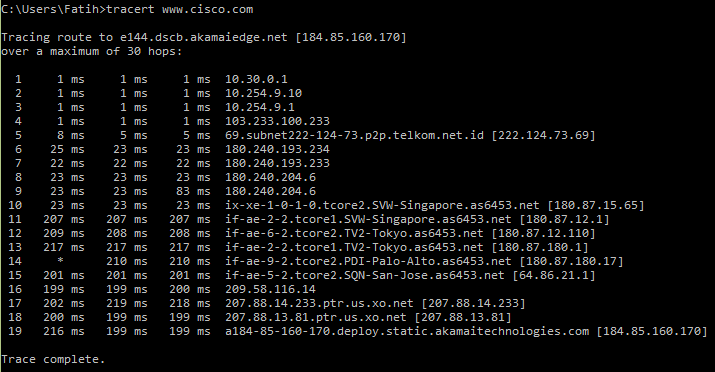


Figure 1. Perintah tracert

Figure1 menampilkan hasil tracert dari lokasi Indonesia. Baris pertama menunjukkan FQDN dan IP address,sehingga dapat disimpulkan bahwa DNS server mampu me-resolve nama ke Ip address.

* + - 1. Coba lakukan tracert ke alamat lain, tentukan:

Jumlah hop\_\_\_\_\_\_\_\_

FQDN\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

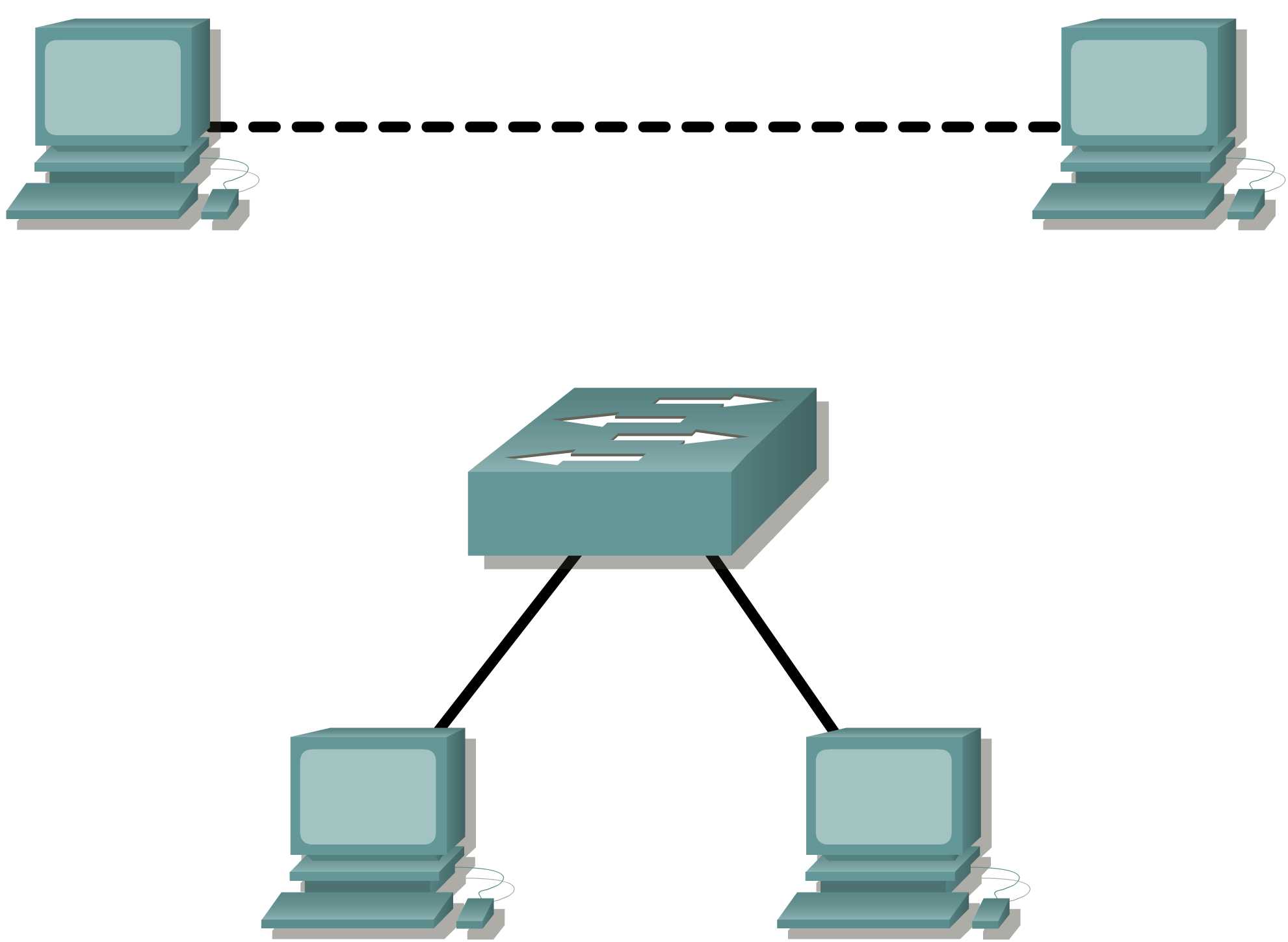
IP address \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Task 2: Trace Route using NeoTrace

* + - 1. Buka program NeoTrace
      2. Pada menu **View**, pilih **Options**. Klik tab **Map** pada bagian **Home Location** lalu klik tombol **Set Home Location**.
      3. Ikuti instruksi untuk memilih negara dan lokasi anda. Alternatif lain, klik tombol **Advanced**, untuk memasukkan posisi lattitude dan longitude dari lokasi anda.
      4. Ketik [www.cisco.com](http://www.cisco.com) pada field **Target** lalu klik **Go**.
      5. Dari menu **View**, **List View** akan menampilkan daftar router seperti halnya perintah tracert.
      6. Dari menu **View**, **Node View** akan menampilkan koneksi secara grafis dengan simbol.
      7. Darimenu **View**, **Map View** akanmenampilkan Link dan router berdasarkan lokasi geografis pada peta dunia.
      8. Pilih setiap view dari nomor 5 – 7 dan catat persamaan dan perbedaannya.
      9. Coba lakukanhal yang sama pada URL atau nama web berbeda dan analisa hasilnya.

### Topology Orientation and Building a Small Network

Diagram Topologi

******

Beberapa masalah jaringan biasanya dapat diselesaikan padalayer Fisik (Physical Layer) dari sebuah jaringan. Berdasarkan itu, sangat penting bagi kita untuk memahami kabel apa yang akan kita gunakan pada jaringan.

#### Scenario

Praktikum ini dimulai dengan bentuk jaringan paling sederhana (peer-to-peer) dan diakhiri dengan jaringanberbasis switch.

**Task 1: Create a Peer-to-Peer Network**

Step 1: pilih partner

Step 2: Siapkan peralatan meliputi:

2 PC/Workstation

2 kabel straigth through

2 kabel crossover

1 switch atau Hub

Task 2: Identify the Cables usedin a Network

Gunakan kabel **Crossover** untuk menghubungkan secara langsung antar PC/workstation melalui Network Interface Card (NIC) / kartu jaringan masing-masing, Jika anda perhatikan setiap ujung kabel di RJ45, kabel warna orange dan hijau berada pada posisi yang berbeda disetiap ujungnya.

Gunakan kabel **Straight Through** untuk menghubungkan PC ke Switch atau Router ke Switch. Jika anda perhatikan pada setiap ujung kabel, semua warna kabel berada pada posisi yang sama.

Task 3: Cable the Peer-toPeer Network

Step 1: Hubungkan kedua PC

Kabelapa yang anda gunakan? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 2: Berikan alamat IP masing-masing PC

IP PC 1: 192.168.1.100

IP PC 2: 192.168.1.200

Step 3: Periksa konektifitas

Ketik perintah ping untuk memeriksa koneksi apakah PC 1 dapat menjangkau PC 2 dan sebaliknya. Dari PC 1 ketik ping 192.168.1.200. Dari PC2 ketik: ping 192.168.1.100

Apakah output dari perintah ping tersebut? Tuliskan!

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jika salah satu kabel dicabut, apakah output dariperintah ping? Tuliskan!

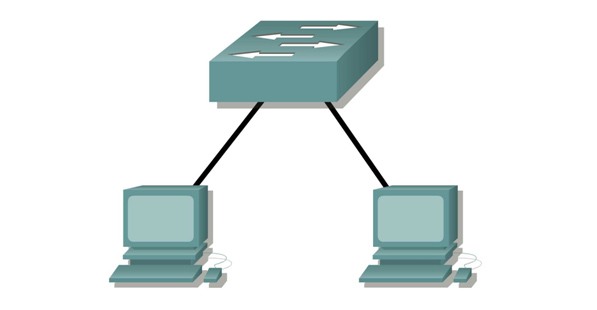
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Task 4: Connect Your Workstations to the Classroom Lab Switch



Step 1: Hubungkan kedua PC/workstation ke switch

Kabel apa yang andagunakan? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 2: Periksa konektifitas

Gunakan ping, apa output perintah ping jika saling terhubung? Tuliskan!

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Apa hasil perintah ping jika anda melakukan ping ke alamat yang tidak terhubung? Tuliskan!

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

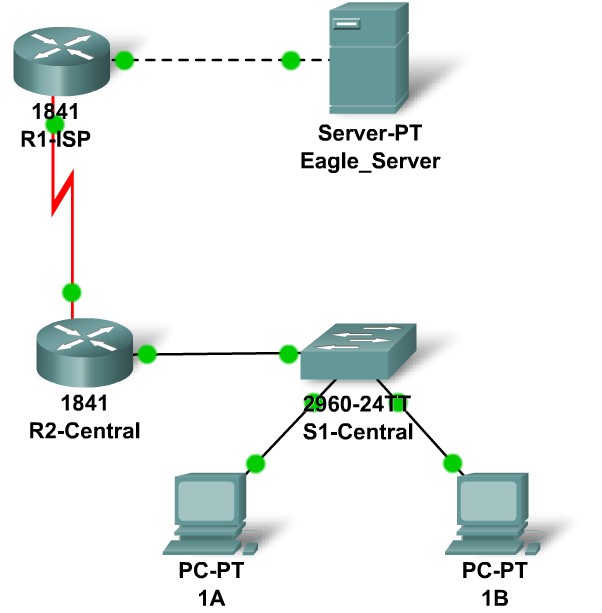
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Latihan

1. Buka Packet Tracer Activity Source Files: Nomor 1.7.1.3.pka

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task berikut:

**Task 1: Explore the PT (Packet Tracer) Interface**

Step 1: Perhatikan Logical Workplace

Step 2: Perhatikan Simbol Navigasi (menu/interface di bagian bawah)

**Task 2: Explore PT Operations**

Step 1: Hubungkan antar device menggunakan auto connect

* Hubungkan EagleServer ke R1-ISP router
* Hubungkan PCV-PT 1A ke S1-Central Switch

Step 2: Perhatikan konfigurasi device dengan mouse over.

Gerakkan mouse ke masing-masing device. Konfigurasi masing-masing device akan muncul secara pop-up. Lengkapi pernyataan di bawah ini sesuai dengan konfigurasinya:

* Router akan menampilkan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Server akan menampilkan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Switch akan menampilkan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* PC akan menampilkan: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Step 3: perhatikan konfigurasi devicedengan klik kanan:

* Router dan Switch terdiridari 3 Tab: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Server dan Hub terdiridari 2 tab: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* PC terdiri dari 3 tab: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Buka Packet Tracer Activity Source Files: Nomor 2.7.1.3.pka

Diagram Topologi dan Addressing Table sama dengan Nomor 1.7.1.3.pka (lihatgambar di atas)

Selesaikan Task berikut:

**Task 1: Complete the Topology**

Step 1: Tambahkan sebuah PC.

Konfigurasi IP address :

IP Address : 172.16.1.2

Subnet Mask: 255.255.0.0

Default Gateway: 172.16.255.254

DNS Server: 192.168.254.254

Display Name: 1B

Step 2: Hubungkan PC 1B ke port Fa0/2 S1-Central Switch. Periksa pekerjaan anda dengan klik tombol **Check Results**, untuk melihat topologi sudah selesai.

**Task 2: Add simple PDUs in Realtime Mode**

Gunakan tombol Add Simple PDU  untukmengirim pesan dari satu device ke device lain. Kirimkan pesan dari PC 1B ke Eagle Server.Periksa di even list kanan bawah apa yang terjadi (Successfull/Failed)

**Task 3: Analyze PDUs in Simulation Mode**

Beralih ke Simulation Mode. DoubleClick tombol “Fire” berwarna merah yang ada di even list. Akan muncul simulation panel. Gunakan tombol Capture/Forward untuk menggerakkan paket melalui jaringan. Klik pada amplop paket, atau kotak berwarna pada simulation panel, untuk memeriksa setiap langkah pada perjalanan paket.

Jelaskan apa yang anda lihat dari simulation mode:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |
|  |

# Application Layer Functionality and Protocols

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami mode lOSI danTCP/IP
2. Memahami Fungsi Layer Aplikasi dan Protokolnya
3. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Protocols

Networking protocols (protokol jaringan) menjelaskan fungsi-fungsi yang terjadi pada saat komunikasi jaringan berlangsung. Sebagai contoh, dalam pembicaraan empat mata antara dua orang, sebuah protokol komunikasi menyatakan bahwa untuk menandakan pembicaraan telah berakhir, salah seorang atau keduanya harus berdiam diri selama 2 detik penuh. Akan tetapi protokol tersebut tidak menentukan bagaimana caranya berdiam selama dua detik. Sebuah protokol secara umum tidak menjelaskan bagaimana menyelesaikan sebuah fungsi, namun hanya menjelaskan fungsi apa yang diperlukan untuk komunikasi tersebut.

Mari kita ambil web server sebagai contoh, HyperText Transfer Protocol (HTTP) tidak menentukan bahasa pemrograman apa yang harus digunakan untuk membuat sebuah aplikasi browser, sistem operasi apa yang harus digunakan, atau spesifikasi hardware seperti apa yang dibutuhkan untuk menampilkan browser.

Setiap device berbeda dapat berkomunikasi antara satu dengan lainnya menggunakan sekumpulan protokol yang sama. Hal ini dapat terjadi karena protokol hanya menentukan fungsionalitas jaringan, bukan teknologi yang dibutuhkan untuk mendukung fungsionalitas ini. Dengan demikian, komputer dan perangkat lainnya seperti telepon genggam, PDA,Tablet, dll, dapat mengakses halaman web yang tersimpan pada web server jenis apa saja yang menggunakan sistem operasi apa saja dan dari mana saja melalui Internet.

#### OSL Layer vs TCP/IP Model

Untuk menggambarkan interaksi antara beberapa protokol berbeda, sebuah layered model (model yang berlapis) biasa digunakan. Layered Model dapat menggambarkan operasi protokol yang terjadi pada setiap layer serta dapat menunjukkan interaksi dengan layer lainnya baik layer diatas atau dibawahnya.

Ada dua tipe model jaringan: protocol models dan referende Model. Protocol Models menyediakan sebuah model yang hampir mirip dengan struktur protokol tertentu. **TCP/IP model** merupakan contoh dari protocol model, karena model TCP/IP menjelaskan fungsi-fungsi yang terjadi di setiap layer protokol dalam ruang TCP/IP. Model TCP/IP terdiri dari empat layer yaitu application, transport, Internet, dan Network Access.

Model yang kedua adalah Reference Model. Model ini menyediakan referensi umum untuk menjaga konsistensi pada semua tipe protokol dan layanan jaringan. Model Referensi yang sangat dikenal adalah **Open System Interconnection (OSI) model**. Model tersebut digunakan untuk merancang jaringan data, spesifikasi operasi, dan troubleshooting. OSI terdiri dari tujuh layer yaitu: application, presentatation, session, transport, network, data link, dan physical.

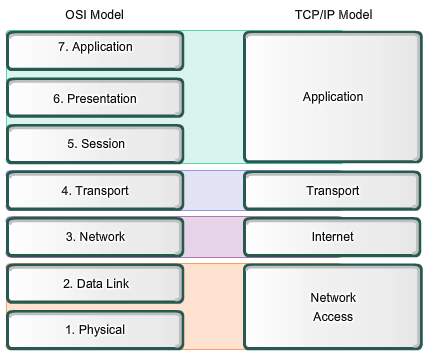
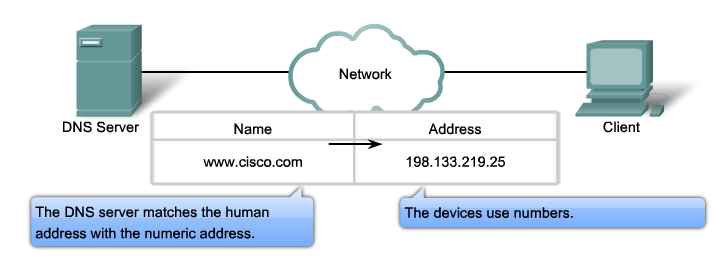


Figure 2.1 OSI Model vs TCP/IP Model

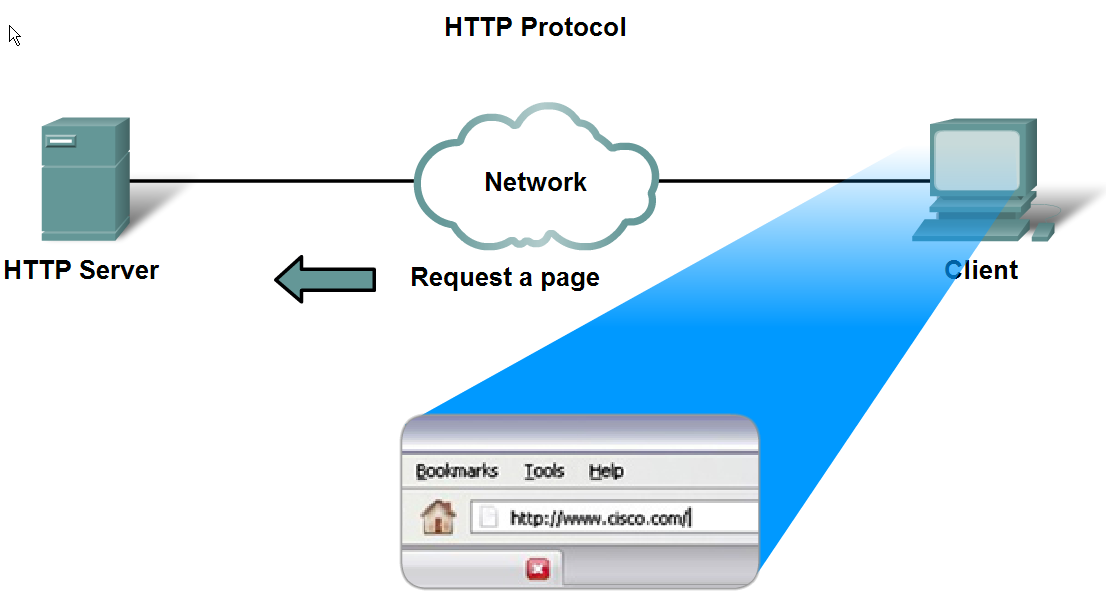
### Application Layer Functionality and Protocol

Application Layer adalah layer bagian teratas baik dalam model OSI maupun TCP/IP. Layer ini menyediakan antarmuka antara aplikasi yang kita gunakan untuk berkomunikasi dengan jaringan yang mengirimkan pesan kita. Protokol layer aplikasi (application layer protocol) digunakan untuk saling bertukar pesan antara program yang berjalan baik di host/komputer sumber maupun di host/komputer tujuan.Protokol tersebut menentukan format dan mengendalikan informasi yang dibutuhkan untuk komunikasi Internet. Beberapa protocol tersebut adalah:

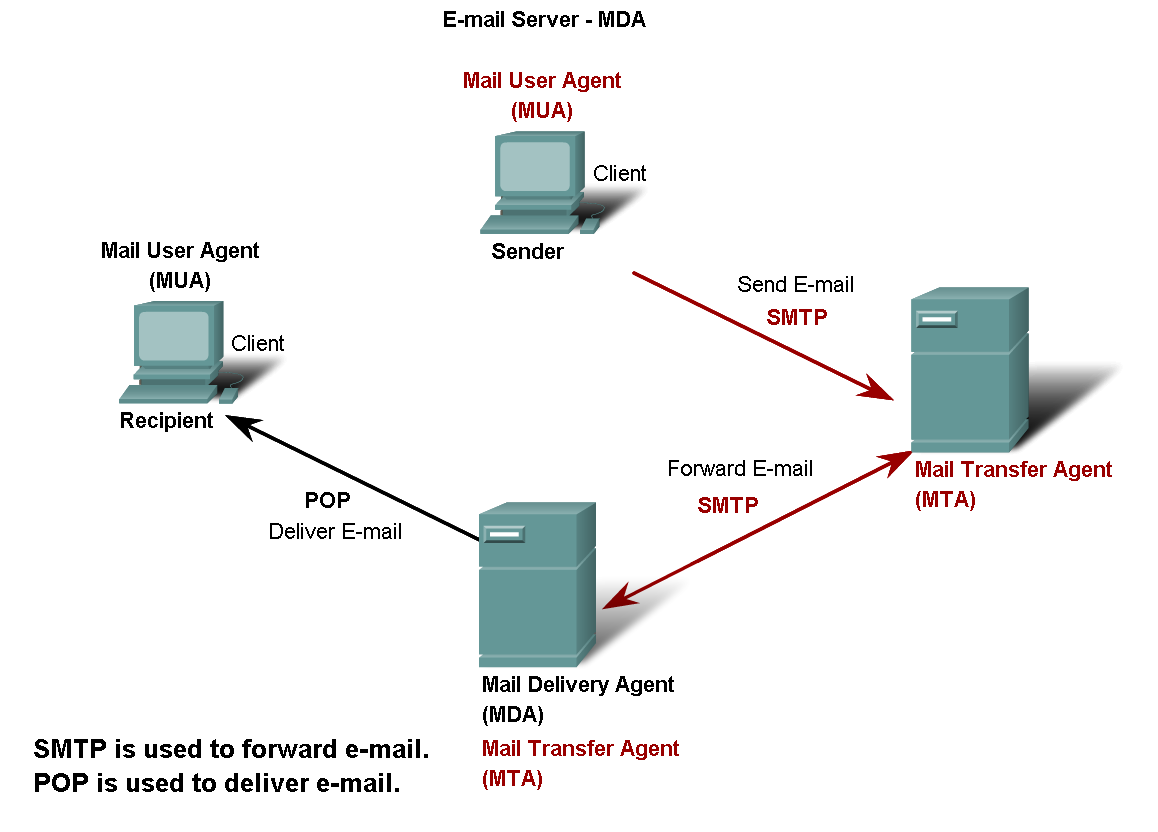
1. Domain Name Service Protocol (DNS) digunakan untuk menerjemahkan Internet name ke IP address.



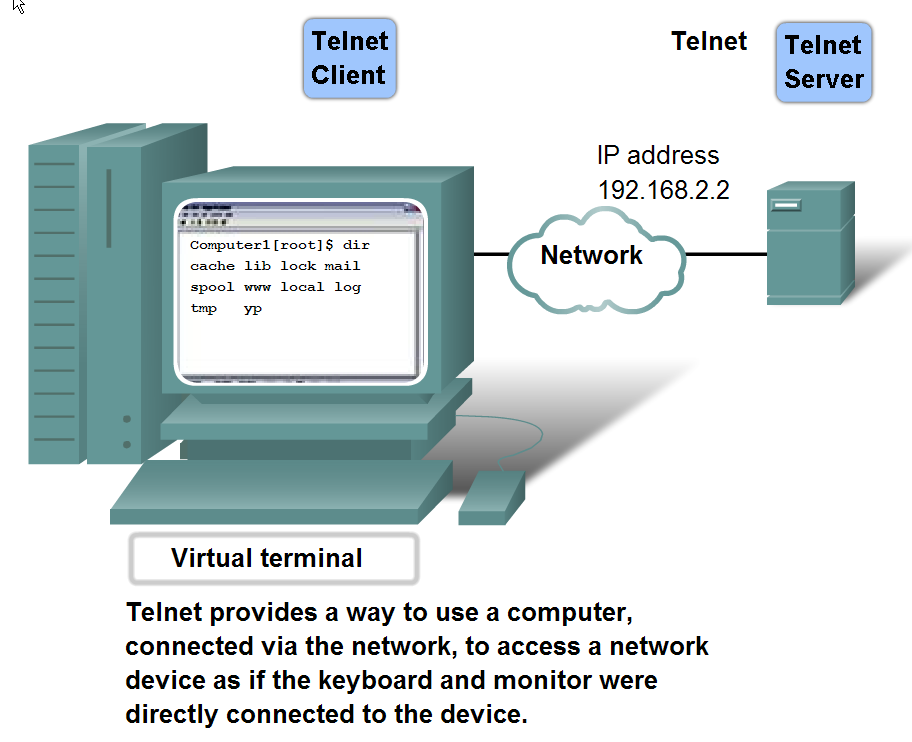
1. HyperText Transfer Protocol (HTTP) digunakan untuk mengirim file yang menghasilkan halaman web (web page)



1. Simple Mail Transfer Protocol (SMTP), digunakan untuk mengirim pesan surat dan lampirannya (attachment)



1. Telnet, digunakan untuk menyediakan aksesjarak jauh ke server atau perangkat jaringan lainnya.



1. File Transfer Protocol (FTP), digunakan untuk transfer file interaktif antar sistem.

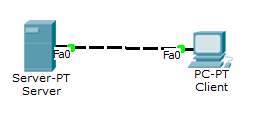
## Latihan

1. Network Representation

**Buka Packet Tracer Activity Source Files: Nomor 3.3.2.3.pka**

Dalam aktifitas ini, anda akan mengkonfigurasi sebuah Server untuk menyediakan layanan DNS (DNS services) dan layanan web page, mengkonfigurasi PC untuk menggunakan DNS service, dan melihat bagaimana DNS services dan HTTP bekerja bersama.

Diagram Topologi



Selesaikan Task berikut:

**Task 1: Configure services and support**

Step 1: Lakukan konfigurasi DNS pada Server

Klik gambar Server. Jendela konfigurasi server akan terbuka, klik tab **Config**. **Global Setting** akan tampil. Klik tombol sebelah kiri untuk **DNS**. Periksa service DNS dalam keadaan **On**. Berikan nama domain (**Domain Name**) pada kolom **Name** dengan [www.example.com](http://www.example.com) dan berikan IP address **192.168.1.254** pada kolom **address**. Lalu klik tombol **Add**. Tetap di tab **Config**. Lanjut ke step 2.

Step 2: Lakukan konfigurasi HTTP pada Server

Klik tombol **HTTP**. Aktifkan layanan HTTP dengan klik radio button **On**. Jendela Default Page Content berisi halaman yang akan tampil ketika web diakses. Halaman ini dibuat dalam format HTML. Anda boleh merubahnya sesuka anda. Lalu tutup jendela konfigurasi server.

Step 3: Lakukan konfigurasi DNS support pada PC Client

Klik gambar PC Client. Klik tab **Config**. Akan muncul jendela **Global Setting**. Pada field **DNS Server** masukkan IP address Server yaitu **192.168.1.254** . Lalu tutup jendela konfigurasi PC.

**Task 2: Verify Connectifity in Realtime Mode**

Step 1: Ping ke Server menggunakan URL

Klik PC Client lalu klik tab **Desktop**. Klik tombol **Command Prompt**. Ketik **ping** [**www.example.com**](http://www.example.com)lalu tekan **Enter**. Setelah ping sukses, tutup command prompt. Tetap di jendela konfigurasi PC

Step 2: Buka Web Page dari PC

Klik **Desktop**, lalu pilih tombol **Web Browser**. Sebuah simulasi dari web browser akan terbuka. Ketik [www.example.com](http://www.example.com) pada box **URL** lalu klik **Go**. Sebuah halaman webakan muncul. Tutup jendela konfigurasi client.

Task 3: View how DNS and HTTP work Together using Simulation Mode

Step 1: dari PC, ping Server menggunakan URL

Masuk ke Simulation Mode. Klik **PC Client🡪 Desktop🡪Command Prompt**, lalu ketik **ping** [**www.example.com**](http://www.example.com) dan **Enter**. Minimize Command Prompt. Gunakan tombol **Capture/Forward** untuk melihat DNS dan paket ICMP pada jaringan. Setiapkali anda klik tombol **Capture/Forward**, proses transferpaket akan berjalan. Selama proses tersebut, anda dapat klik kotak berwarna pada kolom I**nfo** untuk membuka informasi PDU dan melihat detail enkapsulasi dan pemrosesan perangkat. Tutup **Command Prompt**, lalu klik tombol **Reset Simulation**. Masih di jendela konfigurasi PC🡪 Desktop.

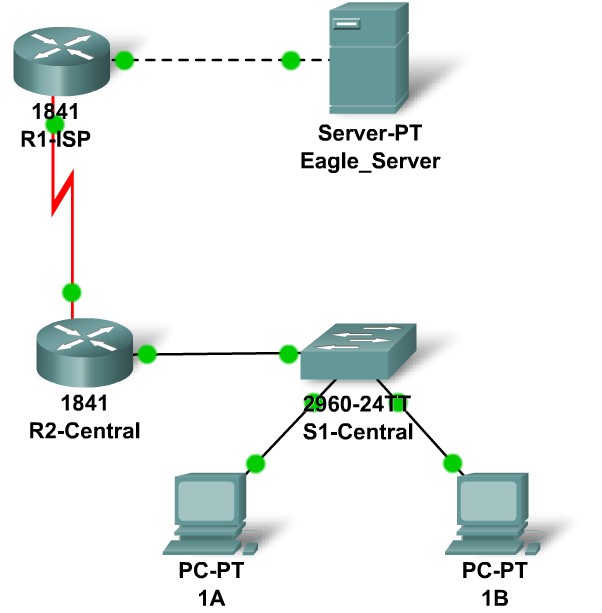
Step 2: dari PC, buka web page menggunakan URL

Klik tombol **Web Browser**, ketik [www.example.com](http://www.example.com) dan **Go**. Minimize browser. Gunakan **Capture/Forward** untuk memeriksa paket DNS dan HTTP.Sama seperti sebelumnya, klik kotak berwarna di kolom Info untuk melihat informasi PDU, detail enkapsulasi dan pemrosesan perangkat.

1. Configuring Hosts and Services

**Buka Packet Tracer Activity Source Files: Nomor 3.5.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: “Repair”and Test the Topology.**

Tambahkan sebuah PC dengan nama 1B ke dalam topologi. Lalu konfigurasi sebagai berikut:

IP Address: 172.16.1.2

Subnet Mask: 255.255.0.0

DefaultGateway: 172.16.255.254

DNS Server: 192.168.254.254

Hubungkan PC 1B ke port Fa0/2 dari Switch S1-Central Switch

Hubungkan Eagle-Server ke port Fa0/0 router R1-ISP. Aktifkan layanan web services dari server dengan menyalakan **HTTP**. Aktifkan layanan **DNS** dan masukkan nama domain pada field **Name** eagle-server.example.com dan masukkan IP address Server pada kolom **Address** (Lihat addressing table).

Sampai disini, periksa pekerjaan anda dengan klik tombol Check Result dan tab Assesment Items. Lalu tes konektifitas dalam **realtime mode** dengan menggunakan **ADD SIMPLE PDU** untuk menguji konektiifitas antara PC 1B dengan Eagle Server.

Catatan: Ketika anda menambahkan **SIMPLE PDU**, akan muncul di **PDU List** Window sebagai Scenario 0. Kemungkinan ketika anda pertama kali melakukan ping dengan SIMPLE PDU, proses tersebut akan ditampilkan **Filed** atau gagal pada **Even List**. Hal ini dikarenakan adanya proses ARP yang akan dijelaskan pada bab lain. Cukup ulangi sekali lagi menambahkan simple PDU dan kali ini pasti akan berhasil / successfull.

**Task 2: Explore How DNS and HTTP Works Together**

Masuk ke **Simulation Mode**. Buka **Web Browse**r di **PC 1B**. Ketik **eagle-server.example.com**, lalu **Go**. Seperti biasa gunakan **Capture/Forward** lalu periksa informasi PDU dengan klik kotak berwarna di kolom **Info** dan seterusnya. Anda bisa melihat bagaimana DNS dan HTTP bekerja bersama.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |
|  |

# Transport Layer Functionality and Protocols

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Transport dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Transport Layer

Transport Layer menyediakan segmentasi data dan kendali yang diperlukan untuk mengumpulkan kembali bagian-bagian tersebut kedalam bentuk arus komunikasi yang berbeda. Tanggung jawab utama dari layer transport adalah sebagai berikut:

* Melacak komunikasi individual antara aplikasi yang berada di perangkat/host sumber dan tujuan.
* Melakukan segmentasi data dan mengelola setiap bagiannya.
* Mengumpulkan atau menyusun kembali segment data tersebut ke dalam bentuk data aplikasi.
* Mengidentifikasi aplikasi yang berbeda.

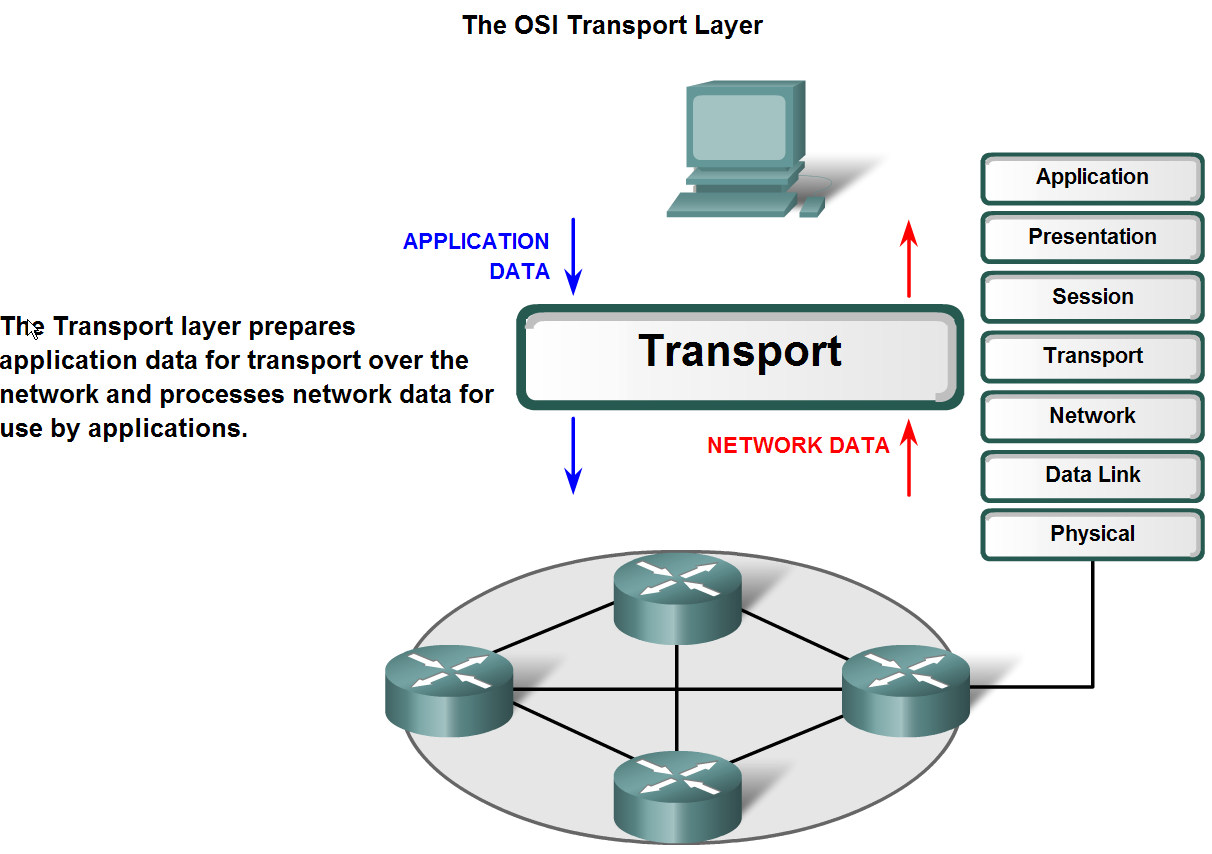


Figure 3.1 The OSI Transport Layer

Berdasarkan gambar 3.1 Transport Layer menyiapkan data aplikasi untuk diantarkan melalui jaringan dan juga memproses data jaringan untuk dapat digunakan oleh aplikasi.

### Transport Layer Protocols

Sebagaimana sudah dibahas sebelumnya bahwa fungsi utama dari transport layer adalah untuk mengelola data aplikasi supaya dapat berkomunikasi antar host/perangkat. Akan tetapi, aplikasi yang berbeda mempunyai kebutuhan data yang berbeda pula. Sehingga harus dikembangkan protokol transport yang berbeda untuk memenuhi kebutuhan tersebut.

Protokol Layer Transport dapat mengimplementasikan sebuah metode untuk memastikan pengiriman data yang dapat diandalkan (reliable delivery). Dalam terminologi jaringan, reliability berarti memastikan bahwa setiap bagian data yang dikirimkan oleh sumber pengirim sampai ke tujuan. Pada layer transport ada tiga operasi dasar reliabilty yaitu:

* Melacak data yang terkirim
* Mengakui (acknowledge) data yang diterima
* Mengirim ulang setiap data yang belum diakui (unacknowledged data)

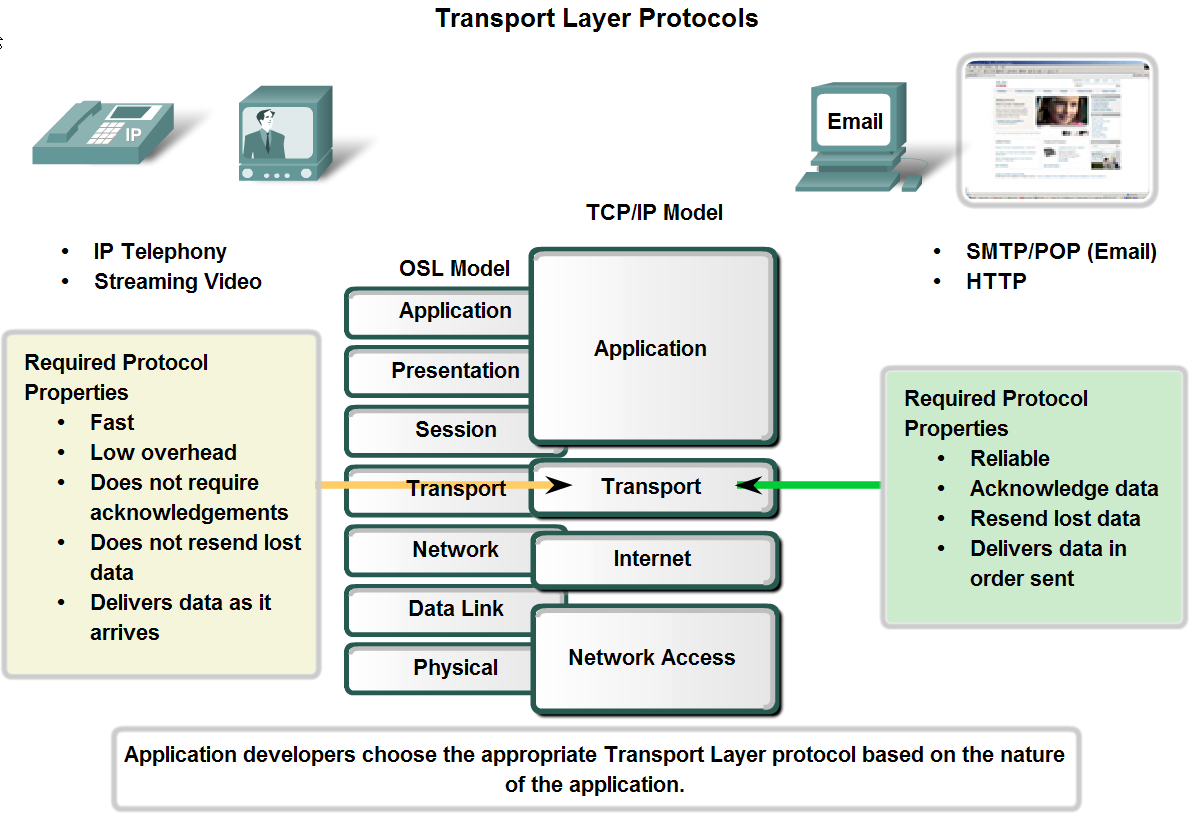


Figure 3.2 Persyaratan Protokol Layer Transport

#### TCP dan UDP

Prtokol Layer Transport yang umum digunakan adalah **Transmission Control Protocol** (TCP) dan **User Datagram Protocol** (UDP). Kedua protokol tersebut mengelola komunikasi dari beberapa aplikasi. Perbedaan antara keduanya adalah fungsi spesifik yang diimplementasikan dari masing-masing protokol.

**UDP**, dijelaskan dalam RFC 768, merupakan protokol yang sederhana dan **connectionless**. UDP memiliki kelebihan dalam menyediakan biaya pengiriman data yang rendah (low overhead data delivery). Bagian-bagian komunikasi dalam UDP disebut sebagai datagram.Aplikasi yang menggunakan UDP diantaranya:

* Domain Name System (DNS)
* Video Streaming
* Voice over IP (VoIP)

**TCP**, kebalikan dari UDP, merupakan sebuah **connection-oriented protocol** yang dijelaskan dalam RFC 793. TCP menimbulkan biaya tambahan pengiriman data untuk menjalankan fungsinya. Fungsi tambahan yang ditentukan oleh TCP adalah pengiriman sesuai urutan (same order delivery), pengiriman yang dapat diandalkan (reliable delivery), dan pengaturan arus (flow control). Setiap segmen TCP memiliki 20 bytes overhead pada header untuk mengenkapsulasi data di Layer Aplikasi, sedangkan segmen UDP hanya memiliki 8 bytes overhead (lihat gambar 3.3). Aplikasi yang menggunakan TCP adalah:

* Web Browsers
* Email
* File Transfers

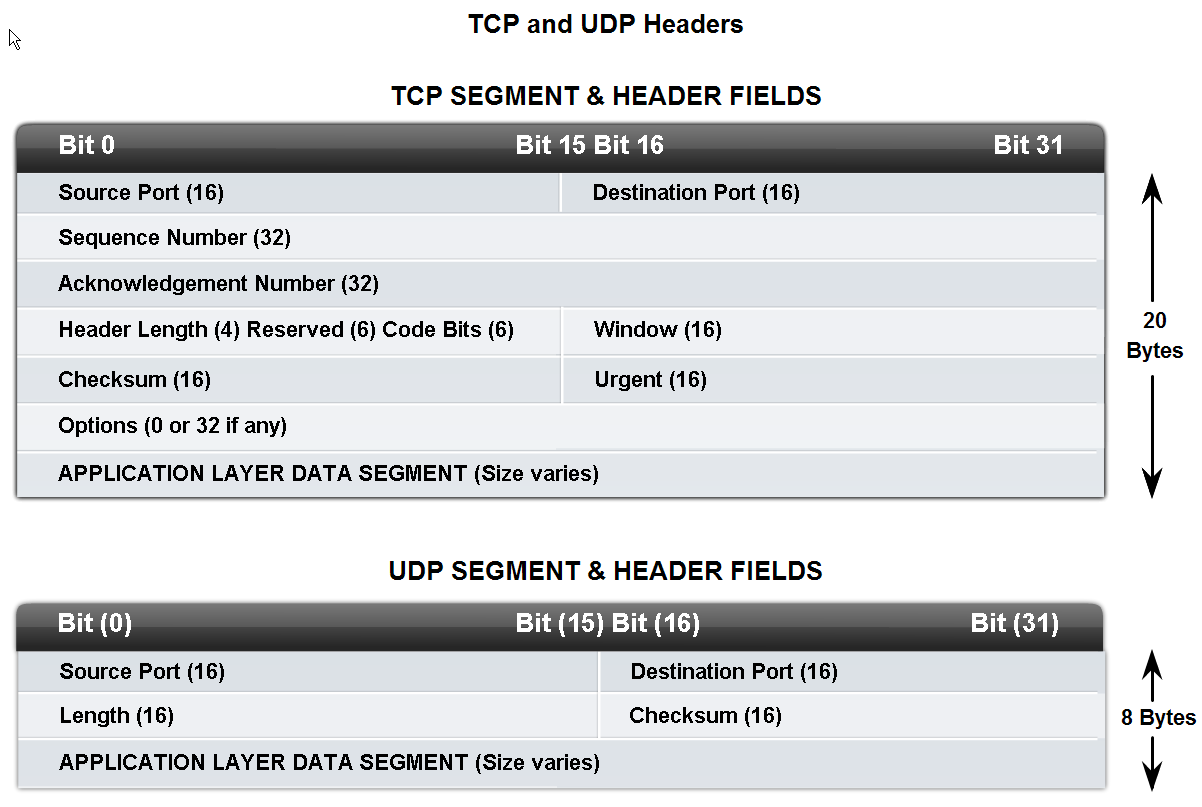


Figure 3.3 TCP dan UDP Header

#### Port Addressing

Perhatikan gambar 3.4 di bawah tentang sebuah komputer yang secara simultan menerima dan mengirim email, instant messages, web pages, dan telepon VoIP. Untuk membedakan segmen dan datagram setiap aplikasi, TCP dan UDP memiliki kolom header yang dapat mengidentifikasi aplikasi secara unik. Identitas unik ini disebut dengan **Port Number**.

Pada header setiap segmen atau datagram ada source port dan destination port. Source port number adalah nomor port untuk komunikasi dari aplikasi pada komputer sumber atau local host. Sedangkan destination port number merupakan nomor port untuk komunikasi dari aplikasi komputer tujuan atau remote host. Sebagai contoh, ketika sebuah aplikasi web browser mengirim permintaan ke web server, browser menggunakan TCP dan port 80.

Kombinasi dari port number dan IP address dari sebuah host dapat mengidentifikasi secara unik proses tertentu yang sedang berjalan pada host tertentu. Kombinasi ini disebut dengan **socket**. Sebagai contoh, sebuah HTTP request yang dikirimkan ke sebuah web server (port 80) yang berjalan pada sebuah host dengan IP address 192.168.1.20, maka request ini akan ditujukan ke socket 192.168.1.20:80.

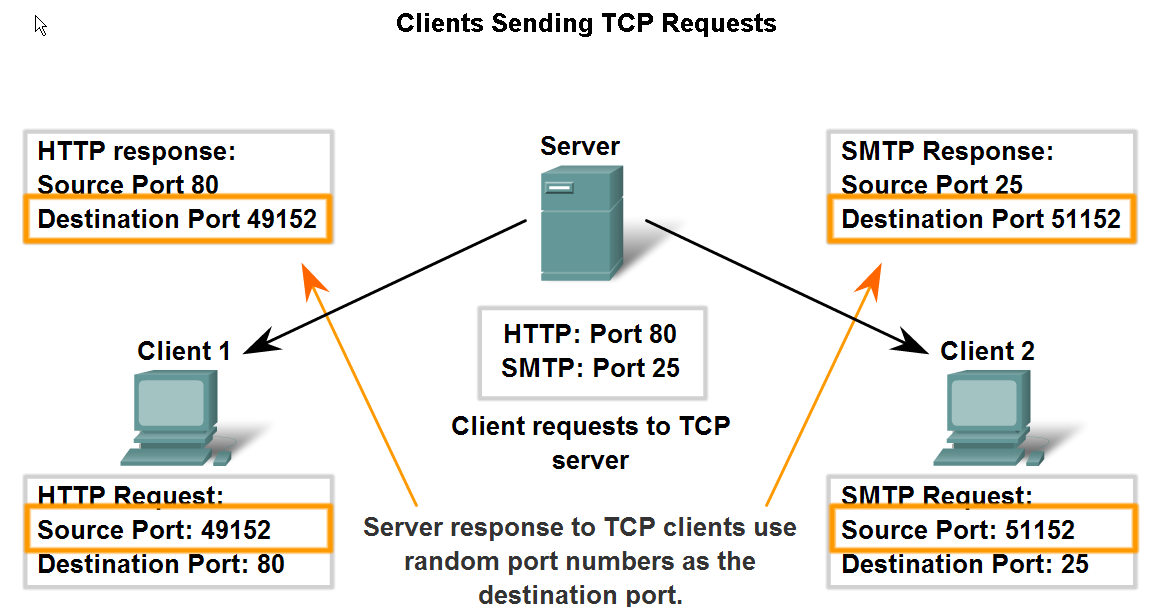


Figure 3.4 Port Adressing

### TCP Connection Establishment and Termination

Ketika ada dua host saling berkomunikasi menggunakan TCP, maka sebuah koneksi harus dibuat sebelum data dapat dipertukarkan. Setelah komunikasi selesai, sesi ditutup dan koneksi dihentikan. Untuk membuat sebuah koneksi, host melakukan three-way-handshake seperti terlihat pada gambar berikut.

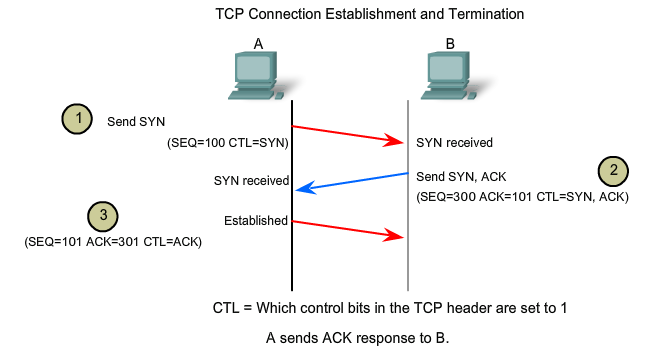


Figure 3.5. TCP Connection Establishment

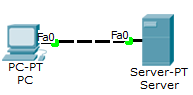
## Latihan

1. TCP Session Establishment and Termination

**Buka Packet Tracer Activity Source Files: Nomor 4.2.5.2.pka**

Aktifitas ini akan fokus pada pembuatan koneksi (conncetion establishment) sebelum pertukaran data dan penghentian sesi setelah pertukaran selesai.

Diagram Topologi



Selesaikan Task berikut:

**Task 1: Setup and run the simulation**

Step 1: Masuk ke simulation mode

Step 2: Set EventList Filters

Kita hanya akan meng-capture TCP events. Pada bagian **Event List Filter**, klik tombol **Edit Filters**. Pilih hanya TCP events. TCP events termasuk di dalamnya TCP based application protocols seperti HTTP dan Telnet.

Step 3: Request a web page dari PC

Masuk ke web browser PC kemudian ketik alamat **192.168.1.2** dalam URL box dan **Go**. Laluminimize browser.

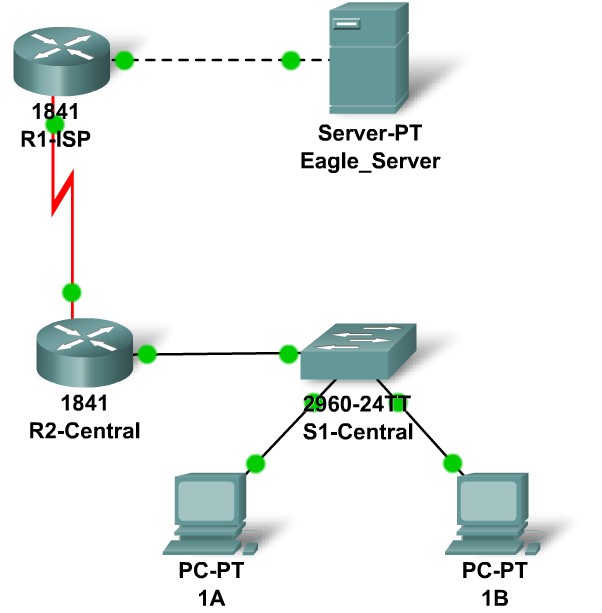
Step 4: Jalankan simulasi

Klik tombol Auto Capture/Play. Pertukatran data antara PC dan Server ditampilkan dalam bentuk animasi dan event yang terjadi ditambahkan dalam event list. Tunggu hingga animasi selesai. Lalu seperti biasa, klik kotak berwarna pada kolom Infodi Even List. Lalu analisa satu persatu informasi dari mulai PC melakukan request hingga sesi dihentikan (session terminated).

1. Analyzing the Application and Transport Layer

**Buka Packet Tracer Activity Source Files: Nomor 4.6.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: “Repair”and Test the Topology.**

Server baru mengalami penggantian sehingga harus dinyalakan.Setelah itu konfigurasi sebagai berikut:

IP Address: 192.168.254.254

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.254.253

DNS Enabled

Domain name: eagle-server.example.com

DNS address: 192.168.254.254

HTTP Enabled

Hubungkan Eagle-Server ke port Fa0/0 router R1-ISPmenggunakan kabel Crossover.

PC 1A kehilangan informasi IP addressnya. Lakukan konfigurasi untuk PC 1A sebagai berikut:

IP Address:172.16.1.1

Subnet Mask: 255.255.0.0

Default Gateway: 172.16.255.254

DNS Server: 192.168.254.254

Hubungkan PC 1A ke port Fa0/1 S1-Central Switch menggunakan kabel straight-through.

Periksa pekerjaan anda dengan menekan tombol Check Result dan tab Assessment Items. Tes konektifitas dengan ADD SIMPLE PDU untuk mengujikoneksiantara PC 1A dengan Eagle-Server.

Catatan: Ketika anda menambahkan **SIMPLE PDU**, akan muncul di **PDU List** Window sebagai Scenario 0. Kemungkinan ketika anda pertama kali melakukan ping dengan SIMPLE PDU, proses tersebut akan ditampilkan **Filed** atau gagal pada **Even List**. Hal ini dikarenakan adanya proses ARP yang akan dijelaskan pada bab lain. Cukup ulangi sekali lagi menambahkan simple PDU dan kali ini pasti akan berhasil / successfull.

**Task 2: Explore How DNS, UDP, HTTP, and TCP Works Together**

Masuk ke **Simulation Mode**. Set Event Filter untukmenampilkan DNS,UDP,HTTP, TCP,dan ICMP.

Buka **Web Browse**r di **PC 1A**. Ketik **eagle-server.example.com**, lalu **Go**. Seperti biasa gunakan **Capture/Forward** lalu periksa informasi PDU dengan klik kotak berwarna di kolom **Info** dan seterusnya. Anda bisa melihat bagaimana DNS, UDP, HTTP, dan TCP bekerja bersama.

1. Observing TCP and UDP using Netstat

Untuk aktifitas ini, gunakan command prompt pada sistem operasi windows komputer anda.

Task 1: Explain common netstat command parameters and outputs

Buka command prompt, ketik:

**C:\> netstat /? <ENTER>**

Gunakan output netstat /? Untuk mengisi tabel berikut sesuai dengan deskripsinya

|  |  |
| --- | --- |
| **Option** | **Description** |
|  | Display all connections and listening ports. |
|  | Display addresses and port numbers in numerical form. |
|  | Redisplay statistics every five seconds. Press CTRL+C to stop redisplaying statistics. |
|  | Shows connections for the protocol specified by proto; proto may be any of: TCP, UDP, TCPv6, or UDPv6. If used with the –s option to display per-protocol statistics, proto may be any of:  IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6. |
|  | Redisplay all connections and listening ports every 30 seconds. |
|  | Display only open connections. This is a tricky problem. |

Ketika statistik netstat menampilkan TCP Connection, status TCP juga ditampilkan. Saat terjadi TCP Connection, koneksi tersebut melalui beberapa seri status. Tabel berikut merangkum status TCP.

|  |  |
| --- | --- |
| **State** | **Connection Description** |
| LISTEN | The local connection is waiting for a connection request from any remote device. |
| ESTABLISHED | The connection is open, and data may be exchanged through the connection. This is the normal state for the data transfer phase of the connection. |
| TIME-WAIT | The local connection is waiting a default period of time after sending a connection termination request before closing the connection. This is a normal condition, and will normally last between 30 - 120 seconds. |
| CLOSE-WAIT | The connection is closed, but is waiting for a termination request from the local user. |
| SYN-SENT | The local connection is waiting for a response after sending a connection request. The connection should transition quickly through this state. |
| SYN\_RECEIVED | The local connection is waiting for a confirming connection request acknowledgment. The connection should transition quickly through this state. Multiple connections in SYN\_RECEIVED state may indicate a TCP SYN attack. |

IP address yang ditampilkan nestat ada beberapa kategori:

|  |  |
| --- | --- |
| **IP Address** | **Description** |
| 127.0.0.1 | This address refers to the local host, or this computer. |
| 0.0.0.0 | A global address, meaning “ANY”. |
| Remote Address | The address of the remote device that has a connection with this computer. |

Task 2: Use netstat to Examine Protocol Information

Step 1: gunakan netstat untuk menampilkan koneksi yangsedang terjadi

**C:\> netstat -a <ENTER>**

Tuliskan tiga TCP dan tiga UDP Connection dari hasil perintah di atas.

|  |  |
| --- | --- |
| Connection | Proto Local Address Foreign Address State |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |
|  |  |
|  |

Coba perintah lain dan perhatikan hasilnya

**C:\> netstat -an 5 <ENTER>**

**C:\> netstat -n <ENTER>**

**C:\> netstat –p TCP <ENTER>**

**C:\> netstat –p UDP <ENTER>**

**C:\> netstat –r <ENTER>**

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |

# Network Layer Functionality and Protocols

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Network dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Layer

Network Layer menyediakan layanan untuk saling bertukar kepingan-kepingan data melalui jaringan diantara end devices/hosts (end-to-end transport). Untuk menyelesaikan end-to-end transport ini, network layer menggunakan 4 proses dasar berikut:

* Addressing
* Encapsulation
* Routing
* Decapsulation

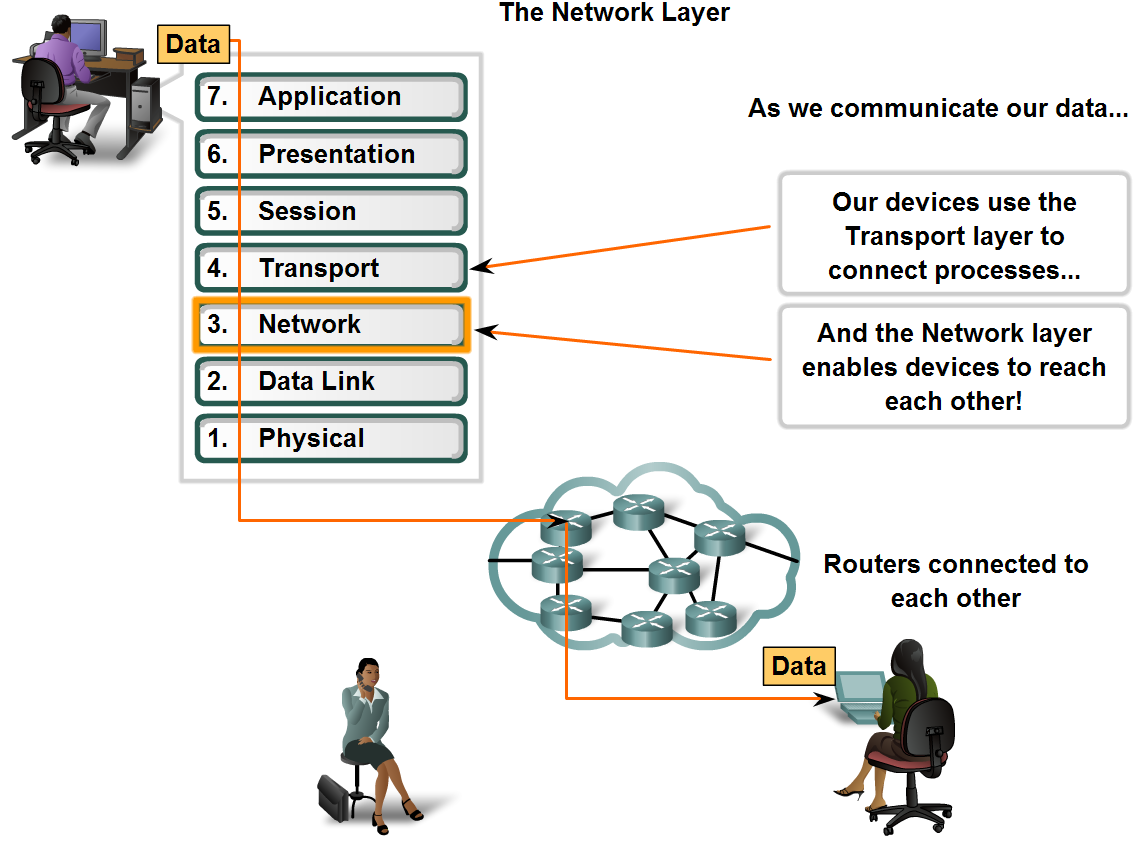


Figure 4.1 Network Layer

### Network Layer Protocols

Protokol-protokol pada Network Layer yang membawa data user adalah sebagai berikut:

* Internet Protocol version 4 (IPv4)
* Internet Protocol version 6 (IPv6)
* Novel Internetwork Packet Exchange (IPX)
* Apple Talk
* Connectionless Network Service (CLNS/DECNet)

### Separating Hosts into Common Group

Salah satu peran utama dari Network Layer adalah menyediakan mekanisme untuk pengalamatan (addressing) host. Ketika jumlah host dalam suatu jaringan semakin bertambah, perlu dilakukan perencanaan yang lebih baik dalam pengelolaan dan pengalamatan sebuah jaringan.

Pembagian jaringan ke dalam beberapa network tertentu adalah suatu hal yang lebih praktis dan mudah untuk dikelola daripada membuat semua host terhubung ke satu jaringan saja. Secara historis, sebuah jaringan yang berbasis IP memiliki asalnya adalah satu jaringan yang besar. Ketika jaringan ini bertambah besar tentunya akan menimbulkan permasalahan. Untuk menyelesaikan masalah ini, jaringan besar tersebut dapat dibagi menjadi beberapa jaringan kecil yang tetap saling terhubung. Jaringan-jaringankecil ini biasanya disebut dengan **subnetwork** atau **subnet**.

Sebuah jaringan besar dapat dibagi menjadi beberapa jaringan kecil dengan petimbangan beberapa faktor berikut:

* Geographic location (letak geografis)
* Purpose (tujuan)
* Ownership (kepemilikan)

#### Grouping hosts geographically

Kita dapat mengelompokkan hosts dari sebuah jaringan berdasarkan letak geofgrafis. Mengelompokkan host dalam lokasi yang sama seperti setiap gedung dalam sebuah kampus atau setiap lantai dalam gedung bertingkat ke dalam jaringan yang berbeda dapat meningkatkan operasional dan pengelolaan jaringan.

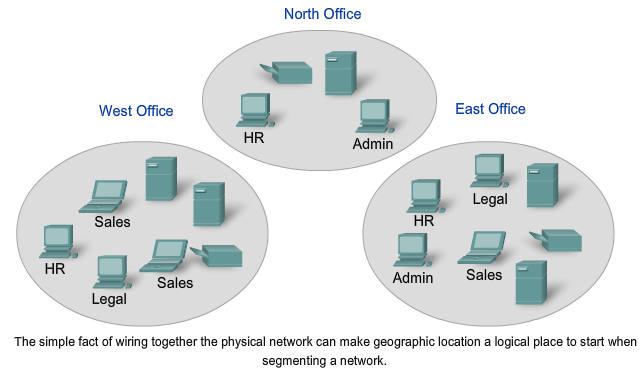


Figure 4.3 Grouping Hosts Geographically

#### Grouping hosts for specific purposes

Volume lalu lintas data dalam jaringan yang dihasilkan oleh beberapa aplikasi akan berbeda secara signifikan. Membagi jaringan berdasarkan penggunaan dapat meningkatkan efektifitas alokasi sumber daya jaringan serta pengelolaan hak aksesnya. Sebagai contoh, sebuah perusahaan mempekerjakan beberapa desainer grafis yang menggunakanjaringan untuk saling berbagi file multimedia yang berukuran sangat besar. File-file tersebut mengkonsumsi banyak bandwidth yang tersedia setiaphari. Selaiin desainer grafis, perusahaan juga mempekerjakan salesperson yang hanya login sehari sekali untuk merekam transaksi penjualan mereka. Kegiatan sales tersebut hanya menghasilkan lalu lintas jaringan yang sangat kecil.

Dalam skenario ini, untuk menghasilkan jaringan yang efektif dalam penggunaan sumberdaya jaringan, perlu dibuat beberapa jaringan kecil untuk memfasilitasi akses para desainer grafis dan sebuah jaringan yang lebih besar untuk diguakan oleh para salesperson.

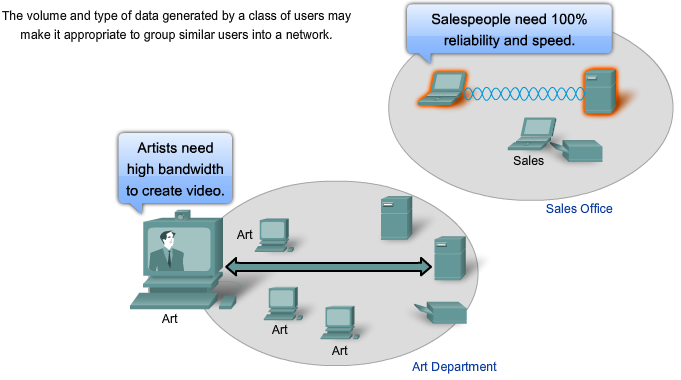


Figure 4.4 Grouping Hosts for specific purposes

#### Grouping hosts for ownership

Menggunakan basis organisasi (perusahaan, departemen, dll) untuk membuat sebuah jaringan akan membantu dalam mengendalikan akses terhadap perangkat dan data serta admnistrasi jaringan. Dalam satu jaringan yang besar akan lebih sulit untuk mendefinisikan dan membatasi tanggung jawab dari setiap personal yang terhubung dan memiliki akses ke jaringan. Dengan membagi host ke dalam beberapa jaringan akan membuat sebuah batasan untuk penerapan keamanan dan pengelolaan setiap jaringan.

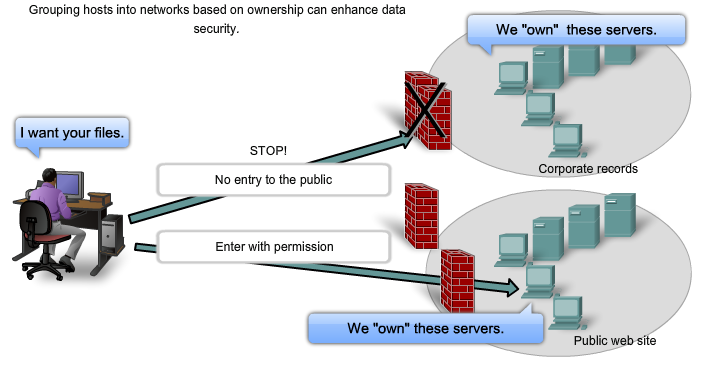


Figure 4.5. Grouping hosts for ownership

### A Gateway – The Way Out of Our Network

Gateway, atau lebih dikenal dengan default gateway, diperlukan untuk mengirim paket ke jaringan yang berada diluar jaringan lokal. Jika bagian jaringan (Network Portion) dari alamat paket yang dituju berbeda dengan jaringan pengirim, paket tersebut harus di-routing keluar dari jaringan asalnya. Untuk melakukan hal ini, paket tersebut dikirimkan ke gateway. Gateway ini biasanya merupakan sebuah port interface router yang terhubung ke jaringan lokal. Interface gateway tersebut memiliki amalat jaringan yang sama dengan alamat jaringan dari host yang terhubung ke router tersebut. Dengan demikian, host harus dikonfigurasi untuk mengenali alamat tersebut sebagai gateway.

Default gateway dikonfigurasi pada komputer/host. Pada komputer berbasis Windows, Properties dari Internet Protocol (TCP/IP) digunakan untuk memasukkan alamat IP default gateway. Baik IP address pada host maupun IP address gateway harus mempunyai porsi network (network portion) yang sama (dan subnet, jika digunakan) pada IP address mereka.

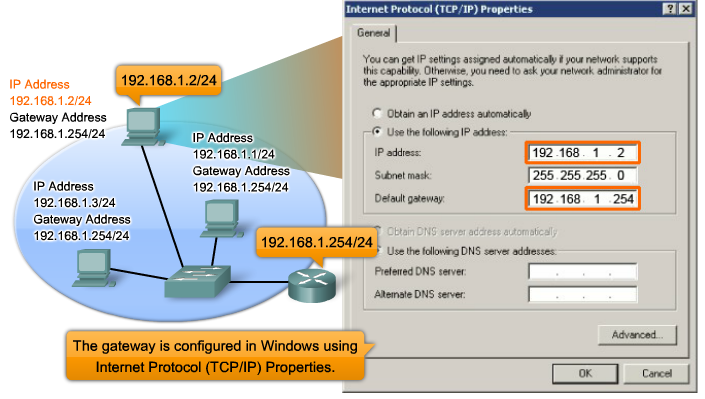


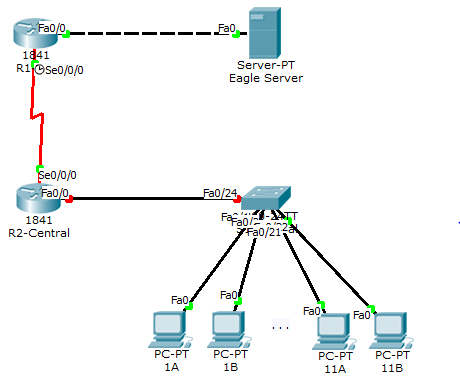
Figure 4.6 Default Gateway in Windows Properties

## Latihan

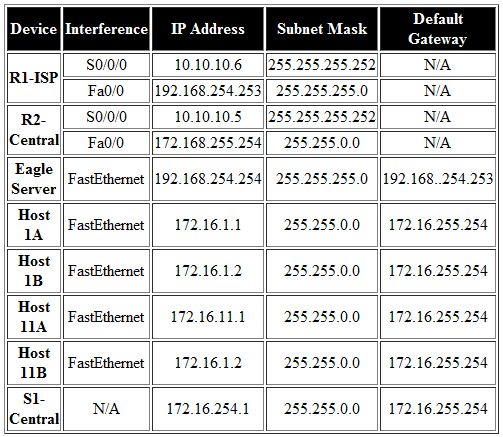
1. Examining a Device’s Gateway

**Buka Packet Tracer Activity Source Files: Nomor 5.5.1.2.pka**

Diagram Topology



Addressing Table



Selesaikan Task berikut:

**Task 1: Understand and Explain the Purpose of a Gateway Address**

Step 1: Masuk ke command prompt

Klik PC 1A, masuk ke comman prompt, ketik ipconfig

Step 2: ping ke IP Address 127.0.0.1

Periksa apakah ping berhasil?

Step 3: Kemudian ping ke IP address lain yang satu network dengan 127.0.0.1, misalkan 127.10.1.1 dan 127.255.255.255

Periksa apakah respon dari komputertujuan sukses?? Apabila tidak jelaskan mengapa?

Task 2: Understand how Network Information is Configured

Biasanya permasalahan konektifitas adalah karena kesalahan dari setting jaringan. Adabeberapa tools yang dapat digunakan untuk melakukan troubleshooting konektifitas.

Step 1: Periksa properties dari IP address jaringan

Klik PC🡪 Desktop🡪 IP Configuration

Atau bisa jugamenggunakan perintah **ipconfig**

Klik PC🡪 Desktop🡪Command Prompt

Lalu ketik **ipconfig** atau **ipconfig /all**

**Task 3: Troubleshoot a Hidden Gateway Address Problem**

**Skenario**

Sebagai seorang Cisco Engineer helpdesk, anda diminta untuk membantu teknisi help desk. Teknisi tersebut menerima trouble ticket dariseoranguser pada komputer host-1A yang komplain bahwa komputer host-11B yaitu **host-11B.example.com** tidak merespon ping. Teknisi tersebut lalu memeriksa kabel dan setting network pada kedua komputer tersebut, namun tidak ada masalah yang ditemukan. Kemudian Anda melakukan crosscek terhadap Network Engineer perusahaan yang melaporkan bahwa router R2-Central iuntuk sementara dimatikan karena ada proses upgrade hardware. Sekarang Anda sudah mengerti permasalahannya, kemudian Anda meminta kepada teknisi untuk melakukan ping ke IP address dari host-11B yaitu 172.16.11.2 dari host-1A. Ping direspon dengan sukses. Lalu Anda meminta teknisi untuk ping ke IP address Gateway yaitu 172.16.254.254, dan hasil dari ping gagal.

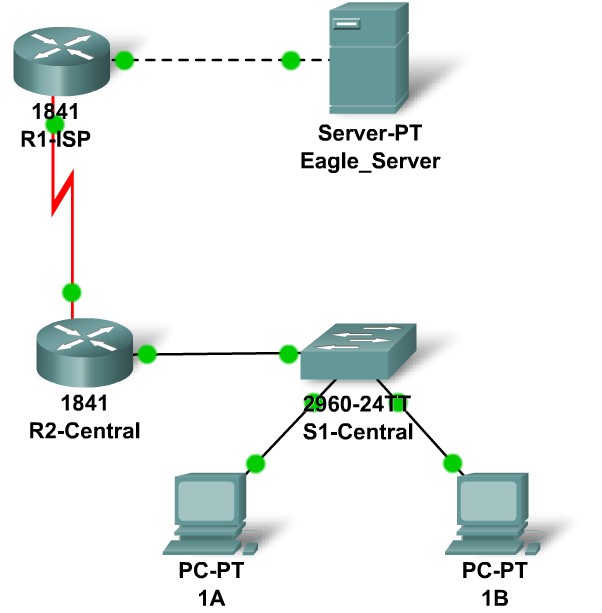
Tugas Anda adalah mencari dan memperbaiki masalah yang terjadipada jaringan Anda.

Jelaskan apa masalahnya, dan bagaimana cara memperbaikinya??

1. Routing IP Packet

**Buka Packet Tracer Activity Source Files: Nomor 4.6.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: Configure a Router Interface**

Ada beberapa masalah pada jaringan lokal: PC1A tidak bisa menjangkau Eagle Server (periksa dalam mode Realtime). Kelihatnnya masalah ada pada router. Lakukan mouse over pada router R2-Central, dan catat kondisi dari interface Fa0/0 (yang terhubung ke switch). Interface ini harus mempunyai IP address, subnet mask, dan dinyalakan supaya dapat digunakan sebagai default gateway untuk LAN.

Klik router R2-Central dan klik tab **Config**. Pada daftar yang ditampilkan, cari **INTERFACE**, **FastEthernet0/0**. Tambahkan IP address 172.16.255.254 dan subnet mask 255.255.0.0, lalu aktifkan port **On**. Tutup jendela router. Periksa interface router sekarang telah berjalan menggunakan mouse over. Cobalah sekarang untuk menjangkau Eagle Server. Akan tetapi request masih gagal. Jelaskan apa kira-kira masalahnya dan kenapa?

**Task 2: Examining Routes**

Gunakan **Inspect Tool** (magnifying glass) untuk memeriksa routing table dari router R2-Central. Anda dapat melihat jaringan yang langsung terhubung ke router, tapi tidak ada jalan untuk menjangkau jaringan Eagle Server.

**Task 3: Configure a Route Using a GUI**

Klik router R2-Central dan klik tab **Config**. Cari **ROUTING**, **Static**. Konfigurasi defaults tatic route menggunakan alamat 0.0.0.0, mask 0.0.0.0 dan hop selanjutnya (next hop) adalah 10.10.10.6 (interface S0/0/0 dari router R2-Central) dan klik tombol **Add**. Rute ini sudah dikonfigurasi bahwa kemanapun paket dari LAN 172.16.0.0/16 ditujukan, paket-paket tersebut akan pergi menuju ke router R1-ISP. Pada **GLOBAL**, **Setting**, klik tombol **Save** untuk menyimpan konfigurasi pada NVRAM. Gunakan **Inspect Tool** (magnfying glass)untuk memeriksa kembali routing table router R2-Central. Sekarang anda pasti akan melihat rute yangsudah anda konfigurasi pada routing table.

Periksa pekerjaan anda dengan klik tombol **Check Result** dan tab **Assessment Items**. Tes konekktifitas pada mode Realtime dengan menambahkan SIMPLE PDU antara PC 1A dengan Eagle Server. Seperti biasa, pingpertama akan gagal dan ulangi lagi sampai sukses.

**Task 4: Examine the Routing ofthe IP Packet**

Masuk ke Simulation mode. Menggunakan PDU yang sudah anda buatdi Task 3, telusuri perjalanan paket dari PC 1A ke Eagle Server, lalu gunakan **Capture/Forward** dan kotak berwarna pada kolom **Info**.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |

# Cabling

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

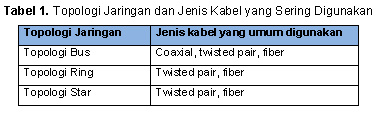
1. Mampu membuat susunan konfigurasi T568A dan T568B untuk kabel Usheild Twisted Pair (UTP)
2. Mampu memasang kabel UTP pada konektor Regitered Jack 45 (RJ-45)
3. Mampu membuat kabel UTP Straight-through dan Cross-over
4. Mampu memasang kabel UTP pada modular Jack

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC, Kabel UTP 5e, Crimp tool, konektor RJ-45, Cable tester

## Dasar Teori

Pemilihan jenis kabel sangat terkait erat dengan topologi jaringan yangdigunakan. Sebagai contoh untuk jenis topologi Ring umumnya menggunakan kabel Fiber Optik (walaupun ada juga yang menggunakan twisted pair). Topologi Bus banyak menggunakan kabel Coaxial. Kesulitan utama dari penggunaan kabel coaxial adalah sulit untuk mengukur apakah kabel coaxial yang dipergunakan benar-benar *matching* atau tidak. Karena kalau tidak sungguh-sungguh diukur secara benar akan merusak NIC (Network Interface Card) yang dipergunakan dan kinerja jaringan menjadi terhambat, tidak mencapai kemampuan maksimalnya. Topologi jaringan Star banyak menggunakan jenis kabel UTP. Topologi jaringan dan jenis kabel yang umum digunakan dapat dilihat pada tabel berikut:

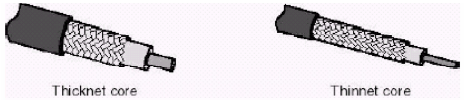


Setiap jenis kabel mempunyai kemampuan dan spesifikasi yang berbeda, oleh karena itu dibuatlah pengenalan tipe kabel. Ada tiga jenis kabel yang dikenal secara umum, yaitu:

* Kabel Coaxial
* Fiber Optic
* Kabel Twisted Pair

### Kabel Coaxial

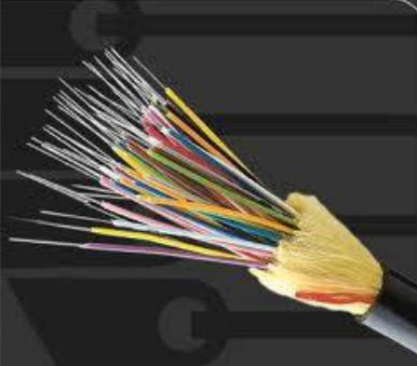
Kabel coaxial terdiri atas sebuah konduktor silindris luar mengelilingi sebuah wire didalamnya, yang terdiri atas 2 elemen utama. Elemen yang terletak di tengah, merupakan sebuah konduktor tembaga bagian ini dikelilingi oleh lapisan insulasi. Ada duajenis kabel coaxial yang dikenal,yaitu thick coaxial (mempunyai diameter besar) dan thin coaxial (mempunyai diameter kecil).



Gambar 5.1. Kabel Coaxial

### Kabel Fiber Optic

Kabel fiber optic merupakan sebuah media jaringan yang mampu melakukan transmisi cahaya yang dimodulasi. Jaringan yang menggunakan *Fiber Optic* (FO) biasanya perusahaan besar, dikarenakan harga dan proses pemasangannya lebih sulit. Namun demikian, jaringan yang menggunakan FO dari segi kehandalan dan kecepatan tidak diragukan. Kecepatan pengiriman data dengan media FO lebih dari 100 Mbps dan bebas pengaruh lingkungan.



Gambar 5.2. Kabel Fiber Optic

### Kabel Twisted Pair

Kabel *Twisted Pair* ini terbagi menjadi dua jenis yaitu shielded twisted pair (STP)

dan unshielded twisted pair (UTP). STP adalah jenis kabel yang memiliki selubung

pembungkus sedangkan UTP tidak mempunyai selubung pembungkus. Untuk

koneksinya kabel jenis ini menggunakan konektor RJ-11 atau RJ-45.

Pada twisted pair (10 BaseT) network, komputer disusun membentuk suatu pola

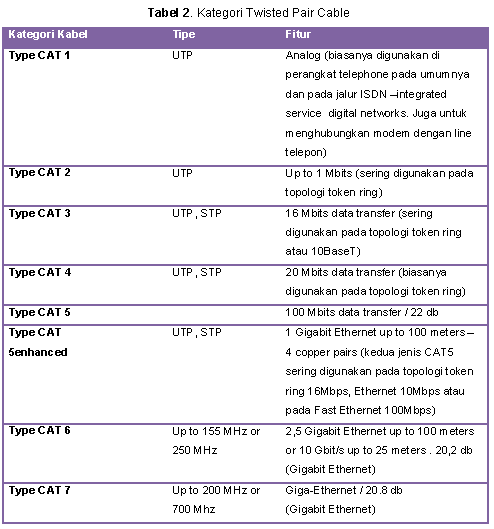
Star. Setiap PC memiliki satu kabel twisted pair yang tersentral pada HUB. Twisted pair

umumnya lebih handal (reliable) dibandingkan dengan thin coax, karena HUB

mempunyai kemampuan data error correction dan meningkatkan kecepatan transmisi.

Saat ini ada beberapa grade atau kategori dari kabel twisted pair. Kategory tersebut

dapat dilihat pada tabel dibawah :



Pemberian kategori 1/2/3/4/5/6 merupakan kategori spesifikasi untuk masingmasing

kabel tembaga dan juga untuk jack. Masing-masing merupakan seri revisi atas

kualitas kabel, kualitas pembungkusan kabel (isolator) dan juga untuk kualitas “belitan”

(twist) masing-masing pasang kabel. Selain itu juga untuk menentukan besaran

frekuensi yang bisa lewat pada sarana kabel tersebut, dan juga kualitas isolator

sehingga bisa mengurangi efek induksi antar kabel (noise bisa ditekan sedemikian

rupa). Perlu diperhatikan juga, spesifikasi antara CAT5 dan CAT5 enchanced

mempunyai standar industri yang sama, namun pada CAT5e sudah dilengkapi dengan

insulator untuk mengurangi efek induksi atau *electromagnetic interference.* Kabel

CAT5e bisa digunakan untuk menghubungkan network hingga kecepatan 1Gbps.

**UTP Cable (khususnya CAT5 / CAT5e)**

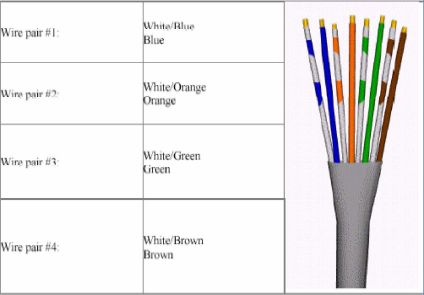
Kategori 5 atau 5e adalah yang paling reliable dan memiliki kompabilitas yang

tinggi, dan yang paling disarankan, baik pada 10 Mbps dan Fast Ethernet (100Mbps).

Konector yang bisa digunakan untuk UTP Cable CAT5 adalah RJ-45. Untuk

penggunaan koneksi komputer, dikenal 2 buah tipe penyambungan kabel UTP ini, yaitu

**straight cable** dan **crossover cable**.



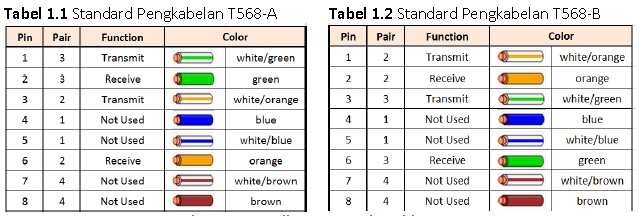
Gambar 5.3 Kabel UTP Cat 5

**Straight-Through**

Jenis kabel ini digunakan untuk menghubungkan antara workstation dengan hub/switch. Kabel ini juga memiliki 4 pairs (8 wire) dimana setiap pin antara ujung satu dengan ujung lainnya harus sama. Maksudnya, bila salah satu ujung memakai standard T568-A maka ujung satunya harus memakai T568-A juga. Begitu pula sebaliknya, jika salah satu ujung menggunakan standard T568-B, ujung satunya juga harus memakai standard yang sama.

**Crossover**

Merupakan jenis kabel yang digunakan untuk menghubungkan antar workstation atau antar hub/switch. Kabel jenis ini menggunakan standard T568-A pada salah satu ujung, dan T568-B pada ujung lainnya.



## Latihan

Praktikum memasang kabel UTP pada koektor RJ 45

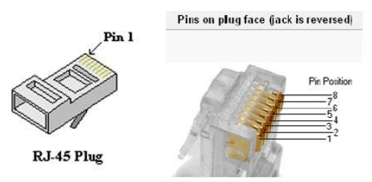
Perangkat yang digunakan adalah sebagai berikut:



Gambar 5.4. Perangkat untuk praktikum cabling

Ikuti langkah-langkah berikut:

1. Kupas ujung kulit kabel UTP secukupnya menggunakan pemotong pada Crimp Tool
2. Buka uliran setiap pasangan kabel dan luruskan
3. Susun kabel menjadi susunan yang diinginkan, lihat Tabel 1.1 untuk T568A dan Tabel 1.2 untuk T568B dengan urutan pin-1 diujung paling kiri
4. Jepit kabel yang sudah tersusun dengan ibu jari telunjuk agartetap merata dan terurut,kemudian ratakan ujung kabel dengan pemotong Crimp Tool
5. Jangan lepaskan jepitan ibu jari dan telunjuk pada kabel agar susunan tidak bergeser, kemudian masukkan ujung kabel pada konektor RJ-45 dengan posisi pin-1 sebagai berikut:



Gambar 5.5 RJ-45 pin

1. Pastikan setiap tembaga ujung kabel mencapai ujung konektor RJ-45
2. Gunakan Crimp Tool untukmenekan tembaga di ujung konektor RJ-45 agar kabel terpasang pada konektor dengan sempurna



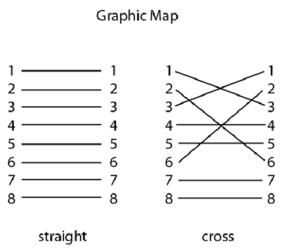
Gambar 5.6. Penggunaan Crimp Tool

1. Pasang konektor pada sisi kabel yang lain dengan cara yang sama
   1. Untuk kabel straigth-trough, kedua ujungkabel menggunakan susunan T568B
   2. Untuk kabel crossover,salah satu ujung kabel menggunakan susunan T568A dan ujung yang lain menggunakan T568B
2. Setelah konektor terpasang dengan baik, gunakan Cable Tester untuk memastikan kondisi konekktor terpasang dengan sempurna



Gambar 5.7. Cable Tester

1. Berikut hasil test untuk kabel straigth-through dan crossover



Gambar 5.8. Hasil Test straigth-through dan crossover

1. Untuk hasil yang maskimal dari gangguan luar (noise), pastikan seluruh kabel tertutup kulit kabel secara sempurna sampai bagian dalam konektor.



Gambar 5.9. Pemasangan Kabel

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy * http://www.scribd.com/doc/14370657/pengkabelan-UTP. (n.d.). Retrieved Maret wenesday, 2012, from www.scribd.com: http://www.scribd.com/doc/14370657/pengkabelan-UTP |

# IP Address

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Merancang Skema Pengalamatan IP untuk memenuhui kebutuhan desain jaringan
2. Mampu melakukan subnetting dengan CIDR
3. Mampu melakukan troubleshooting pada IP address dan Konfigurasi Host

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

IP address merupakan bilangan biner 32 bit yang dipisahkan oleh tanda pemisah berupa tanda titik setiap 8 bitnya. Tiap 8 bit ini disebut sebagai octet. Bentuk IP address adalah sebagai berikut

xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx

setiap symbol akan di gantikan oleh angka 0 dan 1, misalnya:

10000100 . 01011100 . 01111001 . 00000001 = 132.92.121.1

### Alamat Jaringan, Alamat Host, Alamat Broadcast

Alamat IP dapat dilihat sebagai dua bagian kelompok bilangan. Bagian pertama sebagai bagian jaringan dan bagian kedua sebagai bagian host. Bagian Jaringan akan menentukan alamat jaringan peralatan tersebut. Alamat jaringan adalah alamat IP dimana bit bilangan bagian host semuanya bernilai 0. Alamat jaringan akan menentukan lokasi peralatan dalam sistem jaringan. Bagian host menentukan nomor host untuk peralatan jaringan yang dimaksud. Bagian host akan menentukan alamat host.

Selain alamat jaringan dan alamat host, juga dapat diambil pengertian tentang alamat broadcast. Alamat broadcast adalah alamat IP yang semua bit bilangan bagian host dibuat menjadi 1. Alamat broadcast digunakan untuk berbicara secara simultan kepada semua peralatan dalam suatu jaringan.Perhatikan contoh berikut

Alamat Host : 11000000.01011100.01111001.**00000001** = 192 . 92 . 121 . 1

jika yang dicetak tebal adalah bagian host maka

Alamat jaringan : 11000000.01011100.01111001.00000000 = 192.92.121.0

Alamat broadcast : 11000000.01011100.01111001.11111111 = 192.92.121.255

### Kelas IP Adress

Untuk menentukan bagian jaringan dan bagian host suatu alamat IP digunakan pengelompokan alamat IP menjadi kelas-kelas. Dalam hal ini alamat IP dikelompokkan menjadi 5 kelas. Pengelompokan ini didasarkan pada nilai kelompok bit paling kiri dari alamat IP.

Cara pembagian kelas alamat IP adalah sebagai berikut.

0xxxxxxx.--------.--------.-------- : kelas A

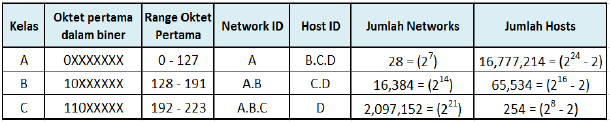
10xxxxxx.--------.--------.-------- : kelas B

110xxxxx.--------.--------.-------- : kelas C

1110xxxx.--------.--------.-------- : kelas D

11110xxx.--------.--------.-------- : kelas E

Tabel 6.1 Pembagian Kelas IP



### Kelas Alamat IP Privat (Private IP Address)

Dari semua alamat IP yang mungkin baik untuk kelas A, B maupun C, ada alamat IP khusus yang disebut alamat IP privat. Alamat IP ini tidak terhubung dengan alamat IP publik atau tidak dirouting. Alamat IP privat digunakan untuk membentuk jaringan yang sifatnya lokal, dalam pengertian tidak terhubung ke jaringan publik secara langsung. Rentangnya yaitu :

Kelas A : 10.0.0.0 – 10.255.255.255

Kelas B : 172.16.0.0 – 172.32.255.255

Kelas C : 192.168.0.0 – 192.168.255.255

Blok pertama adalah blok 24 bit yang merupakan satu alamat jaringan dalam kelompok alamat IP kelas A. Blok kedua adalah blok 20 bit yang merupakan 16 alamat jaringan dalam kelompok alamat IP kelas B. Sedangkan blok ketiga adalah blok 16 bit yang merupakan 256 alamat jaringan dari kelompok alamat IP kelas C. Peralatan networking biasanya secara default sudah dikonfigurasi dengan alamat kelas C antara 192.168.1.1 sampai 192.168.1.255

### Network Mask (Subnetwork Mask)

Network Mask atau istilah lengkapnya Subnetwork Mask atau disingkat Netmask digunakan untuk menginterpretasikan secara lokal satu bagian alamat jaringan. Netmask secara mudah diperoleh dengan cara mengubah semua bit pada bagian jaringan menjadi 1 dan mengubah semua bit pada bagian host menjadi 0. Dengan demikian untuk alamat IP kelas A, B dan C dapat ditentukan netmasknya sebagai berikut.

* Netmask IP kelas A = 255.0.0.0 = 11111111.00000000.00000000.00000000
* Netmask IP kelas B = 255.255.0.0 = 11111111.11111111.00000000.00000000
* Netmask IP kelas C = 255.255.255.0 = 11111111.11111111.11111111.00000000

Netmask akan menentukan rentang alamat IP yang berada pada satu jaringan yang sama. Jika suatu alamat IP sudah bisa diketahui berada pada jaringan yang sama, maka tidak perlu dicari dengan cara routing (melalui table route). Berikut ini diberikan contoh bagaimana netmask menentukan rentang alamat IP yang berada dalam satu jaringan.

Misalnya ditentukan alamat IP 192.168.100.103 netmask 255.255.255.0

Jika ditulis dalam bentuk biner

192.168.100.103 = 11000000.10101000.01100100.01100111

255.255.255.0 = 11111111.11111111.11111111.00000000

maka alamat jaringan untuk alamat IP tersebut adalah

192.168.100.0 = 11000000.10101000.01100100.00000000

Rentang alamat IP yang berada pada satu jaringan dengan alamat IP tersebut ditentukan oleh bagian host alamat IP tersebut yaitu 192.168.100.1 s/d 192.168.100.254.

Contoh yang lain, misalnya ditentukan alamat IP 192.168.100.103 netmask 255.255.255.224

Jika ditulis dalam bentuk biner

192.168.100.103 = 11000000.10101000.01100100.01100111

255.255.255.224 = 11111111.11111111.11111111.11100000

maka alamat jaringan untuk alamat IP tersebut adalah

192.168.100.96 = 11000000.10101000.01100100.01100000

Rentang alamat IP yang berada pada satu jaringan dengan alamat IP tersebut ditentukan oleh bagian host alamat IP tersebut yaitu 192.168.100.97 s/d 192.168.100.126.

Selain seperti yang sudah disebutkan di atas, orang sering menyebut netmask dengan cara menyebut jumlah bit 1 pada netmask.

Misalnya:

10.110.100.11 netmask 255.0.0.0 ditulis 10.110.100.11/8

172.31.80.253 netmask 255.255.0.0 ditulis 172.31.80.253/16

192.168.100.1 netmask 255.255.255.0 ditulis 192.168.100.1/24

192.168.100.1 netmask 255.255.255.128 ditulis 192.168.100.1/25

192.168.100.1 netmask 255.255.255.192 ditulis 192.168.100.1/26

192.168.100.1 netmask 255.255.255.224 ditulis 192.168.100.1/27

192.168.100.1 netmask 255.255.255.240 ditulis 192.168.100.1/28

192.168.100.1 netmask 255.255.255.248 ditulis 192.168.100.1/29

192.168.100.1 netmask 255.255.255.252 ditulis 192.168.100.1/30

192.168.100.1 netmask 255.255.255.254 ditulis 192.168.100.1/31

192.168.100.1 netmask 255.255.255.255 ditulis 192.168.100.1/32

### Subnetting

Sebelumnya sudah dibahas tentang bagaimana mendefinisikan dan mengetahui valid host untuk kelas A, B , dan C. Namun itu baru permulaan dalam mendefiniskan jaringan. Bagaimana jika anda ingin mengambil sebiah network address (alamat jaringan) dan membuat enam jaringan darinya? Anda harus melakukan sesuatu yang disebut dengan subnetting, karena subnetting lah yangmemungkinkan anda untuk mengambil sebuah jaringan yang besar dan membaginya menjadi beberapa jaringan kecil.

Cara menentukan jumlah subnet ada dan jumlah host per subnet adalah dengan menggunakan dua formula berikut ini :

Jumlah Subnet = **2x**

Jumlah host per subnet = **2y-2**

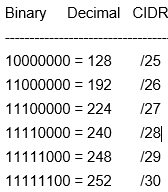
Kedua formula tersebut menghitung jumlah host atau subnet berdasarkan jumlah bit biner yang digunakan. Sebagai contoh, jika Anda meminjam tiga bit dari Host Portion alamat gunakan formula “Jumlah Subnet” untuk menentukan jumlah subnet yang dihasilkan dari meminjam 3 bit. Sehingga, jumlah subnetnya adalah 23 atau 2x2x2 = 8 subnet.

Untuk menentukan jumlah host per subnet Anda tinggal gunakan jumlah bit biner yang ada pada host portion dan terapkan ke formula “Jumlah host per subnet”. Dengan begitu dalam soal ini jumlah hostnya adalah 25 atau sama dengan 32.

Tidak semua host bisa digunakan oleh devais. Anda harus mengurangi 2 dari jumlah host yang didapat karena sudah dialokasikan untuk : 1 IP untuk alamat jaringan (Subnet number), dan yang satu lagi untuk broadcast address.

#### Subnetting Kelas C

Di kelas C hanya ada 8 bit tersedia untuk host portion. Ingat bahwa bit subnet dimulai dari kanan ke kiri. Jadi subnet mask yang mungkin untuk kelas C adalah:



Note:CIDR = Classless Inter Domain Routing.

Untuk melakukan subnetting, anda harus menjawab 5 pertanyaan berikut:

1. How many subnets does the chosen subnet mask produce?
2. How many valid hosts per subnet are available?
3. What are the valid subnets?
4. What's the broadcast address of each subnet?
5. What are the valid hosts in each subnet?

Contoh:

* How many subnets? **2x** = number of subnet. X adalah jumlah bit 1 padahost portion. Misalnya pada 110000000, jumlah bit 1 memberikankita **22** subnet. Jadi jawabannya adalah ada 4 subnet.
* How many host per subnet? **2y - 2** = number of host per subnet. Y adalah jumlah bit 0. Misalkan pada 11000000, jumlah bit 0 memberikan kita **26 - 2** host. Jadi jawabannya adalah 62 host per-subnet.
* What are the valid subnets? 256 – subnet mask = Block Size. Contoh 256 – 192 = 64. Jadi Block Size untuk 192 selalu 64. Jadi subnet nya adalah sebagai berikut 0, 64, 128, dan 192.
* What is the broadcast address for each subnet? Kita sudah mengetahui bahwa subnetnya adalah 0, 64, 128, dan 192. Broadcast address adalah nomor tepats ebelum subnet selanjutnya. Misalkan Subnet 0 mempunyai broadcast 63, sebab subnet selanjutnya adalah 64. Begitupun dengan subnet 64, broadcast addressnya adalah 127, karena subnet selanjutnya adalah 128, dan seterusnya.Ingat bahwa broadcast dari subnet terakhir kelas C selalu 255.
* What are the valid hosts? Valid hosts adalah alamat diantara subnet dan broadcast address. Misalkan jika subnetnya adalah 64 dan 127adalah broadcasatnya, maka valid host adalah dari 65 sampai 126.

**Latihan Subnetting kelas C**

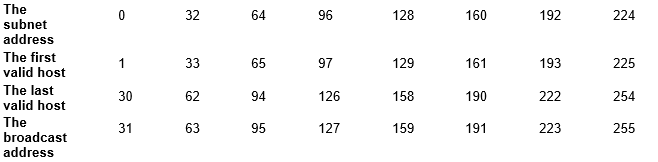
Diketahui:

192.168.10.0/27= Network Adress

255.255.255.224 = Subnet mask

1. How many subnets? 224 adalah 11100000, jadi 23 = 8
2. How many hosts? 25 – 2= 30
3. What are the valid subnets? 256-224 =32.Jadi subnetnya kelipatan 32mulai dari 0,32, 64, 96, 128, 160, 192, 224
4. What’s the broadcast address for each subnet? (selalu nomor sebelum subnet selanjutnya)
5. What are the valid hosts? (alamat antara subnet dan broadcast address)

Jawaban untuk nomor 4 dan 5:



#### Subnetting Kelas B

Sebelum kita lanjutkan, berikut adalah Subnet Mask untuk kelas B:

255.255.128.0 (/17) 255.255.255.0 (/24)

255.255.192.0 (/18) 255.255.255.128 (/25)

255.255.224.0 (/19) 255.255.255.192 (/26)

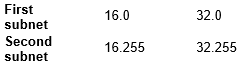
255.255.240.0 (/20) 255.255.255.224 (/27)

255.255.248.0 (/21) 255.255.255.240 (/28)

255.255.252.0 (/22) 255.255.255.248 (/29)

255.255.254.0 (/23) 255.255.255.252 (/30)

Subnetting untuk kelas B sama persis dengan subnetting kelas C, bedanya anda memiliki jumlah bit yang lebih banyak. Bila kelas C subnet number dilakukan pada oktet ke 4, maka untuk kelas B dilakukan pada oktet ke 3. Tambahkan 0dan 255 pada bagian broadcast di oktet ke 4. Dibawah ini contoh rentang host dari 2 subnet kelas B:



**Latihan Subnetting Kelas B**

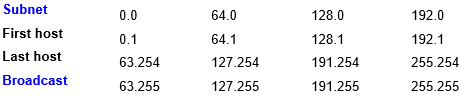
Diketahui:

172.16.0.0/18 = Network Address

255.255.192.0 = Subnet Mask

1. How many subnets? 22 = 4
2. How many hosts? 214 – 2= 16.382 (6 bit di oktetketiga, dan 8 bit di oktet ke 4)
3. What are the valid subnets? 256-192 =64. Jadi subnetnya kelipatan 64 mulai dari 0, 64, 128, 192
4. What’s the broadcast address for each subnet? (selalu nomor sebelum subnet selanjutnya)
5. What are the valid hosts? (alamat antara subnet dan broadcast address)

Tabel berikut ini menunjukkan ke empat subnet, valid hosts (first host dan Last host), dan broadcast address.



#### Subnetting Kelas A

Subnetting kelas A juga tidak berbeda dengan kelas B. Kecuali subnetting kelas A menggunakan 24bits sedangkan kelas B hanya 16 bit. Berikut adalah daftar subnet mask kelas A :

255.128.0.0 (/9) 255.255.240.0 (/20)

255.192.0.0 (/10) 255.255.248.0 (/21)

255.224.0.0 (/11) 255.255.252.0 (/22)

255.240.0.0 (/12) 255.255.254.0 (/23)

255.248.0.0 (/13) 255.255.255.0 (/24)

255.252.0.0 (/14) 255.255.255.128 (/25)

255.254.0.0 (/15) 255.255.255.192 (/26)

255.255.0.0 (/16) 255.255.255.224 (/27)

255.255.128.0 (/17) 255.255.255.240 (/28)

255.255.192.0 (/18) 255.255.255.248 (/29)

255.255.224.0 (/19) 255.255.255.252 (/30)

**Latihan Subnetting Kelas A**

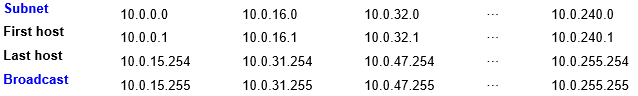
Diketahui:

10.0.0.0/20 = Network Address

255.255.240.0 = Subnet Mask

1. How many subnets? 212 = 4096
2. How many hosts? 212 – 2= 4094
3. What are the valid subnets? 256-240 =16. Jadi subnetnya kelipatan 16 mulai dari 0, 16, 32, 48, dst
4. What’s the broadcast address for each subnet? (selalu nomor sebelum subnet selanjutnya)
5. What are the valid hosts? (alamat antara subnet dan broadcast address)

Tabel berikut ini menunjukkan ke empat subnet, valid hosts (first host dan Last host), dan broadcast address.



## Latihan

Task 1: Tentukan Subnet, First Host, Last Host dan Broadcast Address dari Network Address dan Subnet Mask berikut:

1. Kelas C
   1. 192.168.5.0/25
   2. 192.168.7.0/30
   3. 192.168.9.0/29
2. Kelas B
   1. 172.16.0.0/20
   2. 172.16.0.0/23
3. Kelas A
   1. 10.0.0.0/16
   2. 10.0.0.0/26

Task 2: Tentukan Subnet, Broadcast Address, dan Valid Host range untuk tiap IP Address berikut:

1. 172.16.10.5/25
2. 172.16.10.33/27
3. 172.16.10.65/26
4. 172.16.10.17/30
5. 172.16.10.33/28
6. 192.168.100.25/30
7. 192.168.100.37/29
8. 192.168.100.66/27
9. 192.168.100.17/29
10. 10.10.10.5/20

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy * Todd Lammle (2005), CCNA—Cisco Certified Network Associate Study Guide, 5th Edition, SYBEX Inc, 1151 Marina Village Parkway,Alameda, CA 94501. |
|  |

# Subnetting with VLSM

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami konsep subnetting dengan VLSM
2. Mampu melakukan subnetting dengan VLSM

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Variable Length Subnet Mask (VLSM)

Variable Length Subnet Mask (VLSM) merupakan sebuah cara sederhana untuk menangani sebuah network lalu membagi network tersebut menjadi beberapa network yang menggunakan subnet mask berbeda dalam desain network yang berbeda.

Berbeda dengan subnetting yang kita pelajari pada bab sebelumnya dimana dalam satu network menggunakan subnet mask yang sama (Classfull Routing Protocol), VLSM memungkinkan kita untuk menggunakan subnet mask yang berbeda untuk masing-masing subnet (Classless Routing Protocol).

Perhatikan desain jaringan berikut:

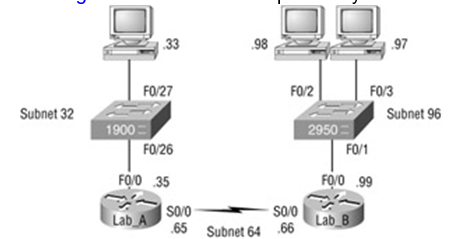


Figure 7.1 Typical Classfull Network

Dalam gambar tersebut, Terdapat dua buah router yang terhubung menggunakan WAN serial Link. Masing-masing router terhubung ke LAN. Dengan Classfull network design yang telah kita pelajari pada bab sebelumnya, kita dapat membuat subnet network tersebut dengan:

**192.168.10.0=Network**

**255.255.255.224 =Subnet Mask**

Sehingga valid subnetnya adalah kelipatan dari 32 mulai dari 0, 32,64, 96, 128, 160, 192, dan 224. Valid host untuk masing-masing subnet adalah 30 host. Berdasarkan gambar 7.1 subnet yang digunakan adalah subnet 32, subnet 64, dan subnet 96. Selintas tidak ada masalah. Coba perhatikan pada subnet 64 yang merupakan point-to-point antara router Lab A dengan router Lab B yangjuga diberikan 30 host. Padahal sebenarnya hanya membutuhkan dua host, sehingga terjadikelebihan IP Address sebanyak 28 host. VLSM dapat menjadi solusi dengan memberikan subnet mask berbeda untuk link antara router A dengan router B.

### Implementing VLSM Network

Untuk membuat VLSM network secara cepat dan efisien, anda harus memahami tabel berikut sebagai acuan:

|  |  |  |  |
| --- | --- | --- | --- |
| **Prefix** | **Subnet Mask** | **Block Size** | **Hosts number** |
| /32 | 255.255.255.255 | 1 | 0 |
| /31 | 255.255.355.254 | 2 | 0 |
| /30 | 255.255.255.252 | 4 | 2 |
| /29 | 255.255.255.248 | 8 | 6 |
| /28 | 255.255.255.240 | 16 | 14 |
| /27 | 255.255.255.224 | 32 | 30 |
| /26 | 255.255.255.192 | 64 | 62 |
| /25 | 255.255.255.128 | 128 | 126 |
| /24 | 255.255.255.0 | 256 | 254 |
| /23 | 255.255.254.0 | 512 | 510 |
| /22 | 255.255.252.0 | 1024 | 1022 |
| /21 | 255.255.248.0 | 2048 | 2046 |
| /20 | 255.255.240.0 | 4096 | 4094 |
| /19 | 255.255.224.0 | 8192 | 8190 |
| /18 | 255.255.192.0 | 16.386 | 16.384 |
| /17 | 255.255.128.0 | 32.768 | 32.766 |
| /16 | 255.255.0.0 | 65.536 | 65.534 |
| /15 | 255.254.0.0 | 131.072 | 131.070 |
| /14 | 255.252.0.0 | 262.144 | 262.142 |
| /13 | 255.248.0.0 | 524.288 | 524.286 |
| /12 | 255.240.0.0 | 1.048.576 | 1.048.574 |
| /11 | 255.224.0.0 | 2.097.152 | 2.097.150 |
| /10 | 255.192.0.0 | 4.194.304 | 4.194.302 |
| /9 | 255.128.0.0 | 8.388.608 | 8.388.606 |
| /8 | 255.0.0.0 | 16.777.216 | 16.777.214 |

Contoh:

Sebuah perusahaan akan membangun jaringan dengan ketentuanhost sebagai berikut:

* Ruang Utama 1000 host
* Ruang Kedua 500 host
* Ruang Ketiga 100 host
* Ruang Server 2 Host

Dengan IP Network 172.16.0.0/16 lakukan subnetting dengan VLSM!

1. Ruang Utama 1000 host

Gunakan tabel diatas, cari di kolom Hosts Number yang mendekati 1000 lalu lihat padanannya dari mulai prefix hingga subnet masknya. Dari tabel yang sesuai dengan kebutuhan host yaitu 1022 dengan subnet mask 255.255.252.0 dengan prefix /22.

Cari IP range dengan mengurangkan 255.255.255.255 dengan subnet mask jaringan ini yaitu 2555.255.252.0

255.255.255.255   
255.255.252.    0   \_

    0.    0.    3.255  
  
Dan untuk mengetahui IP broadcastnya, hasil dari pengurangan diatas ditambah dengan *ip*network diawal 172.16.0.0

172. 16.  0.    0  
    0.   0.  3.255  +  
172. 16.  3.255

Network         : 172.16.0.0/22

IP Pertama    : 172.16.0.1

IP Terakhir    : 172.16.3.254

IP Broadcast : 172.16.3.255

Subnet Mask : 255.255.252.0

Network Selanjutnya 172.16.4.0(gunakan ini sebagai IP Network dari ruang kedua)

1. Ruang Kedua 500 host

Gunakan tabel diatas, cari di kolom Hosts Number yang mendekati 500 lalu lihat padanannya dari mulai prefix hingga subnet masknya. Dari tabel yang sesuai dengan kebutuhan host yaitu 510 dengan subnet mask 255.255.254.0 dengan prefix /23.

Cari IP range dengan mengurangkan 255.255.255.255 dengan subnet mask jaringan ini yaitu 2555.255.254.0

255.255.255.255   
255.255.254.    0   \_

    0.    0.    1.255  
  
Dan untuk mengetahui IP broadcastnya, hasil dari pengurangan diatas ditambah dengan *ip*network lanjutan dari ruang utama yaitu 172.16.4.0

172. 16.  4.    0  
    0.   0.  1.255  +  
172. 16.  5.255

Network         : 172.16.4.0/23

IP Pertama    : 172.16.4.1

IP Terakhir    : 172.16.5.254

IP Broadcast : 172.16.5.255

Subnet Mask : 255.255.254.0

Network Selanjutnya 172.16.6.0(gunakan ini sebagai IP Network dari ruang ketiga)

1. Ruang Ketiga 100 host

Untuk ruang ketiga yang butuh 100 hosts, dari tabel yang sesuai dengan kebutuhan host yaitu 128 dengan subnet mask 255.255.255.128 dengan prefix /25.

Cari IP range dengan mengurangkan 255.255.255.255 dengan subnet mask jaringan ini yaitu 2555.255.255.128

255.255.255.255   
255.255.255. 128   \_

    0.    0.    0.127  
  
Dan untuk mengetahui IP broadcastnya, hasil dari pengurangan diatas ditambah dengan *ip*network lanjutan dari ruang kedua yaitu 172.16.6.0

172. 16.  6.    0  
    0.   0.  0.127  +  
172. 16.  6.127

Network         : 172.16.6.0/25

IP Pertama    : 172.16.6.1

IP Terakhir    : 172.16.6.126

IP Broadcast : 172.16.6.127

Subnet Mask : 255.255.255.128

Network Selanjutnya 172.16.6.128 (gunakan ini sebagai IP Network dari ruang Server)

1. Ruang Server 2 host

Terakhir ruang server membutuhkan 2 hosts. Gunakan subnet mask 255.255.255.252 dengan prefix /30.

Hasilnya sebagai berikut:

Network         : 172.16.6.128/30

IP Pertama    : 172.16.6.129

IP Terakhir    : 172.16.6.130

IP Broadcast : 172.16.6.131

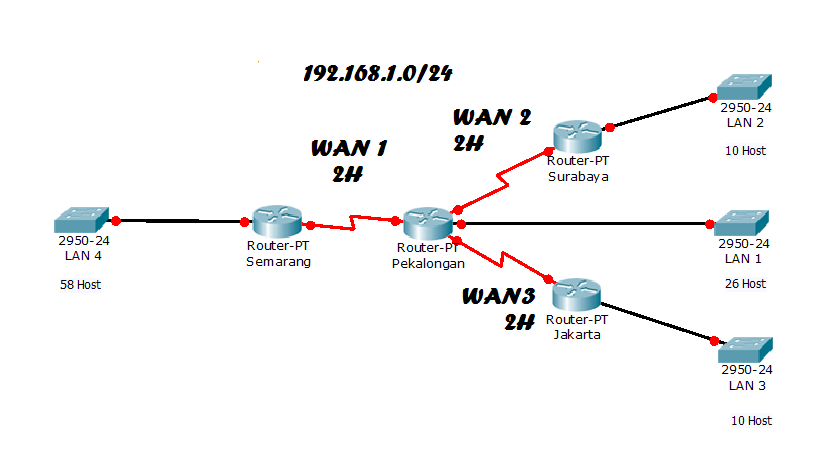
Subnet Mask : 255.255.255.252

## Latihan

1. Akan dibangun sebuah jaringan dengan kebutuhan host sebagai berikut:
   1. Ruang A membutuhkan 289 PC
   2. Ruang B membutuhkan 150 PC
   3. Ruang C membutuhkan 70 PC
   4. Ruang D membutuhkan 26 PC
   5. Ruang Emembutuhkan 14 PC

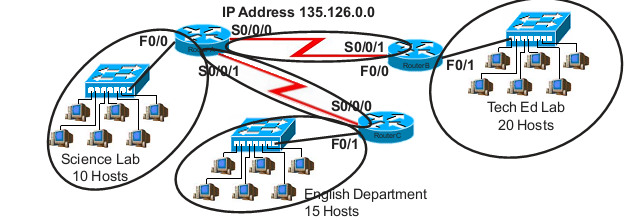
Dengan alamat jaringan 172.16.0.0/17, tentukan range IP Address setiap ruang dengan VLSM!

1. Diketahui Topologi sebuah perusahaan sebagai berikut:



* 1. Ada berapa jaringan pada topologi di atas?
  2. Tentukan alamat IP untuk LAN1, LAN2, LAN3, LAN4, WAN1, WAN2, dan WAN3!

1. Diketahui Topologi sebuah perusahaan sebagai berikut:



* 1. Ada berapa jaringan pada topologi di atas?
  2. Tentukan alamat IP untuk semua subnet!

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy * Todd Lammle (2005), CCNA—Cisco Certified Network Associate Study Guide, 5th Edition, SYBEX Inc, 1151 Marina Village Parkway,Alameda, CA 94501. |
|  |

# Assesment 1

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami konsep jaringan, topologi, OSI Layer, pengkabelan, Pengalamatan IP, Subnetting CIDR dan VLSM.
2. Mampu merancang dan mengkonfigurasi serta troubleshooting jaringan termasuk pengalamatannya.

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC, dan alat tulis.

## Dasar Teori

Soal akan ditentukan pada saat assesment

## Latihan

Akan ditentukan pada saat assesment

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy * Todd Lammle (2005), CCNA—Cisco Certified Network Associate Study Guide, 5th Edition, SYBEX Inc, 1151 Marina Village Parkway,Alameda, CA 94501. |
|  |

# Wireless LAN

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Jaringan Wireless LAN Ad-hoc dan Infrastructure
2. Mampu melakukan konfigurasi Wireless Ad-hoc dan Infrastructure.
3. Mampu memanfaatkan jaringan wireless untuk sharing file, koneksi Internet dan printer.

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet, D-Link Access Point.

## Dasar Teori

### Wireless LAN (WLAN)

*Wireless Local Area Network* sebenarnya hampir sama dengan jaringan LAN, akan tetapi setiap node pada WLAN menggunakan *wireless device* untuk berhubungan dengan jaringan, node pada WLAN menggunakan *channel* frekuensi yang sama dan SSID yang menunjukkan identitas dari *wireless device*. Tidak seperti jaringan kabel, jaringan wireless memiliki dua mode yang dapat digunakan : **infrastruktur** dan **Ad-Hoc**. Konfigurasi infrastruktur adalah komunikasi antar masing-masing PC melalui sebuah *access point* pada WLAN atau LAN. Komunikasi Ad-Hoc adalah komunikasi secara langsung antara masing-masing komputer dengan menggunakan piranti *wireless.* Penggunaan kedua mode ini tergantung dari kebutuhan untuk berbagi data atau kebutuhan yang lain dengan jaringan berkabel.

### Topologi Ad-hoc

Topologi ad-hoc merupakan topologi jaringan WLAN yang dihubungkan tanpa menggunakan access point, tetapi langsung dari komputer ke komputer layaknya peer to peer pada jaringan kabel. Mode ini lah yang akan nanti kita praktekan dalam percobaan ini. Mode ad-hoc dapat kita gunakan apabila ingin membangun sebuah jaringan yang sederhana dalam suatu area yang terbatas atau satu ruangan. Setiap *host* cukup memiliki *transmitter* dan *receiver* wireless untuk berkomunikasi secara langsung satu sama lain seperti tampak pada **gambar** dibawah ini

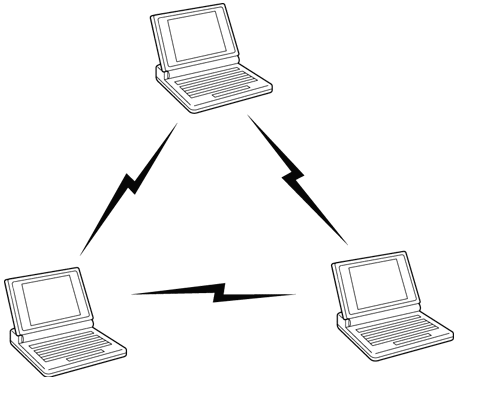


Figure 9.1 Topologi Ad-hoc

Kekurangan dalam mode ad-hoc adalah tidak banyak komputer yang dapat dihubungkan karena maksimal komputer yang dapat terhubung dalam jaringan mode ad-hoc ini sebanyak 11 buah komputer. Dan jangkauan area yang terbatas karena sinyal hanya dipancarkan oleh PC yang hanya dapat memancarkan sinyal yang terbatas.

### WLAN Infrastructure Topology

Jika komputer pada jaringan wireless ingin mengakses jaringan kabel atau berbagi printer misalnya, maka jaringan wireless tersebut harus menggunakan mode infrastruktur Pada mode infrastruktur access point berfungsi untuk melayani komunikasi utama pada jaringan wireless. Access point mentransmisikan data pada PC dengan jangkauan tertentu pada suatu daerah. Penambahan dan

pengaturan letak access point dapat memperluas jangkauan dari WLAN.

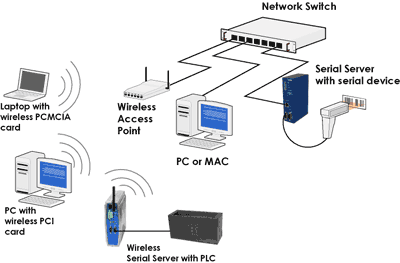


Figure 9.2. WLAN Infrastructure Topology

Salah satu komponen utama dalam mode infrastruktur adalah Access Point. Access Point, merupakan perangkat yang menjadi sentral koneksi dari pengguna (user) ke server, atau sebaliknya. Access-Point berfungsi mengkonversikan sinyal frekuensi radio (RF) menjadi sinyal digital yang akan disalurkan melalui kabel, atau disalurkan ke perangkat WLAN yang lain dengan dikonversikan ulang menjadi sinyal frekuensi radio.

Membuat area hotspot atau membuat access point sebetulnya tidak beda dengan membuat router, tetapi di tambah dengan mengaktifkan wireless dan server DHCP pada router kita. Tetapi tentu saja alat dan fasilitas yang lengkap pada router tersebut yang harus mendukung access point. Jadi alat Access point router ini berfungsi sebagai server router, server DHCP dan pemancar wireless.

## Latihan

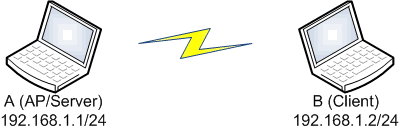
### Bagian I: Konfigurasi WLAN Ad-hoc Toplogy

**Alat dan Bahan:**

Per kelompok minimal terdapat 2 laptop

Modem GSM/CDMA koneksi Internet

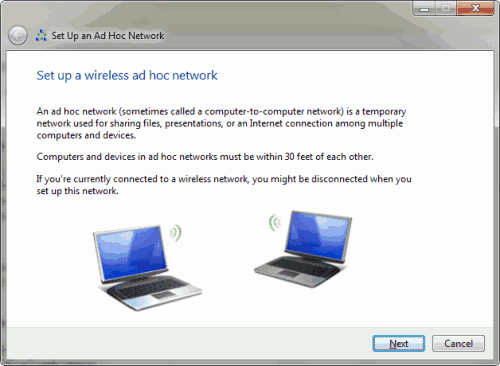
**Diagram Topology**



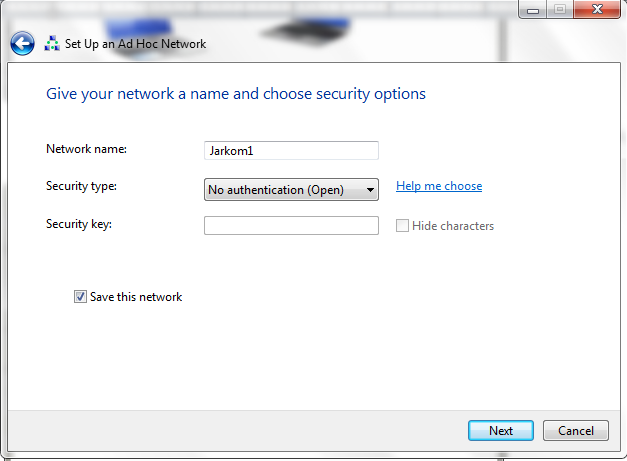
**Praktikum 1: Setting Mode Ad-hoc**

**Setting WiFi KomputerServer:**

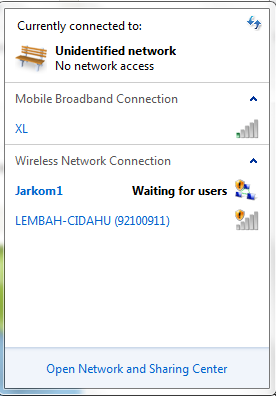
1. Aktifkan terlebih dahulu WLAN padaLaptop
2. Klik Tombol Windows **Start**, pada kolom **search** **programs and files** ketik: adhoc kemudian enter.
3. Kemudian jendela **Setup Ad-hoc (Computer to Computer)** Network akan terbuka, klik Next.



1. Pada kolom Network name: isi dengan nama yang akan kita gunakan sebagai SSID (Service Set Identifier), contohnya: Jarkom1, pilih **security type** = No authentication (open), Save Network, kemudian Next.



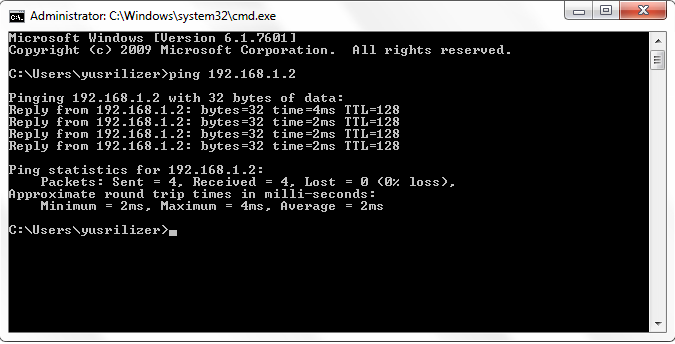
1. Setelah muncul jendela The Jarkom1 network is ready to use, klik Close.
2. Cek koneksi WiFi dengan cara klik icon wireless , pada taskbar sebelah kanan terlihat status Jarkom1 –Waiting for users.



1. Ubah IP wireless interface menjadi 192.168.1.1/24

**Setting WiFi Client (pada laptop client)**

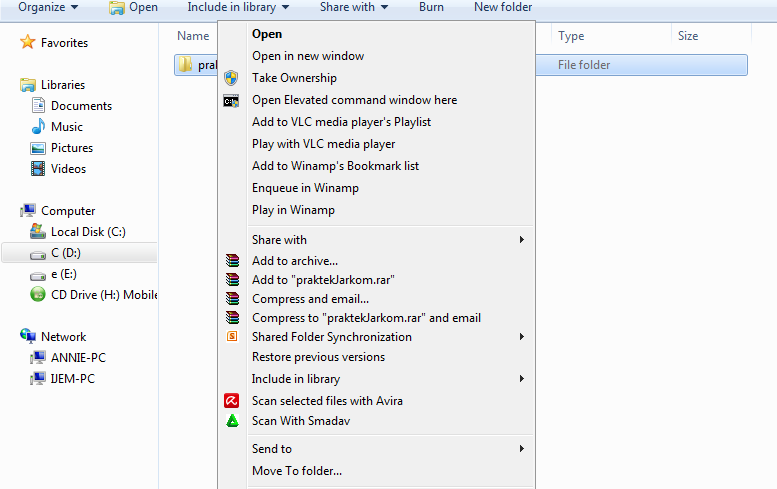
1. Browse jaringan wireless di laptop yang menjadi client, cari AP dengan nama Jarkom 1
2. Sambungkan laptop Client dengan AP kelompok anda dan pastikan status sudah Connected.
3. UbahIP Wireless Interface menjadi 192.168.1.2/24
4. Lakukan ping secara 2 arah, pastikan keduanya sukses—reply.



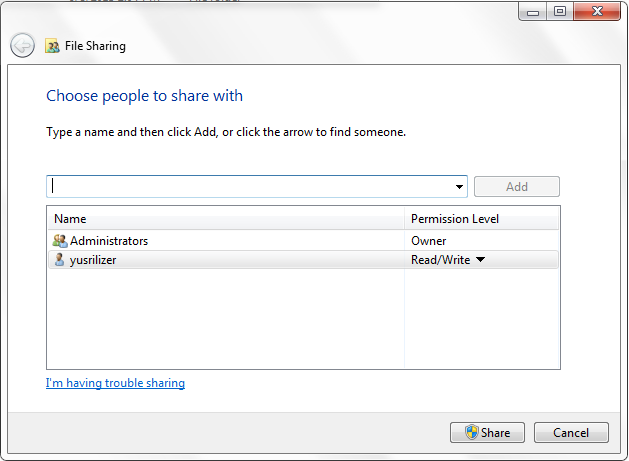
**Praktikum 2: Sharing File**

**File Server (Laptop yang men-sharing file)**

1. Pastikan sudah terhubung dengan jaringan Ad-hoc
2. Pada salah satu laptop, buat sharing folder dengan klik kanan folder yang akan di-share. **Sharing with**>> **Specific People**



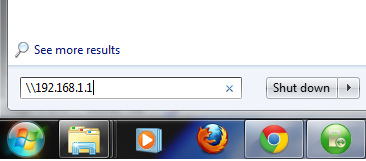
1. Kemudian akan muncul dialog sebagai berikut:



1. Ketik everyone, klik **Add**🡪 **Share**

**Komputer Client (yang menggunakan file)**

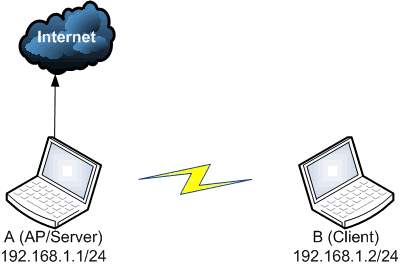
* + 1. Ketik alamt [\\192.168.1.x](file:///\\192.168.1.x) (x = host yang akan diambil file-nya/remote host) pada **search** di taskbar.



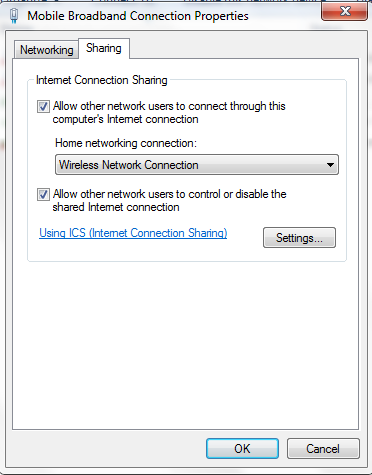
* + 1. Pastikan anda sudah bisa membuka file yang di-share oleh komputer remote/server.

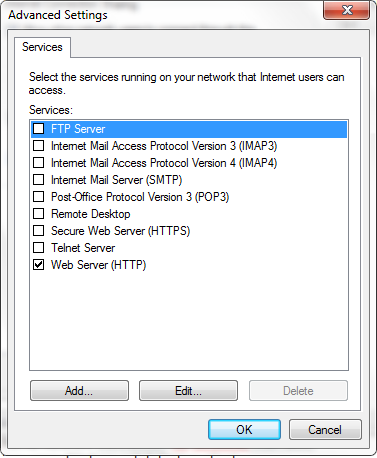
***Catatan :****jika anda tidak bisa membuka file sharing remote, pastikan firewall baik di windows/di antivirus tidak memblokirnya*

**Praktikum 3: Internet Sharing**



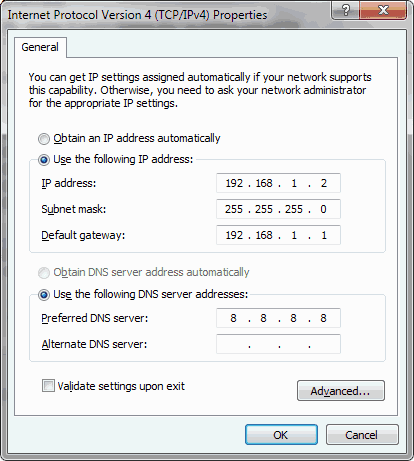
1. Susunlah jaringan Internet Sharing dengan Laptop A sebagai **gateway** (terhubung Internet melalui modem), laptop B menggunakan Internet melalui laptop A.
2. Klik kanan interface modem pada **laptop A >> properties**, kemudian rubahlah setting-nya dengan mengikuti langkah selanjutnya.
3. Check **Allow other network**..., arahkan **home network connection** ke **wireless interface**, kemudian tekan tombol setting, pilih service yang diijinkan untuk laptop client.



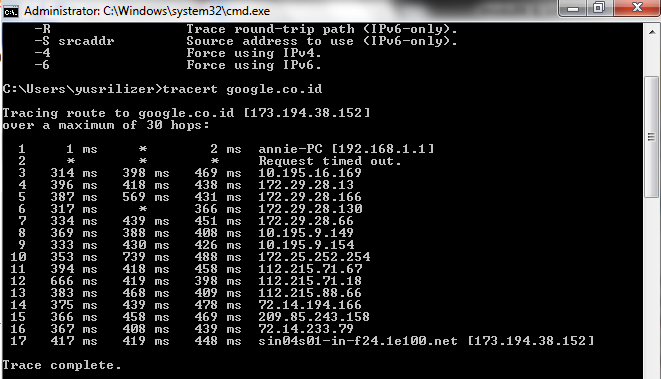


1. Pada interface wireless AP (laptop A), isikan IP 192.168.1.1/24
2. Pada interface wireless client (laptopB), isikan IP 192,168.1.2/, gateway menuju 192.168.1.1, dan primary DNS 8.8.8.8 (atau boleh menggunakan DNS modem)
3. Gambar dibawah ini yang ditandai lingkaran merah menunjukkan indikator bahwa komputer telah terhubung denganjaringan Internet.





1. Pastikan jaringan ad-hoc sudah tersambung kembali (bila perlu ping dulu)
2. Serakarngcoba browsing pada laptop Bke google.co.id, jika sudah terkoneksi silahkan tracert ke google.co.id, lihat rute perjalanannya.



### Bagian II: Konfigurasi WLAN Infrastructure Topology

**Alat dan Bahan:**

* Per kelompok minimal terdapat dua laptop
* Access Point D-Link DWL 2100AP



Bangunlah jaringan seperti diagram topologi berikut:

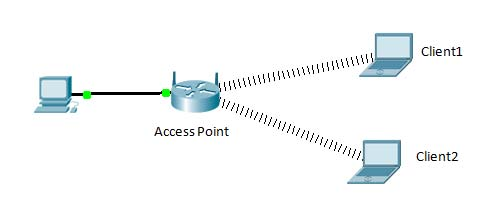
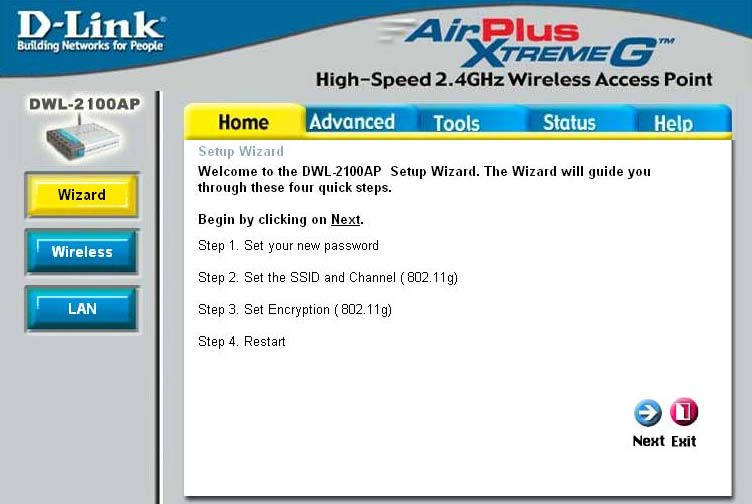
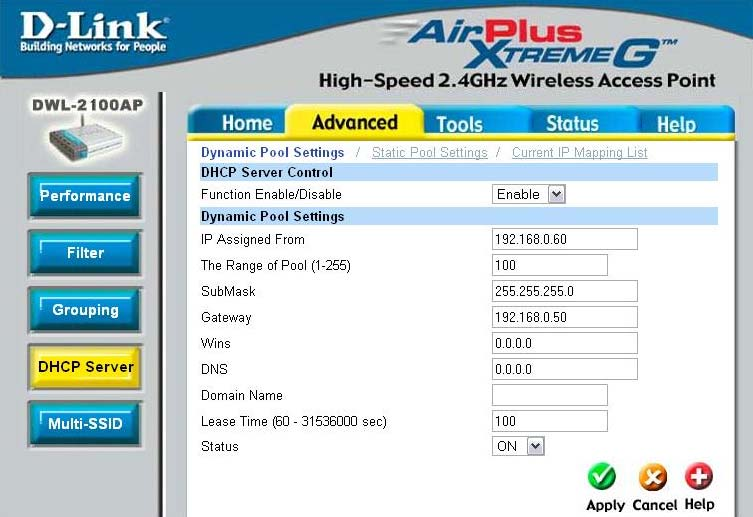


Figure 9.3 Diagram Topology Infrastructure

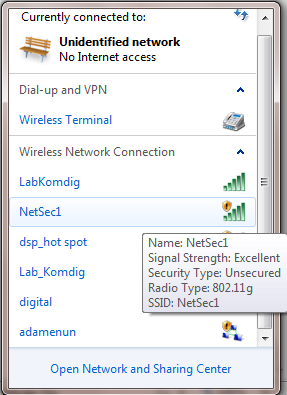
***NB:*** *Default IP untuk access point : 192.168.0.50 Subnet mask : 255.255.255.0 Untuk IP di PC Desktop bisa digunakan yang satu range dengan IP Access Point, misal : 192.168.0.60*

Praktikum 1: Konfigurasi dasar Access Point D-Link

1. Koneksikan Access Point ke PCDesktop
2. Setting IP untuk PC Desktop: **192.168.0.60** netmask 255.255.255.0
3. Setting Access Point sebagai berikut (hanya berlaku pada AP D-Link). Buka browser lalu ketikkan : <http://192.168.0.50>, dengan **username**: admin, **password** : kosong. Akan tampil halaman utama dari setting AP
4. Pilih tombol Wizard untuk melakukan setting AP dengan panduan
5. Langkah pertama, ganti password dengan password yang baru. Misalnya password barunya: **jarkom**. Lalu klik Next.
6. Langkah kedua, Set SSID dan Channel. Secara default nama **SSID**: dlink. Silahkan ganti nama **SSID: NetSec1**. Untuk **Channel: 6.**
7.  Langkah ketiga: set security encryption. Bila ingin mengamankan AP dengan password silahkan pilih WEP atau WPA-PSK. Tapi untuk kali ini kita buat tanpa password. Jadi pilih **No Security**.
8. Langkah ke-empat: Restart Access Point.
9. Setelah di-restart. Klik Tab Status untuk melihat informasi IP dari Access Point
10. Kita akan membuat AP menjadi DHSCP Server, sehingga client akan mendapatkan IP secara otomatis. Klik **Advanced**, lalu set **Enable** pada **DHCP Server Control Function Enable/Disable**. Kemudian set IP dari mulai **192.168.0.60**, dengan **gateway IP AP yaitu 192.168.0.50**.

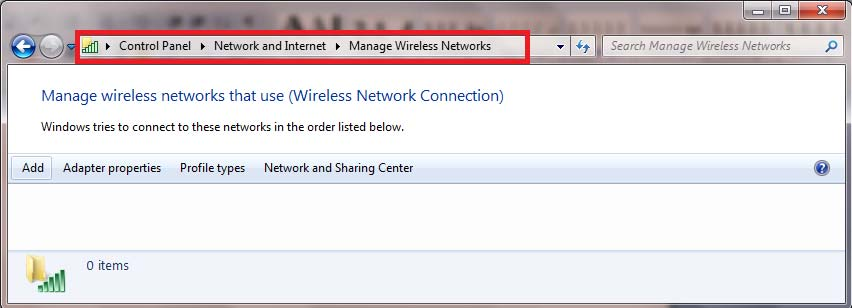


1. Beralih ke PC –Client (Laptop). Klik icon wireless pada taskbardikanan bawah, kemudian lihat apakah jaringan NetSec1 sudah terdeteksi.



1. Lakukan koneksi, dan di client akan muncul: Netsec 1 Connectes
2. Cek no IP yang diberikan oleh DHCP Server dan lakukan ping dari client ke AP.

Praktikum 2: Men-Disable SSID

1. Agar nama SSID tidak terlihat dari client, maka AP harus di-set sebagai berikut:
2. Klik tombol **Wireless** pada men sebelah kiri. Lalu pada field **SSID Broadcast** pilih **Disable**.
3. Beralih ke PC/Laptop Client. Karena SSID atau nama jaringan tidak bisa terdeteksi otomatis, maka untuk dapat terhubung ke jaringan tersebut harus dilakukan manual. Masuk ke **Control Panel 🡪Network and Internet🡪Manage Wireless Network🡪Add**
4. Lalu pilih **Manually create a network profile**
5. Masukkan nama SSID jaringan termasuk otentikasi yang digunakan (WEP/WPA/atau tanpa pasword). Next.
6. Cek IP client dengan **ipconfig** lalu ping ke AP.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy * M. Yusril Helmi (2015), Job Sheet WLAN Ad-hoc and Infrastructure Topology. |
|  |

# Virtual Local Area Network (VLAN)

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Network dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### VLAN

VLAn merupakan suatu model jaringan yang tidak terbatas pada lokasifisik seperti LAN, hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik perangkat. Penggunaa VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen.

### Cara kerja VLAN

VLAN diklasifikasikan berdasarkan metode atau tipe yang digunakan yang terdiri dari 4 tipe yaitu berdasarkanport, MAC Address, protokol, dan alamat subnet IP. Semua informasi yang mengandung penandaan/pengalamatan suatu VLAN (tagging) disimpan dalamsuatu database (tabel), jika penandaannya berdasarkan port maka databse harus mengindikasikan port-port yang digunakan oleh VLAN. Untu mengaturnya maka biasanya digunakan manageable switch. Switch inilah yang bertanggung jawab menyimpan semua informasi dan konfigurasi suatu VLAN dan dipastikan semua swicth memiliki informasi yang sama. Switch akan menentukan kemana data akan diteruskan dan sebagainya atau dapat pula digunakan suatu software pengalamatan (bridging software) yang berfungsi mencatat/menandai suatu VAN beserta workstation yang berada pada jaringannya.

### Perbandingan antara LAN dan VLAN

Perbedaan yang sangat jelas dari model jaringan Local Area Network denganVirtual Local Area Network adalah bahwa bentuk jaringan dengan model LocalArea Network sangat bergantung pada letak/fisik dari workstation, serta penggunaan hub dan repeater sebagai perangkat jaringan yang memiliki beberapakelemahan. Sedangkan yang menjadi salah satu kelebihan dari model jaringandengan VLAN adalah bahwa tiap-tiap workstation/user yang tergabung dalam satu VLAN/bagian (organisasi, kelompok dsb) dapat tetap saling berhubunganwalaupun terpisah secara fisik. Atau lebih jelas lagi akan dapat kita lihat perbedaan LAN dan VLAN pada gambar dibawah ini.



Figure 10.1 Contoh LAN

Pada LAN untuk membagi jaringan dibutuhkan 3 Switch.



Figure 10.2 Contoh VLAN

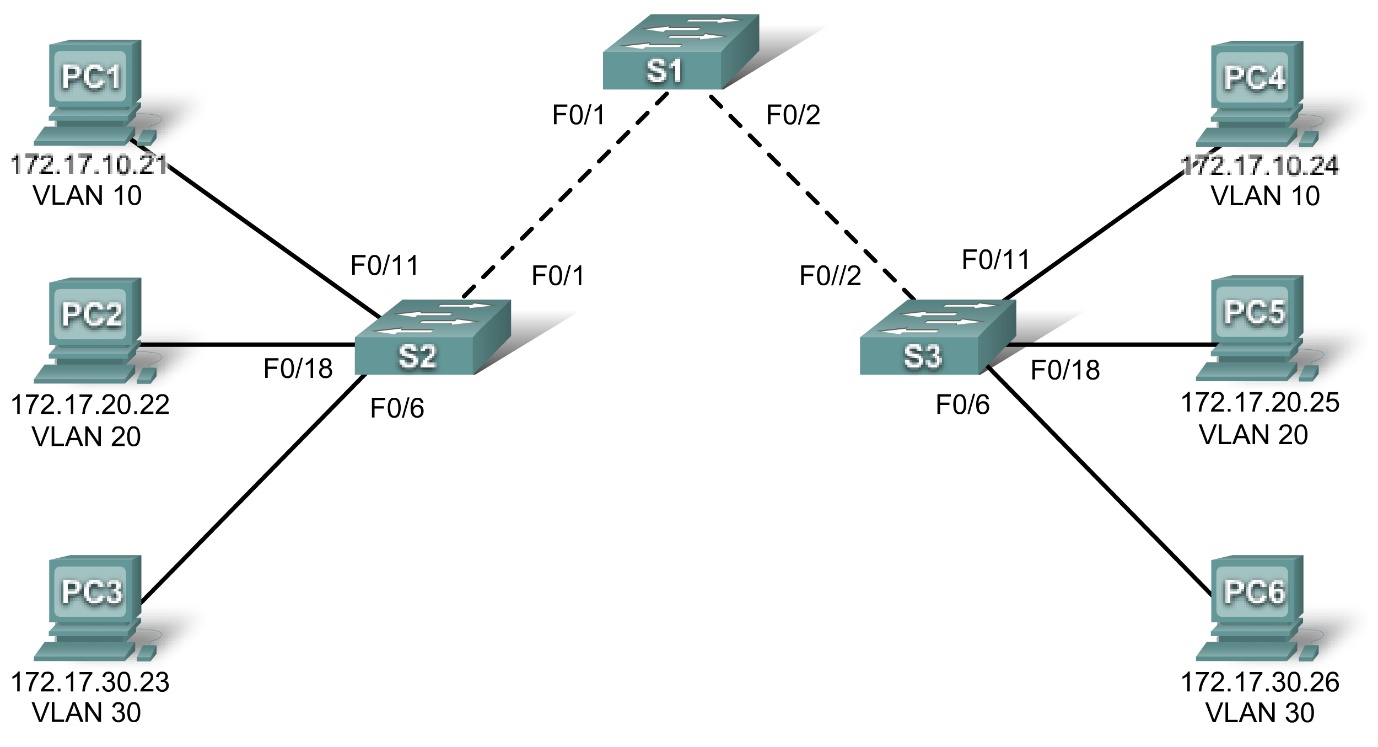
Pada VLAN untuk membagi jaringan cukup dengan menggunakan 1 switch.

## Latihan

1. Basic VLAN Configuration

**Buka Packet Tracer Activity Source Files: Nomor 3.5.1.pka**

**Diagram Topology**



**Addressing Table**

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| --- | --- | --- | --- | --- |
| S1 | VLAN 99 | 172.17.99.11 | 255.255.255.0 | N/A |
| S2 | VLAN 99 | 172.17.99.12 | 255.255.255.0 | N/A |
| S3 | VLAN 99 | 172.17.99.13 | 255.255.255.0 | N/A |
| PC1 | NIC | 172.17.10.21 | 255.255.255.0 | 172.17.10.1 |
| PC2 | NIC | 172.17.20.22 | 255.255.255.0 | 172.17.20.1 |
| PC3 | NIC | 172.17.30.23 | 255.255.255.0 | 172.17.30.1 |
| PC4 | NIC | 172.17.10.24 | 255.255.255.0 | 172.17.10.1 |
| PC5 | NIC | 172.17.20.25 | 255.255.255.0 | 172.17.20.1 |
| PC6 | NIC | 172.17.30.26 | 255.255.255.0 | 172.17.30.1 |

**Port Assignments (Switches 2 and 3)**

| **Ports** | **Assignment** | **Network** |
| --- | --- | --- |
| Fa0/1 – 0/5 | VLAN 99 – Management&Native | 172.17.99.0/24 |
| Fa0/6 – 0/10 | VLAN 30 – Guest(Default) | 172.17.30.0/24 |
| Fa0/11 – 0/17 | VLAN 10 – Faculty/Staff | 172.17.10.0/24 |
| Fa0/18 – 0/24 | VLAN 20 – Students | 172.17.20.0/24 |

Selesaikan Task berikut:

**Task 1:Perform Basic Switch Configurations**

**Lakukan konfigurasi dasar pada ke-tiga switch:**

* Konfigurasikan nama hostname switch
* Disable DNS Lookup
* Konfigurasikan EXEC mode password dari Class
* Konfigurasi password cicsco untuk koneksi console
* Konfigurasi password cisco untuk koneksi vty

Untuk menyelesaikan task di atas, lakukan langkah-langkah berikut pada semua switch:

enable  
configure terminal  
no ip domain-lookup  
enable secret class  
!  
!  
line con 0  
 password cisco  
 login  
!  
line vty 0 4  
password cisco  
login  
end  
copy running-config startup-config

Prosentasi pengerjaan 25% setelah menyelesaikan task di atas.

**Task 2: Configure and activate EthernetInterfaces**

Klik **Desktop**, pilih **IP Configuration** untuk konfigurasi Interface Ethernet **ke-enam PC** dengan IP Address dan default gateway sesuai addressing table di atas.

**Task 3: Configure VLAN on tje Switch**

**Step 1: Buat VLAN pada switch S1**

Gunakan perintah **vlan vlan-id** padamode global configuration untuk menambah VLAN pada switch S1. Ada 4 (empat) buah VLAN yang harus dikonfigurasi. Setelah membuat VLAN, anda akan masuk ke mode VLAN Configuration, dimana anda dapat memberi nama VLAN dengan perintah **vlan name**. Selengkapnya, ikuti langkah-langkah konfigurasi VLAN pada switch berikut:

S1(config)#**vlan 99**

S1(config-vlan)#**name Management&Native**

S1(config-vlan)#**exit**

S1(config)#**vlan 10**

S1(config-vlan)#**name Faculty/Staff**

S1(config-vlan)#**exit**

S1(config)#**vlan 20**

S1(config-vlan)#**name Students**

S1(config-vlan)#**exit**

S1(config)#**vlan 30**

S1(config-vlan)#**name Guest(Default)**

S1(config-vlan)#**exit**

**Step 2: Verifikasi apakah VLAN sudah selesai dibuat pada S1.**

Lakukan perintah show vlan brief untuk menampilkan VLAN yang sudah dibuat:

S1#**show vlan brief**

VLAN Name Status Ports

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

1 default active Fa0/1, Fa0/2, 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, Gi0/1

Gi0/2

10 Faculty/Staff active

20 Students active

30 Guest(Default) active

99 Management&Native active

**Step 3: Konfigurasi dan beri nama VLAN pada switch 2 dan 3**

Buatlah VLAN 10, 20, 30, dan 99 pada switch 2 menggunakan perintah step 1 di atas. Lalu periksa konfigurasi dengan perintah **show vlan brief**.

**Step 4: Tambahkan port switch pada VLAN di Switch S2 dan Switch S3**

Perhatikan table **Port Assignment** di atas. Port diberikan kepada Interface VLAN dengan menggunakan mode interface configuration, dengan perintah **switchport access vlan vlan-id**. Ikuti langkah-langkah berikut:

S2(config)#**interface fastEthernet0/6**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan** **30**

S2(config-if)#**interface fastEthernet0/11**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan 10**

S2(config-if)#**interface fastEthernet0/18**

S2(config-if)#**switchport mode access**

S2(config-if)#**switchport access vlan 20**

S2(config-if)#**end**

S2#**copy running-config startup-config**

Destination filename [startup-config]? [**enter**]

Building configuration...

[OK]

Catatan: Fa011 access VLAN akan menampilkan **incorrect**. Abaikan saja, karena anda akan memperbaikinya dalam step selanjutnya.

Catatan: Lakukan hal yang sama pada switch 3 (S3)

**Step 5: Tentukan port mana saja yang sudah ditambahkan**

Gunakan perintah **show vlan id vlan –number** pada S2 untuk melihat port mana yang diberikan pada VLAN 10.

Port berapakah yang diberikan pada VLAN 10?\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Catatan: perintah lain untuk menampilkan port VLAN:

**show vlan name** *vlan-name*

**show interfaces** **switchport**

**Step 6: Buat Manegement VLAN**

Management VLAN adalah VLAN yang anda konfigurasikan untuk dapat mengaksses kemampian manajemen dari sebuah switch. Secara default VLAN 1 akan menjadi Management VLAN. Akan tetapi menjadikan VLAN 1 sebagai management VLAN bukan pilihan yang baik. Sebaiknya anda mengkonfigurasi VLAN lain. Dalam aktifitas ini Konfigurasi VLAN 99 sebagai Management VLAN. Ikuti langkah-langkah berikut:

S1(config)#**interface vlan 99**

S1(config-if)#**ip address 172.17.99.11 255.255.255.0**

S1(config-if)#**no shutdown**

S2(config)#**interface vlan 99**

S2(config-if)#**ip address 172.17.99.12 255.255.255.0**

S2(config-if)#**no shutdown**

S3(config)#**interface vlan 99**

S3(config-if)#**ip address 172.17.99.13 255.255.255.0**

S3(config-if)#**no shutdown**

**Step 7. Konfigurasi Trunking dan Native VLAN untuk semua port trunking pada semua switch**

Trunk adalah koneksi antar switch yang memungkinkan switch dapat bertukar informasi untuk semua VLAN. Untuk konfigurasi trunk, lakukan hal berikut pada semua switch.

S1(config)#**interface fa0/1**

S1(config-if)#**switchport mode trunk**

S1(config-if)#**switchport trunk native vlan 99**

S1(config-if)#**interface fa0/2**

S1(config-if)#**switchport mode trunk**

S1(config-if)#**switchport trunk native vlan 99**

S1(config-if)#**end**

S2(config)#**interface fa0/1**

S2(config-if)#**switchport mode trunk**

S2(config-if)#**switchport trunk native vlan 99**

S2(config-if)#**end**

S3(config)#**interface fa0/2**

S3(config-if)#**switchport mode trunk**

S3(config-if)#**switchport trunk native vlan 99**

S3(config-if)#**end**

Cek konfigurasi trunk dengan perintah berikut:

S1#**show interface trunk**

Port Mode Encapsulation Status Native vlan

Fa0/1 on 802.1q trunking 99

Fa0/2 on 802.1q trunking 99

Port Vlans allowed on trunk

Fa0/1 1-1005

Fa0/2 1-1005

Port Vlans allowed and active in management domain

Fa0/1 1,10,20,30,99,1002,1003,1004,1005

Fa0/2 1,10,20,30,99,1002,1003,1004,1005

Port Vlans in spanning tree forwarding state and not pruned

Fa0/1 1,10,20,30,99,1002,1003,1004,1005

Fa0/2 1,10,20,30,99,1002,1003,1004,1005

**Step 8: Verifikasi apakah semua switch dapat saling berkomunikasi.**

Dari **S1**, ping management address dari **S2** dan **S3** seperti di bawah ini:

S1#**ping 172.17.99.12**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.12, timeout is 2 seconds:

..!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/9 ms

S1#**ping 172.17.99.13**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.17.99.13, timeout is 2 seconds:

..!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

**Step 9. Ping beberapa host dari PC2**

Ping dari PC2 ke PC1 (172.17.10.21). Apakah ping sukses?\_\_\_\_\_\_\_\_\_\_ jelaskan mengapa?

Ping dari PC2 ke swicth VLAN 99 dengan Ipaddress 172.17.99.12. Apakah ping sukses?\_\_\_\_\_\_\_\_\_ , jelaskan mengapa?

Ping dari PC2 ke PC5, apakah ping sukses?\_\_\_\_\_\_\_ Mengapa?

**Step 10. Pindahkan PC1 ke VLAN yang sama dengan PC2**.

Port yang terhubung ke PC2 (S2 Fa0/18) diberikan ke VLAN 20, dan port yang terhubung ke PC1 (S2 Fa0/11) dimasukkan ke VLAN 10. Untuk memindahkan PC1 ke VLAN 20, lakukan hal berikut:

S2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

S2(config)#**interface fastethernet 0/11**

S2(config-if)#**switchport access vlan 20**

S2(config-if)#**end**

Coba ping dari PC2 ke PC 1, apakah sukses?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Step 11. Ganti IPaddress dan network dari PC 1**

Ganti IP address PC1 menjadi 172.17.20.21. Subnet mask dan default gateway tidak perlu diganti. Coba ping lagi dari PC2 ke PC1.

Apakah ping berhasil?\_\_\_\_\_\_\_\_\_\_

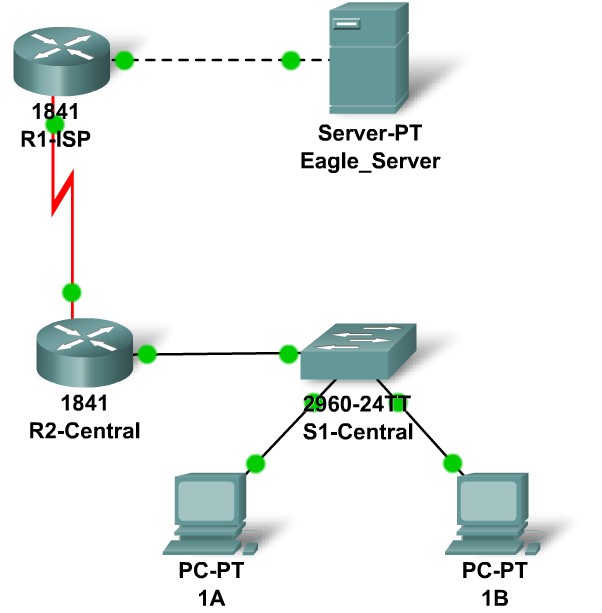
Jelaskan mengapa?\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Setelah menyelesaikan ini, prosentase penyelesaian 100%.

1. Routing IP Packet

**Buka Packet Tracer Activity Source Files: Nomor 3.5.2.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: Configure a Router Interface**

Ada beberapa masalah pada jaringan lokal: PC1A tidak bisa menjangkau Eagle Server (periksa dalam mode Realtime). Kelihatnnya masalah ada pada router. Lakukan mouse over pada router R2-Central, dan catat kondisi dari interface Fa0/0 (yang terhubung ke switch). Interface ini harus mempunyai IP address, subnet mask, dan dinyalakan supaya dapat digunakan sebagai default gateway untuk LAN.

Klik router R2-Central dan klik tab **Config**. Pada daftar yang ditampilkan, cari **INTERFACE**, **FastEthernet0/0**. Tambahkan IP address 172.16.255.254 dan subnet mask 255.255.0.0, lalu aktifkan port **On**. Tutup jendela router. Periksa interface router sekarang telah berjalan menggunakan mouse over. Cobalah sekarang untuk menjangkau Eagle Server. Akan tetapi request masih gagal. Jelaskan apa kira-kira masalahnya dan kenapa?

**Task 2: Examining Routes**

Gunakan **Inspect Tool** (magnifying glass) untuk memeriksa routing table dari router R2-Central. Anda dapat melihat jaringan yang langsung terhubung ke router, tapi tidak ada jalan untuk menjangkau jaringan Eagle Server.

**Task 3: Configure a Route Using a GUI**

Klik router R2-Central dan klik tab **Config**. Cari **ROUTING**, **Static**. Konfigurasi defaults tatic route menggunakan alamat 0.0.0.0, mask 0.0.0.0 dan hop selanjutnya (next hop) adalah 10.10.10.6 (interface S0/0/0 dari router R2-Central) dan klik tombol **Add**. Rute ini sudah dikonfigurasi bahwa kemanapun paket dari LAN 172.16.0.0/16 ditujukan, paket-paket tersebut akan pergi menuju ke router R1-ISP. Pada **GLOBAL**, **Setting**, klik tombol **Save** untuk menyimpan konfigurasi pada NVRAM. Gunakan **Inspect Tool** (magnfying glass)untuk memeriksa kembali routing table router R2-Central. Sekarang anda pasti akan melihat rute yangsudah anda konfigurasi pada routing table.

Periksa pekerjaan anda dengan klik tombol **Check Result** dan tab **Assessment Items**. Tes konekktifitas pada mode Realtime dengan menambahkan SIMPLE PDU antara PC 1A dengan Eagle Server. Seperti biasa, pingpertama akan gagal dan ulangi lagi sampai sukses.

**Task 4: Examine the Routing ofthe IP Packet**

Masuk ke Simulation mode. Menggunakan PDU yang sudah anda buatdi Task 3, telusuri perjalanan paket dari PC 1A ke Eagle Server, lalu gunakan **Capture/Forward** dan kotak berwarna pada kolom **Info**.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |

# Network Layer Functionality and Protocols

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Network dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Layer

Network Layer menyediakan layanan untuk saling bertukar kepingan-kepingan data melalui jaringan diantara end devices/hosts (end-to-end transport). Untuk menyelesaikan end-to-end transport ini, network layer menggunakan 4 proses dasar berikut:

* Addressing
* Encapsulation
* Routing
* Decapsulation

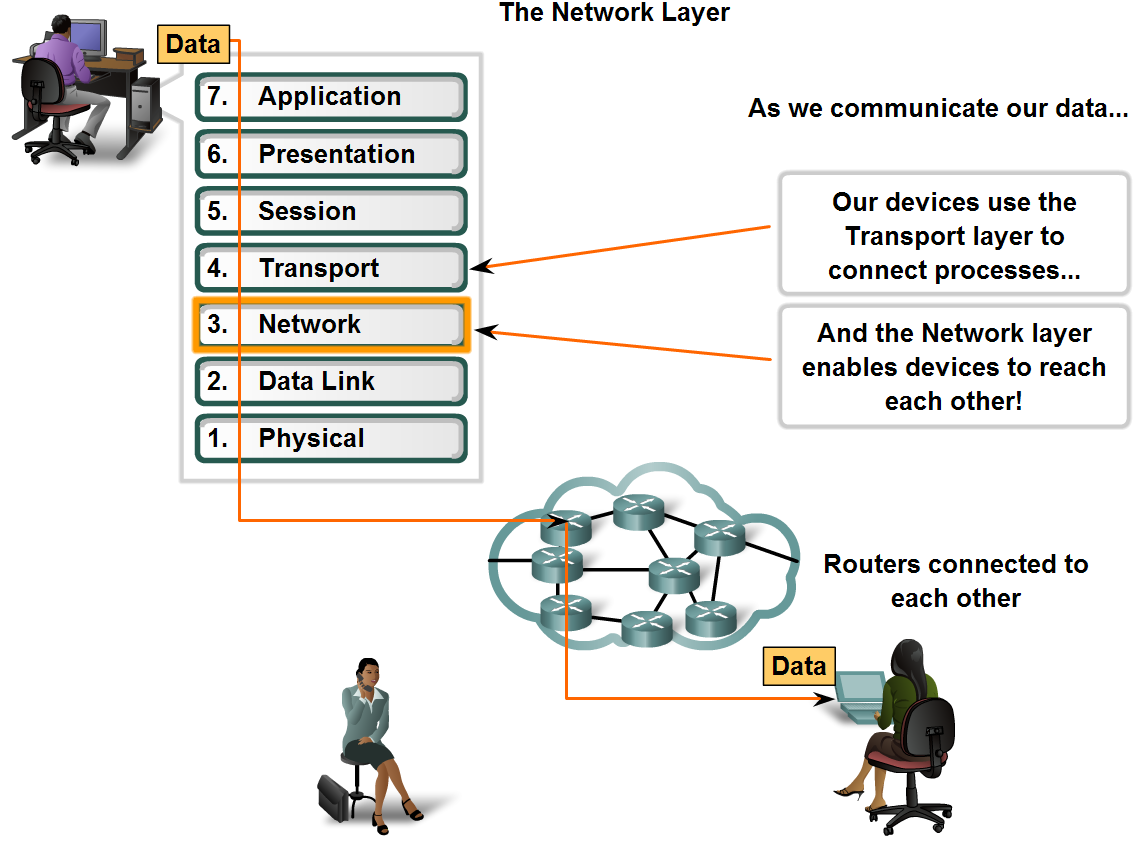


Figure 4.1 Network Layer

### Network Layer Protocols

Protokol-protokol pada Network Layer yang membawa data user adalah sebagai berikut:

* Internet Protocol version 4 (IPv4)
* Internet Protocol version 6 (IPv6)
* Novel Internetwork Packet Exchange (IPX)
* Apple Talk
* Connectionless Network Service (CLNS/DECNet)

### Separating Hosts into Common Group

Salah satu peran utama dari Network Layer adalah menyediakan mekanisme untuk pengalamatan (addressing) host. Ketika jumlah host dalam suatu jaringan semakin bertambah, perlu dilakukan perencanaan yang lebih baik dalam pengelolaan dan pengalamatan sebuah jaringan.

Pembagian jaringan ke dalam beberapa network tertentu adalah suatu hal yang lebih praktis dan mudah untuk dikelola daripada membuat semua host terhubung ke satu jaringan saja. Secara historis, sebuah jaringan yang berbasis IP memiliki asalnya adalah satu jaringan yang besar. Ketika jaringan ini bertambah besar tentunya akan menimbulkan permasalahan. Untuk menyelesaikan masalah ini, jaringan besar tersebut dapat dibagi menjadi beberapa jaringan kecil yang tetap saling terhubung. Jaringan-jaringankecil ini biasanya disebut dengan **subnetwork** atau **subnet**.

Sebuah jaringan besar dapat dibagi menjadi beberapa jaringan kecil dengan petimbangan beberapa faktor berikut:

* Geographic location (letak geografis)
* Purpose (tujuan)
* Ownership (kepemilikan)

#### Grouping hosts geographically

Kita dapat mengelompokkan hosts dari sebuah jaringan berdasarkan letak geofgrafis. Mengelompokkan host dalam lokasi yang sama seperti setiap gedung dalam sebuah kampus atau setiap lantai dalam gedung bertingkat ke dalam jaringan yang berbeda dapat meningkatkan operasional dan pengelolaan jaringan.

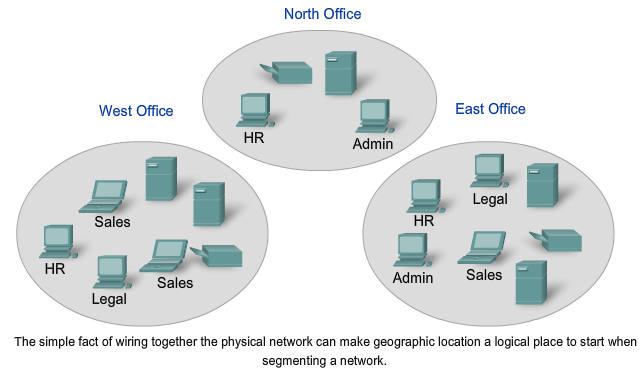


Figure 4.3 Grouping Hosts Geographically

#### Grouping hosts for specific purposes

Volume lalu lintas data dalam jaringan yang dihasilkan oleh beberapa aplikasi akan berbeda secara signifikan. Membagi jaringan berdasarkan penggunaan dapat meningkatkan efektifitas alokasi sumber daya jaringan serta pengelolaan hak aksesnya. Sebagai contoh, sebuah perusahaan mempekerjakan beberapa desainer grafis yang menggunakanjaringan untuk saling berbagi file multimedia yang berukuran sangat besar. File-file tersebut mengkonsumsi banyak bandwidth yang tersedia setiaphari. Selaiin desainer grafis, perusahaan juga mempekerjakan salesperson yang hanya login sehari sekali untuk merekam transaksi penjualan mereka. Kegiatan sales tersebut hanya menghasilkan lalu lintas jaringan yang sangat kecil.

Dalam skenario ini, untuk menghasilkan jaringan yang efektif dalam penggunaan sumberdaya jaringan, perlu dibuat beberapa jaringan kecil untuk memfasilitasi akses para desainer grafis dan sebuah jaringan yang lebih besar untuk diguakan oleh para salesperson.

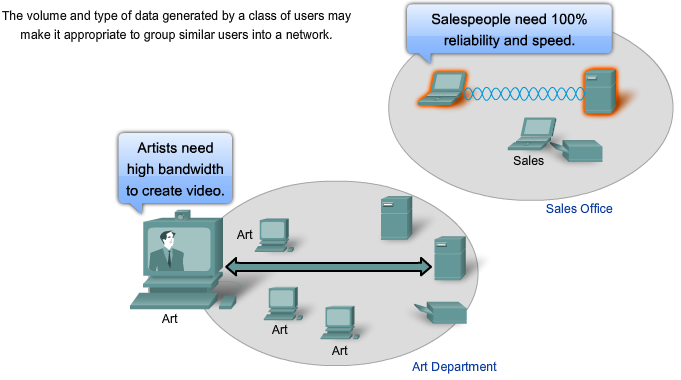


Figure 4.4 Grouping Hosts for specific purposes

#### Grouping hosts for ownership

Menggunakan basis organisasi (perusahaan, departemen, dll) untuk membuat sebuah jaringan akan membantu dalam mengendalikan akses terhadap perangkat dan data serta admnistrasi jaringan. Dalam satu jaringan yang besar akan lebih sulit untuk mendefinisikan dan membatasi tanggung jawab dari setiap personal yang terhubung dan memiliki akses ke jaringan. Dengan membagi host ke dalam beberapa jaringan akan membuat sebuah batasan untuk penerapan keamanan dan pengelolaan setiap jaringan.

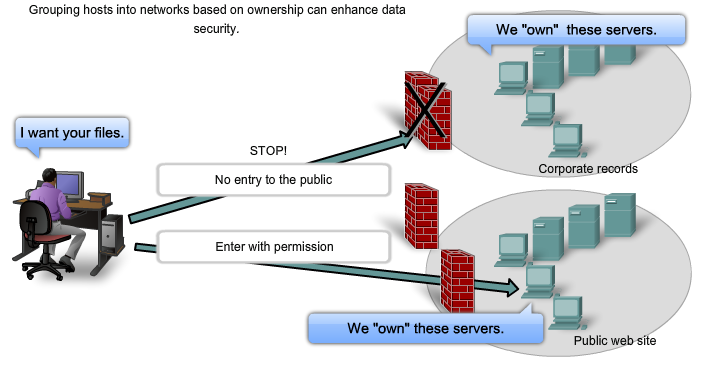


Figure 4.5. Grouping hosts for ownership

### A Gateway – The Way Out of Our Network

Gateway, atau lebih dikenal dengan default gateway, diperlukan untuk mengirim paket ke jaringan yang berada diluar jaringan lokal. Jika bagian jaringan (Network Portion) dari alamat paket yang dituju berbeda dengan jaringan pengirim, paket tersebut harus di-routing keluar dari jaringan asalnya. Untuk melakukan hal ini, paket tersebut dikirimkan ke gateway. Gateway ini biasanya merupakan sebuah port interface router yang terhubung ke jaringan lokal. Interface gateway tersebut memiliki amalat jaringan yang sama dengan alamat jaringan dari host yang terhubung ke router tersebut. Dengan demikian, host harus dikonfigurasi untuk mengenali alamat tersebut sebagai gateway.

Default gateway dikonfigurasi pada komputer/host. Pada komputer berbasis Windows, Properties dari Internet Protocol (TCP/IP) digunakan untuk memasukkan alamat IP default gateway. Baik IP address pada host maupun IP address gateway harus mempunyai porsi network (network portion) yang sama (dan subnet, jika digunakan) pada IP address mereka.

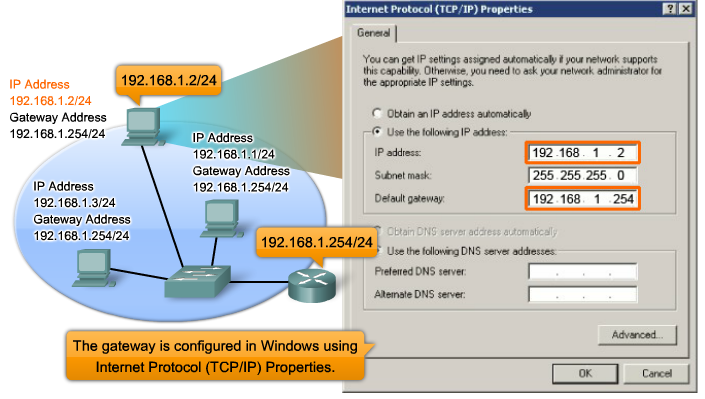


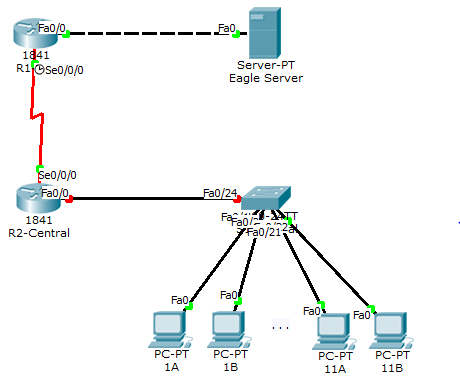
Figure 4.6 Default Gateway in Windows Properties

## Latihan

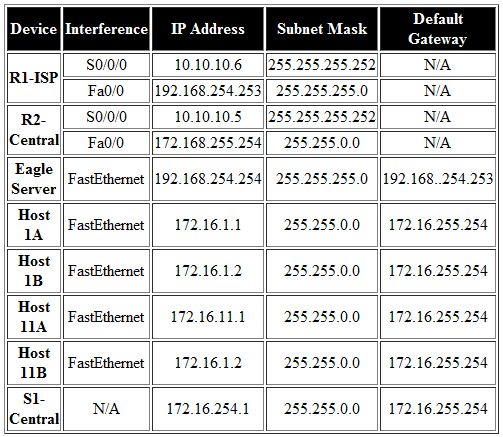
1. Examining a Device’s Gateway

**Buka Packet Tracer Activity Source Files: Nomor 5.5.1.2.pka**

Diagram Topology



Addressing Table



Selesaikan Task berikut:

**Task 1: Understand and Explain the Purpose of a Gateway Address**

Step 1: Masuk ke command prompt

Klik PC 1A, masuk ke comman prompt, ketik ipconfig

Step 2: ping ke IP Address 127.0.0.1

Periksa apakah ping berhasil?

Step 3: Kemudian ping ke IP address lain yang satu network dengan 127.0.0.1, misalkan 127.10.1.1 dan 127.255.255.255

Periksa apakah respon dari komputertujuan sukses?? Apabila tidak jelaskan mengapa?

Task 2: Understand how Network Information is Configured

Biasanya permasalahan konektifitas adalah karena kesalahan dari setting jaringan. Adabeberapa tools yang dapat digunakan untuk melakukan troubleshooting konektifitas.

Step 1: Periksa properties dari IP address jaringan

Klik PC🡪 Desktop🡪 IP Configuration

Atau bisa jugamenggunakan perintah **ipconfig**

Klik PC🡪 Desktop🡪Command Prompt

Lalu ketik **ipconfig** atau **ipconfig /all**

**Task 3: Troubleshoot a Hidden Gateway Address Problem**

**Skenario**

Sebagai seorang Cisco Engineer helpdesk, anda diminta untuk membantu teknisi help desk. Teknisi tersebut menerima trouble ticket dariseoranguser pada komputer host-1A yang komplain bahwa komputer host-11B yaitu **host-11B.example.com** tidak merespon ping. Teknisi tersebut lalu memeriksa kabel dan setting network pada kedua komputer tersebut, namun tidak ada masalah yang ditemukan. Kemudian Anda melakukan crosscek terhadap Network Engineer perusahaan yang melaporkan bahwa router R2-Central iuntuk sementara dimatikan karena ada proses upgrade hardware. Sekarang Anda sudah mengerti permasalahannya, kemudian Anda meminta kepada teknisi untuk melakukan ping ke IP address dari host-11B yaitu 172.16.11.2 dari host-1A. Ping direspon dengan sukses. Lalu Anda meminta teknisi untuk ping ke IP address Gateway yaitu 172.16.254.254, dan hasil dari ping gagal.

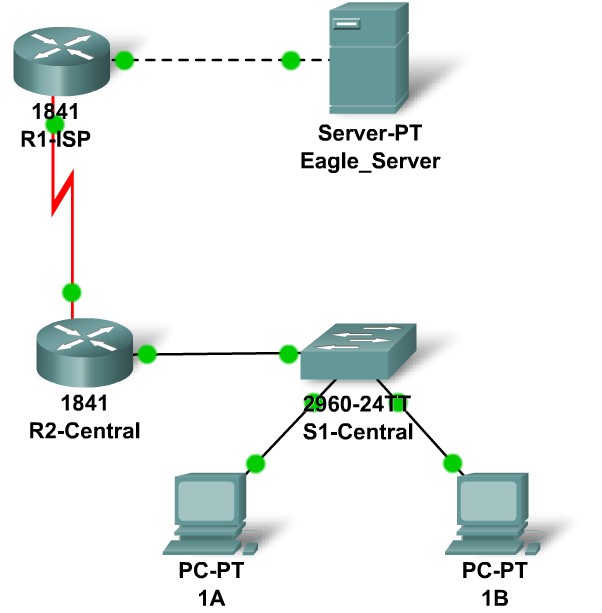
Tugas Anda adalah mencari dan memperbaiki masalah yang terjadipada jaringan Anda.

Jelaskan apa masalahnya, dan bagaimana cara memperbaikinya??

1. Routing IP Packet

**Buka Packet Tracer Activity Source Files: Nomor 4.6.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: Configure a Router Interface**

Ada beberapa masalah pada jaringan lokal: PC1A tidak bisa menjangkau Eagle Server (periksa dalam mode Realtime). Kelihatnnya masalah ada pada router. Lakukan mouse over pada router R2-Central, dan catat kondisi dari interface Fa0/0 (yang terhubung ke switch). Interface ini harus mempunyai IP address, subnet mask, dan dinyalakan supaya dapat digunakan sebagai default gateway untuk LAN.

Klik router R2-Central dan klik tab **Config**. Pada daftar yang ditampilkan, cari **INTERFACE**, **FastEthernet0/0**. Tambahkan IP address 172.16.255.254 dan subnet mask 255.255.0.0, lalu aktifkan port **On**. Tutup jendela router. Periksa interface router sekarang telah berjalan menggunakan mouse over. Cobalah sekarang untuk menjangkau Eagle Server. Akan tetapi request masih gagal. Jelaskan apa kira-kira masalahnya dan kenapa?

**Task 2: Examining Routes**

Gunakan **Inspect Tool** (magnifying glass) untuk memeriksa routing table dari router R2-Central. Anda dapat melihat jaringan yang langsung terhubung ke router, tapi tidak ada jalan untuk menjangkau jaringan Eagle Server.

**Task 3: Configure a Route Using a GUI**

Klik router R2-Central dan klik tab **Config**. Cari **ROUTING**, **Static**. Konfigurasi defaults tatic route menggunakan alamat 0.0.0.0, mask 0.0.0.0 dan hop selanjutnya (next hop) adalah 10.10.10.6 (interface S0/0/0 dari router R2-Central) dan klik tombol **Add**. Rute ini sudah dikonfigurasi bahwa kemanapun paket dari LAN 172.16.0.0/16 ditujukan, paket-paket tersebut akan pergi menuju ke router R1-ISP. Pada **GLOBAL**, **Setting**, klik tombol **Save** untuk menyimpan konfigurasi pada NVRAM. Gunakan **Inspect Tool** (magnfying glass)untuk memeriksa kembali routing table router R2-Central. Sekarang anda pasti akan melihat rute yangsudah anda konfigurasi pada routing table.

Periksa pekerjaan anda dengan klik tombol **Check Result** dan tab **Assessment Items**. Tes konekktifitas pada mode Realtime dengan menambahkan SIMPLE PDU antara PC 1A dengan Eagle Server. Seperti biasa, pingpertama akan gagal dan ulangi lagi sampai sukses.

**Task 4: Examine the Routing ofthe IP Packet**

Masuk ke Simulation mode. Menggunakan PDU yang sudah anda buatdi Task 3, telusuri perjalanan paket dari PC 1A ke Eagle Server, lalu gunakan **Capture/Forward** dan kotak berwarna pada kolom **Info**.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |

# Network Layer Functionality and Protocols

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Network dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Layer

Network Layer menyediakan layanan untuk saling bertukar kepingan-kepingan data melalui jaringan diantara end devices/hosts (end-to-end transport). Untuk menyelesaikan end-to-end transport ini, network layer menggunakan 4 proses dasar berikut:

* Addressing
* Encapsulation
* Routing
* Decapsulation

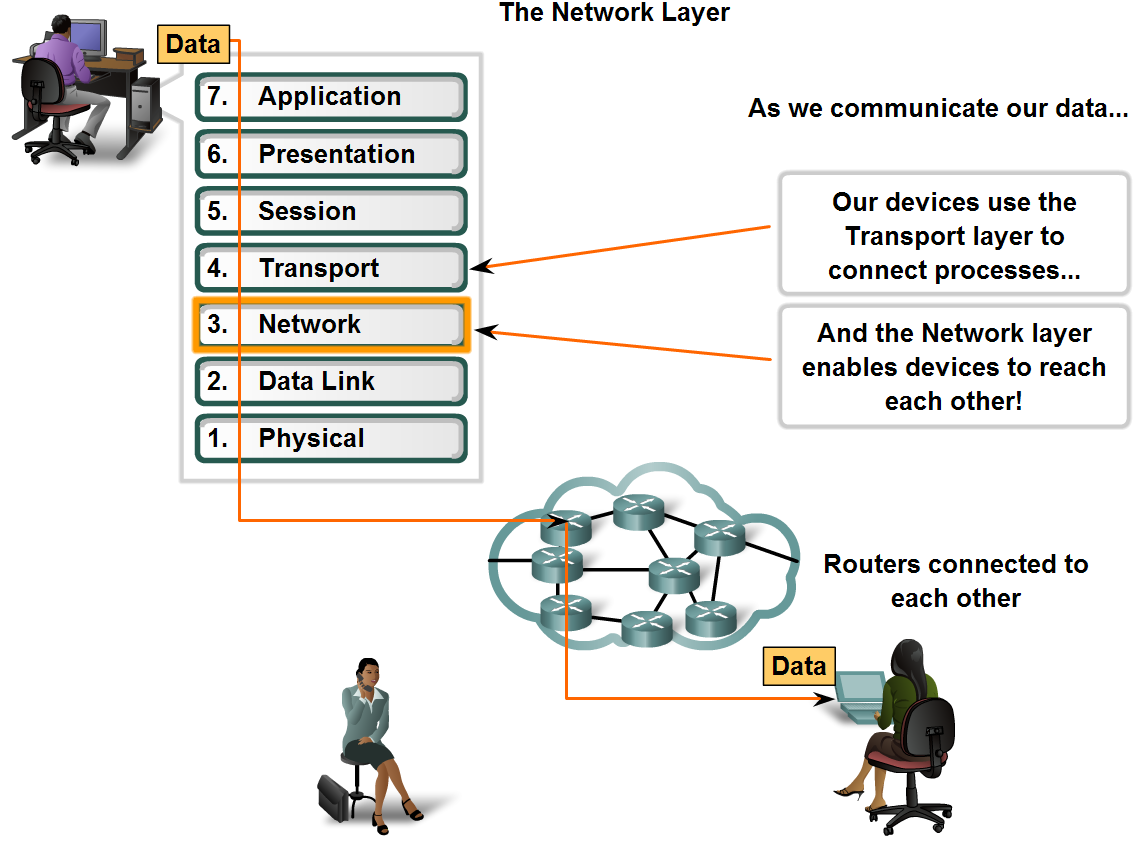


Figure 4.1 Network Layer

### Network Layer Protocols

Protokol-protokol pada Network Layer yang membawa data user adalah sebagai berikut:

* Internet Protocol version 4 (IPv4)
* Internet Protocol version 6 (IPv6)
* Novel Internetwork Packet Exchange (IPX)
* Apple Talk
* Connectionless Network Service (CLNS/DECNet)

### Separating Hosts into Common Group

Salah satu peran utama dari Network Layer adalah menyediakan mekanisme untuk pengalamatan (addressing) host. Ketika jumlah host dalam suatu jaringan semakin bertambah, perlu dilakukan perencanaan yang lebih baik dalam pengelolaan dan pengalamatan sebuah jaringan.

Pembagian jaringan ke dalam beberapa network tertentu adalah suatu hal yang lebih praktis dan mudah untuk dikelola daripada membuat semua host terhubung ke satu jaringan saja. Secara historis, sebuah jaringan yang berbasis IP memiliki asalnya adalah satu jaringan yang besar. Ketika jaringan ini bertambah besar tentunya akan menimbulkan permasalahan. Untuk menyelesaikan masalah ini, jaringan besar tersebut dapat dibagi menjadi beberapa jaringan kecil yang tetap saling terhubung. Jaringan-jaringankecil ini biasanya disebut dengan **subnetwork** atau **subnet**.

Sebuah jaringan besar dapat dibagi menjadi beberapa jaringan kecil dengan petimbangan beberapa faktor berikut:

* Geographic location (letak geografis)
* Purpose (tujuan)
* Ownership (kepemilikan)

#### Grouping hosts geographically

Kita dapat mengelompokkan hosts dari sebuah jaringan berdasarkan letak geofgrafis. Mengelompokkan host dalam lokasi yang sama seperti setiap gedung dalam sebuah kampus atau setiap lantai dalam gedung bertingkat ke dalam jaringan yang berbeda dapat meningkatkan operasional dan pengelolaan jaringan.

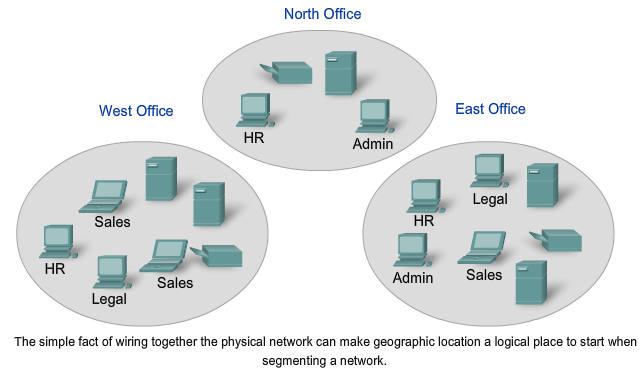


Figure 4.3 Grouping Hosts Geographically

#### Grouping hosts for specific purposes

Volume lalu lintas data dalam jaringan yang dihasilkan oleh beberapa aplikasi akan berbeda secara signifikan. Membagi jaringan berdasarkan penggunaan dapat meningkatkan efektifitas alokasi sumber daya jaringan serta pengelolaan hak aksesnya. Sebagai contoh, sebuah perusahaan mempekerjakan beberapa desainer grafis yang menggunakanjaringan untuk saling berbagi file multimedia yang berukuran sangat besar. File-file tersebut mengkonsumsi banyak bandwidth yang tersedia setiaphari. Selaiin desainer grafis, perusahaan juga mempekerjakan salesperson yang hanya login sehari sekali untuk merekam transaksi penjualan mereka. Kegiatan sales tersebut hanya menghasilkan lalu lintas jaringan yang sangat kecil.

Dalam skenario ini, untuk menghasilkan jaringan yang efektif dalam penggunaan sumberdaya jaringan, perlu dibuat beberapa jaringan kecil untuk memfasilitasi akses para desainer grafis dan sebuah jaringan yang lebih besar untuk diguakan oleh para salesperson.

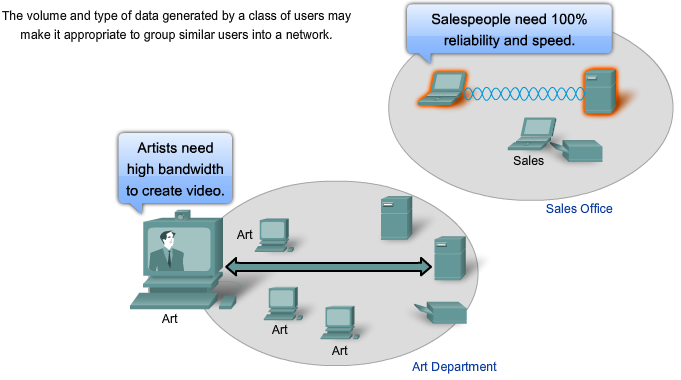


Figure 4.4 Grouping Hosts for specific purposes

#### Grouping hosts for ownership

Menggunakan basis organisasi (perusahaan, departemen, dll) untuk membuat sebuah jaringan akan membantu dalam mengendalikan akses terhadap perangkat dan data serta admnistrasi jaringan. Dalam satu jaringan yang besar akan lebih sulit untuk mendefinisikan dan membatasi tanggung jawab dari setiap personal yang terhubung dan memiliki akses ke jaringan. Dengan membagi host ke dalam beberapa jaringan akan membuat sebuah batasan untuk penerapan keamanan dan pengelolaan setiap jaringan.

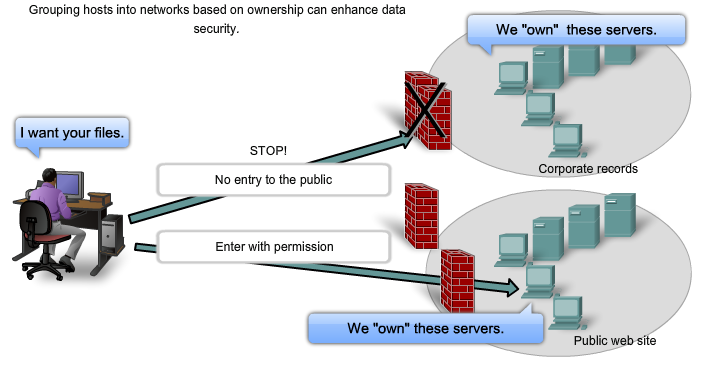


Figure 4.5. Grouping hosts for ownership

### A Gateway – The Way Out of Our Network

Gateway, atau lebih dikenal dengan default gateway, diperlukan untuk mengirim paket ke jaringan yang berada diluar jaringan lokal. Jika bagian jaringan (Network Portion) dari alamat paket yang dituju berbeda dengan jaringan pengirim, paket tersebut harus di-routing keluar dari jaringan asalnya. Untuk melakukan hal ini, paket tersebut dikirimkan ke gateway. Gateway ini biasanya merupakan sebuah port interface router yang terhubung ke jaringan lokal. Interface gateway tersebut memiliki amalat jaringan yang sama dengan alamat jaringan dari host yang terhubung ke router tersebut. Dengan demikian, host harus dikonfigurasi untuk mengenali alamat tersebut sebagai gateway.

Default gateway dikonfigurasi pada komputer/host. Pada komputer berbasis Windows, Properties dari Internet Protocol (TCP/IP) digunakan untuk memasukkan alamat IP default gateway. Baik IP address pada host maupun IP address gateway harus mempunyai porsi network (network portion) yang sama (dan subnet, jika digunakan) pada IP address mereka.

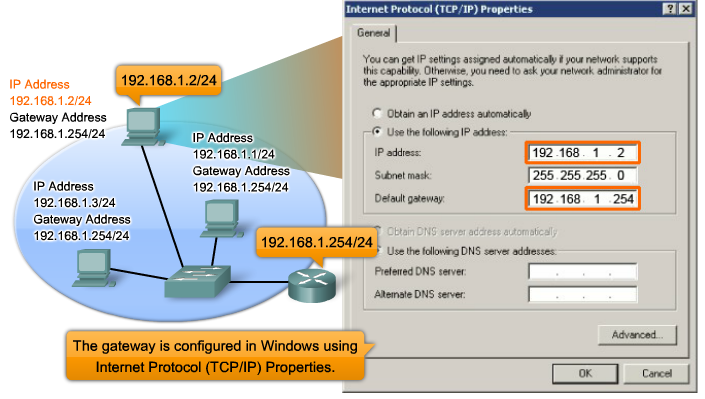


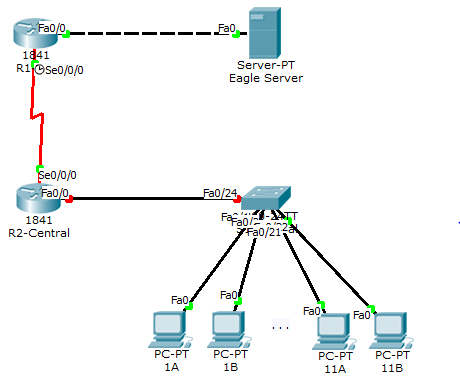
Figure 4.6 Default Gateway in Windows Properties

## Latihan

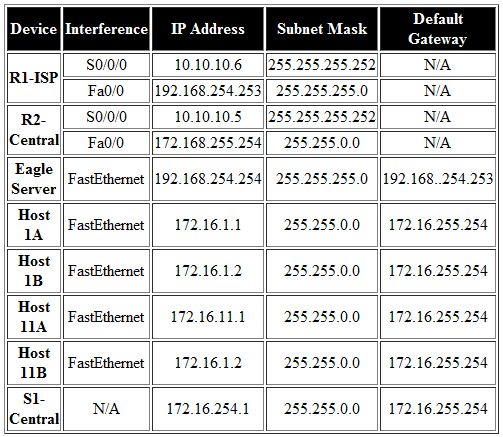
1. Examining a Device’s Gateway

**Buka Packet Tracer Activity Source Files: Nomor 5.5.1.2.pka**

Diagram Topology



Addressing Table



Selesaikan Task berikut:

**Task 1: Understand and Explain the Purpose of a Gateway Address**

Step 1: Masuk ke command prompt

Klik PC 1A, masuk ke comman prompt, ketik ipconfig

Step 2: ping ke IP Address 127.0.0.1

Periksa apakah ping berhasil?

Step 3: Kemudian ping ke IP address lain yang satu network dengan 127.0.0.1, misalkan 127.10.1.1 dan 127.255.255.255

Periksa apakah respon dari komputertujuan sukses?? Apabila tidak jelaskan mengapa?

Task 2: Understand how Network Information is Configured

Biasanya permasalahan konektifitas adalah karena kesalahan dari setting jaringan. Adabeberapa tools yang dapat digunakan untuk melakukan troubleshooting konektifitas.

Step 1: Periksa properties dari IP address jaringan

Klik PC🡪 Desktop🡪 IP Configuration

Atau bisa jugamenggunakan perintah **ipconfig**

Klik PC🡪 Desktop🡪Command Prompt

Lalu ketik **ipconfig** atau **ipconfig /all**

**Task 3: Troubleshoot a Hidden Gateway Address Problem**

**Skenario**

Sebagai seorang Cisco Engineer helpdesk, anda diminta untuk membantu teknisi help desk. Teknisi tersebut menerima trouble ticket dariseoranguser pada komputer host-1A yang komplain bahwa komputer host-11B yaitu **host-11B.example.com** tidak merespon ping. Teknisi tersebut lalu memeriksa kabel dan setting network pada kedua komputer tersebut, namun tidak ada masalah yang ditemukan. Kemudian Anda melakukan crosscek terhadap Network Engineer perusahaan yang melaporkan bahwa router R2-Central iuntuk sementara dimatikan karena ada proses upgrade hardware. Sekarang Anda sudah mengerti permasalahannya, kemudian Anda meminta kepada teknisi untuk melakukan ping ke IP address dari host-11B yaitu 172.16.11.2 dari host-1A. Ping direspon dengan sukses. Lalu Anda meminta teknisi untuk ping ke IP address Gateway yaitu 172.16.254.254, dan hasil dari ping gagal.

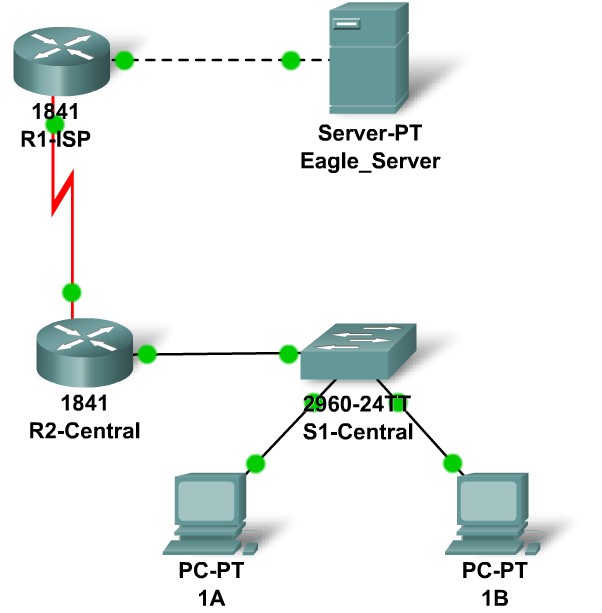
Tugas Anda adalah mencari dan memperbaiki masalah yang terjadipada jaringan Anda.

Jelaskan apa masalahnya, dan bagaimana cara memperbaikinya??

1. Routing IP Packet

**Buka Packet Tracer Activity Source Files: Nomor 4.6.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: Configure a Router Interface**

Ada beberapa masalah pada jaringan lokal: PC1A tidak bisa menjangkau Eagle Server (periksa dalam mode Realtime). Kelihatnnya masalah ada pada router. Lakukan mouse over pada router R2-Central, dan catat kondisi dari interface Fa0/0 (yang terhubung ke switch). Interface ini harus mempunyai IP address, subnet mask, dan dinyalakan supaya dapat digunakan sebagai default gateway untuk LAN.

Klik router R2-Central dan klik tab **Config**. Pada daftar yang ditampilkan, cari **INTERFACE**, **FastEthernet0/0**. Tambahkan IP address 172.16.255.254 dan subnet mask 255.255.0.0, lalu aktifkan port **On**. Tutup jendela router. Periksa interface router sekarang telah berjalan menggunakan mouse over. Cobalah sekarang untuk menjangkau Eagle Server. Akan tetapi request masih gagal. Jelaskan apa kira-kira masalahnya dan kenapa?

**Task 2: Examining Routes**

Gunakan **Inspect Tool** (magnifying glass) untuk memeriksa routing table dari router R2-Central. Anda dapat melihat jaringan yang langsung terhubung ke router, tapi tidak ada jalan untuk menjangkau jaringan Eagle Server.

**Task 3: Configure a Route Using a GUI**

Klik router R2-Central dan klik tab **Config**. Cari **ROUTING**, **Static**. Konfigurasi defaults tatic route menggunakan alamat 0.0.0.0, mask 0.0.0.0 dan hop selanjutnya (next hop) adalah 10.10.10.6 (interface S0/0/0 dari router R2-Central) dan klik tombol **Add**. Rute ini sudah dikonfigurasi bahwa kemanapun paket dari LAN 172.16.0.0/16 ditujukan, paket-paket tersebut akan pergi menuju ke router R1-ISP. Pada **GLOBAL**, **Setting**, klik tombol **Save** untuk menyimpan konfigurasi pada NVRAM. Gunakan **Inspect Tool** (magnfying glass)untuk memeriksa kembali routing table router R2-Central. Sekarang anda pasti akan melihat rute yangsudah anda konfigurasi pada routing table.

Periksa pekerjaan anda dengan klik tombol **Check Result** dan tab **Assessment Items**. Tes konekktifitas pada mode Realtime dengan menambahkan SIMPLE PDU antara PC 1A dengan Eagle Server. Seperti biasa, pingpertama akan gagal dan ulangi lagi sampai sukses.

**Task 4: Examine the Routing ofthe IP Packet**

Masuk ke Simulation mode. Menggunakan PDU yang sudah anda buatdi Task 3, telusuri perjalanan paket dari PC 1A ke Eagle Server, lalu gunakan **Capture/Forward** dan kotak berwarna pada kolom **Info**.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |

# Assesment 2

## Tujuan

Setelah mengikuti praktikum ini mahasiswa diharapkan dapat:

1. Memahami Fungsi Layer Network dan Protokolnya
2. Mampu melakukan konfigurasi DNS dan HTTP Server

## Alat & Bahan

Alat & Bahan Yang digunakan adalah hardware perangkat PC beserta Kelengkapannya berjumlah 40 PC serta Software Packet Tracer yang telah terinstall pada masing-masing PC dan setiap PC terhubung Internet.

## Dasar Teori

### Network Layer

Network Layer menyediakan layanan untuk saling bertukar kepingan-kepingan data melalui jaringan diantara end devices/hosts (end-to-end transport). Untuk menyelesaikan end-to-end transport ini, network layer menggunakan 4 proses dasar berikut:

* Addressing
* Encapsulation
* Routing
* Decapsulation

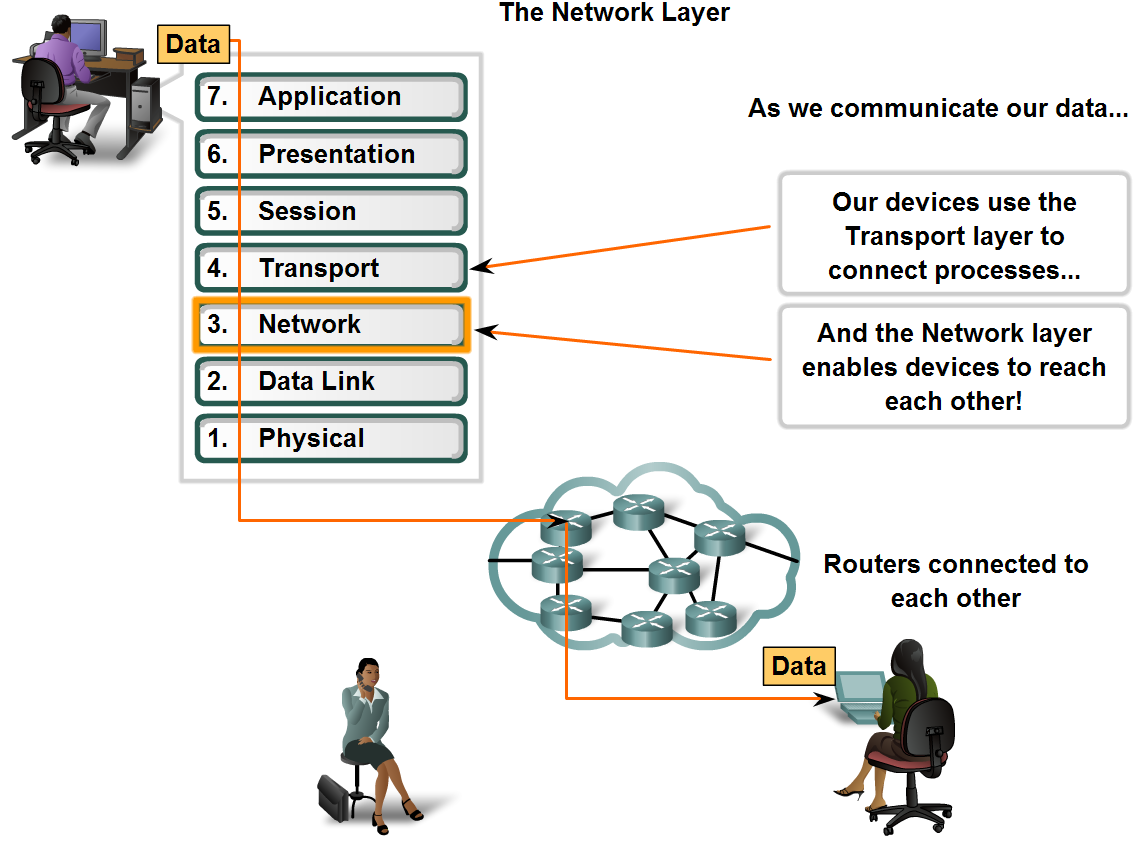


Figure 4.1 Network Layer

### Network Layer Protocols

Protokol-protokol pada Network Layer yang membawa data user adalah sebagai berikut:

* Internet Protocol version 4 (IPv4)
* Internet Protocol version 6 (IPv6)
* Novel Internetwork Packet Exchange (IPX)
* Apple Talk
* Connectionless Network Service (CLNS/DECNet)

### Separating Hosts into Common Group

Salah satu peran utama dari Network Layer adalah menyediakan mekanisme untuk pengalamatan (addressing) host. Ketika jumlah host dalam suatu jaringan semakin bertambah, perlu dilakukan perencanaan yang lebih baik dalam pengelolaan dan pengalamatan sebuah jaringan.

Pembagian jaringan ke dalam beberapa network tertentu adalah suatu hal yang lebih praktis dan mudah untuk dikelola daripada membuat semua host terhubung ke satu jaringan saja. Secara historis, sebuah jaringan yang berbasis IP memiliki asalnya adalah satu jaringan yang besar. Ketika jaringan ini bertambah besar tentunya akan menimbulkan permasalahan. Untuk menyelesaikan masalah ini, jaringan besar tersebut dapat dibagi menjadi beberapa jaringan kecil yang tetap saling terhubung. Jaringan-jaringankecil ini biasanya disebut dengan **subnetwork** atau **subnet**.

Sebuah jaringan besar dapat dibagi menjadi beberapa jaringan kecil dengan petimbangan beberapa faktor berikut:

* Geographic location (letak geografis)
* Purpose (tujuan)
* Ownership (kepemilikan)

#### Grouping hosts geographically

Kita dapat mengelompokkan hosts dari sebuah jaringan berdasarkan letak geofgrafis. Mengelompokkan host dalam lokasi yang sama seperti setiap gedung dalam sebuah kampus atau setiap lantai dalam gedung bertingkat ke dalam jaringan yang berbeda dapat meningkatkan operasional dan pengelolaan jaringan.

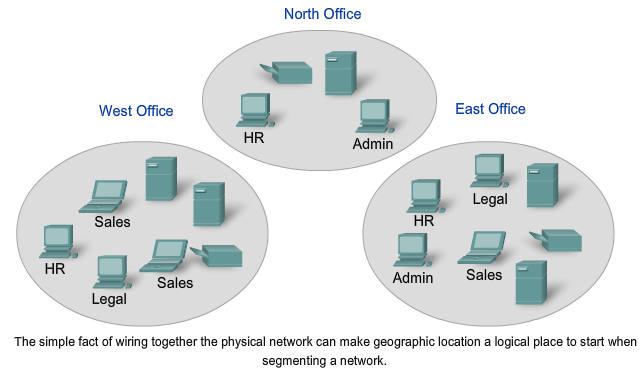


Figure 4.3 Grouping Hosts Geographically

#### Grouping hosts for specific purposes

Volume lalu lintas data dalam jaringan yang dihasilkan oleh beberapa aplikasi akan berbeda secara signifikan. Membagi jaringan berdasarkan penggunaan dapat meningkatkan efektifitas alokasi sumber daya jaringan serta pengelolaan hak aksesnya. Sebagai contoh, sebuah perusahaan mempekerjakan beberapa desainer grafis yang menggunakanjaringan untuk saling berbagi file multimedia yang berukuran sangat besar. File-file tersebut mengkonsumsi banyak bandwidth yang tersedia setiaphari. Selaiin desainer grafis, perusahaan juga mempekerjakan salesperson yang hanya login sehari sekali untuk merekam transaksi penjualan mereka. Kegiatan sales tersebut hanya menghasilkan lalu lintas jaringan yang sangat kecil.

Dalam skenario ini, untuk menghasilkan jaringan yang efektif dalam penggunaan sumberdaya jaringan, perlu dibuat beberapa jaringan kecil untuk memfasilitasi akses para desainer grafis dan sebuah jaringan yang lebih besar untuk diguakan oleh para salesperson.

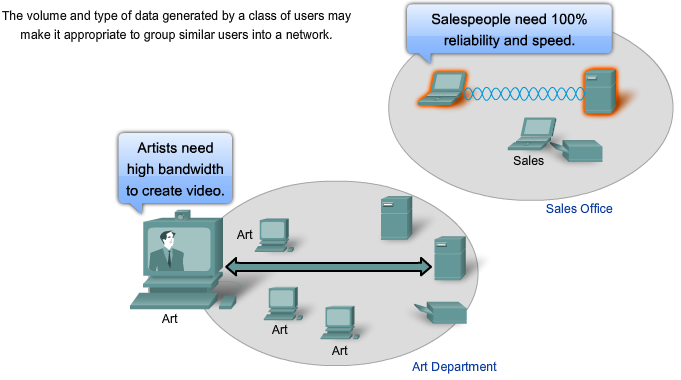


Figure 4.4 Grouping Hosts for specific purposes

#### Grouping hosts for ownership

Menggunakan basis organisasi (perusahaan, departemen, dll) untuk membuat sebuah jaringan akan membantu dalam mengendalikan akses terhadap perangkat dan data serta admnistrasi jaringan. Dalam satu jaringan yang besar akan lebih sulit untuk mendefinisikan dan membatasi tanggung jawab dari setiap personal yang terhubung dan memiliki akses ke jaringan. Dengan membagi host ke dalam beberapa jaringan akan membuat sebuah batasan untuk penerapan keamanan dan pengelolaan setiap jaringan.

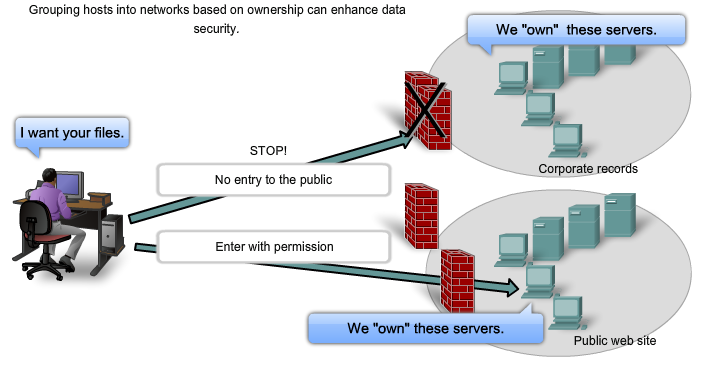


Figure 4.5. Grouping hosts for ownership

### A Gateway – The Way Out of Our Network

Gateway, atau lebih dikenal dengan default gateway, diperlukan untuk mengirim paket ke jaringan yang berada diluar jaringan lokal. Jika bagian jaringan (Network Portion) dari alamat paket yang dituju berbeda dengan jaringan pengirim, paket tersebut harus di-routing keluar dari jaringan asalnya. Untuk melakukan hal ini, paket tersebut dikirimkan ke gateway. Gateway ini biasanya merupakan sebuah port interface router yang terhubung ke jaringan lokal. Interface gateway tersebut memiliki amalat jaringan yang sama dengan alamat jaringan dari host yang terhubung ke router tersebut. Dengan demikian, host harus dikonfigurasi untuk mengenali alamat tersebut sebagai gateway.

Default gateway dikonfigurasi pada komputer/host. Pada komputer berbasis Windows, Properties dari Internet Protocol (TCP/IP) digunakan untuk memasukkan alamat IP default gateway. Baik IP address pada host maupun IP address gateway harus mempunyai porsi network (network portion) yang sama (dan subnet, jika digunakan) pada IP address mereka.

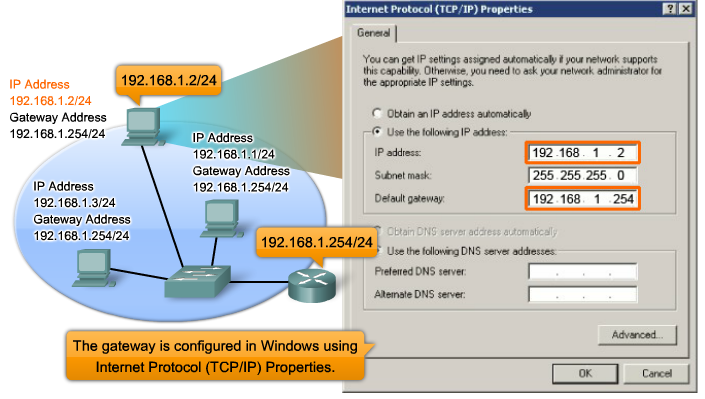


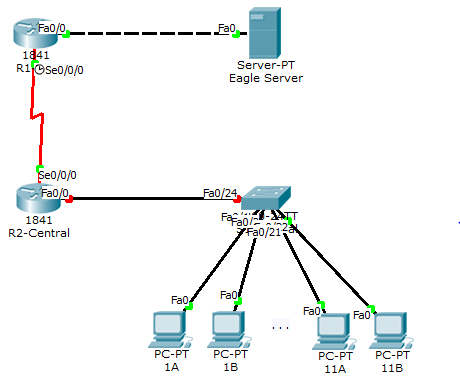
Figure 4.6 Default Gateway in Windows Properties

## Latihan

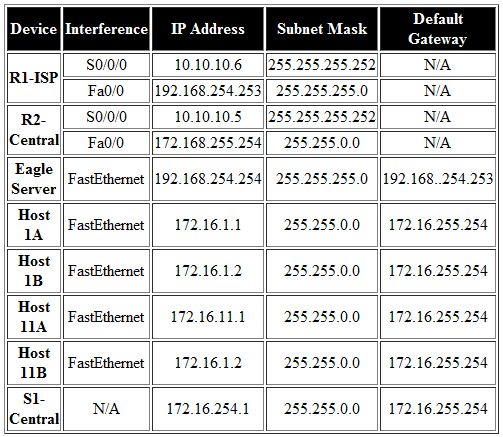
1. Examining a Device’s Gateway

**Buka Packet Tracer Activity Source Files: Nomor 5.5.1.2.pka**

Diagram Topology



Addressing Table



Selesaikan Task berikut:

**Task 1: Understand and Explain the Purpose of a Gateway Address**

Step 1: Masuk ke command prompt

Klik PC 1A, masuk ke comman prompt, ketik ipconfig

Step 2: ping ke IP Address 127.0.0.1

Periksa apakah ping berhasil?

Step 3: Kemudian ping ke IP address lain yang satu network dengan 127.0.0.1, misalkan 127.10.1.1 dan 127.255.255.255

Periksa apakah respon dari komputertujuan sukses?? Apabila tidak jelaskan mengapa?

Task 2: Understand how Network Information is Configured

Biasanya permasalahan konektifitas adalah karena kesalahan dari setting jaringan. Adabeberapa tools yang dapat digunakan untuk melakukan troubleshooting konektifitas.

Step 1: Periksa properties dari IP address jaringan

Klik PC🡪 Desktop🡪 IP Configuration

Atau bisa jugamenggunakan perintah **ipconfig**

Klik PC🡪 Desktop🡪Command Prompt

Lalu ketik **ipconfig** atau **ipconfig /all**

**Task 3: Troubleshoot a Hidden Gateway Address Problem**

**Skenario**

Sebagai seorang Cisco Engineer helpdesk, anda diminta untuk membantu teknisi help desk. Teknisi tersebut menerima trouble ticket dariseoranguser pada komputer host-1A yang komplain bahwa komputer host-11B yaitu **host-11B.example.com** tidak merespon ping. Teknisi tersebut lalu memeriksa kabel dan setting network pada kedua komputer tersebut, namun tidak ada masalah yang ditemukan. Kemudian Anda melakukan crosscek terhadap Network Engineer perusahaan yang melaporkan bahwa router R2-Central iuntuk sementara dimatikan karena ada proses upgrade hardware. Sekarang Anda sudah mengerti permasalahannya, kemudian Anda meminta kepada teknisi untuk melakukan ping ke IP address dari host-11B yaitu 172.16.11.2 dari host-1A. Ping direspon dengan sukses. Lalu Anda meminta teknisi untuk ping ke IP address Gateway yaitu 172.16.254.254, dan hasil dari ping gagal.

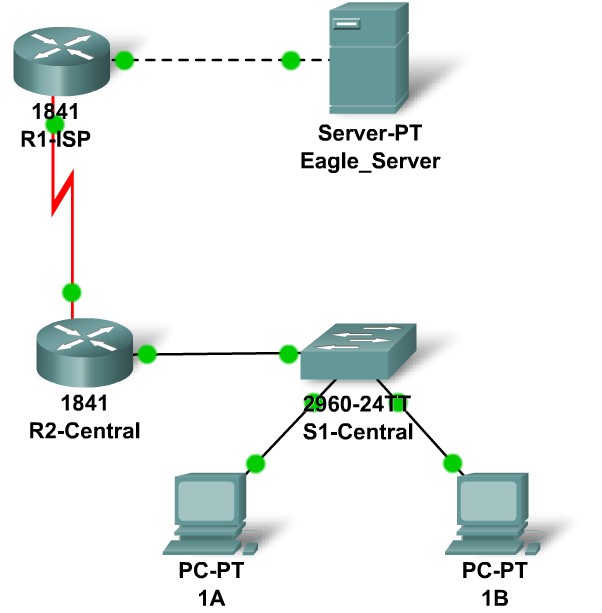
Tugas Anda adalah mencari dan memperbaiki masalah yang terjadipada jaringan Anda.

Jelaskan apa masalahnya, dan bagaimana cara memperbaikinya??

1. Routing IP Packet

**Buka Packet Tracer Activity Source Files: Nomor 4.6.1.3.pka**

Diagram Topologi



Addressing Table

| **Device** | **Interface** | **IP Address** | **Subnet Mask** | | **Default Gateway** |
| --- | --- | --- | --- | --- | --- |
| R1-ISP | Fa0/0 | **192.168.254.253** | | **255.255.255.0** | **N/A** |
| S0/0/0 | **10.10.10.6** | | **255.255.255.252** | **N/A** |
| R2-Central | Fa0/0 | **172.16.255.254** | | **255.255.0.0** | **N/A** |
| S0/0/0 | **10.10.10.5** | | **255.255.255.252** | **N/A** |
| S1-Central | VLAN 1 | 172.16.254.1 | | 255.255.0.0 | 172.16.255.254 |
| PC 1A | NIC | 172.16.1.1 | 255.255.0.0 | | 172.16.255.254 |
| PC 1B | NIC | 172.16.1.2 | 255.255.0.0 | | 172.16.255.254 |
| Eagle Server | NIC | 192.168.254.254 | 255.255.255.0 | | 192.168.254.253 |

Selesaikan Task di bawah ini:

**Task 1: Configure a Router Interface**

Ada beberapa masalah pada jaringan lokal: PC1A tidak bisa menjangkau Eagle Server (periksa dalam mode Realtime). Kelihatnnya masalah ada pada router. Lakukan mouse over pada router R2-Central, dan catat kondisi dari interface Fa0/0 (yang terhubung ke switch). Interface ini harus mempunyai IP address, subnet mask, dan dinyalakan supaya dapat digunakan sebagai default gateway untuk LAN.

Klik router R2-Central dan klik tab **Config**. Pada daftar yang ditampilkan, cari **INTERFACE**, **FastEthernet0/0**. Tambahkan IP address 172.16.255.254 dan subnet mask 255.255.0.0, lalu aktifkan port **On**. Tutup jendela router. Periksa interface router sekarang telah berjalan menggunakan mouse over. Cobalah sekarang untuk menjangkau Eagle Server. Akan tetapi request masih gagal. Jelaskan apa kira-kira masalahnya dan kenapa?

**Task 2: Examining Routes**

Gunakan **Inspect Tool** (magnifying glass) untuk memeriksa routing table dari router R2-Central. Anda dapat melihat jaringan yang langsung terhubung ke router, tapi tidak ada jalan untuk menjangkau jaringan Eagle Server.

**Task 3: Configure a Route Using a GUI**

Klik router R2-Central dan klik tab **Config**. Cari **ROUTING**, **Static**. Konfigurasi defaults tatic route menggunakan alamat 0.0.0.0, mask 0.0.0.0 dan hop selanjutnya (next hop) adalah 10.10.10.6 (interface S0/0/0 dari router R2-Central) dan klik tombol **Add**. Rute ini sudah dikonfigurasi bahwa kemanapun paket dari LAN 172.16.0.0/16 ditujukan, paket-paket tersebut akan pergi menuju ke router R1-ISP. Pada **GLOBAL**, **Setting**, klik tombol **Save** untuk menyimpan konfigurasi pada NVRAM. Gunakan **Inspect Tool** (magnfying glass)untuk memeriksa kembali routing table router R2-Central. Sekarang anda pasti akan melihat rute yangsudah anda konfigurasi pada routing table.

Periksa pekerjaan anda dengan klik tombol **Check Result** dan tab **Assessment Items**. Tes konekktifitas pada mode Realtime dengan menambahkan SIMPLE PDU antara PC 1A dengan Eagle Server. Seperti biasa, pingpertama akan gagal dan ulangi lagi sampai sukses.

**Task 4: Examine the Routing ofthe IP Packet**

Masuk ke Simulation mode. Menggunakan PDU yang sudah anda buatdi Task 3, telusuri perjalanan paket dari PC 1A ke Eagle Server, lalu gunakan **Capture/Forward** dan kotak berwarna pada kolom **Info**.

**DAFTAR PUSTAKA**

|  |
| --- |
| * Networking Academy (2015), CCNA Exploration 4.0.4.0 Network Fundamental, Cisco Networking Academy |
|  |