Kerangan :

Warna cover sesuai dengan **warna departemen**

BUKU PETUNJUK PRAKTIKUM
WORKSHOP ADMINISTRASI DAN MANAJEMEN JARINGAN
(VIT1934305)

Oleh:
Dr.Eng. Idris Winarno, S.ST., M.Kom.
NIP. 198203082008121001

Fitri Setyorini, ST., M.Sc.
NIP. 197707072001122001

PRGRAM STUDI D-III TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2019

BUKU PETUNJUK PRAKTIKUM
WORKSHOP ADMINISTRASI DAN MANAJEMEN JARINGAN
(VIT1934305)

Oleh:
Dr.Eng. Idris Winarno, S.ST., M.Kom.
NIP. 198203082008121001

Fitri Setyorini, ST., M.Sc.
NIP. 197707072001122001

PRGRAM STUDI D-III TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
2019

LEMBAR PERSETUJUAN

1. Judul Mata Kuliah : Workshop Administrasi dan Manajemen Jaringan VIT1934305 (4 jam/minggu)
2. Ketua Tim
   - Nama Lengkap : Dr.Eng. Idris Winarno, S.ST., M.Kom.
   - Jenis Kelamin : Laki-Laki
   - Golongan/Pangkat/NIP : III-d / 198203082008121001
   - Jabatan Fungsional : Lektor
   - Jabatan Struktural : -
   - Program Studi : Teknik Informatika
   - Departemen : Teknik Informatika dan Komputer

3. Anggota Tim

   A.
   - Nama Lengkap : Fitri Setyorini, ST., M.Sc.
   - Jenis Kelamin : Perempuan
   - Golongan/Pangkat/NIP : IV-a/ 196904041995121002
   - Jabatan Fungsional : Asisten Ahli
   - Jabatan Struktural : -
   - Program Studi : Teknik Informatika
   - Departemen : Teknik Informatika dan Komputer

Surabaya, 1 Juli 2019

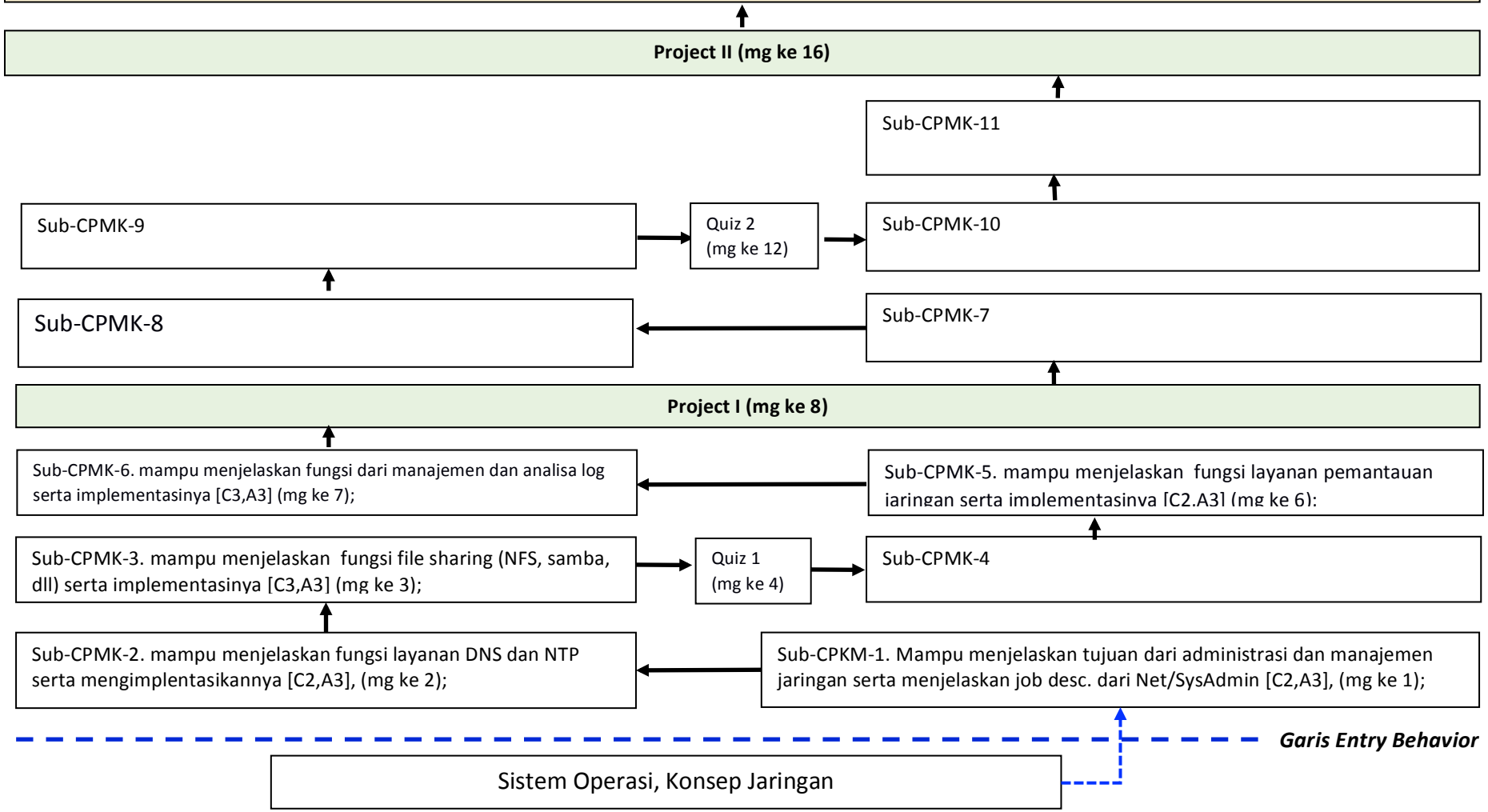
Ketua Tim Penyusun,

Dr.Eng. Idris Winarno, S.ST., M.Kom.
NIP. 198203082008121001

Mengetahui,	Menyetujui,
Kepala Departemen TIK	Kaprodi Teknik Informatika
Tri Harsono, S.Si.,M.Kom., Ph.D.	Isbat Uzzin Nadhori, S.Kom., M.T.
NIP. 196901071994031001	NIP. 197405052003121002

I. Analisis Pembelajaran

CPMK Mata Kuliah Workshop Administrasi dan Manajemen Jaringan:
Mahasiswa mampu memahami jenis layanan-layanan yang ada di jaringan serta mengembangan layanan jaringan khususnya menggunakan sistem operasi Linux dan juga mampu melakukan instalasi dan konfigurasi layanan-layanan yang dibutuhkan pada suatu sistem jaringan.



1.Rencana Pembelajaran Semester

	PROGRAM STUDI DIPLOMA 3 TEKNIK INFORMATIKA **DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER** **POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**	

RENCANA PEMBELAJARAN SEMESTER

MATA KULIAH (MK)	**KODE**	**Rumpun MK**	**BOBOT (sks)**		**SEMESTER**	**Tgl Penyusunan**
Workshop Administrasi dan Manajemen Jaringan	VIT1934305	Keilmuan Inti	T=1	P=1	4	23 - 09 - 2019
OTORISASI / PENGESAHAN	**Dosen Pengembang RPS**		**Koordinator RMK**		**Ka PRODI**	
			(Jika ada) Tanda tangan		Tanda tangan	

Capaian Pembelajaran	**CPL-PRODI yang dibebankan pada MK**	
	S7	Menginternalisasi nilai, norma, dan etika akademik.
	S8	Menunjukkan sikap bertanggungjawab atas pekerjaan di bidang keahliannya secara mandiri;
	P-2	Menguasai metode pengembangan produk TIK untuk memberikan solusi yang tepat melalui satu atau lebih domain aplikasi.
	P-3	Menguasai teknik dokumentasi dan penjaminan mutu produk TIK.
	P-4	Menguasai prinsip komputasi cerdas untuk menghasilkan alternatif solusi yang efektif.

	P-6	Menguasai pengetahuan tentang teknik berkomunikasi lisan dan tulisan menggunakan bahasa nasional dan internasional.
	P-7	Menguasai pengetahuan tentang perkembangan teknologi dan issue terkini (etika, sosial, legal dan ekonomi) terkait bidang TIK.
	KK-2	Mampu mendesain dan mengimplementasikan kebutuhan jaringan dan infrastrukturnya dalam pengembangan perangkat lunak.
	KK-3	Mampu mengidentifikasi dan menganalisis kebutuhan, merancang, merealisasikan dan melakukan pengujian produk TIK yang inovatif dan aplikatif sesuai standar yang berlaku dengan memperhatikan faktor etika, sosial, legal dan ekonomi
	KK-4	Mampu mendokumentasikan dan melakukan penjaminan mutu pada setiap proses pengembangan, penggunaan, modifikasi, pemeliharaan dan keamanan produk TIK menggunakan standar yang berlaku.
	KK-6	Mampu menggunakan teknologi terkini dan menganalisis dampak komputasi terhadap individu, organisasi dan masyarakat.
	KU-1	Mampu menerapkan pemikiran logis, kritis, inovatif, bermutu, dan terukur dalam melakukan pekerjaan yang spesifik di bidang keahliannya serta sesuai dengan standar kompetensi kerja bidang yang bersangkutan.
	KU-5	Mampu mengambil keputusan secara tepat berdasarkan prosedur baku, spesifikasi desain, persyaratan keselamatan dan keamanan kerja dalam melakukan supervisi dan evaluasi pada pekerjaannya.
	KU-7	Mampu bertanggungjawab atas pencapaian hasil kerja kelompok dan melakukan supervisi dan evaluasi terhadap penyelesaian pekerjaan yang ditugaskan kepada pekerja yang berada di bawah tanggungjawabnya.
	KU-11	Mampu berkomunikasi dengan menggunakan bahasa internasional secara lisan dan tulisan.
	Capaian Pembelajaran Mata Kuliah (CPMK)	
	CPMK	Mahasiswa mampu memahami jenis layanan-layanan yang ada di jaringan serta mengembangan layanan jaringan khususnya menggunakan sistem operasi Linux dan juga mampu melakukan instalasi dan konfigurasi layanan-layanan yang dibutuhkan pada suatu sistem jaringan.
	CPL ⇒ Sub-CPMK	
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-1. Mampu menjelaskan tujuan dari administrasi dan manajemen jaringan serta menjelaskan job desc. dari Net/SysAdmin

	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-2. mampu menjelaskan fungsi layanan DNS dan NTP serta mengimplentasikannya.
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-3. mampu menjelaskan fungsi file sharing (NFS, samba, dll) serta implementasinya.
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-4. mampu menjelaskan fungsi layanan proxy serta implementasinya.
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-5. mampu menjelaskan fungsi layanan pemantauan jaringan serta implementasinya.
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-6. mampu menjelaskan fungsi dari manajemen dan analisa log serta implementasinya.
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-7
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-8
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5,	Sub-CPMK-9

	KU-7, KU-11	
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-10
	S7, S8, P-2, P-3, P-6, P-7, KK-2, KK-3, KK-4, KK-6, KU-1, KU-5, KU-7, KU-11	Sub-CPMK-11
Diskripsi Singkat MK	Mata kuliah ini melengkapi matakuliah sebelumnya yaitu konsep jaringan, Mata kuliah ini sebagai pelengkap untuk pemahaman dari teori dan praktek yang diberikan pada mata kuliah workshop administrasi dan manajemen jaringan sehingga bisa terjadi korelasi antara teori dan praktek. Mata kuliah ini berisi aplikasi server yang umum digunakan pada server-server. Pada matakuliah ini akan dipraktekkan jenis server berbasiskan linux. Diharapkan dengan diberikannya mata kuliah ini akan mampu membekali mahasiswa pada dunia nyata yang berhubungan dengan jaringan sehingga diharapkan pula mahasiswa telah siap untuk diterjunkan ke dalam dunia industri utamanya yang berhubungan dengan jaringan komputer secara lebih luas	
Bahan Kajian: Materi pembelajaran	1. Pengenalan Administrasi dan Manajemen Jaringan 2. DNS (Domain Name System) 3. File sharing 4. Proxy/Cache Server 5. NMS (Network Monitoring System) 6. Analisis dan Manajemen log 7. (materi pembelajaran 7) 8. (materi pembelajaran 8) 9. (materi pembelajaran 9) 10. (materi pembelajaran 10) 11. (materi pembelajaran 11)	
Pustaka	**Utama:**	

	1. Kemp, Juliet. *Linux System Administration Recipes: A Problem-solution Approach*. Apress, 2009. 2. LaCroix, Jay. *Mastering Linux network administration*. Packt Publishing Ltd, 2015. 3. Nemeth, Evi, et al. *UNIX and Linux system administration handbook*. Pearson Education. 2018. **Pendukung:** 1.
Dosen Pengampu	Idris Winarno, Iwan Syarif, Isbat Uzzin N, Fitri Setyorini, Ferry A.S.
Matakuliah syarat	Sistem Operasi, Konsep Jaringan

Mg Ke-	**Sub-CPMK** **(sbg kemampuan akhir yg diharapkan)**	**Penilaian**		**Bantuk Pembelajaran;** **Metode Pembelajaran;** **Penugasan Mahasiswa;** **[Estimasi Waktu]**		**Materi Pembelajaran** **[Pustaka]**	**Bobot Penilaian (%)**
		Indikator	**Kriteria & Bentuk**				
(1)	**(2)**	**(3)**	**(4)**	**Tatap Muka (5)**	**Daring (6)**	**(7)**	**(8)**
1	Sub-CPMK-1. Mampu menjelaskan tujuan dari administrasi dan manajemen jaringan serta menjelaskan job desc. dari Net/SysAdmin [c3,a3,p2]	• Mempu menjelaskan tentang tujuan dari administrasi dan manajemen jaringan. • Mampu menjelaskan peranan *IT professional* pada sebuah organisasi. • Mampu menjelaskan jenis layanan-layanan jaringan. • Mampu menjelaskan struktur organisasi dan *job desc.* dari Net/Sys Admin	● Tanya-jawab ● Demonstrasi percobaan	● **Kuliah (Teori Pengantar)**; ● **Diskusi;** ● **Percobaan** **[TM: 2x(6x50")]**		○ Pengenalan administrasi dan manajemen jaringan ○ Peranan *IT professional* pada sebuah organisasi. ○ Evolusi jaringan internet. ○ Layanan-layanan jaringan (web, ftp, proxy, dll). ○ Struktur organisasi dan *job desc.* dari Net/Sys Admin	**10**

2	Sub-CPMK-2. mampu menjelaskan fungsi layanan DNS dan NTP serta mengimplentasikannya. [c3,a3,p2]	• Mampu menjelasan layanan DNS dan NTP. • Mampu menjelaskan *dynamic DNS.* • Mampu menginstall, mengkonfigurasi serta mengujicoba NTP server dan DNS untuk nama domain yang telah dirancang.	• Tanya-jawab • Demonstrasi percobaan	• **Kuliah (Teori Pengantar)**; • **Diskusi;** • **Percobaan** **[TM: 2x(6x50")]**		○ Struktur DNS ○ Cara kerja DNS ○ Recursive query ○ Resource record ○ Instalasi ○ Konfigurasi	**10**
3	Sub-CPMK-3. mampu menjelaskan fungsi file sharing (NFS, samba, dll) serta implementasinya. [c3,a3,p2]	• Mampu menjelaskan berbagai layanan untuk berbagi file dengan NFS dan SAMBA • Mampu menjelaskan perbedaan antara SAN dan NAS • Mampu menginstall, mengkonfigurasi serta mengujicoba file sharing dengan membangun NAS dengan Openfiler and ownCloud.	• Tanya-jawab • Demonstrasi percobaan	• **Kuliah (Teori Pengantar)**; • **Diskusi;** • **Percobaan** **[TM: 1x(6x50")]**		• NFS • Samba • NAS vs SAN • P2P • ownCloud	**5**
5	Sub-CPMK-4. mampu menjelaskan fungsi layanan proxy	• Mampu menjelaskan tentang layanan proxy • Mampu menginstall,	• Tanya-jawab • Demonstrasi percobaan	• **Kuliah (Teori Pengantar)**; • **Diskusi;**		• Konsep dasar proxy • Kelemahan dan kekurangan dari	**5**

	serta implementasinya. [c3,a3,p2]	mengkonfigurasi serta mengujicoba layanan proxy dengan beberapa studi kasus.		● **Percobaan** **[TM: 1x(6x50")]**		proxy ● Fungsi dari proxy ● Connection sharing ● Filter dan caching ● Desain dari cache ● Transparent proxy	
6	Sub-CPMK-5. mampu menjelaskan fungsi layanan pemantauan jaringan serta implementasinya. [c3,a3,p2]	● Mampu menjelaskan layanan sistem pemantauan jaringan. ● Mampu menginstall, mengkonfigurasi serta mengujicoba sistem monitoring jaringan dengan beberapa studi kasus.	● Tanya-jawab ● Demonstrasi percobaan	● **Kuliah (Teori Pengantar)**; ● **Diskusi;** ● **Percobaan** **[TM: 1x(6x50")]**		● Latar belakang NMS ● Solusi ● Pengertian NMS ● Kemampuan NMS ● Teknik NMS ● Komparasi NMS	**5**
7	Sub-CPMK-6. mampu menjelaskan fungsi dari manajemen dan analisa log serta implementasinya. [c3,a3,p2]	● Mampu menjelaskan tentang manajemen log ● Mampu menginstall, mengkonfigurasi serta mengujicoba sistem analis dan manjemen log (berbasis web/text).	● Tanya-jawab ● Demonstrasi percobaan	● **Kuliah (Teori Pengantar)**; ● **Diskusi;** ● **Percobaan** **[TM: 1x(6x50")]**		● Pemahaman pentingnya manajemen log ● Kebijakan log ● Tipe dari log ● Perangkat jaringan untuk log ● Manajemen log ● Tantangan utama log ● Terminologi dan arsitektur log	**10**
8	**Project-1**						
9	Sub-CPMK-7						
10	Sub-CPMK-8						
11	Sub-CPMK-9						
13	Sub-CPMK-10	.					

14-15	Sub-CPMK-11						
16	**Project II**						

Catatan:

1. Capaian Pembelajaran Lulusan PRODI (CPL-PRODI) adalah kemampuan yang dimiliki oleh setiap lulusan PRODI yang merupakan internalisasi dari sikap, penguasaan pengetahuan dan ketrampilan sesuai dengan jenjang prodinya yang diperoleh melalui proses pembelajaran.
2. CPL yang dibebankan pada mata kuliah adalah beberapa capaian pembelajaran lulusan program studi (CPL-PRODI) yang digunakan untuk pembentukan/pengembangan sebuah mata kuliah yang terdiri dari aspek sikap, ketrampulan umum, ketrampilan khusus dan pengetahuan.
3. CP Mata kuliah (CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPL yang dibebankan pada mata kuliah, dan bersifat spesifik terhadap bahan kajian atau materi pembelajaran mata kuliah tersebut.
4. Sub-CP Mata kuliah (Sub-CPMK) adalah kemampuan yang dijabarkan secara spesifik dari CPMK yang dapat diukur atau diamati dan merupakan kemampuan akhir yang direncanakan pada tiap tahap pembelajaran, dan bersifat spesifik terhadap materi pembelajaran mata kuliah tersebut.
5. Indikator penilaian kemampuan dalam proses maupun hasil belajar mahasiswa adalah pernyataan spesifik dan terukur yang mengidentifikasi kemampuan atau kinerja hasil belajar mahasiswa yang disertai bukti-bukti.
6. Kreteria Penilaian adalah patokan yang digunakan sebagai ukuran atau tolok ukur ketercapaian pembelajaran dalam penilaian berdasarkan indikator-indikator yang telah ditetapkan. Kreteria penilaian merupakan pedoman bagi penilai agar penilaian konsisten dan tidak bias. Kreteria dapat berupa kuantitatif ataupun kualitatif.
7. Bentuk penilaian: tes dan non-tes.
8. Bentuk pembelajaran: Kuliah, Responsi, Tutorial, Seminar atau yang setara, Praktikum, Praktik Studio, Praktik Bengkel, Praktik Lapangan, Penelitian, Pengabdian Kepada Masyarakat dan/atau bentuk pembelajaran lain yang setara.
9. Metode Pembelajaran: Small Group Discussion, Role-Play & Simulation, Discovery Learning, Self-Directed Learning, Cooperative Learning, Collaborative Learning, Contextual Learning, Project Based Learning, dan metode lainnya yg setara.
10. Materi Pembelajaran adalah rincian atau uraian dari bahan kajian yg dapat disajikan dalam bentuk beberapa pokok dan sub-pokok bahasan.
11. Bobot penilaian adalah prosentasi penilaian terhadap setiap pencapaian sub-CPMK yang besarnya proposional dengan tingkat kesulitan pencapaian sub-CPMK tsb., dan totalnya 100%.Rencana Penilaian & Evaluasi

DAFTAR ISI

PERCOBAAN 1

Pengenalan Administrasi dan Manajemen Jaringan

1.1. TUJUAN

Tujuan dari pada percobaan 1 ini adalah Mahasiswa mampu:

1. Menjelaskan tentang tujuan dari administrasi dan manajemen jaringan.
2. Menjelaskan peranan IT professional pada sebuah organisasi.
3. Menjelaskan jenis layanan-layanan jaringan.
4. Menjelaskan struktur organisasi dan job desc. dari Net/Sys Admin.

1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 1 diantaranya adalah:

1. Komputer
2. Switch
3. Aplikasi: Debian GNU Linux 9

1.3. DASAR TEORI

Jaringan komputer merupakan salah hal yang esensial di era digital saat ini. Hampir semua kebutuhan teknologi informasi membutuhkan komunikasi jaringan komputer. Oleh karenanya sebuah lembaga atau institusi sudah seharusnya dapat melakukan administrasi dan manajemen jaringan dengan baik dan benar guna memperoleh kinerja dari sebuah layanan yang optimal.

Persyarataratan pada perkuliahan workshop administrasi dan manajemen jaringan adalah perserta didik diwajibkan memahami tentang sistem operasi dan juga konsep jaringan komputer serta pemrograman komputer. Sistem operasi dibutuhkan karena diharapkan peserta didik memahami setiap perintah yang akan dijalankan untuk melakukan administrasi jaringan. Selain itu sistem hirarki file dari sistem operasi juga memiliki peranan penting dalam melakukan konfigurasi layanan. Pemahaman tentang jaringan komputer juga memiliki peranan yang tidak kalah pentingnya, peserta didik diharapkan bisa melakukan perbaikan (*troubleshoot*) ketika komputer tidak terhubung dengan jaringan dan menghitung ketersediaan alamat IP (*Internet Protocol*) pada saat melakukan instalasi maupun konfigurasi layanan jaringan.

Materi administrasi dan manajemen jaringan terdapat beberapa materi yang diajarkan yang berfokus pada penyediaan layanan jaringan diantaranya adalah:

- Web (*Hosting)* Server
- DNS (*Domain Name System*)
- Berbagi File (*File Sharing*)
- Proxy/Cache Server
- NMS (*Network Monitoring System*)
- Analisis dan Manajemen Log
- Dan lain-lain

Secara garis besar pembelajaran materi Administrasi dan Manajemen Jaringan meliputi proses:

- Installasi layanan
- Konfigurasi layanan
- Uji coba layanan
- Anailsa dan pemecahan masalah (*troubleshoot*) terhadap layanan jaringan

1.4. PROSEDUR PERCOBAAN

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Versi sistem operasi

  Sistem operasi yang akan digunakan pada perangkat mayoritas adalah menggunakan Debian GNU Linux oleh karenanya perangkat ujicoba diharapkan sudah terpasang sistem operasi Debian.

- Tes konektifitas

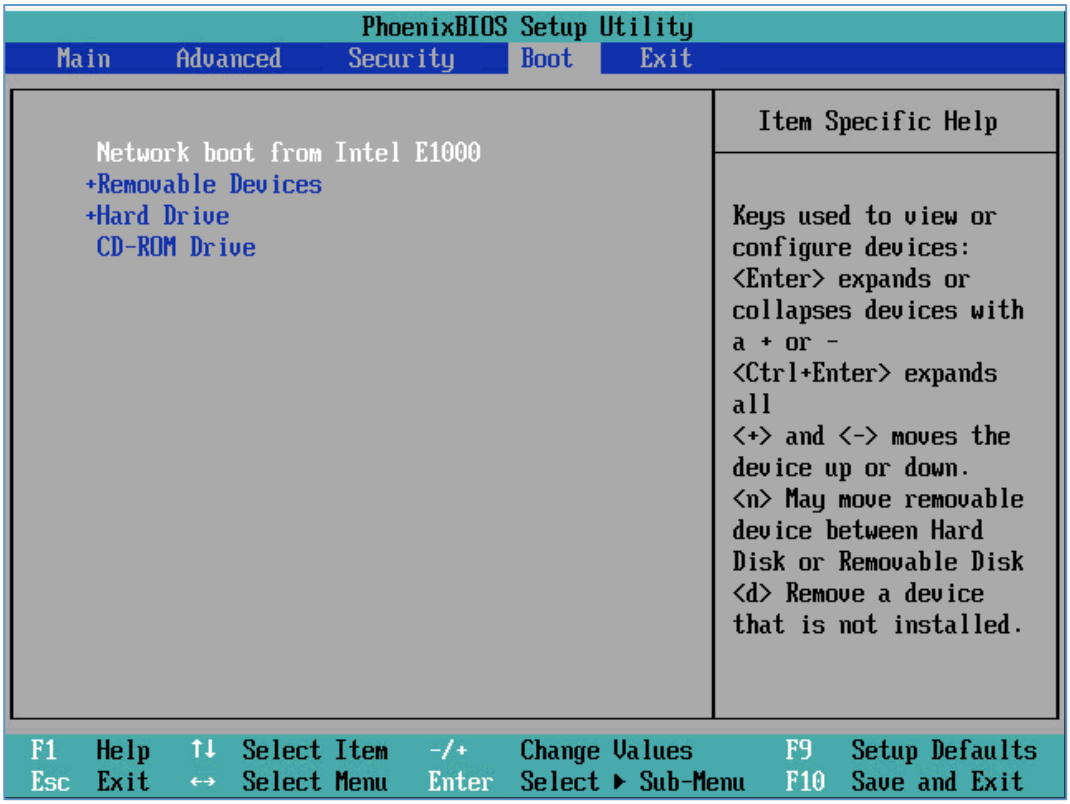
  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

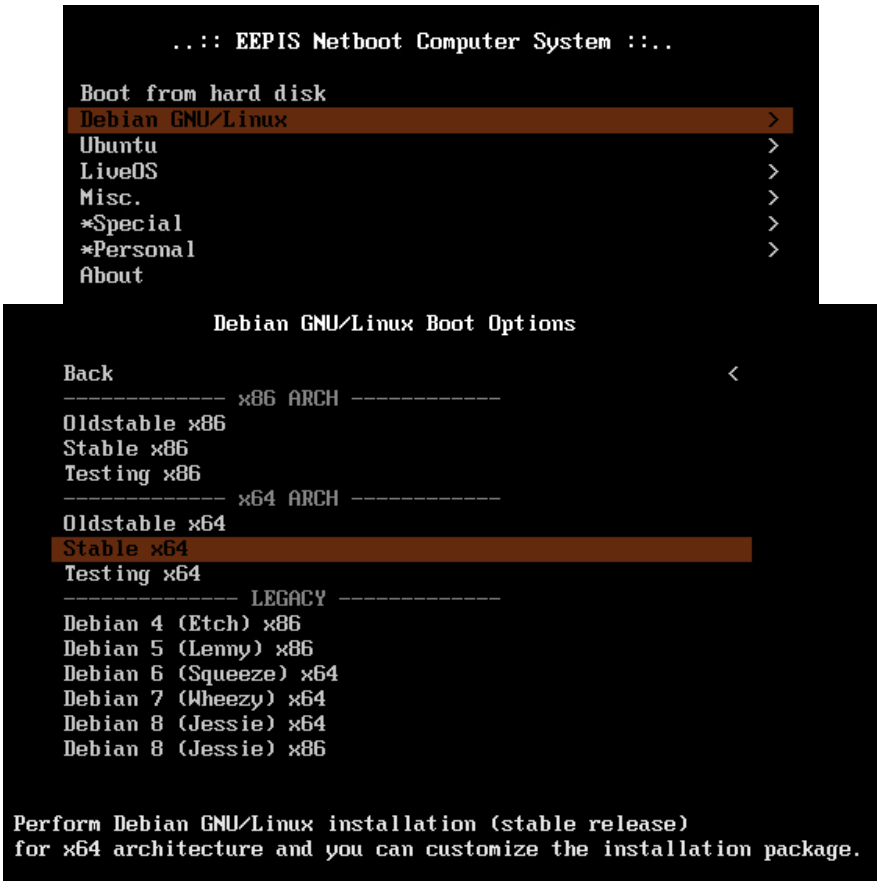
Pada perobaan 1 ini hanya akan berfokus pada tahap persiapan ujicoba dengan kriteria persiapan yang telah tersebut sebelumnya yaitu:

1. Persiapan sistem operasi
   PENS telah menyediakan Net-Install oleh karenanya untuk menginstal sistem operasi Debian dapat menggunakan fasiliatas ini dengan cara mengaktifkan fitur PXE (*Pre-Execution Environment*) yang ada pada BIOS seperti tampak pada gambar 1.1.



Gambar 1.1. Seting PXE pada BIOS

Selanjutnya restart komputer dan jika jaringan sudah terhubung ke PC maka akan tampil menu layanan Net-Install dari PENS seperti tampak pada gambar 1.2.



Gambar 1.2. Menu Net-Install.

Dengan menu pada gambar 1.2. maka akan dengan mudah dapat melakukan instalasi sistem operasi Debian dengan tanpa meggunakan media CD/Disc ataupun flash drive.

2. Tes konektifitas
   Cara sederhana melakukan pengecekan atau pegetesan konektifitas adalah dengan cara menggunakan perintah ping:

```
# ping  10.252.1.1
64 bytes from 10.252.1.1: icmp_seq=0 ttl=255 time=4.641 ms
64 bytes from 10.252.1.1: icmp_seq=1 ttl=255 time=4.010 ms
64 bytes from 10.252.1.1: icmp_seq=2 ttl=255 time=4.525 ms
^C
--- 10.252.1.1 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 4.010/4.392/4.641/0.274 ms
```

   Jika pada pengujian konektifitas tidak mendapatkan respon maka hendaknya segera melakukan pemeriksaan mulai dari kabel jaringan sampai dengan alamat IP, netmask, DNS dan lain-lain

   Dan juga apabila dalam praktikum dibutuhkan koneksi ke internet dalam rangka mengunduh aplikasi yang tidak tersedia di repositori PENS maka hendaknya dapat dilakukan penambahan konfigurasi proxy sebelum mengunduh aplikasi menggunakan *command-line* dengan perintah berikut ini:

```
# export http_proxy=http://proxy3.pens.ac.id:3128
# export https_proxy=http://proxy3.pens.ac.id:3128
# export ftp_proxy=http://proxy3.pens.ac.id:3128
```

3. Repositori instalasi
   Tahapan akhir untuk proses persiapan adalah memastikan bahwa repositori telah diarahkan ke alamat **kebo.pens.ac.id** dengan cara:

```
# vim  /etc/apt/sources.list.d/base.list
deb http://kebo.pens.ac.id/debian  stretch  main contrib non-free
```

   Selanjutnya update database repositori dengan cara:

```
# apt-get update
```

PERCOBAAN 2

Domain Name System (DNS)

1.1. TUJUAN

Tujuan dari pada percobaan 2 (DNS) ini adalah Mahasiswa mampu:

1. Mengetahui dan memahami bagaimana cara kerja dari DNS.
2. Mampu menginstall, mengkonfigurasi serta mengujicoba DNS untuk nama domain yang telah dirancang.

1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 2 diantaranya adalah:

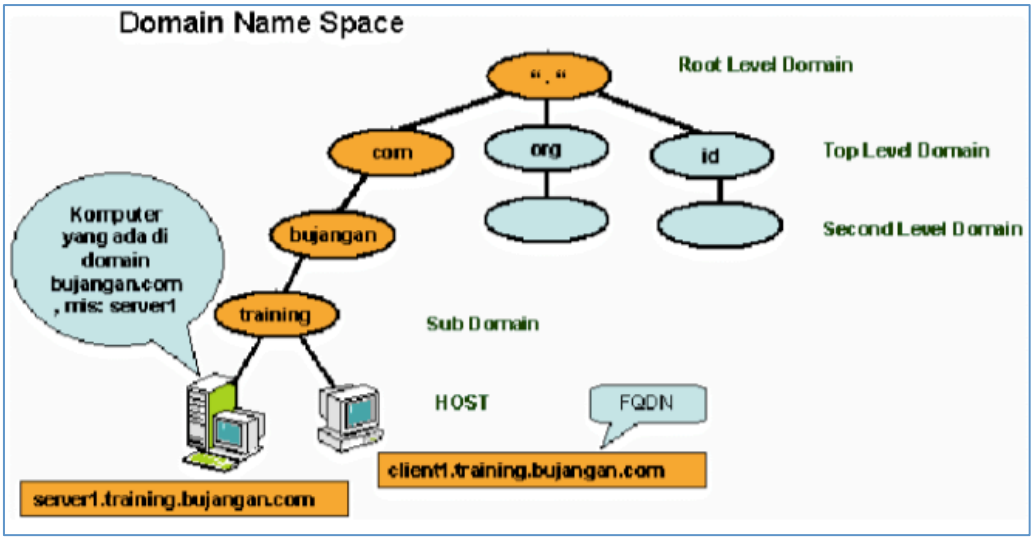
1. Komputer
2. Switch
3. Aplikasi: Bind

1.3. DASAR TEORI

Domain Name System (DNS) adalah suatu bentuk database yang terdistribusi, dimana pengelolaan secara lokal terhadap suatu data akan segera diteruskan ke seluruh jaringan (internet) dengan menggunakan skema *client-server*. Suatu aplikasi yang dinamakan dengan name server, mengandung semua segmen informasi dari database dan juga merupakan *resolver* bagi client-client yang berhubungan ataupun menggunakannya.

Struktur dari database DNS bisa diibaratkan dengan struktur file dari sebuah sistem operasi UNIX. Seluruh database digambarkan sebagai sebuah struktur terbalik dari sebuah pohon (*tree*) dimana pada puncaknya disebut dengan *root node*. Pada setiap *node* dalam *tree* tersebut mempunyai keterangan (label) misalnya, .org, .com, .edu, .net, .id dan lain-lainnya, yang relatif rerhadap puncaknya (*parent*). Ini bisa diibaratkan dengan relative pathname pada sistem file UNIX, seperti direktori *bin, usr, var, etc* dan lain sebagainya. Pada puncak root node dalam sebuah sistem DNS dinotasikan dengan "." atau "/" pada sistem file UNIX seperti tampak pada gambar 2.1.

Pada setiap node juga merupakan *root* dari *subtree*, atau pada sistem file UNIX merupakan *root* direktori dari sebuah direktori. Hal ini pada sistem DNS disebut dengan nama domain. Pada tiap domain juga memungkinkan nama subtree dan bisa berbeda pula, hal ini disebut subdomain atau subdirektori pada sistem file UNIX. Pada bagian subdomainjuga memungkinkan adanya *subtree* lagi yang bisa dikelola oleh organisasi yang berbeda dengan domain utamanya.



Gambar 2.1. Struktur dari DNS.

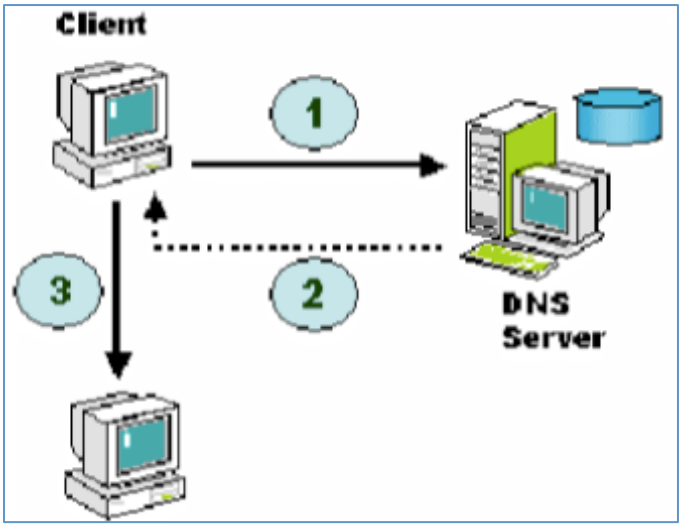
Cara Kerja DNS

DNS bekerja dengan konsep *client-server*, sebuah komputer yang menjalankan fungsi *server* disebut DNS atau *name server*. Sedang komputer lain yang meminta penerjemahan *hostname* ke *IP address* disebut sebagai *client* DNS. DNS juga merupakan sistem *database* yang terdistribusi, sehingga memungkinkan setiap bagian dari *database* dikelola secara terpisah.

DNS umumnya diterapkan dengan menggunakan *server* terpusat yang disebut *server* DNS atau *name server* yang memiliki wewenang atau otoritas dalam mengelola beberapa nama domain dan mengacu ke beberapa domain lainnya yang dikelola server DNS lain .

Gambar 2.2. memperlihatkan cara kerja dari DNS dengan alur kerja sebagai berikut:

1. Ketika komputer *client* meminta informasi *IP address* suatu *hostname* ke *name server*, biasanya memalui port 53. kemudian *name server* mencoba menerjemahkan berdasarakan *library resolv*-nya, apakah *hostname* merupakan nama domain yang dikelola oleh *name server*.
2. *Name server* akan memberikan jawaban berdasarkan *cache* dari data informasi yang sama yang pernah ditanyakan sebelumnya dan berhasil dijawab.
3. Setelah mendapatkan jawaban *IP address* dari DNS *server*, selanjutnya komputer *client* akan melajutkan komunikasi ke domain yang telah ter-*resolv*.



Gambar 2.2. Cara kerja dari DNS

3.1. PROSEDUR PERCOBAAN

BIND (Berkeley Internet Name Domain) adalah salah satu aplikasi server DNS yang menjadi standar untuk aplikasi DNS dalam semua distribusi *Linux*. Paket BIND itu berisi program *server* DNS yaitu */usr/bin/named* yang bertanggung jawab dalam merespon pertanyaan *client* DNS. Paket ini perlu kita install dan mengkonfigurasinya . Paket Bind 9 adalah versi terbarunya.

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Tes konektifitas

  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

- Persiapkan domain

  Pada implementasi nyata, domain didapatkan dengan cara mendaftarkan melalui Top Level Domain (TLD). Di Indonesia domain .id dikelola oleh PANDI (Pengelola Nama Domain Indonesia), sehingga untuk mendapatkan domain .id maka pengguna dapat melakukan pendaftaran melalui registrar PANDI

diantaranya adalah INDOREG, Melsa, Belidomain, dan lain-lain. Namun untuk kebutuhan praktikum maka dapat didefinisikan sendiri domain yang akan digunakan pada DNS (misal: netadmin.pens).

Jika komputer untuk uji coba telah dipastikan terhubung ke jaringan dan menggunakan repositori yang benar, maka percobaan dapat dilanjutkan sebagai berikut:

1. DNS Server
   a. Lakukan instalasi BIND9

```
# apt-get install bind9
```

   b. Edit file pada "/etc/resolv.conf" untuk mengkonfigurasi DNS *client* agar menggunakan DNS *server* yang terpasang dikomputer kita.

```
# vim /etc/resolv.conf

search netadmin.pens
domain netadmin.pens
nameserver 127.0.0.1
```

   c. Menyiapkan konfigurasi dan menambahkan *zone* (domain)

```
# vim  /etc/bind/named.conf.local

zone "netadmin.pens" {
     type master;
     file  "/var/cache/bind/netadmin.pens.db";
};

//reverse zone
zone "108.252.10.in-addr.arpa" {
      type master;
      file "/var/cache/bind/netadmin.pens.rev";
};
```

   d. Meyiapkan dan mengkonfigurasi database *zone* (domain)

```
# cp  /etc/bind/db.local   /var/cache/bind/netadmin.pens.db
# vim  /var/cache/bind/netadmin.pens.db

$TTL 604800
@ IN SOA netadmin.pens. root.netadmin.pens. (
         2019120100     ;serial
         604800         ;refresh
         86400          ;retry
         2419200        ;expire
         604800         ;minimum
)
@          IN  NS    ns.netadmin.pens.
```

```
@          IN  NS    ns2.netadmin.pens.
@          IN  A     10.252.108.200
@          IN  MX    5  mail.netadmin.pens.
NS         IN  A     10.252.108.200
www        IN  A     10.252.108.200
student    IN  A     10.252.108.201
mail       IN  A     10.252.108.202
ns2        IN  A     10.252.108.205
```

e. Meyiapkan dan mengkonfigurasi *reverse zone*

```
# cp  /etc/bind/db.127   /var/cache/bind/netadmin.pens.rev
# vim  /var/cache/bind/netadmin.pens.db

$TTL 604800
@ IN SOA netadmin.pens. root.netadmin.pens.(
          2019120100     ;serial
          604800         ;refresh
          86400          ;retry
          2419200        ;expire
          604800         ;minimum
)
@          IN  NS    ns1.netadmin.pens.
@          IN  NS    ns2.netadmin.pens.
@          IN  A     10.252.108.200
@          IN  MX    5  mail.netadmin.pens.
200        IN  PTR   www.netadmin.pens.
201        IN  PTR   student.netadmin.pens.
202        IN  PTR   mail.netadmin.pens.
205        IN  PTR   ns2.netadmin.pens.
```

f. Merestart BIND

```
# service bind9 restart
```

g. Ujicoba DNS

```
# nslookup netadmin.pens
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name: pens.ac.id
Address: 10.252.108.200

# nslookup student.netadmin.pens
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name: pens.ac.id
```

```
Address: 10.252.108.201

# nslookup 10.252.108.202
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
202.108.252.10.in-addr.arpa        name = mail.netadmin.pens.
```

2. DNS Forwarder

   DNS Forwarder berfungsi untuk meneruskan domain yang tidak terdaftar didatabase. Cara mengkonfigurasinya adalah:

   a. Konfigurasi file zone

```
# vim  /etc/bind/named.conf.local

zone “pens.ac.id” {
     type forward;
     forwarders {202.9.85.3;};
};
```

   Dari konfigurasi diatas dapat diartikan bahwa semua subdomain dari *pens.ac.id* akan diteruskan ke *server* DNS dialamat 202.9.85.3.

   b. Konfigurasi opsi dari BIND

```
# vim  /etc/bind/named.conf.options

options {
          directory   “/var/cache/bind”;
          forwarders {
                    202.9.85.4;
          };
};
```

   Dengan menambahkan opsi *forwarders* maka dapat diartikan semua domain yang tidak ditemukan pada database akan diteruskan ke server DNS dialamat 202.9.85.4;

   c. Merestart BIND

```
# service bind9 restart
```

   d. Ujicoba

```
# nslookup pens.ac.id
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name: pens.ac.id
Address: 202.9.85.176

# nslookup its.ac.id
Server:         127.0.0.1
Address:        127.0.0.1#53

Non-authoritative answer:
Name: pens.ac.id
Address: 103.94.189.5
```

3. DNS AXFR (Asynchronous Full Transfer Zone)
   Pada dasarnya, sangat disarankan DNS server lebih dari satu mesin untuk memperkuat ketersediaan dari layanan DNS. Oleh karenanya maka harus ada yang minimal 2 server DNS untuk zone (domain) yang sama. Satu server DNS difungsikan sebagai *master* dan lainnya difungsikan sebagai *slave*.
   Untuk itu maka siapkan 1 server lagi sebagai DNS slave (misal: slave dns berada di IP 10.252.108.205) yang juga terinstall aplikasi BIND9. Selanjutnya pada DNS master dikonfigurasi sebagai berikut:
   a. Konfigurasi file opsi

```
# vim /etc/bind/named.conf.options
options {
        directory   "/var/cache/bind";
        forwarders {
                202.9.85.4;
        };
        allow-query {
                10.252.108.205;
        };
};
```

   b. Konfigurasi file zone

```
# vim  /etc/bind/named.conf.local

zone "netadmin.pens" {
    type master;
    file  "/var/cache/bind/netadmin.pens.db";
    allow-transfer{10.252.108.205;};
    also-notity{10.252.108.205;};
```

```
};
```

c. Merestart BIND

```
# service bind9 restart
```

Selanjutnya di DNS client juga dilakukan penyesuaian konfigurasi sebagai berikut:

d. Konfigurasi file zone

```
# vim  /etc/bind/named.conf.local

zone “netadmin.pens” {
     type slave;
     file  “/var/cache/bind/netadmin.pens.db”;
     masters{10.252.108.200;};
};
```

e. Merestart BIND

```
# service bind9 restart
```

f. Perhatikan database dari BIND9 di komputer *client,* jika file database sudah terbentuk maka proses transfer zone telah berhasil.

3.2. TUGAS

1. Buatlah DNS server dengan domain yang sama menggunakan aplikasi dnsmasq

PERCOBAAN 3

Berbagi File (File Sharing)

1.1. TUJUAN

Tujuan dari pada percobaan 3 (File Sharing) ini adalah Mahasiswa mampu:

1. Mengetahui dan memahami bagaimana cara melakukan berbagi file.
2. Memasang, mengkonfigurasi dan menguji coba layanan berbagi file dengan menggunakan NFS dan SAMBA.

1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 3 diantaranya adalah:

1. Komputer
2. Switch
3. Aplikasi: NFS, SAMBA

1.3. DASAR TEORI

NFS atau Network File System adalah protocol yang digunakan untuk berbagi file atau direktori secara terdistribusi di jaringan dengan mudah seakan-akan file tersebut berada pada disk lokal . Protokol ini diciptakan oleh Sun Microsystem di tahun 1984. NFS disebutkan dalam RFC 1094, 1813 dan 3530

NFS menggunakan model client-server dimana server bertugas untuk mengatur otentikasi, otorisasi dan manajemen client serta data yang disharing dengan file system berbeda. Setelah proses otorisasi, user dapat mengakses data seakan-akan berada pada storage internal.

File : /etc/exports

File konfigurasi NFS diletakkan di /etc/exports dan memiliki susunan dengan format sebagai berikut:

```
<export directory di server>    <nomor IP client>/<netmask client>(<opsi hak akses NFS>)
```

Contoh :

```
/mnt/sharedfolder      192.168.30.10/24(rw,sync)
```

Keterangan :

- /mnt/sharedfolder : directory yang diexport pleh NFS server
- 192.168.30.10/24 : Nomor IP client beserta netmasknya
- (rw,sync) : opsi hak akses dari NFS adalah read-write dan synchronize

Tabel 3.1.1 Opsi NFS server di /etc/exports

Opsi hak akses NFS	Definisi
rw	client untuk dapat read dan write terhadap folder yang dishare
ro	client hanya boleh read terhadap folder yang dishare
sync	Opsi synchronize akan menuliskan setiap perubahan terhadap folder yang dishare di disk server.
no_subtree_check	Opsi ini mencegah terjadinya pembacaan/scanning direktori dibawahnya
no_root_squash	Opsi ini membolehkan root untuk tersambung ke folder yang di share

File /etc/fstab

File ini adalah file yang dipergunakan OS saat booting untuk menyusun mount pointnya. Tiap baris pada file/etc/fstab digunakan untuk mendeskripsikan bagaimana mount menyusun OS file system yang berbeda-beda (termasuk yang diexport lewat NFS), mountpointnya, dan sejumlah opsi mount untuk tiap mount point. Pada kasus NFS, tiap baris /etc/fstab memuat nama server, path name dari direktory yang diexport server, local directory yang menjadi mount point, dan sejumlah opsi untuk mount point tersebut. Untuk fstype pada NFS digunakan nfs

```
server:path   /mountpoint   fstype   option,option,...   0 0
```

Contoh :

```
203.0.113.0:/home   /nfs/home  nfs    auto,nofail,noatime,nolock,intr,tcp,actimeo=1800
0   0
```

203.0.113.0:/home : server address dan path yang diexport
/nfs/home : mount point di sisi client
nfs : filesystem
auto,nofail,noatime,nolock,intr,tcp,actimeo=1800 : opsi nfs
0 : dumping
0 : fschecking
Jika nilai dumping 0 = false, 1 = true. Biasanya nilai yang diberikan adalah 0
Jika nilai 0=tidak perlu fsck, 1=fsck saat booting, 2=fsck setelah /root. Filesystem yang harus dicek saat booting biasanya adalah root. Sedangkan untuk filesistem lain dilakukan sehabis root atau sesuai kebutuhan. Pengecekan ini biasanya membutuhkan waktu yang berbeda-beda, tergantung filesystem yang dipergunakan.

Tabel 3.1.2 Opsi-Osi dari /etc/fstab

Opsi /etc/fstab	
auto / noauto	Tentukan apakah partisi harus secara otomatis di-mount saat boot. Anda dapat memblokir partisi tertentu dari pemasangan saat boot-up dengan menggunakan "noauto".
exec / noexec	Menentukan apakah partisi dapat mengeksekusi binari. Jika Anda memiliki partisi awal yang Anda kompilasi, maka ini akan berguna, atau mungkin jika Anda memiliki / home pada sistem file terpisah. Jika Anda khawatir tentang keamanan, ubah ini menjadi "noexec".
ro/rw	ro / rw: "ro" adalah read-only, dan "rw" adalah baca-tulis. Jika Anda ingin dapat menulis ke sistem file sebagai pengguna dan bukan sebagai root, Anda harus memiliki "rw" yang ditentukan.
atime / noatime /	noatime : tidak perlu mengupdate inode tentang akses time dari filesystem. Dengan opsi ini anda dapat meningkatkan performansi. Sebaliknya berlaku untuk atime.
user/nouser	user adalah opsi mount yang memungkinkan semua user biasa untuk me mount partisi, sedangkan nouser hanya mengijinkan super user (root) yang boleh melakukan mount partisi tersebut.
default	jika menggunakan opsi default maka yang opsi mount yang akan digunakan adalah ” rw, suid, dev, exec, auto, nouser, and async”
sync/async	Sync: opsi ini menentukan input dan output ke sistem berkas dilakukan serempak, misal saat me-copy file kedalam flash disk dengan opsi “sync” maka perubahan fisik dilakukan pada saat yang sama. Sebaliknya berlaku untuk async
dev / nodev	nodev memblokir perangkat khusus pada filesystem, sebaliknya
suid / nosuid	Mengijinkan / Memblokir operasi bit suid , dan sgid .

Tabel 3.1.3 Tipe filesystem dari NFS

Jenis filesystem di NFS	Keterangan
ext2, ext3, ext4	File system yang umum dipakai untuk sistem operasi linux
reiserfs	File system untuk linux yang lebih advanced
Swap	File system yang digunakan untuk membantu RAM ketika RAM membutuhkan memori yang lebih
Vfat	File system biasa di pakai windows, contohnya FAT32 biasa di pakai windows juga
Ntfs	File system yang biasa di pakai windows juga
Auto	opsi untuk mendeteksi secara otomatis jenis partisi yang dituju

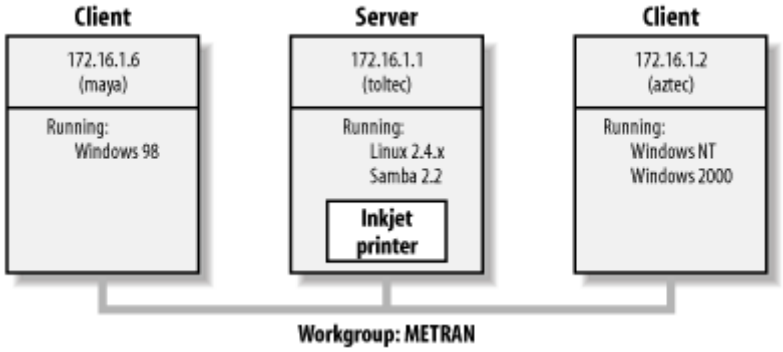
SAMBA Server

Samba adalah aplikasi berbasis Unix yang menggunakan protolol Server Message Block (SMB) Microsof Windows dan system operasi OS/2 menggunakan

SM untuk sharing file dan printer dengan menggunakan jaringan berbasis client-server. Selain kedua system operasi diatas, Samba memungkinkan computer berbasis Unix untuk berkomunikasi dengan computer berbasis Windows.Ketika menggunakan Samba, di jaringan, computer berbasis Unix akan nampak seperti computer berbasis Windows bagi client yang berbasis Windows.

Server Samba menyediakan layanan berikut :

- Sharing directory
- Sharing filesystem
- Sharing printer
- Menyediakan layanan browsing lewat jaringan untuk client
- Otentikasi client yang login ke domain Windows
- Menyediakan layanan resolusi name-server berbasis Windows Internet Name Service (WINS)
- Menyediakan layanan agar user dengan system UNIXdapat mengakses folder dan printer yang disediakan Windows dan server Samba lewat jaringan.



Gambar 3.2.1 Samba server dengan client

1.4. PROSEDUR PERCOBAAN

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Tes konektifitas

  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan

digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

Jika komputer untuk uji coba telah dipastikan terhubung ke jaringan dan menggunakan repositori yang benar, maka percobaan dapat dilanjutkan sebagai berikut:

NFS (Network File System)

1.Instal NFS server

```
server # apt-get update
server# apt install nfs-kernel-server
```

2. Membuat Direktory Export

Di computer server, direktori yang hendak dishare ke client disebut directory export. Anda dapat menciptakan direktori ini di /mnt/sharedfolder

```
server # mkdir -p /mnt/sharedfolder
```

3. Sekarang ubah kepemilikan direktori tersebut dari root:root menjadi nobody:nogroup. Ubah hak aksesnya menjadi rwx-rwx-rwx

```
server # chown nobody:nogroup /mnt/sharedfolder
server# sudo chmod 777 /mnt/sharedfolder
```

4. Setting file konfigurasi NFS server. Buka file /etc/exports.

```
server # nano /etc/exports
```

Bekerjasamalah dengan teman anda. Catat IPnya dan gunakan untuk konfigurasi /etc/exports. Misal IP addressnya adala 10.252.108.30

Tambahkan baris berikut.

```
/mnt/sharedfolder   10.252.108.30(rw,sync,root_squash,no_subtree_check)
/home               10.252.108.30(rw,sync,no_root_squash,no_subtree_check)
```

Restart NFS server

```
server #systemctl restart nfs-kernel-server
```

5. Setting Firewall. Cek status firewall

```
server # ufw status
```

Jika firewall aktif, dan hanya openssh yang diperbolehkan mengakses firewall, maka kita harus menambahkan agar trafik NFS diperbolehkan lewat firewall.

```
Status: active
To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
OpenSSH (v6)               ALLOW       Anywhere (v6)
```

Lakukan perintah berikut di terminal. Ganti 10.252.108.30 dengan nomor IP teman anda

```
server # ufw allow from 10.252.108.30 to any port nfs
```

Cek dengan perintah berikut,apakah firewall sudah meng-allow trafik NFS

```
server # ufw status
```

Jika sudah, maka akan muncul trafik menuju port 2049 telah diperbolehkan untuk nomor IP yang kita tambahkan

```
Status: active

To                         Action      From
--                         ------      ----
OpenSSH                    ALLOW       Anywhere
2049                       ALLOW       10.252.108.30
OpenSSH (v6)               ALLOW       Anywhere (v6)
```

6. Menginstal nfs client

```
client #  apt update
client# apt install nfs-common
```

7. Menciptakan mount point di client

Setelah server NFS dikonfigurasi dan siap mengexport sharefile / direktori, maka client harus dipersiapkan agar dapat menerima share tersebut. Agar remote share dari server dapat diakses client, maka kita perlu melakukan mount remote share dari server ke direktori kosong dari client. Di sisi client, buatlah 2 direktori untuk melakukan mount direktori server.

```
client #  mkdir -p /nfs/sharedfolder
client# mkdir -p /nfs/home
```

8. Melakukan mount direktori server ke client. Perintah ini akan melakukan mount dari server ke client.

```
client# mount 10.252.108.30:/mnt/sharedfolder   /nfs/sharedfolder
client# mount 10.252.108.30:/home  /nfs/home
```

Cek apakah proses mount berhasil dengan perintah df.

```
client #  df -h
```

Output dari df -h :

```
Filesystem                    Size  Used  Avail  Use%  Mounted on
udev                          238M     0   238M   0%        /dev
tmpfs                          49M  628K    49M   2%        /run
/dev/vda1                      20G  1.2G    18G   7%        /
tmpfs                         245M     0   245M   0%        /dev/shm
tmpfs                         5.0M     0   5.0M   0%        /run/lock
tmpfs                         245M     0   245M   0%        /sys/fs/cgroup
tmpfs                          49M     0    49M   0%        /run/user/0
10.252.108.30:/mnt/sharedfolder   20G  1.2G   18G   7% /nfs/sharedfolder
10.252.108.30:/home  20G    1.2G    18G       7%      /nfs/home
```

Karena kedua folder dimount dari filesistem yang sama, maka pemakaian disk menunjukkan kapasitas yang sama. Untuk melihat ukuran sesungguhnya yang dipakai di tiap mount point digunakan perintah du. Du-s akan menampilkan summary pemakaian untuk keseluruhan pemakaian dan –h untuk output yang human readable.

```
client# du -sh /nfs/home
client# du –sh /nfs/shared folder
```

9. Testing akses NFS

Di computer client, sekarang coba untuk mengakses /nfs/sharedfolder dan buatlah file di client di /nfs/sharedfolder. Berhasilkah ? Cek ownership shared.test, harusnya user dan groupnya nobody:nogroup. ‘

```
client# cd /nfs/sharedfolder
client# touch root.test
client# ls –l /nfs/sharedfolder/root.test
```

Login sebagai user biasa dan lihat perubahan file userownership dan group ownershipnya. Berhasilkah ? Cek ownership shared.test, harusnya user dan

groupnya nobody:nogroup. Perbedaan ownership ini disebabkan opsi root_squash yang tidak memperbolehkan user dan group ownershipnya sebagai root.

```
client#su student
student# touch student.test
student# ls –l /nfs/sharedfolder/student.test
```

Berikutnya, buat file di direktori /nfs/home di computer client. Cek ownership dari file tersebut. Berhasilkah ?

```
client # su root
client# cd /nfs/home
client# touch home.test
client# ls –l /nfs/home/home.test
```

10. Melakukan mount saat computer client dibooting. Buka file /etc/fstab. Cek nomor IP server. Misal IP server 10.252.108.40.

```
client# nano /etc/fstab
```

```
10.252.108.40:/mnt/sharedfolder /nfs/sharedfolder   nfs auto,nofail,noatime,
nolock,intr,tcp,actimeo=1800 0 0


10.252.108.40:/home /nfs/home nfs auto,nofail,noatime,nolock,intr,tcp,
actimeo=1800 0 0
```

Tambahkan baris berikut

Reboot linux anda dan check apakah sudah termount di client dengan df –h

```
client# df -h
```

Jika belum lakukan perintah berikut untuk melakukan mount /etc/fstab

```
client# mount  -a
```

11. Melakukan unmounts direktori yang diakses

```
client# umount -l /nfs/home
client# umount –l /nfs/sharedfolder
```

SAMBA

1. Instalasi samba

```
server#apt update
server#apt install samba samba-common
server#whereis samba
```

2. Konfigurasi samba. File konfigurasi samba terletak di /etc/samba/smb.conf.Buka file /etc/samba/smb.conf

```
server#nano /etc/samba/smb.conf
```

Tambahkan baris berikut pada bagian yang paling bawah dari /etc/samba/smb.conf. Misalkan sharename tersebut bernama [sambashare], path yang dipakai adalah /home/student/sambashare, isi direktori hanya dapat diubah user student, sementara untuk user lain hanya dapat melihat isi [sambashare]

```
[sambashare]
   comment = Samba on Ubuntu
   path = /home/student/sambashare
   browsable = yes
   write list = student
```

Test dengan testparm

```
server#testparm
```

3. Membuat direktori samba share, mengubah hak akses dan kepemilikan file.

```
server# mkdir /home/student/sambashare
server# chmod 777 /home/student/sambashare
server#chown –R student:student /home/student/sambashare
```

4. Restart Samba

```
server#systemctl restart smbd
server#systemctl status smbd
```

5. Update rule firewall

```
server#ufw allow samba
server#ufw status
```

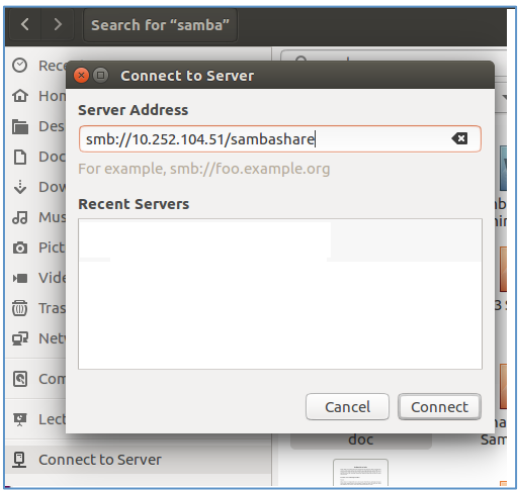
6. Setting user account dan koneksi ke sharename. Misalkan username adalah student.

```
server#smbpasswd –a student
```

7. Restart samba server

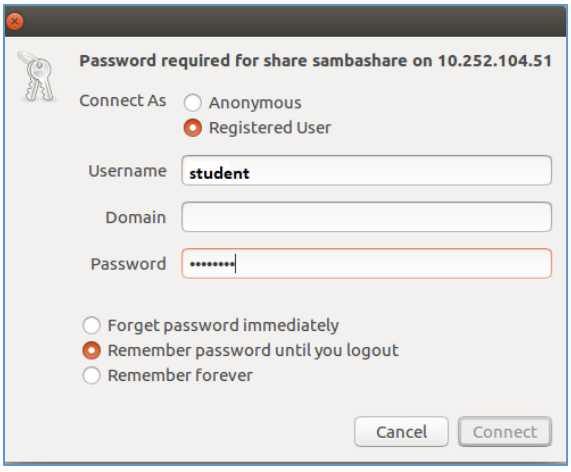
```
server#systemctl restart smbd
```

8. Di sisi linux client, buka File Manager. Klik Connect to Server. Masukkan nomor IP dari samba server, yaitu 10.252.104.51 dan sharename : sambashare. Klik Connect



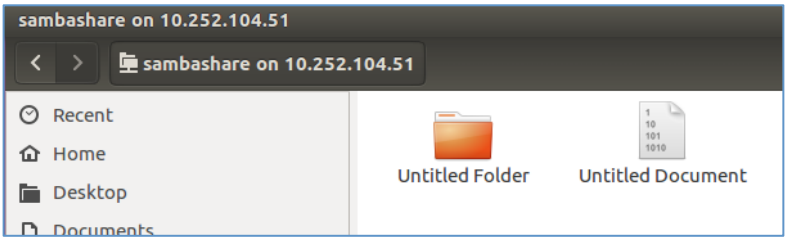
Gambar 3.2.2 Koneksi ke Samba Server

Sekarang masukkan username dan password. Klik Connect



Gambar 3.2.3 Username dan Password User

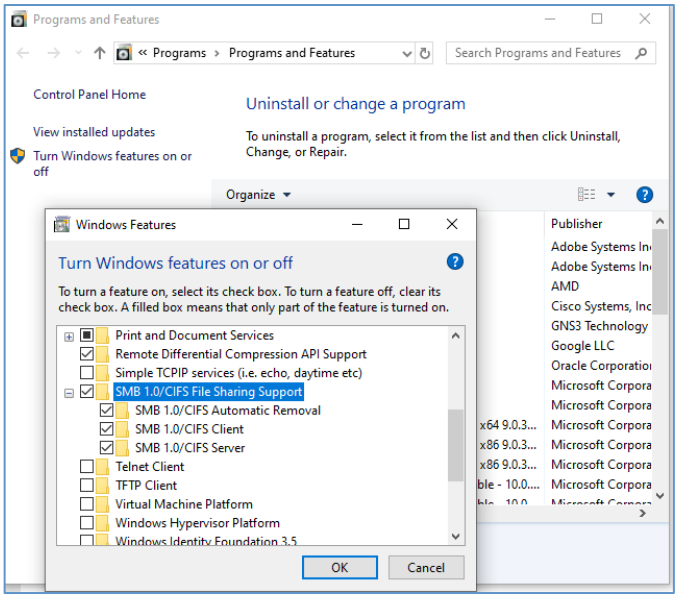
Sekarang buat file dan direktori baru di samba. Klik kanan dari mouse, pilih New Folder. Kemudian klik kanan lagi, pilih New Document, Empty Document. Screenshot hasilnya.



Gambar 3.2.4 Membuat dokumen dan folder di Samba

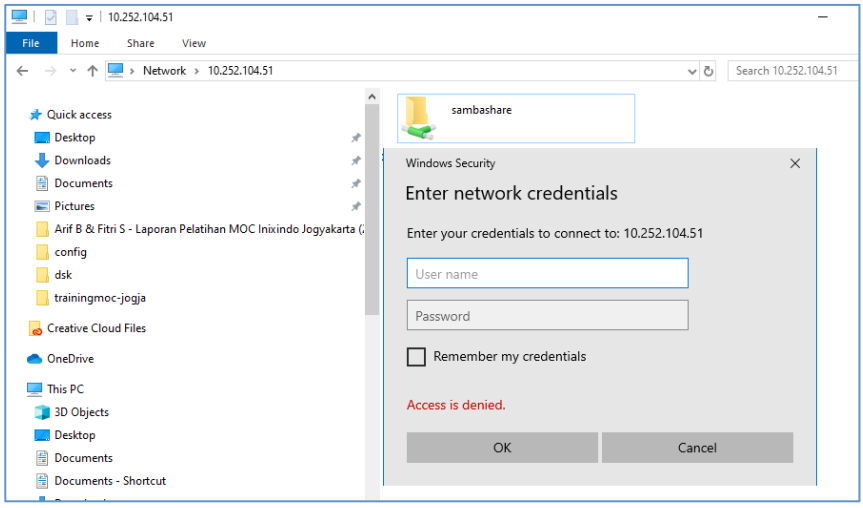
9. Sekarang di sisi Windows user.

   Pada windows 10, ketik Control Panel, kemudian klik Program and Features. Pilih Turn Windows features on or off. Klik opsi seperti dibawah.



Gambar 3.2.5 Windows features untuk Samba

Buka File Explorer. Klik Network di bagian kiri bawah. Pada Search, masukkan nomor IP dari samba server.Masukkan username dan password. Klik OK



Gambar 3.2.6 Username dan password di Windows

10. Sekarang kita akan mensetting bahwa setiap samba user akan login di directory /home masing-masing. Buat user baru di server,missal : nana. Masukkan passwordnya

```
server#adduser nana
```

Set samba password untuk user nana

```
server#smbpasswd –a student
```

Restart samba server

```
server#systemctl restart smbd
```

11. Buka file /etc/samba/smb.conf dan carilah sharename [homes]

```
server# nano /etc/samba/smb.con
```

Sesuaikan bagian berikut

```
[homes]
comment= Home Directories
browseable = no
read only = no
create mask = 0700
directory mask = 0700
```

12. Sekarang logout sebagai student dan login sebagai user nana. Seperti pada langkah 8, pada File Manager, masukkan alamat berikut smb://10.252.104.51/nana atau smb://10.252.104.51/homes. Perhatikan bahwa sharename [homes] berisi user-user yang terdaftar di samba, yaitu nana dan student. Connect as registered user. Masukkan username nana dan passwordnya. Buatlah direktori bernama : nana dan file baru bernama file.nana. Screenshoot hasilnya. File dan directory yang anda buat di client, disimpan di /home/nana.

13. Sekarang kita akan membuat sharename [accounting] dan [engineering]. Group engineering dapat melakukan write di [engineering], namun hanya dapat melakukan read di [accounting]. Group accounting dapat melakukan write di [accounting], namun hanya dapat melakukan read di [engineering]. Group accounting punya user : acc1 dan acc2 , group engineering punya user: eng1 dan eng2.

```
server#adduser eng1
server#adduser eng2
```

```
server#adduser acc1
server#adduser acc2
```

Lakukan juga untuk PC client

```
client#adduser eng1
client#adduser eng2
client#adduser acc1
client #adduser acc2
```

Buat group baru di server dan lakukan juga di PC client

```
server#addgroup engineering
server#addgroup accounting
```

Sekarang ubahlah agar eng1 dan eng2 grupnya adalah engineering, acc1 dan acc2 grupnya adalah accounting. Lakukan juga di PC client.

```
server# usermod –g engineering eng1
server# usermod –g engineering eng2
server# usermod –g accounting acc1
server# usermod –g accounting acc2
```

Set samba password untuk eng1,eng2,acc1, acc2.Cukup lakukan di server

```
server#smbpasswd –a eng1
server#smbpasswd –a eng2
server#smbpasswd –a acc1
server#smbpasswd –a acc2
```

Restart samba server

```
server#systemctl restart smbd
```

14. Buat file /home/samba/engineering dan file /home/samba/accounting

```
server# mkdir –p /home/samba/engineering
server# mkdir –p /home/samba/accounting
server#chmod 775 /home/samba/engineering
server# chmod 775 /home/samba/accounting
server# chown –R  root:engineering  /home/samba/engineering
server# chown –R  root:accounting  /home/samba/accounting
```

15. Buka file /etc/samba/smb.conf. Pada bagian paling bawah, tambahkan baris berikut.

```
server# nano /etc/samba/smb.conf
```

Sesuaikan bagian berikut

```
[engineer]
comment = Engineering Directories
path = /home/samba/engineering
browsable = yes
read list = @accounting
write list = @engineering

[account]
comment = Accounting Directories
path = /home/samba/accounting
public = no
browsable = no
read list = @engineering
write list = @accounting
```

Restart samba server

```
server#systemctl restart smbd
```

16. Di computer client, loginlah sebagai user : eng1. Buka File Manager. Klik Connect to Server. Jika IP server adalah 10.252.104.51, maka : smb://10.252.104.51/ Klik Connect. Masukkan username : eng1 dan password. Gunakan Registered User. Apakah anda melihat sharename [engineer] dan [account] ?
    Klik sharename [engineer]. Buat file bernama : test.eng1 dan directory bernama : eng1 di dalamnya. Berhasilkan ?

    Sharename [account] tidak nampak karena disetting di smb.conf browsable = no. Untuk melihat sharename tersebut, buka File Manager. Klik Connect to Server. Jika IP server adalah 10.252.104.51, maka : smb://10.252.104.51/account Klik Connect. Masukkan username : eng1 dan password. Gunakan Registered User. Klik sharename [account]. Buat file dan directory di dalamnya. Berhasilkan ?

17. Ulangi langkah ke 16 untuk user acc1 atau acc2.

1.5. TUGAS

1. Buatlah sharename [public] yang hanya bisa dibaca (read only) oleh semua user dan group

2. Buatlah sharename [anonymous] dimana semua bisa melakukan read and write tanpa harus melakukan otentikasi.

PERCOBAAN 4

Proxy/Cache Server

1.1. TUJUAN

Tujuan dari pada percobaan 4 (Proxy/Cache Server) ini adalah Mahasiswa mampu:

1. Mengetahui dan memahami bagaimana cara kerja dari layanan proxy pemantauan jaringan yang.
2. Mampu menginstall, mengkonfigurasi serta mengujicoba layanan proxy dengan beberapa studi kasus.

1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 4 diantaranya adalah:

1. Komputer
2. Switch
3. Aplikasi: Squid, Peramban web (firefox)

1.3. DASAR TEORI

Proxy server merupakan server yang menyediakan berbagai layanan seperti meneruskan setiap permintaan client ke server lain, melakukan pemblokan situs yang tidak di inginkan dan menyaring data yang lewat pada portnya.

Perlu diketahui Proxy mempunyai tiga fungsi utama, yaitu :

1. Connection Sharing
   Bertindak sebagai gateway yang menjadi batas antara jaringan lokal dan jaringan luar. Gateway juga bertindak sebagai titik dimana sejumlah koneksi dari pengguna lokal akan terhubung kepadanya dan koneksi jaringan luar juga terhubung kepadanya. Dengan demikian koneksi dari jaringan lokal ke internet akan menggunakan sambungan yang dimiliki oleh gateway secara bersama-sama (connecion sharing).

2. Filtering
   Bekerja pada layar aplikasi sehingga berfungsi sebagai Firewalll paket filtering yang digunakan untuk melindungi jaringan lokal terhadap gangguan atau serangan dari jaringan luar. Dapat dikonfigurasi untuk menolak situs web tertenu pada waktu-waktu tertentu.

3. Caching
   Proxy Server memiliki mekanisme penyimpanan obyek-obyek yang sudah diminta dari server-server di internet. Mekanisme caching akan menyimpan obyek-obyek yang merupakan permintaan dari para pengguna yang di dapat dari internet.

Aplikasi yang akan digunakan yaitu Squid3, salah satu software yang digunakan untuk mengelola lalu lintas data dari client ke internet.

1.4. PROSEDUR PERCOBAAN

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Tes konektifitas

  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

Jika komputer untuk uji coba telah dipastikan terhubung ke jaringan dan menggunakan repositori yang benar, maka percobaan dapat dilanjutkan sebagai berikut:

Percobaan 1: Setting Proxy Server

1. Install aplikasi Squid3

```
#apt update
#apt install squid3
```

Cek versi squid dengan perintah

```
# squid -v
```

2. Cek alamat IP anda. Catat alamat IP tersebut

```
#ip addr
```

Berikutnya, cek file konfigurasi IP yang ada di /etc/network/interfaces.

```
#nano /etc/network/interfaces
```

Jika anda masih menggunakan alamat IP dinamis, ubahlah menjadi alamat IP statik. Masukkan baris berikut

```
auto ens33
iface ens33 inet static
address 192.168.43.246
netmask 255.255.255.0
gateway 192.168.43.1
network 192.168.43.0
broadcast 192.168.43.255
```

Restart service network

```
#systemctl restart networking
```

3. Mengkonfigurasi file squid
   Masuklah pada direktori squid lalu buka file konfigurasi squid dengan mengetikan perintah berikut

```
# nano /etc/squid/squid.conf".
```

Lalu cari baris "And finally deny all other access to this proxy" dengan tombol Ctrl+W, edit dan tambah file konfigurasi squid sebagai berikut

```
http_access allow all
```

Restart squid dan cek statusnya

```
#systemctl restart squid
#systemctl status squid
```

4. Cek apakah squid sudah bekerja di port 3128

```
#netstat -ntlupn | grep squid
```

Atau anda dapar menggunakan nmap

```
#apt install nmap
#nmap localhost
```

Hasil netstat :

```
root@mail:/etc/squid# netstat -ntlupn | grep squid
tcp6       0      0 :::3128                 :::*                    LISTEN
6917/(squid-1)
udp        0      0 0.0.0.0:59267           0.0.0.0:*
6917/(squid-1)
udp6       0      0 :::44590                :::*
6917/(squid-1)
```

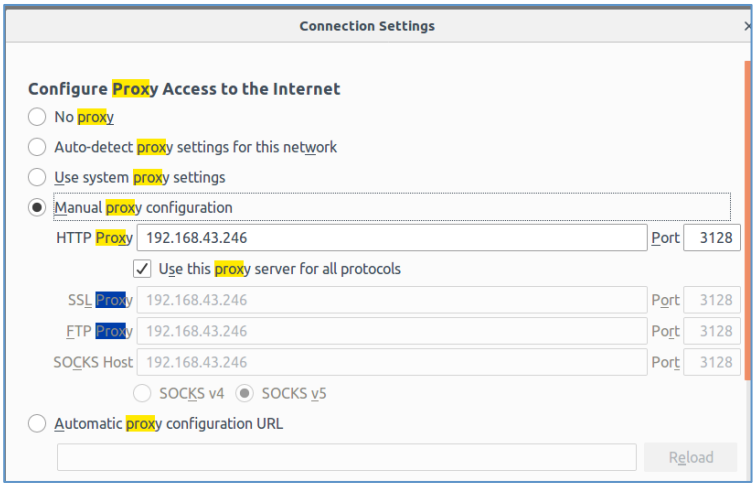
Gambar 4.1 Hasil Netstat

Sedang hasil nmap :

```
root@mail:/etc/squid# nmap localhost

Starting Nmap 7.01 ( https://nmap.org ) at 2019-05-01 21:32 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000025s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
80/tcp   open  http
110/tcp  open  pop3
139/tcp  open  netbios-ssn
143/tcp  open  imap
445/tcp  open  microsoft-ds
631/tcp  open  ipp
902/tcp  open  iss-realsecure
3128/tcp open  squid-http
3306/tcp open  mysql
```

Gambar 4.2 Gambar Nmap

5. Sekarang, di komputer client, buka browser. Pada Preferences, masuklah ke Network Settings. Carilah setting proxy. Masukkan alamat IP dari proxy server. Browser yang digunakan penulis adalah Firefox. Namun anda dapat menggunakan browser lain sesuai dengan komputer anda. Simpan dan keluarlah dari Settings.



Gambar 4.3 Setting proxy di browser client

Note: Jika anda tidak memiliki komputer lain untuk mengetes proxy, anda dapat menggunakan virtual mesin dg vmware atau virtual box.

6. Buka browser. Ketikkan halaman http://www.google.com. Jika anda berhasil, maka proxy server anda telah berjalan dengan baik.

Percobaan 2: Menggunakan proxy server untuk mengeblok situs tertentu

Di komputer server, lakukan langkah berikut :

1. Buka file konfigurasi squid dengan mengetikan perintah berikut

```
# nano /etc/squid/squid.conf".
```

Lalu cari baris "And finally deny all other access to this proxy" dengan tombol Ctrl+W, edit dan tambah file konfigurasi squid sebagai berikut . Kita akan mengeblok situs detik, youtube dan facebook.

```
acl bloksitus  dstdomain "/etc/squid/urlblok"
http_access deny bloksitus
#http_access allow all
```

Buatlah file /etc/squid/urlblok

```
#nano /etc/squid/urlblok
```

Masukkan baris berikut. Perhatikan bahwa ada . sebelum facebook, youtube dan detik

```
.detik.com
.facebook.com
.youtube.com
```

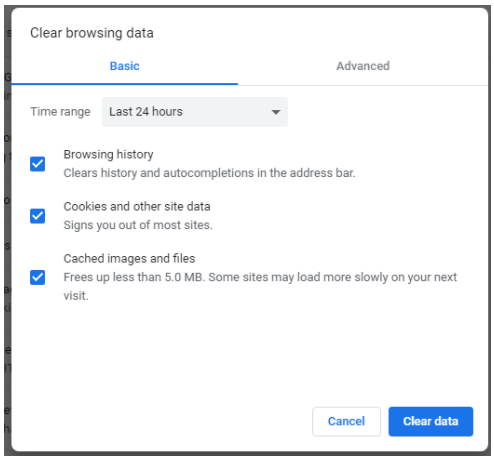
Restart squid

```
#systemctl restart squid
#systemctl status squid
```

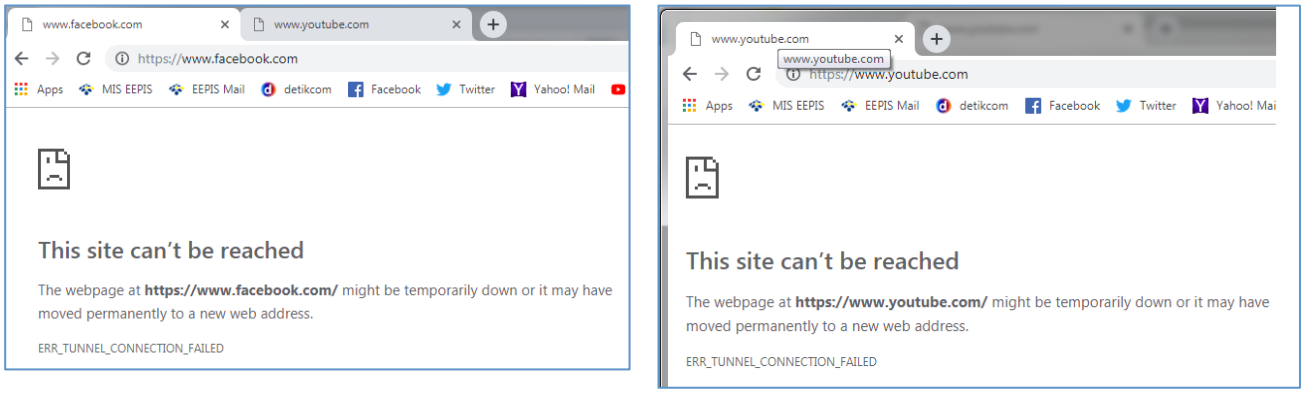
Di komputer client, lakukan langkah berikut:

2. Sebelumnya bersihkan dulu cache browser anda. Kemudian tekan Clear Data.

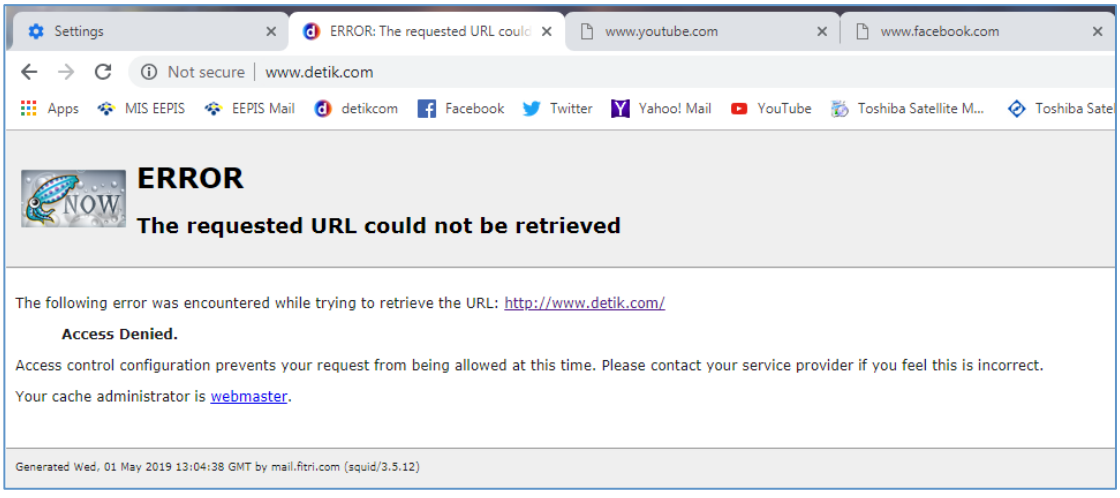
3. Coba buka website yang kita blok, yaitu detik, facebook dan youtube dengan browser. Jika bloking yang dilakukan squid berhasil, anda tidak bisa membuka situs-situs tersebut.



Gambar 4.4 Membersihkan cache di browser client



Gambar 4.5 Hasil mengeblok facebook dan youtube



Gambar 4.6 Hasil mengeblok youtube

Percobaan 3: Menambahkan otentikasi pada user

Di komputer server, lakukan langkah berikut :

1. Install software apache2-utils

```
#apt install apache2-utils
```

2. Buka file konfigurasi squid dengan mengetikan perintah berikut

```
# nano /etc/squid/squid.conf
```

Lalu cari baris “And finally deny all other access to this proxy” dengan tombol Ctrl+W, edit dan tambah file konfigurasi squid sebagai berikut . Kita akan menambahkan otentikasi pada user

```
auth_param basic program /usr/lib/squid3/basic_ncsa_auth  /etc/squid/users
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
acl ncsa_users proxy_auth REQUIRED
http_access allow ncsa_users
```

3. Pilihlah user yang ada di server dan masukkan ke list user yang boleh mengakses proxy server. Buat juga passwordnya. Misal, username : fitri dengan password : fitri

```
# htpasswd –c /etc/squid/users fitri
```

Squid server akan membuat file /etc/squid/users yg berisi nama user dan encrypted passwordnya. Coba buka file /etc/squid/users, maka anda akan melihat entry sbb :

```
fitri:$apr1$Yo7Gr3V5$k7Xc.SYSFf/6fbH3p0xxy1
```

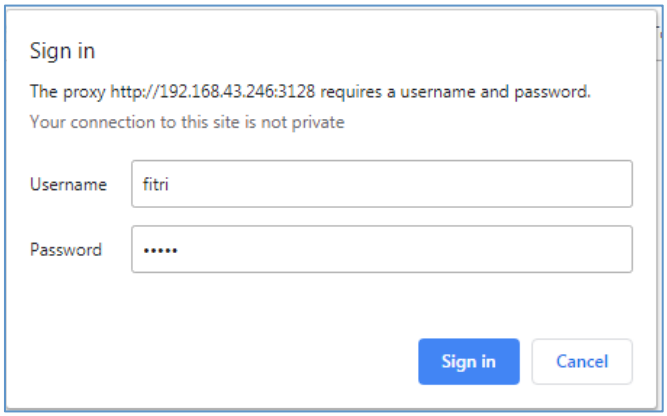
4. Restart squid

```
#systemctl restart squid
```

Di komputer client, lakukan langkah berikut :

5. Sebelumnya bersihkan dulu cache browser anda. Kemudian tekan Clear Data.

6. Coba buka browser. Akan muncul permintaan otentikasi. Masukkan username dan password sesuai yang anda buat



Gambar 4.7 Otentikasi di browser client

Percobaan 4: Transparent Proxy

Skenario : Kita akan membuat transparent proxy, dimana transparent proxy tersebut akan mengeblok semua situs pens (*.pens.ac.id) sementara mengijinkan akses ke situs lain. Dengan menggunakan transparent proxy, kita dapat memaksa client untuk menggunakan proxy server, tanpa harus mengeset di browser client.

1. Update linux dan install squid3. Jika sudah menginstall squid3, skip saja langkah 1.

```
#apt update
#apt install squid3
```

Cek versi squid dengan perintah

```
# squid -v
```

2. Cek nomor IP anda. Catat nomor IP tersebut

```
#ip addr
```

Berikutnya, cek file konfigurasi IP yang ada di /etc/network/interfaces.

```
#nano /etc/network/interfaces
```

Jika anda masih menggunakan alamat IP dinamis, ubahlah menjadi alamat IP statik. Masukkan baris berikut

```
auto ens33
iface ens33 inet static
address 192.168.43.246
netmask 255.255.255.0
gateway 192.168.43.1
network 192.168.43.0
broadcast 192.168.43.255
```

Restart service network

```
#systemctl restart networking
```

3. Mengkonfigurasi file squid

Masuklah pada direktori squid lalu buka file konfigurasi squid dengan mengetikan perintah berikut

```
# nano /etc/squid3/squid.conf
```

Port yang digunakan adalah 3128. Intercept digunakan untuk mensetting proxy menjadi tranparent. Jika masih ada tanda # hilangkan untuk mengatifkan konfigurasi port. Carilah kata http_port , ubah menjadi

```
http_port 3128 intercept
```

Berikutnya, kita setting acl untuk memblok dan meng-allow situs. Perhatikan bahwa urutan penulisan acl menentukan penerapan allow dan deny pada situs. Pada http_access deny internal bloksitus, kita mengeblok jaringan 192.168.43.0/24 yang mengakses situs di urlblok.txt. Bagaimana dengan situs lain ? Pada http_access ke dua, http_access allow internal, kita mengijinkan situs selain yang ada di urlblok.txt untuk diakses. Save dan exit.

```
acl internal src 192.168.43.0/24

acl bloksitus dstdomain "/etc/squid/urlblok.txt"
```

```
http_access deny internal bloksitus

http_access allow internal
```

Buat file /etc/squid/urlblok.txt

```
#nano /etc/squid/urlblok.txt
```

Masukkan baris berikut. Perhatikan bahwa ada . sebelum pens.ac.id, yang artinya semua domain yg berakhiran dengan pens.ac.id, misalnya www.pens.ac.id, mail.pens.ac.id, dst. Save dan Exit

```
.pens.ac.id
```

Restart squid

```
#systemctl restart squid
#systemctl status squid
```

4. Setting firewall
Sebelumnya kita hapus ule firewall yang ada sebelumnya

```
sudo iptables -t nat -F

sudo iptables -t mangle -F

sudo iptables -F

sudo iptables -X
```

Kita setting firewall untuk transparent proxy. Gantilah 192.168.43.0/24 sesuai dengan nomor network address server dan client

```
#iptables -t nat -A PREROUTING -p tcp -s 192.168.43.0/24 --dport 80 -j
REDIRECT --to-port 3128
```

Sekarang cek firewall yang telah kita beri rule baru dengan

```
#iptables -t nat -L
```

Harusnya ada output seperti berikut :

```
root@mail:/var/log/squid# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  192.168.43.0/24      anywhere             tcp dpt:http redir
 ports 3128
```

Gambar 4.8 Output iptables setelah setting NAT

5. Jika anda mendapati output iptables NAT masih tetap kosong setelah setting NAT di langkah 4, maka lakukan langkah berikut. Sebaliknya, skip langkah di nomor 5 ini jika entry iptables telah terisi seperti no 4.

```
root@mail:/home/fitri# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
```

Gambar 4.9 Output IP Tables tetap kosong

Entry iptables pada chain PREROUTING yang kosong menunjukkan bahwa setting iptables tidak berhasil. Mungkin ini disebabkan oleh perubahan di systemd-networkd yang didapati di Ubuntu 16.04. Agar iptables dapat bekerja, maka forwarding harus dienable di network interface terlebih dulu.

```
#sysctl -w net.ipv4.ip_forwarding=1
```

Untuk mengecek, apakah ip_forwarding sudah berhasil atau belum, maka lakukan :

```
#sysctl -a | grep forwarding
```

Apabila berhasil anda akan melihat output berikut. Perhatikan bahwa wlp3s0 adalah nama interface yang digunakan oleh komputer anda. Sesuaikan dengan nama interface yang anda pakai. Cek dengan perintah ip addr

```
net.ipv4.conf.wlp3s0.forwarding = 1
net.ipv4.conf.wlp3s0.mc_forwarding = 0
```

Gambar 4.10 Setting Sysctl

Bila masih berbeda hasilnya, lakukan berikut. Jika sudah sesuai, anda tidak perlu melakukan langkah berikut

```
sysctl net.ipv4.conf.eth0.forwarding=1
```

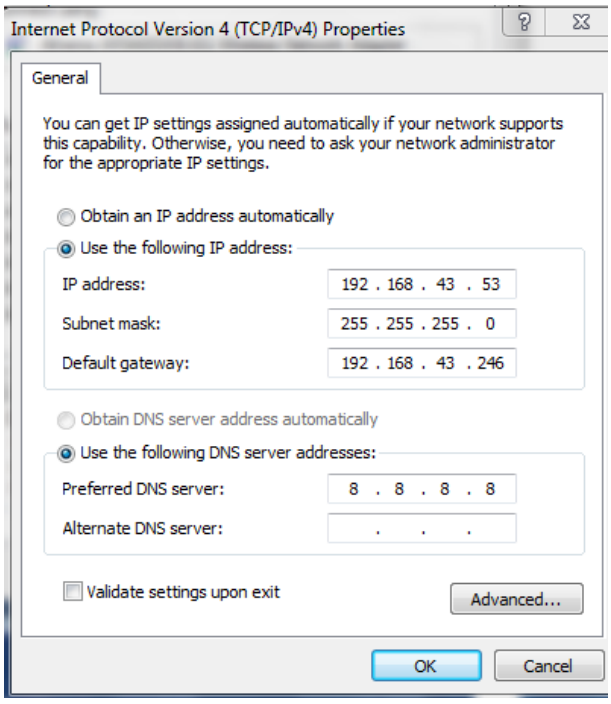
Lakukan kembali langkah 4 untuk memasukkan rule iptables

```
#iptables -t nat -A PREROUTING -p tcp -s 192.168.43.0/24 --dport 80 -j
REDIRECT --to-port 3128
```

Sekarang cek firewall yang telah kita beri rule baru dengan

```
#iptables -t nat –L
```

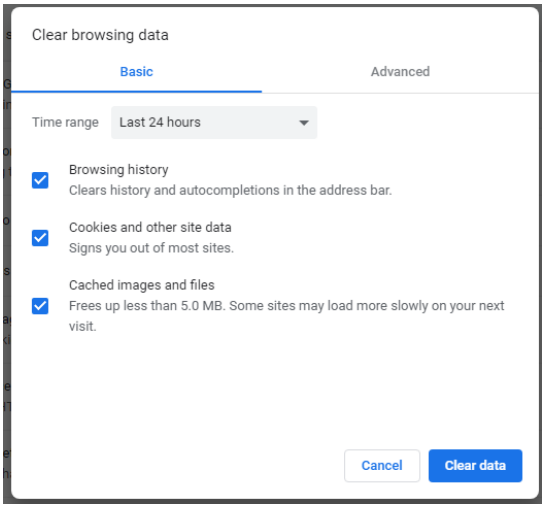
6. Setting di TCP/IP properties di PC client.
Buka TCP/IP properties. Lengkapi entry sebagai berikut. IP address dan subnet mask adalah IP address dan subnetmak dari PC client. Default gateway diisi dengan nomor IP adress dari server. Untuk DNS, kita set menggunakan DNS dari google 8.8.8.8.



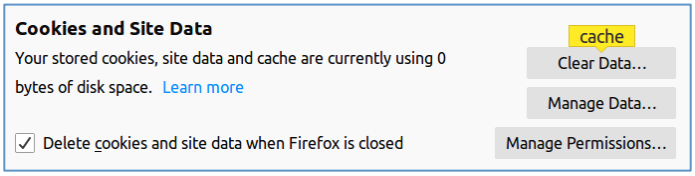
Gambar 4.11 Setting TCP/IP properties

7. Setting di browser client.
   Sebelumnya pastikan bahwa cache browser dalam keadaan kosong.Pada tombol settings atau preferences, carilah lokasi cache dengan mengetikkan cache di

Kosongkan cache dengan mengklik Clear Data



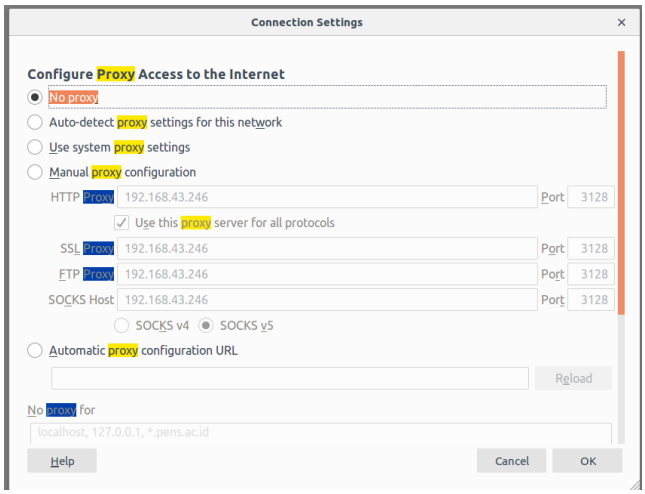
(a)



(b)

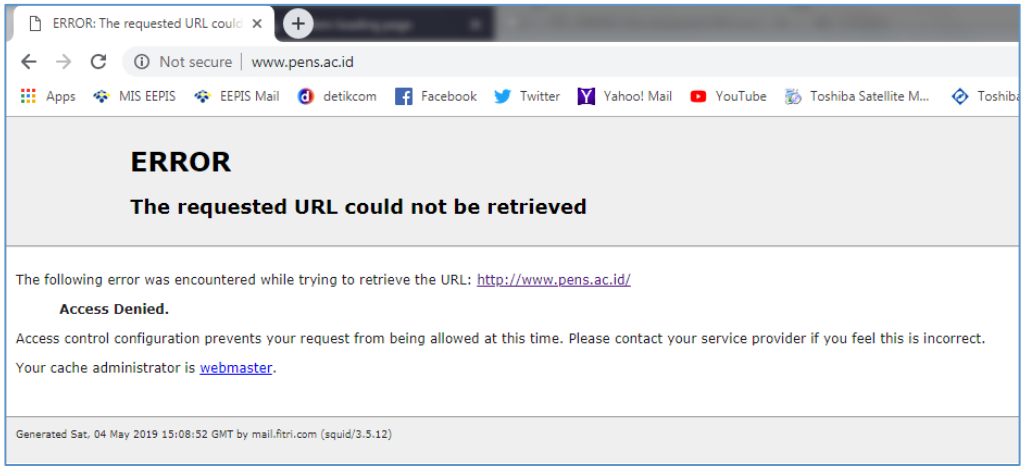
Gambar 4.12 (a) Membersihkan cache di Google Chrome (b) Membersihkan cache di Mozilla Firefox

8. Setting di browser client
   Pada setting/preference proxy, pilih No Proxy



Gambar 4.13 Setting transparent proxy di browser client

9. Coba buka browser di sisi client.
   Bukalah halaman web yang tadinya diblok. Yaitu www.pens.ac.id. Apakah sudah terblok?



Gambar 4.14 Halaman web www.pens.ac.id yang terblokir

10. Cobalah buka webpage lain, selain *.pens.ac.id, yaitu www.detik.com

Gambar 4.15 Halaman web www.detik .com yang tidak terblokir

PERCOBAAN 5

NMS (Network Monitoring System)

1.1. TUJUAN

Tujuan dari pada percobaan 5 (NMS) ini adalah Mahasiswa mampu:

1. Mengetahui dan memahami bagaimana cara melakukan pemantauan jaringan yang dikelolanya.
2. Menggunakan berbagai aplikasi NMS untuk pengoptimalan akses jaringan yang dikelolanya.
3. Memasang (install), mengkonfigurasi, serta menguji coba aplikasi NMS.

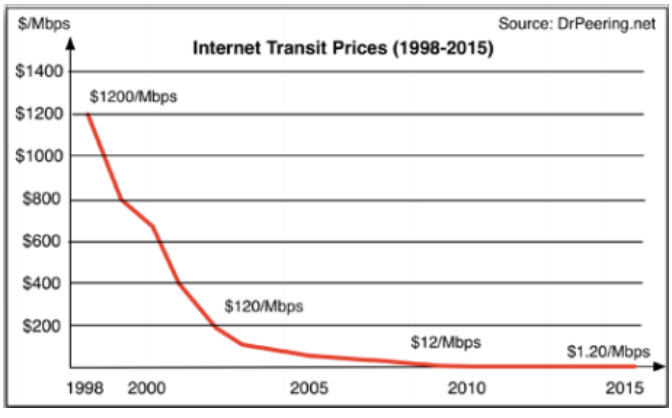
1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 5 diantaranya adalah:

1. Komputer
2. Switch
3. Aplikasi: Iperf, Iptraf, Nload, Iftop, SNMP, Cacti

1.3. DASAR TEORI

Sistem Pemantauan Jaringan (NMS - Network Monitoring System) adalah sebuah sistem yang dimanfaatkan atau digunakan untuk memantau kondisi jaringan sebuah disuatu institusi. Dengan adanya NMS maka akan membantu serta memudahkan System Administrator dalam mengetahui kondisi jaringan yang dikelolanya. Ketika terjadi permasalah ataupun anomali pada jaringan maka akan dengan cepat diketahui untuk kemudian dapat dilakukan perbaikan atau penyelesaiannya.



Gambar 5.1. Harga layanan internet dunia.

Salah satu fungsi lain dari NMS adalah dapat memantau penggunaan dari jaringan yang dikelola. Fungsi ini dapat ditindaklanjuti untuk menentukan kebijakan dalam pendistribusian penggunaan atau pemanfaatan akses internet. Selain itu juga terdapat beberapa kemampuan atau fungsi dari NMS yang dapat dijelaskan sebagai berikut:

1. Mengidentifikasi layanan atau server yang tidak resmi
2. Memantau penggunaan jaringan
3. Penyelesaian masalah jaringan
4. Investigasi kejadian/pelanggaran keamanan jaringan.
5. Menyimpan catatan aktivitas pengguna untuk akuntabilitas

Dengan adanya NMS maka System Administrator juga akan dapat mengetahui:

1. Siapa yang mengakses jaringan?
   – Mahasiswa, karyawan, dosen, tamu atau lainnya?
2. Apa yang mereka akses?
   – Materi ajar, sosial, pembalajaran, penggunaan ilegal
3. Darimana mereka mengakses jaringan?
   – Internal atau eksternal
4. Bagaimana cara meraka mengaksesnya?
   – remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN
5. Kapan mereka mengaksesnya?
   – Hari ini, kemarin, minggu lalu, bulan lalu...

Meski harga layanan internet dari tahun ke tahun semakin murah (lihat gambar 5.1.) namun kebutuhan akan kecepatan akses ke internet juga semakin tinggi karena konten internet yang semakin beragam (misal. streaming video berkualitas high-definition) maka anggaran yang dibutuhkan pun juga tetap tinggi. Seperti diketahui bahwa salah satu pengeluaran terbesar yang selalu rutin dianggarkan sebuah institusi dalam operasinya setiap tahun adalah untuk berbelanja layanan internet (selain listrik). Oleh karenanya penggunaan dan distribusi akses internet harus optimal karena berdasarkan penelitian yang dilakukan oleh Gwynn ditahun 2006 menunjukkan bahwa terdapat 59% institusi yang melakukan pemantauan terhadap jaringan yang mereka kelola.

Maka solusi untuk melakukan peningkatan performa jaringan dan pengoptimalan akses internet yang telah kita langgan maka diusulkan:

1. Mengganti infrastruktur jaringan dengan yang terbaru.
2. Memasang sistem (aplikasi) yang handal dan cepat.
3. Mencari penyedia layanan internet yang lebih murah dan cepat

Alternatif lainnya dalam pengoptimalannya dapat juga dengan melakukan: pemahaman terhadap sumber daya yang ada (misal. bandwidth internet yang sudah dilanggan), bahwa bandwidth internet adalah aset yang sangat berharga bagi sebuah institusi atau lembaga sehingga perlu diatur pemanfaatannya seoptimal dan sebijak mungkin.

Terdapat 2 jenis NMS yaitu Real-time dan Historical. Real-time adalah salah satu jenis NMS yang memiliki kemampuan untuk menampilkan atau menunjukkan kondisi jaringan yang saat ini sedang berlangsung. Aplikasi yang dapat digunakan

pada jenis ini diantaranya adalah Iptraf-ng, iftop, dan lain-lain. Sedangkan NMS yang berjenis Historical adalah NMS yang melakukan pendokumentasian hasil pemantauan dari waktu ke waktu dan disimpan untuk kemudian dapat dianalisa dikemudian hari. Contoh NMS yang bersifat historical adalah MRTG, Webalizer, SARG, dan lain-lain.

1.4. PROSEDUR PERCOBAAN

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Tes konektifitas

  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

Jika komputer untuk uji coba telah dipastikan terhubung ke jaringan dan menggunakan repositori yang benar, maka percobaan dapat dilanjutkan sebagai berikut:

1. IPERF

   Iperf adalah sebuah aplikasi yang dapat digunakan untuk mengetahui performa jaringan yang kita kelola. Dengan Iperf akan diketahui kecepatan pengiriman data dari 1 komputer ke komputer yang lainnya.

   Ujicoba iperf dibutuhkan 2 buah komputer yang berfungsi sebagai client dan server. Kedua komputer tersebut harus diinstall aplikasi iperf. Detail langkah-langkah percobaan adalah sebagai berikut:

   a. Instalasi paket IPERF

   ```
   # apt-get install iperf
   ```

   b. Uji coba
      - Server, disisi server dapat menjalankan perintah:

```
# iperf -s
```

```
root@server:/home/student# iperf -s
------------------------------------------------------------
Server listening on TCP port 5001
TCP window size: 85.3 KByte (default)
------------------------------------------------------------
[  4] local 10.252.209.102 port 5001 connected with 10.252.209.243 port 45710
[ ID] Interval       Transfer     Bandwidth
[  4]  0.0-10.0 sec  6.23 GBytes  5.35 Gbits/sec
```

Gambar 5.2. iperf pada komputer server

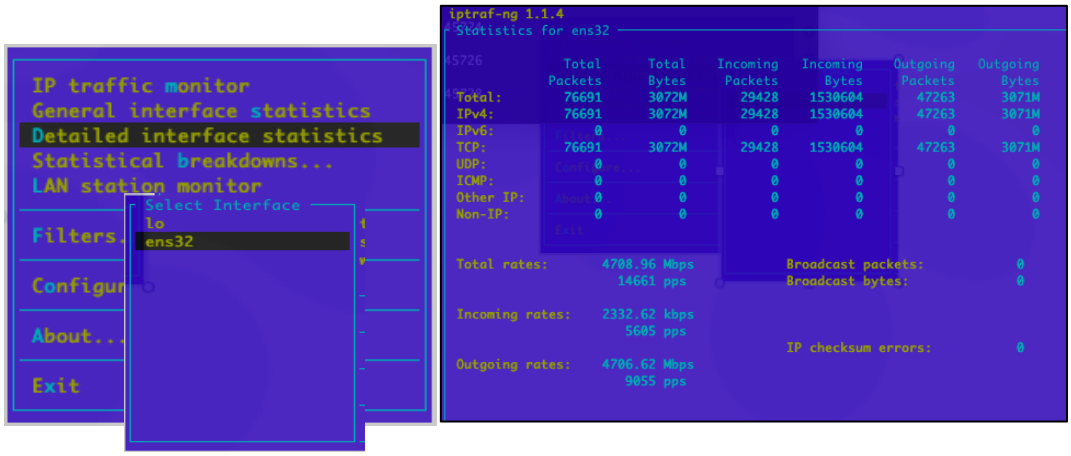
- Client, disisi client dapat menjalankan perintah:

```
# ipert -c <ip address dari server>
```

```
root@client:/home/student# iperf -c 10.252.209.102
------------------------------------------------------------
Client connecting to 10.252.209.102, TCP port 5001
TCP window size: 85.0 KByte (default)
------------------------------------------------------------
[  3] local 10.252.209.243 port 45710 connected with 10.252.209.102 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-10.0 sec  6.23 GBytes  5.35 Gbits/sec
```

Gambar 5.3. iperf pada komputer client

Pada gambar 5.2 dan 5.3 tampak bahwa kecepatan pengiriman data dari kedua komputer tersebut adalah 5.35 Gbit/sec.



Gambar 5.4. Pemantauan kecepatan pengiriman data secara *real-time* dengan iptraf-ng.

2. IPTRAF-NG

Berbeda dengan Iperf, Iptraf-ng berfungsi untuk mendapatkan infromasi kecepatan pengiriman data secara *real-time*. Instalasi dari iptraf-ng adalah sebagai berikut:

```
# apt-get install iptraf-ng
```

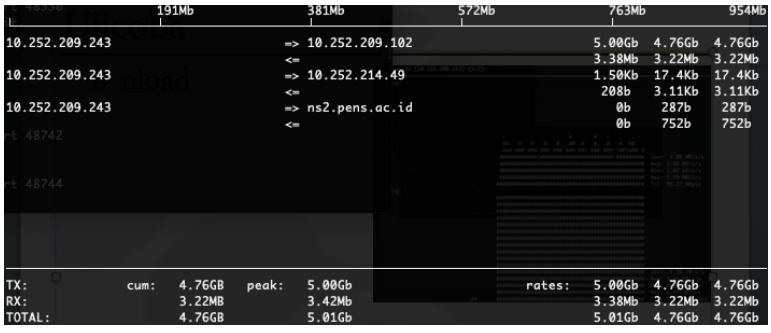
Pada gambar 5.4. ditunjukkan aplikasi iptraf-ng yang telah dijalankan. Pada gambar tersebut tampak kecepatan pengiriman data ditunjukkan secara detail yaitu diantaranya kecepatan untuk TCP, UDP, ICMP, dan lainnya.

3. NLOAD & IFTOP

Nload dan Iftop memiliki kemiripan dengan iptraf-ng yaitu data bersifat real-time, namun memiliki penyajian data yang berbeda dimana nload dapat menampilkan dalam bentuk grafik sedang Iftop dapat menampilkan kecepatan pengiriman data setiap port ata layanan yang digunakan seperti yang tampak pada gambar 5.5. dan 5.6. Instalasi dari Nload dan Iftop adalah sebagai berikut:

```
# apt-get install iftop nload
```

Gambar 5.5. Aplikasi nload yang menampilkan data dalam bentuk grafik.



Gambar 5.6. Aplikasi Iftop yang mampu menampilkan kecepatan pengiriman data setiap port atau layanan.

4. SNMP

SNMP (Simple Network Management Protocol) merupakan protokol standar yang digunakan untuk mengkoleksi dan mengorganisasi informasi tentang perangkat jaringan yang dikelola seperti switch, router, modem, server, printer dan lain lain. SNMP akan diolah lebih lanjut oleh aplikasi lainnya (misal: MRTG, cacti, dll.) untuk dipresentasikan dalam bentuk grafik sehingga mudah dalam pembacaannya. Proses instalasinya adalah sebagai berikut:

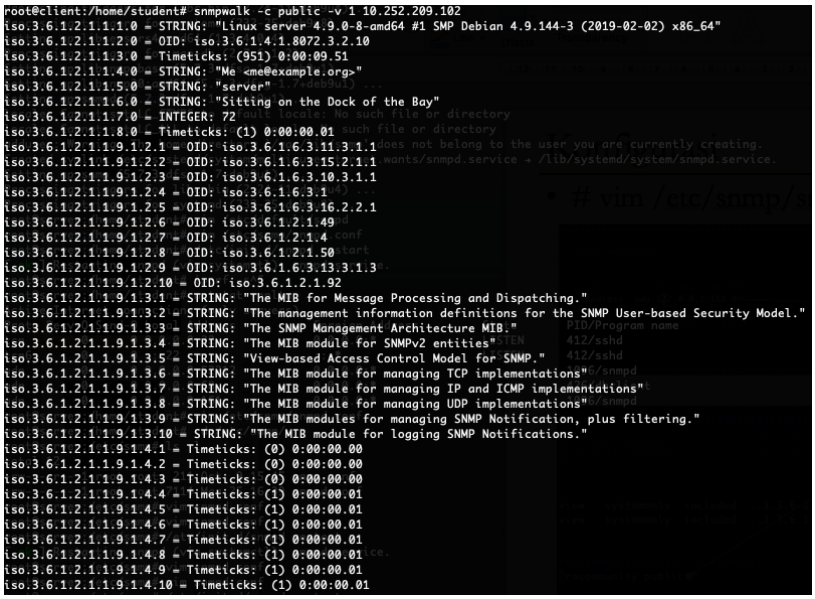
```
# apt-get install snmp snmpd
```

Sebelum snmpd dijalankan pada komputer server, maka snmpd harus dikonfigurasi dengan mengedit file "/etc/snmp/snmpd.conf" seperti yang tampak pada gambar 5.7. Setelah dilakukan edit terhadap file konfigurasi, selanjutnya layanan snmpd harus direstart dengan cara:

```
# service snmpd restart
```

Paket snmpd digunakan untuk menyajikan layanan snmp kepada komputer client dengan menggunakan paket snmpwalk yang terdapat pada paket snmp seperti yang tampak pada gambar 5.8.

Gambar 5.7. Konfigurasi snmpd.conf



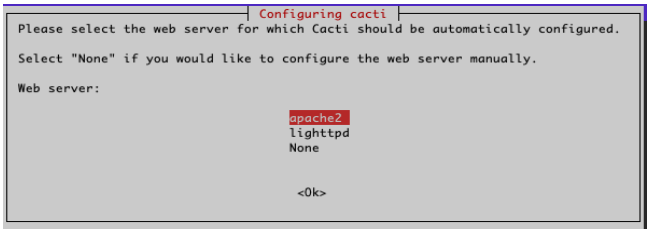
Gambar 5.8. Hasil uji coba akses snmp.

5. CACTI

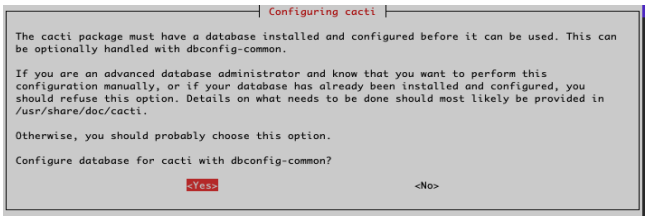
Dari gambar 5.8. masih berupa teks, selanjutnya data tersebut dapat diolah menjadi grafik yang memudahkan pengguna untuk menganalisanya. Aplikasi yang dapat digunakan untuk memproses data yang dihasilkan oleh SNMP salah satunya adalah Cacti. Instalasi Cacti dapat dilakukan dengan cara:

```
# apt-get install cacti cacti-spine
```

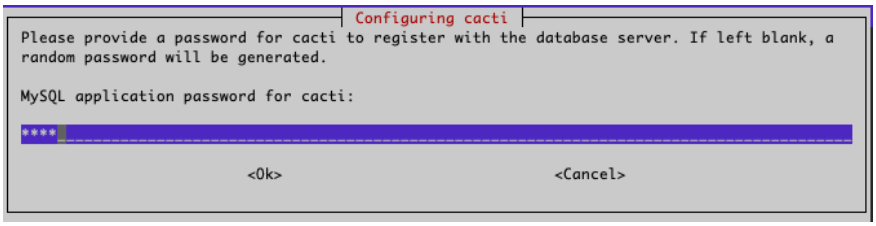
Proses installasi cacti tampak seperti pada gambar 5.9. Pada saat instalasi akan muncul beberapa pertanyaan diantaranya adalah jenis web server yang digunakan dan password baru untuk database cacti.



(a)



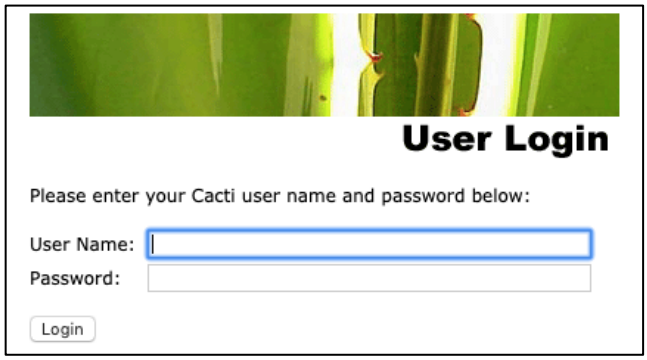
(b)



(c)

Gambar 5.9. Proses instalasi cacti

Setelah proses instalasi cacti telah selesai, selesai selanjutnya aplikasi cacti bisa dibuka dengan menggunakan browser dengan cara mengakses http://localhost/cacti seperti tampak pada gambar 5.10.

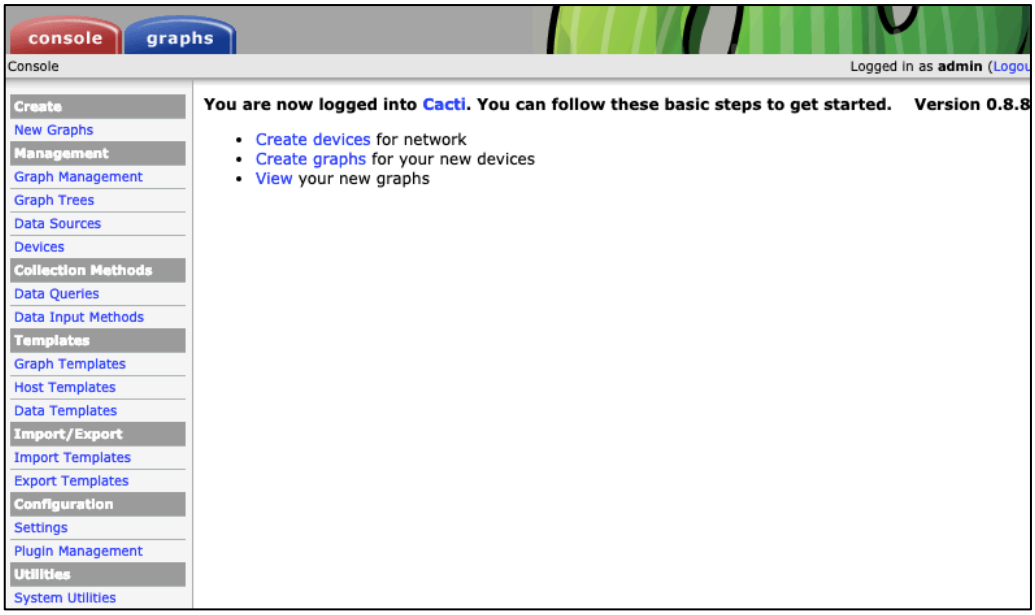


Gambar 5.10. Login pada aplikasi Cacti.

Namun untuk dapat melakukan login terhadap aplikasi Cacti maka kita harus melakukan reset terhadap passwordnya yaitu dengan cara:

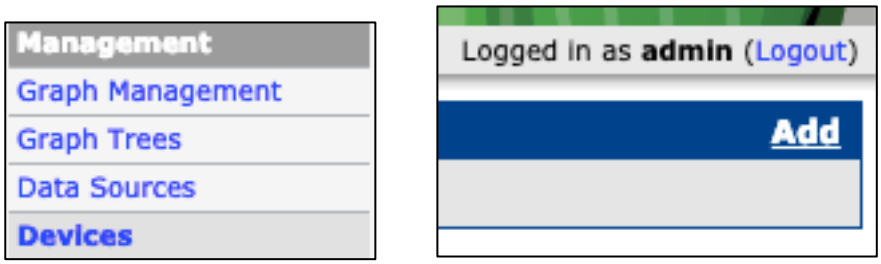
```
# mysql -u cacti -p cacti -e "UPDATE user_auth SET password=md5('admin') WHERE username='admin'";
```

Selanjutnya kita bisa login dengan menggunakan username “admin” dan password “admin” sehingga tampilan dilayar tampak seperti pada gambar 5.11.



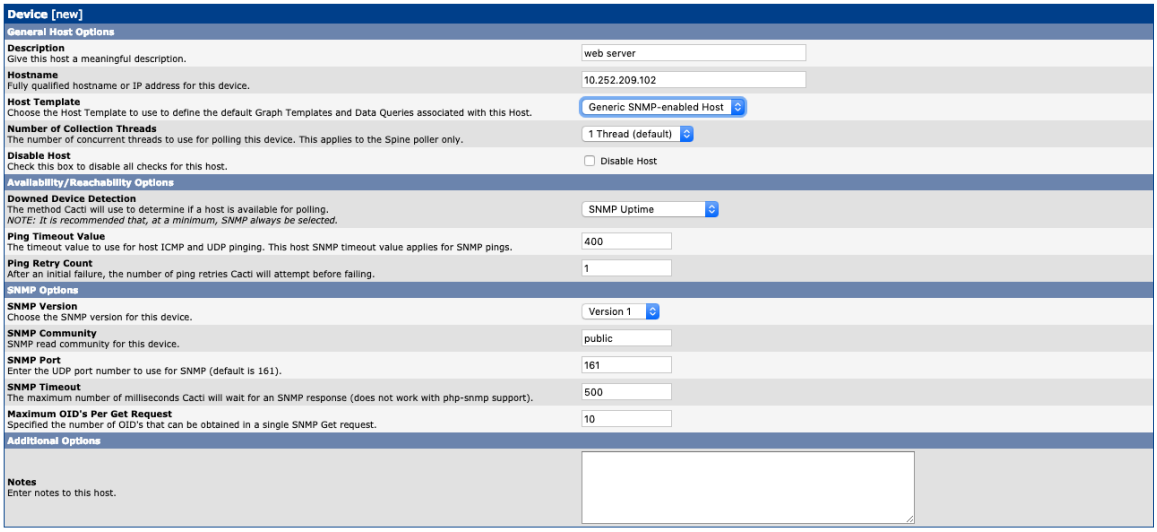
Gambar 5.11. Tampilan aplikasi Cacti setelah proses login.

Proses berikutnya adalah kita dapat menambahkan perangkat jaringan yang ingin di pantau dengan menggunakan aplikasi Cacti. Caranya dengan mengakses menu Device → Add seperti pada Gambar 5.12.



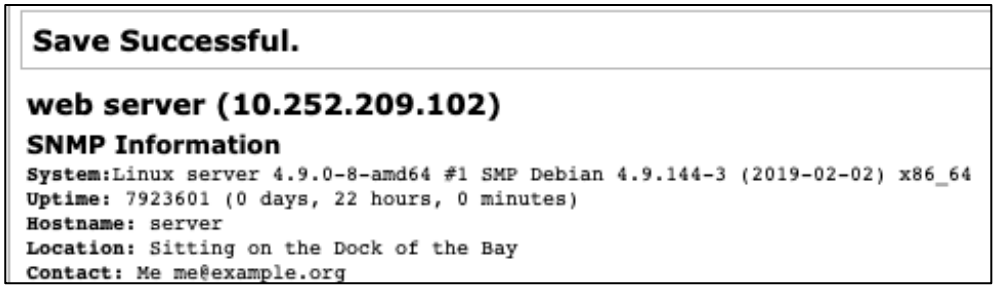
Gambar 5.12. Menu penambahan perangkat baru untuk dipantau.

Berikutnya kita dapat memasukkan data teknis mengenai perangkat yang kita targetnya diantaranya meliputi deskripsi, *hostname*, *host template*, dan lain-lain seperti tampak pada gambar 5.13.



Gambar 5.13. Halaman entri data perangkat jaringan.

Setelah proses entri data perangkat telah selesai maka jika aplikasi Cacti berhasil terhubung dengan perangkat jaringan akan ada notifikasi bahwa perangkat telah terkoneksi seperti tampak pada Gambar 5.14.

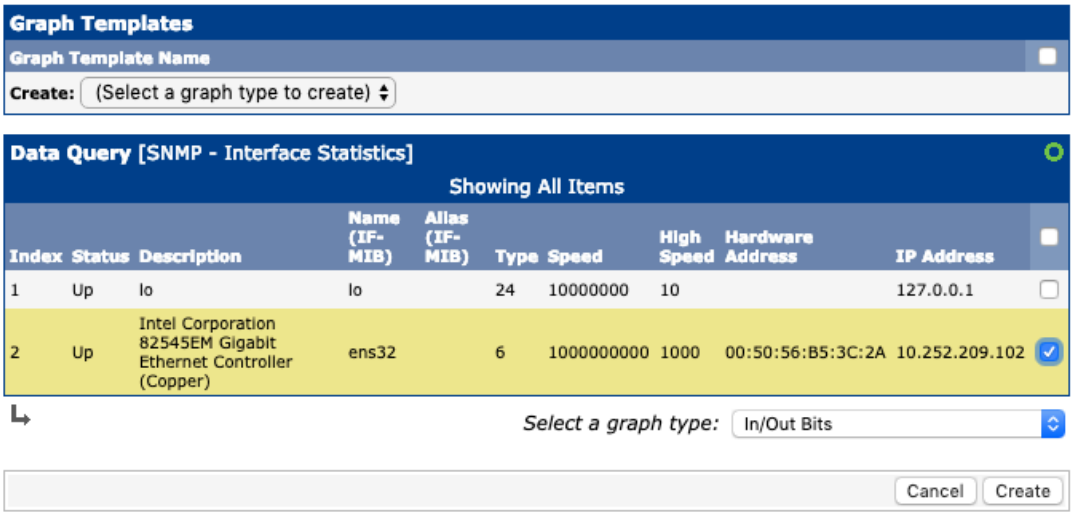


Gambar 5.14. Perangkat jaringan telah berhasil terhubung ke aplikasi Cacti.

Tahapan akhir dari konfigurasi Cacti adalah dengan pembuatan grafik dari data SNMP yang dikirimkan oleh perangkat jaringan yang akan dipantau dengan memilih menu “Create graph for this Host” seperti tampak pada gambar 5.15.

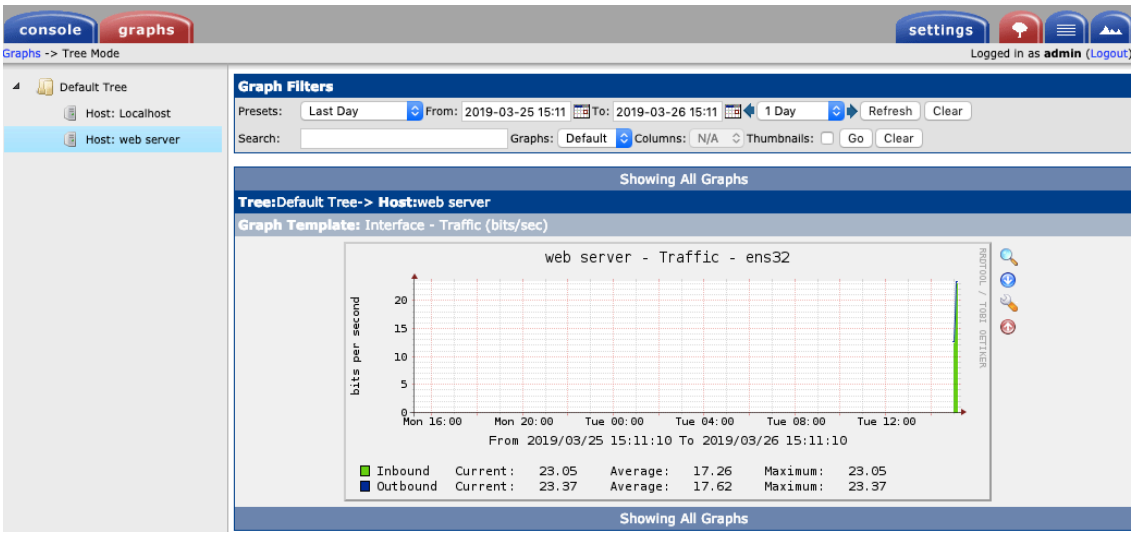
Gambar 5.15. Menu untuk membuat grafik baru.

Berikutnya kita dapat memilih antarmuka jaringan mana yang ingin dipantai seperti yang terlihat pada gambar 5.16.



Gambar 5.16. Pemilihan perangkat antarmuka jaringan.

Setelah beberapa menit maka grafik akan dibangkitkan oleh aplikasi Cacti yang dapat dilihat seperi pada gambar 5.17.



Gambar 5.17. Grafik kecepatan pengiriman data pada aplikasi Cacti.

1.5. TUGAS

1. Instal modul (add-on) pada aplikasi pada Cacti untuk dapat melihat ketersediaan (availability) layanan dari sebuah perangkat jaringan yang terpantau.
2. Instal NMS lain yang mirip dengan Cacti yaitu Nagios (Icinga), kemudian bedakan fitur-fitur antar kedua NMS tersebut

PERCOBAAN 6

Analisis dan Manajemen Log

1.1. TUJUAN

Tujuan dari pada percobaan 6 (Analisa dan Manajemen Log) ini adalah Mahasiswa mampu:

1. Mengatur log yang dihasilkan oleh beberapa aplikasi atau layanan jaringan seperti web server, proxy server, dan lain-lain.
2. Menggunakan berbagai aplikasi analisa dan pelaporan Log untuk proses pemecahan masalah jika terjadi kegagalan sistem atau layanan.
3. Memasang (install), mengkonfigurasi, serta menguji coba aplikasi Log server.

1.2. ALAT YANG DIGUNAKAN

Peralatan yang digunakan pada percobaan 6 diantaranya adalah:

1. Komputer
2. Switch
3. Aplikasi: SARG, AWSTAT, SysLog

1.3. DASAR TEORI

Hampir semua aplikasi yang beroperasi akan menghasilkan sebuah file pencatatan (Log) yang dapat digunakan untuk mengetahui kondisi atau proses yang sedang terjadi pada aplikasi tersebut. Seperti halnya pesawat terbang yang memilik “kotak hitam”, Log pada aplikasi akan dapat digunakan dikemudian hari untuk proses investigasi mengenai kinerja ataupun kegagalan yang dialami oleh aplikasi pada suatu waktu tertentu. Selain itu log juga membantu ketika ada aplikasi baru yang memiliki fitur-fitur baru yang masin pada fase pengembangan (*development*).

File log yang dihasilkan sebuah aplikasi hendaknya selalu dikelola dengan baik. Jika file log tidak dikelola dengan baik maka file log yang seharusnya dapat membantu System Administrator dalam melakukan penyelesaian masalah akan berubah menjadi pembuat masalah ketika file log tersebut dikonfigurasi dengan benar. Hal ini terjadi karena aplikasi terlalu sering melakukan pelaporan yang mengakibatkan media penyimpanan menjadi habis dan sistem operasi bisa menjadi terganggu operasionalnya. Untuk mengatasi hal tersebut maka System Administrator hendaknya memiliki kebijakan sebagai berikut:

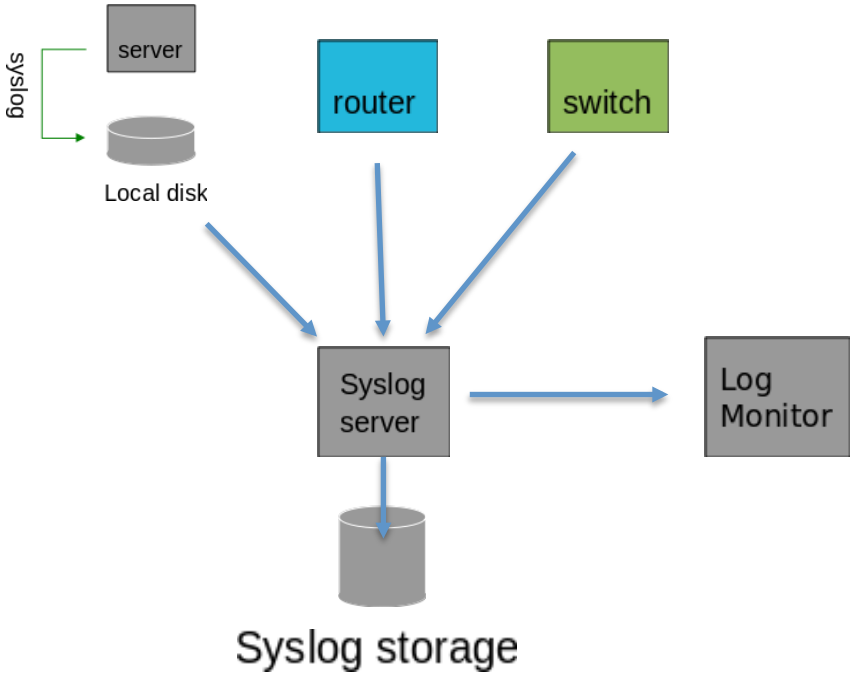
1. Mengatur ulang (*reset*) file log pada interval atau periode tertentu.
2. Melakukan rotasi log agar data tersedia untuk durasi waktu yang diinginkan.
3. Melakukan kompresi dan pengarsipan file lige pada media penyimpanan lainnya (misal: flash drive).

Terdapat beberapa jenis log yang dapat digunakan oleh System Administrator dalam mengelola jaringan diantaranya adalah:

1. Perangkat jaringan: log dari router, trafik jaringan, paket keluar dan masuk, penggunaan bandwidth, SNMP traps, dan lain-lain
2. Firewall: Paket keluar dan masuk, paket yang terblokir, dan lain-lain
3. Aplikasi server: log untuk web server, log untuk mail server, dan layanan lainnya.
4. Sistem Operasi: log keamanan, log aplikasi, log kernel dan lain-lain.

Tantangan utama dari log saat ini terbagi menjadi 4 bagian utama yaitu:

1. Volume: Data log bisa mencapai ratusan GB per hari dan tantangannya adalah mengkoleksi atau menyimpan data tersebut.
2. Normalization: Data log dihasilkan dengan berbagai macam format dan proses normalisasi akan berguna untuk proses analisa lebih lanjut.
3. Velocity: Kecepatan dalam menghasilkan log mengakibatkan kesulitan dalam koleksi dan agregasi.
4. Veracity: Aktifitas yang dilaporkan di-log mungkin tidak akurat, terutama permasalahan dari sistem-sistem yang menjalankan sistem deteksi seperti IDS.



Gambar 6.1. Arsitektur manajemen log.

Dalam mengoperasikan manajamen log, terdapat 3 komponen utama pada arsitektur sistem log yaitu seperti terlihat 6.1., ketiga komponen tersebut adalah:

- Pembangkitan log: komputer atau perangkat lainnya yang dapat menghasilkan log.

- Analisa dan penyimpanan log: komputer atau server yang menerima data log.
- Pemantauan log: komputer yang berfungsi untuk memantau atau *mereview* data log menjadi sebuah laporan.

1.4. PROSEDUR PERCOBAAN

Sebelum memulai percobaan maka langkah pertama adalah memastikan semua peralatan yang akan digunakan untuk praktikum dapat beroperasi dengan benar yaitu diantaranya adalah:

- Tes konektifitas

  Pastikan komputer yang digunakan telah terhubung ke jaringan dengan menggunkan perintah ping. Jika komputer belum terhubung ke jaringan maka hendaknya komputer diperiksa semua semua komponennya mulai dari sistem pengkabelan sampai dengan pengalamatan jaringannya.

- Repositori instalasi

  Karena PENS memiliki repositori yang menyediakan aplikasi atau paket-paket yang digunakan untuk praktikum maka hendaknya komputer yang akan digunakan untuk praktikum dipastikan konfigurasi repositori telah menggunakan repositori PENS yang beralamat di **kebo.pens.ac.id**

Jika komputer untuk uji coba telah dipastikan terhubung ke jaringan dan menggunakan repositori yang benar, maka percobaan dapat dilanjutkan sebagai berikut:

1. AWSTATS

   AWSTATS adalah sebuah aplikasi yang berfungsi untuk menampilkan statistik dari penggunaan layanan web (Apache2). Dengan menggunakan AWSTATS maka System Administrator dapat mengetahui jumlah pengunjung web, asal pengunjung, jenis peramban web yang digunakan, dan lain-lainnya sehingga sebelum adapun proses installasinya adalah:

```
# apt-get install awstat apache2
```

   Selanjutnya, karena AWSTATS menggunakan CGI maka modul tersebut harus kita aktifkan di apache2 dengan cara:

```
# a2enmod cgi
# systemclt restart apache2
```

   Setelah modul CGI aktif, lakukan konfigurasi AWSTATS dengan mengedit file konfigurasinya yaitu dengan cara:

```
# cp  /etc/awstats/awstats.conf   /etc/awstats/awstats.com0.eepis-its.edu.conf
# vim /etc/awstats/awstats.com0.c307.eepis-its.edu.conf
```

Sesuaikan isi file konfigurasi dengan domain yang akan dipantau seperti tampak pada gambar 6.2.

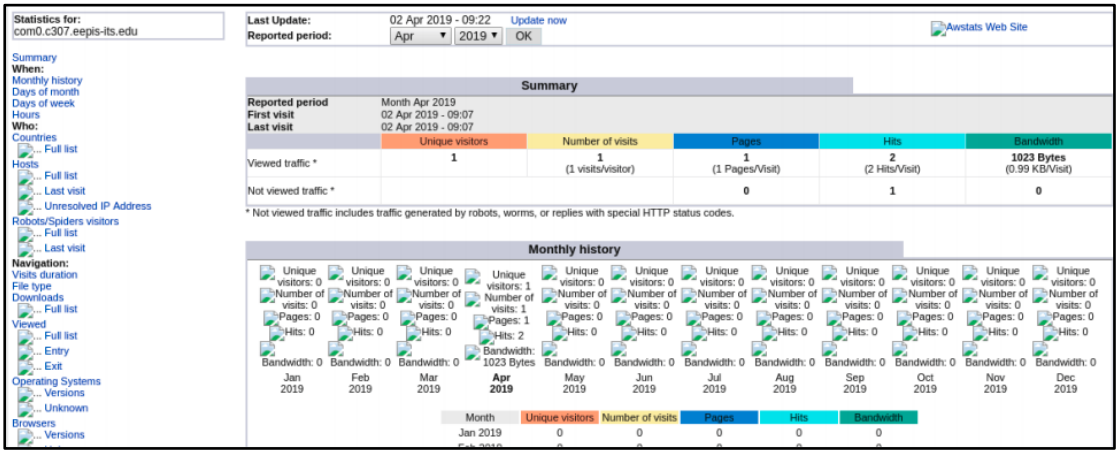
```
# Change to Apache log file, by default it's /var/log/apache2/access.log
LogFile="/var/log/apache2/access.log"

# Change to the website domain name
SiteDomain="com0.c307.eepis-its.edu"
HostAliases="www.com0.c307.eepis-its.edu localhost 127.0.0.1"

# When this parameter is set to 1, AWStats adds a button on report page to allow to "update"
statistics from a web browser
AllowToUpdateStatsFromBrowser=1
```

Gambar 6.2. Konfigurasi AWSTATS

Untuk mengetahui hasil dari konfigurasi update AWSTATS, lakukan perintah berikut ini:

```
# /usr/lib/cgi-bin/awstats.pl -config=com0.c307.eepis-its.edu -update
```

Kemudian buka peramban web dengan mengakses alamat http:///(domain)/cgi-bin/awstats.pl seperti tampak pada gambar 6.3.



Gambar 6.3. Tampilan AWSTATS

Dari gambar 6.3. tampak statistik dari web server sudah muncul, namun ada tampilan tidak sempurna karena hampir semua gambar tidak dapat tampil. Untuk memperbaikinya edit file "/etc/apache2/sites-enabled/com0.c307.eepis-its.edu.conf" dan tambahkan "Alias /awstats-icon /usr/share/awstats/icon" seperti tampak pada gambar 6.4.

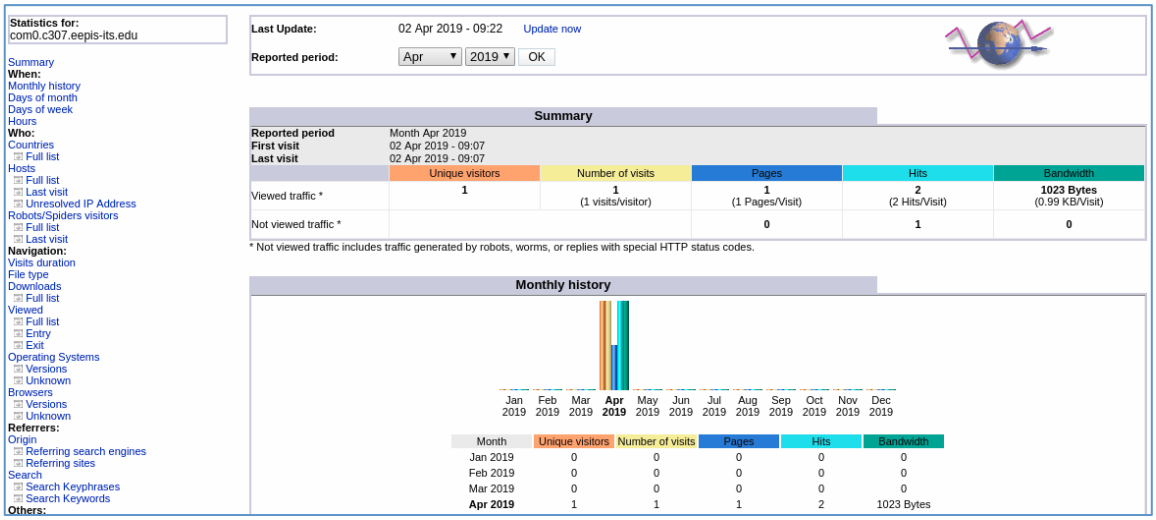
Selanjutnya reload layanan web server dengan cara:

```
# systemctl reload apache2
```

Selanjutnya reload peramban web untuk melihat hasil perubahan konfigurasinya seperti tampak pada gambar 6.5.

```
ServerName  com0.c307.eepis-its.edu
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/com0

Alias /awstats-icon /usr/share/awstats/icon/
```

Gambar 6.3. Konfigurasi apache2 dengan penambahan Alias untuk icon AWSTATS.



Gambar 6.4. Hasil update konfigurasi apache2

2. SARG

Squid Analysis Report Generator (SARG) merupakan sebuah aplikasi yang digunakan untuk menampilkan statistik untuk penggunaan layanan proxy (Squid). Untuk dapat menggunakan aplikasi ini maka untuk mengujicobanya diasumsikan aplikasi Squid sudah terinstall dan berjalan dengan baik. Selanjutnya SARG diinstall dengan cara:

```
# apt-get install sarg
```

Setelah melakukan instalasi, lanjutkan dengan melakukan konfigurasi dari SARG dengan mengedit file “/etc/sarg/sarg.conf” dengan cara:

```
# vim /etc/sarg/sarg.conf
```

Sesuaikan isi konfigurasi dari SARG seperti tampak pada gambar 6.5:

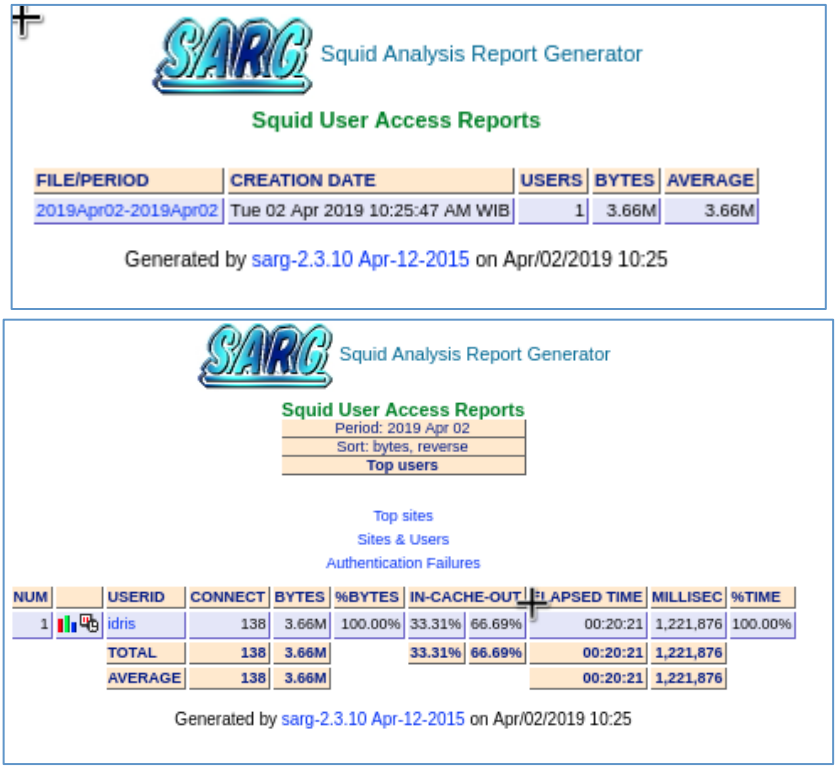
```
output_dir  /var/www/html/squid-reports
# output_dir  /var/lib/sarg
 resolve_ip   yes
```

Gambar 6.5. Konfigurasi SARG.

Selanjutnya update SARG untuk mendapatkan statiskin dari penggunaan layanan Squid dengan cara:

```
# sarg -c /etc/sarg/sarg.conf
```

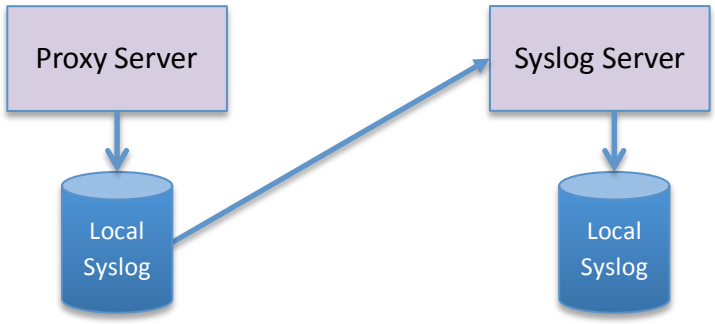
Hasil dari aplikasi SARG bisa diakses dengan cara mengaksesnya menggunakan peramban web dialamat “http://(domain)/squid-reports” seperti tampak pada gambar 6.6.



Gambar 6.6. Hasil akhir tampilan statistik pada aplikasi SARG.

3. SysLog

Syslog merupakan standar untuk pengiriman Log dari mesin pembangkit Log ke mesin penyimpan atau penganalisa Log. Untuk mengujicoba Syslog maka skenario topologinya adalah tampak seperti pada gambar 6.7.



Gambar 6.7. Skenario ujicoba Syslog.

Pada gambar 6.7, Proxy server dijalankan untuk menghasilkan file laporan atau Log yang akan dikirimkan ke mesin Log Server.

Untuk itu pada mesin Log Server diinstall aplikasi rsyslog dengan cara:

```
# apt-get install rsyslog
```

Kemudian lakukan konfigurasi pada rsyslog untuk dapat menerima komunikasi dari mesin pembangkit log (Squid) pada port tcp/514 dan udp/514 seperti dengan cara mengedit file "/etc/rsyslog.conf":

```
# vim /etc/rsyslog.conf
```

Lakukan penyesuaian konfigurasi rsyslog seperti tampak pada gambar 6.8.

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

#$AllowedServer UDP, 127.0.0.1, 10.252.209.0/24, 10.252.108.0/24
#$AllowedServer TCP, 127.0.0.1, 10.252.209.0/24, 10.252.108.0/24

$template FILENAME,"/var/log/%fromhost-ip%/%programname%.log"
*.* ?FILENAME


#############################
#### GLOBAL DIRECTIVES ####
#############################

#
                                                              26,1
```

Gambar 6.8. Konfigurasi rsyslog.

Setelah melakukan perubahan dan me-restart layanan rsyslog, pastikan rsyslog konfigurasi telah terimplementasi dengan benar dengan cara menggunakan netstat seperti tampak pada gambar 6.9.

```
root@debian:/home/student# /etc/init.d/rsyslog restart
[ ok ] Restarting rsyslog (via systemctl): rsyslog.service.
root@debian:/home/student# netstat -npltu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      435/sshd
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      519/rsyslogd
tcp6       0      0 :::22                   :::*                    LISTEN      435/sshd
tcp6       0      0 :::514                  :::*                    LISTEN      519/rsyslogd
udp        0      0 0.0.0.0:514             0.0.0.0:*                           519/rsyslogd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           451/dhclient
udp6       0      0 :::514                  :::*                                519/rsyslogd
root@debian:/home/student#
```

Gambar 6.9. Rsyslog sudah siap menerima komunikasi pada port 514

Berpindah pada mesin pembangkit log (Squid), lakukan perubahan pada file rsyslog seperti pada gambar 6.10.

```
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

local2.* @10.252.209.111:514
~
~
-- INSERT --                                                    93,1
```

Gambar 6.10. Konfigurasi rsyslog pada mesin server proxy.

Pada gambar 6.10 terlihat mesin pembangkit log akan mengirimkan log menuju ke mesin Log server di alamat 10.252.209.111 yang selanjutnya di mesin server log akan menerima log seperti tampak pada gambar 6.11.

```
root@debian:/var/log# cd 10.252.209.249/
root@debian:/var/log/10.252.209.249# ls
(squid-1).log
root@debian:/var/log/10.252.209.249# cat \(squid-1\).log
2019-04-02T12:39:41+07:00 debian (squid-1): 1554183581.529     58 10.252.214.49
2019-04-02T12:39:41+07:00 debian (squid-1): 1554183581.529     58 10.252.214.49
2019-04-02T12:40:04+07:00 debian (squid-1): 1554183604.611    108 10.252.214.49
2019-04-02T12:40:04+07:00 debian (squid-1): 1554183604.611    108 10.252.214.49
2019-04-02T12:40:06+07:00 debian (squid-1): 1554183606.882     19 10.252.214.49
2019-04-02T12:40:06+07:00 debian (squid-1): 1554183606.882     19 10.252.214.49
2019-04-02T12:40:09+07:00 debian (squid-1): 1554183609.365     27 10.252.214.49
2019-04-02T12:40:09+07:00 debian (squid-1): 1554183609.365     27 10.252.214.49
2019-04-02T12:40:10+07:00 debian (squid-1): 1554183610.565     11 10.252.214.49
2019-04-02T12:40:10+07:00 debian (squid-1): 1554183610.565     11 10.252.214.49
2019-04-02T12:40:11+07:00 debian (squid-1): 1554183611.538      5 10.252.214.49
2019-04-02T12:40:11+07:00 debian (squid-1): 1554183611.538      5 10.252.214.49
2019-04-02T12:40:30+07:00 debian (squid-1): 1554183630.437     39 10.252.214.49
2019-04-02T12:40:30+07:00 debian (squid-1): 1554183630.437     39 10.252.214.49
2019-04-02T12:40:41+07:00 debian (squid-1): 1554183641.405  61644 10.252.214.49
2019-04-02T12:40:41+07:00 debian (squid-1): 1554183641.405  61644 10.252.214.49
2019-04-02T12:40:41+07:00 debian (squid-1): 1554183641.408  60402 10.252.214.49
2019-04-02T12:40:41+07:00 debian (squid-1): 1554183641.408  60402 10.252.214.49
```

Gambar 6.11. Server Log telah menerima pelaporan dari server proxy (Squid).

1.5. TUGAS

1. Pasang/install aplikasi lain (misal. ftp) sebagai pembangkit log dan intergrasikan pelaporan log-nya ke server Log.