

**IMPLEMENTASI KEAMANAN JARINGAN TERHADAP
SERANGAN DNS CACHE POISONING MENGGUNAKAN
FIREWALL BERBASIS ROUTERBOARD MIKROTIK DI
SMAN 1 KOBA**

SKRIPSI



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG
2023**

**IMPLEMENTASI KEAMANAN JARINGAN TERHADAP
SERANGAN DNS CACHE POISONING MENGGUNAKAN
FIREWALL BERBASIS ROUTERBOARD MIKROTIK DI
SMAN 1 KOBA**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



Oleh:
SADAM MEIRIO ALDITYA

1911500087

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT SAINS DAN BISNIS ATMA LUHUR
PANGKALPINANG
2023**

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

Nim : 1911500087

Nama : Sadam Meirio Alditya

Judul Skripsi : IMPLEMENTASI KEAMANAN JARINGAN TERHADAP
SERANGAN *DNS CACHE POISONING* MENGGUNAKAN
FIREWALL BERBASIS *ROUTERBOARD MIKROTIK* DI
SMAN 1 KOBA

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Pangkalpinang, 17 Juli 2023



Sadam Meirio Alditya

LEMBAR PENGESAHAN SKRIPSI


**IMPLEMENTASI KEAMANAN JARINGAN TERHADAP SERANGAN *DNS*
CACHE POISONING MENGGUNAKAN *FIREWALL* BERBASIS
ROUTERBOARD MIKROTIK DI SMAN 1 KOBA**

Yang dipersiapkan dan disusun oleh

Sadam Meirio Alditya
1911500087

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 28 Juli 2023

Susunan Dewan Penguji
Anggota



Yohanes Setiawan, M.Kom
NIDN. 0219068501

Dosen Pembimbing



Dian Novianto, M.Kom
NIDN. 0209119001

Kaprodi Teknik Informatika




Chandra Kirana, M.Kom
NIDN. 0228108501

Ketua Penguji



Bambang Adiwino, M.Kom
NIDN. 0216107102

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 28 Juli 2023

DEKAN FAKULTAS TEKNOLOGI INFORMASI
ISB ATMA LUHUR




Ellya Helmud, M.Kom
NIDN. 0201027901

KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi Teknik Informatika Institut Sains dan Bisnis (ISB) Atma Luhur.

Penulis menyadari bahwa laporan skripsi ini masih jauh dari kata sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Ayah dan Emak juga keluarga yang tercinta, yang selalu memberikan dukungan baik moral, materi, doa, semangat dan kasih sayang.
3. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
4. Bapak Prof. Dr. Moedjiono, M.Sc, selaku Rektor ISB Atma Luhur.
5. Bapak Ellya Helmud, M.Kom, selaku Dekan Fakultas Teknologi Informasi.
6. Bapak Chandra Kirana, M.Kom, selaku Kaprodi Teknik Informatika.
7. Bapak Dian Novianto, M.Kom, selaku dosen pembimbing.
8. Bapak Yunisfu, M.Pd, selaku kepala SMAN 1 Koba.
9. Bapak Malfy Sandy selaku admin jaringan di SMAN 1 Koba.
10. Seluruh Guru dan Staff SMAN 1 Koba atas bantuan yang diberikan dalam melakukan penelitian dan memperoleh informasi yang diperlukan selama penulisan skripsi ini.
11. Endesti Anandita, Sirotin Amalia, dan seluruh keluarga yang terus memberikan semangat dalam menyelesaikan skripsi ini
12. Teman-teman tongkrongan Grup Hybrid, Putra Selindung, Genk Atok, Mahmud Racing dan semua pihak yang telah membantu hingga terselesaikannya skripsi ini.

13. Sahabat dan seluruh teman-teman seperjuangan angkatan 2019 yang telah memberikan dukungan moral untuk terus menyelesaikan skripsi ini.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Pangkalpinang, Juli 2023

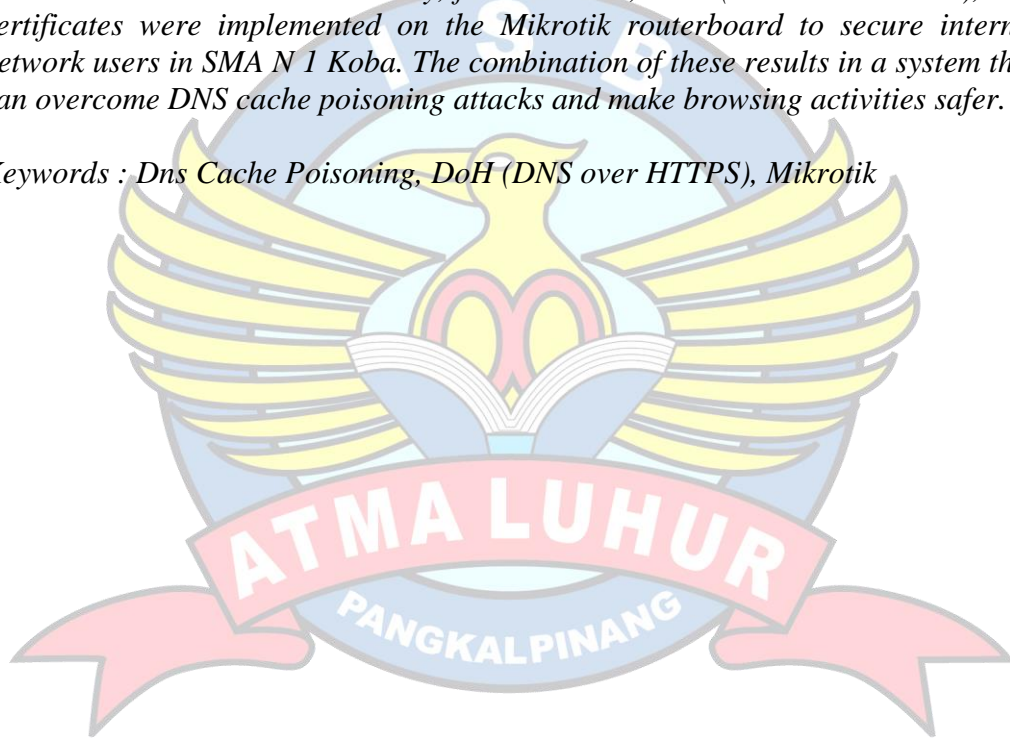
Penulis



ABSTRACT

The high number of network users in SMA N 1 Koba can lead to the occurrence of misuse or cybercrime. There have been many cases circulating about cyber crimes that have frequently occurred lately and continue to increase. One of the methods used to commit this crime is through DNS cache poisoning. DNS cache poisoning is a type of attack that exploits vulnerabilities in the Domain Name System (DNS) to redirect traffic from legitimate websites to fake ones, which can also occur on the SMA N 1 Koba network. To overcome this problem, the method used is a filter rule combined with DoH (DNS over HTTPS) and certificates. The PPDIIO (Prepare, Plan, Design, Implement, Operate, Optimize) method is used as the methodology in this research, and data is collected through observation, interviews, and literature studies. In this study, firewall rules, DoH (DNS over HTTPS), and certificates were implemented on the Mikrotik routerboard to secure internet network users in SMA N 1 Koba. The combination of these results in a system that can overcome DNS cache poisoning attacks and make browsing activities safer.

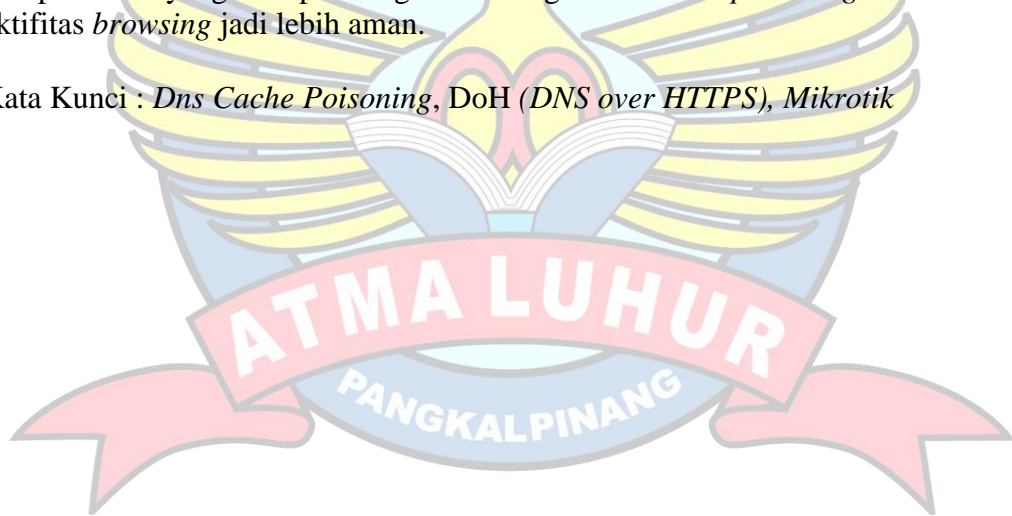
Keywords : Dns Cache Poisoning, DoH (DNS over HTTPS), Mikrotik



ABSTRAK

Banyaknya pengguna jaringan pada SMA N 1 Koba dapat menimbulkan terjadinya penyalahgunaan atau kejahatan *cyber*. Sudah banyak kasus yang beredar tentang kejahatan *cyber* yang sering terjadi akhir-akhir ini dan terus meningkat. Salah satu cara yang digunakan untuk melakukan tindak kejahatan ini yaitu melakukan *dns cache poisoning*. *Dns cache poisoning* adalah jenis serangan yang mengeksploitasi kerentanan dalam sistem nama domain (DNS) untuk mengalihkan lalu lintas dari situs web yang sah dan menuju yang situs yang palsu, hal ini juga bisa terjadi pada jaringan SMA N 1 Koba. Untuk mengatasi permasalahan tersebut metode yang digunakan adalah *filter rule* yang dikombinasikan dengan DoH (*DNS over HTTPS*), *certificate*. Metode PPDIOO (*Prepare, Plan, Design, Implement, Operate, Optimize*) digunakan sebagai metodologi yang digunakan dalam penelitian ini, teknik pengumpulan data yaitu dengan melakukan observasi, wawancara, dan studi pustaka (literatur). Pada Penelitian ini dilakukan implementasi *firewall rule*, DoH (*DNS over HTTPS*), *certificate* pada *routerboard mikrotik*. Implementasi ini dilakukan untuk mengamankan pengguna jaringan internet di SMA N 1 Koba menggunakan *routerboard mikrotik RB951Ui*. Dan hasil kombinasi tersebut berupa sistem yang mampu mengatasi serangan *dns cache poisoning* dan membuat aktifitas *browsing* jadi lebih aman.

Kata Kunci : *Dns Cache Poisoning, DoH (DNS over HTTPS), Mikrotik*



DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN SKRIPSI	ii
KATA PENGANTAR	ii
ABSTRACT	v
ABSTRAK	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR SIMBOL	xiii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penulisan	3
1.4.1 Tujuan Penelitian	3
1.4.2 Manfaat Penelitian.....	3
1.5 Sistematika Penulisan	4
BAB II LANDASAN TEORI	5
2.1 Model Pengembangan Jaringan Komputer.....	5
2.1.1 Model PPDIOO	5
2.2 Tools Pengembang Jaringan	6
2.2.1 UML	6
2.3 Teori Pendukung.....	7
2.3.1 Jaringan Komputer	7
2.3.2 LAN	8
2.3.3 Topologi Jaringan	8
2.3.4 Topologi Star	8

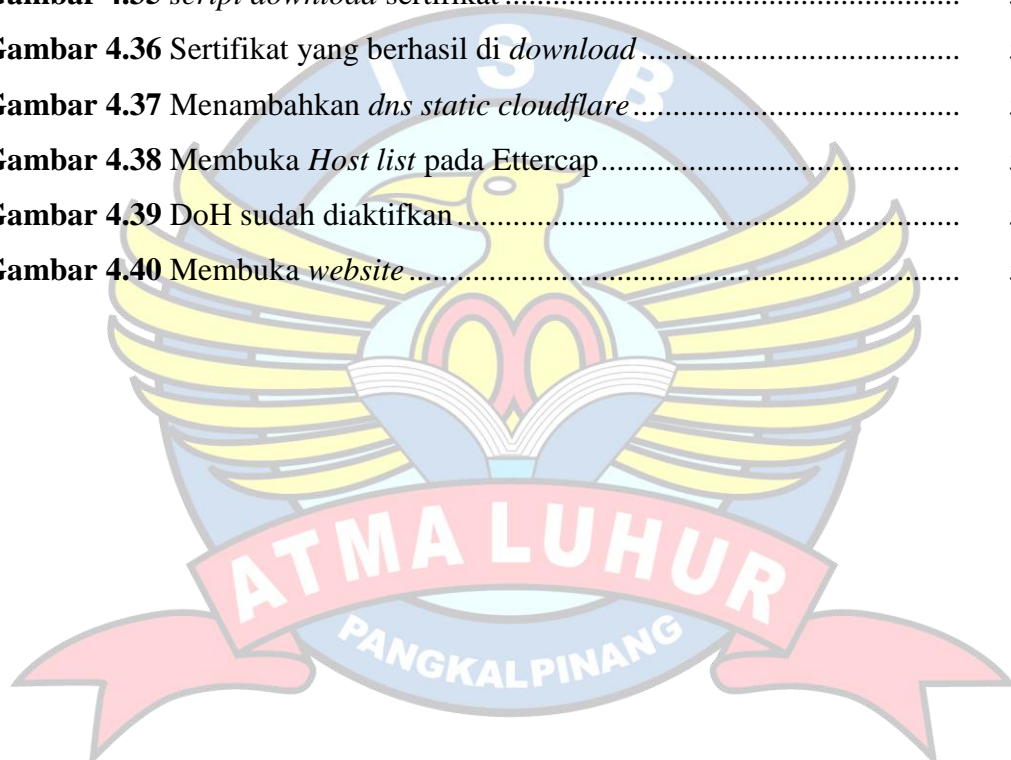
2.3.5	Internet.....	9
2.3.6	TCP/IP	9
2.3.7	DNS	9
2.3.8	Router	10
2.3.9	Mikrotik	10
2.3.10	Mikrotik Routerboard.....	11
2.3.11	Mikrotik RouterOS.....	11
2.3.12	Switch	11
2.3.13	Modem	12
2.3.14	Kabel UTP.....	12
2.3.15	RJ45.....	12
2.3.16	Keamanan Jaringan.....	13
2.3.17	Ancaman Keamanan Jaringan.....	13
2.3.18	Dns Cache Poisoning	14
2.3.19	Firewall	15
2.3.20	Kali Linux.....	15
2.3.21	Cisco Packet Tracer	15
2.3.22	Winbox	16
2.3.23	Ettercap	16
2.3.24	Oracle VM Virutal Box.....	16
2.4	Peneliti Terdahulu.....	17
BAB III METODOLOGI PENELITIAN		19
3.1	Model Pengembangan Jaringan	19
3.2	Teknik Pengumpulan Data	20
3.3	Alat Bantu Pengembangan Sistem.....	21
3.3.1	Use Case Diagram	21

3.3.2	<i>Activity Diagram</i>	21
3.3.3	<i>Deployment Diagram</i>	21
BAB IV HASIL DAN PEMBAHASAN		22
4.1	Profil Sekolah	22
4.1.1	Sejarah Singkat SMAN 1 KOBA	22
4.1.2	Visi dan Misi	23
4.1.3	Struktur Organisasi	23
4.1.4	Tugas dan Wewenang	24
4.2	Analisa Masalah	31
4.2.1	Solusi Pemecahan Masalah	31
4.2.2	Analisa Kebutuhan Sistem	31
4.3	Perancangan Sistem	33
4.3.1	Desain Topologi Jaringan	33
4.3.2	Desain <i>Use Case Diagram</i>	36
4.3.3	Desain <i>Activity Diagram</i>	37
4.3.4	Desain <i>Deployment Diagram</i>	40
4.4	Implementasi	41
4.4.1	Konfigurasi Awal	41
4.4.2	Uji coba serangan sebelum <i>firewall</i> diimplementasi	47
4.4.3	Konfigurasi <i>Firewall</i>	52
4.4.4	Uji coba serangan setelah <i>firewall</i> diimplementasi	58
BAB V PENUTUP		60
5.1	Kesimpulan	60
5.2	Saran	60
DAFTAR PUSTAKA		61
LAMPIRAN		63

DAFTAR GAMBAR

Gambar 2.1	Model PPDIOO[9].....	5
Gambar 2.2	Router[14].....	10
Gambar 2.3	Switch[14]	12
Gambar 4.1	Struktur Organisasi SMAN 1 KOBA.....	23
Gambar 4.2	Topologi jaringan gedung utama yang sedang berjalan.....	33
Gambar 4.3	Topologi Jaringan gedung laboratorium komputer	34
Gambar 4.4	Topologi jaringan usulan gedung utama	35
Gambar 4.5	Topologi jaringan usulan gedung laboratorium komputer	36
Gambar 4.6	<i>Use Case Diagram</i> Usulan	37
Gambar 4.7	Desain <i>activity diagram</i> berjalan.....	38
Gambar 4.8	Desain <i>activity diagram</i> usulan	39
Gambar 4.9	<i>Deployment Diagram</i> berjalan	40
Gambar 4.10	<i>Deployment diagram</i> usulan	41
Gambar 4.11	Halaman Awal Winbox	41
Gambar 4.12	Menambah <i>ip address client</i>	42
Gambar 4.13	<i>DHCP Server Interface</i>	43
Gambar 4.14	<i>DHCP Address Space</i>	43
Gambar 4.15	<i>Gateway for DHCP Network</i>	44
Gambar 4.16	<i>Address to Give Out</i>	44
Gambar 4.17	<i>DNS Server</i>	45
Gambar 4.18	<i>Lease Time</i>	45
Gambar 4.19	Konfigurasi DNS	46
Gambar 4.20	mengkonfigurasi NAT	47
Gambar 4.21	Tampilan <i>Login KaliLinux</i>	48
Gambar 4.22	Tampilan Konfigurasi <i>Ettercap dns</i>	48
Gambar 4.23	Tampilan file html	49
Gambar 4.24	Tampilan Utama <i>Ettercap</i>	49
Gambar 4.25	Tampilan konfigurasi <i>ARP Poisoning</i>	50
Gambar 4.26	Tampilan konfigurasi <i>dns spoof</i>	50

Gambar 4.27 Tampilan <i>Website</i> terkena serangan	51
Gambar 4.28 Tampilan Halaman <i>Plugin</i> pada <i>Ettercap</i>	51
Gambar 4.29 Menambahkan <i>filter rule</i>	52
Gambar 4.30 Menambahkan <i>address list</i>	53
Gambar 4.31 Menambahkan NAT	53
Gambar 4.32 Memodifikasi dhcp server	54
Gambar 4.33 <i>Use DoH Server</i> dan <i>verify DoH Certificate</i>	55
Gambar 4.34 sebelum sertifikat di <i>download</i>	55
Gambar 4.35 <i>script download</i> sertifikat	56
Gambar 4.36 Sertifikat yang berhasil di <i>download</i>	56
Gambar 4.37 Menambahkan <i>dns static cloudflare</i>	57
Gambar 4.38 Membuka <i>Host list</i> pada <i>Ettercap</i>	58
Gambar 4.39 DoH sudah diaktifkan.....	58
Gambar 4.40 Membuka <i>website</i>	59





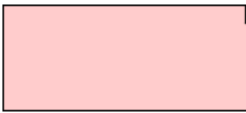

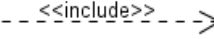
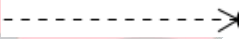
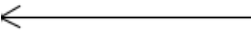


DAFTAR TABEL


Tabel 2.1	Peneliti Terdahulu	17
Tabel 3.1	Perencanaan Kebutuhan	19
Tabel 4.1	Spesifikasi <i>Hardware</i>	31
Tabel 4.2	Spesifikasi <i>Software</i>	32








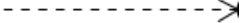

DAFTAR SIMBOL

1. Usecase Diagram

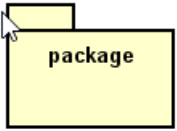
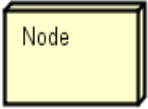


No	Gambar	Nama	Keterangan
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i>
2		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu <i>actor</i>
3		<i>Note</i>	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputansi
4		<i>System</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas
5		<i>Include</i>	Menspesifikasikan bahwa <i>use case</i> sumber secara eksplisit
6		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri
7		<i>Generalization</i>	Hubungan dimana objek anak (<i>decendent</i>) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (<i>ancestor</i>)
8		<i>Extend</i>	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan
9		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya.

10		<i>Collaboration</i>	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya
----	---	----------------------	--







2. Activity Diagram



No	Gambar	Nama	Keterangan
1		<i>Nary Associat</i>	Upaya untuk menghindari asosiasi dengan lebih dari 2 objek
2		<i>Generalization</i>	Hubungan dimana objek anak (<i>decendent</i>) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (<i>ancestor</i>)
3		<i>Collaboration</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
4		<i>Class</i>	Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama
5		<i>Realization</i>	Operasi yang benar-benar dilakukan oleh suatu objek
6		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri
7		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya

3. Deployment Diagram

No	Gambar	Nama	Keterangan
1		<i>Package</i>	Untuk mengelompokkan satu atau lebih <i>node</i>
2		<i>Node</i>	Biasanya mengacu pada <i>hardware</i> dan <i>software</i>
3		<i>Link</i>	Relasi antara <i>node</i>
4		<i>Dependency</i>	Kebergantungan antar <i>node</i> , arah panah mengarah pada <i>node</i> yang dipakai

4. Simbol Perangkat Jaringan

No	Gambar	Nama	Keterangan
1		<i>Cloud</i>	untuk menggambarkan <i>internet</i>
2		<i>Modem</i>	Mengubah sinyal digital menjadi sinyal analog atau sebaliknya
3		<i>Router</i>	Menghubungkan dua atau lebih jaringan yang berbeda untuk menghubungkan jaringan lokal ke jaringan luar seperti internet
4		<i>Switch</i>	Menghubungkan beberapa perangkat jaringan di dalam sebuah jaringan LAN
5		<i>Access Point</i>	Untuk menyediakan jaringan nirkabel (wireless) di dalam sebuah jaringan LAN
6		Komputer	Untuk menggambarkan perangkat komputer di dalam jaringan

- | | | | |
|---|---|------------|---|
| 7 |  | Laptop | Untuk menggambarkan perangkat laptop di dalam jaringan |
| 8 |  | Smartphone | Untuk menggambarkan perangkat <i>smartphone</i> atau <i>mobile device</i> di dalam jaringan |

