

Undang Syaripudin.,M.Kom
Drs.Asep Herdi.,M.Ag

PERANCANGAN BLUEPRINT PENGEMBANGAN TIK UIN SUNAN GUNUNG DJATI BANDUNG



Tahun
2016

ISBN 978-602-5823-36-7



9 786025 823367

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan laporan penelitian dengan judul “Perancangan Blueprint Pengembangan TIK UIN Sunan Gunung Djati Bandung”.

Berdasarkan sebuah proses yang partisipatif bersama dari para civitas akademika; Fakultas, Lembaga, Biro, Bagian dan unit-unit kerja lainnya sehingga dihasilkanlah suatu pedoman yang memberikan kesamaan pola pikir, visi dan misi dalam pemanfaatan teknologi informasi (TIK).

UIN Sunan Gunung Djati berharap, cetak biru (*blueprint*) yang dirancang dapat menjadi langkah besar untuk pengembangan teknologi informasi yang akan dilakukan serta diharapkan dapat berjalan lebih baik lagi, lebih terstruktur, lebih terukur dan tepat sasaran.

Blueprint teknologi informasi ini merupakan dokumen yang bersifat dinamis, sehingga isinya akan selalu dimutakhirkan sesuai perkembangan dan pelaksanaan dilapangan oleh karenanya dukungan dari berbagai pihak, terutama civitas akademika sangat diharapkan.

Pada kesempatan ini pula penulis ingin menyampaikan terima kasih kepada pihak-pihak yang telah mendukung dalam penyusunan blueprint teknologi informasi ini, yaitu para pimpinan dari fakultas, lembaga, biro, bagian dan unit-unit kerja lainnya.

Penghargaan yang tinggi penulis sampaikan kepada para anggota tim penyusun dan tim perumus dari blueprint teknologi informasi UIN Sunan Gunung Djati Bandung ini. Semoga kerja keras kita menjadi pemicu bagi semua pihak untuk bergerak mencapai terwujudnya “UIN Sunan Gunung Djati Bandung menjadi Universitas Islam Negeri yang unggul dan kompetitif berbasis wahyu memandu ilmu dalam bingkai akhlak karimah di ASEAN tahun 2025”.

Bandung, November 2016

Penulis

DAFTAR ISI

KATA PENGANTAR	i
DAFTAR ISI.....	iii
DAFTAR GAMBAR	vi
DAFTAR TABEL.....	vii
1. PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Tujuan Penelitian	2
1.4 Batasan Masalah	2
1.5 Metodologi.....	3
1.6 Sistematika Penulisan	3
2. TINJAUAN PUSTAKA	5
2.1 Peta Tinjauan Pustaka.....	5
2.2 Profil UIN Sunan Gunung Djati Bandung.....	5
2.3 Teknologi Informasi dan Komunikasi (TIK).....	6
2.4 Perancangan Arsitektur Enterprise	8
3. METODOLOGI PENELITIAN.....	11
3.1 <i>Design Science Research Methodology</i>	11
3.2 Metode yang Digunakan.....	13
3.3 Penjelasan Tahapan Penelitian	13
3.3.1 Identifikasi Masalah.....	13
3.3.2 Tujuan Penelitian	13
3.3.3 Desain dan Pengembangan.....	13
3.3.4 Demonstrasi.....	14
3.3.5 Evaluasi	14
3.3.6 Komunikasi	14
4. HASIL PENELITIAN.....	15
4.1 Kasus Bisnis.....	15
4.2 Keperluan Bisnis Keseluruhan.....	15
4.2.1 Keperluan Bisnis Untuk Perbaikan Infrastruktur	16
4.2.2 Kepentingan PTIPD Untuk Perbaikan Infrastruktur	17
4.3 Perencanaan Blueprint	18
4.4 Jaringan Terpasang	19

4.4.1	Protokol Routing	19
4.4.2	Wireless.....	19
4.4.3	Manajemen Jaringan	19
4.4.4	Keamanan Jaringan	20
4.5	Model Arsitektur.....	20
4.5.1	Topologi	21
4.5.2	Lapisan Inti (<i>Core Layer</i>).....	21
4.5.3	Lapisan Distribusi (<i>Distribution Layer</i>).....	22
4.5.3.1	Pusat Data–Area Kampus 1/Kampus 2.....	23
4.5.3.2	Bangunan Lapisan Distribusi Jauh.....	23
4.5.3.3	WAN & Konektivitas Internet	24
4.5.4	Lapisan Akses - Full Redundancy.....	24
4.5.4.1	Bangunan Tipe A1 (A2 Untuk Redundansi Terbatas) ...	25
4.5.4.2	Bangunan Tipe B1 (B2 Untuk Redundansi Terbatas)....	25
4.5.4.3	Bangunan Tipe C1 (C2 Untuk Redundansi Terbatas)....	25
4.5.4.4	Bangunan Tipe D1 (D2 Untuk Redundansi Terbatas) ...	26
4.5.5	Lapisan Akses – No Redundancy.....	26
4.5.6	Wireless.....	27
4.5.7	Model Data Center	28
4.5.8	Jaringan Residensial	29
5.	PEMBAHASAN	32
5.1	Model Logis	32
5.1.1	Jaringan Inti (Core Network)	32
5.1.2	Area Bangunan.....	33
5.1.3	Jaringan Akses (Access Network).....	33
5.1.4	Protokol Routing	34
5.1.5	Daerah Wewenang VTP.....	35
5.1.6	Port Trunk	35
5.1.7	Port Uplink.....	35
5.2	Manajemen Jaringan	36
5.2.1	Pelaksanaan Khusus UINSGDNet	36
5.2.2	Manajemen Jaringan - Perangkat Keras.....	38
5.2.3	Manajemen Jaringan - Perangkat Lunak	38
5.2.4	Migrasi	39
5.2.5	Fitur CiscoWorks	40
5.2.6	Dukungan dari Jauh (<i>Remote Support</i>)	42
5.2.7	Pelayanan-pelayanan Monitoring, Automation & Response Centre (MARC)	43
5.3	Keamanan Jaringan.....	43
5.3.1	Model Manajemen Keamanan	43
5.3.2	Keamanan Lapisan Akses 802.1X	44
5.3.3	Keamanan LAN	45
5.3.4	Cisco Clean Access	46

5.3.5	Network Admission Control	48
5.3.6	Keamanan Perangkat Jaringan	49
5.4	Proses Migrasi.....	50
5.4.1	Prasyarat Migrasi	50
5.4.2	Tahap-Tahap Migrasi	50
5.4.2.1	Tahap 1 (Core Network Services).....	51
5.4.2.2	Tahap 2 (Jaringan Distribusi).....	53
5.4.2.3	Tahap 3 (Integrasi Jaringan)	56
5.4.2.4	Tahap 4 (Pilot)	56
5.4.2.5	Tahap 5 (Rollout).....	57
5.4.2.6	Tahap 6 (Remote Campus)	58
5.5	Integrasi Bisnis	59
5.5.1	Proses yang Diikuti	59
5.5.2	Keperluan Jaringan Wireless.....	59
5.6	Teknologi Masa Depan.....	60
5.6.1	Telephony.....	60
5.6.1.1	Tinjauan Umum	60
5.6.1.2	Keuntungan Teknis	61
5.6.1.3	Keuntungan Bisnis	61
5.6.1.4	Kebutuhan Implementasi (Lapisan Jaringan).....	62
5.6.2	IPv6	62
5.6.2.1	Tinjauan Umum	62
5.6.2.2	Keuntungan Teknis	63
5.6.2.3	Keuntungan Bisnis	63
5.6.2.4	Kebutuhan Implementasi (Lapisan Jaringan).....	68
5.6.2.5	Switch-Switch Layer 2.....	68
5.6.3	Content Networking	69
5.6.3.1	Tinjauan Umum	69
5.6.3.2	Keuntungan teknis	69
5.6.3.3	Keuntungan Bisnis	70
5.6.3.4	Kebutuhan Implementasi (Lapisan Jaringan).....	71
5.6.4	IPTV	71
5.6.4.1	Tinjauan Umum	71
5.6.4.2	Keuntungan Teknis	72
5.6.4.3	Keuntungan Bisnis	72
5.6.4.4	Kebutuhan Implementasi (Lapisan Jaringan).....	72
6.	SIMPULAN DAN SARAN	74
6.1	Simpulan	74
6.2	Saran	74
	DAFTAR PUSTAKA	75

DAFTAR GAMBAR

Gambar 2.1 Literature Map.....	5
Gambar 2.2 Hirarki Arsitektur Sistem	8
Gambar 2.3 Arsitektur TOGAF	9
Gambar 3.1 <i>Framework</i> DSRM.....	12
Gambar 3.2 Tahapan Penelitian	13
Gambar 4.1 Area Jaringan Inti (Core Network).....	21
Gambar 4.2 Area Lapisan Distribusi.....	23
Gambar 4.3 Arsitektur Lapisan Akses (Full Redundancy)	24
Gambar 4.4 Arsitektur Lapisan Akses (No Redundancy).....	26
Gambar 4.5 Arsitektur Data Center	28
Gambar 4.6 Arsitektur Jaringan Residensial.....	30
Gambar 5.1 Model Flow CCA.....	47
Gambar 5.2 Arsitektur NAC	49
Gambar 5.3 Fase Migrasi	51
Gambar 5.4 Migrasi Remote Campus.....	58
Gambar 5.5 Migrasi IPv6.....	65
Gambar 5.6 Content Networking	71

DAFTAR TABEL

Tabel 3.1 Panduan DSRM	11
Tabel 5.1 Alokasi IP Address Area Core	32
Tabel 5.2 Penggunaan IP Address	33
Tabel 5.3 Alokasi IP Address Area Gedung	34
Tabel 5.4 Area OSPF	34
Tabel 5.5 Domain VTP	35
Tabel 5.6 Model Manajemen Jaringan.....	36
Tabel 5.7 Model Manajemen Keamanan	43
Tabel 5.8 Perangkat Mendukung IPv6.....	68

1. PENDAHULUAN

1.1 Latar Belakang

Sebagaimana telah diamanatkan dalam Rencana Strategis (Renstra) UIN Sunan Gunung Djati 2015-2019, UIN Sunan Gunung Djati Bandung (UINSGD) memiliki tanggung jawab besar untuk menjadi institusi pendidikan tinggi yang unggul dan mampu membarui masyarakat Indonesia memasuki era *knowledge society*. Salah satu ciri utama era ini adalah berkembangnya Teknologi Informasi dan Komunikasi (*Information and Communication Technology*) untuk selanjutnya disingkat TIK, yang sangat mempengaruhi tingkat kemajuan, kemakmuran, dan daya saing suatu bangsa.

Dengan penerapan yang tepat, TIK sanggup memberdayakan dan mencerdaskan masyarakat ke tingkat kemajuan yang lebih tinggi. Dalam skala mikro, UINSGD meyakini sepenuhnya bahwa hanya dengan melalui TIK yang tepat, visi dan misi UINSGD segera dapat direalisasikan. Dengan demikian pengembangan UINSGD sebagai *ICT-Based Campus* merupakan suatu keniscayaan. Penerapan TIK yang tepat menuntut masyarakat kampus dan lingkungannya serta civitas akademika UINSGD untuk mampu menguasai teknologi ini sebagai salah satu kompetensi intinya. Dengan kata lain, tujuan pengembangan TIK di UINSGD harus diarahkan untuk mendukung tercapainya visi dan misi UINSGD dan meningkatkan peran civitas akademika UINSGD untuk membarui masyarakat Indonesia memasuki era pengetahuan. Pada saat yang sama pula, civitas akademika UINSGD menguasai TIK sebagai sebuah kompetensi sesuai bidangnya.

Proses pengembangan TIK di UINSGD sepenuhnya diarahkan pada pencapaian visi UINSGD sebagai pusat pengembangan budaya peradaban Islam. Sejalan dengan hal tersebut, maka arah pengembangan TIK UINSGD adalah *ICT-Based Campus* yaitu suatu lingkungan kampus yang didukung oleh layanan-layanan TIK yang memadai. Untuk menuju arah tersebut perlu diidentifikasi program dan aktivitas, fasilitas fisik, dan sumber daya yang berada dalam suatu sistem TIK terintegrasi. Layanan-layanan TIK UINSGD yang baik akan meningkatkan peran civitas akademika Unhas untuk menghasilkan ilmu pengetahuan, teknologi dan seni, serta konten yang dibutuhkan masyarakat dan industri. Dengan demikian, misi UINSGD sebagai *knowledge server* dapat dilaksanakan dengan efektif, efisien dan akuntabel.

Fungsi utama dari sistem *ICT-Based Campus* di UINSGD adalah menyediakan layanan informasi, komputasi, dan komunikasi secara terintegrasi pada semua anggota civitas akademika dan masyarakat luar yang memadai untuk membangun komunitas pengetahuan yang adaptif, kreatif dan mampu merajut realitas. Dalam pelaksanaannya, sistem ini menopang layanan inti akademis yakni pendidikan, penelitian, serta pemberdayaan masyarakat. Selain itu,

sistem ini juga menopang kebutuhan sistem informasi manajemen universitas yang diperlukan.

1.2 Rumusan Masalah

Dari latar belakang masalah yang telah dikemukakan diatas, maka dapat dirumuskan beberapa masalah yang menjadi inti dari penelitian ini, yaitu :

- 1) Belum adanya Standar Operasional Prosedure (SOP) pelaksanaan tugas pokok dan fungsi organisasi IT di universitas;
- 2) Kurang optimalnya layanan TIK publik (personal, sarana dan konten);
- 3) Kurang maksimalnya Keamanan Jaringan (Network Security), pemanfaatan Aplikasi yang telah dibangun, Akses Jaringan Internet maupun Intranet sampai ke gedung dan ketersediaan standar teknis penerapan infrastruktur di setiap unit kerja.

1.3 Tujuan Penelitian

Dokumen ini dibuat dengan tujuan sebagai panduan pengembangan, implementasi, dan pengelolaan TIK di UINSGD, dan digunakan sebagai bagian dari strategi universitas untuk mencapai visi, misi dan sasaran yang telah ditetapkan.

Realisasi Dokumen Blueprint UINSGD akan mendorong tercapainya:

- a) Cita-cita sebagai *ICT-Based Campus*.
- b) Keselarasan implementasi TIK dengan rencana strategis universitas.
- c) Kesesuaian implementasi TIK dengan kebutuhan stakeholder.
- d) Terbangunnya integrasi semua unit, yaitu semua jurusan/program studi, lembaga, pusat studi, maupun bidang-bidang dalam manajemen.
- e) Penggunaan sumber daya secara efektif dan efisien.
- f) Dukungan TIK yang optimal terhadap kegiatan Tridharma.
- g) Perkembangan TIK yang bermutu di Indonesia.
- h) Kualitas SDM yang tinggi dalam beradaptasi dengan TIK.

1.4 Batasan Masalah

Dengan luasnya cakupan penelitian ini, maka penulis akan membatasi pembahasan penelitian. Lingkup dokumen blueprint pengembangan TIK UIN Sunan Gunung Djati meliputi hal-hal berikut:

- 1) Menganalisis UINSGD dan kebutuhan-kebutuhan dan harapan-harapan dari pengguna akhir untuk menentukan kecocokan untuk bauran keperluan-keperluan kegunaan.
- 2) Merencanakan kembali jaringan kampus UINSGD.
- 3) Melaksanakan infrastruktur jaringan yang diubah.
- 4) Mengadakan fasilitas manajemen jaringan pusat.
- 5) Melaksanakan secara selektif jaringan nirkabel (*Wireless LAN*).
- 6) Memungkinkan untuk perlindungan investasi masa depan dan fleksibilitas pada fungsionalitas.

1.5 Metodologi

Tahap pengerjaan yang dilakukan di dalam penelitian ini, antara lain:

1. Identifikasi Masalah
Eksplorasi awal dilakukan dengan mengidentifikasi masalah terhadap kondisi ekisting jaringan kampus dan kebutuhan pengguna kampus dikaitkan dengan proses bisnis yang berlaku di universitas. Pada tahapan ini juga perlu dilakukan pengenalan metode *IT Audit* dan pendekatan *Business Process Based System*.
2. Studi Literatur
Berdasarkan temuan masalah, dilakukan kajian teoritis berdasarkan penelitian-penelitian terdahulu, serta mempelajari literatur-literatur baik yang berupa buku, jurnal dan artikel ilmiah, maupun website untuk memahami konsep enterprise, IT audit serta konsep pengembangan blueprint enterprise. Dari pemahaman tersebut didapatkan identifikasi masalah dalam penelitian ini.
3. Pengumpulan Data
Dilakukan pengumpulan dataset melalui pengumpulan data dari unit di universitas dan berdasarkan data penelitian-penelitian sebelumnya.
4. Perancangan dan Implementasi Sistem
Melakukan perancangan blueprint TIK beserta berdasarkan pola penggunaan TIK di universitas.
5. Pengujian
Merancang dan melakukan tahapan pengujian menggunakan dokumen blueprint yang telah disiapkan.
6. Penulisan Laporan Penelitian
Penulisan laporan dilakukan sesuai dengan urutan metode penelitian secara paralel.

1.6 Sistematika Penulisan

Sistematika penulisan laporan penelitian ini akan terbagi ke dalam enam bab, sebagai berikut:

1. Bab I Pendahuluan

Bab ini memaparkan hal yang melatar belakangi masalah, kemudian masalah tersebut dirumuskan sehingga memiliki tujuan tertentu, diberikan batasan supaya masalah tidak keluar dari topik, kemudian tahapan metodologi penyelesaian penelitian, terakhir sistematika penulisan.

2. Bab II Tinjauan Pustaka

Bab ini menjelaskan penelitian yang telah dilakukan sebelumnya dan teori-teori yang berkaitan dengan pengenalan konsep enterprise, IT audit dan perancangan blueprint organisasi berbasis TIK. Pola-pola tersebut akan dikolaborasikan dengan konsep *smart campus* yang dilakukan di dalam penelitian ini.

3. Bab III Metodologi Penelitian

Bab ini menjelaskan tentang tahapan penyelesaian dalam penelitian ini.

4. Bab IV Hasil Penelitian

Bab ini menjelaskan tentang hasil yang telah dihasilkan di dalam penelitian.

5. Bab V Pembahasan

Bab ini merupakan pembahasan, implementasi dan pengujian terhadap hasil pada Bab IV serta definisi akhir terkait pengujian tersebut.

6. Bab VI Penutup

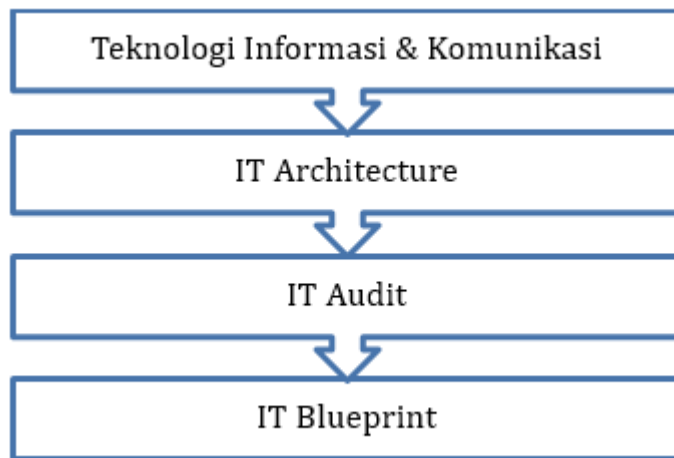
Bab ini menjelaskan tentang rangkuman hasil penelitian berdasarkan simulasi dan analisis yang telah dilakukan dan saran-saran yang dapat digunakan untuk pengembangan penelitian lebih lanjut.

2. TINJAUAN PUSTAKA

Pada bab ini dibahas mengenai teori-teori yang melandasi penelitian ini. Adapun teori yang dibahas secara rinci melalui *literature map*.

2.1 Peta Tinjauan Pustaka

Pada penelitian ini dibutuhkan landasan teori yang dapat membantu dalam melaksanakan penelitian. Landasan teori diambil dari beberapa bidang ilmu maupun topik penelitian yang mendukung. Pada gambar di bawah dijelaskan mengenai *literature map* pada penelitian ini.



Gambar 2.1 Literature Map

2.2 Profil UIN Sunan Gunung Djati Bandung

UIN Sunan Gunung Djati Bandung sebagai salah satu PTKI negeri (yang pada saat berdiri yakni tahun 1968 bernama IAN kemudian pada tahun 2005 berubah menjadi UIN) hendaknya terus berkomitmen dan aktif dalam membangun bangsa, negara dan agama. Dengan wawasan keislaman yang toleran, UIN Sunan Gunung Djati Bandung diharapkan turut memberi kontribusi dalam membangun politik bangsa yang lebih demokratis dan berupaya menciptakan keamanan kawasan dengan penuh rahmat dan damai. Di bidang ekonomi UIN Sunan Gunung Djati Bandung diharapkan dapat berperan dalam menyiapkan SDM Indonesia yang siap berkompetisi di tingkat ASEAN karena lulusannya kecuali menguasai ilmu pengetahuan dan teknologi juga mampu bekerja dengan penuh amanah dan kesungguhan (ibadah). Di bidang sosial-budaya, UIN Sunan Gunung Djati Bandung juga hendaknya

turut serta dalam membentuk karakter bangsa melalui pembinaan *al akhlak al karimah* dan membangun silaturahmi keutamaan terutama dengan negara-negara Islam lain di kawasan Asia Tenggara.

Sejumlah harapan di atas akan mampu dijawab oleh UIN Sunan Gunung Djati Bandung jika prestasi demi prestasi terus ditorehkan. Seperti pada tahun 2015, UIN Sunan Gunung Djati Bandung merupakan satu-satunya universitas dari PTKI yang berhasil mendapatkan Penganugerahan Keterbukaan Informasi Badan Publik untuk kategori Perguruan Tinggi Negeri yang diselenggarakan oleh Komisi Informasi Pusat (KIP) Republik Indonesia bersama dengan: Universitas Brawijaya Malang, UGM, UNPAD, UI, ITS, USU, Universitas Jambi, ULM, dan Universitas Bengkulu.

Harapan-harapan di atas pun akan terwujud jika sejumlah potensi terus diberdayakan secara maksimal. Sebagai perguruan tinggi keagamaan Islam negeri yang mengemban amanah selain menyelenggarakan program pendidikan tinggi bidang ilmu Agama Islam juga menyelenggarakan program pendidikan tinggi bidang ilmu umum, UIN Sunan Gunung Djati Bandung bertekad menjadi Universitas Negeri Islam yang unggul dan kompetitif berbasis wahyu memandu ilmu dalam bingkai akhlak karimah di Asia Tenggara. Dengan demikian, memiliki peluang besar dalam melakukan berbagai otonomisasi, khususnya studi, menerima mahasiswa, mengelola pendidik dan tenaga kependidikan, kemitrausahaan baik regional, nasional maupun internasional dalam rangka pengembangan perguruan tinggi.

2.3 Teknologi Informasi dan Komunikasi (TIK)

Teknologi informasi dan komunikasi (TIK) adalah suatu konsep yang berkaitan dengan kumpulan sumber daya informasi, penggunaan, infrastruktur pendukung dan manajemen yang menjalankannya. Sedangkan pada Undang-Undang no.11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) disebutkan bahwa teknologi informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi. Secara umum teknologi apa pun yang membantu manusia dalam membuat, mengubah, menyimpan, mengkomunikasikan dan/atau menyebarkan informasi dapat dikatakan sebagai teknologi informasi dan komunikasi [1] [2].

Secara garis besar road map perkembangan teknologi informasi pada beberapa dasawarsa terakhir ini dapat dilihat pada beberapa aspek-aspek antara lain aspek aplikasi, jaringan, database, server dan programming.

Dari aspek aplikasi dapat dilihat bahwa aplikasi teknologi informasi khususnya untuk dunia industri telah mengalami perkembangan yang cukup

signifikan sejalan dengan perkembangan teknologi pada umumnya. Pada awalnya aplikasi dibuat untuk memenuhi suatu kebutuhan tertentu saja tanpa mempertimbangkan keterpaduan dengan aplikasi-aplikasi lain yang terkait dengannya. Misalnya aplikasi untuk pengelolaan penyediaan material di industri atau yang lebih dikenal dengan Material Requirement Planning (MRP), dengan tujuan untuk dapat menyediakan material yang dibutuhkan dalam proses produksi secara akurat jumlahnya serta kapan dan dimana material tersebut dibutuhkan. Sejalan dengan perkembangan teknologi aplikasi ini kemudian berkembang menjadi apa yang disebut dengan Enterprise Resource Planning (ERP) yang merupakan aplikasi yang dapat memberikan solusi terpadu dalam pengelolaan semua sumberdaya yang dimiliki oleh suatu industri [3].

Jika dilihat dari aspek jaringan dan topologi server yang digunakan, terlihat perkembangan yang sangat signifikan, dengan semula hanya menggunakan stand alone dan main frame komputer, kemudian berkembang dalam bentuk jaringan Local Area Network (LAN) dengan Client Server. Perkembangan dibidang jaringan dan server ini pada hakekatnya berperan sebagai pemicu pada aspek-aspek lainnya. Salah satu perkembangan yang patut untuk dicermati dalam aspek jaringan ini adalah penggunaan teknologi wireless, yang memungkinkan konektivitas tanpa menggunakan media kabel.

Salah satu bentuk dari implementasi teknologi wireless ini yang mulai banyak digunakan saat ini adalah Wave LAN. Sedangkan dari aspek bentuk database yang dipergunakan, semula digunakan database dengan bentuk hierarchical atau network, yang banyak digunakan pada main frame yang ada disaat itu. Saat ini hierarchical atau network database dirasakan kurang efektif untuk mendukung perkembangan dibidang-bidang lain, untuk itu kemudian dikembangkan apa yang disebut dengan relational database. Kesederhanaan dan basis matematik yang kuat dari relational database, menjadikannya sebagai pemain utama dalam teknologi database saat ini. Selain relational database, dikenal pula object oriented database yang diperkirakan akan berkembang pada masa-masa yang akan datang. Untuk mendukung aplikasi-aplikasi yang banyak melakukan transaksi data diperkirakan database relational masih akan banyak digunakan dimasa-masa yang akan datang, sedangkan untuk aplikasi-aplikasi yang menonjolkan daya analisis seperti datawarehouse dan lainnya relational database ternyata kurang efektif untuk digunakan dan sebagai alternatif adalah *object oriented database*.

Dari sisi bahasa pemrograman, kedepan diperkirakan akan semakin banyak dipengaruhi oleh perkembangan Internet. Tuntutan agar aplikasi dapat dijalankan dalam semua platform (open platform) diperkirakan akan semakin menguat, dari sisi ini Java dan PHP merupakan pilihan di masa-masa yang akan datang. Salah satu teknologi yang saat ini banyak dibicarakan

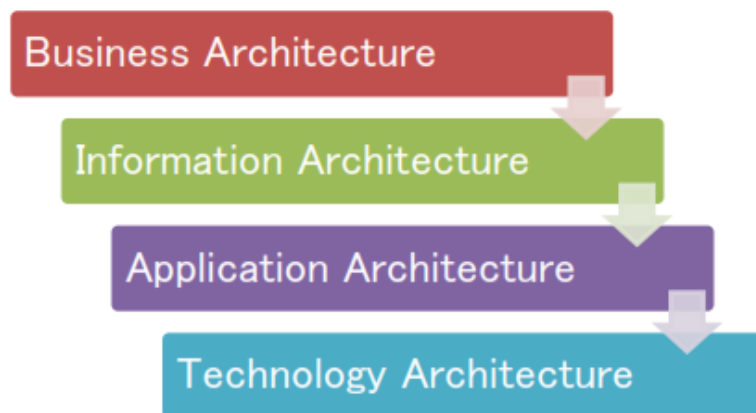
penggunaannya adalah teknologi XML untuk mendukung interoperabilitas dari aplikasi yang akan dikembangkan.

Salah satu hal terpenting dimasa yang akan datang adalah fungsi integrasi antar sistem sehingga dapat membentuk satu kesatuan sistem yang solid dalam mendukung interoperabilitas proses bisnis secara keseluruhan. Hal ini juga menjadi sangat penting dengan semakin berkembangnya konsep modularisasi sistem, dimana konsep “all or nothing” yang menuntut perusahaan untuk menerapkan keseluruhan komponen yang disediakan oleh vendor, akan berubah ke konsep modular, dimana perusahaan dapat memilih modul-modul yang akan diterapkan.

2.4 Perancangan Arsitektur Enterprise

Salah satu kunci utama dalam perencanaan teknologi informasi adalah perancangan arsitektur teknologi informasi. Untuk itu, berikut ini dipaparkan gambaran umum kerangka kerja perancangan arsitektur sistem informasi yang dipergunakan dalam industri teknologi informasi dan komunikasi [4].

Arsitektur sistem informasi secara menyeluruh digambarkan dalam hirarki sebagai berikut:



Gambar 2.2 Hirarki Arsitektur Sistem

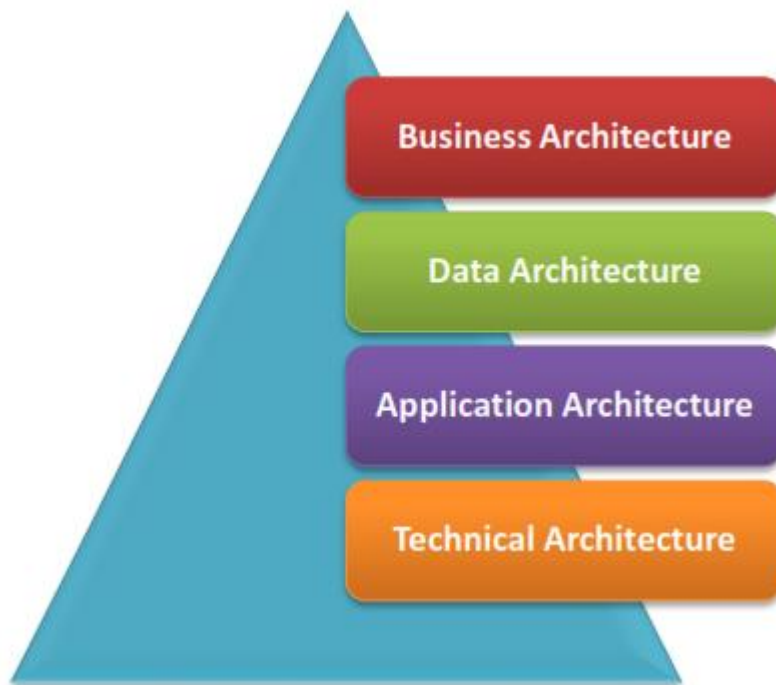
Melalui asesmen dan evaluasi terhadap tugas pokok & fungsi serta high-level business process dirancang arsitektur proses bisnis yang mendeskripsikan proses-proses kunci pada UIN Sunan Gunung Djati bandung dalam menyelenggarakan tugas pokok dan fungsinya. Proses-proses bisnis kunci ini dipaparkan dalam bentuk diagramatik yang menunjukkan relasi antar bagian/unit kerja.

Perancangan arsitektur dapat menggunakan berbagai framework yang umum dipergunakan dalam industri teknologi informasi dan komunikasi.

Perencanaan arsitektur sistem informasi organisasi adalah sebuah proses yang kompleks, karena itu proses perencanaan harus dikelola berdasarkan suatu petunjuk yang jelas dengan tujuan menyelaraskan strategi bisnis organisasi dan strategi teknologi yang mampu memberikan hasil maksimal bagi organisasi.

TOGAF (The Open Group Architecture Framework) merupakan sebuah framework untuk arsitektur enterprise dimana menyediakan pendekatan secara komprehensif untuk mendesain, merencanakan, mengimplementasi dan melakukan control dengan otoritas pada sebuah informasi arsitektur enterprise [5].

TOGAF adalah pendekatan secara holistic untuk mendesain, dimana biasanya dimodelkan dengan 4 tingkat : business, aplikasi, data dan teknologi. Hal tersebut memberikan kelayakan secara menyeluruh sebagai model awal yang dipergunakan sebagai arsitektur informasi, dimana dapat dibangun nantinya. Merupakan modularisasi, standarisasi dan telah tersedia, perbaikan teknologi dan produk.



Gambar 2.3 Arsitektur TOGAF

Seperti ditunjukkan dalam gambar, TOGAF membagi arsitektur enterprise ke dalam empat kategori, yaitu sebagai berikut:

- 1) Business architecture, menjelaskan proses bisnis untuk memenuhi tujuannya.
- 2) Data architecture, menjelaskan bagaimana enterprise datastores diatur dan diakses.
- 3) Application architecture, menjelaskan bagaimana aplikasi khusus dirancang dan bagaimana aplikasi berinteraksi satu dengan yang lainnya.
- 4) Technical architecture, menjelaskan infrastruktur hardware dan software yang mendukung aplikasi dan interaksinya.

3. METODOLOGI PENELITIAN

3.1 *Design Science Research Methodology*

Sistem informasi dikembangkan di dalam suatu organisasi dengan tujuan meningkatkan efisiensi dan efektifitas organisasi. Pengembangan sistem dilakukan dengan memperhatikan keadaan dan perilaku organisasi. Adaptasi terhadap situasi pun harus tetap dilakukan agar sistem dapat mengikuti kebutuhan yang selalu berubah tergantung kondisi persaingan atau hubungannya dengan pihak luar [6].

Penelitian dalam sistem informasi mempunyai dua paradigma yang berbeda. Pertama adalah *behavioral science* yang berfokus pada pengembangan dan membuktikan teori tentang perilaku manusia atau perilaku organisasi. Sedangkan yang kedua adalah *design science* yang berfokus terhadap pengembangan kapasitas manusia dan organisasi dengan menciptakan inovasi. DSRM diciptakan sebagai alat bantu dalam *design science* yang berupa *framework* konsep dan panduan dalam memahami, mengaplikasikan dan mengevaluasi penelitian.

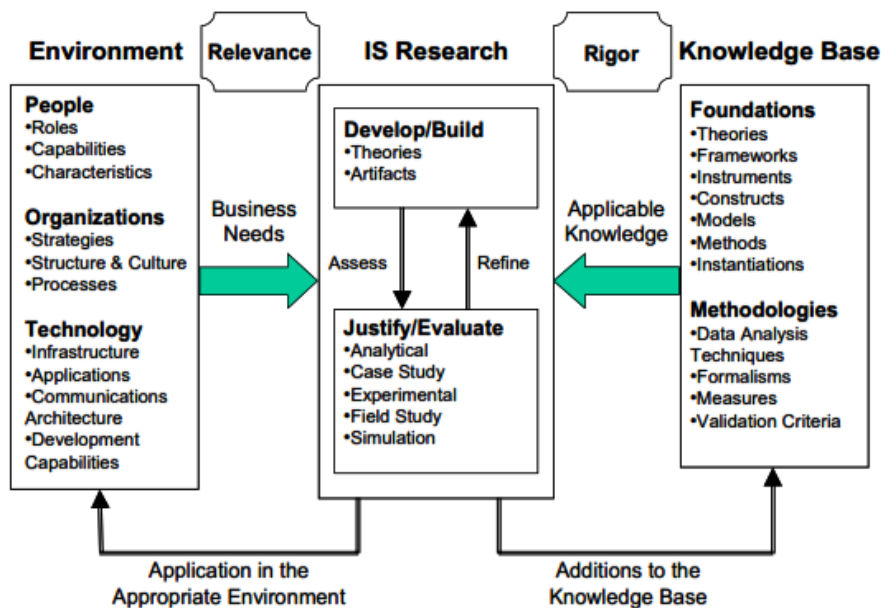
Model diciptakan menggambarkan keadaan sebenarnya. Adanya model digunakan untuk memahami hubungan antara masalah dan solusi, Dari hubungan ini didapatkan proses untuk mengembangkan solusi dari masalah tersebut. Hevner dan kawan-kawan memberikan 7 panduan yang digunakan dalam melakukan riset desain [7].

Tabel 3.1 Panduan DSRM

Panduan	Penjelasan
Desain Sebagai Sebuah Komponen	Riset <i>design science</i> harus dapat menciptakan komponen yang berbentuk sebuah konstruksi, model, metode, ataupun contoh.
Hubungan Masalah	Tujuan riset adalah mengembangkan solusi berbasis teknologi yang penting dan relevan terhadap masalah bisnis.
Evaluasi Desain	Kegunaan, kualitas, dan akurasi dari desain harus secara terstruktur didemonstrasikan dengan metode evaluasi yang baik.
Kontribusi Penelitian	Penelitian harus memberikan gambaran yang jelas terhadap kontribusi yang dihasilkan sesuai dengan area masalahnya.

Konsistensi Penelitian	Penelitian bergantung pada aplikasi dari metode yang terstruktur baik dalam konstruksi dan evaluasi dari komponen desain.
Desain Sebagai Proses Pencarian	Pencarian akan komponen yang efektif membutuhkan cara apapun yang tersedia untuk mencapai akhir yang diinginkan dan tetap dalam aturan-aturan di dalam lingkup masalah.
Komunikasi Penelitian	Penelitian harus dipresentasikan dengan baik secara teknologi maupun secara manajemen kepada audiens.

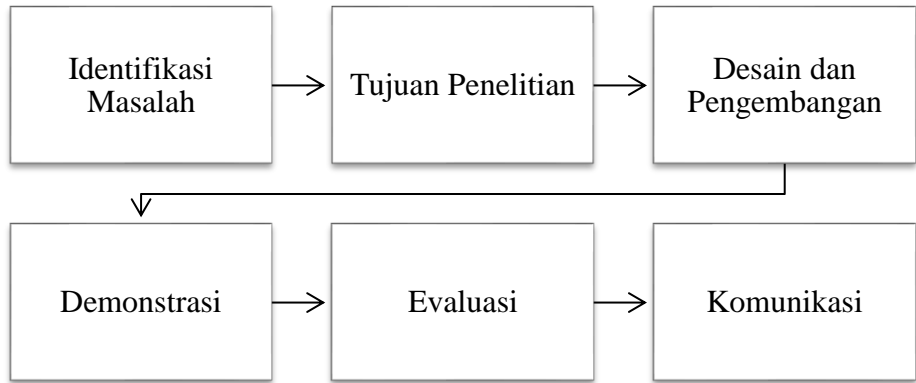
Paduan yang diberikan oleh Hevner dan kawan-kawan berdasarkan *framework* konseptual yang mereka kembangkan. *Framework* konseptual ini bertujuan untuk memahami, mengeksekusi, dan mengevaluasi riset sistem informasi yang menggabungkan perilaku, sains dan paradigma sains desain [6].



Gambar 3.1 *Framework* DSRM

3.2 Metode yang Digunakan

Untuk menjawab tujuan penelitian pada bab sebelumnya, maka perlu dibentuk tahapan-tahapan penelitian berdasarkan metode DSRM sebagai berikut [6].



Gambar 3.2 Tahapan Penelitian

3.3 Penjelasan Tahapan Penelitian

Untuk memperjelas tahapan yang dilakukan pada penelitian ini, berikut merupakan deskripsi masing-masing tahapan tersebut.

3.3.1 Identifikasi Masalah

Perumusan masalah telah dijabarkan pada Bab I (Pendahuluan). Masalah yang diangkat dalam penelitian ini adalah belum adanya dokumen blueprint pengembangan infrastruktur TIK di UIN Sunan Gunung Djati Bandung. Dokumen blueprint dikembangkan berdasarkan proses bisnis yang berlaku di universitas serta pola penggunaan civitas akademika terhadap infrastruktur TIK di UIN Sunan Gunung Djati Bandung.

3.3.2 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Memahami proses bisnis dan pola penggunaan infrastruktur yang berjalan di UIN Sunan Gunung Djati;
2. Mengembangkan dokumen blueprint pengembangan infrastruktur TIK yang sesuai dengan kondisi di UIN Sunan Gunung Djati Bandung.

3.3.3 Desain dan Pengembangan

Pada tahap desain dan pengembangan, setiap data pendukung proses bisnis dikumpulkan oleh sistem, lalu diolah sedemikian rupa sehingga diperoleh hasil yang diharapkan, serta tahapan-tahapan implementasi yang akan dilakukan. Dokumen blueprint yang telah dirancang akan disesuaikan

dengan proses analisa dan perancangan yang telah dibahas pada bagian sebelumnya.

3.3.4 Demonstrasi

Rancangan blueprint diimplementasikan dalam bentuk dokumen blueprint yang berisi tentang beberapa rekomendasi pengembangan infrastruktur TIK di UIN Sunan Gunung Djati Bandung.

3.3.5 Evaluasi

Tahapan ini merupakan proses yang dilakukan untuk membuktikan rancangan dokumen blueprint pengembangan infrastruktur TIK dengan melakukan Focus Group Discussion kepada pihak-pihak yang berkepentingan terhadap pengembangan infrastruktur TIK di UIN Sunan Gunung Djati Bandung.

3.3.6 Komunikasi

Hasil penelitian ini nantinya akan dipublikasikan pada buku laporan penelitian sebagai laporan hasil penelitian. Hasil penelitian ini diharapkan dapat membantu untuk memberikan panduan bagi *stakeholder* UIN Sunan Gunung Djati Bandung dalam merencanakan pengembangan infrastruktur TIK UIN Sunan Gunung Djati Bandung.

4. HASIL PENELITIAN

Pada bab ini akan dibahas mengenai hasil penelitian. Blueprint TIK dibuat dengan tujuan untuk membantu merencanakan rencana strategis maupun rencana teknis dalam rangka meningkatkan fungsi TIK dalam proses bisnis yang berlaku di dalam universitas. Penelitian ini dititikberatkan pada perancangan *blueprint* infrastruktur TIK beserta komponen pendukungnya.

4.1 Kasus Bisnis

Information and Communication Technology (ICT) mendukung penelitian, pengajaran dan pembelajaran dalam konteks pendidikan lebih tinggi internasional. Pada bulan Nopember 2003, Dewan mengadopsi Strategi ICT untuk UINSGD yang mendorong pembaharuan infrastruktur ICT Universitas. Proyek UINSGDNet telah dimulai untuk melaksanakan rekomendasi-rekomendasi penting dari strategi ICT. Dasar pemikiran untuk UINSGDNet sebagai berikut:

Ketergantungan UINSGD pada ICT semakin meningkat dalam dekade terakhir ini pelayanan-pelayanan TIK ini telah menjadi penting sekali dalam mendukung penelitian, pengajaran dan pembelajaran yang unggul dan bersaing secara internasional. Pelayanan-pelayanan tersebut menjadi kritis untuk proses-proses administrasi, komunikasi internal dan juga fungsi sehari-hari.

UINSGD telah menjadi pengadopsi awal teknologi, tetapi tidak selalu mengikuti perkembangan-perkembangan baru. Dengan adanya hal mengandalkan pada teknologi tersebut, kami harus menjamin bahwa infrastruktur ICT disesuaikan untuk memenuhi kebutuhan-kebutuhan masa sekarang dan masa depan.

Komponen penting dari UINSGDNet adalah perbaikan jaringan kampus UINSGD untuk menjamin infrastruktur yang aman, diatur, diganti sepenuhnya yang cukup dapat dipercaya, fleksibel dan efektif biaya guna memenuhi tuntutan-tuntutan sekarang ini dan menyediakan platform dan kapasitas untuk pertumbuhan di masa mendatang.

4.2 Keperluan Bisnis Keseluruhan

Pembaharuan jaringan kampus diperlukan untuk:

1. Memperbaharui dan memperbaiki infrastruktur yang sudah tua;
2. Menahan biaya kepemilikan infrastruktur jaringan kampus;
3. Meningkatkan produktivitas;
4. Mendukung praktik-praktik bisnis masa depan;

Keperluan-keperluan bisnis lembaga tersebut dan keperluan-keperluan PTIPD diuraikan lebih lanjut di bagian berikut.

4.2.1 Keperluan Bisnis Untuk Perbaikan Infrastruktur

Perbaikan jaringan kampus UINSGD harus memungkinkan dan meningkatkan dukungan IT untuk “bisnis” penelitian, pengajaran, pembelajaran dan administrasi.

Jaringan yang baru tersebut harus:

- a) Menawarkan fleksibilitas dalam mendukung jenis-jenis lalu lintas bisnis.
- b) Memberikan skalabilitas dipandang dari sudut kecepatan dan bandwidth hubungan jaringan yang diperlukan untuk aplikasi-aplikasi bisnis.
- c) Menjamin kebebasan pribadi informasi khusus bisnis yang melintasi jaringan tersebut.
- d) Menambahkan kelambatan minimal ke aplikasi-aplikasi bisnis.
- e) Tersedia selama jam-jam bisnis (pada dasarnya 24/7 untuk penelitian).
- f) Ditempatkan di masa mendatang untuk merangkul teknologi-teknologi baru selama teknologi-teknologi tersebut berhubungan dengan bisnis.
- g) Disediakan sebagai pelayanan yang diatur oleh Service Level Agreements (SLA).
- h) Menyebutkan atau menghadapi fleksibilitas akses (misalnya akses jauh dan konektivitas nirkabel).
- i) Memberikan rute-rute kekuatan alternatif ke bangunan-bangunan dan kampus-kampus utama.
- j) Memberikan model penahanan biaya

Cetak biru jaringan ini harus memenuhi keperluan-keperluan jaringan:

- a) Kampus, bangunan, dan tempat individu dalam bangunan-bangunan yang mungkin memiliki keperluan-keperluan khusus.
- b) Pelayanan jaringan tambahan yang akan ditawarkan oleh UINSGD (termasuk akses nirkabel).
- c) Pemulihan bencana dan redundansi.
- d) Pusat Penghitungan Kinerja Tinggi.

- e) Pusat Data (Data Center).
- f) Solusi-solusi penyimpanan dan dukungan.
- g) Aplikasi-aplikasi.
- h) Protokol-protokol jaringan.
- i) Arus-arus kerja UINSGDNet lainnya.
- j) Unit-unit bisnis (fakultas dan departemen).
- k) Laboratorium kecil penghitungan mahasiswa.
- l) Tempat-tempat akses nirkabel

4.2.2 Kepentingan PTIPD Untuk Perbaikan Infrastruktur

Pembaharuan jaringan kampus UINSGD harus menempatkan PTIPD untuk memberikan pelayanan jaringan yang konsisten dengan praktik terbaik dalam bidang-bidang:

- a) Penahanan biaya ICT.
- b) Fleksibilitas ICT.
- c) Perjanjian-perjanjian tingkat pelayanan untuk pengadaan dan pelaksanaan.
- d) Informasi manajemen.
- e) Konektivitas yang terjamin aman.
- f) Jaringan yang baru akan memberikan:
 - 1) Arsitektur jaringan yang menyumbang kepada:
 - a) Model terstruktur (inti, distribusi dan akses) yang akan memuat atau menahan lalu lintas jaringan dalam segenap-segmen yang diperlukan.
 - b) Manajemen terpusat melalui alat-alat yang tepat dan memenuhi standar-standar.
 - c) Pencakupan keamanan jaringan.
 - d) Pilihan-pilihan untuk rencana-rencana pemulihan bencana dan redundansi.
 - 2) Model-model jaringan modular
 - a) Kemudahan penyebaran
 - b) Redundansi dan kebebasan
 - c) Kemudahan manajemen

- d) Skalabilitas dalam jumlah tempat akses dan kecepatan transfer
- 3) Fasilitas-fasilitas manajemen jaringan dalam mendukung:
- a) Perjanjian-perjanjian Tingkat Pelayanan (manajemen pengadaan dan pelaksanaan pelayanan) dengan fakultas-fakultas UINSGD dan unit-unit bisnis lainnya.
 - b) Aplikasi sumber daya manusia yang efisien untuk mengatur semua aspek pelayanan jaringan.
 - c) Mengumpulkan data kinerja jaringan.
 - d) Administrasi jaringan.
 - e) Perencanaan kapasitas.
 - f) Keamanan jaringan.
 - g) Konfigurasi yang sedikit.
- 4) Fasilitas-fasilitas keamanan jaringan dalam mendukung:
- a) Segmentasi kelompok pengguna.
 - b) Otentikasi tingkat tempat akses.
 - c) Bidang-bidang wewenang lalu lintas IP.
- 5) Infrastruktur jaringan yang ditempatkan untuk masa depan yang akan menjamin:
- a) Perlindungan perbaikan masa depan yang pantas.
 - b) Skalabilitas dalam kecepatan, skalabilitas dalam jumlah pengguna jaringan dan dalam fungsionalitas teknologi masa depan.

4.3 Perencanaan Blueprint

Cetak biru jaringan kampus UINSGD yang diusulkan dan disetujui harus meliputi, tetapi tidak terbatas pada, aspek-aspek berikut:

- a) Arsitektur jaringan modular yang ditempatkan sebagai tipologi jaringan UINSGD.
- b) Model pemusatan lapisan jaringan.
- c) Protokol-protokol pengiriman.
- d) Komponen-komponen keamanan jaringan.
- e) Manajemen jaringan.
- f) Ukuran-ukuran lapisan dasar.

- g) Keterangan bahan-bahan.
- h) Standar-standar konfigurasi.
- i) Spesifikasi-spesifikasi keperluan pemasangan kabel.
- j) Rencana pemulihan bencana.
- k) LAN yang ada di WAN.
- l) Model jaringan *To-Be*.
- m) Model yang menggabungkan teknologi-teknologi masa depan.
- n) Model manajemen untuk menilai keperluan-keperluan kapasitas terus-menerus.
- o) Rencana migrasi yang didokumentasikan.
- p) Validasi internasional dari vendor.
- q) Perluasan jaringan kampus ke semua tempat tinggal mahasiswa.

4.4 Jaringan Terpasang

Bagian ini menggambarkan secara singkat jaringan UIN Sunan Gunung Djati Bandung (UINSGD). Diagram-diagram jaringan dari jaringan yang ada sekarang ini diberikan untuk acuan. Aspek-aspek berikut digambarkan:

- a) Protokol-protokol pengiriman
- b) Nirkabel
- c) Manajemen jaringan
- d) Keamanan jaringan

4.4.1 Protokol Routing

Routing Informasi Protocol version 2 (RIPv2) digunakan sebagai protokol pintu gerbang interior (IGP) untuk penyebaran informasi pengiriman yang dinamis di seluruh jaringan daerah UINSGD (WAN).

Open Shortest Path First (OSPF) versi 2 telah disusun, disamping RIPv2 pada FreeBSD routers yang diatur oleh PTIPD yang dihubungkan secara langsung ke kekuatan untuk tujuan-tujuan mengembangkan sebuah rencana untuk perpindahan dari RIP ke OSPF.

4.4.2 Wireless

Berbagai perangkat wireless digunakan untuk memperluas jaringan UINSGD ke lokasi-lokasi yang sulit dijangkau.

4.4.3 Manajemen Jaringan

Jaringan UINSGD memiliki sistem-sistem manajemen jaringan terbatas di tempat dengan semua sistem yang ada yang ditempatkan di pusat data Nirkabel.

- a) Sistem di nm.uinsgd.ac.id merupakan sebuah sistem lama yang akhirnya akan digantikan oleh netmon.uinsgd.ac.id. Cricket digunakan untuk menjelaskan jaringan dan informasi tuan rumah tersedia melalui SNMP

- dari roter-router dan server-server. Kebanyakan digunakan untuk memantau tersedianya server dan router.
- b) Cacti digunakan untuk menjelaskan jaringan dan informasi tuan rumah yang tersedia melalui SNMP dari router-router dan server-server. Nagios digunakan untuk memantau tersedianya server dan router.
 - c) Ini merupakan sebuah sistem non-produksi tetapi sekarang ini menjadi satu-satunya sumber statistik QoS. Cricket digunakan untuk menjelaskan statistik QoS yang dicari dari router-router menggunakan SNMP.
 - d) Sistem netman2.uinsgd.ac.id. Sistem ini sekarang tetap dilaksanakan.
 - e) HP Openview Network Node Manager (NNM) disusun untuk memantau berbagai aspek jaringan.

4.4.4 Keamanan Jaringan

Langkah-langkah keamanan jaringan pada jaringan UCT dimaksudkan terutama untuk:

- a) melindungi jaringan dari virus dan lalulintas yang mengganggu lainnya dari Internet.
- b) mengontrol akses ke an dari tempat tinggal.
- c) memaksa jenis-jenis lalulintas tertentu (HTTP, FTP dan SMTP) melalui wakil-wakil untuk tujuan-tujuan manajemen keamanan dan bandwidth.

Kebijakan yang berlaku untuk sebagian besar firewall merupakan kebijakan yang terbuka. Otentikasi merupakan mekanisme keamanan utama yang digunakan dalam jaringan tersebut.

Internet

Semua lalulintas dari Internet melewati firewall pusat UINSGD, sebuah server FreeBSD yang menjalankan IPFW firewalling suite.

Pihak-Pihak Ketiga

Berbagai provider pihak ketiga dihubungkan dengan jaringan pada Nirkabel dan Kampus 2 melalui Metro Ethernet atau Diginet untuk memberikan akses yang disediakan ke berbagai pelayanan dan saluran dukungan. Jaringan-jaringan pihak ketiga ini sebagian besar dihubungkan ke jaringan UINSGD di belakang firewall di Nirkabel.

4.5 Model Arsitektur

Sebuah metodologi yang sangat terjamin disahkan oleh vendor telah diikuti untuk menciptakan model jaringan kampus UINSGD yang baru. Sebagai bagian integral dari metodologi tersebut, lalulintas jaringan kampus sekarang ini, keperluan-keperluan bisnis dan kemungkinan-kemungkinan teknologi masa depan telah dinilai dalam menghasilkan sebuah model jaringan yang akan melayani kebutuhan-kebutuhan sekarang ini dan yang akan mampu

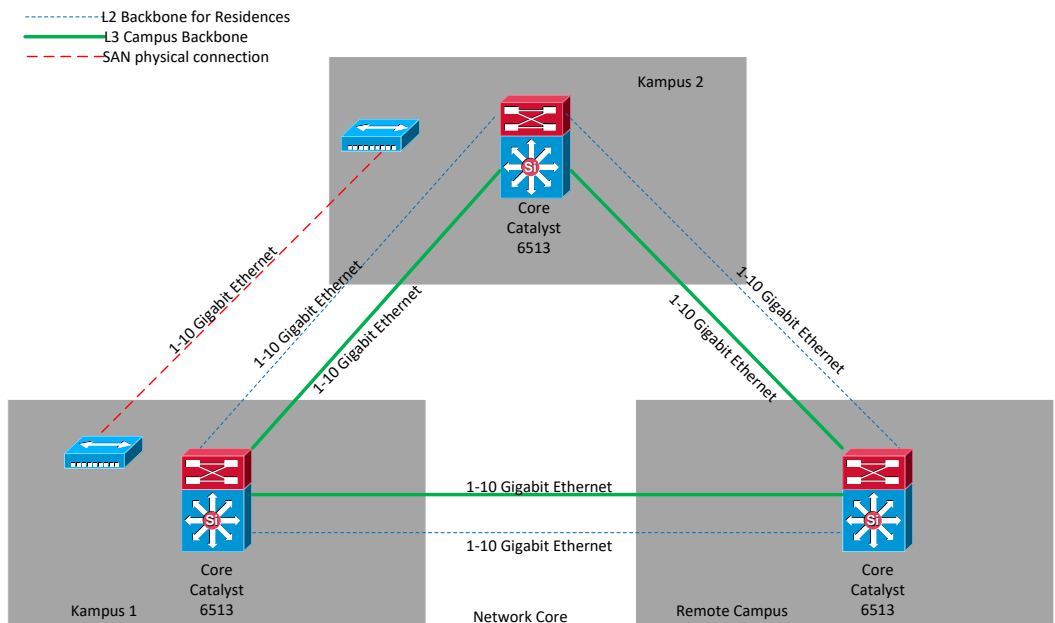
mengukur untuk mengakomodasi kebutuhan-kebutuhan masa depan yang diramalkan.

4.5.1 Topologi

Jaringan kampus baru yang diusulkan di UINSGD akan dibangun sesuai dengan jaringan kampus praktik terbaik, terdiri dari kekuatan kecepatan tinggi (Inti), daerah-daerah konsentrasi (Distribusi) dan tempat-tempat hubungan pengguna (Akses).

4.5.2 Lapisan Inti (Core Layer)

Lapisan Core akan dibentuk antara Kampus 1 dan Kampus 2. Perangkat switch Layer 3 akan digunakan sebagai perangkat keras untuk memperlengkapi kekuatan lapisan inti. Dua area kampus tersebut akan dihubungkan ke satu sama lain melalui Metro Ethernet seperti yang dapat dilihat dibawah.



Gambar 4.1 Area Jaringan Inti (Core Network)

Kecepatan hubungan pertama pada inti akan menjadi 1 Gbps meskipun 10Gbps akan didukung jika timbul kebutuhan untuk meningkatkan. Gigabit Ethernet Trunk tambahan akan dilaksanakan untuk memperlengkapi kekuatan lapisan 2 untuk jaringan tempat tinggal. Hal ini akan memungkinkan UINSGD memisahkan secara fisik dan juga secara logis jaringan tempat tinggal tersebut dari jaringan Campus LAN.

Redundansi fisik akan disediakan lewat hubungan-hubungan Gigabit EtherChannel antara masing-masing blok Inti. Sekumpulan EtherChannel merupakan sekelompok hingga delapan hubungan Fast atau Gigabit Ethernet. Kumpulan tersebut berfungsi sebagai hubungan tersendiri atau logis antara switch-switch dan router-router. EtherChannel adalah tepat karena ia mengukur bandwidth tanpa menambah kepada kerumitan model tersebut. Spanning-Tree Protocol memperlakukan kumpulan EtherChannel sebagai hubungan tersendiri, jadi tidak ada putaran-putaran spanning-tree yang diperkenalkan. Protokol-protokol pengiriman juga memperlakukan kumpulan EtherChannel sebagai hubungan tersendiri atau diarahkan jalannya dengan alamat IP umum, jadi tidak ada jaringan-jaringan cadangan atau pengganti IP tambahan yang diperlukan, dan tidak ada hubungan-hubungan pengamatan router tambahan yang diciptakan. Menjaga keseimbangan beban ditangani oleh perangkat keras hubungan tersebut.

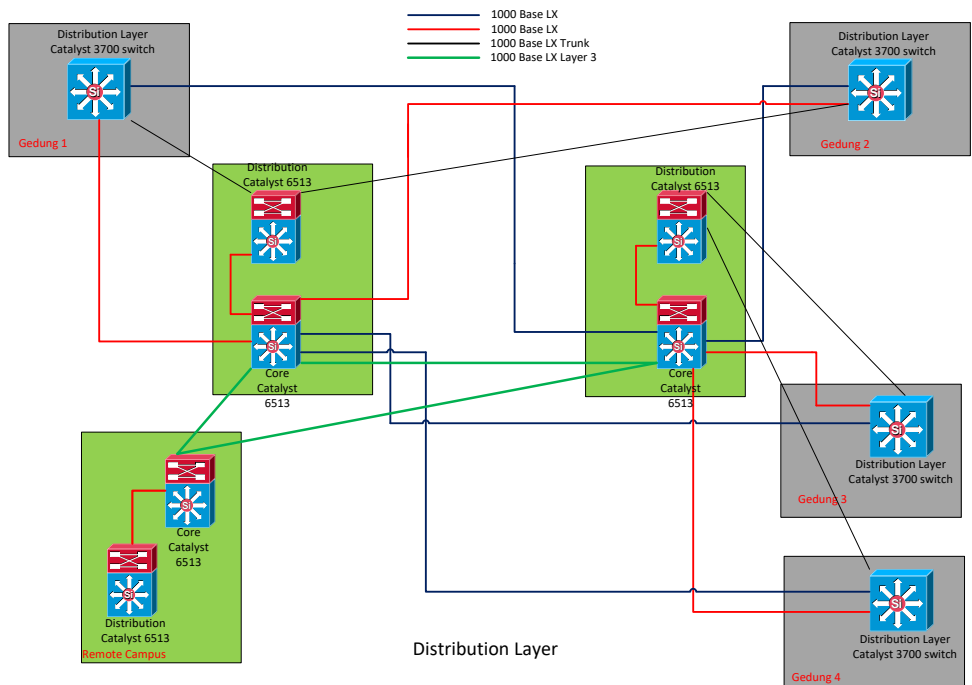
Di sisi perangkat keras switch, dua mesin Switch Layer 3 dan juga dua persediaan tenaga akan dipasang pada masing-masing Switch Layer 2. Hal ini akan menciptakan solusi dengan redundansi yang signifikan menggunakan satu casis perangkat keras. Dengan menggunakan mesin tersebut 2 port atau tempat tambahan disediakan untuk penggunaan kartu-kartu garis. Mesin Supervisor yang kedua akan diatur untuk hot standby untuk mengambil alih dengan segera dalam peristiwa kegagalan pada mesin Supervisor utama. Hal ini juga akan memungkinkan UINSGD meningkatkan IOS pada satu mesin Supervisor dan memiliki kemampuan untuk menurunkan kembali dengan segera dalam peristiwa masalah dengan IOS.

OSPF akan digunakan sebagai protocol pengiriman pilihan pada inti tersebut. Masing-masing blok inti akan disediakan sejumlah jaringan cadangan IP dan jumlah jaringan cadangan ini akan dibagi lagi menjadi jaringan-jaringan cadangan yang lebih kecil dan dialokasikan ke bangunan-bangunan berbeda yang berhubungan dengan inti tersebut. Hanya rute-rute singkat yang akan ditekankan pada kekuatan tersebut untuk membatasi pembaharuan-pembaharuan pengiriman yang tak perlu yang disebarkan melewati jaringan tersebut.

Serat fisik yang sama yang digunakan untuk konektivitas antara pusat data Kampus 2 dan Kampus 2 akan digunakan untuk memperlengkapi konektivitas fisik jaringan daerah penyimpanan (SAN). Serat tersebut akan memiliki jalan-jalan pengganti untuk mengurus redundansi.

4.5.3 Lapisan Distribusi (*Distribution Layer*)

Daerah-daerah jaringan distribusi akan bertindak sebagai pintu-pintu gerbang konsentrasi ke lapisan jaringan Inti yang mendukung arsitektur jaringan kampus tersusun praktik terbaik. Diagram di bawah menunjukkan konektivitas dan susunan daerah-daerah jaringan distribusi.



Gambar 4.2 Area Lapisan Distribusi

4.5.3.1 Pusat Data–Area Kampus 1/Kampus 2

Switch-switch Catalyst 6513 Cisco akan dipasang di masing-masing dari tiga pusat data Campus untuk membentuk lapisan-lapisan distribusi utama untuk masing-masing Campus. Switch-switch Catalyst 6513 akan memiliki dua mesin Supervisor 720 yang dipasang dan juga dua persediaan tenaga untuk mengurus redundansi perangkat keras. Switch-switch ini akan berhubungan dengan switch-switch inti lewat Gigabit EtherChannel. Hubungan-hubungan Gigabit EtherChannel akan berakhir pada blade-blade terpisah pada switch-switch Core 6513 untuk mengurus redundansi antara lapisan-lapisan inti dan distribusi. Switch-switch ini juga akan memberikan fungsional lapisan distribusi kepada tempat-tempat server.

4.5.3.2 Bangunan Lapisan Distribusi Jauh

Di bangunan lapisan distribusi jauh akan dipasang sebuah switch lapisan distribusi Catalyst 3750G-12SS-S Cisco. Tempat-tempat hubungan Gigabit Ethernet mode tersendiri akan digunakan untuk menghubungkan Catalyst 3750 ke Catalyst 6513 lapisan distribusi pusat data. Bangunan-bangunan lapisan akses akan memiliki konektivitas Gigabit Ethernet lewat serat mode khusus

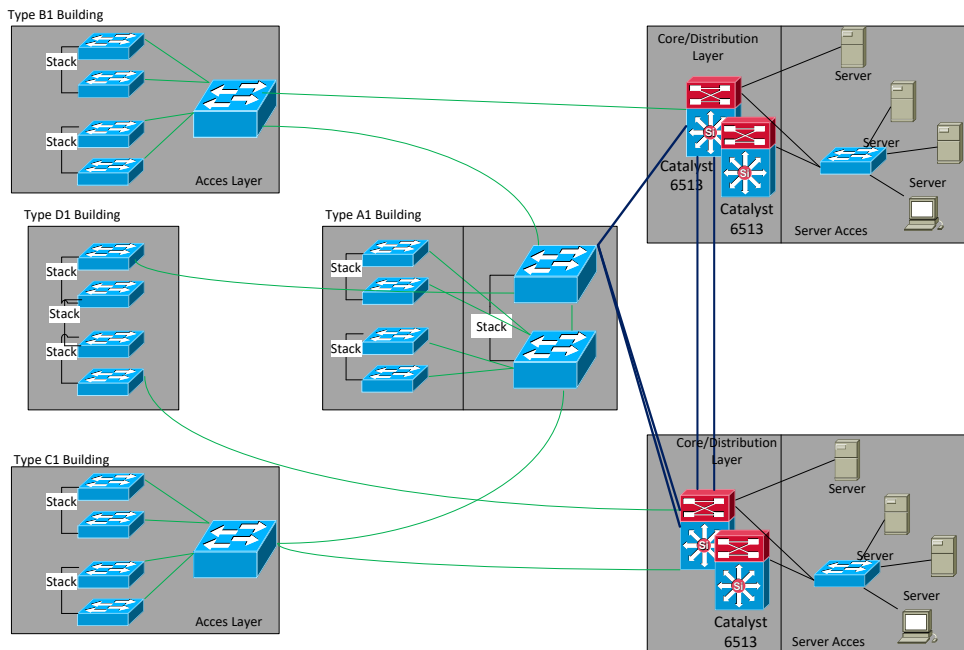
ke Catalyst 6513 pusat data dan juga Catalyst 3750 yang ditempatkan di bangunan distribusi jauh. Switch Catalyst 6513 akan menjadi switch distribusi utama dengan Catalyst 3750 yang mengurus redundansi dalam peristiwa outage di pusat data.

4.5.3.3 WAN & Konektivitas Internet

Pusat data Kampus 1 juga akan bertindak sebagai tempat penghentian semua LAN jauh yang dihubungkan ke WAN. Internet dan pihak-pihak ketiga juga akan berakhir di sini. Pilihan untuk memindahkan sebagian dari hubungan-hubungan ini ke pusat data Middle Campus harus dapat diselidiki untuk mengurus redundansi dalam peristiwa outage di pusat data Kampus 1. VLAN yang terpisah akan diciptakan untuk lingkungan-lingkungan WAN dan Internet untuk menciptakan pemisahan lingkungan-lingkungan ini yang logis.

4.5.4 Lapisan Akses - Full Redundancy

Lapisan Akses dari jaringan kampus menyediakan tempat-tempat konektivitas ke alat-alat jaringan pengguna dan alat-alat sekeliling jaringan, yaitu printer jaringan, server jaringan, dan lain-lain. Diagram di bawah menggambarkan jenis-jenis jaringan akses untuk skenario-skenario bangunan yang berbeda.



Gambar 4.3 Arsitektur Lapisan Akses (Full Redundancy)

Model ini menyediakan empat model lapisan akses berikut:

4.5.4.1 Bangunan Tipe A1 (A2 Untuk Redundansi Terbatas)

Model ini akan menyediakan switch lapisan distribusi hubungan (seri Catalyst 3750) yang akan dipasang di bangunan kampus jauh. Switch Catalyst 3750 akan menghubungkan kembali ke pusat data lewat Gigabit EtherChannel ke switch Catalyst 6513 lapisan inti. Lingkungan ini juga secara khusus akan memiliki tempat server kecil yang akan memuat server-server arsip, dll. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch.

Masing-masing switch akan menjadi subnet (jaringan cadangan) (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana sebagian besar pelayanan terletak di bangunan-bangunan yang sama seperti para pengguna. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

Model di atas juga akan disebarakan di kampus-kampus yang dihubungkan ke WAN selama fungsionalitas lapisan 3 akan diperlukan bagi para pengguna untuk mengakses server di LAN lokal.

4.5.4.2 Bangunan Tipe B1 (B2 Untuk Redundansi Terbatas)

Model ini akan menyediakan switch agregasi kecil (seri Catalyst 3560) untuk mengakhiri hubungan-hubungan Gigabit Ethernet dari masing-masing switch Catalyst 2960&-24 lapisan akses. Switch Catalyst 3560 akan menghubungkan kembali ke pusat data lewat Gigabit EtherChannel ke switch Catalyst 6513 lapisan distribusi. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch. Masing-masing switch akan menjadi subnet (VLAN) dan spanning tree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada konsentrasi-konsentrasi besar pengguna yang memiliki sebagian besar pelayanan mereka yang diberikan dari pusat data. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

4.5.4.3 Bangunan Tipe C1 (C2 Untuk Redundansi Terbatas)

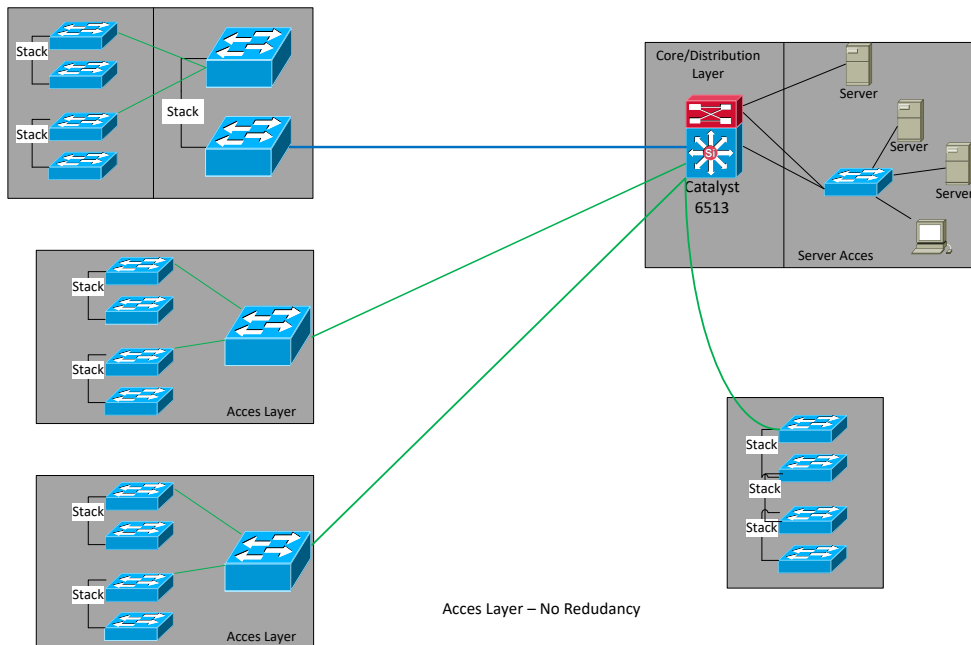
Switch-switch lapisan akses Gigabit Ethernet Catalyst 2970G-24 menghubungkan kembali ke switch-switch Catalyst 6513 lapisan distribusi di pusat data melalui tempat-tempat hubungan Gigabit Ethernet. Para pengguna secara khusus dapat menghubungkan secara langsung ke Catalyst 2970 lewat 10/100/1000mb Ethernet. Masing-masing switch akan menjadi subnet

(VLAN) dan Spanning Tree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada keperluan terhadap Gigabit Ethernet ke desktop.

4.5.4.4 Bangunan Tipe D1 (D2 Untuk Redundansi Terbatas)

Switch-switch lapisan akses Catalyst 2960G-48 meng-hubungkan kembali ke switch-switch Catalyst 6513 lapisan distribusi di pusat data melalui tempat-tempat hubungan Gigabit Ethernet. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch. Masing-masing switch akan menjadi subnet (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada konsentrasi kecil pengguna yang memiliki sebagian besar pelayanannya yang dibeikan dari pusat data.

4.5.5 Lapisan Akses – No Redundancy



Gambar 4.4 Arsitektur Lapisan Akses (No Redundancy)

Model ini akan menyediakan konektivitas yang sama seperti yang diusulkan pada model sebelumnya kecuali kalau hubungan-hubungan

redundan dihapuskan. Switch-switch dan router-router yang sama akan digunakan dan meskipun akan ada serat yang cukup dipasang namun port-port Gigabit Ethernet tambahan pada switch-switch tersebut tidak akan diperlukan. Model-model **A2**, **B2**, **C2** dan **D2** akan menjadi model ini. Model ini dapat digunakan di lingkungan-lingkungan dimana pengguna dapat menerima downtime sementara, tetapi sebenarnya hal itu akan berakhir sebagai biaya versus solusi fungsionalitas.

4.5.6 Wireless

Wireless Access Points akan disebabkan di lapisan akses untuk mengurangi persediaan konektivitas jaringan. Penting menempatkan kebijakan keamanan yang sangat kuat untuk mencegah setiap pengguna yang tidak sah dari mengakses jaringan UINSGD. Tempat-tempat akses seri AP 1130/1230 Cisco merupakan alat-alat yang lebih disukai untuk disebar di jaringan tersebut selama mereka mendukung 802.11a/b/g dan memiliki 12 frekuensi yang tidak saling melengkapi yang dapat digunakan.

Wireless LAN Services Module (WLSM) Seri Catalyst 6500 Cisco juga akan dipasang pada switch-switch lapisan distribusi 6513 untuk membantu dalam penanganan penyebaran skala lebih besar. WLSM adalah sebuah sistem penggantian berkabel dan nirkabel yang dapat diukur yang memungkinkan penjelajahan Lapisan 3 yang aman dan cepat di seluruh kampus dalam dan melewati subnet-subnet IP, mempertinggi keamanan WLAN (segmentasi kelompok pengguna dan pelayanan-pelayanan keamanan terpadu Catalyst, misalnya), dan mempermudah penyebaran dan manajemen WLAN. Komponen integral dari kerangka SWAN Cisco, WLSM mengabungkan pelayanan-pelayanan nirkabel ke infrastruktur-infrastruktur jaringan yang ada.

a) Pertimbangan-pertimbangan penyebaran

Di antara langkah-langkah paling pokok untuk diambil apabila merencanakan LAN nirkabel adalah mempelajari tentang berbagai jenis jaringan dan standar IEEE 802.11, menentukan jenis-jenis dan standar-standar mana yang tepat untuk keperluan-keperluan aplikasi anda, dan merencanakan penyebaran sesuai dengan itu.

b) Jaringan Infrastruktur

Pada sebuah jaringan infrastruktur, klien-klien WLAN menghubungkan ke jaringan melalui tempat akses nirkabel, dan kemudian beroperasi seperti yang akan dilakukan oleh klien berkabel. Metode ini akan digunakan untuk pelaksanaan tempat ramai pribadi.

c) Tempat Ramai

Tempat ramai nirkabel adalah lokasi geografik khusus di mana tempat akses memberikan pelayanan-pelayanan jaringan broadband umum nirkabel kepada pengunjung-pengunjung yang suka berpindah-pindah tempat melalui WLAN. Tempat-tempat ramai sering ditempatkan di tempat-tempat berpenduduk padat seperti pelabuhan udara, stasiun kereta api, perpustakaan, pusat-pusat konvensi dan hotel-hotel. Metode ini akan digunakan untuk menyediakan akses umum di perpustakaan-perpustakaan, dll.

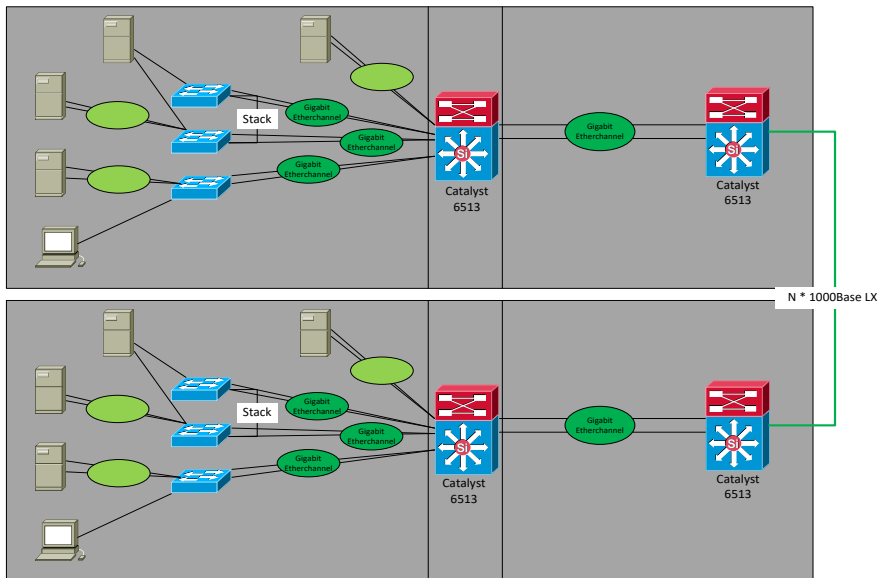
d) Jaringan-Jaringan Khusus

Untuk alasan-alasan keamanan jaringan-jaringan khusus tidak akan disediakan. Jaringan khusus adalah jaringan daerah lokal independen yang tidak dihubungkan ke infrastruktur berkabel dan dimana semua stasiun dihubungkan secara langsung ke satu sama lainnya (disebut topologi hubungan).

e) Standar-standar WLAN

Sekarang ini ada dua kategori dasar standar WLAN IEEE 802.11. Pertama adalah kategori-kategori yang menetapkan protokol-protokol dasar untuk sistem Wi-Fi lengkap. Standar-standar ini disebut 802.11a, 802.11b, dan 802.11g. Kedua, adanya perluasan-perluasan yang menghadapi kelemahan-kelemahan atau memberikan fungsionalitas tambahan kepada standar-standar ini. Standar-standar ini adalah 802.11d, e, f, h, i, dan j.

4.5.7 Model Data Center



Gambar 4.5 Arsitektur Data Center

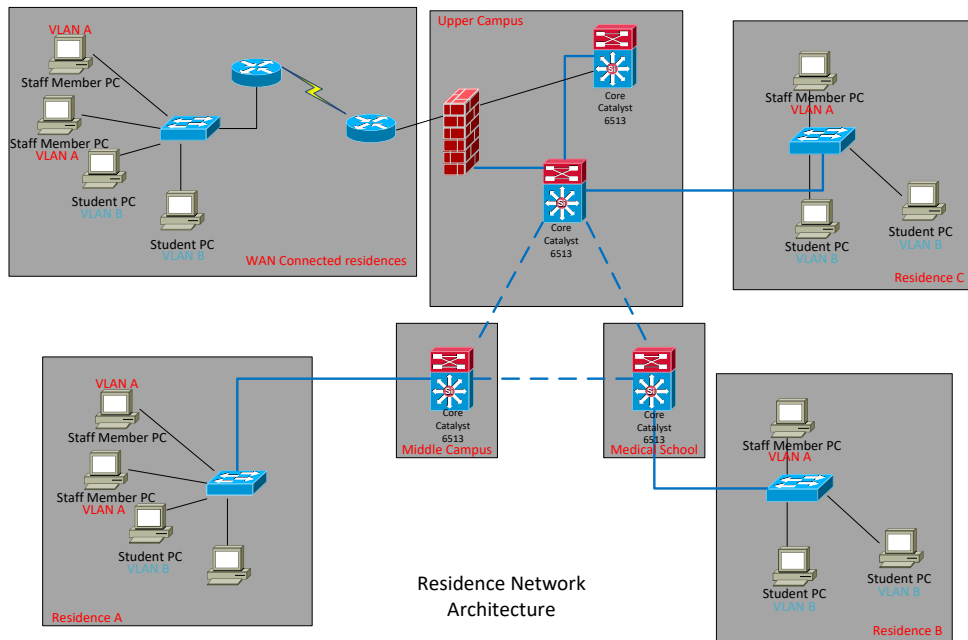
Data Center akan ditempatkan di bangunan-bangunan Kampus 1 dan Kampus 2. Data center ini juga akan menampung switch-switch lapisan inti

dan lapisan distribusi untuk kampus-kampus ini. Konektivitas server akan disediakan dengan cara berikut:

- a) **Konektivitas 10/100Mbps** – Switch-switch Catalyst 2960T-24 Cisco akan dihubungkan ke switch-switch Catalyst 6513 lapisan Distribusi melalui Gigabit EtherChannel. 2 port Gigabit akan menghubungkan ke dua blade berbeda pada Catalyst 6513 untuk mengurus redundansi. Server-server dapat menghubungkan ke switch-switch Catalyst 2960 ini lewat satu hubungan 10/100Mbps atau lewat EtherChannel jika server NIC mendukung fitur ini. Untuk tujuan-tujuan redundansi, sebuah switch Catalyst 2960 tambahan dapat diatur dan server NIC dapat dipisahkan di antara 2 switch tersebut. Namun fungsionalitas EtherChannel menjadi hilang dengan melakukan hal ini.
- b) **Konektivitas 1000Mbps (Pilihan 1)** – Blade WS-X6748-GE-TX akan dipasang pada switch Catalyst 6513 lapisan distribusi untuk menyediakan 48 port tembaga 10/100/1000Mbps yang dapat dihubungkan oleh server-server. Server-server ini akan menghubungkan ke switch Catalyst 6513 lewat satu hubungan 1000Mbps atau lewat Gigabit EtherChannel jika server NIC mendukung fitur ini. Blade WS-X6748-GE-TX tambahan dapat dipasang sehingga server NIC dapat dipisahkan di antara blade-blade untuk tujuan-tujuan redundansi. Fungsionalitas Gigabit EtherChannel tetap akan tersedia dalam solusi ini.
- c) **Konektivitas 1000Mbps (Pilihan 2)** – Switch-switch seri Catalyst 2970 atau 3700 Cisco akan menghubungkan ke switch lapisan distribusi Catalyst 6513 melalui Gigabit EtherChannel. 2 hubungan ke atas Gigabit akan menghubungkan ke dua blade berbeda pada Catalyst 6513 untuk mengurus redundansi. Server-server dapat menghubungkan ke switch-switch Catalyst 2970 ini lewat satu hubungan 1000Mbps atau lewat Gigabit EtherChannel jika server NIC mendukung fitur ini. Untuk tujuan-tujuan redundansi, sebuah switch Catalyst 2970 tambahan dapat diatur dan server NIC dapat dipisahkan di antara 2 switch tersebut. Namun fungsionalitas Gigabit EtherChannel menjadi hilang dengan melakukan hal ini.

4.5.8 Jaringan Residensial

Model-model jaringan yang dipertimbangkan untuk daerah-daerah tempat tinggal disoroti di bagian berikut:



Gambar 4.6 Arsitektur Jaringan Residensial

Tempat tinggal yang dihubungkan ke LAN akan memiliki switch-switch Catalyst 2960T-24 Cisco yang dipasang di tempat tinggal tersebut untuk menyediakan akses pengguna. Sebuah Catalyst 2960G-48 akan dipasang di masing-masing tempat tinggal untuk menyediakan konektivitas Gigabit Ethernet kembali ke switch Catalyst 6513 inti. Hubungan antara switch Catalyst 6513 dan Catalyst 2960G-48 akan diatur sebagai trunk 802.1Q untuk menyediakan banyak VLAN melewati hubungan ini. Masing-masing port pada switch tersebut akan diatur pada VLAN khusus untuk membedakan antara pengguna staf UINSGD dan pengguna tempat tinggal. Dalam peristiwa lebih dari satu switch yang digunakan, switch kedua akan menghubungkan ke switch pertama melalui trunk 802.1Q. Wireless Access Points juga dapat disebar di tempat-tempat tinggal untuk membatasi pengeluaran yang diadakan dengan memasang kabel di masing-masing ruangan.

Fungsionalitas lapisan 3 akan disediakan oleh switch lapisan distribusi Catalyst 6513 Kampus 1. Switch ini juga akan bertindak sebagai pintu gerbang kegagalan untuk semua tempat tinggal yang dihubungkan (LAN & WAN). Switch Catalyst 6513 lapisan distribusi Middle Campus akan digunakan sebagai switch failover. Satu-satunya pembatasan adalah bahwa hanya ada satu firewall yang dipasang pada saat sekarang ini, tetapi arsitektur yang baru tersebut akan mampu mengurus redundansi jika firewall yang kedua akan disebar di masa depan.

Keamanan akan diatur oleh firewall pusat sebagaimana jaringan tempat tinggal akan menghubungkan ke luar firewall tersebut. Semua akses yang dibutuhkan ke jaringan internal dan Internet akan diatur oleh firewall ini. Sebuah server ACS Cisco pusat akan digunakan untuk membuktikan semua pengguna nirkabel ke jaringan tersebut guna mencegah setiap akses yang tidak sah ke jaringan tersebut. Switch-switch Catalyst 2960T-24 juga akan mendukung pembuktian berbasis port 802.1X untuk menyediakan lapisan keamanan tambahan.

Tempat-tempat tinggal yang dihubungkan ke WAN akan mendapatkan router Cisco 1721 yang ada yang menyediakan konektivitas WAN di tempat jauh. Tempat jauh tersebut akan memiliki switch-switch Catalyst 2960T-24 Cisco yang dipasang untuk menyediakan akses pengguna. Hubungan antara router dan switch Catalyst 2960T-24 akan diatur sebagai trunk 802.1Q untuk menyediakan banyak VLAN melalui hubungan ini. Masing-masing port pada switch tersebut akan diatur di VLAN khusus untuk membedakan antara pengguna staf UINSGD dan pengguna tempat tinggal. Dalam peristiwa lebih dari satu switch digunakan, switch kedua akan menghubungkan ke switch pertama melalui trunk 802.1Q. Wireless Access Points juga dapat disebarkan di tempat-tempat tinggal untuk mengurangi persediaan konektivitas jaringan.

Untuk tujuan-tujuan keamanan, router akan memiliki daftar-daftar akses yang diatur untuk membaasi akses pengguna tempat tinggal ke pelayanan-pelayanan tertentu yang disediakan pada jaringan tersebut dan untuk merintangai setiap ancaman-ancaman virus yang potensial pada jaringan tersebut. Server ACS Cisco pusat akan digunakan untuk membuktikan semua pengguna nirkabel ke jaringan guna mencegah setiap akses tidak sah ke jaringan tersebut. Switch-switch Catalyst 2960T-24 juga akan mendukung pembuktian berbasis port 802.1X untuk menyediakan lapisan keamanan tambahan.

Pada hubungan WAN router QOS akan dilaksanakan untuk menilai batas pengguna tempat tinggal sehingga pengguna staf akan mampu bekerja dan menghentikan pengguna tempat tinggal dari membanjiri saluran bersambung tersebut. Masing-masing tempat tinggal akan disediakan subnet IP yang unik dan subnet ini akan dipisahkan menjadi 2 subnet dimana satu subnet akan digunakan oleh pengguna staf dan subnet lainnya oleh pengguna tempat tinggal. OSPF akan digunakan sebagai protokol pengiriman.

5. PEMBAHASAN

Pada bab ini akan dibahas mengenai tahapan implementasi dan juga pengujian dari blueprint yang telah dirancang supaya diketahui seberapa jauh tingkat keberhasilannya.

5.1 Model Logis

Model logis memberikan informasi yang diperlukan untuk membagi jaringan menjadi jaringan-jaringan cadangan Internet Protocol (IP) yang logis. Pemisahan logis ini diperlukan untuk membangun pengelompokan-pengelompokan jaringan modular yang mendukung sifat dapat diatur dari jaringan-jaringan yang kompleks. Bagian ini menyoroti struktur logis jaringan UINSGD yang diusulkan.

5.1.1 Jaringan Inti (Core Network)

Lingkungan logis akan menggunakan tingkat subnet kelas A 10.0.0.0/8 untuk seluruh jaringan kampus. Subnet ini akan dibagi menjadi segmen-segmen lebih kecil untuk menyediakan model yang lebih terstruktur, yang akan memungkinkan penggunaan ikhtisar-ikhtisar rute. Dalam melakukan hal itu setiap lalulintas pengiriman yang tak perlu akan dibuka kekuatan lapisan 3 dan dengan demikian membuat bandwidth tambahan ini menjadi tersedia untuk aplikasi-aplikasi pengguna.

Kampus utama akan dibagi menjadi 2 lingkungan subnet logis yakni Kampus 1 dan Kampus 2. Kampus-kampus yang dihubungkan ke WAN juga akan disediakan sejumlah subnet untuk membaginya secara logis dari sisa kampus utamanya. Lingkungan Internet dan pihak ketiga akan mencocokkan dengan skema pengalamatan baru dan sedikit atau tidak ada perubahan akan dilakukan di sama untuk membatasi gangguan.

Tabel berikut menggambarkan jumlah-jumlah subnet tingkat tinggi yang dialokasikan ke masing-masing blok kampus.

Tabel 5.1 Alokasi IP Address Area Core

Lingkungan	Jumlah Subnet
Kampus 1	192.168.18.0/24
Kampus 2	192.168.19.0/24
Area Pusat Pelatihan IT	192.168.20.0/24

5.1.2 Area Bangunan

Masing-masing bangunan di kampus tersebut akan disediakan sejumlah alamat TCP/IP tergantung pada jumlah pengguna per bangunan. Tingkat subnet ini kemudian akan dibagi menjadi subnet-subnet yang lebih kecil untuk menyediakan subnet yang unik per switch lapisan akses. Dokumentasi pengalamatan TCP/IP bangunan terperinci akan dilakukan sebagai bagian dari rencana pelaksanaan selama ada sejumlah perubahan yang harus terjadi untuk melakukan alokasi yang tepat per bangunan. Jumlah pengguna yang tepat per bangunan, perpindahan pengguna yang direncanakan dan juga gerakan server-server ke pusat-pusat data akan mempunyai dampak penting terhadap pengalamatan TCP/IP.

Sebagian besar dari bangunan tersebut akan cukup dengan sejumlah alamat TCP/IP kelas C (255.255.255.0) karena hal ini memungkinkan untuk 254 alamat yang dapat dipergunakan per bangunan. Namun ada bangunan-bangunan yang akan membutuhkan lebih dari 254 alamat TCP/IP dan dimana jumlah subnet yang lebih besar akan diperlukan. Banyak pekerjaan juga harus dapat dilakukan untuk mengubah alamat-alamat TCP/IP yang ada sekarang ini untuk mencocokkan dengan jumlah-jumlah alamat yang baru.

Jumlah-jumlah alamat berikut akan disediakan per bangunan untuk menampung jumlah pengguna dan juga memungkinkan untuk pertumbuhan di masa depan.

Tabel 5.2 Penggunaan IP Address

Jumlah pengguna	Tingkat subnet	Alamat yang dapat digunakan
0 sampai 200	255.255.255.0	254
200 sampai 400	255.255.255.0	510
400 sampai 1000	255.255.255.0	1022
Lebih dari 1000	255.255.248.0	2046

5.1.3 Jaringan Akses (Access Network)

Masing-masing switch lapisan akses akan disediakan sejumlah subnet terpisah dengan subnet mask 255.255.255.224. hal ini akan memungkinkan penggunaan hingga 30 host per subnet diantaranya 24 alamat akan digunakan untuk port-port yang ditetapkan oleh pengguna. Empat alamat akan digunakan untuk konfigurasi switch yaitu dua untuk switch-switch lapisan distribusi, satu untuk switch lapisan akses dan satu untuk alamat HSRP.

Enam alamat TCP/IP pertama dalam sebuah rangkaian akan selalu disediakan/dicadangkan bagi penggunaan tim jaringan untuk memungkinkan konfigurasi lingkungan switch. Alamat TCP/IP pertama akan selalu dialokasikan ke alamat standby HSRP dan akan menjadi pintu gerbang

kegagalan untuk VLAN khusus. Switch lapisan distribusi utama akan disediakan alamat TCP/IP kedua dan switch lapisan distribusi pendukung akan disediakan alamat TCP/IP ketiga. Switch lapisan akses akan disediakan alamat TCP/IP keempat.

Masing-masing switch juga akan diatur sebagai VLAN terpisah dan jumlah VLAN akan ditetapkan menurut jumlah bangunan, jumlah lantai dan jumlah switch. Sebagai contoh: switch ketiga yang dipasang di bangunan satu di lantai kedua akan dialokasikan ke VLAN1010.

Tabel 5.3 Alokasi IP Address Area Gedung

IP	Network Mask	Catatan	VLAN ID
10.161.10.0	255.255.255.0	Area CCTV	VLAN 1010
10.161.11.0	255.255.255.0	Area Lantai 1	
10.161.12.0	255.255.255.0	Area Lantai 2	
10.161.13.0	255.255.255.0	Area Lantai 3	
10.161.14.0	255.255.255.0	Area Lantai 4	
10.161.15.0	255.255.255.0	Area Hotspot 1	
10.161.16.0	255.255.255.0	Area Hotspot 2	
10.161.17.0	255.255.255.0	Alamat cadangan	
10.161.18.0	255.255.255.0	Alamat cadangan	
10.161.19.0	255.255.255.0	Alamat cadangan	

5.1.4 Protokol Routing

OSPF telah dipilih sebagai protokol pengiriman pilihan disebabkan karena fakta bahwa protokol ini merupakan protokol berbasis standa dan dapat saling beroperasi dengan setiap produk vendor. Model OSPF terperinci akan dimasukkan kedalam topologi jaringan yang baru, tetapi prinsip-prinsip berikut akan berlaku.

Daerah 0.0.0.0 akan dibentuk antara kampus-kampus Upper, Middle dan Medical Schooldan juga hubungan-hubungan rangkaian WAN.

Sisa dari daerah-daerah OSPF akan disediakan menurut blok-blok bangunan berbeda seperti digambarkan pada tabel di bawah.

Tabel 5.4 Area OSPF

Kampus	Daerah OSPF
Kampus 1	10.161.0.0
Kampus 2	10.171.0.0

5.1.5 Daerah Wewenang VTP

VLAN Trunking Protocol (VTP) adalah protokol pengiriman pesan Lapisan 2 yang mengatur penambahan, penghapusan, dan penamaan kembali VLAN atas dasar seluruh jaringan. Keuntungannya adalah bahwa jika VLAN diatur pada switch lapisan distribusi utama maka secara otomatis VLAN akan disambungkan ke switch dukungan. Penting sekali diingat bahwa nama VTP menjadi sensitif terhadap kasus. Switch-switch lapisan akses ada di daerah wewenang VTP yang sama seperti switch lapisan distribusi yang dihubungkan dengan switch-switch lapisan akses tersebut. Mode VTP dapat menjadi mode klien atau transparan pada switch-switch lapisan akses dan mode server pada switch-switch lapisan distribusi. Switch-switch inti juga diatur ke daerah wewenang VTP terpisah. Daerah-daerah wewenang VTP di kampus UINSGD akan dibagi menjadi daerah-daerah logis berikut:

Tabel 5.5 Domain VTP

Kampus	VTP Domain
Kampus 1	VTP_Kampus_1
Kampus 2	VTP_Kampus_2
Kampus Remote (WAN)	UINSGDWAN

5.1.6 Port Trunk

802.1Q akan digunakan sebagai protokol Trunking antara masing-masing switch. Trunking akan diatur hanya antara switch-switch lapisan akses dan masing-masing switch lapisan distribusinya. Juga akan ada contoh-contoh dimana trunking akan dimungkinkan antara dua switch lapisan akses. 'Mode' ini harus selalu diatur ke 'on' pada kedua sisi trunk tersebut. Hanya VLAN yang disusun pada switch-switch tersebut akan disediakan pada trunk-trunk.

5.1.7 Port Uplink

Konfigurasi port saluran harus dilakukan dengan mode yang 'diinginkan' yang diatur pada kedua ujung saluran. Hubungan-hubungan fisik juga harus dipisahkan di antara kartu-kartu saluran terpisah untuk mengurus redundansi dalam peristiwa kegagalan kartu yang tak mungkin akan terjadi. UDLD juga harus diatur pada masing-masing hubungan untuk mencegah adanya kegagalan-kegagalan perangkat keras yang menyebar ke jaringan tersebut.

Gambaran-gambaran harus disusun pada masing-masing hubungan uplink untuk mengurangi gangguan. Semua port yang tidak digunakan juga harus dilumpuhkan untuk mencegah para penggunaan yang tidak sah dari menyambungkan PC mereka ke switch tersebut.

Perangkat-perangkat SNMP dan pesan-pesan Syslog harus dihasilkan dalam peristiwa outage dan dikirimkan ke stasiun manajemen pusat.

5.2 Manajemen Jaringan

Manajemen Jaringan telah dirancang dari posisi praktik terbaik dan dibatasi ke komponen-komponen yang relevan yang diperlukan untuk jaringan baru yang diusulkan tersebut.

5.2.1 Pelaksanaan Khusus UINSGDNet

UINSGDNet memiliki keperluan-keperluan khusus tentang manajemen jaringan dan masing-masing dari keperluan-keperluan tersebut membutuhkan modul khusus untuk menghadapi keperluan-keperluan ini. Di bawah adalah keperluan-keperluan khusus dan juga hasil yang ditetapkan untuk memenuhi masing-masing keperluan:

Tabel 5.6 Model Manajemen Jaringan

Keperluan-keperluan Model Manajemen Jaringan	
Komponen-komponen	Keperluan-keperluan
Manajemen Pelaksanaan	HP Network Node Manager / E-Health
Pengukuran dan pemantauan suhu dengan pemeriksaan-pemeriksaan yang dapat diakses oleh jaringan pada router-router dan switch-switch	
Pengukuran QOS	
Pelaporan tentang penggunaan semua uplink inti dan distribusi	
Grafik-grafik Penggunaan – hubungan-hubungan WAN	
Visualisasi lalu lintas jaringan yang melewati WAN, inti dan distribusi (Netflow)	
Pelaporan sejarah paket-paket masuk, paket-paket keluar, lalu lintas unicast, lalu lintas broadcast dan kesalahan-kesalahan pada semua hubungan router	
Memory / CPU util dari router dan switch	
Perencanaan kapasitas (H/W dan Jaringan)	
Manajemen Konfigurasi	
Tempat konfigurasi di tengah-tengah untuk semua switch dan router	

Menempatkan alamat MAC di antara semua switch dari lokasi pusat	<p align="center">CiscoWorks LMS / Resource Manager Essentials & HP Network Node Manager (L3) / QPM</p>
Pencatatan semua perubahan untuk router dan switch (syslog, penghitungan radius)	
Dukungan terpusat konfigurasi router dan switch	
Tempat distribusi di tengah-tengah untuk perbaikan firmware switch dan router (versi kontrol)	
Manajemen kebijakan	
Manajemen Kesalahan	<p align="center">CiscoWorks Device Fault Manager (DFM) & Internetwork Performance Manager (IPM) & HP Network Node Manager (L3)</p>
Pemberitahuan terpusat tentang perubahan-perubahan keadaan hubungan (perangkap-perangkap SNMP) – uplink WAN & Inti/ Distribusi	
Pencatatan dan pengarsipan terpusat perubahan-perubahan keadaan hubungan (syslog server)	
Pemberitahuan dan pelaporan kesalahan-kesalahan/masalah-masalah	
Deteksi kesalahan-kesalahan/masalah-masalah	
Pencatatan kesalahan-kesalahan	
Pemisahan masalah-masalah	
Analisis masalah-masalah	
Identifikasi kecenderungan-kecenderungan	
Manajemen Laporan	
Jejak audit akses yang dibuat ke peralatan jaringan	<p align="center">CiscoWorks Device Fault Manager (DFM) / Resource Manager Essentials / ACS</p>
Jejak audit untuk penggunaan jaringan	

Seperti yang dapat dilihat dari tabel di atas, CiscoWorks (L2) dan HP Network Node Manager (L3) dan E-Health mengurus fungsi-fungsi manajemen jaringan. HP Node Manager adalah sebuah alat manajemen jaringan yang memberikan informasi tentang penggunaan hubungan, penggunaan router/switch memory, dll. Alat ini juga memberikan data historis terbatas dan memberikan pelaporan analisis kecenderungan dasar.

5.2.2 Manajemen Jaringan - Perangkat Keras

Vendor menganjurkan agar aplikasi CiscoWorks dipasang pada sebuah sistem Sun Solaris selama aplikasi ini menyediakan platform yang lebih stabil. Sistem yang mengoperasikan Windows tersebut lebih mudah mendapat serangan-serangan virus dan peretasan.

5.2.3 Manajemen Jaringan - Perangkat Lunak

Seperti yang dapat dilihat dari daftar keperluan-keperluan di atas, Cisco LMS suite harus dapat dibeli untuk memenuhi keperluan-keperluan UINSGD:

CiscoWorks bekerja pada platform yang diresmikan (dan tidak berbagi sumber-sumber dengan aplikasi-aplikasi lain). Seperti disebutkan di atas, CiscoWorks dapat bergabung sepenuhnya dengan remote node manager seperti HP Network Node Manager. Ciscoworks muncul dengan sebuah alat integrasi yang akan menempati daftar-daftar, bidang-bidang, obyek-obyek, trap format file (trapd.log), juga menambah pokok-pokok menu yang relevan. Setelah integrasi, obyek-obyek switch/router akan beralih dari obyek-obyek 'umum' ke obyek-obyek 'Cisco'. Aabila obyek Cisco dipilih, CiscoView dapat diluncurkan, dan gambaran grafis switch/router ditampilkan. Grafik-grafik waktu nyata menampilkan muatan-muatan lalulintas dan kesalahan-kesalahan pada port-port switch/router.

HP Network Node Manager akan menampilkan tipologi lapisan 2/3, sementara CiscoWorks Campus Manager akan menampilkan topologi lapisan 2, yang dapat digunakan untuk memeriksa susunan fisik jaringan tersebut. Semua peristiwa Syslog dapat dikirimkan ke CiscoWorks dan dikelompokkan menjadi sejumlah total masalah-masalah besar, kritis dan kecil per alat. Pada dan di atas solusi manajemen CiscoWorks, vendor juga menganjurkan agar HP Node Manager digunakan untuk mengurus pelaporan pelaksanaan seperti yang diminta di atas. hal ini akan memberikan grafik-grafik waktu nyata kepada UINSGD yang menggambarkan penggunaan bandwidth, dll.

Kami mengemukakan CiscoWorks sebagai alat aplikasi manajemen paling tepat untuk manajemen peralatan Cisco. CiscoWorks bergabung sepenuhnya dengan HP Network Node Manager. HP Network Node Manager adalah sebuah alat Fault Management yang merupakan produk bebas, sementara di pihak lain CiscoWorks adalah Element Manager yang merupakan produk terikat (dapat dipergunakan untuk semua peralatan Cisco).

Kami mengemukakan lebih lanjut CiscoWorks LAN Management Solution (LMS) sebagai alat manajemen paling tepat. Alat ini terdiri dari serangkaian aplikasi jaringan kuat yang memberikan dasar kuat aplikasi-aplikasi manajemen yang lebih maju untuk mempertahankan, memantau, dan mencari dan memecahkan persoalan sejumlah alat yang luas pada sebuah jaringan Cisco dari akhir ke akhir. LMS adalah anggota keluarga produk-

produk CiscoWorks. Produk-produk ini bekerja bersama-sama untuk memberikan solusi-solusi paling penting untuk memperbaiki ketelitian dan efisiensi dari staf operasi, meningkatkan ketersediaan jaringan yang menyeluruh melalui perencanaan proaktif, dengan cara demikian juga memaksimalkan keamanan jaringan.

5.2.4 Migrasi

Salah satu tindakan paling penting yang harus dilakukan apabila berpindah tempat ke sebuah infrastruktur jaringan yang baru adalah menetapkan dasar-dasar kinerja jaringan untuk jaringan yang baru guna mempertahankan spesifikasi-spesifikasi dan ambang-ambang batas kinerja. Sebuah tim spesialis jaringan akan menjadi bertanggung jawab untuk menentukan keperluan-keperluan dari jaringan tersebut. Keperluan-keperluan ini meliputi kapasitas, kinerja dan sifat-sifat pengiriman jaringan lainnya yang akan diidentifikasi dari dasar tersebut dan yang akan membantu dalam mengatur jaringan yang ada sekarang ini dan jaringan yang baru selama migrasi (perpindahan tempat).

Untuk menjelaskan persepsi-persepsi di sekitar kinerja jaringan, dianjurkan agar statistik kinerja dikumpulkan dari hubungan-hubungan akhir ke akhir pada jaringan yang baru dalam status tidak diisi dan dibandingkan terhadap informasi dasar dari jaringan yang ada. Selama komunitas pengguna berpindah tempat melewati ke jaringan yang baru, ukuran-ukuran yang sama ini harus diulang untuk menjamin bahwa kinerja jaringan tetap dalam tingkat-tingkat yang dapat diterima untuk menghindari gangguan reaktif dan perdebatan-perdebatan pengguna jaringan.

Dengan demikian penting sekali sistem manajemen jaringan tersebut disebarkan secepat mungkin, untuk mengadakan kontrol infrastruktur jaringan secara proaktif. Konfigurasi manajemen jaringan CiscoWorks LMS memiliki modul-modul cadangan seperti Resource Manager Essentials, Internet Performance Manager DFP dan Campus Manager. Alat-alat ini harus digunakan dari tahap-tahap awal untuk memberikan instalasi, konfigurasi dan manajemen infrastruktur yang baru dan juga untuk memantau dan mengontrol integrasi dengan jaringan yang lama. CiscoWorks adalah sebuah alat teknis yang digunakan terutama untuk konfigurasi dan pencarian dan pemecahan masalah gangguan. Penggunaan yang terbatas adalah untuk pelaporan online/langsung.

Di antara rangkaian produk-produk Catalyst, Cisco telah menanamkan kemampuan-kemampuan termasuk SNMP, RMON, Netflow Statistics, HTTP, diagnostics/debug, Syslog, protokol-protokol plug-and-play, alat-alat penemuan tipologi, dan banyak lagi. CiscoWorks mengambil keuntungan dari kemampuan-kemampuan ini dan memberikan akses ke manajemen jaringan berbasis Internet.

Produk-produk dalam keluarga CiscoWorks melakukan banyak fungsi manajemen penting untuk mengatur berbagai macam alat jaringan yang ada, termasuk router, switch, pusat, dan alat0akat SNMP umum. Resource Manager Essentials melakukan perbaikan-perbaikan perangkat lunak Cisco, mengurut inventaris, melaporkan tersedianya alat, menganalisis pesan-pesan Syslog, dan melaporkan perubahan-perubahan konfigurasi untuk switch-switch dan router-router.

Untuk mengatur perpindahan tempat infrastruktur kampus, sebuah sistem manajemen CiscoWorks LMS yang diperkecil terdiri dari modul-modul dasar berikut akan dilaksanakan:

- a) CiscoWorks Device Fault Manager (DFM) 2.0
- b) CiscoWorks Campus Manager 4.0
- c) CiscoWorks Resources Manager Essentials (RME) 4.0
- d) CiscoWorks Internetwork Performance Monitor (IPM) 2.6
- e) CiscoWorks Common Service 3.0 dengan CiscoView 6.1

5.2.5 Fitur CiscoWorks

CiscoWorks LMS meliputi lima modul yang memainkan peranan-peranan berbeda dalam menemukan dan mengatasi gangguan dari jaringan tersebut. Modul-modul ini mengatur bidang-bidang berikut pada jaringan tersebut:

- a) Switch-switch dan router-router Cisco
- b) Analisis kesalahan waktu nyata alat-alat jaringan
- c) Manajemen inventaris waktu nyata
- d) Gambaran-gambaran status dinamis dari jaringan tersebut
- e) Server manajemen sebagai tempat switch CiscoWorks merupakan fasilitas komunikasi dan keamanan seluruh aplikasi.

Penggunaan utama alat-alat tersebut adalah untuk membantu para ahli teknik jaringan dalam menemukan kesalahan dan mengatur alat. Fitur-fitur pelaporan terbatas diberikan pada alat-alat Jaringan dan pemantauan batas ambang terbatas disediakan. CiscoWorks adalah sekumpulan aplikasi untuk mempertahankan, memantau dan menemukan dan mengatasi gangguan alat-alat Cisco. Bagian depan CiscoWorks berbasis jaringan, memungkinkan personil teknis yang disahkan mengakses sistem tersebut dari manapun pada jaringan tersebut.

CiscoWorks terdiri dari alat-alat terfokus secara operasional yang memberikan teknologi-teknologi penemuan; gambaran-gambaran topologi yang dapat diukur; alat-alat penempatan port analisis jalur layer 2 atau layer3;

analisis konektivitas; alat-alat manajemen konfigurasi; dan alat serta kemampuan diagnostik jaringan (termasuk manajemen kesalahan dan pemantauan lalu lintas Remote Monitoring [RMON]) untuk membantu mengatur kerumitan-kerumitan dari sebuah jaringan yang bersatu.

CiscoWorks adalah sebuah alat yang sangat berguna bagi staf teknis untuk mengatur, menyusun dan menemukan serta mengatasi kesulitan jaringan Cisco dengan cepat dan efisien. Berbagai modul menghapuskan tugas-tugas yang membosankan atau menghabiskan waktu yang sering menyebabkan masalah-masalah dalam jaringan-jaringan. CiscoWorks adalah sebuah alat konfigurasi dan mencari dan mengatasi kesulitan untuk digunakan hanya oleh staf teknis. Disebabkan karena kemampuan-kemampuan yang kuat dari alat ini, maka penting bahwa hanya staf teknis yang disahkan memiliki akses ke alat tersebut. Sistem ini dilindungi oleh password sehingga hanya personil yang disahkan memiliki akses ke sistem tersebut. Meskipun alat ini memiliki kemampuan-kemampuan jaringan yang kuat, namun harus diperhatikan bahwa:

- a. CiscoWorks bukan merupakan alat pelaporan. Laporan-laporan waktu nyata yang khusus dapat berjalan selama mencari dan mengatasi kesulitan, tetapi laporan-laporan ini hanya untuk penggunaan yang nyata. CiscoWorks tidak mengurus penelusuran pengguna.
- b) CiscoWorks tidak mengumpulkan dan menyimpan data SNMP dari alat-alat tersebut. Hanya data konfigurasi dan versi-versi IOS yang disimpan oleh CiscoWorks 2000.
- c) CiscoWorks hanya memantau alat-alat TCP/IP.
- d) CiscoWorks tidak menggantikan sniffer selama sniffer menangkap paket-paket.
- e) CiscoWorks tidak mengetahui tentang aplikasi-aplikasi selama ia beroperasi pada lapisan jaringan.
- f) CiscoWorks mengurus pemantauan alat jaringan dan tidak memeriksa kesalahan-kesalahan pemasangan kabel atau NIC.

Laporan-laporan bulanan harus dikerjakan melalui alat-alat pelaporan lainnya. Cisco menganjurkan mitra dalam hal ini adalah Concord (E-Health).

CiscoWorks adalah alat manajemen teknis untuk digunakan oleh *network engineers*. Meskipun ada keperluan-keperluan khusus dari CiscoWorks, namun fitur-fitur *network management* yang ada sekarang ini, sebagai berlawanan dengan *network monitoring*, telah ditetapkan di dalam *blueprint* pembaharuan jaringan kampus ini.

5.2.6 Dukungan dari Jauh (*Remote Support*)

CiscoWorks dapat mengirimkan setiap peristiwa kritis ke Node Manager lain (mungkin lebih dari satu) dan datang dengan web client interface yang memberikan akses penuh ke sistem manajemen kepada seseorang dengan dukungan dari jauh. Kemampuan ini memberikan fleksibilitas sangat besar kepada UINSGD dalam mengatur keperluan-keperluan dukungan dan manajemennya. Sebagai contoh, Vendor memberikan fasilitas-fasilitas pemantauan dan manajemen dari jauh melalui 24x7 Monitoring, Automation & Response Centre (MARC) kita yang terpusat. MARC memantau sejumlah alat dan peristiwa di beberapa negara di benua-benua yang berbeda atas dasar 24x7.

Perangkat-perangkat atau peristiwa-peristiwa kritis tertentu harus dapat dipantau di luar kemampuan inti UINSGD atau dimana biaya untuk memberikan dukungan tersebut di dalam negeri dapat terbukti menghambat (misalnya, 24x7 pemantauan alat-alat atau peristiwa-peristiwa kritis). UINSGD akan memilih peristiwa atau alat mana yang akan memantau atau mengatur secara lokal dan mana yang akan beralih ke MARC Vendor. Berdasarkan jumlah alat yang akan dipantau, dan kumpulan peristiwa-peristiwa yang akan disebar dan diatur dari MARC kita, sebuah model finansial yang dapat dipertimbangkan dapat ditentukan. Service Level Agreement kemudian disetujui dan digunakan untuk mengatur dan mengurus pelayanan satu sama lain.

Susunan yang fleksibel ini, yang akan ditinjau secara berkala dan dapat dipertimbangkan atas permintaan, memberikan kemampuan kepada UINSGD untuk mengoptimalkan manajemen biaya dan resiko.

CiscoWorks LMS memberikan:

- a) Penemuan jaringan, gambaran-gambaran topologi, penelusuran stasiun akhir dan manajemen VLAN untuk jaringan-jaringan berswitch Cisco.
- b) Analisis kesalahan jaringan waktu nyata dengan template-template praktik terbaik khusus alat yang mudah menyebar.
- c) Manajemen inventaris perangkat keras dan perangkat lunak, alat-alat konfigurasi terpusat, dan pemantauan Syslog.
- d) Alat waktu nyata, hubungan, dan manajemen lalu lintas port, analisis, dan pelaporan.
- e) Klien yang dimungkinkan oleh jaringan yang memberikan akses jauh ke sistem manajemen.

5.2.7 Pelayanan-pelayanan Monitoring, Automation & Response Centre (MARC)

Kumpulan pelayanan-pelayanan pemantauan yang tersedia dari MARC Vendor adalah luas dan diberikan menurut permintaan. Solusi pemantauan dan manajemen dapat meliputi switch-switch/router-router baik pusat atau jauh, dan kampus-kampus satelit selama diperlukan. Pemantauan semua saluran data dilakukan secara khusus, dengan fokus pada penggunaan dan tersedianya bandwidth.

MARC Vendor ditempatkan di Midrand dan digunakan untuk memantau jaringan-jaringan di seluruh negara dan internasional SA Vendor. Pemantauan server-server di Afrika Selatan dan di lokasi-lokasi lain di Eropa dan seluruh dunia juga berlangsung dari pusat ini. MARC bekerja 24x7 dan dilengkapi dengan personil cakap yang memiliki pemahaman mendalam tentang keperluan-keperluan dan bisnis pelanggan selama mereka berubah-ubah pada window 24 jam. Dihubungkan dengan pemantauan dari MARC adalah prosedur-prosedur dan waktu-waktu eskalasi yang berbeda-beda, tergantung pada skenario kegagalan atau masalah yang berkembang pada saat tertentu.

Apabila pemnataun diadakan dari MARC, laporan-laporan manajemen jaringan diberikan atas dasar bulanan sebagai bagian dari perjanjian tingkat pelayanan dan tawaran pelayanan. Namun, laporan manajemen jaringan dapat diberikan pada setiap saat, hal ini akan diperlukan untuk masalah atau kejadian khusus dalam jaringan tersebut.

5.3 Keamanan Jaringan

Keamanan jaringan merupakan bagian dari strategi keamanan IT seluruhnya dan meskipun keamanan IT UINSGD sepenuhnya tidak dihadapi di dalam Cetak Biru ini, namun keamanan komponen jaringan yang relevan dimasukkan.

5.3.1 Model Manajemen Keamanan

Keperluan-keperluan manajemen keamanan khusus UINSGD berikut telah diidentifikasi:

Tabel 5.7 Model Manajemen Keamanan

Keperluan-Keperluan Model Manajemen Keamanan Jaringan	
Keperluan	Komponen
Manajemen Keamanan	
Pembuktian Keaslian ke Petunjuk Baru untuk:	
– Akses manajemen ke switch-switch dan router-router	
– Akses nirkabel	

- Pembuktian port akses lewat 802.1x	ACS Cisco
Konfigurasi kategori-kategori pengguna ber-beda berdasarkan berbagai kriteria:	
- Akses membaca	
- Akses menulis	
- Akses ke dialup lewat RAS	
- Akses ke callback lewat RAS	
Pemantauan dan pengujian kebijakan-kebijakan	
Akses ke jaringan	
- Akses SNMP	
- Pengujian kerentanan	
- Pembaharuan password administrasi	Fitur IOS
Akses aman versi 3 SNMP ke informasi MIB pada switch-switch – tidak ada akses SNMP v1 / 2c umum/pribadi	
Menggunakan SSH daripada Telnet	

5.3.2 Keamanan Lapisan Akses 802.1X

Jaringan berbasis kebijakan 802.1x yang dilaksanakan sebagai bagian dari solusi jaringan menghadapi masalah-masalah yang berhubungan dengan akses fisik tidak sah ke jaringan tersebut. Jaringan-jaringan modern menggunakan sejumlah mekanisme termasuk DHCP untuk mengurangi jumlah administrasi yang diperlukan untuk menghubungkan para pengguna ke jaringan tersebut dan memberikan konektivitas yang diperlukan untuk melaksanakan pekerjaan mereka. Walaupun mekanisme-mekanisme ini memudahkan bagi para pengguna yang sah untuk menghubungkan ke jaringan, namun orang-orang yang tidak sah dengan akses ke tempat akses LAN yang kosong memiliki kemampuan untuk menghubungkan ke jaringan tanpa mengetahui infrastruktur atau IP addressing. Dari tempat ini mereka dapat menjalankan alat-alat terhadap jaringan tersebut untuk mengumpulkan informasi, memasukkan kode merugikan atau melakukan penyangkalam serangan-serangan pelayanan terhadap para pengguna lain pada jaringan tersebut.

Menggunakan alat jaringan berbasis kebijakan ini memungkinkan untuk membatasi konektivitas dari tempat jaringan khusus ke sumber-sumber tertentu hingga waktu seperti pengguna tersebut telah membuktikan kebenaran. Pembuktian ini dapat menjadi lingkungan Novel Directory, tempat wewenang Windows NT, Windows Active Directory atau database pengguna lainnya. Setelah pengguna tersebut dibuktikan, port diatur kembali oleh sistem untuk memungkinkan konektivitas yang diperlukan oleh pengguna yang dibuktikan tersebut. Bagian kritis dari mencapai keberhasilan dengan menyebarkan 802.1x sebagai bagian dari solusi keamanan adalah memiliki

sebuah model tatakelola yang tepat di tempat. Model tatakelola tersebut harus bersifat menentukan sedapat mungkin untuk pengguna akhir dipandang dari sudut sistem yang beroperasi, paket-paket anti-virus yang dipasang, pembaharuan-pembaharuan patch, dll. Jika tidak ada model tatakelola di tempat maka penyebaran 802.1x akan menjadi model yang sangat sulit disebarakan.

Server ACS Cisco sentral akan digunakan untuk membuktikan semua pengguna nirkabel ke jaringan tersebut guna mencegah setiap akses tidak sah ke jaringan tersebut. Switch-switch Catalyst akan mendukung pembuktian berbasis port 802.1x untuk menyediakan lapisan keamanan tambahan. Untuk menyebarkan 802.1x pada jaringan tersebut ada sejumlah ketergantungan pada stasiun-stasiun kerja dan juga server-server yang harus ditempatkan. Server ACS Cisco akan menyediakan fungsionalitas Radius yang dibutuhkan untuk penyebaran 802.1x ke lingkungan Novel Directory yang relevan, tempat wewenang Windows NT, Windows Active Directory atau database pengguna lain.

5.3.3 Keamanan LAN

Keuntungan dari *private VLAN* adalah fitur yang memiliki arti penting lokal hanya untuk switch tersebut dan tidak ada pemisahan yang diadakan antara dua port dilindungi yang ditempatkan pada switch-switch berbeda. Port yang dilindungi tidak meneruskan setiap lalu lintas (unicast, multicast, atau broadcast) ke setiap port lainnya yang juga merupakan port dilindungi pada switch yang sama. Lalu lintas tidak dapat diteruskan antara port-port yang dilindungi pada lapisan 2, semua lalu lintas yang melewati antara port-port yang dilindungi harus diteruskan melalui alat lapisan 3.

Private VLAN mengadakan pemisahan lapisan 2 antara port-port dalam tempat wewenang broadcast yang sama. Ada tiga jenis port PVLAN:

- a) **Promiscuous**— port tidak memilih-milih ini dapat berkomunikasi dengan semua hubungan, termasuk port-port terpisah dan komunitas dalam PVLAN.
- b) **Isolated**— port terpisah ini memiliki pemisahan Lapisan 2 yang lengkap dari port-port lainnya dalam PVLAN yang sama, tetapi tidak dari port-port yang tidak memilih-milih. PVLAN merintang semua lalu lintas ke port-port terpisah kecuali lalu lintas dari port-port yang tidak memilih-milih. Lalu lintas dari port terpisah diteruskan hanya ke port-port yang tidak memilih-milih.
- c) **Community**— port-port komunitas ini ber-komunikasi di antara mereka sendiri dan dengan port-port yang tidak memilih-milih. Hubungan-hubungan ini dipisahkan pada Lapisan 2 dari semua hubungan lainnya di dalam port-port komunitas atau terpisah lain dalam PVLAN.

VLAN access lists (VACL) memberikan kontrol akses untuk semua paket yang dipertemukan dalam VLAN atau yang dikirimkan ke atau dari VLAN. Tidak seperti IOS ACL Cisco biasa atau tetap yang diatur pada hubungan-hubungan router dan diterapkan hanya pada paket-paket yang dikirimkan, VACL berlaku untuk semua paket.

VLAN Membership Policy Server (VMPS) memungkinkan anda menempatkan port-port switch ke VLAN secara dinamis, berdasarkan alamat MAC sumber dari alat yang dihubungkan ke port tersebut. Apabila anda memindahkan host dari sebuah port pada satu switch dalam jaringan tersebut ke port pada switch lainnya dalam jaringan tersebut, switch menempatkan port yang baru secara dinamis ke VLAN yang tepat untuk host tersebut.

5.3.4 Cisco Clean Access

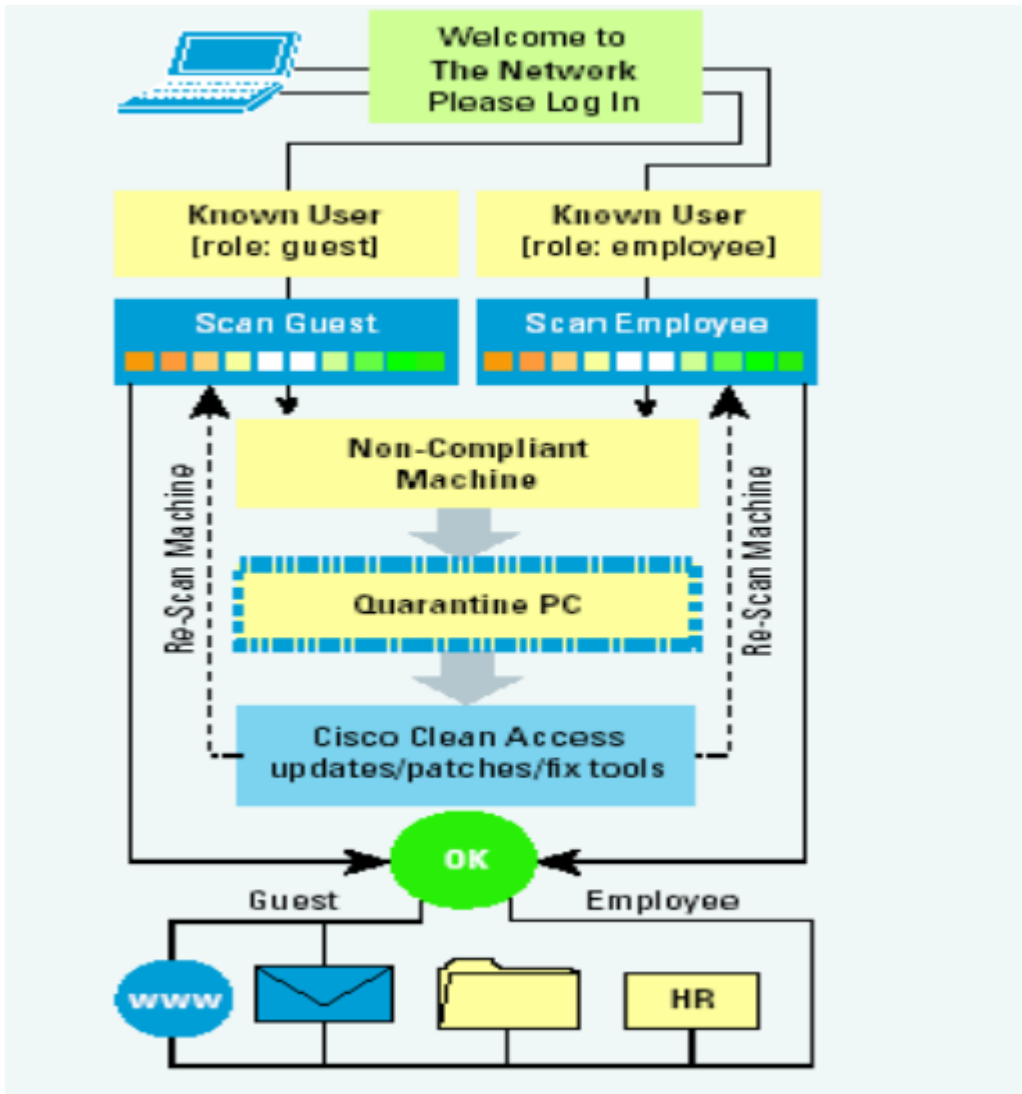
Cisco Clean Access (CCA) adalah solusi sentries jaringan untuk melaksanakan kepatuhan pada kebijakan-kebijakan keamanan pada semua alat yang dihubungkan ke jaringan. Kebijakan-kebijakan ini berlaku untuk staf permanen, kontraktor atau tamu.

Ada tiga faktor perlindungan penting yaitu:

- a) Mengakui pengguna, alat mereka dan peranan yang dimainkan oleh mereka di dalam jaringan tersebut
- b) Mengevaluasi kepatuhan mesin-mesin pada kebijakan keamanan
- c) Melaksanakan kebijakan dengan memperbaharui, memperbaiki atau menghalangi alat tersebut

Keuntungan dari CCA adalah ia merupakan solusi berdiri sendiri atau berkelompok yang dapat disebarkan dengan cepat. CCA menggabungkan manajemen identitas, kontrol lalu lintas jaringan dan penilaian kerentanan dan juga manajemen patch. CCA menghentikan penyebaran virus dan ulat sebelum sebelum dapat memperoleh akses ke jaringan tersebut. CCA juga menurunkan biaya staf dukungan dan pemeliharaan selama CCA mengotomatiskan proses-proses pemeriksaan manual. CCA juga melengkapi arsitektur kontrol pengakuan jaringan.

Rangkaian arus lalu lintas CCA yang khusus diperlihatkan di bawah:



Gambar 5.1 Model Flow CCA

Penting bahwa lingkungan CCA dicakup secara lebih terperinci pada tahap perencanaan keamanan. CCA meliputi komponen-komponen berikut:

- Klien pelaksanaan untuk pengamatan dan perbaikan berbasis alat di lingkungan yang diatur dan tidak diatur
- Server penilaian yang memulai penilaian dan menjalankan akses berdasarkan pemenuhan endpoint
- Manajemen GUI terpusat
- Server penilaian failover pilihan

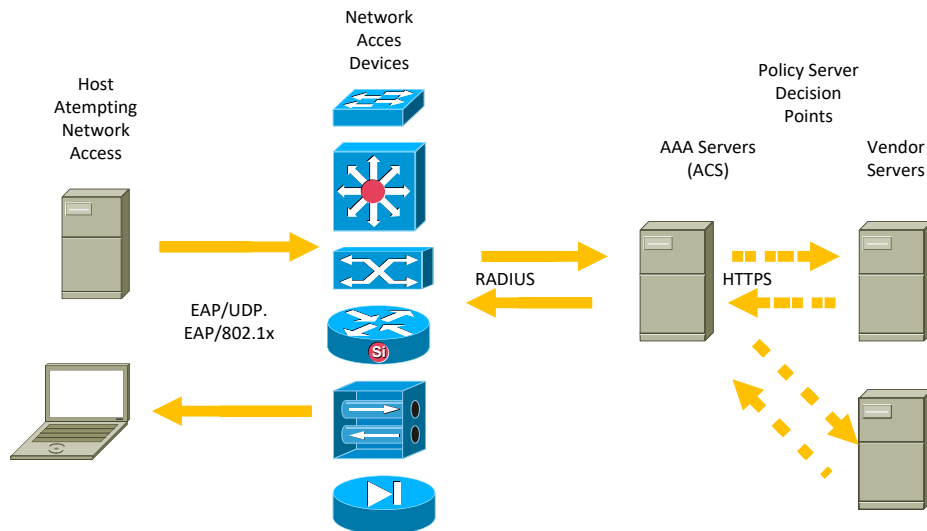
5.3.5 Network Admission Control

NAC merupakan bagian dari inisiatif Cisco yang disebut Delf Defending-Network. NAC menggunakan investasi-investasi infrastruktur yang ada sambil memperluas nilai Cisco Security Agent dan juga perlindungan antivirus dan perangkat lunak keamanan pihak ketiga lainnya.

NAC meliputi komponen-komponen penting berikut:

- a) **Alat komunikasi** – Cisco Trust Agent adalah alat perangkat lunak yang mengumpulkan informasi keadaan keamanan dari solusi-solusi perangkat lunak keamanan pada endpoint, seperti antivirus, OS, dan Cisco Security Agent, dan menghubungkan alat ini ke alat akses jaringan.
- b) **Alat-alat akses jaringan** – Setiap awal yang mencari akses jaringan pada awalnya mengontak alat akses jaringan (router, switch, VPN concentrator, atau firewall). Alat-alat ini dapat menuntut “surat-surat kepercayaan” keamanan endpoint dari endpoint melalui Cisco Trust Agent dan menyampaikan informasi ini ke server-server kebijakan untuk keputusan pengakuan.
- c) **Server-server kebijakan** – Cisco Secure Access Control Server (ACS) dan server-server kebijakan vendor pihak ketiga mengevaluasi surat-surat kepercayaan keamanan endpoint yang dikirimkan dari alat akses jaringan dan menentukan kebijakan akses yang tepat untuk diterapkan (*mengizinkan, menyangkal, meng-karantina, membatasi*).
- d) **Sistem-sistem manajemen** – CiscoWorks VPN/ Security Management Solution (VMS), CiscoWorks Security Information Manager Solution (SIMS), dan unsur-unsur NAC pengadaan solusi-solusi manajemen dukungan bersama NAC, memberikan alat-alat pemantauan dan pelaporan, dan mengatur aplikasi-aplikasi keamanan endpoint.
- e) **Advanced Services** – Advanced Services menawarkan pelayanan-pelayanan konsultasi perencanaan, perancangan dan pelaksanaan terpadu untuk membantu staf IT menyebarkan solusi NAC yang efektif guna melaksanakan pemenuhan host.

Diagram di bawah menggambarkan tinjauan NAC Cisco total.



Gambar 5.2 Arsitektur NAC

5.3.6 Keamanan Perangkat Jaringan

Hal pertama yang harus dilakukan adalah memastikan bahwa semua alat jaringan dipasang di lingkungan yang aman dan bahwa hanya pengguna yang disahkan memiliki akses ke lokasi-lokasi ini. Alasannya adalah bahwa siapa saja yang memiliki akses fisik ke sebuah switch atau router dapat menghubungkan ke alat ini melalui hubungan tempat switch dan menyampaikan password untuk memasuki jaringan tersebut. Hal ini biasanya menjadi metode paling mudah untuk memperoleh akses ke sebuah jaringan.

Keamanan alat jaringan merupakan salah satu lapisan keamanan paling penting selama alat-alat harus dilindungi dari serangan-serangan jahat seperti serangan-serangan pelayanan (DOS), dll. Perangkat produk ACS Cisco akan digunakan untuk memberikan akses pengguna yang disahkan ke alat-alat jaringan. Akses ini akan diatur lebih lanjut melalui ACS Cisco untuk tim operasi misalnya agar dapat melakukan perubahan-perubahan konfigurasi tertentu dan memberikan akses spesialis jaringan ke perintah-perintah konfigurasi spesialis.

a) Versi IOS

Versi 12.2 IOS dan di atas telah diuji secara luas. Menjamin bahwa semua alat Cisco yang ada sudah ada pada kode ini. Peralatan yang baru ini akan dipasang dengan kode penyebaran umum (GD) terbaru untuk membatasi kemungkinan-kemungkinan kerentanan keamanan. Untuk menjalankan SSH dan SNMPV3, kode 3DES Crypto harus dipasang pada semua alat.

b) SSH

SSH akan digunakan daripada aplikasi Telnet standar. Hal ini akan memungkinkan enkripsi lalu lintas pertemuan telnet melewati jaringan UINSGD.

c) SNMPv3

SNMPv3 akan memungkinkan enkripsi semua lalu lintas SNMP ke dan dari alat-alat jaringan

5.4 Proses Migrasi

Bagian ini menggambarkan tugas-tugas yang harus diselesaikan untuk berpindah tempat dari jaringan kampus yang ada ke jaringan kampus yang diusulkan. Kerangka-kerangka waktu yang berhubungan dengan masing-masing kerangka menggambarkan skenario kasus paling buruk dan dapat dipersingkat. Beberapa dari tahap-tahap tersebut juga dapat berjalan secara simultan selama tahap-tahap tersebut tidak akan mempengaruhi satu sama lainnya.

5.4.1 Prasyarat Migrasi

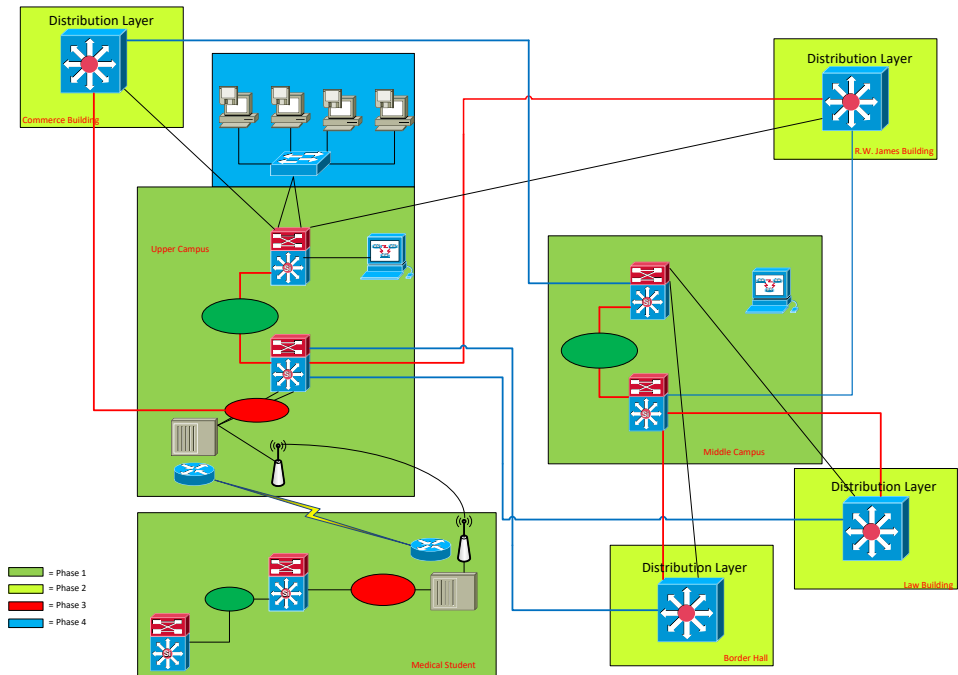
Ada sejumlah prasyarat yang dapat mengubah cara pelaksanaan tersebut akan berlangsung, tetapi dokumen ini menganggap bahwa prasyarat tersebut akan berubah. Keperluan-keperluan ini dicatat di bawah:

- a) Pembangunan Data Center di Kampus 1 diselesaikan (termasuk pemasangan kabel serat yang diperlukan untuk Kampus 1).
- b) Perubahan Kampus 1 Data Centre diselesaikan.
- c) Perencanaan serat antar-bangunan diselesaikan.
- d) Instalasi kabel serat antara Kampus 1 dan Kampus 2 dipasang.
- e) Kabel-kabel serat yang dipasang antara semua bangunan yang relevan dan Data Center.
- f) Kabel-kabel untuk bangunan tipe 'A'.
- g) Lingkungan-lingkungan ditempatkan di semua pusat data. Hal ini meliputi tenaga yang cukup, tempat rak, dan lain-lain.
- h) Topologi logis yang diselesaikan dan ditempatkan.
- i) Model To-Be yang ditempatkan

5.4.2 Tahap-Tahap Migrasi

Tahap 1 (Core Network Services), Tahap 2 (Distribution Networks) dan Tahap 3 (Integrasi Jaringan) akan diselesaikan secara bersamaan, sementara tahap 4 (Pilot) dan tahap 5 (Rollout) harus dilakukan secara berturut-turut setelah tahap 1 sampai tahap 3 diselesaikan. Tahap 6 (WAN) dapat dijadwalkan secara bersamaan dengan tahap 5.

Diagram di bawah menggambarkan tahap-tahap yang berbeda:



Gambar 5.3 Fase Migrasi

5.4.2.1 Tahap 1 (Core Network Services)

Manajemen Jaringan

Tahap pertama migrasi ke jaringan yang baru memerlukan instalasi platform manajemen jaringan CiscoWorks dan susunan fungsi-fungsi antara HP Network Node Manager dan CiscoWorks. Hal ini meliputi konfigurasi perangkat keras dan sistem pengoperasian dan juga instalasi perangkat lunak CiscoWorks pada server-server. CiscoWorks akan menjadi alat yang digunakan oleh tim operasi untuk mengatur semua router dan switch Cisco pada jaringan tersebut. CiscoWorks juga akan menjadi alat untuk menemukan dan mengatasi kesulitan untuk jaringan kampus yang baru.

Keamanan Jaringan

Server ACS Cisco akan disebarkan sebagai bagian dari tahap 1. Keamanan alat jaringan ditangani dari server ini. ACS Cisco menyediakan lapisan-lapisan akses yang aman untuk tim-tim dukungan jaringan, dan juga untuk semua pengguna nirkabel di Campus tersebut.

Jaringan Inti

Selama tahap ini, switch-switch Catalyst 6500 Cisco akan dipasang di tiga pusat data (Kampus 1 dan Kampus 2) dan serat-serat pusat antar-data akan dipasang untuk menghubungkan alat-alat ini ke satu sama lainnya. Modul-modul hubungan yang relevan juga akan dipasang menurut daftar-daftar perbelanjaan. Switch-switch harus diatur menurut model jaringan yang baru dan semua parameter pengalamatan dan konfigurasi TCP/IP akan diatur.

Lapisan Distribusi – Data Center

Switch-switch Catalyst 6500 lapisan distribusi pusat data juga akan dipasang selama tahap ini dan dihubungkan ke switch-switch inti. Switch-switch tersebut akan ditempati sepenuhnya dengan hubungan-hubungan yang relevan untuk penyebaran ke lapisan-lapisan akses. Switch-switch ini harus diatur dengan template-template konfigurasi baru dan komponen-komponen seperti VLAN, Spanning-tree, dll. akan diatur untuk semua konektivitas lapisan akses yang relevan. Hal ini membuat migrasi lapisan akses menjadi kurang kompleks, selama ada komponen-komponen yang lebih sedikit untuk dipikirkan.

Pengujian

Pengujian fungsionalitas perangkat keras dan perangkat lunak yang luas akan dilakukan pada inti dan distribusi selama tahap ini. Unsur-unsur seperti failover antara pusat-pusat data, pembagian beban pada kekuatan, dll. akan diuji dan semua hasilnya didokumentasikan untuk acuan di masa mendatang. Hal ini menjadi bagian sangat penting dari migrasi sebagaimana semua skenario harus diuji sebelum menghubungkan jaringan-jaringan lama dan baru ke satu sama lainnya.

Tim-tim server dan desktop harus dilibatkan selama tahap ini karena mereka harus menyediakan server dan desktop untuk melakukan pengujian aplikasi dan juga menguji fitur-fitur baru yang muncul sebagai bagian dari jaringan baru tersebut. Secara khusus mereka harus menyediakan server uji dan satu atau dua laptop atau desktop.

Semua gangguan IOS juga harus dihilangkan selama tahap ini karena hal itu menjadi lebih sulit untuk melakukan perbaikan-perbaikan IOS setelah pengguna akhir dan server produksi mulai menghubungkan ke peralatan yang baru apabila proses-proses perubahan produksi diikuti kemudian.

Kegagalan-kegagalan perangkat keras juga akan disimulasi selama pengujian ini dengan menghilangkan suplai tenaga, melakukan penempatan online dan pemindahan blade-blade, memindahkan seluruh lapisan inti dan distribusi 6500, dll. Sistem-sistem CiscoWorks dan ACS Cisco juga akan diuji untuk redundansi. Pada tahap ini tidak ada dampak terhadap setiap pengguna produksi selama jaringan yang baru akan berjalan secara terpisah.

5.4.2.2 Tahap 2 (Jaringan Distribusi)

Lapisan Distribusi

Selama tahap ini switch-switch lapisan distribusi di bangunan-bangunan kampus yang jauh akan dipasang dan ini kemudian akan melengkapi konektivitas lapisan distribusi dan inti kampus tersebut. Bangunan-bangunan ini akan menjadi dalam rangkaian berikut:

- 1) Gedung Fak. Sains & Teknologi
- 2) Gedung Kelas Fak. Tarbiyah
- 3) Gedung Ex-Pasca
- 4) Gedung Student Center

Setelah alat-alat ini dipasang, uji redundansi penuh akan dilakukan dan semua hasilnya didokumentasikan. Alat-alat pengatur waktu pengiriman, spanning-tree, waktu *fail-over* HSRP, dll. semuanya akan didokumentasikan dan hasil-hasil ini akan digunakan pada tahap-tahap berikutnya untuk memastikan bahwa baseline tetap konstan.

Lingkungan-lingkungan DHCP dan DNS harus diatur untuk jaringan yang baru pada tahap ini sehingga apabila para pengguna dipindahkan ke jaringan yang baru, mereka akan menggunakan pelayanan-pelayanan DNS dan DHCP yang baru.

Bangunan Lapisan Distribusi Jauh

Di bangunan lapisan distribusi jauh akan dipasang sebuah switch lapisan distribusi Catalyst 3750G-12SS-S Cisco. Tempat-tempat hubungan Gigabit Ethernet mode tersendiri akan digunakan untuk menghubungkan Catalyst 3750 ke Catalyst 6513 lapisan distribusi pusat data. Bangunan-bangunan lapisan akses akan memiliki konektivitas Gigabit Ethernet lewat serat mode khusus ke Catalyst 6513 pusat data dan juga Catalyst 3750 yang ditempatkan di bangunan distribusi jauh. Switch Catalyst 6513 akan menjadi switch distribusi utama dengan Catalyst 3750 yang mengurus redundansi dalam peristiwa outage di pusat data.

WAN & konektivitas Internet

Pusat data Kampus 1 juga akan bertindak sebagai tempat penghentian semua LAN jauh yang dihubungkan ke WAN. Internet dan pihak-pihak ketiga juga akan berakhir di sini. Pilihan untuk memindahkan sebagian dari hubungan-hubungan ini ke pusat data Middle Campus harus dapat diselidiki untuk mengurus redundansi dalam peristiwa outage di pusat data Kampus 1. VLAN yang terpisah akan diciptakan untuk lingkungan-lingkungan WAN dan Internet untuk menciptakan pemisahan lingkungan-lingkungan ini yang logis.

Lapisan Akses – Full Redundancy

Lapisan Akses dari jaringan kampus menyediakan tempat-tempat konektivitas ke alat-alat jaringan pengguna dan alat-alat sekeliling jaringan, yaitu printer jaringan, server jaringan, dan lain-lain.

Model ini menyediakan empat model lapisan akses berikut:

Bangunan Tipe A1 (A2 Untuk Redundansi Terbatas)

Model ini akan menyediakan switch lapisan distribusi hubungan (seri Catalyst 3750) yang akan dipasang di bangunan kampus jauh. Switch Catalyst 3750 akan menghubungkan kembali ke pusat data lewat Gigabit EtherChannel ke switch Catalyst 6513 lapisan inti. Lingkungan ini juga secara khusus akan memiliki tempat server kecil yang akan memuat server-server arsip, dll. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch.

Masing-masing switch akan menjadi subnet (jaringan cadangan) (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana sebagian besar pelayanan terletak di bangunan-bangunan yang sama seperti para pengguna. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

Model di atas juga akan disebarakan di kampus-kampus yang dihubungkan ke WAN selama fungsionalitas lapisan 3 akan diperlukan bagi para pengguna untuk mengakses server di LAN lokal.

Bangunan Tipe B1 (B2 Untuk Redundansi Terbatas)

Model ini akan menyediakan switch agregasi kecil (seri Catalyst 3560) untuk mengakhiri hubungan-hubungan Gigabit Ethernet dari masing-masing switch Catalyst 2960&-24 lapisan akses. Switch Catalyst 3560 akan menghubungkan kembali ke pusat data lewat Gigabit EtherChannel ke switch Catalyst 6513 lapisan distribusi. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch. Masing-masing switch akan menjadi subnet (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada konsentrasi-konsentrasi besar pengguna yang memiliki sebagian besar pelayanan mereka yang diberikan dari pusat data. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

Bangunan Tipe C1 (C2 Untuk Redundansi Terbatas)

Switch-switch lapisan akses Gigabit Ethernet Catalyst 2970G-24 menghubungkan kembali ke switch-switch Catalyst 6513 lapisan distribusi di pusat data melalui tempat-tempat hubungan Gigabit Ethernet. Para pengguna secara khusus dapat menghubungkan secara langsung ke Catalyst 2970 lewat 10/100/1000mb Ethernet. Masing-masing switch akan menjadi subnet (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada keperluan terhadap Gigabit Ethernet ke desktop. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

Bangunan Tipe D1 (D2 Untuk Redundansi Terbatas)

Switch-switch lapisan akses Catalyst 2960G-48 meng-hubungkan kembali ke switch-switch Catalyst 6513 lapisan distribusi di pusat data melalui tempat-tempat hubungan Gigabit Ethernet. Lapisan akses pengguna akan memuat switch-switch Catalyst 2960T-24 yang akan disusun dalam pasangan-pasangan dua switch. Masing-masing switch akan menjadi subnet (VLAN) dan Spanningtree akan digunakan untuk memungkinkan penggunaan infrastruktur tersebut yang optimal. HSRP akan digunakan untuk mengurus ketersediaan yang tinggi dalam peristiwa kegagalan sebuah switch. Model ini akan disebarakan di bangunan-bangunan kampus dimana ada konsentrasi kecil pengguna yang memiliki sebagian besar pelayanannya yang dibeikan dari pusat data. Model ini juga akan disebarakan di jaringan tempat tinggal. Cisco Aironet 1100/1200 Wireless Access Points juga akan disebarakan di lapisan akses untuk mengurangi pengadaan konektivitas jaringan.

Pengujian

Switch-switch baru akan melewati pengujian failover yang teliti seperti yang dilakukan pada tahap satu, tetapi sekarang failover antara masing-masing pusat data juga akan diuji dari perspektif lapisan distribusi yang jauh. Kegagalan-kegagalan perangkat keras juga akan disimulasi selama pengujian-pengujian ini dengan menghentikan suplai tenaga, melakukan penempatan online dan pelepasan blade-blade, mengganti seluruh lapisan inti dan distribusi 6500, dll. Failover HSRP dan juga spanning-tree convergence akan diuji dan didokumentasi-kan.

5.4.2.3 Tahap 3 (Integrasi Jaringan)

Menghubungkan Jaringan-Jaringan Lama dan Baru

Ini merupakan tahap rencana migrasi keseluruhan yang paling kritis karena hal ini adalah dimana jaringan-jaringan kampus yang lama dan baru akan dihubungkan ke satu sama lainnya. Switch Catalyst 6500 di pusat data kampus atas akan menghubungkan ke switch inti Nortel 8600 melalui konektivitas Gigabit EtherChannel. Pada tahap ini ada kesempatan bahwa jaringan yang ada dapat dipengaruhi dan peringatan yang ekstrim harus diikuti apabila membolehkan hubungan-hubungan tersebut. Hal ini akan memungkinkan akses dari kampus-kampus Atas dan Menengah ke jaringan yang baru.

Di pusat data Medical School, Nortel 8610 juga akan menghubungkan ke Catalyst 6500 melewati Gigabit EtherChannel. Bagian penting dari konektivitas ini adalah memastikan tidak ada putaran-putaran pengiriman dan masalah-masalah spanning-tree root bridge yang terjadi selama hal itu dapat membuka secara potensial seluruh jaringan. Tidak ada downtime jaringan yang akan dialami, tetapi sebaiknya menjadwalkan downtime untuk pengujian.

Pengujian

Hal kritis untuk diuji adalah routing antara masing-masing jaringan dan juga bentrokan-bentrokan spanning-tree dan VLAN yang mungkin terjadi. Setelah tahap ini selesai, migrasi pengguna dapat dimulai karena sekarang ada pintu gerbang bagi para pengguna untuk menghubungkan ke aplikasi-aplikasi mereka. Pengujian konektivitas dari jaringan kampus baru ke server-server aplikasi harus dilakukan pada tahap ini untuk menentukan isu-isu konektivitas yang mungkin ada yang harus dipecahkan sebelum memindahkan para pengguna.

5.4.2.4 Tahap 4 (Pilot)

Kelompok Pengguna Pilot

Tahap ini memerlukan pentargetan sekelompok pengguna kecil (kira-kira 20-30 pengguna) yang dapat dipindahkan ke lingkungan baru. Langkah pertamanya adalah mengidentifikasi lokasi fisik dari switch lapisan aksesnya sekarang ini dan memastikan bahwa lingkungan-lingkungan tersebut cukup untuk instalasi peralatan yang baru. Setelah hal ini dilakukan, switch-switch lapisan akses dapat dipasang di kloset pemasangan kabel. Migrasi pengguna ke jaringan yang baru sekarang berlangsung dan DHCP, DNS, dan lain-lain diubah.

Ini adalah dimana kerjasama tim antara tim-tim jaringan, server dan desktop menjadi paling penting. Jika pengguna telah memiliki alamat TCP/IP

statis yang diatur, hal ini harus dapat diubah. Terlepas dari ini, harus tidak ada perubahan pada stasiun kerja kecuali konfigurasi statis kartu jaringan tersebut ke duplex penuh 100Mbps.

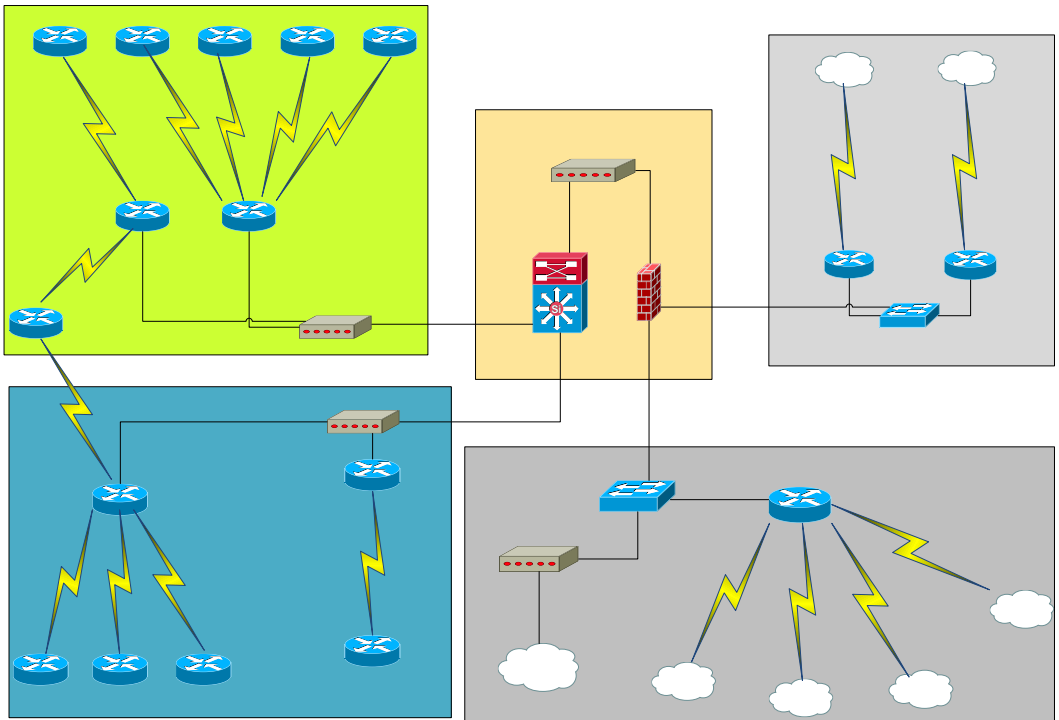
Setelah dipindahkan, para pengguna ini harus diperlakukan seperti emas karena mereka akan memberikan input yang sangat berharga kepada kekurangan-kekurangan pelaksanaan yang mungkin ada dan juga pelaksanaan aplikasi. Tim-tim helpdesk harus menciptakan profil terpisah pada sistem-sistem mereka dan memperluas dengan cepat panggilan-panggilan dari para pengguna ini ke insinyur-insinyur dukungan dan tim perencanaan. Panggilan-panggilan ini kemudian dapat digunakan sebagai bahan acuan untuk membangun para pengguna lebih lanjut. Hal ini akan membantu tim instalasi memecahkan masalah-masalah dengan cepat dan secara efisien. Pilot tersebut harus berjalan selama sekurang-kurangnya 2 minggu.

5.4.2.5 Tahap 5 (Rollout)

Migrasi Pengguna

Setelah tahap 4 diselesaikan, migrasi pengguna sisanya dan juga migrasi server dapat dimulai. Para pengguna harus dipindahkan dalam kelompok-kelompok fungsional. Kelompok fungsional adalah komunitas pengguna yang menggunakan pelayanan yang sama (misalnya file server). Segera setelah kira-kira 60 sampai 70 persen pengguna dipindahkan, server-server yang diakses oleh para pengguna ini akan dipindahkan untuk mengurangi beban lalu lintas pada konektivitas antara dua jaringan tersebut. Hal ini menjadi sangat penting dilakukan selama anda tidak menginginkan para pengguna mengakses server-server mereka pada jaringan yang lama sementara server-server tersebut dihubungkan ke jaringan yang baru karena hal itu akan mempengaruhi kecepatan akses mereka ke server-server ini.

5.4.2.6 Tahap 6 (Remote Campus)



Gambar 5.4 Migrasi Remote Campus

Router WAN dan Firewall

Router WAN dan lingkungan firewall akan dipindahkan selama tahap ini. Migrasi firewall akan berlangsung segera setelah kira-kira 50% dari seluruh kampus tersebut dipindahkan.

Lingkungan WAN dapat dibuat segera setelah infrastruktur tersebut berpindah tempat router-router sudah ada di tempat. Router-router Cisco akan dihubungkan ke switch-switch Catalyst 6500 dan semua mekanisme keamanan dan QOS yang relevan akan diatur pada alat-alat ini. Protokol-protokol pengiriman pada WAN juga akan dimasukkan kedalam model yang baru tersebut, dan OSPF akan menggantikan RIPv2 yang ada saat ini.

Perpindahan WAN hanya memerlukan pemindahan router-router pusat data dan tidak memperhitungkan LAN yang jauh. Tahap ini akan menjadi tahap yang lebih mudah untuk dilakukan selama tim-tim instalasi akan mengatasi semua masalah yang mungkin ada pada jaringan tersebut dan migrasi para pengguna tidak akan memerlukan waktu yang lama untuk diselesaikan. Pada tahap ini tempat-tempat berikut telah diidentifikasi sebagai kampus-kampus yang dihubungkan ke WAN.

Langkah pertama adalah memastikan bahwa lingkungan-lingkungan tersebut sudah ada di tempat untuk menyelesaikan migrasi. Tenaga, tempat rak, pengaturan suhu udara, dan lain-lain harus disediakan sebelum peralatan yang baru dipasang. Langkah berikutnya adalah instalasi peralatan baru sejajar dengan peralatan lama dan kemudian menyelesaikan migrasi para pengguna lewat ke jaringan yang baru. Setelah para pengguna dipindahkan, peralatan lama tersebut dapat dipindahkan.

5.5 Integrasi Bisnis

Bagian merupakan hasil dari input-input ke “To-Be” Network Design dari wakil-wakil fakultas dan departemen, terutama anggota-anggota PTIPD.

5.5.1 Proses yang Diikuti

Tim blueprint meminta pertemuan-pertemuan dengan semua wakil PTIPD dan meminta mereka untuk mengundang wakil-wakil fakultas atau departemen yang tertarik lainnya ke sebuah pertemuan dimana “To-Be Design” yang diusulkan diperkenalkan. Wakil-wakil tersebut diberi kesempatan untuk mengomentari dan menanyakan aspek-aspek dari model tersebut. Lampiran A mencatat mereka yang menghadiri pertemuan-pertemuan singkat tersebut.

Network Requirements Questionnaire telah dikembangkan untuk membantu wakil-wakil ICT menilai keperluan-keperluan jaringan mereka bersama dengan tim model. Mereka diminta mengisi angket tersebut dan mengembalikannya ke tim model. Angket ini dimaksudkan untuk mengumpulkan informasi tentang keperluan-keperluan jaringan khusus yang melebihi tingkat dasar pelayanan yang diberikan oleh model jaringan “To-Be”.

5.5.2 Keperluan Jaringan Wireless

Anggaran belanja memungkinkan untuk instalasi tiga puluh satu tempat akses nirkabel. Tempat-tempat akses ini didasarkan pada keperluan-keperluan yang diterima dari fakultas-fakultas dan pada informasi yang diterima dari Properties and Services dan yang lainnya telah daerah-daerah akses terbuka yang cocok untuk jaringan nirkabel.

Tanggapan-tanggapan kepada bagian jaringan nirkabel dari angket tersebut diringkaskan pada tabel yang menyusul.

Di samping keperluan-keperluan yang diutarakan oleh fakultas, tempat-tempat ramai nirkabel akan dipasang di lokasi-lokasi berikut:

- 1) Area Kampus 1:
 - a) Area Gd. Fakultas Adab & Humaniora,

- b) Area Gd. Fakultas Dakwah & Komunikasi,
 - c) Area Gd. Fakultas Psikologi,
 - d) Area Gd. Fakultas Ilmu Sosial & Ilmu Politik,
 - e) Area Gd. Fakultas Sains & Teknologi,
 - f) Area Gd. Fakultas Syariah & Hukum,
 - g) Area Gd. Fakultas Tarbiyah & Pendidikan,
 - h) Area Gd. Fakultas Ushuluddin,
 - i) Area Gd. Al-Jamiah
 - j) Area Gd. Aula
 - k) Area Kantin
 - l) Area Gazebo
- 2) Area Kampus 2:
- a) Area Gd. Pendidikan

5.6 Teknologi Masa Depan

Fokus khusus dari pembaharuan jaringan ini adalah untuk menjamin teknologi masa depan yang diramalkan dapat dimasukkan setelah teknologi tersebut menjadi dapat berjalan. Teknologi yang paling relevan telah dipertimbangkan dan jaringan UINSGD yang diusulkan telah dinilai dalam memproyeksikan perubahan-perubahan yang akan diperlukan setelah teknologi masa depan tersebut dilaksanakan. Pandangan-pandangan tentang keuntungan-keuntungan bisnis dan teknis yang mungkin ada juga diberikan. Bagian berikut menyoroiti teknologi masa depan yang dipertimbangkan ini.

5.6.1 Telephony

5.6.1.1 Tinjauan Umum

Ada sedikit hal yang membingungkan tentang istilah-istilah voice over IP (VoIP) dan IP telephony pada waktu sekarang ini sebagaimana orang-orang cenderung akan membingungkan satu dengan yang lainnya. Dokumen ini akan menggambarkan dua teknologi dan juga kemungkinan-kemungkinan penyebarannya di Campus LAN baru yang diusulkan.

VOIP adalah teknologi yang memungkinkan pengiriman sinyal suara analog tradisional melewati sebuah jaringan IP. Cara konektivitas ini bekerja adalah melalui menghubungkan PABX anda yang ada ke sebuah voice enable router Cisco. Router ini menangani konversi sinyal analog menjadi sinyal digital dan mengirimkan paket suara tersebut melewati sebuah backbone (kekuatan) IP. Untuk melakukan VOIP pelanggan akan membutuhkan voice enabled routers dan juga modul-modul relevan yang mendukung fitur-fitur suara seperti FXS (port telepon analog) dan port-port FXO (PSTN / PABX). Quality of Service (QOS) juga harus dapat disebarkan pada WAN untuk

memberikan prioritas kepada lalu lintas suara karena jenis lalu lintas ini peka kepada kelambatan.

IP telephony adalah teknologi dimana pelanggan menggantikan handset telepon tradisional mereka dengan telepon IP. Pelaksanaan Cisco Call Manager juga diperlukan untuk memberikan fungsionalitas PABX kepada telepon-telepon ini. Pengaruh-pengaruh IP telephony pada Cisco beralih untuk memberikan satu tempat konektivitas nbagi sebuah telepon dan hubungan stasiun kerja. Telepon-telepon IP Cisco muncul dalam model-model berbeda dan juga dapat menyediakan konektivitas nirkabel.

5.6.1.2 Keuntungan Teknis

Keuntungan teknis dari menyebarkan teknologi-teknologi di atas adalah sangat besar karena hal itu memungkinkan pelanggan memperoleh satu jaringan untuk suara, data dan video. Pelanggan dapat menggunakan perangkat keras yang sama untuk mengirimkan sinyal-sinyal ini. Staf teknis yang sama yang mendukung jaringan-jaringan data sekarang dapat mendukung jaringan suara selama teknologi-teknologi dan perangkat keras yang sama digunakan. Hal ini menurunkan biaya dukungan dan pelatihan untuk sumber-sumber teknis dan juga berarti lebih sedikit orang dibutuhkan untuk mendukung jaringan-jaringan data dan telepon.

Manajemen jaringan-jaringan suara dan data terpusat membuat lebih mudah untuk mencapai tingkat-tingkat pelayanan dan mengurus ketesediaan yang tinggi. Komunikasi pengguna akhir yang bertambah baik dicapai melalui penyebaran aplikasi-aplikasi suara yang benar, misalnya pengiriman pesan dan fitur-fitur mobilitas, integrasi desktop yang tinggi.

5.6.1.3 Keuntungan Bisnis

Keuntungan bisnis dari menyebarkan solusi IP telephony dan VOIP direalisasikan hanya setelah beberapa tahun setelah biaya-biaya susunan pertama menjadi sangat tinggi. Keuntungan-keuntungan jangka panjangnya adalah hal-hal seperti memungkinkan jaringan untuk memberikan teknologi-teknologi konvergensi kepada bisnis tersebut untuk memperbaiki keefektifan staf dalam menghadapi para pelanggan. Di sebuah lembaga pendidikan keuntungan-keuntungan tersebut meliputi kemungkinan untuk memberikan pembelajaran jarak jauh dan juga pembelajaran elektronik.

Keuntungan-keuntungan bisnis utamanya adalah pengurangan biaya panggilan yang dapat direalisasikan dengan menggunakan fitur-fitur seperti toll bypass, penghematan biaya dukungan dan manajemen direalisasikan dengan memiliki satu tim dukungan untuk mengatur dan mendukung jaringan data dan telepon.

5.6.1.4 Kebutuhan Implementasi (Lapisan Jaringan)

Untuk menyebarkan VOIP seorang pelanggan akan membutuhkan voice enabled routers pada WAN yang juga dapat mendukung QOS. Voice enabled routers harus dapat dipasang untuk memungkinkan konversi dari analog ke digital. Router-router tersebut akan membutuhkan port-port FXS untuk menghubungkan telepon-telepon analog ke router dan port-port FXO untuk menyediakan konektivitas ke jaringan PSTN atau PABX yang ada. PABX juga akan menghubungkan ke router melalui hubungan E1.

Untuk menyebarkan IP telephony seorang pelanggan harus dapat memasang sekelompok Cisco Call Manager di lokasi pusat. Call Manager memberikan fungsionalitas PABX pada sebuah jaringan IP telephony. Telepon-telepon IP harus dapat disebarkan pada setiap saat dimana sebuah telepon akan diperlukan. Ada banyak handset di pasar dan jenis yang dipilih akan bergantung pada keperluan-keperluan bisnis. Beberapa telepon memiliki switch-switch terpasang tetap yang mengurangi perlunya memiliki kabel untuk sebuah stasiun kerja dan stasiun kerja terpisah untuk telepon.

Switch-switch lapisan akses baru yang akan dipasang pada jaringan to-be tidak akan mendukung power over Ethernet (PoE) selama keperluan-keperluan yang tepat untuk IP Telephony tidak pernah ditentukan. Hal ini berarti bahwa UINSGD akan memiliki dua pilihan yang ada apabila melihat penyebaran IP Telephony di lingkungan kampus. Pilihan satu akan berupa membeli telepon IP dengan suplai tenaga tambahan dan pilihan dua akan memerlukan mengganti switch non-PoE dengan switch PoE yang cakap. Hal ini akan menjadi bagian dari tahap perancangan IP Telephony dan akan memerlukan dibuatnya daftar perbelanjaan yang lengkap dan membandingkan pilihan-pilihan tersebut.

5.6.2 IPv6

5.6.2.1 Tinjauan Umum

Ruang alamat IPv4 yang ada sekarang ini memungkinkan untuk memenuhi kebutuhan yang semakin meningkat akan alat-alat yang dihubungkan ke jaringan. Mobilitas telah menjadi salah satu urusan utama setelah tipologi IPv4 yang ada sekarang ini diangkat dari skema-skema pengalamatan regional, yang membuat administrasi pengguna ini menjadi tugas yang sulit. Pertumbuhan Internet yang terus-menerus memerlukan diperkenalkannya IPv6 sebagai mekanisme pengalamatan logis untuk melayani pertumbuhan di masa depan. IPv6 memerlukan empat alamat IPv4 32 bit sekarang ini untuk menyediakan skema pengalamatan 128 bit. Keberhasilan dari IPv6 akan ditentukan oleh aplikasi-aplikasi yang dapat dijalankan pada sebuah jaringan IPv6.

Network address translation (NAT) telah disebarakan untuk menjawab kekurangan alamat IPv4, tetapi hal ini memiliki beberapa kekurangan teknis penting yang digambarkan pada RFC 2775 Internet Transparency dan juga RFC 2993 Architectural Implications dari NAT. IPv6 dimaksudkan untuk memenuhi keperluan-keperluan pengguna dan aplikasi untuk kembali ke suatu lingkungan yang lebih sederhana dimana operasi jaringan tersebut menjadi transparan untuk aplikasi-aplikasi.

5.6.2.2 Keuntungan Teknis

IPv6 memberikan keuntungan-keuntungan teknis berikut kepada sebuah organisasi:

- a) IPv6 memperkenalkan kembali keamanan dan kualitas pelayanan (QoS) dari akhir ke akhir yang tidak selalu tersedia dengan cepat di sebuah jaringan berbasis NAT.
- b) Ruang alamat yang lebih besar untuk kemampuan jangkauan dan kemampuan skala global.
- c) Header yang disederhanakan untuk efisiensi dan kemampuan pengiriman.
- d) Hirarki dan kebijakan-kebijakan untuk fleksibilitas arsitektur jaringan.
- e) Dukungan yang efisien untuk pengiriman dan agregasi rute.
- f) Konfigurasi otomatis, penomoran kembali yang lebih mudah, penampungan banyak, dan dukungan plug dan play yang bertambah baik.
- g) Keamanan dengan dukungan IP Security (IPSec) wajib untuk semua alat IPv6.
- h) Dukungan yang bertambah baik untuk Mobile IP dan alat-alat penghitung aktif.
- i) Dukungan multicast yang tinggi dengan alamat-alamat yang meningkat dan mekanisme-mekanisme yang efisien.
- j) NAT tidak perlu didukung atau diatur.

5.6.2.3 Keuntungan Bisnis

Konfigurasi otomatis, alamat-alamat dan mobilitas tanpa batas merupakan beberapa keuntungan utama untuk sebuah organisasi karena hal itu mempercepat pengiriman pelayanan-pelayanan IT untuk memungkinkan bisnis mengurangi waktu ke pasar tawaran-tawaran produk mereka secara signifikan. Selama teknologi berkembang dan semakin banyak perusahaan IT menyelidiki keuntungan-keuntungan teknis dari IPv6, aplikasi-aplikasi menjadi ditulis untuk mendukung dan mengeksploitasi keuntungan-keuntungan teknis baru ini.

IPv6 akan menjadi sebuah kekuatan penggerak yang besar di dunia media dan pembelajaran elektronik di masa depan karena masing-masing tempat tujuan di dunia akan memiliki alamat IPv6 yang unik dan ini akan membuat konektivitas dari tempat ke tempat menjadi lebih mudah disebarakan. Microsoft dan pesaing-pesaingnya telah melihat bahwa masa depan terletak pada IPv6

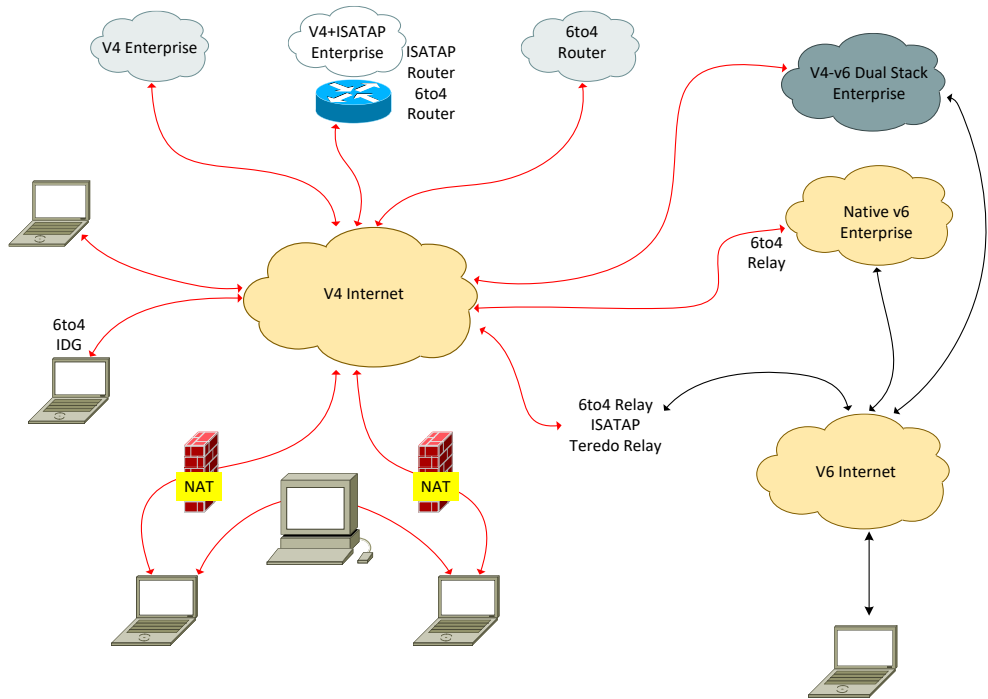
dan sedang melakukan banyak pengembangan pada produk-produk mereka untuk mendukung IPv6. Hal ini berarti bahwa di masa depan aplikasi-aplikasi IPv6 yang siap akan dipercepat selama kebutuhan meningkat untuk menyebarkan jaringan-jaringan IPv6.

Migrasi masa depan ke IPv6 akan diperhitungkan apabila menyebarkan jaringan-jaringan baru karena adanya sejumlah fitur IPv6 yang tersedia sekarang ini dan jika sebuah organisasi bermaksud menggunakan aplikasi-aplikasi ini, jaringan baru tersebut harus mendukung IPv6. Perusahaan-perusahaan tidak ingin melakukan penambahan jaringan mereka beberapa tahun hanya untuk mendukung IPv6.

Walaupun adopsi besar-besaran IPv6 menurun beberapa tahun, namun organisasi-organisasi dapat memulai sekarang ini untuk mengambil langkah-langkah kecil dan menjadi akrab dengan IPv6. Proses ini telah disederhanakan melalui teknologi-teknologi transisi berikut yang telah dibangun oleh sebagian besar perusahaan peralatan ke dalam produk-produk mereka:

- a) 6to4 untuk PC dan access routers yang memiliki sekurang-kurangnya satu alamat IPv4 umum. 6to4 diatur secara khusus oleh perusahaan-perusahaan dan menyediakan saluran lalu lintas IPv6 melewati Internet terbuka. 6to4 dimasukkan dengan Windows Server 2003, Windows XP SP1 dan XP SP2, dan pelepasan-pelepasan Cisco IOS® Software.
- b) Teredo untuk PC dan alat-alat yang memiliki alamat-alamat IP pribadi, terutama di rumah. Teredo adalah teknologi pelintasan NAT yang menyediakan saluran antara dua host apabila yang satu berada di belakang NAT IPv4, dan juga digunakan pada Internet terbuka. Microsoft memasukkan dukungan Teredo kedalam The Advanced Networking Pack, sebuah tambahan gratis untuk Windows XP SP1, dan digabungkan ke Windows XP SP2.
- c) ISATAP adalah solusi perusahaan untuk jaringan-jaringan kampus yang menyalurkan paket-paket IPv6 melewati sebuah intranet, memungkinkan penyebaran alat-alat IPv6 yang lancar bahkan apabila pelepasan-pelepasan server 2003, XP SP1 dan XP SP2, dan Cisco IOS meliputi ISATAP dan dapat saling beroperasi sepenuhnya.

Untuk memungkinkan konektivitas melewati Internet IPv6 untuk pengguna di atas, banyak pemberi pelayanan telah menyebarkan relay dan router 6to4, dan server dan relay Teredo ke jaringan-jaringan mereka. Menyebarkan teknologi-teknologi transisi merupakan cara yang murah dan cepat untuk memperoleh pengalaman beroperasi dengan IPv6 dan memungkinkan aplikasi-aplikasi IPv6 dengan gangguan minimal pada jaringan yang ada.



Gambar 5.5 Migrasi IPv6

Langkah-langkah keamanan jaringan pada jaringan UINSGD dimaksudkan terutama untuk:

- a) Melindungi jaringan dari virus dan lalu lintas yang mengganggu lainnya dari Internet.
- b) Mengontrol akses ke dan dari tempat tinggal.
- c) Memaksa jenis-jenis lalu lintas tertentu (HTTP, FTP dan SMTP) melalui proxy untuk tujuan-tujuan manajemen keamanan dan bandwidth.

Kebijakan yang berlaku untuk sebagian besar firewall merupakan kebijakan yang terbuka. Otentikasi merupakan mekanisme keamanan utama yang digunakan dalam jaringan tersebut.

Semua lalu lintas ke dan dari Internet melewati firewall pusat UINSGD, sebuah server FreeBSD yang menjalankan IPFW firewalling suite. Berbagai pihak ketiga dihubungkan dengan jaringan pada Kampus 1 dan pada Medical School lewat Ethernet atau Diginet untuk memberikan akses yang disediakan ke berbagai pelayanan dan saluran dukungan. Jaringan-jaringan pihak ketiga ini sebagian besar dihubungkan ke jaringan UINSGD di belakang firewall di Kampus 1 dan Medical School.

Sebuah metodologi yang sangat terjamin disahkan oleh Cisco telah diikuti untuk menciptakan model jaringan kampus UINSGD yang baru. Sebagai bagian integral dari metodologi tersebut, lalu lintas jaringan kampus sekarang ini, keperluan-keperluan bisnis dan kemungkinan-kemungkinan

teknologi masa depan telah dinilai dalam menghasilkan sebuah model jaringan yang akan melayani kebutuhan-kebutuhan sekarang ini dan yang akan mampu mengukur untuk mengakomodasi kebutuhan-kebutuhan masa depan yang diramalkan.

Jaringan kampus baru yang diusulkan di UINSGD akan dibangun sesuai dengan jaringan kampus praktik terbaik, terdiri dari kekuatan kecepatan tinggi (Inti), daerah-daerah konsentrasi (Distribusi) dan tempat-tempat hubungan pengguna (Akses).

Campur Core akan dibentuk antara Kampus 1 dan Kampus 2. Switch-switch Catalyst 6513 Cisco akan digunakan sebagai perangkat keras untuk memperlengkapi kekuatan lapisan 3. Tiga bangunan Campus tersebut akan dihubungkan ke satu sama lain lewat satu serat mode (1000Base LX) seperti yang dapat dilihat dibawah.

Kecepatan hubungan pertama pada inti akan menjadi 1 Gbps meskipun 10Gbps akan didukung jika timbul kebutuhan untuk meningkatkan. Gigabit Ethernet Trunk tambahan akan dilaksanakan untuk memperlengkapi kekuatan lapisan 2 untuk jaringan tempat tinggal. Hal ini akan memungkinkan UINSGD memisahkan secara fisik dan juga secara logis jaringan tempat tinggal tersebut dari jaringan kampus LAN.

Redundansi fisik akan disediakan lewat hubungan-hubungan Gigabit EtherChannel antara masing-masing blok Inti. Sekumpulan EtherChannel merupakan sekelompok hingga delapan hubungan Fast atau Gigabit Ethernet. Kumpulan tersebut berfungsi sebagai hubungan tersendiri atau logis antara switch-switch dan router-router. EtherChannel adalah tepat karena ia mengukur bandwidth tanpa menambah kepada kerumitan model tersebut. Spanning-Tree Protocol memperlakukan kumpulan EtherChannel sebagai hubungan tersendiri, jadi tidak ada putaran-putaran spanning-tree yang diperkenalkan. Protokol-protokol pengiriman juga memperlakukan kumpulan EtherChannel sebagai hubungan tersendiri atau diarahkan jalannya dengan alamat IP umum, jadi tidak ada jaringan-jaringan cadangan atau pengganti IP tambahan yang diperlukan, dan tidak ada hubungan-hubungan pengamatan router tambahan yang diciptakan. Menjaga keseimbangan beban ditangani oleh perangkat keras hubungan tersebut.

Di sisi perangkat keras switch, dua mesin Supervisor 720 dan juga dua persediaan tenaga akan dipasang pada masing-masing switch Catalyst 6531. Hal ini akan menciptakan solusi dengan redundansi yang signifikan menggunakan satu casing perangkat keras. Dengan menggunakan mesin Supervisor 720 tersebut 2 lobang atau tempat tambahan disediakan untuk penggunaan kartu-kartu garis. Mesin Supervisor yang kedua akan diatur untuk hot standby untuk mengambil alih dengan segera dalam peristiwa kegagalan

pada mesin Supervisor utama. Hal ini juga akan memungkinkan UINSGD meningkatkan IOS pada satu mesin Supervisor dan memiliki kemampuan untuk menurunkan kembali dengan segera dalam peristiwa masalah dengan IOS.

OSPF akan digunakan sebagai protocol pengiriman pilihan pada inti tersebut. Masing-masing blok inti akan disediakan sejumlah jaringan cadangan IP dan jumlah jaringan cadangan ini akan dibagi lagi menjadi jaringan-jaringan cadangan yang lebih kecil dan dialokasikan ke bangunan-bangunan berbeda yang berhubungan dengan inti tersebut. Hanya rute-rute singkat yang akan ditekankan pada kekuatan tersebut untuk membatasi pembaharuan-pembaharuan pengiriman yang tak perlu yang disebarakan melewati jaringan tersebut.

Serat fisik yang sama yang digunakan untuk konektivitas antara pusat-pusat data Upper dan Middle Campus akan digunakan untuk memperlengkapi konektivitas fisik jaringan daerah penyimpanan (SAN). Serat tersebut akan memiliki jalan-jalan pengganti untuk mengurus redundansi.

- a) Kampus-kampus akan dilayani oleh sebuah infra-struktur jaringan berswitch sepenuhnya yang akan diurus secara sentral. Sebuah jaringan berswitch akan mengurus kinerja dan hasil yang meningkat dengan memberikan hubungan 100Mbps ke switch tersebut kepada masing-masing pengguna.
- b) Tiga blok bangunan utama dari jaringan tersebut akan menjadi lapisan-lapisan Inti, Distribusi dan Akses. Stasiun-stasiun kerja pengguna menghubungkan ke sebuah switch lapisan Akses yang pada gilirannya menghubungkan ke switch lapisan Distribusi yang bertindak sebagai tempat agregasi. Lapisan Inti mengurus konektivitas antara pusat-pusat data yang berbeda.
- c) Inti (lihat diagram di bawah) akan dibentuk antara Kampus 1 (bangunan Computer Science), Middle Campus (bangunan Bremner) dan Medical School (Werner Beit North). Kecepatan konektivitas antara lokasi-lokasi ini sekarang adalah 100Mbps dan akan menjadi 1Gbps di masa yang akan datang, dengan kemampuan meningkatkan konektivitas ini hingga 100Mbps apabila diperlukan (tetapi dengan biaya tambahan). Lokasi-lokasi ini juga akan menampung pusat-pusat data untuk masa depan. Infrastruktur jaringan pusat tersebut akan mengurus konektivitas Gigabit Ethernet untuk mengakomodasi lingkungan server.
- d) Kecepatan akses jaringan yang lebih besar untuk server dan stasiun kerja pengguna akan dicapai pada jaringan yang baru dan tingkat redundansinya akan disediakan guna memungkinkan para pengguna mengakses pelayanan yang sangat diperlukan oleh mereka bahkan dalam peristiwa *outage* pusat data.

- e) Pemeliharaan akan ditingkatkan secara besar-besaran dengan penyebaran sekumpulan produk oleh satu penjual.
- f) Ketentuan telah dibuat untuk tempat-tempat ramai nirkabel (kira-kira 30) di semua kampus. Hotspot ini akan memungkinkan para pengguna menghubungkan melalui teknologi nirkabel ke jaringan.

Empat model lapisan akses telah direncanakan dan masing-masing bangunan telah dialokasikan untuk sebuah model berdasarkan kriteria tertentu. Alasan di belakang empat model tersebut adalah bahwa komunitas pengguna per bangunan berbeda dan ini berarti bahwa di beberapa bangunan banyak switch jaringan akan dipasang, sementara bangunan-bangunan lainnya secara khusus akan memerlukan hanya satu atau dua switch. Keperluan-keperluan hubungan serat antara bangunan-bangunan juga telah dipertimbangkan. Strategi-strategi operasi bersama V4/V6 dan banyak teknologi transisi sekarang dimasukkan kedalam produk-produk vendor untuk memungkinkan migrasi ke IPv6, termasuk ISATAP, Teredo dan 6to4. Migrasi sederhana sebenarnya dapat dimulai sekarang ini pada keunggulan jaringan tanpa memerlukan perbaikan-perbaikan infra-struktur yang mahal. Diagram di bawah menggambarkan tinjauan migrasi.

5.6.2.4 Kebutuhan Implementasi (Lapisan Jaringan)

Jaringan UINSGD to-be akan mendukung IPv6 sebagai protokol angkutan. Peralatan Cisco yang dipasang akan mendukung IPv6. Susunan-susunan IPv6 dimasukkan sekarang ini kedalam router-router inti Cisco berikut: rangkaian CRS-1, 12000, dan 7600, dan switch-switch Lapisan 3, termasuk rangkaian Catalyst 6500, 4500, dan 3750.

Tabel berikut menggambarkan platform-platform lapisan 3 Cisco yang relevan untuk model to-be yang mendukung IPv6.

Tabel 5.8 Perangkat Mendukung IPv6

Produk	Status IPv6	Support IPv6	Keterangan
Cisco 1700 Series	Sekarang	--	
Cisco Catalyst 4500 Series	Sekarang	Ya	Dengan Sup720 dan 720-3BXL
Cisco Catalyst 4500 Series	Sekarang	Ya	HW FW pada CY05 terakhir
Cisco Catalyst 3750 Series	Sekarang	Ya	Tersedianya perangkat lunak yang diatur pada CY05

5.6.2.5 Switch-Switch Layer 2

Pengiriman lalu lintas IPv6 tidak mempengaruhi switch-switch LAN Layer 2, karena alat-alat ini tidak perlu melihat header Layer 3 untuk mengirimkan kerangka IPv6, dengan demikian host IPv6 dapat diberikan secara transparan ke produk-produk Cisco berikut:

- a) Cisco Catalyst 2900XL Series Switch
- b) Cisco Catalyst 3500XL Series Switch
- c) Cisco Catalyst 4000 Series Switch
- d) Cisco Catalyst 6000 Series Switch

Di masa depan, produk-produk baru dapat menggabungkan fitur-fitur IPv6 yang diresmikan seperti kemampuan manajemen jaringan IPv6 asli dan MLD snooping.

Tabel berikut menggambarkan pelepasan IOS minimum untuk fitur diinginkan yang diperlukan.

5.6.3 Content Networking

5.6.3.1 Tinjauan Umum

Memberikan informasi yang dapat dipercaya dan cepat kepada siswa-siswa merupakan salah satu pendorong utama menyebarkan solusi jaringan isi dalam fasilitas-fasilitas pendidikan sekarang ini. Solusi tersebut memungkinkan siswa-siswa untuk mengakses isi dari manapun dan pada setiap saat. Jaringan isi dimaksudkan untuk menyediakan kemampuan aplikasi yang tinggi, keamanan jaringan yang meningkat, jaminan-jaminan jaringan dan pribadi yang berkurang dan juga akses yang lebih cepat ke aplikasi-aplikasi.

Gerakan ke aplikasi-aplikasi berbasis browser telah memperkenalkan perlunya membawa isi ke para pengguna dengan kecepatan yang jauh lebih cepat dan dengan kualitas yang luar biasa. Ini adalah dimana jaringan isi mengirimkan isi yang cepat atau aman kepada para poengguna sambil mengirimkan TCO dengan menghapuskan duplikasi infrastruktur-infrastruktur dukungan dan manajemen.

Solusi Cisco terbaru yang disebut Cisco Application and Content Networking (CAN) juga memungkinkan lembaga-lembaga membawa pelayanan-pelayanan pengiriman isi ke lokasi-lokasi kantor yang jauh.

5.6.3.2 Keuntungan teknis

Ada banyak keuntungan teknis untuk menyebarkan solusi content delivery network (CDN). Faktor utama yang mempengaruhi kemampuan jaringan sekarang ini sebagai akibat dari semua isi yang dialirkan melewati jaringan-jaringan adalah kemacetan dan pengeluaran bandwidth. Dengan melaksanakan solusi CDN, lembaga-lembaga pendidikan merealisasikan pengurangan kemacetan jaringan dan pengeluaran bandwidth.

Serangan-serangan virus dan kode virus yang sangat merugikan menyebabkan downtimes di banyak jaringan sekarang ini dan ini adalah dimana solusi-solusi CDN memberikan perlindungan terhadap jenis-jenis kejadian ini. CDN juga melindungi data kritis misi dari pengacau-pengacau luar.

Waktu-waktu reaksi aplikasi selalu menjadi urusan untuk setiap tim jaringan karena hal ini mempunyai dampak langsung terhadap persepsi pengguna tentang pengiriman jaringan. CDN memperbaiki waktu-waktu reaksi aplikasi secara dramatis dengan menyembunyikan isi lebih dekat ke sisi pengguna dan dengan demikian juga memperbaiki produktivitas setelah para pengguna memperoleh akses lebih cepat ke informasi. Sejumlah besar pengguna juga dapat didukung apabila permintaan-permintaan dikeluarkan dari server semula.

Arsitektur Cisco Content Engine adalah redundan sepenuhnya dan dapat diukur, dengan demikian memberikan dua unsur sangat penting di setiap lingkungan dengan jaringan. Redundansi selalu menjadi unsur yang sangat penting di setiap jaringan dimana pengiriman informasi menjadi prioritas paling tinggi seperti di fasilitas-fasilitas pendidikan.

5.6.3.3 Keuntungan Bisnis

CDN memberikan banyak keuntungan kepada bisnis dan khususnya kepada lembaga-lembaga pendidikan. Pengiriman isi ke siswa-siswa merupakan semua apa tentang pendidikan, tetapi penghematan biaya infrastruktur harus menjadi bagian dari persamaan tersebut.

Penghematan biaya infrastruktur IT direalisasikan dengan cara berikut:

- a) Biaya bandwidth dikurangi secara signifikan.
- b) Optimisasi infrastruktur server dapat dilakukan dan ini membawa penghematan-penghematan biaya perangkat keras, perangkat lunak, dan perizinan kedalam kerangka tersebut.
- c) Lingkungan dukungan dan pemeliharaan terpusat mengurangi biaya staf secara signifikan.

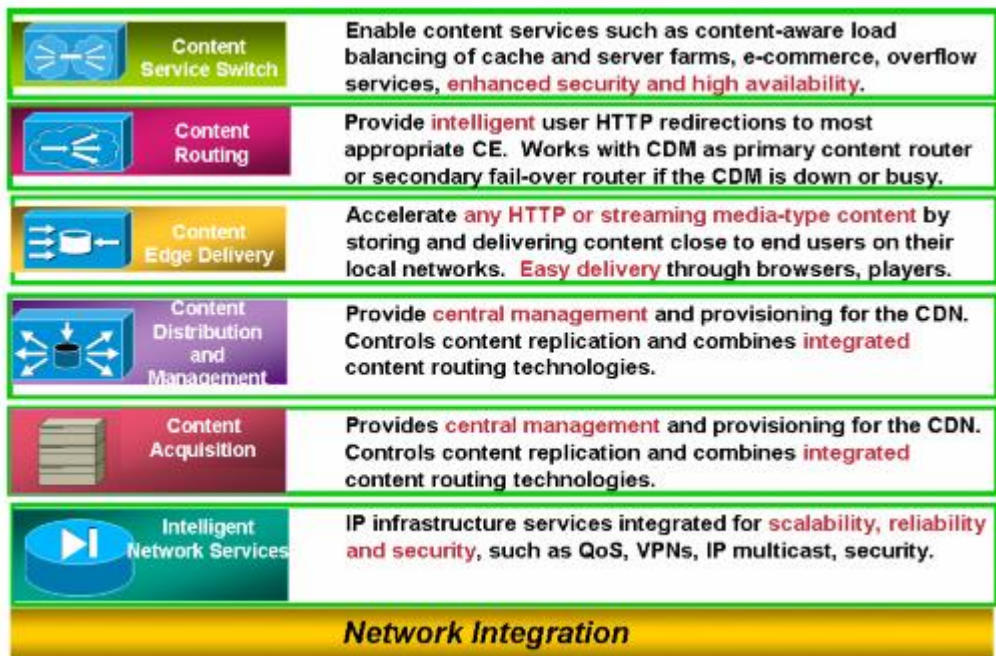
Dengan melaksanakan solusi CDN sebuah lembaga pendidikan dapat memberikan pelayanan yang dapat diandalkan, bergantian, dapat dipercaya dan berkualitas kepada siswa-siswa mereka. Ini merupakan pernyataan yang sangat penting karena ini meliputi semua keperluan yang dibutuhkan oleh siswa-siswa dan dosen-dosen untuk menyampaikan tugas sehari-hari mereka yaitu belajar.

Dalam memberikan semuanya di atas, Universitas diuntungkan dengan meningkatnya pendapatan yang dihasilkan dalam memberikan fasilitas-fasilitas pendidikan yang unggul kepada siswa-siswa mereka. Universitas

tersebut juga sekarang telah memiliki sebuah mekanisme untuk memberikan pembelajaran kepada spektrum orang-orang yang lebih luas.

5.6.3.4 Kebutuhan Implementasi (Lapisan Jaringan)

Infrastruktur yang diusulkan untuk jaringan UINSGD to-be mendukung multicasting, yang menjadi salah satu protokol pengangkutan penting yang digunakan di lingkungan jaringan isi. Ada sejumlah alat tambahan yang harus disebar untuk melaksanakan solusi jaringan isi tersebut. Komponen-komponen ini akan didefinisikan secara terperinci apabila solusi isi yang tepat dirancang dan disebar.



Gambar 5.6 Content Networking

5.6.4 IPTV

5.6.4.1 Tinjauan Umum

Pengadaan isi untuk desktop pada waktu nyata merupakan salah satu keperluan utama di fasilitas-fasilitas pendidikan, tetapi biaya infrastrukturnya harus diperhitungkan. IP/TV Cisco adalah produk CDN yang mengirimkan video ke desktop tersebut. Pembelajaran jarak jauh, komunikasi elektronik dan pembelajaran online merupakan penggerak-penggerak utama ke arah melaksanakan solusi-solusi IP/TV di jaringan-jaringan perusahaan sekarang ini.

Menciptakan video tape dan mendistribusikannya ke berbagai lokasi merupakan tugas yang sulit dan di lingkungan pendidikan yang pernah

berkembang menjadi sering ketinggalan jaman. Solusi IP/TV Cisco mengatasi keterbatasan ini selama isi disimpan secara sentral dan dapat diatur pada fly. Di lembaga-lembaga pendidikan banyak siswa tidak memiliki akses ke laptop dimana mereka dapat mengakses isi tersebut dan ini adalah dimana penggunaan kios-kios informasi menjadi sasaran yang besar. Informasi dapat dikirimkan ke kios dimana siswa dapat mengakses isi pilihan. Lingkungan perpustakaan menjadi sebuah tempat di dalam kotak.

5.6.4.2 Keuntungan Teknis

IP/TV Cisco adalah solusi berbasis standar-standar, yang membuat kemampuan antar-operasi ke sistem-sistem video menjadi migrasi yang mudah. Menyebarkan solusi IP/TV menjadi mudah selama tidak ada pemrograman atau integrasi sistem dibutuhkan untuk menyebarkan solusi tersebut.

Solusi IP/TV Cisco memfasilitasi pengiriman pada jaringan-jaringan multicast untuk meminimalkan bandwidth untuk video langsung dan dijadwalkan, menyiarkan aliran tersendiri pada jaringan tersebut tanpa memperhatikan ukuran pembaca. IP QoS yang menggunakan Resource Reservation Protocol (RSVP) digunakan untuk membantu menjamin bahwa bandwidth yang cukup dialokasikan untuk peristiwa tersebut.

5.6.4.3 Keuntungan Bisnis

Memberikan pelatihan online memberikan pengematan biaya sangat besar dipandang dari sudut pengeluaran perjalanan dan dukungan dan juga memungkinkan pengadaan informasi untuk sekumpulan siswa yang lebih besar dengan sedikit waktu yang dibutuhkan di lingkungan sekarang ini.

Distance learning, video on demand (VOD) dan pelatihan berbasis jaringan memungkinkan Universitas-universitas menjangkau pembaca siswa yang lebih besar dan memperluas penggunaan sumber tersebut. Isi juga dapat diatur secara sentral dan ini mempercepat waktu ke pasar.

5.6.4.4 Kebutuhan Implementasi (Lapisan Jaringan)

IPTV memiliki keperluan-keperluan yang sama pada jaringan to-be sebagai solusi CDN dan dengan demikian akan mendukung teknologi ini.

- a) IP Multicast. IPTV Cisco memfasilitasi pengiriman pada jaringan-jaringan multicast untuk meminimalkan bandwidth untuk video langsung dan dijadwalkan, menyiarkan aliran tersendiri pada jaringan tersebut tanpa memperhatikan ukuran pembaca.
- b) Dukungan untuk Source-Specific Multicast (SSM) menyederhanakan manajemen dan kontrol jaringan jaringan IP Multicast. SSM memudahkan penyebaran multicast, mengatasi masalah-masalah alokasi alamat, dan memperbaiki kemampuan multicast untuk siaran-siaran dari satu ke banyak.

- c) Quality of Service melalui Content Manager IPTV memungkinkan Quality of Service (QoS) IP yang menggunakan Resource Reservation Protocol (RSVP) untuk menjamin bandwidth dialokasikan untuk peristiwa IPTV.

Infrastruktur ini meliputi tiga komponen berikut:

- a) Content Manager IPTV – Memungkinkan manajemen lingkungan pusat.
- b) Broadcast and Archive Servers IPTV – Memungkinkan real-time encoding dan pengiriman video langsung, dijadwalkan, dan atas permintaan.
- c) Viewer IPTV – Memberikan penangkapan aliran-aliran video berkualitas tinggi dan media yang disinkronisasi, baik sebagai aplikasi yang berdiri sendiri atau browser plug-in untuk akses Web.

Content Manager, Broadcast Servers, dan Archive Servers IPTV Cisco dapat dibeli sebagai alat-alat yang telah diatur sebelumnya atau sebagai perangkat lunak yang bekerja pada server-server Windows NT dan 2000 yang diatur secara tepat. Viewer IPTV Cisco berjalan pada Windows 98, 2000, NT, XP, 7, 8 dan 10.

Server-server IPTV 3400 Series Cisco, dengan perangkat lunak yang telah diatur sebelumnya, kartu-kartu penangkap yang dipasang sebelumnya, kartu-kartu hubungan jaringan, dan penggerak-penggerak alat, menawarkan cara mudah untuk menyebarkan video jaringan di sebuah perusahaan. IPTV 3400 Series Cisco meliputi IPTV 3413 Control Server, IPTV 3425 dan 3425A Broadcast Servers, IPTV 3432 Archive Server, dan IPTV 3417 Video Starter System.

IPTV 3417 Video Starter System Cisco memperkenalkan video jaringan IPTV berkualitas tinggi kepada perusahaan yang mengevaluasi penyebaran-penyebaran skala lebih besar di masa mendatang. Sistem ini menggabungkan kemampuan-kemampuan dari Broadcast Server, Control Server, dan Archive Server ke dalam unit tersendiri.

6. SIMPULAN DAN SARAN

6.1 Simpulan

Kesiapan dan kesigapan UIN Sunan Gunung Djati Bandung dalam merespon perubahan akan memperkuat posisi UIN Sunan Gunung Djati Bandung menjadi institusi pendidikan yang mampu menghasilkan keluaran yang berkualitas sehingga mampu berdiri setara dalam pergaulan masyarakat di daerah, nasional, regional bahkan dunia, ikut berperan aktif dalam menggerakkan roda ekonomi dan pembangunan bangsa, dan menghasilkan karya yang mampu mendorong peningkatan keunggulan bangsa.

Untuk itu pengelolaan UIN Sunan Gunung Djati Bandung dewasa ini tidak dapat lagi diselenggarakan secara konvensional namun harus berpedoman pada prinsip-prinsip *Good University Governance* (GUG). Pengelolaan tersebut menjadi semangat dasar UIN Sunan Gunung Djati Bandung sebagai pusat keilmuan, kebudayaan, peradaban, dan inovasi. Hal itu sejalan dengan kondisi kompetisi global yang menuntut UIN Sunan Gunung Djati Bandung untuk secara kontinyu melakukan perbaikan program pendidikannya agar berorientasi pada *stakeholders*.

Harapan besar dengan adanya *blueprint* ini dapat menjadi arah, panduan dalam mengembangkan TI di lingkungan UIN Sunan Gunung Djati Bandung. Terutama yang menjadi pusat perhatian adalah bagian rekomendasi-rekomendasi, baik jangka pendek, jangka menengah maupun jangka panjang. Sehingga apa yang dicita-citakan dapat terwujud dengan baik.

6.2 Saran

Blueprint Teknologi Informasi dan Komunikasi (TIK) UIN Sunan Gunung Djati Bandung memuat keseluruhan perencanaan global pengembangan TIK UIN Sunan Gunung Djati Bandung khususnya pengembangan infrastruktur TIK beserta teknis implementasinya.

Blueprint TIK UIN Sunan Gunung Djati Bandung selanjutnya perlu dilakukan *updating* sesuai dengan dinamika dan perkembangan di UIN Sunan Gunung Djati Bandung setiap tahun, baik karena faktor-faktor kebutuhan internal maupun faktor eksternal terkait kebijakan dan lingkungan strategis. *Updating* ini perlu didokumentasikan dengan pengelolaan *versioning* yang dikelola dan disosialisasi secara tepat.

DAFTAR PUSTAKA

- [1] Turban, Efraim dan L. Volonino, *Information Technology for Management: Improving Strategic and Operational Performace*, New York: John Wiley and Sons Inc., 2011.
- [2] Sekretariat Negara Republik Indonesia, “Undang-Undang No. 11 tentang Informasi dan Transaksi Elektronik,” Sekretariat Negara Republik Indonesia, Jakarta, 2008.
- [3] IT Masterplan Pemerintah Kota Banda Aceh 2010-2014, Banda Aceh: Pemerintah Daerah Kota Banda Aceh, 2009.
- [4] Masterplan Teknologi Informasi dan Komunikasi Provinsi Riau 2016-2020, Pekanbaru: Pemerintah Daerah Provinsi Riau, 2015.
- [5] V. Haren, *TOGAF Version 9.1 (10th ed.)*, Van Haren Publishing, 2011.
- [6] K. Peffers, T. Tuunanen, M. A. Rothenberger dan S. Chatterjee, “A Design Science Research Methodology for Information Systems Research,” *Journal of Management Information System*, vol. 24, no. 3, pp. 45-78, 2007.
- [7] A. R. Hevner, S. T. March, J. Park dan S. Ram, “Design Science in Information Research,” *MIS Quarterly*, vol. 28, no. 1, pp. 75-105, 2004.



PENGEMBANGAN TIK

**PUSAT PENELITIAN DAN PENERBITAN
UIN SGD BANDUNG**