



PUSAT PRESTASI NASIONAL
KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN



PANDUAN TEKNIS PELAKSANAAN LKS SMK TINGKAT NASIONAL XXVIII TAHUN 2020

**Teknologi Informasi
Sistem Administrasi Jaringan**
IT Network System Administration



KATA PENGANTAR

Salah satu dari 4 pilar utama visi Indonesia tahun 2045 adalah pembangunan manusia dan penguasaan IPTEK (Ilmu Pengetahuan dan Teknologi), dengan peningkatan taraf Pendidikan rakyat Indonesia secara merata, peran kebudayaan dalam pembangunan, sumbangan IPTEK (Ilmu Pengetahuan dan Teknologi) dalam pembangunan, derajat kesehatan dan kualitas hidup rakyat, serta reformasi ketenagakerjaan. Sejalan dengan visi tersebut, dalam peningkatan pendidikan IPTEK (ilmu Pengetahuan dan Teknologi) merata pada era digitalisasi ini, siswa Sekolah Menengah Kejuruan (SMK) dituntut tidak saja harus menguasai penggunaan peralatan digital tetapi juga wajib menguasai softskill yang mumpuni.

Karena IPTEK dan komunikasi saling terkait dan tidak bisa dipisahkan, maka pada era digitalisasi disruptif, akan ada pekerjaan baru yang tercipta dan pekerjaan konvensional yang akan hilang. Untuk itu, siswa SMK harus senantiasa meningkatkan kualitas diri dan penguasaan keterampilan agar dapat memenuhi tuntutan pasar kerja, baik di masa kini maupun di masa yang belum kita prediksi. Pekerjaan – pekerjaan yang selama ini dikerjakan yang sudah ada akan digantikan oleh sistem Artificial Intelligence (AI), otomatisasi atau robot yang dapat mengambil alih beberapa peran kerja manusia. Namun secanggih-canggihnya kemajuan IPTEK, hal yang pasti muskil digantikan oleh AI adalah *softskills* seperti Komunikasi & Empati, Berpikir Kritis, Kreatifitas, Strategi, Pengelolaan Teknologi, instalasi dan maintenance, keterampilan fisik, dan visi & imajinasi. Era digitalisasi maupun otomatisasi, dapat mengubah struktur ekonomi maupun tenaga kerja di Indonesia, kecuali beberapa pekerjaan yang sulit diotomasi misalnya kemampuan *softskills* (berinteraksi dengan orang lain dan keahlian khusus).

Lomba Kompetensi Siswa (LKS) SMK Tingkat Nasional XXVIII Tahun 2020 ini akan berbeda dengan LKS pada umumnya, dengan munculnya pandemi Covid-19 mendorong Indonesia untuk berubah dan tidak lagi menjalankan pola-pola yang lama. Seluruh lomba-lomba yang diselenggarakan oleh Pusat Prestasi Nasional dilakukan secara daring dengan memperhatikan protokol kesehatan Covid-19. Sisi baik dari tantangan ini adalah siswa SMK diajak untuk bersahabat dan berkolaborasi dengan teknologi daring. Pusat Prestasi Nasional melakukan pembaharuan dengan melaksanakan LKS 2020 secara daring. LKS Tingkat Nasional Tahun 2020 melombakan sebanyak 42 bidang lomba. Diharapkan pada masa pandemi Covid-19 tidak mengurangi semangat siswa untuk berprestasi.

Sehubungan dengan hal tersebut, Pusat Prestasi Nasional, Sekretariat Jenderal, Kementerian Pendidikan dan Kebudayaan ikut mendukung pengembangan kualitas SMK dalam mengikuti perkembangan IPTEK dan memenuhi Visi Indonesia 2045. LKS Tingkat Nasional Tahun 2020 adalah salah satu kegiatan untuk mendorong semangat berprestasi peserta didik SMK yang diadakan setiap tahun dan sebagai upaya mempromosikan lulusan SMK kepada dunia usaha/dunia industri serta pemangku kepentingan lainnya.

Panduan Teknis LKS SMK Tingkat Nasional XXVIII Tahun 2020 Daring merupakan dokumen pendukung pelaksanaan LKS demi tercapainya kegiatan agar berjalan dengan baik dan dapat memberikan informasi kepada semua pihak yang ikut berpartisipasi dalam pelaksanaan LKS.

Dalam kesempatan ini disampaikan ucapan terimakasih kepada semua pihak yang telah mendukung dalam penyusunan Panduan Teknis pelaksanaan LKS SMK Tingkat Nasional XXVIII Tahun 2020.

Plt. Kepala Pusat Prestasi Nasional



Asep Sukmayadi, S.IP., M.Si
NIP. 197206062006041001

DAFTAR ISI

KATA PENGANTAR	ii
DAFTAR ISI	iv
A. PENDAHULUAN	1
B. STANDAR KOMPETENSI BIDANG LOMBA	3
C. SISTEM PENILAIAN	4
D. TEST PROJECT	5
E. ALAT	12
F. BAHAN	13
G. BAHAN PENUNJANG	13
H. LAYOUT DAN BAHAN LAYOUT	14
I. JADWAL BIDANG LOMBA	15
J. KEBUTUHAN LAIN DAN SPESIFIKASINYA	16

A. Pendahuluan

A.1. Nama dan Deskripsi Lomba

A.1.1. Nama Bidang Lomba

IT Network Systems Administration.

A.1.2. Deskripsi Lomba

Bidang lomba *IT Network Systems Administration* pada Lomba Kompetensi Siswa (LKS) SMK merupakan lomba kompetensi yang menguji keahlian siswa SMK dalam teknologi sistem administrasi server dan sistem jaringan serta integrasi sistem pada teknologi yang sedang berkembang serta digunakan pada industri saat ini.

Seorang Teknisi Jaringan serta *Systems Administrator* bekerja pada organisasi kecil hingga perusahaan besar di sektor komersial atau public dengan menawarkan berbagai layanan IT Infrastruktur yang sangat penting untuk operasional bisnis sehari-hari. Sangat berharga bagi sebuah organisasi setiap terjadinya gangguan yang mengakibatkan matinya sistem. Maka seorang teknisi jaringan serta system administrator memiliki tanggung jawab untuk bekerja secara profesional untuk memenuhi kebutuhan dan memastikan berjalannya sistem. Seorang teknisi jaringan dan sistem administrator juga memberikan saran dan panduan tentang pengembangan sistem dan layanan untuk memajukan organisasi.

Bidang IT Network Systems Administration bekerja di lingkungan pekerjaan yang beragam termasuk teknisi jaringan, *system administrator*, *network operations center*, *internet service provider (ISP)* bahkan menjadi *NetDevOps*. Ia menawarkan berbagai layanan berdasarkan: *user support*, *troubleshooting*, desain, instalasi atau *upgrade* serta konfigurasi sistem operasi dan perangkat jaringan yang saat ini bahkan dapat dilakukan dengan programming dan automation. Dalam pasar tenaga kerja, IT Network Systems Administration dapat bekerja dalam tim, sendiri atau keduanya dari waktu ke waktu. Apa pun struktur pekerjaannya, seorang IT Network Systems Administration yang terlatih dan berpengalaman memiliki tingkat tanggung jawab dan kepribadian yang tinggi dalam memastikan bisnis tetap beroperasi.

Dengan globalisasi sistem IT yang cepat dan mobilitas orang dalam dunia internasional, seorang *IT Network Systems Administrator* menghadapi peluang dan tantangan yang berkembang pesat untuk dihadapi. Untuk seorang *IT Network Systems Administration* yang berbakat ada banyak peluang komersial, sektor publik, dan internasional. Namun, ini membawa serta kebutuhan untuk memahami dan bekerja dengan beragam budaya, dan mengikuti perkembangan industri yang berubah dengan cepat. Keragaman keterampilan yang terkait dengan kemungkinan akan perkembangan *IT Network Systems Administration*.

A.1.3. Sertifikasi Kompetensi Teknis

Bidang lomba *IT Network Systems Administration* merupakan bidang lomba yang berkaitan dengan pekerjaan sebagai *Network Administrator* dan *system administrator* dengan kompetensi tertinggi yang dilombakan setara dengan sertifikasi berikut:

- Cisco Certified Network Associate (CCNA) *Routing and Switching*;
- Cisco Certified Network Associate (CCNA) *Security*;
- Microsoft Certified Solutions Expert (MCSE): *Desktop Infrastructure*;
- Microsoft Certified Solutions Expert (MCSE): *Server Infrastructure*;
- Advanced Level Linux Certification LPIC-2 or *equivalent skill set*.

Tingkat kesulitan soal disesuaikan dengan kurikulum pendidikan SMK dan tingkat kemampuan serta kenyamanan peserta untuk menyelesaikan soal dengan bentuk proyek uji yang diberikan mengikuti *World Skills Standar Spesification (WSSS)*.

A.1.4. Kompetensi Keahlian Peserta Lomba

Bidang Lomba *IT Network Systems Administration* merupakan bidang lomba yang dapat diikuti oleh siswa SMK dengan program keahlian Teknik Komputer dan Informatika khususnya kompetensi keahlian **Teknik Komputer dan Jaringan** dan kompetensi keahlian **Sistem Informatika, Jaringan dan Aplikasi**.

A.2. Dokumen Terkait

Dokumen ini berisi informasi tentang aspek teknis keterampilan, dokumen lain yang berkaitan dengan deskripsi ini yang harus dipelajari adalah:

- Pendoman lomba,

- Informasi di website panitia:
 - a. Kisi-kisi soal LKS
 - b. Rencana Kerja
 - c. Form Kebutuhan Bahan
 - d. Lembar Ceklis Kebutuhan Bahan

Diskusi terkait pelaksanaan lomba dilaksanakan melalui kegiatan:

1. Koordinasi Kepala Dinas Pendidikan
2. *Technical meeting*, pembimbing dan peserta sebelum pelaksanaan lomba.

B. Standar Kompetensi Bidang Lomba

B.1. Ketentuan Umum

Spesifikasi Kompetensi adalah rumusan target kompetensi yang akan dilombakan. Target kompetensi dirumuskan berdasarkan situasi dunia kerja atau industri dengan tetap memperhatikan kurikulum SMK. LKS mengukur pengetahuan dan pemahaman melalui keterampilan atau unjuk kerja.

Proyek uji, skema penilaian dan bobot masing-masing modul proyek uji dikembangkan berdasarkan spesifikasi kompetensi LKS-SMK.

B.2. Spesifikasi Kompetensi LKS-SMK

Hari		Kompetensi	WSC %	LKS Daring %
#H1 4,5 Jam	<i>Future Network Technology</i> (TD WSC2021)	<i>Network Administrator</i> dengan pendekatan teknologi jaringan terbaru seperti teknologi SDN dan implementasi IoT pada Cisco Packet Tracer	-	2,5%
	<i>Linux Environments</i>	<i>System administration Linux Server, Router & client. Instalasi, Upgrade</i> dan konfigurasi sistem operasi Linux	25%	12,5%
#H2 4,5 Jam	<i>Troubleshooting and secret challenges</i>	Menganalisa dan melakukan tahapan-tahapan dalam perbaikan serta perawatan	12,5%	2,5%

		sistem jaringan pada simulasi Cisco Packet Tracer		
	Windows <i>Environments</i>	<i>System Administrator</i> menggunakan sistem operasi Windows sebagai Server, router dan client baik berbasis GUI maupun Core (cmd). Instalasi, <i>Upgrade</i> dan konfigurasi sistem operasi Windows	25%	12,5%
#H3 4,5 Jam	<i>Troubleshooting and secret challenges</i>	Menganalisa dan melakukan tahapan-tahapan dalam perbaikan serta perawatan pada sistem dan jaringan terintegrasi <i>multiplatform</i>	12,5%	2,5%
	Cisco <i>Environments</i>	<i>Network Administrator</i> Perangkat Jaringan menggunakan Cisco untuk <i>Routing, Switching, Voice, Security & System Integration</i> dengan <i>network virtualization</i> .	25%	12,5%
Total			100	45%

C. Sistem Penilaian

C.1. Petunjuk Umum

Penilaian LKS SMK Nasional menggunakan ketentuan yang telah ditetapkan sebelumnya sesuai dengan material *test project* yang diberikan kepada peserta. Penilaian dilakukan oleh tim Juri atau *Expert* menggunakan dua metode, yaitu *judgement* dan *measurement*. Penilaian *judgement* dilakukan dengan cara pengamatan hasil dengan justifikasi sesuai dengan kriteria penilaian yang sudah ditentukan. Sedangkan penilaian *measurement* didasarkan pada pengukuran dengan ketentuan hanya benar atau salah. Pada bidang IT *Network Systems Administration*, sistem penilaian terdiri dari 20% *judgement* dan 80% *measurement*.

Hasil penilaian oleh juri dalam skala nilai akhir 0 sampai 100 akan dimasukan dan diproses kedalam sistem CIS (*Competition Information System*) yang digunakan pada *World Skills Competition* untuk dihitung menjadi skala 700 dalam menentukan juara 1, 2, 3 dan *Medalian of Excelent* kepada peraih nilai diatas 700.

C.1.1. Skema Penilaian

Modul	Kriteria/Sub-Kriteria	Total
A	Packet Tracer – <i>Future Network</i>	5
B	Packet Tracer – <i>Troubleshooting</i>	6,25
C	<i>Troubleshooting System Integration</i>	6,25
D	Linux	27,5
E	Windows	27,5
F	Cisco	27,5
Total		100

D. Test Project

D.1. Petunjuk Umum

Bentuk proyek uji LKS 2020 secara daring bidang IT *Network Systems* tidak jauh berbeda dengan LKS tahun-tahun sebelumnya yang dilaksanakan secara langsung disatu tempat. Setiap peserta mengerjakan secara remote kepada server yang sudah disediakan oleh juri dan panitia dari rumah atau sekolah masing-masing. Infrastruktur server akan disiapkan disatu data center berupa *cloud infrastructure as a service* yang dapat diakses peserta di semua daerah. Setiap peserta dari rumah atau sekolah masing-masing hanya cukup menyediakan laptop atau komputer yang digunakan untuk remote server tersebut serta dilengkapi camera dan aplikasi khusus untuk membantu pengawasan.

Proyek uji atau *Material Test Project (MTP)* dikembangkan untuk mengukur seluruh spesifikasi kompetensi LKS-SMK secara daring. Proyek uji bidang IT Network Systems Administration pada Lomba Kompetensi Siswa (LKS) SMK XXVIII tahun 2020 bersifat **TERTUTUP** dan baru akan dibuka pada pada **C-2** atau pada saat *Technical Meeting*. Persiapan yang dilakukan calon peserta dapat menggunakan panduan pada dokumen **Pedoman Lomba** dan **Kisi-kisi Lomba** yang merupakan gambaran soal yang nanti akan digunakan pada saat kompetisi. **Dari kisi-kisi tersebut nantinya akan berubah 30% seperti topology, services atau layanan server beserta detailnya.**

D.2. Kriteria Penilaian

Kriteria penilaian adalah hal utama dalam sistem penilaian yang ditentukan berdasarkan proyek uji. Bobot masing-masing kriteria penilaian menyesuaikan dengan spesifikasi kompetensi LKS yang ditetapkan.

Modul	Kriteria/Sub-Kriteria	Hari	Waktu	Total
A	Packet Tracer – <i>Future Network</i>	H1	1 jam	5
B	Packet Tracer – <i>Troubleshooting</i>	H2	1 jam	6,25
C	<i>Troubleshooting System Integration</i>	H3	1 jam	6,25
D	Linux	H1	3,5 jam	27,5
E	Windows	H2	3,5 jam	27,5
F	Cisco	H3	3,5 jam	27,5
Total			13,5 jam	100

D.2.1. Persyaratan Proyek Uji

Proyek uji bidang IT Network Systems Administration terdiri dari 6 modul:

A. Packet Tracer – *Future Network*

1. Peserta melakan implementasi konfigurasi berdasarkan studi kasus yang diberikan. Cakupan materi *Future Network* ini adalah SDN dan IoT *Technology*.
2. *Module Future Network* menggunakan cisco packet tracer *activity* yang langsung melakukan penilaian secara otomatis oleh aplikasi sehingga *score* akan langsung terlihat.

B. Packet Tracer – *Troubleshooting*

1. Peserta diharuskan melakukan analisi mencari solusi dan melakukan perbaikan berdasarkan solusi masalah yang terbaik. *Troubleshooting* yang dilakukan pada arena *network administrator* menggunakan Cisco Packet Tracer.
3. Packet tracer – *troubleshooting* menggunakan cisco packet tracer *activity* yang langsung melakukan penilaian secara otomatis pada saat peserta melakukan konfigurasi sehingga *score* akan langsung terlihat pada aplikasi.

C. System Integration – *Troubleshooting*

1. Peserta diharuskan melakukan analisi mencari solusi dan melakukan perbaikan berdasarkan solusi masalah yang terbaik. *Troubleshooting system integration* ini menggunakan Linux, Windows dan Cisco.
2. Peserta akan diberikan masalah dari sudut pandang seorang pengguna. Dari informasi yang diberikan peserta harus mencari tahu masalahnya serta solusi yang harus dilakukan. Setiap masalah dan solusi yang ditemukan disebut satu *ticket*. Peserta akan diberikan beberapa *ticket* yang perlu dicatat *problem* dan solusinya.

D. Linux, Windows & Cisco *Environment*

1. Peserta diminta untuk melakukan instalasi dan konfigurasi layanan menggunakan Linux, Windows atau perangkat cisco secara terpisah bergantung dari module yang sedang dikerjakan. Setiap layanan tersebut harus dikonfigurasi pada server, router atau client baik berbasis GUI atau CLI.
2. Pengujian akan dilakukan pada konfigurasi atau fungsi atau keduanya bergantung dari kebutuhan dan tingkat kesulitan.

D.3. Sub Kriteria

Setiap kriteria terbagi menjadi satu atau lebih sub kriteria yang akan muncul dalam form penilain. Setiap sub kriteria terdapat aspek yang akan dinilai sebagai judgement, measurement atau keduanya.

Sub Criterion ID	Sub Criterion Name or Description
A1	fw.skill39.net
A2	file.skill39.net
A3	client1.skill39.net
Sub Criterion ID	Sub Criterion Name or Description
B1	INTCLIENT
B2	REMCLIENT
B3	PUBCLIENT
Sub Criterion ID	Sub Criterion Name or Description
C1	CAMPUS AND BRANCH LAN
C2	PUBLIC INTERNET
C3	ENTERPRISE ROUTING DOMAIN

D.4. Aspek

Setiap kriteria dirumuskan dalam aspek penilaian yang memungkinkan diamati atau diukur, meliputi:

Sub Criterion ID	Sub Criterion Name or Description	Aspect Type M J	Aspect - Description
A1	fw.skill39.net	M	Basic Configuration
		M	OpenVPN: Site-to-site VPN
		M	OpenVPN: Remote access VPN
		M	DHCP: DNS A record update
A2	file.skill39.net	M	Basic Configuration
		M	DHCP: Static lease
A3	client1.skill39.net	M	Basic Configuration
		M	DHCP: Address assignment
		M	PAM: LDAP authentication
		M	PAM: Local user login restriction
		M	SSH: Private key authentication
		M	OpenVPN: Site-to-site VPN

Sub Criterion ID	Sub Criterion Name or Description	Aspect Type M J	Aspect - Description
B1	INTCLIENT	M	Setup: TCP/IP configured, Domain-joined Web: Access "https://www.wsc2019.ru" Web: Access "https://intra.wsc2019.ru" RAS: Device tunnel configured and connected RAS: Log on as domain user via device tunnel Bitlocker: Volume encrypted File: Test WorkFolders authentication configured File: Test WorkFolders authentication working
B2	REMCLIENT	M	
B3	PUBCLIENT	M	
		M	
		M	
		M	

D.5. Penilaian

D.5.1. Penilaian Subyektif

Judgement menggunakan skala 0 sampai 3. Untuk menerapkan skala dengan ketelitian dan secara konsisten, judgement harus dilakukan menggunakan:

- Tolak ukur (kriteria) dengan penduan terperinci untuk setiap aspek dan setiap skala.
- Kala 0 sampai 3 menunjukkan:
 - 0 : Performa dibawah standar
 - 1 : Performa memenuhi standar
 - 2 : Performa memenuhi dan dalam hal tertentu melebihi standar industri
 - 3 : Performa sepenuhnya melebihi industri dan dinilai sangat baik
- 3 juri akan melakukan judgement untuk satu aspek.

Contoh skala 0-3 penilaian judgement:

Aspect Type M J	Aspect - Description	Judg Score	Extra Aspect Description (Meas or Judg) OR Judgement Score Description (Judg only)
J	VLAN implementation	0	Not implemented
		1	VTPv1
		2	VTPv2

J	STP implementation	3	VTP
		0	Not implemented
		1	Default configuration
		2	RPVST+
J	LAG implementation	3	MST
		0	Not implemented
		1	Static (L2)
		2	Static (L3)
		3	PAgP or LACP

D.5.2. Penilaian Obyektif

Penilaian measurement dilakukan oleh minimal dua juri. Pada penilaian measurement hanya memberikan nilai 1 bila sesuai kriteria atau 0 bila tidak sesuai.

Contoh :

- o Hostname tidak sesuai : 0
- o IP address sesuai : 1

D.6. Komposisi Penilaian Subyektif dan Obyektif

No	Modul	Kriteria/Sub-Kriteria	J	M	Total
1	A	Packet Tracer – <i>Future Network</i>	-	5	5
2	B	Packet Tracer – <i>Troubleshooting</i>	6,25	-	6,25
3	C	<i>Troubleshooting System Integration</i>	6,25	-	6,25
4	D	Linux	2,5	25	27,5
5	E	Windows	2,5	25	27,5
6	F	Cisco	2,5	25	27,5
Total			20	80	100

D.7. Keseluruhan Asesmen

Sub Criterion ID	Sub Criterion Name or Description	TP	Aspect - Description	sc	Extra Aspect Description OR Judgement Score Description	Max Mark
A1	fw.skill39.net	M	Basic Configuration			0.10
		M	OpenVPN: Site-to-site VPN			0.50
		M	OpenVPN: Remote access VPN			0.40
		M	DHCP: DDNS A record update			0.40
		M	DHCP: DDNS PTR record			0.40
		M	iptables: Default chains policy			0.20
		J	iptables: NAT Rules			0.30
				0	No NAT rules implemented	

A2	file.skills9.net	J	iptables: Packet filtering	1	implemented but not limited	0.50	
				2	DNAT all traffic limited to one host		
				3	DNAT restricted to port and protocol		
				0	No firewall implemented or any/any		
				1	Firewall implemented for all services: Allow 192.168.1.0/24 to any, Allow 192.168.2.0/25 to Internet (Need to specify the Internet interface), Allow 192.168.2.2/32 to 192.168.1.2/32 tcp:389, Allow any to 168.2.2/32 tcp:80,143,587, Allow any to 192.168.1.2/32 udp:53, Allow 10.10.10.1/32 to 192.168.1.2/32 udp:137,138 tcp:139,445, Allow OpenVPN access (INPUT and OUTPUT Allow udp:1194).		
				2	Service port and protocols specified		
				3	Extra features added e.g. comments, extra chains or logging of dropped connection attempts		
		M	Basic Configuration				0.10
		M	DHCP: Static lease				0.30
		M	LDAP: OpenLDAP database				0.60
		M	RAID				0.40
M	LVM			0.30			
M	NFS share			0.40			
M	DNS: Forwarders			0.30			
M	DNS: necessary records			0.30			
M	DNS: 192.168.1.0/24 PTR			0.20			
M	DNS: 192.168.2.0/25 PTR			0.20			

D.8. Prosedur Asesmen

Juri melakukan penilaian menggunakan marking form yang berisi Kriteria, sub-kriteria, aspek, bagaimana cara menilai dan standard penilaian. Proses penilaian peserta sejak awal hingga akhir menggunakan standard penilaian yang telah ditentukan tersebut.

Modul	Kriteria/Sub-Kriteria	Hari
A	Packet Tracer – <i>Future Network</i>	H-1
B	Packet Tracer – <i>Troubleshooting</i>	H-2
C	<i>Troubleshooting System Integration</i>	H-3
D	Linux	H-1
E	Windows	H-2
F	Cisco	H-3

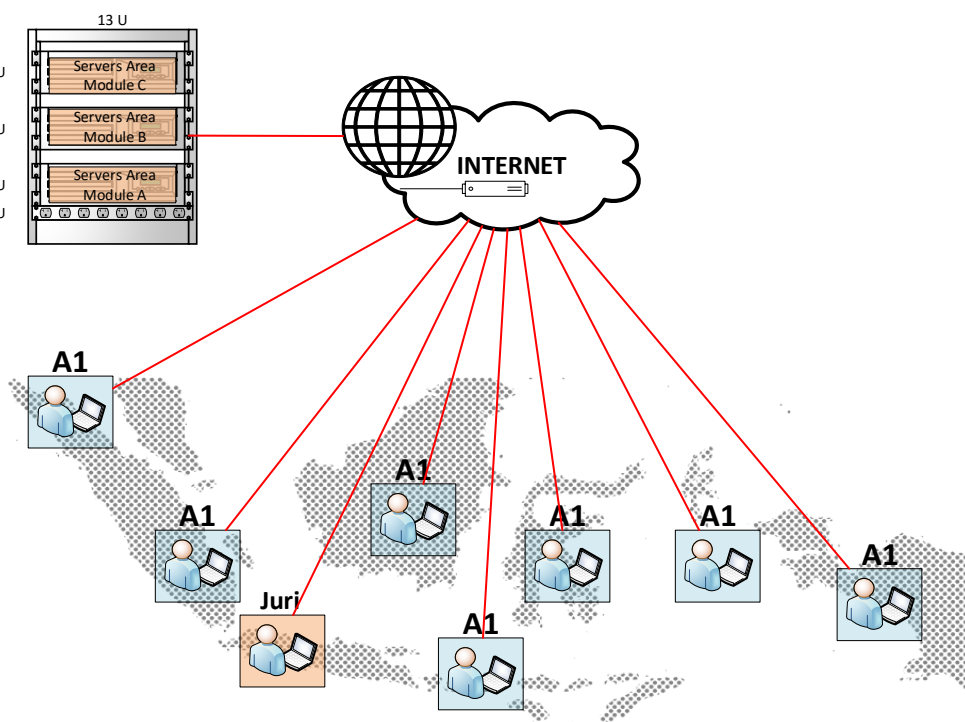
E. Alat

E.1. Ketentuan Umum

Alat dan yang telah disediakan oleh panitia tidak dapat digantikan dengan alat dan bahan yang dibawa oleh peserta kecuali panitia meminta peserta untuk menyiapkan sesuai dengan ketentuan yang sudah di tetapkan. Peserta diberikan waktu familiarisasi fasilitas lomba sebelum lomba dimulai (maksimal 2 jam).

E.1.1. Daftar Sarana Prasarana

Infrastruktur atau prasarana lomba yang digunakan pada bidang IT *Network Systems Administration* pada dasarnya peserta melakukan *remote* kepada *cloud* infrastruktur yang sudah disediakan oleh juri dan panitia. Peserta perlu memastikan memiliki koneksi internet yang baik agar tidak terkendali dalam mengikuti kegiatan lomba.



E.1.2. Daftar Alat para Peserta

Alat yang dipersiapkan oleh peserta meliputi:

No	Alat Lomba	Spesifikasi	Jumlah
1	Komputer / Laptop	Komputer untuk remote ke cloud lomba min: - CPU 4 core - RAM 8 GB	2 Buah Keterangan: - 1 Buah untuk

		<ul style="list-style-type: none"> - HDD 128 GB - Sistem Operasi Windows 10 - Webcam Depan - *Webcam External (Jika menggunakan Komputer) 	pengerjaan test project. - 1 Buah untuk live streaming
2	Webcam	Minimal 2 MP (Internal laptop/webcam external)	2 Buah
3	Mouse	Standard	1 Buah
4	Keyboard	Standard	1 Buah

E.1.3. Alat dan bahan yang dilarang digunakan

1. Komputer / Laptop / *Storage* yang berisi data-data pembahasan materi berkaitan dengan IT *Network Systems*.
2. HDD *External* atau Flashdisk diarea lomba.
3. Alat komunikasi diarea lomba selain yang digunakan untuk *video conference* dengan juri.

F. Bahan

F.1. Bahan dan Aplikasi

No	Bahan / Aplikasi	Spesifikasi
1	<i>Network Virtualization</i>	CML (Cisco Modeling Lab) 20 Node PE
2	Sistem Operasi Linux	Debian 10.x DLBD
3	Sistem Operasi <i>Windows Server</i>	Windows Server 2019 <i>Trial Version</i>
4	Sistem Operasi <i>Windows Client</i>	Windows 10
5	VMWare <i>Workstation</i>	VMWare <i>Workstation 15 Trial Version</i>
6	Cisco Packet Tracer	Packet Tracer 7.3.1

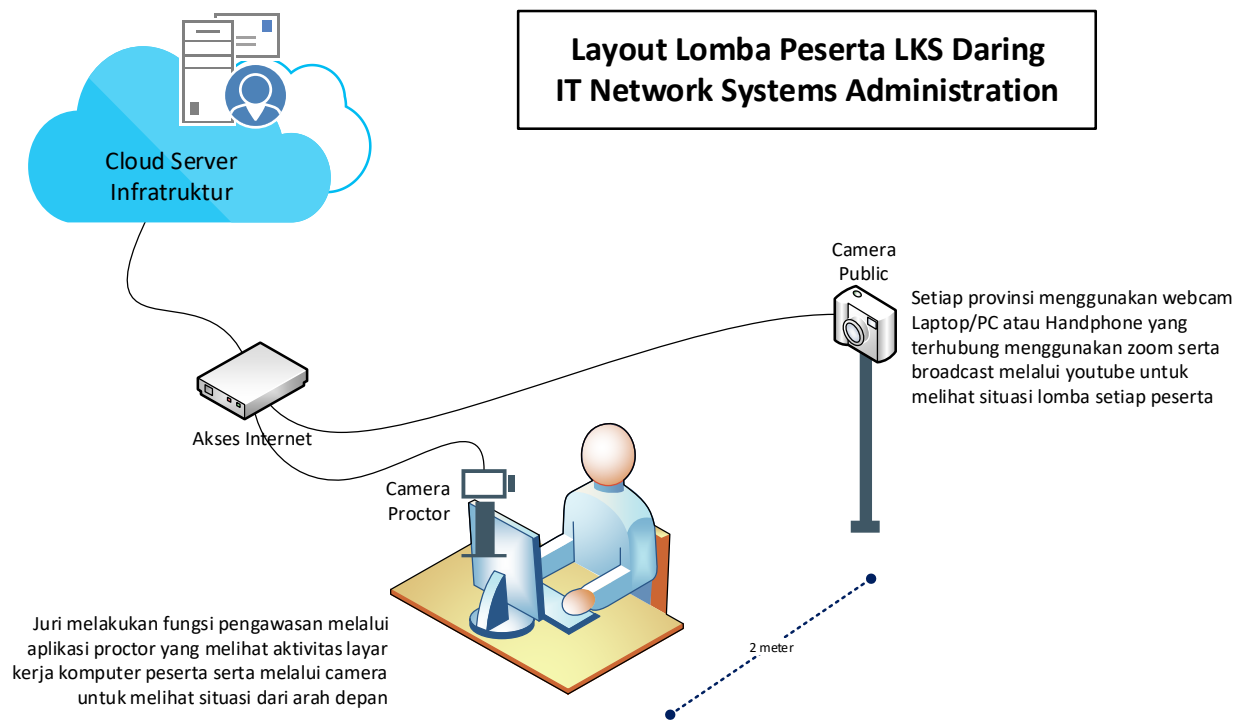
G. Bahan penunjang

G.1. Bahan Penunjang Lomba sebagai Referensi para Peserta



No.	Nama Bahan	Spesifikasi
1	Akses Internet	Min 5 Mbps yang digunakan untuk mengerjakan soal dan <i>live camera</i> serta layar kerja Komputer selama perlombaan dan uji coba
2	Discord	Last update
3	Zoom	Last update



H. Layout dan bahan layout

H.1. Layout



H.2. Tabel Kebutuhan Bahan untuk Layout

No.	Alat / Bahan	Jumlah	Satuan	Gambar
1	Meja Kerja	1	Buah	
2	Kursi Kerja	1	Buah	

3	Webcam	2	Buah	
4	Tripod	1	Buah	

I. Jadwal Bidang Lomba

No	WAKTU		KEGIATAN
1	Persiapan Lomba		
	<i>[Diinformasikan kemudian]</i>		Uji coba mekanisme LKS Daring IT Network System mulai dari Competition Management System dan Test sistem remote peserta ke Infrastruktur
2	Persiapan Lomba		
	<i>[Diinformasikan kemudian]</i>		Technical Meeting, Familiarisasi/pengecekan alat dan koneksi jaringan ke server
3	Lomba Hari ke 1 (H1)		
	07.30 - 08.00	30'	Briefing, Pemeriksaan koneksi jaringan dan server
	08.00 - 08.15	15'	Pengecekan akses soal, remote server dan membaca modul D
	08.15 - 11.45	3,5h	Lomba: Modul D – Linux
	11.45 - 12.45	1h	Peserta: Istirahat, Sholat dan Makan Juri & Panitia: Penguncian akses Module D dan Persiapan Infrastruktur Module A
	12.45 - 13.00	15'	Pengecekan akses soal, remote server dan membaca modul A
	13.00 - 14.00	1h	Lomba: Modul A – Packet Tracer Future Network
	14.00 - 18.00	4h	Marking Juri
4	Lomba Hari ke 2 (H2)		
	07.30 - 08.00	30'	Briefing, Pemeriksaan koneksi jaringan dan server
	08.00 - 08.15	15'	Pengecekan akses soal, remote server dan membaca modul E
	08.15 - 11.45	3,5h	Lomba: Modul E – Windows

	11.45 - 12.45	1h	Peserta: Istirahat, Sholat dan Makan Juri & Panitia: Penguncian akses Module E dan Persiapan Infrastruktur Module B
	12.45 - 13.00	15'	Pengecekan akses soal, remote server dan membaca modul B
	13.00 - 14.00	1h	Lomba: Modul B – Packet Tracer Troubleshooting
	14.00 - 18.00	4h	Marking Juri
5	Lomba Hari Ke 3 (H3)		
	07.30 - 08.00	30'	Briefing, Pemeriksaan koneksi jaringan dan server
	08.00 - 08.15	15'	Pengecekan akses soal, remote server dan membaca modul F
	08.15 - 11.45	3,5h	Lomba: Modul F – Cisco
	11.45 - 12.45	1h	Peserta: Istirahat, Sholat dan Makan Juri & Panitia: Penguncian akses Module F dan Persiapan Infrastruktur Module C
	12.45 - 13.00	15'	Pengecekan akses soal, remote server dan membaca modul C
	13.00 - 14.00	1h	Lomba: Modul C – Troubleshooting System Integration
	14.00 - 18.00	4h	Marking Juri

*Waktu berdasarkan WIB, sehingga untuk WITA & WIT menyesuaikan dengan jadwal tersebut.

J. Kebutuhan lain dan spesifikasinya

J.1. Kebutuhan Juri untuk Menilai

No.	Alat / Bahan	Jumlah	Satuan	Gambar
1	Aplikasi Proctor	34	Peserta	-
2	Zoom Meeting	68	Peserta dan Pembimbing	-
3	Youtube Live	1	Channel	-

J.2. Kebutuhan Perlombaan

No.	Alat / Bahan	Spesifikasi	Jumlah	Satuan	Gambar
1	Cloud Server	- Prosesor Xeon 16 Threads - Memory 128 GB - SSD 480 GB x 4	9	Unit	-

39

**IT NETWORK
SYSTEMS
ADMINISTRATION**



**KISI-KISI SOAL LKS SMK
TINGKAT NASIONAL TAHUN 2020**

***IT NETWORK SYSTEMS
ADMINISTRATION***



**LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT NASIONAL XXVIII 2020**



**TEST PROJECT
MODUL LINUX**

**IT NETWORK SYSTEMS
ADMINISTRATION**

LKS2020_LINUX_Pre

CONTENTS

Part I – Basic Configuration	2
Part II – Infrastructure Management	3
Part III – Security and Maintenance	4
Part IV Remote Connectivity	6
Part V Company Services	6

PART I – BASIC CONFIGURATION

All of our servers and clients are **debian 10.X** server with **pre-configured** hostname and IP-address as specified in the topology. All of our clients uses the default GNOME Desktop Environment. The following tools have been installed on each server and clients : **curl, ssh, smbclient, ftp, dnsutils, and sudo.**

The following requirements must be applied to all servers.

- Make sure root login is not allowed.
- Make a user 'kertarajasa' with **sudo** privilege with password, as specified in the appendix.
- Please configure the domain-name and DNS resolver accordingly.

PART II – INFRASTRUCTURE MANAGEMENT

Nusantara, inc. requires you to setup the following services with specified requirements.

Company web server at private.nusantara.id

- Use **nginx**, and please make sure it can serve php files.
- Serve **internal.nusantara.id** that requires LDAP authentication.
 - Display internal.php file by default with content listed in the appendix.
- Serve **public.nusantara.id** that is accessible without authentication.
 - Display index.php file by default with content listed in the appendix.
- Sync all the files to the company backup server.

Company file server at file.nusantara.id

- Using NFS version 4, please share the '/udd/home/' directory for internal network.
- Permit root and/or owner of respective directories to read and write inside the directory.
- Create samba share /share/smb/ that requires LDAP authentication.
 - Make sure only the user 'fatmawati' that able to delete any file. Other users only allowed to upload and download files.

Company authentication server at file.nusantara.id

- Serve **LDAP** authentication backend.
- Create all users with all attributes listed in the appendix, along with their respective home directories.

- Make sure our internal services and/or clients are able to authenticate using this server.

Company mail server at private.nusantara.id

- Serve smtps at mail.nusantara.cloud port 465 with postfix.
- Serve imaps at mail.nusantara.cloud port 993 with dovecot.
- Make sure its accessible either via internal or external network.
- Use our Authentication Server to authenticate users, make sure their email address are usable like specified in the appendix.
- Encrypt these connections with self-signed SSL Certificate.

Company DNS at file.nusantara.id

- Create A records for all of Nusantara's internal servers.
- Create A records necessary for our websites and web-interface of our monitoring service.
- Create A records and MX records necessary for our email.

Company monitoring service at private.nusantara.id

- Please use **icinga2** and enable the web-interface at **monitor.nusantara.id**
- Monitor website accessibility of both **internal.nusantara.id** and **public.nusantara.id**
- Monitor our LDAP service availability.
- Monitor our site-to-site VPN tunnel connectivity.
- Configure email notification to soedirman@nusantara.id when any of these service are DOWN as soon as possible.

PART III – SECURITY AND MAINTENANCE

The following are setup outside of Nusantara internal servers.

ITNSA backup server at se02.itnsa.id

- We recommend you to use **ssh** and **scp** for this task. However, you can also use other tools; as far as it works, we wouldn't complain.

- Configure our (Nusantara's) web server to upload their '/var/www/' content into this server at '/backup/www/'.
 - Do not change the directory structure
 - Using tools of your choice, make sure to sync **as soon as possible** (we tolerate max. ten seconds delay)
- Backup our LDAP database into '/backup/ldap/' every odd-hour using **cron**.

Company Firewall at fw.nusantara.id

The company requests you to use **iptables**

- Configure so that it will DROP all traffic by default
- Configure so that every internal service that requires access to outside are granted
- Configure nat for our **client.nusantara.id** internet access

Majapahit Firewall at fw.majapahit.net

The company requests you to use **iptables** even at this site.

- Configure so that it will DROP all traffic by default
- Configure so that every internal service that requires access to outside are granted
- Configure nat for our **Gajahmada-PC** internet access

PART IV REMOTE CONNECTIVITY

VPN Tunneling

- Configure **openvpn** site-to-site tunneling to connect Majapahit to our company.
- Use UDP port 1945 for connection.
- Use certificate authentication, create self-signed certificate as you wish.
- Make sure **client.nusantara.id** able to access all resource on Majapahit Zone
- Block traffic **from** Gajahmada-PC to Nusantara Zone via tunnelling
- Make sure Gajahmada-PC still able to access internet

Remote Access VPN

Configure remote access on **openvpn** for **Jane-laptop**. Use TCP port 1708 for this connection. Make sure the VPN Connection in **Jane-laptop** is available in the network manager with name **Krakatau**. Use LDAP for authentication. Make sure **Jane-laptop** able to access all resource on Nusantara Zone and Majapahit Zone after connection established.

PART V COMPANY SERVICES

Webmail Service on **sa01.majapahit.net**

- Use **roundcube** web-mail, and any web server of your choice.
- Use SSL self-signed certificate to serve HTTPS
- Make sure this webmail is accessible at the internet address
<https://webmail.majapahit.net>
 - you need to configure Majapahit firewall to make this work.
- At login prompt, user are able to choose 2 MAIL server, Nusantara and ITNSA.
- If Nusantara is chosen, user will connect to Nusantara's mail server. You may need configure the Nusantara firewall in order to make this work.
- If ITNSA is chosen, user will connect to ITNSA's mail server on the internet.
- make sure user can send/receive email to/from ITNSA and Nusantara mail servers.

FTP Service on **sa01.majapahit.net**

- Use **proftpd**
- Publish this ftp so that it is accessible via the internet address of **ftp.majapahit.net**

- Allow both implicit **ftps** and plain **ftp**
- Disallow anonymous login, use local user database to authenticate users. Please refer to appendix.
- Permit download and upload of new file for users, make sure they cannot delete any file(s) on the server.

Public Mail service on se01.itnsa.id

- Use **dovecot** and **postfix**
- Serve smtps at mail.itnsa.id port 465 with postfix. Use STARTTLS Auth.
- Serve imaps at mail.itnsa.id port 993 with dovecot. Use STARTTLS Auth.
- Use local user database to authenticate users, please refer to appendix. Make sure user's email address are the same as the one listed in appendix.
- Encrypt these connections with self-signed SSL Certificate.
- Configure an autoreply user no-reply@itnsa.id, whenever this user receives an email, an automatic reply must be sent immediately.
 - The message subject is *Automatic Reply from itnsa.id*
 - The message body is :

Your inquiry has not been read by any of our personnel. Kindly visit <http://itnsa.id> for more information on how to contact us.

Public DNS on ITNSA Zone.

- Use **bind9**
- Serve records for **itnsa.id** domain. Create subdomains needed for mail service to work, both A record and MX record.
- Serve records for **majapahit.net** domain. Create subdomains needed for webmail service and ftp to work, both A record and MX record.
- Create master-slave relationship with following detail:
 - Master: **se01.itnsa.id**
 - Slave: **se02.itnsa.id**
 - Encrypt slave-master zone updates using DNSSEC key – Transaction Signature.
 - Whenever record at the master is updated/changed, the record at the slave must also be updated/changed.

DHCP Service

- Majapahit DHCP Server (**sa01.majapahit.net**)
- Create pool for Majapahit clients with following requirements:
- Range : 10.20.19.10-10.20.19.100
- DNS : 172.45.80.3
- Set gateway accordingly

Nusantara DHCP Server (fw.nusantara.id)

- Create static IP lease for Jane-laptop (178.45.80.4/28). Configure DNS and Gateway accordingly.
 - Enable Dynamic DNS to the DNS service at ITNSA zone. Secure the transaction using DNSSEC and make sure the record is automatically replicated to the slave DNS.
- Create pool for Nusantara clients. There are no specific rule, just make sure the client can access our services without any problems.

Nusantara Remote Login

- Allow the PC **client.nusantara.id** to login with LDAP credentials stored in the company's Authentication Server
- Disable local user to login on this PC, so the user will be forced to use their company account stored in the Authentication Server. root should still be able to login just fine on the terminal. Note: on the GUI, root login is disabled by default, you shouldn't mess with this.
- Mount the NFS share at our file server automatically to '/udd/home' upon boot. This will be the LDAP users' homedir when they login remotely, so please configure the permissions accordingly and make sure it works like usual homedir.

Appendix

LDAP_Users

username	password	homedirectory	emailaddress
fatmawati	Skill39	/udd/home/fatmawati	fatmawati@nusantara.id
malakatan	Skill39	/udd/home/malakatan	malakatan@nusantara.id
soedirman	Skill39	/udd/home/soedirman	soedirman@nusantara.id
mohhatta	Skill39	/udd/home/mohhatta	mohhatta@nusantara.id

Local_Users

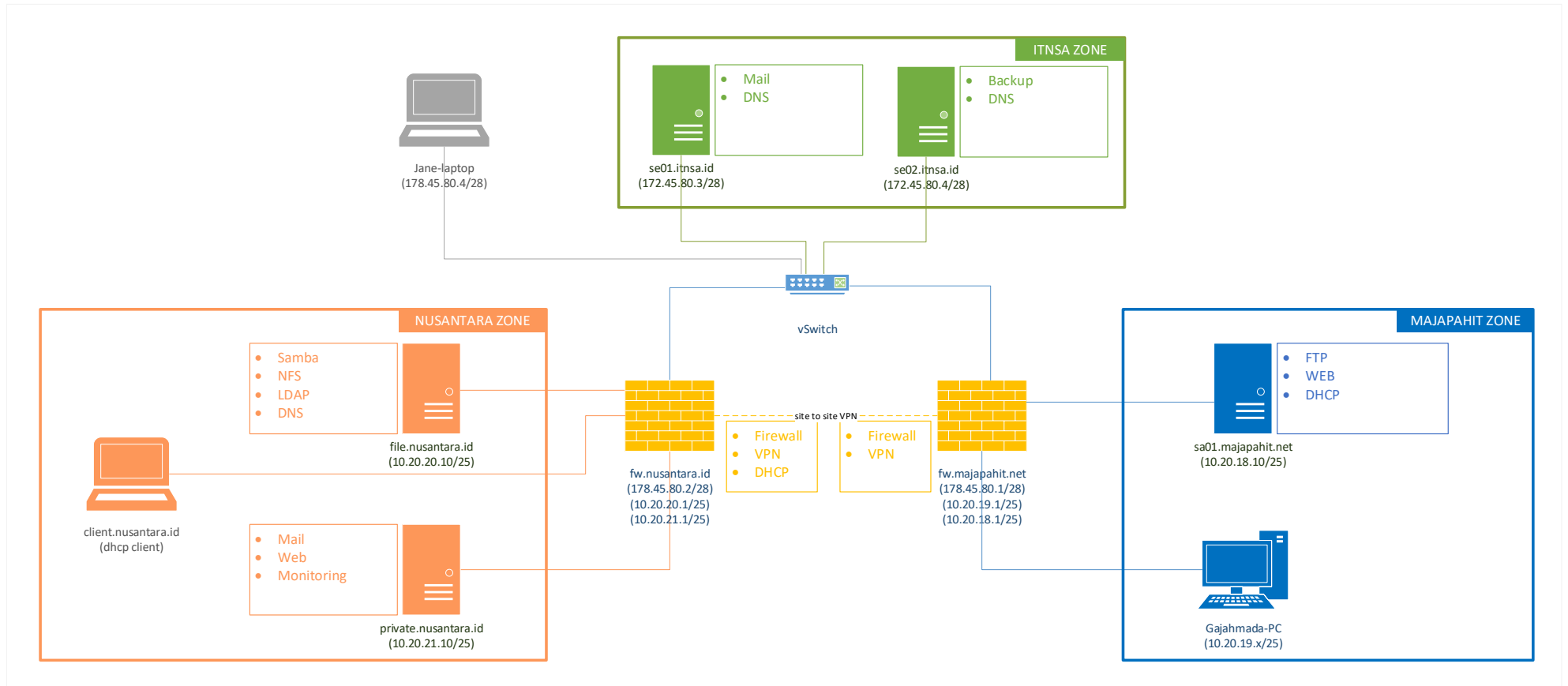
username	password	homedirectory	emailaddress
kertarajasa	Skill39	/home/kertarajasa	kertarajasa@itnsa.id

internal.php

```
<?php
echo "Internal access only. Hosted on " . gethostname();
?>
```

index.php

```
<?php
echo "Welcome to Nusantara public access.";
?>
```





**LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT NASIONAL XXVIII 2020**



**TEST PROJECT
MODUL NETWORK**

**IT NETWORK SYSTEMS
ADMINISTRATION**

LKS2020_NETWORK_Pre

BASIC CONFIGURATION

1. Configure hostnames for ALL devices according to the topology.
2. Configure domain name **lksn2020.id** for ALL network devices on the topology.
3. Create user **lksn2020** on ALL devices.
 - (a) Remote and local console authentication should use local username database.
 - (b) After successful authentication user should automatically land in privileged mode (level 15)
4. Configure privileged mode access on **FW-01** and **TOF** using username's password. E.g. username **lksn2020** with password **indonesia** should be able to enter privileged mode with password **indonesia**.
5. Create all necessary interfaces, subinterfaces and SVIs on ALL devices. Use IP addressing according to the table below.

Device	Interface	IP address
MOW	Gi0/0	132.87.2.100/24
	G0/1	192.168.254.1/30
KVX	Gi0/0	94.121.72.18/24
	G0/1	192.168.30.254/24
YKS	Gi0/0	18.31.192.12/24
	G0/1	192.168.40.254/24
FW-01	G1/0/1	192.168.254.2/30
	Vlan 10	192.168.10.254/24
	Vlan 20	192.168.20.254/24
DSW-01	Vlan 10	192.168.10.11/24
DSW-02	Vlan 20	192.168.20.12/24
RTK	Gi1/0/1	100.10.9.6/30
	Gi1/0/2	94.121.72.96/24
	Gi1/0/8	132.87.2.1/24
	Gi1/0/21	100.71.60.254/29
	Gi1/0/24	18.31.192.71/24
	Gi1/0/9	172.40.20.254/24
	Gi1/0/10	193.166.9.254/24
TOF	Gi1/6	100.10.9.5/30
	Gi1/2	172.16.100.254/24
TJM-01	Gi1/2	100.71.60.252/29
	Gi1/3	172.20.0.251/24
TJM-02	Gi1/2	100.71.60.251/29
	Gi1/3	172.20.0.252/24

HQ AND BRANCH LAN

1. Create VLANs on DSW-01 and DSW-02, assign names and ports according to the topology diagram. When adding any new VLAN to DSW-01, this VLAN should be automatically distributed to DSW-02.
2. DSW-01 should initiate trunk negotiation via DTP and be STP root in ALL VLANs. Use non-default STP protocol. Make necessary configuration to prevent STP root change attacks.
3. Configure link aggregation between DSW-01 and DSW-02. Use any LAG protocol.
4. Make sure that end user devices are not waiting for STP recalculation when plugged into the network.
5. Configure DHCP scopes on Moscow, Kazan, Tyumen, Yakutsk and Sakhalin sites. Use IP address of **Yandex** VM as a DNS server.
6. Ensure protection from DHCP attacks as well as from ARP-spoofing attacks on Moscow site.

PUBLIC INTERNET

1. Configure internet routing domain according to the topology diagram. Use BGP with AS numbers from 65000-65005
2. Make sure that end user virtual machines can access internet resources (www.yandex.com).

ENTERPRISE ROUTING

1. Configure enterprise routing domain according to the topology diagram. Use any dynamic routing protocol.
2. All traffic must be encrypted with IPsec while traversing via public internet.
3. Ensure end-to-end connectivity between all end user virtual machines inside enterprise routing domain.

SERVICES INTEGRATION

1. Synchronize time on all network equipment using NTP (time zone WITA +8). Use **RTK** as the root NTP server. Configure hierarchical NTP infrastructure use **MOW** as a corporate NTP server.
2. Client machines in **Kazan** should receive IP addresses via DHCP service from server **DC**.

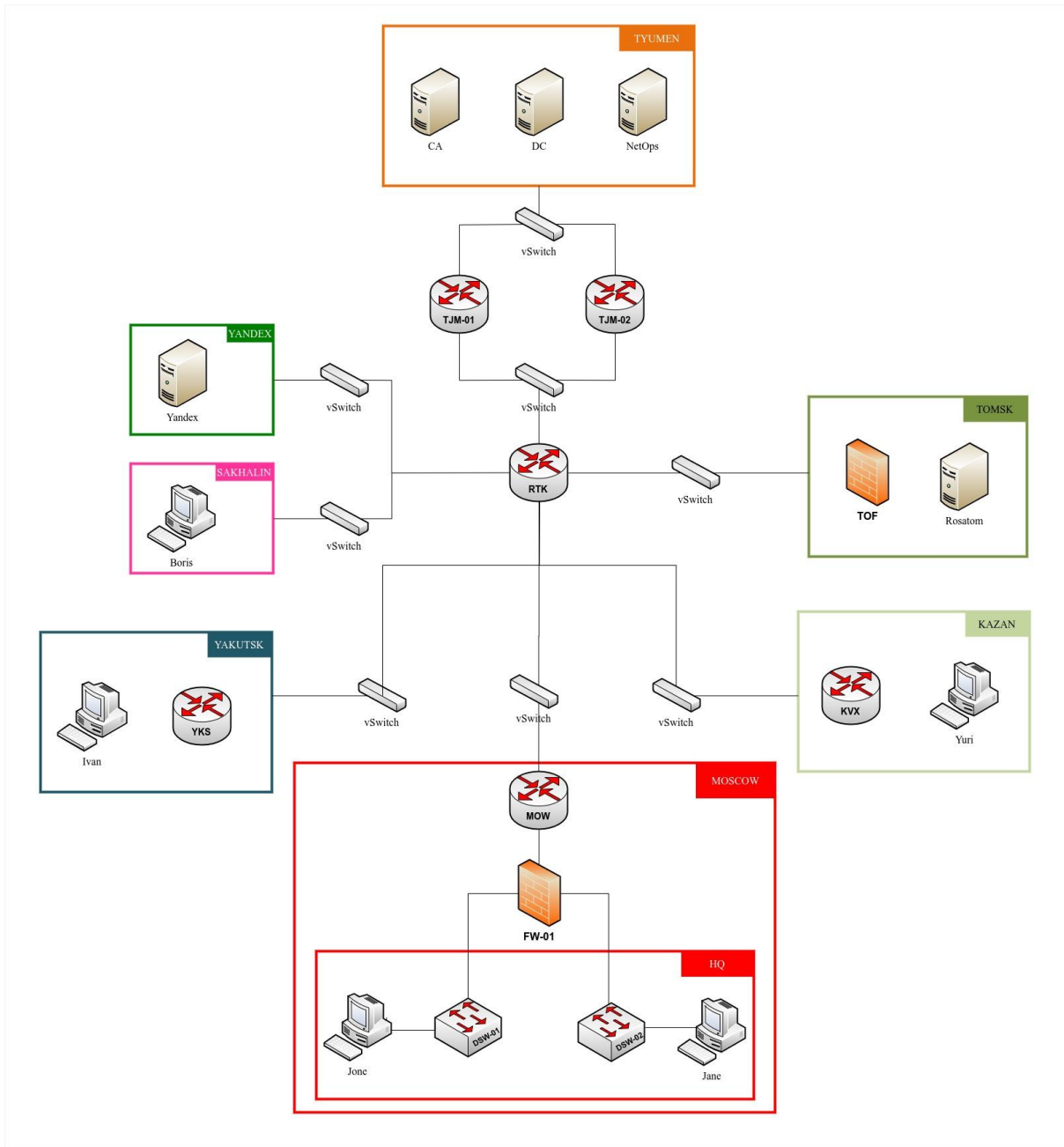
3. Add **MOW** router and **DSW-01** switch to the Observium network monitoring platform via SNMP.
4. For **MOW** router Implement configuration backup to TFTP server located on **NetOps** virtual machine. New backup copy should be created each time configuration is saved on a device.
5. Enable SSH on all network devices and implement local user **lksn2020** with password **Passw0rd\$** with privilege level 15 (use only for VTY lines). Make sure SSH is accessible via anywhere.
6. For **TJM-01** and **TJM-02** only users of **DL-Net-Admins** group in **garuda.id** domain must be able to login remotely. After login users should automatically land in privileged mode (level 15). Use local authentication in case remote authentication server is not available.

UNIFIED COMMUNICATIONS INFRASTRUCTURE

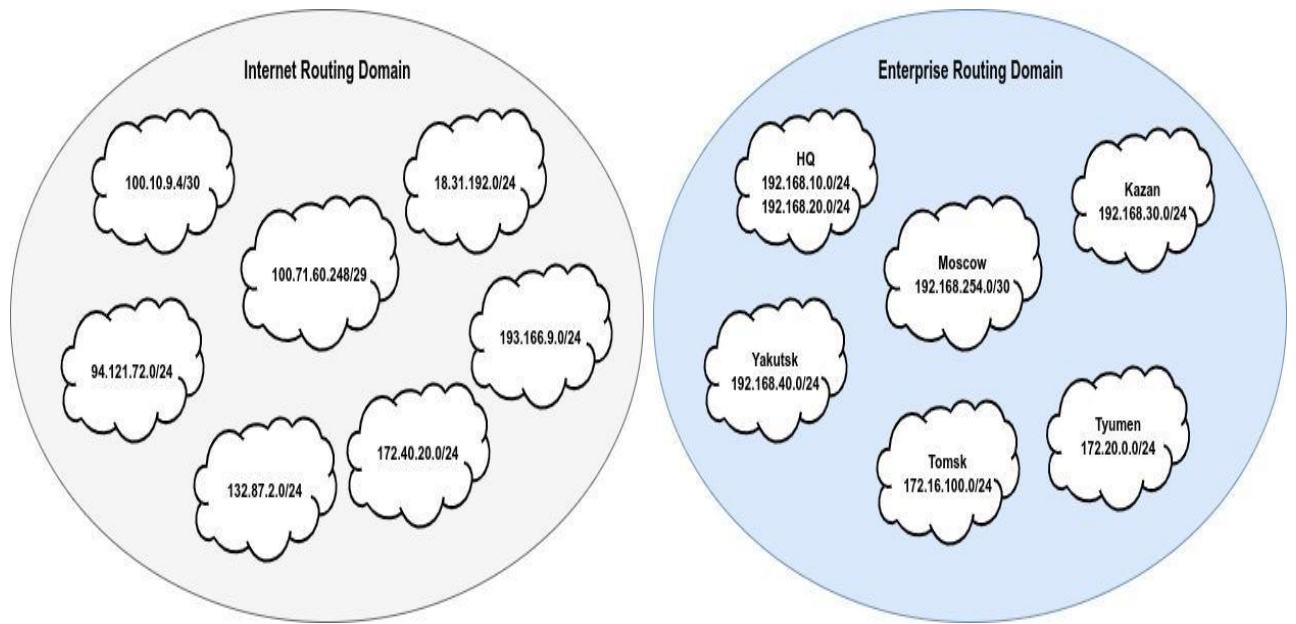
On **MOW** router configure Call Manager Express:

1. Configure custom system message **MOW-CME**.
2. Customize Soft Phones so that username is shown in the upper right corner instead of extension number. Make sure that when calling another extension, username is displayed instead of extension number.
3. Configure Local Directory Services so that users can lookup other users' extension number via the Directory catalog.
4. Configure conferencing services to support at least three parties in a conference call.
5. Configure Call Park on extension 999 to allow any user to park the call so that any user can pick up the call upon dialing the call park extension.
6. On **Jone** softphone upon pressing second line-button, **Ivan's** softphone should automatically answer the call-in speakerphone mode with mute activated and **Ivan** should hear **Jone's** conversation.
7. Both **Yuri** and **Boris** should automatically answer the call-in speakerphone mode when dialing extension 888.
8. On **Jane** configure second line-button to speed dial **Yuri**.
9. Configure Music-on-Hold. Use MOH3.au file located on flash of **MOW** router.

TOPOLOGY



Routing Diagram





**LOMBA KOMPETENSI SISWA
SEKOLAH MENENGAH KEJURUAN
TINGKAT NASIONAL XXVIII 2020**



**TEST PROJECT
MODUL WINDOWS**

**IT NETWORK SYSTEMS
ADMINISTRATION**

LKSN2020_WINDOWS_Pre

Introduction to Test Project

Contents

This Test Project proposal consists of the following documentation/files:

1. LKSN2020_Windows_Pre.docx

This implementation uses nested virtualization and all project VM's are hosted inside a "Host" machine; credentials for the Host machine are **administrator\Skills39**

You are the IT consultant responsible for Skill39. Use the password "**Passw0rd\$**"(without quotes) when no specific password has given. Use the password "**Skills39**" for local accounts.

You have inherited a Windows Domain with some users and configurations already set up but have decided to perform further tasks to improve the network. You will need to host a number of websites securely for people inside and outside the domain to access. In order to do this, you have decided to provide a high availability system based on Hyper-V amongst other improvements. You will use this Hyper-V infrastructure to improve the server infrastructure in the existing domain. Please follow the instructions that follow to complete the project.

DESCRIPTION OF PROJECT AND TASKS

PART 1. INTRANET

You need to upgrade the infrastructure in the network to the existing domain. Some machines will need to be installed from scratch, some machines will exist in a BASE condition (installed, updated, sysprepped and generalized to save time, but still require all other configuration), and some will be completely pre-installed and already configured. Examine the diagrams at the end of this project and the VM Configuration Table for clarification. Some of the tasks will need to be completed after all of the infrastructure and servers have been added, be sure to return to the earlier tasks to make sure you have completed all requirements.

DC1– PREINSTALLED AND PRECONFIGURED

Configure existing machine to match the requirements

- This server is pre-configured as the domain controller of garuda.id.
- Configure Active Directory.
 - Fix the PowerShell script and import users from included excel file. Accounts should be enabled, have the properties listed in the spreadsheet including group membership, and NOT be required to change password at first login.
- Configure DNS service.
 - Create all appropriate A records for all servers on 192.161.139.0/24 subnet.
 - Create all appropriate CNAME records according to the tasks.
 - A record of 192.161.139.101
 - adfs
 - CNAME record of dc2.garuda.id:
 - work
 - CNAME records of web.garuda.id:
 - csweb, www, intra, extra
 - Configure root hint as "ns.msftncsi.com" and remove other root hints.
 - Create a reverse lookup zone creating PTR records for all servers.
- Configure DHCP service.
 - Configure failover scope with DC2 once it is installed. Set DC1 as the active server.
 - Total scope Range: 192.161.139.51 - 192.161.139.75
 - Give DC1 70% of this scope to DC1, and the rest to DC2

- Configure the failover to use Hot Standby mode
- Scope Options
 - DNS: 192.161.139.1, 192.161.139.101, Gateway: 192.161.139.254
- Configure Network Policy Server to authorize network access for VPN-connected users.
 - Users in the Competitor group are not allowed to connect to VPN server.
 - Agents and Experts can use VPN connection by username and password.
- Add WDS service for future Hyper-V server deployments
 - Users running WDS should have an option for installing a Windows 2019 server with either a GUI or Non-GUI interface.
 - Deploy the WEB Virtual Machines in the Hyper-V server cluster once it is created via WDS.
- Configure and apply the following group policies:
 - Disable "first sign-on animation" on each domain-joined client.
 - Change Power settings so machines do not go to sleep for each domain-joined client.
 - Create a GPO which is applied to all machines so that the firewall is modified to allow ping traffic between machines.
 - Automatically issue a certificate for the "Manager" group members.
 - The work folder must be automatically connected when "Experts" group members logged on.
- Create and share a C:\backups folder as \\DC1\Backups\
 - Create a backup job to backup all users home folders located on DC2 at 4 PM daily.
 - Make sure the backup job is written to the event log.

CERT

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Configure the Certification Authority service.
 - Use certificate issued from "ISP-CA".
 - Common Name: "LKSN2020-CA"
 - Enable extensions for CDP and AIA URL through HTTP.

- URL for CDP: • URL for CDP:
http://cert.garuda.id/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl
- URL for AIA: • URL for AIA:
http://cert.garuda.id/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crl
- Create these templates:
 - "_RU_Manager"
 - For users in the "Manager" group.
 - "_RU_Server"
 - To provide a certificate for servers/services ingaruda.id domain.
 - "_External_Client"
 - To provide a certificate for computers on the Internet.
 - Enable key-based renewal.
 - Enable certificate manager approval to issue a certificate.

DC2

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Configure this server as a second domain controller for the garuda.id domain.
- Configure DNS service.
 - The records of Active Directory-Integrated zones should be replicated.
- Configure DHCP service.
 - Configure failover scope - refer to the description for DC1.
- Configure Active Directory Federation Service.
 - This server provides federation service.
 - URL: "https://adfs.garuda.id"
 - Display Name: "LKSN2020-Kazan Single Sign-On"
- Add three extra 10G drives
- Format the attached disks with NTFS into a single RAID 5 array (G:\) and enable de-duplication on this volume.
- Create file share for user's home drives.
 - Access URL: dc2.garuda.id\homes

- Local path: "G:\homes\"
- Configure Work Folders.
 - Access URL: https://work.garuda.id/
 - Local path: "G:\work\"
- Create a file share for each group.
 - Access URL: dc2.garuda.id\WSC
 - Local path: "G:\WSC\"
 - Create three subfolders and configure access control:
 - Junior Skills
 - Allow read-only access for users who have "Junior" as the job title.
 - Allow full access to the users who are also part of the "WSJ" organizational unit and also belong to the "Manager" group.
 - Secret Challenges
 - Allow access only for "Agent" group.
 - This folder should be hidden for the user who has insufficient permission.
 - Public
 - Allow read-only access for domain users.
 - Create a file share for local path G:\witness and share it as [\\DC2\witness](https://dc2.garuda.id/witness).

INTCLIENT – BASE Install

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Join to garuda.id domain.
- Use this machine to:
 - Test access to Manager/Intranet/Extranet websites.
 - Test GPOs.
 - Test home and Work Folders.
 - Ensuring users have been imported correctly.

PART 2. VIRTUALIZED SERVER FARM

You have completed the core domain infrastructure configuration. You now need to configure your virtualized server farm to provide further infrastructure and application services through a high-availability configuration. Follow the instructions given to complete the task.

STORAGE – BASE INSTALL

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- IP Address: 192.168.1.10
- Configure the iSCSI target.
 - Add new disk of 200 G for storing the virtual machines.
 - Format disk using ReFS and mount as "E:\\" drive.
 - Create 100GB of iSCSI virtual disk "E:\iSCSIVirtualDisks\LKSN2020-VM.vhdx".

Configure the target name as "LKSN2020-TGT".

- Create an SMB based witness disk on DC2 on <\\DC2\witness>.

HYPERV1 and HYPERV2

Install HyperV1 with physical attributes that match HyperV2 and configure both Hyper-V servers to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Configure iSCSI Initiator.
 - Connect iSCSI disk "LKSN2020-VM" and create ReFS partition using maximum available size.
 - Mount the volume as "V:\\" drive.
- Configure Failover Cluster.
 - Name: HYPERV-CLUS
 - IP address: 192.161.139.200
 - Create role "LKSN2020-Infra" contains the virtual machines.
 - Set affinity so that LKSN2020-Infra role runs in HYPERV1 unless it fails.

WEB

Install to cluster via WDS Deployment and Configure

- If you are unable to configure or get the WDS to work, you may install this machine manually inside the Hyper-V cluster or, if the Hyper-V is not working, you may install it as a separate VM.
 - Remote administration of IIS on a core server is tricky, the intention is that you can configure the various websites on this server using PowerShell, if you are unable to do this with PowerShell or setup remote configuration, you may set this up as a server with a Desktop Experience, doing this as a core server is a single aspect of the marking scheme.
- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Install and configure IIS and its websites using given HTML files. (from USB)
 - Use a single certificate that only has "www.garuda.id" as a common name.
 - Configure the "Default Web Site" as described below.
 - Path for website root: "C:\inetpub\intranet\".
 - Enable Windows Internal authentication.
 - Use certificate authentication for "/manager/" subdirectory.
 - Create "https://extra.garuda.id" website with the name "Extranet".
 - Path for website root: "C:\inetpub\extranet\".
 - Enable ADFS web authentication via the Web Application Proxy for clients on the Internet.
 - Create "https://www.garuda.id" website with the name "Public".
 - Path for website root: "C:\inetpub\internet\".
- Configure Certificate Enrolment Web Service (CES) and Certificate Enrolment Policy Web Service (CEP).
 - URL: "https://csweb.garuda.id" for both CES and CEP.
 - Computers that are not in garuda.id domain should be able to get a certificate through this server.
 - Authentication should be done by username and password.
 - Friendly Name: "LKSN2020 Enrollment Policy"
 - Make only "_External_Client" template visible.
- Configure IP Address and Domain Restrictions.

- The "https://intra.garuda.id" website can be accessible from:
192.161.139.0/24, 192.168.219.0/24

PART 3. PERIMETER AND INTERNET

You need to build a web application proxy and remote access service that allows you to use the internal resources of the domain outside the domain. Follow the instructions to complete the task.

FIREWALL – BASE

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Enable routing.
- Configure DNS server for the public Internet.
 - Create primary zone "garuda.id" and add these A records of 192.161.140.100.
 - ns, vpn, csweb, extra, work.
 - Add an A record "www.garuda.id" of 192.161.139.103
 - SOA record of the "garuda.id" should be "ns.garuda.id".
- Configure Routing and Remote Access Service.
 - Users and computers on the Internet should be able to establish VPN connection to this server.
 - IKEv2 clients can connect to the intranet through this server.
 - Authorize VPN access through the NPS.
 - IP address pool for remote access clients: 192.168.219.1 - 192.168.219.254
- Configure the Web Application Proxy.
 - Clients on the Internet should be able to:
 - Access "https://extra.garuda.id" website after passing the ADFS web authentication.
 - Access "https://csweb.garuda.id" to reach to the Certification Enrolment Policy and Certification Enrolment Service.
 - Access "https://work.garuda.id" to use work folders for each user.
 - Configure firewall rules to prevent unauthorized access.
 - Allow HTTPS traffic from 192.161.140.0/24 to 192.161.139.103.

- Block any other traffics sourced from 192.161.140.0/24 to 192.161.139.0/24.

REMCLIENT - BASE

Configure to match the following requirements

- Rename, and Set IP address according to configuration table and network diagram at end of project.
- Join in garuda.id domain through VPN.
- Configure the Always-on VPN/Device tunnel.
 - Domain users should be able to log in via this tunnel.
 - Only the dc1 and dc2 can be accessed through this tunnel (not other servers/resources).
- Deploy App-triggered VPN.
- Create an IKEv2 VPN connection named "AppVPN" for "Managers" group members only that automatically connects to "vpn.garuda.id" when a member of the Managers group runs Internet Explorer."
- After connection to the VPN, the user should have access to all resources of the intranet.
- Use bitlocker to encrypt the drive of REMCLIENT. Save the bitlocker recovery key to your USB.

PUBCLIENT – NOT INSTALLED

Install/Configure

- Install, rename, and set IP address according to configuration table and network diagram at end of project.
- Do not join this client to the domain.
- Set the firewall on this machine to allow inbound and outbound “ping” traffic.
- Set the power settings to “never sleep”.
- Test Work Folders service is available via "https://work.garuda.id".
 - ADFS web authentication should be work.
 - Work Folders should be accessible and writable.
- This client should be able to receive a certificate from CES.
 - Create a local Enrolment Policy.
 - Get a certificate contains CN=PUBCLIENT from CES.

- Create an IKEv2connection "LKSN2020-VPN" for test purpose and make don't remember credential.

INET – Preconfigured

Verify configuration if required

- This machine is preconfigured for your use, if you wish to, you may re-install and configure this machine to these specifications.
- Host NCSI website.
 - Clients on the Internet should indicate network connection as the "Internet".
- Configure DNS server.
 - Create zones and records for NCSI.
 - Add an A record "cs.msftncsi.com" of 192.161.140.1.
 - Add an A record "ns.msftncsi.com" of 192.161.140.1.
 - SOA record of the "msftncsi.com" should be "ns.msftncsi.com".
 - Create a root zone(.) to simulate the root DNS server.
 - Create appropriate delegations to resolve DNS records.
- Configure DHCP service.
 - Range: 192.161.140.151 - 192.161.140.175
 - DNS: 192.161.140.1
 - Gateway: 192.161.140.100
- Configure the Certification Authority.
 - Common name: ISP-CA
 - Enable extensions for CDP and AIA URL through HTTP.
 - URL for CDP: <http://cs.msftncsi.com/CertEnroll/ISP-CA.crl>
 - URL for AIA: <http://cs.msftncsi.com/CertEnroll/ISP-CA.crt>
 - Issue certificate request for LKSN2020-CA.

APPENDIX

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
DC1	Windows Server 2019Desktop	garuda.id x`	192.161.139.1	Yes - Configured
DC2	Windows Server 2019Core	garuda.id	192.161.139.101	BASE
CERT	Windows Server 2019Desktop	garuda.id	192.161.139.100	BASE
INTCLIENT	Windows 10 Enterprise	garuda.id	DHCP	BASE
HYPERV1	Windows Server 2019Core	garuda.id	192.161.139.10 192.168.1.1	No – manual install
HYPERV2	Windows Server 2019Desktop	garuda.id	192.161.139.20 192.168.1.2	BASE
STORAGE	Windows Server 2019Desktop	WORKG ROUP	192.168.1.10	BASE
WEB	Windows Server 2019Core	garuda.id	192.161.139.103	No-WDS Deployment
FIREWALL	Windows Server 2019Desktop	WORKG ROUP	192.161.139.254 192.161.140.100	BASE
REMCLIENT	Windows 10 Enterprise	garuda.id	DHCP	BASE
PUBCLIENT	Windows 10 Enterprise	WORKG ROUP	DHCP	No
INET	Windows Server 2019Desktop	WORKG ROUP	192.161.140.1	Yes - Configured

Machines indicated as being preinstalled with "**Yes**" will have the operating system installed.

Machines indicated as being preinstalled with "**Yes - Configured**" will have the operating system installed and pre-configured for Competitor use. Competitors may need to do further configuration to match the specifications laid out in this document.

Machines indicated as "**BASE**" are standard installs which have been sysprepped and generalized to save installation time across the project, they will still need to be configured.

TOPOLOGY

