Skill India

कौशल भारत - कुशल भारत

N·S·D·C

National

Skill Development

Corporation

Transforming the skill landscape

India skills

Test project: IT Network Systems administration

Category: Information and Communication Technology

Skill Explained

Network technologies knowledge has become essential nowadays for people who want to build a successful career in any IT engineering field. This test project contains a lot of challenges from real life experience, primarily IT integration and IT outsourcing. If you are able to complete this project with the high score, you are definitely ready to implement network infrastructure for any multi-branch enterprise.

Eligibility Criteria- Competitors born on or after 01 Jan 1997 are only eligible to attend the Competition

Duration of Test project: 16 hours

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar from the Linux Microsoft and Cisco certification tracks. Tasks are broken down into following configuration sections:

WS-TASK-A Network
WS-TASK-B Network
WS-TASK-C Network

Preface

Section A-Test Project

Section B-Network Infrastructure Design (Tool and equipment including raw material)

Section C-Marking Scheme

Section D- Instruction for Competitors

Section E- Health, Safety and Environment

SECTION A

WS-TASK A – NETWORK

COMPETITOR INSTRUCTION

Resources that will be necessary for the future migration, preparing for secure connectivity between the new domain and the old domain - which will involve setting up a VPN server.

INTRODUCTION

The competition has a fixed start and finish time. You must decide how to best divide your time.

Please **carefully read** the following instructions!

When the competition time ends, please leave your station in a running state. The assessment will be done in the state as it is. *No reboot will be initiated as well as powered off machines will not be powered on!*

Please do not touch the VMware configuration as well as the configuration of the VM itself except the CD-ROM / HDD drives

PHYSICAL MACHINE (HOST)

FOLDER PATHS

ISO Images: VMware ESXi Datastore

LOGIN

Username: root / LDAP-Users

Password: essci18

Domain: ESSCI.com

System Tools

- Install CURL
- Install SSH daemon and allow root access

Description of Project and Tasks

You are a system engineer and you have the task to implement a complex Linux based IT environment for an international assembly of professional experts. The requirements are gathered where possible and documented. Please get an overview of the project by studying the physical and logical diagrams at the end of this document.

System Configuration (General)

All the server and client systems are pre-installed with a basic configuration of Debian Linux. Please use the credentials and settings stated on the introduction page (page **Error! Bookmark not defined.**). You are allowed to change these values to the ones you prefer. But at the end of the day, all the settings must be reverted to its initial values.

Configure all servers with the correct hostname and network settings found in the appendix.

Install on every machine the system tools that have been mentioned in the introduction.

Please use the default configurations if you are not given any details.

For values which do not impact the assessment, such as 'Region' or 'Local', will result in losing minor points. If the process of assessment is impaired you will lose all points respectively.

The "Internet" network/subnet is connected to the management station. This means that you can leverage PUTTY/SSH to manage your virtual machines, given that your network is properly configured.

Login Banner

Must be shown before the login prompt. Must appear for local and network logins.

++
World Skills 2018 – Delhi (India)
WS-TASK A
++

General Tasks

Settings

Configure the system as mentioned as instruction.

Differences between the pre-installed system and the requested system configuration may exist.

DMZ ZONE

SSC-MAIL

Load balancer (HAPROXY)

Configure a HTTP/HTTPS load balancer for “www.india-east.cloud”, which is hosted by wsc-c-saopaulo and wsc-c-leipzig. Connect to back ends by using HTTPS and make sure that certificates are fully trusted (no browser or other certificate errors).

DNS

- Install Bind9.
    - Configure a forward zone called “www.india-east.cloud”.
        - Create for each host an A record to the respective IP
        - Create a CNAME record for ‘www’ that points to the appropriate host that serves websites for all clients
        - Create a CNAME record for ‘mail’ that points to the mail server
        - Create the appropriate MX records
        - Create a CNAME record for ‘ftp’ that points to the ftp server
        - Create a CNAME record for ‘files’ to access the DFS shares
    - Configure a forward zone called “competition.in”
        - Create the appropriate records for email to work
    - Configure a reverse zone for the IP range defined in DMZ network.

MAIL

- Install Postfix and Dovecot.
    - Configure SMTPS and IMAPS server for "india-east.cloud" and “competition.in” domain using certificates issued by SSC-CA.
    - Configure mail directory in /home/[user]/Maildir.
    - Authentication has to be done through LDAP
        - Make sure that the corresponding local user do not exist
        - Allow only users from the OU “mail”.

- Enable SMTP submission (TLS tcp/587).
  - Disable port tcp/25
- Enable secure IMAP (TLS tcp/143)

SSC-WEB1 AND SSC-WEB2

Webserver – Apache

The marking will be done on either of the two servers. Which one will be decided prior the marking starts by the assessment team. So you have to configure both servers!

- Install Apache
  - Configure a HTTPS-only website for "www.india-east.cloud" domain and “localhost” using certificates issued by SSC-CA.
  - The website page should display the following message:
    - *“Welcome to the India east cloud on [HOSTNAME]”.*
    - Add the hostname dynamically with PHP
  - Add the HTTP header “X-Served-By” with the server hostname as the value.
  - Install rsync on SSC-web1 and synchronize /var/www directory (recursive) from SSC-web1 to SSC-web2, automatically every minute.
    - To run the script don’t use crontab, solve it within the script only
    - Script must be running while assessing the test project
    - Make the script available in ‘/root/web_sync.sh’
  - Make sure that PHP scripts can be run
    - index.php should be first priority for index files
  - Install the appropriate Redis module for PHP
  - Create a password protected (basic authentication) subfolder “redis”
    - Use user skills18 with password *Skills18 t*o authenticate
  - Add a PHP script with the name “index.php” inside the redis folder
    - Add the following content the “index.php”

```
<?php
   $redis = new Redis();
   $redis->connect(<server>);
   $content = $redis->get(<key>);
   echo $content;
 ?>
```

Protected Server Zone

SSC-SMB

Install and configure the following services. Make sure that all LDAP users in OU “Misc” can login locally, users from other OU must not be allowed to login locally.

System

- Configure the disks and partitions

- Add three disks to the system (chose the appropriate type and size by yourself)
- Create a RAID 5 array and partition them with EXT4
- Mount the new array to /files (file access must be possible automatically after system start)

File Shares

- Install and use Samba for the following tasks
  - Authentication is done by "SSC-CA", local users are not permitted
  - Home directory of the respective user (authenticated user against Samba)
    - Not visible (nobody)
    - Accessible only for the authenticated user through "\\[server]\[user]"
    - The home share is only accessible from the client's subnet
    - Local data path: /files/users/[user]

Distributed File Share (DFS)

- Configure Samba for DFS
  - Enable DFS
  - DFS should be accessible through "\\SSC-CA\dfs" for clients
    - Local DFS root: /files/samba/dfs
  - Distribute the share "public" through DFS (\\SSC-CA\dfs\public)
    - Local data path: /files/samba/public
    - Share is not visible outside the DFS (e.g. \\SSC-CA\public)
    - Creating a "public" sub-folder inside the DFS share is not allowed (real DFS linking)
    - This share is writable by everyone (authenticated and anonymous)
  - Distribute the share "private" through DFS (\\SSC-CA\dfs\private)
    - Remote data path: \\wsc-i-calgary\private
    - Creating a "private" sub-folder inside the DFS share is not allowed (real DFS linking)
    - This share is readable / writable for every LDAP user

FTP

- Setup FTP with PureFTP
  - Use a virtual user configuration (not system users)
    - User: skills18-ftp / Password: Skills18
    - Home directory: "/files/users/skills18-ftp"
  - The virtual user has to be mapped to the system user/group "ftpuser/ftpgroup"
  - Per user only one active concurrent session is allowed
  - Only allow explicit SSL / TLS (ftpes://)
  - File renaming is not allowed

Internal Server Zone

SSC-MON

Redis

- Install redis server (key-value store)

- Add a new entry to the store with following command line code. Replace the content in brackets with some hard-coded equivalents

```
>> SET skills18:index "Today is the [date] and in one hour is [current time +1]"
```

CACTI Monitoring

- Install Cacti monitoring service
- Change the administrator's password to "Skills18"
- Add a graph of SCC-Mail network traffic

PING MONITORING

- Install Icinga monitoring service, use password "Skills18" as the password for "skilladmin".
- Setup a basic ICMP ping monitor SSC-SMB.
- When monitoring fails, after 60 seconds send a notification to user3@india-east.cloud.

SYSTEM

- Create a script (shell or php) with the name 'index_update.*' in the folder '/root'
- The script should update the redis entry (created above) with the current date and the mentioned time. The same command as above can be used for shell scripts or
  `$content = $redis->get('skills18:index');` if you prefer php
- Schedule the execution of the script
  - Every two minutes where the execution must happen on odd-minutes
- Create a script 'ftp_listing.sh' in the folder '/root' that lists the content of the ftp user

Client Zone

SSC-Clients

Install and configure the following services. Make sure that all LDAP users in OU "Misc" can login locally; users from other OU must not be allowed to login locally.

E-mail

- Use Icedove as the e-mail client and configure using the user "skills18".
  - Configure to use user3@india-east.cloud
  - Send an email to competitor@competition.in
  - Use IMAP to connect to the mailbox

Web

- Use Firefox as the web browser.
  - Make sure that www.insia-east.cloud is accessible.
  - No certificate warning
  - Shows appropriate content

FTP

- Use FileZilla as FTP-client
  - Make sure that a connection to SSC-Clients (ftp.india-east.cloud) can be established.

Samba

- Make sure that users can access the file shares from SSC-Clients
    - Mount DFS share to /mnt/dfs
    - You must be able to access both shares (public, private) through DFS

Login

- Add offline capabilities
- After LDAP is offline, it should still be possible for users to access the host within one minute

Add the india-east.cloud CA certificate as trusted, so that no certificate warnings are shown for all the above

SSC-IPSEC

E-mail

- Use Icedove as the e-mail client and configure using the user “skills18”.
    - Configure to use competitor@competition.in
    - Send an email to user3@india--east.cloud
    - Use IMAP to connect to the mailbox

VPN

- Install a VPN client for (L2TP/IPSEC)
    - Connect to WSC-P-STGALLEN using any of the VPN-Users.
    - Create a script on “/root/vpn.sh start | stop” to start and stop the VPN connection.

Add the wsc17.cloud CA certificate as trusted, so that no certificate warnings are shown for all the above.

WS-TASK-B: Network Windows Environment

Introduction to Test Project documentation

The competition has a fixed start and finish time. You must decide how to best divide your time.

Contents

This Test Project consists of the following document/file:

WS-TAS-B required (This doculmens)

- Excel file for the user import (RU-Users.xlsx)
- Websites for install
    - Manager Website
    - www.RUSSIA.net Website
- RSAT Tools (WindowsTH-RSAT_WS2016-x64.msu)
- Windows 10 ADMX files (Windows_ 10_Creators_Update_ADMX.msi)
- Windows Server 2016 ISO

Description of project and tasks

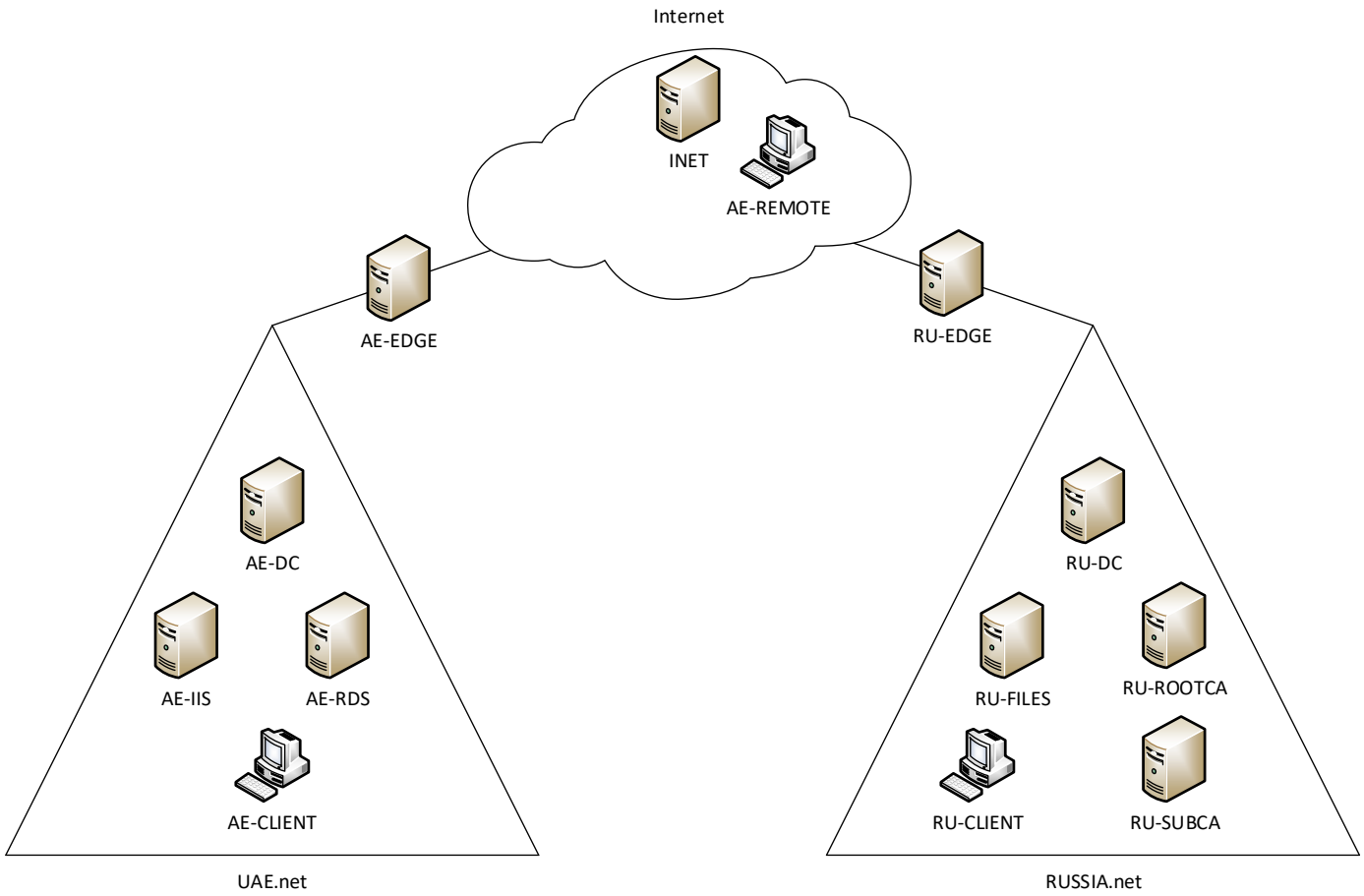
Introduction

There is already an existing domain UAE.net. You have to build and configure the network for the next World Skills competition, which consists of a new domain RUSSIA.net and copy some of the users to this new domain and also implement features for external access to the network, policies and file services.

This project several components, you need to:

1. Build a new domain (RUSSIA.net) which will eventually host all the users and computers for the next competition
2. Maintain connectivity and access to resources between the new domain and the old domain (UAE.net) while the transition is being made
3. Copy some of the users and data from the old domain to the new one
4. Setup a new site-to-site connection

Quick Specifications



Part 1 – RUSSIA.net

In Part 1 you will be responsible for preparing the new domain prior to performing the migration. This will involve building the RUSSIA.net domain, including all of the resources that will be necessary for the future migration,

preparing for secure connectivity between the new domain and the old domain - which will involve setting up a VPN server and a multi-tier PKI infrastructure.

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table. Please use the default configuration if you are not given the details
All local and domain users on ALL machines should have a password of "P@ssw0rd" unless otherwise specified. Pre-supplied machines that the competitor needs to logon to will also be pre-configured with this password.
All supplied software and files needed to complete this project can be found in C:\software on the competitor computer.

WORK TASK RU-DC

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic

Active Directory

- Configure this server as the initial domain controller for RUSSIA.net
- Configure an ONE-WAY (Forest) trust between the domains RUSSIA.net and UAE.net
  - Users from RUSSIA.net must have access to resources from UAE.net but not vice versa

DHCP

- Configure DHCP for the clients
- Mode: Load balancer
- Partner Server: RU-FILES
- State Switchover: 10 minutes
- Range 172.16.0.150-180
- Set the appropriate scope options for both DNS servers and default gateway

DNS

- Configure DNS for RUSSIA.net
- Create a reverse Zone for the 172.16.0.0/24 network
- Add static records for ALL RU-xx servers

GPO

- Disable "first sign in Animation" on all Windows 10 Clients
- Members of the RU-Users_Experts group must be members of the local admin group on all Windows 10 computers in the domain
- www.russia.net must be the default homepage in IE Explorer and Edge browser
  - Install the Windows_10_Creators_Update_ADMX.msi to make Edge group policies available!
- Disable Recycle Bin on the Desktop for all domain users except users in "RU-Users_Experts" Group and domain administrators
- Disable changing the screen saver for all domain users except users in "RU-Users_Experts" Group and domain administrators

- Disable changing the background picture for all domain users except users in "RU-Users_Experts" Group and domain administrators
- Redirect (Folder redirection) only for all users in the Expert group "my Documents" and the "Desktop" to RU-Files -> d:\shares\redirected
  - share path: \\ru-files.russia.net\redirected\%username%
- Create a fine grained password policy required 7 character non-complex passwords for regular users, 8 characters complex password for members of the RU-Users_Experts group
  - Disable “enforce minimum password age”

Users/Groups

- Create OUs named "Expert", "Competitor", "Manager" and "Visitor"
- Create the following AD groups:
  - RU-Users_Experts
  - RU-Users_Competitors
  - RU-Users_Managers
  - RU-Users_Visitors
  - RU-Project_Budget-R
  - RU-Project_Budget-W
  - RU-Project_Intranet-R
  - RU-Project_Intranet-W
  - RU-Project_Logistics-R
  - RU-Project_Logistics-W
  - RU-DAClients

NOTE: This is a required list of groups and OUs that have to be created in the domain. If you believe that you should create additional groups to perform the tasks you can create them.

- Create the users from the excel sheet RU-Users.xlsx (c:\software) on the competitor machine
  - Fill up all fields in the Active Directory user object and add the users to the corresponding RU-Users_xx groups, RU-Project_xx groups and OUs
- Create for every user a home drive in on RU-Files d:\shares\users.
- Connect the home drive automatically to drive U: -> \\ru-files.russia.net\users$\%username%

NOTE: if you are unable to do import all the users from the Excel file create at least the following users manually

Username/Login	Password	Groups
Test_expert	P@ssw0rd	RU-Users_Experts; RU-Project_Budget-R
Test_competitor	P@ssw0rd	RU-Users_Competitors; RU-Project_Intranet-W
Test_manager	P@ssw0rd	RU-Users_Managers; RU-Project_Logistics-W
Test_visitor	P@ssw0rd	RU-Users_Visitors

WORK TASK RU-FILES

This will be the primary file server for the RUSSIA.net domain, but will also provide redundancy for other network services, including DHCP and DNS and AD

Install/Configure

- Install a Windows Server 2016 (no GUI) from ISO
- When creating the VM, build with 4 drives
  - 1 System drive (c:\)
  - Size 25 GB
  - 1 Raid 5 array with the remaining three drives (d:\)
    - Size 10 GB in **total**
- Rename to RU-FILES
- Configure the network settings as per configuration table/network diagram
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to RUSSIA.net domain

Shares

- Create shares for departments (Competitors, Experts and Managers)
- on RU-FILES -> d:\shares\departments
  - \\RU-Files\Experts --> d:\shares\departments\Experts
  - \\RU-Files\Competitors --> d:\shares\departments\Competitors
  - \\RU-Files\Managers --> d:\shares\departments\Managers
- Create a share for projects in RU-FILES -> d:\shares\projects
- Create the following folders in d:\shares\projects
  - Budget
  - Intranet
  - Logistics
- Set the permissions for these folders according to the table in the appendix
- Map the project share (\\ru-files.russia.net\projects) to P:\ for all users except the Visitor group
- Users should see only the folders in P:\ where they have permissions to access them (Access-based Enumeration)

Active Directory

- Promote this server as a DC for RUSSIA.net (but not a GC)

DFS

- Create a Namespace with the name “dfs”
- Add RU-DC as the second server for this Namespace
- Create DFS links for the department shares (Experts, Competitors, Managers)
- Create a DFS Replication to implement a backup of the department shares on RU-DC. The shares should be replicated/backed up like this:
  - RU-Files: D:\shares\departments\Experts → RU-DC: C:\backup\Experts
  - RU-Files: D:\shares\departments\Competitors → RU-DC: C:\backup\Competitors
  - RU-Files: D:\shares\departments\Managers → RU-DC: C:\backup\Managers
- Map the department shares depending on the corresponding group (RU-Users_Experts, RU-Users_Competitors, RU-Users_Managers) to drive G: using the DFS Namespace

DHCP

- Install and configure DHCP
- Mode: Load balancer
- Partner Server: RU-DC
- State Switchover time: 10 minutes

DNS

- Host RUSSIA.net forward and reverse lookup zones

Quota/Screening

- Set the quota to every home drives to 5GB
- Prevent storing .cmd and .exe files on the home drives. All other file extensions are allowed!

Customized error messages

- Make sure that unauthorized users get the following error message, when they want to access one of the three department shares (Experts, Competitors and Managers) they are not allowed to!
    - Expert share:
        - Error message: “Access only for EXPERTS allowed”
    - Competitor share:
        - Error message: “Access only for COMPETITORS allowed”
    - Manager share:
        - Error message: “Access only for MANAGERS allowed”

IIS

- Create a website for the managers (use the provided html file as the default page from C:\software on the competitor computer)
- This website should be accessible via managers.russia.net
- Only users in the in RU-Users_Managers group should have access to the website using "user certificate based authentication"

WORK TASK RU-ROOTCA

This will be the ROOT Certificate authority for the PKI infrastructure.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- DO NOT join this server to any domain

Install AD CS services

- standalone Root CA – Use default key length, hash, etc. if not specified
- Name: RUSSIA Root CA
- Lifetime: 10 years
- CRL location: http://RU-SUBCA.russia.net/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl

- AIA location: http://RU-SUBCA.russia.net/certenroll/<serverdnsname>_<caname><certificatename>.crt
- Create certificate revocation list, and necessary root certificates for RU-SUBCA, and export them to RU-SUBCA, via share or any other method
- Approve subordinate Certificate request from RU-SUBCA
- Take the server offline when not in use (**disable the network interface only**)

WORK TASK RU-SUBCA

This will be the online subordinate CA in the PKI infrastructure.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the machine to the RUSSIA.net domain

Install AD CS and Web Enrolment services

- Install Enterprise Sub CA
- Name: RUSSIA Sub CA
- Import and publish CRL for Root CA
- Lifetime: 5 years
- Configure a template for all clients called "_Skills40_RUClients"
    - Set the "subject name format" to Common Name
    - Auto enroll this template to all RUSSIA.net Windows 10 Clients
- Configure a template for a group of users called "_Skills40_SpecialUsers"
    - Set the "subject name format" to Common Name
    - Auto enroll this template only to the RU-Users_Managers group
- Create the necessary certificates for the two websites on AE-IIS

WORK TASK RU-CLIENT

This is a Windows 10 client in the RUSSIA.net domain and can be used for regular user or administration of the RUSSIA.net servers and test DirectAccess from the "Internet"

Note: Set the power settings to "never sleep" for all Windows 10 clients

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the client to the RUSSIA.net domain
- Install the RSAT tools for server management
- Use this client for testing the DirectAccess connection
- Use this client for testing the GPO settings

NOTE: for testing the Direct Access connection you have to switch this client to the INTERNET Network

Part 2 – UAE.net

In Part 2 you will responsible for making the existing infrastructure available for remote clients, connectivity to the new domain and maintaining the website information for both

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table.
Please use the default configuration if you are not given the details
Local, domain and existing passwords will be "P@ssw0rd"

WORK TASK AE-DC

This is the existing domain controller for the old domain and hosts all the user and group information

Install/Configure

- already preinstalled (domain UAE.net, Users, DNS, DHCP)

Copy Users to Russia.net

- All user with "Expert" in the "Job Title:" should have duplicate accounts created for them in the RUSSIA.net domain (we are not using GPMT – so it is not a migration just a re-creation of the user accounts)
    - Copied Users should be placed to OU "Migration" in RUSSIA.net
    - Set the password to "WorldSkills2018mig"
    - Copy the necessary home folders from AE-DC to RU-FILES d:\shares\migrated
    - Set the necessary permissions on these copied folders/shares (only the user itself and domain administrators should have access to these homefolders)
    - Map the home folder to drive S:\ automatically (\\RU-Files\migrated$\%username%)
    - Disable the copied users in UAE.net and move them to a new OU called MIGRATED on AE-DC

AD

- Create the following three users in OU “Users”. They are necessary for the following work tasks.
    - RDS_user1
    - RDS_user2

Shares

- Create a share for the BitLocker recovery keys.
    - \\AE-DC\bitlocker --> C:\shares\bitlocker

DNS

- DNS records should point to the correct IP addresses for both www.UAE.net and www.RUSSIA.net
- DNS records should point to the correct IP address to the RemoteApp website.

WORK TASK AE-IIS

This server hosts your current UAE.net website and need to have the content for the RUSSIA.net added to your network to provide access to the new RUSSIA.net domain

IIS

- Host www.UAE.net website
    - Move the default website from wwwroot to c:\inetpub\uae
- Host www.RUSSIA.net website (provided) in c:\inetpub\russia

- Both websites should be available by hostname
- Both of these sites should use https using certificate approved in RUSSIA.net

Work Task AE-RDS
This server is used for Published Applications in the UAE.net domain.

Install/Configure

- Install Windows Server 2016 from ISO
- Rename to AE-RDS
- Configure the network settings as per configuration table/network diagram
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to UAE.net domain

Remote Desktop Services

- Install Remote Desktop Services
    - Do not install RD Licensing component.
- Configure web-access for terminal services.
- The RDS login page should be accessible by entering the URL https://rds.uae.net
- On the RU-SUBCA server, generate and use the corresponding SSL certificate for terminal services. Apply this certificate for all components of the terminal services. When connecting to the website https://rds.uae.net from any computer in the UAE.NET domain, the certificate must be trusted and valid (no certificate warning should be shown).
- Make sure, only users RDS_user1 and RDS_user2 are able to login via RDP.
- Publish Wordpad on the web-portal of RemoteApp for the domain user “RDS_user1”
- Publish Notepad on the web-portal of RemoteApp for the domain user “RDS_user2”

WORK TASK AE-CLIENT

Note: Set the power settings to "never sleep" for all Windows 10 clients
Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join the client to the UAE.net domain
- Use this client for all tests in the UAE.net domain

BitLocker

- Encrypt the system drive using BitLocker
- Use the password “P@ssw0rd”
- Save the recovery key in the share \\AE-DC\bitlocker\ on AE-DC with the filename “AE-Client_recovery-key.txt”

WORK TASK AE-REMOTE
Note: Set the power settings to "never sleep" for all Windows 10 clients

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- DO NOT join this client to any domain

VPN

- Configure the VPN client settings for all users on this computer
    - Connect the VPN using the public IP of AE-EDGE
    - Use IKEv2 protocol with machine certificate authentication

Use this client for testing the "external" access to the websites

    - www.russia.net and www.uae.net

Part 3 – INTERNET/VPN/REMOTE ACCESS

In Part 3 you have to setup remote access to the RUSSIA.net domain for the clients, Site-to-Site VPN between the two networks/domains and a client VPN solution for the UAE.net domain.

NOTE: Refer to the diagram on the last page for quick specification reference, as well as the configuration table. Please use the default configuration if you are not given the details

WORK TASK INET

Note: This server has already been preconfigured with all the necessary settings for "simulating the internet in a test lab" and also DHCP is already setup.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic

DNS/IIS

- Create the appropriate resource records (DNS) for external access to the Direct Access server in the RUSSIA.net domain and also for www.UAE.net and www.RUSSIA.net websites access.

WORK TASK AE-EDGE

This is the VPN server that will allow access for external clients to the internal network. It will also create a VPN tunnel to the RUSSIA.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to UAE.net domain
- Install RRAS service
- Install server authentication certificate from RU-SUBCA

NAT configuration

- Port mapping for external access to AE-IIS websites
    - Both RUSSIA.net and UAE.net web content (verify from AE-REMOTE)

VPN

- Configure VPN for client access.
- Use the IKEv2 protocol and make sure authentication is done by client certificate
- Use the IP range 172.19.0.50 – 172.19.0.79
- The VPN clients should have access to all internal networks (UAE.net and RUSSIA.net)

Site-to-Site VPN

- Configure Site-to-Site VPN to RU-EDGE server
- Use machine certificate for the authentication
- Set the connection type to “persistent connection”
- All traffic bound for RUSSIA.net will be placed in the VPN tunnel

WORK TASK RU-EDGE

This is the VPN and DirectAccess server that will allow access for external clients to the internal network. It will also create a VPN tunnel to the old UAE.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to RUSSIA.net domain
- Install server authentication certificate from RU-SUBCA

Configure Direct Access

- Add RU-Client to the AD group "RU-DAClients"
- Only members of "RU-DAClients" group can use remote connection
- Use RU-FILES server as the only NCA
- Generate SSL certificate on the PKI and use it for client connections (no self-signed certs are allowed)
- DirectAccess connection name "my W@rkplace"
- Use connect.russia.net for the access from the internet
- The DA clients must get full access to the resources of RUSSIA.net network and UAE.net

Site-to-Site VPN

- Configure Site-to-Site VPN to the AE-EDGE server
- Use machine certificate for the authentication
- Set the connection type to “persistent connection”
- All traffic bound for UAE.net will be placed in the VPN tunnel

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
AE-DC	Windows Server 2016 GUI	UAE.net	172.19.0.1/24	Yes - configured
AE-CLIENT	Windows 10	UAE.net	DHCP	Yes - configured
AE-IIS	Windows Server 2016 no GUI	UAE.net	172.19.0.3/24	Yes - configured
AE-RDS	Windows Server 2016 GUI	UAE.net	172.19.0.2	NO
AE-EDGE	Windows Server 2016 GUI	UAE.net	172.19.0.250/24 200.100.50.101/24	Yes - configured
RU-DC	Windows Server 2016 GUI	Russia.net	172.16.0.1/24	Yes - configured
RU-FILES	Windows Server 2016 no GUI	Russia.net	172.16.0.2/24	NO
RU-ROOTCA	Windows Server 2016 GUI	None	172.16.0.3/24	Yes - configured
RU-SUBCA	Windows Server 2016 GUI	Russia.net	172.16.0.4/24	Yes - configured
RU-EDGE	Windows Server 2016 no GUI	Russia.net	172.16.0.250/24 200.100.50.100/24	Yes - configured
RU-CLIENT	Windows 10	Russia.net	DHCP	Yes - configured
AE-REMOTE	Windows 10	None	DHCP	Yes - configured
INET	Windows Server 2016 GUI	None	200.100.50.200/24	Yes - configured

Machines indicated as being preinstalled with "**Yes – configured**" will have the operating system installed and Hostname and network settings configured.

Shares/Permission Table

Sharename	Location	Read access group	Read/Write access group
Budget	RU-Files -> D:\shares\projects	RU-Budget-R	RU-Budget-W
Intranet	RU-Files -> D:\shares\projects	RU-Intranet-R	RU-Intranet-W
Logistics	RU-Files -> D:\shares\projects	RU-Logistics-R	RU-Logistics-W

WS-TASK-C: Network Cisco Environment

Description of project and tasks

This test project is designed using a variety of network technologies that should be familiar from the Cisco certification tracks. Tasks are broken down into following configuration sections:

- Basic configuration
- Switching
- WAN
- Routing
- Services
- Security
- Monitoring and backup
- WAN and VPN

All sections are independent but all together they build very complex network infrastructure. Some tasks are pretty simple and straightforward; others may be tricky. You may see that some technologies are expected to work on top of other technologies. For example, IPv6 routing is expected to run on top of configured VPNs, which are, in turn, expected to run on top of IPv4 routing, which is, in turn, expected to run on top of PPPoE, and so on. It is important to understand that if you are unable to come up with a solution in the middle of such technology stack it doesn't mean that the rest of your work will not be graded at all. For example, you may not configure IPv4 routing that is required for VPN because of IP reachability but you can use static routes and then continue to work with VPN configuration and everything that runs on top. You won't receive points for IPv4 routing in this case but you will receive points for everything that you made operational on top as long as functional testing is successful.

Instructions to the Competitor

It is very important to read the whole test project first. However, be aware that not all tasks are written in chronological order. Some sections may require configuration from other sections below them. For example, task 6 in the "Basic configuration" section asks you to configure authentication using RADIUS server which obviously will not work if you do not apply all necessary configurations from the "Switching configuration" section that comes right after. It is your responsibility to manage your time effectively and the sequence you decide to complete the tasks.

As mentioned above, do not waste your time if you're stuck with some tasks. You can use temporary solution (if you have technology stack dependency) and continue to work with other tasks, this may allow you to go back afterwards and fix things that are not working properly if you still have time. In addition, we recommend that you to check all your previous work when you complete following modules.

The RADIUS server is already preconfigured with rsyslog, freeradius, tftpd and snmpd to save your time, you are only required to complete the necessary configuration from your side.

Equipment, machinery, installations, and materials required

It is expected that all Test Projects can be completed by Competitors based on the equipment and materials specified in the Infrastructure List.

Marking Scheme

Marking scheme is designed in the way that every configuration aspect is graded only once. For example, in the "Basic configuration" section you are required to configure hostnames for all devices but it will be checked on only one device and graded only once. The same configuration aspect may be checked and graded more than once if it's done with different configuration options for different devices or for different device classes. For example, in the "Basic configuration" section you are required to configure local AAA model for all devices but it differs for BR3 router and FW1, FW2 firewalls.

Any details about how and from which exact devices experts will perform checking and grading of your work are contained in "How to Mark" document. These details are subject to 30% changes as well as the aspects in marking scheme.

NOTE: Refer to the diagram on the last page for quick specification reference.
Please use the default configuration if you are not given the details.
All user account on ALL machines should have a password of Skill39 unless otherwise specified. Pre-supplied virtual machines that the competitor needs to logon to will also be pre-configured with this password.
Use the default account and password for Cisco VIRL.

All supplied software and files needed to complete this project can be found in the software.iso file in the datastore.

You are reminded to extract configuration in VM Maestro before you leave the competition site.

Network island Task

Basic configuration

1. Configure hostnames for ALL devices as you see on the topology
2. Configure domain name **wsi2018.com** for ALL network devices on the topology
3. Create user **wsc2018** with password **cisco1** on ALL devices
    a. Only scrypt hash of the password should be stored in configuration. (This requirement only applies to the routers and switches, NOT the ASA Firewalls)
    b. User should have maximum privileges.
4. Configure new AAA model for ALL devices.
    a. Remote console (vty) authentication should use local username database.
    b. After successful authentication on vty line users should automatically land in privileged mode (except for FW1 and FW2).
    c. Enable login authentication on local console.
    d. After successful authentication on local console user should land in user mode with minimal privileges (privilege level 1).
    e. After successful authentication on local console of BR3 router user should automatically land in privileged mode with maximal privileges.
5. Configure RADIUS authentication for all remote consoles (vty) on HQ1 router.
    a. Authentication sequence:
        i. RADIUS server
        ii. Local username database
    b. Use “cisco1” as the shared key.
    c. Use port numbers 1812 for authentication and 1813 for accounting.
    d. IP address of the RADIUS server is 192.168.10.10
    e. Configure automatic authorization — after successful authentication on RADIUS server user should automatically land in privileged mode with maximal privileges.
    f. Test RADIUS authentication using **radius**/**cisco1** credentials.
6. Configure **wsi** as a privileged mode password for ALL devices.
    a. Password should be stored in configuration in plain text (not in hash), except for FW1 and FW2.
    b. Configure privileged mode authorization on FW1 and FW2. When entering privileged mode, authenticated username should be used automatically (no username prompt) and only password of authenticated user should be prompted. For example:

```
#Connect to FW1 using SSH or Console
Username: wsc2018
Password: cisco1
Type help or '?' for a list of available commands.
FW1> enable
```

```
Password: cisco1
FW1#
```

c. Set the mode where all the passwords in the configuration are stored as a reversible cipher text.

7. Create all necessary interfaces, subinterfaces and loopbacks on ALL devices. Use IP addressing according to the L3 diagram.
    a. Use VLAN101 as a virtual interface for SW1, SW2 and SW3 switches. Use IP address 192.168.10.51 for SW1, 192.168.10.52 for SW2 and 192.168.10.53 for SW3.
    b. For HQ1 and HQ2 use automatic IPv6 addresses generation (EUI-64) for LAN1 subnet.
8. ALL devices should be accessible using SSH protocol version 2. For FW1 and FW2, allow SSH connection on the "inside" interface.
9. Configure current local time zone (GST/GMT +4) on HQ1 router.

Switching configuration

1. Configure VTP version 2 on SW1, SW2 and SW3. Use SW3 as VTP server, SW1 and SW2 as clients. Use **WSI** as VTP domain name and **2018** as a password. VLAN database on all switches should contain following VLANs:
    a. VLAN 101 with name LAN1.
    b. VLAN 102 with name LAN2.
    c. VLAN 103 with name EDGE.
2. On SW1, SW2 and SW3 switches configure dynamic trunking protocol:
    a. For Gi1/1-2 ports on SW3 switch configure mode that will listen for trunk negotiation but won't initiate it itself.
    b. For Gi1/1 ports on SW1 switch and for Gi1/2 ports on SW2 switch configure mode that will initiate trunk negotiation.
    c. Configure ports Gi0/1-3 on SW1 and SW2 for traffic transmission using IEEE 802.1q protocol.
3. Configure link aggregation between switches SW1 and SW2. Use following port-channel number 1.
    a. SW1 switch should use PAgP desirable mode.
    b. SW2 switch should use PAgP auto mode.
4. Configure spanning tree protocol:
    a. For ALL switches use STP protocol version which is compatible with 802.1w standard.
    b. SW1 switch should be STP root in VLAN 101. In case of SW1 failure, SW2 should become a root.
    c. SW3 switch should be STP root in VLAN 102. In case of SW3 failure, SW1 should become a root.
    d. SW2 switch should be STP root in VLAN 103. In case of SW2 failure, SW3 should become a root.
    e. For traffic transmission in VLANs 101, 102 and 103 on SW1 and SW2 use ports that are not participating in channel-groups.
5. Turn on security mechanism that prevents STP root change on SW1 port which is connected to RADIUS VM. In case a superior BPDU arrives on this port, the port should transfer to root-inconsistent state.
6. Configure port on SW2 switch which is connected to PC1 VM so that it goes to Forwarding state without waiting for STP recalculation.
7. LAN1 subnet traffic between HQ1 router and SW3 switch should be forwarded without IEEE 802.1q tag.

Routing configuration

1. Configure EIGRP with AS number 2018 on ISP, HQ1, HQ2, BR2 and BR3 routers according to the routing diagram. Enable routing updates authentication. Use MD5 algorithm with **WSI** key.
2. Configure BGP on ISP, HQ1, HQ2, BR2 and BR3 according to the routing diagram.
    a. Routers HQ1 and HQ2 should exchange routing updates using iBGP
    b. Configure route filtering so that route 209.136.0.0/16 won't be present in routing table on HQ1 router.
3. Configure OSPFv2 on HQ1, HQ2, BR2, BR3 routers and FW1, FW2 firewalls according to the routing diagram.
4. Configure OSPFv3 on HQ1, HQ2, BR2 and BR3 routers according to the routing diagram. Router HQ1 should be configured as DR, HQ2 — as BDR.
5. On BR2 router configure OSPF route redistribution for Loopback30 subnet into EIGRP AS 2018.
6. Configure routing policy on HQ1 router so that ICMP and UDP traffic from Loopback101 subnet to Loopback30 subnet goes through ISP router.

Services configuration

1. Configure dynamic port translation on HQ1 and HQ2 routers for LAN1 subnet so that all internal IPv4 addresses are translated into IPv4 address of the interface which is connected to the INET11 and INET22 subnets respectively.
2. Configure first-hop redundancy protocols on HQ1 and HQ2 routers:
    a. Configure GLBP group for LAN1 subnet:
        i. Group number 101
        ii. Use 192.168.10.252 as the virtual IP address
        iii. Configure priority 151 for HQ1 router and 101 for HQ2 router.
    b. Configure HSRP group for LAN2 subnet:
        i. Group number 201
        ii. Use 192.168.20.252 as the virtual IP address
        iii. Configure priority 121 for HQ1 router and 111 for HQ2 router.
        iv. Configure MD5 authentication. Key string is "cisco1"
3. Configure DHCP using following parameters:
    a. On HQ1 router for LAN subnet:
        i. Network address — 192.168.10.0/24;
        ii. Default gateway — virtual IP address of GLBP group;
        iii. DNS server — 192.168.10.10;
        iv. Exclude first 50 usable addresses from DHCP pool.
        v. DHCP server should assigned 192.168.10.10 to the "RADIUS" server.
        vi. Make sure "RADIUS" server and "PC01" are configured as DHCP clients.

Security configuration

1. Configure role-based access control on BR3 router:
    a. Create **user1**, **user2**, **user3**, **user4** and **user5** with **cisco1** password.
        i. **user1** should be authorized to issue all privileged mode commands except "**show version**" and "**show ip route**" but should be able to issue "**show ip ***" commands.

ii. **user2** should be authorized to issue all user (unprivileged) mode commands including "**show version**" but not "**show ip route**".

b. Create view-context "**show_view**":
   i. Include "**show version**" command
   ii. Include all unprivileged commands of "**show ip ***"
   iii. Include "**who**" command
   iv. **user3** should land in this context after successful authentication on local or remote console.

c. Create view-context "**ping_view**":
   i. Include "**ping**" command
   ii. Include "**traceroute**" command
   iii. **user4** should land in this context after successful authentication on local or remote console.

d. Create superview-context that combines these 2 contexts. **user5** should land in this superview-context after successful authentication on local or remote console.

e. Make sure that users cannot issue any other commands within contexts that are assigned to them (except show banner and show parser, which are implicitly included in any view).

2. On port of SW2 switch which is connected to PC1 VM enable and configure port-security using following parameters:
   a. Maximum MAC addresses — 2
   b. MAC addresses should be automatically saved in running configuration.
   c. In case of policy violation, security message should be displayed on the console; port should not go to err-disabled state.
3. Turn on DHCP snooping on SW1 switch for LAN1 subnet. Use internal flash to keep DHCP-snooping database.
4. Turn on dynamic ARP inspection on SW1 for LAN1 subnet. Create access control list that permits static IP address 192.168.10.10 for RADIUS server.

Monitoring and backup configuration

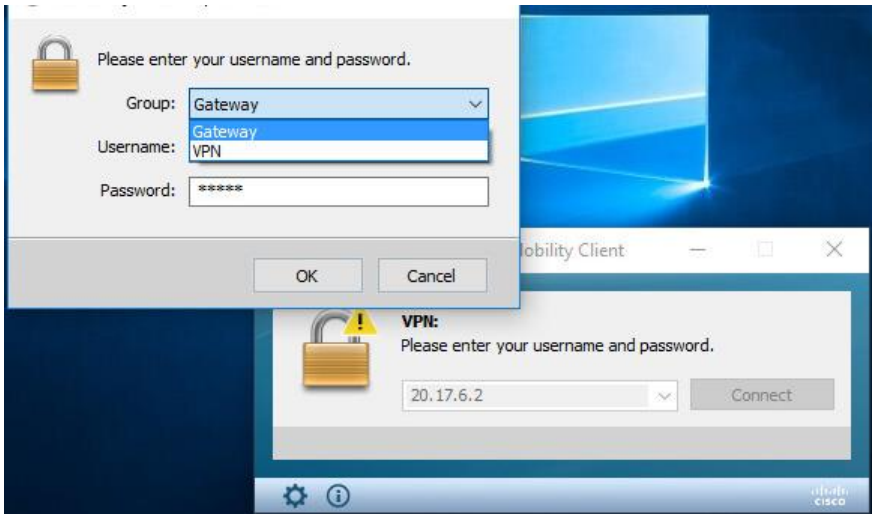
1. Configure logging of system messages on HQ1 router and FW1 firewall. All logs including informational messages should be sent to the RADIUS server (location **/var/log/hq1.log** and **/var/log/fw1.log**).
2. Configure SNMP v2c on HQ1 router and FW1 firewall:
   a. Use read-only community string **snmp_ro**
   b. Configure device location **Abu-Dhabi, UAE**
   c. Configure system contact **admin@wsi.org**
3. Configure configuration backup on HQ1 router:
   a. Backup copy of running configuration should be automatically saved on RADIUS server using TFTP each time configuration is saved (copied to startup);
   b. Use following naming convention for backup files: <hostname>-<time>.cfg
   c. Location for configuration backup files is **/srv/tftp/** on RADIUS server

WAN & VPN configuration

1. Configure ISP router as PPPoE server and BR3 router as PPPoE client. Use PAP for authentication with **papuser\cisco1** credentials.
2. Configure DMVPN on HQ1, HQ2, BR2 and BR3 routers:
   a. Use Tunnel100 as VTI for all routers;

b. Configure MTU 1400 on all VTIs;
c. Configure IP addressing according to the VPN-diagram;
d. Use GRE Multipoint mode;
e. Use Loopback interface as tunnel source interface on each router according to the VPN-diagram;
f. NHRP configuration:
    i. Network ID — **100**
    ii. Authentication key — **wsi2018**
g. Use HQ1 router as DMVPN hub NHS server;
h. Spoke routers should not use hub router for traffic transmission between each other;

3. Configure IKEv2 IPsec Site-to-Site VPN on FW1, FW2 firewalls:
    a. Phase 1 parameters:
        i. Hash – MD5
        ii. Encryption – AES-128
        iii. DH group – 5
        iv. Authentication – pre-shared key (**cisco1**)
    b. Phase 2 parameters:
        i. Protocol – ESP
        ii. Encryption – AES-128
        iii. Hash – MD5
    c. For transmission through IPsec tunnel permit all TCP traffic from network of IP address of HQ2 subinterface in LAN2 subnet to network of IP address of BR2 interface in LAN3 subnet.
4. Configure SSL VPN server on FW2 firewall:
    a. Create local user **vpnuser** with **cisco1** password.
    b. Users should be able to connect using AnyConnect client. Deployment package is located on PC1 desktop.
    c. Create VPN address pool using following addresses: 10.255.255.1 - 10.255.255.30
    d. Create two tunnel groups — VPN and Gateway. After connection on login prompt user should be able to choose tunnel group from drop-down menu as shown on the picture below.
    e.



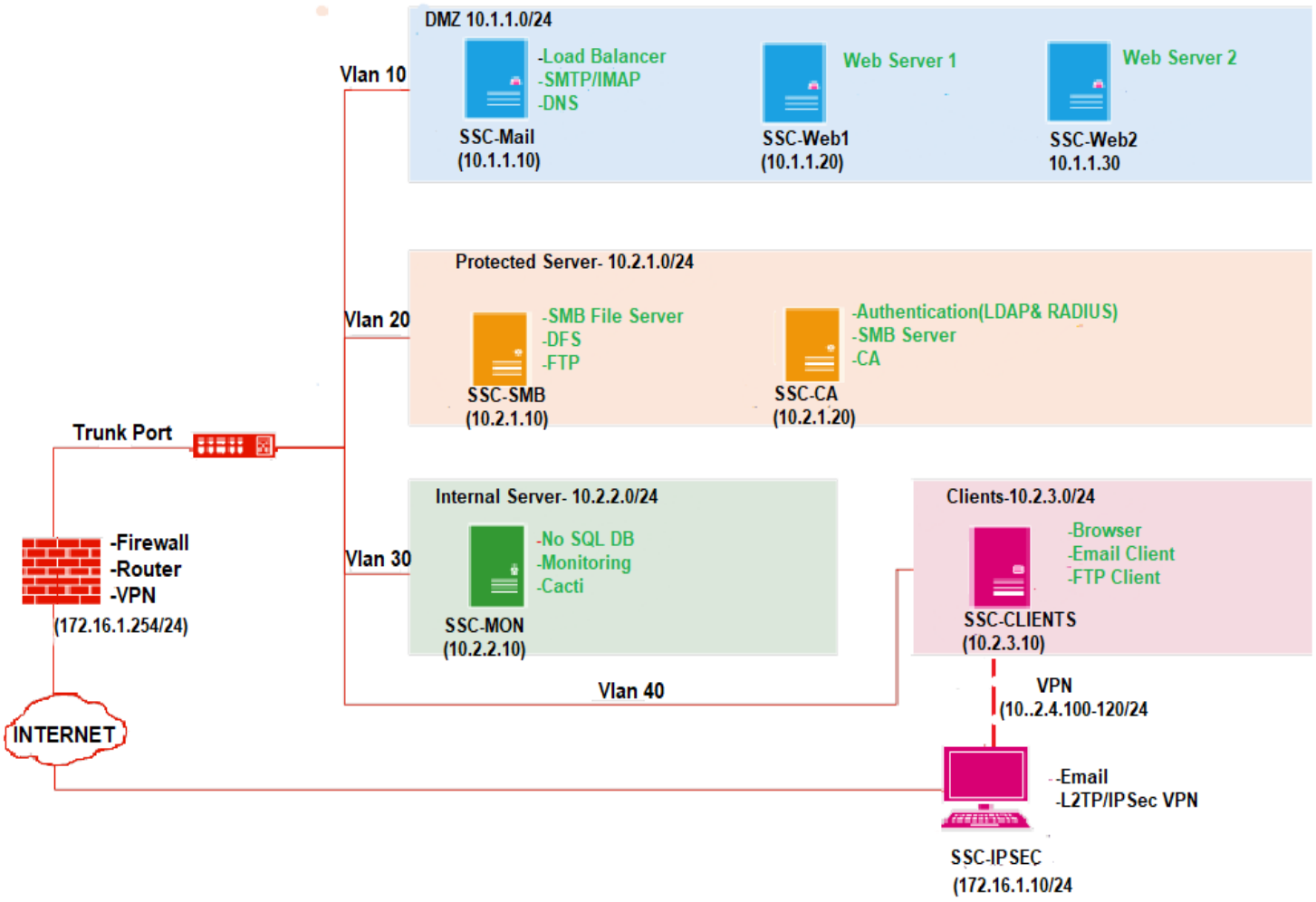
f. When choosing **VPN** profile client should receive secure-route list, which contains only route to Loopback20 subnet.

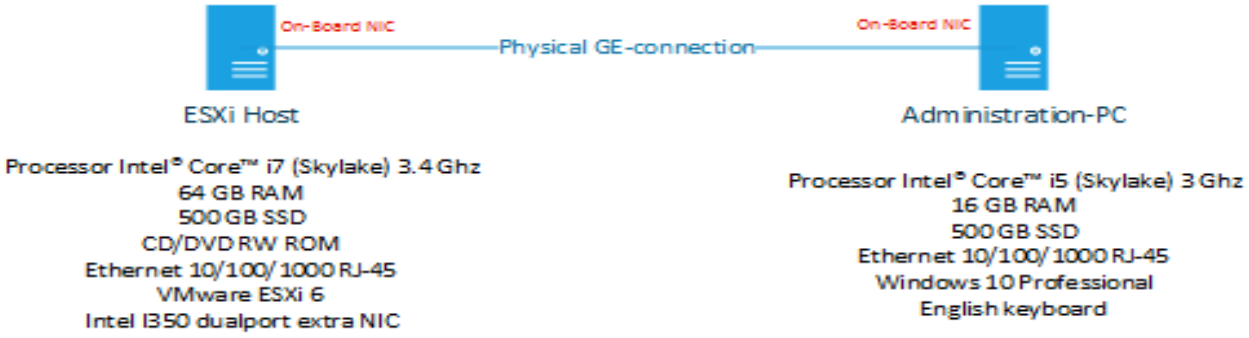
g. When choosing **Gateway** profile all traffic should be tunneled through SSL VPN tunnel.

d. When connecting from PC1, IP address of Loopback20 should be accessible for ICMP echo requests (using any connection profile).

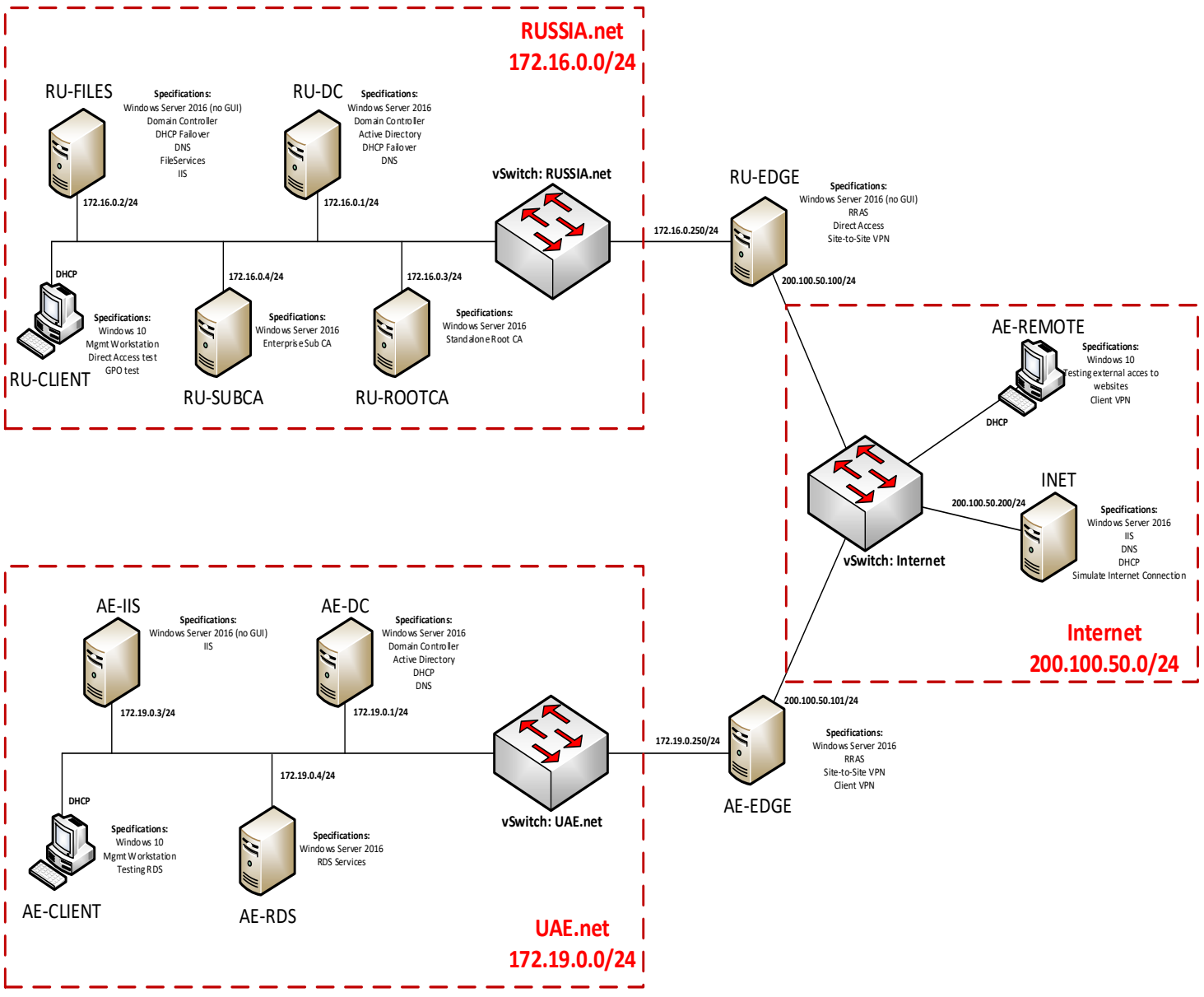
Section B-Network Infrastructure Design (Tool and Equipment Including Raw Material)

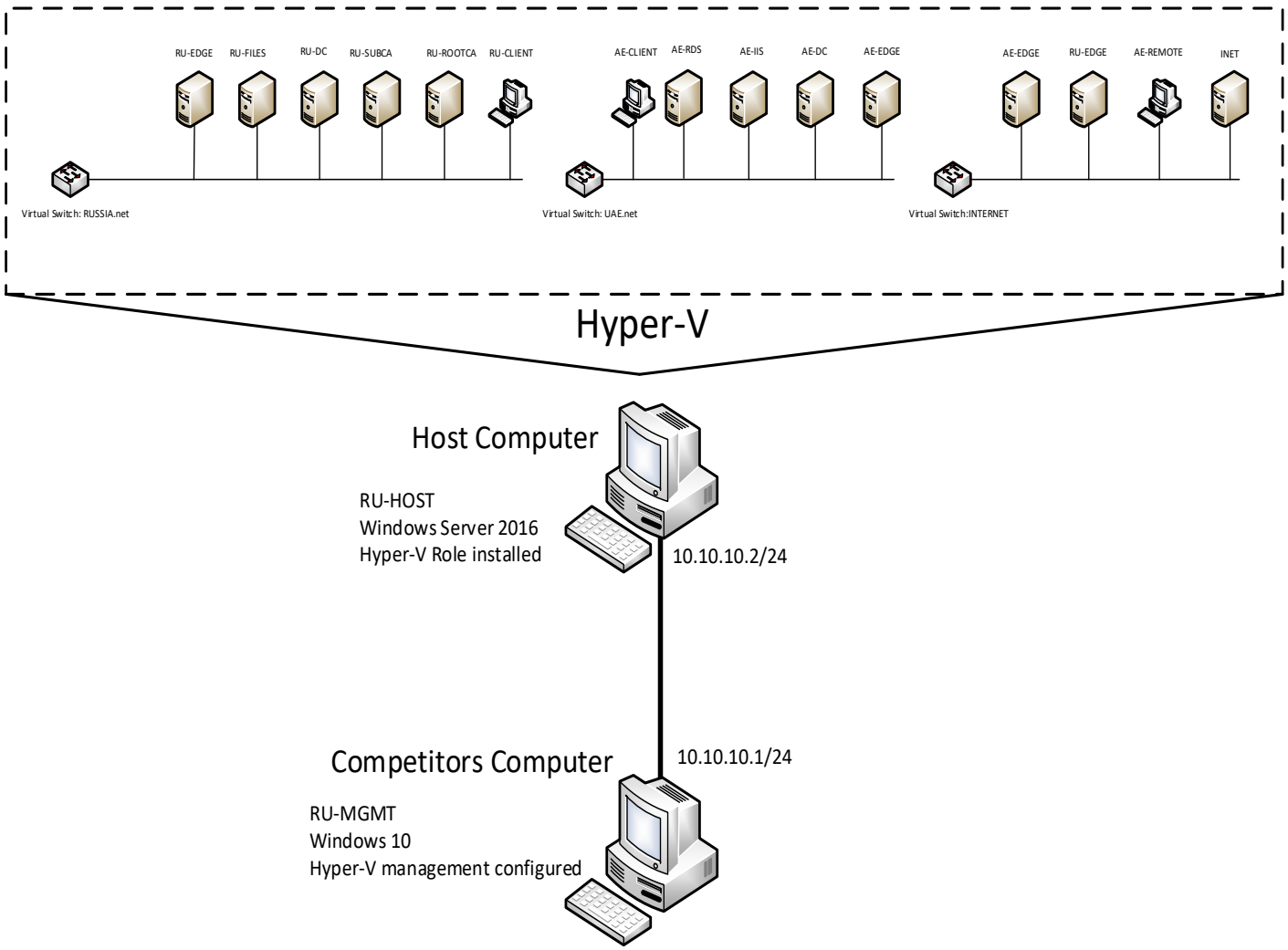
WS-Task A: Network Diagram





WS-TASK-B: Network Diagram





Equipment, Machinery, Installations and Materials Required

Standard/Administration-PC

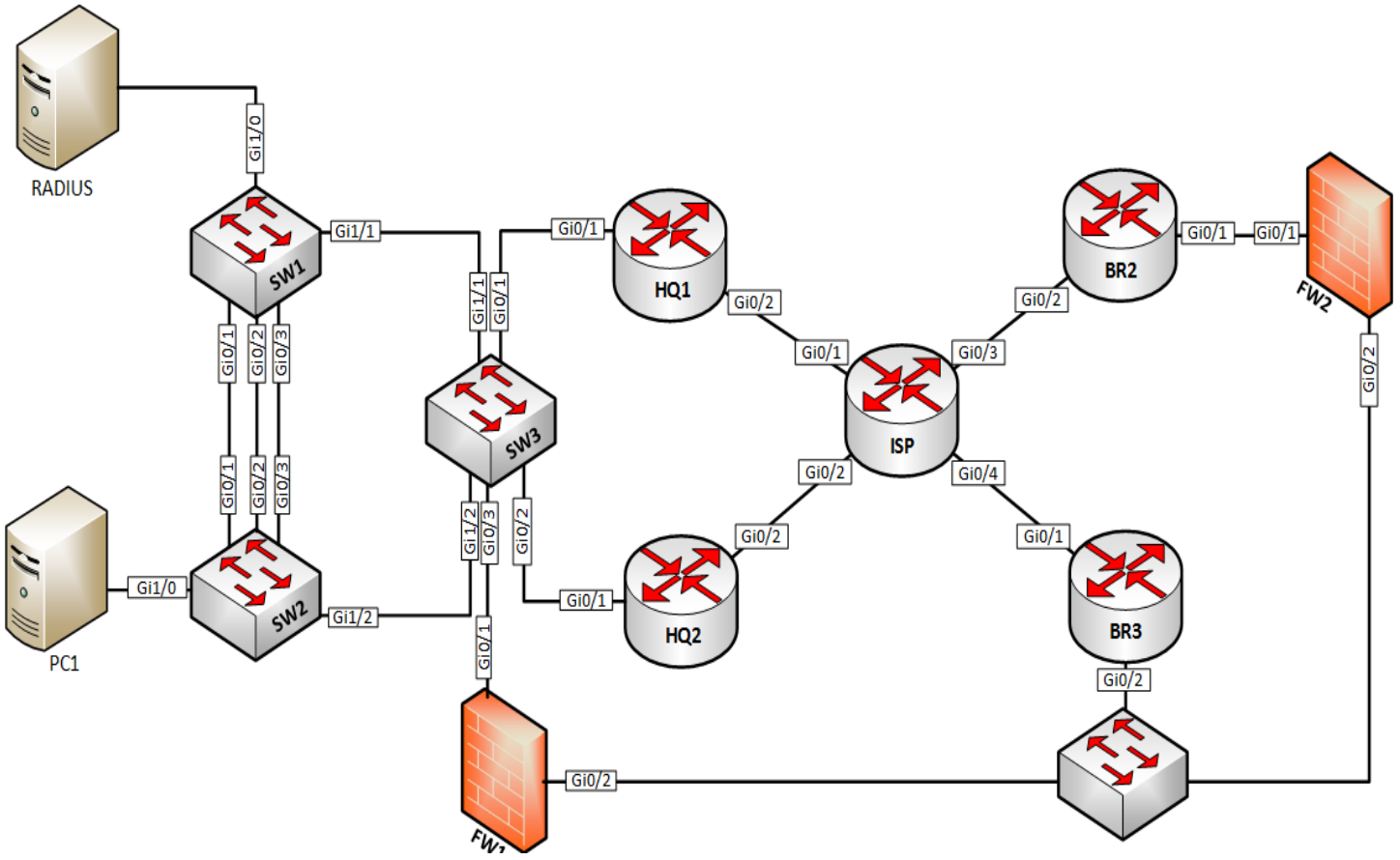
- Intel i5 processor
- 16GB RAM
- 500GB SSD-Drive
- 1x24 inch LED-Monitors
- US Keyboard
- Mouse

Highspec/Host-PC

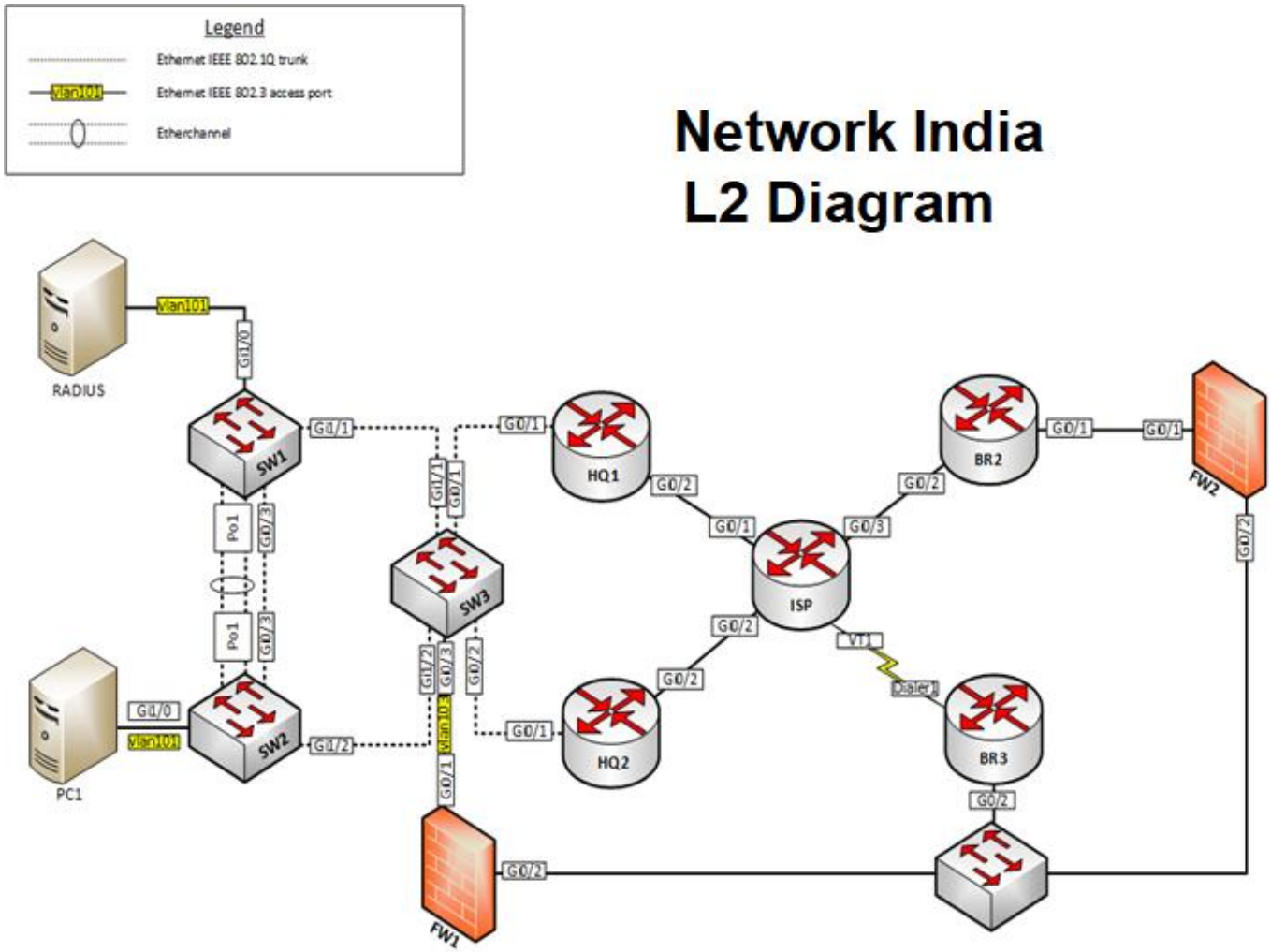
- Intel i7 processor
- 64GB RAM
- 500GB SSD-Drive
- 1x24 inch LED-Monitor
- US Keyboard
- Mouse

WS-TASK-C: NETWORK DIAGRAM

NETWORK INDIA
L1 DIAGRAM

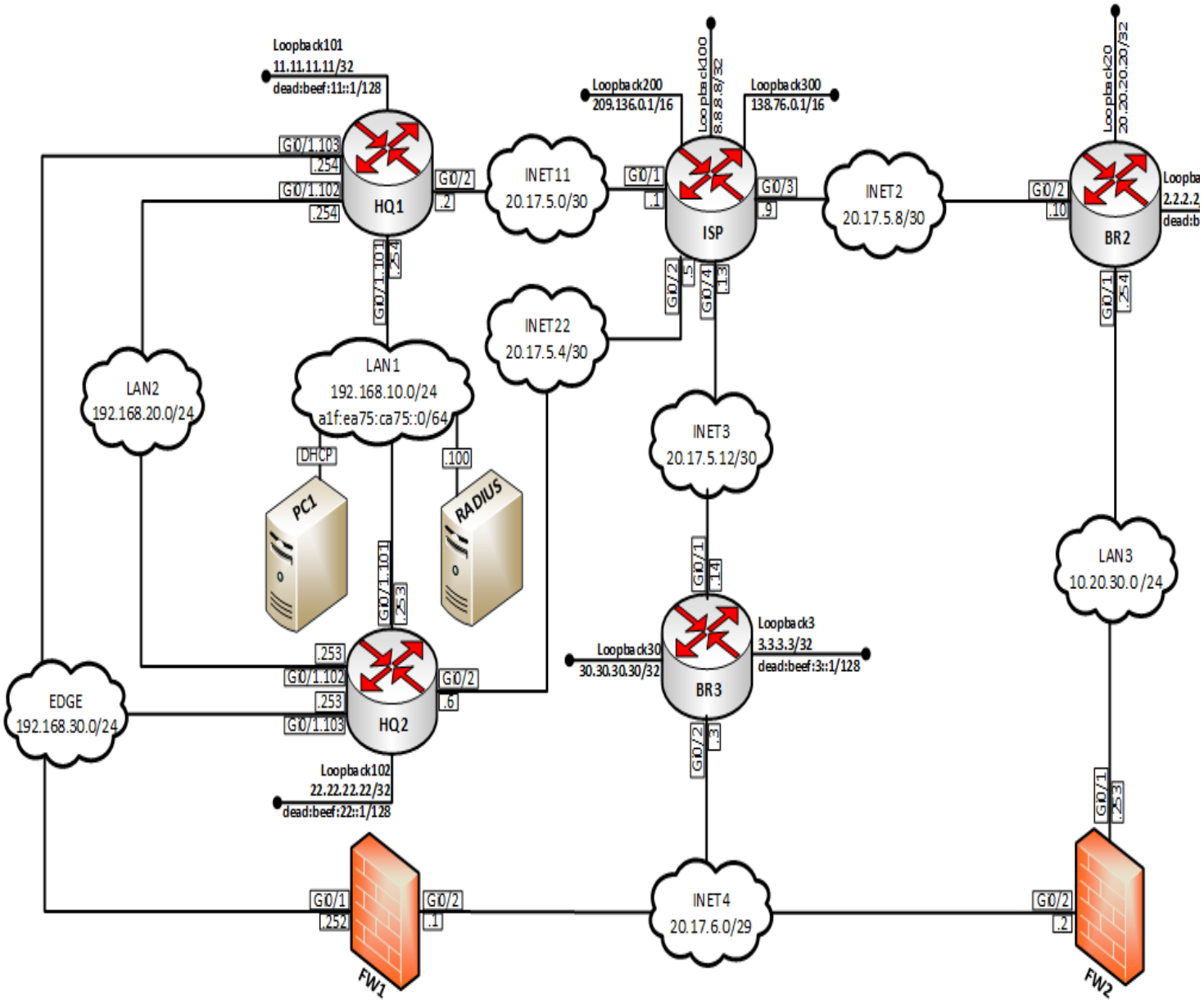


Network India
L2 Diagram

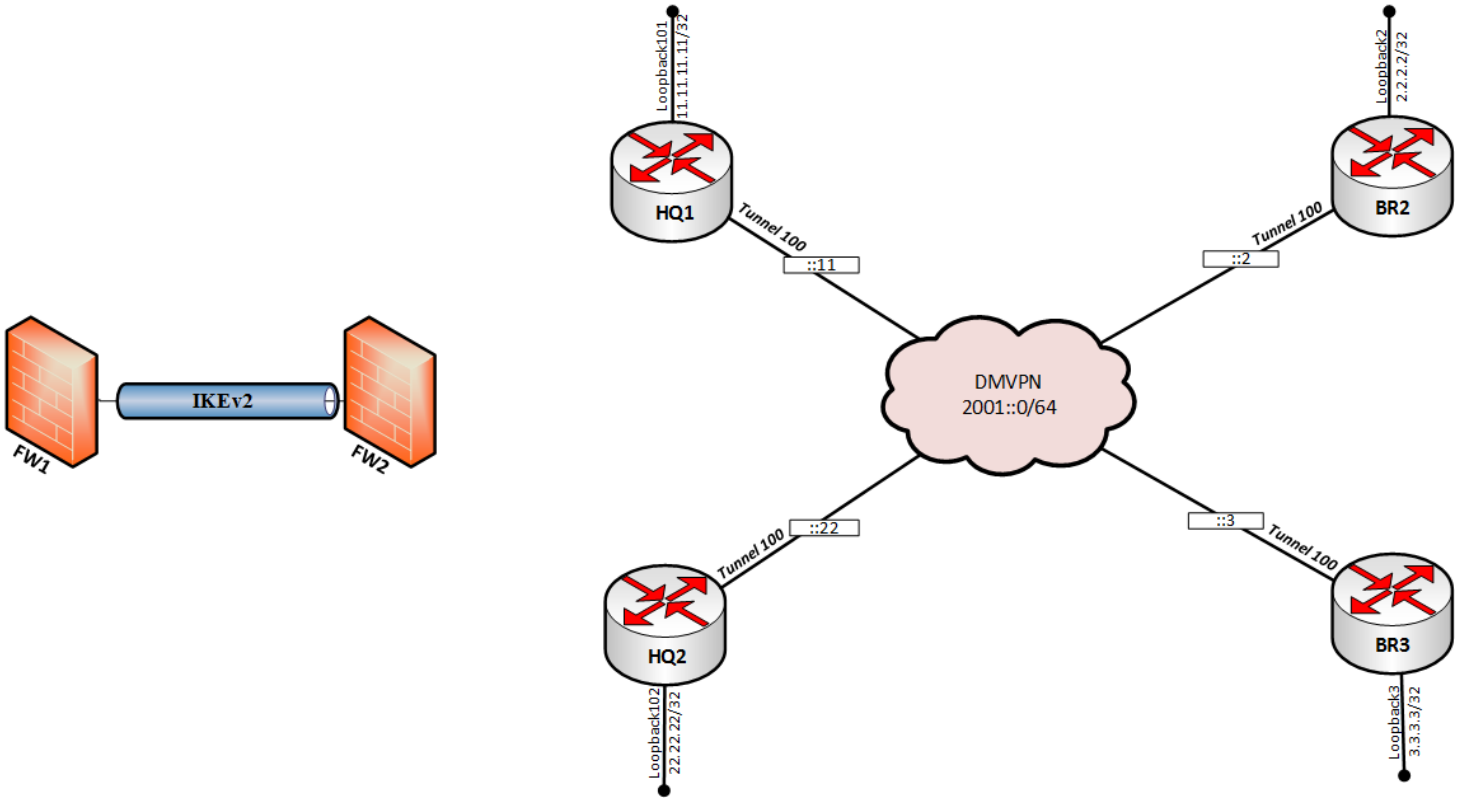


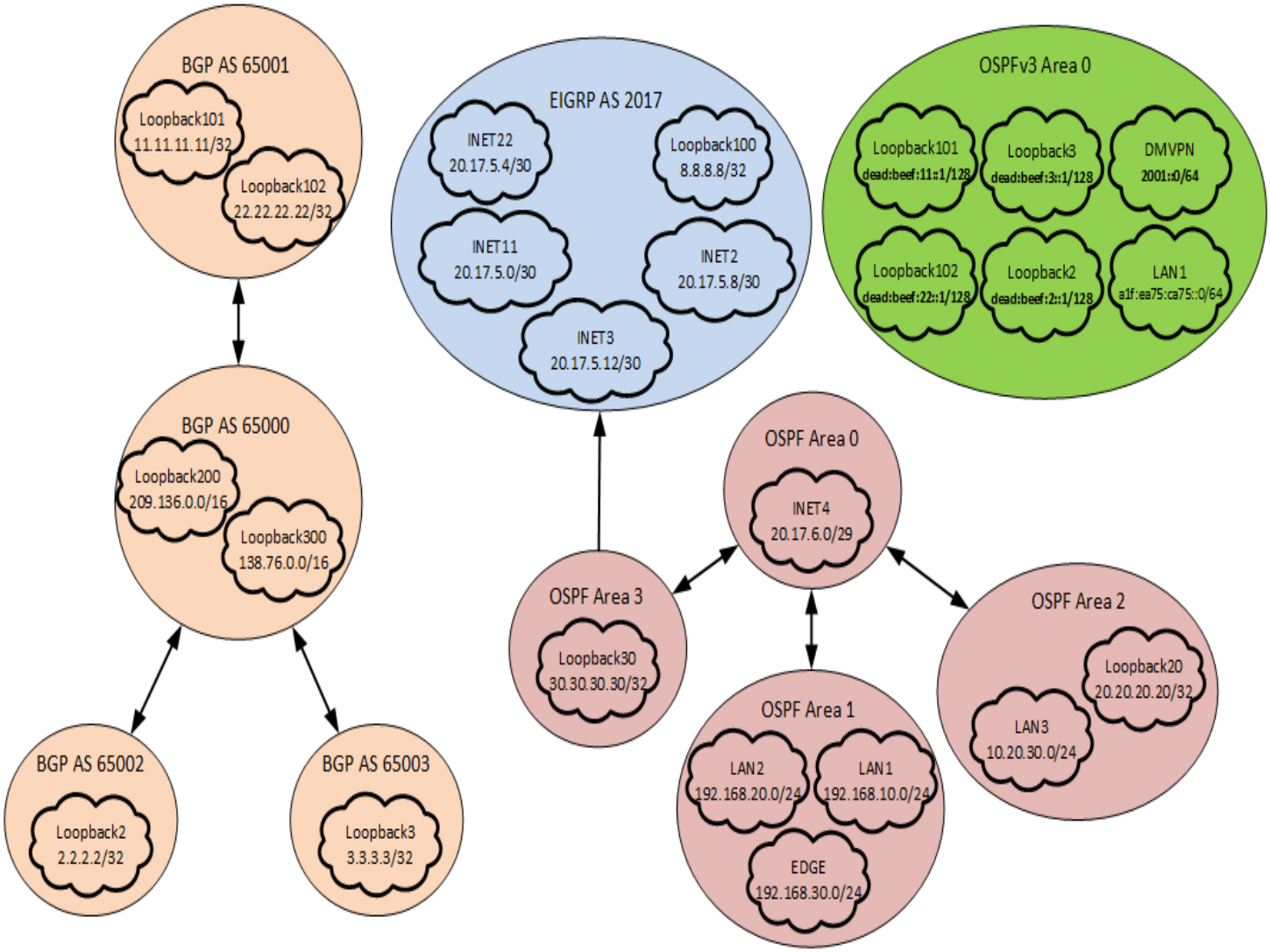
Network India

L3 Diagram



Network Island.
WAN & VPN diagram




BGP AS 65001
Loopback101
11.11.11.11/32
Loopback102
22.22.22.22/32
BGP AS 65000
Loopback200
209.136.0.0/16
Loopback300
138.76.0.0/16
BGP AS 65002
Loopback2
2.2.2.2/32
BGP AS 65003
Loopback3
3.3.3.3/32
EIGRP AS 2017
INET22
20.17.5.4/30
Loopback100
8.8.8.8/32
INET11
20.17.5.0/30
INET2
20.17.5.8/30
INET3
20.17.5.12/30
OSPFv3 Area 0
Loopback101
dead:beef:11::1/128
Loopback3
dead:beef:3::1/128
DMVPN
2001:0/64
Loopback102
dead:beef:22::1/128
Loopback2
dead:beef:2::1/128
LAN1
a1f:ea75:ca75::0/64
OSPF Area 0
INET4
20.17.6.0/29
OSPF Area 3
Loopback30
30.30.30.30/32
OSPF Area 2
Loopback20
20.20.20.20/32
LAN3
10.20.30.0/24
OSPF Area 1
LAN2
192.168.20.0/24
LAN1
192.168.10.0/24
EDGE
192.168.30.0/24

Section C: Network Infrastructure Design & configuration (Tool and equipment including raw material)

WS-TASK A: Configuration Table

HOSTNAME	OPERATION SYSTEM	DOMAIN	IP ADDRESS(ES)	PREINSTALLED
DMZ Zone (10.1.1.0/24)				
SSC-Mail	Linux Server	India-east.cLoud	10.1.1.10/24	Yes – configured
SSC-Web1	Linux Server	India-east.cLoud	10.1.1.20/24	Yes – configured
SSC-Web2	Linux server	India-east.cLoud	10.1.1.30/24	Yes – configured
Protected Server (10.2.1.0/24)				
SSC-SMB	Linux Server	India-east.cloud	10.2.1.10/24	Yes – configured
SSC-CA	Linux Server	India-east.cloud	10.2.1.20/24	Yes – configured
Internet Server (10.2.2.0/24)				
SSC-MON	Linux Server	India-east.cLoud	10.2.2.10/24	Yes – configured
SSC-Clients	Linux Client	India-east.cLoud	10.2.2.20/24	Yes – configured
Internet (172.16.1.0/24)				
SSC-Firewall	Firewall		10.1.1.1/24 (VLAN10) 10.2.1.1/24 (VLAN20) 10.2.2.1/24 (VLAN30) 10.2.3.1/24 (VLAN40) 10.2.4.100-120 (VPN) 172.16.1.254/24 (Internet)	Yes – configured
SSC-IPSEC	Linux Server	India-east.cloud	172.16.1.10/24(Internet) 10.2.4.1xx/24 (VPN)	Yes – configured

LDAP Users

USERNAME	OU	PASSWORD	DOMAIN
user1	VPN	Skills18	India-east.cloud
user2	VPN	Skills18	India-east.cloud
user3	MAIL	Skills18	India-east.cloud
user4	MAIL	Skills18	India-east.cloud
user5	SSC-SMB	Skills18	India-east.cloud
user6 – user99	MISC	Skills18	India-east.cloud
Competitor	MAIL	Skills18	competition.in

DNS

Nameserver address should be equal on all hosts (except on the DNS server itself, which instead uses localhost) and point to the same address as the gateway.

If you are unable to setup SSC-Firewall properly, use the direct IP address of SSC-mail and adjust firewall accordingly. You will lose those points.

Section C-Marking Scheme

SSC-TASK A Network Linux Environment

Aspect ID	Marking Criteria or Description	Requirement	Max Mark	Mark Awarded
SSC-Mail				
1.1	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.2	HAproxy load balancing		0.5	
1.3	Forwardzone: india-east.cloud		0.5	
1.4	A records for india-east.cloud		0.5	
1.5	A record, DNS Reverse		0.5	
1.6	Mail directory		0.5	
1.7	LDAP User not local		0.5	
1.8	Certificates SMTPS e IMAPS		0.5	
1.9	FTP enabled only		0.5	
1.10	Firewall clients network SNAT not working from another networks		0.5	
SSC-Web1				
1.11	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.12	Rsync script and working		0.5	
Webserver				
1.13	Apache HTTPS-only	Debian Linux For all Server and Client	0.5	
1.14	Apache / PHP		0.5	
1.15	WWW Subfolder		0.5	
1.16	Subfolder authentication		0.5	

SSC-Web2				
1.17	Basic Configuration (Hostname, IP, Banner,Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.18	Basic Configuration (Hostname, IP, Banner,Keyboard, Locale, Curl and SSH)		0.5	
1.19	Root login and LDAP Users		0.5	
1.20	SSH Login permissions		0.5	
1.21	RAID 5		1	
1.22	Samba – Login		0.5	
1.23	Samba - Home directory restriction		0.5	
1.24	DFS configured for \\WSC-I-LONDON\dfs		0.5	
1.25	FTP - Virtual user, session		0.5	
SSC-MON				
1.26	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.27	Update script schedule		0.5	
1.28	Listing Script		0.5	
1.29	Cacti installed and collecting data		0.5	
SSC-Clients				
1.30	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.31	Icedove configuration		0.5	
1.32	Icedove sending & receiving		0.5	
1.33	Firefox website		0.5	
1.34	FileZilla connection		0.5	
1.35	Only users in OU Mail can authenticate		0.5	
1.36	DFS accessible		0.5	
1.37	Share is not visible		0.5	
1.38	Firewall all client sourced traffic allowed		0.5	
1.39	Firewall ICMP ping allowed to local machine		0.5	
SSC-Clients				
1.40	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.41	Icedove configuration		0.5	
1.42	VPN is connected		0.5	

1.43	VPN start/stop script		0.5	
1.44	VPN IP-range		0.5	
1.45	VPN services		0.5	
1.46	VPN authentication		0.5	
1.47	VPN Certificate		1	
SSC-Firewall				
1.48	Basic Configuration (Hostname, IP, Banner, Keyboard, Locale, Curl and SSH)	Debian Linux For all Server and Client	0.5	
1.49	Routing enabled		0.5	
1.50	VLAN configuration		0.5	
1.51	Radius installed & running		1	
1.52	Firewall default chains policy		1	
1.53	Firewall LDAP and RADIUS services on wsc-i-calgary		1	
1.54	Firewall L2TP/IPSec		1	
Total Marks			**30**	

SSC-TASK B: Network

RU-DC				
1.1	Trust Relationship to AE domain	Windows Server 2016	0.40	
1.2	Trust relationship functional test		1.00	
1.3	DHCP configuration		0.50	
1.4	DHCP partnership		0.40	
1.5	DNS on both machines all records front and back		1.00	
1.6	Creation of OU's		0.50	
1.7	Creation of Groups		0.50	
1.8	Creation of Users from spreadsheet		1.00	
1.9	RU-Daclients members, from ru-edge, correct users in all groups		0.50	
1.10	Migrated users		1.00	
1.11	Migrated user files copied with perms		0.50	
1.12	All migrated users there?		0.40	
1.13	DFS namespace & replication		0.90	

RU-Files				
1.14	setup as per diagram	Windows Server 2016	0.50	
1.15	Check disks, RAID array		0.50	
1.16	DC but not GC		0.40	
1.17	Check shares – departments		1.00	
1.18	setup as per diagram		0.50	
RU-ROOTCA				
1.19	CA setup	Windows Server 2016	1.00	
1.20	CA offline		0.50	
RU-SUBCA				
1.21	CA Setup - enterprise sub ca	Windows Server 2016	0.40	
1.22	CA issued by ROOTCA		0.80	
1.23	Template and auto enrollment		1.00	
1.24	CRL		0.50	
1.25	CA Setup - enterprise sub ca		0.50	
RU-CLIENT				
1.26	ping all 'round for firewall rules	Windows 10	0.50	
1.27	joined domain		0.40	
1.28	RSAT tools installed and available		0.30	
1.29	disable first sign on GPO		0.40	
1.30	managers website v1		0.40	
1.31	local admin GPO, import user password		0.60	
1.32	GPO expert		0.50	
1.33	fine-grained passwordv1		0.50	
1.34	fine-grained passwordv2		0.50	
1.35	GPOs non expert		0.50	
1.36	default home page – edge		0.50	
1.37	Home folders csv imported users		1.00	
1.38	project share map		0.50	
1.39	project share perms		0.40	
1.40	Customized error messages		0.60	

1.41	managers website v2		0.40	
1.42	DFS check		0.40	
1.43	visitor user		0.30	
1.44	RU-FILES as NCA (connection assistant) server		0.40	
1.45	connect.russia.net as DA name		0.40	
1.46	DA testing		1.00	
1.47	Customized error messages		0.60	
AE-DC				
1.48	find expert users - moved and in migration folder	Windows Server 2016	0.40	
1.49	expert users all disabled		0.50	
1.50	RDS users		0.40	
1.51	DNS - check records for both websites		0.40	
AE-IIS				
1.52	path of websites	Windows Server 2016	0.40	
1.53	Path and contents of russia website?		0.40	
1.54	certs from RU-SUBCA		0.40	
1.55	path of websites		0.40	
AE-RDS				
1.56	setup as per diagram	Windows Server 2016	0.40	
1.57	RDS installed		0.40	
INET				
1.58	DNS Server "create A-records"	Windows Server 2016	0.40	
AE-Edge				
1.59	RRAS installed - configured?	Windows Server 2016	0.50	
1.60	NAT-port mapping		0.40	
1.61	Site to Site VPN		1.00	
1.62	Site to Site VPN		0.50	
1.63	s2s functional		0.40	
RU-EDGE				
1.64	DA Installed	Windows Server 2016	0.40	
1.65	connect.russia.net as DA name		0.50	

1.66	VPN tunnel?		1.00	
1.67	VPN authentication		0.50	
AE-REMOTE				
1.68	connect to VPN for UAE	Windows Server 2016	0.60	
1.69	connect to AE websites		0.40	
1.70	Joined to domain?		0.40	
1.71	connect to AE websites		0.50	
Total marks			**40**	

SSC-TASK C: Network

Aspect ID	Marking Criteria or Description	Requirement	Max Mark	Mark Awarded
Basic config				
1.1	Hostname	Cisco Routers	0.35	
1.2	Domain name		0.35	
1.3	Local passwords and services		0.40	
1.4	RADIUS Database Remote management		0.40	
1.5	RADIUS Fallback Remote management		0.40	
1.6	Remote management		0.40	
1.7	Local AAA: IOS		0.50	
1.8	Server based AAA		1.00	
1.9	Local AAA: ASA		1.00	
1.10	IPv4 addressing and connectivity		0.30	
1.11	IPv6 addressing and connectivity		0.30	
1.12	Local time assignment		0.30	
Switching				
1.13	VTP Test from SW3 VTP server to SW1 Client	Cisco layer 3 and layer 2 Switches	0.45	
1.14	DTP interface status		0.50	
1.15	Trunk link native VLAN		0.20	
1.16	PAgP		0.50	
1.17	Spanning-tree Mode		0.45	
1.18	STP manipulation: priorities		0.50	

1.19	STP manipulation: costs		0.50	
1.20	STP features: root guard		0.25	
1.21	STP manipulation: portfast		0.25	
Routing				
1.22	EIGRP	Cisco Routers	0.60	
1.23	Routing authentication		0.40	
1.24	BGP		1.00	
1.25	Route filtering		0.50	
1.26	OSPFv2 neighbors		0.50	
1.27	OSPFv3: Neighbors		0.45	
1.28	OSPFv3: DR\BDR		0.45	
1.29	Route redistribution		0.75	
1.30	Policy-based routing		1.00	
Services & Monitoring				
1.31	NAT	Cisco Router and layer 3 switches	0.50	
1.32	GLBP		0.50	
1.33	HSRP		0.50	
1.34	HSRP Authentication		0.30	
1.35	DHCP Reservation		0.50	
1.36	DHCP Client		0.50	
1.37	Syslog		0.30	
1.38	SNMPv2		0.50	
1.39	Configuration backup		0.50	
Security				
1.40	Command privilege levels: user1	Cisco Router or layer 3 switches	0.50	
1.41	Command privilege levels: user2		0.50	
1.42	AAA Role-based CLI: user3		0.50	
1.43	AAA Role-based CLI: user4		0.50	
1.44	AAA Role-based CLI: user5		0.50	
1.45	Port-security		0.30	
1.46	DHCP-snooping		1.00	

1.47	Dynamic ARP inspection		1.00	
WAN & VPN				
1.48	PPPoE	Cisco routers	0.50	
1.49	mGRE: connectivity		0.20	
1.50	DMVPN Details		0.50	
1.51	mGRE: NHRP phase 2		1.00	
1.52	IKEv2 VPN connectivity		1.00	
1.53	IKEv2 VPN traffic		0.50	
1.54	Client-based RA VPN: profiling		0.60	
1.55	Client-based RA VPN: Connectivity		0.50	
1.56	Client-based RA VPN: Split-tunneling 1		0.30	
1.57	Client-based RA VPN: Split-tunneling 2		0.30	
Total			30	

Section D: Instruction for Competitors

- Do not bring any materials with you to the competition.
- Mobile phones are not to be used.
- Do not disclose any competition material / information to any person during each day's competition.
- Read the whole competition script prior to you starting work.
- Be aware different tasks attract a percentage of the overall mark. Plan your time carefully.
- If your virtual machines spontaneously turned off, run slmgr /rearm command with the administrator credentials

Judges Advice Sheet to Competitors

- One reminder to use PPE is permitted before deducting marks
- One warning regarding safe practices permitted before deducting marks
- Grab through to Installation & configuration and testing for >75% - award 2 marks. 50% - award 1 mark. Less than 50% - award no marks.

Section E- Health, Safety and Environment

1. All accredited participants, and supporting volunteers will abide by rules and regulations with regards to Health, Safety, and Environment of the Competition venue.

2. All participants, technicians and supporting staff will wear the required protective Personnel clothing.

3. All participants will assume liability for all risks of injury and damage to property, loss of property, which might be associated with or result from participation in the event. The organizers will not be liable for any damage; however in case of Injury the competitor will immediately inform the immediate organizer for medical attention