Sample Test Project

Regional Skill Competition – Level 3

Skill 39- IT NETWORK SYSTEM ADMINISTRATION

Category: Information and Communication Technology

Table of Contents

Section - A

A. Preface

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 (for IndiaSkills 2018 and WorldSkills 2019):

Competitors born on or after 01 Jan 1997 are only eligible to attend the Competition.

Total Duration: 12 Hrs

Section - B

B. Test Project

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
- Windows and Linux Services

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.

TASK A – NETWORK CISCO INDIA

COMPETITOR INSTRUCTION

You have **4 Hour** to complete this task

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.

Basic configuration

1. Configure hostnames for ALL devices as you see on the topology
2. Configure domain name **India2018.com** for ALL network devices on the topology
3. Create user **India2018** 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)
    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 **India** as a privileged mode password for ALL devices.
    a. Password should be stored in configuration in plain text (not in hash)
    b. Set the mode where all the passwords in the configuration are stored as a reversible cipher text.
7. Create all necessary interfaces, sub-interfaces and loopbacks on ALL devices. Use IP addressing according to the diagram.
    a. Use VSALES01 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 SALES 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 +5) 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 **SInd** as VTP domain name and **2018** as a password. VLAN database on all switches should contain following VLANs:
    a. VLAN 101 with name SALES.
    b. VLAN 102 with name ACCOUNT.

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 Gi0/1-5 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. SALES subnet traffic between HQ1 router and SW3 switch should be forwarded without IEEE 802.1q tag.

Routing configuration

1. Configure EIGRP with AS number 2017 on ISP, HQ1, HQ2, BR2 and BR3 routers according to the routing diagram. Enable routing updates authentication. Use MD5 algorithm with **SIND** 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 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 2017.
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 SALES 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 SALES 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 ACCOUNT 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 SALES subnet. Use internal flash to keep DHCP-snooping database.

4. Turn on dynamic ARP inspection on SW1 for SALES 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. 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.
    a. Use read-only community string **snmp_ro**
    b. Configure device location India-Delhi**, India**
    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

Location for configuration backup files is **/srv/tftp/** on RADIUS server.

TASK B–WINDOWS & LINUX ENVIRONMENT

COMPETITOR INSTRUCTION

You have **4 Hour** to complete this task

In task B you will be responsible for preparing the new domain prior to performing the migration. This will involve building the INDIA.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.

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 INDIA-DC

Install/Configure

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

Active Directory

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

DHCP

- Configure DHCP for the clients
- Mode: Load balancer
- Partner Server: IN-FTP
- State Switchover: 10 minutes
- Scope Range 172.16.1.150-180
- Set the appropriate scope options for both DNS servers and default gateway

DNS

- Configure DNS for INDIA.net
- Create a reverse Zone for the 172.16.1.0/24 network
- Add static records for ALL IN-xx servers

GPO

- Disable "first sign in Animation" on all Windows 10 Clients
- Members of the IN-Experts group must be members of the local admin group on all Windows 10 computers in the domain
- www.INDIA.net must be the default homepage in IE Explorer and Edge browser
- Disable Recycle Bin on the Desktop for all domain users except users in "IN-Experts" Group and domain administrators
- Disable changing the screen saver for all domain users except users in IN-Experts" Group and domain administrators
- Disable changing the background picture for all domain users except users in "IN-Experts" Group and domain administrators
- Redirect (Folder redirection) only for all users in the Expert group "my Documents" and the "Desktop" to INDIA-Files -> d:\shares\redirected
  - share path: \\IN-files.INDIA.net\redirected\%username%
- Create a fine grained password policy required 7 character non-complex passwords for regular users, 10 characters complex password for members of the IN-Experts group

Users/Groups Using PowerShell

- Create OUs named "Expert", "Competitor", "Manager" and "Visitor"
- Create the following AD groups:
  - IN-Experts
  - IN-Competitors
  - IN-Managers
  - IN-Visitors
  - IN-Budget-R
  - IN-Budget-W
  - IN-Intranet-R
  - IN-Intranet-W
  - IN-Logistics-R
  - IN-Logistics-W
  - US-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 IN-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 IN-Users_xx groups, IN-Project_xx groups and OUs
- Create for every user a home drive in on IN-Files d:\shares\users.
- Connect the home drive automatically to drive Z: -> \\IN-files.india.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	IN-Experts; IN-Budget-R
Test_competitor	P@ssw0rd	IN-Competitors; IN-Intranet-W
Test_manager	P@ssw0rd	IN-Managers; IN-Logistics-W
Test_visitor	P@ssw0rd	IN-Visitors

Work Task IN-FILES

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

Install/Configure

- Install a Windows Server 2016 (no GUI) from ISO
- When creating the VM, build with 4 drives
  - 1 System drive (c:\)
  - Size 60 GB
  - 1 Raid 5 array with the remaining three drives (d:\)
    - Size 10 GB in **total**
- Rename to IN-FILES
- Configure the network settings as per configuration table/network diagram
- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to INDIA.net domain

Shares

- Create shares for departments (Competitors, Experts and Managers)
- on IN-FILES -> d:\shares\departments
  - \\IN-Files\Experts --> d:\shares\departments\Experts
  - \\IN-Files\Competitors --> d:\shares\departments\Competitors
  - \\IN-Files\Managers --> d:\shares\departments\Managers
- Create a share for projects in IN-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 (\\in-files.india.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)

DFS

- Create a Namespace with the name “dfs”
- Add IN-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 IN-DC. The shares should be replicated/backed up like this:
  - IN-Files: D:\shares\departments\Experts → IN-DC: C:\backup\Experts
  - IN-Files: D:\shares\departments\Competitors → IN-DC: C:\backup\Competitors
  - IN-Files: D:\shares\departments\Managers → IN-DC: C:\backup\Managers
- Map the department shares depending on the corresponding group (IN-Experts, IN-Competitors, IN-Managers) to drive G: using the DFS Namespace

DHCP

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

DNS

- Host INDIA.net forward and reverse lookup zones

Quota/Screening

- Set the quota to every home drives to 10 GB
- 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”

Work Task IN-WSUS

- Install and configure WSUS Service
- Create GPO for install windows 10 security update on INET

Work Task IN-CLIENT
This is a Windows 10 client in the INDIA.net domain and can be used for regular user or administration of the INDIA.net servers.

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 INDIA.net domain
- Install the RSAT tools for server management
- Use this client for testing the GPO settings

TASK C – WORK ON US.NET

You have 2 **Hours** to complete this task

In Task C 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 US-DC
This is the existing domain controller for the old domain and hosts all the user and group information

Install/Configure

- already preinstalled (domain US.net, user, DNS, DHCP)

Copy Users to india.net

- All user with "Expert" in the "Job Title:" should have duplicate accounts created for them in the INDIA.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 INDIA.net
    - Set the password to "WorldSkills2018mig"
    - Copy the necessary home folders from US-DC to IN-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 (\\IN-Files\migrated$\%username%)
    - Disable the copied users in US.net and move them to a new OU called MIGRATED on US-DC

ACTIVE DIRECTORY

- 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.
    - \\US-DC\bitlocker --> C:\shares\bitlocker

DNS

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

WORK TASK US-WEBSERVER

Configure a HTTP/HTTPS for “www.us.cloud”, which is hosted by. Connect to backends 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 “us.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.ae”
    - Create the appropriate records for email to work
    - Configure a reverse zone

MAIL

- Install Postfix and Dovecot.
    - Configure SMTPS and IMAPS server for "US.cloud" and “competition.ae” domain using certificates
    - 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)

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.us.cloud" domain and “localhost” using certificates
- The website page should display the following message:
  - *“Welcome to the US cloud on [HOSTNAME]”.*
  - Add the hostname dynamically with PHP
- 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 *skill40* with password *Skill40* to 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;
?>
```

LDAP

- Install LDAP service.
  - Configure the directory service of wsc17.cloud.
  - Create users with OU and password specified in the appendix.
  - File Share, Web and Mail services should be available for LDAP users.
  - Create a OU named “wsc-i-london” and use this to grant SSH access to “wsc-i-london”. User not in this group, should be denied access. Root access should not be allowed.
- Create a new second domain “competition.ae”.
  - In this domain create the users as stated in the appendix.

RADIUS

- Install RADIUS service.
  - Use LDAP as the authentication back-end.
  - Add wsc-p-stgallen as RADIUS client and VPN user should be authenticated through this server.
  - Use Skill39 as shared secret

CA

- Configure as CA using OpenSSL.
  - Use /etc/ca as the CA root directory
    - Private key should have minimal permission
  - CA attributes should be set as follows:
    - Country code is set to AE
    - Organization is set to WorldSkills International
    - The common name is set to “WorldSkills 2017 CA”
  - Create a root CA certificate.
  - All certificates required in the test project should be published by CA.

Samba

- Install Samba
  - Authentication is done by wsc-i-calgary. Local users are not permitted
  - Distribute the share “private”, which is used for DFS on wsc-i-london
    - Local data path: /files/samba/private
    - Share is not visible outside the DFS (e.g. \\wsc-i-calgary\private)
  - Make sure no other folders are shared (either visible nor hidden)

WORK TASK US-CLIENT

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 “skill40”.
  - Configure to use user3@us.cloud
  - Send an email to competitor@competition.ae
  - Use IMAP to connect to the mailbox

Web

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

FTP

- Use FileZilla as FTP-client
  - Make sure that a connection to wsc-i-london (ftp.wsc17.cloud) can be established.

Samba

- Make sure that users can access the shares file

E-mail

- Use Icedove as the e-mail client and configure using the user “skill40”.
  - Configure to use competitor@competition.ae
  - Send an email to user3@us.cloud
  - Use IMAP to connect to the mailbox

WORK TASK US-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 US-EDGE
  - Use this client for testing the "external" access to the websites
  - www.india.net and www.us.net

TASK D – INTERNET/VPN/REMOTE ACCESS

You have 2 **Hours** to complete this task

In task D you have to setup remote access to the INDIA.net domain for the clients, Site-to-Site VPN between the two networks/domains and a client VPN solution for the US.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 INDIA.net domain and also for www.US.net and www.INDIA.net websites access.

Work Task US-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 INDIA.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to US.net domain
- Install RRAS service

NAT configuration

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

VPN

- Configure VPN for client access.
- Use the IKEv2 protocol and make sure authentication is done by client certificate
- Use the IP range 172.16.2.200 – 172.16.2.250
- The VPN clients should have access to all internal networks (US.net and INDIA.net)

Site-to-Site VPN

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

WORK TASK INDIA-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 US.net domain.

Install/Configure

- Modify the default Firewall rules to allow ICMP (ping) traffic
- Join to INDIA.net domain
- Install server authentication certificate from IN-DC

Configure Direct Access

- Add US-Client to the AD group "US-DAClients"
- Only members of "US-DAClients" group can use remote connection
- 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.india.net for the access from the internet
- The DA clients must get full access to the resources of INDIA.net network and US.net

Site-to-Site VPN

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

Section – C

C. Marking Scheme

Cisco Environments

Aspect ID	Marking Criteria or Description	Requirement	Max Mark	Mark Awarded
Cisco Environments				
1.1	Hostname		1	
1.2	Local passwords and services		1	
1.3	RADIUS Database Remote management		1	
1.4	Local AAA: IOS		1	
1.5	IPv4 addressing and connectivity		1	
1.6	IPv6 addressing and connectivity		1	
1.7	Local time assignment		1	
Switching				
1.1	VTP Test from SW3 VTP server to SW1 Client	4 Layer 2 Switches	1	
1.2	DTP interface status		1	
1.3	Trunk link native VLAN		1	
1.4	PAgP		1	
1.5	Spanning-tree Mode		1	
1.6	STP manipulation: priorities		1	
1.7	STP manipulation: port fast		1	
Routing				
1.1	EIGRP	Cisco 2900/7200 Series Routers	1	
1.2	Routing authentication		1	
1.3	BGP		1	
1.4	Route filtering		1	
1.5	OSPFv3: DR\BDR		1	
1.6	Route redistribution		1	
1.7	Policy-based routing		1	
Services & Monitoring				
1.1	NAT		1	
1.2	GLBP		1	

1.3	HSRP		1	
1.4	HSRP Authentication		1	
1.5	DHCP Reservation		1	
1.6	DHCP Client		1	
1.7	Configuration backup		1	
Security				
1.1	Command privilege levels: user1		1	
1.2	Command privilege levels: user2		1	
1.3	AAA Role-based CLI: user3		1	
1.4	Port-security		1	
1.5	DHCP-snooping		1	
WAN & VPN				
1.1	mGRE: connectivity		1	
1.2	DMVPN Details		1	
1.4	mGRE: NHRP phase 2 & IKEv2 VPN connectivity		1	
1.5	IKEv2 VPN traffic		1	
1.6	Client-based RA VPN: profiling		1	
1.7	Client-based RA VPN: Connectivity		1	
			40	

Windows Environment Work on INDIA.NET

Aspect ID	Marking Criteria or Description	Requirement	Max Mark	Mark Awarded
IN-DC				
2.1.	Trust Relationship to US domain		1	
2.2	DHCP configuration		1	
2.3	DNS on both machines all records front and back		1	
2.4	Creation of OU's		1	
2.5	Creation of Groups		1	
1.6	Creation of Users from spreadsheet		1	
2.7	Migrated users		1	
2.8	Migrated user files copied with perms		1	
2.9	DFS namespace		1	
2.10	DFS replication		1	

IN-Files				
2.11	setup as per diagram		1	
2.12	Check disks, RAID array		1	
2.13	Check shares – departments		1	
IN-WSUS				
2.14	Installing WSUS		1	
2.15	Configuring WSUS		1	
2.16	Updating Security Updates		1	
IN-CLIENT				
2.17	ping all 'round for firewall rules		1	
2.18	joined domain		1	
2.19	RSAT tools installed and available		1	
2.20	disable first sign on GPO		1	
2.21	local admin GPO, import user password		1	
2.22	GPO expert		1	
2.23	fine-grained password policy p1		1	
2.24	default home page – edge		1	
2.25	Home folders csv imported users		1	
2.26	connect.india.net as DA name		1	
2.27	DA testing		1	
IN-EDGE				
2.28	DA Installed		1	
2.29	VPN tunnel?		1	
2.30	VPN authentication		1	
		Total	**30**	

WORKING ON US.NET

Windows and Linux Environment

Aspect ID	Marking Criteria or Description	Requirement	Max Mark	Mark Awarded
US-DC				
3.1	find expert users - moved and in migration folder		1	
3.3	expert users all disabled		1	

3.4	RDS users		1	
3.5	DNS - check records for both websites		1	
US-WEBSERVER				
3.6	Webserver application		1	
3.7	Forwardzone: competition.ae		1	
3.8	Forwardzone: us.cloud		1	
3.9	A records for us.cloud		1	
3.10	CNAME (www, ftp, files and mail)		1	
3.11	DNS Reverse		1	
3.12	Mail directory		1	
3.13	Mail directory		1	
	SMTPS e IMAPS		1	
US-LDAP				
3.14	LDAP User not local		1	
3.15	CA Configuration		1	
3.16	Radius		1	
US-Client				
3.17	Firefox website		1	
3.18	India website files		1	
3.19	FileZilla connection		1	
3.20	Samba		1	
3.21	IMAP Client		1	
US-Edge				
3.22	RRAS installed - configured?		1	
3.23	NAT-port mapping		2	
3.24	Site to Site VPN		2	
US-REMOTE				
3.25	connect to VPN for US		1	
3.26	Joined to domain?		2	
3.27	connect to US websites		1	
		Total	**30**	

Section - D

D. Infrastructure List

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

Configuration Table

Hostname	Operation System	Domain	IP Address(es)	Preinstalled
IN-DC	Windows Server 2016 GUI	INDIA.net	172.16.1.2/24	Yes - configured
IN-FILES	Windows Server 2016 GUI	INDIA.net	172.16.1.3/24	NO
IN-WSUS	Windows Server 2016 GUI	INDIA.net	172.16.1.4/24	Yes - configured
IN-EDGE	Windows Server 2016 GUI	INDIA.net	172.16.1.250/24 172.16.1.100/24	Yes - configured
IN-CLIENT	Windows 10	INDIA.net	DHCP	Yes - configured
IN-REMOTE	Windows 10	None	DHCP	Yes - configured
INET	Windows Server 2016 GUI	None	172.16.3.2/24	Yes – configured

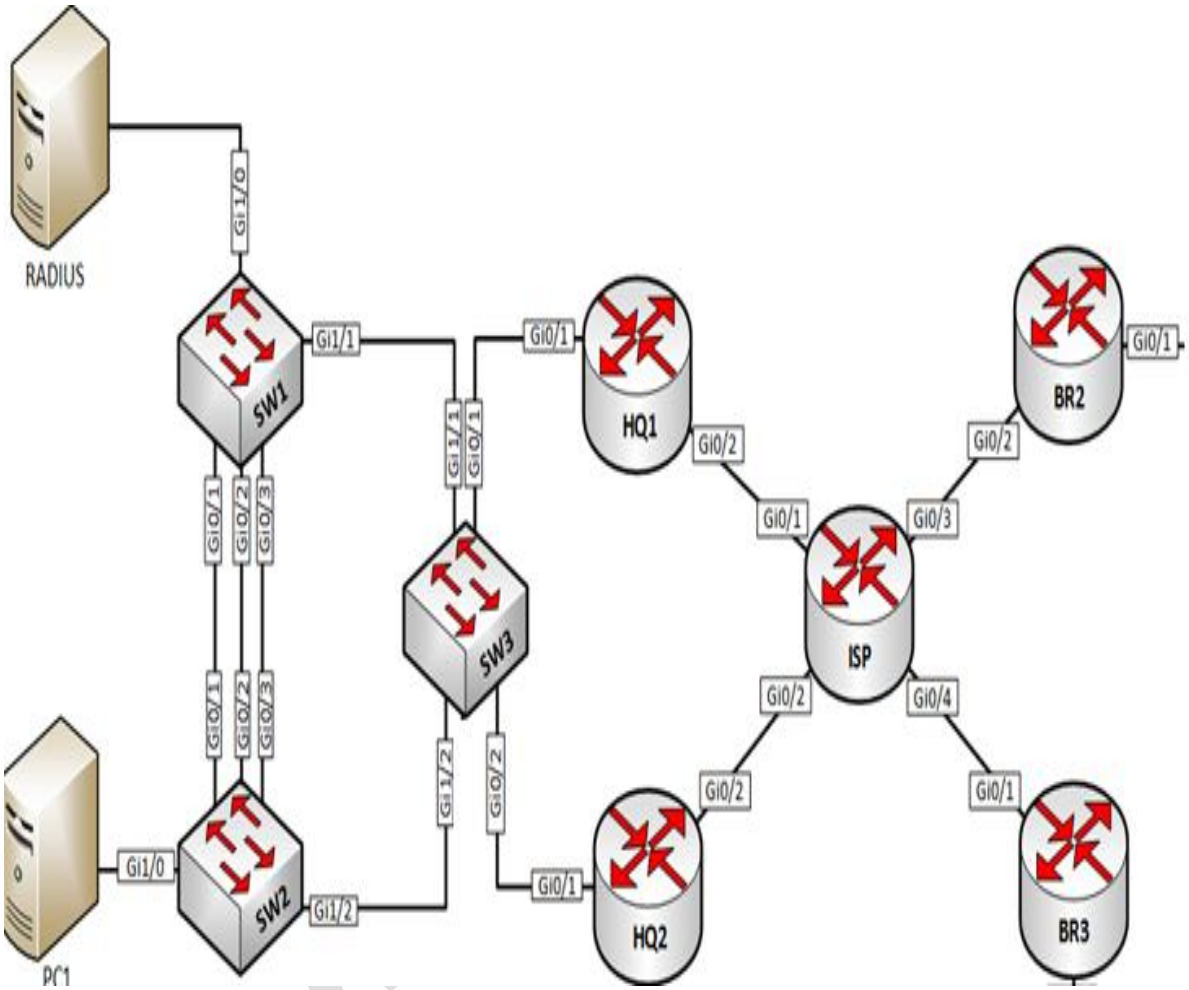
Machines indicated as being preinstalled with "**Yes – configured**" will have the operating system installed and Hostname and network settings configured.

Shares/Permission Table

Share name	Location	Read access group	Read/Write access group
Budget	IN-Files -> D:\shares\projects	IN-Budget-R	IN-Budget-W
Intranet	IN-Files -> D:\shares\projects	IN-Intranet-R	IN-Intranet-W
Logistics	IN-Files -> D:\shares\projects	IN-Logistics-R	IN-Logistics-W

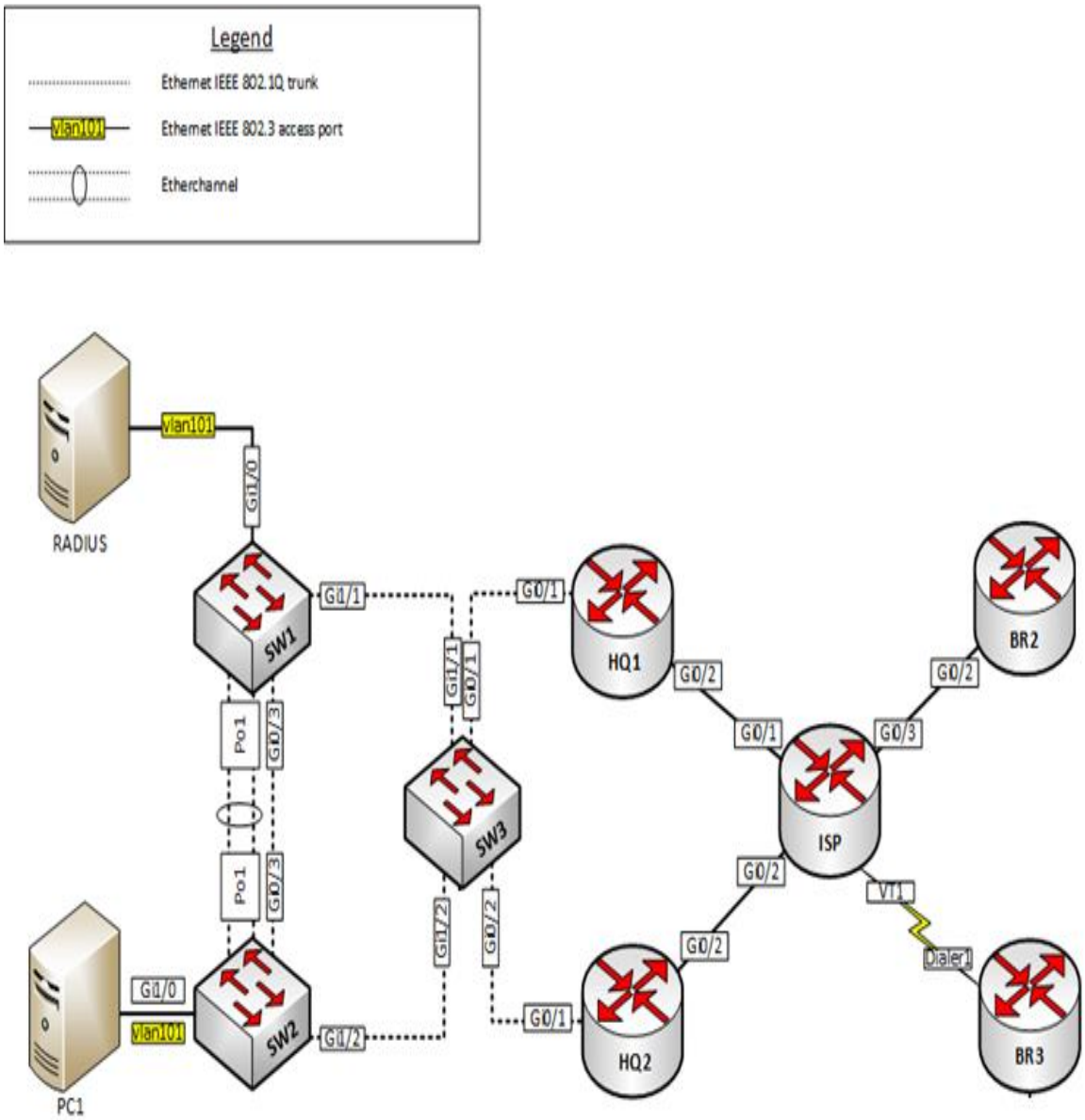
Network India

L1 Diagram



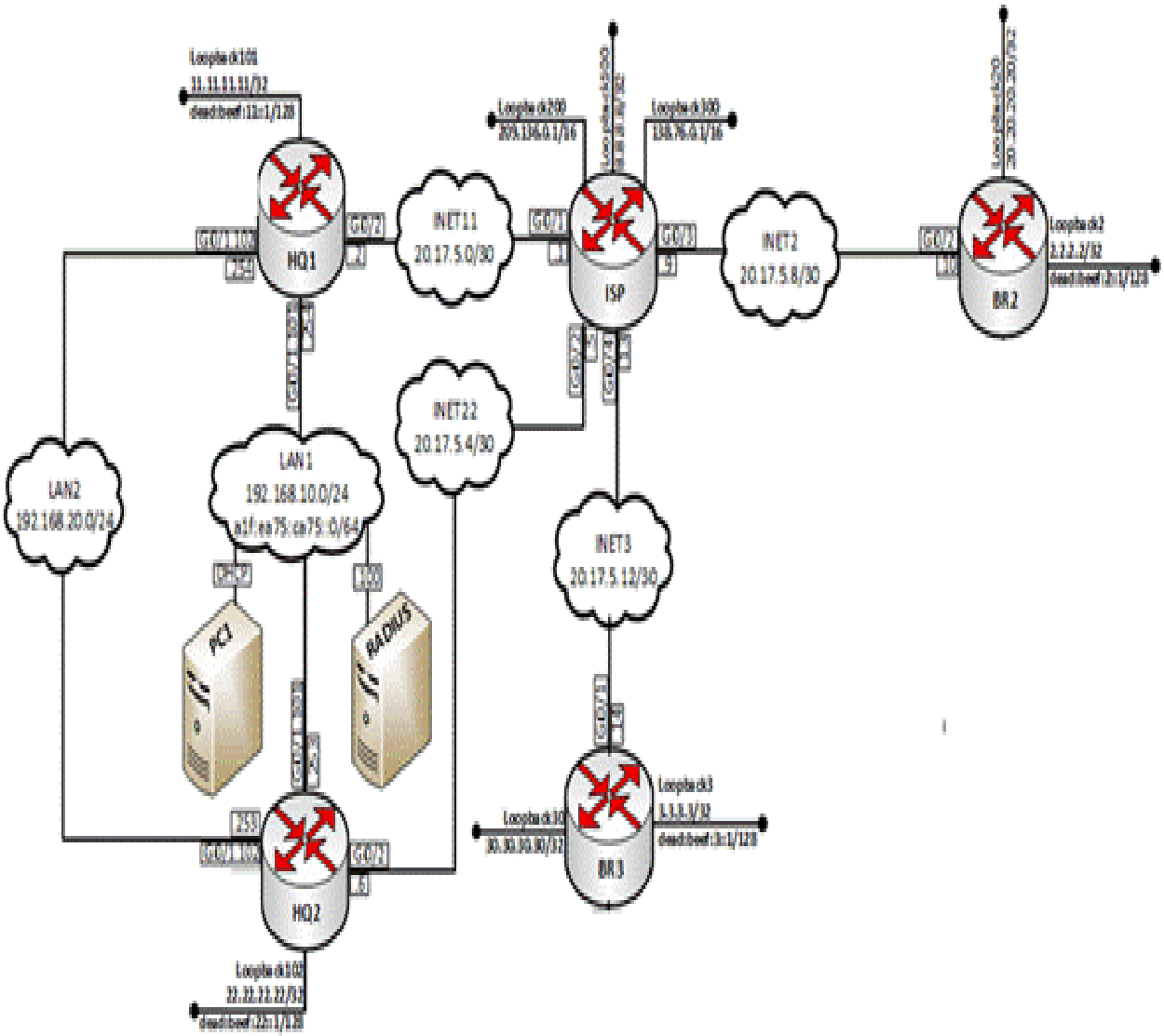
Network India

L2 Diagram



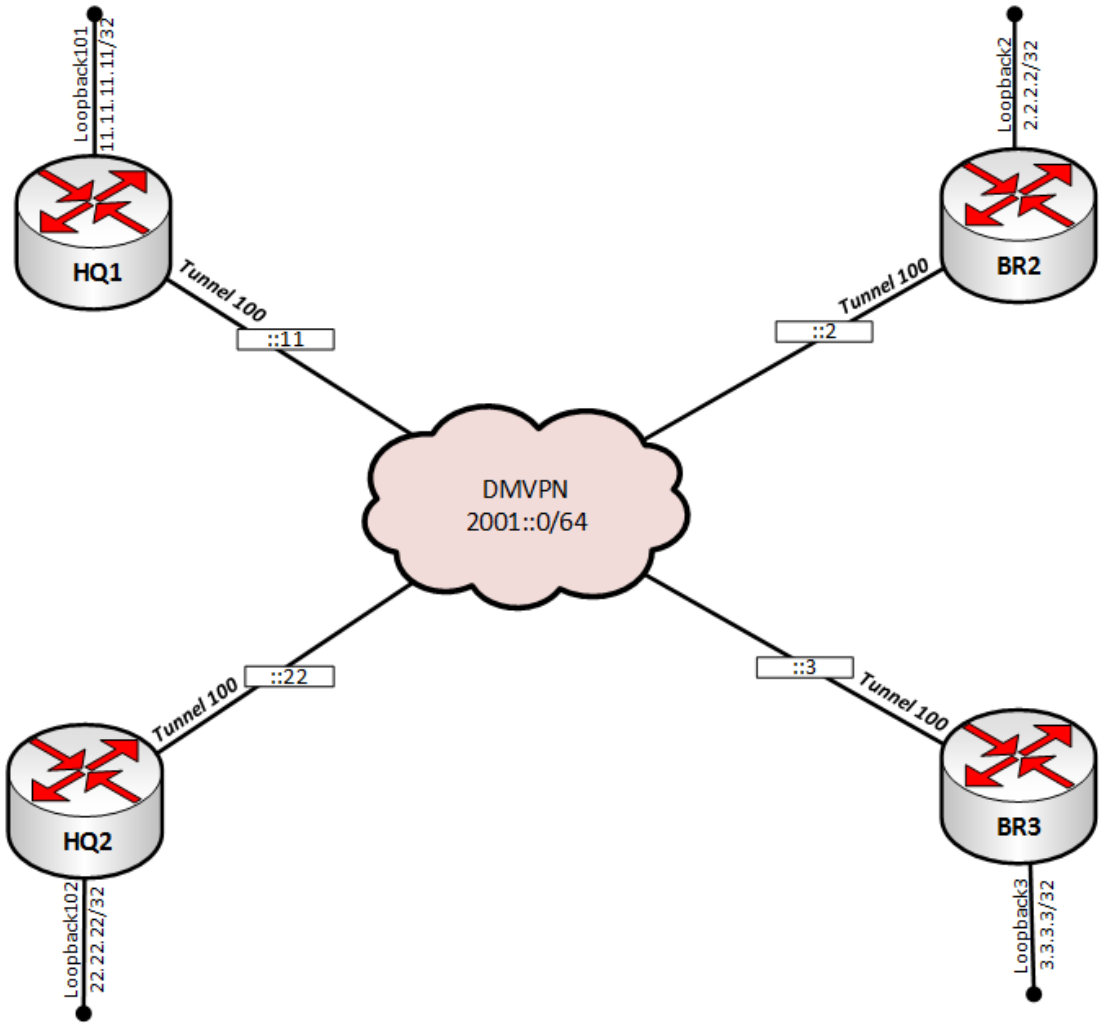
Network India

L3 Diagram



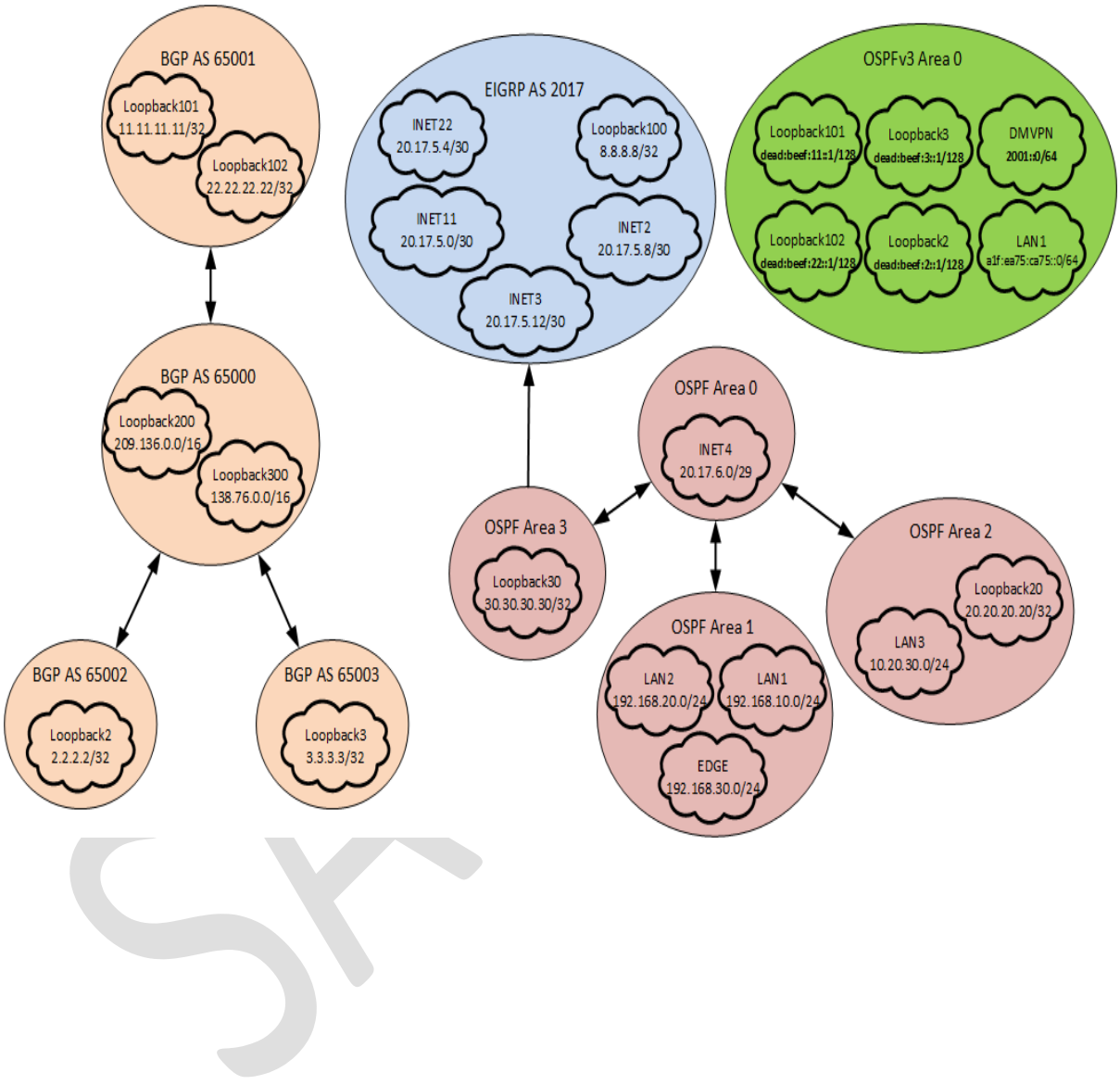
Network Diagram

WAN & VPN



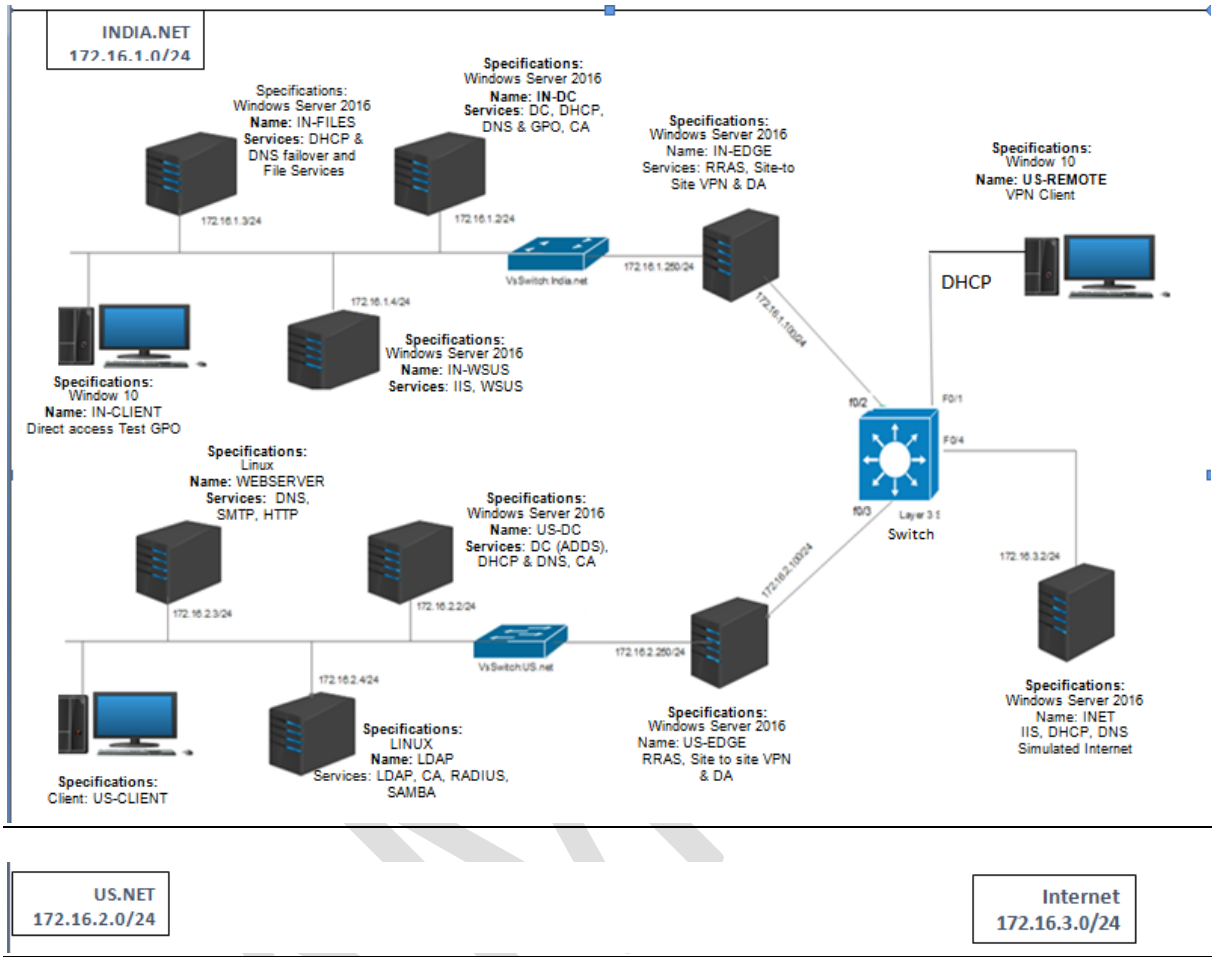
Network India

Routing Diagram



WINDOWS and LINUX Environment

Network Diagram



Equipment & Machinery

Item Description (Standard/Administration-PC)	Number per competitor
Cisco Router 2800/2900 Series	5
Cisco Layer 3 Switch	4
Cross Cable (Cat 5E)	10
Straight through Cable (Cat 5E)	7
Console Cable	5

System Configuration (Standard/Administration-PC)	Number per competitor
Intel i5 processor	2
16 GB RAM	
500 GB SSD-Drive	

24 inch LED-Monitor	
US Keyboard	
Mouse	

System Configuration (High Specification/ Server or Host-PC)	Number per competitor
Intel i7 Processor	1
64 GB RAM	
1 TB SSD-Drive	
24 inch LED-Monitor	
US Keyboard	
Mouse	

Installations and Materials Required

Item Description (High Specification/ Server or Host-PC)	Number per competitor
Windows Server 2016 Standard Edition/Data Center Edition (OS)	1 (License)
Windows 10 OS	2 (License)
Putty.Exe	1
Linux OS (REDHAT)	3
RSET tools	1
Excel file for the user import (India-Users.xlsx)	1
Websites for install o Manager Website o www.INDIA.net Website	1

Section – E

E. Instructions for candidates

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.

Internet Access Rules

- You will have access to internet per module 10 minute except design modules
- Access will be subject to availability of Internet System
- 10 minutes to be utilise at stretch.
- You cannot copy, write from internet machines to your workstation.
- You are not permitted to use any communication application e.g. Chat, Facebook, WhatsApp etc.

Module Rules

- When you have finished the current module, you can proceed to the requirements for the next module.
- Competition Test Project will be in English language

Infrastructure Rules

- Any hardware failure during the completion may get extra time subject to approval of Jury/Experts.
- Candidates should not carry any devices, cell phones, material at competition desk.

Rules of competition

- Competitor will be disqualifying for any misbehaviour.
- All the rights of the competition are revered with State Skill Competition Committee.

Section – F

F. Health, Safety, and Environment

- All accredited participants and supporting volunteers will abide by rules and regulations with regards to Health, Safety, and Environment of the Competition venue.
- All participants, technicians and supporting staff will wear the appropriate / required protective Personnel clothing.
- 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.
- For any electrical or technical support contact the expert/supervision staff.
- Do not plugin/plugin out any eclectic & electronics connections, seek for assistance.
- Be careful while working on workstation so that feet should not strike to electric board or CPU system.